Pirati na mreži

Kultura elektronskog kriminala

Naslov: **Prati na mreži, Kultura elektronskog kriminala**

Urednik: **Centar za nove medije_kuda.org**

Edicija: kuda.read

Izdavač: **Futura publikacije**, Novi Sad

ISBN 978-86-7188-101-2

Prevod sa nemačkog jezika: Relja Dražić, Dragan Prole, Rade Pujin

Lektura: Branka Ćurčić, Relja Dražić

Dizajn: NinjaBoy Creations i kuda.org

Štampa: Daniel Print, Novi Sad

Urednik knjige:
kuda.org
Braće Mogin 2, PO Box 22
21113 Novi Sad, Srbija
tel/fax: +381 21 512 227
mail: office@kuda.org
url: http://www.kuda.org

Izdavač:
Futura publikacije
Dr Zorana Đinđića 1
21000 Novi Sad, Srbija
tel: +381 21 450 023
mail: dracos@ptt.yu

Prati na mreži
Kultura elektronskog kriminala

Sadržaj

Kultura elektronskog kriminala

Pirati na mreži

Predgovor

"Treba li možda da napravimo jedan prokleti website?", pita Robert de Niro u mafijaškoj komediji "Čista stvar živaca", iznerviran, kada su njegovi momci od njega zahtevali reforme. De Niro, koji je decenijama bio nešto poput našeg čoveka u mafiji, u tom filmu iz 1999. godine iznenada postaje čangrizav. Vremena su se promenila, davno isprobane strukture porodičnog klana deluju antikvarno u odnosu na umreženo društvo.

I s one strane filmskog platna dugo se probijalo saznanje, da se u dvadeset i prvom veku kriminal sve više događa na mreži. Pritom se naravno ne radi o mafijaškim porodicama sa vlastitim *website*-ovima. Žedni senzacija i zasnovani na oskudnom poznavanju stvari, izveštaji tradicionalnog medijskog prostora, poput holivudske fabrike snova, odviše često se služe oblikovanjem sličnih klišea. Umesto organizovanih kriminalaca, kao univerzalan obrazac neprijatelja sve više i više se pojavljuju genijalni pojedinačni počinioci, koji vrlo rado dobijaju i paušalnu oznaku *hacker*-a.

Umesto da se dalje trudimo oko tog odviše loše istošenog pojma, ova knjiga želi da se detaljno posveti supkulturama elektronskog kriminala, koja u metežu nastalom oko velikih *hacker*-a često preti da dospe u zaborav: programerima virusa, onima koji ilegalno kopiraju, onima koji "provaljuju" zaštitu od kopiranja, *Script*-deci ovog sveta. Šta njih nagoni da to rade? Kako oni opravdavaju svoj čin? Kakav odnos oni neguju prema suprotnoj strani, prema proizvođačima antivirusnih softvera, prema programerima zaštite od kopiranja i prema progoniteljima koji surfuju? A kakav uticaj ima njihovo delovanje na razvoj interneta, na *mainstream* kulture na mreži? Radi odgovora na to pitanje za knjigu "Pirati na mreži – Kultura elektronskog kriminala" čitav niz stručnjaka smo zamolili da se posveti specifičnoj supkulturi.

Valja primetiti da se pritom ne radi o tome da se opravdaju zakonski prekršaji. Ali, muzička berza razmene Nepster (Napster) napokon pokazuje, da su varljive granice između ilegalnosti i kulturalne inovacije. Iz struktura razmene i muzičke piraterije, ona se razvija u prostore *chat*-ovanja i BBS-sistema, tako da je u međuvremenu i od strane Intelovih stručnjaka za razvoj shvaćena kao negativ budućnosti interneta. Bernard Ginter (Bernhard Günther) je u svom tekstu uverljivo naznačio razvoj te situacije pokazujući pritom, da su pirati i ranije u mnogim stvarima već prednjačili svom vremenu. Uz to, Dejvid Mek Kendls (David McCandless) nas obaveštava o opijenosti koju pri svom činu osećaju oni koji "rasturaju" ilegalno kopirane sofvere i o njihovoj igri mačke i miša sa privatnim detektivima velikih *software* koncerna.

"Gubitnici" elektronskog kriminala o kojima se radi u ovoj knjizi ne moraju samo da se bore sa kaznenim pravom. I od strane etablirane *hacker*-ske zajednice oni često žanju samo pogrdne reči. Boris Grendal (Boris Gröndahl) se stoga posvećuje hakerskoj etici i pokazuje da su takva ograničenja uvek bila samovoljna konstrukcija. Kretanje u otežanim pojmovnim frontovima moglo bi doneti i sukobljavanja u pogledu DeCSS i SDMI – ovde se ipak i univerzitetski profesori pojavljuju kao *cracker*-i u klasičnom smislu, jer svojim *hack*-ovanjem oni istovremeno brane i pravo na slobodno izražavanje mišljenja. Poneki *Telepolis*-članci poslednjih meseci dovoljno temeljno dokumentuju takav razvoj stvari.

U prilog svom delovanju, pravo na slobodno izražavanje mišljenja reklamiraju i programeri virusa. Janko Retgers (Janko Röttgers) dokumentuje tu protivrečnu scenu i pritom nudi pregled istorije kompjuterskih virusa. Peter Milbauer (Peter Mühlbauer) opisuje recepciju epidemije virusa iz *cyber* prostora i povlači paralele sa Aids-debatom, te sa strepnjom od kulturalne dekadencije. Armin Medoš (Armin Medosch) prati fenomen da pogrešna upozorenja od virusa i sama mogu postati jedna vrsta virusa, te da je *hoax* često daleko više od loše šale. Florijan Šnajder (Florian Schnieder) dobijao je veoma često neželjenu poštu, što koristi kao povod da podrobnije izvesti o istoriji i uzročnicima svakodnevne plime *spam e-mail*-ova.

U svom izveštaju o info-ratu, Ralf Bendrat (Ralf Bendrath) pretpostavlja jednu sasvim drugačiju supkulturu. S one strane svih javnih upozoravanja na *cyber*-teroriste, pre svega se kod američkih borbenih snaga uigravaju strategije, čije su granice bliske elektronskom kriminalu. Nasuprot njima, često se kao učesnici u info-ratu ističu oni počinioci koji su sasvim bezazleni, poput *Script Kiddies* i *Web-Graffiti* grupa, kao što je pokazao Armin Medoš u svom tekstu o mladim *hacker*-ima.

Uprkos tome, *Mafia-boys* i *Coolios cracker*-skog sveta u štampi i politici sa velikom pravilnošću podižu visoke talase. Tada se govori o "internetu kao prostoru slobodnom od autorskih prava". Uz pomoć stava da bi u tom nekontrolisanom, slobodnom prostoru naposletku sve moralo biti uklonjeno, projektuju se drakonski zakoni i iznuđuju se sudski slučajevi koji nastoje da točak vremena vrate unatrag, želeći da na internetu zabrane ono što je u stvarnom svetu opšte prihvaćena sloboda. Kristijana Šulcki-Haduti (Christiane Schulzki-Haddouti) stoga se osmelila da ode u slobodne digitalne luke, u zone necenzurisane i nenadzirane komunikacije koje su stvorili angažovani programeri koji vole slobodu. Već danas ti programeri operišu u sivim zonama prava. Ukoliko se nastavi trend koji ide ka potpunom nadziranju mreže, i ove zone bi uskoro mogle potpasti pod polje elektronskog kriminala.

Da bismo to sprečili, prevashodno nam je potrebna tematska, informacijama potkovana debata o činjeničnim opasnostima od umrežavanja našeg društva. Kao časopis kulture na mreži, Telepolis je sebi propisao zadatak da doprinese toj debati utoliko što na takozvane "mračne strane" interneta baca pogled bez predrasuda.

Armin Medoš i Janko Retgers
Berlin/London, juni 2001

1. Pirati u carstvu podataka

Od zlata Inka do duhovnog vlasništva
Istorija jedne drske metafore

Pirati

Bernard Ginter

Oni su nevidljivi. Oni su svuda. Oni menjaju svet.

Kada bi tako glasio reklamni slogan, naredna istorija pirata bila bi producirana za bioskopsku publiku. Ipak, jedino što su fabrikanti snova pronašli u toj istoriji jeste naslov: "Piraterija", prašnjava čarobna reč iz holivudskih starinskih kovčega, u jednom nejednakom duelu treba da pripomogne pružajući više razgovetnosti. U ulozi pozitivca vide se predsedavajući predsedništva, predstavnici za štampu i advokati "kopirajt industrija" (Copyright Industries) - pre svih ispred diskografskih kuća, filmskih studija i proizvođača *software*-a. Uloga negativca – sa kojom nisu računali ni iskusniji studijski bosovi – pripada publici. Industriji zabave se čini da je radnja jedan popriličan horor-trip. Radi borbe protiv vlastite ciljne grupe "Copyright Industries" su se odlučile za "proklinjanje pirata". Ta medijska strategija, čini se, do daljnjeg dobro funkcioniše; od feljtona do tabloida sa velikom samorazumljivošću se pronalaze udarni naslovi à la "Record Moguls Take On Pirates" (1) ili "Kako duh postaje plen" (2). Ipak, malo podrobniji pogled u vlastiti filmski arhiv trebao bi da upozori "Copyright Industries" da na taj način junake bivših blagajničkih šlagera proglašava neprijateljima.

Buntovnici platna

Od bioskopskih početaka pa do šezdesetih godina dvadesetog veka, piratski film bio je jedan od najprisutnijih žanrova. Jedriličari izvan zakona decenijama su ubirali najveće simpatije i donosili su najveće "kvote" filmskoj industriji. Kapetan Kuka, Gospodar sedam mora, Crveni korsar, Kapetan krv, Kraljica pirata, kako god da su se svi oni zvali, sa svojim piratskim storijama navodno su pogađali nerv publike. Kao zastrašujuća slika pirati su svakako pre funkcionisali na dečijem programu – a čak ni tamo ne stvarno: okretni Kapetan Kuka koji u *Disney* crtanom filmu Petar Pan iz 1950. godine tako rado svira čembalo, skoro da i nije prikladan za demonizovanje. Tačno pedeset godina kasnije, on će se mnogo bolje držati od samog Petra Pana. Jer mladić koji nije želeo da odraste, u ekranizaciji Stivena Spilberga (Stephen Spielberg) sa Dastinom Hofmanom (Dustin Hoffman) i Robinom Vilijamsom (Robin Williams) (1991), preobrazio se u ostarelog advokata sa čirem na želucu. On dobija

svoju poslednju bitku protiv naslovnog junaka Kuke samo uz pomoć mnogih specijalnih efekata. Piratska pesma iz ekranizacije *Disney* iznosi privlačnu ambivalentnost predstave o piratu:

> A pirate's life is a wonderful life
> You'll find adventure and sport
> But live every minute
> For all that is in it
> The life of pirate is short. (3)

Onda su u večernjem programu holivudski pirati sa svom jasnoćom stali na pravu stranu: hrabri, slobodni pljačkaši oduzimaju korumpiranim Špancima u 15. i 16. veku pjastere i dublone (španski kovani novac – prim.prev.) koje su ovi oteli od Indijanaca; plemeniti Korsari neljudsku englesku mornaricu u 18. i ranom 19. veku podučavaju boljim formama ophođenja; neustrašivi narodni junaci uspevaju da posada tvrđave pohlepnih zavojevača konačno izvuče deblji kraj. Šema klasičnog piratskog filma je jasna: figure sa kojima se publika identifikuje su Erol Flin (Errol Flynn) i Bert Lankaster (Burt Lancaster) u borbi protiv moćnika – a nipošto španski kapetani, guverneri i zatvorski nadzornici.

Junaci u penziji

Isplati se baciti pogled na kraj ere piratskog filma. U poznim pedesetim godinama čini se da je žanr postepeno bio nadmašen – musketari plašt-i-mač filmova su zajedno sa piratima završili u arhivima istorije filma; kauboji su jahali još neko vreme, a agenti tajnih službi, čovečuljci sa Marsa&Co. postepeno su preuzeli filmsko platno. To nije slučajno. Kada se 1958. godine jedna horda pirata prepadom luksuzne američke jahte pobrinula za naslovne stranice, to je bio istinski izuzetak (ironijom slučaja vlasnik jahte za koju su se čakljom zakačili pirati pred ostrvima Galapagosa, svoj novac je prevashodno zarađivao kao advokat filmske industrije). Ipak, svet je uzaludno gledao na gore: Boing 707 je apsolvirao svoje prve letove, degradirajući moćne okeane na isušeni međuprostor između kontinenata. Pre svega je baš Sputnjik leteo preko Nju Jorka. Da bi prihodi Ujedinjenih Nacija preko velikog mora bili *up-to-date* morali su proširiti pirateriju i na avione – upravo 1958. godine. Tamo stoji:

> "Piraterija je svaki nezakoniti čin nasilne aktivnosti, lišavanja slobode ili pljačkanja koji je počinjen radi privatnih svrha od strane posednika ili saputnika privatnog broda ili privatnog aviona protiv nekog drugog broda ili aviona, ili je počinjen osobama ili vrednostima koje su se nalazile na palubi: a) na otvorenom moru, b) na mestima koji leže iznad visinskih nadležnosti države." (4)

Poslednja rečenica deluje zaista proročanski. Naročito nakon što je Sputnjik, kao što je poznato, imao naknadnu epizodu: kakon što je minuo prvi šok Amerikanaca, odlučno su

doterani planovi za uspostavljanje novovrsne vojne komunikacione mreže. U kategoriji "izvan visinskih nadležnosti države" za svetska mora, vazdušni prostor i svetski prostor sebi je dosledno prokrčio put onaj konkurent koji je danas zadužen za piratsku romantiku: internet.

Od magneta blagajni do neprijatelja

Umesto reklamnih tekstova o spektakularnom povratku buntovnika, na "anarhističkom" internetu su se mogla zapaziti drastična upozorenja od strane vlasnika izdavačkih prava. "Piraterija" je strateška, marketinška ključna reč, na osnovu koje "Copyright Industries" žigoše lakoću, sa kojom se na internetu digitalno može kopirati, širiti i razmenjivati, kao ugrožavanje napretka i kulture. Pritom doduše nema direktnog govora o "nasilnoj aktivnosti, lišavanju slobode ili pljačkanju" iz definicije Ujedinjenih Nacija, ali i drugačije se retko završava. Konačno, to ne pripada ni redovnim piratskim storijama. Već oko 1700. godine, pri operi o morskim pljačkašima "Störtebeker" Rajharda Kajzera (Reinhard Keiser), krv je iz punih svinjskih mehura pod pritiskom prskala daske Hamburške pozornice (5). A ono što su mogli staronemački operski kompozitori, u mnogo većoj meri može današnja industrija zabave. Profesionalne lobi grupe koje operišu širom sveta poput Motion Picture Assotiation (MPA), Recording Industry Assotiation of America (RIAA), International Federation of the Phonographic Industry (IFPI), Business Software Alliance (BSA) i nekolicina drugih sebi su eksplicitno propisali "borbu protiv piraterije". Jedna proba čitanja sa početne stranice *website*-a RIAA, zastupnika interesa američke diskografske industrije, pokazuje sa kojom jednoznačnošću se pirateriji u međuvremenu pripisuju jedino demonizujuće asocijacije – više nema ni traga od poletnog buntovništva starih filmova o morskim razbojnicima:

> "Današnje pirate više ne karakterišu crne zastave sa mrtvačkom glavom i ukrštene kosti, nema kuka, topova ili bodeža. Ne vidi se kada oni dolaze; ne postoji nijedan znak upozorenja na pramcu. Ali, budite sigurni da su pirati tu – jer se danas može podići svaka količina zlata (i platine i dijamanata). Današnji pirati ne operišu na morskoj pučini, vać na internetu, u ilegalnim štamparijama CD-ova, u poslovnim centrima i na ulici. Kredo pirata još uvek je isti: zašto platiti kada se tako jednostavno može ukrasti? Kredo je toliko pogrešan kao što je oduvek bio. Krađa je nezakonita, neetična, ali je u današnjem digitalnom dobu nažalost previše raširena. Zbog toga se RIAA i dalje bori protiv muzičke piraterije." (6)

Malo manje promišljeno, International Federation of the Phonographic Industry (IFPI), objašnjava šta za nju znači piraterija:

> "Izraz piraterija načelno označava namernu povredu izdavačkih prava u komercijalnim razmerama. S obzirom na muzičku industriju, ona se odnosi na nedozvoljeno kopiranje." (7)

U rat protiv kopiranja odlučno polazi i industrija zabave, čiji model poslovanja se zasniva na kopiranju. Već u doba muzičkih kaseta nije se moglo prečuti raspoloženje diskografske industrije koje je govorilo o propasti sveta. U starom holivudskom maniru, u borbi protiv kopiranja je do danas govor o borbi dobra protiv zla. Džej Bermen (Jay Berman), predsedavajući IFPI, na to je manje osetljiv:

> "Krađu duhovnog vlasništva podržavaju kriminalne organizacije. Ona hrani trgovinu drogom i druge teške prekršaje." (8)

No, samo sa tim za sada nema promena: internet adrese Nepstera, MPS.com i ostalih firmi koje su optužene od strane muzičke industrije završavaju se sa .com za "komercijalno" - a ne sa .co za Kolumbija. Ali, u tekstu predsedavajućeg IFPI dalje stoji:

> "Današnja borba protiv muzičke piraterije jeste borba protiv ogromnog, organizovanog, ilegalnog internacionalnog preduzeća. Toj borbi naša industrija posvećuje velike resurse, ali nam je podrška vlasti preča od svega ostalog. Nama su potrebni stroži zakoni i njihovo efektivno provođenje. Nijedna vlada na današnjem globalnom tržištu sebi ne može dozvoliti da prosto posmatra kako joj piraterija upropašćuje privredu, pljačka njenu kulturu i šteti njenom međunarodnom ugledu." (9)

Edgar Bronfmen (Edgar Bronfman), vrhovni menadžer Universal-a, a time i gospodar jedne od najvećih *copyright* imperija sveta, istu opasnost objašnjava zakonodavcima na svoj način:

> "Za razliku od Božijih darova i darova prirode, ono što je slobodno samo je stoga slobodno, što je neko drugi za to platio. Poštenje i pravednost omogućili su našem civilizovanom društvu da preživi i da napreduje, dok se društvo naših saveznika Sovjetskog Saveza raspalo, raskomadalo i razorilo zato što je pokušalo da održi jedan društveni poredak koji je bio duboko nepošten i nepravedan." (10)

Istorija državnih neprijatelja

Odsustvo skrupuloznosti i zlatoljublje klasični su sastavni delovi crno-bele slike o pirateriji. Međutim, u doba istorijskih morskih razbojnika, oba momenta, pre svega, opisivala su način ponašanja zvaničnih moćnika. "Zlato je nešto izvrsno. Sa zlatom se može sve što se poželi na ovom svetu. Pomoću zlata se duše čak mogu odvesti u raj" (11) – tako piše u pismu svojim španskim vladarima ništa manje nego Kristofer Kolumbo (Christopher Columbus). Drugačije rečeno: kada bi se radilo samo o novcu, osim pirata bi se sasvim lako mogli potražiti i drugi junaci. Ipak, poređenje morskih razbojnika sa moćnicima vodi upravo ka izvorima piraterije.

Svetska mora su najpre korišćena kao ekskluzivno vlasništvo najmoćnijih država. Kada je obznanjeno da je Kolumbo 1492. godine otkrio zemlju na zapadu Atlantika, dve najveće pomorske sile tog vremena – uz posredovanje Pape – brzo su se dogovorile oko podele: nehrišćanske zemlje zapadno od demarkacione linije u Atlantiku (oko 311. stepena geografske dužine) treba da pripadnu Španiji, a istočno odatle Portugaliji. Nakon tog sporazuma iz Tordesilje (1494), usledila je odgovarajuća podela Pacifičkog okeana u Saragosi 1529. godine – ponovo kao vlasništvo Španije i Portugalije. Obe države su marljivo izgradile svoju trgovačku moć: Portugalija je monopolizovala trgovinu između Indije i Evrope, španski konkvistadori su brutalno upali u Srednju Ameriku i najveći deo Južne Amerike, načinivši od tamnošnjih resursa zlata motor španske privrede.

Igru monopola dve rimsko-katoličke svetske sile, sve ostale vlade najpre su ostavile netaknutom. Prvi ko je prestao da naprosto začuđeno zuri u monopolizovanje bio je jedan privatni preduzetnik: francuski trgovac i brodovlasnik Žan Ango (Jean Ango) poslao je više jedrenjaka u potragu za legendarnim brodovima koji su transportovali zlato; piratu Žanu Fleriju (Jean Fleury) pošlo je za rukom da Caru Karlu V preotme nekoliko španskih brodova sa zlatom i da blago Acteka 1522. godine preusmeri ka Dipu. Radost u Francuskoj bila je velika, a postepeno je i na nivou evropskih vlada rastao otpor protiv špansko-portugalske podele sveta. Ubrzo nakon Angoove privatne inicijative, francuski kralj je, visoko službeno, osorno postupio prema jednom španskom izaslaniku:

> "Sunce sija za mene kao i za sve druge. Ja bih rado video klauzulu u Adamovom testamentu, prema kojoj sam ja isključen iz podele sveta." (12)

Pedeset godina kasnije. Poluprivatno, polu uz blagoslov svoje kraljice, britanski mornar Frensis Drejk (Francis Drake) napada Panamu, zaposednutu od strane Španaca. Slobodni pljačkaš iz ostrvskog carstva koje je ranije bilo nevažno, postaje 1572. i 1573. godine užasni uljez španske vlade – a nacionalni heroj usahnule Engleske. Sa dva mala jedrenjaka i oko sedamdeset ljudi, Drejk je mesecima unosio nesigurnost na obalama dominantne sile svog vremena. Poređenja radi: kada je petnaest godina nakon toga Španija nastupila protiv tog Engleza koji je predstavljao sve veće opterećenje, to se desilo sa 130 brodova i trideset hiljada ljudi. Španci su imali svoju armadu koja je izazivala strahopoštovanje: džinovska plovila sa visokim katarkama, teške stotine tona, impozantne kao i nezgrapne. Englezi su imali brze jedrenjake kojima se lako moglo upravljati, naoružane sa dalekometnim topovima.

Lope de Vega je kao mladi pesnik bio svedok uništenja armade od strane engleske flote (1588). Iz španske perspektive prikazao je Drejka kao zmaja apokalipse. Nasuprot tome, savremeni engleski izveštaji nemaju problema sa Drejkovom borbom protiv moćnih država, naprotiv:

> "Kao što postoji boginja osvete koja potajno prati počinioce zla i stara se o tome, da oni, premda ih niko nije optužio, ne izbegnu svoju pravednu kaznu, tako postoji i jedna vrsta protivljenja koja se nalazi duboko u grudima svih onih kojima je počinjena nepravda, a oni će sa svim sredstvima koja im stoje na raspolaganju pokušati da se osvete za pričinjenu nepravdu. Utoliko se čini da vode veoma opasan kurs za svoju sigurnost i svoj mir svi veliki i moćni ljudi koje je izvanredni posed zaveo, pa su postali drski, te čine nepravdu svojim potčinjenima i zbog toga ih još i preziru." (13)

Na strani moći

Podsećanja radi: iz ekonomske perspektive je upravo današnja muzička industrija tipičan primer moći. Pogotovo pošto je branša nosača zvuka preuzela ulogu onoga ko utire staze, putem nekoliko spektakularnih procesa koji su postali obrasci "Copyright Industries" na internetu, naredno razmatranje će se skoncentrisati na tu oblast. Ekonomska karakteristika broj jedan: neobična oligopolitička koncentracija tržišta. Jednom je upravo pet preduzeća – koja su odavno pregovarala, da bi se putem *merger*-a (postupak kupovine deonica korišćen od strane kompanija za širenje njihovog posla i uvećanje profita – prim. prev) redukovala na četiri – vladalo je nad oko osamdeset procenata svetskog tržišta nosača zvuka. Karakteristika dva: veoma visoka "vertikalna integracija". Od ugovorno licenciranog *copyright*-a preko studija za snimanje, štampe, marketinških odeljenja i pogonske mreže, pa do velikih prodavnica CD-ova – u ekstremnom slučaju celokupna proizvodnja vrednosti završava u kasi jednog jedinog preduzeća – uz razliku od nekoliko centi materijalnih troškova plus jedan do dva eura za muzičare i trgovačku maržu prodavnice, minus porez na dodatu vrednost. Lanac stvaranja vrednosti koji iziskuje strahopoštovanje. Džinovsko plovilo sa visokim katarkama, teško stotine tona, impozantno kao i nezgrapno. Za razliku od njega, novodolazeći imaju brze jedrenjake kojima se lako moglo upravljati, naoružane dalekometnim topovima. A industrija zabave iz svoje perspektive prikazuje internet kao zmaja apokalipse.

Muzička industrija reaguje na nov izazov

Već odavno se dobro uočavaju napadi svih vrsta od strane solidno zidane tvrđave industrije bazirane na *copyright*-u. "Piratski proizvodi", naknadno proizvođenje trgovinske robe zaštićenih marki, patenata ili autorskih prava dugo je poznato kao kažnjiva delatnost. Spektar seže od dirljivo pogrešno napisanih imena robnih marki na smešno jeftinoj kineskoj opremi za džoging, pa do zaplenjenog vagonskog skladišta falsifikovanih roleks časovnika koje je demonstrativno spljošteno parnim valjkom, opkoljenim novinarskim fotografima.

I "Piratske radio stanice" su jedan stari borbeni pojam u bogatom rečniku vlasnika autorskih prava. U tom slučaju se na strani "pirata" mogu jasno pročitati (pozitivno interpretirani) motivi klasične piraterije – poput neprihvatanja postojećih odnosa moći ili snabdevanje sa dobrima i uslugama nezavisno od dotada uobičajene kontrole. "Piratska himna" britanske scene piratskih stanica osamdesetih godina prošlog veka

izražava uverenost i istrajnost sa kojim su entuzijasti piratskih stanica delimično doneli licencirani slobodni radio. Time postaje razjašnjeno i ono obeležje "piratske scene", koje je bilo odgovorno za to, da mnogi pirati ultrakratkih talasa brzo pređu na internet i postanu pioniri digitalnog presnimavanja muzike (14): brzina sa kojom su prepoznavali praznine u ponudi postojećih distributera – "trude se najviše što mogu da uskrate slušanje muzike" – i dospevali do tržišta za odgovarajuću muziku, "samo zato što sviramo ono što ljudi žele da čuju". Evo par odlomaka, uz to se misli na relaksirani *Jamaica-Sound*:

"Them a call us a pirates.
Them a call us illegal broadcasters
Just because we play what the people want.
so them a call us pirates.
Them a call us illegal broadcasters.
DTI try stop us, but they can't.
(...) If they brught down one we build five more strong.
They're passing laws,
They're planning legislation,
Trying their best to keep the music down.
DTI why don't you live us alone,
We only play the music others want.
One station, it couldn't run England.
Two station, they couldn't run England.
Three station, they could not please the nation.
Everybody want to listen to the free station." (15)

"Muzička piraterija" progonjena je još pre vremena interneta, a odnosila se na ilegalno kopiranje muzike zaštićene autorskim pravima različitog reda veličina – od "piraterije školskog dvorišta" – što je izraz za razmenu individualno presnimljenih muzičkih kaseta među drugovima iz razreda – preko rukotvorine pune međusobno povezanih kasetnih dekova u malom studiju, pa do visoko industrijske, ali ipak ne i ugovorom licencirane proizvodnje CD-ova u jednom od "piratskih gnezda" na Dalekom Istoku. Uprkos tih strategija u ophođenju sa piraterijom svih vrsta, ipak nije bila očekivana aktuelna medijska slava stare metafore za morske razbojnike.

Sve do sredine devedesetih godina internet je odbijan, odnosno ignorisan kao sporedni medijum za frikove. Za samouverene procene od strane muzičke branše, pobrinule su se, između ostalog, spore dial-up veze ranih godina i oskudnost muzičkih lista na FTP serverima i ostalim "piratskim sajtovima" koje gotovo da se i nisu mogle dovesti u sklad sa šarolikim marketinškim svetom velikih preduzeća. Kada je interes za muziku na internetu postao nepregledan, vlasnici autorskih prava najpre su plaćali nešto novca pri pokušaju da kratko i jasno zabrane muziku na internetu.

Nakon toga proklamovan je cilj, da se rad pirata tehnički i pravno značajno oteža. Mašinama za traženje – poput neskromnog "MP3-vuka", kako je nazvan softver u upotrebi nemačkog Društva za naplatu GEMA (16), povrede prava su trebali biti uočljive i u skladu sa tim pravno gonjene. Naredni korak – nalazimo se otprilike u zimi 1988/1999 – bio je uvid, da na internetu nema razvoja bez vlastite, legitimne ponude muzike. Početkom 2000. godine datira pokušaj da se pod naslovom koji dobro zvuči, "Rights Protection System", postavi internet filter oko cele Nemačke; prema predstavama nemačkog IFPI, jedna baza podataka upravljana od strane carinskih vlasti trebala je da odredi koje internet adrese bi mogle biti pozivane iz Nemačke.

Dodatno je usledila i PR ofanziva koja je ciljala na to, da slušaoce muzike osvesti o problemu i o njihovoj krivici. Istovremeno je inicijativa nemačkog IFPI, "Kopiranje ubija muziku", reklamirala izreku koja se ne može održati uz pomoć analize "deset hiljada kopiranih CD-ova uništava jedan mladi demo bend". Nakon nekoliko meseci, internet *site* koji je izvrgavan ruglu ponovo je bio *offline*. Takozvani konzumenti očevidno su mnogo radije govorili o muzici i nisu pokazivali naročito mnogo razumevanja za teškoće koncerna. Njihov sledeći partner u obraćanju bio je zakonodavac. Naročito oko nastanka Digital Millenium Copyright Act (DMCA) u Sjedinjenim Američkim Državama i "Pravne smernice za harmonizovanje autorskih prava i srodnih prava zaštite u informatičkom društvu" Evropske Unije (1997-2001), stavljen je u pogon zavidan trošak za lobiranje, da bi perspektive pogođenih industrijskih grana što je moguće dalekosežnije mogle da budu uvedene u novo zakonodavstvo. Godine 1999/2000 počeo je novi veliki poredak dotičnih sudskih procesa u SAD; mnoga preduzeća muzičke industrije zahtevala su spektakularne sume od novih "Music Service Providers" MP3.com i Nepstera.

Doduše, to su bili tek prvi obrasci procesa koji su doveli do toga da slučaj "muzička industrija versus pirati" postane trajna tema udarnih naslova. Početkom 2001. godine, medijska hipersenzibilisanost je toliko napredovala da su čak i rutinska obelodanjivanja relativno normalnih godišnjih rezultata u branši nosača zvuka vodila ka stotinama naslova à la "Nepster pritiska prodaju CD-ova". Kada je početkom 1999. godine prodaja CD-ova povećana oko osam procenata, predstavnici za javnost RIAA i IFPI žurili su da načelno relativizuju iskaznu moć brojeva (17). Još jedan primer za usijanu poker-atmosferu godine 2001: mobilna telefonija je jedna od malobrojnih oblasti nove mreže komunikacija, u kojoj su još uvek formulisana optimistična prodajna očekivanja – međutim, uprkos atraktivnoj muzičkoj ponudi za nove korisnike mobilnih telefona, obznanjeni su sledeći preuveličani proračuni: "Melodije na mobilnim telefonima koštaju muzičku industriju milion dolara dnevno" (18).

Naredni elementi uobičajene anti-piratske retorike: kompleksno sažimanje celokupnih interesa u okruženju autorskih prava šematski je redukovano na suprotstavljanje dva protivnika. Male, slabe "Copyright Industries" na jednoj strani i velike, proždrljive Telekom-industrije na suprotnoj strani. S jedne strane, o odnosu ta dva učesnika na tržištu svakako već postoji manje napadnih analiza à la "Content is not king" (19), s druge strane, 38,5 milijardi dolara godišnjeg prometa branše nosača zvuka ne predstavlja tričariju. Utoliko

više energije troši industruja zabave na predstavu o vlastitoj nekoristoljubivosti. Jedna tipična formulacija takve argumentativne strategie iz usta Tomasa Štajna (Thomas Stein) kao menadžera Bertelsmann Music Group: “Lako se može reći da tako velike firme već mogu oprostiti nekoliko eura, što je duboko pogrešno! Poenta je da je umetniku naposletku najteže, jer on ništa ne zaradi.” (20)

Među umetnicima koji se bore protiv takvog tipa naplaćivanja, svakako se nalaze Prins (Prince) i Kortni Lov (Courtney Love). Ipak, naprosto ima zvezda koje internet vide isto kao i njihovi izdavači, potpisuju peticije ili čak šalju na internet advokate u potragu za piratima – na primer Žan-Mišel Žar (Jean-Michel Jarre), Smudo iz Fantastične četvorke (popularni nemački rok&roll bend – prim.prev.), hard rok bend Metalika (Metallica) i Bečki filharmoničari. Pritom je vredno zapaziti, zbog čega se upravo zvezde zalažu za snažnu kontrolu interneta – drugačije formulisano – za koliko neznatni procentni udeo muzičara, merila koja rezultiraju iz autorskih prava uopšte dosegnu značajnu korist. “Hit lutrija” muzičke industrije gotovo da i nema više od dva do tri procenta dobitnika. Većina izdatih albuma pravi gubitak (odnosno služi kao vizit karta), ostatak biva prevashodno iskorišćen za to, da se uigraju enormni marketinški troškovi. Usled ugovora koji su po pravilu nepovoljni, umetnicima ostaje veoma malo; finansijski dobici iz posla sa nosačima zvuka za veliki deo muzičara su potpuno nerealni; mnogi za to plaćaju. Zbog toga je dohodak od autorskih prava koji brani industrija za većinu autora isto tako neautorski kao što je Inkama moglo biti svejedno, da li će blago koje su im oduzeli Španci završiti u Madridu, Dipu ili na dnu mora.

Paljba na “Copyright Industries”

“Piraterija je kada se delo jednog umetnika krade bez namere da se za njega plati. Ja pritom ne mislim na bilo koji *software* à la Nepster. Govorim o ugovorima za albume sa najvećim izdavačima” (21). Pevačica Kortni Lov nipošto ne spada u one koji bi autorska prava smatrali suvišnim. Pre će biti da ona detaljno računa koliko daleko su samostilizovani lovci na pirate i čuvari autorskih prava udaljeni od fer isplate autorima.

Umetnici su se udružili u “Recording Artists Coalition” da bi konačno dobili bolje uslove ugovora (22). Dvadeset i osam saveznih država SAD podigli su optužnice protiv muzičke industrije zbog ilegalnog osporavanja cena u slučajnu preskupih CD-ova (23). Evropska Komisija preduzela je prve korake u pravcu jednog antimonopolskog zakona protiv muzičke industrije. Porodice nekoliko žrtava masakra u Kolubajnu podigle su optužnice teške pet milijardi dolara protiv dvadeset i pet firmi koje pripadaju industriji zabave (tu su, između ostalih Nintendo, Sega, Sony i Time Warner); prigovor glasi da se bez kreiranja proizvoda sa nasiljem i seksom - amok-napad (reč potiče sa Dalekog Istoka, a odnosi se na nekontrolisano ispoljavanje ubilačke agresije posle koje počinioci po pravilu izvršavaju samoubistvo – prim. prev.) obojice igrača video igrica ne bi ni dogodio (25). Gotovo istovremeno jedna studija, naručena od Vlade SAD, proziva produkciju ploča zbog nasilja u “lirskim” tekstovima (26). Kao što je rečeno, klasični sastavni deo crno-bele slike o

pirateriji su zlatoljublje i beskrupuloznost. A oba elementa postaju istinski, trajni deo imidža današnjih lovaca na pirate.

Naprednost istorijskih pirata

O piratskom kapetanu iz ranog osamnaestog stoleća, Hauelu Dejvisu (Hovell Davies), sačuvana je uspomena da je svoju posadu nakon borbe prizivao pameti: oni nisu postali pirati zbog naklonosti prema tuči, već da bi se osvetili krvožednim trgovcima i okrutnim zapovednicima brodova (27). Kapetan Semjuel Belami (Samuel Bellamy), sa nadimkom “Govornik”, pokušao je 1716. godine da nagovori jednog kapetana zaplenjenog trgovačkog broda na saradnju, da pređe na stranu pirata. Nije došlo do sporazuma, pa Belami drži govor:

> “Meni je žao to što Vi nećete ponovo da preuzmete Vašu jedrilicu; meni nije stalo do toga, da bilo kome pričinim štetu, ako od toga neću imati koristi; do đavola sa jedrilicom, moramo je potopiti, a Vi ste je mogli učiniti korisnom. Uprkos tome, Vi ste jedan licemeran pas, isto kao i svi oni koji prihvataju da budu potčinjeni zakonima, a od njih su bogati ljudi načinili svoju vlastitu zaštitu – jer ti kukavni psi nisu imali hrabrosti da na drugačiji način brane ono što su stekli svojim nepoštenjem – ali neka ste svi vi zajedno prokleti: moja kletva se odnosi na tu gomilu prepredenih mrcina i na Vas koji ste sebe stavili u službi kretena pilećeg srca. Vi od nas pravite nitkove, bez najmanje uzdržanosti, a pritom je jedina razlika to što Vi pljačkate siromašne pod skutom zakona, a mi uzimamo od bogatih pod zaštitom naše vlastite hrabrosti. Nije li bolje da postanete jedni od nas, umesto da radi zaposlenja pritrčavate tim varalicama?”

Kada je kapetan na to odgovorio da mu savest ne dopušta da krši Božije i ljudske zakone, Belami nastavlja:

> “Vi ste proklete mrcine-savesti, a ja sam slobodni princ, i ja imam puno pravo da celom svetu objavim rat, kao što bilo ko drugi ima pravo da na moru ima stotine brodova a na kopnenom bojištu stotine hiljada ljudi; a moja savest kaže: ah, zbog čega diskutovati sa tako plačljivim psetom koji bilo kojem pretpostavljenom dozvoljava da ga prema trenutnom raspoloženju počisti preko palube.” (28)

“Piratska republika” kao prethodnica socijalne države

Sredina sedamnaestog stoleća. Državni pravni sistemi baziraju se na zlostavljanju i smrtnoj kazni. Poredak u vojsci, državnim službama i u radionicama bio je ekstremno hijerarhizovan, prilikom kažnjavanja se postupalo bez oklevanja. Na dnevnom redu bili su ratovi.

Istovremeno, kod pirata u Zapadnoj Indiji – na Haitiju i Tortugi – postojali su regulisano pravo na osiguranje, zapisan pravni sistem i oblik vladavine koji je po mnogo čemu bio

više demokratski nego što je bio slučaj u tadašnjim vladama. Postojala je jedna zajednička kasa za zdravstveno i socijalno osiguranje. Plen je između svih (uključujući i kapetana) bivao pravedno podeljen.

Poređenja radi: državna mornarica je svoje ljudstvo neretko regrutovala uz pomoć kidnapovanja, a obične mornare najčešće uopšte nije plaćala. Nakon pokušaja bega usledile bi neljudske kazne. Plata mornara je i na trgovačkim brodovima bila neznatno mala, a disciplina nemilosrdna. Kod Korsara koji su se, na osnovu gusarske povelje, za razliku od jednoznačnih piratskih brodova uvek mogli predstavljati kao politički legitimna jedinica za napad, kapetan je od plena zadržavao četrdeset puta veći udeo od svoje posade. Konačno, nezavisni pirati su u isto vreme imali jedan značajno drugačiji model poslovanja. Kapetan broda morskih razbojnika dobijao je najviše dvostruko više od svojih saboraca. Prava i dužnosti bili su regulisani putem ugovora koji je važio za sve. (28)

Istoričar Klajv Senior (Clive Senior) rezimira: "U poređenju sa dogmatizmom svog vremena, pragmatizam pirata se mora naprosto pozdraviti." (29) Dakle još jednom: šta čini pirate simpatičnim? U metafori o pirateriji tokom različitih vekova se oblikovala ideja o tome, da ljudska zajednica ne fukcioniše uvek na najbolji mogući način – i da se protiv toga nešto može učiniti.

Sa koje pozicije "pirati" operišu danas?

Pokušaji IFPI, RIAA itd., da pirate razgovetno učvrste u blizini organizovanog kriminala, imaju jednu začkoljicu. Oni podržavaju utisak da industrija još uvek nije shvatila internet. Internet, Silikonska dolina i nova ekonomija kao propadajuća sovjetska imperija? Milione korisnika Napstera oni tretiraju kao narko-mafiju? Teško se zaboravljaju dramatična poređenja Džeja Bermana i kolega o odlučujućem kvalitativnom skoku ka današnjoj "pirateriji" kao masovnom fenomenu. Nije da nema industrijske "piraterije" velikog stila, ilegalna postrojenja za preštampavanje CD-ova su odavno gonjena od strane industrije, a nipošto nisu nestala sa ovog sveta. Ali današnje polazno stanovište o "internet-pirateriji" ipak je potpuno izokrenuto: uznemiravajući utisak, da se u klasičnom muzičkom poslovanju radi još samo o novcu, za kritičnu masu fanova muzike postaje okidač "piraterije u malom formatu". Trijumfi "Copyright Industries" u sudnici imaju svoje naličje u kidanju niti koja spaja predstavnike prava sa njihovim mušterijama. Koji ljubitelj muzike ima razumevanja za to, da najveći izdavač, Universal, za svaki pojedini CD koji je bio dostupan na sajtu my-MP3.com treba da dobije dvadeset i pet hiljada dolara od MP3.com – pogotovo, kada je na pitanje, koliko će od milionske sume pripasti njemu kao muzičaru, Piter Gebrijel (Peter Gabriel) mogao odgovoriti samo na sledeći način: "Do sada nisam sreo muzičara koji je dobio nešto od toga. Dokle god muzičari ne budu dovoljno pametni da se udruže i da zajednički deluju, ponovo će prolaziti isključivo loše." (31) Milijarda dolara koju je Napster radi poravnanja ponudio izdavačima – sa ukazivanjem na promet te branše od trideset i osam i po milijardi dolara godišnje – od strane "Copyright Industries" bila je odbijena kao od šale. Ukratko: čini se da se "legalni" deo muzičkog poslovanja vrti samo oko komercijale – a ujedno novac biva

revalorizovan u istinski novac koji je u igri putem razobručene prljave borbe sa zahtevima za prava, milionskim potraživanjima i preuveličanim proračunima. Za mnoge fanove to je dobrodošla prilika da se jednom pokuša bez novca.

Razvoj "muzičke piraterije" na internetu

Usled velike količine podataka još se čini da je "filmska piraterija" na internetu nerealna. Ta oblast je ipak žestoko napadnuta, počev od 1999. godine kada je mnoštvo *hacker*-a krekovalo CSS-zaštite DVD-filmova. Da bi digitalizovana filmska traka mogla da se odmotava ne samo na Apple-sistemu i PC-sistemu, nego i na Open-Source Linux-u, samosvojna industrijska zaštita od kopiranja stavljena je izvan snage. Od tada besni ogorčena borba – između ostalog o tome, u kojoj meri se ovde radi o (u mnogim državama dozvoljenom) reverzibilnom inženjeringu (Reverse Engeering), a u kojoj o prostoj povredi autorskih prava (32).

Borba protiv "softverske piraterije" ima nešto dužu tradiciju. Bussines Software Alliance (BSA) na svojoj austrijskoj web stranici navodi 1996. godinu kao početak borbe protiv pirata (33), nemačka BSA uprkos svoje kampanje-straha ("Svi imate razloga da budete nervozni"), 2001. godine konstatuje boom internet-piraterije i obelodanjuje 533 mirujuća sajta (34). Warez-scene (ilegalno kopiranje software-a, termin nastao u USA poznih sedamsedetih godina – prim.prev.) koje na duge staze nisu podsticane komercijalom već strašću, ukazuju na onu oblast u kojoj su internet-pirati načinjeni medijskim zvezdama, oblast prema kojoj filmska i *software*-ska piraterija deluju kao bagatela: muzičke fanove na internetu.

Sa početkom osamdesetih godina, muzička industrija je u akciji velikih razmera prebacivala posao za konzumente u digitalnu formu. CD (kompakt disk), kao sledbenik LP (longplej ploče) još uvek je bio shvaćen kao fizički nosilac podataka i isto tako malo je čuvan od kopiranja kao i analogna vinilska ploča. Naučnici na Fridrih-Aleksander univerzitetu u Erlangenu su u isto vreme, od 1987. godine na tamnošnjem Fraunhofer-Institutu za integrisane ploče (IIS-A) razvili komprimovanje digitalizovanih zvukova. Erlangenški tim je unutar Moving Pictures Expert Group (MPEG) postao vodeće pero u razvoju "MPEG Audio Layer-3", ukratko: MP3, u internacionalnim standardizovanim oznakama. Izvorni *encoder* bio je mali i komplikovan za korisničku upotrebu – a širio se eksplozivno. Naredni programi koji su vrlo brzo kursirali Shareware, bili su CD-Ripper koji je audio podatke sa nosača zvuka kopirao na hardisk. Sa jeftinom raspoloživošću CD-rezačima i CD-romovima na kojima se mogao unositi zapis, otpala je i poslednja barijera koja je sprečavala identično umnožavanje digitalnih nosača zvuka bez gubitka kvaliteta, što je postao raširen fenomen. Ali pre svega, to je omogućilo internetu da tako nastale kolekcije fajlova svih vrsta i bez fizičkog transporta podataka objedini u respektivne nosače zvuka. Postoji sve više programa koji muzičkim fanovima omogućavaju da preko interneta dođu do muzike.

Gigantska zajednica koja više nije bila upućena na školsko dvorište da bi razmenjivala kasete, započela je na internetu živu diskusiju u vezi sa muzikom. Uskoro su se lokalne piratske stanice sa ultrakratkih talasa prebacile na Real Audio Stream. Od 1996. godine,

postojala je Internet Chat Groups (IRC) koja je sebi pripisala širenje MP3 fajlova. Muzika je brzo našla put od korisnične mreže do WWW, od tekstualne naredbe do grafičke korisničke površine, od specijalnog znanja do masovnog fenomena. Sve više su programi nalik *browser*-ima nudili pristup muzici; inspirisan IRC-om i MP3-mašinama za pretragu, mladi student Šon Fening (Shawn Fenning) je u januaru 1999. godine u igru uveo istinsku "Killer Application". Kada je startovala beta-verzija njegovog *software*-a, Napster na download.com, odmah je u maju 1999. godine osnovao Napster.com i tako dao podsticaj strmoglavoj karijeri Peer-to-Peer (P2P) menjanju *file*-ova.

Muzičkoj industriji su bili potrebni meseci da bi samo primetila novinu. Slušaoci su utoliko brže reagovali: prema studiji firme PC Pitstop (koja nije iznosila neodmerene podatke) u jesen 2000. godine *software* je već bio instaliran na gotovo svakom trećem personalnom računaru priključenom na internet. Prema podacima firme, na Napster je istovremeno pristupalo do milion korisnika. Poređenja radi: kao najveći servis provajder na svetu AOL (America On Line) u vreme najveće posete na mreži, istovremeno gotovo da i nema više do 1,5 miliona korisnika (35). Na pozadini snažno centralizovane muzičke branše orijenstisane prema objektima i još uvek nadasve masovne legalne ponude muzike na mreži, naredne P2P platforme su rasle kao pečurke posle kiše – Gnutella, Scour, Mojo Nation & Co. a sledeće iznenađenje sigurno tek dolazi.

Ako ne možeš da ih pobediš...

> "Internet menja naš život, menja radno vreme prodavnica, menja sve. Za muzičku industriju internet ima ujedno i prednosti i mane, s jedne strane, muzika je, pored slika, jedini medijum koji se odmah može konzumirati putem interneta. Time su prednosti i mane u jednakoj meri povezane. MP3 će za muzičku industriju postati jedan veoma, veoma prikladan, verovatno futuristički instrument, da naše proizvode iznesemo na tržište." (36)

Još jednom je to bio Tomas Štajn iz Bertelsmann Music Group, iz ranog perioda pozitivnih reakcija početkom 2000. godine. Pola godine kasnije već je bilo obrnuto. 31. Oktobar 2000. - doba je neizvesnih sudskih postupaka protiv Napster-a, MP3.com i protiv drugih skraćenica starog načina trgovine. Bertelsmann AG, jedan od najvećih zastupnika autorskih prava na svetu, održava konferenciju za štampu. Pored Bertelsmanovih menadžera sede predstavnici ljutih neprijatelja. Šon Fening i Henk Beri (Hank Berry), osnivači i poslovođe Napster-a. Moglo se dogovoriti o jednoj strateškoj alijansi, ali Bertelsman je želeo da preuzme veći deo Napster-a:

> "Razmena podataka od osobe do osobe razigrala je imaginaciju miliona ljudi putem svoje jednostavnosti, izbora mogućnosti sadržaja iz celog sveta i putem svih aspekata jedne zajednice. Napster je ukazao put jedne nove vrste distribucije muzike, a mi u njemu vidimo osnove važnog i podsticajnog modela poslovanja za muzičku industriju. Pozivamo druge diskografske kuće, izdavače, umetnike i ostale učesnike u industriji da sarađuju na razvoju jednog sigurnog i na članstvu baziranog servisa." (37)

Kako će pokazati naredni meseci, dovesti muzičku industriju na zajednički (piratski-) kurs nije jednostavan posao. A kako se podnose profitni interesi industrije sa okretnošću pirata?

Piraterija kao posao

Engleski kralj Henri VIII, 1547. godine prima od bankarske kuće *Fugger* jedan kredit: 400.000 karolus guldena – bogatstvo – uz kamatnu stopu od 12%. Druge bankarske kuće se žale. Za tih neverovatnih 48.000 guldena godišnje bilo bi, konačno, lako opremiti piratske brodove, koji bi sumu kredita za kralja vrlo brzo sakupili u Ermel kanalu. Više ne treba previđati: istinski pirati su velike trgovačke kuće. Bankari u pozadini, oni koji još nikada nisu stupili na palubu broda, rade sa kalkulabilnim dobitkom koji njima, kao investitorima, donosi morsko razbojništvo. Naravno, ujedno na enormnim premijama zarađuju i osiguravajuća preduzeća, a i špedicije na visokim otpremnim troškovima.

U Francuskoj, podela marži od piratskih dobitaka najčešće je slično funkcionisala, sve do duboko u osamnaesti vek. Konzorcijumi brodovlasnika i investitora koji su morsko razbojništvo otkrili kao isplativ posao, plaćali su kralju nekoliko procenata poreza, a zauzvrat su dobijali gusarsko pismo koje im je davalo punomoć da pljačkaju brodove neprijateljskih zemalja, ovlašćujući tako pirate koji su za političko pokrivanje leđa zauzvrat smeli da zadrže jedan mali udeo plena. Kod Henrija VIII iz takvog razvoja stvari rezultira prvi zakon protiv piraterije; dodatno je jedan odgovoran viceadmiral ovlašćen za prekidanje posla sa piraterijom (38).

Sporedni efekti borbe protiv piraterije

Brojne firme čekaju, spremne da zarade mnogo novca posredstvom zahteva za sigurnost, zaštitu od kopiranja i nadziranja. "Tehničke mere" i "Informacije za razumevanje prava" koje su opraštajuće EU-Pravne smernice 2001. godine u međuvremenu decidirano stavile pod pravnu zaštitu, postaviće na nove osnove naviknuto ophođenje sa *file*-ovima-tekstovima, nosačima zvuka, videom koji su zaštićeni autorskim pravima. Digital Records Menagement (DRM) nudi mogućnost, da internet od strane "Copyright Industries" prikazan u najužasnijim bojama piratskog raja, postane medijum totalne kontrole. Američki ekspert za ustavno pravo i za prava na internetu Lorens Lesig (Lawrence Lessig) upozorava na, među apologetama interneta, rasprostranjeno verovanje u "prirodu informacija ili informacionih tehnologija". Statički optimizam legendarnih stavova poput "informacija želi da bude slobodna" (39) ili "Mreža interpretira cenzuru kao štetu i odbacuje je" (40), on klasifikuje kao naivni "je-izam" (Is-Ism). Riskantno je poći od toga, da internet "jeste, kakav jeste" - jer internet

konačno nije šaka puna protokola, kôd stvoren od strane čoveka – koji je s vremenom iskusio drastične promene. (41)

I zakonodavci su sasvim sigurno svesni da se svet ne sastoji samo od vlasnika prava. Takođe ne zvuči ni naročito verovatno da će korisnici industrije zabave masovno biti spremni da radi slušanja muzike pokažu dozvolu za posedovanje digitalnog oružja ili *Dongle* (mali *hardware* koji se konektuje na kompjuter da bi identifikovao neke delove *software*-a – prim. prev.). Koliko dalekosežno bi mogla da ode izgradnja digitalnog sveta u toku "borbe protiv pirata" tumačila su 2001. godine prodorna razmišljanja Intela, IBM-a, Tošibe (Toshiba) i Matsušite (Matsushita), da naprave zaštitu od kopiranja u okviru generičkog hardvera (42). Da biste kopirali hard disk C na hard disk D, molimo Vas pokažite nam Vašu legitimaciju. Još pre nego što su se zadimili topovi usmereni ka navodnim piratima, svet je postao kovčeg sa blagom konkvistadora.

Uostalom, jedan pogled ka muzici može ponuditi podsticaje za originalne izlaze iz konfuzne situacije kako za "konzumente", tako i za Copyright-industriju. Na primer, istorija uspeha benda "Grateful Dead" započinje kada su muzičari prestali svojim fanovima da uskraćuju autorskim pravima "zabranjene" delove koncerata. Njihov tekstopisac Džon Peri Barlou (John Perry Barlow) uostalom zna da barem u oblasti umetničkog stvaranja bez daljnjeg nije moguće ne biti "pirat": "Koliko muzičara može iskreno reći da nikada nisu iskoristili nešto čega je bilo i ranije?" (43).

I profesionalni protivnici kopiranja počinju da osećaju da je to pitanje prikladno; ponuđač DRM-a Inter Trust je početkom 2001. godine optužio kolege iz Microsoft-a zbog povrede patenta od strane tehnike zaštite od kopiranja ugrađene u Windows Media Player (44). Iz piratske perspektive posmatrano, to je jedan mnogo obećavajući feedback – ali ipak, naočigled sve češće igre među firmama koje razvijaju hardver i softver u vezi sa optužbama za patente, bilo bi prenagljeno očekivati da će različiti naraštaji zaštite autorskih prava jedni druge kočiti u tolikoj meri, da između njih još uvek ostane prostora za sasvim normalan napredak. U svakom slučaju, čini se da bi osnovnim mislima zaštite autorskih prava – nagrađivanju i podsticanju kreativnosti – fundamentalno protivrečilo, da razvoj i napredak kao zadatak svih, budu prepušteni samo piratima.

Poslednji pogled u prošlost – povezan sa nadom, da će nezgrapna anti-piratska propaganda ponovo ustupiti mesto začuđujućoj višeslojnosti, koja je u Evropi pre milenijuma bila dovođena u vezu sa "piraterijom". Ključna reč pripada grčkom rečniku: "peirates: morski razbojnici; od pieráomai: pokušati, prioniti na posao, truditi se, težiti, preduzeti, odvažiti se; nešto pokušati ili isprobati, proveriti, istraživati; okušati sebe ili svoju sreću u nečemu; odvažiti se na napad, zapodenuti borbu sa nekim; dovesti u iskušenje; truditi se oko nečije naklonosti; udvarati se ljubljenoj, učiti iz iskustva" (45).

Literatura

(1) Metro, 3. april 2001. (17. centimetara visoki naslov besplatnog časopisa londonske podzemne železnice)

(2) Die Zeit, 15. mart 2001

(3) Oliver Wallace, Peter Pan. A Pirates life is a wonderful life, © 1951 Walt Disney Music Company (ASCAP)

(4) Seerechtskonferenz der Vereinten Nationen, Genf 1958

(5) Hans Leip, Bordbuch des Satans. Eine Chronik der Freibeuterei vom Altertum bis zur Gegenwart, Berlin/Darmstadt/Wien: Deutche Buchgemeinschaft, 1961, S. 364

(6) Riaa, "Old as the Barbary Coast – New as the Internet", http://www.riaa.com/Protect-Campaign-1.cfm, 10/2000

(7) IFPI, "What is piracy?", http://www.ifpi.org/antipiracy/what_is_piracy.html, 2000

(8) Jay Berman, IFPI Chaurman, Musikwoche, 10. April 2000, S. 12

(9) Jay Berman, http://www.grayzone.com/ifpi61099.htm

(10) http://www.infoculture.cbc.ca/archives/newmedia/newmedia_05312000_bronfman.pthml

(11) Christoph Kolumbus, citirano prema: Hellmut Diwald, Der Kampf um die Weltmeere, München/Zürich: Droemer Knaur, 1980, S. 131

(12) Ibid, S. 200

(13) Philip Nichols, to follow his noble steps for Golde & Silver, London: printed by E.A. for Nicholas Borne dwelling at the South Entrance of the Royall Exchange, 1626 (Ms. von ca. 1592), citirano prema: Sir Francis Drake. Pirat im Dienst der Queen. Berichte, Dokumente und Zeugnisse des Seehalden und seiner Zeitgenossen 1567-1596, hrsg. von John Hampden, aus dem Englischen übertragen von Günter Thimm, Tübingen: Horst Erdmann Verlag, 1977, S. 64

(14) Home T, Cocoa Tea, Shabba Ranks, "Pirates Anthem", Greensleeves Records, 1989; vgl. http://website.lineone.net/~anthonypage/PirAnt.htm

(15) Uporedi GEMA-saradnik Alexander Wolf; nije u vezi sa http://mp3-wolf.de/

(16) Brad King, "Despite 'Piracy,' CD sales up", Wired News, 24.4.2000, http://wired.com/news/business/0,1367,35848,00.html

(17) Tim Richardson, "Ringtones cost music industry $1m a day", The Register 23.4.2001, http://www.theregister.co.uk/content/7/18441.html

(18) Sa time se uostalom bavi Telekom-Unternehmen AT&T – Andrew Odlyzko, pogledati: http://www.firstmonday.dk/issues/issue6_2/odlyzko/

(19) Iz intervjua sa Thomas-om Stein-om (kao Managing Director-om BMG Ariola), http://www.iface.at iz televizijske emisije "Interface 02", ORF, 30.3.2000

(20) Courtney Love u jednom govoru pri konferenciji Digital Hollywood Online Entertainment, New York, 16.2.2000, citirano prema: Salon.com, "Courtney Love does the math", http://salon.com/tech/feature/2000/06/14/love/index.html

(21) http://www.recordingartistscoalition.com/

(22) http://www.heise.de/tp/deutsch/inhalt/musik/8514/1.html

(23) http://www.spiegel.de/wirtschaft/maerkte/0,1518,114227,00.html

(24) Associated Press, 24.4.2001

(25) http://www.msnbc.com/news/563947.asp

(26) Leip, a .a. O., S. 413

(27) Capt. C. Johnson: A General History of the Robberies and Murders of the Most Notorious Pirates, London 1724, Kapitel XXVIII. Vgl. Peter Lamborn Wilson: Pirate Utopias, Moorish Corsairs & European Renegadoes. Brooklyn/NY: Autonomedia, 1995, S. 52 f.

(28) Pogledati Leip, a. a. O., S. 277 f. + 242; Peter Lamborn Wilson, a. a. O., S. 145

(29) Clive M. Senior, A nation of pirates: English Piracy in its heyday, New York: Crane Russack, 1976, S. 94. Citirano prema: Peter Lamborn Wilson, a. a. O., S. 68

(30) Pogledati Peter Rantaša, "Alles Napster oder was?", Profil 13/01, 26.3.2001

(31) Na Midement konferenciji im Januar2001, http://www.miaminewtimes.com/issues/2001-02-15/music2.html

(32) Pogledati http://www.quintessenz.at

(33) http://www.bsa.or.at/rechtundpolitik/urheberrecht.phtml

(34) http://www.bsa.de

(35) Pogledati http://www.heise.de/tp/deutch/inhalt/musik/3583/1.html

(36) Iz intervjua sa Thomas-om Stein-om (kao Managing Director-om BMG Ariola), http://www.iface.at , iz televizijske emisije "Interface 02", ORF, 30.3.2000

(37) Thomas Middelhoff, Bertelsmann, citirano prema saopštenju za štampu BMG od 31.10.2000

(38) Pogledati: Leip, a. a. O., S. 155, 372, 612

(39) Whole Earth Catalog-Gründer Steward Brand 1984 pogledati http://www.yale.edu/yup/gyd/media.html

(40) John Gilmore

(41) Lawrence Lessing, Code and other laws of cyberspace, New York: Basics Books, 1999, S. 24 ff.

(42) CPRM Content Protection for Recordable Media; vgl. "4C retreats in Copy Protection storm", theregister.co.uk, 4.1.200, http://www.theregister.co.uk/content/2/15797.html, und "Stealth plan puts copy protection into every hard drive“, theregister.co.uk, 20.12.2000, http://www.theregister.co.uk/content/2/15620.html

(43) John Perry Barlow u svom saopštenju "The Abolition Of Property In Cyberspace" na DDMI Europe u Londonu, 3.4.2001, http://www.ddmiglobal.com; pogledati. http://www.eff.org/~barlow/barlow.html

(44) John Borland, "Anti-piracy firm sues Microsoft", CENT News 26. April 2001, http://news.cnet.com/news/0-1005-200-5744735.html?tag=mn_hd

(45) Langenscheidt Griechisch-Deutsch, 1913/1964 (skraćeno)

Bernard Ginter (Bernhard Günther) je kurator MICA – Music Information Center Austria (sa fokusom na: internet, autorska prava, nova muzika, muzikologija), kao i nezavisni autor različitih festivala, izdavača i medija.

Svet nelegalnog kopiranja.
Jedna priča o skupljačima i lovcima.

Warez World

Dejvid Mek Kendls

Prolaziš pored prodavnice *Hi-Fi* opreme. U izlogu vidiš jedan *Hi-Fi* uređaj. Lep, ali skup, daleko od tvojih finansijskih mogućnosti. U normalnim okolnostima ne bi se dalje interesovao/-la za taj uređaj, ali ova prodavnica je neobična. Izlog nema stakla, ne postoji alarm. Ako uzmeš *Hi-Fi* uređaj, vlasnik neće trpeti štetu, jer se odmah u izlogu pojavi drugi uređaj. I onda ono najbolje: možeš da mazneš uređaj i niko te neće sprečavati jer te niko i ne vidi. Niko te neće pratiti. Niko neće saznati da poseduješ uređaj. Nikad nećeš biti uhvaćen. Sada reci iskreno: Da li bi uzeo uređaj?

Internet je stvoren isključivo zbog jednog razloga: za slobodnu razmenu informacija. Informacija je pak veoma jedinstvena roba. Možeš je poslati, a ipak zadržati jednu kopiju za sebe. Ako informacija u realnom svetu ima vrednost, konkretnu cenu kao na primer kompjuterski *software* ili komercijalna muzika u MP3 formatu, e onda imaš problem, i to golem problem.

Rat dva sveta

Kada se posmatraju pokušaji *software* industrije koja se trudi da zapuši *copyright* rupe koje su nastale internetom, a nasuprot njima su napori *underground*-a da održi piratsku mrežu, onda u ovoj priči postoje dva suprotstavljena gledišta, dva različita ali isprepletena sveta. S jedne strane je svet biznisa, poznat i dosadan. Svet 15 milijardi dolara teške *software* industrije sa svim svojim troškovima razvoja, marketinškim odeljenjima, izračunavanja dobiti i gubitaka, advokatima i policijom. Nasuprot njega stoji *Warez World*, šareni, tehnički visoko opremljeni *underground* u kome *cracker*-i, piratske grupe koje pljačkaju i vredni kuriri koji svi zajedno potkopavaju tehnologiju interneta, tako da mogu oko cele zemaljske kugle da se razmenjuju elektronski podaci. To je svet uzbuđenja, prestiža, paranoje i straha. Svet u kome spretni *cracker*-i "crack-uju" zaštitne funkcije skupog *software*-a i već nekoliko sati posle njihove premijere iste programe puštaju ih u internet. Svet "onih koji bi rado želeli" i opsednutih kolekcionara koji svoje *hard* diskove pune ilegalnim *software*-om, baš kao i filatelisti, i nikad ih neće koristiti. To je svet Meda Hatera (Mad Hatter), nedelja ujutro, negde na Floridi. 44-godišnjak, bivši vozač drag trka, pijucka iz čaše Sigramovo đumbirovo

pivo. Proverava svoj kompjuter kojim su cele noći defilovali automatizovani *script*-ovi. Med Hater je glava zavere jedne grupe softverskih pirata koji sebe nazivaju "Unutrašnji krug" (Inner Circle). Med ne nalazi greške, može da čita svoj *e-mail*. Ima oko 30 novih poruka: nešto ličnih poruka, nešto od obožavaoca, nekoliko interesantnih informacija, dva *Flame*-a, četiri zahteva. Med je otvorio *Shell Account* na jednom FTP serveru u Švedskoj. Dok njegov IRC program bez prekida radi u jednom prozoru, on proverava sadržaje nekih privatnih servera. Brzo kuca, pravi zabeleške, bira filtere i šalje *file*-ove sa jednog na drugi server. Dok doručkuje sa porodicom, ubacuje novi talas automatizovanih *script*-ova. Medova ISDN konekcija se budi zujeći. Neprekidna struja informacija napušta računar i nestaje u etru. Do kraja dana, Med je ubacio u internet 100 megabajta ilegalnog *Warez*-a.

"Većinu proizvoda koje kupuješ u prodavnici, možeš da vratiš, ukoliko nisi zadovoljan", kaže Med Hater. "Kod *software*-a to nije moguće". "*Warez* je mogućnost da se program pre kupovine može i proceniti", dopunjuje TAG (The Analog Guy – analogni momak). Analogni momak je kompjuterski animator i takođe jedan od vodećih članova "Inner Circle"–a . "Ako ti se *software* stvarno dopada i često ga koristiš, naravno da smo za to da ga onda i kupiš".

Na drugoj strani sveta, Kajl se pojavljuje na svom radnom mestu. Petospratni glavni štab mrežnog giganta Novell u Breknelu (Bracknell), Engleska, jedno velelepno zdanje. Nasuprot tome, u Kajlovoj kancelariji vlada haos. U ormanima su poslagani računari: svetleći desktopovi, rastureni mini *tower*-i i ramponirani serveri, svi priključci su na DAT rekorderima i CD-rom rezačima, svaka ekstenzija je zatvorena dodatnim matičnim pločama. U ćošku stoji metalni regal prepunjen monitorima, video opremom i rezervnim tastaturama. U odelu sa mašnom, 24 godišnji inženjer za mreže izgleda kao bilo koji *desk jockey* (DJ), ali njegov posao je jedinstven i visoko specijalizovan. "Po ceo dan se igram na internetu", priča Kajl, "i za to me još i plaćaju". Kajl je "maskirani" internet detektiv i kao takav je vrlo važan član u Novells Internet Piracy Unit-u (IPU), grupi tehničkih tragača koja operiše po celom svetu, "češljajući" internet 24 časa na dan u potrazi za ljudima kao što je Med Hater, znači za onima koji barataju nelicenciranim *software*-om, da bi ih na kraju razotkrili. Kajl provodi svoju radnu nedelju u infiltriranju u *Warez World* i sakupljanju dokaza. Pri tome se on predstavlja na sve moguće načine: kao *trader* (neko ko mulja sa *software*-om), kurir, *cracker*, *newbie* (novajlija), *lamer* (neko ko zapravo nema pojma), *lurker* (neko ko visi stalno u pozadini i samo posmatra) ili *leecher* (neko ko uzima *Warez*, ali ništa ne pušta u mrežu, tj. internet).

Napster je celom svetu pokazao da u internetu postoji ogromna *copyright* rupa. Pri tom, ovaj novi talas *filesharing* tehnologija kao što je Napster je u stvari samo jedna nova dimenzija već stare bitke koja se vodi između *software* industrije i *software* pirata. Bitka koja je počela ranih 1990-tih godina, *bulletin board*-ovima i modemima, a onda se dohvatila interneta i sada uključuje i profitne gusare i falsifikatore iz istočne Evrope i Azije. Napster je dao do tada "naivnoj" i samozadovoljnoj muzičkoj idustriji prvi utisak o tome kako može da izgleda naličje informacijske revolucije. Jedno neprijatno buđenje, što su još i ranije okusili Microsoft, Novell i ostali, kada su svi shvatili da većina zakona

ne vredi ništa čim se dođe u dodir sa mrežom. I to da će, ako postoji mogućnost da se materijal sa interneta može besplatno uzimati, a da se ne bude uhvaćen, ljudi onda to i koristiti.

U Kajlovom svetu pravila su jasna. *Software* je dragocena roba. *Software* je novac. Korišćenje programa kao što su AutoCad, 3D Studio, Microsoft-ovi serverski programi ili Novell-ovi mrežni programi – koštaju hiljade dolara po programu. Znači piraterija je krađa. *Software* industrija tvrdi da zbog piraterije gubi godišnje 15 milijardi dolara, a veći deo tog gubitka odnosi se na upotrebu nelicenciranih kopija u internim mrežama firmi, kao i na organizovano falsifikovanje u Istočnoj Evropi i Aziji. Pet milijardi nestaju kroz internet, pet miliona dnevno zahvaljujući *Warez World*-u.

U svetu Meda Hatera smeju se ovim ciframa. Cene i izgubljena zarada njima ništa ne znače. Ako je kopirani *software* takav da ga ne bi nikada kupili ili se ne bi mogao priuštiti, kako da se onda to smatra kao izgubljena zarada.

USENET: Mesto za povremenu pirateriju (prilika stvara pirata)

Na izdancima *Warez World*-a nalazi se Usenet, slično jednoj brani koja se izliva u more. Od desetine hiljada diskusionih grupa na Usenet-u, oko 100 ih se bave piraterijom. U (tj. na) *alt.binaries.warez.ibm-pic* se besplatno nude programi za *download*-ovanje, i to za svakoga, bez ikakvog problema. Treba da aktiviraš samo svoj *newsreader*, uputiš ga na odgovarajući forum i već se na tvom ekranu pojavljuje lista najnovijeg programa i čitaš je kao u nekom katalogu za kupovinu. Treba samo da *download*-uješ. Ako ti se atmosfera dopada, možeš da se priključiš zajednici i da joj daš svoj doprinos.

Warez u Usenet-u je star možda nekoliko dana ili nekoliko nedelja. Najnoviju "robu ćeš naći u veoma dinamičnom Trade Rooms Internet Relay Chats-u (IRC). Svakako da Usenet nudi dobar ulaz, pogotovo za novajlije pirate po potrebi – ili za one koji traže neki veoma specifičan softver. U jednoj tipičnoj nedelji nudi se Adobe Photoshop, Microsoft Office, 3D Studio Max, takođe i najnovije verzije Mircrosoft Windows-a. Mimo svega toga postoje i alfa i beta verzije, i to neverovatno - skoro pre zvaničnog objavljivanja, kao na primer *web tools*, mrežni programi, igrice i ostalo. Bolje rečeno, baš sve šta želi jedan napredan korisnik računara. Opseg slanja kreće se od takvih koji imaju nekoliko bitova (za crack-ovanje zaštite), do stotine megabitova koji su potrebni za kompletan ISO-imidž jednog CD-a. Ranije su se ove količine podataka, zbog modema, pakovale u više manjih paketa. Danas, u vremenu xDSL i kablovskih modema, teku svaki dan gigabiti svežih ilegalno kopiranih podataka.

Igra za opsednute

"Mi spadamo u sam kraj *Warez*-ovog lanca ishrane, tako da ne pravimo profit od toga", tvrdi TAG. *Warez cracker*-i, trgovci i kolekcionari ne kopiraju softver da bi zarađivali novac. Oni to rade jer su u stanju to da rade. Što su zahtevniji programi proizvođača za zaštitu,

utoliko je veće zadovoljstvo pirata da ih krekuju. Da li je to krađa? Ne, pre bi bilo da je to igra, jedno ludo takmičenje. To je jedan hobi, čin digitalnog terorizma, ali bez krvi. To znači: "Fuck you Microsoft". Radi se o sledećem: imati nešto prvi, ono što drugi još nemaju. "To je jedna igra za opsednute" – objašnjava Med Hater. "Moj kompjuter je non-stop *on-line*. Kada zbog bolesti duže vremena nisam mogao da radim, bio je pravi izazov koji me je motivisao kod *upload*-ovanja ogromne količine podataka. Četiri meseca sam dnevno najmanje 40 MB na dan *load*-ovao".

Warez-glave ne mogu da spavaju, pre nego što svom "kovčegu sa blagom" nisu dodali još nešto. Fazon je u tome da im uopšte ne trebaju ni *Java development kit* kao ni ovaj ili onaj *Photoshop plug-in*. Njihovo je zadovoljstvo više u tome da naprave novu listu, tj. spisak i da onda fino spakovani *zip file* čisto i sa strahopoštovanjem dodaju svojoj zbirci. Čak će možda i instalirati softver, i onda se, potpuno odsutni duhom, malo poigrati sa *toolbar*-om i paletama, i onda će ga ponovo spakovati i nikada više dotaknuti. Med Hater zna taj osećaj: "Mi to doživljavamo svaki dan, ljudi moljakaju za nešto da bi samo upotpunili svoju kolekciju. Ima puno kolekcionara (lamer)".

Usenet je magnet za pomenute *lamer*-e. Po važećoj mrežnoj predrasudi, (dis)kvalifikuje se automatski svako ko koristi *AOL*, ostali kardinalni gresi su *upload*-ovanje datoteke zaražene virusom (traljavo i opasno),"Me-too" slanje kao dodatak na porudžbinu drugih (zagušivanje opsega), slanje pojedinačnih diskova umesto kompleta (da se naljutiš), slanje *OBZ*-ova (One Big Zip – jedan veliki zip) umesto čisto fragmentiranih delova (loša karma za one koji imaju nepouzdan server). Kao najveće nedelo na toj sceni je bogami obznanjivanje tajnih *FTP* – sajtova ili skrivenih servera. Ipak, panduri stalno posmatraju i motre. "Brzo smo ukapirali koliko su opasni pretraživači, kao recimo *Altavista"* – objašnjava TAG. "75% ljudi, koji slali *Warez,* moglo se prilično jednostavno utvrditi koje su im prave *e-mail* adrese". Pošto ga je to uznemiravalo, TAG se uhakerisao u programski kôd *Forte Agent*-a. Tu se radi o jednom veoma upotrebljivom *newsreader*-u, koji je već ranije bio krekovan tako da izbegava manje vredan *shareware*. TAG je oslobodio ovu verziju od *x-newsreader header-a*. Ovakav zahvat je garantovao pošiljaocima veću anonimnost. Kao nuz-efekat, preko *patch*-a je smanjena količina *spam*-a za dve trećine. "Ovaj hak je imao takav odziv kod ljudi koji nisu imali veze sa *Warez*-om, tako da ga je *Forte* u poslednjoj verziji integrisao u *agent* kao "Feature'"– ponosno kaže TAG. "Ipak ne mislim da bi nam zbog toga skinuli kapu".

Jedno vreme je *Inner Circle* sebi dao zadatak da opslužuje pojedinačne *Warez* grupe. Objavili su svoj *Warez FAQ*, gde su postojala tri pravila: dobro ponašanje, dobro korišćenje opsega i dobar *Warez*, i nadali su se da će se ljudi toga pridržavati. Ali, kao i softverske firme, uskoro su primetili da uvođenje određenog reda u takvoj pustinji bezakonja jednostavno nije bilo moguće. "Spržio nas je pokušaj da vaspitamo mase", kaže Med Hater.

Umesto da se dalje troši, *Inner Circle* je naknadno napravio *IPL* (Interesting Parties List, spisak zainteresovanih strana), jedna lista garantovano visoke klase *newsgroup*-a, bez *lamer*-a, u kojoj će izabrani članovi moći da šalju svoj *Warez* kodiran uz pomoć *PGP* (Pretty Good Privacy). Oni koji su na ovoj listi, mesečno dobijaju novu lozinku za dekôdiranje softvera. Jedini preduslov da bi bio primljen na ovakvu listu je prihvatljivo poznavanje u

pogledu *PGP*-a. “Kada se već neko odlučuje da šalje kôdirano, onda se nadam da to znači i da taj nije kompletno nekompetentan”, smatra TAG. Čak i danas, nekoliko godina posle uvođenja, još uvek se trguje na IPL-u.

IRC: Trgovački centar *Warez World*-a

Za trgovačke potrebe velikog dela *Warez World*-a, kôdirani Usenet *post*-ovi postali su prespori i nepouzdani. Oni su se okrenuli ka internet *relay chat*-u (IRC). IRC je trgovački centar *Warez World*-a, neka vrsta potpune fuzije devizne berze i uličnog tržišta. U IRC-u ima stotine mesta za četovanje o softveru i tamo se i krše autorska prava – *free warez, warez 4 free, warezsites, audiowarez, warezgames*. U vremenu Napster-a, ovo su bila mesta trgovine MP3 zajednice. Postoje privatni *chatroom*-ovi, skrivena mesta za sastanke i piratske zabave gde pristup imaju samo poznati gosti. Zajednica je jeziva mešavina realnih ljudi i *Bots*-a. Ovi drugi (Bots), su automatizovani makroi sa sopstvenom ličnošću i osobinama, slično animiranim figurama u kompjuterskim ulogama. Treba da pritisneš samo jedan *Bot* i već ti se može desiti da zaobilaznim putem završiš na nekom FTP sajtu, negde u etru. Ako pritisneš neki drugi, saznaćeš najnovije *Warez* tračeve. Neki *Bot*-ovi fungiraju kao barmeni, kod kojih se učesnici uzajamno časte virtuelnim pićima ili pozivaju na cigaretu. U IRC-u su uvek najnovija i najsvežija izdanja. Svakako treba odmah otkloniti pomisao da se ovde radi o dobrotvornoj akciji. Svaki komadić *software*-a mora biti plaćen - *software*-om. Što je aktuelnija mogućnost primene, to je veća vrednost. Ultimativne vrednosti razmene su *Zero Day Warez* – znači *software* koji je promovisan u poslednjih 24 časa, po potrebi i *crack*-ovan. Trgovina sa *Zero Say Warez*-om automatski ti diže reputaciju na sceni. Ako imaš dobre veze i brzu konekciju, možeš da dostigneš taj status da možeš odmah da skidaš s nekog ekskluzivnog servera. Ili, dobiješ *login* i lozinke za elitne FTP *site*-ove. Možda ćeš biti primljen i u moćne kartele kao što su *Razor 1911, Class, Paradigm, Siege, Xforce* ili *RiSC*. “*Zero Day* sajtovi su zaista stvar elite”, objašnjava TAG, poznati zagovornik elitnog *Inner Circle*-a. “Pristup dobijaju samo oni ljudi koji mogu dnevno da pokrenu više stotina megabita. Uglavnom se tu isključivo radi o pozvanim gostima. Prosečnom *Warez* trgovcu, pristup IRC-u nije dozvoljen, osim ako ne investira mnogo rada u te svrhe.” Pri trgovini sa *Zero Day* mnogo se vara. Direktno takmičenje između grupa dovodi često do zanemarivanja inače uobičajene tačnosti. “Na primer: Dobije se dosta premijernih izdanja koja su loše *crack*-ovana”, izveštava TAG. “Jednostavno zato da bi neko mogao tu akciju da pripiše sebi. Dva dana kasnije dobije se *crack*-ovana verzija koja zaista funkcioniše.”

Stepenik niže u lancu nalaze se *Drop site*-ovi, gde se u razmeni za *upload*-ove dobija svež *Warez*. Neki od *Drop site*-ova idu preko privatnih računara trgovaca, drugi koriste *crack*-ovane velike računare vlade, velikih firmi, *shareware mirror servere* ili univerzitetske mreže. Često su ti *Drop site*-ovi na mreži samo 24 časa ili tokom vikenda, tj. onda kada su administratori kod kuće i kada niko ne nadzire logove.

IRC se samoorganizuje i reguliše. Mnogi trgovci su postali prijatelji. Ton u *chat*-ovanju je pristojan i osmišljen. “Pozdrav. Imam 1,5 giga na anonimnom T1, pristup sada. Pošalji poruku za više informacija, *lamer* nepoželjan. Hvala”. “Niko od onih koji pripadaju pravoj

Warez sceni nije prisutan zbog profita", kaže trgovac poznat kao Dajmond (Diamond).” “Mi to radimo iz istih razloga zbog kojih neki drugi skaču sa biciklima 70 metara. Nama je bitno da zasijamo. I da budemo *cool*. A osim toga upoznaju se i mnogi novi prijatelji, što je za mene najvažnije.”

Stvoriti klimu straha

Kao i u svakom “podzemlju”, tako i u *Warez World*-u vlada paranoja. Mora stalno da se pazi ko se sve predstavlja kao prijatelj. U Novell-u, u svojoj kancelariji, Kajl stalno motri na upadajuće fore, proverava *username*-ove i dijaloge u nadi da će sakupiti dovoljno detalja i dokaza da bi moglo da se opravda hapšenje. Postojalo je i takvo vreme kada je BSA-u (Business Software Alliance, udruženje *software* industrije za borbu protiv ilegalnog kopiranja i *software* piraterije) bilo važnije “iskorenjivanje piraterije” nego hvatanje pojadinačnih pirata. Kada je taj plan propao, jer apelovanje na svest, savest i osećaj krivice nije doneo rezultate, onda se prešlo na to da se scena zaplaši i zapreti pojedinačnim visokim kaznama. “Naša strategija je da izdejstvujemo kritičnu masu presuda”, kaže Martin Smit (Martin Smith), bivši vođa Novell-ovog antivirusnog odeljenja. “Prvo uhvatimo nekoliko ljudi koji takve stvari *download*-uju, takozvani 'Gwats', onda 'ćapimo' nekoliko onih koji su bolje organizovni, veći igrači. Ono što mi želimo jeste da stvorimo klimu straha!”

Rezultat toga je da se godišnje zadaje dva ili tri žestoka udarca *Warez World*-u. Poslednjih godina BSA je uhapsila više “trgovaca” u Kaliforniji. Oni su pokupili studente koji su sa njihovih koledž servera operisali u MIT-u (Massachusets Institute of Technology). I uz pomoć policije razvalili su vrata i upali u stanove u Holandiji, Južnoj Africi i Čileu. Kajl je bio prisutan u nekim od tih akcija i to zato da bi se sačuvali svi dokazi na računarima. Jedna od njegovih prvih akcija sprovedena je 1996. godine u Cirihu. Za Novell je taj slučaj bio “odlučan udarac protiv osoba i organizacija koje na internetu distribuiraju nelicencirani *software*”. A radilo se o 27-godišnjem kompjuterskom tehničaru koji je sebe, veoma zgodno za islednike, nazvao Pirat. Imao je svoj FTP sajt, koji je sve do hapšenja bio prepunjen *Warez*-om, bilo je tu nelicenciranog Novell-ovog *software*-a u vrednosti od 60.000 dolara, kao i uputstava za pravljenje bombi koja su u međuvremenu postala obavezna. “On je bio ta nova vrsta *Warez* tipova koji su se reklamirali na internetu”, priča Kajl. “Njegovi *file*-ovi su se mogli naručiti *e-mail*-om". Kajl je sebe predstavio kao trgovca, otišao na *site*, sakupio dokaze i predao ih švajcarskoj policiji. Jedna druga policijska racija “zaskočila” je sedište izvesne BBS koja se zove M-E-M-O. Ova BBS je vođena od strane kolege pirata sa nadimkom *The Shadow*. Na nesreću, on je baš u to vreme bio na godišnjem odmoru sa roditeljima. Kada se porodica vratila posle dve nedelje, naišla je na provaljena vrata od stana, pa su morali da gledaju kako im odvode sina.

Hapšenja kao ova u to vreme su bila tipičan način ophođenja BSA. U međuvremenu se pojavilo toliko mnogo novih “nekontrolisanih tehnologa”, da islednici to više ne mogu da prate. “Imamo sve više problema sa licitacionim *site*-ovima kao što je recimo Ebay”, priznaje Mat Tomset (Matt Thomset – novi anti-pirat manager u Novell-u). “Po našim

procenama, oko 90% ponuđenih programa na Ebay-u u SAD su ilegalne kopije." Microsoft ide punom snagom protiv 7500 *posting*-a na raznim licitacionim *site*-ovima gde se nudi falsifikovan *software*.

Istovremeno i vlade otkrivaju problem krijumčarenja podataka. Zamah *E-commerc*-a (elektronske trgovine) je u nekoliko zapadnih država doveo do toga da se pokrenu i angažuju takozvani *Cybercrime Squad*-ovi (dobro zvuči, a?), i to po devizi: "Hej, da li mi gubimo novac od poreza?!" Ali, još uvek postoji problem zone sivih država.

Sive zone i tajni savezi

"Sve što je potrebno jeste: server u jednoj državi u kojoj ne postoje zakoni protiv krađe autorskih prava, a takvih ima dosta" – objašnjava Martin Smit. "Jedna takva država dovoljna je, naravno ako ima telefonsku mrežu koja može da se koristi u ove svrhe, da poništi stotine hapšenja na zapadu." Uzmimo primer: Program proizveden u SAD šalje se preko nekog rutera u Kanadi na server u Južnoj Africi, a odatle ga *download*-uje Norvežanin koji radi u Nemačkoj, pri čemu on koristi anonimni *Remailer* u SAD-u. Zatim se u Bugarskoj sve narezuje na CD-ove koji se onda 'valjaju' u Velikoj Britaniji. "Kako u ovakvoj zbrci da se podigne optužnica?", pita Smit. "Sve je to pravni košmar". Onima koji se bave piraterijom da bi zaradili, može se lako ući u trag. Samo se prate tragovi koji nastaju plaćanjem kreditnim karticama na internetu. Ali kod trgovaca kao što su Inner Circle, koji robinhudovskim manirima ubacuju besplatno *software* na internet, tu je drugi slučaj u pitanju. "Kada je tamo (negde na net-u) neko ko ima predstavu o tome kakvim tehničkim sredstvima se može lokalizovati, onda nije preterano ako tvrdim da takav može itekako uspešno da se 'krije' ili da koristi neki sistem tako da je nemoguće da bude lociran", smatra Kajl. "Tehnički, tim ljudima uopšte nije problem da njihove vesti optrče ceo svet, dok mi kao podbodeni mamuzama jurimo po svetskoj istoriji."

Najiskusnije i najkonspirativnije piratske grupe ujedno imaju i najveći prestiž: *Razor1911, DOD, Pirates with Attitude* (PWA). Ovi tajni savezi izgradili su usko povezane strukture, članovi ovih klubova se uglavnom poznaju već godinama. Međusobno se smatraju dobrim prijateljima, iako se većina od njih veoma retko i susreće. Pravi identiteti i među njima ostaju tajna. Ove grupe imaju svoju mitologiju. Na nezvaničnim *web* stranicama obožavatelja slave svoje najveće pobede. Na tim stranicama nalaze se i veoma umiljate biografije, druge priče o istorijatu grupe kao i osvrt na one koji su uhvaćeni od policije ("We feel for ya!"). Postati član jedne ovakve grupe sve je samo ne jednostavno. Pozicije se upražnjavaju samo ako neki član prestane sa radom ili 'padne', tj. glasa se prilikom širenja operativnog polja. Reputacija je najvažnija, tj. reputacija je sve! Ako te ne bije neki glas unutar scene, možeš da zaboraviš. Čak i Kajl ne može da prikrije određeno divljenje. "Neki od ovih ljudi su neverovatno talentovani", priznaje on. "Logika i organizacija koja je iza ovih saveza jednostavno vam oduzima dah". Reakcija raskrinkanih pirata govori za sebe. Kada Kajl sa kolegama iz policije upada u stan, on ne zatiče strah. Nikada još nije doživeo da pirat sateran u ćošak pokušava da se baci kroz prozor ili da matičnu ploču baca u WC šolju. "Upadneš u stan i oni kažu samo "Oh!". Oni su deprimirani, kao da se predaju. Znaju da su nadmudreni i da je igri došao kraj".

Ni *dongles* ne pruža zaštitu

Alternativa racijama i specijalizovanoj policiji je obezbeđenje od nasilne provale. Razvoj zaštite od kopiranja koja ne može da se *crack*-uje. Ali, upravo to nije uspelo *software* industriji 'teškoj' milijarde dolara – iako ti pokušaji ne prestaju. Uporedimo li jedan uređaj u stvarnom svetu, čiji je zadatak da sačuva nešto od nepoželjnih, kao što je banka, sa zadatkom programera da razvije sistem zaštite za neki program, onda postaje jasno da je programer u znatno nepovoljnijem položaju. Obično grupa razbojnika upada u banku, i oni imaju samo jedan pokušaj. Ali, sada treba zamisliti čitavu armiju lopova iz najrazličitijih krajeva sveta, i svi napadaju istovremeno istu banku. I to ne samo jednom, nego stalno i stalno ponovo pokušavaju. Dalje, treba zamisliti da se lopovi među sobom klade ko će prvi da provali. I zamislite da su neki od tih lopova toliko tehnički potkovani da su mogli sigurno da prave i alarmni sistem, sef, čak i čitavu banku. I da su već provalili u stotine banaka koje su imale sigurnosni sistem. I da pri svakoj provali nauče još nešto, jer ih nikad ne uhvate. Nijedan sigurnosni sistem ne bi izdržao ovakav napad, tj. ne bi odoleo takvom napadu. Rešenje s kojim bi *software* industrija u današnje vreme napravila efektivnu zaštitu od kopiranja je *hardware* ključ – nazivaju ga i *Dongle*. A tu se radi o veoma nezgodnoj kombinaciji *hardware*-a i *software*-a. Prizivanje *Dongle*-a je ugrađeno u najniži nivo *software* kôda. Ako se *Dongle* ne ubaci u kompjuter, onda ni *software* neće raditi. A bez *software*-a, *Dongle* može da se koristi kao ukras. "Dongle će biti upotrebljen možda svaki put kada kliknete mišem, ili onda kada želite nešto da štampate, ili ako na *desktop*-u hoćete da promenite nešto", objašnjava ekspert za *Dongle.* Ako je odgovor na zahtevanu stvar pogrešan ili ako se na otvaranje programa ne daje odgovor, onda se program automatski isključuje. Za dodatnu zaštitu je i razmena podataka između *software*-a i *Dongle*-a kôdirana u neprovaljivim algoritmima. A ugrađeni osigurač služi da se *Dongle* sam uništi u slučaju mehaničkog otvaranja. Po mišljenju eksperata, morao bi se koristiti elektronski mikroskop da bi se izvukao algoritam iz elektronske zbrke.

Najveći ponuđač na tržištu *Dongle*-a je firma Rainbow Technologies, čiji *Sentinel-hardware* kôd pokriva 55% zaštićenog *software*-a. Na svetu postoji 8 miliona *Dongle*-a, koji su povezani s osam miliona računara. Sama firma opisuje proizvod kao "najefikasniji proizvod na svetu u zaštiti od *software* piraterije". Ova izjava je u svetskoj zajednici *cracker*-a shvaćena kao poziv na buđenje, tj. uzbunu, ako uopšte ima potrebe za tim. "U današnje vreme, *crack*-ovanje zaštite je sve samo nije lako", kaže TAG, *cracker* iz Inner Circle-a. "Software industrija čini sve da njihovi proizvodi budu sigurno zaštićeni od kopiranja. Ali, upravo ta činjenica ljudima koje bije dobar glas na sceni čini sve još interesantnijim". Logična procena za *crack*-ovanje *Dongle*-a bi bila da se kreira neka vrsta pseudo-*Dongle*-a, znači na *hard* disku skriven 'grumen' kôdova, koji sebe predstavlja kao ključ za *hardware* i koji na bilo koje pitanje daje tačne odgovore. Da bi se konstruisao takav pseudo-*Dongle*, *cracker* bi morao teoretski da nadzire sve informacije koje se razmenjuju između kompjutera i *Dongle*-a, a ujedno i da ih registruje i da onda napravi tačnu tabelu pitanja i odgovora. Na nesreću, da bi se odgovorilo na šifru od 6 znakova, postoji preko 280 biliona mogućih odgovora. Tačnije rečeno: 281.474.976.710.700, da bi se isprobale sve kombinacije,

modernom računaru bi trebalo 44.627 godina. A *SentinelSuperPro-Dongle* od Rainbow-a (po reklamnom oglasu "najsigurnija i najfleksibilnija zaštita koja postoji"), šifra može biti duga i do 56 znakova. Tako da bi izračunavanje kompletne tabele rajalo 10 na 125 (10^{125}) godina. Kod *SentinelSuperPro-Dongle*-a, koji štiti Kinetikov 3D-Studio-Max-Software, nije trajalo ni 7 (sedam) dana (računato od dana premijere preko Forcekill-a), kada je jedna vodeća *hacker*-ska grupa koja se zove DOD (Drink or Die) *crack*-ovala kôd. Svi ostali *high-end* programi koji koriste *Sentinel-Dongle*, kao *NewTek*-ov *Lightware,* Microsoft-ov *Softimage* ili Autodesk-ov *AutoCAD* – doživeli su istu sudbinu: bili su *crack*-ovani, ponovo upakovani i u roku od nekoliko dana posle premijere, poslati u svaki kutak interneta.

Umesto pokušaja da simuliraju *Dongle*, istaknuti *hacker*-i su raspertlavali programske kôdove, i to red po red, funkcija za funkcijom, prizivanje za prizivanjem i odnose su raspertljali sve dok konačno nije počelo da funkcioniše i bez *Dongle*-a. Na celom svetu postoji verovatno 8 ili 9 *hacker*-a koji su u stanju da izvedu ovakvo majstorsko delo. Ali, zahvaljujući internetu, dovoljan je i uspeh jednog jedinog *hacker*-a da bi rezultat bio rasprostranjen u svaki kutak sveta. I kada takav genijalan potez uspe, onda i ekipa koja je zaslužna za to čini sve da to bude i opštepoznato i uspeh se galantno slavi i to u *attachment*-u *crack*-kovanog *software*-a, kao NFO-*file* (informacioni tekst *file*). "Savršeno genijalan rad čuvenog člana grupe DOD - Replikatora. Drugih pet *crack*-era je pre toga već odustalo! Odlučili smo da ne pravimo *crack patch,* jer je kôdiranje značilo previše utrošenog vremena. Zašto? Jer je 72 (!!!) EXE trebalo *patch*-ovati. Sada sve opcije funkcionišu 100%".

Bolji od originala

Ti NFO tekstovi su više od sjajnog priznanja. Istovremeno daju i uputstva za instalaciju i prezentuju dubiozne ASCII-Art slike. To je u *Warez World*-u certifikat o autentičnosti, dokaz o ispravnom objavljivanju i garancijska deklaracija da sve funkcioniše. Na sceni ništa nije važnije od dobrog glasa. Svako objavljivanje se zato prethodno pažljivo testira na beti. Konačno, uspešni pirati smatraju *crack*-ovani *software* kao svoj 'proizvod', i naravno, niko ne želi da posle sedam sati *download*-a ima loš *crack* koji ne funkcioniše.

U 21. veku, posle mnogo godina treniranja, znanje i umeće *crack*-era dostiže novi nivo. Ne samo da nadmudruju zaštitu *software*-a, već uranjaju u same kôdove i zaista popravljaju programe. Godine 1996., Institut Frauenhofer je objavio jednu kompresionu tehnologiju koja je u povezanosti sa Napster-om postala veoma brzo sinonim za krađu *copyright*-a na internetu. Naziv, tj. ime te tehnologije je bio *MPEGAudioLayer3* ili skraćeno MP3. Sa tom tehnologijom se mogla komprimovati muzika CD kvaliteta u male *file*-ove, koji se mogu lako slati po internetu. U početku se radilo o ekstremnim *Codec*-ima. Što znači da je kompresiona forma bila primenjiva kod svakog programa. Ali onda, posle niza poboljšanja i daljeg razvoja, eksperti iz Frauenhofera su odlučili da integrišu i *Codec* i da se primena ograniči samo na oficijelno licenciran *software*. Poznata *Audiowarez* grupa *Radium* je imala nešto protiv agresivne zaštite patenta ljudi iz Frauenhofera i onda je zadužila njihovog glavnog hakera IgNorAMUS-a da *Codec* bude opet dostupan svima. Drugim rečima rečeno: pokrasti bogate da bi dao

siromašnima. Dok je navedeni IgNorAMUS po metodi mreže koja se vuče, prerađivao hiljade redova Assembler Code-a, došao je do uzbuđujućeg saznanja. I to da je u mogućnosti da napravi poboljšanja na algoritmu. Posle kratke intervencije *Debugger*-a, implementirano je niz promena koje su dovele do optimiranja performansi i na kraju je dovelo i do toga da je program za 12% brže radio. Radium je upakovao MP3-Codec i ponosno ga opremio i dijagramom koji je prikazivao koliko je Radium varijanta nadmoćnija od originalnog Frauenhofera. Odmah potom se Radium Codec munjevito raširio po celom svetu i na kraju je korišćen za komprimovanje miliona komercijalnih MP3-ova i to upravo onih koji su razmenjivani kôd Napster-a.

Bitka se nastavlja

Napster je nešto najbolje što se dogodilo softverskoj industriji. Godinama su oni (oni – razni zvaničnici) izdvajali milione za lobiranje i stalno se žalili na nedovoljnu zainteresovanost i razumevanje vlade što se tiče internetom uslovljenim *copyright* problema. Zajedno sa bombastičnm usponom Napstera-a upravo su ove teme katapultirane na naslovne strane sve moguće štampe, direktno u *mainstream*, da bi se na kraju našle i na dnevnom redu u parlamentu Evropske Unije i Američkog Senata. Brzinom vetra se usvajaju čvrsti i rigorozni zakoni koji zabranjuju tehnologije razmene kao što su Napster, Gnutella, Freenet i ostale, a sa druge strane, vlasnicima autorskih prava otvaraju mogućnost da njihove knjige, muzika i *software* na internetu zaštite visokim taksama.

Ali i pored svih ovih novih tehnologija, kôdiranja i zakona, piraterija neće prestati. Bitka se jednostavno nastavlja. U samoj prirodi interneta je to da ne poznaje zakone. Internet je usmeren na slobodnu razmenu informacija, a naglasak je u ovom slučaju na "slobodnoj" razmeni. Dok god bude postojalo tržište, postojaće i crno tržište. Ili, kako je primer Napster-a to pokazao, dokle god postoje informacije koje imaju određenu vrednost, biće i ljudi koji će ih jednostavno koristiti. I što se tiče Hi-Fi radnje sa početka, ukojoj se može svako poslužiti a da nikoga ne ošteti ili bude uhvaćen, ljudi će se i dalje služiti iz takve radnje. BSA i *software* industrija koju reprezentuje, će i u budućnosti nastaviti da za primer uhvate nekolicinu internet pirata. I dalje će investirati u programe za zaštitu i na svaku novu tehnologiju će reagovati sa podozrenjem i strahom. Ali i *Warez World* će nastaviti da postoji. Dalje će se usavršavati i regulisati i nalaziće nove kreativne načine kako da upotrebi tehnologiju protiv onih koji sa tim prave profit. Mreža *Warez World*-a je proširena i njeni članovi su toliko na mreži da ih *software* industrija ne može kontrolisati.

Iza svakog pirata koji okrene leđa sceni – odraste, odluči se za karijeru sa nošenjem leptir mašne ili bude uhvaćen i optužen od islednika kao što je Kajl, stoje već deset novih koji su spremni i samo čekaju da zauzmu njegovo mesto. "Mi smo svi porodični ljudi, oženjeni, sa decom. Imamo normalne poslove i bezbroj telefonskih linija", kaže Med Hater. "Naša deca su godinama posmatrala šta radimo. Oni će biti sledeći kuriri, novi *Warez* bogovi".

Dejvid Mek Kendls (David McCandless) živi i radi kao autor i muzičar u Londonu. Više od 15 godina piše o kulturološkim aspektima informacionih tehnologija. Više o njemu možete naći na njegovom *website*-u http://www.wakeywakey.com

2. Kultura virusa

Programeri virusa:
njihova istorija, njihove zajednice,
njihova igra mačke i miša s antivirusnom industrijom

Oni nas vole.txt.vbs

Janko Retgers

"Skupljanje stvari je nešto što sam oduvek rado činio. Kao klinac skupljao sam poštanske marke, sad skupljam kompjuterske viruse". Luis ima 27 godina, srećno je oženjen, radi u jednom španskom IT-preduzeću, a u slobodnom vremenu najradije se posvećuje programima koje drugi kompjuterski korisnici obilaze u širokom luku.

Sakupljača virusa kakav je Luis, verovatno ima par stotina. Ipak, samo nekolicina taj hobi uzima tako ozbiljno kao on, i niko od njih nema tako veliku zbirku. Nije želeo da kaže koliko elektronskih štetočina drema na njegovom *hard*-disku. U tim odnosima Luis je veoma stegnut. Zna da se o broju postojećih virusa piše puno besmislica. Zna da proizvođači antivirusnog *software*-a pokušavaju da se uzajamno nadmaše brojevima koji počivaju s one strane dobra i zla. Luis ne bi želeo da još potpiruje tu diskusiju. Odaje samo ovoliko: tek tri ili četiri od najvećih proizvođača *software*-a raspolažu zbirkom većom od njegove. Najzad, njemu uopšte nije stalo do veličine zbirke, već do svakog primerka ponaosob. Nema šta, sakupljač od formata.

Elem, već gotovo deset godina Luis je pod imenom *Virusbuster* deo vitalne scene elektronskog podzemlja, koja sebe označava kao vX-eri. Čine je programeri virusa, sakupljači i drugi prijatelji autoreproduktivnih programa, koji se zatvaraju u male grupe, razmenjujući se preko usko razapete mreže *chatroom*-ova, *website*-ova i elektronskih magazina. Luis je član grupe 29a, koju je 1996. osnovao španski programer sa pseudonimom Mr Sandman. Kako među vX-erima, tako i među saradnicima firmi za antivirusni *software*, 29a važi za jednu od najinovativnijih grupa na sceni. Prvi virus za Windows-2000, prvi crv-Gnutella, prvi virus koji preseže platformu, pa stoga inficira kako Windows tako i Linux – 29a trasira stalno nove mogućnosti za elektronske štetočine. Time stalno primorava i programere antivirusnog *software*-a da poboljšavaju svoje programe te da premišljaju njihove temeljne koncepte. Večna igra mačke i miša.

Crvi, kunići i klonirani losovi

Igra koju ovde igraju Luis i njegovi prijatelji nije bez tradicije. Prve programirane štetočine pojavljuju se već u šezdesetim godinama na nekoliko velikih računara. Oni umnožavaju sami

sebe u glavnoj memoriji mašina, grabeći tako drugim korisnicima u ono doba tako dragoceno računarsko vreme, a zbog svog nagona za razmnožavanjem nazvani su kunićima.

Početkom sedamdesetih, izvesni Bob Tomas (Bob Thomas) eksperimentiše s programom koji je u stanju da unutar mreže prelazi s računara na računar. Tomas radi kod Beraneka i Njumana (Beranek & Newmana) koji su razvili ARPANET, i tamo aktivno učestvuje u razvoju tehničkih osnova sadašnjeg interneta. U pravom smislu reči, posao budućnosti. Jedan od onih koje bi čovek rado zadržao. Šašavo, njegov mali eksperiment – Tomas ga je krstio *Creeper* (puzavica – prim. prev.) – pokazao se kao krajnje uspešan. Bez kontrole prenosi se u *Tenex*-mreži firme od računara do računara i čini se da ga je nemoguće zaustaviti. Bez otezanja, Tomas programira drugi program pod imenom *Reeper* (igra reči, (C)reeper bez C upućuje na Repair, tj. popravku - prim. prev.), koji progoni štetočinu i uspešno ga isključuje.

Na taj način Reeper je na izvestan način prvi antivirusni *software* na svetu. Naravno, iz sadašnjeg ugla antivirusni eksperti *Creeper* ne bi zvali virusom, pošto program ne inficira druge datoteke već se jedino autonomno samoumnožava u mreži. Takve tvorevine danas se zovu "crvi" – pojam koji su 1982. godine uveli Džon Hap (John Hupp) i Džon Šoh (John Shoch) iz Xerox-ovog istraživačkog centra Palo Alto. Oba, naučnom fantastikom oduševljena, istraživača inspirisala je pritom kultna knjiga Džona Branera (John Brunner) *Shockwavereiter.* Braner tu već sredinom sedamdesetih godina govori o "Tape worm"-u, o samoreproduktivnom programu kojim junak romana obara kompjuterski sistem jednog totalitarnog režima.

Potom, u godinama 1981. i 1982. nekoliko klinaca - kompjuterskih entuzijasta razvijaju ono što se može označiti prvim kompjuterskim virusima. Petnaestogodišnje novo meso na koledžu, Rič Skrenta (Rich Skrenta) piše program za Apple 2, s lepim imenom *Elk Cloner.* Samoreproduktivni *los* inficira diskete s Apple Disk Operating System-om 3.3, pritom ne brišući podatke. Startuje li se zaražena disketa po peti put, na monitoru se pojavljuje pesmica:

"It will get on all your disks
It will infiltrate your chips
Yes it's cloner!
It will stick to you like glue
It will modify RAM too Send
in the Cloner!" (1)

Kasnije, Rič Skrenta postaje saosnivač *Open Directory Projects*. Činjenica da je on po svemu sudeći napisao prvi virus, i danas ima svoj eho: "Najgluplji *hack* koji sam ikad programirao, ali je izazvao najviše pažnje", kaže on o tome godinama kasnije (2).

Džo Dilindžer (Joe Dellinger) u to vreme studira na *Texas A&M University* i upravo se mnogo igra s Apple 2. Kao Skrenta, piše nekoliko samoreproduktivnih programa. Bez mnogo razmišljanja naziva ih *Virus 1, Virus 2* i *Virus 3*, zauzimajući time pojam koji nas prati do danas.

Fred Koen: Svaki sistem podleže infekciji

Međutim, ovaj pojam probio se tek onda kad je Fred Koen (Fred Cohen) 1984. godine objavio rezultate svojih istraživanja samoreproduktivnih programa pod naslovom "Kompjuterski virusi – teorija i eksperimenti". Koen ovde po prvi put definiše šta je tačno kompjuterski virus: samoreproduktivni program koji može da inficira druge, ugrađujući im sopstveni kôd. Uz svoj zaključni rad, Koen daje i par sitnih apstrahovanih primera za izgradnju takvog virusa – korak koji bi ne jednog profesora danas pokrenuo da odbije rad.

Međutim, 1984. godine još nije bilo zlih virusa, nije bilo podzemne scene programera virusa, antivirusne industrije i senzacionalističkih novinskih članaka. Nanosi li virus štetu onda svakako zbog nepažnje ili rđavog programiranja. Onaj ko u tim danima želi da podučava ili da nauči nešto o virusima, hteo ne hteo mora neke i da programira. Uprkos tome, Koen već sluti da će se jednog dana koristiti zaštita od virusa i "crva", da bi oni mogli postati opasni.

On preispituje različite bezbednosne koncepte prema efikasnosti, ali ubrzo tvrdi: potpunu sigurnost obećava samo kompletno zatvoreni sistem. Onaj koji izlazi na kraj bez kôdova spolja, koji nije umrežen i, ako je moguće, koji ne dopušta ni bilo kakve zahteve. Zacelo, sasvim različito od onog što se očekuje od jednog računara. Svi ostali sistemi podložni su napadu virusa, toliko od Koena. To bi važilo i za sisteme koje tek treba razviti, jer: "Predstavljeni rezultati nisu pogonsko-sistemsko-, ili implemantaciono-specifični, već se zasnivaju na temeljnim svojstvima sistema." (3) Drugim rečima: nema apsolutne zaštite od virusa. Inficiran može biti svaki računar, svaki sistem.

Prvi virusi s potpisom

Neki sistemi svakako lakše od drugih, kao što će se uskoro pokazati. Marta 1982. godine, pojavljuje se prva verzija Microsoft MS DOS. Zahvaljujući vešto sklopljenom ugovoru s IBM-om, osnivač firme Bil Gejts (Bill Gates) položio je kamen temeljac za to da taj sistem kroz nekoliko godina postane standard za desktop PC. A zahvaljujući njegovoj arhitekturi koja ne poznaje privilegije i zaštitne mehanizme, ubrzo postaje najvažnija platforma programera virusa.

Godine 1986. po prvi put se svetom širi jedan MS-DOS-virus. Dva brata, Bazit i Amjad Faruk Alvi (Basit i Amjad Farooq Alvi) poseduju malu *software* firmu pod imenom *Brain Computer Services* u Lahoreu, glavnom gradu Pakistana. Da bi predupredili neizmerno piratsko kopiranje u svojoj zemlji, programiraju sasvim bezazlen *Brain*-virus. Svakako iznenađeni, konstatuju već posle kratkog vremena da su se po celom svetu raširile diskete u čijem u *boot*-sektoru počiva virus – a s njim i važeća adresa i telefon obojice.

Isto tako odvažno, pravim imenom i prezimenom svoje viruse obeležava nemački programer Ralf Burger. Svojim *Virdem*-virusom u prtljagu 1986. godine posećuje *Chaos Communicaion Congress*, koji jednom godišnje organizuje grupa *Chaos Computer Club* (CCC). Te godine virusi čine težište priredbe. Po prvi put, šira zainteresovana javnost

može se informisati o fenomenu. Navodno, u ponuđenoj radionici učestvuje 20 aktivnih programera virusa. Scena se formira.

Negde oko 1987. godine, pojavljuje se sve više virusa za MS DOS računare. Programerima odavno više nije stalo tek do samoumnožavanja. Njihove tvorevine s imenima kao *Kaskada*-virus, *Vienna*-virus ili *Jerusalem*-virus razlikuju se i po tome šta će prirediti napadnutom računaru – tzv. *Payloads* (bojevo punjenje). Burgerov *Virdem*-virus u jednom trenutku poziva korisnika da pogodi jedan broj. Samo ko pogodi moći će da nastavi s radom. *Stoned*-virus postaje čuven po tome što informiše: "Your PC is stoned!". Ipak, pojedini programeri služe se i već raširenim izvorno-virusnim kôdom da bi dali slobodu destruktivnoj energiji opasnog *Payload*-a. Jedna varijanta Burgerovog *Virdem*-virusa, recimo, u petak trinaestog, formatira napadnuti *hard* disk. Pored takvih zlonamernih iznenađenja, programeri virusa razvijaju i prve tehnike za prikrivanje svojih aktivnosti. Na primer, virus *Kaskada* igra na šifrovanje – jasan doprinos još mladoj antivirusnoj industriji.

S *Ghost Buster*-odnosom prema elektronskim štetočinama

Jedna od pojava s najviše preliva u to je vreme Džon Mekafi (John McAfee), šef firme Interpath, i kasnije osnivač McAfee Asociates. Godine 1988. on osniva gransko udruženje "Computer Virus Industry Asociation". Ipak, brojne antivirusne firme ne žele da pristupe jer krive Mekafija da kao osnivač National Bulletin Board Society-Network-a sam širi viruse. Iako taj prigovor nastavlja da ga prati među ekspertima, u očima javnosti uspeva mu da postane najistaknutiji od svih lovaca na viruse.

Peter Norton, poznat po svom *Utility*-paketu, u to je vreme navodno još izjavio da ne veruje u postojanje virusa. Ali, to je najverovatnije samo legenda, poput krokodila u njujorškoj kanalizaciji. Nasuprot tome, Mekafi je brzo otkrio da neiskusan kompjuterski korisnik itekako veruje u bezbrojne opasnosti u tom njemu nerazumljivom limenom sandučetu. Godine 1988. on oprema jedna servisna kola s kompjuterima, daje im ime "Virus Bug Buster" i angažuje posadu koja će čistiti viruse u Silikonskoj dolini vozeći od mušterije do mušterije. *Rent-to-kill meets High Tech Ghost Busters* – to su metafore koje bolje prolaze kod kompjuterskoh korisnika od bezbojnih tonova konkurencije.

U to vreme broj postojećih virusa još se kreće između dvocifrenog i trocifrenog područja. A *de facto*, u divljini malo od toga se da i uloviti. Umesto toga, virusi tada počinju da inficiraju medije. Pored prvih horor-najava u različitim dnevnim novinama, po prvi put se virusi publikuju i u izvornom kôdu i postaju pristupačni široj javnosti. Ralf Burger 1987. godine, kod *Data Becker Verlag*-a objavljuje "Veliku knjigu kompjuterskih virusa" sa izvornim kôdom nekoliko egzemplarnih virusa koje je delom sam programirao. Godinu dana kasnije, knjiga se pojavljuje i u engleskom prevodu.

Potom, 1990. godine, Amerikanac Mark Ludvig (Mark Ludwig) sledi sa svojom "Malom crnom knjigom kompjuterskih virusa", koja se čak isporučuje zajedno s disketom s egzemplarnim virusima. Ta izdanja naišla su na oštru kritiku u antivirusnoj zajednici. Tako bugarski ekspert Veselin Bonćev prebacuje autorima da naučnost zloupotrebljavaju samo kao štit za *Walker*-

viruse, te da provociraju imitatore. U odnosu na Ludvigovu knjigu on sudi: "Sve što se tamo može naći jeste gomila besmislen MS-DOS virusa koji jedva da funkcionišu." (4)

Ipak, čak i najjednostavniji opis fenomena dovoljan je da oduševi kompjuterske frikove širom sveta. U septembarskom izdanju nemačkog kompjuterskog časopisa "Chip" pojavljuje se članak o članu *Chaos Computer Club*-a, Štefenu Verneriju (Steffen Wernery), pod naslovom "Kompjuterski virusi – nova opasnost?". Bugarski kompjuterski časopis "Kompjuter za vas" preštampava članak pola godine kasnije i time polaže kamen temeljac za jednu od najvitalnijih virusno-programerskih scena. Za tri godine bugarski virusi dosežu udeo od 10% ukupnog svetskog tržišta.

Socijalistički kompjuterski raj

Ali, zašto baš Bugarska? Ako poverujemo predavanjima antivirusnog eksperta Bonćeva (5), Bugarska je krajem osamdesetih nešto kao socijalistički kompjuterski raj. Centralni Komitet bugarskih komunista odlučuje polovinom decenije da otpočne sa proizvodnjom sopstvene serije mikrokompjutera, da ih distribuira celom Istočnom bloku, i tako se provuče kroz eksportnu zabranu Zapada. Dakako, Bugari ne razvijaju neke potpuno nove sisteme već se specijalizuju za kloniranje postojećih modela. Najpre se s IMKO-om i Pravecom 82 razvijaju sistemi koji predstavljaju koliko je moguće savršene kopije Apple 2. Godine 1984., konačno se razvija Pravec 8 – osmobitni mikrokompjuter koji radi i s Microsoft DOS-om 3.3. Važna pretpostavka za njegov uspeh, jer da bi se dostigla prednost Zapada ovde se ne ulaže u razvoj sopstvenih *software*-a. Umesto toga, na tim su se mašinama obrazovale generacije informatičara u reversnom inženjeringu. Njihovi studijski zadaci morali su izgledati od prilike ovako: uzmi nešto *hardware*-a sa Zapada i po njemu napravi nešto štoje moguće jeftinije. Ili: uzmi najnoviju verziju MS DOS-a, instaliraj ga na Praveca – ali molim te – ukloni *bug*-ove. Kad se onda Vernerijev članak pojavio u bugarskom prevodu, neki od tih studenata momentalno se inficiraju. Do tada virusi su im bili nepoznati. Dakle, posvećuju se virusu *Vienna* koji se opisuje u članku i potom postupaju onako kako su navikli sa zapadnjačkim *software*-om: deasembliraju, analiziraju, optimizuju. Pošto u Bugarskoj nema ni antivirusne industrije s kojom bi se mogla igrati igra mačke i miša, moraju u isti mah da izmisle i mačku. Programer *Yankee Doodle*-virusa stoga sam sebi gradi sopstveni antivirusni program po imenu *Vaesina*. Na njemu on isprobava svoj virus, pojačava zaštitu poboljšava virus, itd. Neki od njegovih virusa povezuju čak obe tehnike i deaktivišu druge viruse koji se nalaze na napadnutom sistemu. Potom, 1990. godine u Sofiji nastaje prvi *Virus Exchange (vX) Bulletin Board – mailbox* sistem za razmenu elektronskih štetočina – koji radi s *upload/download* proporcijom. Ko želi da skine viruse, mora zauzvrat doneti nove. Kako su uskoro u sistem pohranjeni svi poznati virusi, korisnici moraju, na dobro ili zlo, programirati nove viruse. Uskoro BBS sa svojih gotovo 300 korisnika postaje poznat kao "virtualni univerzitet za viruse". Jedan od najaktivnijih studenata ovog univerziteta zove se *Dark Avenger* i ekstremno je talentovan programer iz Sofije. Početkom 1991. godine on obaveštava da razvija virus s više od 4.000.000 mogućih mutacija.

Mi smo dobri

Gotovo u isto vreme, socijalna radnica Sara Gordon (Sarah Gordon) kupuje svoj prvi PC. Ubrzo se na njenom monitoru pojavljuje loptica-skočica – siguran znak prisustva *ping-pong* virusa. Gordonkin interes je pobuđen. Pošto je već rano stekla iskustva s *mail-box*-ovima u mreži *Fido,* traži više informacija i pritom nailazi na *News*-grupe virusno-programerske scene.

Uvek iznova pojavljuje se jedno ime: *Dark Avenger.* On je autor istoimenog virusa koji važi kao ekstremno opasan jer zna da se sakrije pred skenerima za viruse, da ih inficira i tako napadne i svaku ispitanu datoteku. Sara Gordon uzalud pokušava da stupi u kontakt s Dark Avenger-om. A onda pokušava s jednim trikom. Od jedne *News*-grupe koja se probija traži virus koji nosi njeno ime.

I opet ništa od Dark Avenger-a. Sve dok se januara 1992. godine ne pojavi njegov dugo najavljivani mutacioni virus, generator za polimorfne viruse s bezbroj pojavnih mogućnosti. Zapanjujuće, već za nekoliko dana većina antivirusnih programa prepoznala je Dark Avenger-ovu "Mutation Engine". No, očigledno su neki programeri bili brzopleti priprilagođavanj skenera. Pored Dark Avenger-ovih mutacija, sada su iznenada kao virusi prepoznate i hiljade neinficiranih datoteka. Antivirusna industrija ima problem. I usred tog problema stoji rečenica: "Ovaj mali virus posvećujemo Sari Gordon" - kao da *Mutation Engine* nije ništa više od simpatične novogodišnje čestitke.

U antivirusnoj zajednici Mutation Engine najpre zovu "Posvećena" i Saru Gordon odjednom svi znaju kao zlu paru. Međutim, nju to ne sprečava da nastavi da se bavi temom. Početkom devedesetih već su jasno utvrđeni frontovi između programera virusa i antivirusne industrije. Mnogi u antivirusnoj industriji već zahtevaju oštrije kazne za širenje kompjuterskoh virusa i usrdno se trude da programere virusa po sebi prikažu kao kriminalce.

Ali Sara Gordon kao socijalna radnica poseduje drukčije metode pristupa: "Utvrdila sam da postoji jasna diskrepancija između onoga što antivirusni ljudi govore o 'Bad Guys' i mojih posmatranja." (6) Gordon je odlučila da se intenzivnije posveti "Bad Guys"-ima te da po prvi put sistematski istraži njihove strukture i motivacije. Scena je doduše prihvata, ali je opet mnogi smatraju jednom od "loših momaka"; najzad, njen istraživački rad počinju da plaćaju firme kao IBM i Simantec.

Sara Gordon rado ironizuje to uzajamno crno-belo bojenje. Njen privatni *website* dosledno se potvrđuje na adresi www.badguys.org.

Luis postaje *Virusbuster*

Kao Sara Gordon, tako je i Luis početkom devedesetih godina došao u kontakt s *ping-pong*-om. Razume se, ne svojom voljom. "Jedino što me je zanimalo u vezi s virusom, bilo je da ga ubijem", kaže on danas o tome. U to vreme on skuplja i razmenjuje nelegalno kopirane programe. U potrazi za nekolicinom novih igara naleće na osobu koja takođe razmenjuje *Warez*, ali u ponudi ima i nekoliko sasvim osobenih programa. "On mi je pokazao kako virusi mogu da budu zanimljiva stvar, ako umeš njima da barataš. On mi je dao svoju zbirku virusa, gore-dole 40 komada, i ja sam započeo svoje sopstvene eksperimente."

Godine 1994., *Virusbuster* otkriva internet a snjim i vX-scenu. Ta scena je negde oko 1990. godine oformila čvrste strukture. Od elementarnog značaja su pored *mailbox*-ova dve funkcije interneta: avgusta 1988. godine, Finac Jarko Oirkarinen (Jarkko Oikarinen) je razvio *Internet-Relay-Chat-Network* (IRC). Godine 1989., Tim Berners-Li (Tim Berners-Lee) otkriva *World Wide Web*, a 1990. razvija prvi *Web-Browser*. IRC je i danas za vX-scenu najvažniji medijum za neformalnu razmenu. *World Wide Web* je pritom pomogao da se iz tih neformalnih struktura iskuju čvrsti savezi. Ljudi se priključuju nekoj grupi, *website*-om se personalizuju i preko njega razmenjuju viruse i osnivaju *E-zine*. Juna 1991. pojavljuje se prvo izdanje "40-hex" magazina s mešavinom virusnih izvornih kôdova i uputstava za programiranje. On služi kao uzor mnogobrojnim magazinima ove vrste.

Prva hapšenja

Godina 1992. je loša godina za antivirusnu industriju. Za šesti mart su zbog virusa *Michelangelo* neke firme najavile 'ispadanje' kompjutera u milionskom broju. Ipak, na kraju je pogođeno svega 10.000 računara širom sveta. U isto vreme te godine pojavili su se prvi zaista jednostavno pokretani generatori virusa s kojima bi svaki laik mogao istipkati sopstveni virus.

Kao protivmera pojačava se pritisak na vX-scenu. Godine 1993. dolazi do prvih hapšenja kod članova britanske asocijacije *Really Cruel Viruses* (ARCV). Antivirusni tabor ovo slavi kao uspeh i nada se da bi slične akcije mogle zagorčati život novim autorima virusa. Ipak, tačnijim posmatranjem slučaja ispostavlja se da su članovi ARCV-a okrivljeni zbog drugog prekršaja: koristili su uređaje za manipulaciju telefonskom mrežom (tzv. Brown Boxes) da bi besplatnim telefonskim kontaktom pristupili vX-mejl boksovima u Sjedinjenim Državama.

Do prve osude jednog programera virusa dolazi tek 1995. godine. 26-godišnji Britanac Kris Pajl (Chris Pile) osuđen je na 18 meseci zatvora zbog širenja svog virusa SMEG i širenja jednog manipulisanog antivirusnog programa. Mnogi programeri virusa šokirani su zbog presude nad Crnim baronom – kako se on zove na sceni. Ali zbog toga se samo retko ko od njih uzdržava od kreiranja virusa. Ipak, od tada mnogi dvaput razmisle pre nego što virusa puste u divljinu. Većina virusa cirkuliše samo na sceni, samo mali postotak katkad inficira računare van scene. Sâmo programiranje programa koji sami sebe reprodukuju, u većini zemalja nije zabranjeno.

Onaj ko ipak pušta svoje viruse u divljinu radije ostaje potpuno anoniman. "Programeri virusa koji šire svoje tvorevine povezuju se s IRC-om preko *Proxy*-servera", objašnjava Luis jednu od raširenih mera opreza. On sam nije nikada programirao nijedan virus, niti bi svoje tvorevine puštao u 'divljinu'. Slično važi i za većinu njegovih prijatelja iz grupe 29a. Njihova je politika: "Programiramo viruse zbog uživanja u samoj stvari jer nam je to hobi, a ne da bismo naškodili drugima". (7) Oni ipak ne žele da se distanciraju od virusa koji se pojavljuju u divljini.

Windows 95: Novi početak ili teror

Za udarne naslove brinu većinom samo virusi koji *de facto* izazivaju infekcije, bezbrojne kompjutere ostavljaju van funkcije ili se naročito neobično šire. Kao recimo virus *Tremor* koji je 1994. godine kao prvi program svoje vrste dospeo među narod putem televizije. U to vreme, nemačka firma *Chanel Videodat* koristi prazan interval TV-emitera *Pro 7* da bi sa oko 15 kbit u sekundi kupcima distribuirala *software* videodata dekodera. Maja 1994. godine istom putanjom je put do mnogobrojnih *hard* diskova našla i jedna inficirana verzija dekompresionog programa *PkUnzip*. Tri meseca posle infekcije, hiljade korisnika VideoData bilo je suočeno s treperenjem svojih monitora pre no što se računar potpuno priključi. U nekim slučajevima *Tremor* se javljao i citatom: Front 242 "Trenutak terora je početak života". (8)

Novi početak ili teror – to pitanje pokreće mnogi beta-taster Windows-a 95. U nekim slučajevima Microsoft šalje sistemske diskete koje su zaražene *Form*-virusom. Ipak, taj nezgodan defekt gotovo je beznačajan spram svih novih mogućnosti koje sistem pruža programerima virusa. Početkom 1996. godine, s *Bizatsch*-om se pojavljuje prvi virus specifičan za Windows 95. (9) "Već par meseci ranije s *Concept*-om se u 'lovištu' javlja prvi makro-virus za Word. Ta dva virusa polažu temelj za bezbrojne sledbenike. Godine 1996. do prve Window-virusne epidemije.

U istoj godini nekolicina programera oko izvesnog Mr Sandmana osniva vX-grupu 29a kojoj malo kasnije pristupa i Luis, alias *Virubuster*. Njegovo ime je heksadecimalni izraz satanskog broja 666, a članovi grupe 29a i inače vole male igre brojevima. U petak, 13. decembra 1996. godine u šest sati i 66 ujutro, pojavljuje se prvo izdanje njihovog magazina s kojim se grupa, takoreći oficijelno, osniva. Ono sadrži uputstva za programiranje, izvorne kôdove i analize virusa, i tuce virusa, kao i migove za zaobilaženje antivirusnih odbrambenih mehanizama koji se ovde nazivaju "Klingon Tech" mehanizmi. Uz to članovi 29a isporučuju i sopstveni *text-viewer* koji kao *screen saver* upotrebljava *Payload*-izdanje LSD-virusa. Takvi marketinški štosevi javljaju se i u narednim izdanjima. Broj dva magazina 29a pojavljuje se s jednim animiranim uvodom kakve znamo iz izdanja demo-scene.

Interno, grupa je organizovana bazno-demokratski. Ne postoji predvodnik, samo se za svako novo izdanje magazina određuje neka vrsta redaktora: "Svako ko želi da postane član 29a mora nam poslati svoje članke i svoje viruse kako bismo mogli prosuditi kvalitet njegovog rada". Članovi onda ocenjuju njegov materijal i njega kao osobu. Ako su svi za, on može postati član. "Ako je samo jedan glas protiv, ništa od članstva", objašnjava Luis. Ostale odluke donose se većinski. Po proceni Sare Gordon, ovog časa postoji oko dvadeset stalno aktivnih grupa kao 29a. Uz to egzistira još i masa grupa koje se samo kratko pojavljuju na sceni, ali ponovo iščezavaju ili se stapaju s nekom drugom grupom. Grupa 29a pak pokazuje kontinuitet – doduše ona objavljuje po jedan magazin godišnje, ali zato na konto članova grupe idu neki od najinovativnijih i najkreativnijih virusa poslednjih godina.

U drugom izdanju njihovog magazina, pojavljuje se u Esperanto izdanju prvi virus koji može inficirati kako Windows tako i Macintosh računare. Svakog 26. jula, na dan kad se 1887. godine pojavila prva knjiga o veštačkom jeziku Esperanto – virus ističe proglas:

> *Never* mind your culture / Ne gravas via kulturo, Esperanto will go beyond it/ Esperanto preterpasos gxin; never mind the differences / ne gravas la diferencoj, Esperanto will overcome them / Esperanto superos ilin.
> *Never* mind your processor / Ne gravas via procesoro, Esperanto will work in it/ Esperanto funkcios sub gxi; never mind your platform / Ne gravas via platformo, Esperanto will infect it/ Esperanto infektos gxin. (10)

Mimo tog malog jezičkog kursa virus koji je programirao Mr Sandman, ne nanosi nikakvu drugu štetu.

Virusi: politika, istraživanje, pubertetska zabava

U istom magazinu pojavljuje se i Anti ETA virus od *Griyo*-a, s kojim se grupa kolektivno zalaže protiv baskijskog terorizma. To nije prvi virus s političkom porukom. Međutim, da li su virusi pogodni kao sredstvo izražavanja političkih mišljenja? Danas članovi 29a na to gledaju sa skepsom i na kraju kao na grehe mladosti. Kao autor virusa, *Griyo* se u međuvremenu distancirao od te akcije, a Luis komentariše: "To je više lična strast pojedinaca na sceni. Većina programera virusa ne meša politiku i viruse. Sumnjam da se velika većina programera virusa na sceni uopšte bakće s takvim stvarima". Čak i pokušaj da se programiranje samog virusa shvati kao političko, budući na neki način difuzno upravljeno protiv sistema, on odmah blokira kao nedopuštenu projekciju: "U programiranju virusa ne vidim nikakav politički čin".

Ali zašto to onda rade? Tim pitanjem bavi se i Sara Gordon otkako je scenu otkrila kao svoj predmet istraživanja. Neki jednoznačan odgovor na to do danas se ne može dati, "jer su programeri virusa različiti koliko i njihovi virusi", kazaće Gordon. Neki deluju jer ih ta stvar zabavlja, neki žele da se s nečim pojave na sceni, ili uživaju kad antivirusne firme recenziraju njihove programe. Drugi opet na tim kreacijama prosto vežbaju svoja programerska znanja ili pak uživaju u draži ilegale – recimo ako neku od svojih kreacija puste u divljinu. Perikle, sakupljač virusa i Luisov poznanik kroz šalu ovako obrazlaže svoju strast: "Možda sam zainteresovan za viruse jer imam kompleks entomologa poput Jungera (Juenger). U svakom slučaju nalazim da je zanimljivo istraživati slabosti nekog pogonskog sistema".

Ovaj istraživački motiv uvek se iznova pojavljuje na sceni. Početna stranica 29a *website*-a zove se "29a Labs", a njen član *Gryio* uz to održava i svoj privatni *website* pod imenom „BiO.net – Virus Research Labs". Nasuprot tome, antivirusni istraživači neumorno će isticati da bez "odgovarajuće etike, bez odgovornog ophođenja s virusnim kôdom nije moguće nikakvo istraživanje. Ipak, vX-scena krepko odbacuje takve pouke.

"

Zatvor ili ponude za posao

26. aprila 1998. godine, tajvanski vojni službenik Čen Ing-hau (Chen Ing-hau) pušta svoj CIH-virus u 'divljinu'. Već kroz nedelju dana virus preko interneta dospeva u Evropu i SAD

gde se verovatno širi preko promotivnih *downloud*-ova i besplatnih CD-romova. CIH tako ubrzo postaje jedan od najraširenijih virusa, i uz to jedan od najopasnijih: 26. aprila 1999. izbrisao je podatke na gazdinom kompjuteru. Na samo nekolicini računara uspelo mu je čak da prepiše i BIOS. Po razotkrivanju njegovog identiteta, Čen Ing-hau biva na kratko uhapšen, no kako ga u Tajvanu niko ne tuži, uskoro bez tužbe biva ponovo oslobođen. Malo kasnije biva angažovan od Linux-ovog distributera *Wahoo*-a kao bezbednosni ekspert. Antivirusna industrija je ogorčena.

U svakom slučaju, godinu dana kasnije, njegov virus je ponovo aktivan. Ovog puta tuži ga jedan tajvanski student i Čen biva osuđen na tri godine zatvora. Zastupnik firme *Sophos antivirus* izjavljuje: "Ovo je jasan signal programerima virusa da neće umaći kazni za svoja dela". (12)

Ipak, odnos između antivirusnih eksperata i vX-scene nije određen samo tako tvrdim tonovima zakona i reda. Sara Gordon, na primer, opisuje članove 29a kao "veoma simpatične momke. Uvek mi je činilo zadovoljstvo da se s njima razmenjujem". Ali bez razmene ona i njene kolege ne mogu dobiti ništa ako žele da njihovi antivirusni *scan*-programi što je moguće ranije prepoznaju nove štetočine. Antivirusni programeri često ih dobijaju direktno od autora koji se uvek raduju kompetentnoj analizi njihovih programskih ostvarenja. Osim toga, Luis izveštava da je već godinama u vezi s antivirusnim programerima. "Oni me koriste kao izvor za njihov rad, a ja njih kao izvor za moju zbirku."

Ako mu je za verovati, u nekima od tih firmi rade bivši programeri virusa, pa čak i aktivni učesnici na sceni. Pitamo ga da li bi on mogao zamisliti da se ikad zaposli u nekoj takvoj firmi. "Ikad?" "Već sutra, ako dovoljno plate!"

Prekomerne ponude čine se svakako i na drugoj strani. Kad je češki programer iz 29a, *Benny,* razvio svoj Win98 mileniumski virus, jedna beta verzija je nepoznatim putem dospela u ruke rumunskog antivirusnog specijaliste Adrijana Marineskua (Adrian Marinecu). Marinesku objavljuje analizu štetočine i *Benny* je pun hvale: "Dobar rad Adrijane!". Zabave radi izaziva ga u jednom magazinu sa scene: "Fuck off AV, join 29a!" (13).

Adrijan Marinesku pripada mladoj generaciji antivirusnih eksperata koja već optički nema puno toga zajedničkog Mekafijima i PeterNortonima ovog sveta. On nosi bradicu, otrcane prnje i pivopija je iz hobija. Uprkos tome, sa zahvalnošću odbija *Benny*-evu ponudu: "Nikad ne bih prešao na drugu stranu. Za sebe ne vidim zabavu u tome da škodim drugim korisnicima. Neki programeri virusa govore da pišu samo poučne viruse koji nikome ne škode. To nije istina. Već time što se samoreprodukuju oni nanose štetu". On sam se, kako kaže, programerima virusa ne sklanja s puta, već pokušava da ih ubedi da napuste svoj hobi. Najzad, iz svog svakodnevnog rada on zna: "Neki od njih su obdareni programeri".

Primitivni makroi i autonomni mutanti

Ali, još nijednog nije uspeo da preobrati. I tako se nastavlja igra mačke i miša. U petak 26. marta 1999. godine, u *News*-grupi *at.sex* po prvi put se pojavio *Word*-makro virus s imenom *Melissa*. Kroz nekoliko sati raširio se preko Microsoft-ovog *Outlook E-mail Client*-a

po celoj severnoj Americi. FBI pokreće potragu za autorom *Melissa*-e. Kad se u ponedeljak 29. marta u brojnim kancelarijama ponovo uključuju desktop računari eksponencijalno se ubrzava širenje *Melissa*-e. Navodno, toga dana biva inficirano više od 100.000 računara. Prvog aprila, Dejvid L. Smit (David L. Smith) biva uhapšen kao verovatni autor *Melissa*-e. Za njega biva sudbonosna prikačena AOL adresa s kojom je u *News*-grupi pohranio virus.

Melissa podjednako iznenađuje proizvođače antivirusa kao i programere virusa: "Zatekao nas je sa spuštenim pantalonama", godinu dana kasnije, na *Virus Buletin* konferenciji, kaže Džon Bladvort (John Bloodworth), istraživač *Network Associates* (14). Kombinacijom makroa za *Word* i rasejavanjem putem *e-mail*-a virus se širi toliko brzo da je jedva ijedan računar dovoljno zaštićen, da je jedva ijedan korisnik na njega pripremljen. Antivirusne firme moraju da gledaju kako hiljade vlasnika kompjutera otvaranjem *attachment*-a *Melissa* 'klikću' u propast. No i u sledećim nedeljama će i vX-scena trpeti od *Melissa*-e. FBI posećuje različite ISPs-ove i *Webmaster*-e vX sajtova. Neki usled toga iz predostrožnosti kompletno gube svoj nalog. Na *site*-u pretpostavljenog autora *Melissa*-e, danas se šepuri još samo logo antivirusnog softvera AVP.

U nadolazećim mesecima za udarne naslove brinu makro-virusi slični *Melissa*-i, recimo, poput virusa *I-Love-You*. Ipak, sa gledišta scene te su tvorevine pre primitivne. Ovde se radije petlja na virusima koje je krajnje teško otkriti, poput virusa *Marburg*, ili HPS-virusa, koji u oba slučaja idu na konto člana 29a, *Griyo*-a, a koje je nepažnjom raširio magazin PC-igara. Oba virusa koriste polimorfne tehnike da bi umakli skenerima virusa. Pomoću šifrovanja zasnovanog na slučaju, oni se sakrivaju u uvek novi kôd, tako da se više ne mogu pronaći preko jednostavnog kôdnog sravnjivanja.

Ali to nije sve: stvar postaje još kompleksnija kad se dva takva virusa uzajamno inficiraju. Drastično padaju šanse da se potom još i otkriju. Nađe li se ipak neki to može izazvati još katastrofalnije posledice. Ako ga antivirusni program odstrani i pritom modifikuje, kôd neotkrivenog virusa onda pod okoolnostima kao autonomna mutacija nastaje potpuno novi virus – virus koji ne može biti otkriven, koji nema autora.

Virusi u carstvu pingvina

Februara 1997. godine, s *Lin-Bliss*-om pojavljuje se prvi *Linux*-virus; do tada su mnogi Open-Source operativni system smatrali imunim, no očigledno nisu bili još ništa čuli o Fredu Koenu. Na kraju krajeva, on je još 13 godina ranije utvrdio: nijedan system nije bezbedan. Problem još više zaoštrava Linux-bum koji se upravo dešava. Za viruse poput *Lin.Bliss*-a prijemčivi su upravo Linux-početnici koji su sve vreme ulogovani kao *system-administrator* (Root). Marta 2001. godine, po članu 29a, *Benny*-u, najzad uspeva nešto zaista izvanredno. On objavljuje prvi virus koji može zaraziti kako Windows, tako i Linux računare.

Virusi poput ovog pružaju doduše mogućnost proizvođačima antivirusnog softvera da prošire svoje tržište na novi teren, ali kriju u sebi i nove konflikte. Linux-zajednica navikla je na sasvim drukčiju informacionu politiku nego AV-firme. Ako se pod Linux-om pojavi neka bezbednosna rupa, onda se to publikuje u pripadajućim *mailing*-listama i *Webblog*-ovima

kao “Slashdot.org”, kako bi administratori mogli što pre otkloniti rupu u svom sistemu. Pritom su izvorni kôd i detaljna objašnjenja ovde deo bontona. Naprotiv, za antivirusne eksperte svako publikovanje virusnog izvornog kôda je amoralno. Oni razumeju viruse samo u zatvorenim krugovima i objavljuju samo analize bez izvornog kôda.

U jeziku Open-Source zajednice, takva praksa se prezrivo naziva “Security by Obscurity“. AV-istraživači protiv toga argumentišu da se virus ne može poreditи s bezbednosnom rupom u odbrambenom pojasu (Firewall). Ona bi se po njima mogla zapuširi redovno objavljivanim *Bug-Fix*-ovima – a onda je sistem bezbedan. S druge strane, po njima, dovoljna je i mala promena virusa pa da on predstavlja bezbednosni rizik. Moderator *Bugtraq-Mailing*-liste Elijas Levi (Elias Levy) ne slaže se s tim. “U tome je problem cele antivirusne zajednice. Proizvođač nikad nije objavio neki b*ug-fix*. Vi ste toliko uljuljkani time što proizvođač nikad nije objavio neki *bug-fix* da verujete kako *bug-fix*-ova i nema.

RFC za mrežne viruse

Proizvođač o kome je ovde reč je naravno Microsoft. I mada će broj Linux-računara sigurno rasti, i mada su se u međuvremenu već pojavili virusi za *Palm-Pilote*, a po svemu sudeći samo je pitanje vremena kad će se pojaviti i za *Playstation 2*, jedno je sigurno: “Windows ostaje glavno polje programera virusa“. Oni već sada, šale radi, u svojim publikacijama zahvaljuju Microsoft-u za mnoge stvari koje im je ta firma do sad omogućila. Luis je siguran da se tu i u budućnosti neće ništa menjati: “Najinteresantniji trendovi će i nadalje biti povezani s Microsoft-om. Kao i dosad, virusi će zavisiti od toga šta će raditi Microsoft.“

Naredni trend počiva u mreži. Među autorima virusa pored IRC-crva i makro-virusa druge generacije izgleda da su poslednji krik samoažurirajući virusi. Ima ironije u tome da je tu funkciju izumela antivirusna industrija kako bi mušterije redovno snabdevala novim definicijama virusa. Programeri virusa su pak brzo otkrili da se i njihove tvorevine mogu dobavljati preko mreže. U četvrtom magazinu 29a, programer pod imenom *Venca* po prvi put objavljuje virus koji sebi može *downloud*-ovati dodatne module – *Venca* ih zove *Plug-ins* – preko *website*-a. Sličnu tehniku koristi i virus MTX kome uspeva da se jako proširi tokom jeseni 2000. godine.

Korak dalje čini hibridni virus koga upravo programira *Venca*: za njega postoje do 32 *plug-in*-a koji se šifrirani mogu skinuti s jednog *website*-a. U međuvremenu je taj *site* zatvoren, ali *hibris* zbog toga nije ispao iz trke: dodatno on *plug-in*-ove može dobaviti i preko *news*-grupe *alt.comp.virus* – diskusionog foruma koji koriste i antivirusni eksperti. Ostali virusi i “crvi” ažuriraju se preko FTP-servera, ili se automatski loguju u određeni IRC-kanal da bi sačekali nove daljinske komande.

Ali, ovo je tek početak. Programeri virusa odavno mozgaju na kompleksnijim mogućnostima iskorišćavanja mreže. Probni test za to mogao bi da bude *Gnutella*-crv *Gspot* člana 29a *Mandragore*. U junu 2000. godine, on se raširio među korisnicima *Filesharing* mreže slične Napster-u, tako što je iskorištavao upite za pretragom i na njih odgovarao paušalno pozitivno. Recimo, ako neko traži Photoshop, Gspot se izdaje za *Photoshop.exe*.

Ipak, interesantnija od ovog prostog trika je mreža kojom se služi crv. Šta ako virusi izgrade svoju sopstvenu *peer-to-peer* mrežu kako bi preko zaraženog kompjutera neprimetno razmenjivali informacije i *update*-ovali se? Ono što zvuči kao muzika budućnosti možda više uopšte nije toliko udaljeno od stvarnosti. U magazinu 29a broj pet, izvesni *Bumblebee* opisuje koncept kojim se virusi mogu sami *update*-ovati šifrovani preko sopstvene mrežne strukture. Šale radi, on svoj članak završava pozivom: “Let’s start our own RFC!“. (16)

Koga od ovoga podilaze žmarci taj bi trebalo da se radije drži buduće perspektive jednog antivirusnog eksperta kakav je Adrijan Marinesku: “U narednim godinama sve češće ćemo sretati samoažurirajuće, na internetu zasnovane metamorfne viruse. To su tehnike budućnosti – ali kladim se da će virusi koji opstoje u divljini u narednim godinama biti isto toliko blesavi kao recimo virus *I-Love-You*“.

Literatura

(1) Virus Rich Skrentas sa izvornim kodom postoji na http://www.skrenta.com/cloner/

(2) http://www.skrenta.com/cloner/clone-post.html

(3) Fred Cohen, Computer Viruses. Theory and Experiments, IFIP Conference 1984, online na http://www.alLneUbooks/virus/part6.html

(4) http://venus.soci.niu.edu/-cudigesUCUDS5/cud521.txt

(5) Vesselin Bontchev, The Bulgarian and Soviet Virus Factories, Sofia 1991, online, npr. na http://www.complex.is/-bontchev/papers/factory.html. U međuvremenu je osporavano koliko je zaista presudna bila uloga PC-Praveca na bugarsku produkciju virusa. Više o tome u tekstu Ralfa Bendrata u ovoj knjizi.

(6) Iz FAQ-a Sare Gordon, online na http://www.badguys.org/faq.htm /

(7) 29a Magazine Nr. 5, Policies and goals, Online na http://vx.netlux.org/dat/z001.shtml

(8) Frank Ludke, Die Geschichte des Tremor-Virus, online na http://www.outerspace.de/ccn/info-tremor.html

(9) Kao mnogim slučajevima, antivirusni istraživači davali su virusu različita imena. U njihovim bankama podataka naleteo je na ime Boza. Iz protesta prema takvom „falš“ imenovanju od strane Computer Antivirus Research Organisation (CARO), osnivač 29a Mr. Sandman posebno je programirao Anti-CARO-virus. Ako njime inficirani AVP-skener virusa otkrije Boza-virus, on ga detektuje kao Bizač-virus. Nije koristilo: antivirusne banke podataka navode protestni virus Mr Sandmana kao Anti-AVP.1235.

(10) Mr. Sandman, Esperanto - Sourcecode propraćen komentarima, objavljeno u 29a-Magazinu nr 2, online na http://vx.netlux.org/dat/z001.shtml /

(11) Sarah Gordon, Technologically Enabled Crime: Shifting Paradigms for the Year 2000, Computers & Security 1994, online na http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html

(12) http://www.sophos.com/virusinfo/articles/cihauthor.html

(13) BadByte Magazine Issue 3, online na http://www.badsector.org.uk/archives/badbyte/bbyte003.txt

(14) John Bloodworth, The AV Industry, Smug or Smart?, Virus Bulletin Conference 2000, online na http://www.virusbtn.com/vb2000/Programme/papers/bloodworth.pdf

(15) Citirano prema: Sarah Gordon, Richard Ford, When Worlds Collide: Information Sharing for the Security and Anti-virus Communities, Virus Bulletin Conference 1999, online na http://www.research.ibm.com/ antivirus/SciPapcrs/Gordon/V B99/vb99firal.html

(16) RFC = Request for Comment

Janko Retgers (Janko Röttgers) živi i radi kao *free lance* novinar i pisac u Berlinu. Više o njemu na *website*-u www.lowpass.de

Uloga virusa u globalizacijskom i bezbednosnom diskursu

Zašto u stvari Manila?

Peter Milbauer

Pomisao na kompjutere, koji imaju sličnosti sa živim bićima, koji se razmnožavaju i čak bez volje korisnika prelaze iz računara u računar, bila je početkom 1980-tih godina jedno uzbudljivo polje delovanja za naučnike kao što su Jirgen Kraus (Juergen Kraus) ili Frederik B. Koen (Frederick B. Cohen) (1). Sredinom dekade, opažanje postojanja kompjuterskih virusa (2) pomerilo se od aspekta zanimljivog naučnog problema ka pretnji. Ovakav pogled na stvari održao se još neko vreme bez histerije, ali sa pojavom prvih kompjuterskih virusa 'u divljini' 1987. godine, kada je to gotovo svakodnevno objavljivano preko štampe, televizije i radija, manifestovala se nova preteća fantazma i časopis *PM-Computer* je stavio naslov: “Virusi u programima. Da li nam preti kompjuterska SIDA”? (3)

Izvori zla

Utvrđeno je da bolest imunog sistema – SIDA potiče iz Afrike. Saznati poreklo kompjuterskog virusa nije bilo tako lako. Kamen spoticanja na tom putu bilo je pitanje: Koliko virusa uopšte postoji? *Sophos*, proizvođač antivirusnog softvera, objavljuje 5.marta 2001. godine ukupan broj do tada otkrivenih virusa – 61.069, a *McAfee Virus Information Library* (4) istovremeno dostavlja podatak o postojanju više od 57.000, a Jun-San Ve (Yun-Sun Wee) iz *Symantec*-a “više od 45.000” poznatih kompjuterskih virusa. Problem sa brojem virusa nas se manje tiče ne zbog toga što ih niko ne broji, nego što ih broje previše različitih instituta, firmi, naučnika i kolekcionara i koji na osnovu komplikovanosti virusa dolaze do različitih rezultata. Setovi za konstrukciju virusa daju već mnoštvo varijacija već poznatih virusnih konstrukcija. Kako ih brojati? Da li su stilske razlike beznačajne ili je u pitanju novi virus?

Zbunjenost izazivaju posebno različiti nazivi za viruse. Uprkos više pokušaja standardizacije, između ostalog i od strane *Computer Anti Virus Organisation* (CARO) i *Wildlist Organisation*, ne postoje vežeća pravila za davanje imena virusima. Zbog toga često potpuno isti virus dobija potpuno različito ime (kao na primer virus postao poznat pod nazivom “Piter”, a inače je virus 529). Ranije su virusima davali ime po veličini (na primer 1704 format virus), po *software*-u koji napadaju (kao dBASE virus) ili po stringu u programu (na primer kod Brain virusa). Danas se često virusima daje ime po upotrebljenom *attachment*-u ili po predmetu, na primer: *ILOVEYOU* virus. Virusi često dobijaju i ime

po mestu otkrivanja (kao Jerusalimski virus). Geografsko određenje nije uvek značajno i pouzdano. Jula 1996. godine, pojavio se *Exell* virus u isto vreme i na Aljasci i u Africi. Kao što i mesto otkrivanja nipošto nije i mesto nastanka virusa: *Arusiek* virus napravljen je u Poljskoj, a pronađen je u Maroku. (5)

Iako su mnogi virusi nazvani po mestima, ne postoji materijal koji bi makar približno naznačio zemlju porekla. Razlog tome je što to upravo leži u prirodi ove stvari. Jedan posting Džona Elsberija (John Elsbury) u *alt.comp.virus*, u ironičnoj formi objašnjava razloge nemogućnosti takve statistike: "*Virus Publisher Association* difinisala je standard za prepoznavanje države koja bi se morala nalaziti u serijskom broju svakog autorizovanog virusa. Uobičajeno je da se taj broj stavlja zajedno sa bar-kôdom na virus" (6). Što naravno nije slučaj. Programeri virusa uglavnom ne odaju svoj identitet i većina virusa se šalje anonimno. Ipak, među proizvođačima antivirusnog *software*-a postoje veoma konkretne predstave o poreklu virusa.

Jun-San Vi iz firme *Symantec*- proizvođač antivirusnog softvera, naziva istočnu Evropu i Aziju kao leglo virusa. Cifre, čak i kada ih tražite, ne može da navede (7). Torlav Diro (Torlav Dirro) iz *Network Associates* smatra da su "Kina, Tajvan i Filipini" glavna mesta proizvodnje virusa, ali ovu tvrdnju ne može statistički da potvrdi.

Diro objašnjava njegovo viđenje, zašto je težište nastanka virusa u tim državama sa strukturnim faktorima, kao što su velika mogućnost pristupa računarima i lošoj situaciji na tržištu rada. Objašnjenje koje možda vredi za Kinu i Filipine ali teško i za Tajvan, jer je procenat nezaposlenih u Tajvanu decenijama bio ispod 2%, a i posle azijske krize 1998. godine pomerio se samo na 2,7%. Njemu koristan, ali i ni za odbacivanje je argument da je upotreba antivirusnog softvera u istočnoj Aziji manje rasprostranjena nego u Evropi ili Severnoj Americi. Ali, da li se zaista želi Narodnoj Republici Kini preporučiti *software* firme, čiji se osnivač i predsednik Džordž Samenuk (George Samenuk) na jednoj PR manifestaciji početkom 2001. godine u Minhenu hvali time da je veći deo razvoja projekata bio plaćen od američke vlade i da "veoma tesno sarađuje sa državnim firmama kao što je između ostalog i NASA".

Mit-Bugarska

Znači, ne postoje pouzdane cifre, ali postoje pouzdane predstave o leglima virusa. Ove predstave o poreklu virusa su tesno povezane s dva faktora: s kulturološkim fantazmama i političkim suprotnostima. "Opšte je poznato da Bugarska predvodi u proizvodnji virusa i da ih Sovjetski Savez prati u stopu", napisao je Veselin Bončev (8) 1991. godine u svom poznatom članku "The Bulgarian and Soviet virus factories" (9), a Vin Švartau (Winn Schwartau) u svojoj informaciji na *Warefare*-u: "Virusi se uopšte pripisuju jednom neuhvatljivom i mitski brilijantnom programeru ili jednostavno 'Bugarima'" (10). Malobrojni, ali vrlo uspešni virusi učvrstili su predstavu o bugarskoj radionici virusa. Po Džonu Mekafiju (John McAfee), početkom 90-tih godina deset procenata svih infekcija u SAD-u činili su bugarski virusi, ali daleko najveći udeo u tome je imao *Dark-Avenger*-virus. (11)

Krajem 1980-tih godina, bugarski naučnik, istraživač virusa Veselin Bončev, utvrdio je dominaciju domaćih, originalno programiranih primeraka spram virusa "s druge strane zavese". Njegov izveštaj je samo žestoko podstakao proizvođače novih virusa: mesec dana nakon što je Bončev u bugarskom kompjuterskom časopisu izjavio da je infekcija većih *exe*-datoteka "veoma teška", pojavio se virus upravo sa tom osobinom (12). Novembra 1989. godine, u Bugarskoj se pojavio se novi virus s potpisanim imenom svog stvaraoca, a ime je ovome trebalo da mu pomogne u sticanju svetske slave: *Dark Avenger*. Neobično i novo na ovom virusu bilo je to da je inficirao datoteke prilikom samog otvaranja. Na taj način se ovaj virus širio jako brzo.

Virus ima u sebi jedan string koji je na početku imao "Eddie lives... somewhere in time", a na kraju je imao "This program was written in the city of Sofia (C) 1988-89 Dark Avenger". Ovaj veoma neobičan čin lokalpatriotizma za programera virusa bio je povezan sa priznatom strasti za pop kulturu. U jednom intervjuu, Dark Avenger je dao i objašnjenje o poreklu imena: "Sam izraz je iz jedne stare pesme, a ne iz pesme *Iron Maiden*-a, kao što neki tvrde. U velikoj meri, mislim da je to i stvorilo Dark Avenger-a" (13). Dark Avenger je ime dela pesme *Battle Hymus* koju su 1982. objavili klasici *heavy* metala – *Manowar*. Ostali virusi *Dark Avenger*-a kao što su: Number of the *Beast-virus* i *Antrax-virus* mogu takođe da se predstave kao metal citati. Spominjanje naziva longplejke *Iron Maiden*: *Somewhere in Time* zajedno sa *Iron Maiden* monstrumom Edijem u stringu ukazuje na uticaj ovog dela pop-kulture, tako da je i zapadnim virus-zinima (virus-časopisi) kao što je "40Hex" bio prepoznat kao "Metal Head" i "Heavy Metal Fanatic" (14).

I drugi bugarski proizvođači virusa takođe su se više orijentisali na internacionalnu pop kulturu nego na istočne osobenosti: W.T. je dao ime svom najpoznatijem virusu po liku iz serijala Rat Zvezda (Star Wars): "Darth Vader", a u bugarskom *virus-eXchange-Mailbox*-u su se pojavili posetioci sa pseudonimima kao "Ozzy Osburn" (sic!). Veze između muzičke i kompjuterske supkulture u 1980-tim i 90-tim godinama nisu bile jake samo u Bugarskoj, što je jasno iz mnogobrojnih pseudonima i poruka iz kopiranih programa. Ipak, *heavy metal* supkultura nije došla na glas kao leglo virusa, nego država Bugarska. To jednostavno ima veze sa tim (kao što će se i kasnije još videti) da je nacionalna forma veoma adekvatna za prenos svetskih političkih zastrašivanja (Bugarska je nekada bila deo Istočnog bloka), a drugo bi bilo da supkulturalna forma i nacionalna forma nisu međusobna konkurencija, već da se nalaze jedna naspram druge i da se međusobno dopunjuju. Iz pojačane kulturološke razmene nastaju oblici pop kulture koji su naizgled nazavisni od nacionalnih kultura i nacionalnih država. Ipak, gledano sa strane, takav način davanja identiteta se povezuje sa nacionalnom formom. Kao što se predstava o *Slacker* generaciji odmah povezuje sa Amerikom ili *Otaku* sa Japanom, tako se supkulturalno programiranje virusa povezuje sa Bugarskom.

Veselin Bončev je u Bugarskoj izložio kreiranje virusa kao sport koji je bio podoban i za postizanje određenog statusa. Za strukturne povoljnosti ovog razvoja naveo je veliki broj dobro edukovanih mladih ljudi koji nisu bili uključeni u ekonomske aktivnosti. Još za vreme Živkova, težište planske privrede bilo je na edukaciji za rad sa računarima kao i na

same računare. Država od 8 miliona stanovnika trebalo je da postane silikonska dolina Varšavskog pakta. Ali, Bugarska nije bila obećana zemlja za kompjutere, a prodor i širenje računara nije moglo da se poredi sa Severnom Amerikom i Zapadnom Evropom. Razlika u odnosu na zapadne države koja je i pogodovala širenju virusa je to da skoro i nije bilo "personalnih" računara, znači računara na kome radi jedna osoba (takvih je bilo jako malo). Glavni razlog širenja virusa, bar se tako tvrdilo, bila je razmena i podela (zajedničko korišćenje) *software*-a, ali pre svega je to bila upotreba računara na kome je radilo više osoba. To je bio glavni razlog širenja virusa početkom i sredinom 1990-tih godina, taj faktor je važio i za druge države Istočnog bloka i zemlje u razvoju. U bivšem Sovjetskom Savezu strukturne pretpostavke nisu bile povoljne kao u Bugarskoj: bilo je manje računara po glavi stanovnika i edukacija za rad na računarima je bila manje rasprostranjena. A i sami programeri živeli su udaljeni jedni od drugih. Nastanak supkulture koja programira viruse ovde je usledio nešto kasnije, ali to nije sprečilo da ih bije glas da su kovnica virusa (15). Poznati sovjetski, tj. ruski virusi su na primer: *Beer-, Leningrad-* i *Sverdlov*-virus.

Pored Bugarske i Rusije, i Aziju bije glas da je leglo virusa. Ove predstave su, pre svega, izazvane zbog nekih spektakularnih virusa koji su imali veliki odjek u medijima, kao na primer: Černobilski- ili Cih-virus sa Tajvana. A rasprostirao se preko demo igrica na CD-ima koji su bili u časopisima, zatim ILOVEYOU virus iz Pandakana, predgrađa Manile.

O virusima i vampirima

Poznati virusi doveli su do nastanka i učvršćenja predstave o leglima virusa. Ali, poznati virusi su dolazili i iz drugih država, a o njima nije bilo takvih predrasuda: *Melissa*-virus je programirao jedan Amerikanac, *Tequila*-virus je napravio švajcarski tinejdžer, a *Stoned*-virus su stvorili novozelandski studenti s univerziteta u Velingtonu. Bez obzira što ne postoje statistički podaci o proizvodnji virusa u celom svetu, predstava o nastanku virusa stvara određena težišta, tj. određena mesta – države. Virusni simbol antivirusnog *software*-a Dr.Solomona sjedinjuje sve te popularne predstave o poreklu virusa: insekt sa crvenim telom, obrve kao Leonid Brežnjev, kose oči i vampirske zube, a nos podseća na kinesko pismo.

U javnosti se rado opaža da pretnje dolaze spolja od strane imaginarnog "drugog". Balkan (koji se po predstavama u anglo-američkom podneblju prostire čak do Ingolštata, grada na Dunavu u Bavarskoj), već od 19. veka služio je kao upravo takvo mesto gde se fino mogu smestiti ono zlo i preteće. Recimo, "Drakula", Brama Stokera (Bram Stokers) dolazi iz Transilvanije (16) a u filmu Murnaua (F.W.Murnau) "Nosferatu", pacovi donose kugu iz bugarske Varne, a iz istog broda se u Vismaru (Nemačka) iskrcava i vampir. Efikasnost ovih simbola doprinela je i predstavama o poreklu virusa. Virus koji je poreklom iz Drakulinog grada Varne (kao MG, DIR ili Shake) deluje kao veća pretnja nego virusi iz Kalifornije.

Ta simbolika se koristi čak se i u kreiranju virusa van Bugarske: prvi virus za Windows 95, *Boza,* napravilo je članstvo australijske grupe za programiranje virusa koja se zove VLAD (kao Vlad Drakula). Drugi virusi nose imena kao *Werewolf* (vukodlak), a otkriven je u Francuskoj, ili Frankenštajn-virus koji je nepoznatog porekla. Azija je takođe već dugo

vremena simbol pretećih fantazmi, počev od najezde Mongola pa do žarišta novih bolesti: u Srednjem veku kuga je došla iz centralne Azije u Evropu (17), a vakcinisanje protiv gripa vrši se serumom dobijenim od gripa prethodne godine raširenog u Aziji. Čak su navodno i slinavka i šap preneseni krmom od ostataka hrane iz kineskih restorana. U SAD-u je predstava o Kinezima negativna, i to od *Chinese Exclusion Act*-a iz 1882. godine, pa preko "Bokserske pobune" sve do popularnog šlagvorta o "žutoj opasnosti". Sve to potkrepljuju i likovi sa kineskim atributima u pop kulturi, kao što je zli Ming iz serije Flaš Gordon ili Dr.Fu Manču. Preko takvih slika i simbola funkcioniše i stvaranje predstave o poreklu virusa. Tako je na primer i Fu Manču-virus nazvan po kineskom naučniku.

Virusi kao oružje *cyber*-terorista?

Već i sam nedostatak pouzdanih statističkih podataka čini da se na polju kompjuterskih virusa stvara idealno leglo za glasine i teorije zavere. Još ako se dodatno uzme u obzir i razvoj i pravac svetske politike, neizbežno je zaglibljivanje u močvari punoj špekulacija.

"Eksperti upozoravaju na opasnost od hakerskog delovanja" – to je bio naslov jednog članka u *San Francisko Examiner*-u, 7. decembra 1999. godine, u njemu je službenik Američke federalne policije FBI – Alan B. Kerol (Alan B.Carroll) upozoravao na napade na kompjutere i kompjuterske sisteme, reda veličina napada na Svetski Trgovački Centar (9.11.), i proricao da će Osama Bin Laden uskoro da učestvuje i u "*cyber*-terorizmu". (18)

Kako izgleda taj "*cyber*-terorizam"? Marta 2001. godine, pojavio se jedan pro-palestinski virus koji se zvao *VBS/Staplea* – jedan jednostavan *visual-basic-script* crv, koji je koristio Microsoft Outlook za svoje širenje. *E-mail* sa subjektom: "RE:Injustice" je imao *attachment* "injustice.txt.vbs". *Attachment* je onda slao dalje 'crve' na 50 adresa iz računara. Takođe je slao i na jednu listu od 23 *e-mail* adresa, uglavnom izraelskih vladinih ustanova, jedan mail sa pristojnim obraćanjem i sadržajem da se 'to' od njih nije očekivalo. I na kraju 'crv' priziva sa Internet Explorer-om listu URL-ova koji ukazuju na brigu o Palestincima. Na samom kraju, izvinjava se na smetnji i opisuje slučaj kada izraelski vojnik ubija dvanaestogodišnjeg Mohameda al Dura (Mohammad Al Durr). Pri detaljnijoj analizi ovog 'crva', nalazi se poruka, napisana manjkavim engleskim da je to bezopasan virus koji ne čini štetu na kompjuteru i da nema razloga za brigu. (19)

Ono što je pompezno nazvano "*cyber*-terorizam" uglavnom se svodi na slanje *e-mail*-ova ili na izmenu tuđih *website*-ova. Sve je to stvar definicije: pod informacijskim ratom, na primer, tajvansko ministarstvo odbrane smatra svako delovanje koje: "Vrši promenu svojih podataka koji su zaštićeni, a i podataka o neprijatelju". Jedna veoma rastegljiva definicija, pri kojoj bi se radilo o ratu čak i pri instalaciji kakvog skenera za viruse. (20)

Dokumentovani američki interes za vođenje rata virusima znatno je stariji od kineskog: General Karl Stiner (Carl Stiner), komandant specijalnih jedinica SAD-a, najavio je već početkom 1990-tih godina da će se sa kompjuterskim virusima napraviti haos u komunikacionom sistemu i elektronskom upravljanju oružja kod neprijatelja. Kada je

4. marta 1992. godine bio upitan od strane senatora Vilijama Koena (William Cohen) iz Komiteta za naoružanje, da li ima veze sa razvojem programa koji brišu neprijateljske kompjuterske baze, on je odgovorio: “Ne upuštajući se u područja koja se smatraju tajnom, rekao bih da to polje pokazuje veliki potencijal (...)”. Godinu dana kasnije je američka “School of Information Warfare and Strategy” primila svojih prvih 16 studenata. (22)

Pošto nakon kraja Sovjetskog Saveza nije bilo ozbiljnog vojnog neprijatelja sem Kine, morale su dodatne Davidovske teorije da održavaju budžet. Za kompjuterske napade nije potrebna vojna ili industrijska infrastruktura, i u zemljama u razvoju to izgleda razumljivo. Jedan takav napad je pogodna stvar za novinare, jer se o tome može pisati: prvo, što ne mora nešto zaista i da se dogodi, a drugo, što se ne moraju imati i prave informacije. Izvori za takve vesti uglavnom dolaze od bezimenih iz Pentagona, iz krugova vlade, tajnih službi ili neprecizno imenovanih bezbednosnih firmi.

Svaki migrant - potencijalni programer virusa

Pretnja se očekuje u stranom, neistraženom virtuelnom prostoru, i zbog toga upravo stvaranje te pretnje prate glasine kakve su pratile i vreme otkrivanja i osvajanja novih prostranstava van Evrope, i to od 16. do 20. veka. Putopisi su izveštavali, tj. pravili sliku o stranim kulturama, koja je Evropljanima dala mnogo razloga za osvajanje i ovladavanje tim oblastima: žrtvovanje ljudi, kanibalizam, slobodno seksualno ponašanje i rasna inferiornost. Uvedeni prigovori su se vremenom još i nadograđivali. Činjeni su pokušaji da se nadmaše prethodnici brojnijim i drastičnijim opisivanjem senzacija (23). Na taj način je, na primer, sledilo i idealno pravdanje, tj. nalaženje opravdanja za osvajanja kao što je to bilo u pismima Hernana Kortesa (Hernán Cortés): “Ovi ljudi su bili izuzetno nepokorni i ratnom silom sam ih zarobio. Pri tom su još jeli i ljudsko meso. Pošto je ovo opštepoznato, nije neophodno da vašem kraljevskom veličanstvu šaljem dokaze” (24). Ovo je napisao osvajač Meksika kralju Karlu V i na taj način je postavio shemu koja važi i za izveštaje o *cyber-* i virusnom ratu: ako dovoljno ljudi veruje u to, dokazi nisu potrebni.

Posledica takve histerije o virusnom ratu, osim žigosanja određenih država i delova planete kao legala virusa, je i stvaranje rastućeg nepoverenja prema manjinama. Programeri, koji su stranci ili su stranog porekla, oklevetani su, tj. dovedeni na loš glas kao potencijalni *cyber*-saboteri (25). Avgusta 1999. godine, časopis “Signal” objavio je intervju sa Ričardom Klarkom (Richard Clarke), nacionalnim koordinatorom za bezbednost, zaštitu infrastrukture i kontraterorizam. Zaposleni stranog porekla se u tom intervjuu žigošu kao potencijalni saboteri: “Mnoge američke *software* i *hardware* firme zavise u većem obimu od stručnjaka iz drugih država. Većina ovih ljudi ostaje u SAD-u i čak dobija državljanstvo, ali neki od njih bi mogli da služe neprijatelja, da li iz uverenja, zbog ucene ili podmićivanja” (26). 24. oktobra 1999. godine, izašao je članak u *Los Angeles Time*s-u u kome upozoravaju da pre svih indijski eksperti za kompjutere koji osposobljavaju američki Y2K kompjuter, istovremeno mogu na računare instalirati i upotrebljive viruse, doduše u tom izveštaju se citira jedan CIA-in saradnik koji označava Indiju i Izrael kao posebno aktivne države u

cyber-naoružanju, ali se ne navodi ni jedna konkretna činjenica za bilo koji slučaj (da se bilo gde upravo to desilo) ovakve zloupotrebe (27).

Zašto se stvara slika, tj. predstava da baš Azija predstavlja leglo virusa, a ne Afrika ili Južna Amerika – oblasti iz kojih su takođe dolazili virusi, kao na primer *Freddy, Z-90, Blood* ili *StinkFoot*. Ove oblasti ne predstavljaju ni vojnu niti ekonomsku potencijalnu pretnju, za razliku od Istočne Evrope i Azije. Predstava o kontinentu kao leglu virusa u slučaju Azije je ekonomski i vojno obojena. Rastućim tenzijama između SAD i Kine pridodaje se i privredno čudo u državama “Azijskih tigrova” u 1980-tim i ranim 1990-tim godinama. 1980-tih godina su Tajvan i Južna Koreja postale države izvoznice kapitala, a SAD uvoznik kapitala (28). Pre azijske krize, u američkim medijima je cela Istočna Azija pretežno predstavljana kao ekonomska opasnost. Ova situacija je i posle oporavka američke ekonomije u 1990-tim godinama imala povratno kulturološko i socijalno dejstvo: Amerikanci azijskog porekla su u okviru *Pacific Rim Viewpoint*–a viđeni kao produžeci azijskih nacija tj. azijskog kapitala i samim tim su bili potencijalna pretnja (29).

Stavljanje svetske politike na grbaču imigranata ima određenu tradiciju u SAD: iako su 1930-tih godina mnogi amerikanci japanskog porekla oštro osuđivali japanski imperijalizam, po početku rata je skoro 112.000 amerikanaca japanskog porekla bilo deportovano i internirano u dobro obezbeđene logore u središnjem delu SAD (30).

Virusi kao kazna zanepoštovanje autorskih prava

Pored birokratije ima još potencijalnih dobitnika histerije o ratu sa virusima, tj. virusnom ratu. Kao prateći uživaoci straha od virusa sebe vide i razni proizvođači regularnog vlasničkog softvera. Već nakon pojave prvih virusa, u nekim izjavama se pokazalo zadovoljstvo zbog očekivanog smanjenja umnožavanja i razmene softvera usled rizika da se prenese virus. Reuven Ben Zvi je u izraelskim dnevnim novinama napisao: “Kompjuterska zajednica je srećna što je zaustavljen proces neautorizovanog kopiranja softvera, koji je u skorije vreme poprimio neverovatne razmere. Upravo kao i SIDA, koja je proizvela fenomen sigurnog seksa, tako i kompjuterski virusi prizvode fenomen korišćenja legalnog softvera” (31).

Upitnija bi bila često izlagana pretpostavka da je nedostatak etike u korišćenju autorskih prava uticao na proizvodnju virusa: niti je – kako je na primer tvrdio Veselin Bončev (32): zaobilaženje zaštite od kopiranja imalo veze s razvojem (pre bi bilo da to pogoduje proizvodnji same zaštite), niti korišćenje nelicenciranog softvera čini da se prinudno gubi nada u sopstvene privredne uspehe od programiranja i usmerava kreativni potencijal na proizvodnju virusa.

U jednom ranijem intervjuu, *Dark Avenger* je napustio značajnu opsesiju autorskim pravima i istovremeno utvrdio da proizvodnja virusa i legalnog softvera koriste jedna drugoj: “Virusi bi se znatno manje širili kada 'nevini' korisnici ne bi krali softver i kada bi malo više radili na svojim radnim mestima, umesto da igraju kompjuterske igrice. Zna se, na primer, da je *Dark Avenger*-virus preko igrica dospeo u SAD iz Evrope (33).

Opasnija od virusa: zavisnost

Trajna i ozbiljna pretnja u to vreme narasta manje od zamišljenog planiranog virusnog rata iz Azije i Istočne Evrope, već iz realnih poslovnih i političkih praksi kakve su, između ostalog, primenjivali proizvođači antivirusnog softvera. Pretnja koju treba suzbiti nisu bili virusi, već zavisnost. Zavisnost koja nastaje preko patenata koji monopolizuju metode odbrane od virusa. Patenti kakvi u medicini ugrožavaju razvoj i proizvodnju generičkih lekova i alternativnih rešenja protiv SIDE u zemljama poput Južne Afrike i Brazila i kakvi se sve više pojavljuju i u području *software*-u. Finjan Softver, Inc., kalifornijski ponuđač sigurnosnog *software*-a je 1. februara 2001. godine davanjem patenta 6.157.520 preko *US Patent and Trademark Office*-a, obznanio svoju zaštitu od virusa *SURFIN Shield Corporate*. Patent se prostire na nadzor *download*-ovanja programa i sadržaja sa interneta u realnom vremenu do primene sigurnosnih odredbi na *download*-ovan program i na blokiranje programa ako se prekrše sigurnosne odredbe.

Aktivni *web* sadržaji predstavljaju potencijalni infektivni rizik zbog mogućnosti neželjenog pristupa datoteci, i time opasnost. Znatno veća opasnost je trivijalni patent koji sprečava razvoj rešenja za ophođenje sa ovom opasnošću.

Literatura

(1) Jurgen Kraus, "Selbstreproduzierende Programme", Dortmund 1981 (Forschungsberichte der Universitat Dortmund, Abteilung Informatik 110), und Frederick B. Cohen, "Computer Viruses", Los Angeles, CA 1986

(2) U društvenoj recepciji pravi se mala razlika između pravih virusa, crva i trojanaca. Stoga se i istraživanje tih fenomena mora sažeti pod pojmom "virusa".

(3) PM-Computer 10/87, Zit. nach Ralf Burger, "Das grof3e ComputervirenBuch", Diisseldorf 1989 [1987], S. 34-35

(4) Network Associates Inc., "Virus Information Library", http://vil.nai.com/vil/default.asp, 26. Marz 2001

(5) "F-Secure Virus Descriptions", http://www.europe.f-secure.com/v-descs/ arusiek.shtml, 31.03.2001

(6) John Elsbury, "Country Statistics", Online-Posting vom 14. Marz 2001, online posting od 14. marta 2001, odgovori dati istog dana, news:alt.comp.virus

(7) Yun-Sun Wee, "Re: Fwd: Re: Country Statistics?", e-mail od 19. marta 2001

(8) Bugarska imena transkribovana su prema ISO standardu, Tabela, 1 za transliteraciju južnoslovenskih jezika. Zahvaljujem se Maren Rot za savet i pomoć.

(9) Veselin Boncev, "The Bulgarian and Soviet Virus Factories", in: Proceedings of the First International Virus Bulletin Conference, Buckinghamshire 1991, S. 11-25,_http://www.complex.is/-bontchev/papers/ factory.html, 31. mart 2001

(10) Winn Schwartau, "Influenza, Malicious Software, and OOPS!", u: Winn Schwartau (Ur.), Information Warfare. Cyberterrorism: Protecting Your Personal Security In The Electronic Age, New York 1996 [1994], S. 148-166, S. 155

(11) Veselin Boncev, "The Bulgarian and Soviet Virus Factories", a. a. O.

(12) Karlhorst Klotz, "Die Virenjager", in: Computerviren'95, Chip Spezial Anwenderpraxis, Wiirzburg 1995, 48-50, S. 48

(13) Sarah Gordon, "Inside the Mind of Dark Avenger", u: Virus News International 20 (01) 1993, http:// vx.netlux.org/lib/asg02.html, 28. mart 2001

(14) "Interview with Skism One - AKA Lord SSS (triple S)", u: 40Hex 1 (2), http://www.ladysharrow. ndirect.co.uk/library/Magazines/40hex/ 40hex21.htm, i "The Dark Avenger", u: 40Hex 1 (2), http:// www. ladysharrow.ndirect.co.uk/library/Magazines/40hex/40hex21.htm, 20. mart 2001

(15) Veselin Boncev, "The Bulgarian and Soviet Virus Factories", a. a. O.

(16) Hans Schmid, Michael Farin i Arnold Loy, "Nosferatu. Fine Symphome des Grauens", Minhen 1999, S. 20 ff.

(17) Jacques Ruffie i Jean-Charles Sournia, "Les epidemies dans 1'histoire de 1'homme: essai d'anthropologie medicale", Paris 1984

(18) "Experts warn of hacker threat", u: San Francisco Examiner, 7. decembar 1999, http://www. businesstoday.com/techpages/hacker12071999.htm, 27. mart 2001

(19) "Sophos Virus info", http://www.sophos.com/virusinfo/analyses/ vbsstaplea.html, 27. mart 2001

(20) Florian Rotzer, "Taiwan sieht sich im Info War", u: Telepolis. Magazin der Netzkultur, 11. avgust 1999, http://www.heise.de/tp/deutsch/special/info/ 6466/l.html, 29. mart 2001

(21) "U.S. General Wants Ray Guns for Commandos", Reuters Newswire, 5. maj 1992

(22) Winn Schwartau, "Introduction to Information Warfare", u: Winn Schwartau (Ur.), Information Warfare. Cyberterrorism: Protecting Your Personal Security In The Electronic Age, New York 1996 [1994], S. 8-14, S. 8

(23) Erwin Frank, “Sie fressen Menschen, wie ihr scheuf3liches Aussehen beweist“, u: Hans-Peter Duerr (Ur.), Authentizitat und Betrug in der Ethnologie, Frankfurt/M. 1987, S. 199-224

(24) Osvajanje Meksika Ferdinanda Kortesa. Sa svojeručnim izveštajima vojskovođe kralju Karlu V iz 1520-1522. Leipzig 1918, S. 188 (Memoiren und Chroniken 3)

(25) George Smith, “Electronic Pearl Harbor: A slogan for U.S. Info-warriors“, http://www.soci.niu.edu/-crypUother/harbor.htm, 31. mart 2001

(26) Robert K. Ackerman, “Hidden Hazards Menace U.S. Information Infrastructure”, u: Signal, August 1999, http://www.us.nebsignal/Archive/ August99/hidden-aug.html, 27. mart 2001

(27) Elizabeth Shogren iBob Drogin, “Some Fear Sabotage by Y2K Consultants”, u: Los Angeles Times, 24. oktobar 1999, http://www.warroomresearch.com/MediaPresenSpeak/LATimes.htm, 27. Marz 2001 na Google-Archiv

(28) United Nations, World Investment Report 1992, Transnational Corporations as Engines of Growth, New York 1992, S. 14-24, und Steve Chan, Introduction, in: Steve Chan (Ur.), Foreign Direct Investment in a Changing World, Houndmills 1985, S. 1-2

(29) Glenn Omatsu, Recenzija: Mike Davis, City of Quartz, David Rieff, Los Angeles. Capitol of the Third World, und David Reid, Sex, Death and God in L.A., u: Amerasia journal 18 (3) 1992, S. 73-77, S. 75-76

(30) Su-Cheng Chan, “Asian Americans. An Interpretive History”, Boston 1991, S. 117-118 i 125

(31) Reuven Ben-Zvi, “The Virus Reached Haifa”, u: Ma’ariv. Zit. nach Philip Fites, Peter Johnston i Martin Kratz, “The Computer Virus Crisis”, New York 1989, S. 124

(32) Veselin Boncev, “The Bulgarian and Soviet Virus Factories”, a. a. O.

(33) Sarah Gordon, “Inside the Mind of Dark Avenger”, a. a. O.

Peter Milbauer (Peter Mühlbauer**)** živi u Minhenu i promoviše severnoameričku kulturnu istoriju.

O upozorenjima na viruse koja i sama postaju virusi, Virus-*Hype* i Virus-Histeriji, viralnom marketingu, *Hoax*-politici i umetnosti internet-*hoax*-a

On želi da napravi *hoax*

Armin Medoš

***Good Times*, klasični virus-*hoax* (1)**

Početkom decembra 1994. godine, na internetu je počeo da kruži jedan *e-mail*, čija prva rečenica je glasila: “Ovde je jedna važna informacija. Obratite pažnju na jedan fajl pod imenom 'Good Times'”. Nakon toga je kratki *e-mail* upozoravao da u America Online (AOL) cirkuliše jedan virus koji se širi putem *e-mail*-a. Ko god primi *e-mail* pod naslovom “Good Times” ne bi trebao niti da ga čita niti da ga sačuva. Radi se o jednom virusu koji bi pobrisao sve podatke sa *hard* diska, navodilo je dalje upozorenje na virus i zaključilo sa tim, da bi se to upozorenje trebalo “dalje poslati svim svojim prijateljima”, jer bi se na taj način i njima veoma pomoglo.

Već nekoliko dana nakon prvog zajamčenog pojavljivanja upozorenja na “Good Times”, CIAC, koji pripada Ministarstvu energetike Sjedinjenih Država, u službenom izveštaju od 6. decembra obelodanila je da je “Good Times” *e-mail* šala, da takva vrsta virusa ne postoji te da stoga ne preti ni opasnost od njega. Nije potrebno biti ekspert za kompjutere da bi se razumelo da se kompjuterski virusi ne mogu širiti posredstvom pukog otvaranja jednog *e-mail*-a. Virusi ili *e-mail* 'crvi' mogu biti skriveni u iscrpnim programima, koji sa *e-mail*-om bivaju poslati zajedno sa prilogom (attachment). Puki deo teksta jednog *e-mail*-a ne može pokrenuti takve događaje koji će izbrisati *hard* disk. Ipak, rasprostranjivanje virusa “Good Times” nisu sprečili niti relativno šaljivi karakter upozorenja na viruse, niti razjašnjavajuća obrazloženja AOL, administratora sistema, moderatora *mailing* lista, antivirus eksperata, firmi za zaštitu od virusa.

Lažni virus-alarmi raširili su se na univerzitetskim mrežama, na mrežama vlada i firmi, infiltrirali su se u *mailing* liste, *news*-grupe, *bulletin-board*-ove, prokrstarili su Atlantik i vrlo brzo su bili prevedeni na različite jezike. Nakon prvog vrhunca epidemije u zimu 1994/95 učinilo se da su popustili, ali je uvek iznova dolazilo do novih pojava takvih alarma. Kao kod glasina, ogovaranja i sličnih poruka koje se održavaju u životu tako što u miru “pošte koja se prenosi šaputanjem” bivaju dalje prepričavane, sadržaj “upozorenja” se vremenom proširio. U jednoj varijanti to znači da je “Good Times” opasan zbog toga, što pri njegovom očuvanju biva aktiviran *ACII-Buffer* računara. Jedna varijacija na tu varijaciju okončava u tvrdnji da je

"procesor izmešten u stanje beskonačnog binarnog proklizavanja n-te kompleksnosti", što bi naposletku vodilo ka uništenju procesora. Ni takva, očevidno pseudo-naučna zavaravanja nisu mogla da zaustave širenje "Good Times"-a. Usled toga je "Good Times" mutirao i ponovo se pojavio pod novim imenima, na pr. kao *Irina, Deeyeda*, a kasnije i kao *Penpal Greetings*, a na mreži je još i danas aktivan pod različitim identitetima, napokon i kao "It takes guts to say Jesus". Uprokos svim prosvetiteljskim podsticanjima snaga uma, "Good Times" i njegovi sledbenici su otporni na svoje potpuno gašenje. Upozorenje na viruse je i sâmo postalo virus.

Eksperti se spore oko toga sa čije strane je taj *hoax* (prevara) pušten u svet. U nekim izveštajima stoji da je "Good Times" istovremeno poslat od strane jednog AOL korisnika i jednog studenta. Međutim, ne postoji dokazivi, prvi izvor, kao što ne postoji ni pismo priznanja. Gotovo verodostojno, u smislu stvaranja legende, pojavila se teorija "spontanog nastanka" iz humusa interneta. Prema njoj bi se u naglašeno izokrenutom izveštaju moglo raditi o istinitom ili poluistinitom događaju. Prema jednoj drugoj varijanti postojalo je lančano pismo sa imenom "Good Times". Da bi se ono prekinulo, neko je u svet pustio buvu da "Good Times" sadrži virus. Naprotiv, trebalo bi biti dokazivo, da je pre "Good Times"-šale postojalo lančano pismo nazvano "Good Luck". U njemu je stajalo da bi dalje slanje tog lančanog pisma-*e-mail*-a donelo sreću svima koji u tome učestvuju.

Napad na racionalnost

"Good Times" i slični načini obrade teksta ne sadrže nijedan kôd koji bi poput pravog kompjuterskog virusa mogao da pričini štetu podacima napadnute mašine ili samom *hardware*-u. Ipak upozorenja na viruse, koja su i sama postala virusi, prouzrokuju objektivne štete. Upravo u velikim organizacijama može opasti produktivnost, ukoliko je polovina zaposlenih u potrazi za virusom koji ne postoji. Administratori sistema trpe od bombardovanja *e-mail*-ovima zabrinutih korisnika, strepnje za njihove računare i rada koji je zbog toga nagomilan. Jedan takav lažni alarm se naročito na *mailing* listama može zakotrljati prema principu grudve od snega. I demantovanje upozorenja od strane moderatora liste koje ukazuje da se radi o *hoax*-u ponekad ne može zaustaviti lavinu. Pod određenim okolnostima demantovanje upozorenja samo još više skreće pažnju na *hoax*. Pod teretom priloga diskusiji prouzrokovanoj od strane *hoax*-a, *e-mail* server može da bude položen na kolena. Izvesno je da se može sporiti o tome, koliko velike štete u obliku gubitka produktivnosti nastaju posredstvom virus-*hoax*-a. Sigurno je samo da se uvek iznova pronađe neko ko će nasesti na šalu i ponovo uhvatiti nit, te ponovo uspostaviti đavolji krug – ne postoji nijedna tobožnja tehnička "inekcija zaštite" protiv te vrste "virusa" poput one koju, primera radi, programi zaštite od virusa nude u odnosu na prave kompjuterske viruse.

Kompjuterski virus je jedan program koji se može pripojiti drugom programu, čijim aktiviranjem on onda upravlja tako što utiče na dalje širenje virusa, ali ponekad nanosi i štetu podacima i obavlja druge uništavajuće procese. Nasuprot tome, upozorenje na virus koje je postalo virus ne inficira mašine, nego ljude. Korisnik sebe stvara domaćinom jednog programa

koji sadrži jednostavno uputstvo za delovanje: "raširi me". Samim tim, ta vrsta "virusa" u stvari nije tehnička tema. Uspeh te vrste počiva na usudnom "social engineering"-u tj. na nadmudrivanju razumskih barijera i igranjem na kartu praljudskih osobenosti poput strepnje, praznoverja i spremnosti na pomoć. Taktike onih koji prave virus-*hoax* imaju više veze sa reklamom, književnošću, psihologijom i grupnom dinamikom nego sa tehnikom.

Da bi se poverovalo u njih i da bi se mogli dalje širiti, virus-*hoax*-i iziskuju određene setove pretpostavki. Relativno neiskusni korisnici kompjutera i interneta su ponajviše ugroženi od mogućnosti da dopuste da budu zaraženi lažnim upozorenjem na viruse. U *hoax*-viruse takođe se umešala klima virusne histerije koji su mediji poodavno stvorili. U jednom trenutku kompjuterski virusi su već osvojili naslovne stranice i to kada ih je još bilo relativno malo i kada većina ljudi još nije koristila lični računar, barem ne kod kuće. Moguće je da njihova atraktivnost kao medijske teme potiče odatle da virusi oslovljavaju duboko ukorenjene, iracionalne strahove – strah od epidemije koja se ne može kontrolisati, a izaziva iznenadne prekide funkcija u ljudskom organizmu koji se ne mogu objasniti, jer se o odgovarajućem pogonskom sistemu premalo zna. Ipak, pored podstrekivanja strahova virus-*hoax*-i bacaju i jedan mamac: onaj ko upozorenje pravovremeno pošalje dalje time postaje i omiljen kod svojih prijatelja, postaje spasilac zajednice. Upozorenja na viruse rado se odnose na autoritet, što znači da ih navode kao izvor istraživačkog rada neke od vodećih IT firmi ili službi za korisničku podršku nekih od vodećih internet provajdera. Naposletku, lažna upozorenja na viruse koriste određeno utišavanje glasa, tj. određen način pisanja i tipografske metode da bi u primaocu uspostavili stanje povećanog uzbuđenja u kojem se razum najčešće da nadmudriti. Oni često upotrebljavaju velika slova i mnoštvo znakova uzvika, što u *e-mail* etiketi odgovara urlanju u realnom svetu. Oni u primaocu često bude osećaj da je svedok jedne ekskluzivne, ali ekstremno važne informacije, utoliko što ukazuju na to da "za sada o tome niko ne zna", ali je virus ipak "za dvadeset i četiri časa već inficirao milione kompjutera". (Ne) logična posledica je da se deluje SADA, da se vest ODMAH mora dalje poslati SVIM PRIJATELJIMA.

Upravo taj šematski postupak koji se danas pre svega koristi pri *e-mail spam*-ovima u različitim varijacijama, virus-*hoax* u stvari čini lako prepoznatljivim. Onaj ko je jednom prozreo princip, semantičku i tipografsku konstrukciju takvih lažnih alarma, sa velikom verovatnoćom više nikada neće nasesti na to. A ko želi da bude sasvim siguran treba samo da pretraži jedan od anti-virus *site*-ova proizvođača ili univerziteta i da na potraži liste sa poslednjim pravim upozorenjima i poslednjim *hoax*-ima. Međutim, takav pristup koji se oslanja na činjenice upravo nije poenta ove stvari. Kada bi sve išlo sa racionalnim stvarima, "Good Times" bi izumro nakon dve nedelje.

Univerzum *Hoax*-era

Virus-*hoax*-i su programirani tako da nadmudruju razum, večnu sumnjalicu i poput trojanskog konja se ušuljaju u svet osećaja. Tamo oni umeju da pritisnu pravo dugme, da bi nas odobrovoljili da omogućimo njihovo umnožavanje. Utoliko je upozorenje na virus

poseban tip jedne veoma raširene vrste poruka koji se viralno širi na internetu. U to se ubrajaju dalji *hoax*-i koji se odnose na kompjuterske teme, pozivi na humanitarne akcije, piramidalna-lančana pisma i preko *e-mail* raširene urbane legende (bajke velikih gradova). Viralni marketing, te umetnički i literarni *e-mail hoax*-i su posebni slučajevi, o kojima će još biti reči. Valja spomenuti i probleme u vezi sa prekrajanjima i kategorizacijom sa *spam*-ovima (pogledati članak "Postani bogat, srećan i sit" Florijana Šnajdera) i sa *cyber*-, odnosno informatičkim ratom (videti članak "Ratnici u mrežama podataka" Ralfa Bendrata).

Čini se da su motivi *hoax*-a relativno jasni. Pri različitim formama *hoax*-a, u skladu sa njihovom definicijom, uvek se radi o momentu obmane. Neko sebi uzima slobodu da napakosti svojim bližnjima, utoliko što ih zavarava sa nečim što nije tačno ili ne postoji. Nagrada za te *hoax*-ere mogla bi biti oskudna radost, da pritom vide kako se 'patka' šiti mrežom. Mnogi *hoax*-i ipak imaju i dodatne motive. Oni su često komercijalne prirode kao na primer u slučajevima lančanih pisama, dok se kod nekih drugih može raditi o akcijama lične osvete, a drugi se opet usmeravaju u borbu Davida protiv Golijata, protiv moći režima ili velikih koncerna. Najkasnije od "Good Times"-a, *e-mail hoax*-i su postali deo folklora interneta koji više ne treba zanemarivati. Oni su neiskorenjivi poput *spam*-ova, ekstremno dosadni kada se pojavljuju u velikom broju, u najpovoljnijem slučaju su razveseljujući poput dobrog vica, a ponekad mogu imati i literarne kvalitete.

Prvi virus-*hoax* datira u 1988. godine (2), a odaziva se na ime "2400 baud modem virus". Jedan upozoravač koji se predstavlja kao ekspert, iscrpno opisuje u tehničkom žargonu kako se virus navodno širi posredstvom takozvanog "Subcarrier"-a - kanala koji se "normalno koristi samo za protokolarnu razmenu između modema". Nakon dužeg testa autor dolazi do rezultata, da stariji "1200-baud-modem time" nije pogođen i stoga savetuje da se upotrebljava samo taj sporiji tip modema. Jedna od najlepših 'patki', što se tiče kompjutera i interneta bio je *Internet-Cleaning-Day* koji je pre nekoliko godina bio proglašen u mesecu februaru. *E-mail* počinje sa iznenađujućom tvrdnjom "kao što mnogi od Vas znaju, internet svake godine mora jednom dvadeset i četiri časa biti zatvoren zbog čišćenja". Radi se o tome, da bi mreža morala biti očišćena od "mrtvih *e-mail*-ova, neaktivnih FTP sajtova, *Gopher* sajtova i WWW sajtova" (kao kada bi štetne arterijske materije bile obložene na unutrašnjim zidovima i time ugrozile krvotok). Da bi *Cash* i *Proxy* mogli biti očišćeni na najvažnijim čvorištima, korisnici računara koji su stalno povezani sa internetom bi jedan dan trebali biti skinuti sa mreže a svaki fizički kontakt bi trebao biti otkačen, da pri akciji čišćenja ne bi došlo do nenamernog brisanja podataka. Nažalost ne postoje informacije o tome, koliko *WEB master*-a se odazvalo pozivu. Jedan drugi internet-*hoax* za koji se čini da nikada nije izumro govori o *e-mail* porezu u Sjedinjenim Državama koji namerava da uvede Federal Communications Commission (FCC) u okviru jednog novog zakona. Široko rasprostranjeni su i *hoax*-i koji pozivaju na pomoć ženama pod talibanskim režimom ili na spasavanje bolesnog deteta.

U jednoj maloj privatnoj anketi obratio sam se ljudima koji su mi u prošlosti poslali te ili slične poruke. Jedno od saznanja koje sam stekao na osnovu odgovora jeste, da dalje slanje takvih *e-mail*-ova može biti bojažljivi pokušaj očuvanja kontakta. Pokušava se komunicirati

sa većom grupom ljudi, sa kojima se inače ne održavaju permanentni kontakti. Pritom dalje poslati *e-mail* služi kao jedna vrsta vizit karte, neko se čini korisnim, pokazuje koje interese ima, nije samo "na" mreži, nego i "pri" mreži, deo jedne kontaktne mreže *e-mail* istomišljenika. Kako pokazuju odgovori, pretežno je reč o ponašanju početnika sa kojim se prestaje najkasnije tada, kada *e-mail* koji je jednom bio poslat u uverenju da se čini dobro, nakon šest meseci ponovo završi u vlastitom *inbox*-u.

Mem je mem je mem

Suštinska tačka *hoax*-fenomena je da se daljim slanjem upozorenja na viruse ili poziva u okviru kampanje zamišlja "community" u kojoj se želi osetiti pripadnost. Internet nam pruža osećaj da "nismo sami tu napolju". Postojanje zajednice pretpostavka je za prihvatanje i dalje slanje tih *e-mail* virusa. I kreatori lažnih upozorenja i lančanih pisama međusobno na prikriveni način deluju sa zajednicom. Suštinski motiv je povezanost posredstvom mreže.

Paralelno sa fazom brzog rasta interneta iz čuvanih zajednica istraživanja, vojske i ponekih privrednih pogona u širu javnost, u opticaju su različita teorijska stanovišta – od "kolektivne inteligencije", preko "globalnog mozga", pa do "mimetike". Ona se odnose na one okolnosti koje omogućavaju virus-*hoax*-e i ne bi moglo biti slučajno, da te teorije svoje publicističke vrhunce slave upravo u fazi kada je "Good Times"-*hoax* doživljavao klimaks. Zajednica više nije ograničena na fizički svet, tračevi se više ne šire samo u kafeima, na zabavama i prilikom drugih društvenih dešavanja, već su elektronski ojačani i putem geografski raspršene zajednice interneta se ubrzano šire oko celokupne Zemljine kugle.

Pokušaj evaluacije i razjašnjenja filozofskih i naučnih stavova koji leže iza pojmova kolektivna inteligencija, globalni mozak i mimetika prevazišao bi temu ovog članka. Napokon, *mem*-ovi su, kao pokušaj objašnjenja širenja *e-mail hoax*-a, vredni okretanja jedne stranice (3).

Pojam *Meme* skovao je britanski istraživač evolucije Ričard Doukins (Richard Dawkins). Biološke pojmove gen i geneza on stavlja analogno razvoju ideja kao *meme* i *memesis*. Prema Doukinsu, meme su misli koje se oblikuju u jedinstva kojih se možemo sećati i koje odlikuje jedan fizički izraz. One bi bile prihvaćene od strane ljudi bez njihovog vlastitog učinka, tako da oni postaju domaćini tih *meme*-a. Upravo to se može reći i o virus-*hoax*-ima. Oni se mogu posmatrati kao set informacija koji vode računa o daljem vlastitom odgajivanju, a za to su im neohodni domaćini – mi ljudi. U ekonomiji pažnje oni egzistiraju u obliku *e-mail inbox*-a svakog pojedinog recipijenta. Tamo oni konkurišu mnoštvu drugih poruka: privatnim *e-mail*-ovima i onima koji se odnose na posao, pretplaćenim informatorima i *mailing* listama, *spam*-ovima. U toj naglašeno takmičarski orijentisanoj okolini, pre svega dva faktora odlučuju o tome da li ćemo otvaranje vesti uopšte smatrati vrednim truda. S jedne strane, to je adresa pošiljaoca i dotični naslov, sa druge. Budući da *hoax*-i najčešće funkcionišu uz pomoć trika da treba dalje da budu poslati prijateljima, oni ovde već beleže dodatni plus. A najviše uspešnih *hoax*-a imaju genijalno jednostavne naslove. *E-mail* pod

naslovom “dobra vremena” (Good Times) ili “pozdrav od jednog prijatelja” (Penpal Greetings) rado se otvara, naročito ako stiže od nekog prijatelja. Isti mehanizam je uostalom na delu i prilikom pravih kompjuterskih virusa koji bivaju šireni posredstvom *e-mail*-a, kao na primer “I LOVE YOU”, odnosno “Homepage”. I u slučaju komercijalnih *spam e-mail*-ova naslovljavanja postaju sve rafiniranija. U poslednje vreme naslovi na primer glase “from John” (gotovo svako poznaje nekog ko se zove Džon), “information that you requested” (da li sam u poslednje vreme zatražio neku informaciju? Može biti...) ili “Re: Your Future” (tema koja je uvek interesantna).

Ako je naslov shvaćen ozbiljno, *e-mail* je dakle otvoren, tada se stvar zakuvava. *E-mail* virusi i *e-mail* 'crvi' počivaju na tome da se ujedno otvara još i dodatni *attachment* (i funkcioniše u *e-mail* okruženju koje dozvoljava izvođenje *attachment*-a). *E-mail hoax*-i počivaju na tome da bivaju dalje poslati, kada im se poveruje, ili se barem smatraju dovoljno interesantnim, da bi bili poslati drugima. Ono što nakon toga sledi u saglasju je sa Doukinsovom teorijom mema, darvinističkim iščitavanjem u oblasti ideja. *E-mail hoax*-i nastoje da pobude što je moguće snažnije osećaje – strepnja, seks, profit, usamljenost, odnosno želja za pripadnošću, želja za vrednošću, znatiželja, potreba za važenjem - koji u nama okidaju evolucionistički okidač i nagone nas da panično pritisnemo dugme: *Forward*...

Kritičari mimetike ne slažu se sa time da je socijal-darvinističko učenje o evoluciji primenjivo na polju kulture. Oni argumentuju da se nalazimo u određenom periodu istorijskog razvoja civilizacije koji se u zapadnom svetu može identifikovati sa pojmovima kapitalizam i demokratija, a oni ipak ne mogu biti posmatrani kao istoznačni sa “prirodnim zakonitostima” evolucije. Napokon, prihvaćena pasivnost njima je trn u oku, budući da nas prema mimetici, parazitske *meme* koriste samo kao pasivne okidače (4).

***Hoax*-politika**

Središnji mit interneta je takozvana *Many-to-many* komunikacija, komunikacija mnogih sa mnogima, koji raskida sa tradicionalnim modelom slanja sa jednog centralnog izvora vesti koje se emituju mnogim primaocima. Doduše, ta teza nije dokazana jer retko se radi o jednom jasnom linearnom sledu razvoja, pri čemu bi jedan sistem zamenjivao drugi, ali dalje slanje vesti u mrežama prijatelja i poznanika putem interneta, ponekad se činjenično pokazuje kao moćna komunikacijska mašina. Najznačajniji izraz te decentralizovane komunikacije danas su tehničke *Pear-to-pear* mreže (P2P) u stilu Napster-a ili Gnutella-e. Ali, *Pear-to-pear* ponovo pokazuje svoju moć i bez tehničke realizacije, kao na primer početkom 2001. godine u slučaju *e-mail*-a koji se ticao firme *Nike*, a obišao je ceo svet.

Proizvođač sportske opreme ponudio je kupcima sprinterskih patika najvišeg kvaliteta mogućnost da robu personalizuju. Ukoliko za donekle uvećanu cenu poruče patike preko jednog *website*-a, na patiku će biti ušiven natpis prema vlastitom izboru. Kako kaže legenda, jedan američki student je poručio da mu ušiju reč “Sweatshop”. Taj pojam se odnosi na eksploatatorske prakse rada u fabrikama koje ne odgovaraju standardima zaštite radnika

zapadnog sveta – a firma *Nike* je već godinama trpela prigovore da u najmanju ruku toleriše iste takve “Sweatshop” prilike u subkontrarnim proizvodnim pogonima trećeg sveta. Kada je *Nike* odbila da mušteriji ušije takav natpis razvio se kako interesantan, tako i zanimljiv *e-mail* dijalog između mušterije i firme, pri kojem je uobraženi ispitivač uvek iznova bio prinuđen na “verbalno hvatanje krivina” od strane odgovornog predstavnika firme. Taj *e-mail* dijalog pušten je na mrežu i raširio se sa tendencijama viralne zaraze. Nakon što sam po prvi put video, taj *e-mail* na jednoj *mailing* listi, u roku od nekoliko dana sam ga primio barem dvadeset puta sa različitih strana. Teško se može prosuditi koliko velika je činjenična šteta putem kampanje *trkač* nanesena imidžu *Nike*, ali se svakako radi o slučaju *e-mail* zaraze koji je naposletku završio u etabliranim medijima i postao udarna vest širom sveta.

Ipak, bilo bi pogrešno slaviti takav događaj kao dokaz za decentriranu, demokratsku moć interneta i time ga proglasiti apsolutno dobrim. Takvi “rezultati” P2P-komunikacija počivaju na određenim pretpostavkama koje se teško mogu kontrolisati i ne daju se generalizovati. Drugi *e-mail hypes* skorašnje prošlosti pre svedoče o zgražavanju, kao u slučaju jedne engleske službenice. Ona se uplela u razmenu erotskih *e-mail*-ova sa ljubavnikom kojeg je skoro upoznala. On je radio u jednoj velikoj firmi i celokupne rezultate razmene je prepun ponosa poslao dalje na adrese pet najboljih prijatelja u firmi. Njima se to učinilo toliko zabavno da su *e-mail* smesta dalje prosledili svojim svagdašnjim prijateljima, i tako dalje i tako dalje. U roku od dvadeset četiri časa, navodno je milion ljudi imalo došlo u priliku da se naslađuje nenašminkanom diskusijom o oralnom seksu. (5)

Korišćenje *Bottom-up-Power* (mož odozdo) interneta za ambiciozni politički *hoax*, pošlo je za rukom birou za komunikacije Ubermorgen.com tokom američkih predsedničkih izbora 2000. godine. Ubermorgen.com se sastoji od Lucijusa Bernharda (Luzius Bernhard) – koji se pojavljuje i kao Hans Bernhard, Hans Ekstrem (Hans Etxtrem) i NET_Callboy – i partnerke LIZVLX, u svoje favorizovane taktike pored *hoax*-a ubraja i Šok-marketing i Drama-marketing. Ono što oni nazivaju “medijski-hack” predstavlja cilj i centar njihovog manevra obmanjivanja i konfrontacije: što pre je moguće dospeti na CNN.

To im je uspelo u jesen 2000. godine sa projektom *Voteauction.com*, što je *web* platforma za licitaciju glasova birača prilikom predsedničkih izbora u Sjedinjenim Državama, a takođe i prilično slobodna interpretacija slobodne tržišne privrede. Jedan američki student prvobitno je programirao *Voteauction.com* kao protest protiv prakse finansiranja predizborne kampanje u Sjedinjenim Državama, u kojoj firme i lobiji različitih branši putem vlastitih izdataka pokušavaju da steknu uticaj na buduću politiku. Nakon sudske presude u državi Nju Jork, sajt su preuzeli Bernhard i partnerka, uspostavili su server izvan SAD i posredstvom *e-mail* kampanje počeli su da skreću pažnju na akciju. Sa argumentom da bi, ako je politika potkupljiva, od toga trebali da imaju profita i obični birači, *Voteauction.com* je brzo raspirio kovitlac publiciteta. Pažnja američkih sudova je u svakom slučaju pobuđena, koji su putem presuda i prekidanja domena pokušali da doskoče očevidno ilegalnoj delatnosti. Međutim, to je glasačkoj licitaciji (kasnije je mutirala u *vote-auction.net*, gde se i danas može pročitati lični doživljaj u obliku izveštaja) pribavilo još više publiciteta, a na završetku medijskog *hack*-a bilo je preko četiri stotine novinskih članaka i televizijskih izveštaja, kao

i pet sudskih postupaka s tim u vezi, u različitim izbornim okruzima Sjedinjenih Država. Činjenično nije licitirao nijedan jedini birački glas, budući da je celokupna akcija od početka izgrađena kao lažnjak – ili *Web-Hoax*.

Viralni marketing

Zarazna moć virus-*hoax*-a i *e-mail* 'patki' napokon je zapažena i od strane onih koji se bave privredom. Od pre nekoliko godina već cirkuliše pomodni pojam "viralnog marketinga". Njegova polazna tačka je da se izvesne grupe konzumenata, pre svega medijski i robno osvešćeni mladi pokazuju kao sve otporniji u odnosu na klasične forme reklamiranja. Stoga se započelo sa suptilnim *brand*-iranjem, sa događanjima poput *clubbing*-a i *rave*-a, *snowboard* i *skateboard* dešavanja. Pritom je ultimativna ideja da sponzori više ne dovode svoj logo u vezu sa dešavanjem, već ono sami postaju dešavanje. Konzumenti treba da proizvedu kampanju vlastitim podsticajima, utoliko što će posegnuti za jedan od mamaca bačenih od strane firme i što će ga među sobom dalje deliti. U najpovoljnijem slučaju mamac, kao u slučaju "Flat Eric", može i sam postati pop zvezda. Asocijacija sa nalogodavcem onda usledi na zadnja vrata jer nipošto ne sme delovati da je kampanja nametnuta: sve mora izgledati tako, ako da je jedan takav "medijski-događaj" u stvari činjenično proizveden od strane samih kupaca.

Na sceni firmi za proizvodnju zaštite od virusa i *software*-a, viralni marketing biva shvaćen manje metaforično, a više praktično. Tamo već odavno ima sve više prigovora da pažnja koju mediji poklanjaju virusima i virus-histerija koja iz nje proizlazi, uopšte nisu toliko uzaludni. To doseže sve do okrivljavanja da su pravi virusi zapravo izuzeti iz medija, da bi se pravovremeno pripremila odgovarajuća digitalna zaštita (o tome vidi članak "Vi nas volite.txt.vbs" Janka Retgersa).

Čak i najveće branše su već podlegle naklapanju kada se radi o tome, da se usisavanjem virus-*hypes* poput *Melissa* i *I LOVE YOU*, mreža korisnika povećava. Međutim, čini se da su oni koji posredstvom negativnog publiciteta pokušavaju da povećaju svoje učešće na tržištu najčešće mali autsajderi. Izveštaji na udarnim *websites* poput *vnunet.com* svedoče o takvim slučajevima, u kojima su firme širile upozorenja o navodnim epidemijama virusa, a za ta upozorenja se naposletku ispostavilo da su drastično preterana. Vrhunac ironije nastaje kada, kao što se već događalo, *software* za zaštitu od virusa i sam proizvodi lažna upozorenja na viruse. Opravdano upozorenje manjeg proizvođača na 'crv' koji se nalazi na *homepage* - virus-skener renomiranog proizvođača treba pogrešno da identifikuje kao virus, te da nakon toga pošalje upozorenje na virus. Na kraju se čini da ni sami programi za zaštitu od virusa više nisu zaštićeni od virus-*hoax*-a.

Jedan izdavač knjiga sebi može pripisati sumnjivu slavu koja se sastoji u zastupanju klasičnog virus-*hoax*-a kao sredstva za podsticanje prodaje proizvoda koji nema veze sa kompjuterom. Godine 1996. na ekranima se pojavilo upozorenje na viruse pod naslovom "Irina" (6). Jedan istraživač virusa prepoznao je sličnost sa "Good Time" *hoax*-om, raširivši svoje saznanje na odgovarajućim *bulletin board*-ovima. Prema jednim engleskim dnevnim

novinama, radilo se o *PR-Gag*-u koji je dospeo na stranputicu. Izdavaču *Penguin Books* palo je na pamet da na *web*-u objavi roman pod naslovom "Irina". Tadašnji direktor *Electronic Publishing*-a imao je zadatak da lažno upozorenje na viruse "Irina" pošalje izabranim časopisima, svakako bez spominjanja *Penguin Books* i njihovog projekta interaktivne knjige. Kao pošiljalac upozorenja na viruse naveden je profesor Eduard Predo (Edward Prideaux) sa (nepostojećeg) "College of Slavonic Studies in London".

Pojam "viralnog marketinga", tri mladića iz Holandije shvatila su previše doslovno. Oni su priznali krivicu za slanje *homepage* 'crva' u svet (7). Iskoristili su *feature* koji je u međuvremenu postao široko poznat, naime da Microsoft Outlook putem jednog API može pokrenuti druge programe za izvođenje *Scripts*. "Homepage" je funkcionisao tako da bi korisnik koji klikne na *attachment* HOMEPAGE.HTML.VBS, između ostalog, otvorio četiri prozora Internet Explorer-a koji vode ka porno-*site*-ove. Nije poznato da li su autore i činjenično povezivali poslovni interesi sa tim porno-*site*-ovima. Prema njihovim vlastitim izjavama oni su se samo nadali da će sa svojim crvom započeti karijeru u stvarima viralnog marketinga i da će ljudima moći da pokažu "radost da se na mreži bude zloban".

E-Mail-Hoaxes u umetničkoj sceni na mreži

Kao što se moglo i očekivati, *e-mail hoaxes* su u umetničkoj sceni na mreži stekli veliku popularnost. *Hoax*-i imaju veliku tradiciju pre svega u književnosti. Rasprave iznošene u prepisci između rivalskih frakcija, članci i pamfleti potpisani lažnim imenima i vesti širene u klevetničkoj nameri, određivali su međusobne sporove generacija umetnika, izazivajući u njihovim krugovima velika talasanja – pri čemu su pojedinci izvan tih krugova na te provokacije najčešće ostajali u potpunosti hladni. Tako se odvijala i elektronski ubrzana komunikacija umetničke scene na mreži u drugoj polovini devedesetih godina. Ta faza donela je ponovno oživljavanje neokonceptualizma oslonjenog na mrežu, pri kojem se često činilo da je komunikacija važnija od produkcije umetničkih dela. To u svakom slučaju nije prigovor, već stav. U doba burnog razvoja čisto nastavljanje kretanja duž razvojnih linija novih ideja čini se važnije nego ustrajavanje na jednom pronađenim istinama. Pod tim stanovištem valja sagledati budni interes za *hoax*-taktike u umetničkoj sceni na mreži, pri čemu je navođenje lažnog identiteta u *e-mail*-ovima i širenje lažnih činjenica pod takvim pokrivenim-identitetima, jedan od najomiljenijih načina postupanja.

Onaj nepoznati *Hoaxer*, koji je na mailing listi *Syndicate* pokušao da inscenira sukob između teoretičara medija Herta Lovinka (Geert Lovink) i aktiviste mreže, odnosno ICANN-specijaliste Ted Bajfilda (Ted Byfield), odviše opušteno je shvatio *hoax*-taktiku. U svakom slučaju, gotovo niko nijedne sekunde nije poverovao u to. Jednostavno se nije uklapalo u profil ličnosti tih prepredenih zvezda scene na mreži, da jedan drugom javno nabacuju prejake izraze poput "seronjo". Pošiljalac takođe nije bio zaista vešto prikriven, već je lako putem analize *e-mail* uzglavlja identifikovan od strane anonimnog Šveđanina koji mu je odgovorio na *mail*. Mnogo više truda uložio je *Hoaxer* koji je preuzeo *e-mail* identitet umetničkog kritičara i teoretičara Timoti Drakrija (Timothy Druckrey), kao i pisca i umetnika

Marka Amerike, šaljući pod njihovim imenima priloge na *mailing* liste koji su se činili prikladni da izazovu nezadovoljstvo i da formiraju raspoloženje protiv Drakrija i Amerike. Protiv njih ili protiv *Hoaxer*-a radila je činjenica da i Drakri i Amerika neguje krajnje individualni stil pisanja koji uprkos očevidnog truda nije mogao biti zaista verodostojno imitiran. Uprkos tom nedostatku "mnogo buke ni oko čega" imalo je barem izvesnu literarnu auru.

Da su male, tesno povezane zajednice na mreži naročito prikladne kao ciljevi *hoax*-a, pokazao je onaj *hoaxer* koji je 1999. godine diskreditovao odluku za dodeljivanje nagrade umetničkog festivala medija *Ars Electronica* (8). Tada se radilo o *e-mail*-u koji je na udarne *mailing* liste poslat tačno početkom festivala, pobudivši privid da je poslat kao protestna nota od strane četiri od pet članova žirija nagrade *Prix Ars* u kategoriji *.net* umetnost. Prestižna nagrada je 1999. godine dodeljena je poslovnom sistemu Linux. Četiri navodna člana žirija žalila su se da je glasanje petog člana žirija bilo izmanipulisano u interesu sponzora festivala. Festival su sponzorisala velika IT-preduzeća koja su planirala, tako se moglo pročitati u obaveštenju, da ponude i samu Linux distribuciju, pa su stoga podmitili jednog člana žirija da bi još više favorizovali Linux-Hype. Premda su u potpunosti pali sa neba, ti prigovori su igrali na kartu očekivanog ponašanja u zajednici na mreži i nesputanog priključivanja na Linux-Hype koji je tada dosegao svoj prvi vrhunac sa rezultatom da je proključala kuhinja za zakuvavanje tračeva u umetničkoj sceni na mreži. Jednom probuđenu sumnju više nije moglo u potpunosti da odstrani iz sveta ni prikrivanje *hoax*-a na *Telepolis*-u.

Gotovo legendaran je kombinovani *e-mail* i *web-hoax* koji je početkom 1996. godine inscenirala grupa umetnika *Etoy* sa "Digital Highjack"-om. Etoy je najpre uz pomoć *software* robota analizirala pet najfrekventnijih internet pretraživača da bi ustanovili koji pojmovi za pretragu bi najčešće bili u opticaju, odnosno kako ti pojmovi moraju biti aktivirani u izvorni kôd *wesite*-a, da bi u redosledu (ranking) mašine za pretragu bili što je moguće više pozicionirani. Tada je redosled funkcionisao na temelju principa koji su bili doista jednostavni. Odgovarajući pojam za pretragu morao bi se javljati što je moguće češće, svakako u tekućem tekstu a ne jednostavno pedeset puta ponovljen u HTML-Tag-u na početku opisa stranice. U skladu sa zadobijenim rezultatima, Etoy je programirao *website* koji je često sadržavao pojmove za pretragu poput "sex" i "Porshe", sa ciljem da, ukoliko je moguće, dospe među prvih trideset izlistavanja neke pretrage. Kada bi oni što pretražuju stigli na Etoy-*site*, uz pomoć *Refresh Metatag*-a koji je u unapred programiranim intervalima bez ikakvog učinka korisnika, pozivao nove stranice. Korisnici bi "ostali zarobljeni" u njihovom *website*-lavirintu. Na taj način, Etoy grupi je pošlo ua rukom da za svega nekoliko meseci "otmu" milion i po korisnika. Sa pratećom *e-mail* kampanjom i za to adekvatnom, ekstremnom retorikom o "digitalnoj otmici", Etoy je dospela u tada veoma uticajni *Wired-Magazine* i dobila je prvu nagradu u kategoriji umetnosti na festivalu *Ars Electronica* (9).

U sličnom duhovnom ambijentu odvijale su se i akcije grupe RTMark, koja se specijalizovala za dizajniranje lažnih *website*-a političara i firmi, i najstojeći da plimu poseta skrene prema tom *site*-u balansiranjem između činjenica i fikcije. Hit Banting (Heath Bunting) i Rejčel Bejker (Rachel Baker) su nastojali da lansiraju upravo praktične ludorije koji su preko svog servera *irational.org,* između ostalog, izdavali i lažne studentske legitimacije

iz Meksiko Sitija, nagovarali surfere na živciranje svojih sugrađana putem policijskih *web* kamera, a zajedno sa ruskim umetnikom Aleksejem Šulginom (Alexeij Shulgin) dodeljivali su "zlatne internet medalje" najnemaštovitijim korisničkim *Homepages*. Umetnički par *Jodi* dizajnirao je *website* koji se igrao sa korisničkim strahom od *browser-crash*-a, virusa i rušenja sistema. U jednom ranijem radu Jodi se i eksplicitno pozvao na omaž "Good Times" *hoax*-u. Zajedno sa Vukom Ćosićem, umetnikom koji živi u Sloveniji, Banting, Bejker i Šulgin su mogli zahtevati da se pojam net.art oblikuje u istom tom rukopisu i da odlučujuće utiču na ranu umetnost na mreži. Čini se da je njihov poslednji zajednički *hoax* da su se – izuzimajući Jodi – od otprilike 1999. godine deklarisali kao "retired net.artists", takoreći rano penzionisani umetnici mreže.

Ono što povezuje pomenute umetnike moglo bi biti okarakterisano kao uspešni viralni marketing na mreži. Bez prisustva na uobičajenim instancama pogonskog sistema umetnosti, oni su sebi stvorili publiku čisto putem komunikacije na mreži, a samim tim i izvesan stepen slave. Rasipanje medijalnih virusa koji se poput trojanskog konja uvlače u sisteme koji prerađuju informacije korisnika, povećalo je njihovu vrednost na mreži – bolje rečeno na engleskom "net value" - kao umetnika. Na sličan način je u poslednjih par godina "Netočka Nezvanova" (koja se docnije pojavila) postala ekstremno poznata osoba na mreži – po dobrom kao i po lošem.

Pod pseudonimom Netočka Nezvanova (Netochka Nezvanova) koji je pozajmljen iz jednog romana-fragmenta od Dostojevskog, pomenuta osoba je razvila sasvim ličan *e-mail* stil. Po promenljivim korisničkim adresama i domenima poput "god-emil", "m9ndfukc" i napokon "relativno" konstantnim domenom "integrer", svoje *e-mail*-ove ona je formatirala tako, kao da su prošli kroz ludo zabavni program mešanja slova. Prema zakonitosti koju je bilo teško prozreti, pojedinačna slova bi bila zamenjena drugim znakovima ASCII-kôdovima poput uzvičnika, zareza, zagrada i brojeva. Rezultat je ponekad podsećao na programski kôd, a nekad opet na prirodni jezik pri čemu je ovaj potonji bilo teško razlučiti. Samo onaj ko se upustio u taj kôd i potrošio mnogo vremena na njegovo dešifrovanje mogao je isfiltrirati nešto poput značenja iz *mail*-ova Netočke Nezvanove. Sa tim *e-mail* stilom ona se vrzmala oko brojnih *mailing* lista i njihove moderatore dovodila do napada besnila. U svojim najlošijim danima bombardovala je *mailing* liste sa tucima takvih vesti, što je dovodilo do isključenja niza foruma. Pri okršajima koji su se pritom razgoreli, mnoge muške *mail* moderatore ona je rado psovala kao "mail korporativni fašisti", što ih je samo još više izluđivalo. Pri delimično visokom broju dnevnih *post*-ova, razumljiv je bes moderatora i učesnika na listama. Ono što ipak začuđuje jeste stepen neprijateljstva koji provocira takav stil komunikacije. Premda njeni *e-mail*-ovi nisu sadržali virus i nisu iznosili upozorenja na viruse, čini se da njena tehnika na suptilan način oslovljava virus-paranoju. Oni su se pojavljivali kao neka vrsta prljavštine na forumima koji su u stvari predodređeni za racionalnu diskusiju – haotične zbirke ASCII-znakova siglaniziraju opasnost od subverzije i zaraze zajedno sa strahom od onoga što se ne može identifikovati. Muškarce određenog karakternog sklopa njene poruke doista mogu dovesti do ivice ludila, pa se utoliko njihov paušalni prigovor i ne čini sasvim neutemeljen. Pritom se Nezvanova *e-mail*-ovi u stvari veoma lako mogu identifikovati,

pa samim tim i profiltrirati bez ikakvog posebnog truda. Ali, pri podrobnijem uvidu, oni sadrže zaista suptilne vesti koje se često na dekonstruktivan način odnose na prethodnu poštu i uokviruju se sa ASCII-grafikom i indirektnim komentarima. Čitljivi redovi koji su tu između moduluju i variraju određene teme, poput "umetnost mašina", "memepool" i druge zanimljive reči insajderske kulture na mreži. Putem konsekventnog prikrivanja vlastitog identiteta, Netočka Nezvanova je stvorila umetničku ličnost u kojoj je postala ultimativna *hoax*-kraljica mreže. Njeni *e-mail*-ovi bude asocijacije, kao da negde na mreži postoji neka veštačka inteligencija koja permanentno reciklira novosti, meša značenja, izaziva konflikte i sa proročkim kvalitetima dešavanjima na mreži daruje čaroliju koja se inače tako retko može osetiti u uobičajenoj fiksiranosti na korist i produktivnost mreže (11).

Rezime

Moja namera sigurno nije da nešto ulepšavam. Kada bih u svom vlastitom sistemu pronašao virus, odmah bih ga bezobzirno istrebio. Lažna upozorenja na viruse prouzrokuju nepotrebne troškove upravo u većim organizacijama. *Hoax*-i se mogu svrstati na granici prevare ili preko čak prelaze preko nje. Ipak, sa druge strane, obmane koje su provođene sa različitim namerama, a koje smo ovde opisali, imaju i određenu korist. One nisu toliko razorne, niti imaju, poput virusa koji zaista formatira *hard* disk, neposredne fatalne posledice. Parazitske vesti koje opsedaju imuni sistem naše pažnje, poput virusa u stvarnom životu, ako već od njih ne obolimo nego ih savladamo - mogle bi čak ojačati imuni sistem. One doprinose da budemo budnog duha i održavaju vrlinu zdrave skepse. Takođe doprinose i raznolikosti vrsta, donose nove nijanse, stvaraju podsticaje. Odbrambena borba protiv takvih virusa može delovati poput dopinga. Odbrambeni mehanizmi koje pritom razvijamo mogu nam pomoći i u prosuđivanju drugih situacija, kao na primer kada mediji generišu određene *hype*s, ili kada politika pokušava da polarizuje na prostački način. Ukratko, koliko god ta vrsta virusa u pojedinačnim slučajevima mogla biti dosadna, toliko je njeno postojanje u celokupnom sistemu možda manje nedostatak, a više znak za nužnu diversifikaciju. Život sa virusima nas može učiti toleranciji koja se naspram života pokazuje kao velikodušna. Oni "prljaju" naše sisteme ali ih time takođe i obogaćuju. Teoretičari evolucije su u poslednjih nekoliko godina ustanovili da bez parazitskih formi života verovatno ne bi bilo ni života (12). Utoliko i težnja za njihovim potpunim istrebljenjem znači i dodeljivanje otkaza životu. Potpuna uspešnost bi mogla biti idealna, ali njeno dosezanje sprečava svaki dalji razvoj. Zato, pohvalimo *Hoax*-kulturu.

Literatura

(1) Opširne informacije o "Good Times"-u nalaze se u nemačkom prevodu Good-Times-Scherz-Faq na stranici http://www.rafael-seifert.de/goodtime.htm Opšte informacije o virus *hoax*-ima nudi, primera radi Hoax-Info-Service TU-Berlin na: http://www.tu-berlin.de/www/software/hoax.shtml

(2) Ferbrache, "A Pathology of Computer Viruses", Springer, London, 1992

(3) Interesantno je da su i sara Gordon, Ričard Ford i Džoe Vels u jednom inače stvarno dosadnom tekstu o Hoaxes i Hypes na anti-virus stranicama IBM dotakli teoriju mema. IBM Virus Research Papers, http://www.research.ibm.com/antivirus/SciPapers.htm

(4) Više o temi memetike u "Meme-Special": Telepolis, http://www.heise.de/tp/deutsch/special/mem/default.html

(5) Michaela Simon, "Fütter mein E-mail Ego", u: Telepolis http://www.heise.de/tp/deutsch/inhalt/co/4494/1.html Website sa celokupnim e-mail dijalogom http://www.bradley-chait.formosa.ch/

(6) Virus Myths Web sajt: http://www.Vmyths.com

(7) Florian Rötzer, "Virales Marketing buchstäblich genommen?", u: Telepolis, http://www.heise.de/tp/deutsch/special/auf/7596/1.html

(8) Armin Medosch, "Email-Fälscher spielt Ars Electronica bösen Streich", u: Telepolis: http://www.heise.de/tp/deutsch/inhalt/sa/3424/1.html

(9) Etoy, http://www.etoy.com

(10) Jodi.org, Hommage an Good Times, http://404.jodi.org/

(11) Website Netochka Nezvanova, http://m9nfukc.com/

(12) Florian Rötzer, "Ein Lob der Parasiten": Telepolis, http://www.heise.de/tp/deutsch/special/mem/2087/1.html

Armin Medoš (Armin Medosch) je saosnivač i urednik online-magazina *Telepolis.*

Spam: Tamna strana E-Comerce

Budi bogat, srećan i sit!!!

Florijan Šnajder

Događaj iz poslednjeg dana 1936. godine: Džej C. Hormel (Jay C. Hormel), fabrikant kobasica iz Ostina svoje prijatelje, saradnike i poslovne partnere pozvao je u svoju privatnu kuću na proslavu nove godine. U stvari, trebalo je naprosto slaviti, ali častoljubivi mladi preduzetnik Hormel nije se mogao tek tako dati: pošto je neodložno tražio odgovarajuće, nezamenjivo ime za pobedonosni hod revolucionarnog inovativnog proizvoda, goste okupljene na zabavi pozvao je na jedno takmičenje. Obećao je stotinu dolara onome, kome bi već u novogodišnjoj noći sinula ideja kako bi ubuduće trebalo nazvati kobasice, zapakovane u mala limena pakovanja. Sa porastom konzumiranja alkohola predlozi su bivali sve bolji i bolji, sve dok napokon u poodmaklim satima glumac Kenet Denjo (Kenneth Daigneau), brat potpredsednika "Hormel Foods Corporation" nije stavio nagradu u džep. On je došao na ideju da spoji prva i poslednja dva slova od "Spiced Ham" u veštačku reč "Spam".

"SPAM Luncheon meat", kako se od sada trebao zvati proizvod, sastoji se od šunke, svinjske plećke i mešavine začina koja se čuvala u strogoj tajnosti. Utoliko su intenzivnije bujali komentari oko mesnog nareska: ljubitelji su vojevali verske ratove u vezi sa pitanjem da li bi ružičastu masu trebalo seći na trake ili je bolje na šnite. Britanci tvrde da zbog toga Drugi Svetski rat nisu samo pretrpeli, nego su u njemu i pobedili. Američki veterani reklamirali su SPAM upravo putem njegovog odlučujućeg ratnog značaja: oni su se borili što žešće, da bi što je moguće pre mogli ponovo da jedu hamburgere i svinjski stek, a nikada više SPAM. A legendarna omiljenost SPAM-a među stanovnicima pacifičkog ostrvskog arhipelaga mogla bi biti u vezi sa ranije praktikovanim kanibalizmom.

Neverovatna svedočanstva virtuelne veličanstvenosti

SPAM (1) pravno je zaštićena robna marka u 101 zemlji na svetu od strane "Hormel Foods Corporation". To je potpuno uzaludno jer ono što se u međuvremenu najčešće razume pod *spam*-om sa prvim dnevnim obrokom ima jednako malo veze kao i svinjska kolenica sa Havajima. U uobičajenom slengu interneta, *spam* važi za elektronske poštanske pošiljke, neželjene reklame, *junk e-mail*-ove ili, kako se zvanično zove "Unsolicited Commercial Email" (UCE) ili "Unsolicited Broadcast Email" (UBE).

Za puritanske grupe na mreži *spam* naprosto otelovljuje zlo, još veće od dečije pornografije i nacističkih *site*-ova. Dakle, reč je o vestima koje najčešće započinju rečenicama poput: "Mnogo hvala na Vašem interesu…", "Molim Vas pročitajte ovu vest dva puta!" ili "Gotovo da sam dopustio da mi se upropasti ova prilika…" i onda sadrže ponude koje, kada bi se shvatile doslovno, doista ne bi mogle biti odbijene: "Finansijska nezavisnost zauvek", "50.000 dolara u narednih devedeset dana", "Momentalno vraćanje dugova", pa sve do "Preokretanje procesa starenja". U *spam*-ovima se često radi o sumnjivim ponudama poput pornografskih, ili o pristupu nepoznatom *software*-u koji je dosada držan u tajnosti, o izradi putničkih isprava, ili o dekoderu koji navodno otključava TV-programe koji podležu pretplati. Da i ne govorimo o gotovo neverovatnim svedočanstvima virtuelne velikodušnosti: skupoceni mobilni telefoni nude se besplatno, gratis porno filmovi, besplatne deonice firmi, gotov novac u ruke…

To da sada ukalkulisani mesni narezak mora važiti kao metafora za jednako suvišnu kao i uznemiravajuću komunikaciju, prema legendi potiče od jednog klasika engleske komičarske trupe "Monty Python" (2). Skeč iz 1970. godine (3) odigrava se u jednom restoranu u kojem se služe isključivo jela sa mesnim nareskom. Gospođa Ban, koja je gošća zajedno sa svojim mužem, preklinjući moli jelo bez *spam*-a, ali njeno protivljenje biva ugušeno od strane vikinškog hora koji je sve glasnije pevao pesmu "Spam, lovely spam, wonderful spam".

Reklame za zelenu kartu i politička propaganda

Slično su se morali osećati i korisnici Usenet-a početkom devedesetih godina kada su postali žrtve prvih *spam*-napada. Zloslutni Serdar Argik (Serdar Argic), poznat i kao "Zumabot", "Ahmed Cosar" ili "Hasan B-) Mutlu" verovatno je prvi serijski *spam*-er u istoriji interneta, prapredak svih neželjenih vesti (4). U samo dve nedelje, Serdar Argik mogao je poslati više od sedam megabajta smeća od podataka: 935 poruka, u proseku 66 dnevno ili pola procenta celokupne količine podataka Usenet-a. Argikove namere su bile isto tako nekomercijalne kao i rana istorija interneta. Za njega se radilo o tome, da uz pomoć bezbrojnih poruka opravda genocid nad Jermenima tokom Prvog svetskog rata. Krajem aprila 1994. godine, Argik je od dana do dana obavljao svoje aktivnosti, a korisnici Usenet-a spekulišu do danas ko je zaista skriven iza fasade fanatičnog mrzitelja Jermena.

Tek u aprilu 2001. godine na Slashdot-u pojavila se misteriozna vest koja je iznela neke naznake o identitetu prvog *spam*-era. Argik, odnosno Kozar, služio se jednim malim *script*-om koji je automatski citirao prvu rečenicu uobičajene Usenet pošte, produkovao je slučajno izabranu psovku i onda bi dalje nastavio sa pro-turskom propagandom (5). Zbog čega se on tako iznenada nametao, trebalo bi da je u vezi sa tim, da je izgubio svoju US vizu te da više nije raspolagao pristupom internetu. Drugi izvori iza Argika naslućuju US ili tursku tajnu službu, ali jedno je sigurno: u istorijske knjige interneta Argik je ušao kao prvi *spam*-er, a čak i njegove žrtve su mu posthumno odavale počast na majicama (6).

Kao legitimni Argikovi naslednici važe "Cantel&Siegel", advokatska kancelarija iz Finiksa koja je na stotinama diskusionih foruma nudila svoje usluge imigracionih savetnika toliko glupo i drsko, da su se na hiljade korisnika Usenet-a odlučile na protiv-odbranu zatrpavši "Cantel&Siegel" sa protestnim *e-mail*-ovima (7). U to doba to je još bilo oprobano sredstvo: dubiozna kancelarija je od strane svog internet provajdera dva puta bila isključivana zbog nečasnog ponašanja u pristupu mreži. Ne mogavši tada čak ni u snu da zamisli da na taj način ulazi u istoriju, moderator jedne *news* grupe upozorio je advokata Lorensa Kentela (Laurence Canter). Ipak, ovaj se zajedno sa svojom partnerkom Martom Zigel (Martha Siegel) video na vrhuncu istorijske misije - priključivanju mreži u komercijalne svrhe. U skladu sa tim, oboje su samosvesno održali lekciju svim protestima. “Ukoliko pogledate pažljivije na sve što se događa, pronaćićete grupu *oldtimer*-a koji ne žele da njihovi privatni domeni budu ugroženi.“

Mogućnosti virtuelne selekcije smeća

Navodni večni-ječerašnji uskoro su osnovali vlastitu *news* grupu “alt.current-events.net-abuse” gde je onda po prvi put opširno diskutovano kako bi mogla biti zabranjena zloupotreba korišćenja Usenet-a. Dosta pre nego što je bilo uopšte govora o *E-Business, E-Comerce* i *New Economy*, ovde se diskutovalo kako bi se moglo zabraniti raspojasano dilovanje, prevara i bezgranično nadmudrivanje. U suprotnosti od telefonskog marketinga ili reklamnih fakseva pri Usenet- ili *e-mail-spam*-ingu, primalac, napokon, plaća račun za neželjeno primljenu poštu. *Spam*-era masovno slanje košta samo par eura za saobraćaj plus samo jednom nešto više od stotine eura za sijaset miliona *e-mail* adresa. Uz pomoć naročitog programa one bivaju ulovljene sa *website*-ova, arhiva *mailing* lista i *news* grupa, da bi onda od vetropirastih trgovaca adresama bile dalje rasturane u njihovom *spam*-napadu (“68 miliona e-mail adresa za samo 149 dolara”).

Stotine stranica, sve pre “Spam.abuse.net”, u međuvremenu se u potpunosti posvetilo ogorčenoj borbi protiv *spam*-a. Virtuelna selekcija smeća takođe se trebalo i automatizovati: prvobitni *Anti-Spam-Software* zvao se *Cancelmoose* i u stvari je bio nešto poput testa za *e-mail* (9). Vesti *news* grupe, identifikovane kao *spam*, bile bi markirane kao već pročitane, tako da ne bi bile primljene pri čitanju vesti sa *news* grupe. Prema sličnim principima funkcionišu i filteri koji *spam* sortiraju od strane servera ili od strane klijenta, pa im tako ne dopuštaju da prodru u domaći *inbox*. Primera radi, sprečen biva i dalji transport *e-mail*-ova koji potiču sa *mail* servera koji vode ka odgovarajućim crnim listama. Ta metoda dovoljno pogađa i *e-mail*-ove koji nisu oklevetani, pa uopšte nemaju nikakve veze sa *spam*-om, ali su slučajno koristili isti SMTP server koji je jednom koristio i neki *spam*-er. *Spam*-eri, u konačnom, pristup sebi najčešće obezbeđuju bez znanja administratora sistema, da bi svoje masovne pošiljke ubacili u tuđe mreže poput kukavičjeg jajeta u gnezdo.

Druga mogućnost da se zabrani *spam*-ovanje, stoga se sastoji u tome da se zlo obuhvati u korenu i da se sa korišćenjem *mail* servera barata principijelno restriktivno, koliko god je moguće. Borba protiv “nesigurnih” servera koji dozvoljavaju “Open Relaying”, dakle

mogu biti korišćeni i spolja za slanje *e-mail*-ova, do sada nalikuje još jednoj borbi protiv vetrenjača i uz to biva dodatno otežana putem besplatnih *web-mail* usluga, gde se *spam*-eri kratkoročno mogu pokrivati sa naloga korisnika.

“Jedna sablast kruži Evropom”, u toj meri patetično započinje “Opt-In-Manifesto”: “Sablast bezgranično raširenih, neželjenih e-mail-ova”. CAUCE je zajednički skup korisnika interneta, profesionalaca koji rade na mreži i administratora sistema koji je oglasio borbu protiv *spam*-inga (10). Njegov evropski Dependence Euro-CAUCE početkom 1999. godine započeo je zajedno sa kompjuterskim časopisom “c’t” i online magazinom “Politik-Digital” jednu peticiju koja bi se trebala pobrinuti da *spam*-ing bude zabranjen zakonom Evropske Unije (11). “Glas protiv spam-a!” zove se akcija koju najveći broj korisnika svako jutro provodi sa *delete*-dugmetom, a sada je organizovana u tišini *online*-glasanja. Tačno četrdeset hiljada učesnika je za dve godine htelo da sa jednim klikom miša pledira za zabranu širom Evrope.

U maju 2000. godine, Parlament Evropske Unije rastao se pri trećem čitanju zakona koji propisuje da se neželjeno poslati reklamni *e-mail*-ovi učine jasno prepoznatljivi kao takvi. Pošiljaoci ne smeju slati nikakve reklame adresantima koji su se upisali u odgovarajući Opt-Out-registar. Protiv generalne zabrane *spam*-a, odnosno Opt-In-registra, u kojem su se korisnici jednoznačno trebalo izjasniti za prijem određenih reklamnih poruka, zalagali su se Vlada Sjedinjenih Država i lobi organizacije poput nemačkog multimedijalnog udruženja (12). Nezavisno od toga, u Nemačkoj *spam*-ing jeste zabranjen i ostaje zabranjen. Već 1997. godine, Pokrajinski sud Traunštajn ustanovio je da je slanje neželjenih reklamnih *e-mail*-ova privatnim licima protiv zakona, da je prekršaj protiv fer konkurencije i da je time protivpravno (13).

Obećanje interneta izokrenuto u apsurd

Koliko bespomoćno deluju zakoni u odnosu na, bez daljnjeg, najčešće anonimne *spam*-ere koji operišu iz 'digitalne ničije zemlje', dokazuje Opt-Out opcija koja danas ukrašava bazične redove mnogih *spam*-ova. Ko na milostivu poruku odgovori takozvanom *Remove*-adresom, da bi navodno jednom za svagda bio spašen od slanja, dospeva s konja na magarca. *Spam*-eri dobijaju dragocenu potvrdu da se iza *e-mail* adrese krije osoba koja realno egzistira, pa frekvencija napada biva znatno češća. Svi filteri i zakoni su potpuno bespomoćni protiv naročito perfidne varijante *spam*-inga. Lančana pisma se na mreži šire poput elektronske kuge pri čemu primaoci, iz razloga koji su jednako razumljivi kao i nerazumljivi, bivaju zamoljeni da *e-mail* dalje pošalju na što više adresa. Pritom se ne apeluje samo na pohlepu, već sve češće i na dobročinstvo: da se ispuni poslednja želja detetu bolesnom od raka, da se avganistanske žene oslobode od prisilnog nošenja marama, da se nacisti proteraju sa *news* grupa – sve su to izgovori za otrcane i potpuno nepotrebne kružne pošiljke koje godinama kruže, a napokon i diskredituju ozbiljne kampanje, uredno datirane i poslate sa važećih ličnih i *web* adresa (14).

Verovatno će *spam* postojati toliko dugo, dok ima ljudi koji će mu nasedati. *Spam* otelovljuje nešto poput antihrista *E-Commerce*-a i nerazdvojno ide ruku pod ruku sa

komercijalizovanjem interneta, koliko god se asketi – iznad svih Usability-Guru Jakob Nilsen (Jakob Nielsen) – tome želeli odupreti. Nilsen je već godinama neumoran u propovedanju generalne nepodesnosti interneta za reklamne svrhe (15). Ambiciozno zamišljeno, ugrožavanje talasne dužine putem masovnih kružnih pošiljki, konačno nije ništa drugo nego ono, u besmisao izokrenuto obećanje da će od sada svaki čovek potencijalno moći da komunicira sa svim drugim ljudima. Takozvani *Direct Marketing*, kako je *spam* eufemično nazvan od strane svojih tvoraca, utoliko nije ništa više od korova koji, kao i uvek, raskošno uspeva na masnom tlu izobilja i mnogo osporavanog oslobođenja u koje se verovalo u doba prvih dana mreže.

A budući da je napokon u potpunosti svejedno šta je sadržaj *spam-mail*-a i na osnovu kojih motiva je on poslat, protiv njega može pomoći samo jedno radikalno rešenje. Poput onog, za kojim je posegao umetnik na mreži Hit Banting već 1997. godine: radi neophodne odbrane od bezličnih *e-mail* poruka koje su postajale sve masovnije, on je ustanovio identitet na mreži koji bi se prema određenoj šemi menjao mesečno (16). Da se oslanjao na ljudsku inteligenciju, mogao je barem neko vreme prelistavati doista jednostavno izrađene robote uz čiju pomoć trgovci adresama skeniraju mrežu u potrazi za *e-mail* adresama.

Od neurotičara do ljubitelja *spam*-a

Ko postane žrtva *spam*-inga, u principu može birati između tri različite reakcije: pametnija bi se mogla sastojati u tome da se neželjeni *e-mail* ignoriše kao i prospekti velikih robnih kuća koji kasno popodne zakrče poštanske sandučiće, ili kao "na divlje" isplakatirane najave za koncerte. Neurotična varijanta je poznata upravo iz *offline*-sveta: nedeljama i nedeljama iznervirani susedi pokušavaju da na poštovanje malih plakata "Zabranjeno reklamiranje" obavežu mlade, poluodrasle ljude koji raznošenjem gratis-štampanih stvari sami zarađuju svoje prve eure. Za takve karaktere se čini da su u međuvremenu uspeli da uskoče u *online*-svet i da na najavu svakog događaja odgovaraju sa automatski generisanim saopštenjem na "abuse.net" *clearing*-mestu.

Treći, a možda i najrafiniraniji odgovor glasi: *spam* odobravati, a možda čak i razjasniti. Napokon, neotesane vesti mogu biti shvaćene kao prodiranje realnog u domaći *mailbox*. Simbolički poredak elektronskog slanja pošte dospeva u opasnost: jer *spam* je otrov koji rastače atmosferu komunikacije koja pretenduje da ne bude ciljno orijentisana i korisna. A najgore je od svega: navodno se protiv slanja reklama, lančanih pisama i piramidalnih igara ne može učiniti ništa, njima je krajnji korisnik bespomoćno isporučen. Ta bespomoćnost vodi ka poučnim oblicima eskapizma. Tako se čini da je *spam* na jedinstven način fascinirao poneke ljude. Ako se već ne može pokloniti poverenje sadržaju, i ako već nema nikakvog smisla protiv njega se boriti, onda ta fascinacija barem dopušta da se takve vesti ipak akribično registruju, arhiviraju i sačuvaju.

Pasionirani skupljači *spam*-a rado se šepure sa ličnim statistikama ("38 megabajta u više od 5200 pojedinačnih poruka. To je količina *spam*-a za nešto više od tri godine") ili ujedno nude na presnimavanje kompletne privatne kolekcije – besplatno, razume se.

"Cspam.com" animirao je velik izbor *spam*-ova koji se stalno menjaju, omogućavajući da se uzbudljive poruke stalno skroluju kroz *browser* prozor, a prema izboru čak i sa odgovarajućom muzičkom pratnjom Baha (Bach) ili Verdija (17). I pravi *spam*-ovi su mogući u *Online-Shop*-u *Cspam*-a: limenka "Original Hormel Lucheon Meat" biva poslata po želji primaoca. Kolekcija izabranih *spam*-ova dostupna je u prestižnom izdanju sa platnenim povezom. Ostaje samo se da sačeka na personalizovano izdanje "myCSpam", tj. na individualni pristup hiljadama zabavnih i informativnih internet ponuda.

Njegove aktivnosti su u međuvremenu zaokupljene "Istorijskim Spam muzejem i arhivom" koji je od 1996. do 1999. godine skupio oko 5,6 megabajta *spam*-a, da bi ga budućoj generaciji arheologa mreže stavio na raspolaganje u istraživačke svrhe (18). Zamišljen je kao muzej, ali i kao omaž enormnoj razmeri beznačajnog i trivijalnog koje se zadržava na internetu. Najpoznatiji je ipak "Make Money Fast (MMF) – Hall of Humilation" koji je već 1997. godine na *Ars Electronica* festivalu odlikovan zlatnom *Nike* nagradom u kategoriji ".net". Radi se o javno dostupnoj platformi koja *spam* ne samo da polaže u jednu bazu podataka, već pre svega omogućuje jedno: opterećujuće reklamiranje pratiti unatrag sve do mesta nastanka.

Protiv *Echelon*-a i male gladi

Poput smeća u bilo kom vidu, i hrpa podataka koja nam stiže pri *spam*-ingu i završava u virtuelnoj korpi za papir može biti ponovo procenjena, pa čak i upotrebljena u neke praktične svrhe. To su barem pokušali da dokažu delatnici "Spammimic.com" (20). U jednom *dialogbox*-u na njihovoj *homepage*, kratke poruke mogu biti zaključane i ponovo otključane tako da kôdirane kao uobičajeni *spam* deluju potpuno bezazleno i gotovo da ne privlače pažnju tajnih službi i drugih elektronskih prisluškivača. Ideja je upravo idealna za ljude kojima je stalno korišćenje tekućih programa za kriptografiju odviše zahtevno ili putem iznenada kôdiranih poruka ne žele da otkriju, da sada odjednom razmenjuju tajne. To je zasigurno najčudnovatija metoda čuvanja tajne u pismima, pa bi stoga mogla da podstakne na razmišljanje čak i *High-Tech*-sisteme za prisluškivanje poput *Echelon*-a (tajni sistem praćenja setelitskih komunikacija, fakseva, telefonskih poziva i e-mail-ova – prim. prev) ili *Carnivore*-a (sporni projekat FBI čiji cilj je nadziranje e-mail komunikacije i on-line ponašanja internet korisnika radi navodnog otkrivanja kriminalnih aktivnosti – prim. prev). Pravi *spam*, pišu osnivači "Spammimic" toliko je šokantno glup, da gotovo i nije moguće razlikovati veštački proizvedeni besmisao od strane mašine od autentičnog *spam*-a.

To je problem sa kojim se morao napokon suočiti i "Hormels Food Corporation". Ipak, proizvođači pra-*spam*-a odustali su od građansko-pravnih koraka protiv izjednačavanja njihove robne marke sa opterećenjima poput *junk-e-mail*-a koje šteti njihovom poslu, stavivši u opticaj jedan predlog: Onaj ko misli na pravi mesni narezak, trebalo bi SPAM da napiše jednostavno velikim slovima.

Literatura

(1) Spam Homepage, http://www.spam.com

(2) Monty Python Online, http://www.pythonline.com

(3) Vikinški skeč http://www.btinternet.com/~basedata/sinkordie/spam.htm

(4) Serdar Aagric, HOWLING IN THE WIRES. A net.poltergeist horros story, http://www.kkc.neteyenet/1994/net0728.html

(5) http://www.slashdot.org/comments.pl?sid=01/03/25/1617212&cid=141

(6) http://www.geekt.org/geekt/comment.cgi?newsid=1113

(7) http://www.coin.org.uk/roadshow/presentation/canter.html

(8) http://www.spam.abuse. net

(9) http://www.cm.org

(10) http://www.cause.org

(11) http://www.politik-digital.de-spam

(12) http://www.europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000__31ec_.depdf

(13) Okružni sud Trauštajn, AZ: 2 HKO 3755/97

(14) http://www.tu-berlin.de/www/software/hoax.shtml#8

(15) http://www.useit.com/alertbox/9709a.html

(16) http://www.irational.org/heath

(17) http://www.cspam.com

(18) http://www.visi.com/~drow/spam

(19) http://ga.to/mmf

(20) http://www.spammimic.com

Florijan Šnajder (Florian Schneider) je umetnik i novinar. Živi u Minhenu. Aktivno učestvuje u Pokretu za građanska prava “Nijedan čovek nije ilegalan”, uređuje umetnički temat o imigraciji i građanskim pravima. Redovno piše feljtone u *Süddeutsche Zeitung*-u.

3. Skriptovi ne poznaju etiku

"Script Kiddies" su žrtveni jarčevi
krivičnih gonilaca i kompjuterske industrije
ali da li su oni zaista takvi, kakvi su prikazani?

The Kids are Out to Play

Armin Medoš

Ako postoji grupa osoba oko čije percepcije kao "zlih klinaca interneta" navodno postoji univerzalna saglasnost, onda su to tzv. "Script Kiddies". Tako najčešće bivaju nazvani mladići koji, kao "cracker-i", sebi obezbeđuju pristup tuđim računarima, narušavaju *website*-ove i posredstvom *Denial-of-Service-Attacs* bacaju servere na kolena. Budući da pritom (navodno) ne koriste autentične programe koje su sami napisali već posežu za programima rasprostranjenim preko specijalizovanih IRC-kanala, Web i FTP-servera, pripisan im je atribut "script", dok se "kiddies" odnosi na njihovo mladalačko doba. Najkasnije nakon DDos-napada na CNN.com, Yahoo!, eBay i druge vodeće komercijalne servise na internetu u februaru 2000. godine (1), o "Script Kiddies" se govorilo na sva usta. Do danas nije sa sigurnošću razjašnjeno ko je mogao nekoliko sati tako drastično nauditi nekima od svetskih servera koji su zasigurno najbolje čuvani i povezani najdebljim vodovima. Procene iznosa štete leže između 1,5 i 3 milijarde američkih dolara. Kao verovatni počinilac kasnije je optužen i izveden pred sud jedan Kanađanin koji je u trenutku čina imao petnaest godina, ali su eksperti ipak jedinstveni da on nije mogao biti jedini počinilac napada (2). Njegovo pravo ime nikada nije objavljeno zbog mladalačke dobi, ali je kao "Mafiaboy", što je bio njegov internet pseudonim, ušao u istoriju mreže. Pretnja od strane "Script Kiddies", poput "Mafiaboy" ili "Coolio" postala je udarni naslov na prvim stranicama novina i na večernjim vestima elektronskih medija, služeći organima gonjenja kao razlog više za zaoštravanje zakona protiv *cyber*-kriminala. Bivši britanski Ministar isnostranih poslova Robin Kuk (Robin Cook) otišao je čak toliko daleko, da je utvrdio da su "hacker-i" "gori od terorista". Visoko rangirani državni službenici skicirali su situaciju u kojoj iz svojih dečjih soba u roditeljskim domovima tinejdžeri posredstvom kompjutera, modema i kopiranih *software*-a mogu dovesti do sloma kritične nacionalne infrastrukture: do gradova odsečenih od struje, do komešanja u bolnicama, finansijskim centrima i vojnim bazama, ili pak, u najmanjem slučaju do izbacivanja iz posla poslovnih servera na interenetu i do državnih tajni u rukama neodgovornih mladića. Ipak i oni, koji bi to trebali bolje da znaju, pošto su trpeli i još uvek trpe ista ili slična demonizovanja, iskusni, pravi "hacker-i" iskazuju malo simpatija za klince. Oni koriste pojam "Script Kiddies" da bi se kao *hacker*-i jedne drugačije, starije

etike razgraničili od njih. Oni ih preziru zbog podređenog nedostatka istinski dubokih znanja kompjutera i zbog toga što klinci svojim nepromišljenim delima daju vladama legitimaciju za širi spektar kriminalizovanja sigurnosno relevantnih kompjuterskih aktivnosti – u žargonu "hack-ovanja". U pogledu ovog poslednjeg oni naprosto imaju pravo. Ipak, u istom momentu moramo dodati, da će stroži pripadnici policijskih i političkih krugova uvek pronaći razloge za zaoštravanje zakona i kaznenih praksi gonjenja.

Moguće je da su takozvani "Script Kiddies" mnogo manje homogena i stereotipna grupa nego što bi želeli da nas uvere policija, mediji i stari *hack*-eri. Sa velikom verovatnoćom možemo reći da je potencijal štete koji oni reprezentuju mnogo manji od onog koji im se pripisuje. Sa tim iskazom ne treba da bude dovedeno u sumnju da mladi *crack*-eri čine zakonske prekršaje, da oni prouzrokuju lične i privredne štete, te da protiv takve, brojno rastuće pretnje nešto treba preduzeti. Ipak da li su "Script Kiddies" zaista takva "pošast društva", izazov vrednostima društva? Ili su oni pre produkt istog tog društva koji ga tako proklinje? Možda je njihovo ponašanje simtpom grešaka koje leže suštinski dublje i široko su rasprostranjene, takoreći sistemski uslovljenih grešaka koje podstiču njihova (ne)dela? Slično kao i kod pitanja, da li kriminalca treba čisto individualno osloviti "krivim" za njegova dela ili su njega tek okolnosti načinile onakvim kakav je, takva pitanja nisu rešiva na opštoj moralnoj ravni. "Script Kiddies" ovde ne treba da budu niti paušalno uzeti u zaštitu, niti razrešeni krivice, niti treba da bude replicirano negativnoj slici o njima koja bez daljnjeg već preovlađuje. Ako se tim fenomenom podrobnije pozabavimo, relativno brzo se dolazi do shvatanja da tih stereotipnih "Script Kiddies" ustvari i nema, nego ima pre svega klinaca sa nizom različitih stanovišta i motivacija koje povezuje samo jedno: naime, da veliki deo svog slobodnog vremena provode baveći se kompjuterima i mrežom. Najkasnije na tom mestu valja *ad acta* odložiti pojam "Script Kiddies" kao spolja nametnutu negativnu ocenu. Njih bi najpre, bez unapred utvrđenih moralnih vrednovanja trebalo videti kao ono što reprezentuju: kao relativno novu, tehnološku, neprilagođenu, do sada neposlušnu, ometačku i razornu omladinsku kulturu, pri čemu naglasak ipak leži na kulturi.

Korene mladalačke *hacker*-ske kulture opisuje knjiga "Underground" (1997) iz perspektive mladih učesnika, istražujući njihove motivacione razloge (3). U toj knjizi se radi o mladim *hacker*-ima u Australiji, Sjedinjenima Američkim Državama i Engleskoj u periodu, od otprilike, 1988. do 1992. godine. Parametri su tada još bili sasvim drugačiji jer je "hack-ovanje", upad u tuđe kompjuterske sisteme, služilo jednoj osnovnoj svrsi, naime zadobijanju pristupa u širom sveta rasprostranjenim elektronskim mrežama, što mladima tada uopšte nije bilo legalno omogućeno bez kreativnog zaobilaženja sigurnosnih mera. Događaji u vezi sa *mail box*-ovima poput "The Realm" u Melburnu ili *chat* sistemom "Altos" u Nemačkoj ipak predstavljaju nešto poput kopije budućeg razvoja situacije. Kao što nagoveštavaju priče u "Underground"-u, kod tih *hacker*-a ili *cracker*-a se s jedne strane radilo o tome, da pronađu vlastite puteve kroz upravo rastući svet mreže. Putem otimanja naloga korisnika i otvaranjem zadnjih vrata, oni su mogli poći putevima koji gotovo nikome nisu bili poznati, a njima su davali slobodu kretanja u internacionalnim mrežama, što se još uvek činilo potpuno utopijskim. Jedna važna motivacija bilo je i priznanje koje

se sa uspešnim *hack*-ovanjem moglo steći u maloj, ali prefinjenoj *hacker*-skoj zajednici. Uz to dolaze i znatiželja, želja da se prisvoje tehnička znanja u postupku "uradi sam" i da se zaviri u svet odraslih. Minimalna etika sastojala se u tome da se tuđim sistemima ne pričine štete, da se sistem nijednog računara ne sruši, da se podaci ne obrišu i da se sebi ne obezbede nikakve finansijske dobiti. Važan je bio i *Fair Play* razmena informacija unutar zajednice – na primer znanja o zadnjim vratima i šifra-*crack*-metodama. Doduše, moralne granice su naprosto bile porozne, tako da je postojalno mnoštvo *carding*-a (prevara sa kreditnim karticama) i *phreaking*-a (zloupotrebe telefonskih konekcija), ali se istinski izazov sastojao u zadobijanju gospodarenja nad *Unix-System*-om.

"Underground" pokazuje sliku mladića različitog porekla koji nisu kriminalno opredeljeni, ali su svakako spremni da prekorače određene granice legalnosti. Podvučene su i snažne veze sa drugim kulturama mladih, pre svega muzikom (indi rokom poput Midnight Oil), odnosno suprotnosti u odnosu na svet odraslih. Konflikt kultura i generacija, uključujući i uzajamna nerazumevanja, nije mogao biti veći – što je takođe element koji je do danas ostao takav. Tu je i svet sigurnosnih naloga sa vizit kartama, ulančeni elektronski kao i realni identiteti u čvrsto povezanim hijerarhijama i karijerama. Naspram njih stoje samo *Slacker*-tipovi, mladi koji deluju samo pod kriptičnim internet-pseudonimima (nadimcima, takođe nazvanim "handles") iz kvartova u predgrađu Melburna ili Mančestera. Različite storije koje će se deset godina kasnije gotovo identično ponavljati vodile su ka postepenoj izgradnji protiv udara realnog sveta, a time i ka negativnom vrhuncu. FBI i tane službe obraćaju pažnju na aktivnosti *hacker*-a. Spektakularni slučajevi dospevaju na naslovne stranice. Bivaju uvedeni novi anti-*hacker*-ski zakoni, krivci moraju biti pronađeni i kažnjeni za primer.

Za današnje mladiće sam pristup internetu više nije problem, oni gotovo sa svih strana na njega bivaju ohrabrivani. Draž za ilegalne aktivnosti ili prostor za igru time ipak nisu iščezli. Kao što je jedan sigurnosni ekspert sažeto formulisao, postoji jedna vrsta nove monete na internetu: zadnja vrata (4). U osnovi se pritom radi o istoj igri kao i pre deset godina: poći putevima koji su drugima neprohodni, nadmudriti profesionalne službenike sveta odraslih, dobiti "root" (administratorske privilegije) na tuđim serverima i pokazati insajderskoj zajednici da se, kako se u žargonu kaže, postalo "elitom", dakle da se pripada eliti istinskih službenih *hacker*-a. Ko sebi obezbedi pristup najvećem mogućem broju sistema (i, ukoliko nije oglašena na sva zvona, ta privilegija se zadržava na duže vreme), poboljšava svoj status u grupi. Najveća nagrada je etabliranje prihvaćenog *nom de guerre*, vlastitog internet nadimka, kao priznate marke u *hacker*-skoj zajednici. U svakom slučaju, taj cilj ne može biti postignut samo gomilanjem tesnih, domaćih, mirnih i tihih zadnjih vrata i pristupnih prava. Stoga važi da se kada se ukaže zgodna prilika, javno uspostavi jedan znak. Vandalske aktivnosti koje se najčešće pripisuju internet-zlikovcima, a verovatno su i stvarno počinjene sa njihove strane jesu *Website-Defacement*, takođe nazvan i *Web-Graffiti*, odnosno DoS-napadi, tj. *Distributed-DoS-Attacs*.

Prilikom "Distributed Denial of Service" napadima (DDoS), u osnovnom principu se radi o tome da se neki server bombarduje sa što je moguće većim paketima podataka, da

bi mu se putem tog neželjenog saobraćaja zaustavila paleta internet veza koje mu stoje na raspolaganju, tako da "normalni" paketi podataka više ne mogu biti ispunjeni zahtevi *web*-servera od strane korisnika zainteresovanih za njegove usluge. Sa razvojem različitih oblika DDoS-napada usavršile su se metode za tu vrstu napada. Preko programa koje sadrže dotični kanali poput "Stacheldraht" ili "Tribal Flood Net" u ruke relativno neiskusnih korisnika dospevaju moćna oružja za napad, što posredstvom "Script Kiddies" samo daje krila medijskom *hype*-u. U stvari, mladi *hacker*-i ne žele da se vide označeni tim pojmom i mogu veoma nabusito reagovati kada osete da su nepravedno svrstani u tu kategoriju. To iskustvo je imao i Stiv Gibson (Steve Gibson), stručnjak za kompjutere čiji poslovni server je postao žrtva stalnog DDoS-napada (5). U slučaju koji je on sâm iscrpno dokumentovao na mreži, dogodio se DDos-napad od strane preko četiri stotine Windows-PC kompjutera raširenih širom sveta u kojem je napadač krišom uvukao male *script*-e (zvane "Zombie" ili "Bot") i preko specijalnih IRC kanala razaslao ih njihovom "gospodaru". Povezanost Gibsonove firme GRC na internet bila je u potpunosti preplavljena ogromnim paketima podataka. Budući da napadi nisu prestajali, oštećeni se latio obaveštavanja podzemlja mreže. Zahvaljujući svojim sposobnostima kao starog *hacker*-a pošlo mu je za rukom da kao počinioca identifikuje jednog trinaestogodišnjaka koji se pojavljivao sa nadimkom "Wicked" i da putem jednog foruma stupi u dijalog sa njim. "Wicked" je priznao da je prouzrokovao napade, jer je iz druge ruke čuo da ga je Gibson nazvao "Script Kid". On je preplavio njegovu konekciju sa mrežom da bi mu demonstrirao svoju moć. Gibson, koji je prošao kroz iskustvo katarze, zaključuje:

- da je uprkos svim znanjima bio bez odbrane u odnosu na te napade, tako da je priznao "odustajem, ti si pobedio",
- da osetljivost Misrosoft-sistema sačinjava jezgro nevolje kada "Zombies" bivaju preuzeti za DDoS-napade i da je sa novim generacijama, Windows 2000 i Windows XP situacija još više pogoršana,
- da mu provajderi korisničkog računara ne mogu ili ne žele pomoći kada "Zombies" napadnu, tj. jednostavno zatvaraju oči i
- da mu ni FBI nije mogao ili želeo pomoći.

Tek nakon što je obelodanio svoj poraz i nakon što je svom protivniku mogao saopštiti da on navodnu izjavu u vezi sa "Script Kiddies" nikada nije izrekao, napadi "Wicked-a" su dobrovoljno prestali. Nakon toga se Gibson bacio na posao da razvije oruđe protiv DDoS-napada. Pri naružavanju *website*-ova koje je prikladno nazvano i "Web-Graffiti", radi se o tome da se obezbedi privremeni pristup nekom *web*-serveru i da se njegova *homepage* zameni sadržajima prema vlastitom izboru. Ta praksa je zadobila gotovo već epidemijske razmere. Dnevno navodno šezdeset do osamdeset *site*-ova biva preuzeto i 'obeleženo grafitima'. Oni imaju najrazličitije sadržaje, ali iskazuju i neke zajedničke karakteristike: umetnici digitalnim sprejem ostavljaju signaturu svog imena, ime napisano u tipičnom *hacker*-skom žargonu koje se sastoji od slova, brojeva i znakova (na primer "Z3BR4 X",

"Digi Almighty", "f0rpaxe"), žargon poput "XY rulez" ili "ownz", tj. "Soundso" preuzeo je kontrolu nad serverom. Mnogi takođe rade u grupama koje se pojavljuju pod imenima poput "PoizonB0x" ili "World of Hell". Ali često su nenasilni "shouts", tj. pozdravi vlastitoj zajednici, drugim grupama, a ponekad i poruke devojkama i *hacker*-skim veličinama poput Kevina Mitnika (Kevin Mitnick) i 2600-Magazine. Sastavni deo specifičnih napisa su obelodanjivanja opštih raspoloženja (Bier, Joints) a ponekad i političke poruke, grafikoni pa čak i *Midi* ili *MPEG*-podaci. Proteklih godina gotovo da nijedan popularan *web*-server nije ostao nenaružen takvim povremenim preuzimanjima, bio on server *New York Times*-a, NASA-e ili Bele Kuće. Što centralniji značaj neki server ima u javnom procenjivanju, utoliko je veća "cracker-ova" pobeda. *Crack*-ovanje servera poput *New York Times*-a do skora bi prouzrokovalo udarne naslove. Danas su ona toliko frekventna, da se mora raditi o istovremenom, koncentrisanom preuzimanju brojnih servera da bi se još privukla pažnja nekog od novinara. Interesantnije od pojedinačnih slučajeva su serije ili određeni konflikti. Tako postoje *crack*-erske trupe koje su se specijalizovale za preuzimanje servera iz vojno-industrijskog kompleksa. Druge pak favorizuju ciljeve među izabranim, velikim svetskim koncernima. U kontekstu političkih konflikata protivnički *crack*-eri međusobno ruše *website*-ove – kao nedavno US Amerikanci protiv Kineza, Palestinci protiv Izraelaca, Srbi protiv Hrvata i kosovskih Albanaca. Takve događaje mediji rado uvode u igru kao razgorevanje davno prognoziranih informatičkih ili *cyber*-ratova. Pritom jedno ipak nipošto ne bi trebalo da se previdi. Radi se "samo" o privremenom uništenju informacija na javno pristupačnom *web*-serveru koji biva promenjen ili načinjen nepristupačnim. Kritične aplikacije time ne bi trebalo da su pogođene, budući da one, što je jedno od osnovnih pravila svakog udžbenika bezbednosti, treba da cirkulišu drugim računarima koji nisu direktno povezani sa nekim *web*-serverom i trebali bi biti dodatno čuvani. *Crack*-ovanje *web*-servera jednog elektrifikovanog društva ne znači da se stekao pristup računaru sa čime bi se mogao srušiti dotični energetski sistem. Ipak, u medijskoj percepciji takvih događaja pomenuta razlika često biva (svesno?) zapostavljena. Kada se *crack*-eri, koji u stvari samo žele da publikuje svoj *Web-Graffiti*, spotiču preko banaka podataka sa informacijama o klijentima, informacijama o kreditnim karticama ili drugim osetljivim informacijama, onda se radi o značajnom nedostatku bezbednosne politike dotičnog preduzeća. Treba izričito reći da nije verovatno da neko na koga se odnosi oznaka "Script Kiddie", dakle početnik koji operiše samo sa unapred pripremljenim programima, može prodreti u jedan dobro čuvani sistem u kojem su zaključane sve poznate bezbednosne rupe. Čini se da je ipak lakše preko medija stvoriti 'žrtvene jarce', nego ozbiljno shvatiti bezbednost. Povrh toga, monokultura Microsoft-a predstavlja prividno idealno okruženje za aktivnosti "Script Kiddies" – na primer povredivost MS Outlook Express-a posredstvom virusa i crva koji su opremljeni sa virusnim *Standard-Tool-Kits*.

Website "Alldas.de" (6) u međuvremenu je jedini *website* koji još uvek objavljuje arhiv *crack*-ovanih *website*-ova. Intervjui sa *Web-Graffiti* atentatorima koji su tamo objavljeni izazivaju slutnju da je stadijum "Script-Kiddie" nešto poput prve stepenice na merdevinama učenja prilikom bavljenja temama kompjutera i bezbednosti. Sasvim drugačije nego što sugerišu medijski izveštaji, mladi *crack*-eri nisu bezuslovno fiksirani za karijeru

tvrdokornih *cyber* kriminalaca ili *cyber* terorista. Mnogo radije oni potajno čeznu za poslom u kompjuterskoj industriji kao – iznenađenje – bezbednosni eksperti, zvani i "White Hat Hacker" ili "Ethical Hackers". Aktivnosti u podzemnom kompjuterskom svetu, a to je i među njima često upravo tako shvaćeno, služe sticanju reputacije među prijateljima, među proširenim krugom eksperata, a time kvazi pripremi u docnijem toku karijere. Njihovo kriminalizovanje ili čak izjednačavanje sa teroristima, može se uporedi samo sa slavnom poslovicom "topovima gađati vrapce".

Mladi prijatelji kompjutera, pogrešno nazvani "Script Kiddies", često su pre idealistični mladi ljudi koji se vide konfrontirani sa svemoćnim institucijama države ili privrede. Nepoverljivi prema poštovanju autoriteta, oni smatraju da je legitimno počiniti zakonske prekršaje koji su u njihovim očima manji. Ono što se ranije označavalo kao vojno-industrijski kompleks, na internetu je udaljeno odmah iza ugla. Bez sasvim jasne svesti sa kim imaju posla, oni testiraju granice civilnog i vojnog interneta i izazivaju državnu moć. U svojim protiv-reakcijama ona nije nežna. Racije protiv petnaestogodišnjaka sa neuniformisanim, teško naoružanim agentima nisu retkost, pre svega u Severnoj Americi. Javno žigosanje kao kriminalaca i terorista, te dodeljivanje zatvorskih kazni šalju signal za zatvaranje redova u podzemlju. Tendencija je slična kao i u "Ratu protiv droge". Ko zbog posedovanja jednog grama marihuane ide u zatvor godinu dana ili duže, sa velikom verovatnoćom se vraća u svet kao očvrsnuli kriminalac. Ubrzo nakon DDoS-napada na Yahoo! itd. Američki *cyber* kritičar Daglas Raškof (Douglas Rushkoff) napisao je da ga ti uspešni napadi ne ispunjavaju samo sa potajnom željom za nanošenje štete, nego da takođe ima naznaku o motivacijskim razlozima za te napade. To je rastuća komercijalizacija mreže koja prinuđuje da se od nje stvori sve sigurnije i bolje nadzirani prostor. Moguće je da se ti napadi sagledaju poput oslobađajućeg udara protiv konsekvenci komercijalizacije mreže, piše Raškof (7). Mladi se danas osećaju konfrontirani sa jednim višestruko regulisanim svetom u kojem vladaju potrošnja, robne marke i vlasti. Omladini pripada pobuna, isto kao i sazreo interes za seks i rastući osećaj za pravednost. Često korišćena predrasuda protiv mladih kompjuterskih čudaci glasi da su oni usamljeni tipovi, bez socijalnog života u "normalnom" svetu. Intervjui na "Alldas.de" jednako kao i knjiga "Underground" protivreče tom klišeu. Mladi kompjuterski čudaci su sasvim normalni mladići koji se interesuju za priznanje u grupi, za samopotvrđivanje i kontakt sa drugim polom. Njihovo demonizovanje i kriminalizovanje može značiti stvaranje stigmatizovanih autsajdera od nekih među najtalentovanijim i najznatiželjnijim ljudima u ovom društvu, ljudi koji mogu pružiti vredan doprinos, a zakoračivanje u normalan život im se nepotrebno otežava. Vredno je spomena da je godinu dana nakon DDoS-napada na CNN, Yahoo! itd. značajno popustila frekvencija medijskih izveštaja o "Script Kiddies". Na udarnim kompjuterskim *Newssites* još se nalaze vesti o postupcima protiv pseudonima poput "Mafiaboy" ili "Coolio", ali o zatvorskim kaznama na koje su oni konačno osuđeni ili nisu osuđeni, uprkos opsežnom istraživanju ne može se pronaći baš ništa. Jedan razlog može biti malaksavanje *Dot-Com-Boom*-a i da je samim tim opala i udarna vrednost takvih vesti. Jedan drugi razlog zvuči već nešto konspirativnije. Praktično sve visoko industrijalizovane zemlje u međuvremenu imaju drakonske zakone protiv *cyber* kriminala koji gotovo da i ne prave razliku između kriminalnih aktivnosti (krađa identiteta, prevara sa kreditnim karticama) i tipičnih "Script Kiddies"-aktivnosti. Na internacionalnoj ravni Evropski Savet, Evropska Unija, države G-8, vremenom su razrezali naredne internacionalne izdatke koji su zatrpali svaku jazbinu *cyber* kriminala, sasvim u smislu politike iz koje odsustvuje tolerancija. Javni otpor protiv takvog zakonodavstva koje preti odstranjivanjem mnogih građanskih prava u *cyber* prostoru, u liberalnoj štampi je minimalan, pa gotovo da čak i ne postoji. Kako god da se taj sklop – između zakonodavstva, buma i kraja izveštavanja o "Script Kiddies" – mogao kauzalno sagledati, čini se, da "Script Kiddies" zasada odrađuju krivicu kao žrtveni jarčevi pretnje od interneta.

Literatura

(1) Florian Rötzer, Ecommerce-Websites lagmgelegt, Telepolis 09.02.2000, http://www.heise.de/tp/deutsch/inhalt/te/5766/1.html

(2) Stefan Krempl, Rätseln um die Hintermänner der Cyberattacken auf US-Sites, Telepolis 10.02.2000, http://www.telepolis.de/deutsch/special/info/6616/1html

(3) "Underground", Suelette Dreyfus with research by Julian Assange, Random House, Australia 1997, http://www.underground-book.com

(4) "Hakeri dakle međusobno razmenjuju ranjive informacije" kazao je Tom Nunan, predsednik Ceo of Internet Security Systems Inc u Atlanti. "Postoji potpuno nova valuta na internetu koju zovu zadnja vrata" rekao je dodavši da napadači trguju informacijama u vezi sa zadnjim vratima da bi sebi omogućili pristup različitim sistemima. http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_ST059280-,00.html

(5) Anatomija jednog DDos-napada, Heise Online, http://www.heise.de/newsticker/result.xhtml?url=newsticker/data/ps-04.06.01-000/default.shtml&words=Kiddies) dokumentacija slučaja: http://grc.com/dos/grcdos.htm

(6) Arhiv Web-Grafita na Aiidas.de, http://defaced.alldas.de

(7) Douglas Rushkoff, Yahoos letztes Gefecht, Telepolis 11.02.2000, http://www.telepolis.de/deutsch/kolumnen/rus/5776/1.html

Od *Underdogs* do starova mrežne zajednice

Novi *Cracker*-i

Janko Retgers

'Provaljivanje' šifri, zaštitnih mehanizama protiv kopiranja i ograničavanja pristupa, stara je igra. Od poljskog kripto-specijaliste Mariana Rajevskog (Marian Rajewski), koji je 1933. godine 'provalio' kôd Enigme – nemačke mašine za šifrovanje, preko *Unix-hacker*-a sedamdesetih godina, do provaljivača kôdova današnje *Warez*-scene, programeri su uvek iznova pokušavali da razmrse tajne drugih programera i njihovih zaštićenih tvorevina.

Motivi za to su bili i jesu krajnje različiti: neki *crack*-napadi su motivisani politički ili čak vojno, drugima je stalo samo do uživanja u provaljivanju. Međutim, u javnosti se provaljivač (Cracker) često opaža kao egoist, kao neko kome je stalo samo do kršenja autorskog prava i besplatnog *software*-a. Slika u kojoj ni "moralni" *hacker*-i koji se ograđuju od *cracker*-a nisu nevini.

Dabome da bi se slika začas mogla ponovo promeniti. S procesom oko DeCSS-a, alata za otključavanje DVD-ova, i raspravama o mehanizmima zaštite od kopiranja koje je pokrenula SDMI (Secure Digital Music Initiative), u žižu javnosti je dospeo novi red *cracker*-a. Debatom iznenada više ne dominiraju bubuljičavi adolescenti u potrazi za najnovijim *Quake-Patch*-om, već univerzitetski profesori koji provaljuju kôdove i aktivisti organizacije *Electronic Frontier Foundation*.

Slučaj DeCSS

CSS je postupak zaključavanja koji je razvijen po nalogu Asocijacije DVD-Copy Control (DVD-CCA) kojim treba da bude sprečen direktan pristup video podacima DVD-a. Time treba da bude presečeno konvertovanje video podataka u druge formate kao i svaki drugi nelicencirani pristup tim podacima. U tu svrhu sistem koristi 40-bitno šifrovanje. Jedan od dva ključa nalazi se naravno na DVD-u, a drugi u *hardware player*-a, odnosno odgovarajućem *software*-u – ukoliko je takav bio licenciran od DVD-CCA.

Međutim, za Open-Source-operativni sistem Linux, do sad ne postoji softver s takvom licencom. De facto su se doskora DVD-ovi mogli reprodukovati samo na Windows i MAC računarima. To je nekim *cracker*-ima u leto 1999. godine dalo povod da se bliže pozabave sistemom-CSS. Nemački *cracker* otkrio je da je proizvođač jednog Windows-DVD-plejera

samo površno zaštitio CSS-ključ od pristupa. Pomoću tog ključa on je rekonstruisao CSS-izvorni kôd. Potom se krajem septembra/početkom oktobra na mreži pojavio program DeCSS koji na *hard* disk pohranjuje dešifrovani sadržaj DVD-a. DeCSS i CSS-izvorni kôd raširili su se na mreži brzinom svetlosti i stvorili osnovu za mnogobrojne programe za reprodukciju i kopiranje (Ripper).

U novembru 1999. godine, prvi ISP bio je pobuđen da s DeCSS-om sa mreže skine jednu *web*-stranicu. Krajem decembra, DVD-CSS tužilo je brojna privatna lica zbog povrede poslovnih i komercijalnih tajni. Sredinom januara usledila je druga tužba filmskih studija ujedinjenih u *Motion Picture Aliance of America* protiv pokretača četiri *website*-a, među njima i *website*-a američkog hakerskog magazina "2600", a zbog navodnog kršenja paragrafa *Digital Millenium Copyright*, koji zabranjuje zaobilaženje mera protiv kopiranja. Erik Korli (Eric Corley), pokretač "2600.com" dobio je potporu *Electronic Frontier Foundation* i do sad vodio proces kroz dve instance.

SDMI-debakl

U međuvremenu je do tužbe došlo i u slučaju SDMI, premda u obrnutom pravcu. Kratko pre redakcijskog zaključenja ove knjige, prinstonski profesor Edvard Fejten (Edward Feiten) uz potporu *Electronic Frontier Foundation* podneo je tužbu protiv: Secure Digital Music Initiative (SDMI), Recording Industry Association of America (RIAA), proizvođača vodenih žigova Verance, i US-Justicedepartment-a, našavši da mu je pretnjama industrijskih lobija ugrožena istraživačka sloboda. Predistorija: ispred pozadine CD-pisača koji se sve više šire i buma MPS-formata, od sredine devedesetih godina, muzička industrija je razvila bezbednosne koncepte za digitalnu prodaju muzike. Posle nekoliko bezuspešnih solo-prodora, krajem 1998. godine osnovana je Secure Digital Music Initiative kao spoj okruglo 180 preduzeća za izdavanje ploča i proizvođača tehnologije.

Strategija ove inicijative izgleda od prilike ovako: uz sadejstvo *hardware*-a i *software*-a stvoriti sigurnije okruženje u kome se određene vrste medijuma mogu reprodukovati samo na za njih predviđenim *player*-ima. Kao kod CSS ovde se najpre nije toliko radilo o tome da se učini nemogućim kopiranje CD-a 1:1, već o njihovom konvertovanju u druge medijske forme, specijalno MP3 datoteke. Cilj stremljenja, kako bilo, onda predstavlja čisto digitalna distribucija sa striktnim menadžmentom digitalnih prava – u svakom slučaju tako kaže teorija. (2)

U praksi, grupa se godinama bavila internim raspravama, sve dok u septembru 2000. godine nije usledio neobičan praktični test. Takmičenje nazvano "Hack SDMI" trebalo je zapravo da pomogne u evaluaciji mogućih SDMI tehnika. Ipak, *hacker*-i su odmah skršili sve predložene mehanizme i tako grupu bacili u duboku krizu.

Nastavak sledi

DeCSS i SDMI-Hack su *cracker*-ima opet dali novu legitimaciju. Veliki delovi javnosti kršenje ograničenja kopiranja vide kao legitiman pokušaj da se odbrane fer-korisnička

prava konzumenata. Javno dokumentovanje *crack*-ova ne vredi samo mrežnoj zajednici kao opravdani opažaj prava na izražavanje mišljenja. Naredni članci dakle ne opisuju samo dve važne rasprave oko budućnosti distribucije digitalnih medija, već i promenu paradigme u odnosu na *cracker*-sku scenu i njene motive.

Naravno, ovi članci mogu pružiti samo snimak trenutnog stanja. Rasprave se nastavljaju. Pri redakcijskom zaključenju ove knjige (juni 2001), Erik Korli je u drugostepenom postupku. SDMI-konzorcijum još nije bliži svom cilju, te je susret u maju bez rezultata odložen za septembar 2001. godine. Istovremeno se DVD-CCA obazire za tehnologijama koje obećavaju više sigurnosti od CSS – ironija je da se interesuje naročito za vodeni žig. Novim *cracker*-ima ni u buduće neće biti dosadno.

Literatura

(1) Vidi http://home.us.net/~encore/Enigma/enigma.html

(2) Podrobniji opis te strategije nalazi se na http://www-julienstern.org/sdmi/system.php3

DVD-proces: sukob u sudnici

Armin Medoš

Glavna rasprava u procesu osam holivudskih studija protiv Emanuela Goldštajna (Emmanuel Goldstein), građanina Erika Korlija (Eric Corley), izdavača magazina "2600 Hacker Quartely" i njegovog *wesite*-a http://www.2600.com, četvrtog dana raspravljanja je pored obaveznog čvrstog bandažiranja dovela i do maštovitog poređenja. Sudija Luis A. Keplan (Lewis A. Kaplan) je jednom prilikom uporedio širenje "Windows Utility DeCSS" sa "otvaranjem vrata od staje, tako da je konj izašao napolje". Od njega se sada zahtevao "pravni lek protiv toga, da su vrata od staje još jednom otvorena, premda je konj već napolju".

Branilac sponzorisan od strane "Electronic Frontier Foundation" (EFF) se izjasnio da će slučaj, ako bude moguće, terati sve do Vrhovnog suda Sjedinjenih Američkih Država. Ništa manje odlučni nisu bili ni tužioci: studio *Columbia, Disney, Fox, MGM, Paramount, Time Warner, Tristar* i *Universal*, kao i zastupnik njihovih interesa, Motion Picture Alliance of America (MPPA). Oni su budućnost filmske industrije videli stavljenu na kocku, ukoliko oruđa poput DeCSS bude nekažnjeno smela da budu stavljena u opticaj. U svojoj uvodnoj izjavi, branilac je zauzeo stanovište da stavljanje u pogon i primena DeCSS spada pod garantovana prava kupca na kopije u privatnoj upotrebi ("fair use"). Uz to, ograničenja u DMCA protiv *Reverse Engineering* ugrozila bi pravo na kopije u privatnoj upotrebi. Pored toga, sa optužbom protiv linkova ka eksternim *site*-ovima, ugrozilo bi se i pravo na slobodno izražavanje mišljenja.

Kao prvog svedoka tužbe, flmski studiji su doveli naučnika koji se bavi kompjuterima sa *Carnegie Melon* univerziteta, Majkla Šemosa (Michael Schamos), koji je trebao da pokaže kako je uz pomoć DeCSS-a jednostavno otključati jedan DVD i proizvesti jedan DivX DVD. U unakrsnom ispitivanju Šamos je morao priznati da je provođenje eksperimenta ukupno trajalo dvadeset časova, podeljenih na četiri noćne radne sednice. Šta više, on je takođe priznao da je "piratsku kopiju" holivudskog filma proizveo po zadatku advokatske firme tužioca *Proskaur& Rose*, za čiju narudžbenicu je primio 30.000 dolara.

Drugog dana rasprave EFF je kao svedoka pozvao kompjuterskog eksperta Frenk Endrju Stivensona (Frank Andrew Stivenson). On je radio u istraživačkom odeljenju jedne od vodećih norveških firmi, među prvima je analizirao CSS-algoritam i objavio je svoje rezultate. Jedno njegovo objašnjenje koje je već objavio, ne ostavlja nikakvu sumnju da DeCss nije oruđe koje otvara vrata pirateriji sa DVD-em, kao što tvrde studiji. Aktivni pirati bi sa DeCSS-om uštedeli trud i sve podatke koji se nalaze na DVD-u bi jednostavno kopirali

bit po bit, protiv čega CSS ne nudi zaštitu. DVD otključan sa DeCSS-om bi zauzeo toliko memorijskog mesta, naime 6 gigabajta, koliko na potrošačkom DVD-u koji je uobičajen u prodavnicama ne bi moglo biti upisano, jer on zauzima svega 4,7 gigabajta memorije. Uz to, cena za potrošačke DVD-diskove viša je od cene komercijalno dostupnih filmova.

Naredni svedok odbrane, naučnik koji se bavi kompjuterima sa *Prinston* univerziteta Eduard Filten (Edward Felten), sa naučnom razgovetnošću je predstavio smisao i svrhu CSS-a. Svrha njegovog razvijanja je da bi sprečio da sa DVD-a dekodiranog od strane CSS-a, *player* ne pusti podatke koje CSS ne sadrži. Njegov je drugi učinak da spreči svako drugo korišćenje nakon što se dovrši projekcija DVD-a. Cilj koji je odbrana postavila iza takvih teza jasan je: trebalo je biti pokazano da CCA "fair use" potpomaže politiku licence DVD-a i legitimiše *Reverse Engineering* CSS-a, budući da međusobno služe kooperativnosti sistema, bez koje nijedan Linux-Player ne bi stajao na raspolaganju za DVD-eve uobičajene u prodavnicama. Grupa za razvoj Linux-videa navodno nije htela da DVD CCA-u dodeli nikakvu CSS-licencu.

Bez zadiranja u tehničke detalje, on je izveo koje greške su načinjene prilikom razvoja CSS-a. Umesto da primenjuje neki afirmisani sistem šifrovanja koji je poznat kao siguran, razvijan je poseban sistem, a povrh toga je pala odluka za upotrebu 40-bitnog ključa. On može biti otključan uz pomoć takozvanog "brute force" napada. Naredne dizajnerske greške omogućile bi čak još brže razbijanje zaštite.

Juče je kao drugi svedok optužbe svedočila Mihaila Rejder (Mikhail Reider). Ona je najodgovornija u MPAA za internet-pirateriju. Ona je izjavila da Unija filmske industrije redovno nadzire i pretražuje piratske aktivnosti *website*-ova, FTP-*site*-ova, *File Sharing Utilities* (FSUs), IRC i *news* grupa. Njeno odeljenje je na četrdeset *site*-ova otkrilo da se piratski kopirani DVD nude na razmenu ili prodaju. Međutim, ona nije mogla reći da li se može dokazati da bilo ko od onih koji nude koristi DeCSS. Time što se pozvala na istrage koja su u toku, odbacila je i pitanje šta će MPAA preduzeti protiv tih *site*-ova. Na njima MPAA radi zajedno sa "US-carinom, tajnom službom i FBI".

Prethodni vrhunac predstavlja nastup norveškog tinejdžera i DeCSS-programera Jona Johansena u ulozi svedoka. Zajedno sa svojim ocem on boravi u Nju Jorku, da bi učestvovao na trećoj *hacker*-skoj konferenciji koju organizuje "2600" pod naslovom "HOPE 2000". Johansen je opisao istoriju nastanka DeCSS i posvedočio svoju nezainteresovanost za pirateriju. Za razvoj DeCSS.a on je primio jednu norvešku nagradu za kompjutere. Upitan, šta je učinio sa tim novcem, odgovorio je da je sebi kupio Sony-ev High-End-DVD-Player za 1.200 dolara.

Redakcijski skraćena verzija po prvi put objavljena u *Telepolis*-u, 21.07.2000. godine.

Majica, koja nosioca iste pretvara u hakerski alat

Geek Chic

Peter Milbauer

Proizvođač majica *Copyleft* (http://www.copyleft.net/) je za potrebe profesora informatike Dejvida Tureckog (David Touretzky) naštampao majice sa izvornim DeCSS kôdom i to za potrebu davanja njegove izjave u DeCSS sudskom procesu u nameri da praktično ilustruje da kôd može može da bude, u stvari, izražavanje mišljenja. Isti taj proizvođač se zbog širenja DeCSS-a takođe našao pred sudom.

"Kada se nešto naštampa na jednu majicu, onda je to izražavanje misli", smatrao je Turecki, koji je kao ekspert izrazio svoj tehnološki pogled u razjašnjavanju postavljenih pitanja sudskom procesu koji je pokrenuo Udruženje filmskih stvaralaca SAD protiv vlasnika *website*-a Erika Korlija (Eric Corley). Korli je optužen jer je na svom *website*-u stavio na raspolaganje DeCSS kôd koji je bio dostupan preko linkova. Korli je optužen prvo jer je na svom *website*-u stavio DeCSS kôd, kojim DVD-ovi mogu da se koriste na Linux-u, ali teoretski mogu i da se ilegalno kopiraju i kasnije je omogućio i linkove na *website*-ove koji sadrže taj kôd i na taj način praktično stavio kod na raspolaganje. *Copyleft* (reklamni slogan "Geek Chic") nudi majicu "OpenDVD", koja na prednjoj strani ima simbol zabrane parkiranja sa precrtanim "DVD CCA" natpisom, a na leđima je naštampan izvorni kôd *DeCSS*.

Majica se eksplicitno koristi kao izražavanje mišljenja (ili stava) protiv DVD Copy Control Association (DVD CCA) i njihovog ponašanja. Cena majice je 15 dolara, a od tog iznosa, 4 dolara *Copyleft* odmah usmerava na *Electronic Frontier Foundation* (EFF) jer finansijski pomažu sudski proces. *DVD CCA* je tužbom bukvalno smatrala da, ako se protera *DeCSS* kôd sa *website*-ova, da onda mora da sleduje i zabrana opisa na engleskom jeziku i slikovitih prikaza.

Prvi put objavljeno u Telepolis-u, 02.08.2000.

Presuda koja je slavljena u Holivudu

Filmska industrija je postigla svoju prvu pobedu

Florijan Recer

U prvoj presudi magazinu i *website*-u “2600.com”, zabranjeno je da se objavljuje kôd DeCSS-a, koji je u stvari radni program za zaštitu DVD-ova (onemogućavanje umnožavanja) ili da se postavi link za *website* koji sadrži taj kôd. Njujorški sudija Luis Kaplan (Lewis Kaplan) je u svom obrazloženju presude od 90 stranica objašnjavao da kompjuterski kôdovi nisu onakvi kako su ih predstavili optuženi, znači nisu zaštićeni kao sloboda mišljenja, kao jedno od osnovnih ustavnih prava Sjedinjenih Američkih Država. Kôdovi mogu da se koriste u okviru političkih ili umetničkih izjava, ali da se koriste u svrhu kršenja autorskih prava jednostavno je nelegalno.

Sudski proces koji je vodilo Motion Picture Assotiation (MPA) SAD protiv Emanuela Goldštajna (Emmanuel Goldstein), kao i protiv Erika Korlija (Eric Corley), izdavača časopisa “2600 Hacker Quarterly” kao i vlasnika odgovarajućeg *website*-a www.2600.com, predstavlja odlučujući korak u predstavljanju autorskih prava u digitalnoj eri. Goldštajn je optužen za širenje DeCSS-a. Najvažnija tačka optužbe i najvažniji predmet sudskog procesa je paragraf *Digital Millennium Copyright Act*-a da: se zabranjuje svako zaobilaženje zaštite od nedozvoljenog umnožavanja. Već u januaru su tužioci kod sudije Kaplana izdejstvovali zabranu distribucije DeCSS-a, a sa njegovom presudom je isto i potvrđeno.

Goldštajn i njegov branilac su pre svega ciljali na to da su kompjuterski kôdovi zaštićeni kao (slobodan) govor i da zbog toga ne može da se ograniči njihovo širenje (prostiranje, ili distribucija). Argumente koje je iznela odbrana, sudija je okarakterisao kao neosnovane. Tako je na primer: "U doba kada širenje kompjuterskih virusa može dovesti do smetnji u sistemima od kojih zavisi nacija i ako drugi kompjuterski programi mogu prouzrokovati štetu, društvo mora biti u stanju da reguliše upotrebu i distribuciju kôdova”. Kaplan je uporedio distribuciju kompjuterskih kôdova preko interneta sa epidemijom: “Širenje sredstava koja služe za zaobilaženje zaštite autorskih prava u digitalnoj formi analogna je izbijanju epidemije. Kad se pronađe izvor zaraze (znači autor DeCSS-a ili prva osoba koja ga je koristila) od toga nema nema nikakve vajde jer je bolest (tj. DeCSS-om omogućena povreda zaštite autorskih prava i iz toga proizašla raspoloživost dekodiranih DVD-ova) s jedne osobe koja ima slobodan prilaz programu za dekodiranje ili već može da koristi dekodirani DVD prešla na drugu. Znači, sve je 'inficirano', tj. omogućava savršene kopije digitalnog zapisa".

Normalno je da osobe koje su žrtve neke bolesti traže medicinsku pomoć, što nije slučaj sa DeCSS-om. Ne može se poći od toga da će one poželeti da se izleče od ove bolesti. Stoga je i u ovom slučaju “kauzalna povezanost između širenja kompjuterskih programa kao takvih i njihove ilegalne upotrebe” smeštena tamo gde se obično ne nalazi. Već samo širenje može naneti štetu i otvara mogućnost “praktično neograničene povrede autorskih prava” koje bi samo napredovalo. Kaplan se nije ustručavao od jednog drastičnijeg poređenja kad je rekao: "Kompjuterski kôdovi nisu čisto (govorno) izražavanje, kao što i ubistvo političara nije čisto političko opredeljenje”.

Tekst je redakcijski skraćen. Prvi put je objavljen u Telepolis-u, 18.08.2000.

Beta-test koji se pretvorio u fijasko

SDMI - Bezglava više nego ikad

Janko Retgers

Ričard Kijariljone (Richard Chiariglione), poslovodni direktor *Secure Digital Music Initiative* (SDMI) obznanio je svoje povlačenje. Kratko vreme pre toga, dvojica francuskih *hacker*-a počeli su da na *web*-u dokumentuju svoje uspešne napade na SDMI-tehnologije. Razume se, trenutak povlačenja je za SDMI-projekat rđavo izabran: on se nalazi u svojoj najtežoj krizi od svog osnivanja u decembru 1998. godine. Tada se u inicijativu spojilo okruglo 180 preduzeća za izdavanje ploča i proizvođača tehnologije kako bi stvorili jedan standard za bezbedniju distribuciju muzike. Kao ambiciozan cilj bilo je najavljeno da će se na tržište s definitivnim uređajima izaći još pre Božića 1999. godine. Ipak, veličina grupacije i težina poduhvata dovela je pomeranja, tako da je umesto ovoga određen Božić 2000. godine.

Ali, ni od ovoga nije bilo ništa. Dosad je inicijativa pokazala tek jedan skroman uspeh. U junu 1999. godine objavila je specifikacije za tzv. "prvu fazu kompatibilnog portabl audio *player*-a". Pošto u tom trenutku još uopšte nije bila razvijena prava bezbednosna tehnologija, specifikacija-prve-faze ne sadrži mnogo više od mogućnosti da uređaji jednom kasnije budu mogli da se *update*-uju na *player*-e faze dva.

Došla je jesen i opet su predstojali božićni praznici bez SDMI-uređaja. Među članovima Inicijative širio se nemir, opominjali su na rezultate. U toj situaciji konzorcijum SDMI došao je na kobnu ideju: želelo se dotad razvijene tehnologije podvrgnuti javnom ispitu i izazvati *hacker*-e ovog sveta da se ogledaju na njima. Onaj ko bi uspeo provali predstavljene tehnologije trebalo je da dobije 10.000 dolara.

Ubrzo po okončanju takmičenja proneo se glas da su sve tehnike pale žrtvom *hacker*-a. Ono što je usledilo ravno je drugorazrednoj sapunici: Konzorcijum SDMI je smesta demantovao. Ipak, pojedini članovi SDMI nasuprot tome izjavili su online magazinu Salon.com da je demanti samo eskivaža, da su *hacker*-i zapravo pobedili na celom frontu. SDMI-konzorcijum je i dalje demantovao. Onda je nekoliko *krypto*-eksperata Prinstonskog univerziteta izjavilo da su bili uspešni kod svih vodenih žigova. Precizna dokumentacija napada trebalo je da uskoro usledi na njihovom *website*-u.

U januaru je prinstonski profesor Edvard Fejten (Edward Feiten) na toj tački morao da načini uzmak: firma za *Watermarking–Verance* – usprotivila se objavljivanju, pozivajući se na paragraf *Digital Millenium Copyright*-a. Bez dokumentacije, konzorcijum SDMI naravno nije priznao *hack*, usled čega je s olakšanjem mogao da objavi kako su samo dve tehnologije

pale žrtvom *hacker*-a. Oba srećkovića dobila su po 5.000 dolara. Svih ostalih 445 pokušaja bilo je prema tome bezuspešno – ili naprosto samo rđavo dokumentovano.

Apsolutno izvanredno svoj napad na SDMI dokumentovala su dva francuska *hacker*-a – Žilijen Štern (Julien Stern) i Žilijen Buf (Julien Beuf) i na svom *website*-u aktiviranom početkom nedelje (http://www.julienstern.org/sdmi) objavili precizne detalje za jednu od predstavljenih tehnologija: ovde se razmatraju kako moguće metode napada tako i pretpostavljeni način funkcionisanja dotičnog vodenog žiga.

Neizvesno je da li su objavljivanja doprinela Kijariljonevom povlačenju. Malo pre toga konzorcijum je morao da istrpi još dva opora udarca: frajburški proizvođač čipova *Micronas,* objavio je da želi da istupi iz Inicijative. Osim toga, *Sony* je na *Computer Entertainment Show*-u u Las Vegasu po prvi put predstavio CD-*player*-e koji osim normalnih CD-a mogu reprodukovati i "narezane" CD-ROM-ove s MP3. Do tada je *Sony* zahvaljujući sopstvenoj izdavačkoj marki važio kao priznati neprijatelj MP3. Stoga u *Sony*-evom zaokretu nisu samo kritičari videli jasan znak u pravcu SDMI-konzorcijuma. Ričard Kijariljone je očigledno razumeo taj znak.

Redakcijski skraćena verzija

Prvi put objavljeno u *Telepolis*-u 25. 01, 2001.

Čovek koji je provalio SDMI-zaštitu protiv kopiranja

Kad profesori previše hakuju

Janko Retgers

Prinstonski profesor Edvard Fejten (Edward W. Feiten) izgleda onakav kakvog bi čovek sebi želeo za zeta. U svakom slučaju, ako ste Amerikanac i uz to oko pedesete. Pristao, okretan, samo tek malo čudan. Neko ko ti garantovano nikada ne bi pokvario popodnevnu nedeljnu kafu. Neko kome se ne može odbiti nijedna želja, kome se ništa ne može uskratiti.

Pa ipak može, kao što je to dokazala *Recording Industry of America* (RIAA). Udruženje velikih američkih muzičkih izdavačkih kuća očito je prilično ravnodušno prema zetovima, ali ni Fejten ne mari za njih. Predistorija: u septembru poslednje godine, *Secure Digital Music Initiative* (SDMI) izazvala je hakere sveta da se ogledaju na različitim mehanizmima zaštite od kopiranja. Takmičenje je nazvano „Hack SDMI“. Fejten i njegovi studenti sa Univerziteta *Princeton* (http://www.cs.princeton.edu/sip/sdmi) shvatili su to doslovno i provalili svih šest predstavljenih postupaka.

Zatrčali su se. Samo što grupa-SDMI nije htela da sebi i nama prizna taj poraz, zbog čega je Fejtenu trebalo zapušiti usta. Kružio je glas da bi mu pretila tužba zbog kršenja paragrafa *Digital Millenium Copyright Act*-a ako bi publikovao svoje rezultate. Fejten se povinovao.

U svakom slučaju, do kraja aprila. Tada je u toku bio “Fourth International Information Hiding Workshop“ i Fejten nije više želeo da uskraćuje istraživačku zajednicu kako je provalio SDMI. Njegova grupa je sastavila dokument pod naslovom “Reading Between the Lines- Lessons from the SDMI Challenge” i podnela ga priređivačima Kongresa, jednoj šarenoj grupi sastavljenoj od ljudi sa CERTA, preko Intel-a do IBM Research Lab-a. Oni su bili oduševljeni ovim i zdušno pozdravili Fejtenov nastup.

Manje je bila oduševljena RIAA kad je saznala za Fejtenove planove. Poslala mu je jedno opako pismo, govorila o pravnim sredstvima i stavila na znanje da bi s planiranim nastupom bila povređena prava proizvođača vodenog žiga *Verance*. Na dobro ili zlo, Fejten je morao nanovo da uzmakne. Međutim, s ovim očito nije bio zadovoljan svako iz kruga priređivača Kongresa, usled čega je dokument prosledio na kontracenzurni server *Cryptome.org* (http://cryptome.org/sdmi-attack.htm).

Ovom indiskrecijom sada svako može steći sliku o tome kako je prinstonski tim provalio mehanizme zaštite protiv kopiranja. Pobliže su analizirane dve tehnike i pokazuju kojom su detektivskom pronicljivošću istraživači prilegli na zadatak. U slučaju prvog vodenog znaka,

otkrili su niz nečujnih, veoma kratkotrajnih odjeka u određenom delu frekventnog pojasa. Čim su dovoljno saznali o tom fenomenu, procunjali su malo po arhivu Patentnog zavoda SAD i gle: nađoše ga pod brojem 5940135.

Patent za “Zaključavanje i otključavanje informacija u analognim signalima“, prijavljen od firme *Aris* koja danas pripada proizvođaču vodenih žigova *Verance*. S tipično praznjikavim jezikom patentnog zavoda, dokument istraživačima doduše nije doneo mnogo novih informacija. Ali, barem su doznali da su bili na pravom putu. S nekoliko daljih testova i analiza mogli su nacrtati prilično tačnu sliku načina funkcionisanja postupka zaštite protiv kopiranja.

U svakom slučaju, nije bilo potrebno toliko mnogo truda. Svi predstavljeni vodeni žigovi dali su se relativno prosto provaliti takozvanim *Brute-Force*-napadima, dakle, takoreći metodom štapa i kanapa. Istraživači su tako dodali male, nečujne *delays* (odjeke) u test-kanale, pa minimalno menjali visinu tona, pa jednostavno isfiltrirali nekoliko događaja u određenom frekventnom području. I svaki put javljalo se SDMI-proročište koje je tokom takmičenja automatski analiziralo sve pošiljke: test potvrđen, postupak provaljen.

Fejtenova grupa je stoga zaključila da se nijedan vodeni žig ne može odupreti reversnom inženjeringu. I dalje: “Ako je za konzumenta moguće da sluša ili gleda zaštićene sadržaje onda će za njega tehnički biti moguće i da ih kopira.“ Ovo je naravno voda na vodenicu protivnika zaštite protiv kopiranja.

Do sad su se oni uvek morali boriti s problemom da se u raspravama kao oko DeCSS uvek radilo o čudnovato dvoličnom *hacker*-u koga je javnost pre smatrala u osnovi opakim. Dan Burke sa Univerziteta Minesota k tome je izjavio vezano za ZDNET: “Čim sudija kaže ’hacker’, znaj da si izgubio.“

Nasuprot tome, jednom pristalom bati poput Fejtena većina bi pretpostavila samo časne ciljeve. Stoga inicijative poput *Electronic Frontier Foundation* razmišljaju o tome da ga učine kipom zaštitnikom (figura na pramcu galije – prim. prev.) protiv ludila-zaštite-protiv-kopiranja. Jer ako organizacije kao RIAA jednom profesoru poput Fejtena uskraćuju pravo na slobodan govor, onda to tastovima i taštama Amerike ne izgleda veselo.

Tekst se po prvi put pojavio u izdanju 47 (maj 2000) De:Bug magazina.

Podvajanja i diferencijacije među hakerima

The Script Kiddies are not Alright

Boris Grendal

U izveštajima stvar je jasna: skoro da ne prođe mesec dana, a da se u nekim novinama, novinskom žurnalu ili u nekom informacionom prilogu obično na komercijalnim TV kanalima između reklamnih blokova, ne pojavi horor-priča o *hacker*-ima. Na jednom mestu paralizuju neki *website*, na drugom mestu postavljaju brojeve kreditnih kartica, još negde dalje šire viruse i "crve", ljubavnim ili sličnim pismima zagušuju *e-mail* sisteme širom sveta. U javnoj jezičkoj upotrebi je već davno odlučeno: *hacker*-i su u najboljem slučaju mladi delinkventi, a u najgorem slučaju destruktivni teroristi. Oni vrebaju u *cyber*-svemiru i zahvaljujući crnoj kompjuterskoj magiji u mogućnosti su da isključe prekidač informacijskog društva.

U kanonskom *hacker*-skom pismu, barem američkom, stvar je dabome sasvim jasna: ono što se u medijima zove "hacker" nema blage veze sa "pravim *hacker*-ima". Neka vrsta enciklopedije *hacker*-izma – žargon *file*, koju kontinuirano dopunjuju i proširuju dobrovoljni autori, objašnjava u stilu mantre da hakeri ne mogu biti zli, nego zli treba da se zovu "cracker". Ova enciklopedija zahteva od čitalaca da se novinarima koji mešaju ove pojmove, šalje isto pismo koje je svojevremeno Ričard Stalman (Richard Stallman), osnivač *Free Software* fondacije i poznat kao "poslednji pravi hacker", poslao *Wall Street Journal*-u. Pismo je glasilo: "Ja sam *hacker*. Drugim rečima, zabavno mi je da se igram sa kompjuterima i da na njima da radim sa pametnim programima i da shvatim te programe, i da i sam pišem programe. Ja nisam *cracker*, ja se ne bavim time da "*crack*-ujem" kompjuterske sigurnosne sisteme. *Hacker*-isanje, onako kako ga ja obavljam, nije nešto čega bih se morao stideti. Ali, kada ljudima pričam da sam *hacker*, onda oni misle da priznajem da sam jeretik, jer novine kao što su vaše zloupotrebljavaju reč *hacker*. I to na taj način što ostavljaju utisak da to znači isključivo probijanje zaštitnih sistema i da to ništa drugo ne znači. Vi ozloglašavate *hacker*-a. Dužni ste *hacker*-ima jedno izvinjenje, čak i više od toga, dužni ste nam jednostavno poštovanje."

Potpuno je javno i jasno da mediji od sredine 1980-tih godina proizvode sliku o *hacker*-ima koja je uglavnom denuncijatorska i senzacionalistička i često se ne brinu o autentičnosti izveštaja. Ali, u ovom prilogu se neće raditi na tome, jer je vrlo interesantna a i nimalo nevina druga strana ove rasprave. Osetljivost "pravih hacker-a" na pogrešnu upotrebu izraza nije samo jezička brljotina i nije samo njihov zahtev za poštovanjem. U borbi pojmova za značenje reči *hacker*, manifestuje se pokušaj razgraničenja od drugih

hakera. Jedan pokušaj koji ima jako puno veze sa onim promenama što su se odigrale u poslednjih 40 godina na kompjuterima, mrežama i samoj *hacker*-skoj sceni.

Hacker-etika Stivena Levija

Već na samom početku problema pojma "hacker", nalazi se jedan novinar. Najvažnije osnovno objašnjenje "hackerstva" nije dao *hacker* nego Stiven Levi (Steven Levy), autor, između ostalog, i muzičkog magazina "Rolling Stone". Levi je 1984. godine prvi put široj javnosti približio ove kompjuterske frikove preko svoje knjige "Hacker". *Hacker*-ska scena koju je tada opisao imala je iza sebe skoro 30 godina staža. Jedno poglavlje iz Levijeve knjige je napravilo veliki uticaj na samu *hacker*-sku scenu. Tamo opisuje kako je sa prvim kompjuterima iz 1950-tih zamišljao nešto novo: novi način života s jednom filozofijom, etikom i snom. Iz mnogih razgovora koje je Levi vodio u prvom i drugom času, destilovao je osnovne vrednosti *hacker*-ske scene i tekst nazvao "Hackerethik":

1. Pristup kompjuteru – i svemu što te može naučiti o načinu funkcionisanja sveta - treba da bude neograničeno i sveobuhvatno.
2. Sve informacije bi trebalo da budu slobodne (pristup svim informacijama bi trebalo da bude slobodan).
3. Ne veruj autoritetu – zahtevaj decentralizaciju.
4. *Hacker*-i ne treba da budu osuđivani zbog *hacker*-isanja, niti po besmislenim kriterijumima kao što su akademske titule, godine starosti, po rasi ili položaju.
5. Svojim kompjuterom možeš stvarati umetnost i lepotu.
6. Kompjuteri mogu da ti poprave život.

Levijeva *hacker*-etika se često koristi kao definicija pojma *hacker* ili kao nešto univerzalno (samo po sebi jasno) podrazumevajuće za scenu. Ali, to ipak nije slučaj. Ne radi se ovde o zaključcima ili diskusijama neke grupe, niti o uslovima pristupa, niti o samoobavezivanju. Levijeva *hacker*-etika je ništa drugo nego jedna naknadna i dobronamerna interpretacija određene istorijske konstelacije. Ona je obeležena jednom sociološkom situacijom: Levi opisuje mlade momke, bele anglosaksonce na američkim univerzitetima u periodu od 1950-tih do 1970-tih godina. Ovi akteri su se uz to tada morali prilagođavati tehničkim mogućnostima jer su kompjuteri i računarsko vreme bila dobra koja su ljubomorno čuvana i prikrivana od strane birokratske elite i visokih sveštenika velikih računara. Kompjuteri su tendenciozno bili stvar vojske, a ni u kom slučaju tehnika za svakog pojedinca.

To, da li je Levijeva interpretacija odgovarajuća, barem što se tiče grupe koja se regrutovala 1950-tih godina na legendarnom Masačusets Institutu za tehnologiju (MIT), ne može se ovde odrediti, važno je samo držati se čvrsto toga da njegova *hacker*-etika nije ulaznica u svet *hacker*-a ili da je bila tipična ili čak jedina motivacija nekome da bi postao *hacker*.

U jednoj diskusiji, u legendarnom *mailbox*-u "The well", koja je vođena 1989. godine, povodom jednog *hacker*-skog kongresa, Levi je bio kritikovan za njegovu selektivnu

percepciju. Po rečima jednog od učesnika u *online* diskusiji, Džefa Poskanzera (Jef Poskanzer): "Meni je u međuvremenu postalo jasno da *hacker*-etika u stvari nikada nije ni postojala. Konačno je Ričard Stalman nagovorio Stivena Levija da predstavi neke *hacker*-e u veoma ograničenom polju i da se onda pravi kao da je to kompletna priča. Ali, to ona nikada nije bila. Čak i u to vreme je bilo više toga u *hacker*-isanju nego što je Stalmanova filozofija želela da veruje i da učini verodostojnim. Kod *hacker*-isanja se radi o istraživanju i stvaranju. *hacker*-isanje leži dijagonalno naspram etičkih principa."

Praktično u isto vreme s Levijevom knjigom došao je u bioskope i film "War Games", a u tom filmu američki tinejdžer iz predgrađa, iz svoje dečije sobe sa svojim PC-om upada u Pentagon i tako skoro izazove Treći Svetski rat. Na taj način je Levijevo jasno razumevanje *hacker*-a bilo zaprljano medijima, a sam Levi se na to naknadno gorko žalio u kasnijem izdanju svoje knjige.

Dobri *hacker*-i, loši *hacker*-i

Od tada se vodi rasprava o njegovom veličanstvu definiciji pojma *hacker*. Žargon *file* daje sledeće opise:

- Neko kome je zabavno da istražuje delove sistema koji mogu da se programiraju sve do granica mogućnosti samog sistema. Znači suprotno od normalnih korisnika, koji uče samo neophodan minimum.
- Neko ko oduševljeno (čak opsesivno) programira ili mu programiranje čini veće zadovoljstvo od teoretisanja.
- Neko, ko je u stanju da prepozna dobar "hack".
- Neko, ko može izuzetno brzo da programira.
- Ekspert za neki određeni program ili neko ko često radi sa određenim programom. Kaže se recimo: *Unix hacker*. (Definicije od 1 – 5 su povezane i ljudi koji odgovaraju tom opisu su često isti).
- Ekspert ili entuzijasta svake vrste. Na primer astronomski *hacker*.
- Neko, ko voli intelektualni izazov da na kreativan način prevazilazi ili zaobilazi prepreke.
- Zlonamerno čeprkalo koji svojim čeprkanjem pokušava da otkrije tajne informacije. U tom smislu: *hacker* za lozinke, *hacker* za mrežu... Tačan opis za ovo značenje je "cracker".

Protiv ovih *cracker*-a, autori žargon *file*-a (najprominentna ličnost u to vreme je Erik Rejmond [Eric Raymond], predstavnik desnog neoliberalnog krila pokreta za Open Source Software) izrazili su podrugljivo zapažanje: cracker - neko ko samo probija sigurnost jednog sistema. Obeleženo 1985. godine od strane *hacker*-a koji su se branili od novinarske zloupotrebe izraza "hacker". Polazi se od toga da svaki pravi *hacker* ima sakupljeno iskustvo sa *crack*-ovanjem igrica i da vlada osnovnim tehnikama. Ali od svakog ko je ispileo iz jajeta,

očekuje se da će da se odupre ovom nagonu sem ako u nekoj situaciji, i to iz dobronamernih, praktičnih razloga, mora da *crack*-uje (na primer: ako je negde potrebno zaobići neke sigurnosne mere da bi mogao da se obavi posao).

Iako se vidljivo ulaže trud da se velikom snagom pomogne medijska denuncijacija "crack"-era, ipak obe definicije otkrivaju u stvari osnovnu dilemu. Granica, koja je u tački 7. definisana kao "intelektualni izazov da na kreativan način savladate ili zaobiđete prepreke" i one u tački 8. "čeprkanje", njuškanje, istorijski je naravno potpuno promenljiva i konačno, veštačka i svojevoljna. Kao što je i za autore očigledno potpuno neproblematična kavaljerska granica između "crack-uckanja" i *crack*-ovanja kao tipične razvojne faze koja se naravno preraste, tako je sve samorazumljivo praktično prikriveno.

Diskusije unutar *hacker*-ske scene

Novinari neznalice nisu bili jedini koji su 17 godina posle objavljivanja interpretirali Levijevu *hacker*-etiku ne baš onako kako bi autor želeo. Stavovi su se 1980-tih godina podelili na pitanje da li već ulaz u tuđe računarske sisteme znači kršenje *hacker*-etike ili je nedozvoljeno samo zlonamerno manipulisanje. Žargon *file* je opet restriktivan, doduše citira se moguća definiciju *hacker*-etike, ali vrhovima prstiju i sa zapušenim nosom: "Ubeđenje da je *crack*-ovanje sistema zabave radi ili iz radoznalosti etički u redu sve dok *crack*-er ne počini krađu, vandalizam ili ne otkrije poverljive stvari", s tim da da ovo razumevanje ne dele svi *hacker*-i.

Primere drukčijeg tretiranja ove teme pruža istorija nemačkog udruženja *hacker*-a "Chaos Computer Club" (CCC). Članovi ovog udruženja, osnovanog početkom 1980-tih godina, su ne svojom voljom, zbog smešno restriktivnog nemačkog zakona o slanju informacija, stajali jednom nogom u zatvoru. Jedna od prvih akcija ovog udruženja je bila distribucija kita za pravljenje modema. Onaj ko je sklopljeni uređaj priključio na telefonsku mrežu, nije postao pionir informacijskog društva nego prestupnik. Sve strane ranih izdanja CCC novina "Datenschleuder" kipele su od nonšalantnih ali istrgnutih aluzija na preporučeno ignorisanje zakona. Tokom godina CCC je ujedno primetio da se duh ne vraća u bocu tako lako: kompjuterski fanovi koji su posedovali ilegalni modem želeli su nešto i da urade sa njim, a s nedostatkom interesantnioh javnih ponuda oni su se usmerili na one koje nisu javne. To je donelo nove probleme. Jer, bilo je jednostavno odbaciti autoritarna pravila savezne pošte, ali u svom "putovanju" po podacima, ljudi iz CCC okruženja naišli su na stvari koje su probudile pohlepu kod konkurentskih firmi, tajnih službi i medija. I *hacker*-i obavezani na informacionu slobodu, našli su se iznenada usred podataka koje bi radije zapravo kao zaštićene. To je dovelo do moralnih konflikata, koji su najzad CCC doveli do prilagođavanja pravilima koje je postavio Levi. CCC je preuzeo Levijeve principe kao da su njihovi, naglasio je da niti su boja kože, društveni status ili pol pouzdani etaloni za ocenjivanje *hacker*-a, i dodali još dva pravila koja su proizišla iz iskustva kretanja po mreži podataka:

"Nemoj rovariti po podacima drugih ljudi.
Koristi javne podatke, štiti privatne podatke."

Pozicija CCC očigledno je potpuno nespojiva sa shvatanjem žargon *file*-a. Činjenica da je u žargon *file*-u klub (CCC) ružno opisan kao banka "Alienated drug-addled crackers" (Otuđeni, drogom filovani crack-eri), znači jedan imidž CCC-a u SAD-u koji je nastao zahvaljujući denuncijatorskim delima Kliforda Stola (Clifforda Stoll), a nešto je ublažen od strane Keti Hafner (Katie Hafner) i Džona Markofa (John Markoff). Isto udruženje je u SR Nemačkoj sinonim za maltene zvanične *hacker*-e i kao što je poznato, njih konsultuju kao NVO eksperte: Vlade, partije, banke, industrija, banke podataka i mediji. Da bi zbrka bila kompletna, članovi CCC-a koji u SAD-u važe kao otpadnici, u diskusijama o mladim zlim informacionim momcima optužuju skoro istim rečima kojima ih obeležavaju u američkim debatama.

Eksterno i interno povlačenje granica

Jasno je da se unutrašnje shvatanje i samodefinisanje grupa kao što su *hacker*-i ne stvara po naučnim kriterijumima, nego po njihovim unutrašnjim granicama koje su prvenstveno postavljene prema spoljašnjem svetu. Ukoliko se radi o *hacker*-ima možemo razlikovati četiri važna kompleksa samorazumevanja:

"Pravi Hackeri"

Pravi *hacker*-i su normativni ideal žargon *file*-a. Po svom samorazumevanju: neortodoksni, genijalni programeri, koji su obavezani idealu informacione slobode i koji odbacuju državne autoritete, velike kompanije (IBM, Microsoft) i kulturološke konvencije. Ova varijanta je sada prisutna uglavnom u Linux -/Open-Source/Free softver zajednicama. Iako tendenciozno ne poštuju pravila (koja nisu sami stvorili ili ih smatraju za besmislena i suvišna ograničenja), ne propagiraju ilegalne akcije i unutar ove definicije postoji paleta diferencijacija koje se mogu učvrstiti u ličnostima, kao antipodi, kao što su Erik Rejmond (predstavnik tipično američkog ultraliberalnog fetišizma tržišta i oružja) i Ričard Stalman (takođe tipičnog američkog levo orijentisanog liberala).

***Hacker* koji prosvećuje**

Karakteristično samorazumevanje CCC-a protivi se prosvećivanju informacijskog društva o samom sebi o "duhovima" koje ono priziva. Sličan stav se može pronaći kod holandskih *hacker*-a kao i u SAD-u kod *hacker*-a okupljenih oko časopisa "2600". Od 1983. godine neguju strategiju da pronađu greške u zaštiti kod banaka i telefonskih kompanija i onda ih javno prezentuju. U SAD-u su tako dobili gore naveden *crack*-er imidž, a u SR Nemačkoj, imidž informacijskog Robina Huda, znači nekoga čije su informacije prvenstveno ozbiljne a potom nisu upotrebljene u svoju korist, nego u korist javnosti. Snažnije politički utemeljen deo ove grupe prikazuje se i u primeni socijalnih *hacker*-skih tehnika kao što je "adbusting" ili *hacker*-isanje medija. Mnogi predstavnici ove verzije ne bi na sebe primenili razgraničenje žargon *file*-a, nego bi polagali pravo na to da su "pravi hakeri".

Zli momci: *Script Kiddies, Warez d00dz* i prijatelji

Čak i *hacker*-i druge generacije distanciraju se od takozvanih "Script Kiddies"-a. Procenjena primedba o ovim zlim momcima (kojima se ovde uglavnom i bavimo) izriče najstrašniju presudu koja može zadesiti jednog *hacker*-a: da zapravo ne zna da programira, nego da ume samo da petlja sa već pripremljenim alatom. Jedan deo *hacker*-ske scene, kome se upućuju ovakve uvrede, uopšte se ne oseća neugodno nego to integriše u svoje samopredstavljanje. U uzore iz pop kulture koji se reflektuju u pseudonimima i nazivima grupa spadaju: punk, heavy metal, grunge i hip hop. Demo/Warez/virus scena je tendenciozno mlada i znatno jače obeležena imigrantima nego tradicionalne *hacker*-ske scene – žena tu takođe nema.

Polithackeri: od Jipi-a do Sijetla

Posebnu podgrupu predstavljaju oni *hacker*-i koji svoje zabranjeno tehničko znanje stavljaju u službu političkih akcija. Ova grupa ima dugu tradiciju. Najpoznatiji predstavnik 1960-tih godina u SAD-u bila je "Youth International Party" (Omladinska međunarodna partija), takozvani Jipi-i (Yippies). Jipi-i su bili zabavna gerilska formacija koja je izazivala priličnu pažnju, a *beat* generacija je bila poznata po situacionističkim akcijama kao što je bilo kandidovanje svinje protiv Ričarda Niksona (Richard Nixon) u američkim predsedničkim izborima. U njihovom glasilu "Youth International Party Line", davali su praktične savete za besplatno telefoniranje uz pomoć takozvanih plavih kutija (blue box) koje su propagirali kao protest protiv Vijetnamskog rata. Poslednjih godina sprovedene su sabotaže kao "Denial-of-service-attack" ili manipulisanje sa *website*-ovima ("Defancing") i to posebno u političkim kampanjama. Primeri su internet napadi na meksičku vladu zbog pobune Čiapas-a (Chiapas) ili akcije protivnika globalizacije na prostorima gde se sastaju Svetska Trgovačka Organizacija (WTO) ili Svetski Ekonomski Forum u Davosu. Ovi polithakeri su poseban slučaj, jer uopšte ne polažu pravo na to da sebe predstavljaju kao "hacker"-e iako je savršeno jasno da koriste *hacker*-ske tehnike.

Zbog čega postoji ta mahnita potreba za razgraničenjem?

Pokušaj "pravih hackera" da se distanciraju od svojih ozloglašenih rođaka, mora nužno da se vrati na veštačke i samovoljne kriterijume. Ne postoji pozitivna definicija pojma "hacker" koja bar malo, makar implicitno ne uključuje ilegalne, zabranjene čak nelegitimne delatnosti. Jer, nijedna, kako god formulisana definicija pojma, koji uopšte može da izvrši razgraničenje, ne pribegavajući kršenju pravila, ne izlazi na znanje, koje ili nije pripadalo *mainstream*-u ili se odvraćalo od njega, na rukovanje sa tehnikom na nenplaniran način. Ako se izostavi eksplicitni anti-*crack*-er paragraf iz žargon *file*-a, neće se naći ništa u njemu što bi zabranjivalo da opisuje *cracker*-a kao *hacker*-a. Naprotiv, paragraf sedam ("zaobilaženje prepreka") upravo poziva da se on shvati kao deo zajednice.

Jasno je i to da je kavaljerski delikt po jednom, u stvari krivično delo po drugom. Levijev "hacker", a i haker žargon *file*-a zna, tj. poznaje mnogobrojne primere kršenja pravila koja su u očima pravih *hacker*-a predstavljale bezopasne mladalačke grehe, oslobađajuća herojska dela ili opravdanu neposlušnost. Ali oni prema kojima su bili upereni su u svoje vreme naravno psovali "delinkventnu omladinu" kao što to danas čine pravi *hacker*-i.

Zašto postoji onda ta mahnita potreba za razgraničenjem? Promenjene individualne okolnosti života mogu sigurno delimično služiti objašnjenju ova dva merila. Ko se s mukom sa margine probio u središte društva, ne želi da bude podsećan od kasnijih generacija da mu je teško da prizna da je napustio svoj buntovnički položaj, i da mu današnji kodovi kulture mladih – njihova muzika, njihova moda, njihov jezik – više ništa ne govore. Za četrdeset godina *hacker*-ske istorije promenio se i društveni kontekst. Kompjuteri danas nisu, zahvaljujući i *hacker*-ima, ustanova zaklonjenog zdravog sveta belih elitnih univerziteta.

Time su umnožile i svrhe u koje se mogu koristiti. I ne na posletku, masivna kriminalizacija *hacker*-ske scene koja se odvija posebno u SAD s početka 1990-tih godina, kako su upečatljivo opisali Brus Sterling (Bruce Sterling) u "The Hacker Crackdown" i Džoš Kvitner i Mišel Slatala (Josh Quittner, Michelle Slatalla) u "Masters of Deception", proizvela je distancirajući pritisak od koga se mnogi nisu mogli osloboditi.

Literatura

(1) Steven Levy, Hackers. Heroes of the Computer Revolution, New York 1984

(2) The on-line hacker jargon File, Version 4.3.0, http://www.tuxedo.org/-esr/jargon/, 7. maj 2001

(3) Steven Levy, a. a. O.

(4) Chaos Computer Club, Die Hacker-Ethik, http://www.ccc.de/Hackerethik.html, 7. maj 2001

(5) Clifford Stoll, The Cuckoo's Egg. Tracking a Spy through the Maze of Computer Espionage, New York 1989

(6) Katie Hafner i John Markoff, Cyberpunk. Outlaws and Hackers on the Computer Frontier, New York 1991

(7) Josh Quittner und Michelle Slatalla, Masters of Deception. The Gang that Ruled Cyberspace, New York 1995

(8) Bruce Sterling, The Hacker Crackdown. Law and Disorder on the Electro¬nic Frontier, New York 1992

Boris Grendal (Boris Gröndahl), je rođen 1967.godine u Marburgu, berlinski je korespondent magazina "The Industry standard". Nakon studija matematike i fizike, radio je kao urednik magazina, izdavačkih kuća i novinar i urednik "Financial Times Germany". Godine 1996. bio je kustos izložbe "Hacker" u Heinz Nixdorf Museumsforum, Paderborn. Godine 2000., pojavila se knjiga "Hacker" u izdanju Reihe Rotbuch 3000.

4. Informatički ratnici i borci za slobodu

Američke vojne snage osvajaju *cyber* prostor

Ratnici u mreži podataka

Ralf Bendrat

Opasnost od velikog napada iz *cyber*-prostora danas spada u standardni repertoar govora, razvoja strategija i studija američke bezbedonosne politike. Već deset godina stižu upozorenja na "elektronski Perl Harbur" koji bi trebalo da bude izazvan "software-skom bombom na tržištu akcija" ili ispadom sistema sigurnosti letova koje može da prouzrokuje jedan *hacker* ili masivan napad tipa: *Denial of Service* (odbijanje pružanja usluga) na američku internet-privredu. Po navodima američkih obaveštajnih službi, u potencijalne protivnike koji se pripremaju na vođenje virtualnog rata u mrežama podataka spadaju Kineska narodnooslobodilačka vojska, islamski teroristi Osame Bin Ladena ili čak zaostala vojska Kube. Ono što se u ovim strateškim analizama nikad ne pominje, nasuprot svakoj horor vesti koje mediji vrlo rado objavljuju, uzrok je te nove trke u naoružavanju. Vojno osvanje *cyber*-prostora nije počelo u avganistanskim planinama, ili na vojnim akademijama u Kini, već u samim Sjedinjenim Američkim Državama. Od početka 1990-tih godina, američka vojska je u svojim istraživačkim laboratorijama razvila elektronsko oružje za *hacker*-ski rat. A u "fabrikama ideja" postavljene su temeljne teorijske analize i konačno, u štabovima su napisane nove doktrine. Već više puta su američke specijalne jedinice izvodile *cyber* dejstva i poslednji je bio rat na Kosovu 1999. godine. Mnogo toga se do dana današnjeg čuva kao stroga tajna. Od onoga što je dostupno u javnim izvorima, može da se napravi sasvim zadovoljavajuća slika američkih *cyber*-ratnika, njihovog oružja i organizacije. A pri svemu tome se pokazuju unutrašnje protivrečnosti i teškoće koje su povezane sa takvom slikom rata, i ispostavlja se potreba da se razmisli o novim formama kontrole naoružanja na ovom polju.

Dve razvojne linije – tehnička i strategijska – dovele su do aktuelnih napora SAD za vođenje rata na mreži. S jedne strane, vojna upotreba elektronike i kompjuterske tehnologije je prilično duga priča – ipak, kao što je poznato, prve kompjutere razvili su britanskih i američki stručnjaci za prisluškivanje radi dekôdiranja nemačke vojne komunikacije u Drugom svetskom ratu.

Posle uvođenja radara, bežične komunikacije i elektronski upravljivih bombi, razvilo se i posebno polje takozvanog "elektronskog rata" ometanjem signala, elektronskim maketama (lažna vojna oprema) i oružjem koje traži signale i uništava odašiljače; tokom 1980-tih godina razvilo se čak i takmičenje između "elektronskih kontramera" i "elektronskih

kontra-kontramera", a njihov cilj je bio da se elektromagnetni spektar koristi u potpunosti, a da se protivniku upravo to onemogući. Sredstva za tako nešto bili su oružani sistemi kao anti radarska raketa "HARM", specijalni elektronski "borbeni avioni" kao što je EC-130H "Compass Call" ili EA- 6B "Prawler", kao i visoko razvijena elektronika za komunikaciju bez ometanja i mogućnosti prisluškivanja. Ovaj razvoj, u situaciji nuklearnog zastrašivanja, politički nije bio posebno interesantan, i zbog toga je samo tehnološki forsiran. Dodajmo još i da su takve mere uvedene u "Operations Security" i bile su prisutne u vojnim obaveštajnim službama i izviđačkim jedinicama. Njihova posebna institucionalna uloga – da nisu podređeni komandantima jedinica u borbi – sprečila je razmišljanje o tome da li i kako se vođenje rata može iz osnova promeniti uz pomoć moderne elektronike.

Da bi se to ostvarilo, bili su potrebni drugi uticaji na vantehničkim putevima. A ti uticaji su došli od istorijski obrazovanih mislilaca iz Pentagona, koji su predavali i istraživali, poput Džona Arkvila (John Arquilla) sa *Naval Postgraduate School* u Montereju, zatim Dejvida Ronfelda (David Ronfeldt) i Martina Libickog iz "fabrike misli" koja je bliska Pentagonu - *Rand Corporation* iz Santa Monike ili Dana Kuela (Dan Kuehl) sa *National Defense University*-a iz Vašingtona. Oni, a i drugi počeli su početkom 1990-tih godina da razmišljaju o društvenim, a time i vojnim promenama uslovljenim novim informacionim tehnologijama. U skladu sa neoliberalnim duhom vremena, prve studije su bazirane na novim menadžmentskim koncepcijama sa fleksibilnim organizacionim oblicima i "plitkom" hijerarhijom. Sa širenjem interneta i nastajuće diskusije o "informacijskom društvu", koncept informacije dospeo je u središte pažnje kao resurs. Ako postindustrijsko društvo i njena vojna sila nisu usmereni na ljude i mašine kao sredstvo produkcije ili destrukcije, tako se razmišlja, onda ciljevi napada vojnih operacija nisu više snaga protivnika, već njegovi sistemi obrade podataka. (1)

Institucionalizacija i operacionalizacija

Time je "informacijski rat" dosegao status vojno strateške misli. Prve ideje i razmišljanja bile su postavljene već u 1970-tim godinama, ali konačan oblik dobile su tek 1990-tih godina u širokoj diskusiji o novim ciljevima, strukturnim principima i mogućnostima vođenja rata. Već 1992. godine napisana je prva strogo poverljiva direktiva Pentagona TS-3600.1 "Information warfare" sa kojim je počeo proces stalne organizacione i strateške reforme traje sve do dana današnjeg.

Debata o vođenju informacijskog rata usidrila se vrlo brzo i organzaciono u vojnom aparatu. Posledica je bila osnivanje S*chool for Information Warfare and Strategy* na *National Defense University* u Vašingtonu 1994. godine, kao i postavljanje i obuhvatanje različitih jedinica za "informacijski rat". Već godinu dana kasnije "Information warfare" postao je uzor za sve istraživačke i razvojne planove američke vojske. Avijacija i kopnena vojska su prvi postavili sopstvene strategijske predloge. Mornarica je 1995. godine postavila svoju instrukciju OPNAVINST 3430.26 za prebacivanje na informacijski rat, a u međuvremenu i marinski korpus raspolaže sa instrukcijom 3430.1 "Policy for information operations".

Tokom 1996. godine, stvarani su dodatni ključni dokumenti. Dva dana posle nove godine u Pentagonu, predsedavajući ujedinjenih šefova štabova predstavio je instrukciju CJCSI 3210.01 "Joint information operations policy". Avgusta iste godine, kopnene snage su predstavile svoj novi priručnik za upotrebu na terenu, 100-6 "Information operations", a u decembru je generalštab sastavio tajnu dopunu svoje direktive iz 1992. godine: S-3600.1 "Information operations".

Prema tada važećim predstavama američke vojske, "informacijski rat" je koncept koji obuhvata mnogo više od kompjuterskog napada. U srži sastoji se od ideje da se više ne osvajaju snage ili prostor neprijatelja, nego da se kontrolišu njegovi informacijski tokovi. Cilj je potpuna nadmoć u "informacionom polju". Sredstva za tako nešto mogu biti i elementi psihološkog rata kao što su leci ili radioodašiljači, manevarske varke, "normalno" bombardovanje komunikacionih centara ili vodova kao i elektronski napadi.

Ovako obuhvatan zahtev mogao je biti samo delimično ispunjen – previše je teško tačno poznavati jedan tuđi društveni sistem, čija tehnička infrastruktura ipak predstavlja samo jedan deo celine, i proceniti dejstva pojedinačh intervencija u lancu. To važi do dana današnjeg, kao što je i jasno prepoznatljivo u aktuelnoj praksi. Vojno premeštanje u oblik "Command and control warfire", čija je vojna doktrina takođe predstavljena 1996. godine (2), cilja dakle, na stari način, pre svega na uništenje komunikacionih infrastruktura neprijatelja, da bi borbene jedinice bile odsečene od "glave" u komandnim centrima. Ovo je već isprobano u Zalivskom ratu 1991. godine: prvi irački ciljevi koje je SAD napala bili su repetitori, antene, telefonske centrale, mostovi kroz koje su prolazili komunikacioni kablovi. Mnoge iračke jedinice su na taj način bile odsečene od nivoa komande i postale su nesposobne za dejstvo. Dodatno su još bili napadnuti i irački komandni bunkeri.

Konkretni napori američke vojske, što se tiče ovog polja, do sredine 1990-tih godina usmerili su se, pre svega, na to da od *hacker*-skih napada kao i od protivnikovog prodiranja brane sopstvene informacijske mreže, senzore i komandne sisteme. Prioritet dobija ponovno uspostavljanje sistema u slučaju napada, pa je razvoj vojnog *software*-a bio usmeren ka tom cilju. Ovo s jedne strane ima i smisla, jer pre nego što se prodre u tuđe kompjutere da bi ih se pokvarilo ili uništilo, trebalo bi se temeljno zaštititi od kontraudara. S druge strane, generalna politika Klintonove administracije reflektuje upravo ovo težište, jer ona se od 1996. godine bavila sistematskom zaštitom američke infrastrukture od *hacker*-skih napada. (3)

U pozadini i pod velom stroge tajne, u oružanim snagama, započelo se sistematičnije s razvojem ofanzivnih koncepata. Prvi put je u direktivi S-3600.1 upotrebljen novi pojam "Napad na kompjuterske mreže" (Computer Network Attack-CNA). Ti napadi obuhvataju "operacije za prekid, odbijanje, oštećenje ili uništenje informacija koje se nalaze u računarima ili mrežama ili čak i samih kompjutera i mreža". Do kraja 1990-tih godina, tekao je ovaj razvoj u tišini i osamljenosti vojnih tajnih službi kao i u istraživačkim laboratorijama, a pripadnicima oružanih snaga je još 1998. godine bilo zabranjeno da pojam "Ofanzivne kompjuterske operacije" koriste u javnosti. I u Kongresu se o programima nije otvoreno diskutovalo. Prilikom jednog saslušavanja u Senatu u vezi defanzivne strane informacijskog

rata u junu 1998. godine, direktor CIA Džordž Tenet (George Tannet) je na pitanje da li su razvijane ofanzivne mogućnosti, odgovorio jednom rečenicom: "Mi uzimamo odgovornost za naš posao vrlo ozbiljno".

Istovremeno je i javna debata koja je vođena na *website*-u Vina Švartaua (Win Schwartau), www.infowar.com, bila u stvari niz popularnih objavljivanja, a različiti konceptualni članci iz stručnih vojnih časopisa kao i nekih reportaža iz štampe otišli su tako daleko da Pentagon više nije mogao da se drži politike čuvanja tajne. Takva politika je takođe sprečavala da komandanti borbenih jedinica mogu sebi predstaviti tačnu sliku kakve instrumente će u ovom novom polju imati na raspolaganju i kako da postupaju u svojim planovima primene. Objedinjeni šefovi štaba su već 1997.godine napravili brošuru za vojsku u kojoj je između ostalog pisalo: "Informacijski rat će biti primenjen na i u svim fazama i u celokupnom polju vojnih operacija i na svakom nivou vođenja rata". Ovo prilično uopšteno uputstvo zahtevalo je jedno jasnije objašnjenje za komandante, pogotovu što su oni bili naviknuti na jasne operativne procedure. Ta objašnjenja predstavio je 9. oktobra 1998. godine, predsedavajući u generalštabu Henri Šelton (Henry Shelton) u obliku vojne doktrine JP 3-13 "Information operations". Pored odbrane sopstvenih informacionih sistema i načina sprovođenja uputstvo opisuje "ofanzivne informacijske operacije" i koji se ciljevi biraju na strateškom ili taktičkom nivou, kakva je struktura organizacije i lanac komandovanja i način obaveštavanja o uspesima operacija.

Uprkos sveopšte javnosti u vezi teme "informacijskih operacija" u američkim vojnim snagama, u oblasti kompjuterskih napada pretežno još uvek vlada tišina. Koje su tehnike na raspolaganju američkim *cyber*-ratnicima, e, to je najstrožija tajna. U "Joint doctrine for information operations", u drugom tomu "ofanzivne informacijske operacije", detaljno se upućuje na druge metode kao što su vođenje psihološkog rata, varke, elektronsko vođenje rata ili medijske aktivnosti, samo za oblast "Computer network attacks" uputstvo se nalazi na tajnom aneksu A "Suplemental information operations guidance". Ipak, iz javnih izvora se mogu izvući određeni zaključci o tome s kakvim metodama rade informacijski ratnici.

Traženje cilja: kako se mogu obuhvatiti sve datoteke ove planete

Najveći izazov u kompjuterskom ratu sastoji se u tome da se sakupi što više informacija i podataka o informacionom sistemu protivnika. To se radi uobičajenim načinom: špijunažom, elektronskim nadzorom telekomunikacija drugih država (signals intelligence) i procenom javnih izvora. Tu se nalazi i tesna povezanost sa tehnikama vođenja elektronskog rata. I ovde se ubacuju elektromagnetni signali u sisteme potencijalnog protivnika (electronic probing) da bi se dobile informacije o tome kako one funkcionišu (5). *Air Force Information Warfare Center* (AFIWC) radi takve procene u okviru projekta "sensor harvest". Iznad svega toga neguje se oblast "funkcionalne mreže" u integrisanoj banci podataka u Pentagonu pod imenom "Constant web"', koja snabdeva podacima borbene trupe informacijama o komandnim mestima i mrežama neprijatelja. Za izabrane države se ovde identifikuju kritična čvorišta njihovih mreža i infrastrukture. A *National Air Intelligence Center* ima

banke podataka o telekomunikacionim mrežama različitih država, *National security Agency* (NSA) održava jednu opširnu "advesaries" banku podataka i *Joint Warfare Analysis Center* bavi se takođe sličnim zadacima. (6)

Rad se često graniči sa Sizifovim poslom. Mnoge države za bezbedonosne potrebe koriste odgovarajuće kompjuterske sisteme, čiji način rada bez izvornog kôda (šifre) ne može da se otključa. Pri tome, su oni napisani u egzotičnim ili posebno razvijenim programskim jezicima. Jedan saradnik Pentagona izrazio se izuzetno tačno: "Tamo napolju (u drugim državama) postoji više od stotinu ideja za oružja informacijskog rata i ja bih rekao da za 98% od tih oružja nemamo saznanja neophodna za shvatanje sistema." Ljudi ne mogu da kažu da neka određena zemlja koristi kompjuterski kod "X" na "Y" kompjuteru. Često su to računari napravljeni i razvijeni tamo, a *software* je takođe pisan u isto vreme. Pošto je veoma teško klasifikovati računarsko okruženje i detaljno ga opisati, isto je tako teško i definisati oružje koje može da se upotrebi protiv toga. (7)

Treba dodati još jednu otežavajuću stvar, da mnogi vojni i civilni ciljevi ne mogu striktno da se razdvoje. Mnoge vojne sile koriste satelitske kapacitete i kablove širokog opsega koji su iznajmljeni od strane civilnih telekomunikacionih ponuđača. Povrh svega toga, kompjuterski napadi će se vršiti ne samo protiv drugih vojnih snaga, već i protiv civilne infrastrukture, terorista ili kao kontranapad protiv *cyber*-napadača. Bez obzira što američke vojne snage imaju *echelon*-ski nadzor i tesnu saradnju sa obaveštajnim službama, one nisu u stanju da elektronski istraže sve moguće sisteme. U praksi se zbog toga ograničava opet na uobičajene sumnjivce: moguća vojna konkurencija, "banditske države" ili međunarodni teroristi. Čak i *hacker*-ski aktivisti mogu predstavljati izazov: kada je 1998. godine *Electronic Disturbance Theater* (EDT) protesta radi hteo da zauzme *website* Pentagona (jer je Pentagon podržao Meksičku vladu u intervenciji protiv pobune Čiapasa), *hacker*-i *Defense Information System Agency* su uzvratili udarac: oni su na *website* ugradili jedan Java-applet, koji je omogućio da se sruši Floodnet-Tool koji je koristio EDT, a time i *web browser*.

Izbor ciljeva za napad i odgovarajućeg oružja sada više nije tehnički problem. Pošto ovakav način vođenja rata ne može da se poredi sa klasičnom tenkovskom bitkom ili strateškim bombardovanjem, komandantima nedostaje praktično iskustvo, koje im može pomoći u odlučivanju između obične bombe i *cyber*-napada. Otuda je *Air Force Information Warfare Center* (AFIWC) razvio niz simulacijskih potpora za informacijski rat, a korišćen je za obuku od strane *39. Information Operations Squadrona* iz Hulburta na Floridi. Na takvom školovanju učestvuju, na primer, i članovi štaba iz *Combined Air Operations Center*-a iz Vićence u Italiji, a oni i dan danas vode NATO operacije na Balkanu. Pošto uspesi nekog *cyber*-napada ne mogu da se snime iz aviona ili sa satelita (da bi se video krater od bombe), AFIWC radi na razvoju sistema koji bi upravo te efekte mogli da vizualizuju. Jedan od tih sistema je SIMDAS, koji omogućuje vrhovnom komandantu da prezentuje posledice *cyber*-napada, kao "hard kill" mere. Koristi se i u *Joint Information Operations Center 5* (JOIC), a on se nalazi kao i AFIWC-u vazdušnoj bazi *Kelly*, San Antonio, u Teksasu. A i *Naval Information Warfare Activity* (NIWA) čija je centrala u NSA u Fort Meade u Merilendu, razvija jedan sistem za simulaciju i planiranje za pomoć komandirima na terenu pri napadu

na komandne sisteme protivnika. Različite jedinice razvijaju i naprednije alate s kojima se automatski pravi spisak ciljeva za napad, a sistem planiranja vazdušnih snaga treba da bude gotov do kraja godine. Ovaj razvoj nosi sa sobom i određene probleme, jer ako se ne samo rat prebacuje u *cyber*-prostor, nego se sprovodi i implementacija *software*-a, onda se vrlo brzo može podleći fascinaciji novih tehnologija i mogu se iz vida izgubiti realni-stvarni i politički ciljevi rata. U krajnjem slučaju, u svakom ratu još uvek se radi samo o tome da se zauzme teritorija i da se tamošnjim vladarima ili narodu nametne svoja volja, a za tako nešto nije dovoljan *cyber*-rat, iako njegove apologete crtaju najlepše vizije o "elektronskom ratu bez krvi".

Cyber-napadi još uvek važe kao vrlo riskantno oružje, i to ne samo zbog toga što se ne mogu proceniti domino-efekti napadnutih sistema te na taj način napad na vojni sistem takvim okolnostima uvlači i štetu u civilnom sektoru, nego i zbog toga što se onda stvaraju međunarodni presedani. Upravo zbog toga, svaki pojedinačni kompjuterski napad mora da odobri predsednik SAD-a, i oni se izvode samostalno, bez saglasnosti saveznika iz NATO-a. Proći će još vremena dok *cyber*-oružje postane standardni element *Air Tasking Order*-a koji u svakom pojedinačnom slučaju određuje spisak ciljeva za napad.

Oružja *cyber*-rata

Koja su to uopšte oružja kojim su opremljeni američki *cyber*-ratnici? Pentagon ocenjuje napade na kompjuterske mreže kao "pasivne prislušne napade" (posmatranje – monitoring mreže ili dekodiranje), "insajderski napad"[1] (slučajni ili namerni), kao i "hardware/software distributivni napadi" (zlonamerna modifikacija sistema kod proizvođača ili u distribuciji) (8). Od tih stvari "prisluškivanje" i "insajder" već su davno poznati. Prislušne aktivnosti NSA, preko *Echelon*-skog sistema (9) su opštepoznate i to po celom svetu, ali spadaju u značajno niži nivo ispod klasične špijunaže. Ubačeni agenti su stari način rada obaveštajnih službi, svejedno da li snimaju mikrokamerama tajna dokumenta ili to čine autorizovanim lozinkama. Otuda su pre svega interesantni "napadi na mrežu" i "distribucioni napadi". Ovi drugi se sprovode u okviru standardizacija pravila, izvoznih kontrola ili preko tesne praktične saradnje između američkih kompjuterskih firmi i NSA, i u toj fazi se ne mogu opsluživati tj. reagovati. Ali, kako je i primećeno, oni su bili razlog za masovno korišćenje Open Source sistema kako u Rusiji i Kini, tako i u nekim evropskim državama. Ubuduće će se reagovati adekvatno pre svega na napade na mrežu (zovu ih još "hacker-sko vođenje rata").

Sredstva za to su raznovrsna, i *crack*-eri i *hacker*-i ih koriste često u civilnom sektoru: Virusi koji se kače na druge programe, "crvi" koji se sami šire, trojanski konji kao normalan program aktiviraju u pozadini neželjene aktivnosti, logičke bombe koje se mogu aktivirati sa velike udaljenosti. Tome možemo još dodati razne kôdove i pomoćne programe koji služe za savladavanje sigurnosnih prepreka neke kompjuterske mreže. Još jedna od mogućnosti su i *Denial-of-service* napadi, koji tako izbombarduje kompjuter upitima, da ne može da vrši svoju ulogu ili da se blokira mrežni opseg.

NSA, koja je zadužena i za sigurnost i bezbednost kompjuterskih sistema nacionalnog bezbedonosnog aparata SAD, veoma pažljivo motri *hacker*-ske aktivnosti širom sveta i u toku je sa najnovijim alatima i trikovima. *National Security Incident Response Center* (NSIRC), koji je smešten u NSA, stvara centralnu banku podataka sa informacijama o problemima sa bezbednošću kompjutera. A njihov ogranak, *Network Intrusion Analysis Capability,* ima zadatak da "svoje mušterije" snabdeva sa detaljnim znanjem o *hacker*-skim tehnikama. (10) Zvanično, ovo služi samo za odbranu od napada, ali to znanje se može naravno upotrebiti i u ofanzivnom smislu. Nije slučajno da borbene jedinice koje se bave informacijskim ratom imaju veoma bliske odnose sa NSA ili su čak tamo i smeštene. U NSA, od 1997. godine postoji *Information Operations Technical Center* (IOTC) u kojem specijalni ogranci iz tajnih službi i borbenih jedinica rade zajednički: *P42 – Information Warfare Support Cell NSA-a, Critical Defense Technologies Divsion CIA*-e i ogranak Pentagona J-33 "Special technology Operations". J-33 upravlja sa desetinama "crnih programa" američke vojske i oprema specijalne timove za tajne operacije. (11)

Mora se poći od toga da su kompjuterski stručnjaci NSA-a u stanju da sa standardnim metodama *hacker*-ske scene izvrše kompjuterske upade na svim dostupnim mrežama. A ono što ove upade čini mnogo žešćim od upada hobi *hacker*-a su unutrašnji resursi koji za ovako nešto stoje na raspolaganju. Sakupljeno znanje o svim poznatim rupama u sigurnosnim sistemima povezano sa tehničkim informacijama o svim svetskim komunikacionim sistemima iz "Constant Web"-a – banke podataka, ogromnim mogućnostima njihovih računara za testove lozinki i otključavanja kao i odgovarajućim brojem osoblja, čini da je NSA daleko opasnija od "Script Kiddies"-a koji se prave važni, a njih obično političari koji nemaju pojma navode kao pretnju za nacionalnu bezbednost.

Pored toga poznato je da je američka vojska već od kraja 1980-tih godina učestvovala u istraživanju i razvoju kompjuterskih virusa. Takve, više brutalne metode da se ometa neprijateljski kompjuterski sistem danas se ne uzimaju kao ozbiljni načini upotrebe, isto kao i "crvi" ili DOS napadi. Cilj *cyber*-ratnika je da se prodire u mreže, a da se to uopšte i ne primeti. Virusi i "crvi" su skoro neupotrebljivi u vojnom smislu, jer se njihovo širenje može vrlo teško ograničiti. Tome još treba dodati da je i imidž *cyber*-rata kao nekontrolisanog elektronskog pustošenja do sada suzdržavao komandante i političare da se takve mere odobre u većem obimu. Zbog toga su *cyber*-ratnici usmereni na to da svoje tehnologije predstave kao veoma precizno oružje. "Kada se diskutuje o vođenju rata u kompjuterskim mrežama, može se izleteti iz koloseka i razgovarati o virusima, "crvima" i programima koji se sami šire i svako misli da je to nešto kao oružje za masovno uništavanje i to bez ograničenja" – kaže pukovnik Dejvid Kirk (David Kirk), vršilac dužnosti komandanta *Joint Operations Center*-a. Premda se, za svaki slučaj, ovakvi scenariji takođe planiraju. Po izjavama saradnika iz Pentagona, kompletan ispad mrežnih sistema jedne države (koju bi prouzrokovale SAD), može da služi u jednoj zaoštrenoj kriznoj situaciji kao hitac upozorenja da se ta država ukroti. (12)

Pošto su *cyber*-napadi mere sa specijalnom tehnologijom, moraju se posebno odobravati. To znači da se moraju unapred davati podaci o ciljevima, sredstvima i eventualnoj kolateralnoj

šteti. "Nacionalni zapovednici žele da budu sigurni da je sistem ili čvorište mreže tačno identifikovano" (onaj protiv koga se želi upotrebiti takva tehnologija), kaže pukovnik Kirk. Cilj tadašnjeg razvoja je da *cyber*-ratnici mogu u sledećeh nekoliko godina da kažu svojim komandantima: "Mogu vam sa visokim stepenom sigurnosti reći da je rizik kolateralne štete X, da je rizik otkrivanja tehnologije Y i da je rizik za sisteme SAD-a Z". Znači, pokušava se razviti tehnologija koja će izazvati tačno definisane efekte. Već 1997. godine u *Joint Warfighter Science and Technology Plan*-u, sa žaljenjem je utvrđeno da za ofanzivni informacijski rat nedostaju pre svega još dve sposobnosti: brzo i automatski otkriti slabe tačke protivnika i fleksibilni sistemi napada koji mogu da se upotrebe protiv najrazličitijih kompjuterskih sistema. Generisan je, znači, razvoj "zalihe različitog novog oružja koje se bazira na usavršenim tehnologijama eletronski vođenog rata." (13)

Upravo to se i do danas praktikuje. Odstranjuju se poznate tehnike vođenja elektronskog rata, pre svega ometanje odašiljača i lažna manevarska sredstva i vrše se pripreme za kompjutersko vođenje rata. Pri tome se isprobava veliki broj mogućnosti. Samo kod *Information Warfare Battlelab* (koji je smešten u *Air Force Information Warfare Center* [AFIWC] u San Antoniju), od osnivanja 1997. godine istraženo je više od 270 koncepata, a detaljnije se isprobava 37 koncepata.

U *Army Science and Technology Master Plan*-u iz 1997. godine, poslednji koji je javno dostupan, može se naći još podataka o planiranim tehnologijama *cyber*-napada. U projektima koji su nazvani III.F07, III.F.09 i III.F.10 nalaze se tajne radnje za "elektronske napade na digitalnu komunikaciju", i "napadi informacijskog rata – kao i odbrana" i "informacijski rat". Po ovom planu, od kraja 1997. godine već postoje prototipovi s kojima se mogu izvesti napadi na postojeće komercijalne mreže, a od 1999. godine (američka) vojska je navodno u stanju da prekine i sve ostale komercijalne mreže. Do 2002. godine žele da budu u mogućnosti da tačno izabrana polja informacionog sistema potpuno onesposobe ili da ih ometaju, a do 2003. godine treba da bude moguće da se izvrši ciljani uticaj manevrima elektronske obmane i manipulacije podataka. Tek od 2004. godine očekuju se tehnologije koje će moći elektronski da unište informacione sisteme (14). Kako kaže *Joint Warfighter and Science Technology Plan*, tada treba da budu u pripravnosti sistemi za vođenje "integrisanog ofanzivnog informacijskog rata".

To sve izgleda veoma sporo, kada se posmatraju ti tako punim ustima izgovoreni info-rat govori, članci, knjige, strateški papiri jer oni se sastavljaju već deset godina. Brigadni general Džon Bejker (John B. Baker), nekada direktor *Air InterIligence Agency* i šef *Joint Information Operations Center*-a je još 1999. godine rekao: "Ako se radi o tome da pored čistog prisluškivanja prenosa podataka, manipulišemo i iskoristimo 'nule i jedinice' (onda je pred nama još dug put)". Ali, ne treba da se zaboravi da se baš na napadima na informacijske mreže radi o potpuno novoj vrsti oružja i da se i drugi projekti naoružavanja delimično protežu i na 15 i više godina. Konstantan problem koji je ovde znatno oštrije izražen (u odnosu na druge projekte naoružavanja) je neverovatno brz razvoj informacione tehnologije upravo u civilnom sektoru. Jednom razvijeni ratni sistemi informacijskog rata mogu u stvarnosti da se koriste u veoma kratkom vremenskom periodu, i to pre nego što

postanu neupotrebljivi zahvaljujući novim zaštitnim sistemima i *upgrade*-ovanju ciljeva. Sledeći problem koji može imati *cyber*-ratnik je da se njihove tehnike mogu koristiti u ograničenom obimu: ko je jednom bio napadnut, može da evaluira svoje iskustvo i sa nešto stručnog znanja da se odbrani od drugog napada.

Mnoga oružja za *cyber*-rat razvijaju se u okviru davno planirane modernizacije postojećih sistema za vođenje elektronskog rata. Srž elektronskog arsenala vazduhoplovstva (Air Force) je modifikovana verzija Lokidovog transportnog aviona C-130 "Hercules". Specijalna verzija EC-130H sa oznakom "Compass Call" raspolaže sa tovarnim prostorom prepunim elektronike i raznim antenama s kojima se prisluškuju radio veze neprijateljskih trupa, da bi se posle evaluacije mogli ciljano uništiti. Uobičajeno je da se napravi slobodan prolaz bombarderima i to tako što se ometaju integrisani sistemi protiv-vazdušne odbrane. Srce uređaja je malo zastareli odašiljač i prijemnik sa tri modula za UHF frekvencije, jedan za VHF, jedan KY-58 satelitski sistem i dva KY-75-HF modula. (15)

Za sistematičnu primenu i protiv tehnološki visoko razvijenog neprijatelja ili protiv komercijalnih veza, sistem koji su prvobitno razvijali za analogne signale nije dovoljan. Dalji razvoj treba da ide na dva koloseka: s jedne strane se za 2007. godinu planira *Common Sensor* avion koji će biti u stanju da nastupi i protiv digitalnih signala i to sistematično i da vodi zaista kibernetske ratove iz vazduha. Projekti *Information Warfare* i *Digital Communications Electronic Attack* iz *Science and Technology Master Plan*-a vojske upravo se za to i izvode. Povrh toga, za elektronsko i digitalno uvođenje rata kao pojačanje treba da se koriste i bespilotne letilice koje će da presreću, automatski evaluiraju i ometaju signale protivnika. Upravljanje se vrši sa *Compass Call*-a ili sličnih raspoloživih aviona, kao na primer RC-7 *Airborne Reconnnaissance Low* (ARC), RC-135V/W *Rivet Joint* ili RC-12 *Guardrail*, a njihov zadatak treba da preuzme novih 40 *Common sensor* sistema. Vazduhoplovstvo (US Air Force) upravo modernizuje glavni model *Global Hawk*, kopnene snage u istu svrhu razvijaju *Tactical Unmanned Areial Vehicle* (TUAV). Još jedan dodatni modul za elektronsko vođenje rata treba da bude kompaktna stanica na terenu za prisluškivanje i elektronsko ometanje i pravljenje lažnih signala neprijatelju, a radili bi u saradnji i koordinaciji sa sistema iz aviona. Uređaj može da stane u vozilo sa prikolicom, kao i u tovarni prostor transportnog aviona. (16)

Neki od defanzivnih sistema koji služe za zaštitu sopstvenih računara, može da se upotrebi i u ofanzivne svrhe. *Air Force Information Warfare Center* je razvio jedan program sa kojim se sumnjivim uljezima može staviti pečat – time bi uobičajene maskirne tehnike kao što je stalno menjanje korisničkog imena i lozinke postalo potpuno nedelotvorno. Pošto se praćenjem elektronskog traga hakera može doći do njegovog kompjutera, potrebno je pod određenim okolnostima upadati i u tuđe mreže, a onda treba da je moguće ubaciti i virus ili manipulisati podacima.

Prve primene

Već od sredine 1980-tih godina, američki *hacker*-i su pravili upade u kompjuterske mreže Varšavskog pakta. Saradnik CIA-e i NSA beleži po sopstvenim podacima – da su imali

"značajne uspehe u penetraciji u tajne vojne kompjuterske sisteme Sovjetskog Saveza, kao i drugih država". Tada se to pretežno radilo radi špijunaže. Tehnološki napori su se tada koncentrisali na elektronsko vođenje raketa i ratnih aviona. U jednoj vojnoj akciji, prvi put su primenjeni kompjuterski upadi u okviru *Uphold Democracy* na Haitiu 1994. godine, kada su SAD vratile na vlast oborenog predsednik Bertrana Aristida (Bertrand Aristida). Mere je tada odobrio lično predsednik Klinton (Clinton). Posle toga je izvedeno nekoliko "relativno beznačjnih" kompjuterskih napada – barem po priči pripadnika američke vojske *Washington Post*-u. Mnogi od njih su služili pre svega kao nadzor nad protokom informacija protivnika. U mnogim drugim slučajevima stizali su predlozi od Pentagonovog odeljenja za "specijalne tehničke operacije" i razvijani su za ministra odbrane i predsednika. Ali, proces odobravanja je trajao tako dugo da više nisu mogli biti upotrebljavani. (17)

Rat NATO-a protiv Srbije za Kosovo se smatra, i to višestruko kao prvi pravi *cyber*-rat. Ovaj naziv je dobio pre svega zbog jakog učešća *hacker*-ske scene na obe strane, i to pre svega kao psihološke i političke rasprave na internetu. Često su *crack*-ovani *website*-ovi i punjeni sa podacima za ili protiv rata, a posle bombardovanja Kineske ambasade u Beogradu su se u virtualne rasprave uključili i kompjuterski frikovi iz Narodne Republike Kine. Povrh toga, izvođeni su napadi pre svega protiv NATO, *Denial-of-service-attack* i *mail*-server je bombardovan *e-mail*-ovima inficiranim virusima. Ali, ovo je više bila elektronska forma političkog divljaštva nego nešto što bi se nazvalo "rat". Manje poznato je da su SAD elektronskim putem napale srpske protiv-vazdušne sisteme i to ne samo da su ih ometali, nego i ciljano manipulisali. Da bi to postigli, sa EC-130H *Compass Call*-a prisluškivali su visokofrekventne mikrotalasne podatke, onda su ih modifikovali i sa jakim predajnikom opet emitovali. Na kraju su operateri odbrambenih položaja na svojim monitorima videli ciljeve koji uopšte nisu postojali. Dalje, izvršen je napad na srpski telefonski sistem (fiksna mreža) da bi prinudili komandante u Beogradu da sa svojim trupama na Kosovu komuniciraju preko mobilnih telefona, jer se mobilni telefoni lakše prisluškuju, pošto se ne mora imati direktan kontakt sa telefonskim kablovima.

U Kosovskom ratu su se pokazali i problemi koje američka vojska još uvek ima sa vođenjem *cyber*-rata: strogo poverljiva operacija bila je još ranije pripremljena od strane *Joint Information Warfare Center*-a u saradnji sa komandantima u Evropi i to još onda kada su se događaji na Balkanu počeli zaoštravati. Politička dvoumljenja sprečila su primenu odmah pri početku rata 24. marta, a odobrenje iz Vašingtona je stiglo tek nešto kasnije. Kada su onda *cyber*-ratnici sakupili sve potrebne informacije i pripremili sisteme, bombardovanjem terena je već bilo uništeno toliko mnogo da je bilo teško proceniti koji su zaista uticaj imali *cyber*-napadi. Naknadne procene su došle do zaključka da se moglo postići i više da su *cyber* oružja korišćena sistematičnije. Ljudi iz Pentagona procenjuju da je možda iskorišćeno deset posto mogućnosti. (18) U jednom internom izveštaju mornaričkih jedinica, a koji je procurio u štampu, tvrdilo se čak da bi rat trajao upola manje da su informacijski napadi izvođeni bolje i opsežnije.

Da se u informacijskom ratu ne radi samo o napadima na vojne mreže i podatke, dokazuje i saopštenje *Newsweek*-a u maju 1999. godine. Navodno je Bil Klinton ovlastio

CIA-u da u okviru jedne *Special technical operation* upadne elektronski u banke u Rusiji, na Kipru i u Grčkoj da bi ispraznio inostrane račune predsednika Jugoslavije, Slobodana Miloševića. Potpuno u suprotnosti sa do sada navedenim akcijama, koje su usmerene protiv vojne sile jedne od zaraćenih strana, u ovom slučaju su pod američkom "paljbom" bili i civilni sistemi država koje nisu učestvovale u sukobu. Čak je i NATO partner Grčka bila izložena virtualnoj 'prijateljskoj vatri'. Čak ni NATO saveznici nisu bili uključeni u ove planove. Kasnije se ispostavilo da je ova akcija očigledno bila stopirana od strane pravnika iz američke vlade, ali po jednom izveštaju *United Press International*-a, Amerika je upala u skrivena konta aktuelnog omiljenog neprijatelja, Osame Bin Ladena. Pošto je tajnim službama uspelo da prozru finansijsku mrežu islamističkog milionera, američki *hacker*-i su mogli da upadnu na račune i da preusmere novac ili da ugase račun. "Tri klika na tastaturi i nema ga" – rekao je jedan američki službenik UPI-u. (20) Da li nečega ima u ovoj priči – treba sumnjati, jer postoje tesne veze između UPI i mračne sigurnosne firme *iDefense*-a koja je firma u direktnom podređenom položaju u odnosu na NSA i Pentagon. Džejms Adams (James Adams), bivši šef UPI-a, a danas direktor *iDefense*-a, više puta je javno prozvan zbog pogrešnih informacija. Po izjavama *Chaos Computer Club*-a, tehnički je moguće preko međunarodnog bankarskog sistema falsifikovati SWIFT doznake. Tajne službe kao što je NSA su u stanju to da izvedu.

U svakom slučaju, priča skreće pažnju na realnu opasnost: *cyber*-napadi ne mogu se više nadzirati od strane parlamenta i javnosti kao što je slučaj sa normalnim ratovima, i civilni ciljevi su svakako predviđeni u ofanzivnim američkim doktrinama. Članovi odbora tajne službe Senata i predstavničkog doma SAD-a koji su na tajnoj sednici bili informisani o virtualnim napadima CIA-e na bankovne račune Miloševića, takođe su izrazili zabrinutost. Takva akcija protiv inostranih banaka ne da je prekršila mnoge međunarodne ugovore, nego bi mogla i ugroziti vodeću ulogu SAD-a u svetskom bankarskom poslovanju. Takođe, ovaj slučaj kršenja suvereniteta čak i savezničkih država je jedan opasan presedan i prosto poziva da se imitira, znači da se napadnu američke banke. Uostalom, SAD bi jednog *hacker*-a, koji bi pokušao nešto slično kod neke njujorške banke, označila kao *cyber*-teroristu.

Problemi prihvatanja i problemi kadrova

Izvan takvih spektakularnih pojedinačnih akcija, integracija *cyber*-ratnih planova u normalna vojna dejstva veoma sporo napreduje. Spomenuti Kosovo-*breafing* mornarice bio je interesantan jer je navodio i uzroke. Autor je opisao osoblje *Information Operations Cell*-a kao "vanredne ljude" ali je dopunio: "Imali su suviše male činove i dolazili su iz pogrešnog miljea i nisu imali dovoljan uticaj na planiranje i sprovođenje akcija, kakav su trebali da imaju." (21) Za mnoge komandante su i sopstveni *hacker*-i još uvek jedna sumnjiva grupa koja sa uobičajenim fizičkim opterećenjem vođenja rata nema mnogo zajedničkog. Vođenje rata sa klikovima na mišu ili sa bespilotnim letilicama i bez realnog oružja za vojsku koja obožava heroje, telesnu disciplinu i angažovanje sopstvenog tela, još uvek je neuobičajena ako ne i neprijatna stvar. To što poreklo vođenja *cyber*-rata vodi iz tajnog aparata izviđačkih

jedinica, takođe ne doprinosi tome da se informacijsko oružje posmatra kao još jedno "oružje sa police" kako je to rado formulisao general Ričard Majers (Richard Myers) koji je vodio odeljenje za kompjutersko vođenje rata u *Space Command*-u. Često su planovi za napad sa konvencionalnim oružjem već bili spremni, kada se neko seti i vojaka za informacijski napad, i da bi se i oni mogli nešto pitati. Tako se žale mnogi vojnici zaduženi za *cyber*-rat. Veliki deo posla u *Air Force Information Warfare Center*-u sastoji se sada u tome da unutar trupa propagiraju svoj *know-how* i njegove tehnologije.

Za sada još uvek nedostaju jasne smernice delovanja za *cyber*-napade. Jer one do danas spadaju u nedovoljno precizno definisan prostor "informacionih operacija", a planeri Pentagona imaju puno teškoća da postave uslove i pravila postupanja za takve intervencije. Svaki scenario, koji bi eventualno zahtevao upotrebu *cyber*-oružja, mora biti posebno razvijen i isto tako odobren. Sada se pravnici američke vojske bave time da li, i pod kojim okolnostima pravo naroda tako nešto uopšte dozvoljava. Paralelno s tim radi se na opsežnoj vojnoj strategiji za informacijski rat – Oplan 3600. Termin za završetak nije postavljen. (22)

Još jedan problem koji stalno pritiska je i nedostatak kadrova. Pentagonu nedostaju na svakom koraku kompjuterski eksperti, jer oni nalaze višestruko primamljivije poslove u privatnom sektoru. Neki ipak idu i drugim putem, jer cene radno vreme koje je regulisanije nego u Silikonskoj dolini ili podlegnu iskušenju da upadaju u tuđe računare a da pri tome ne budu zakonski gonjeni. Ali, to nije dovoljno da se pokrije potreba u ovoj oblasti. Vojsku jednim delom napuštaju i *software*-aši jer njihove ideje u škrtom aparatu često nailaze na zid. Jedan od primera je i *Wheel Group* koja danas pripada mrežnom gigantu *Cisco Systems*. Osnovali su je visokokvalifikovani kompjuterski eksperti *Air Force Information Warfare Center*-a (AFIWC), koji je 1998. godine vodio istragu kada su britanski *hacker*-i izvršili upade u *Air Force Rome Laboratories* i u *Air Force Materiel Command*. Tada su razvili "netsnifera" i nazvali ga "NetRanger". Ovaj se nije dopao AFIWC-u, jer je tamo jedan drugi proizvod smatran za pravu stvar, i onda su kompjuterski frikovi napustili *Air Force*, tj. avijaciju i osnovali svoju firmu. A komercijalno rasprostranjen "NetRanger", kasnije je koristio čak i od *609th Information Warfare Squadron*.

Da bi popravio ionako malobrojno osoblje u IT sektoru, Pentagon je u decembru 2000. godine počeo da poziva rezerviste sa kompjuterskim znanjem. Ukupno pet planiranih timova, takozvani *Joint Reserve Information Operations and Informations Assurance Organizations* treba između ostalog da budu upotrebljeni za sigurnost – bezbednost sopstvenih mreža kod operacija prisluškivanja ali i u svrhu kompjuterskih napada. Do 2007. godine treba da bude postavljeno 600 ljudi koji bi čak i u *part-time* aranžmanu radili za NSA ili *Joint Infornmation Operations Center*. Da bi se zaobišla kratkotrajna uska grla, Pentagon je bio prinuđen da pojačano angažuje privatne firme. A tako nešto opet povećava troškove. Naravno da se mnoge firme motaju između mrežne zaštite, studije rizika, analiza i kompjuterskih napada, koji su de facto *cyber*-plaćenici za *hacker*-ske ratove SAD-a. Na primer, firma *Sytex Inc.* pomaže pri "analizi, pripremi i podeli podataka o informacijama relevantnih za *cyber*-rat" – jasno je rečeno, to znači: saradnja pri izboru ciljeva – meta za napad.

Sytex je još i u Bosni bio uključen i na osnovu rastućih zahteva, upravo su osnovali jedan *Information Warfare Center of Excellence*. I druge firme su angažovane na ovom polju, kao na primer *SAIC* ili *Veridian*. *Veridian* je dobio zadatak od preko 38 miliona dolara da isporuči *Infowar odeljenju Naval Air Warfare Center*-u jedan kompletan paket za planiranje i realizaciju informacijskih ratova. *Syracuse Research Corporation* nudi mogućnost školovanja u informacijskim operacijama, a i *hacker*-isanje je u ponudi. Klijenti su pored raznih *cyber*-jedinica američke vojske takođe i CIA, kanadska vojska i veliki proizvođači oružja kao što je koncern *Lockheed-Martin*.

Nova trka u naoružanju?

U roku od deset godina, iz prvobitno skeptičnih diskusija eksperata na vojnim akademijama, došlo se do nove vrste oružja (praktično novi rod vojske). I taj novi rod treba zadržati pogotovo ako se želi razmišljati o političkim posledicama i problemima američkih planova za *cyber*-rat. Iako je još uvek prilično neprecizna definicija šta je zaista "informacijski rat", iako su nejasna pravila dejstvovanja kao i pravni problemi, iako postoje tehnički problemi i nedovoljna prihvaćenost unutar jedinica: *cyber*-rat je počeo da sazreva. Učvrstio se u vojnom aparatu sa svojim jedinicama, odeljenjima za planiranje, vojnom doktrinom i skoro nepreglednom teorijskom literaturom. Mnoga od otvorenih pitanja se obrađuju u vojnoj birokratiji i u razvojnim laboratorijama oružanih snaga i industrije oružja, i može se poći od toga da će najkasnije za pet godina većina tih pitanja biti rešena.

Sve to postavlja pitanje o političkoj kontroli nečega što je do sada pre svega bio tehnološki i vojnostrateški razvoj. Ako američki *cyber*-ratnici mogu neotkriveni, i isključujući parlament i javnost, da upadaju u bilo koju mrežu na svetu, ako pri tome komercijalne mreže mogu da budu ciljevi-mete kao i kompjuterski upravljana infrastruktura industrijskih društava, kada se zbog potere za teroristima vrše neovlašćeni upadi u internacionalne banke, čak iako se pride još i usavrše nadzorne tehnike i ugrađuju čak i tajna vrata na američke kompjuterske proizvode – onda će oni koji čuvaju podatke biti jednako nervozni kao i branioci ljudskih prava, čak i čitave privredne grane.

Ovome treba dodati i uzornu funkciju SAD. Mnoge države su pažljivo pratile američki razvoj i počinju sada da kuju sopstvene planove za *cyber*-rat. Kao prvi kandidati smatraju se: Kina, Indija, Pakistan i Izrael, kao i neke evropske države, među njima i Nemačka. Svi su oni u startnim pozicijama. U međuvremenu upozoravaju i direktori američkih tajnih službi, pri saslušanjima u kongresu, o "Narodnom informacijskom ratu" iz Kine i traže da se ulaže više u naoružanje SAD-a na ovom polju. Posmatraču koji je obrazovan u domenu bezbedonosne politike, ovo su prvi pokazatelji klasične trke u naoružanju. Preteče *cyber*-rata, kao što su Džon Arkvila (John Arquilla) ili Den Kuel (Dan Kuehl), već brinu može li da se kontroliše razvoj onoga što su oni pokrenuli.

Sada se nailazi na veliko interesovanje u akademskim diskusijama o prvoj ideji kontrole *cyber*-naoružavanja, kako su je između ostalog razvili nemačko-austrijska istraživačka grupa informacijskog društva i bezbedonosne politike (FoG:IS) ili *Information Assurance Advisory Council* (IAAC) sa londonskog *Kings* koledža. Prvi koraci za obezbeđenje mira u *cyber*-prostoru bili bi na primer: dogovor o "No first use" i izjavljeno odustajanje od napada na civilne ciljeve. Kao srednjoročni cilj postavlja se jedna međunarodna konvencija za mirnodopsko korišćenje *cyber*-prostora. A vreme ističe. U februaru 2001. godine *Air Intellingence Agency* (u kojoj je većina od više hiljada *cyber*-ratnika obavljalo svoju dužnost) podređena je *Air Combat Command*-u. Tako da je ona sada deo borbenih jedinica i prava upotreba njihovih nevidljivih oružja je sve bliža. U Nemačkoj je vlada uspela da da ispoštuje svoje koaliciono obećanje: "crveno-zelena spoljna politika je politika mira i za budućnost i to tako što je u razvoju mira, ali i u Generalnoj Skupštini Ujedinjenih Nacija počela tj. pokrenula napore za ograničenje trke u elektronskom naoružanju. Zašto ovde ne bi funkcionisalo ono što se već desilo u oslobođenju kriptografije ili u potenciranju *Open-Source software*-a, znači i dalje se u Nemačkoj misli više civilno negu u vojnoj sili zvanoj SAD.

Literatura:

(1) Deo debate u John Arquilla / David Ronfeldt (Ur.), In Athena's Camp. Preparing for Conflict in the Information Age, Santa Monica, 1997

(2) Joint Chiefs of Staff, Joint Pub 3-13.1, joint Doctrine for Command and Control Warfare, Washington, D.C., 7. 2. 1996

(3) Ralf Bendrath, Elektronisches Pearl Harbor oder Computerkriminalitat? Die Reformulierung der Sicherheitspolitik in Zeiten globaler Datennetze, in: S+F, Vierteljahresschrift fiir Sicherheit und Frieden, Nr. 2/2000, S. 135-144 [4] Joint Chiefs of Staff, Joint Pub 3-13, joint Doctrine for Information Operations, Washington, D.C., 9. 10. 1998

(5) Joint Chiefs of Staff, Joint Pub 3-51, Joint Doctrine for Electronic Warfare, Washington, D.C., 7. 4. 2000

(6) USAF Intelligence Targeting Guide, Air Force Pamphlet 14-210, Intelligence, Washington, D.C., 1. 2. 1998, Kapitel 11: Targeting in the Information Age, S. 88

(7) David A. Fulghum / Rober Wall: Cyber-Arsenal Needs Testing, in: Aviation Week & Space Technology, 26. 2. 2001

(8) John L. Woodward, Jr., Department of Defense Director for Command, Control, Communications and Computer Systems, Information Assurance through Defense in Depth, Washington, D.C., Februar 2000, S. 5

(9) Pogledaj izveštaj u Telepolis-u, http://www.heise.de/tp/deutsch/special/ech/default.html

(10) William Clinton, Defending America's Cyberspace. National Plan for Information Systems Protection Version 1.0. An Invitation to a Dialogue, Washington, D.C., 7.1.2000, S. 49

(11) William M. Arkin: A Mouse That Roars?, washingtonpost.com, 7.7.1999

(12) David A. Fulghum / Robert Wall, Information Warfare Isn't What You Think, in: Aviation Week & Space Technology, 26.2.2001

(13) Office of Secretary of Defense, Joint Warfighter Science and Technology Plan, Washington, D.C., 1997, Kapitel IV.I "Information Warfare" [14] Department of the Army, Army Science and Technology Master Plan, Washington, D.C., 1997, Annex A: Science And Technology Objectives (STOs), Kapitel IILF.

(15) David A. Fulghum, Compass Call To Dominate Electronic, Info Warfare, in: Aviation Week & Space Technology; 18.10.1999

(16) David A. Fulghum, Army Hackers Go Airborne, in: Aviation Week & Space Technology, 18.10.1999

(17) William M. Arkin, The Cyber Bomb in Yugoslavia, wash ingtonpost.com, 25.10.1999

(18) Lisa Hoffman, Special Report: U.S. opened cyber-war during Kosovo fight, in: Washington Times, 25.10.1999

(19) Gregory L. Vistica, Cyberwar and Sabotage, u: Newsweek, 31.5.1999, S.22

(20) U.S. Makes Cyberwar on Bin Laden, United Press International, 9.2.2001

(21) Bob Brewin, Kosovo ushered in cyberwar, in: Federal Computer Week, 27.9.1999

(22) Ellen Messmer, U.S. Army kick-starts cyberwar machine, in: Network World, 20.11.2000

Ralf Bendrat (Ralf Bendrath)**,** doktorirao na berlinskom Slobodnom univerzitetu, temom "Vojska u informatičkom društvu". Sem toga je poslovođa istraživačke grupe Informatičko društvo i bezbednosna politika, pokretač *mailing* liste *Infowar* i redovno piše u *Telepolis*-u na ove i slične teme. Više informacija na http://userpage.fu-berlin.de/-bendrath

Alati za zaštitu podataka za anonimnu i 'zaključanu' komunikaciju omogućuju izuzetno vredan slobodan prostor u informacionom svetu koji se sve više kontroliše.

Digitalne slobodne luke

Kristijana Šulcki-Haduti

U privatnom životu je razdvajanje između javnog i privatnog jednostavno za regulisanje: iza vrata vašeg stana sve je privatno – i toga je svako svestan. Informacione tehnike prelaze kućni prag bez problema. Upad u privatnu sferu može biti podstaknut s različitih strana i s različitim motivima: komercijalni interes, razni islednici, tajne službe, represivni politički sistemi, svi oni imaju interes za uvid u komunikacije privatnih lica, organizacija i firmi. Iako bi trebalo pretpostaviti, barem u demokratskim državama, da i sama vlast ima interes da njeni građani mogu slobodno i sigurno da koriste elektronsku komunikaciju, ipak je već nekoliko godina odbacivan razvoj odgovarajućh alata kroz debatu o kriptopolitici. U isto vreme, kod zakonodavaca se javljaju policija i tajna služba sa svojim željama, tako da svaka komunikacija može da se prisluškuje, a anonimnost se skoro poistovećuje sa zločinom i to uvek sa istim argumentima: dečija pornografija, politički ekstremizam i organizovani kriminal, pokušava se ditribucija alata koji omogućuju sigurnu komunikaciju za svakoga – ili da se spreči ili da se proglasi ilegalnom. Na drugoj strani na tehnikama rade angažovani pojedinci, akademske i komercijalne grupe za razvoj koje treba da pomognu u proboju do osnovnog prava na privatnu i necenzurisanu komunikaciju. Oni predstavljaju digitalne slobodne luke.

Alati za zaštitu podataka u osnovi rade na dva principa: podatak se zaključa (kôdira) i onda se tako raspodeljuje da bilo kad centralna kontrola postaje nemoguća. Opšti način zaštite ne postoji, ali zavisno od potreba, ima različitih alata na tržištu. Da biste čitali *e-mail*-ove u četiri oka, od pomoći su programi kao što je *Pretty Good Privacy*. Za slanje neprepoznatlivog *e-mail*-a postoje *remail*-eri. Anonimno *surf*-ovanje je takođe želja mnogih, pogotovu zbog napada raznih *cookie*-a kao i zbog *bug*-ova koji mogu da špijuniraju privatne podatke. Ostali alati služe da bi se zaobišle moguće cenzure. Većina ovih alata je još u ranoj razvojnoj fazi, ili su komplikovani za upotrebu, ili ne garantuju dovoljnu sigurnost. Ali, vredne zajednice entuzijasta vehementno rade na daljem razvoju alata za zaštitu podataka, od kojih će ovde biti predstavljeni oni najvažniji:

Pretty Good Privacy (PGP)

Sve ono što korisnici ne žele da saopšte dopisnicom nego stavljaju u koverat, trebalo bi da kôdiraju i na internetu, jer *e-mail* "protrči" kroz mnogo računara dok ne stigne na računar primaoca. Poruka se može pročitati na svakom od tih usputnih računara, a i sadržaj se može izmeniti tako da to ne primete ni pošiljaoc ni primalac.

PGP kao program za kôdiranje i dekôdiranje je u ponudi, i to za skoro sve vrste računara, i što je bitno, besplatan je za privatnu upotrebu. Skraćenica *PGP* znači "Prilično dobra privatnost". Ovaj *software* za kôdiranje i dekôdiranje važi već godinama kao *de facto* standard za sigurnu komunikaciju na internetu, a i pomogao je da se probije američka zabrana kripto izvoza. Kod je izvezen preko knjiga i u Evropi je mukotrpno opet uskeniran, jer izvoz knjiga nije bio zabranjen.

Policija i tajne službe još uvek ne mogu da "prisluškuju" *PGP* kôdirane mailove, pod pretpostavkom da ga korisnik ispravno koristi. Napad na poslednji kompjuter bi bio moguć velikom "strategijom prisluškivanja" i mogao bi da da pozitivan rezultat, jer se na matičnoj ploči nalazi tajni kôd. "Islednici" tada moraju samo da nađu tajnu lozinku.

U međuvremenu postoji mnogo vezija *PGP*-a. Kritički raspoloženi stručnjaci preporučuju spartansku (osnovnu) verziju PGP-a 2.6.3. Taj program je besplatan na internetu zajedno sa grafičkom platformom kao mail PGP program (za Windows 95, 98, NT). Svejedno je koja se verzija koristi, tokom prvog koraka se automatski stvara jedan par kôdova. Kasnije se mogu stvarati dodatni kôdovi. Mora se izabrati kojim kriptografskim principom će se proizvesti kôd (ključ): *RSA* ili *Diffie hellmann DSS*. Korisnici 2.6x verzije mogu koristiti samo RSA kôdove (ključeve). Korisnici novijih verzija biraju po pravilu *Diffie Hellmann DSS,* jer se ovde mogu napraviti duži, a samim tim i sigurniji ključevi: na primer, jedan par *RSA* kôdova od 2048 BIT-a sa neograničenim trajanjem, a i jedan drugi par koji će biti validan samo dva meseca. Ovakve stvari povećavaju sigurnost.

Onda se unosi kôdirana fraza, tj. tajna lozinka. Najsigurnija opcija je upotreba izmišljenog reda brojeva i slova. Minimum je osam znakova, i bilo bi preporučljivo da mogu da se pamte (bez pisanja na papiriću), jer ti znakovi moraju da se upišu prilikom dekôdiranja. Na kraju se par kôdova generiše. Na sporim računarima ovaj postupak može trajati nekoliko minuta.

Posle se javni kôd klikom na miša može poslati na internet, na jedan od takozvanih *key servera*. To su banke podataka u kojima se nalazi veliki broj javnih kôdova (ključeva) i odatle se isti mogu koristiti. Po pravilu, računari međusobno razmenjuju ključeve ili se taj ključ eksportuje klikom na miša u jednu datoteku koja se može poslati i *mail* partneru ili se može javno staviti na raspolaganje na svom *homepage*-u.

Kôdiranje principijelno funkcioniše tako da *mail* partner ima jedan par kôdova iz javnog dela, a takođe poseduje i tajni kôd. Sa javnim kôdom se poslati *mail* kôdira, a primalac može da ga dekôdira samo uz pomoć tajnog ključa. Kôdirati se mogu čitave datoteke kao i pojedini delovi teksta. Uz pomoć PGP-alata mogu se izabrati odgovarajuće datoteke. Dekôdiranje funkcioniše vrlo slično. Postoje takođe programi koji tajne kôdove memorišu na

matičnoj ploči. Tako na primer postoji makro program koji se nalazi u *Word* dokumentima, koji ove kôdove pokušava da pošalje preko interneta.

Sa napadačkim programima "Back Orifice" ili "Netbus" može se lako prisluškivati datoteka u kojoj je memorisan tajni kôd, iako je kôdirana i zaštićena lozinkom. Pre svega se jednostavne lozinke lako mogu provaliti automatskim isprobavanjem.

Znači, preporučljivo je datoteku sa tajnim kôdom memorisati na disketu, a ne na matičnu ploču. Još sigurnije bi bilo tajne kôdove memorisati na čip karticu ili na neku sigurnu pokretnu spravicu.

Remailer

Mix-računari koji isključivo anonimizuju *e-mail* poruke zovu se *remailer*-i. Preko jednog *remailer*-a moguće je poslati poruku u neku *usenet* grupu ili nekome lično poslati *mail,* a da primalac ne zna ime ili adresu pošiljaoca. Luc Donerhake (Lutz Donnerhacke) je donedavno u Jeni imao *remailer* (2), ali ga je zbog prevelikog opterećenja deaktivirao.

Pseudoanonimni (takozvani anonimni) *remailer*-i su skoro iščezli sa interneta, oni anonimizuju poruke tako što jednostavno izmene ime i adresu i stave neku drugu adresu i ime. Pozitivno je bilo to što se preko ovih *remailer*-a mogao slati i odgovor (koji je i stizao). Negativno je to što su kod ovih r*emailer*-a pravo ime i pseudonim bili na jednom mestu. Godine 1996., sajentologija je sudskim nalogom dobila pravo da prisvoji protokolne podatke finskog *remailer*-a "Penet". Navodno se jedan "Penet"-ov korisnik negativno izrazio o sajentolozima, naravno sa njihove tačke gledišta, i preko *remailer*-a je slao poruke u *Usenet*. Ali, na ovaj način policija je dobila i identitete ostalih 700.000 korisnika "Penet"-a. Potom je vlasnik Johan Helsingius zatvorio svoj *remailer.*

Za zaista anonimne *remailer*-e postoje danas dva tehnička koncepta: oni koji koriste *Cypherpunk remailer* – koriste *PGP*, a *Mixmaster remailer* Lensa Kotrela (Lance Cottrel) koristi specijalno razvijen format za anonimizovanje. Sadržaji *e-mail*-ova se šifruju sa *triple-DES*. Paket *header* kao i *triple-DES* kod kôdiraju se *RSA* algoritmom.

U međuvremenu postoje *e-mail* klijenti ili *mixmaster frontends* za anonimno slanje *e-mail*-ova. Sa obe tehnologije rade "Private Idaho" (3) i "Jack B.Nymble" (4) na Windows-ima. Oba pretpostavljaju da je korisnik instalirao PGP, ali i na *World Wide Web*-u postoje neki *homepage*-ovi preko kojih se može direktno, uz pomoć *Cypherpunk*-a ili *Mixmaster*-a slati *e-mail*. Takav je, na primer, *remailer* projekat *Orange* (5). Pozitivno je ovde to što korisnik može sam da odredi preko kojih *remailer*-a će poslati svoj *e-mail*. Onda može i da proceni koliko vremena treba *e-mail*-u da stigne kod primaoca.

Safeweb

Software "Safeweb" (6) kôdira kompletan *web* saobraćaj i na taj način štiti ličnu razmenu podataka. Engleski guru za zaštitu podataka, Sajmon Dejvis (Simon Davies), je entuzijasta što se tiče *Safeweb*-a: "Ova vrsta besplatnog *software*-a, kao i *hushmail*

ili *Freedom* mreža poništiće sve napore vlasti". Treba napomenuti da saobraćaj ide samo preko računara *Safeweb*-a. Eksperti kritikuju da se na taj način nudi jedan jedini cilj u slučaju napada.

Neke vladine službe mogu da se sprijatelje sa ovakvim *software*-skim alatima. Pre svega špijuni su tradicionalno uvek cenili što veću anonimnost: u jesen 2000. godine je služba anonimiranja stupila u savez sa američkom tajnom službom CIA. Pre dve godine uprava je pokrenula svoj rizični kapital u *Q-tel* firmi, da bi pretražila ove službe za anonimizovanje. Sada hoće i CIA da koristi *Safeweb*, da bi mogla da prikrije sopstvene aktivnosti na internetu.

Za mnoge korisnike saradnja sa CIA-om nije baš potez koji uliva poverenje. Čak i 34-godišnjem šefu *Safeweb*-a Stivenu Hsu (Stephen Hsu) jasno je da će imati pad od 5% i to od najparanoidnijih korisnika, a doprinos *Safeweb*-a treba da se sastoji samo u tome da upravi obezbedi odgovarajući *software*.

Sama CIA nije imala pristup *web* kompjuterima firme ili načinu rada *software*-a. Tehnologija koja se koristi u *Safeweb*-u zove se *Triangle Boy*. Svaki PC računar s tim može da se pretvori u jednu vrstu *web* servera, tako da korisnici mogu da posećuju *web* stranice a da ne ostavljaju tragove. Zahtev za željenim *website*-om se prosleđuje na *website Safeweb*-a i onda se uspostavlja veza.

CIA je mogla da prikrije tragove ne samo u internet *surf*-ovanju, nego je mogla da uspostavi sigurne komunikacione veze za svoje ljude tako da su mogli bezbedno da komuniciraju sa CIA sedištem. *Safeweb* tehnologija je veoma zgodna i za neidentifikovano slanje poruka u druge države. Upravo ovu namenu je imao umu i Stiven Hsu kada je prošle godine kontaktirao CIA-u. Naravno, na ovaj način nisu slate samo propagandne poruke, nego su započeti i *cyber*-napadi, a da se ne otkrije odakle dolaze.

Moglo bi se sada spekulisati o tome da li je pravi interes CIA-e bio da se *crack*-uje *Triangle Boy* i da se kompromituje njegova upotreba u javnosti. Ipak ovakve tehnike kao i kriptografske metode otežavaju pravu delatnost tajnih službi: elektronsku proveru podataka. Međutim, bila bi dovoljna jedna presuda da se istražiteljima dozvoli pristup računarima koji vrše anonimizovanje. Naime, vlasnici tih računara vrlo verovatno mogu da dodele komunikaciji pojedinačnim korisnicima.

Anonymizer

Vrlo sličan *Safeweb*-u i veoma poznat je *Anonymizer*. Jednostavnim otvaranjem *website*-a u koji korisnik ubacuje jednu internet adresu, mogu da se anonimno koriste druge *web* stranice. *Anonymizer* radi kao običan *proxy* server. Ali odstranjuje sve lične informacije, kao i *cookie* ili IP adrese iz *header*-a *web*-upitnika (7). Ali, *Anonymizer* ne radi kao *Safeweb* sa više računara. Dovoljan je pristup na *Anonymizer*-ov računar da bi se došlo do korisnika. Ne postoji tehnička sigurnost. Korisnik mora verovati da *Anonymizer* neće sakupljati interesantne podatke. Napadač bi mogao da "presluša" komunikaciju između *Anonymizer*-ovog računara i korisnika i mogao bi čak da napravi analizu razmene podataka. Brzina konekcije je nešto sporija, ali kod brzih internet veza se to ne primeti.

Crowds

Ovaj projekat je prvi put predstavljen u leto 1997. godine. Suština ovog projekta je da se tragovi korisnika sakriju u *World Wide Web*-u. Tragovi pojedinca mešaju se s tragovima gomile korisnika: korisnik se pomeša u mnoštvo korisnika, a njegov prestup na neki *web* server dodeljuje se slučajnim odabirom nekog iz mnoštva, a ovaj onda može da prosledi pristup direktno na željeni server ili na nekog drugog slučajno izabranog iz mnoštva. Kada je pristup ostvaren, onda se prenosi preko slučajno izabranog člana iz mnoštva. Server polazi od toga da ima posla sa članom koji je želeo pristup. Navodno ni članovi mnoštva ne mogu da identifikuju onog koji je tražio pristup.

Eksperti kritikuju da član mnoštva može da se smatra kao pošiljalac, s druge strane taj isti član s dobrim razlogom može uvek to porekne (9). Napadači ne mogu da "prisluškuju" podatke, jer su pristupi kôdirani simetričnim kriptosistemom. Ako napadač pravi analizu razmene podataka, kôdirani podaci se mogu povezati i posmatrati. Bez obzira na pozitivan izveštaj američke štampe o projektu, on se nije pokazao uspešnim. Do početka 2000. godine retko se koristi. Američke kripto-eksportne kontrole (10) sprečavale su da se može u potpunosti koristiti i u Evropi. Ali i onda je bilo problema da se *Crowds* izvozi. Do danas nije dobilo značajnu podršku.

Kod *Crowds*-a se pristup kanališe preko više računara – i u tome je njegova prednost. Na taj način *Crowds* preuzima recept uspeha samog interneta: pre samo nekoliko godina su mnogi smatrali da internet ne može da se cenzuriše. Konačno, tako je i bio organizovan – decentralizovano, tako da bi mogla opstati komunikacija između različitih tačaka i u slučaju nuklearnog rata. Ali, ako je unifikacija unutar jednog pravnog sistema, znači jedne države, i ide samo preko jednog centralnog čvorišta, onda može da se kontroliše. U međuvremenu se javlja više pokušaja da se stvori necenzurisana mreža, u kojoj bi se podaci mogli ekontrolisano razmenjivati. Što su sistemi decentralizovaniji, to su otporniji na pokušaje manipulacije.

Napster

Napster je najpoznatija berza za razmenu na internetu. Omogućava korisnicima brzo i jednostavnu razmenu muzičkih *file*-ova (pesama) na internetu. Da li su među tim *file*-ovima i muzička dela koja podležu pod zaštitu autorskih prava - to pre preuzimanja od strane Bertelsmana (Bertelsmann) nije provereno. Sistem je stvoren za fer upotrebu (fair use) i ne koristi nikakve kôdove. Pošto je Bertelsman blokirao nelicencirane i pesme sa zaštićenim autorskim pravima, pao je broj korisnika sa 15,5 na 12,1 miliona, znači za 3 miliona manje. Istraživanje je izveo *Jupiter Media Metrix* i to na korisnicima koji su *Napster* klijentom razmenjivali pesme.

Gnutella

Gnutella je malo teža za rukovanje od *Napster*-a, jer radi decentralizovanije nego *Napster*. Kod *Gnutella*-e je reč o *Open-Source-Software*-u za razmenu podataka. To se dešava u jednoj mreži

računara koji međusobom razmenjuju razne pretrage. Kada korisnik pokrene pretragu, ona se sprovodi dalje na sve priključene računare. Zahtevi i odgovori idu preko više računara i ne mogu se dodeliti nekoj određenoj IP adresi. Odgovori ipak sadrže IP adrese ponuđača podataka, što je preko provajdera vidljivo. Znači, anonimna razmena preko *Gnutella*-e nije moguća. Za *Gnutella*-u postoji više programa za primenu, takozvani klijenti. Tu spada *Gnutella* ili *Toadnode* za Windows, *Mactella* za Mac, *MyGnut* za BeOs, *Hagelslag* za Unix ili *Java client furi*.

Onion Routing

Po mišljenju izuzetno kritički raspoloženog profesora informatike iz Drezdena – Andreasa Ficmana (Andreas Pfitzman), *Onion Routing* (11) je jedini prihvatljivi koncept za anonimno *surf*-ovanje. Može da se koristi kao *Napster* ili *Gnutella* za prenos podataka, daljinskog logovanja i druge svrhe spajanja i razmene podataka. Kod *Onion Routing*-a podaci se mogu uglavnom anonimno razmeniti. Više računara je zaduženo za anonimizovanje. Komunikacija je kôdirana. Analiza razmene podataka je takođe ograničena. Ali, primaocu poruke je poznata adresa pošiljaoca. Sve u svemu, *Crowds* štiti od jačih napadača nego *Anonymizer*, a *Onion Routing* nudi još jaču zaštitu od *Crowds*-a.

Istraživački projekat je sponzorisan od strane ministarstva odbrane SAD i istraživačke grupe DARPA (12) takođe iz SAD. Prototip je dokazao da koncept funkcioniše. U fazi testiranja, mreža je bila ostvarena u proseku sa 50.000 poseta dnevno. Do početka 2000. godine nije bio dozvoljen izvoz *software*-a iz SAD koji sadrži kriptografske elemente. Od 28.01.2000. godine, prototip je *offline* i čeka na primenu. U inostranstvo, pak, ne treba da se izvozi zbog vojnog porekla. A ipak je Ulf Moler (Ulf Möller) na univerzitetu u Hamburgu iskopirao prototip.

Kod *Onion Routing*-a, *browser* pravi konekciju sa prvim *Onion Routing proxy* serverom. Onda taj (proxy server) pravi anonimnu rutu, tj. konekciju kroz različite *Onion Router*-e sve do željenog servera. A pri svemu tome samo jedan *Onion Router* zna put do sledećeg servera. Pre nego što se podaci pošalju, oni se višestruko kôdiraju. Kôdiranje se sprovodi u slojevima oko podataka, pri tom svaki sloj sadrži adresu sledećeg *Onion Router*-a. Ovi slojevi su dali i ime projektu, jer koncept kodiranja liči na luk (13).

Zaštitu od posmatranja pruža takozvani *Dummy traffic* ili prazan saobraćaj koji se obavlja između *Onion Router*-a. Ako se ovaj sistem malo koristi, onda ne pruža odgovarajuću zaštitu, jer tada mogu da se povežu krajevi komunikacionih kanala, preko razmenjene količine podataka.

AN.ON

Do sada predstavljene mogućnosti anonimnog surfovanja nisu zapravo zadovoljavajuće. Savezno ministarstvo (SR Nemačke) za privredu zahteva zbog toga razvoj službe za anonimnost. Projekat "AN.ON anonimnost u internetu" koji sprovode tehnički univerzitet iz Drezdena i nezavisni centar za zaštitu podataka iz Šlesvig Holštajna (Schleswig-Holstein), treba da razvije jednu uslugu preko koje bi bila kodirana internet komunikacija. A osnova

bi bila mnoga nezavisna čvorišta, takozvani *Mix proxy*, i ne samo tajne službe, već i sami *provider*-i ne bi mogli saznati ko i šta radi na internetu.

Svaki korisnik može samostalno da pokreće jedan *Mix proxy,* ako poseduje odgovarajuće široku internet konekciju. *Software* koji je razvijen u projektu treba u budućnosti da bude besplatno dostupan kao *Open-Source*, dakle krajnje pristupačan. Ministarstvo privrede želi pre svega da otkloni dosadašnje prekpreke za *e-commerc*. Glavna prepreka je to što korisnici nemaju poverenja u mrežu.

Korisnici bi trebalo da budu sigurni da pri *on-line* kupovini neće iza sebe ostaviti debeli informacioni trag. Nije ni čudo: porast trgovine preko interneta daleko je manji od onog što očekuje privreda. Po analizama ispitivača tržišta, odlučujući razlog leži u zabrinutosti korisnika u vezi sa sigurnošću poslovanja na internetu.

Gostujući profesor informatike na slobodnom univerzitetu (Freien Universität) u Berlinu, Hens Federat (Hannes Federath), ima plastičan primer za to: "Zamislite da slučajno tražite medicinske informacije na internetu, jer neki vaši prijatelji pate od jedne teške bolesti. Istovremeno se informišete na nekom *website*-u nekog osiguravajućeg društva o najpovoljnijoj polisi životnog osiguranja. Obe stvari daju jedan profil, koji će biti procenjen i biće prodat zainteresovanim stranama i možda će vam onda biti ponuđena nepovoljnija polisa životnog osiguranja." (14)

Program *Java Anon Proxy* (JAP) (15) već sada je dostupan besplatno, njega je u okviru projekta *AN.ON* razvio profesor Federat. JAP radi kao virtuelna mimikrija: komunikacioni podaci ne idu direktno na *web* server, nego preko takozvane *Mix proxy* kaskade. A pri tome se konekcija korisnika skriva među ostalim JAP korisnicima. Konekcija se može povezati sa jednim određenim korisnikom. Svaki korisnik bi mogao da bude onaj koji je pokrenuo konekciju. Na *website*-u piše: "Niko, ni neko ko stoji sa strane, ni koji drugi korisnik, čak ni onaj koji vrši uslugu anonimizovanja ne može razaznati koje konekcije upotrebljavaju određeni korisnici."

Po pravilu u jednoj kaskadi rade najmanje tri *Mix proxy*-a kojima upravljaju nezavisne institucije. Oni izjavljuju i obavezuju se da neće memorisati *log-file*-ove niti da će sa drugim koji rade sa *Mix proxy*-jima razmenjivati podatke koji bi mogli dovesti do toga da se može identifikovati određeni korisnik. Nezavisni kontrolni punktovi treba da garantuju da se prethodno preuzete obaveze i izjave poštuju. Najidealnije bi bilo, kako kaže Andreas Ficman, kada bi katolička crkva imala jedan *proxy*, politička partija drugi, univerzitet treći i robna kuća četvrti *proxy* – čak i *proxy* u inostranstvu bi doprineli većoj bezbednosti, jer korisnika je moguće identifikovati jedino kada bi svi koji upravljaju dozvolili prilaz *proxy*-u.

FREENET

Freenet je još radikalniji od AN.ON. On uspostavlja paraleleni internet koji je otporan na cenzuru, anoniman je i omogućava efikasno objavljivanje i povlačenje informacija. Cilj je potpuno otklanjanje autorskih prava i slobodan pristup svim informacijama, i to za svakoga. 400 osoba sada rade (muškarci i žene za razvoj software-a) pod vođstvom škotskog studenta Jana Klarka (Ian Clark) na razvoju prototipa. Na potpuno decentralizovanoj mreži

ne sme više biti centralnih kontrolnih čvorišta. To nije baš jednostavno. Klark i njegov tim imaju problema sa skaliranjem, efikasnošću i raspodelom opterećenja mreže i sa time se bore. Sistem će biti implementiran u *Java*-u, da bi se dobila platformska nezavisnost.

Već sada simulacije pokazuju da je mreža relativno stabilna: čak do 20 čvorišta mogu ciljano da se zatvore i 30% može slučajno da ispadne a da mreža ne pukne. Korisnici se mogu osloniti na autentičnost primljenih podataka i sadržaj jedne datoteke je vezan preko jednog konkretnog zbira sa njihovim imenom. Iako se podaci još ne mogu ciljano tražiti.

Peekabooty

Projekat koji mnogo obećava a nije na nivou mreže nego na nivou (korisnika) klijenta: U proleće 2001. godine, američka *hacker*-ska grupa "Cult of the Dead Cow" (CDC) najavila je objavljivanje sopstvenog *browser*-a po imenu *Peekabooty*. Žele da ga predstave na *hacker*-skom kongresu *DetCom* u junu 2001. godine.

Peekabooty ne da će kôdirati kompletan protok informacija između servera i *browser*-a, nego će raspodeljenim računanjem sprečiti identifikaciju korisnika. Korisnici mogu da kontaktiraju sa drugim *Peekabooty* korisnicima i na taj način treba da nastane posebna komunikaciona mreža. Unutar te mreže komunikacija je kôdirana – korisnici *Peekabooty*-a mogu sigurno da šalju čak i *e-mail*-ove. *Peekabooty* korisnici bi na ovaj način mogli da savladaju čak i *firewall*-ove.

Peekabooty korisnici mogu i da traže informacije. Korisnik iz Kine bi uz pomoć ovog *browser*-a mogao da dođe do internet informacija koje je kineska vlada cenzurisala. Jedan računar izvan Kine bio bi "prolaz": odavde bi mogli da se kôdiraju zahtevani podaci i šalju dalje kineskom disidentu.

"Cult of the Dead Cow" postali su poznati kada su razvili alate za skoro neograničen prilaz tuđim Microsoft računarima: "Back Orifice" i "Back Orifice 2000". Danas te programe koriste sistem adimistratori kao alat za daljinsko opsluživanje, a koriste ga i *hacker*-i.

Literatura

(1) Program je pristupačan bez plaćanja licence za privatno korišćenje i može se skinuti preko PGP-Server ftp://ftp.de.pgpi.com/pub/pgp ili preko Network Associates, Inc. (http://www.pgpinternational.com)

(2) http://www.iks-jena.de/mitarb/lutz/anon/as-node.html

(3) http://www.itech.net.au/pi/, Download sa Private Idaho

(4) http://www.skuz.net/potatoware/index.html, Download-site za -Potato¬(DOS), "Jack B. Nymble" (Windows) i -Reliable- (Remailer-Server za Windows)

(5) http://www.remailer.cjb.net, Homepage Orange-Projekata

(6) http://www.safeweb.com, Homepage za Safeweb

(7) engl. header

(8) engl. crowd

(9) Hannes Federrath, Kai Martius, Anonymitat und Authentizitat u World Wide Web, TU Dresden, http://www.int.tu-dresden.de/-hf2/publ/1998/FeMal98itg/

(10) Na osnovu Wassenaar-dogovora od decembra 1998. godine više ne postoje eksportne kontrole za 64-bitne proizvode za masovno tržište, ni za 512-bitne proizvode za upravljanje šifrovanjem. Iz: Christiane Schulzki-Haddouti, Kontrollierte Liberalisie¬rung, telepolis, 13.1.2000, http://www.heise.de/tp/deutsch/inhalt/te/5683/l.htm

(11) http://www.onion-router.neU, Homepage Onion Routing-a

(12) Defense Advanced Research Projects Agency (DARPA)

(13) engl. onion

(14) Nenadzirano surfovanje. Razgovor s Hanesom Federatom, čovekom koji je razvio Java Anon Proxi. Burkhard Schroder in telepolis, 11.4.2001, http://www.heise.de/tp/deutsch/inhalt/te/7347/l.html

(15) http://anon.int.tu-dresden.de/

(16) http://freenet.sourceforge.net, Homepage Freenet-a, "The Free Network Project"

(17) http://www.sanity.uklinux.net, Homepage Ian Clark-a

(18) Frank Patalong, "PeekaBooty"; Jetzt kommt der Hacker-Browser, Spiegel Online, 8.5.2001, http://www.spiegel.de/druckversion/0,1588,132661,00.html

Kristijana Šulcki-Haduti (Christiane Schulzki-Haddouti) je novinarka i od 1996. godine korespondentkinja *Telepolis*-a. Priredila za štampu "O kraju anonimnosti. Globalizacija nadziranja", kod *Heise Verlag*-a.

Centar za nove medije_kuda.org
www.kuda.org

Centar za nove medije_kuda.org je organizacija koja okuplja umetnike, teoretičare, medijske aktiviste, istraživače i široku publiku na polju informacijskih i komunikacijskih tehnologija (ICT - Information and Communication Technologies). U tom smislu, kuda.org je posvećen istraživanju novih kulturnih odnosa, savremene umetničke prakse i društvenih tema.

Aktivnost rada kuda.org je posvećena pitanjima uticaja elektronskih medija na društvo, na kreativnu upotrebu novih komunikacijskih tehnologija i na savremenu kulturnu i društvenu politiku. Neke od glavnih tema su interpretacije i analize istorije i značaja informacijskog društva, potencijala same informacije i rasprostranjenosti njenog uticaja na političke, ekonomske i kulturne odnose u savremenom društvu. Centar za nove medije kuda.org otvara prostor za kulturu dijaloga, alternativne metode obrazovanja i istraživanja. Društvena pitanja, medijska kultura, nove tehnologije umetnost, princip slobodnog softvera i softvera otvorenog kôda su oblasti kojima se kuda.org bavi.

Programi kuda.org:

kuda.info / infocentar
pruža informacije iz oblasti kulture novih medija, savremene umetnosti i društvenih fenomena; omogućava istraživanja i edukaciju preko biblioteke, medijateke i arhive iz ove oblasti.

kuda.lounge / prezentacije i predavanja
sastoji se od predavanja, razgovora, javnih prezentacija umetnika, medijskih aktivista, teoretičara umetnosti, naučnika, istraživača i inžinjera; (izložbe, prezentacije, tribine, simpozijumi, predavanja su mesto aktivnog dijaloga i interakcije, koja doprinosi stvaranju novog kvalitetnog jezgra na obe strane: kod publike i predavača).

kuda.production / produkcija i izdavaštvo
obezbeđuje uslove za neprofitno umetničko stvaralaštvo na polju novih medija i tehnologija; kuda.org kao producent, koproducent pruža uslove za interdisciplinarna istraživanja i eksperiment.

Telepolis, Magazin der Netzkultur
www.telepolis.de

Telepolis je nemački internet magazin, koji počev od 1996. godine objavljuje izdavačka kuća *Heinz Heise Verlag*. Magazin su osnovali novinar Armin Medoš i Florijan Recer i obrađuje teme koje se tiču privatnosti, nauke, kulture, politike interneta i generalno, politike i medija. *Telepolis* je 2000. godine primio nagradu "Evropska nagrada za online novinarstvo" za "istraživačko novinarstvo" za izveštavanje o projektu *Echelon*. Godine 2001., *Telepolis* je primio "Online Grimme prize". Izdanje "Netzpiraten" je jedno iz serije publikacija koje je inicirao *Telepolis* i objavio *Heinz Heise Verlag*, a koja se bave pitanjima internet politike, bezbednosti podataka, kritike kulture, politike i medija.

CIP – Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

004.738.5:316(082)
004.738.5(082)

Pirati na mreži : kultura elektronskog kriminala /
[prevod sa nemačkog Relja Dražić, Dragan Prole, Rade Pujin].
– Novi Sad : Futura publikacije, 2008 (Novi Sad : Daniel
print). – 133 str. ; 20 cm. – (Edicija: kuda.read)
Prevod dela: Netzpiraten. - Str. 5-6: Predgovor / Armin Medoš i Janko Retgers. - Bibliografija.

ISBN 978-86-7188-101-2

a) Интернет – Социолошки аспект – Зборници b) Интернет –
Злоупотреба - Зборници

COBISS.SR-ID 233079559