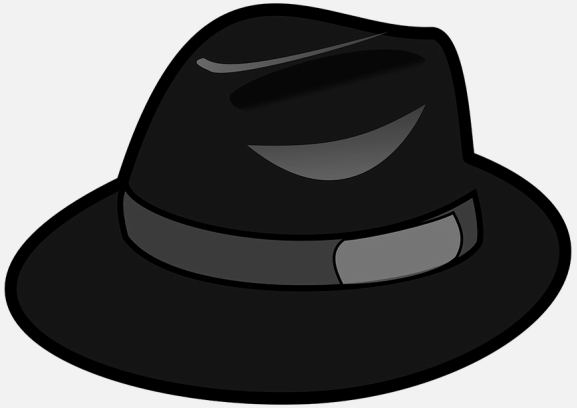


Kiberkriminal

Magija, radovednost, zabava, posel in imunski sistem interneta

Matej Kovačič

https://infosec-seminar.si | 22. junij 2018

Kiberkriminal in kiberkriminalci

Kiberkriminal

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.

Kiberkriminal

Kiberkriminal se 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;
- sledenje izvornemu komunikacijskemu sredstvu, preko katerega se je nekdo povezal v kiberprostor, ni vedno mogoče, saj napadalci pogosto uporabljajo tehniko povezovanja preko različnih sistemov, kar onemogoči ali vsaj oteži sledenje.

»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 se ga dojema kot sofisticirano ilegalno dejavnost.

»Hekanje«

Levy pravi, da obstajajo štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas.

- Prva generacija: izvira iz MIT, je v 50-tih in 60-tih letih prejšnjega stoletja razvila prve programske tehnike.
- Druga generacija: posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam.
- Tretja generacija: vodilni razvijalci računalniških iger.
- Četrta generacija: osebe, ki na nedovoljene načine vstopajo v tuje računalnike.

Prvotni hekerji so bili 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.

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 mnenja da je to bolj način razmišljanja, želja po znanju, izziv...*".

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.*" (Bruce Schneier).

Richard Pryce, »Datastream Cowboy«, ki je leta 1994 v starosti 16 let vdrl v več visoko zaupnih ameriških vojaških sistemov: "*Nekateri so gledali televizijo po šest ur na dan, jaz pa sem hekal računalnike.*".

Vrste »hekerjev«

Beli hekerji ali **etični hekerji** svoje znanje uporabljajo za zakonito preverjanje varnosti sistemov.

Črni hekerji hekersko znanje zlorabljajo za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter za povzročanje škode.

Krekerji (ang. *cracker*) so posamezniki, ki se ukvarjajo s tim. reverznim inženiringom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem.

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. Motivi so večinoma samodokazovanje, zabava ali vandalizem.

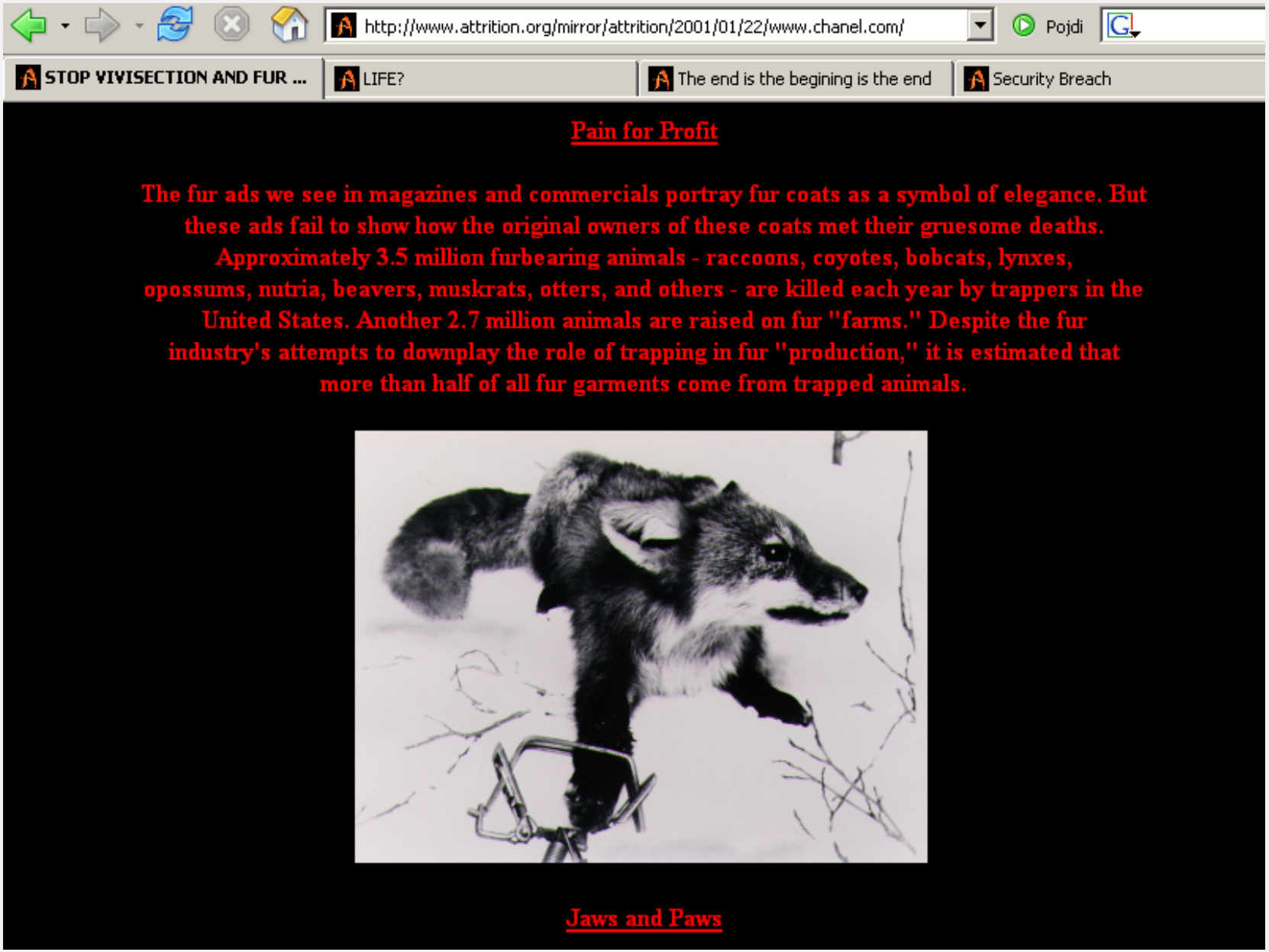
Haktivizem

Obstajata dve definiciji "haktivizma":

- nudenje informacijske (tehnične) podpore političnim aktivistom (praviloma povsem zakonito);

- nelegalno politično delovanje na internetu. Denningova ga 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.

Haktivizem


http://www.attrition.org/mirror/attrition/2001/01/22/www.chanel.com/
Pojdi
STOP VIVISECTION AND FUR ...
LIFE?
The end is the begining is the end
Security Breach
Pain for Profit
The fur ads we see in magazines and commercials portray fur coats as a symbol of elegance. But these ads fail to show how the original owners of these coats met their gruesome deaths. Approximately 3.5 million furbearing animals - raccoons, coyotes, bobcats, lynxes, opossums, nutria, beavers, muskrats, otters, and others - are killed each year by trappers in the United States. Another 2.7 million animals are raised on fur "farms." Despite the fur industry's attempts to downplay the role of trapping in fur "production," it is estimated that more than half of all fur garments come from trapped animals.
Jaws and Paws

Haktivizem

```
------------------------------------------------------------------------
01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
01101110  01000111 01101100 01101111 01100010 01100001 01101100
01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
------------------------------------------------------------------------
  ___                      _   _             ___ _     _          _
 / _ \ _ __  ___ _ _ __ _| |_(_)___ _ _    / __| |___| |__  __ _| |
| (_) | '_ \/ -_) '_/ _` |  _| / _ \ ' \  | (_ | / _ \ '_ \/ _` | |
 \___/| .__/\___|_| \__,_|\__|_\___/_||_|  \___|_\___/_.__/\__,_|_|
      |_|
 ___ _         _            _
| _ ) |__ _ __| |_____ _  _| |_
| _ \ / _` / _| / / _ \ || |  _|
|___/_\__,_\__|_\_\___/\_,_|\__|

------------------------------------------------------------------------
01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
01101110  01000111 01101100 01101111 01100010 01100001 01101100
01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
------------------------------------------------------------------------
```

Kiberterorizem in kibersabotaža

Kiberterorizem in kibersabotaža:

- uporaba hekerskih tehnik v aktivistične ali vojaške, a destruktivne namene (povzročanje ekonomske škode ali ogrožanje življenja ljudi);

Primeri:

- Morris worm, 2. november 1988 (bolj vandalizem);
- 1990-ta leta: večinoma pošiljanje SPAM sporočil;
- 911 worm (leta 2000), računalniški virus, ki je po uspešni okužbi skušal z modemom klicati na številko za klic v sili;
- napad na pristaniške v Houstonu (leta 2003): motnje v delovanju pristanišča;
- pogojno: napad SQL Slammerja na jedrsko elektrarno v Ohiu leta 2003.

Kiberterorizem in kibersabotaža

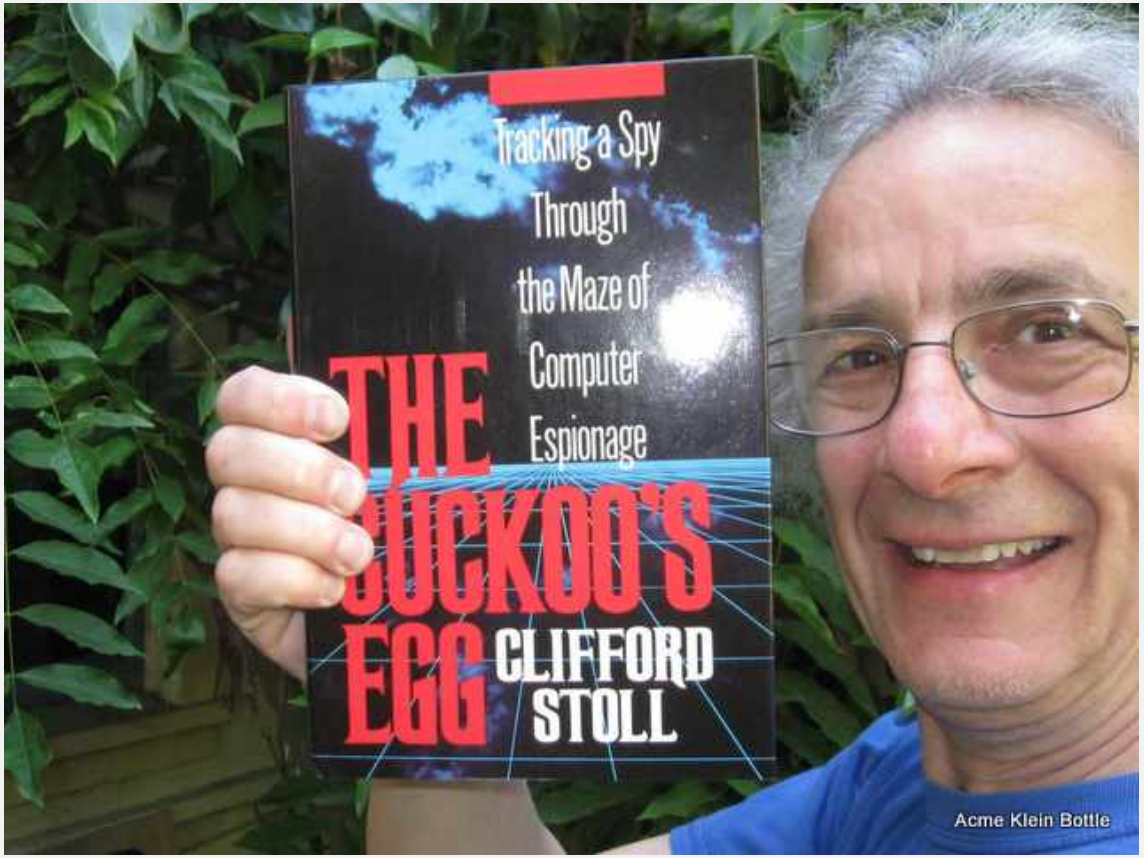
Primeri:

- DoS napad na NATO strežnike leta 1999 kot znak protesta proti bombardiranju kitajske ambasade v Beogradu;
- leta 2000 bivši zaposleni v Maroochy Shire v Avstraliji povzroči izpust 800.000 litrov odpadnih voda v okolje;
- kibernapad na Estonijo leta 2007 zaradi odstranitve spomenika sovjetskemu vojaku;
- v zadnjih letih napadi na finančni sektor, vladne službe, kritično infrastrukturo,...

Kiberkriminal in država

Informacijsko-obveščevalni napadi:

- »Cuckoo's Egg« (KGB hack)



Kiberkriminal in država

Informacijsko-obveščevalni napadi:

- ZDA (NSA, industrijska špijonaža);
- Rusija (industrijska špijonaža, APT napadi na zahodne države, vojaško-obveščevalno hekanje (Ukrajina, Estonija…), virusi, FancyBear);
- Stuxnet (napad na iranski jedrski program);
- Severna Koreja (Mirrim College, Lazarus Group);
- Kitajska (sile kibernetske varnosti (»Blue Army«), Enota 61398, APT napadi na zahodne države, napadi na politične aktiviste).

Kiberkriminal in država

Kibervojna:

- DDoS napadi na Gruzijo julija 2008 s strani Rusije (napad na medijske organizacije, državne spletne strani,...);
- v Ukrajini so leta 2014 ruske sile za nekaj časa prevzele nadzor nad več središči s TK opremo - s tem naj bi preprečili uporabo mobilnih telefonov članom parlamenta in drugim pomembnim posameznikom;
- decembra 2015 je 80.000 gospodinjstev na zahodu Ukrajine ostalo brez električne energije, saj so napadalci izključili razdelilne transformatorske postaje;
- konec 2014: napadi na turške državne strežnike, telekomunikacijski in finančni sektor, zaradi sestrelitve Ruskega letala na meji s Sirijo.

Kiberkriminal in država

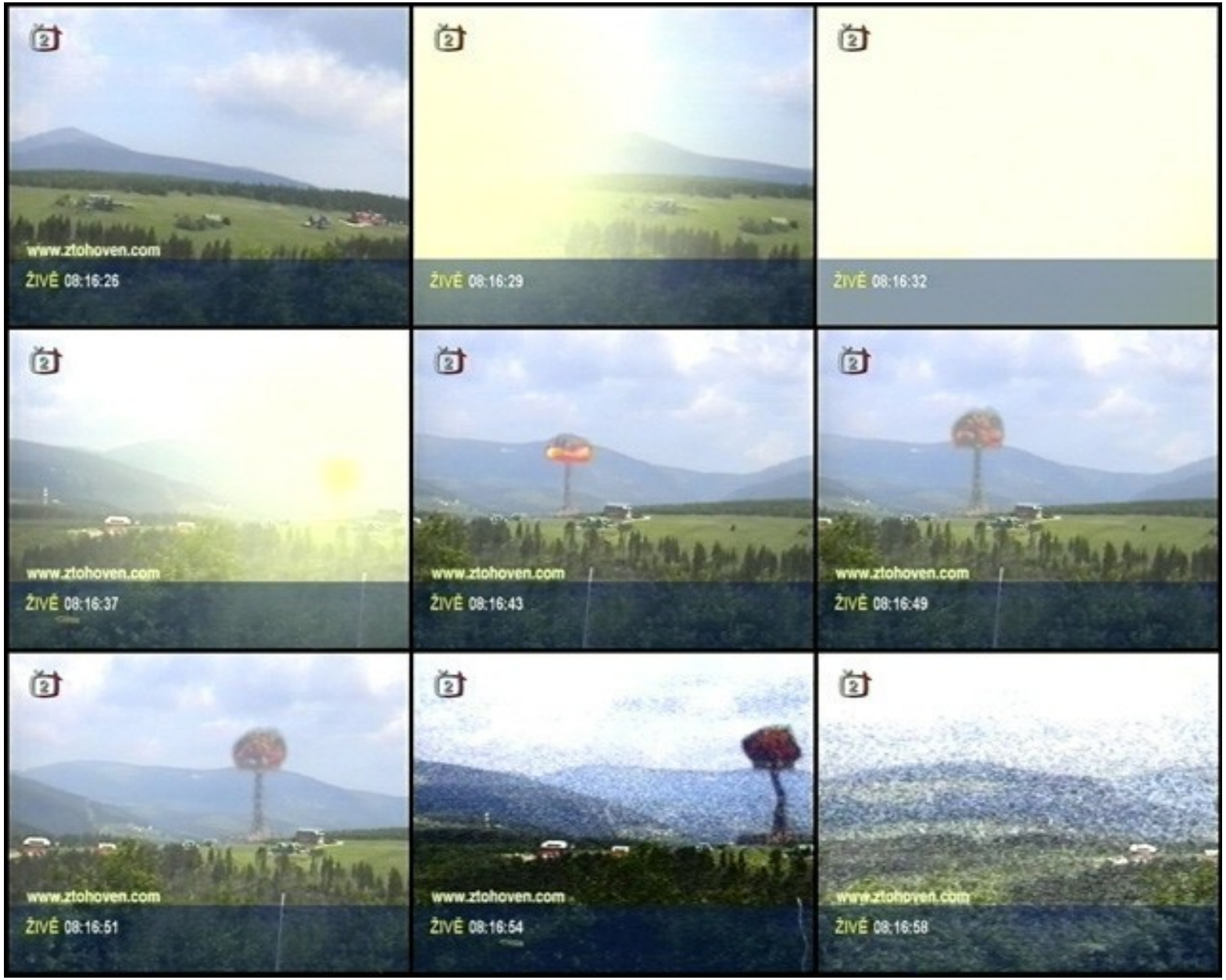
Zmogljivosti kibernetskih napadov kot sredstvo odvračanja kibernapadov:

> »*In 2016, the US was successfully deterred from attacking Russia in cyberspace because of fears of Russian capabilities against the US.*«

(Bruce Schneier, <https://www.schneier.com/blog/archives/2018/06/an_example_of_d.html>)

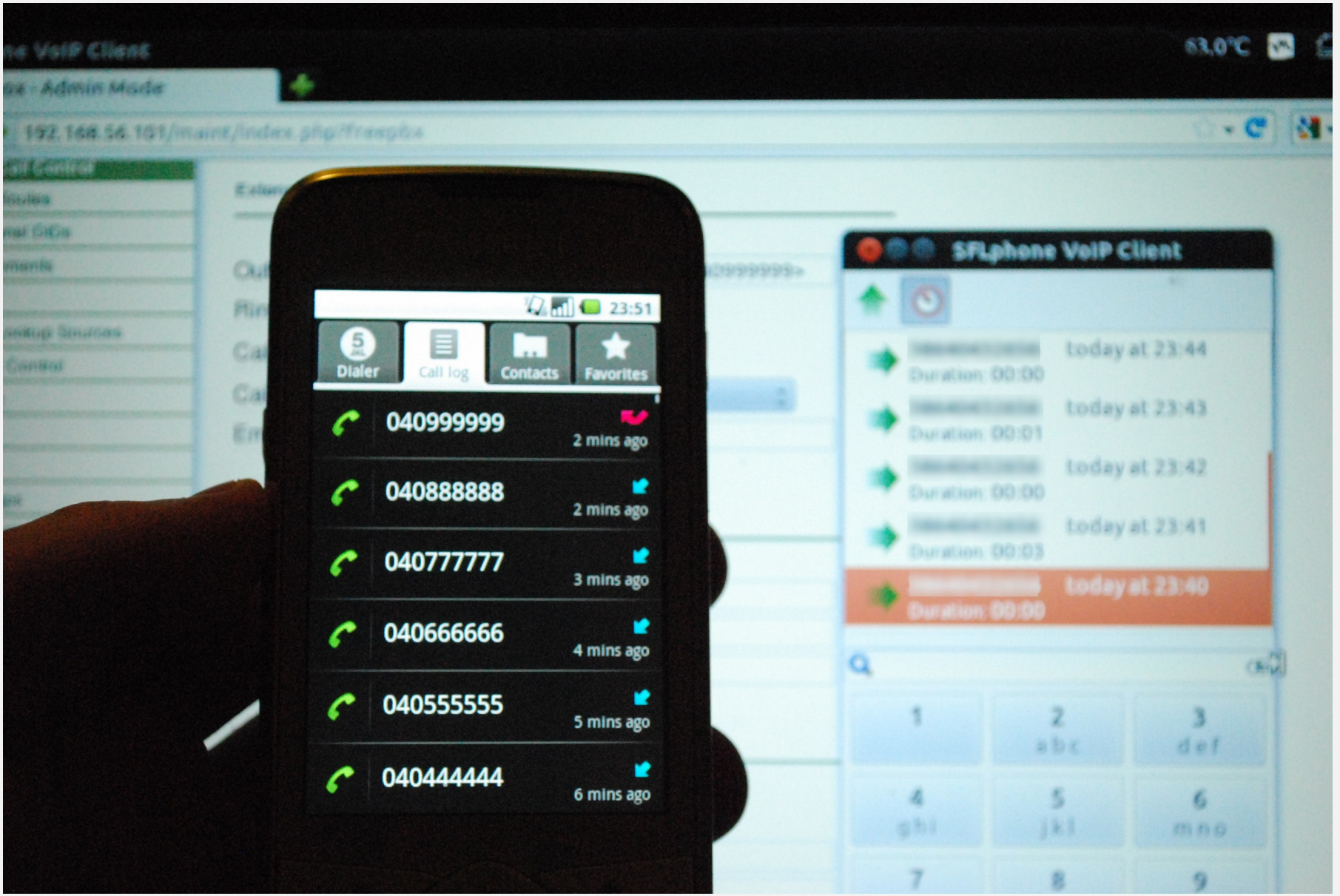
Magija

Kiberkriminal kot magija



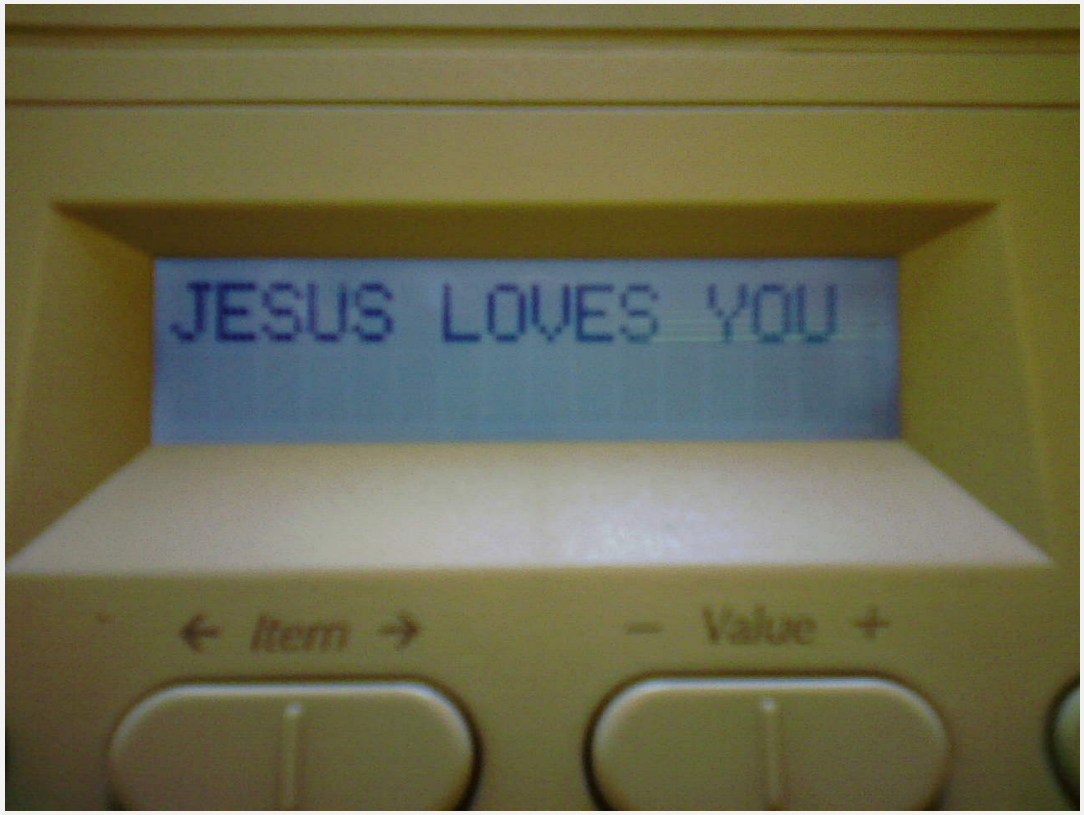
Kiberkriminal kot magija

Kiberkriminal kot magija



Radovednost in zabava

Kiberkriminal kot zabava



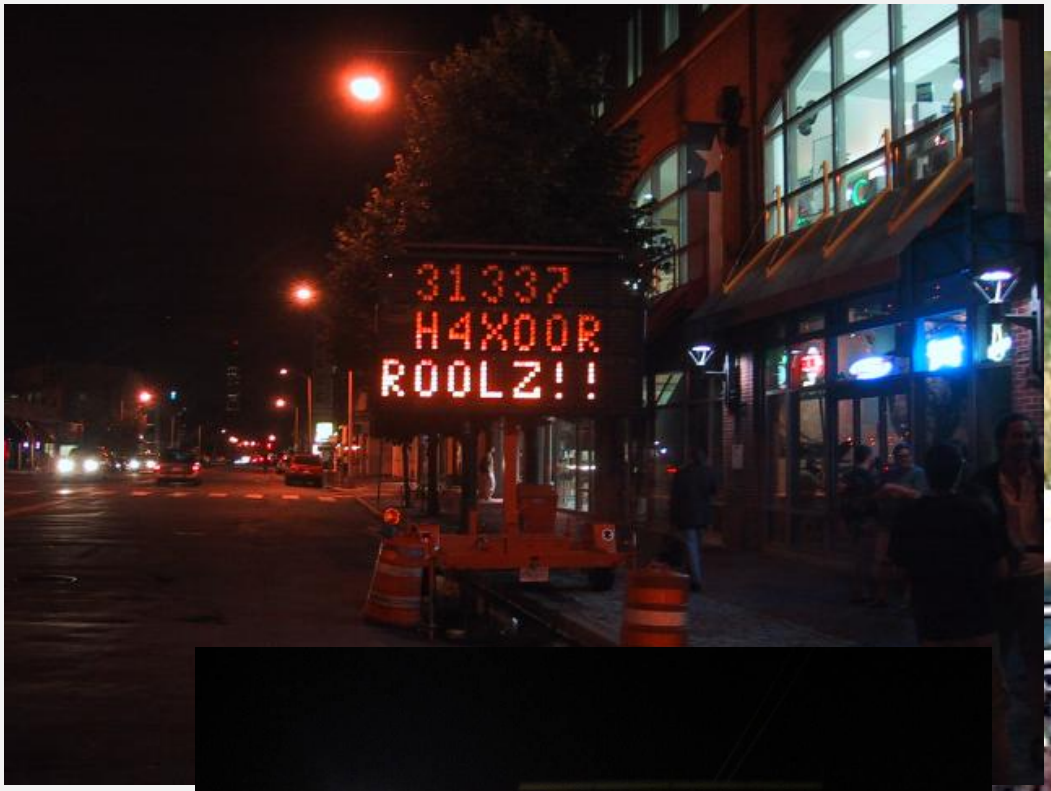
Hekerski napad na tiskalnik.

Kiberkriminal kot zabava

Razobličena spletna stran odvetniške pisarne (okrog 2003).

Razobličenje spletne strani rimokatoliške cerkve (leto 2001).

Kiberkriminal kot zabava

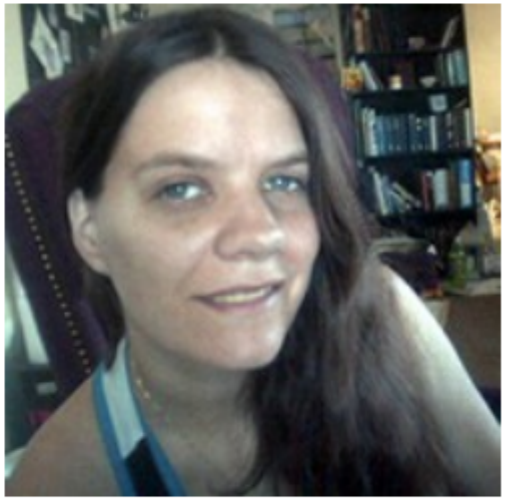


Hekerski napad na prometne znake.

Kiberkriminal kot »zabava«

Hackers embed flashing animations on epilepsy support forum

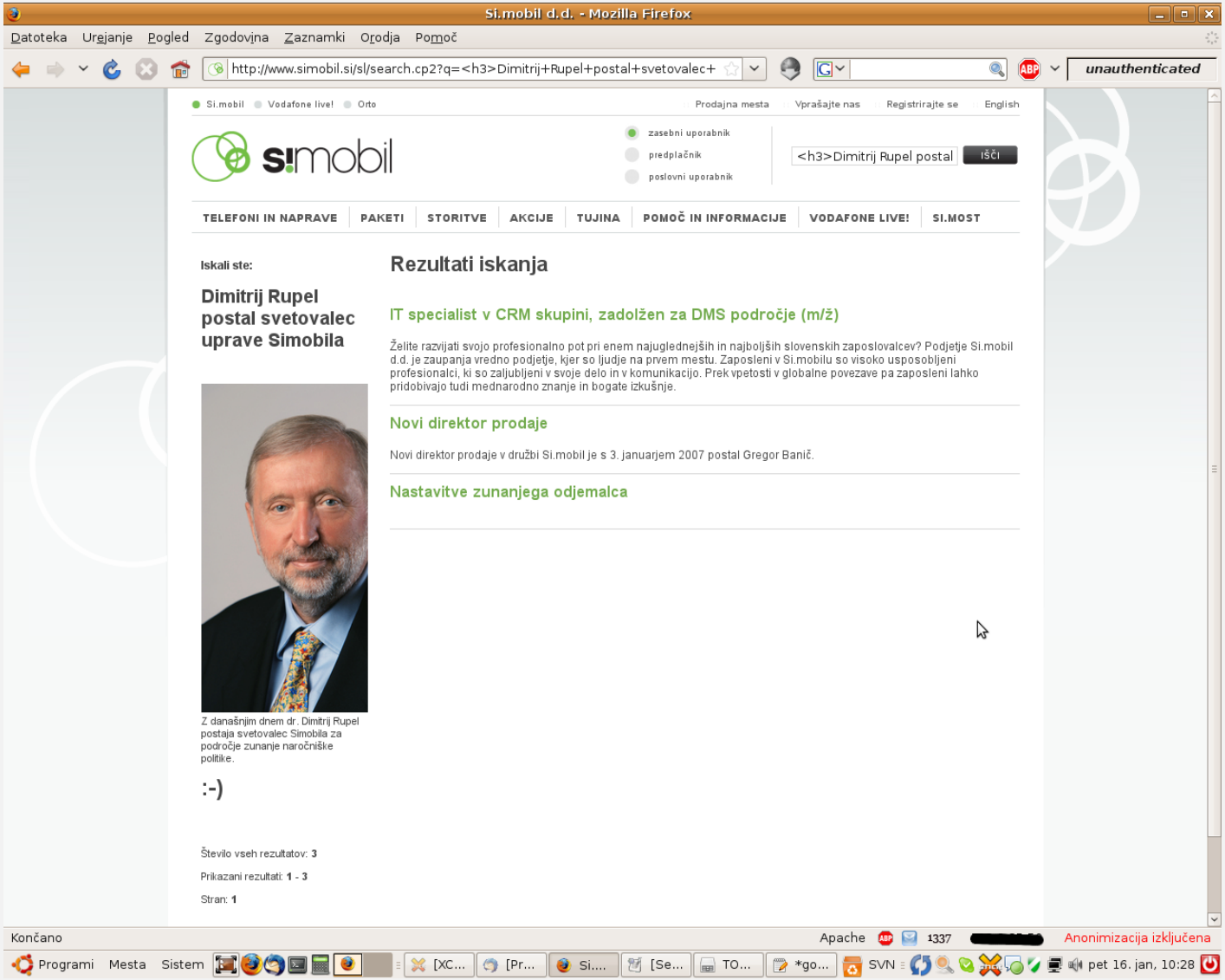
By Darren Murph posted March 29th 2008 8:50PM



Shortly after hearing a sad tale of a 7-year old cancer patient having his medication and PSP stolen whilst en route to treatment comes yet another story of the world's meanest preying on the innocent. This go 'round, a group of griefers (which appear to be members of Anonymous) managed to invade a support forum established by the nonprofit Epilepsy Foundation and use JavaScript code and messages littered with flashing animations to effectively assault dozens of visitors who suffer from the disorder. The Foundation managed to catch wind of the problem within 12 hours of the attack, and while the boards were closed down temporarily to purge it of offending messages, many readers (such as RyAnne Fultz, pictured) experienced headaches and seizures before rescue arrived. Let's just say we sincerely hope the culprits get what's comin' to 'em.

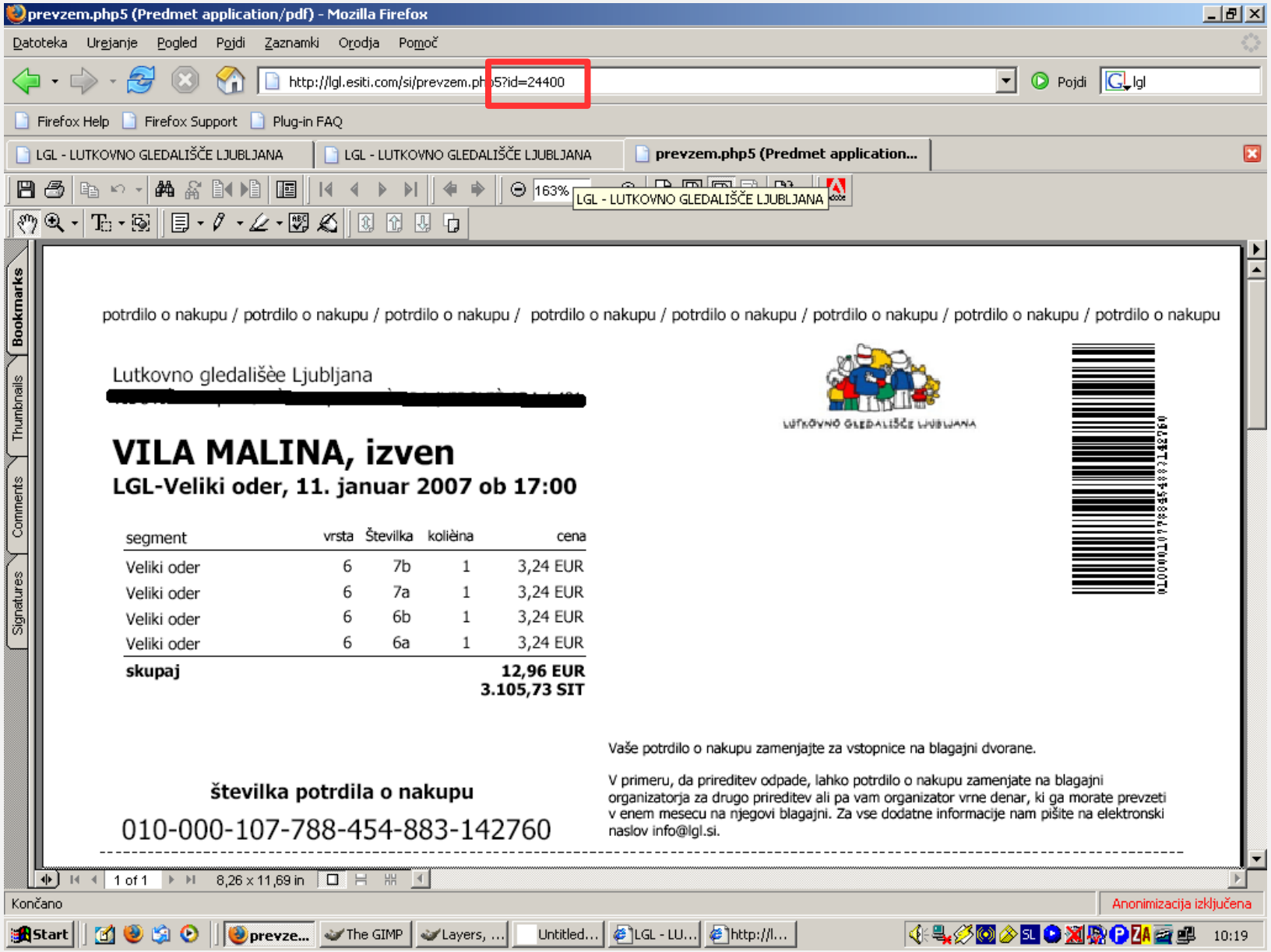
Hekerski napad na bolnike z epilepsijo.

Kiberkriminal kot zabava



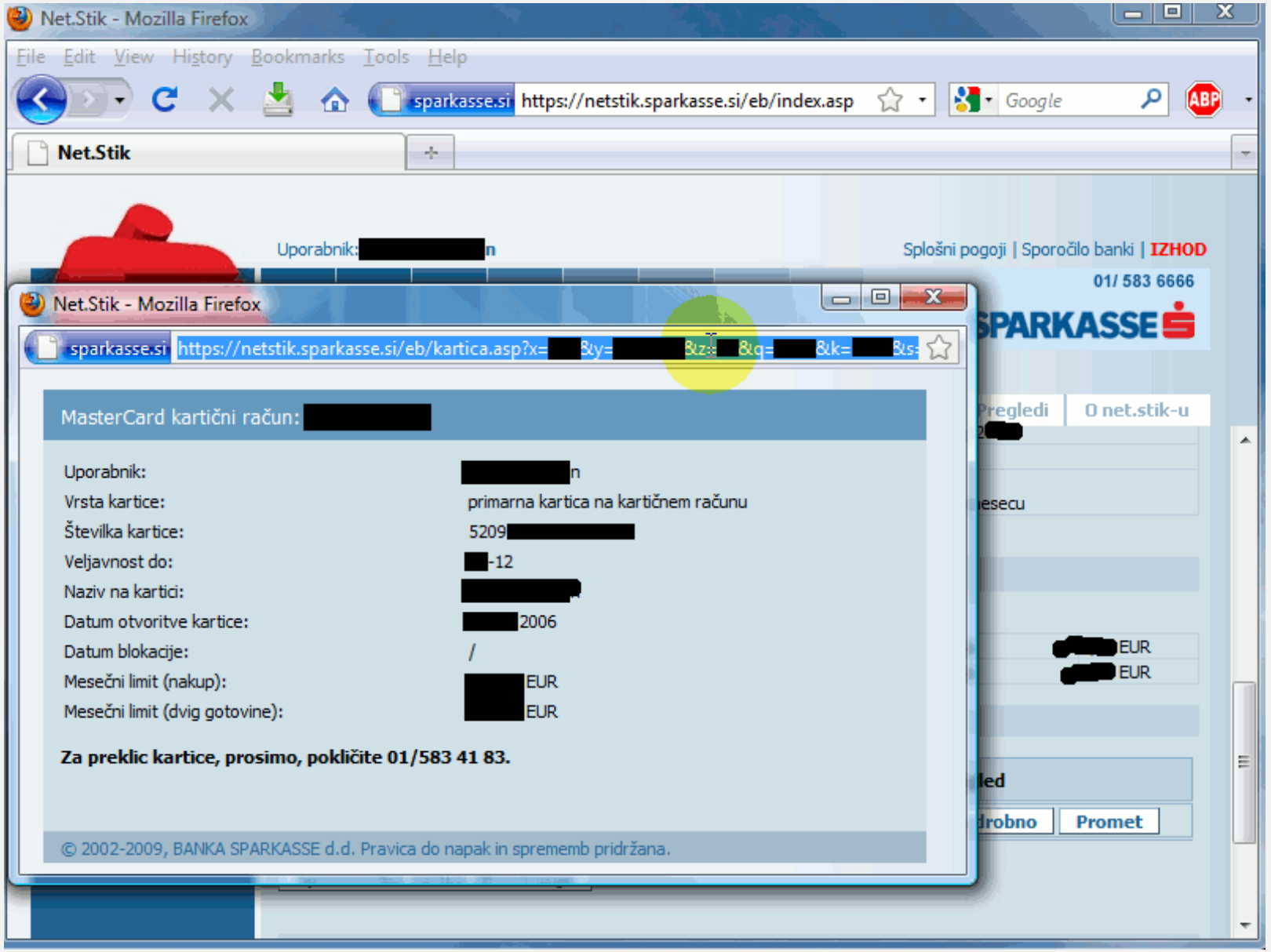
»Prvi april«.

Kiberkriminal kot radovednost



»Igranje« z URL naslovi...

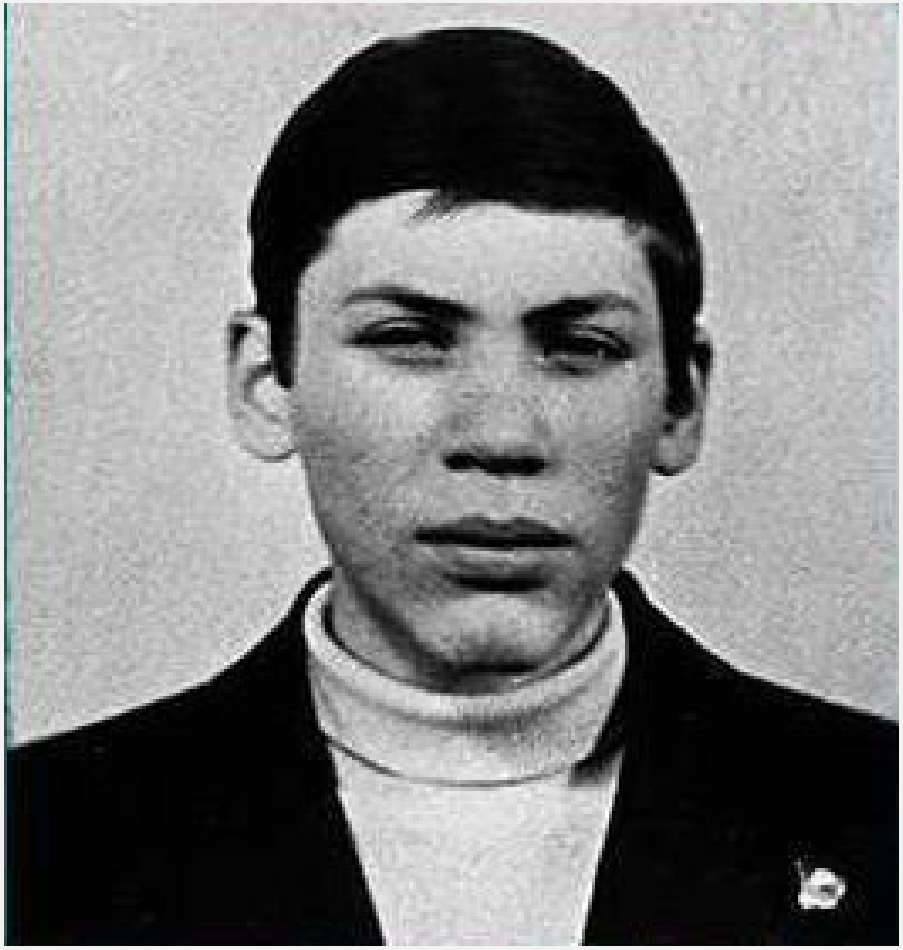
Kiberkriminal kot radovednost



»Igranje« z URL naslovi v spletni banki.

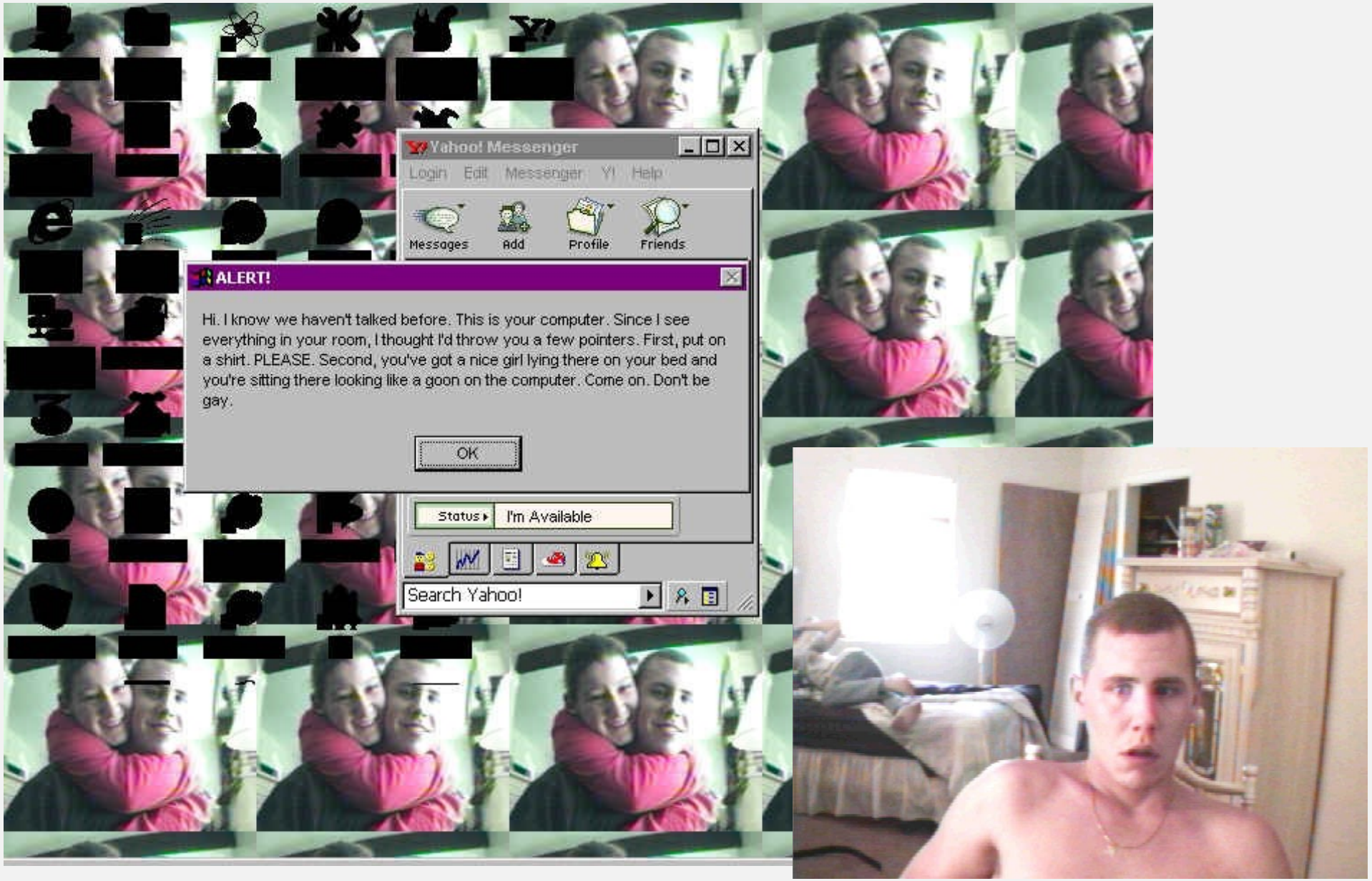
Posel

Kiberkriminal kot posel



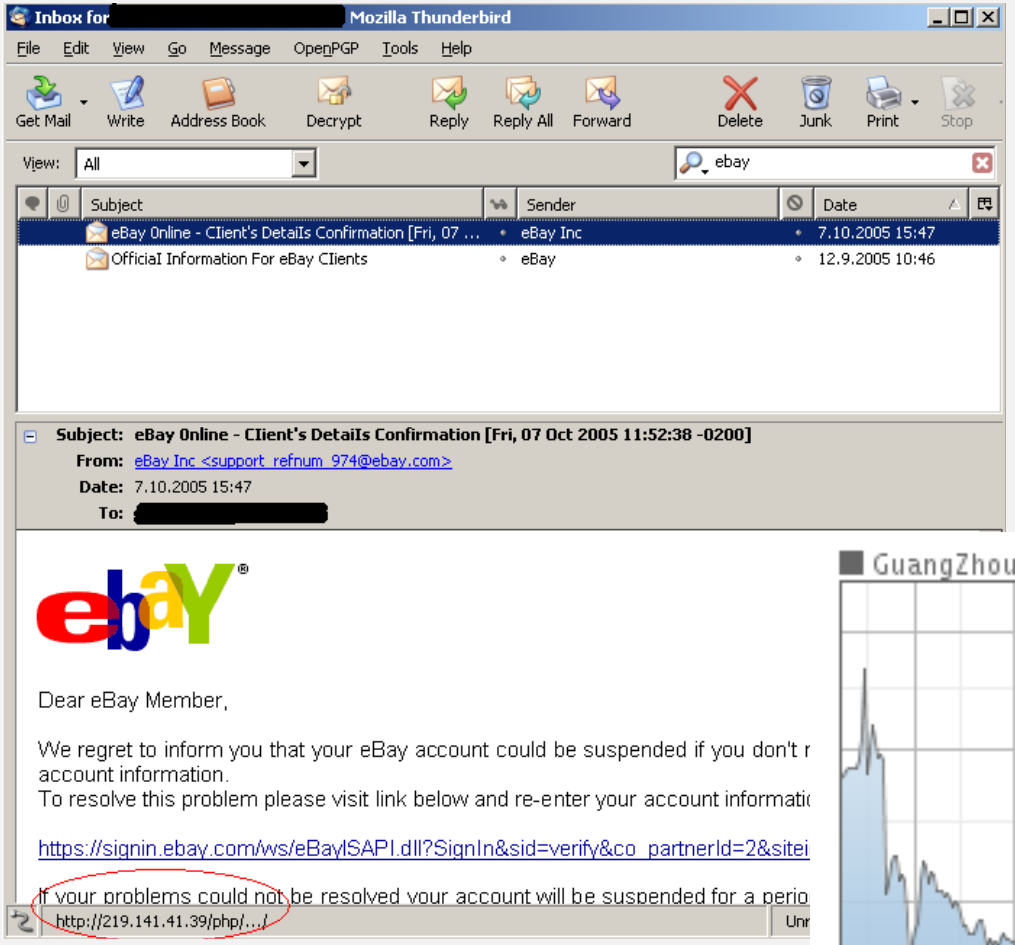
Vladimir Leonidovič Levin je leta 1994 vdrl v Citibank in ukradel 10,7 milijona USD.

Kiberkriminal kot posel



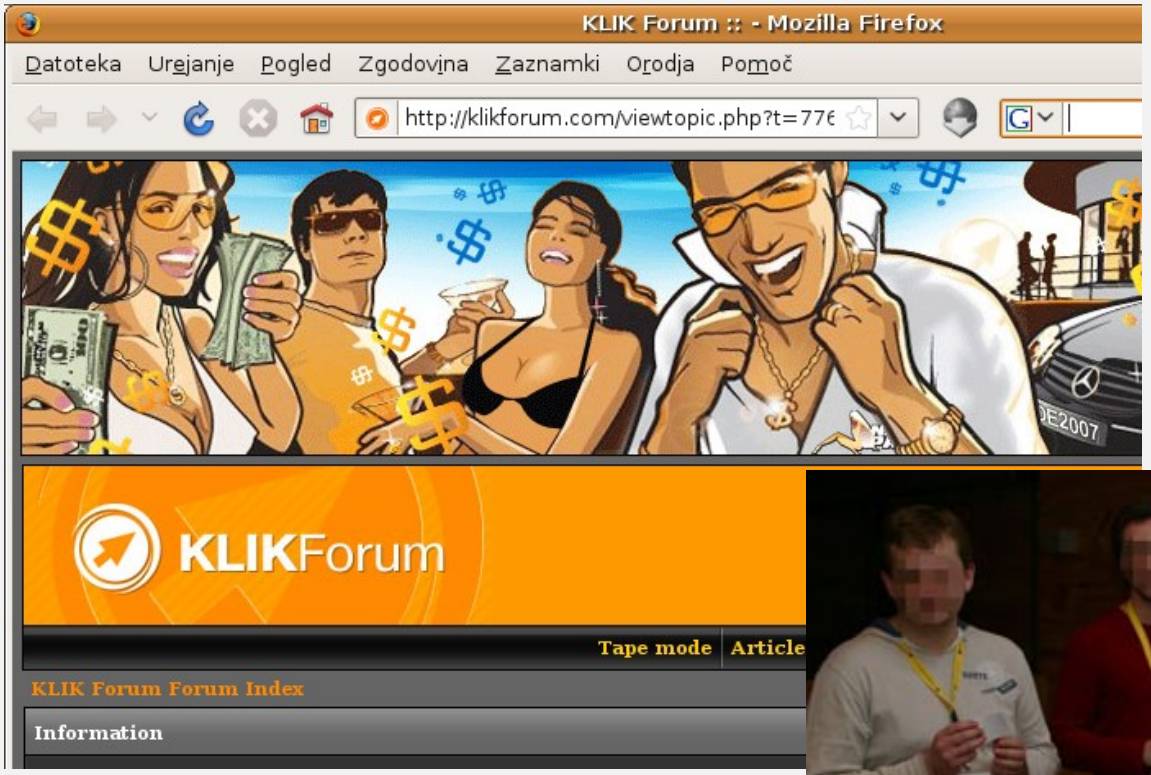
Izsiljevanje...

Kiberkriminal kot posel



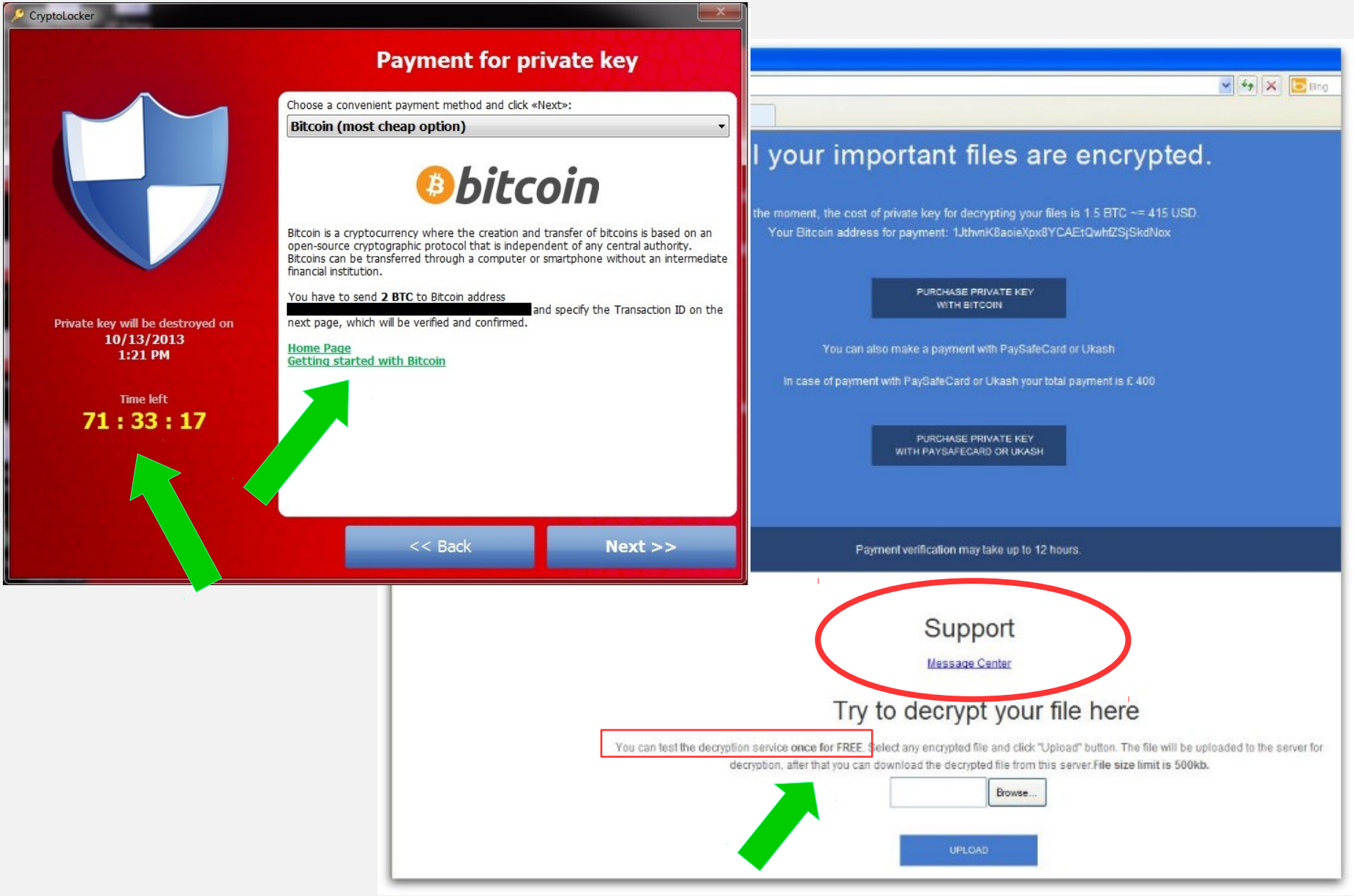
Ribarjenje (phishing), »pump-and-dump«.

Kiberkriminal kot posel



»Podjetje« KlikTeam, s 95 zaposlenimi leta 2006.

Kiberkriminal kot posel



Izsiljevalski virusi, vdori v kripto menjalnice.

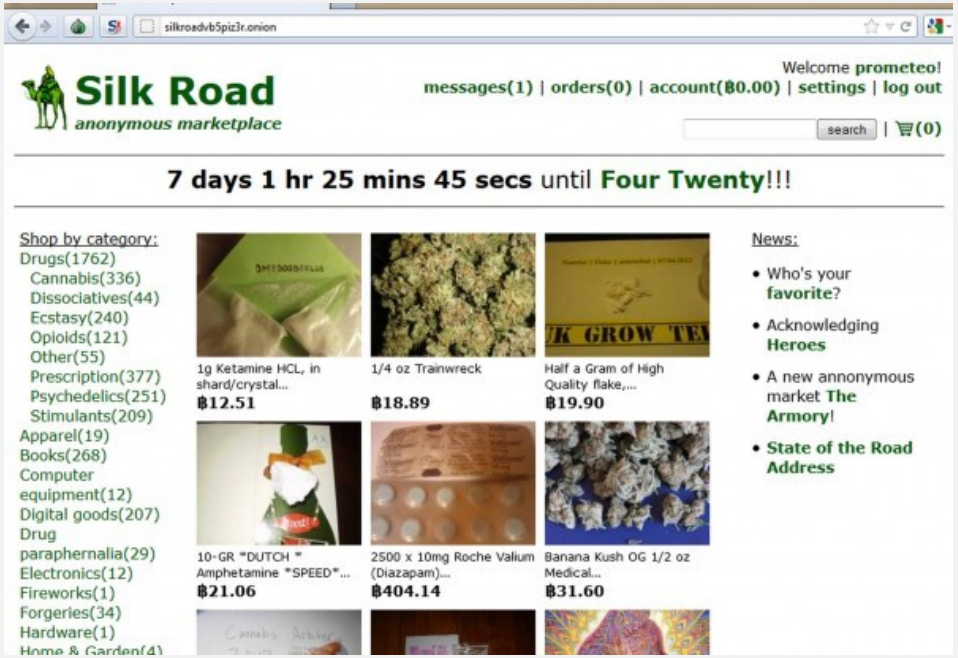
Kiberkriminal kot posel

- Leta 2009 je Wikileaks objavil anonimno pismo osebe, ki je 10 let delala v poslu z otroško pornografijo. Oseba je v pismu razkrila nekaj podatkov o tej »industriji«:
  - **Mesečni promet** enega izmed »podjetij«: **1,8 milijona USD** (na letni ravni okrog 21,6 milijona USD) - neobdavčeno.
  - Po odbitju vseh stroškov (za fotografe, iskalce gradiva po forumih, modele, spamerje, hekerje, itd.) **lastniku ostane okrog pol milijona USD - mesečno**.
  - **Problem marketinga**: odkrito oglaševanje ni mogoče. Marketing se zato izvaja s pomočjo spama (in preko vdorov na pornografske in druge spletne strani). Po navedbah anonimnega avtorja naj bi spamerji pobrali okrog 20 odstotkov vsega dobička.
  - **Skrivanje vsebine**: večina vsebin naj bi se nahajala na nemških strežnikih na šifriranih diskih. Strežniki niso neposredno dostopni, pač pa so dostopni preko posebnih posredniških strežnikov (tim. *proxy*), le-ti pa preko Fast Flux domen.
  - Ruske kriminalne združbe so namesto spletnih vsebin začele ponujati **virtualne stroje** s prednaloženo ilegalno vsebino ter celo **RDP dostop do strežnikov**.

Vir: https://wikileaks.org/wiki/My_life_in_child_porn

Kiberkriminal kot posel

- Spletišče *Silk Road* je od 6. februarja 2011 do 23. julija 2013 ustvarilo 1,2 milijarde USD prometa in 79,8 milijonov USD (neobdavčenega!) dobička.



- Silk Road je omogočal ocenjevanje prodajalcev, skrbel za anonimnost prodajalcev in kupcev, omogočal anonimno plačevanje z BitCoini, izvajali so tudi teste čistosti drog…

Kiberkriminal kot posel

- Po zaprtju Silk Road s strani FBI se je pojavilo še več podobnih strani. *Atlantis* in *Project Black Flag* sta kmalu po ustanovitvi ugasnila ter izginila z denarjem svojih strank.

Atlantis je ubral precej inovativen način oglaševanja [https://youtu.be/uD1y0kK_aH8]

Imunski sistem

Kiberkriminal kot imunski sistem

Na računalniška omrežja bi morda morali gledati kot na nekakšne **organizme z imunskimi sistemi**, za katere je značilno, da jih napadi bolezni krepijo.

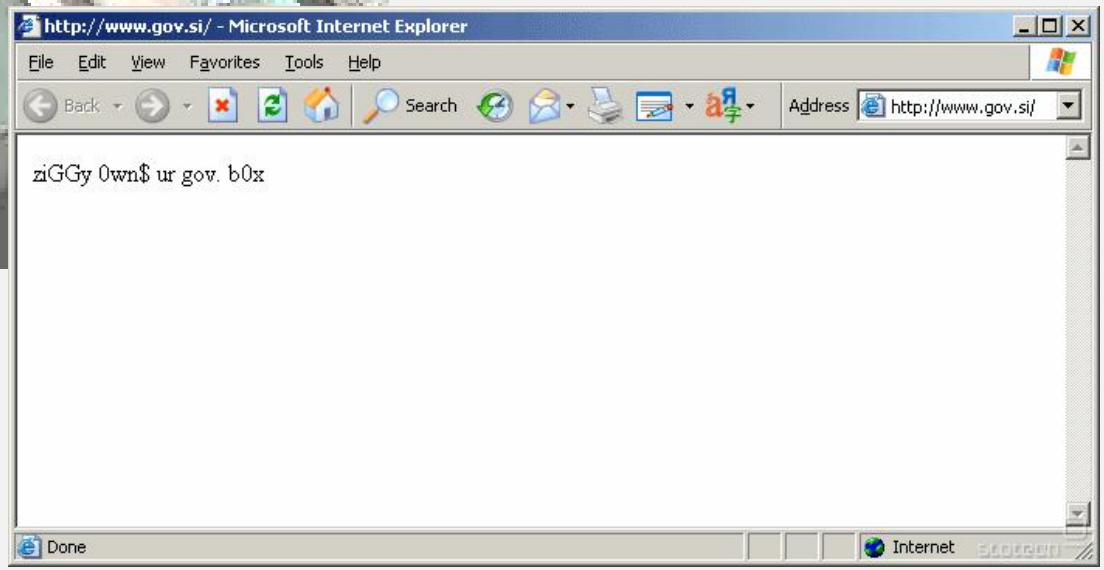
Odkrite in izrabljene varnostne ranljivosti imajo za posledico **reakcijo** – odpravo teh ranljivosti s strani proizvajalcev ter povišano varnostno kulturo uporabnikov.

To na nek način **krepi "imunski sistem" interneta** in zmanjšuje verjetnost, da bi nekoč prišlo do katastrofalnega napada, ki bi lahko ogrozil nacionalno ali celo globalno varnost.

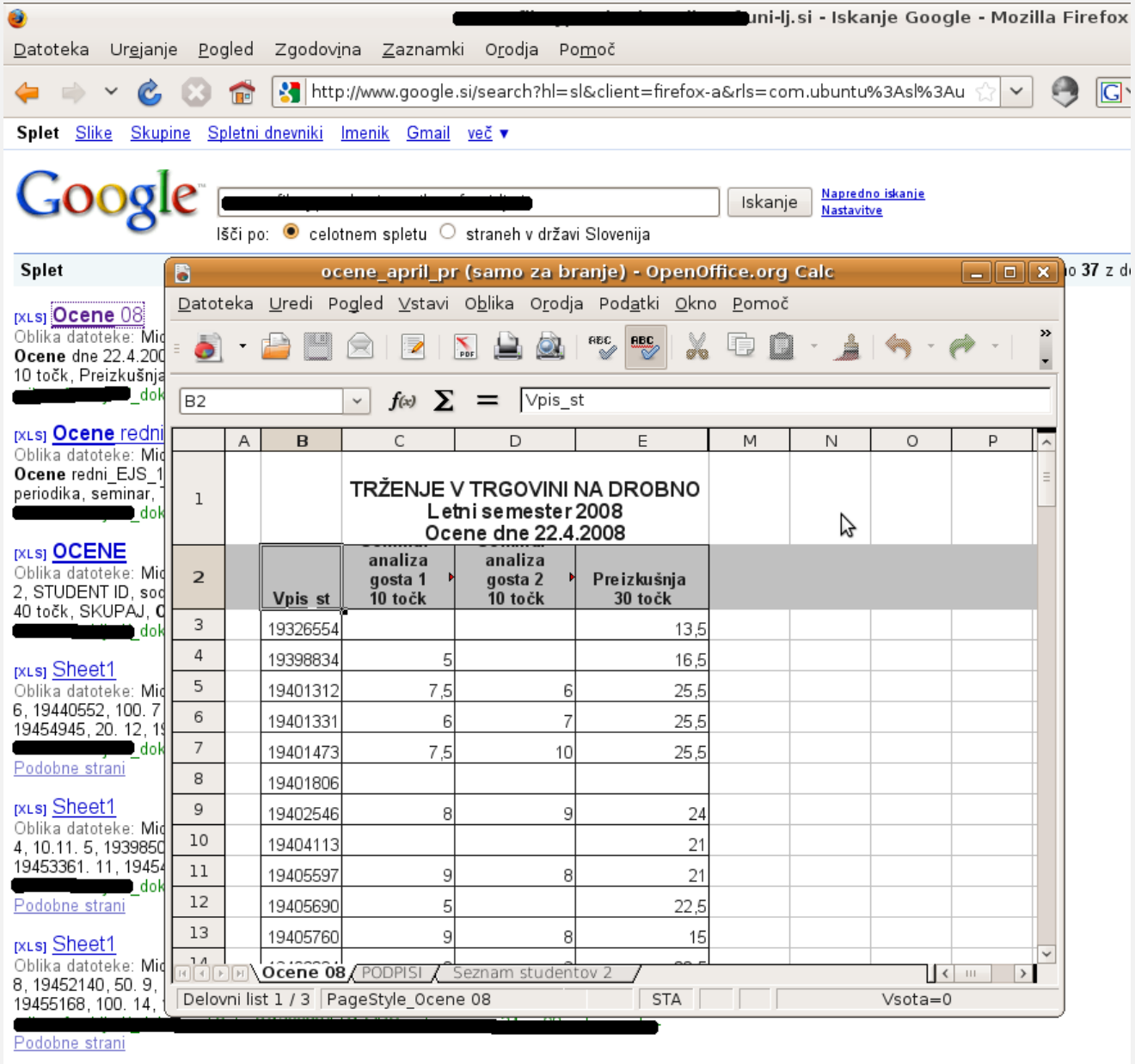
Kiberkriminal tako na nek način prinaša tudi koristi.

(Harward Law Review, 2006: 2442)

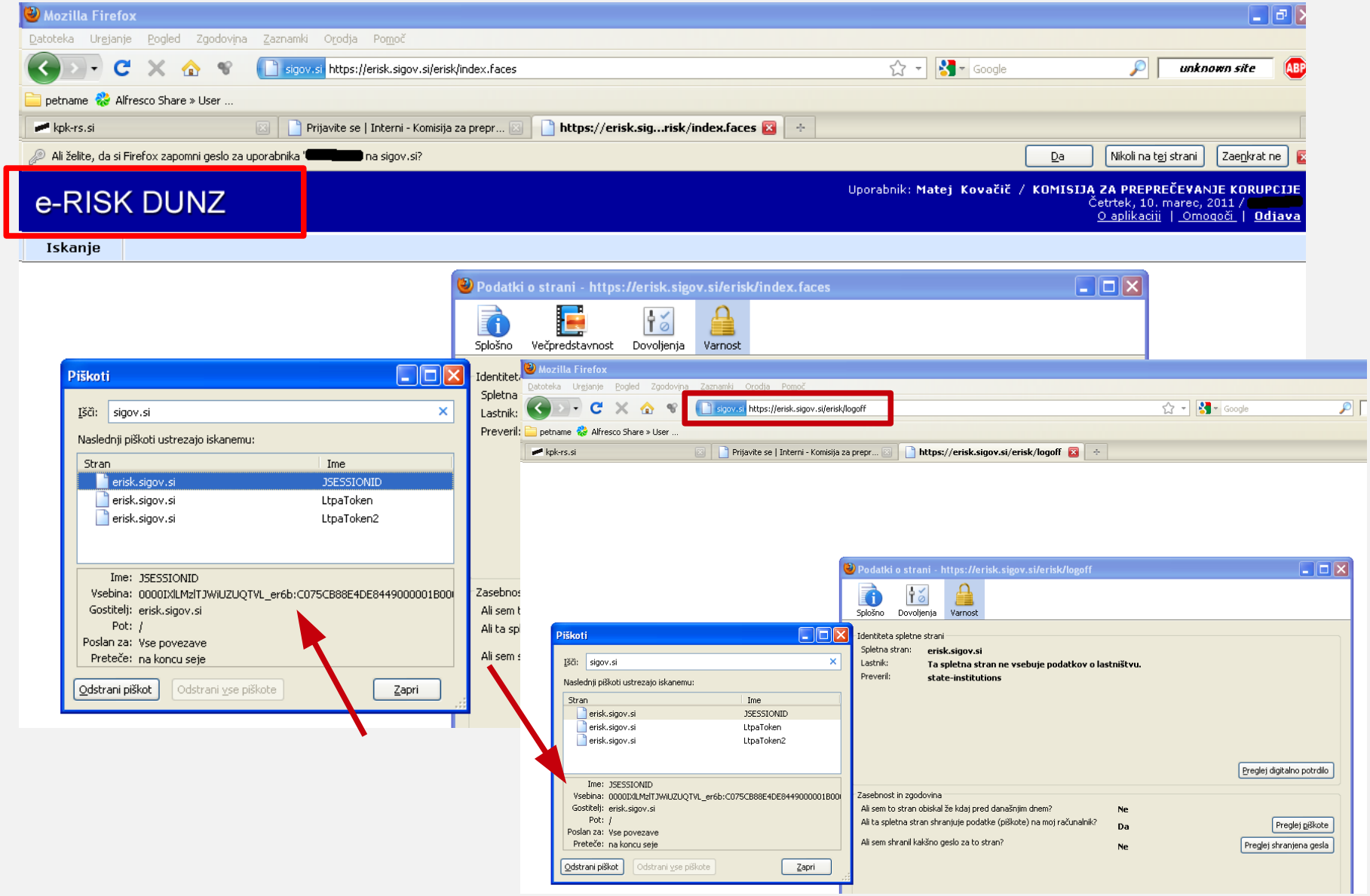
Kiberkriminal kot imunski sistem



Kiberkriminal kot imunski sistem



Kiberkriminal kot imunski sistem



Kiberkriminal kot imunski sistem

GSM modul za odpiranje garažnih ali vhodnih vrat

Ponujamo vam uporabno napravo, ki z enostavnim telefonskim klicem odpre ali zapre avtomatizirana garažna ali vhodna vrata.

GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z namenom, da s hitrim klicem odpre ali zapre avtomatizirana vrata. Naprava prepozna največ pet določenih telefonskih številk, iz katerih se lahko na GSM modul pokliče in se s takim klicem sproži odprtje ali zaprtje vrat.

IKU d.o.o. vam nudi:

- dobavo paketa z navodili za uporabo,
- montažo na dogovorjena mesta (pokličite nas in poslali vam bomo ponudbo).

Uporaba GSM modula za odpiranje vrat:

na avtomatizirana garažna, vhodna ali druga vrata se namesti GSM modul, v katerega se zapiše do pet telefonskih (mobilnih) številk, s katerimi je možno s hitrim telefonskim klicem omenjena vrata odpreti ali zapreti. S tem načinom odpade uporaba daljinskih upravljalnikov oziroma dodatnih naprav in aparatov, ker predpostavljamo, da je mobilni telefon že »obvezna oprema« vseh ljudi.

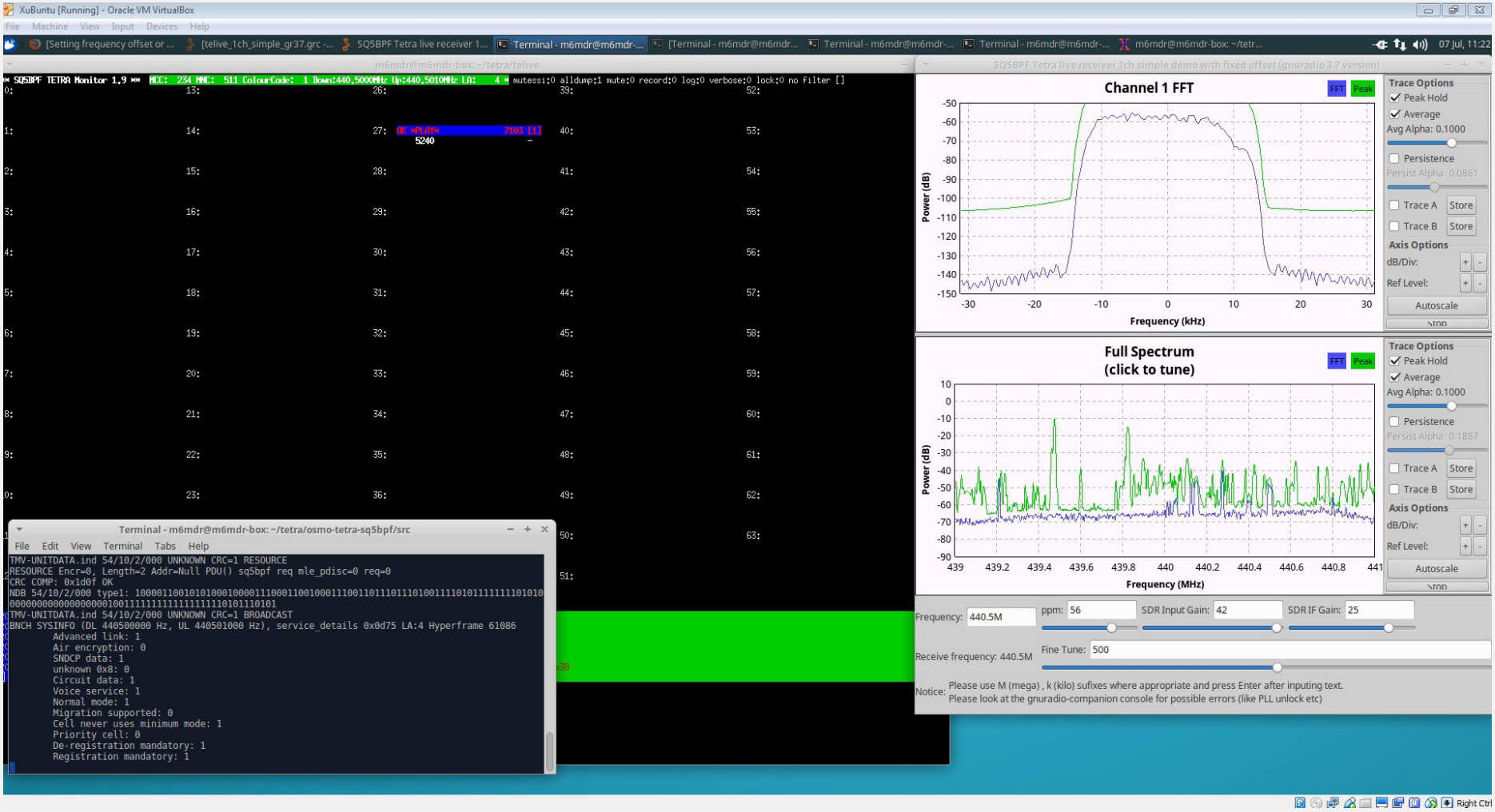


Kiberkriminal kot imunski sistem

Kiberkriminal kot imunski sistem

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
```

Kiberkriminal kot imunski sistem



Razkritje

Popolno razkritje

Full disclosure -- the practice of making the details of security vulnerabilities public -- is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure.

-- Bruce Schneier

Neodgovorno nerazkritje

Popolno razkritje varnostnih ranljivosti je glavni razlog zakaj proizvajalci oprema ali upravljavci varnostno posodabljajo svoje sisteme.

Za podjetja so varnostne ranljivosti **zunanji strošek**, saj precej močneje prizadenejo uporabnika kot proizvajalca. Zato podjetja varnostne ranljivosti razumejo bolj kot PR problem kakor pa problem programske kode.

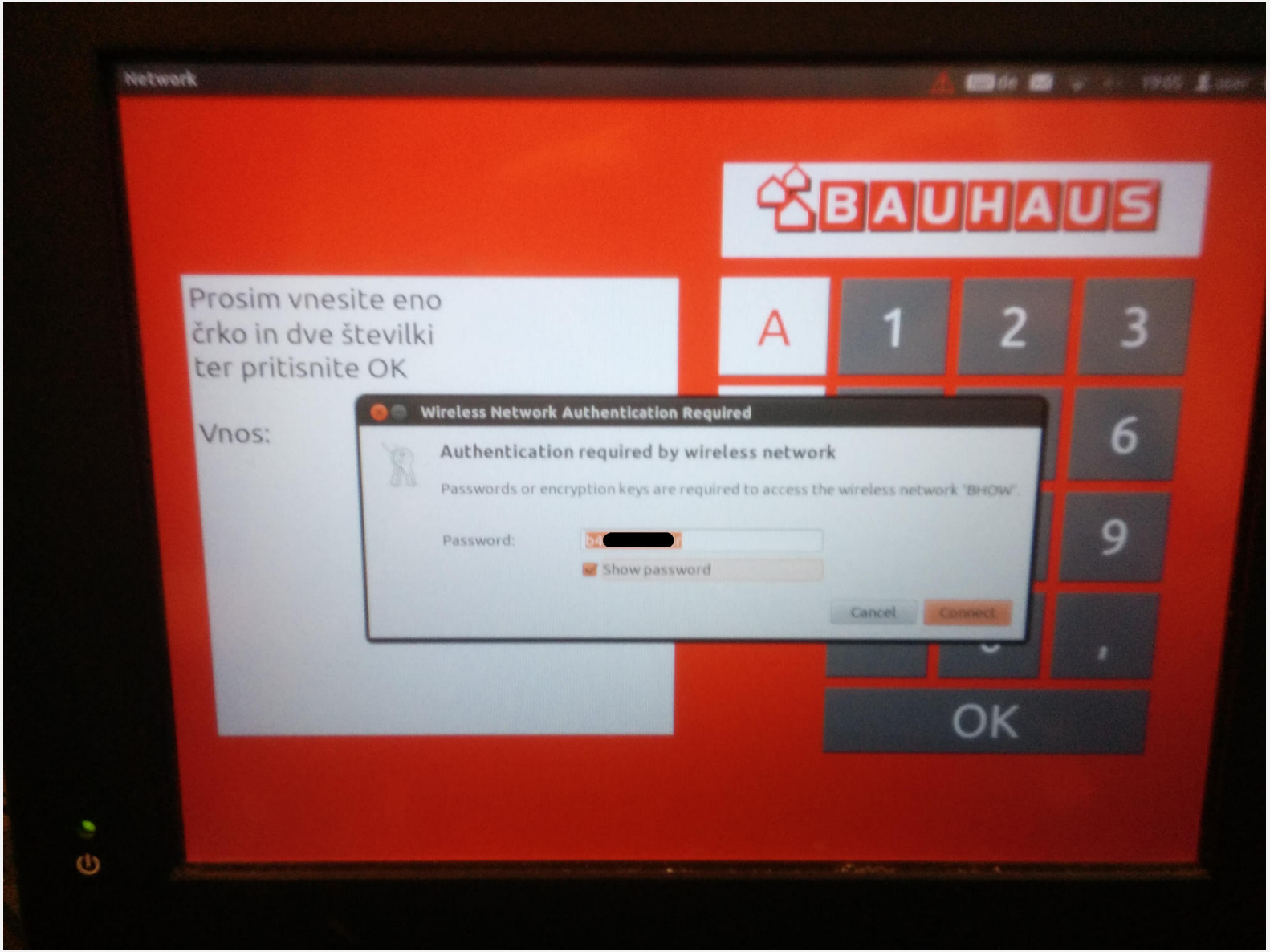
Neodgovorno nerazkritje

To pomeni, da morajo varnostni raziskovalci »povečati« PR problem, ki bolj neposredno prizadene podjetje in poveča njegovo motivacijo za odpravo ranljivosti.

Popolno razkritje torej poveča PR problem in ustvari pritisk na proizvajalca, da sistem popravi in izboljša.

Neodgovorno nerazkrivanje, po drugi strani bolj spodbuja kulturo skrivaštva in pometanja pod preprogo.

Odgovorno razkritje



10. avgust 2017 – 28. avgust 2017.


Vprašanja?
https://telefoncek.si