Pravni vidiki in praktični primeri kiberkriminala

Matej Kovačič
Fakulteta za družbene vede, Univerza v Ljubljani

Kiberkriminalci

Kiberkriminal

- 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.
  - Primer vdora v T-Mobile, kjer je napadalec pridobil dostop do podatkov o 16,3 mio. strankah.

“Hekanje”

- 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); najbolj pogosto pa se ga dojema kot sofisticirano ilegalno dejavnost.

“Kiberkriminalci” - prva delitev

- 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;

“Kiberkriminalci” - prva delitev

- 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.).

“Kiberkriminalci” - druga delitev

- 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.

“Kiberkriminalci” - druga delitev

- Tretjo generacijo označujejo vodilni razvijalci računalniških iger.
- Četrto pa osebe, ki na nedovoljene načine vstopajo v tuje računalnike.

- 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.

“Heker”

- Izraz “heker” (ang. *hacker*) je prvi uporabil Joseph Weizenbaum leta 1976.
- Popularno 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.

“Heker”

- Po samodefiniciji 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*”.

“Heker”

- Eden izmed slovenskih hekerjev, 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...*”.

“Heker”

- Bruce Schneier hekanje razume kot stanje duha, pri čemer 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. ...*”

“Heker”

- “*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).

“White hat” vs. “Black hat”

- 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.
- “Črni hekerji”, včasih jih označujejo tudi z izrazom kreker (ang. *cracker*), pa so osebe, ki hekersko znanje zlorabljajo za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter povzročanje škode.

“Cracker”

- Izraz kreker (ang. *cracker*) se sicer uporablja tudi za posameznike, ki se ukvarjajo s tim. reverznim inženiringom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem.

“Script kiddie”

- Skriptarji (ang. *script kiddies*) 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 poskušajo vdreti.
- Motivi so večinoma samodokazovanje, zabava ali vandalizem.

“Script kiddie” vs. “heker”

- Eden izmed slovenskih hekerjev je skriptarje opisal takole: “*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*”.
- Izjava 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*.”.

Kriminal ali radovednost?

- "*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.*"
- "*Da, kriminalec sem. 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.*"

-- "*The Mentor*", član hekerske skupine *Legion of Doom*

Škodljiva in koristna uporaba znanja

- "*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, potem jih je pa nadomestil z svojim programom napisanim v delphiju. ddosnet je bil majhen, kake 70 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 1000 EUR.*"

Klasifikacija napadov

Nekatera kiberkriminalna dejanja

- Pošiljanje nezaželene elektronske pošte
- Razobličenja spletnih strani
  - XSS napadi
- Internetne goljufije in prevare
- Zlonamerno (vohunsko) programje
- Prikrita omrežja in napadi s poplavljanjem
- Vdor v informacijski sistem
- Prestrezanje
  - Napad s posrednikom (MITM napad)
  - Prestrezanje v brezžičnih omrežjih in kraja dostopa do interneta
  - Tajnost e-pošte, prestrezanje komunikacij zaposlenih in zasebnost na delovnem mestu

Pošiljanje nezaželene elektronske pošte

- Ni kaznivo dejanje, pač pa prekršek, ki ga obravnavajo naslednji zakoni:
  - *Zakon o varstvu potrošnikov*,
  - *Zakon o elektronskih komunikacijah*,
  - *Zakon o varstvu osebnih podatkov*,
  - *Zakon o elektronskem poslovanju na trgu*.
- Lahko vodi do kaznivega dejanja:
  - pošiljanje virusov,
  - poskusi prodaje lažnih ali goljufivih izdelkov (npr. ponarejenih zdravil),
  - poskusi prevare z namenom zbiranja osebnih podatkov ali dostopnih gesel.

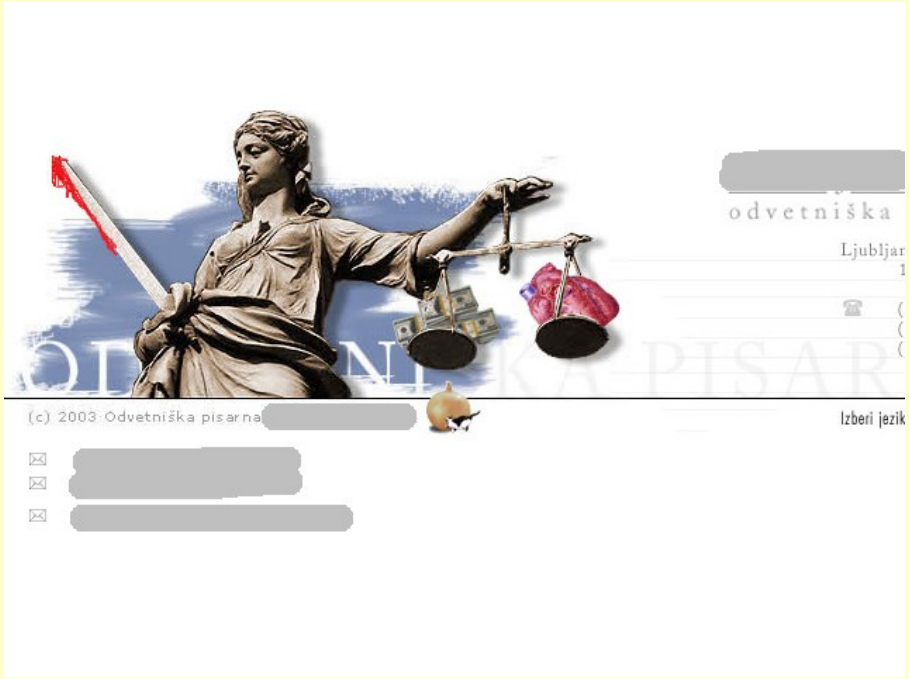
Razobličenja spletnih strani

- Razobličenje (ang. *defacement*): napadalec spremeni vsebino spletne strani.
  - novodobne oblike vandalizma oz. pisanja grafitov,
  - politični motivi,
  - maščevanje ali škodovanje "konkurenci",
  - poskusi goljufije!
- Motivi: samodokazovanje in dolgočasje, iskanje medijske pozornosti in tekmovanje med razobličevalskimi skupinami, pridobitni motivi.
- Praviloma je razobličenje posledica vdora **in** spremembe informacijskega sistema.

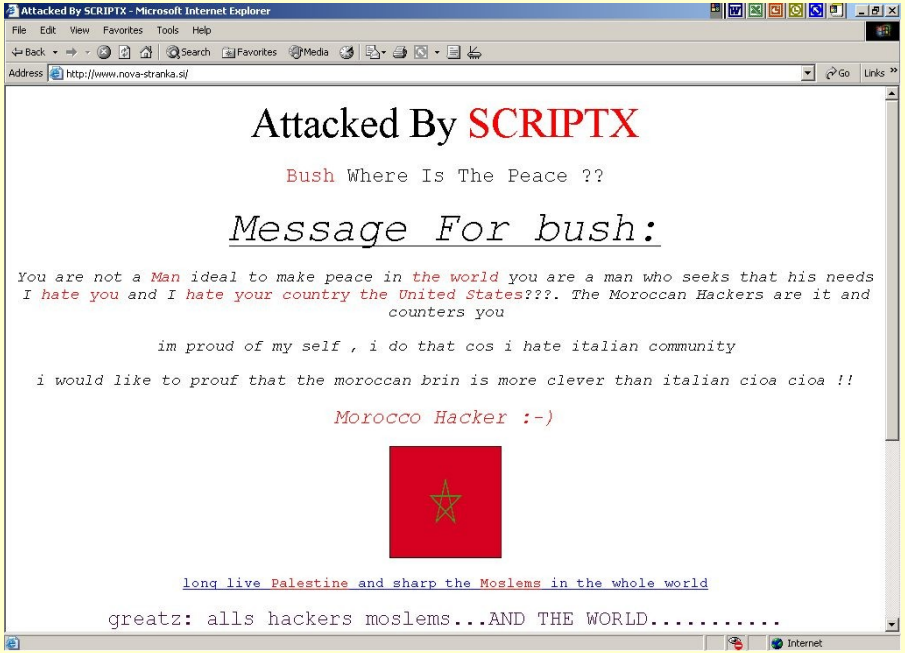
Razobličenja spletnih strani (z XSS napadom)

- XSS napad (*Cross-site Scripting*): navzkrižno izvajanje skriptov na spletnih straneh.
- Gre za tehniko, ki se izvaja v uporabnikovem spletnem brskalniku in ne na strežniku.
- Ni vdora v informacijski sistem, le sprememba prikaza spletne strani **pri uporabniku**.

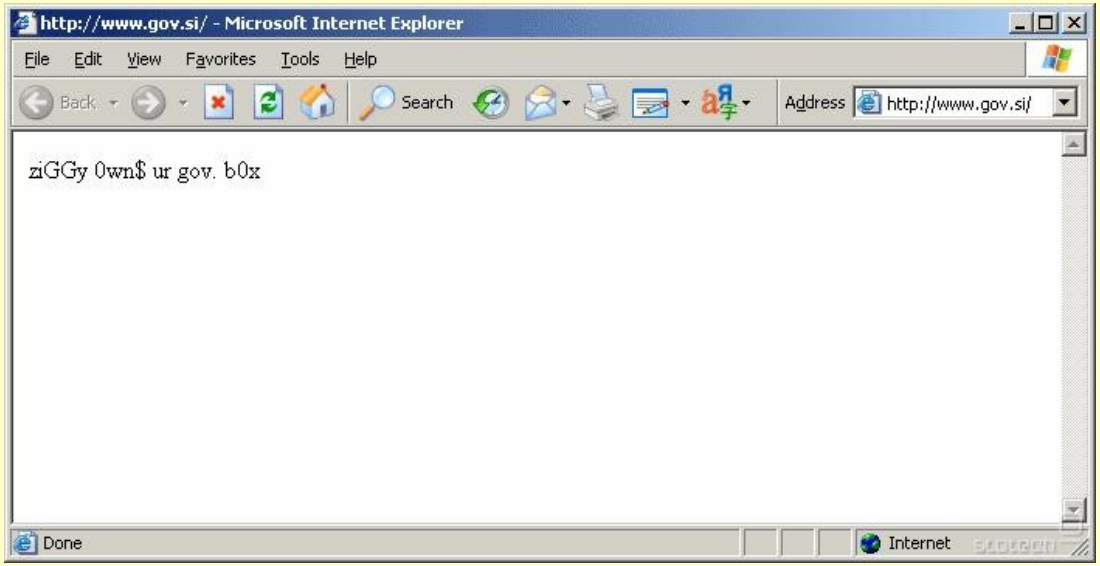
Primeri...



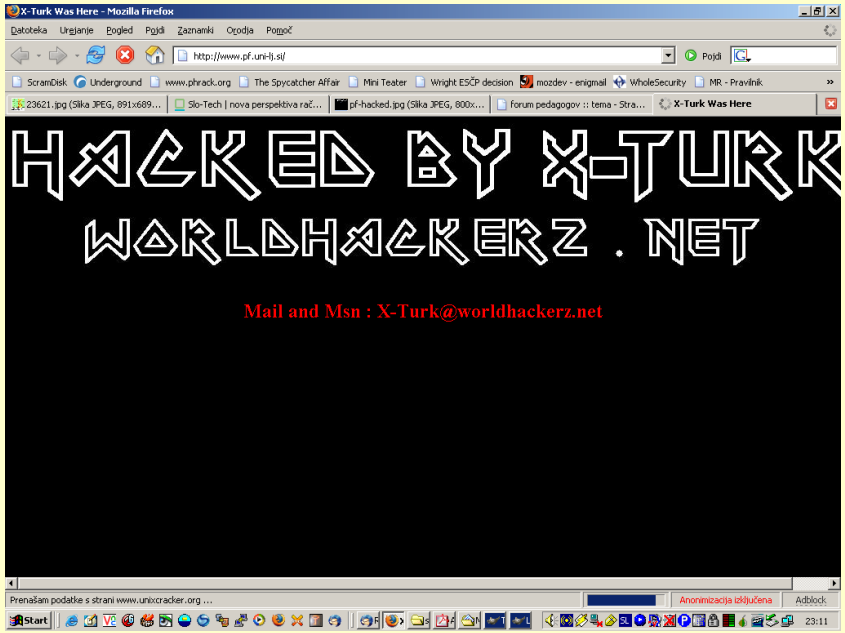
Razobličena spletna stran odvetniške pisarne.



Razobličenje spletne strani politične stranke.

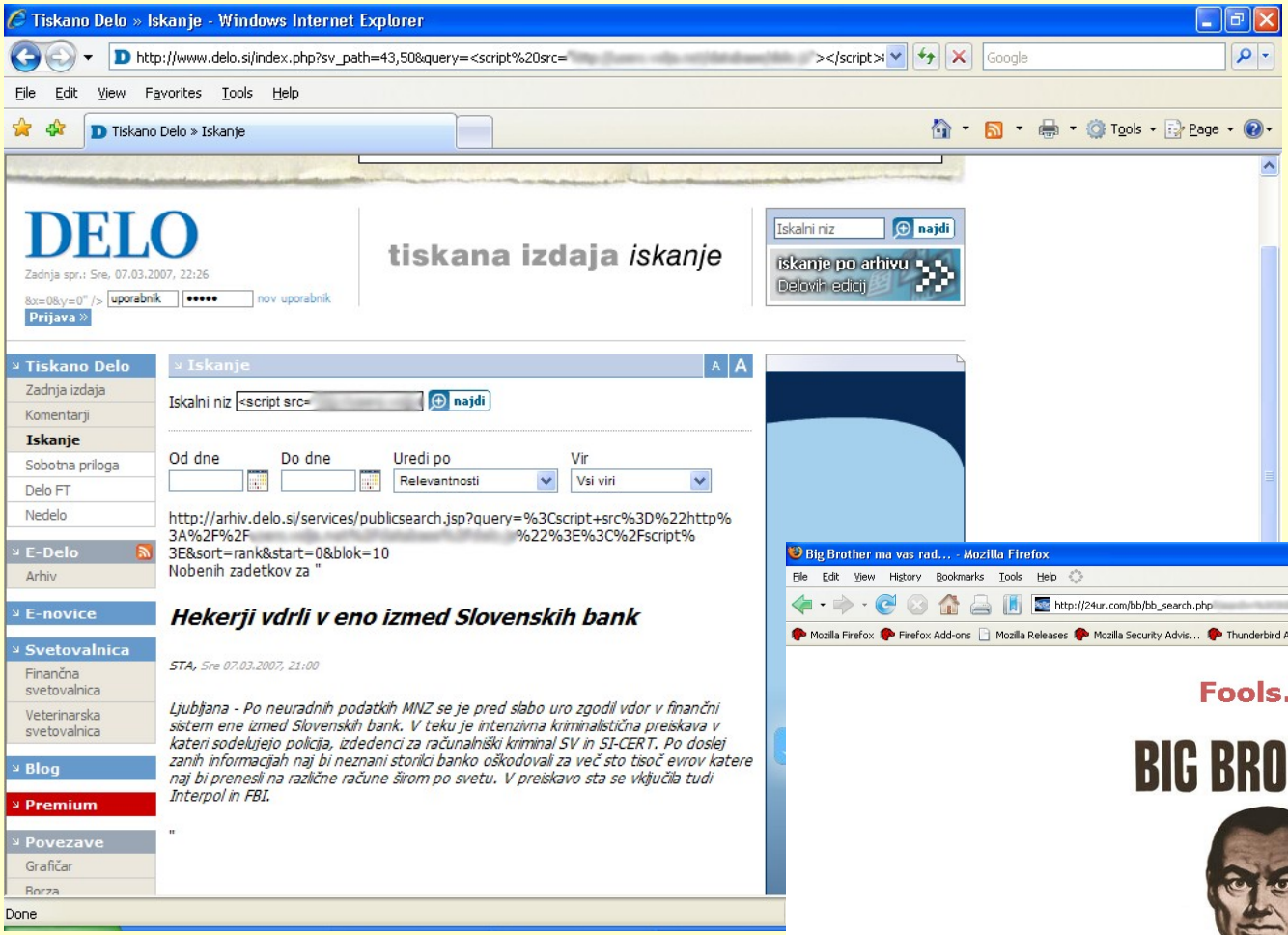


Razobličenje vladne strani (gov.si).



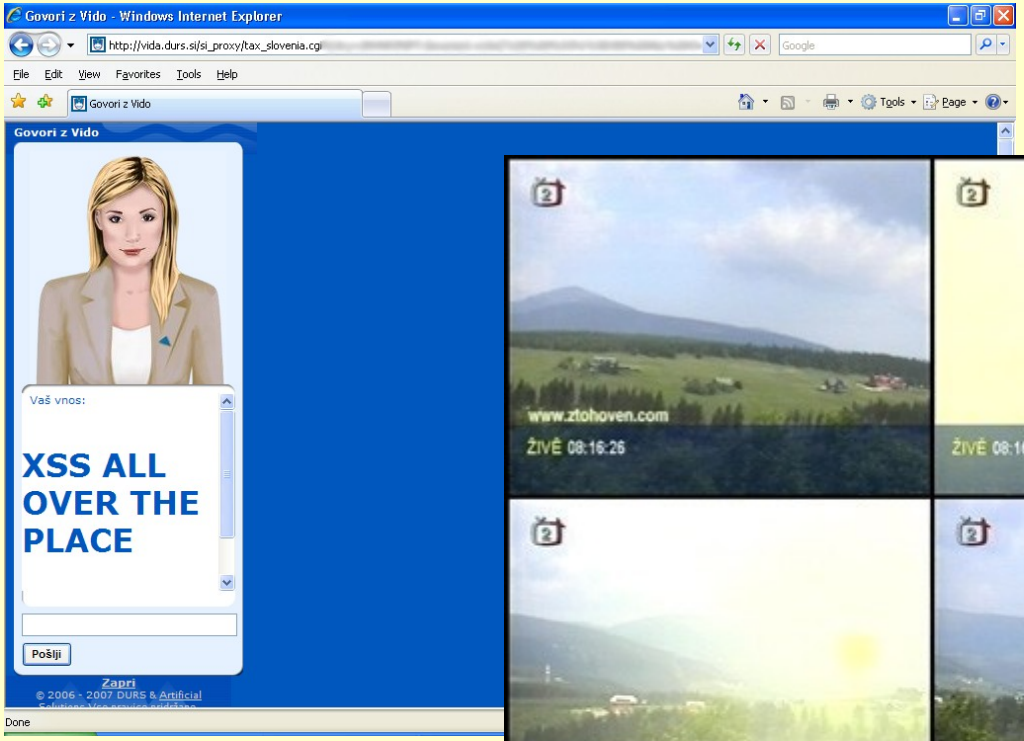
Pravna fakulteta, Univerza v Ljubljani (razobličenje).

Razobličenje spletne strani rimokatoliške cerkve.



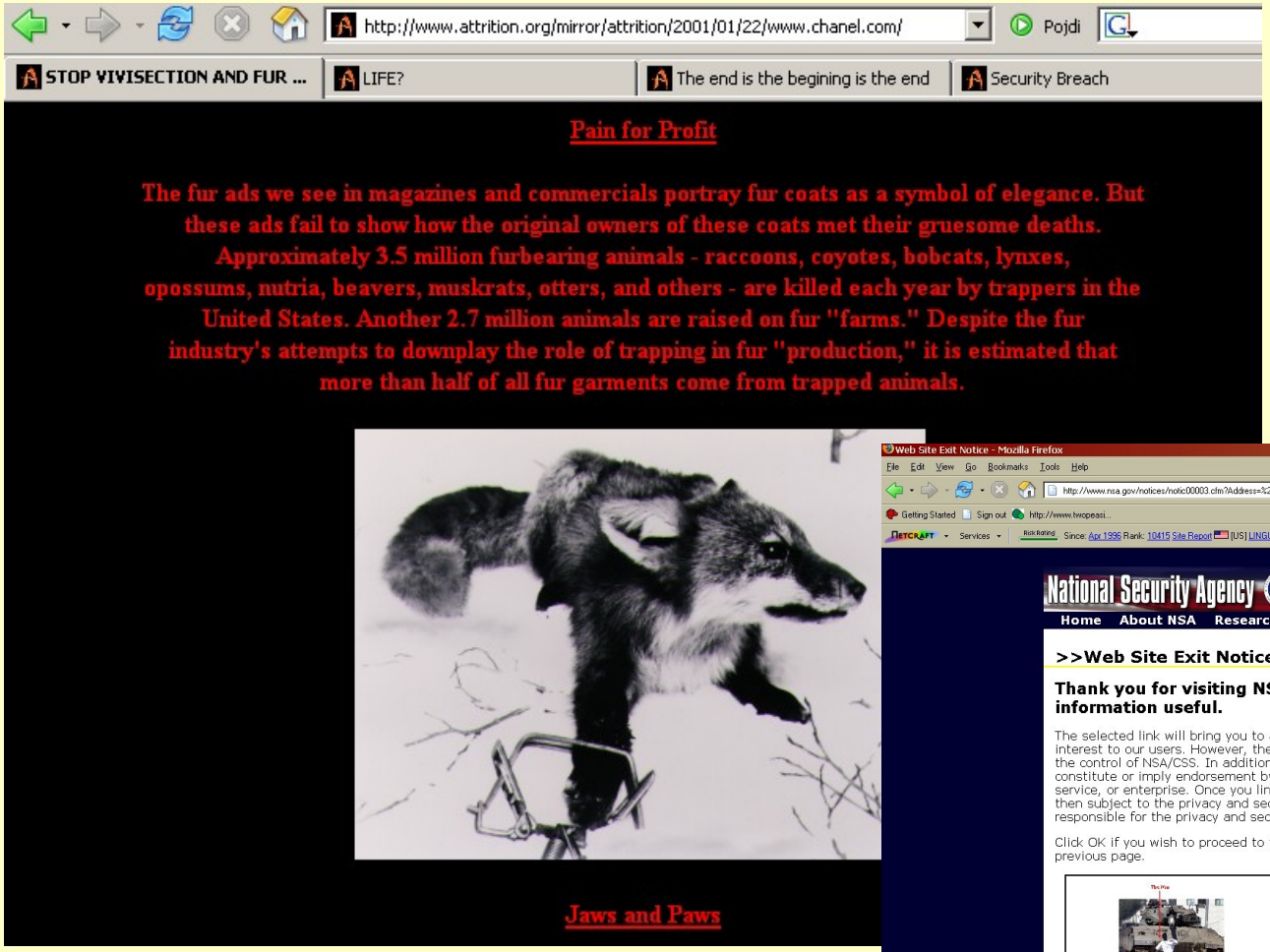
Lažna novica na spletni strani časnika DELO (XSS napad).

"Big Brother" na 24ur.com (XSS napad).



XSS napad na "davčno Vido".

Lažna jedrska eksplozija vrinjena v živi video prenos na eni izmed čeških TV postaj leta 2006.
[prikaz videoposnetka]



Razobličenje spletne strani modne hiše Chanell.com

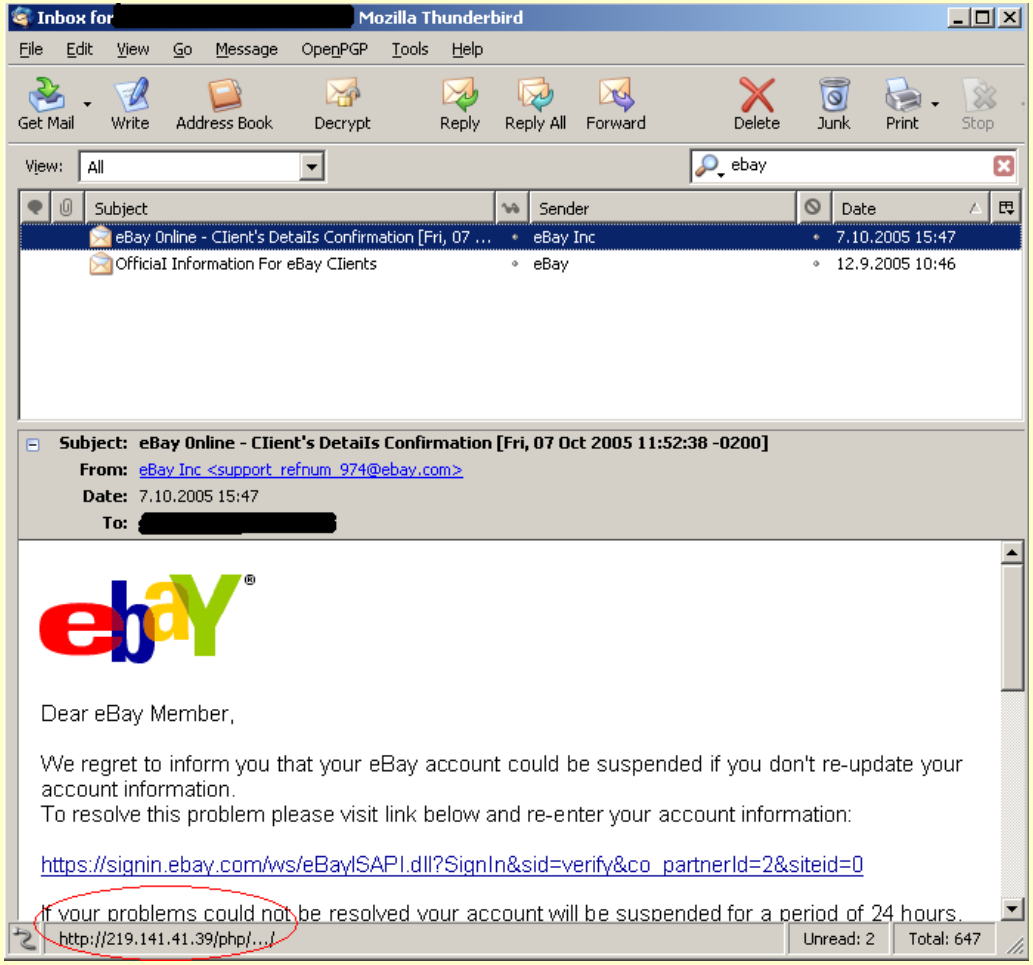
[prikaz XSS napada v živo]

XSS napad na spletno stran ameriške tajne službe National Security Agency.

Internetne goljufije in prevare

- Socialni inženiring (ang. *social engineering*);
- ribarjenje (ang. *phishing*);
- pharming napad (napadalec pomočjo DNS preusmeritev uporabnike usmerja na lažne spletne strani);
- scam 419 (nigerijska prevara).

[slike iz zabave Klik team]



Primer ribarjenja (phisinga) preko neželene e-pošte.

Zlonamerno (vohunsko) programje

- "*Spyware*" (programska oprema namenjena zbiranju podatkov o uporabniku), "*adware*" (programska oprema namenjena prikazovanju oglasov), "*malware*" (zlonamerna programska oprema namenjena izključno nezakonitim dejavnostim).
  - Primer: klicalniki (ang. *dialer*), zamenjajo telefonsko številko ponudnika dostopa do interneta v uporabnikovih nastavitvah omrežja na klic;
  - korenski kompleti (ang. *rootkit*), so namenjeni prevzemu popolnega nadzora nad računalnikom in skrivanju napadalca v sistemu.

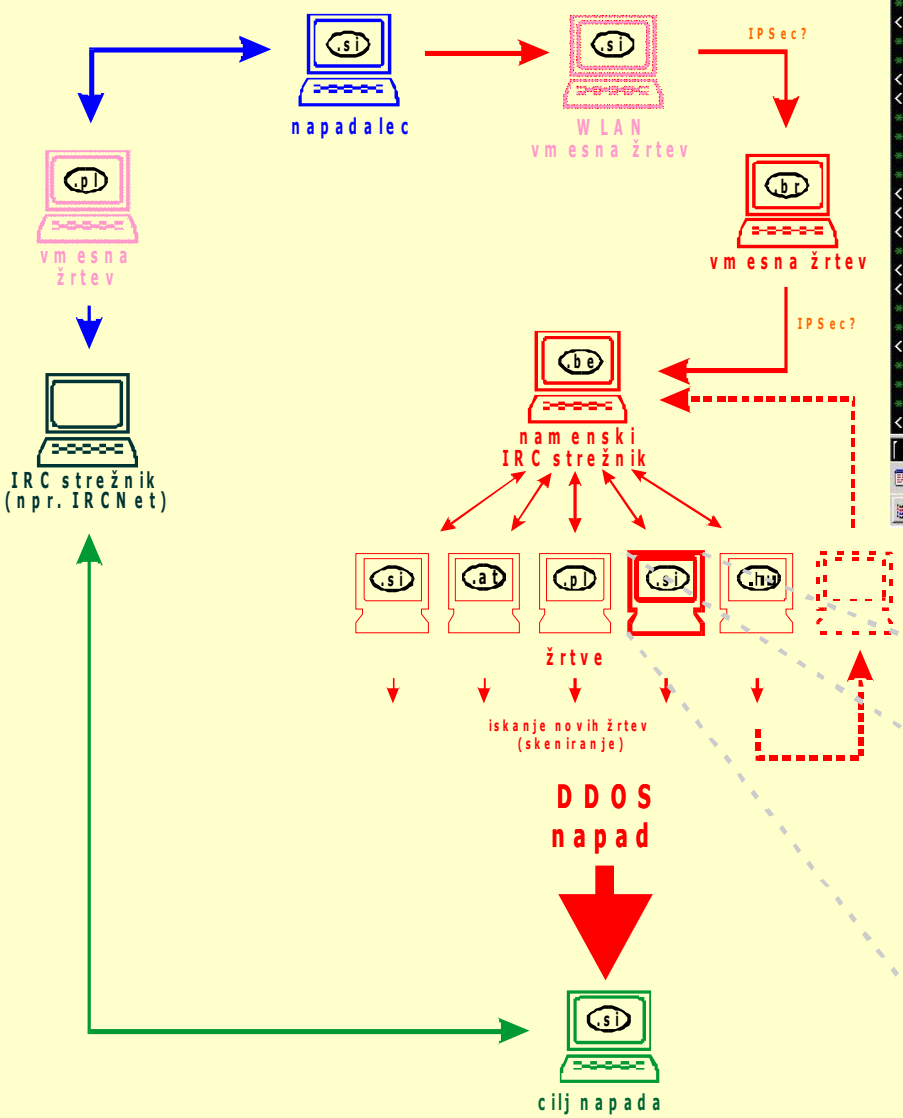
Prikrita omrežja in napadi s poplavljanjem

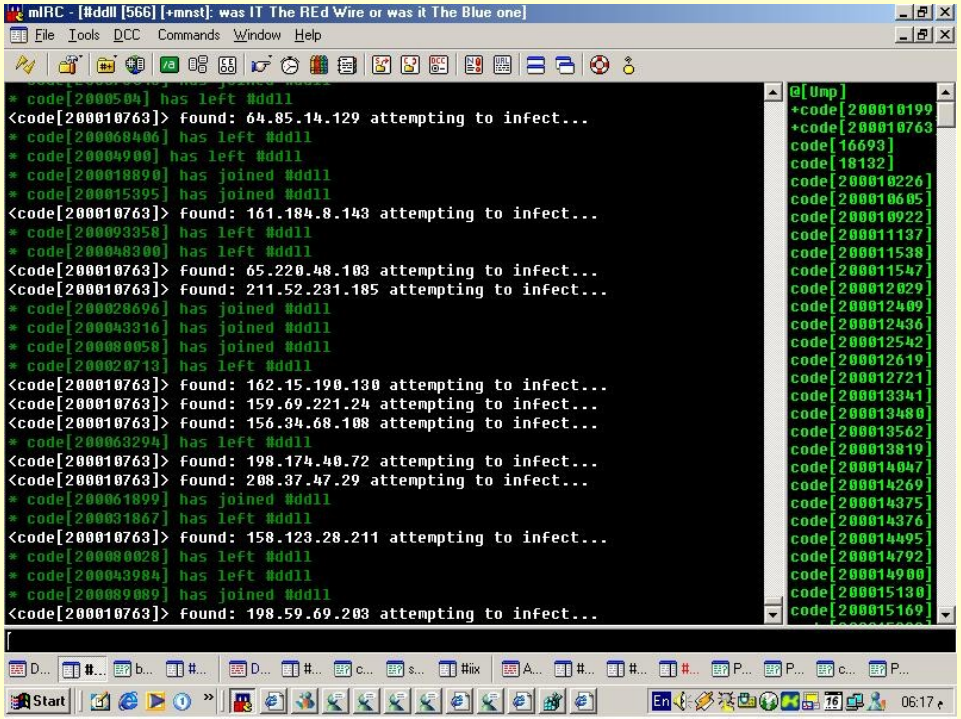
- Napadi s poplavljanjem so napadi na razpoložljivost sistema oziroma oviranje njegovega delovanja:
  - DOS (ang. *Denial Of Service*) napadi
  - DDOS (ang. *Distributed Denial Of Service*) napadi
- Prikrito omrežje (*botnet* - izraz izvira iz besed 'ro**bot**' ter '**net**work').
- Ka začetku se uporabljajo večinoma zgolj za izvajanje napadov s poplavljanjem v času tim. IRC vojn.
- Kasneje čedalje bolj prihaja do zlorabe v kiberkriminalne namene:
  - skrivanje spletnih strežnikov (*invisible bulletproof hosting*),

Prikrita omrežja in napadi s poplavljanjem

  - pošiljanje nezaželene elektronske pošte,
  - kraja osebnih podatkov in podatkov za elektronsko bančništvo, itd.
- JavaScript ugrabljanje oz. spletni virusi (Jitko).
- Prikrita omrežja nove generacije (*Storm*, *Gozi*, *Nugache*,...):
  - za komuniciranje uporabljajo P2P princip (ni enega Command&Control centra);
  - točke v omrežju med seboj komunicirajo po šifriranih kanalih;
  - programska koda uporablja različne načine prikrivanja (mutatorji programske kode, stiskanje in šifriranje kode);
  - *Nugache*: prva povezava v internet šele po mesecu dni.

Shema prikritega omrežja:

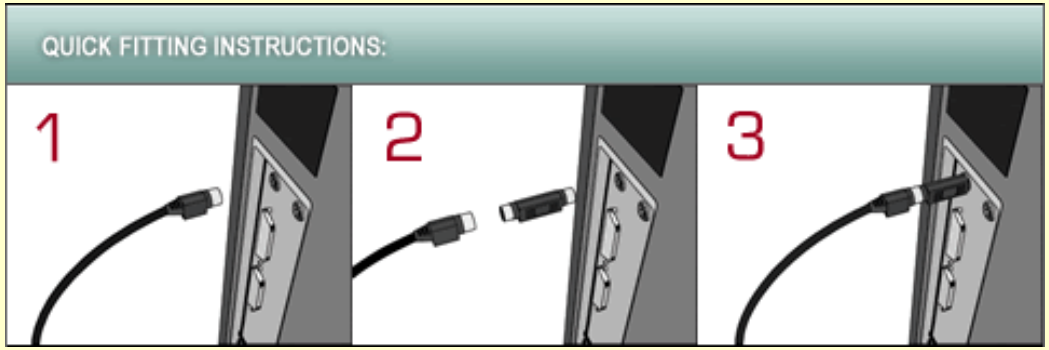




Pogled na prikrito omrežje s strani napadalca.

Vdor v informacijski sistem

- Fizični dostop (kraja, izguba, nepooblaščen dostop do prostorov, kjer se nahaja računalniška oprema, podtikanje strojnih in programskih dodatkov).
- Problem razmejitve med javnim in zasebnim prostorom na internetu.
  - Google hacking (iskanje javno dostopnih informacij) [primeri]
- Motivi za klasičen vdor:
  - kraja podatkov in sistemskih sredstev,
  - podtikanje podatkov in izsiljevanje ali maščevanje,
  - prikrivanje (“odskočna deska” za kasnejše napada),
  - radovednost, priložnost,...
- Vdiralska orodja in tehnike razmeroma lahko dostopne
  - Primer: za izvedbo SQLI zadostuje že spletni brskalnik
- Ogroženi niso samo računalniki! [vdor v bankomat, primer iztirjenja tramvaja]



Strojni prestrezniki tipkanja (vir in avtorstvo: www.keyghost.com)

Prestrezanje komunikacij

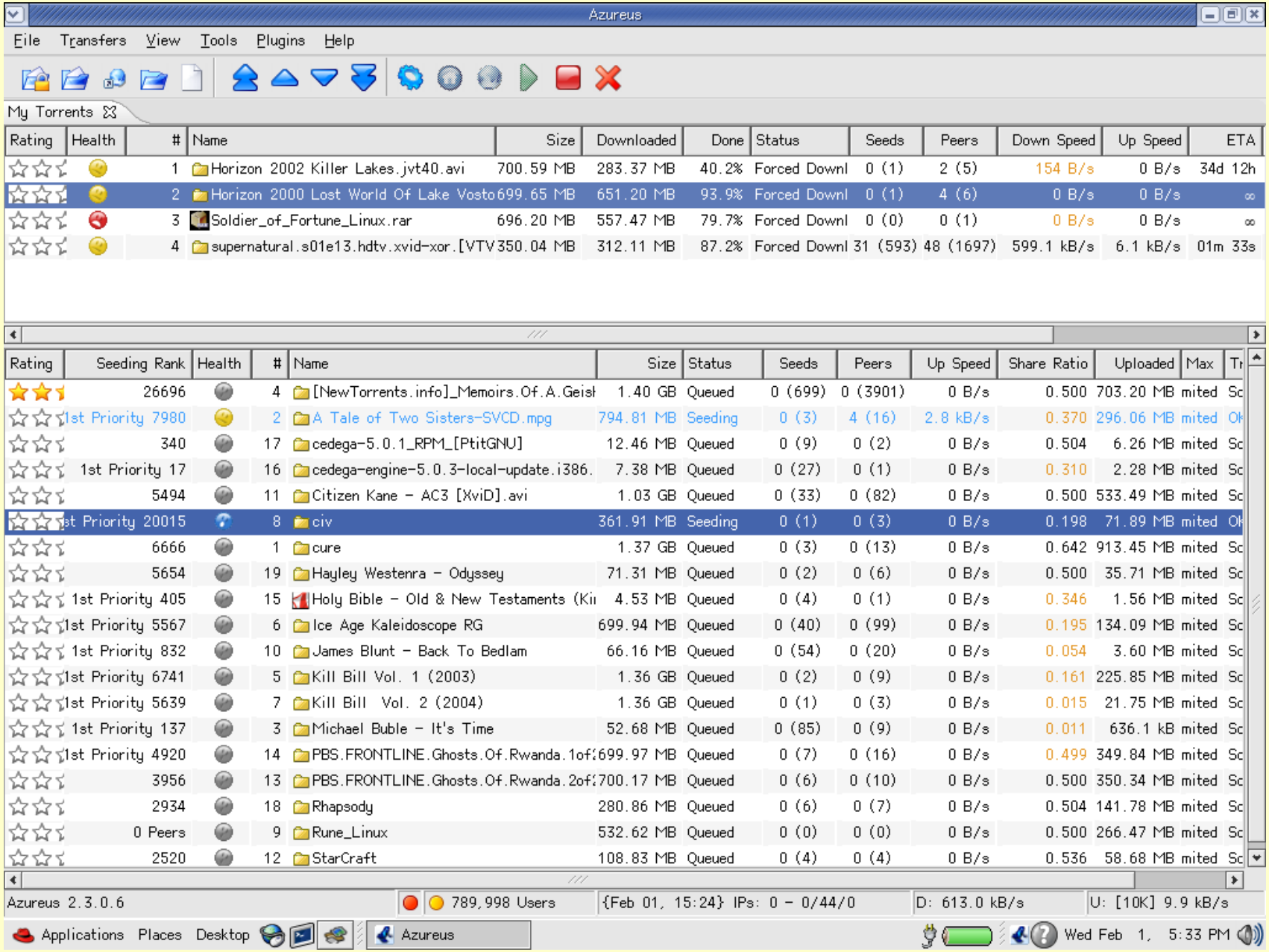
- Prestrezanje (*packet sniffing*, na internetu tehnično lažje izvedljivo kot v telefonskih omrežjih)
  - prestrezanje internetne telefonije (VoIP): primer MediaDefender leta 2007
- Izvedba mogoča tudi z legitimnimi orodji za analizo omrežij.
- Napad s posrednikom (MITM napad), za napad na (SSL) šifrirane komunikacije.
- Prestrezanje v brezžičnih omrežjih in kraja dostopa do interneta (odprta omrežja, kriptoanaliza WEP, WPA, *wardriving*).
  - Primer vdora v poštno banko v Haifi.

Zasebnost na delovnem mestu

- Tajnost e-pošte, prestrezanje komunikacij zaposlenih in zasebnost na delovnem mestu:
  - **Halford proti Veliki Britaniji** iz leta 1997: ESČP je v razsodbi izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.
  - **Copland proti Veliki Britaniji** iz leta 2007: ESČP je v zvezi z uporabo interneta in elektronske pošte na delovnem mestu delavki priznalo širok krog pravice do zasebnosti in presodilo, da je delodajalec neupravičeno posegal v njeno zasebnost. Ključni element sodbe je, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira e-pošto.

Zasebnost na delovnem mestu

- Odločitev Kasacijskega sodišča Francije v primeru **Societe Nikon France, SA v. Onof**, št. 99–42.942 iz leta 2001: *»delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah ... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene... Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.«*


Azureus
File Transfers View Tools Plugins Help
My Torrents
Rating Health # Name Size Downloaded Done Status Seeds Peers Down Speed Up Speed ETA
1 Horizon 2002 Killer Lakes.jvt40.avi 700.59 MB 283.37 MB 40.2% Forced Downl 0 (1) 2 (5) 154 B/s 0 B/s 34d 12h
2 Horizon 2000 Lost World Of Lake Vosto 699.65 MB 651.20 MB 93.9% Forced Downl 0 (1) 4 (6) 0 B/s 0 B/s ∞
3 Soldier_of_Fortune_Linux.rar 696.20 MB 557.47 MB 79.7% Forced Downl 0 (0) 0 (1) 0 B/s 0 B/s ∞
4 supernatural.s01e13.hdtv.xvid-xor.[VTV 350.04 MB 312.11 MB 87.2% Forced Downl 31 (593) 48 (1697) 599.1 kB/s 6.1 kB/s 01m 33s
Rating Seeding Rank Health # Name Size Status Seeds Peers Up Speed Share Ratio Uploaded Max Tr
26696 4 [NewTorrents.info]_Memoirs.Of.A.Geisl 1.40 GB Queued 0 (699) 0 (3901) 0 B/s 0.500 703.20 MB mited Sc
1st Priority 7980 2 A Tale of Two Sisters-SVCD.mpg 794.81 MB Seeding 0 (3) 4 (16) 2.8 kB/s 0.370 296.06 MB mited Ok
340 17 cedega-5.0.1_RPM_[PtitGNU] 12.46 MB Queued 0 (9) 0 (2) 0 B/s 0.504 6.26 MB mited Sc
1st Priority 17 16 cedega-engine-5.0.3-local-update.i386. 7.38 MB Queued 0 (27) 0 (1) 0 B/s 0.310 2.28 MB mited Sc
5494 11 Citizen Kane - AC3 [XviD].avi 1.03 GB Queued 0 (33) 0 (82) 0 B/s 0.500 533.49 MB mited Sc
st Priority 20015 8 civ 361.91 MB Seeding 0 (1) 0 (3) 0 B/s 0.198 71.89 MB mited Ok
6666 1 cure 1.37 GB Queued 0 (3) 0 (13) 0 B/s 0.642 913.45 MB mited Sc
5654 19 Hayley Westenra - Odyssey 71.31 MB Queued 0 (2) 0 (6) 0 B/s 0.500 35.71 MB mited Sc
1st Priority 405 15 Holy Bible - Old & New Testaments (Ki 4.53 MB Queued 0 (4) 0 (1) 0 B/s 0.346 1.56 MB mited Sc
1st Priority 5567 6 Ice Age Kaleidoscope RG 699.94 MB Queued 0 (40) 0 (99) 0 B/s 0.195 134.09 MB mited Sc
1st Priority 832 10 James Blunt - Back To Bedlam 66.16 MB Queued 0 (54) 0 (20) 0 B/s 0.054 3.60 MB mited Sc
1st Priority 6741 5 Kill Bill Vol. 1 (2003) 1.36 GB Queued 0 (2) 0 (9) 0 B/s 0.161 225.85 MB mited Sc
1st Priority 5639 7 Kill Bill Vol. 2 (2004) 1.36 GB Queued 0 (1) 0 (3) 0 B/s 0.015 21.75 MB mited Sc
1st Priority 137 3 Michael Buble - It's Time 52.68 MB Queued 0 (85) 0 (9) 0 B/s 0.011 636.1 kB mited Sc
1st Priority 4920 14 PBS.FRONTLINE.Ghosts.Of.Rwanda.1of2 699.97 MB Queued 0 (7) 0 (16) 0 B/s 0.499 349.84 MB mited Sc
3956 13 PBS.FRONTLINE.Ghosts.Of.Rwanda.2of2 700.17 MB Queued 0 (6) 0 (10) 0 B/s 0.500 350.34 MB mited Sc
2934 18 Rhapsody 280.86 MB Queued 0 (6) 0 (7) 0 B/s 0.504 141.78 MB mited Sc
0 Peers 9 Rune_Linux 532.62 MB Queued 0 (0) 0 (0) 0 B/s 0.500 266.47 MB mited Sc
2520 12 StarCraft 108.83 MB Queued 0 (4) 0 (4) 0 B/s 0.536 58.68 MB mited Sc
Azureus 2.3.0.6
789,998 Users
{Feb 01, 15:24} IPs: 0 - 0/44/0
D: 613.0 kB/s
U: [10K] 9.9 kB/s
Applications Places Desktop
Azureus
Wed Feb 1, 5:33 PM

Kazensko pravni vidiki

Kazenski zakonik RS

- V *Kazenskem zakoniku* (KZ-1) 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, opredeljena naslednja ravnanja:
  - neupravičeno prisluškovanje in zvočno snemanje (137. člen KZ-1, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
  - neupravičeno slikovno snemanje (138. člen KZ-1, v osnovi ne gre za tim. "računalniško kaznivo dejanje");

Kazenski zakonik RS

- kršitev tajnosti občil (2. točka 2. odstavka 139. člena KZ-1, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- nedovoljena objava zasebnih pisanj (140. člen KZ-1, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- zloraba osebnih podatkov (143. člen KZ-1, 4. odstavek – kraja identitete);
- kršitev moralnih avtorskih pravic (147. člen KZ-1, v osnovi ne gre za tim. "računalniško kaznivo dejanje");

Kazenski zakonik RS

- kršitev materialnih avtorskih pravic (148. člen KZ-1, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- kršitev avtorski sorodnih pravic (149. člen KZ-1, 1. in 2. odstavek – P2P omrežja, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- napad na informacijski sistem (221. člen KZ-1);
- vdor v poslovni informacijski sistem (237. člen KZ-1);

Kazenski zakonik RS

- izdelovanje in pridobivanje orožja in pripomočkov namenjenih za kaznivo dejanje - pripomočki za vdor ali neupravičen vstop v informacijski sistem (3. odstavek 306. člena KZ-1).

Kršitev tajnosti občil

139 člen KZ-1

...

(2) Z denarno kaznijo ali z zaporom do enega leta se kaznuje:

2) kdor se z uporabo **tehničnih sredstev** neupravičeno seznani s sporočilom, ki se prenaša po telefonu ali s kakšnim drugim **telekomunikacijskim sredstvom**;

...

(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, poštni **ali drug delavec**, ki mu je zaupano prevzemanje, prenos ali predaja tujih pisem, tujih brzojavk ali kakšnih drugih pisanj ali pošiljk, se kaznuje z zaporom od treh mesecev do petih let.

Zloraba osebnih podatkov

143 člen KZ-1

(1) Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.

(2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.

...

(4) Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.

...

Kršitev materialnih avtorskih pravic

148 člen KZ-1

(1) Kdor **z namenom prodaje** neupravičeno uporabi eno ali več avtorskih del ali njihovih primerkov, katerih skupna tržna cena pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let.

(2) Če tržna cena avtorskih del iz prejšnjega odstavka pomeni veliko premoženjsko vrednost, se storilec kaznuje z zaporom do petih let.

(3) Če je bila z dejanjem iz prvega ali drugega odstavka tega člena pridobljena velika protipravna premoženjska korist in je šlo storilcu za to, da sebi ali komu drugemu pridobi tako premoženjsko korist, se kaznuje z zaporom od enega do osmih let.

(4) Primerki avtorskih del in naprave za njihovo reproduciranje **se vzamejo**.

Kršitev avtorski sorodnih pravic

149 člen KZ-1

(1) Kdor **neupravičeno reproducira, da na voljo javnosti, razširja** ali da v najem eno ali več izvedb, fonogramov, videogramov, rtv-oddaj ali podatkovnih baz, katerih **skupna tržna cena** pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let.

(2) Kdor neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, rtv-oddaj ali podatkovnih baz, katerih skupna tržna cena pomeni veliko premoženjsko vrednost, se kaznuje z zaporom do petih let.

(3) Če je bila z dejanjem iz prvega ali drugega odstavka tega člena **pridobljena** velika protipravna premoženjska korist in je šlo storilcu za to, da sebi ali komu drugemu pridobi tako premoženjsko korist, se kaznuje z zaporom od enega do osmih let.

(4) Primerki izvedb, fonogramov, videogramov, rtv-oddaj ali podatkovnih zbirk in naprave za njihovo reproduciranje se vzamejo.

Napad na informacijski sistem

221. člen KZ-1

(1) Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.

(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

(3) Poskus dejanja iz prejšnjega odstavka je kazniv.

(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

Vdor v poslovni informacijski sistem

237. člen KZ-1

(1) Kdor pri **gospodarskem poslovanju** neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen svoj podatek, ovira prenos podatkov ali delovanje informacijskega sistema ali kako drugače vdre v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let.

(2) Če je bila z dejanjem iz prejšnjega odstavka pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda in je storilec hotel sebi ali komu drugemu pridobiti tako premoženjsko korist ali drugemu povzročiti tako premoženjsko škodo, se kaznuje z zaporom do petih let.

Izdelovanje in pridobivanje pripomočkov namenjenih za kaznivo dejanje

306. člen KZ-1

(1) Kdor orožje, razstrelilne snovi ali pripomočke, s katerimi se lahko napravijo, ali strupe, za katere ve, da so namenjeni za kaznivo dejanje, izdela ali si jih pridobi ali jih hrani ali komu omogoči, da pride do njih, se kaznuje z zaporom do treh let.

(2) Kdor napravi ali komu odstopi ponarejen ključ, odpirač ali kakšen drug pripomoček za vlom, čeprav ve, da je namenjen za kaznivo dejanje, se kaznuje z zaporom do enega leta.

(3) Enako kot v prejšnjem odstavku se kaznuje, kdor **z namenom storitve kaznivega dejanja** poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali kako drugače zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem.

Primeri iz prakse

Mladoletnik osumljen piratstva

- *"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'...*
- *Preiskavo so naredili pri vseh istočasno, ostale tri so, ker so bili polnoletni, za 48 ur dali tudi v pripor..."*.

Mladoletnik osumljen piratstva

- Policisti so "*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)*"
- 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*".
- Zasegli so tudi 360 CD-jev, za katere so sumili, da vsebujejo piratske vsebine.

Polnoletnik osumljen piratstva

- Osumljenec je preko Bolhe kupoval CD-je s kopijami različnih filmov.
- Ker se je selil, se je starih CD-jev želel znebiti in je dal oglas, da proda nekaj sto CD-jev za razmeroma nizko vsoto.
- Približno pol leta po tem je nekega jutra pozvonilo...
- Sledila je hišna preiskava in vložitev obtožnice zaradi suma piratstva.
- Ocenjena materialna škoda je bila okrog 9 mio. SIT (37.556 EUR), zagrožena pa je bila tudi zaporna kazen.

Kako “pirat” postane “pedofil”...

- P2P zastrupljanje (ang. *P2P poisoning*): napadalci v P2P omrežjih ponujajo lažno vsebino.
- Primer: uporabnik si želi prenesti najnovejši film, pod iskanim naslovom pa prenese nekaj povsem drugega.
- Pogosto gre za neprimerne vsebine (npr. stare pornografske filme).
- Kaj bi se zgodilo v primeru, da bi si uporabnik tako nevede prenesel otroško pornografijo?
- V večini držav je za distribucijo ali samo prenos (posedovanje) otroške pornografije zagrožena zaporna kazen.

Kako “pirat” postane “pedofil”...

- **26-letnik ovaden zaradi posredovanja otroške pornografije**
  Koper, 18. 9. 2007 - ... Kot so sporočili s Policijske uprave Koper, gre za mladeniča z območja občine Izola, ki ima na svojem računalniku **inštaliran program eMule**. S tem programom je z interneta na svoj osebni računalnik prenašal datoteke z otroško pornografijo ter te datoteke tudi ponujal in izmenjeval z drugimi uporabniki internetne mreže.
- ...Navedena švicarska preiskava je pokazala, da so si **številni uporabniki preiskovanih internetnih omrežij izmenjevali ali imeli v posesti otroške pornografske fotografije in video posnetke**. Ugotovljeno je bilo tudi, da so na ta omrežja dostopali tudi uporabniki **iz Slovenije**.
- Vir, spletno DELO, 18. 9. 2007, <http://delo.si/index.php?sv_path=41,1735,240209>

Zlorabljeno geslo učenke

- Mladoletna učenka si je med obiskom pri sošolki ustvarila MSN račun.
- Učenka MSN-ja ni uporabljala, nekdo (domnevno eden izmed sošolcev), pa je z njenim geslom dostopil na njen uporabniški profil (MSN Space) in nanj vpisal neprimerne in žaljive vsebine o njej.
- Vnos na MSN je učenka opazila šele čez dobro leto.
- Sledil je spor med starši, ki so želeli sprožiti uraden kazenski pregon.
- Šola je zavzela stališče, da se s problemom ne bo ukvarjala, ker se dogodek ni zgodil v času pouka ali v prostorih šole.

Zlorabljeno geslo učenke

- Z vpisom na MSN je bilo omadeževano dobro ime učenke, do vpisa je prišlo s pomočjo kaznivega dejanja (neupravičen vstop v informacijski sistem).
- Problem pa je z dokazovanjem na sodišču, kazensko odgovornostjo mladoletnikov ter sodnim reševanjem medsebojnih otroških sporov.

- Kazenski pregon ali pogovor?

Zlorabljeno geslo uporabljeno za prevaro

- Uporabnica interneta je dobila obvestilo, da "mora" poslati neke podatke na Yahoo (kjer ima odprt e-poštni naslov), češ da nekaj preverjajo.
- Naslednji dan ni več mogla dostopati do svojega poštnega predala.
- Osebe iz njenega adresarja pa so pričele dobivati sporočilo, da je v Nigeriji in v težavah, in naj ji pošljejo denar.

- **Zaupanje**: ljudje bodo bolj zaupali osebi, ki jo poznajo (posebej še, če jim pošlje e-pošto iz "svojega" uporabniškega računa), kot popolnemu neznancu.

Zlorabljeno geslo uporabljeno za prevaro

Hi!,

I am sorry I didn't inform you about my traveling to Africa for a program called Empowering Youth to Fight Racism, HIV/AIDS, Poverty and Lack of Education, the program is taking place in three major countries in Africa which are Ghana , South Africa and Nigeria . It as been a very sad and bad moment for me, the present condition that I found myself is very hard for me to explain.**I am really stranded in Nigeria because I forgot my little bag in the Taxi where my money, passport,documents and other valuable things were kept on my way to the Hotel am staying,I am facing a hard time here because I have no money on me.** I am now owning a hotel bill of $1,000 and they wanted me to pay the bill soon else they will have to seize my bag and hand me over to the Hotel Management.

Zlorabljeno geslo uporabljeno za prevaro

I need this help from you urgently to help me back home,I need you to help me with the hotel bill and i will also need $1,500 to feed and help myself back home **so please can you help me with a sum of $2,500 to sort out my problems here?** I need this help so much and on time because i am in a terrible and tight situation here,**I don't even have money to feed myself** for a day which means i had been starving so please understand how urgent i needed your help.

I am sending you this e-mail from the city lagos and I only have 30 min,I will appreciate what so ever you can afford to send me for now and I promise to pay back your money as soon as i return home,**you need to transfer the money through Western Union** , please **email me back so that i can email you** one of the Hotel Management name that you will send the western union to.Thanks

Regard

<podpis>

Posledice objave podatkov na spletu

- Eden izmed študentov na Lousiana State University je na spletišču Facebook odprl uporabniški račun, kjer je objavljal različne prispevke in fotografije iz svojega študentskega življenja.

- Po končanem študiju se je želel zaposliti in preden je zaprosil za državno službo je podatke o sebi zaklenil samo za svoje prijatelje, saj ni želel, da se z vsebino *neumnosti*, ki jih je objavljal kot študent seznani tudi njegov potencialni delodajalec.

Posledice zaupanja neznancem na spletu

- Januarja 2008 je slovenski uporabnik opisal prevaro katere žrtev je bil:
  - "Imam namreč naslednji problem: tipu sem nakazal preko Western Uniona 1250€ za 5 mobilnih telefonov znamke Nokia. Živi v Angliji. Njegovo ime je Raymond Bully. Imam njegov naslov, številko, e-mail naslov. No, ko sem mu nakazal, mi sploh ni poslal telefonov, kar nekaj mi je začel nakladat, naj mu nakažem še dodatnih 450€ za poštnino. Rekel sem mu, da je 450€ preveč za poštnino in da mu ne bom nakazal, ter da naj mi pošlje denar nazaj. In sedaj mi denarja noče vrniti."

Posledice zaupanja neznancem na spletu

- “Sploh ne vem kaj naj naredim. Ker 1250€ je zame zelo zelo veliko. Shranjena imam vsa njegova sporočila, ki jih je poslal preko maila.”

...

- “Dobil sem na internetu številko pa naslov ter poklical tipa. Potem mu poslal denar in bilo je kar je bilo.”

...

- “Ja naslov in hiša obstaja-je šel prijatelj v Angliji preverit. Je plačal za neko storitev ko lahko pogledaš na naslov.”

Posledice javne objave številke bančnega računa

- Novembra 2007 so v britanskem davčnem uradu izgubili dva diska z osebnimi podatki 25 milijonov oseb. Izgubljena diska sta med drugim vsebovala tudi bančne podatke, policija pa je opozorila na možnost kraje identitete.
- Voditelj britanske avtomobilistične oddaje Top Gear Jeremy Clarkson je bil mnenja, da je zgodba prenapihnjena in je javno objavil številko svojega bančnega računa.
- "*Vse kar s temi podatki lahko storite je, da mi nakažete denar na moj račun. Ne pa da mi ga vzamete.*"

Posledice javne objave številke bančnega računa

- V začetku leta pa je nekdo iz njegovega računa na dobrodelno organizacijo Diabetes UK nakazal 500 funtov.

- "*To jutro sem si ogledal svoje bančne izpiske in ugotovil, da je nekdo na mojem računu odprl trajnik, ki samodejno nakazuje 500 funtov"*.

- "*Motil sem se in bil sem kaznovan za svojo napako."*

VPRAŠANJA?