

Kiberkriminal



Magija, radovednost, zabava, posel in imunski sistem interneta

Matej Kovačič
(CC) 2018

<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.

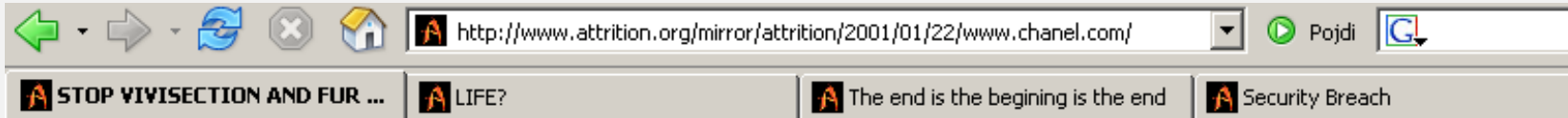
Skriptarji (ang. *script kiddies*) so osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi. Motivi so večinoma samodokazovanje, zabava ali vandalizem.

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



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

```
1. -----
2. 01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
3. 01101110 01000111 01101100 01101111 01100010 01100001 01101100
4. 01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
5. -----
6.
7. / \ _ _ _ _ _ | | ( ) _ _ _ / \ | | | | | _ | |
8. | ( ) | ' \ / - ) ' / \ | | / \ \ / \ / \ / \ | |
9. \ / | . \ / \ | | \ / \ / \ / \ | | \ / \ / . \ / \ | |
10. | |
11. _ _ _ _ _
12. | _ ) | _ _ _ | | _ _ _ | | |
13. | _ \ / \ / \ / \ / \ | | | |
14. | _ \ / \ / \ / \ / \ | |
15.
16. -----
17. 01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
18. 01101110 01000111 01101100 01101111 01100010 01100001 01101100
19. 01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
20. -----
```



Kiberterrorizem in kibersabotaža

Kiberterrorizem 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 Ohio leta 2003.

Kiberterrorizem in kibersabotaža

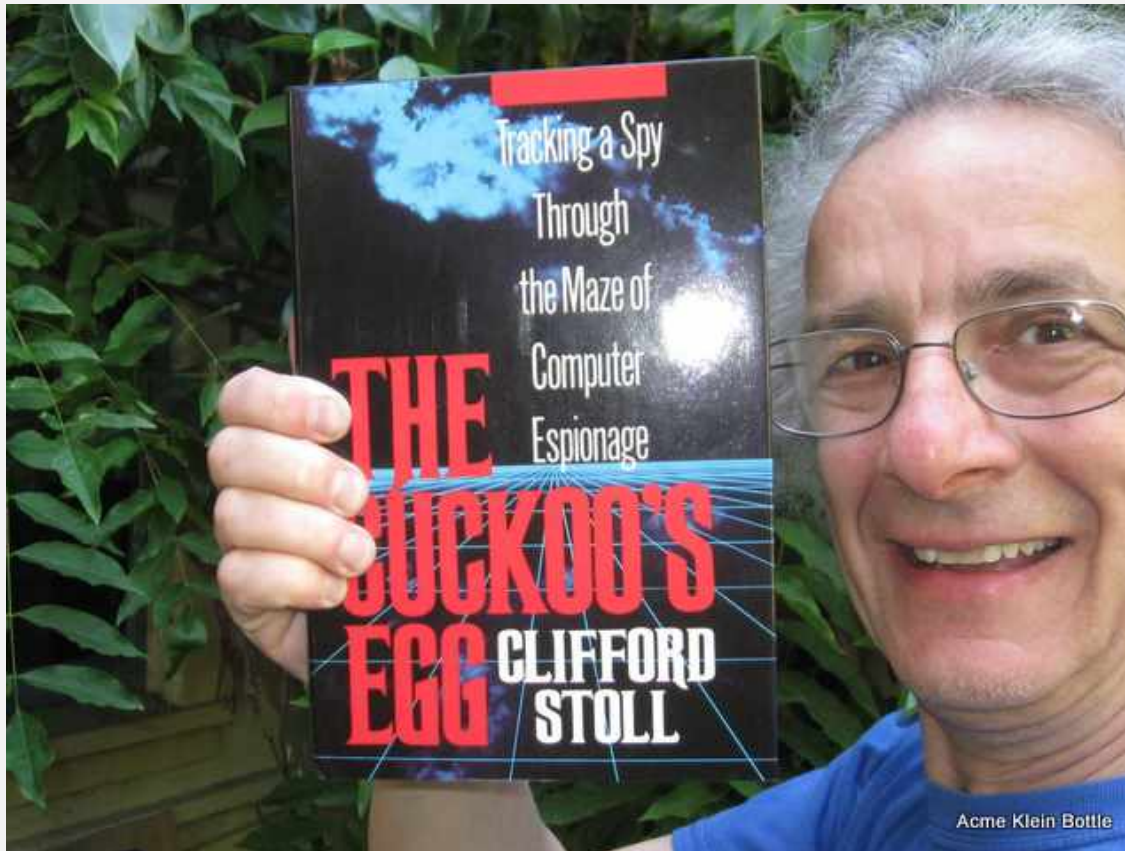
Primeri:

- 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 kibernetične 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

Zmoglјivostі kibernetiskih napadov kot sredstvo odvraćanja kibernetiskih napadov:

»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



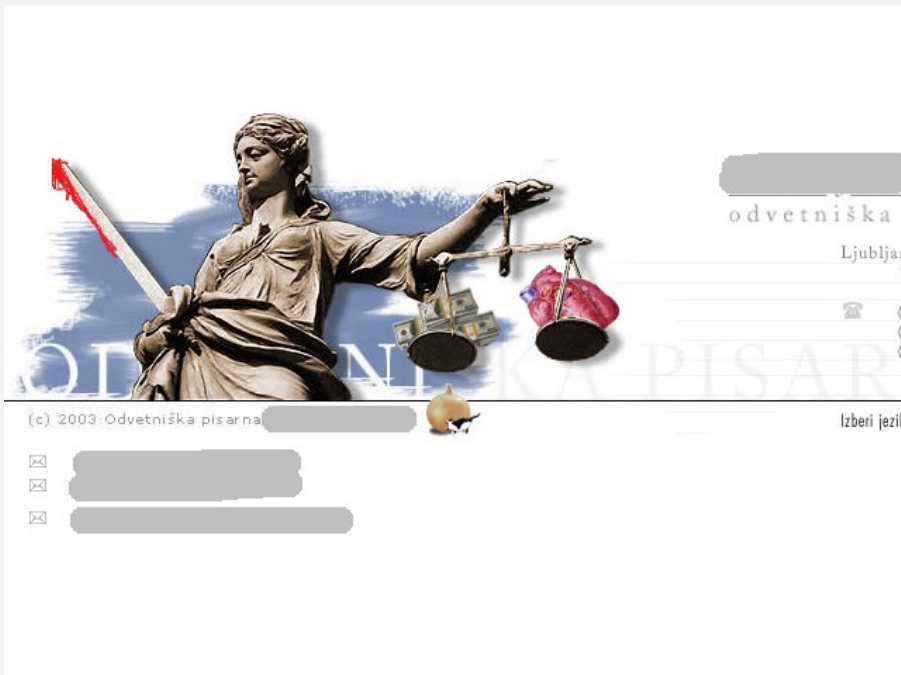
Radovednost in zabava

Kiberkriminal kot zabava



Hekerski napad na tiskalnik.

Kiberkriminal kot zabava



Razobličena spletna stran odvetniške pisarne (okrog 2003).

Slovensko satanistično gibanje

Pavlihove domače strani na internetu: [Prva stran](#) | [Aktualno](#) | [Povezave](#)

Slovensko satanistično gibanje se predstavi

NAMEN

- *Slovensko biblično gibanje* si prizadeva po besedah 2. vatikanskega cerkvenega zbora v dogmatični konstituciji *O Božjem razodetju* (22), da bi bil "na široko odprt dostop do Svetega pisma".
- Zato hočemo *Sveto pismo* vsem ljudem predstaviti, ponuditi, posebej vernim pa pomagati, da ga bodo mogli zavestno sprejemati kot Božjo besedo znotraj živega izročila celotne Cerkve.

NALOGE

- povezovati svetopisemske ali biblične skupine,
- spodbujati nastajanje novih in jim pomagati pri delu
- prirejati biblične tečaje, razstave, predavanja

Razobličenje spletne strani rimokatoliške cerkve (leto 2001).


Kiberkriminal kot zabava



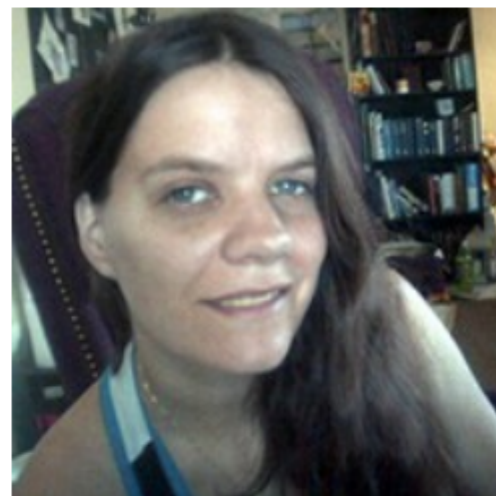
Hekerski napad na prometne znake.

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 grievers (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

The screenshot shows a Mozilla Firefox browser window displaying the search results for 'Dimitrij Rupel postal svetovalec' on the Si.mobil website. The browser's address bar shows the URL: <http://www.simobil.si/sl/search.cp2?q=<h3>Dimitrij+Rupel+postal+svetovalec+>. The website header includes the Si.mobil logo and navigation links such as 'Prodajna mesta', 'Vprašajte nas', 'Registrirajte se', and 'English'. A search bar contains the query '<h3>Dimitrij Rupel postal' with an 'IŠČI' button. Below the search bar, there are menu items: 'TELEFONI IN NAPRAVE', 'PAKETI', 'STORITVE', 'AKCIJE', 'TUJINA', 'POMOČ IN INFORMACIJE', 'VODAFONE LIVE!', and 'SI.MOST'. The search results are displayed under the heading 'Rezultati iskanja'. The first result is for 'Dimitrij Rupel postal svetovalec uprave Simobila', accompanied by a portrait photo of a man in a suit. The text below the photo reads: 'Z današnjim dnem dr. Dimitrij Rupel postaja svetovalec Simobila za področje zunanje naročniške politike.' Below this, there is a smiley face ':-)'. The second result is 'IT specialist v CRM skupini, zadolžen za DMS področje (m/ž)', with a short description: 'Želite razvijati svojo profesionalno pot pri enem najuglednejših in najboljših slovenskih zaposlovalcev? Podjetje Si.mobil d.d. je zaupanja vredno podjetje, kjer so ljudje na prvem mestu. Zaposleni v Si.mobilu so visoko usposobljeni profesionalci, ki so zaljubljeni v svoje delo in v komunikacijo. Prek vpetosti v globalne povezave pa zaposleni lahko pridobivajo tudi mednarodno znanje in bogate izkušnje.' The third result is 'Novi direktor prodaje', with the text: 'Novi direktor prodaje v družbi Si.mobil je s 3. januarjem 2007 postal Gregor Banič.' The fourth result is 'Nastavitve zunanjega odjemalca'. At the bottom of the search results, it says 'Število vseh rezultatov: 3', 'Prikazani rezultati: 1 - 3', and 'Stran: 1'. The browser's status bar at the bottom shows 'Končano', 'Apache', '1337', and 'Anonimizacija izključena'. The taskbar at the very bottom shows various application icons and the system clock: 'pet 16. jan, 10:28'.

»Prvi april«.

Kiberkriminal kot radovednost

prevzem.php5 (Predmet application/pdf) - Mozilla Firefox

Datoteka Urjanje Pogled Pojdi Zaznamki Orodja Pomoč

http://lgl.esiti.com/si/prevzem.php?id=24400

LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA

potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu

Lutkovno gledališče Ljubljana

VILA MALINA, izven
LGL-Veliki oder, 11. januar 2007 ob 17:00

segment	vrsta	Številka	količina	cena
Veliki oder	6	7b	1	3,24 EUR
Veliki oder	6	7a	1	3,24 EUR
Veliki oder	6	6b	1	3,24 EUR
Veliki oder	6	6a	1	3,24 EUR
skupaj				12,96 EUR 3.105,73 SIT

številka potrdila o nakupu
010-000-107-788-454-883-142760

Vaše potrdilo o nakupu zamenjajte za vstopnice na blagajni dvorane.

V primeru, da prireditev odpade, lahko potrdilo o nakupu zamenjate na blagajni organizatorja za drugo prireditev ali pa vam organizator vrne denar, ki ga morate prevzeti v enem mesecu na njegovi blagajni. Za vse dodatne informacije nam pišite na elektronski naslov info@lgl.si.

Končano Anonimizacija izključena

»Igranje« z URL naslovi...

Kiberkriminal kot radovednost

The screenshot shows a Mozilla Firefox browser window displaying the Sparkasse website. The address bar shows the URL `https://netstik.sparkasse.si/eb/index.asp`. A pop-up window is open, showing the details of a MasterCard account. The URL in the pop-up window's address bar is `https://netstik.sparkasse.si/eb/kartica.asp?x=...&y=...&z=...&q=...&k=...&s=...`, with the URL highlighted by a yellow circle. The pop-up window contains the following information:

MasterCard kartični račun: [redacted]

Uporabnik:	[redacted]n
Vrsta kartice:	primarna kartica na kartičnem računu
Številka kartice:	5209 [redacted]
Veljavnost do:	[redacted]-12
Naziv na kartici:	[redacted]
Datum otvoritve kartice:	[redacted] 2006
Datum blokacije:	/
Mesečni limit (nakup):	[redacted] EUR
Mesečni limit (dvig gotovine):	[redacted] EUR

Za preklic kartice, prosimo, pokličite 01/583 41 83.

© 2002-2009, BANKA SPARKASSE d.d. Pravica do napak in sprememb pridržana.

»Igranje« z URL naslovi v spletni banki.

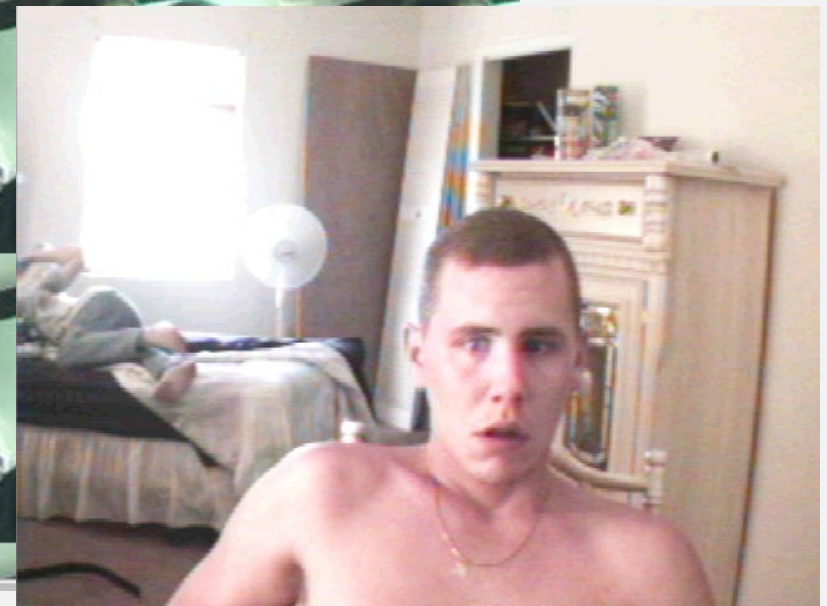
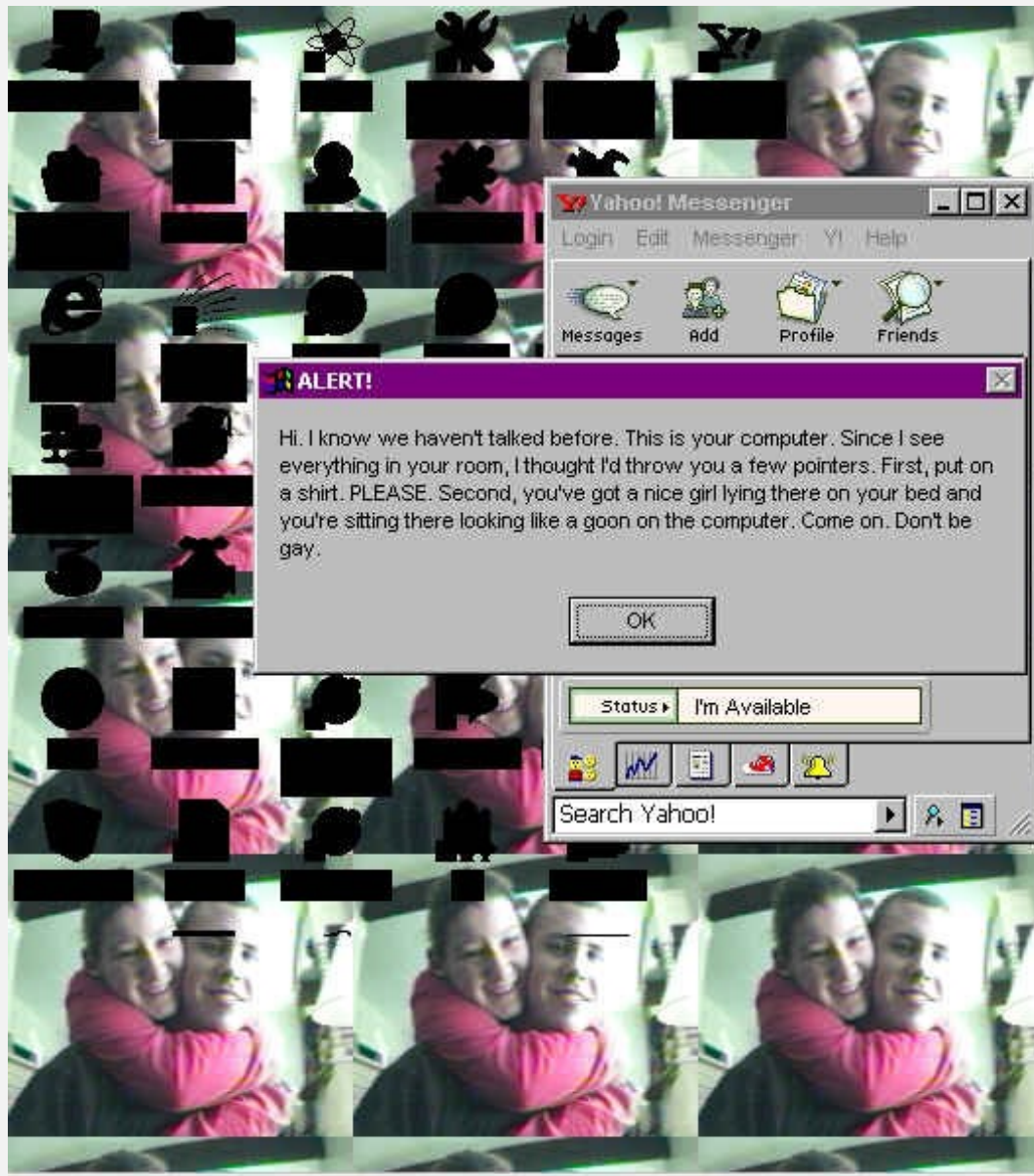
Pose1

Kiberkriminal kot posej



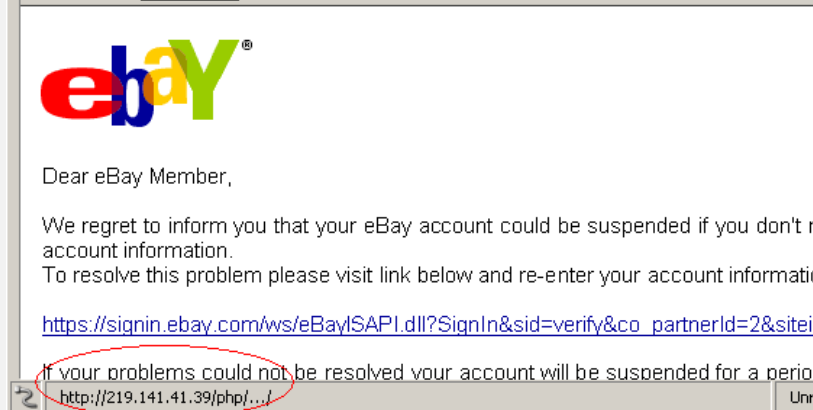
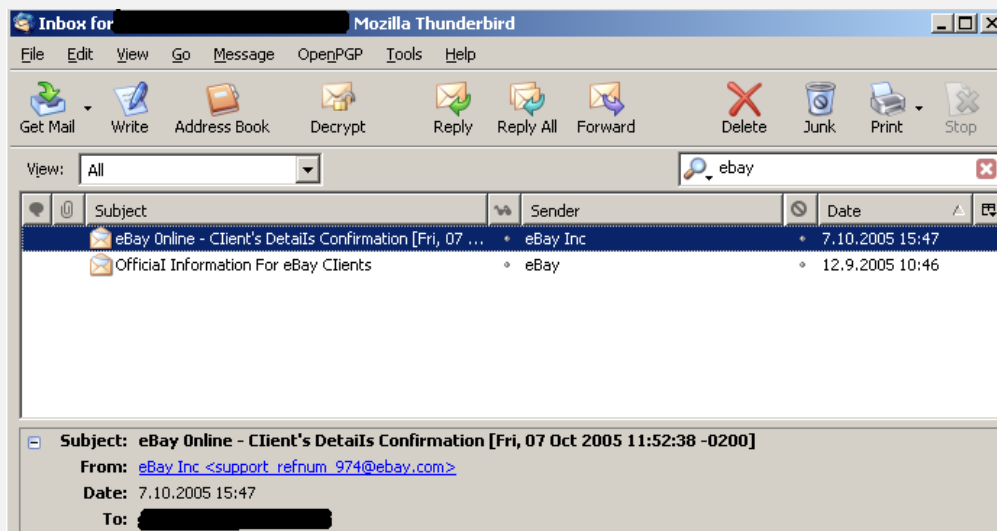
Vladimir Leonidovič Levin je leta 1994 vdrl v Citibank in ukradel 10,7 milijona USD.

Kiberkriminal kot pose1



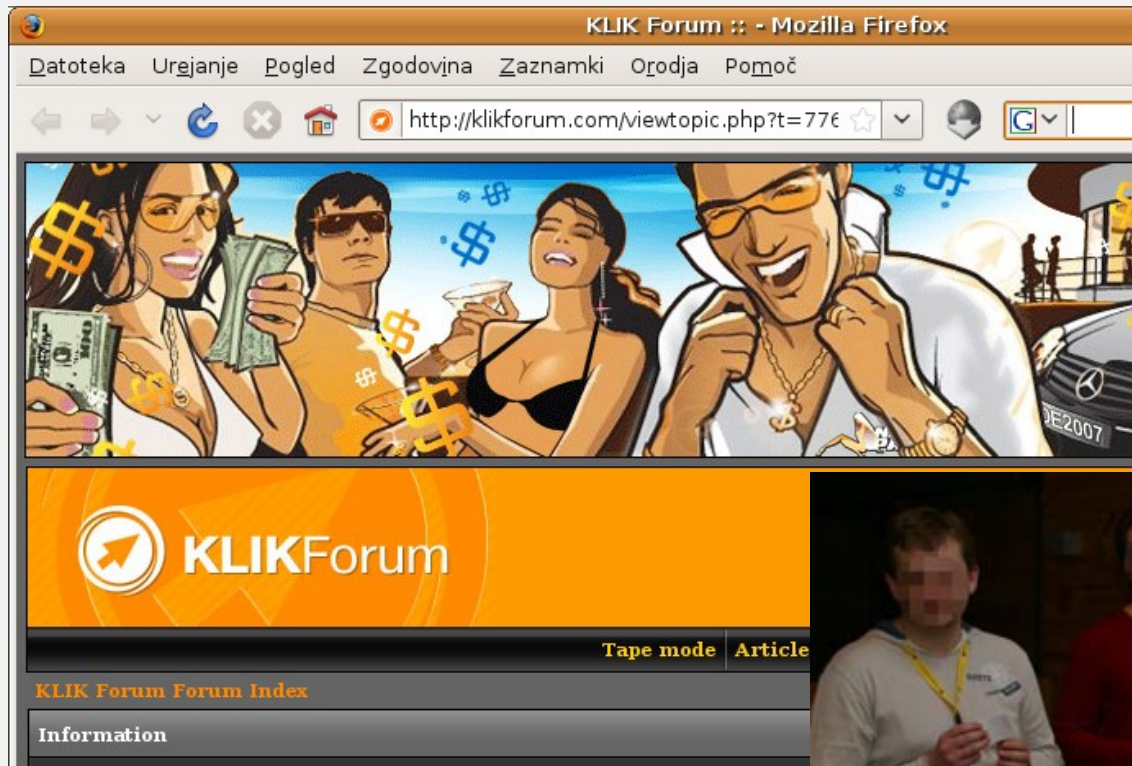
Izsiljevanje...

Kiberkriminal kot posel



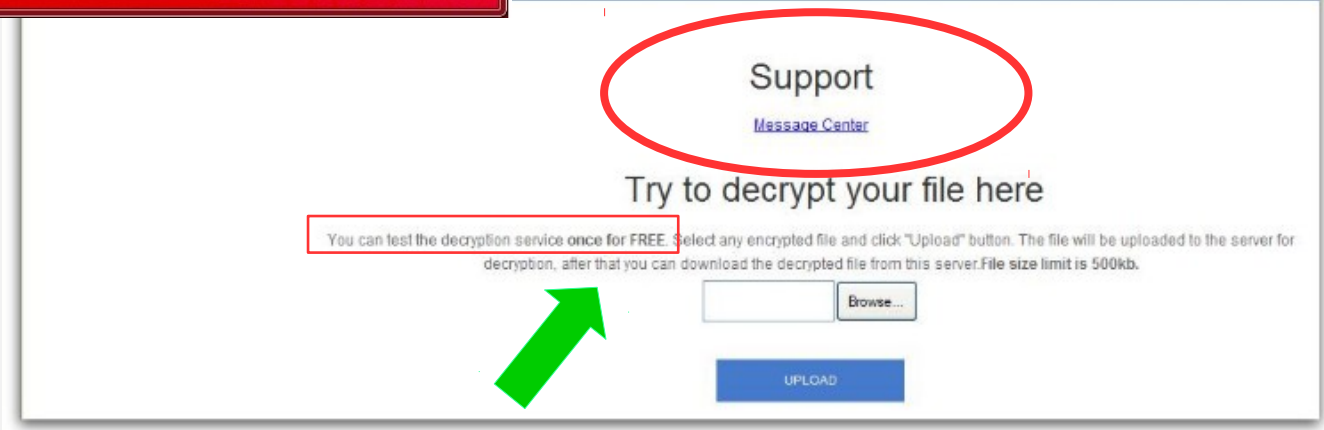
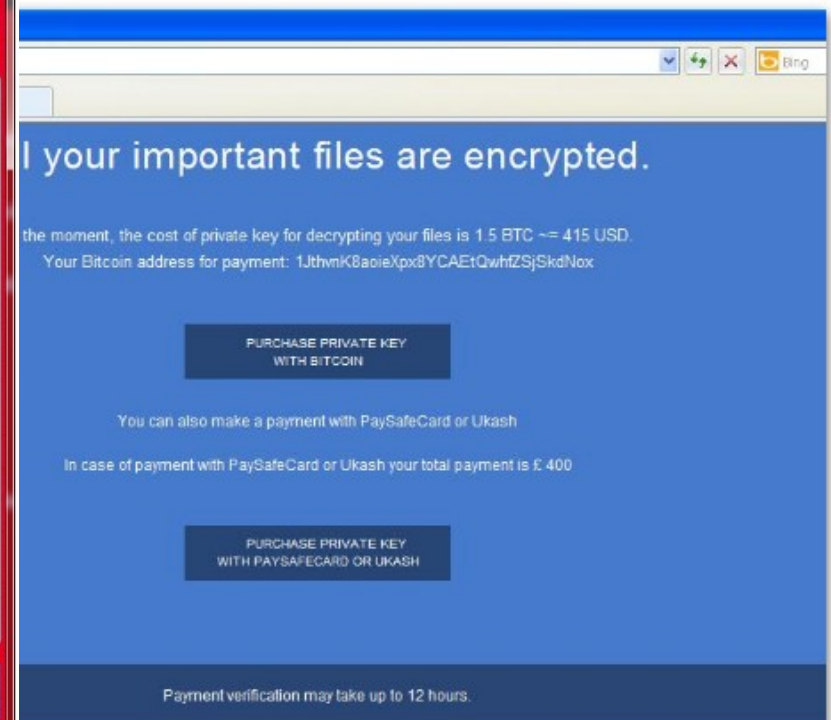
Ribarjenje (phishing), »pump-and-dump«.

Kiberkriminal kot posel



»Podjetje« KlikTeam, s 95 zaposlenimi leta 2006.

Kiberkriminal kot posel



Izsiljevalski virusi, vdori v kripto menjalnice.

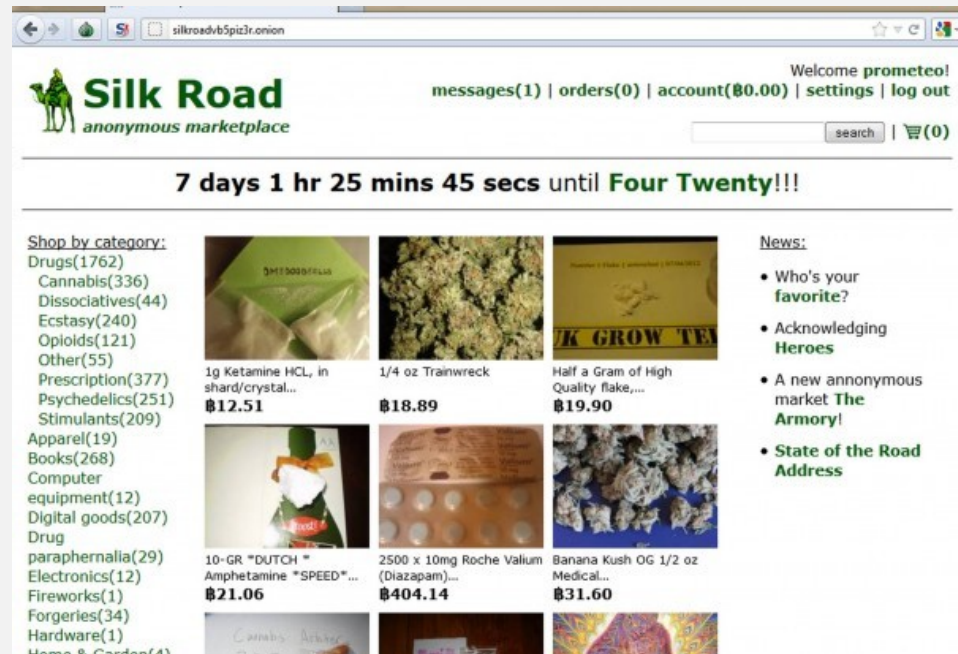
Kiberkriminal kot posel

- 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.

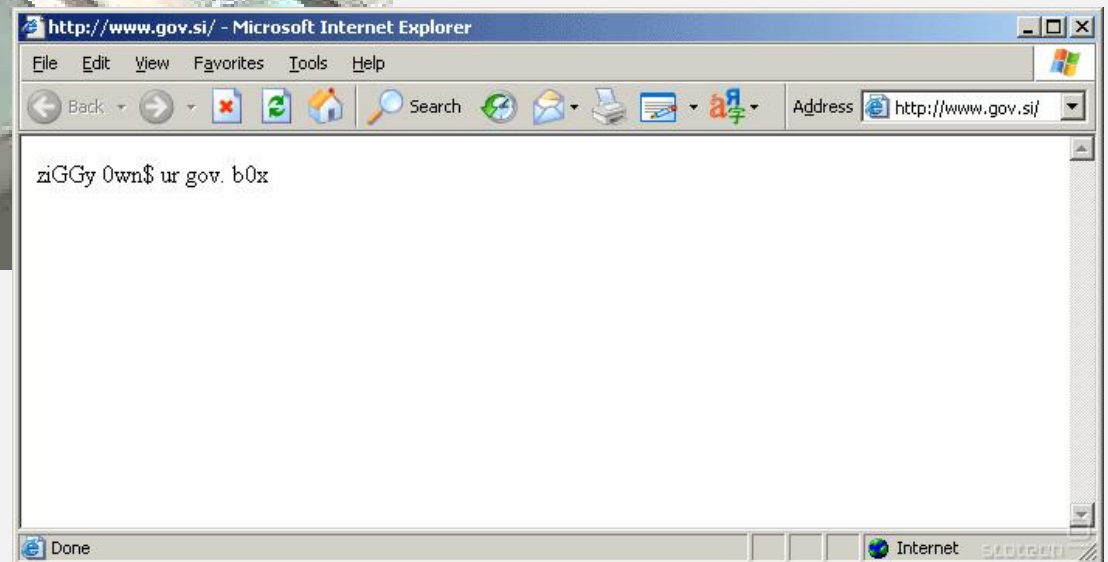
Odkrite in izrabljene varnostne ranljivosti imajo za posledico **reakcijo** - odpravo teh ranljivosti s strani proizvajalcev ter povišano varnostno kulturo uporabnikov.

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.

(Harvard Law Review, 2006: 2442)

Kiberkriminal kot imunski sistem



Kiberkriminal kot imunski sistem

The image shows a Mozilla Firefox browser window displaying the website <https://erisk.sigov.si/erisk/index.faces>. The browser's address bar and tabs are visible. A blue banner at the top of the page contains the text "e-RISK DUNZ" in white, which is highlighted with a red box. To the right of the banner, it says "Uporabnik: Matej Kovačič / KOMISIJA ZA PREPREČEVANJE KORUPCIJE" and "Četrtek, 10. marec, 2011".

Below the browser window, there are three overlapping windows:

- Podatki o strani - https://erisk.sigov.si/erisk/index.faces**: A window showing site information, including "Splošno", "Večpredstavnost", "Dovoljenja", and "Varnost".
- Piškotki**: A window showing cookies for "sigov.si". It lists cookies for "erisk.sigov.si" with names "JSESSIONID", "LtpaToken", and "LtpaToken2". Below the list, it shows details for the "JSESSIONID" cookie, including its value: "0000IXLMzITJWUZUQTVL_er6b:C075CB88E4DE844900001B00". A red arrow points from this window to the "Zasebnost" window.
- Zasebnost**: A window showing privacy settings. It includes a "Piškotki" window (highlighted with a red box) and a "Zasebnost in zgodovina" section with several questions and answers. A red arrow points from the "Piškotki" window to this section.

The "Zasebnost in zgodovina" section contains the following text and options:

- Ali sem to stran obiskal že kdaj pred današnjim dnem? Ne
- Ali ta spletna stran shranjuje podatke (piškote) na moj računalnik? Da
- Ali sem shranil kakšno geslo za to stran? Ne

Buttons for "Preglej digitalno potrdilo", "Preglej piškote", and "Preglej shranjena gesla" are visible at the bottom of the privacy window.

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 števil, 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) števil, 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

The screenshot displays a virtual machine environment with the following components:

- Terminal Window (Left):** Shows network traffic analysis. A green bar highlights a packet with the following details:
 - TMV-UNITDATA.ind 54/10/2/000 UNKNOWN CRC=1 RESOURCE
 - RESOURCE Encr=0, Length=2 Addr=NULL PDU() sq5bpf req mle_pdisc=0 req=0
 - CRC COMP: 0xid0f OK
 - NDB 54/10/2/000 type1: 1000011001010100010000111000110010001100110110110100111110111111101010
 - 000000000000000000010011111111111110101110101
 - TMV-UNITDATA.ind 54/10/2/000 UNKNOWN CRC=1 BROADCAST
 - BNCH SYSINFO (DL 440500000 Hz, UL 440501000 Hz), service_details 0x0d75 LA:4 Hyperframe 61086
 - Advanced link: 1
 - Air encryption: 0
 - SNDP data: 1
 - unknown 0x0: 0
 - Circuit data: 1
 - Voice service: 1
 - Normal mode: 1
 - Migration supported: 0
 - Cell never uses minimum mode: 1
 - Priority cell: 0
 - De-registration mandatory: 1
 - Registration mandatory: 1
- Channel 1 FFT Graph (Top Right):** Shows Power (dB) vs Frequency (kHz). The x-axis ranges from -30 to 30 kHz, and the y-axis ranges from -150 to -50 dB. A prominent signal is visible between -10 and 10 kHz.
- Full Spectrum Graph (Bottom Right):** Shows Power (dB) vs Frequency (MHz). The x-axis ranges from 439 to 441 MHz, and the y-axis ranges from -90 to 10 dB. Multiple peaks are visible across the frequency range.
- Control Panel (Bottom Right):** Includes sliders for Frequency (440.5M), ppm (56), SDR Input Gain (42), SDR IF Gain (25), and Receive frequency (440.5M). A Fine Tune slider is set to 500.

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 posodablajo svoje sisteme.

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

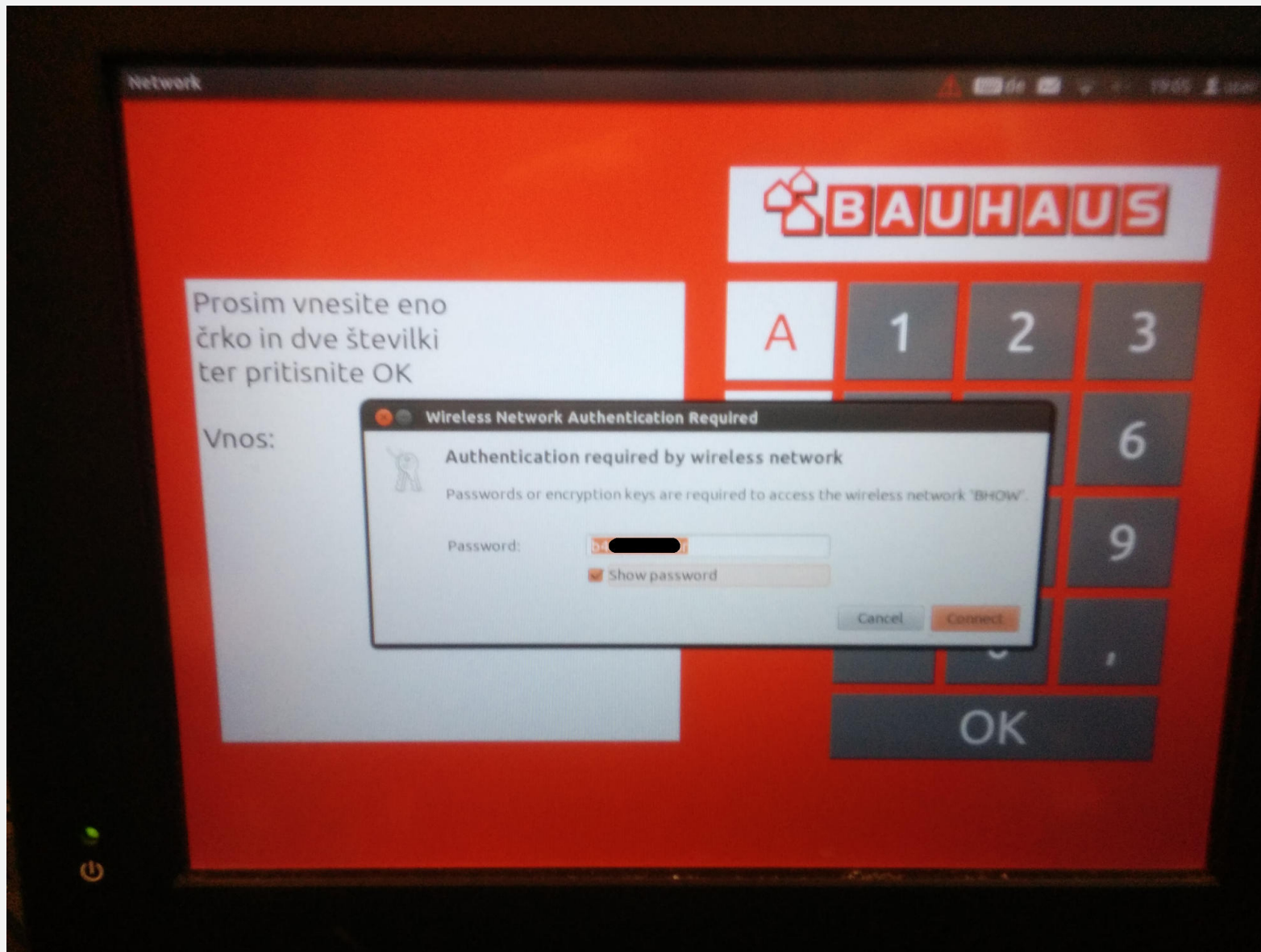
Neodgovorno nerazkritje

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>