Napadi na informacijske sisteme (in ljudi)

Matej Kovačič
https://telefoncek.si

Varnost ni izdelek

Varnost ni izdelek oziroma nekaj, kar lahko kupimo, namestimo in pozabimo, pač pa gre za proces.

Varnostno kulturo je treba razvijati in gojiti neprestano.

Informacijska varnost in varnost v prometu: ni dovolj samo dober avto in opravljen izpit, znanje o varnosti je potrebno obnavljati in uporabljati neprestano.

Napadi na informacijske sisteme...

...in ljudi!

Napadi, ki zahtevajo fizični dostop do sistema.

Omrežni napadi (napadi na komunikacije ter napadi na »virtualni prostor«).

Zbiranje različnih (javno objavljenih) informacij na internetu.

Posredni napadi - napadi na uporabnika (socialni inženiring, prevare).

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.

»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.*".

Kiberkriminal

Včasih:

- raziskovanje,
- radovednost,
- samodokazovanje,
- zabava,
- vandalizem,...

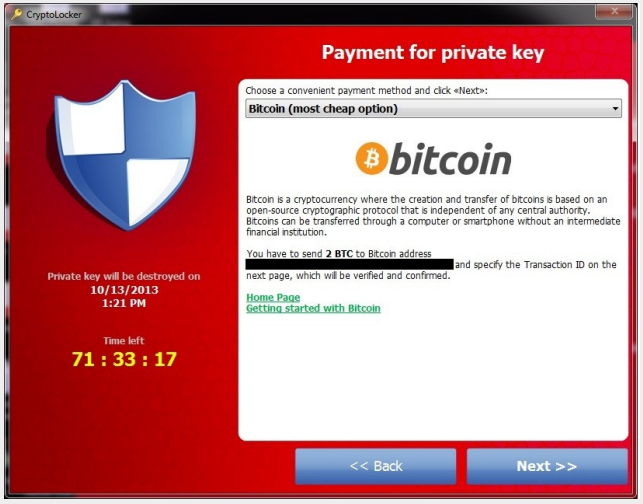
Kiberkriminal

Danes:

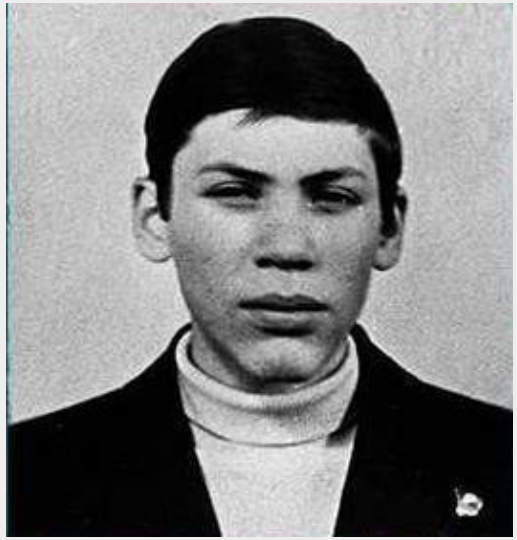
- posel in denar!

Spletna stran "podjetja".

Zabava 95 zaposlenih v ruskem podjetju *Klik team* v Črni gori, februar 2008.



Šifrirno-izsiljevalski virus Cryptolocker.



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

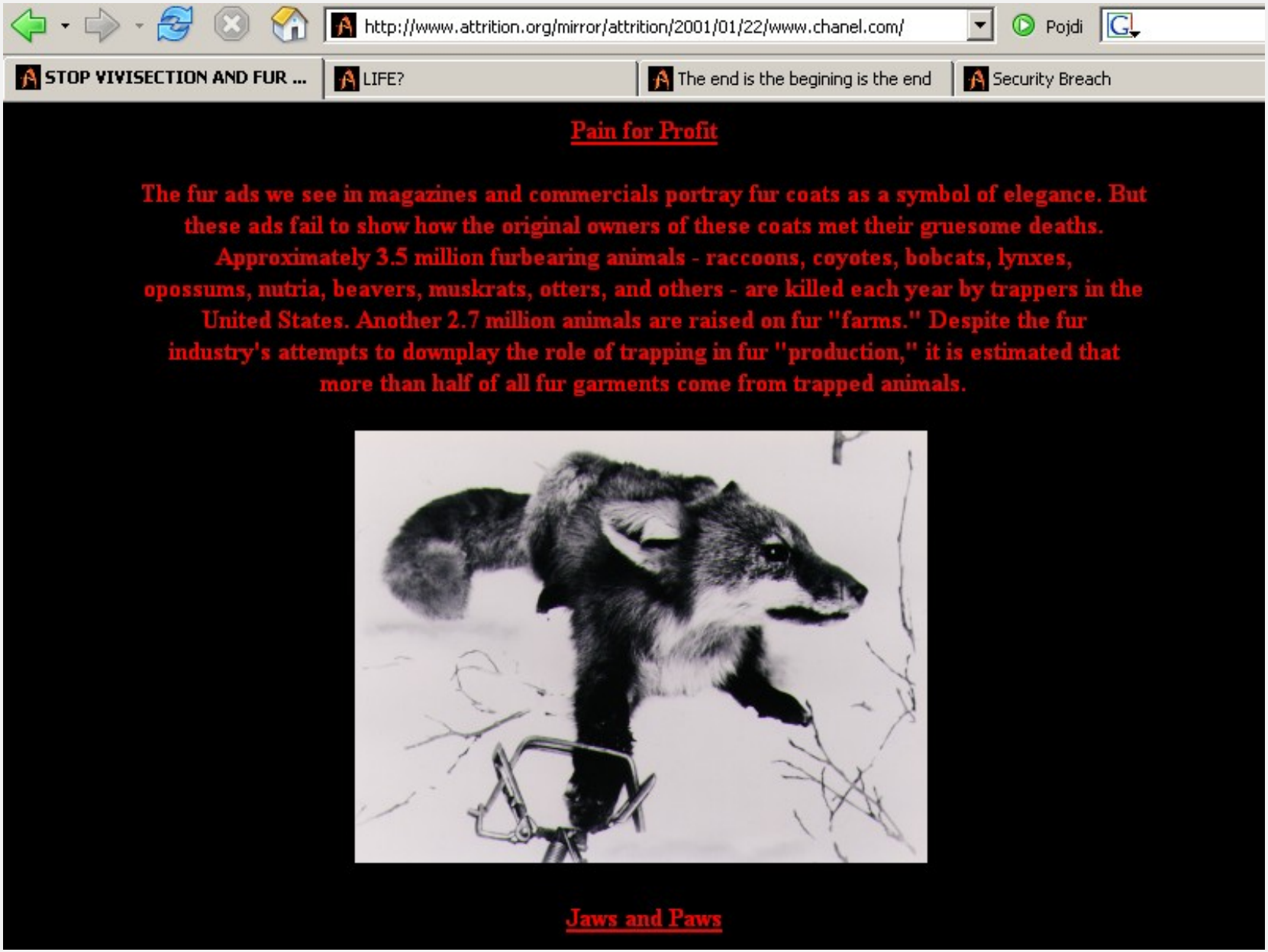
»Etično hekanje«

Informacijski sistemi kot organizmi z imunskimi sistemi.

Odkrivanje varnostnih ranljivosti ima za posledico njihovo odpravo ter povišano varnostno kulturo uporabnikov.

Etično hekanje krepi »imunski sistem« interneta in zmanjšuje verjetnost, da bi nekoč prišlo do katastrofalnega napada.

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

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

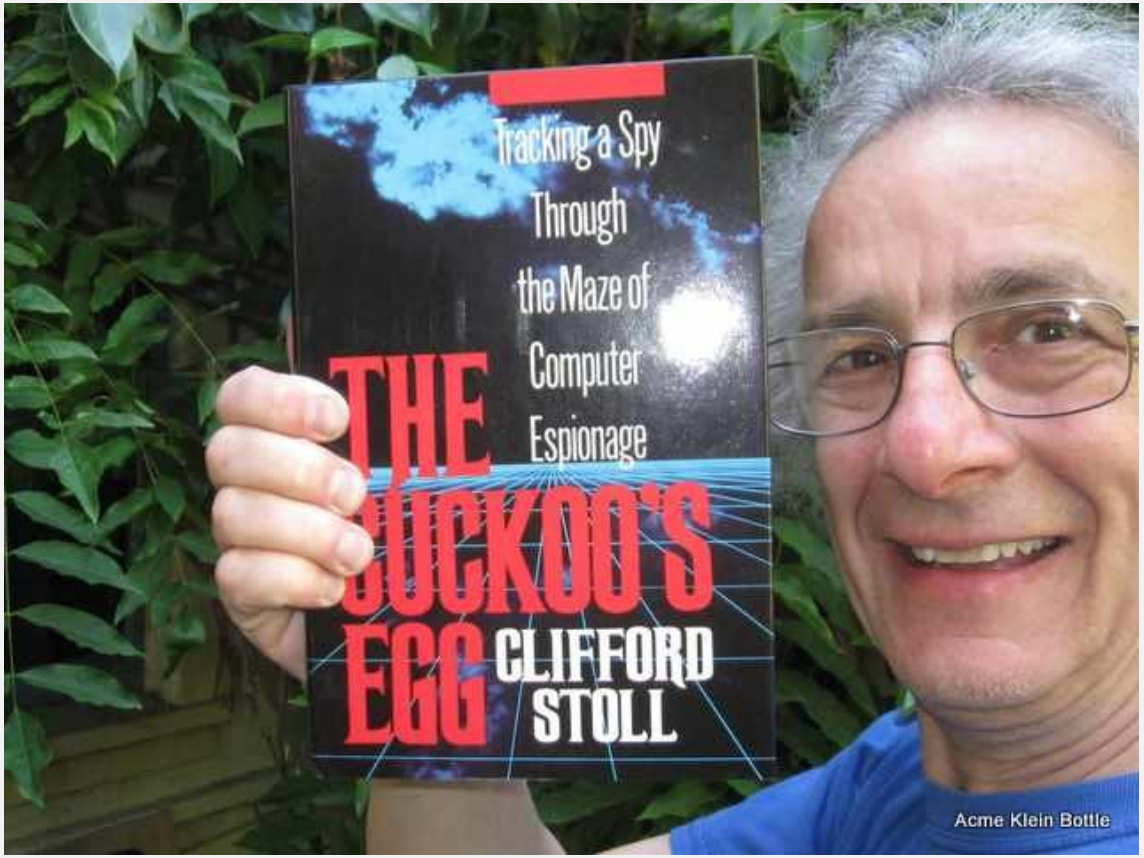
Primeri:

- 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>)

Napadi na informacijske sisteme

Fizični dostop do sistema

Nepooblaščeni dostop do podatkov.

Podtikanje prikritih mehanizmov za oddaljeni dostop ali krajo šifriranih podatkov (npr. programske aplikacije ali strojni dodatki).

Zavržene računalniške komponente, ki vsebujejo nosilce podatkov (trdi diski, tiskalniki, mobilni telefoni,...).

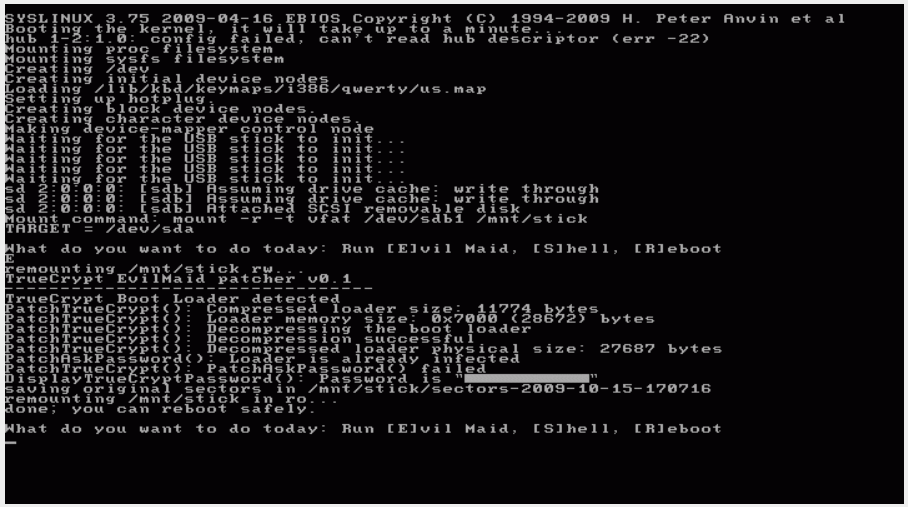
Nameščanje aplikacij z »dvojno funkcijo«.

Priklapljanje neznanih naprav na sistem (najdeni USB ključki, »polnjenje« mobilnih telefonov,...)

Večuporabniška okolja (eskalacija privilegijev).

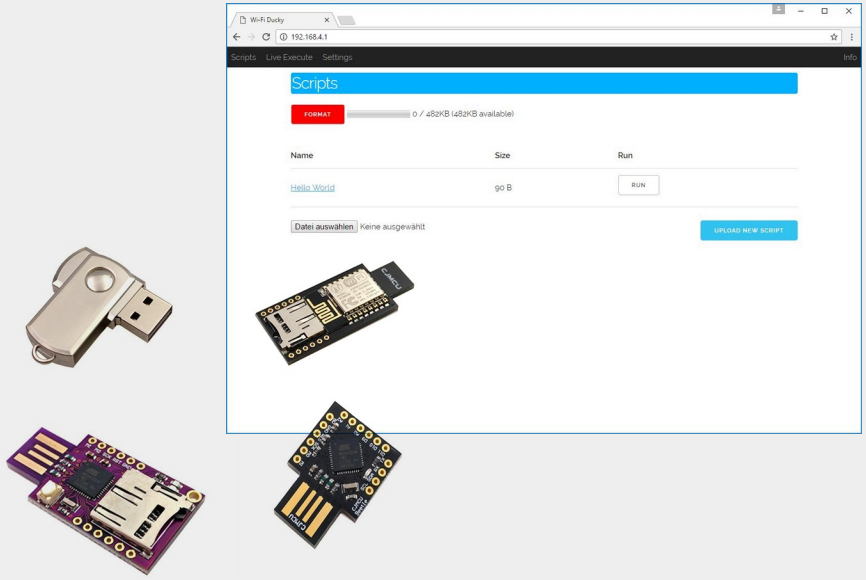
Podtikanje prikritih mehanizmov

Programski prestrezniki tipkanja.



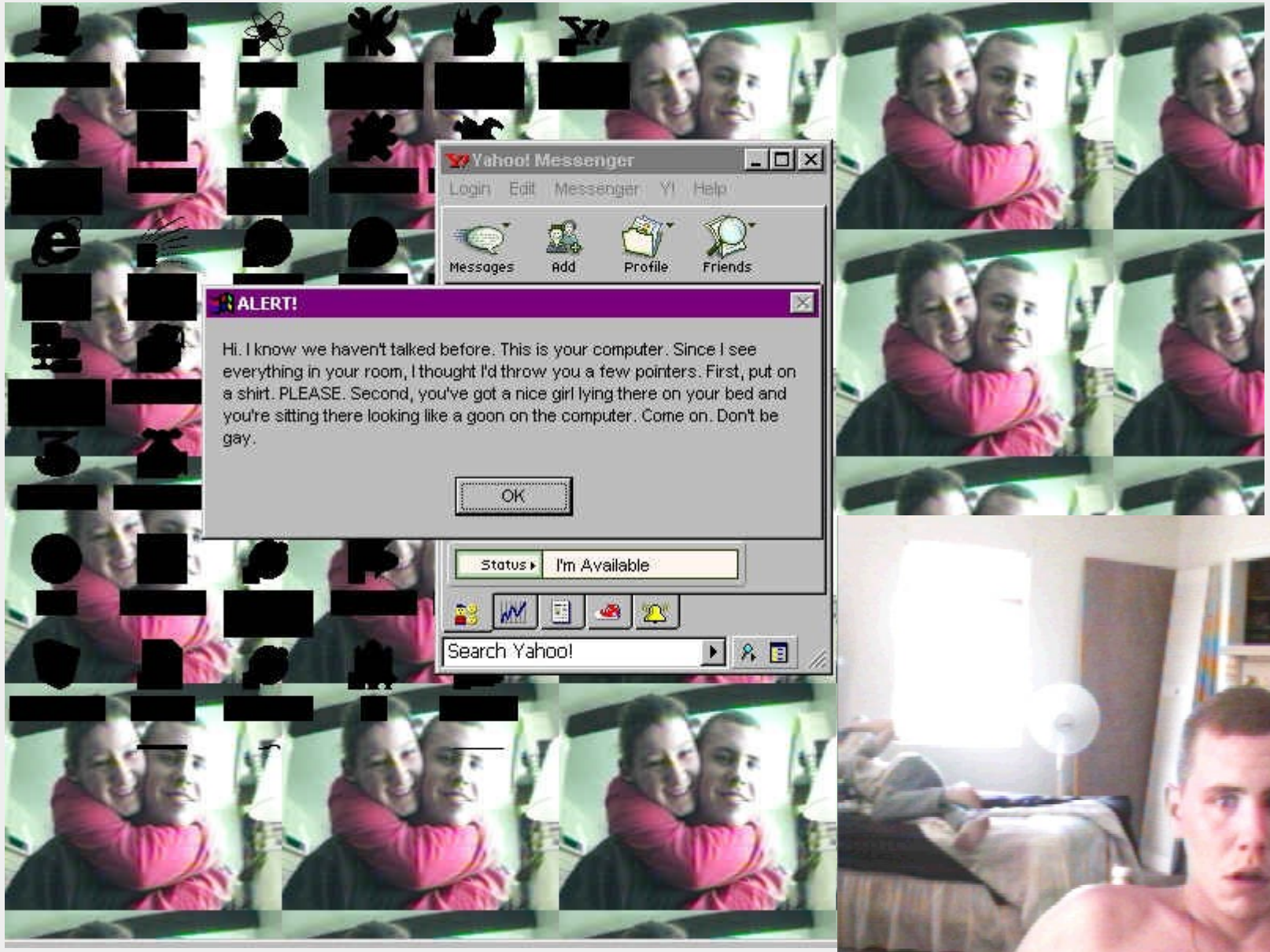
Evil Maid napad na TrueCrypt in...

Strojni prestrezniki tipkanja.



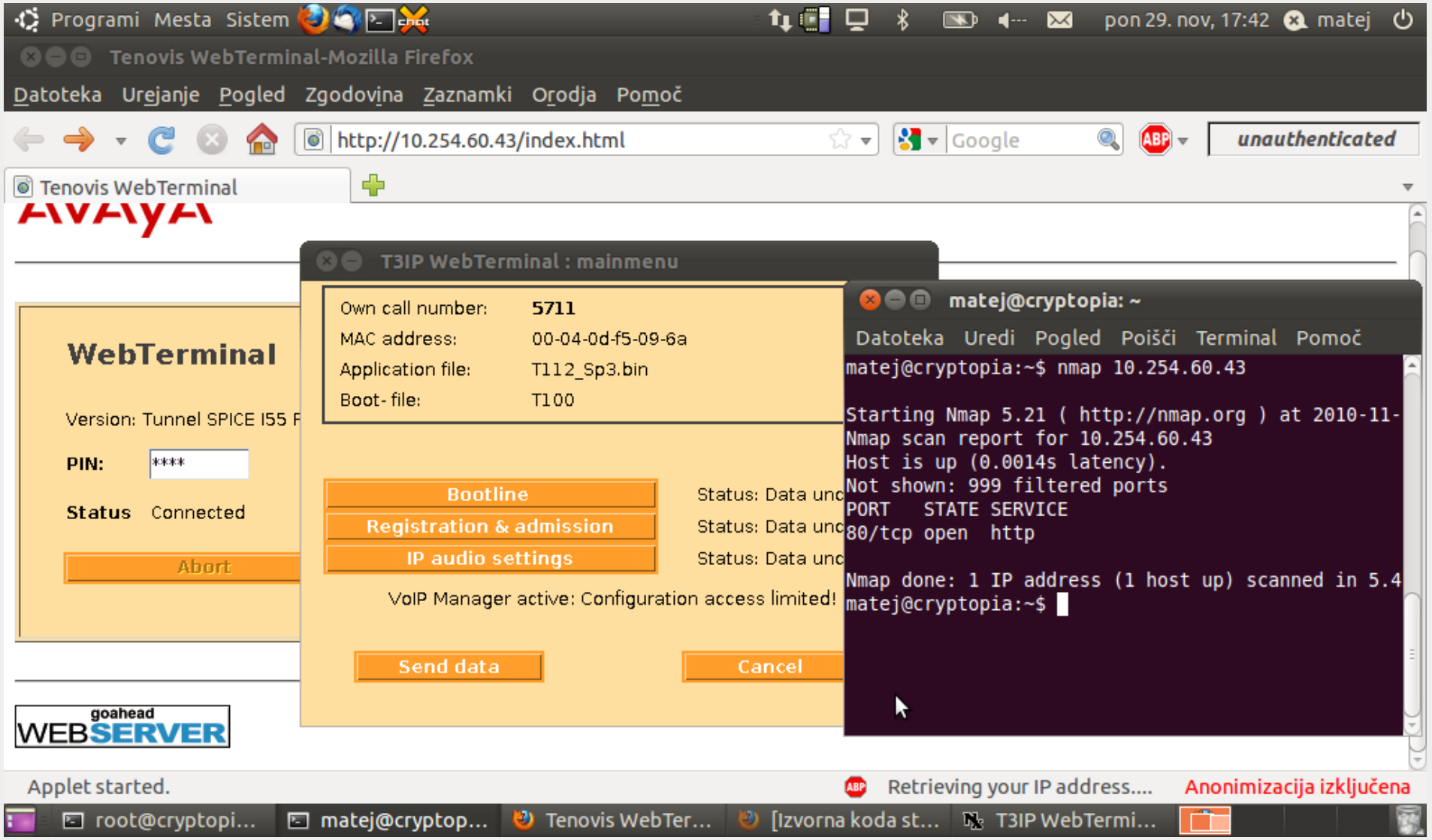
BadUSB z Wi-Fi podporo.

Posledice...


Yahoo! Messenger
Login Edit Messenger Y! Help
Messages
Add
Profile
Friends
ALERT!
Hi. I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.
OK
Status
I'm Available
Search Yahoo!

Ranljivi niso samo računalniki...

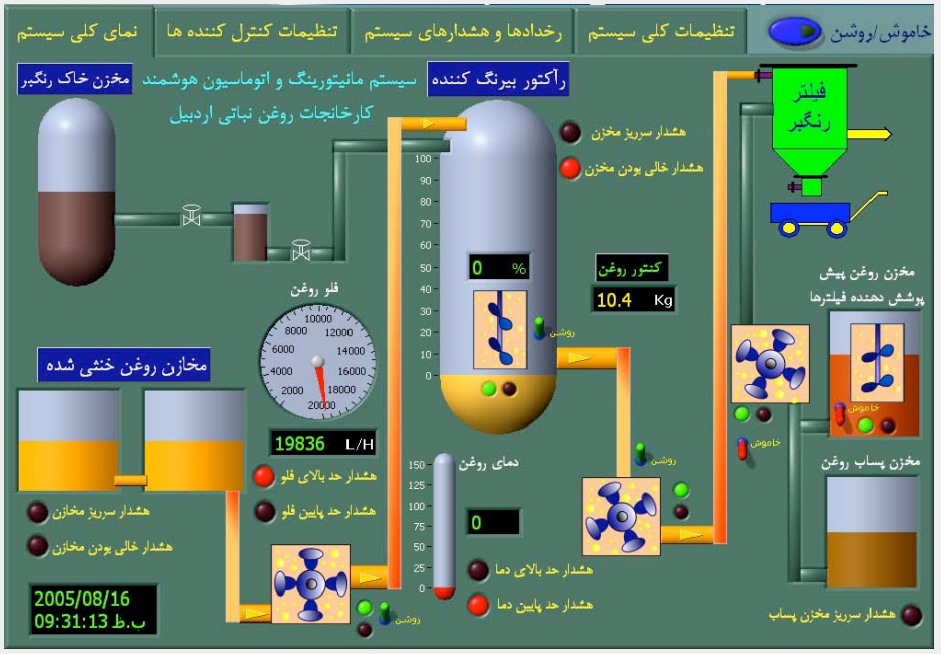
Ranljivi niso samo računalniki...



Napad na VOIP telefon.

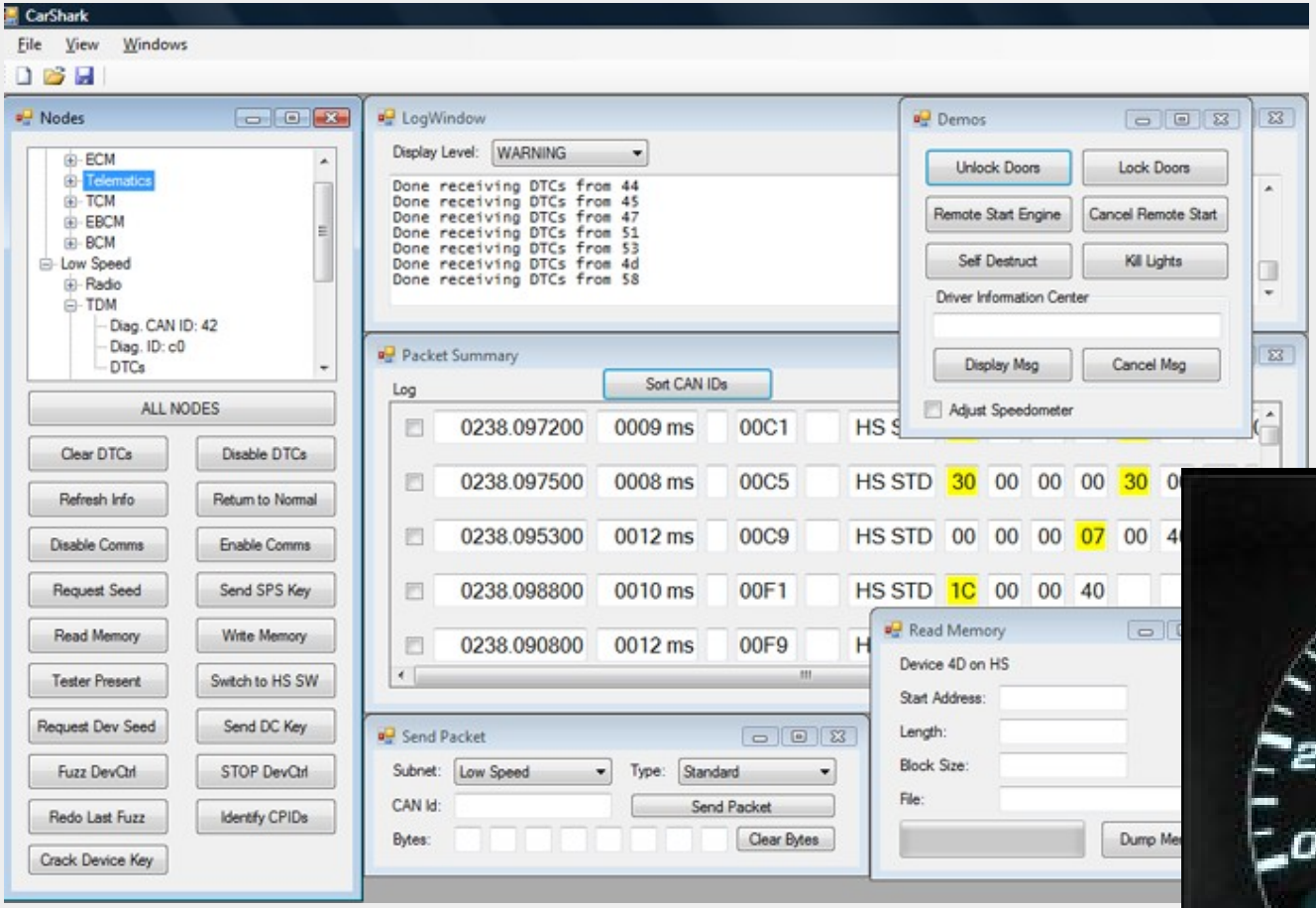
Ranljivi niso samo računalniki...

Napadi na RFID potne liste.



Napadi na SCADA sisteme.

Ranljivi niso samo računalniki...



Napadi na avtomobile.

Ranljivi niso samo računalniki...

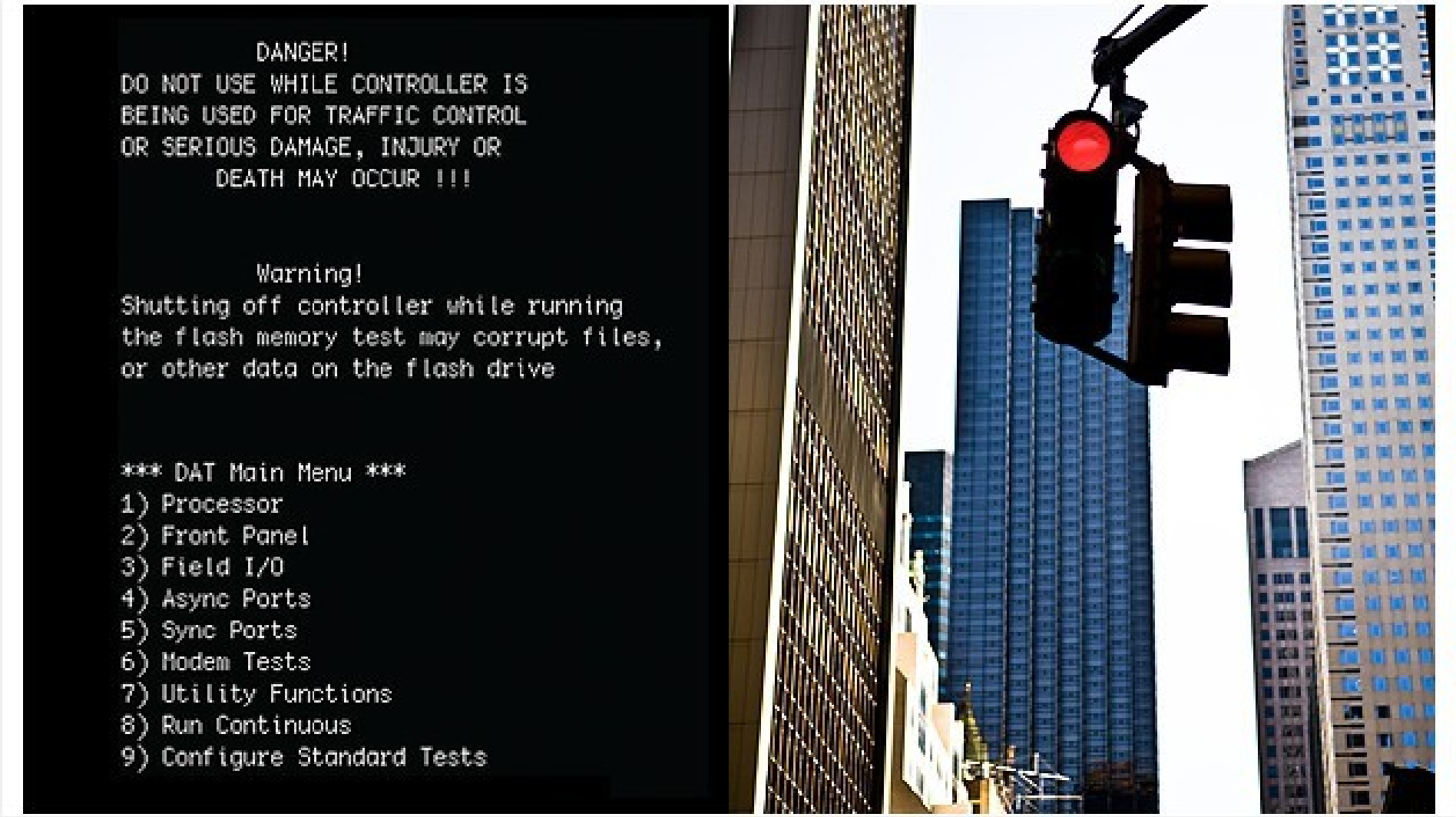


foto: Dan Tentler.

Nekoč, pred davnimi časi...

»L0pht Heavy Industries was a hacker collective active between 1992 and 2000 and located in the Boston, Massachusetts area. The L0pht was one of the first viable hackerspaces in the US, and a pioneer of Responsible disclosure.«

...je živel Mudge

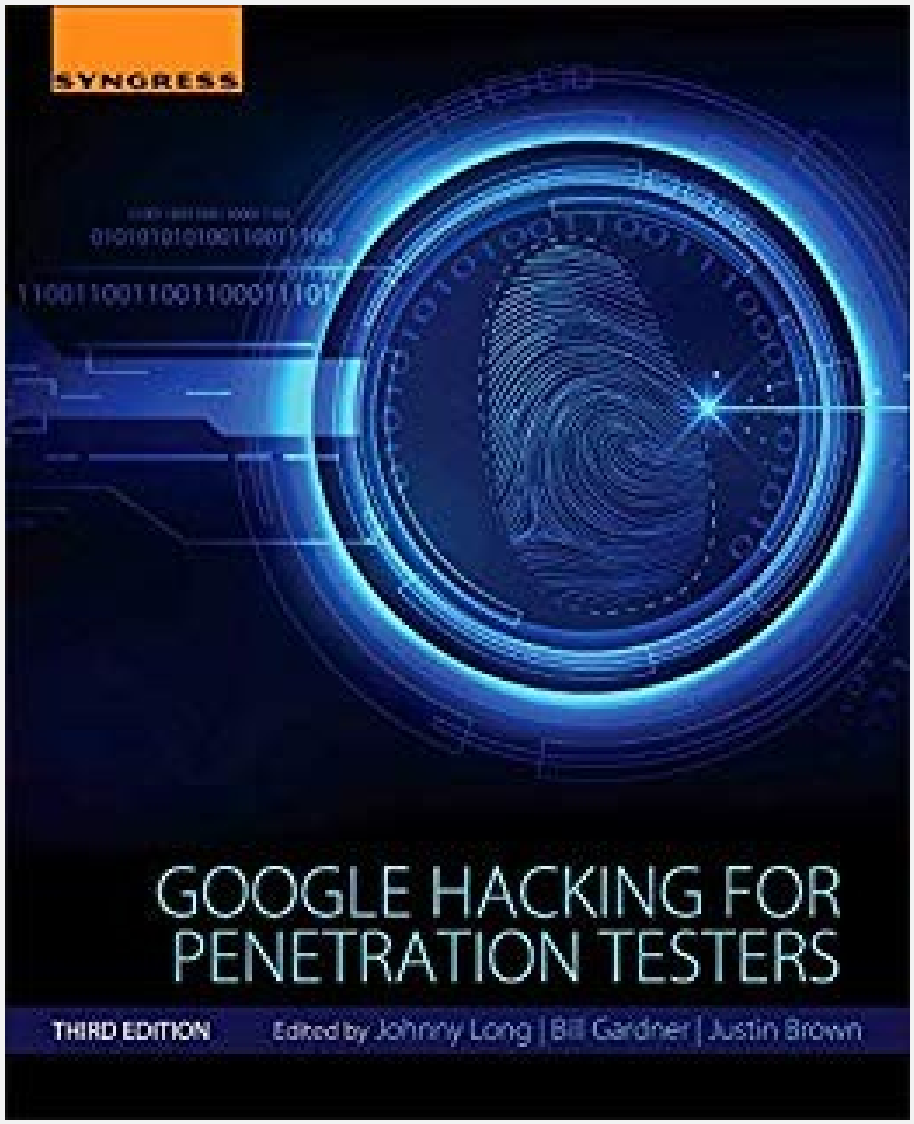
Mudge has written a program to scan utility companies' Web sites for words like »*confidential*« or »*password*.« »*I'm not breaking any laws by doing this, I'm just grabbing public stuff,*« he is quick to point out. »*They don't realize that they're putting it up there for the world to see.*«

In potem je prišel »Google hacking«...

Vincent Gaillot,
»How to use Google
to find confidential
informations«, 2001

Google hacking je prvič
omenjen avgusta 2003
na Defconu.

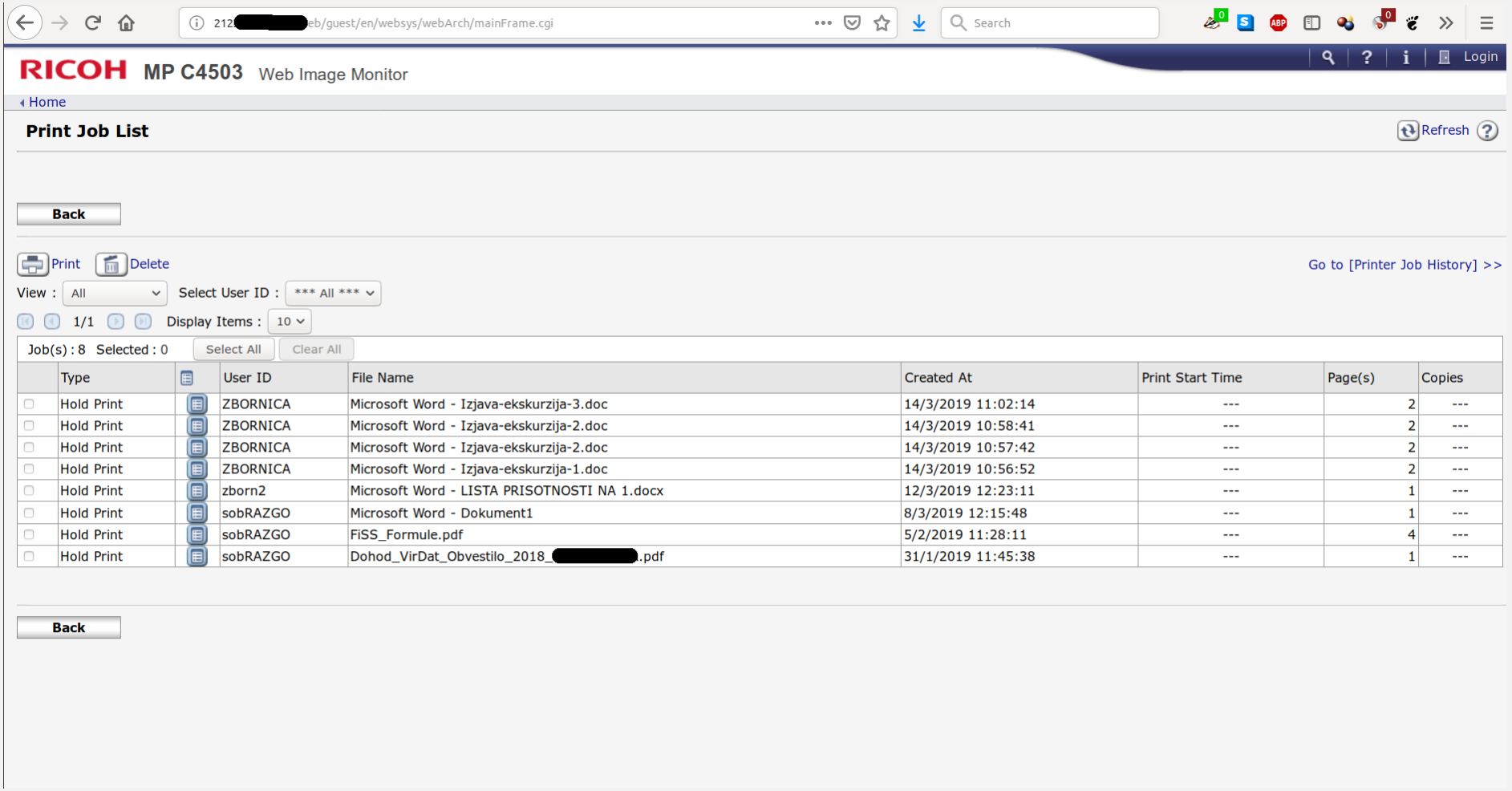
Johnny Long je leto
kasneje o tem napisal
še knjigo »Google Hacking
for Penetration Testers«.



Javno dostopne naprave

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

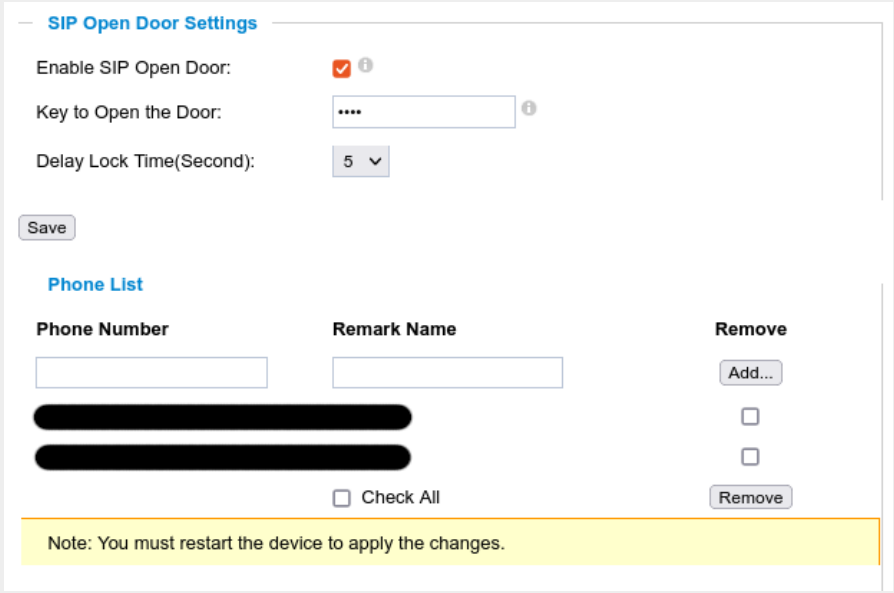
Javno dostopne naprave



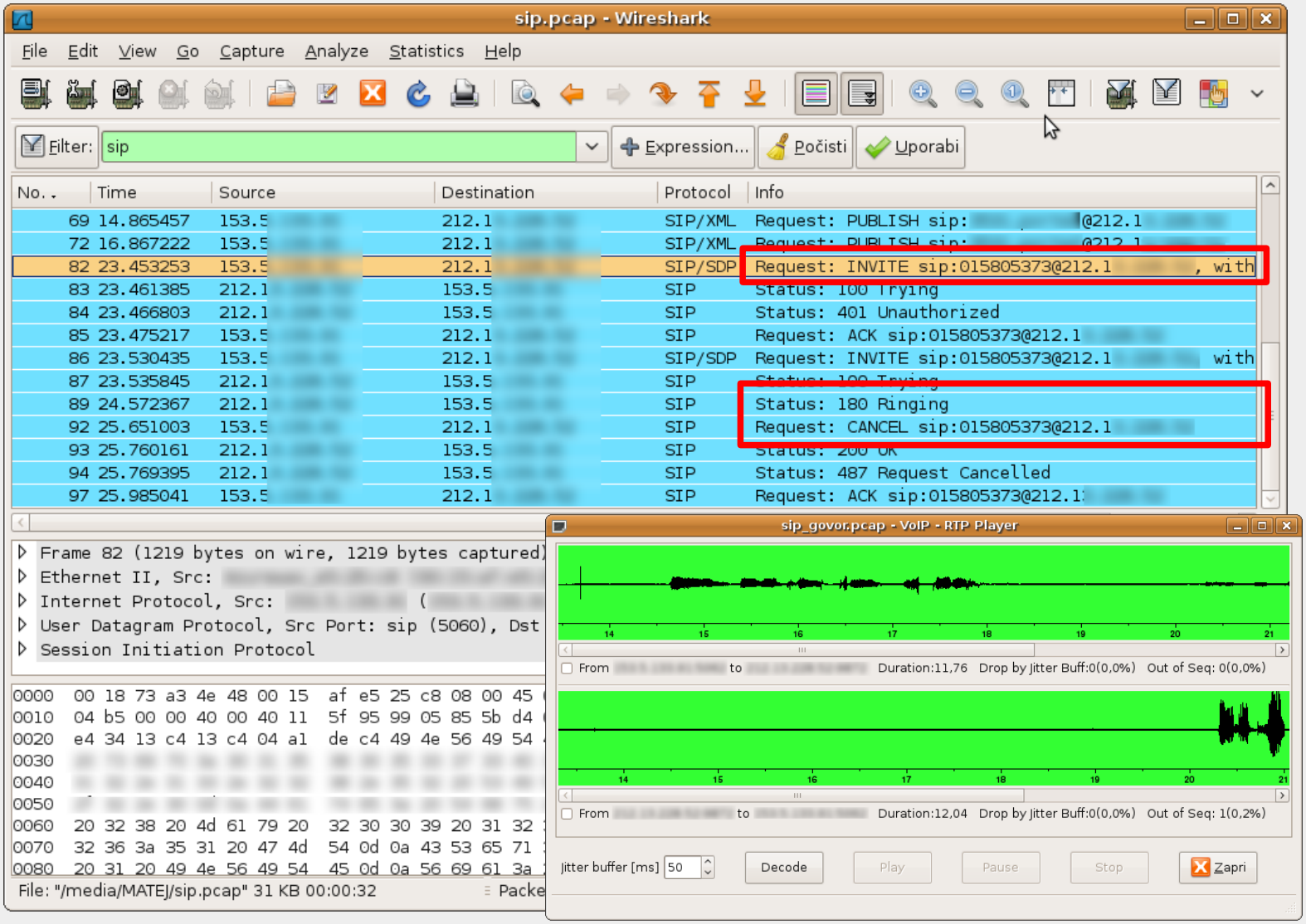
	Type		User ID	File Name	Created At	Print Start Time	Page(s)	Copies
☐	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-3.doc	14/3/2019 11:02:14	---	2	---
☐	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-2.doc	14/3/2019 10:58:41	---	2	---
☐	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-2.doc	14/3/2019 10:57:42	---	2	---
☐	Hold Print		ZBORNICA	Microsoft Word - Izjava-ekskurzija-1.doc	14/3/2019 10:56:52	---	2	---
☐	Hold Print		zborn2	Microsoft Word - LISTA PRISOTNOSTI NA 1.docx	12/3/2019 12:23:11	---	1	---
☐	Hold Print		sobRAZGO	Microsoft Word - Dokument1	8/3/2019 12:15:48	---	1	---
☐	Hold Print		sobRAZGO	FiSS_Formule.pdf	5/2/2019 11:28:11	---	4	---
☐	Hold Print		sobRAZGO	Dohod_VirDat_Obvestilo_2018_[redacted].pdf	31/1/2019 11:45:38	---	1	---

Varnost IoT

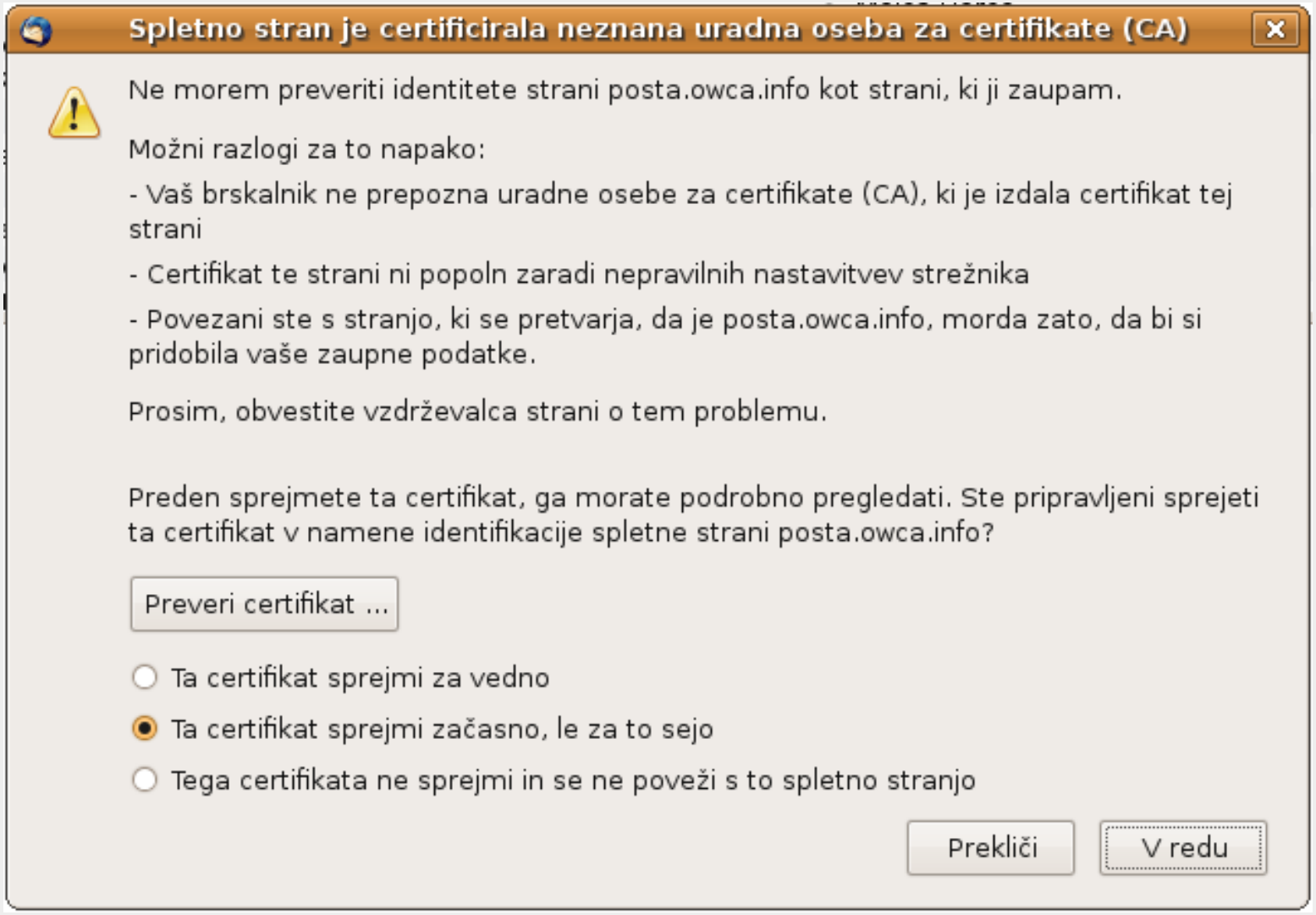
- Mirai botnet (napadal je domače usmerjevalnike in – IP kamere)…
- tiskalniki
- IP telefoni
- pametne pisarne,
- alarmi…



Prestrezanje komunikacij

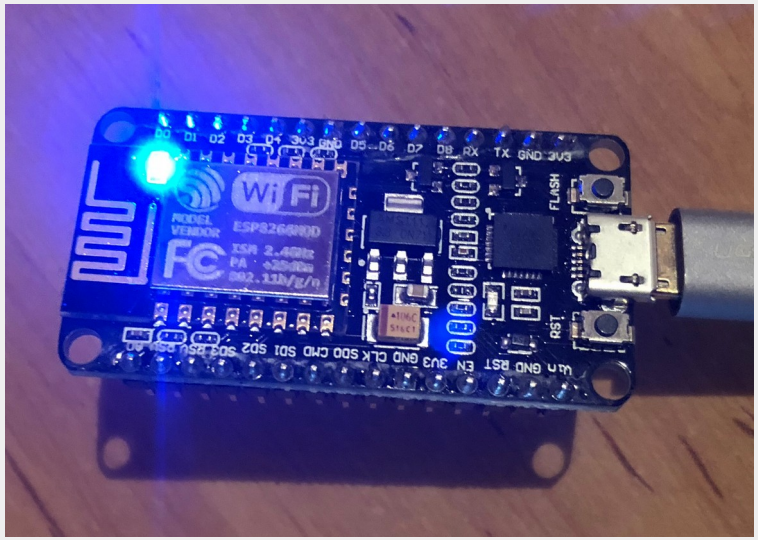


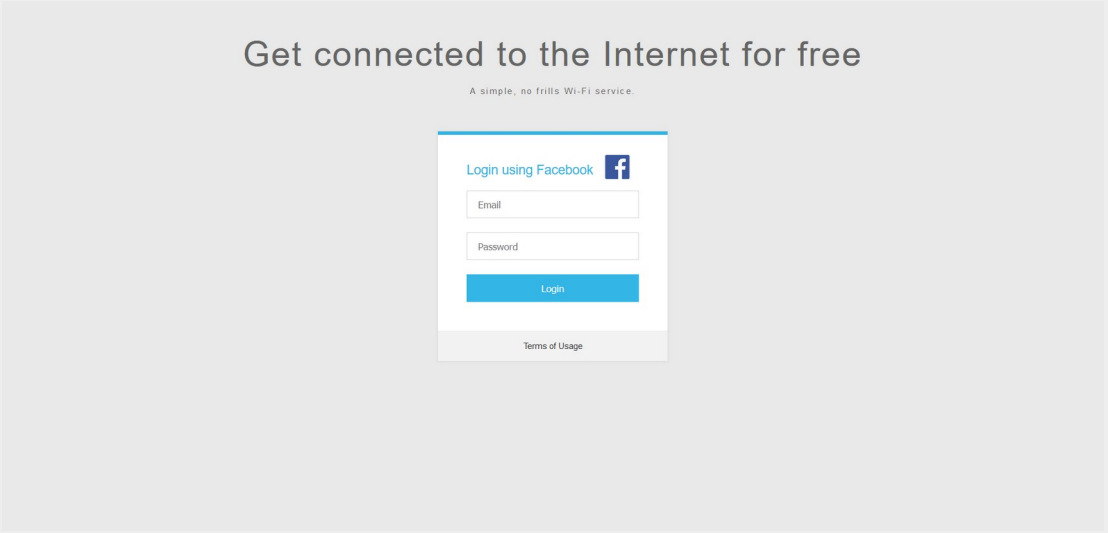
Prestrezanje komunikacij



Previdno pri sprejemanju neznanih digitalnih potrdil!

Javno dostopna (Wifi) omrežja...

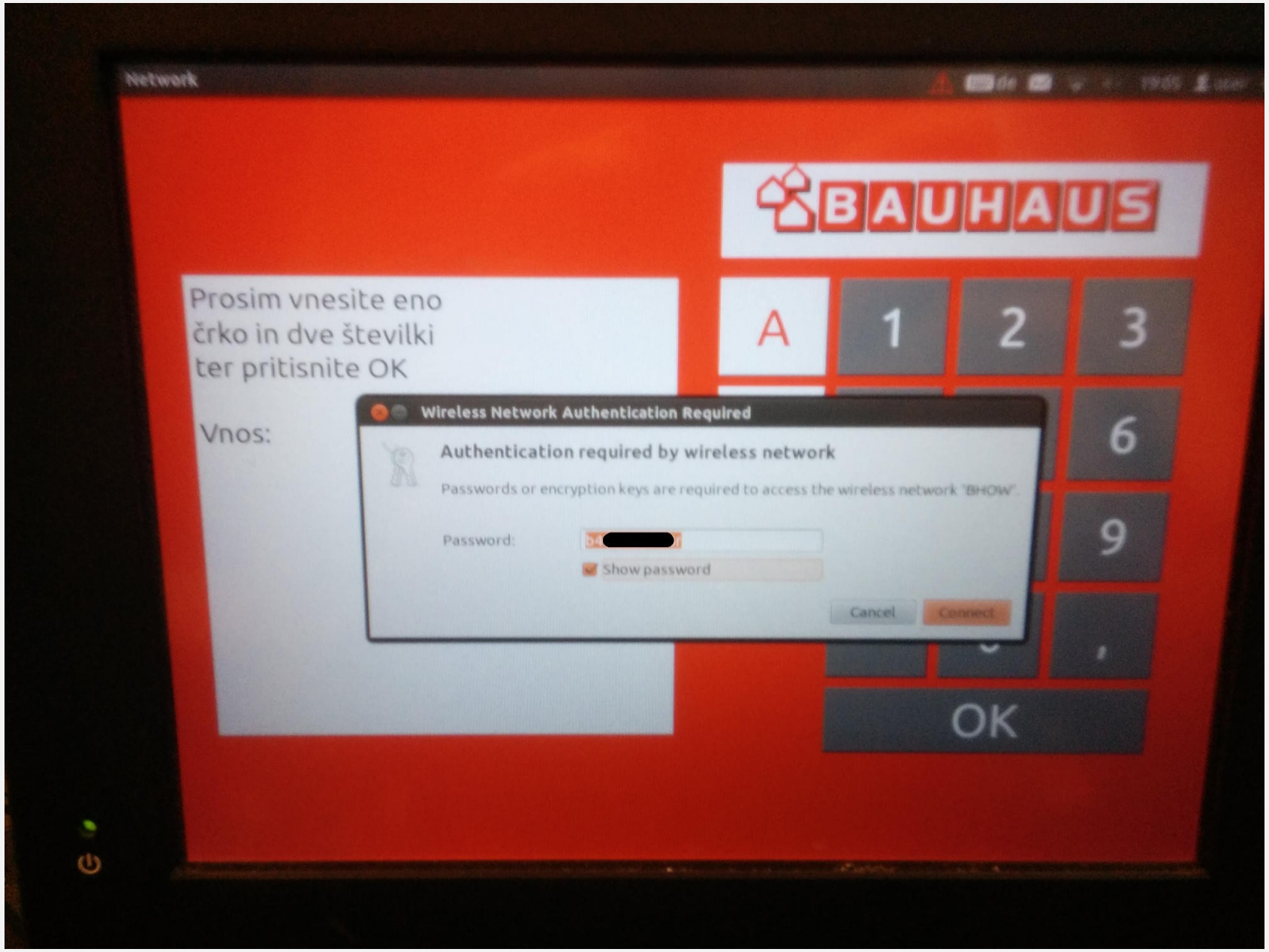




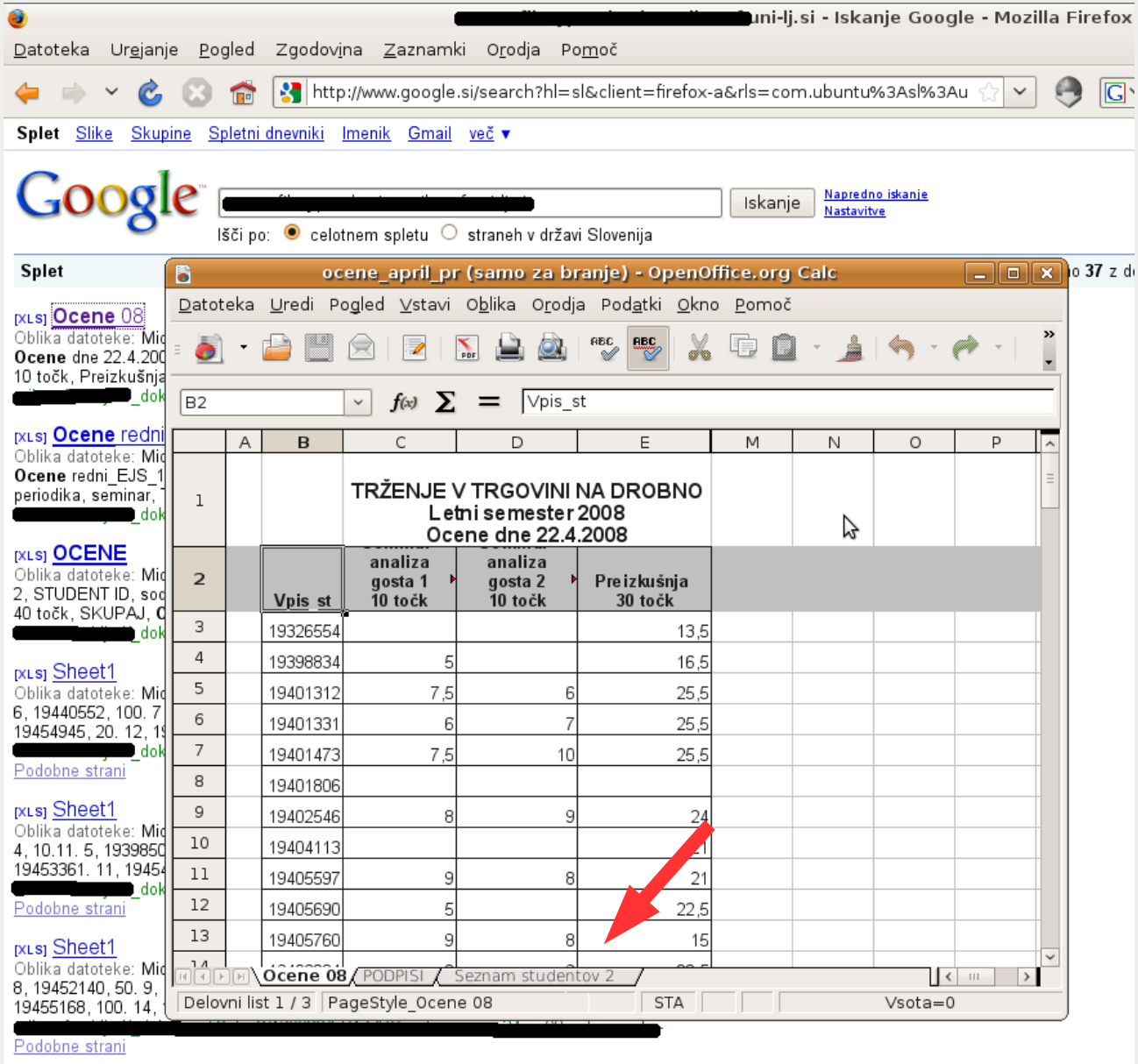

```
Extensions feed:
Sending 60 known beacons (OnAir ... HAM AIRPORT FREE WIFI)
Sending 60 known beacons (AEROPUERTO WIFI ... XFINITY)
Sending 60 known beacons (cablewifi ... backup)
Victim f4:91:          probed for WLAN with ESSID: 'Stargate' (KARMA)
Victim 40:f3:          probed for WLAN with ESSID: 'Telekom_FON' (Known Beacons)
DHCP Leases:
1533330793 40:f3                  android-6c              01:40

HTTP requests:
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] POST request from 10.0.0.94 with wfphshr-email=Victim@victim.com&wfphshr-password=crippledblackphoenix
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204

| Wifiphisher 1.4GIT
| ESSID: Free WiFi
| Channel: 6
| AP interface: wlan0
| Options: [Esc] Quit
```

https://github.com/wifiphisher/wifiphisher

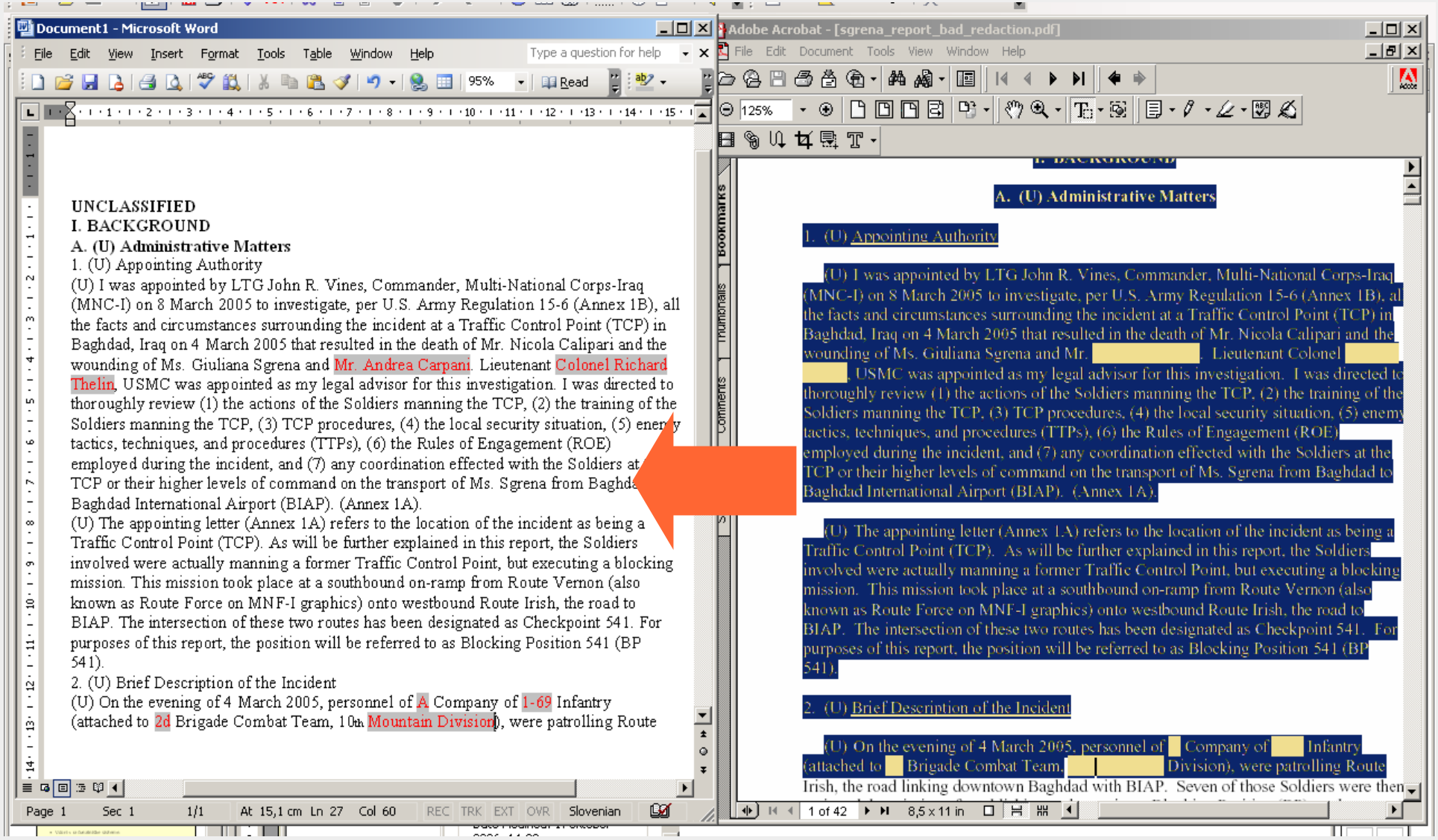
WiFi omrežja...



Zbiranje javnih (?) informacij



Zbiranje javnih (?) informacij



Zbiranje javnih (?) informacij

Zbiranje javnih (?) informacij

https://kidstar.si/wp-content/uploads/2018/02/

Index of /wp-content/uploads/2018/02

Name	Last modified	Size	Description
Parent Directory		-	
Dobavnica-12018.pdf	2018-02-13 21:31	1.1M	
Dobavnica-22018.pdf	2018-02-15 07:51	1.1M	
Dobavnica-32018.pdf	2018-02-15 07:51	1.1M	
Dobavnica-42018.pdf	2018-02-15 07:51	1.1M	
Dobavnica-52018.pdf	2018-02-15 07:51	1.1M	
Dobavnica-62018.pdf	2018-02-16 07:45	1.1M	
Dobavnica-72018.pdf	2018-02-16 07:45	1.1M	
Dobavnica-82018.pdf	2018-02-16 07:45	1.1M	
Dobavnica-92018.pdf	2018-02-16 07:45	1.1M	
Dobavnica-102018.pdf	2018-02-16 07:46	1.1M	
Dobavnica-112018.pdf	2018-02-16 07:46	1.1M	
Dobavnica-122018.pdf	2018-02-20 07:12	1.1M	
Dobavnica-132018.pdf	2018-02-20 07:12	1.1M	
Dobavnica-142018.pdf	2018-02-20 07:12	1.1M	
Dobavnica-152018.pdf	2018-02-20 07:12	1.1M	
Dobavnica-162018.pdf	2018-02-20 07:12	1.1M	
Dobavnica-172018.pdf	2018-02-21 08:29	1.1M	
Dobavnica-182018.pdf	2018-02-21 08:29	1.1M	
Dobavnica-192018.pdf	2018-02-21 08:29	1.1M	
Dobavnica-202018.pdf	2018-02-21 08:29	1.1M	

izpis.proteini.si/1[redacted]39.pdf

1 of 1 — 100%

RAČUN ŠT: 1[redacted]39

Sklic na: [redacted]
Jesenice, dne: 04.03.2019 10:19
Datum valute: 18.03.2019
Datum opravljene storitve: 04.03.2019 10:19

PROTEINI.SI SPORT NUTRITION CENTER

ROLnet d.o.o.
Blejska Dobrava 42
SI-4273 Blejska Dobrava

TRR: SI56 3000 0001 6408 944
Banka: Sberbank banka d.d.
ID za DDV: SI 44085206
Matična številka: 2024691

E: info@proteini.si
www.proteini.si

Vesna[redacted]

Tel:
Kontakt:
ID za DDV:

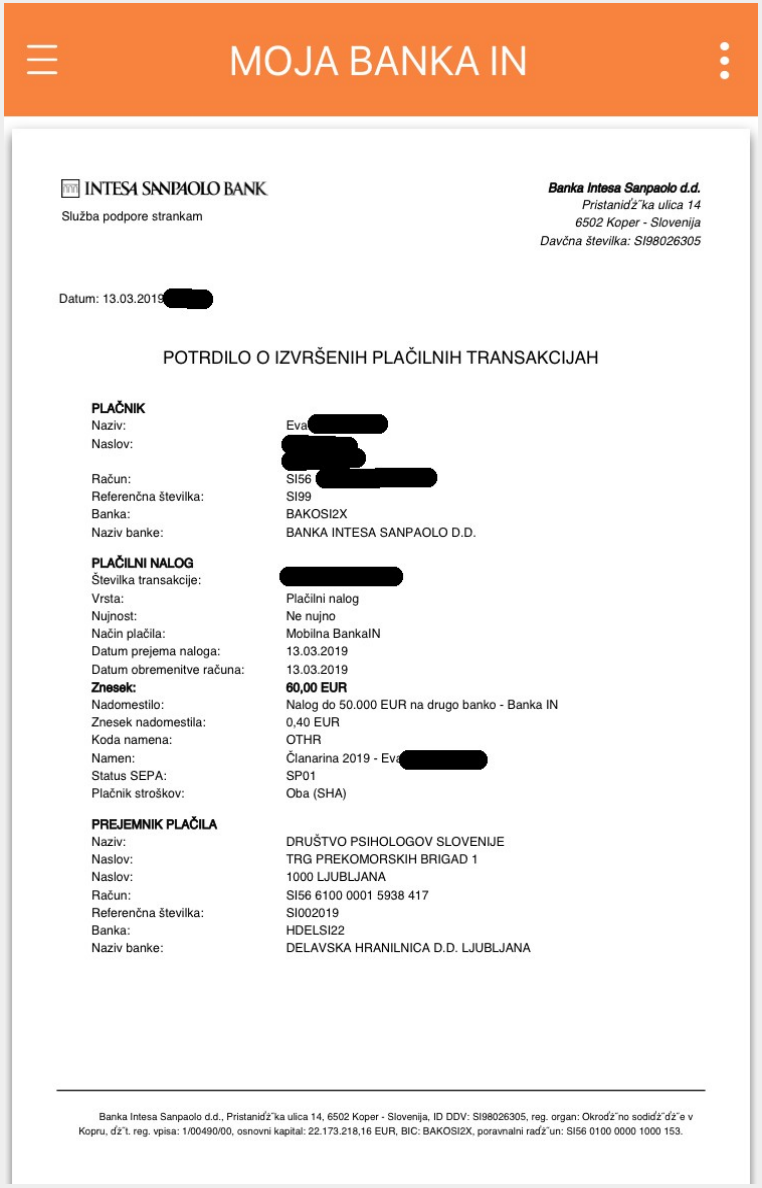
Naziv storitve	Količina	Cena	Popust %	Brez DDV	DDV %	Skupaj
PROTEINI.SI 100% NATURAL WHEY PROTEIN, 500g, White Choc. Straw.	2	10,04	0,00	10,04	9,50	**21,98**
Dostava Pošta Slovenije SLOVENIA	1	2,45	0,00	2,45	22,00	**2,99**

Skupaj bruto znesek:	22,53
Popust:	0,00
Skupaj neto znesek:	22,53
Davek:	2,44
Skupaj:	**24,97 EUR**

Obračun DDV:

Stopnja	Osnova	Davek
9,50%	20,08	1,90

Zbiranje javnih (?) informacij



MOJA BANKA IN

INTESA SANPAOLO BANK
Služba podpore strankam

Banka Intesa Sanpaolo d.d.
Pristaniška ulica 14
6502 Koper - Slovenija
Davčna številka: SI98026305

Datum: 13.03.2019[redacted]

POTRDILO O IZVRŠENIH PLAČILNIH TRANSAKCIJAH

PLAČNIK

Naziv:	Eva[redacted]
Naslov:	[redacted]
Račun:	SI56 [redacted]
Referenčna številka:	SI99
Banka:	BAKOSI2X
Naziv banke:	BANKA INTESA SANPAOLO D.D.

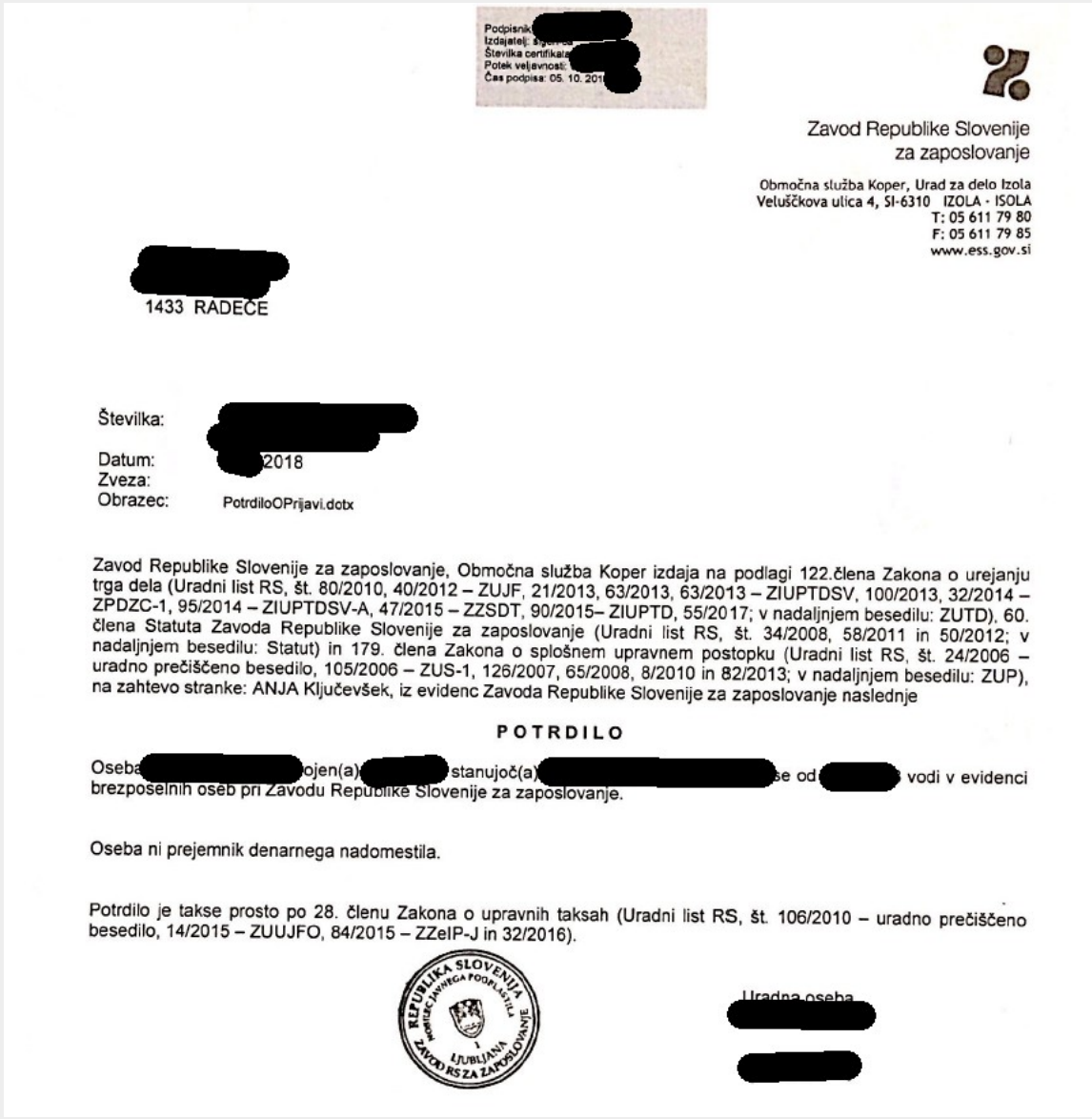
PLAČILNI NALOG

Številka transakcije:	[redacted]
Vrsta:	Plačilni nalog
Nujnost:	Ne nujno
Način plačila:	Mobilna BankaIN
Datum prejema naloga:	13.03.2019
Datum obremenitve računa:	13.03.2019
Znesek:	**60,00 EUR**
Nadomestilo:	Nalog do 50.000 EUR na drugo banko - Banka IN
Znesek nadomestila:	0,40 EUR
Koda namena:	OTHR
Namen:	Članarina 2019 - Eva[redacted]
Status SEPA:	SP01
Plačnik stroškov:	Oba (SHA)

PREJEMNIK PLAČILA

Naziv:	DRUŠTVO PSIHOLOGOV SLOVENIJE
Naslov:	TRG PREKOMORSKIH BRIGAD 1
Naslov:	1000 LJUBLJANA
Račun:	SI56 6100 0001 5938 417
Referenčna številka:	SI002019
Banka:	HDELSI22
Naziv banke:	DELAVSKA HRANILNICA D.D. LJUBLJANA

Banka Intesa Sanpaolo d.d., Pristaniška ulica 14, 6502 Koper - Slovenija, ID DDV: SI98026305, reg. organ: Okrožno sodišče v Kopru, vl. reg. vpisa: 1/00490/00, osnovni kapital: 22.173.218,16 EUR, BIC: BAKOSI2X, poravnalni račun: SI56 0100 0000 1000 153.



Podpisnik: [redacted]
Izdajatelj: [redacted]
Številka certifikata: [redacted]
Potek veljavnosti: [redacted]
Čas podpisa: 05. 10. 201[redacted]

Zavod Republike Slovenije
za zaposlovanje

Območna služba Koper, Urad za delo Izola
Veluščkova ulica 4, SI-6310 IZOLA - ISOLA
T: 05 611 79 80
F: 05 611 79 85
www.ess.gov.si

[redacted]
1433 RADEČE

Številka: [redacted]
Datum: [redacted]2018
Zveza:
Obrazec: PotrdiloOPrijavi.dotx

Zavod Republike Slovenije za zaposlovanje, Območna služba Koper izdaja na podlagi 122.člena Zakona o urejanju trga dela (Uradni list RS, št. 80/2010, 40/2012 – ZUJF, 21/2013, 63/2013, 63/2013 – ZIUPTDSV, 100/2013, 32/2014 – ZPDZC-1, 95/2014 – ZIUPTDSV-A, 47/2015 – ZZSDT, 90/2015– ZIUPTD, 55/2017; v nadaljnjem besedilu: ZUTD), 60. člena Statuta Zavoda Republike Slovenije za zaposlovanje (Uradni list RS, št. 34/2008, 58/2011 in 50/2012; v nadaljnjem besedilu: Statut) in 179. člena Zakona o splošnem upravnem postopku (Uradni list RS, št. 24/2006 – uradno prečiščeno besedilo, 105/2006 – ZUS-1, 126/2007, 65/2008, 8/2010 in 82/2013; v nadaljnjem besedilu: ZUP), na zahtevo stranke: ANJA Ključevšek, iz evidenc Zavoda Republike Slovenije za zaposlovanje naslednje

POTRDILO

Oseba[redacted]ojen(a)[redacted]stanujoč(a)[redacted]se od[redacted] vodi v evidenci brezposelnih oseb pri Zavodu Republike Slovenije za zaposlovanje.

Oseba ni prejemnik denarnega nadomestila.

Potrdilo je takse prosto po 28. členu Zakona o upravnih taksah (Uradni list RS, št. 106/2010 – uradno prečiščeno besedilo, 14/2015 – ZUUJFO, 84/2015 – ZZelP-J in 32/2016).

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
ZAVOD RS ZA ZAPOSLOVANJE
1
LJUBLJANA

Uradna oseba
[redacted]

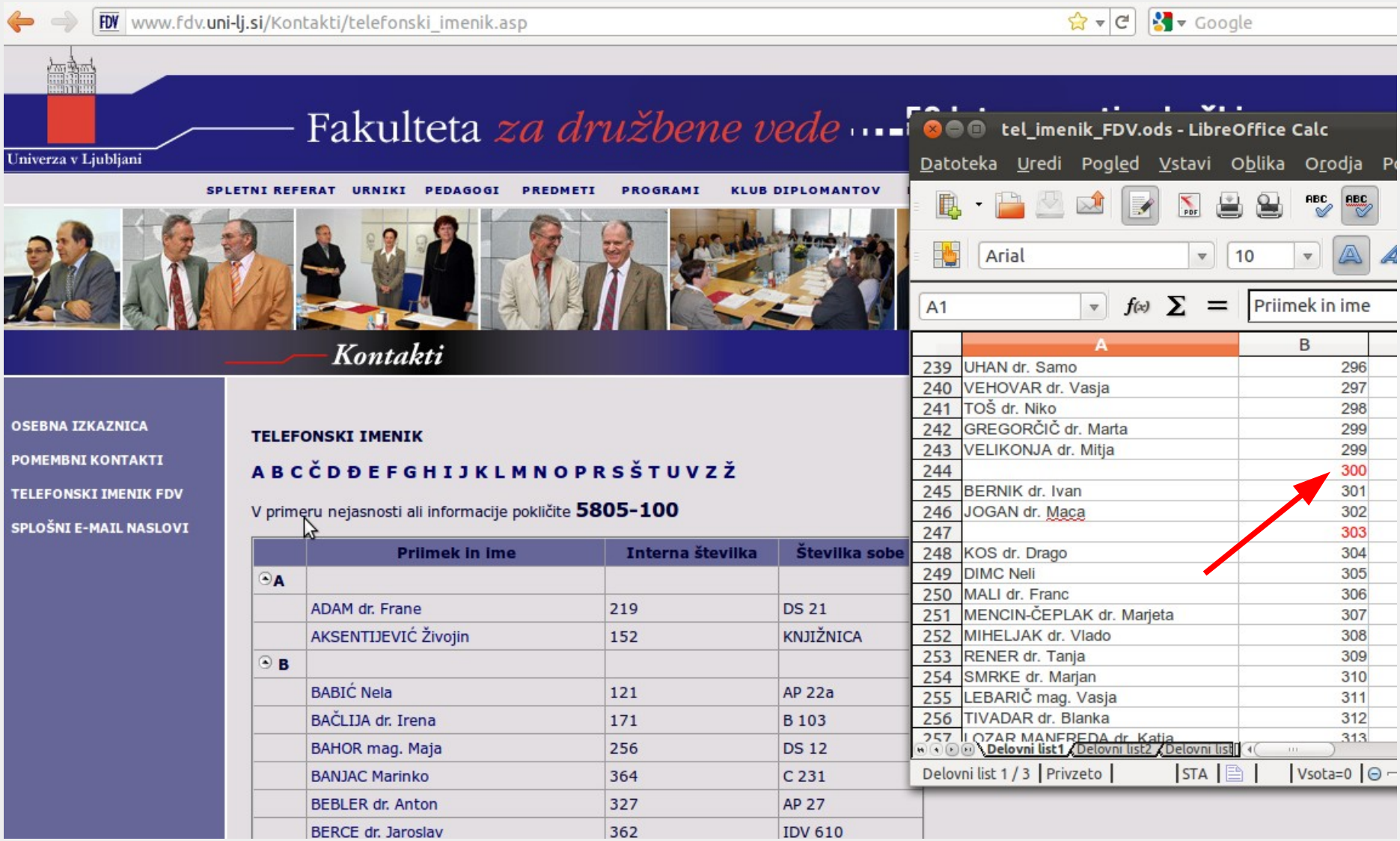
Zbiranje javnih (?) informacij

(8 of 10)

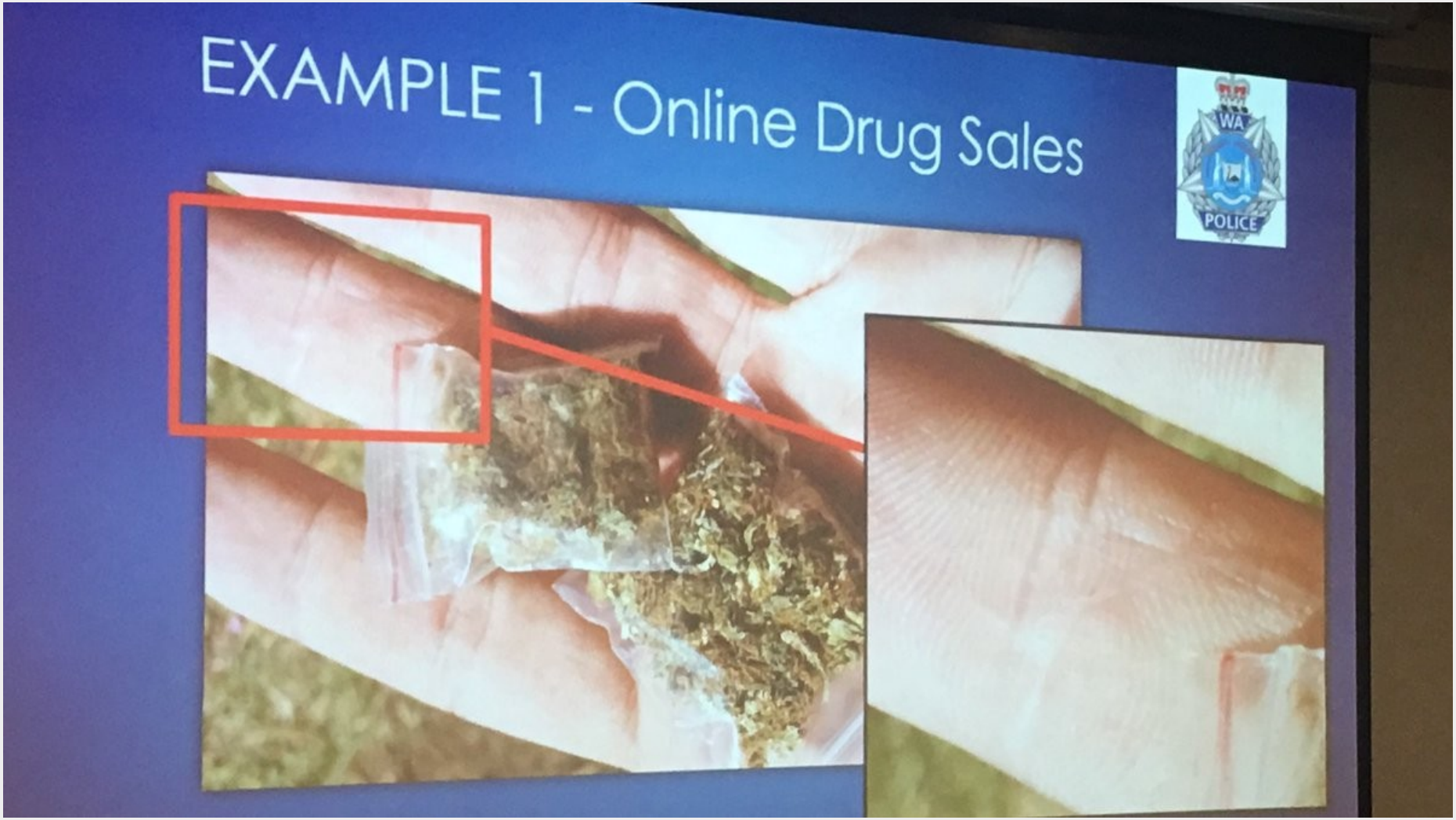
My sweethearts! ❤💋🥂🎈🎁 #birthday #birthdaygirl #friends #lovethem #womanpower #specialmoments #thankful #love

A post shared by Sabina Remar (@sabinaremar) on Dec 3, 2017 at 5:34am PST

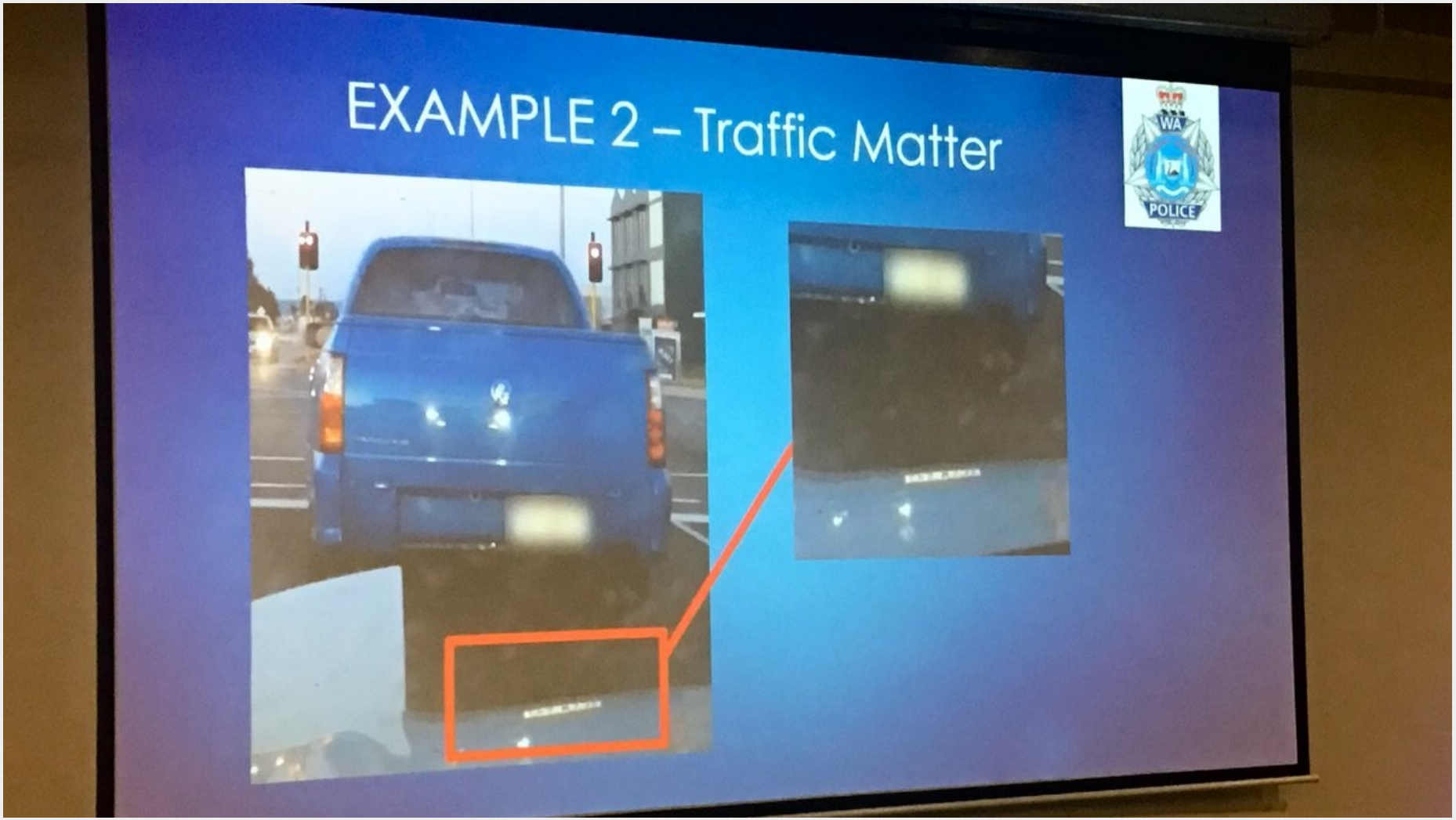
Zbiranje javnih (?) informacij



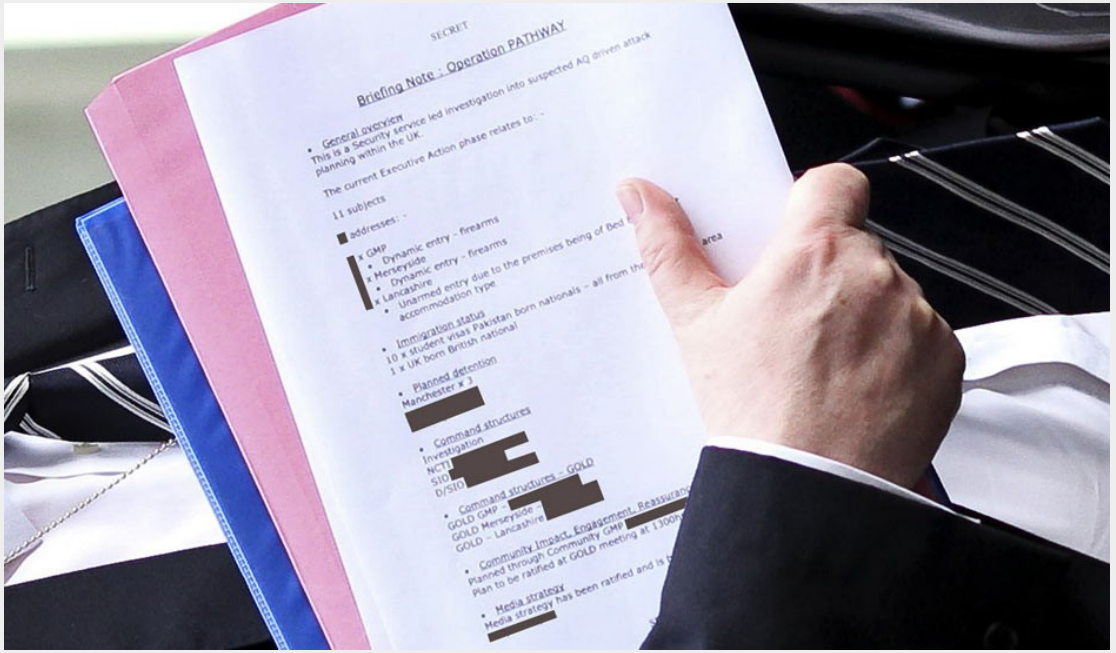
Zbiranje javnih (?) informacij



Zbiranje javnih (?) informacij



Zbiranje javnih (?) informacij



Zbiranje javnih (?) informacij

[redacted]**SARA**. Spol: Datum roj.: z. [redacted] iimek in ime:
Naroe ilo sprejema :[redacted]
12:04:07. AMBULANTA[redacted] ...

Untitled
https://www.sb-izola.si/wp-content/uploads/2018/01/izvid.pdf
Sedež: [redacted]. Enota: [redacted]
GINEKOLOŠKA AMBULANTA.[redacted] **Sara**, rojena
[redacted] ul. 16, 6000 Koper.

Untitled
https://www.sb-izola.si/wp-content/uploads/2017/05/doc043155201705110742 50.pdf
9. maj 2017 -[redacted] **SARA**.[redacted] 6274 ŠMARJE.

Zbiranje javnih (?) informacij

VISOKOŠOLSKI STROKOVNI ŠTUDIJ

Elektrotehnika – Telekomunikacije

POROČILO PRAKTIČNEGA IZOBRAŽEVANJA

v podjetju

[redacted]

poslovna enota Maribor

Čas opravljanja: o[redacted].2009 do[redacted]2010
Mentor v podjetju: [redacted]

Študent: [redacted]
Vpisna številka: 9[redacted]
E-pošta: [redacted]@gmail.com
Telefon: 041[redacted]

VISOKOŠOLSKI STROKOVNI ŠTUDIJ

Računalništvo in informacijske tehnologije

POROČILO PRAKTIČNEGA IZOBRAŽEVANJA

v podjetju

[redacted]

Čas opravljanja: [redacted]**2010 - [redacted]2010**
Mentor v GD: [redacted]
Študent: [redacted]
Vpisna številka: [redacted]
E-pošta: [redacted]@uni-mb.si
Telefon: **041**[redacted]

Metapodatki

Jeffrey's Exif Viewer

Jeffrey Friedl's Image Metadata Viewer
(How to use)

Some of my other stuff
· My Blog · Lightroom plugins · Pretty Photos
· "Photo Tech"

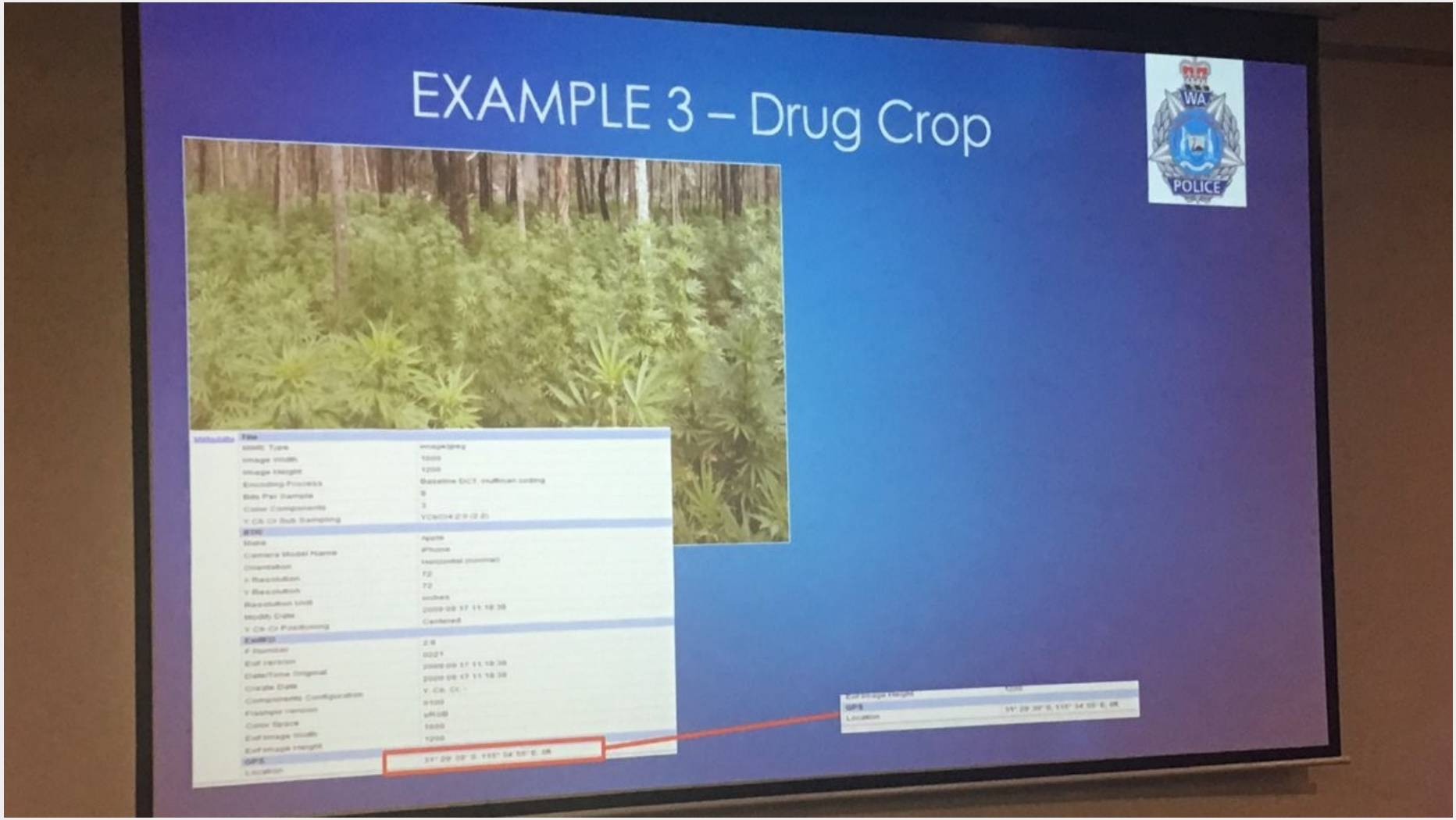
From Web / From File Image URL: View Image At Url [CLEAR IMAGE]

Basic Image Information

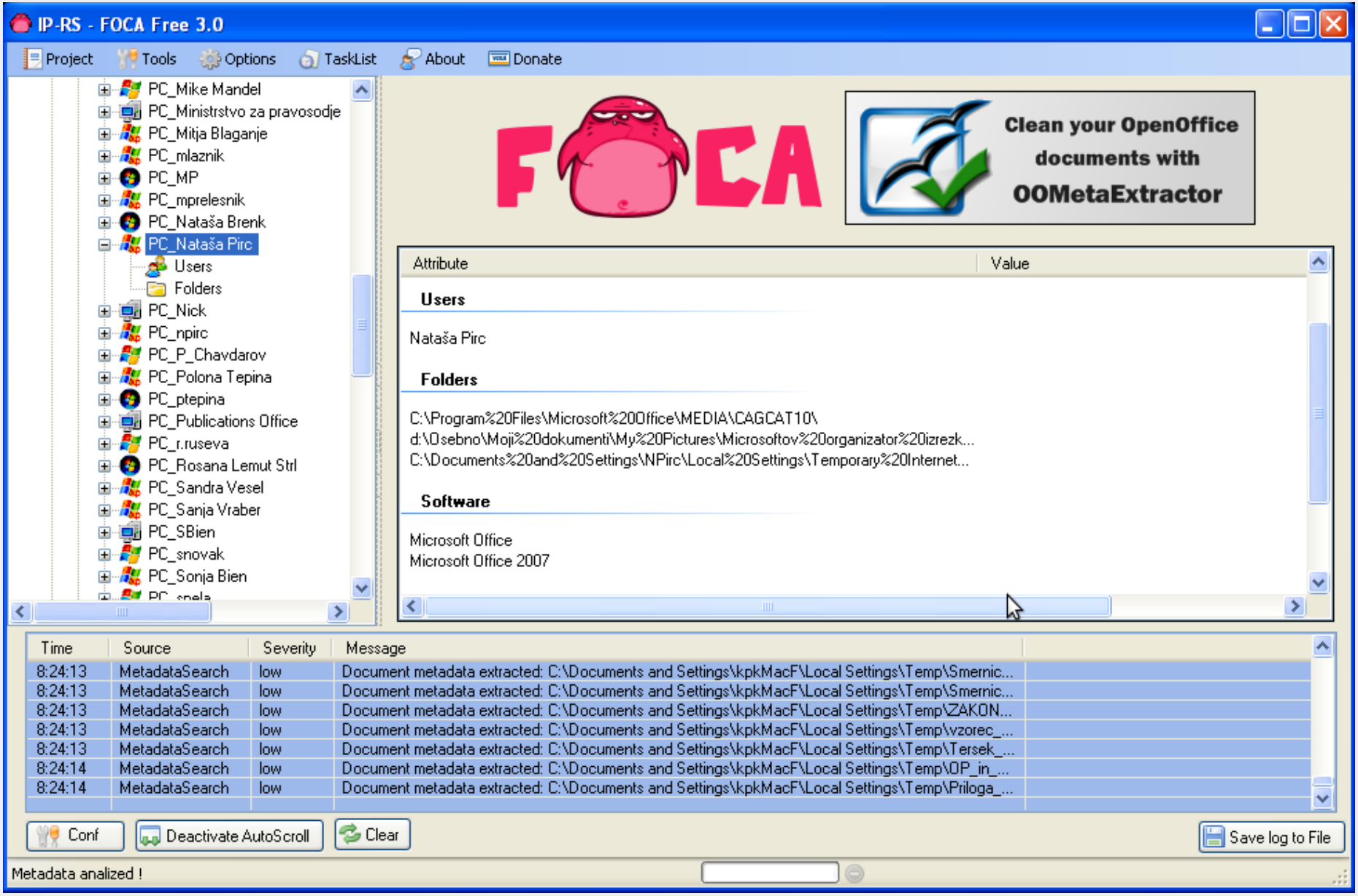
Target image: http://www.wired.com/images_blogs/gadgetlab/2012/12/8b6cd78e0012f7754f1dc6212f49f8d751.jpg

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125
Flash:	Off, Did not fire
Date:	**December 3, 2012** 12:26:00PM (timezone not specified) (2 years, 5 months, 23 days, 9 hours, 5 minutes, 34 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: **15°** 39' 29.4" North, **88°** 59' 31.8" West (15.658167, -88.992167) Location guessed from coordinates: *Dummy Road, Rio Dulce, Guatemala* Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 7 meters (23 feet)

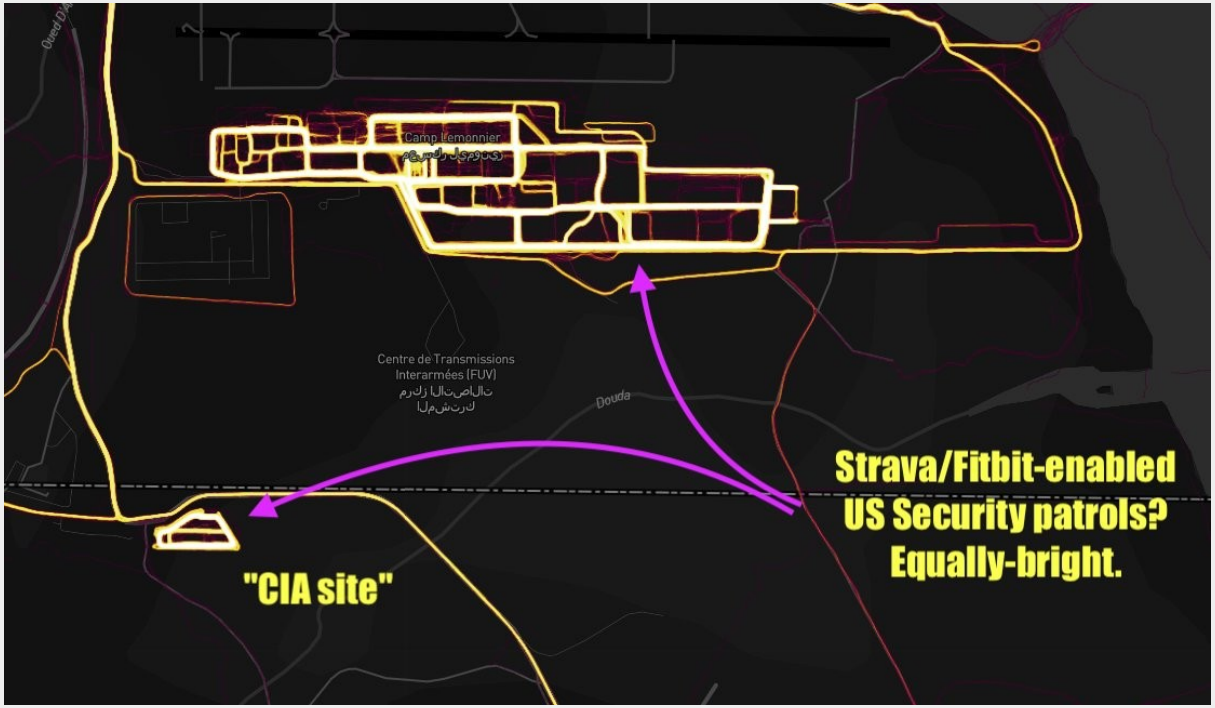
Metapodatki



Metapodatki



Metapodatki



7) The article said there were a lot of other militaries living side-by-side up in Djibouti, let's scan around with Google maps and see what else is there.

8) Well, looky here: about a half mile from the camp, a short hop, but isolated: [google map link]

Wow, that was a bit too easy. Look the nice cleared perimeter, walls, crash-trenches so nobody can ram a truck-bomb through, complex gate to defeat assaults or truck-bombs. Expensive security. Good security. And the architectural tone looks pretty familiar, too; for one thing, only Americans spend money like that. [stderr]

9) Google "CIA black site djibouti" and you find [alj]

> The legal case of a former CIA detainee suing the government of Djibouti for hosting the facility where he says he was detained could be helped by the contents of a still-classified Senate report. Djibouti, a key U.S. ally, has denied for

Metapodatki

US bombs terror HQ after ISIS 'moron' takes selfie there

By Yaron Steinbuch

June 5, 2015 | 4:11pm

ype to Search

SEARCH

NEW YORK POST

A U.S. Navy F-18E Super Hornet used in airstrikes against the Islamic State.
AP

MORE ON:
ISIS

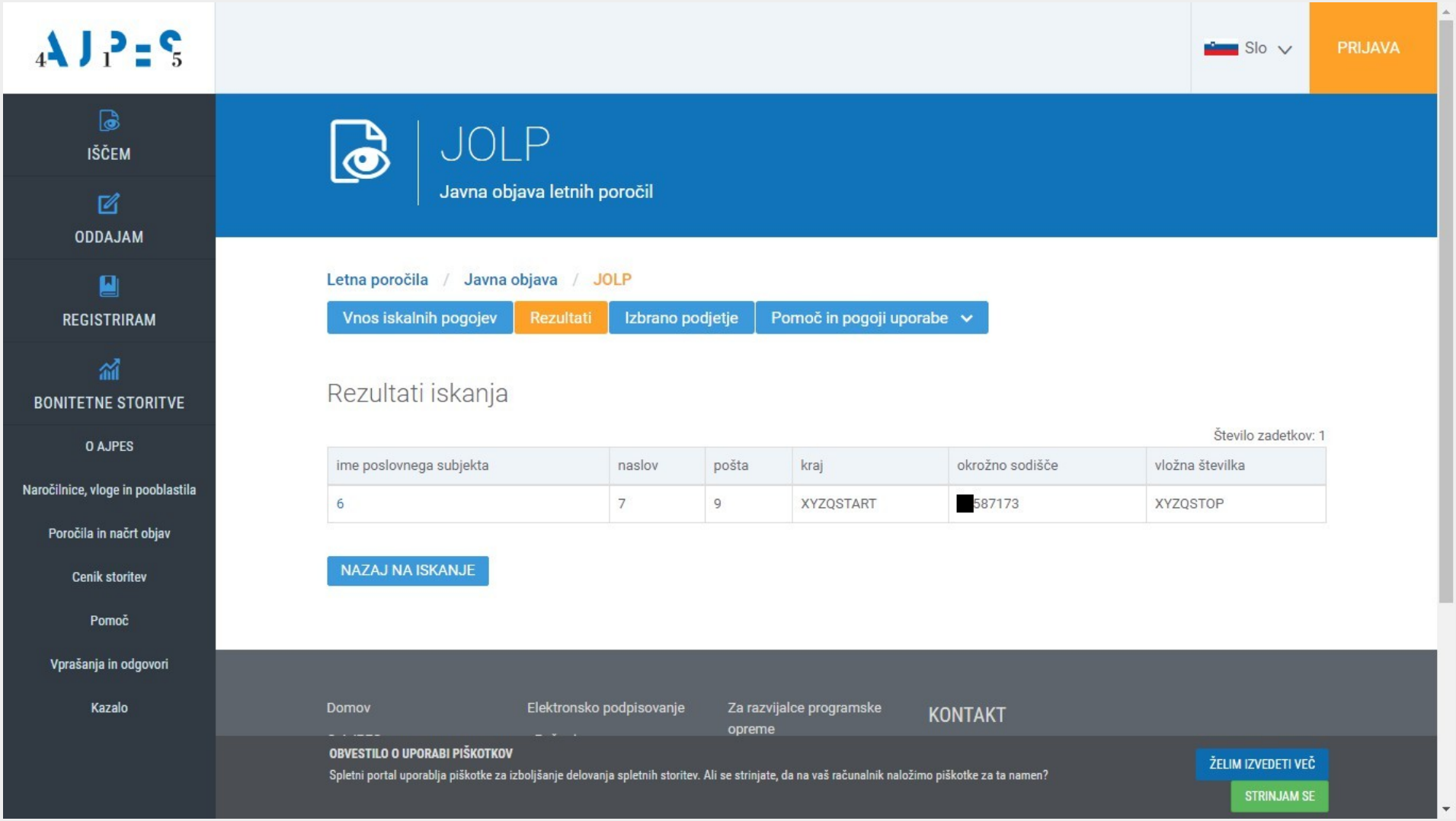
ISIS supporter gets at least 30 years for plot to kill Theresa May

US soldier to plead guilty to trying to help ISIS

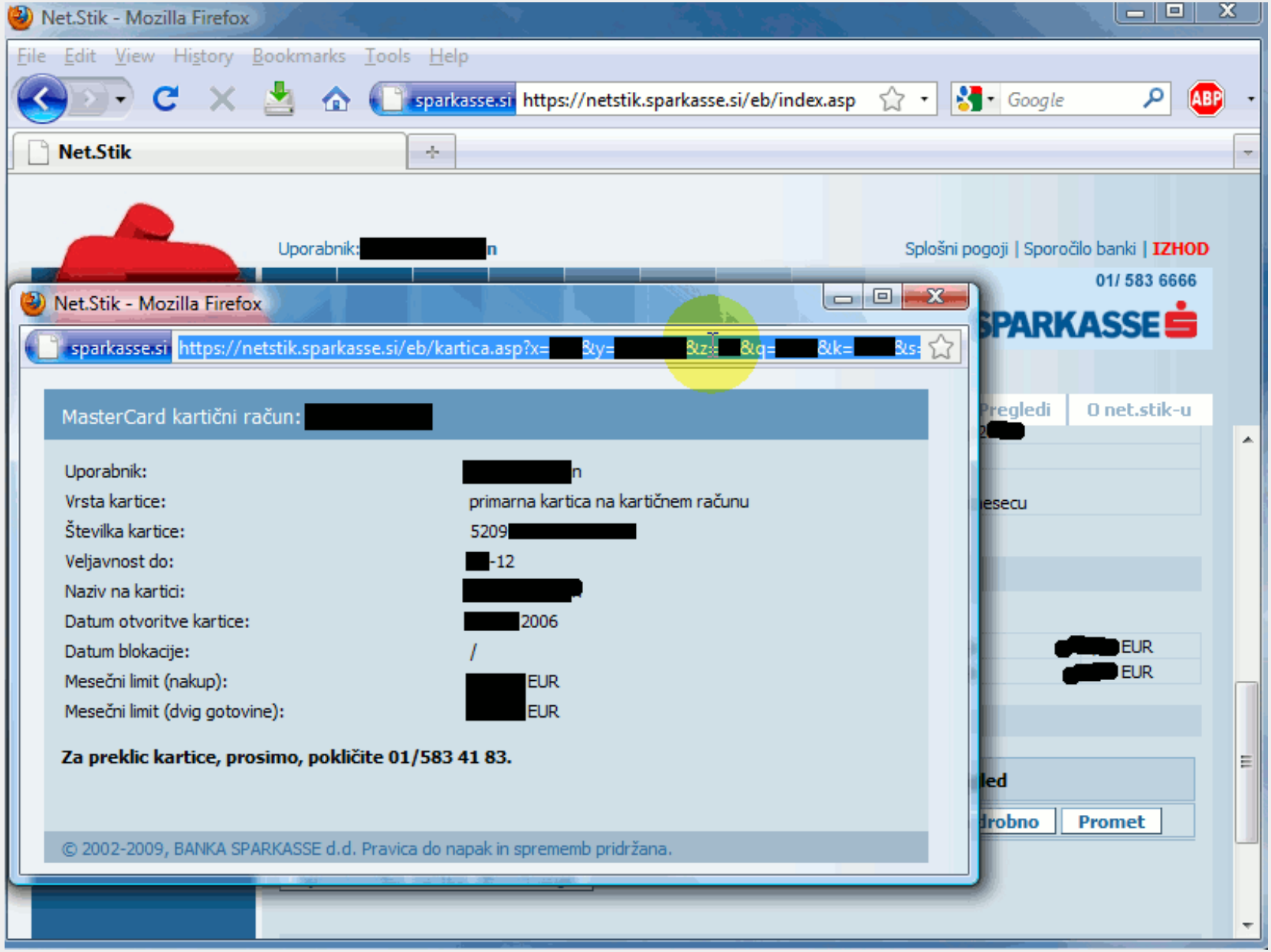
Islamic State thugs can blame the destruction of a headquarters building on a social media "moron" in their ranks who posted a selfie that pinpointed the site.

Air Force Gen. Hawk Carlisle, head of Air Combat Command, said that eagle-eyed airmen with a recon and surveillance group in Hurlburt Field, Florida, spotted the telltale post, Defense Tech reported via Military.com.

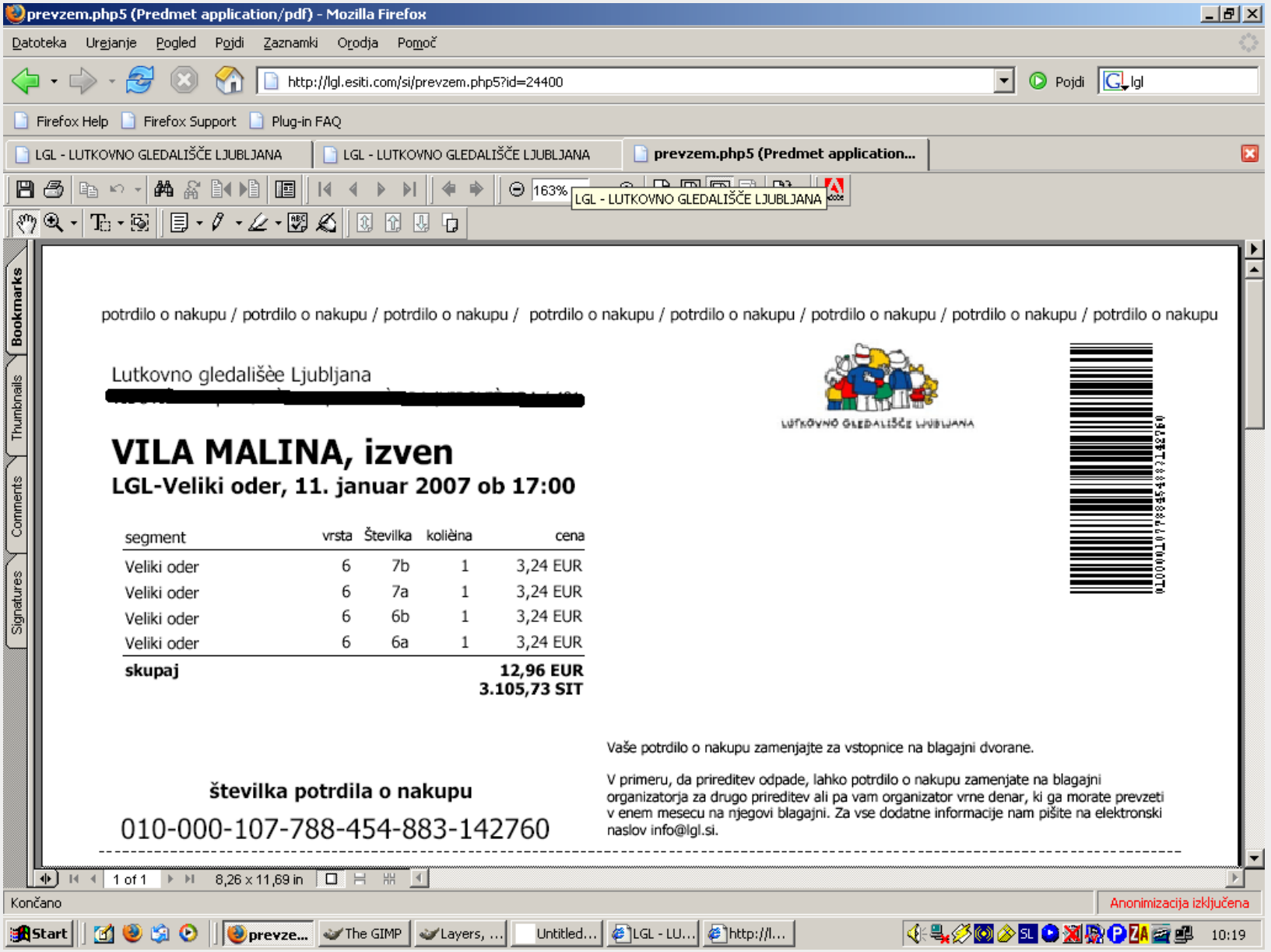
Napadi preko spletnih aplikacij



Napadi preko spletnih aplikacij



Napadi preko spletnih aplikacij



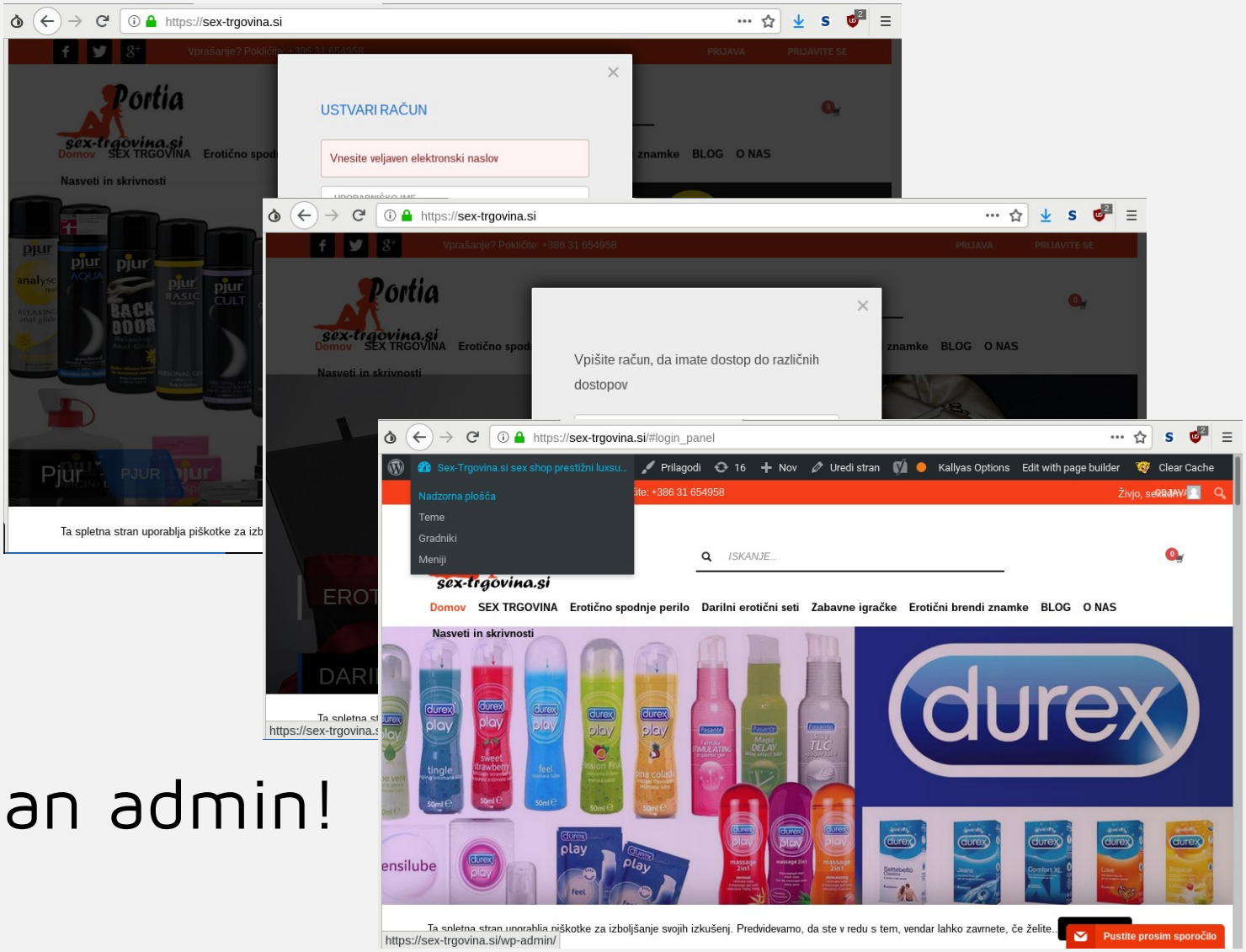
Napadi preko spletnih aplikacij

How to become a hacker?

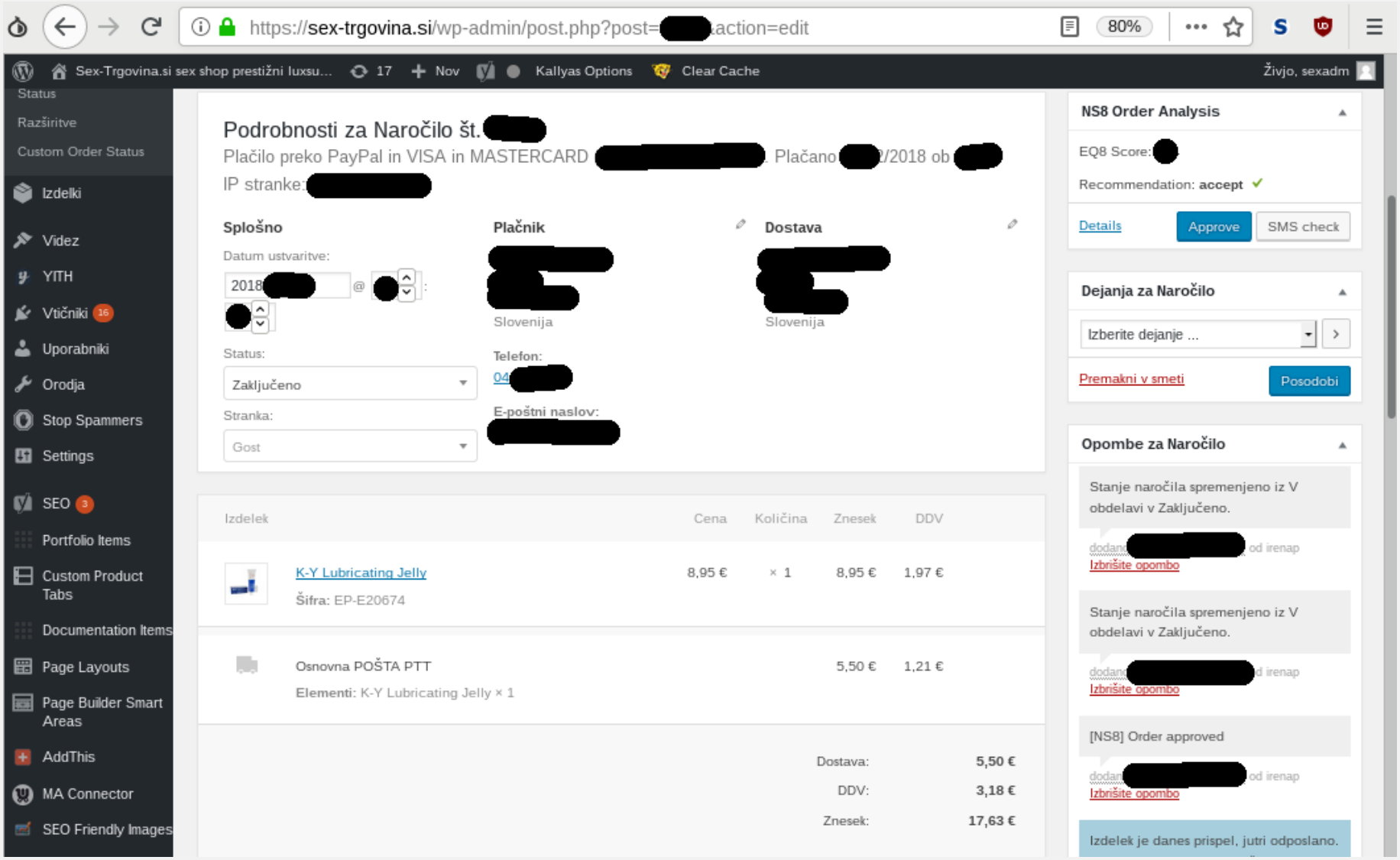
1. Register.

2. Login.

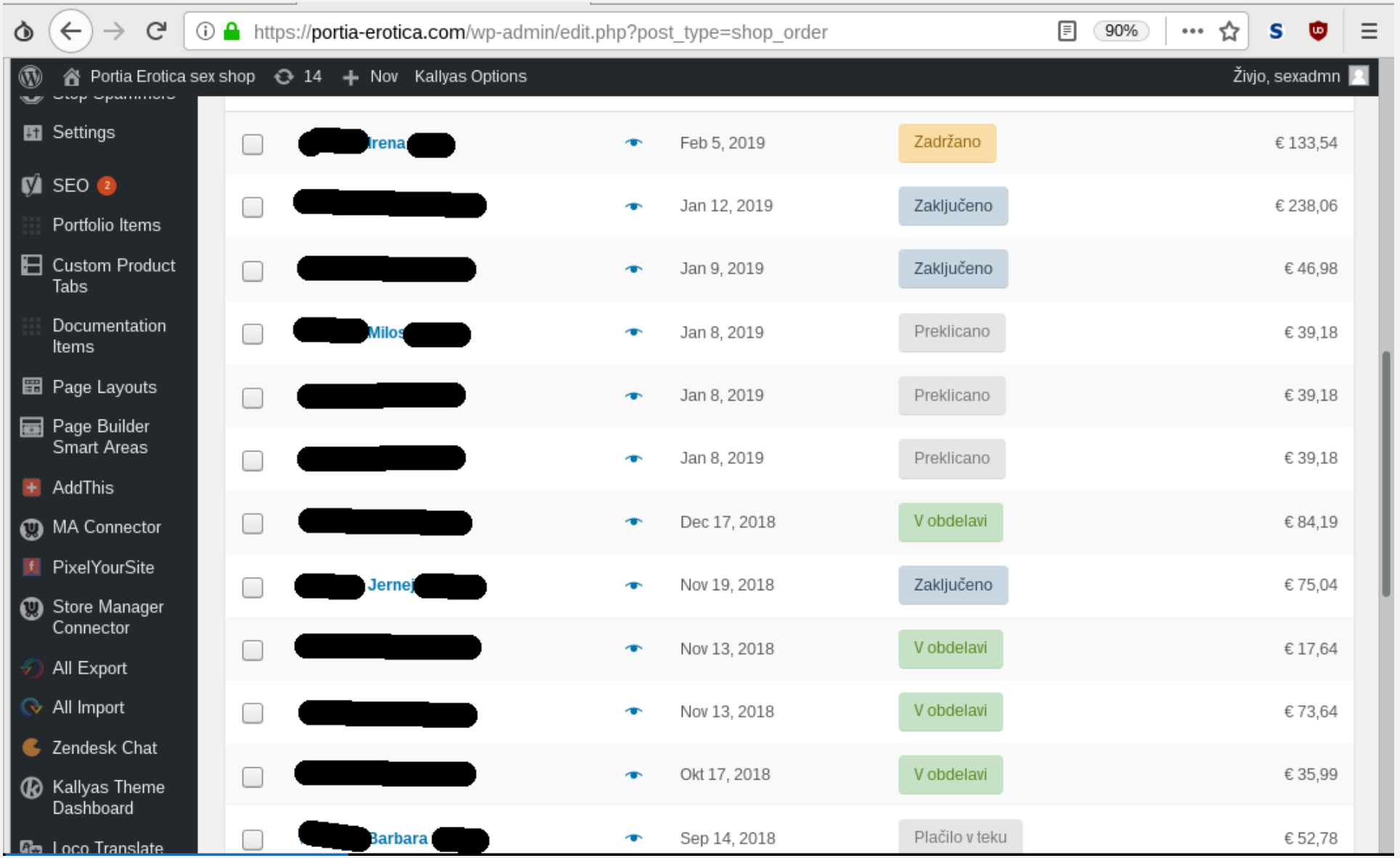
3. Become an admin!



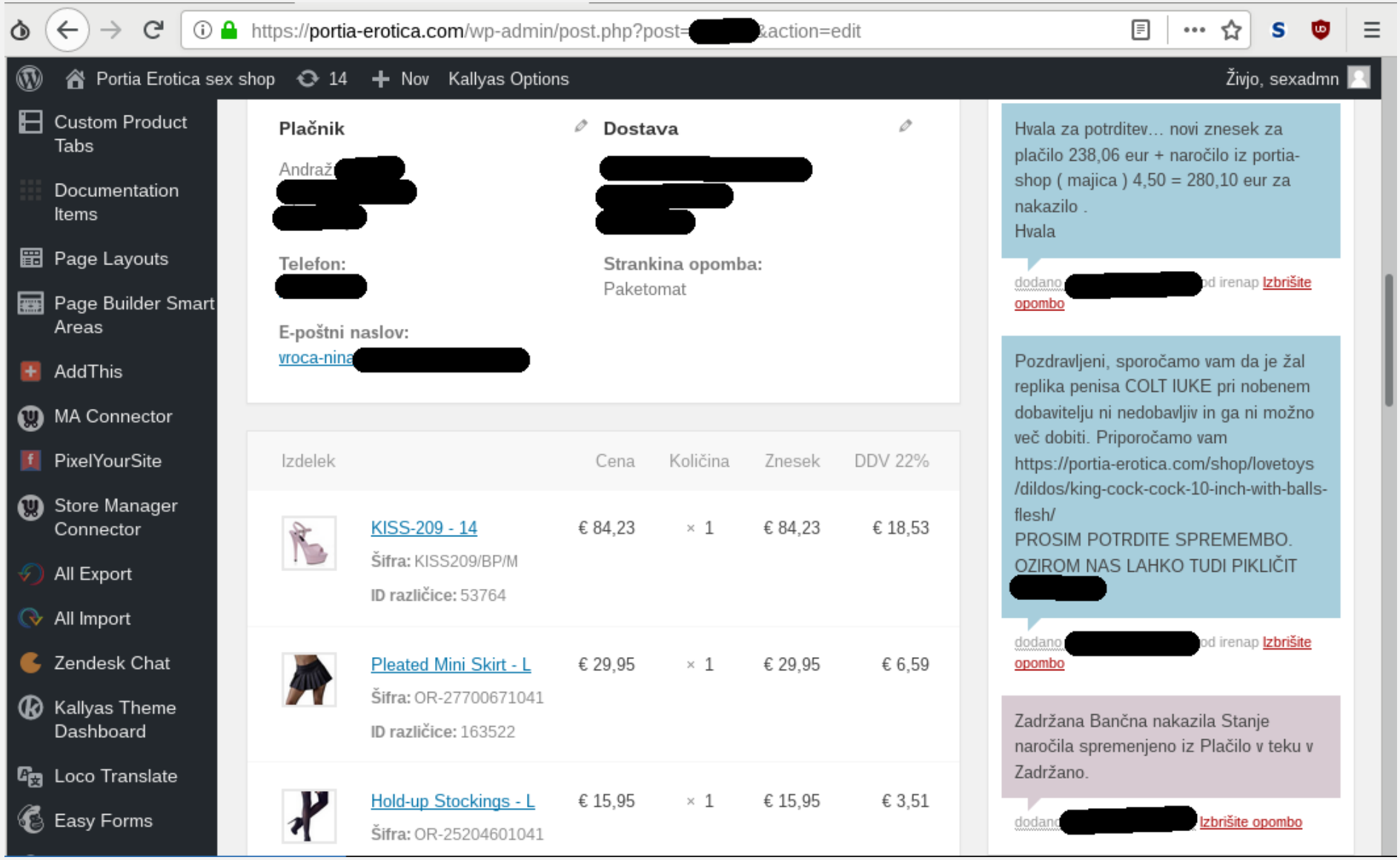
Napadi preko spletnih aplikacij



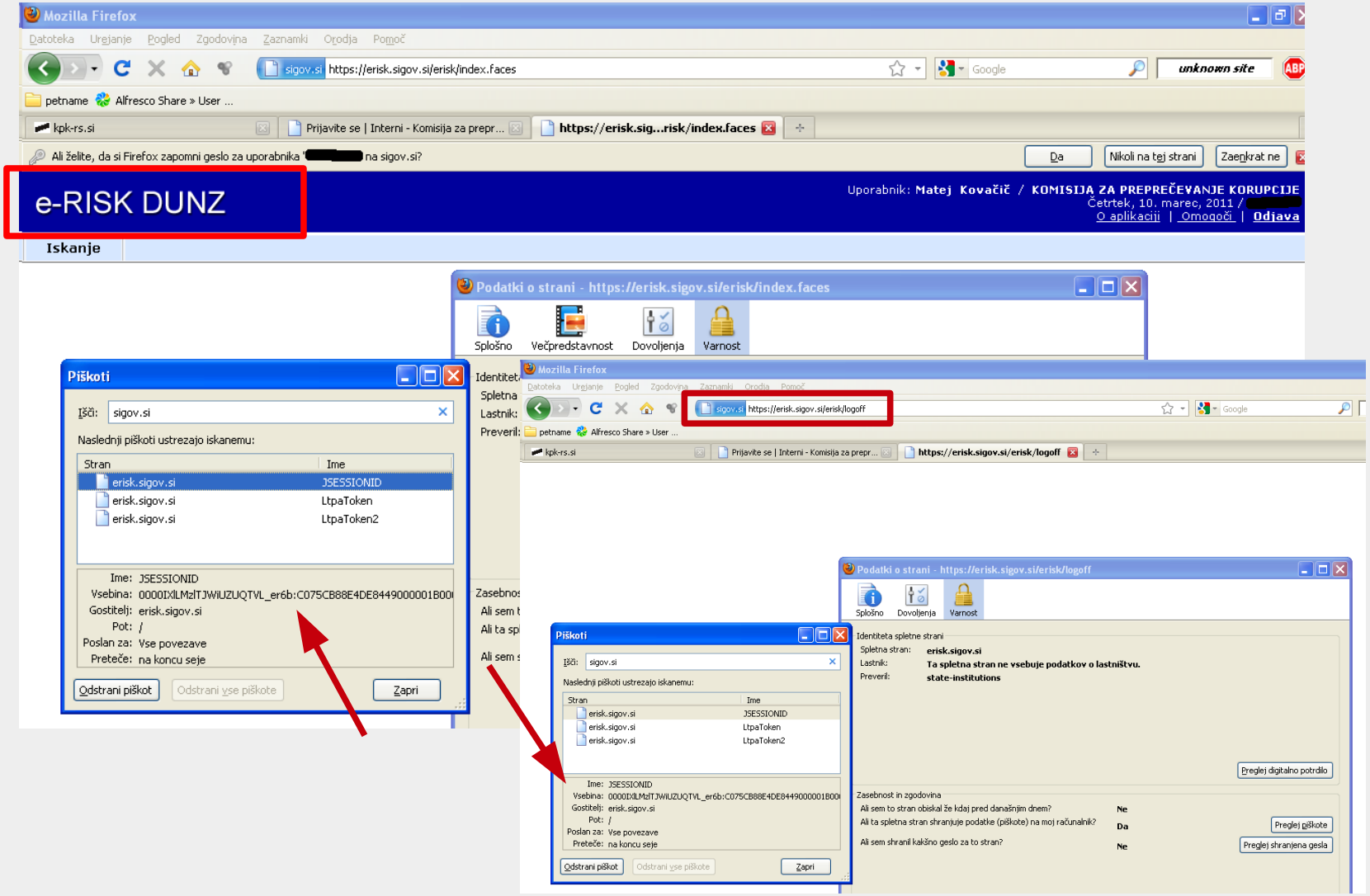
Napadi preko spletnih aplikacij



Napadi preko spletnih aplikacij



Interne aplikacije...



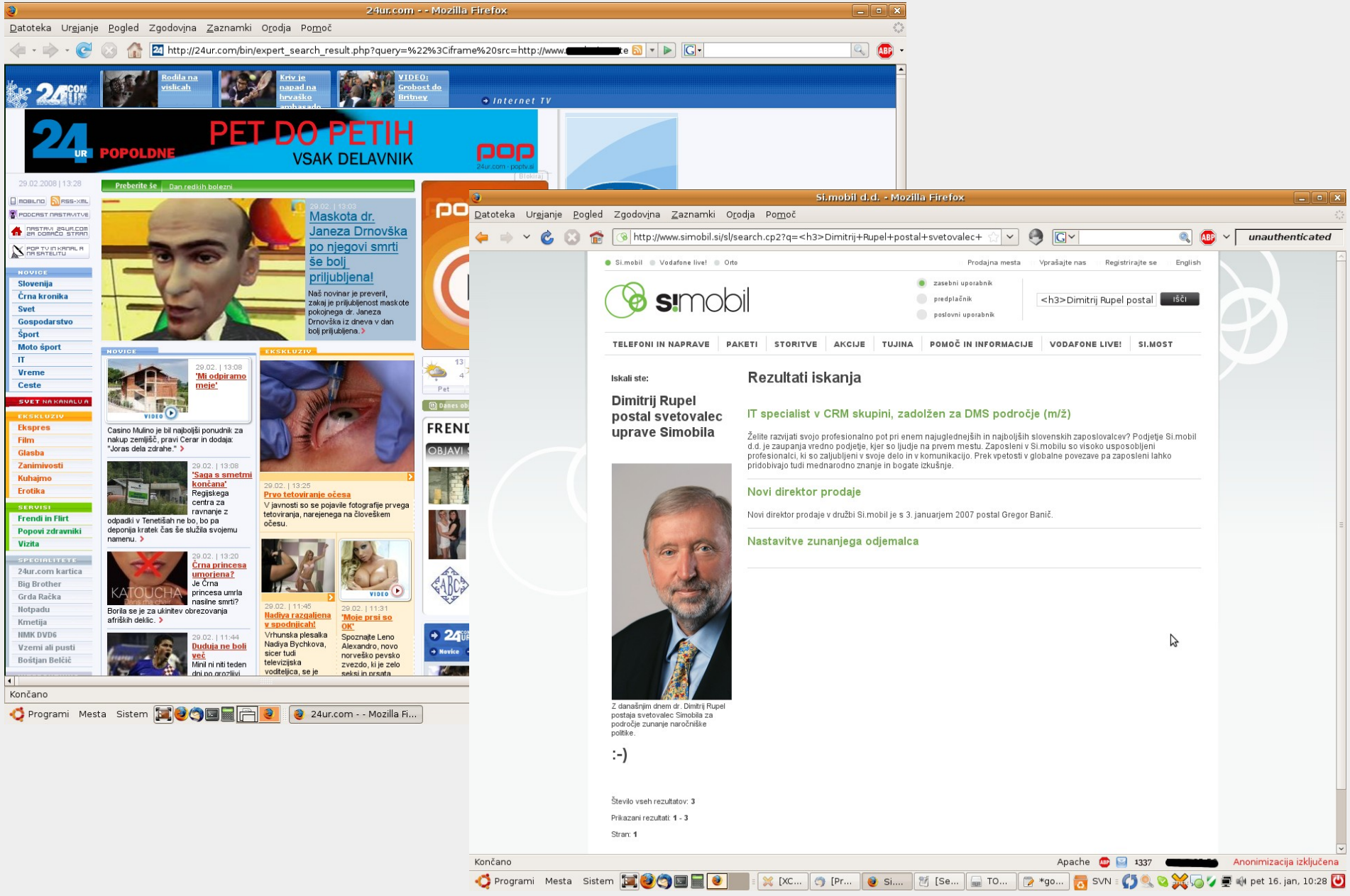
Ali pa... :)

In West Memphis District Court yesterday, Tristian Wilson was set to appear on the docket for a bond hearing on the charges. When he did not appear, Judge William "Pal" Rainey inquired about his release and found that a jail staff member released Wilson by the authority of a fax sent to the jail late Saturday night.

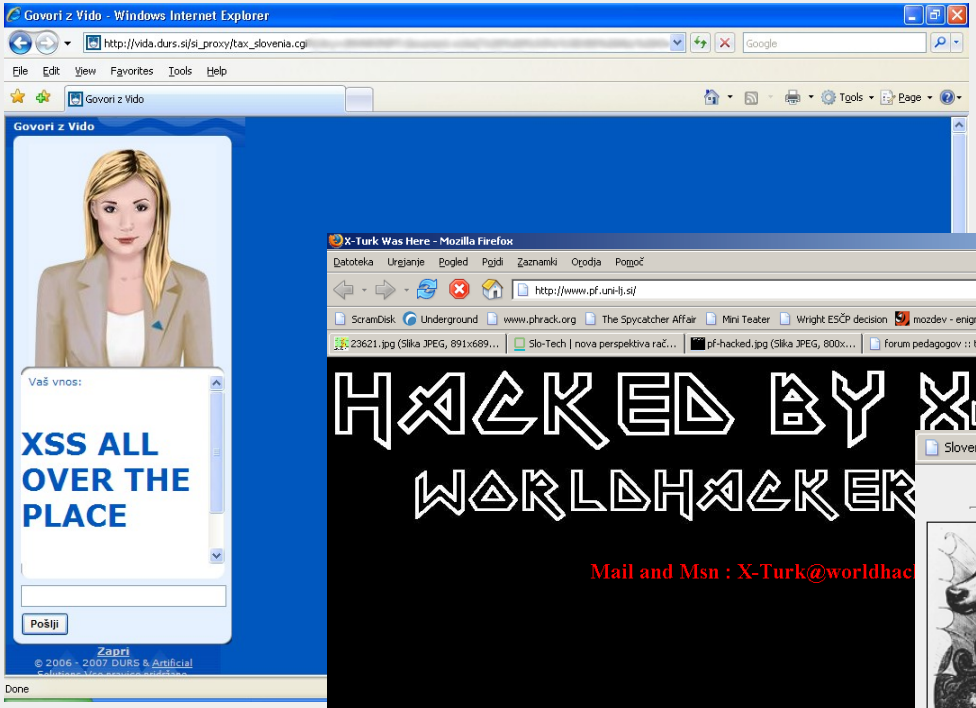
According to Assistant Chief Mike Allen, a fax was sent to the jail which stated "*Upon decision between Judge Rainey and the West Memphis Police Department CID Division Tristian Wilson is to be released immediately on this date of October 30, 2004 with a waiver of all fines, bonds and settlements per Judge Rainey and Detective McDugle.*"

Vir: `https://www.schneier.com/blog/archives/2004/11/hacking_faxes.html`

Zaupanje vsebini na spletu?



Zaupanje vsebini na spletu?

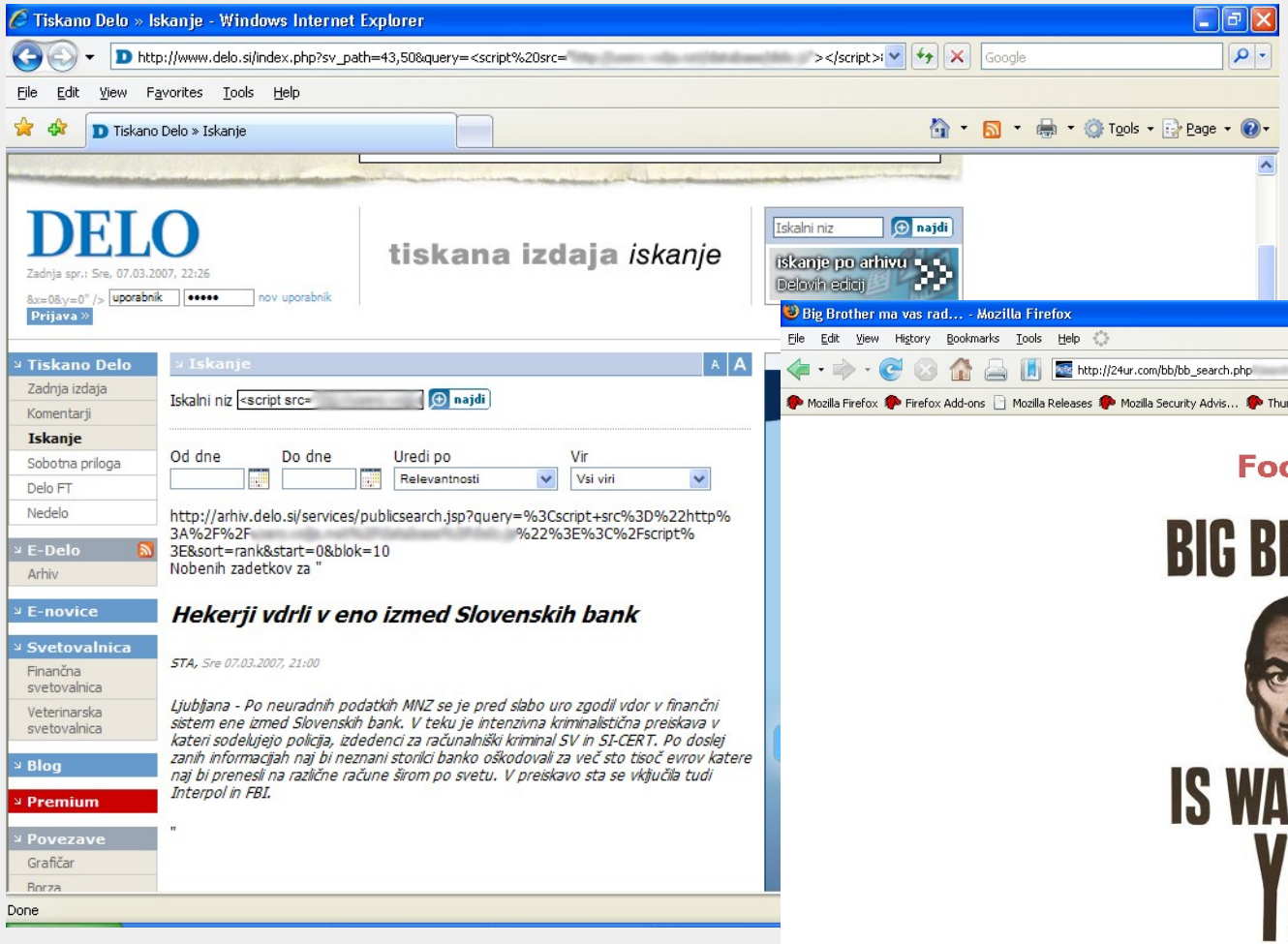


XSS napad na "davčno Vido".

Pravna fakulteta, Univerza v Ljubljani, februar 2007

Razobličenje spletne strani rimokatoliške cerkve.

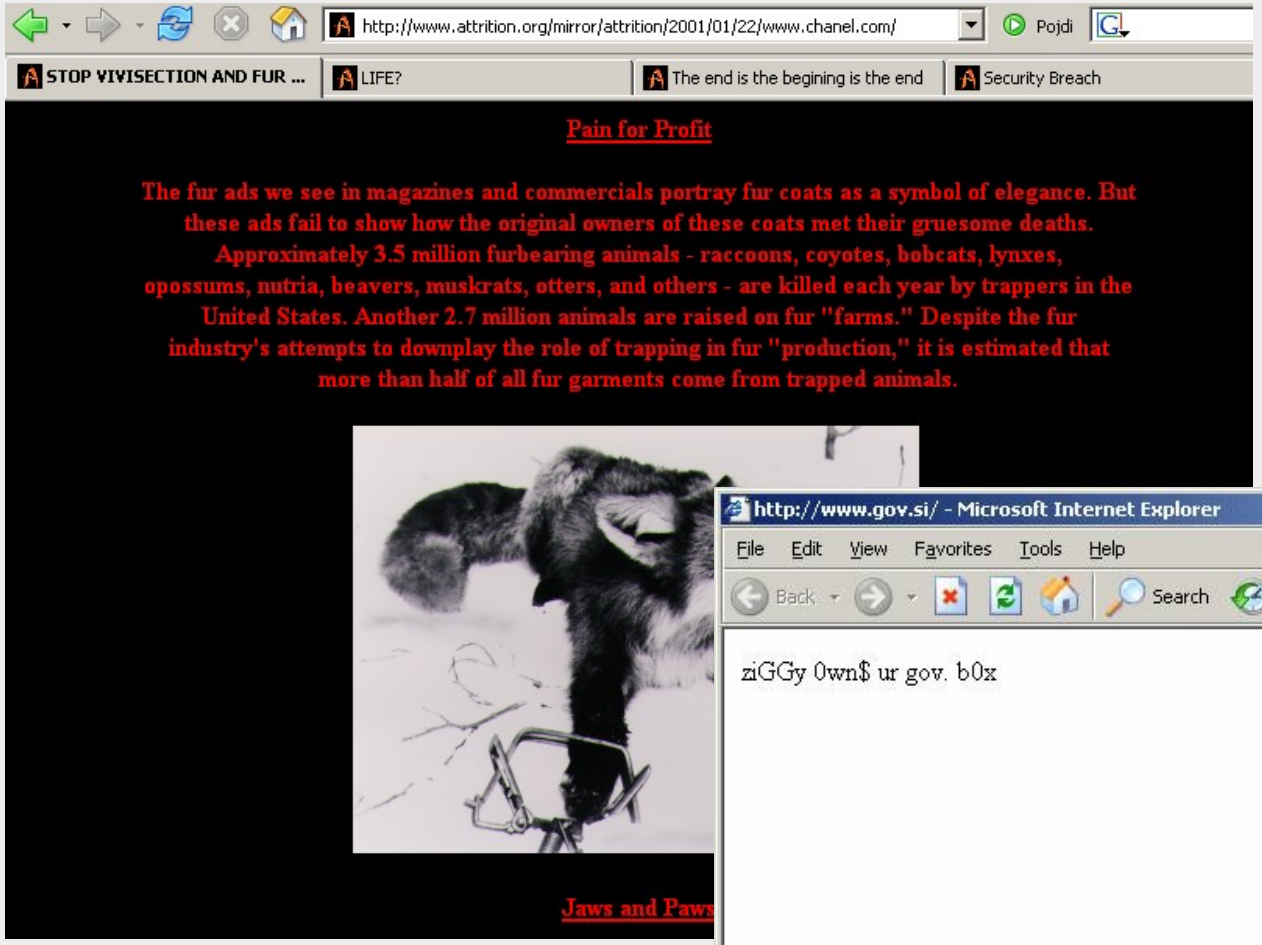
Zaupanje vsebini na spletu?



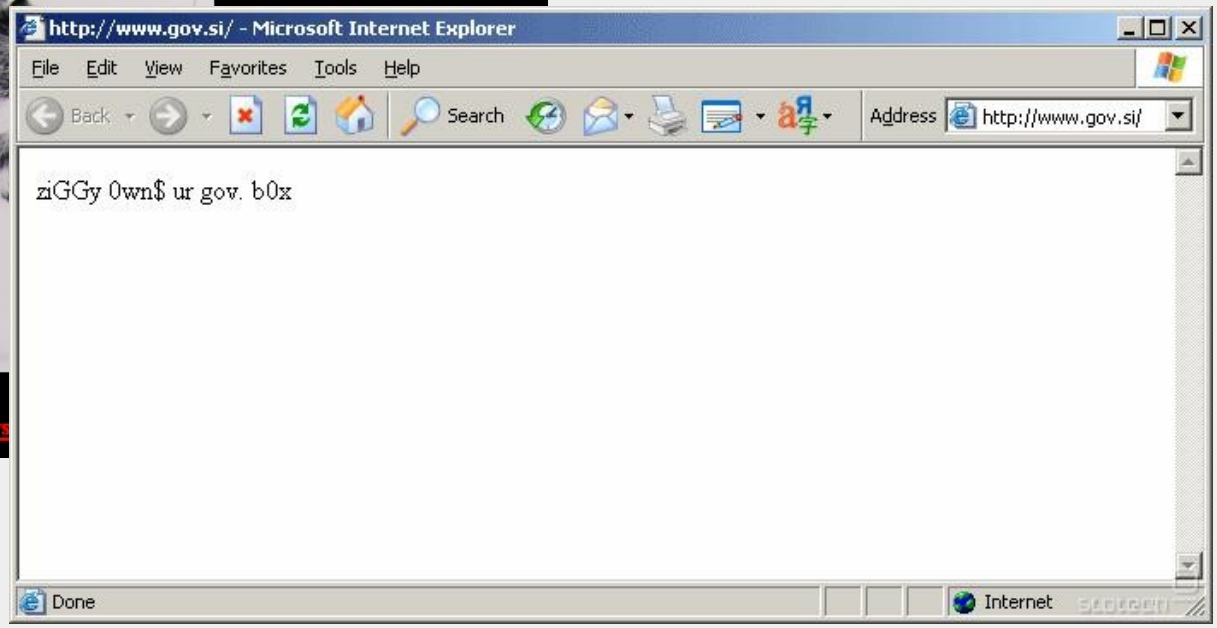
Lažna novica na spletni strani časnika DELO (XSS napad).

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

Zaupanje vsebini na spletu?



Razobličenje spletne strani modne hiše Chanell.com



Razobličenje vladne strani (gov.si).

Prevare (scam) in socialni inženiring

Scam (prevara)

A scam is a deceptive scheme or trick used to cheat someone out of something, especially money. Scam is also a verb meaning to cheat someone in such a way.

> **noun**: *a confidence game or other fraudulent scheme, especially for making a quick profit; swindle.*
>
> **verb** (*scammed, scamming*): *to cheat or defraud (someone) with a scam*.

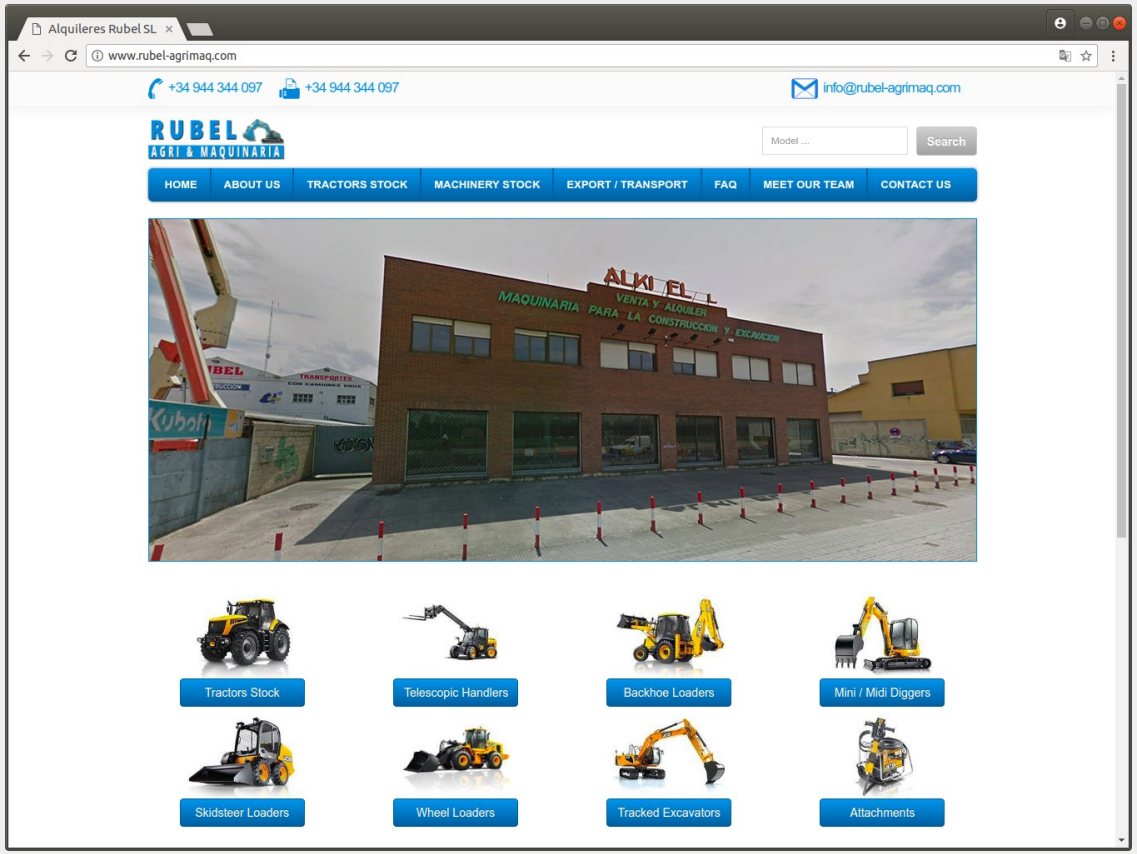
Tipi prevar

- Poskusi pridobivanja osebnih podatkov.
- Prodaja ali nakup.
- Zmenki in romantika.
- Lažna dobrodelnost.
- Investicije.
- Službe in zaposlitev.
- Grožnje in izsiljevanje.
- Nepričakovan denar (dediščina, nagrade,...).
- Piramidne sheme.
- Prevare z lažnim predstavljanjem za državne organe.

Prevarantska spletna trgovina #1

Zgodba:

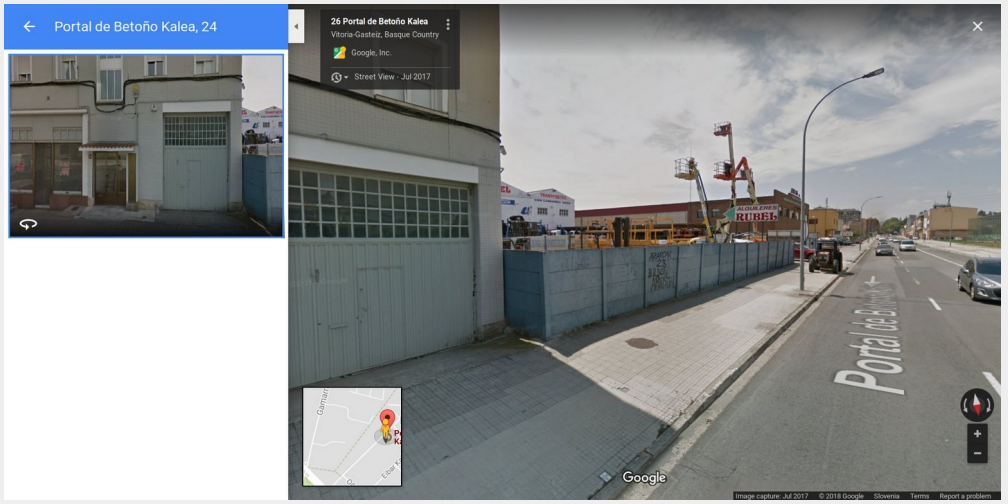
- Uporabnik je želel kupiti manjši bager. Našel je spletno trgovino z zelo ugodnimi cenami.



Prevarantska spletna trgovina #1

Zgodba:

- Nizke cene so mu bile sumljive, zato se je odločil za dodatno preverjanje.
- Preveril je obstoj podjetja, pridobil bilanco podjetja, ki je vsebovala podatke o lastnikih, letni promet, število zaposlenih...
- Na Google StreetView je preveril celo sedež podjetja.



Prevarantska spletna trgovina #1

Zgodba:

- Preko e-pošte je kontaktiral predstavnika podjetja. Komunikacija je bila hitra, profesionalna in v dobri angleščini.
- Vendar pa je podjetje želelo, da kupnino nakaže na bančni račun njihove podružnice na Portugalskem, "*da bi se izognili nekaj davkom*".
- Ko je želel preveriti VIN številko delovnega stroja, se mu predstavniki podjetja niso več oglašali.

Prevarantska spletna trgovina #1

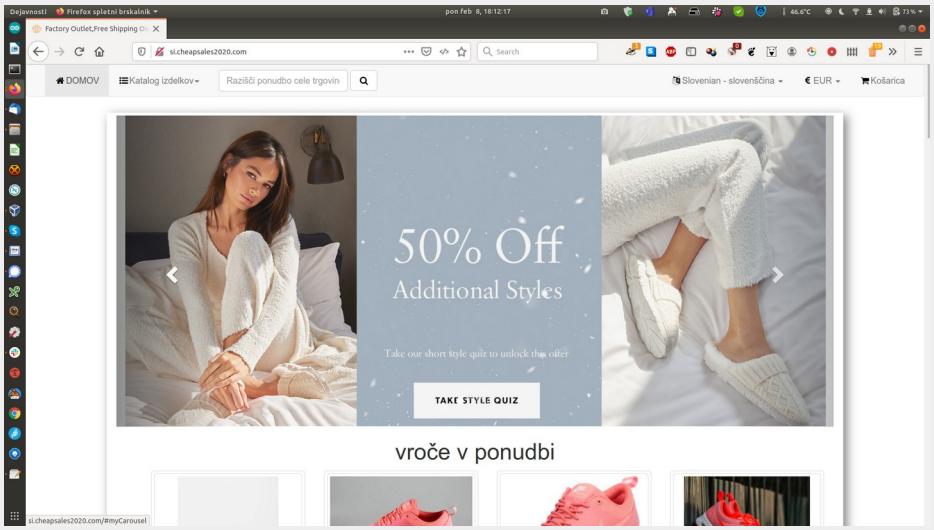
Analiza:

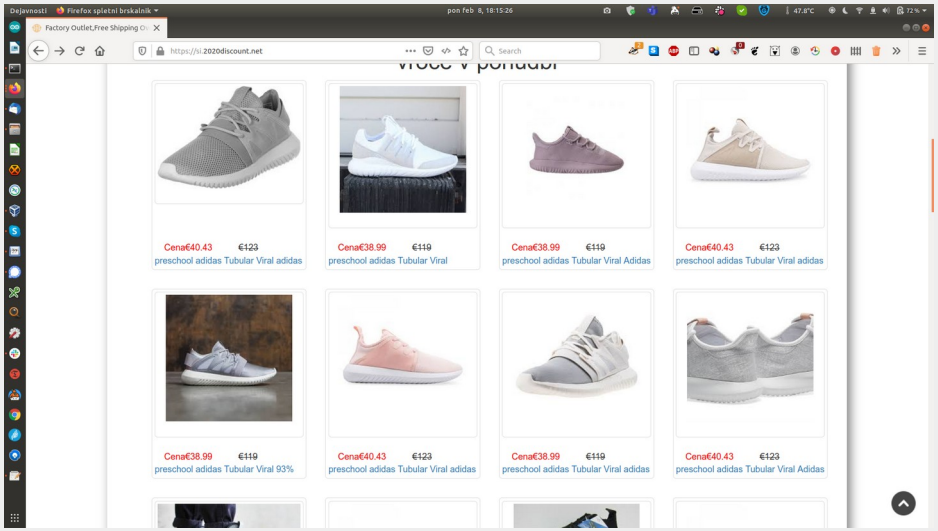
- Spletni strežnik se je nahajal v Rusiji (omrežje *nic.ru*). Prav tako je bila v Rusiji registrirana domena.
- Iskanje je pokazalo, da je bila podobno zveneča domena (*rubel-maquinaria.com*) pred tem registrirana v Maleziji. Storilci so upravljali tudi goljufivo spletno stran z gradbenimi stroji na domeni *budo-maszyny.com* (nahajala naj bi se na Poljskem). Uporabljali so enako spletno predlogo. Obe spletni strani sta bili razkriti kot prevarantski in umaknjeni s spleta.
- Danes domena *rubel-agrimaq.com* ni več dostopna.

Prevarantska spletna trgovina #2

Preko neželjene e-pošte so storilci oglaševali več lažnih spletnih strani, ki so v slovenskem jeziku ponujale poceni blago.

Različne, a podobno zveneče domene: *si.2020discount.net*, *sisale2021.com*, *si.cheapsales2020.com*, itd.





Prevarantska spletna trgovina #2

Prvi opozorilni znak:

- Zelo poceni izdelki ("*Če je preveč dobro, da bi bilo res, potem najverjetneje ni res*").

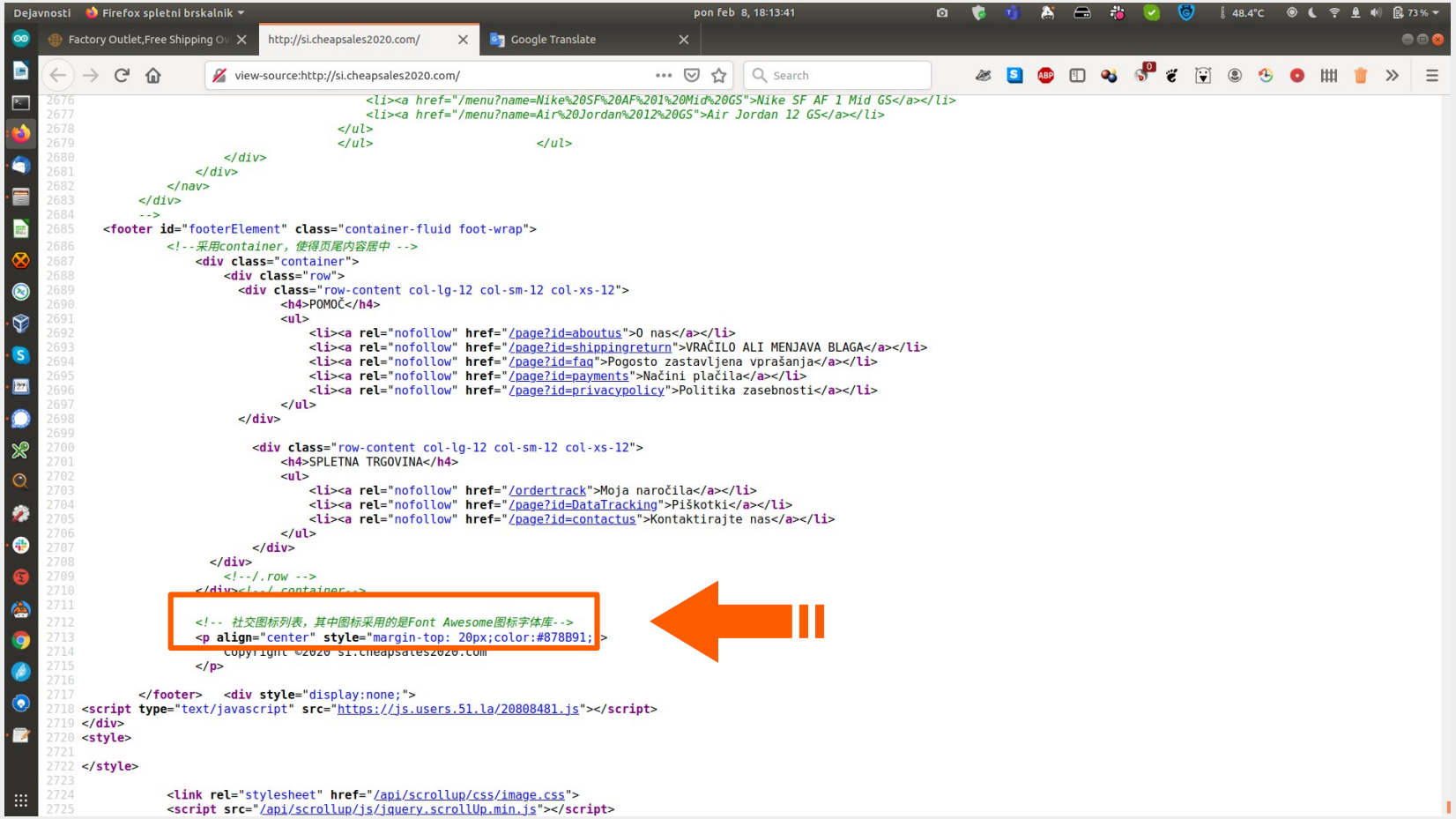
Poglobljena analiza:

- IP naslov skrit za Cloudflare omrežjem.
- Spletne strani so delovale preko HTTPS (zagotavljal ga je Cloudflare).

Prevarantska spletna trgovina #2

Poglobljena analiza:

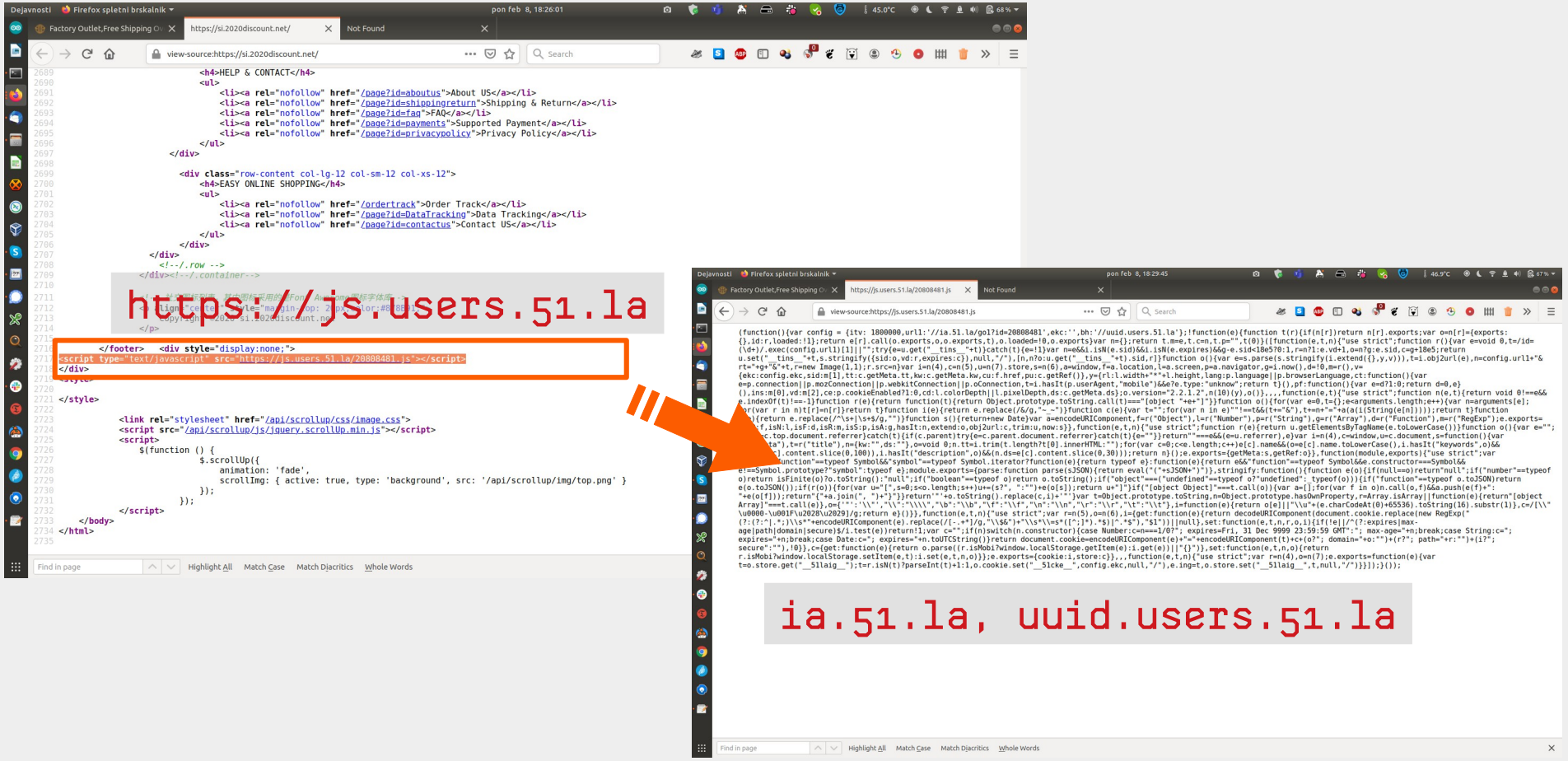
- komentarji HTML kode v kitajščini.



Prevarantska spletna trgovina #2

Poglobljena analiza:

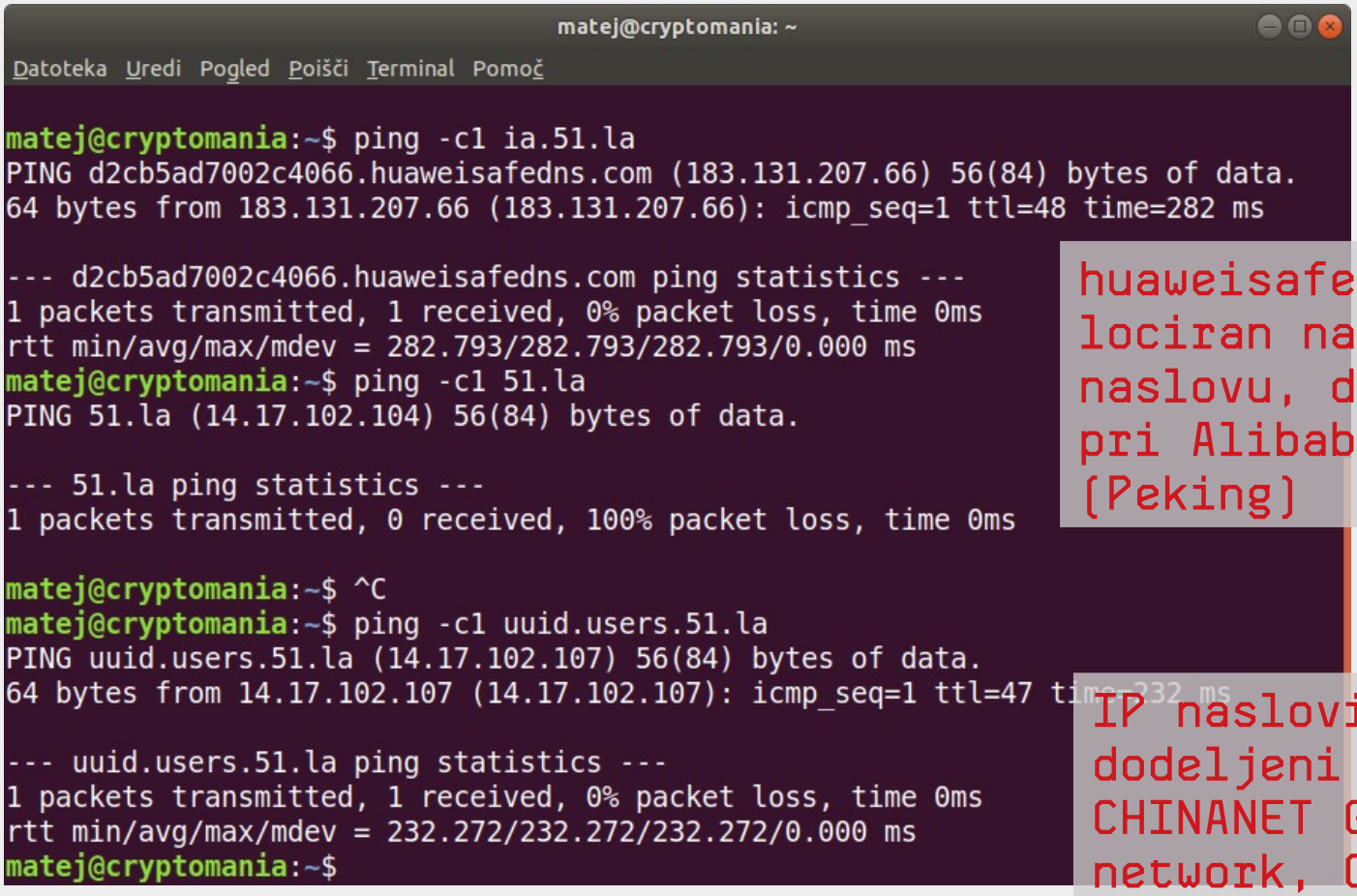
- najdena JavaScript sledilna koda...



Prevarantska spletna trgovina #2

Poglobljena analiza:

- ...ki je vodila na kitajske strežnike.



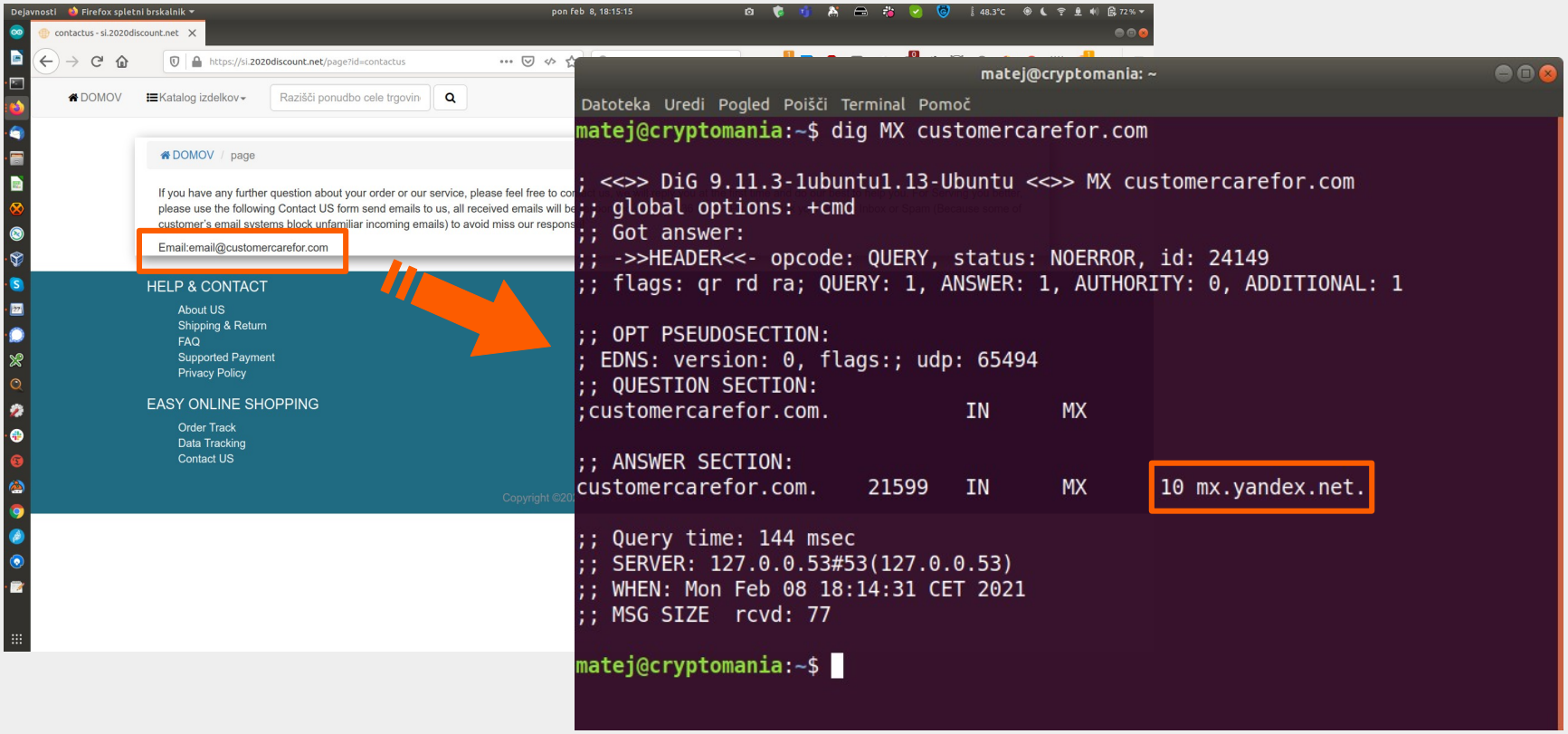
huaweisafedns.com
lociran na švicarskem IP naslovu, domena registrirana pri Alibaba Cloud Computing (Peking)

IP naslovi 14.17.100.0/22 dodeljeni CT-FOSHAN-IDC CHINANET Guangdong province network, CN

Prevarantska spletna trgovina #2

Poglobljena analiza:

- kontaktni e-naslov (email@customercarefor.com) na ruskih strežnikih (Yandex.net).



Zbiranje osebnih podatkov

Zgodba:

- Google Ads oglasi na spletnih straneh slovenskih medijev so oglaševali intervju z znano slovensko novinarko o njenih zdravstvenih težavah in lažnem zdravilu, ki ji je pomagalo.
- Lažni intervju je izgledal podobno kot bi bil objavljen na znani novičarski strani.
- Besedila so bila slovnično zelo pravilna (boljše kot prevodi z Google Translate).

Zbiranje osebnih podatkov

Zgodba:

- Komentarji pod člankom so bili večinoma pozitivni (a tudi negativni!), napisani s strani lažnih uporabnikov s slikami in s slovensko zvenečimi imeni.

Zbiranje osebnih podatkov

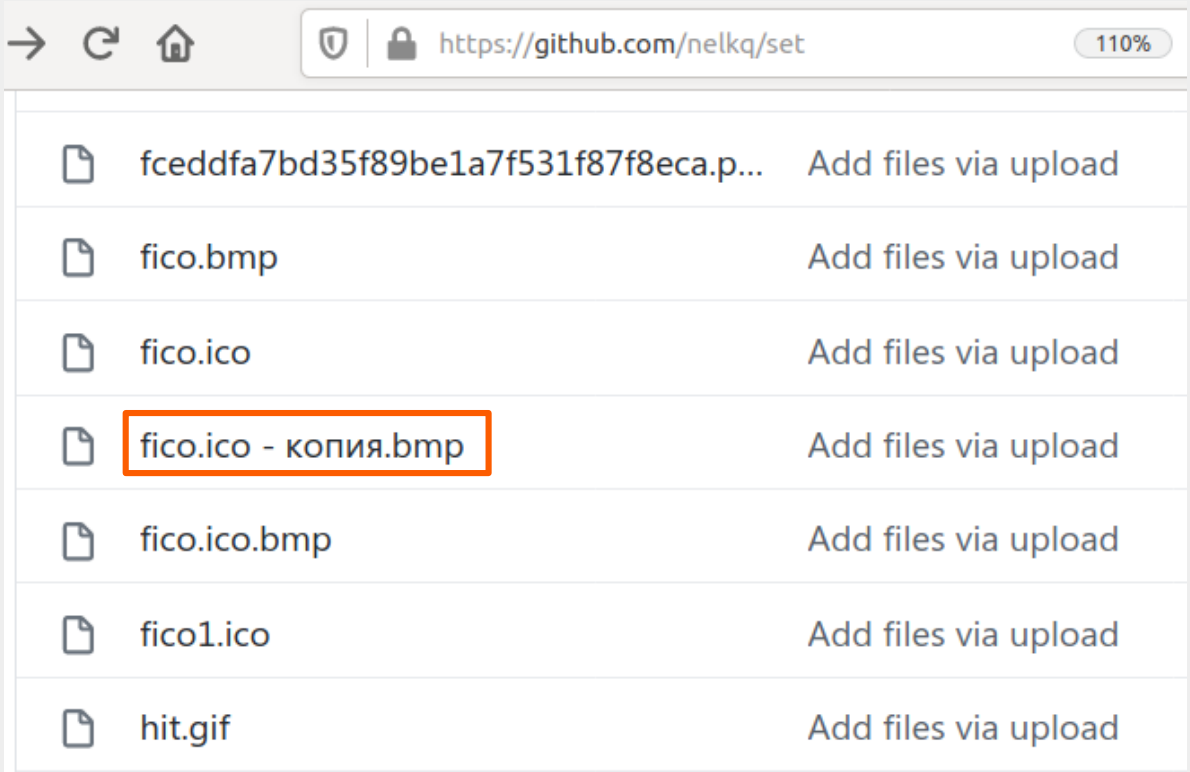
Analiza:

- Lažna spletna stran je gostovala na Github Pages.
- Uporabnike so vabili, da se registrirajo za prejem brezplačnega zdravila.
- Vnosni obrazec je zbiral osebne podatke, **ne pa tudi podatkov o kreditni kartici**.
- Vnosni obrazec je gostoval na ruskem spletnem strežniku.

Zbiranje osebnih podatkov

Analiza:

- Najdena je bila datoteka z imenom v ruskem jeziku (“fico.ico – копия.bmp”).
- Komentarji HTML kode v ruskem jeziku.



Zbiranje osebnih podatkov

Analiza:

- Z nadaljnjim iskanjem smo našli kontaktne informacije (e-naslov, mobilni telefon) osebe, ki je registrirala lažno domeno in ugotovili, da gre za Rusa, ki živi na območju Moskve.
- Ta oseba se je zahvaljevala prevajalcem na spletni strani *kwork.ru* za "hitre in točne prevode" v različne vzodnoevropske jezike (to razloži kvaliteto prevodov na lažnih spletnih straneh).

Zbiranje osebnih podatkov

Analiza:

- Našli smo podobne prevare, namenjene publiki na Poljskem in Češkem (lažni intervjuji v lokalnem jeziku, kjer so se pojavljale njihove lokalne slavne osebe,...).
- O lažnih straneh so bili obveščeni na Github Pages in lažne strani so bile umaknjene. Žal pa se novi lažni članki še vedno pojavljajo preko Google Ads oglasov, prevarantje pa odpirajo nove račune na Github Pages...

Usmerjen napad preko Facebooka

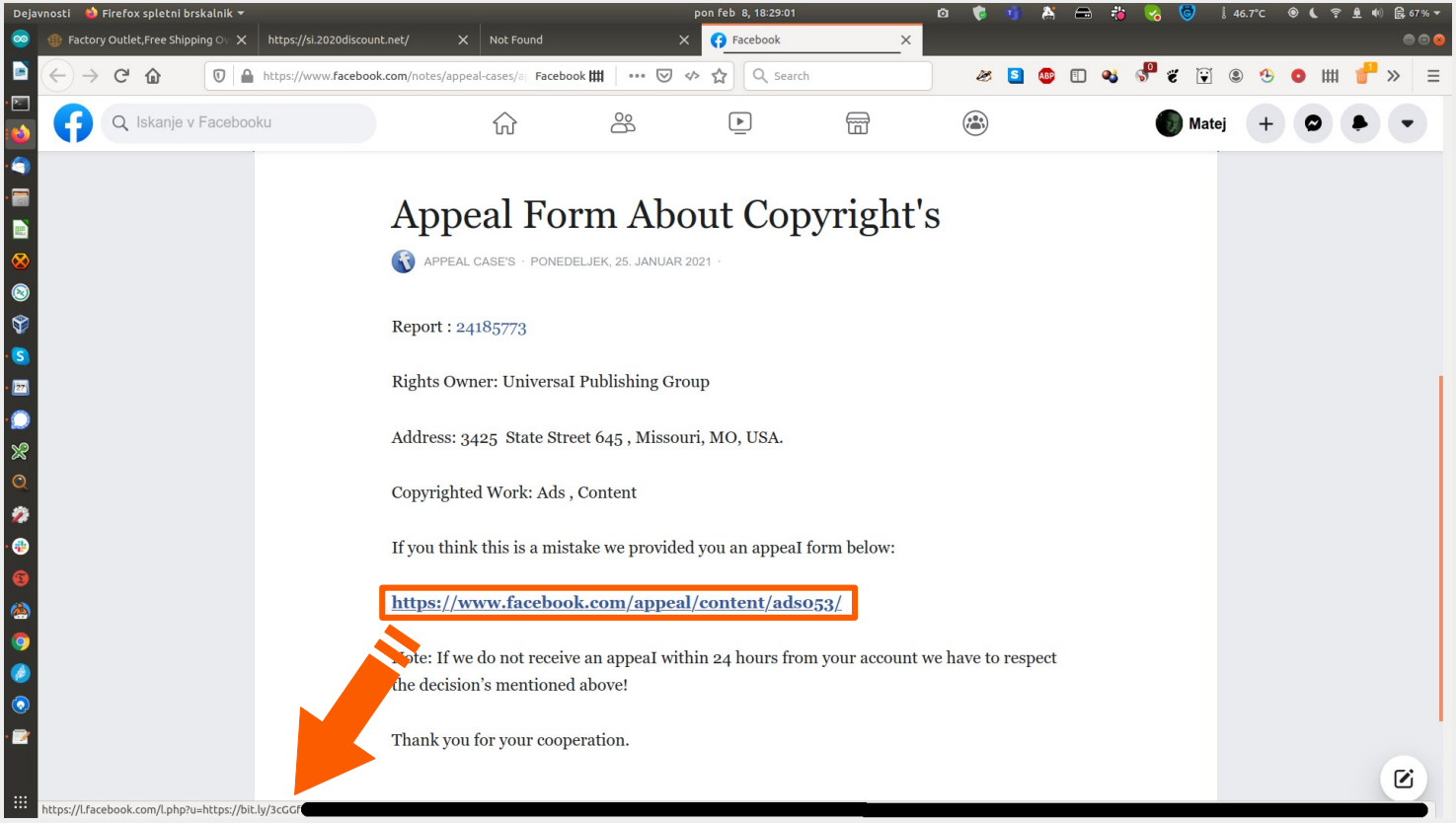
Zgodba:

- Uporabnik je na svojem Facebook profilu objavil sliko.
- Nekaj dni za tem (8. februarja 2021) je prejel obvestilo, da objava krši avtorske pravice in da se mora o kršitvi izjasniti.
- E-pošta je vsebovala povezavo na Facebook.
- Vendar pa je povezava kazala na Facebook Notes – gre za del Facebooka, ki ga ustvarjajo uporabniki (a se nahaja na Facebookovi domeni).

Usmerjen napad preko Facebooka

Kaj se je v resnici zgodilo:

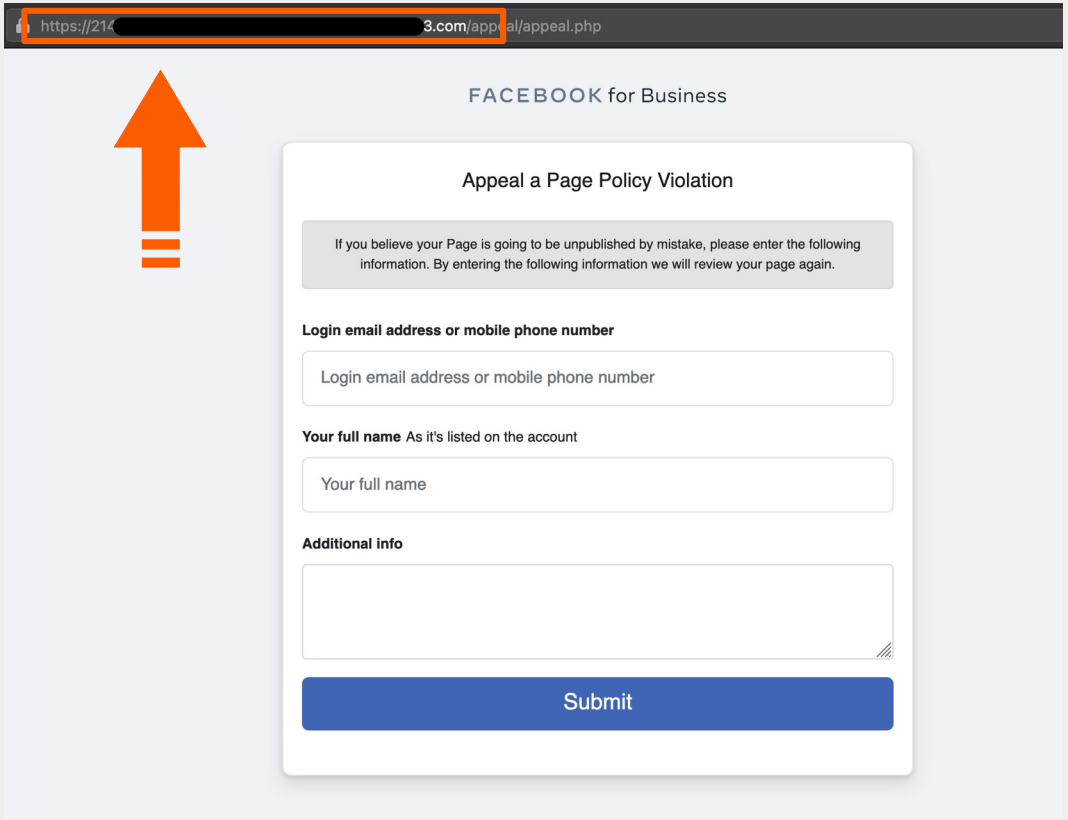
- Facebook Notes stran je vsebovala povezavo na "pritožbo". URL je kazal na bit.ly URL skrajševalec...



Usmerjen napad preko Facebooka

Kaj se je v resnici zgodilo:

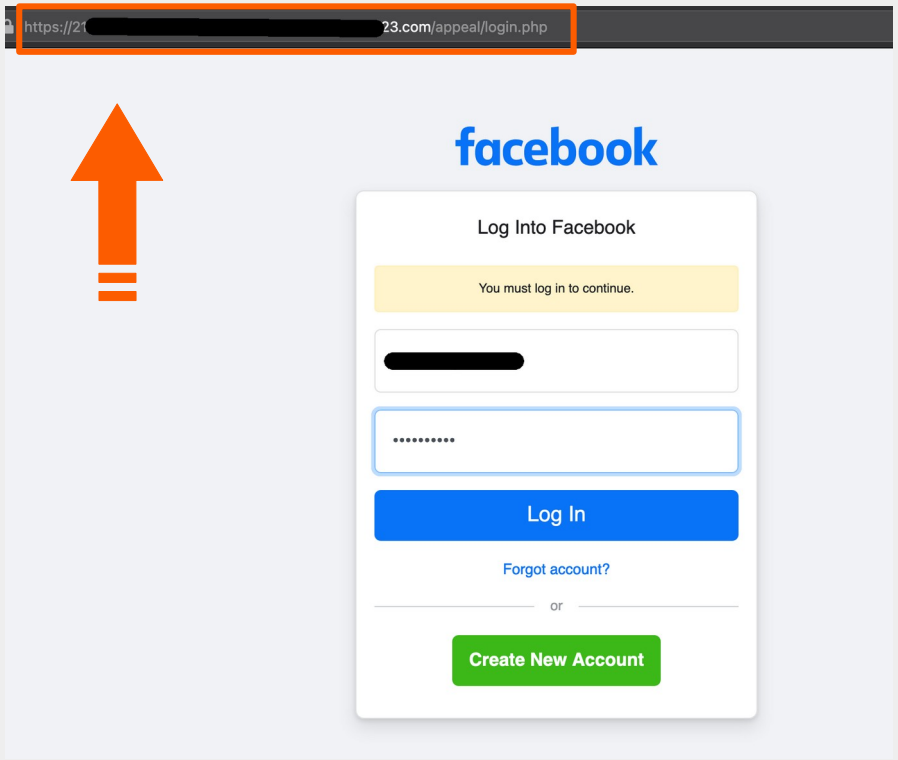
- ...bit.ly je uporabnika preusmeril na storilčevo domeno, registrirano v ZDA (3. februarja 2021).



Usmerjen napad preko Facebooka

Kaj se je v resnici zgodilo:

- ...ko je uporabnik oddal pritožbo, je stran od njega zahtevala, da se ponovno prijavi v Facebook ter mu ukradla geslo.



Ciljana oseba je bila lokalni poslovnež. Incident je bil posredovan na policijo, ki je začela s preiskavo.

Phishing napad na HBGary

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 1:59 PM
To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:06 PM
To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 2:08 PM
To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because im ready for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:10 PM
To: Greg Hoglund <greg@hbgary.com>

ok,
takes couple mins, i will mail you when ready. ssh runs on 47152

Napad na informacijsko-varnostno podjetje HBGary (podjetje je za ameriško vlado izvajalo "napade" proti skupini Anonymous).

```
...a little later:

bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
[hoglund@www hoglund]$ unset HIST
[hoglund@www hoglund]$ unset HISTFLE
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ uname -a;hostname
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed
Mar 15 14:21:45 EST 2006 i686 i686 i386 GNU/Linux
www.rootkit.com
[hoglund@www hoglund]$ su -
Password:
[root@www root]# unset HIST
[root@www root]# unset HISTFILE
[root@www root]# uname -a;hostname;id
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP Wed
Mar 15 14:21:45 EST 2006 i686 i686 i386 GNU/Linux
www.rootkit.com
uid=0(root) gid=0(root)
groups=0(root),1200(varmistus
```

Zaščita pred prevarami

- Zavedajte se, da prevare na internetu obstajajo.
- Vedite s kom imate opravka oz. s kom komunicirate.
- Ne odpirajte sumljivih povezav ali priponk v e-pošti.
- Previdno pri spletnem nakupovanju.
- Pred vnosom gesla ali finančnih podatkov se prepričajte, da ste na pravi spletni strani, ki je dostopna na HTTPS povezavi.
- Ne odgovarjajte na sporočila ali telefonske klice, kjer vas sprašujejo za oddaljen dostop do vašega računalnika.
- Ne odgovarjajte na sporočila ali zgrešene klice iz številk, ki jih ne poznate.
- Hranite svoje osebne podatke in gesla (vključno z bančnimi podatki) na varnem mestu.
- Poskrbite za to, da bodo vaši računalniki in mobilne naprave ustrezno zavarovani.
- Redno pregledujte varnostne in zasebnostne nastavitve na socialnih omrežjih.
- Bodite pozorni, če kdo želi vaše osebne podatke ali denar.

Če ponudba izgleda predobro, da bi bila resnična, potem najverjetneje tudi ni resnična.

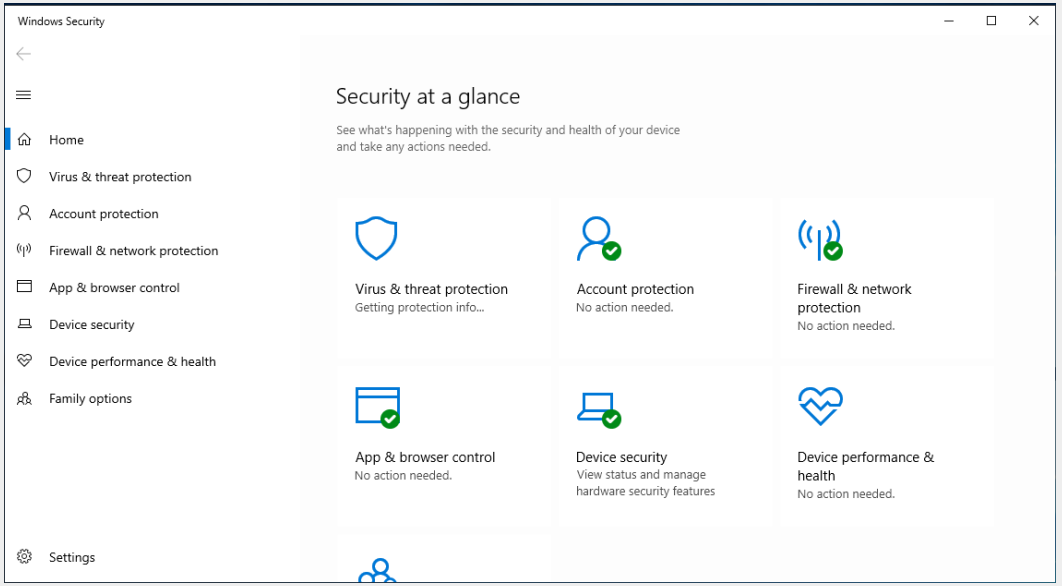
Varovanje informacijskih sistemov

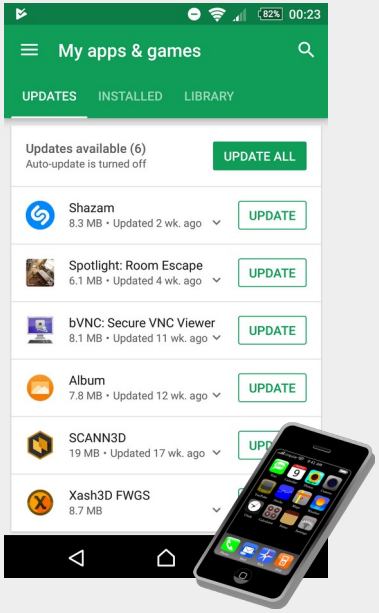
Osnovna zaščita IT sistemov

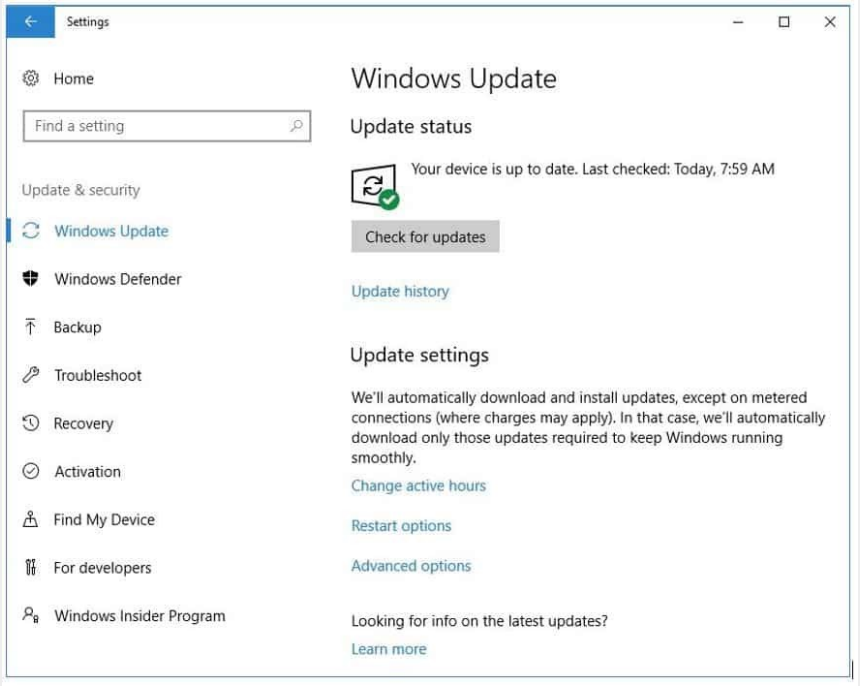
Nekatere tehnike osnovne zaščite računalniških sistemov:

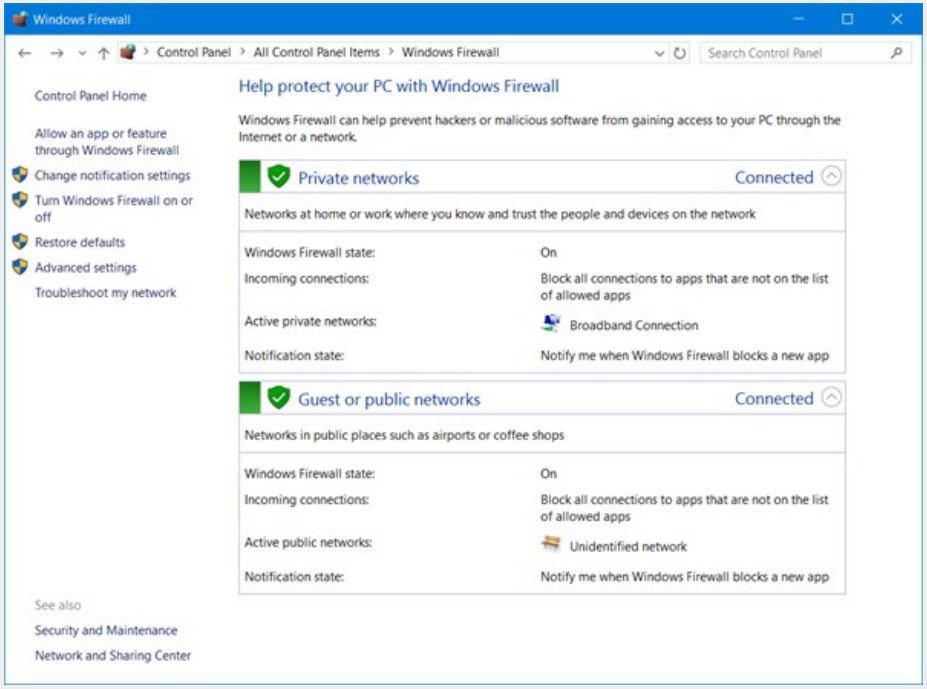
- uporaba ustreznih (in »nerecikliranih«) gesel;
- uporaba dvo- in multifaktorske avtentikacije kjer je mogoče (2FA, MFA);
- redno posodobljen sistem (vse aplikacije na vseh napravah);
- požarni zid;
- uporaba protivirusnih in protismetnih programov (blokada telemetrije?);
- varnostno arhiviranje;
- uporaba šifriranje kjer je mogoče;
- nameščanje samo tistih aplikacij, ki jih res potrebujemo;
- fizična varnost.

Osnovna zaščita









Gesla...

Vir: Schneier.com, <http://www.schneier.com/blog/archives/2009/07/information_lea_1.html>.

Pri 4-mestnem geslu je vseh možnih kombinacij 10.000. V zgornjem primeru je možnih kombinacij samo še 24. Levo geslo je najbolj verjetno 1986 ali 1968, desno pa 1234.

Gesla

Pravilo:

- čim daljše
- čim bolj kompleksno (mešanica črk in številk, po možnosti tudi mešanica velikih in malih črk ter številk)

Kako pomembno je posamezno geslo (za kaj ga uporabljamo)?

Gesla morajo biti med seboj (dovolj) različna.

Metode oblikovanja gesel

Pri **prvi metodi** geslo sestavimo iz stavka, oziroma je geslo enako stavku. Npr. “To je moje geslo”. Na ta način ni težko ustvariti dovolj dolgega gesla. Izmislimo si lahko tudi neko (nesmiselno) zaporedje besed, npr. “gore Morje hrib Dolina”. Smiselna je tudi uporaba številk in drugih znakov.

Pri **drugi metodi** določene črke v besedah gesla zamenjamo s številkami. Npr, “O” zamenjamo z nič, “L” z ena, “E” z tri, itd. Primer: “t0j3m0j3g3s10”.

Pri **tretji metodi** pa geslo sestavimo iz prve (ali druge, ali zadnje,...) črke daljšega besedila. Tako iz “an ban pet podgan” nastane “abpp”. Seveda so možne še druge kombinacije (npr. kombinacija besed in števil), pomembno je le, da je geslo dovolj dolgo in dovolj kompleksno, da ga ni mogoče uganiti.

Gesla

Geslo mora biti čim bolj odporno na napad z metodo grobe sile ter na ugibanje.

Če gre za geslo za dostop do nekega sistema, ki ima **časovno omejitev** za ponovne poskuse vnosa gesla, ali če je **število poizkusov** vnosa gesla omejeno, je geslo lahko krajše.

Geslo mora imeti dovolj visoko stopnjo entropije (npr. vsaj 64 bitov entropije – mera za nedoločenost sistema sporočil).

ASCII abeceda ima približno okrog 5 bitov entropije. Zato za dosego 64 bitov entropije potrebujemo vsaj 13 znakov dolgo geslo (64/5 = 12,8).

Angleško besedilo ima po nekaterih ocenah v povprečju približno 1,2 do 2 bita entropije na znak: geslo v angleškem jeziku mora biti dolgo med 32 in 54 znakov.

Povprečna entropija **slovenskih leposlovnih besedil** je 2,2 bita na znak: geslo v slovenskem jeziku mora biti dolgo vsaj 30 znakov.

Gesla

Enkratna gesla

"Biometrična gesla": biometričnih parametrov ni mogoče zamenjati oziroma preklicati, ponarejanje prstnih odtisov,...

Identiteta ("Kdo si?") in avtentikacija ("Kako lahko to dokažeš?") uporabnika morata ostaneta ločeni, kar pa pri uporabi biometričnih gesel ne velja.

Geslo, za katerega sumimo, da je bilo zlorabljeno je potrebno **takoj spremeniti**.

Ustrezna uporaba gesel?

We hacked Dan's assets first through finding bugs and writing Oday, and then through abusing him giving away passwords and his silly password scheme. Check out just some of his passes:

`fuck.hackers`, `øhnøz` (root account on his mail box), `fuck.omg`, `fuck.vps`,

`ohhai`

Five character root password? Niiiiiiice.

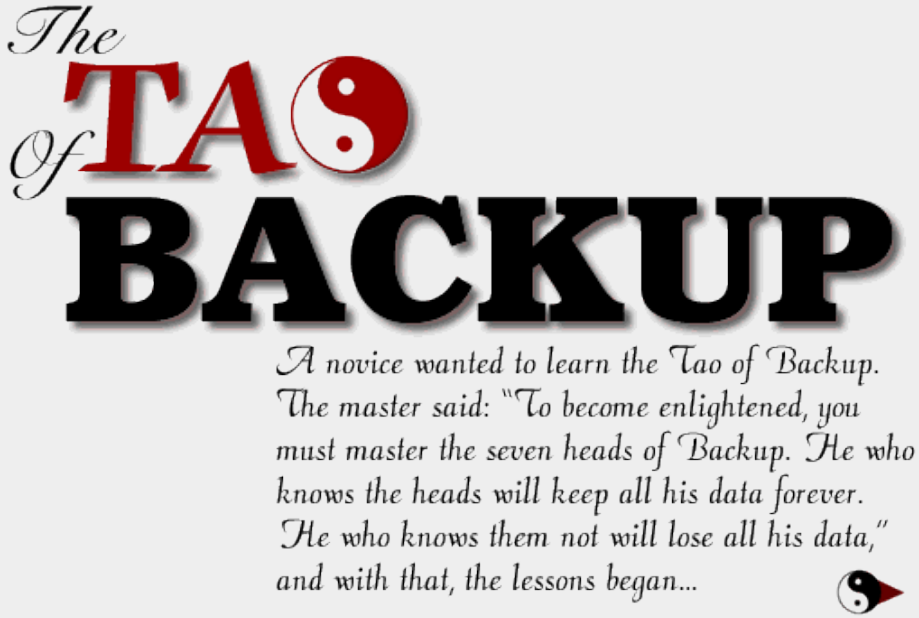
From .mysql_history:

SET PASSWORD FOR 'root'@'localhost' = PASSWORD('`fuck.mysql`');

See the pattern?

`https://sites.google.com/site/zeroforowned/dan-kaminsky-1`

Varnostne kopije



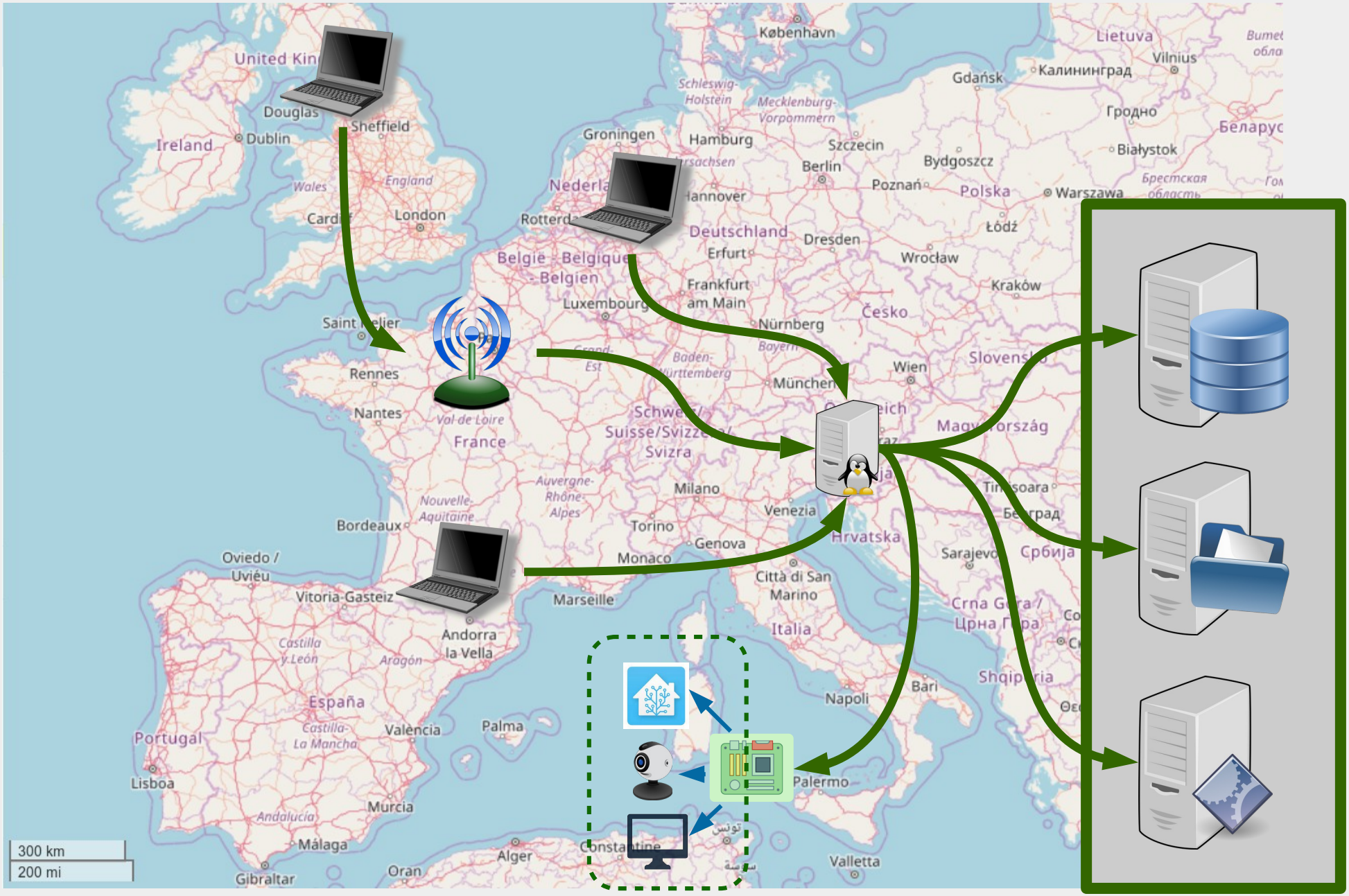
- uporaba (šifriranih?) oblačnih storitev (+/- dosegljivost,...);
- uporaba lokalnega NAS strežnika;
- arhiviranje samo pomembnih datotek;
- arhiviranje celotnega sistema (+ načrt okrevanja po katastrofi?);
- inkrementalne varnostne kopije.

Naprednejša zaščita

Nekatere tehnike naprednejše zaščite:

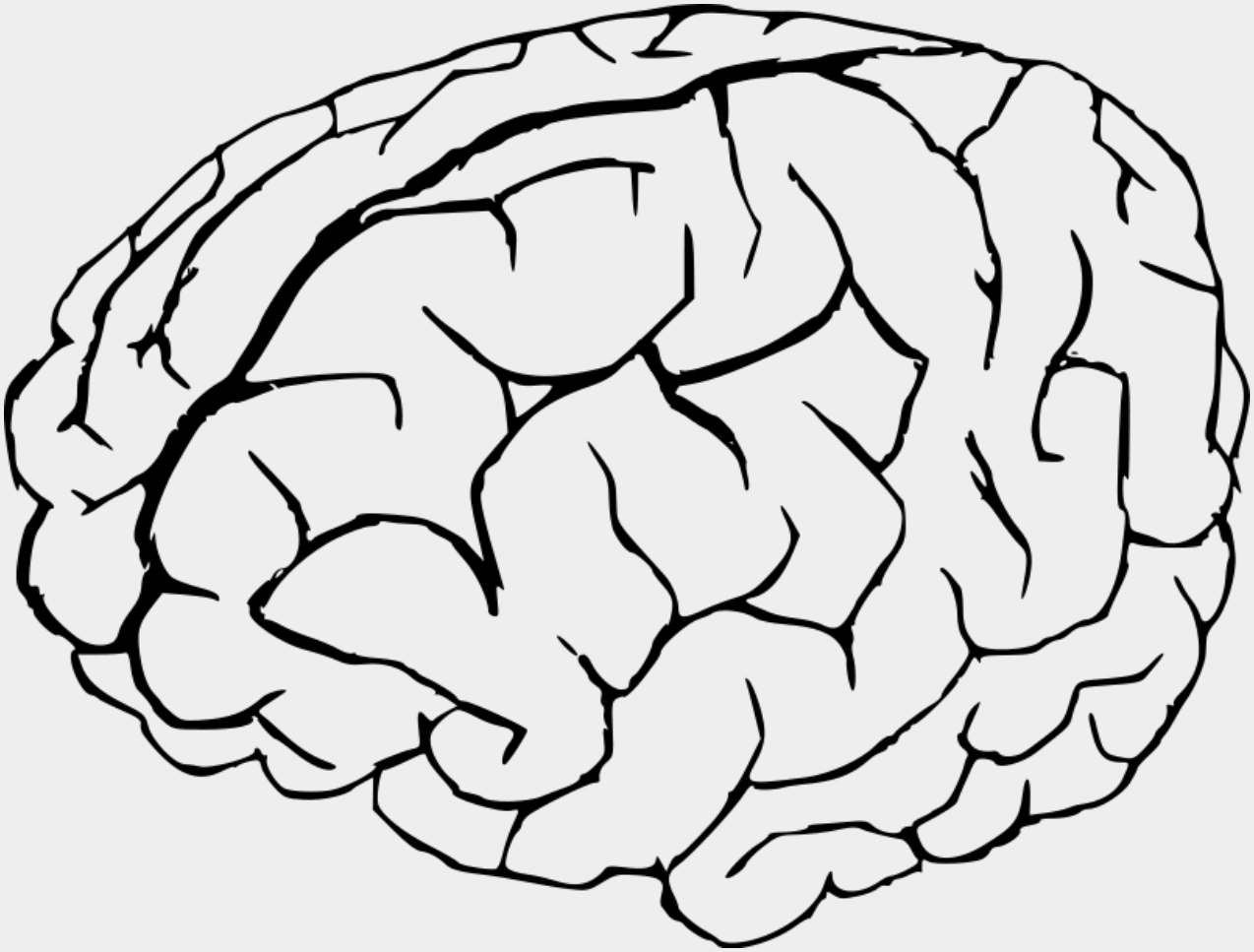
- **šifriranje** (*preprečimo dostop do vsebine*):
  - šifriranje nosilcev podatkov,
  - šifriranje elektronske pošte, neposrednih/hipnih sporočil, govorne in video komunikacije,
  - uporaba šifriranih povezav in protokolov (HTTPS,...),
- **trajno brisanje podatkov**,
- **anonimizacija** uporabe interneta (*preprečimo analizo prometnih podatkov*):
  - anonimizacijska omrežja,
  - "remailerji",
- **VPN**

VPN (Virtual Private Network)

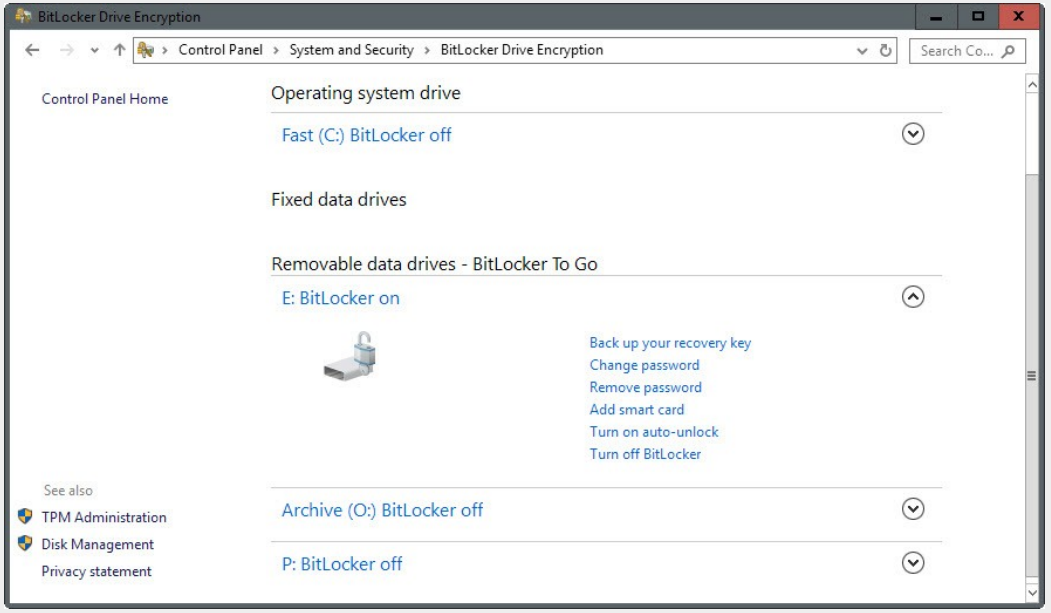


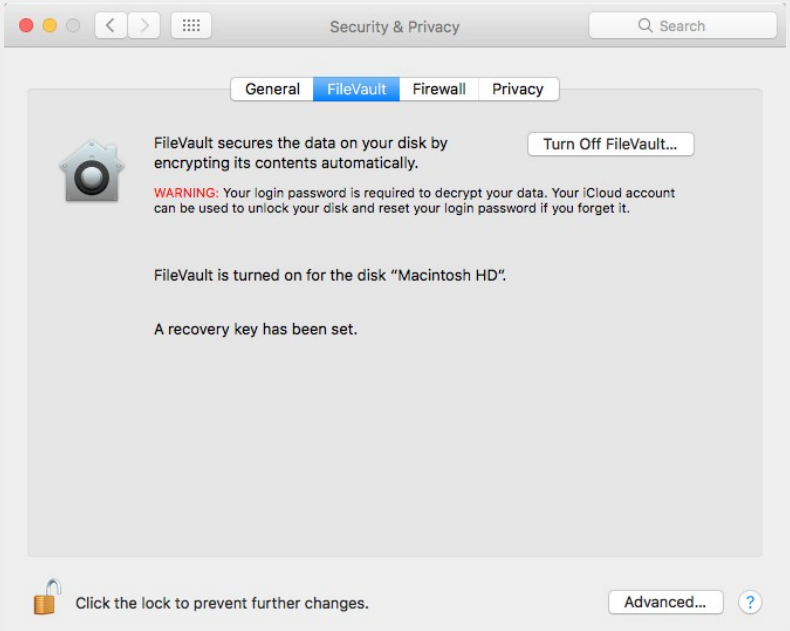
Še bolj napredna zaščita

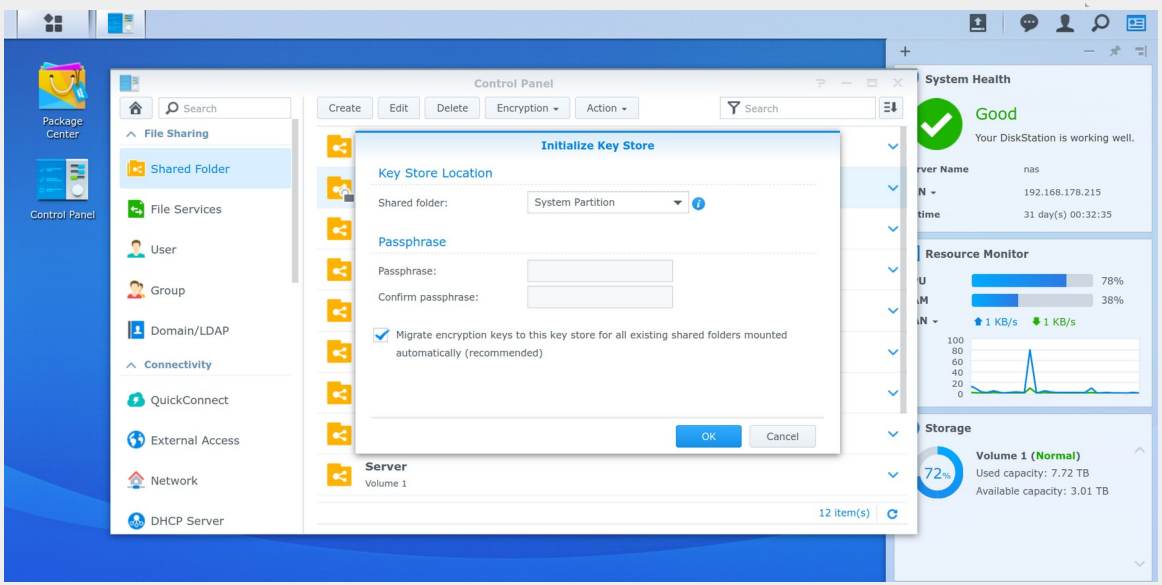
Nekaj znanja, doslednosti in zdrava pamet. ;-)



Šifriranje nosilcev podatkov







Dodatne aplikacije

Dodatki za brskalnik:

- HTTPS Everywhere,
- odstranjevalci spletnih tehnologij za sledenje (angl. *online trackers*): Ghostery, Privacy Badger, Adblock Plus, uBlock Origin,...),
- NoScript.

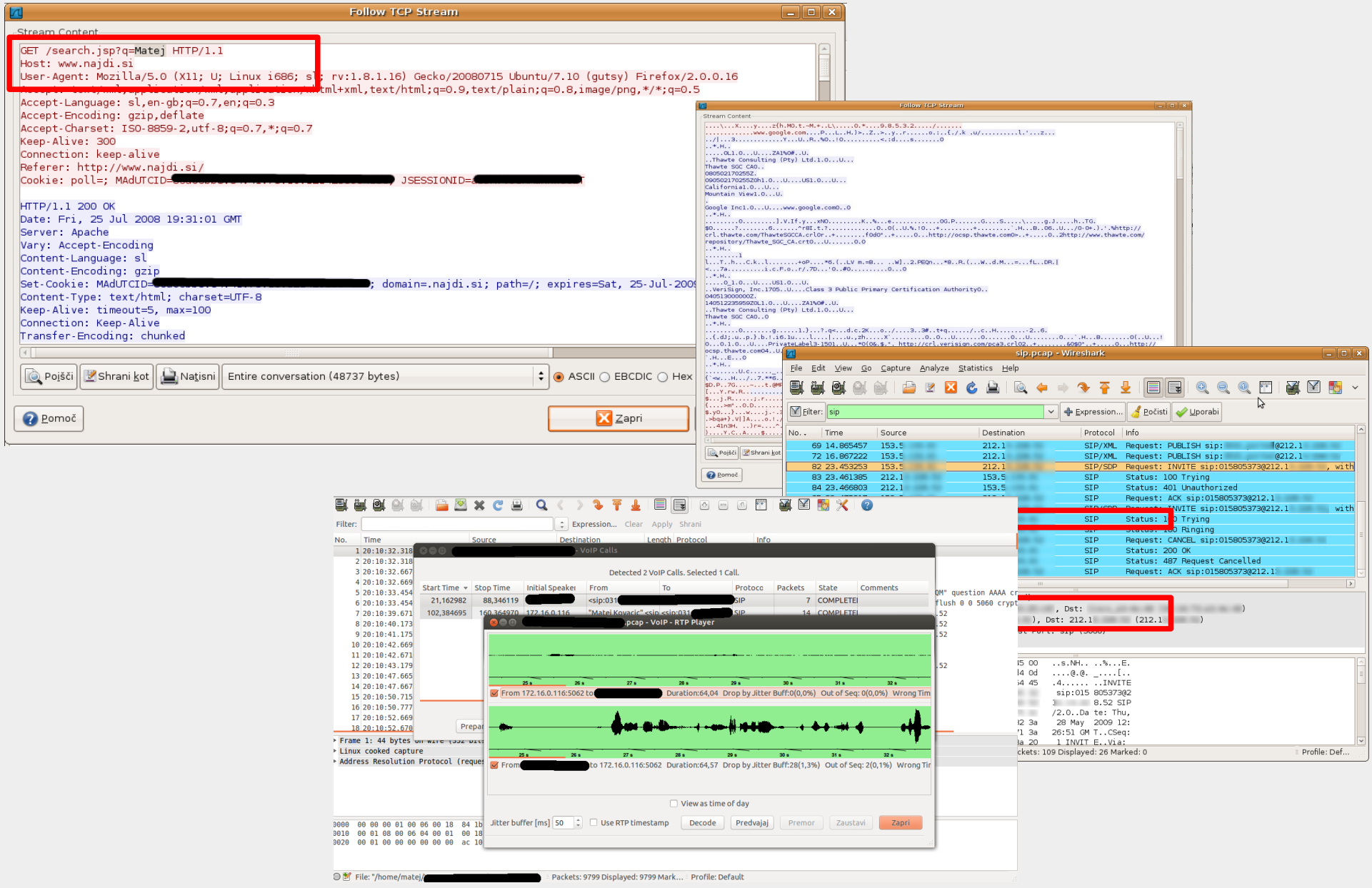
Odstranjevalci »nesnage« (BleachBit, CCleaner,...).

Blokada Windows telemetrije (Blackbird, WPD,... PiHole?).

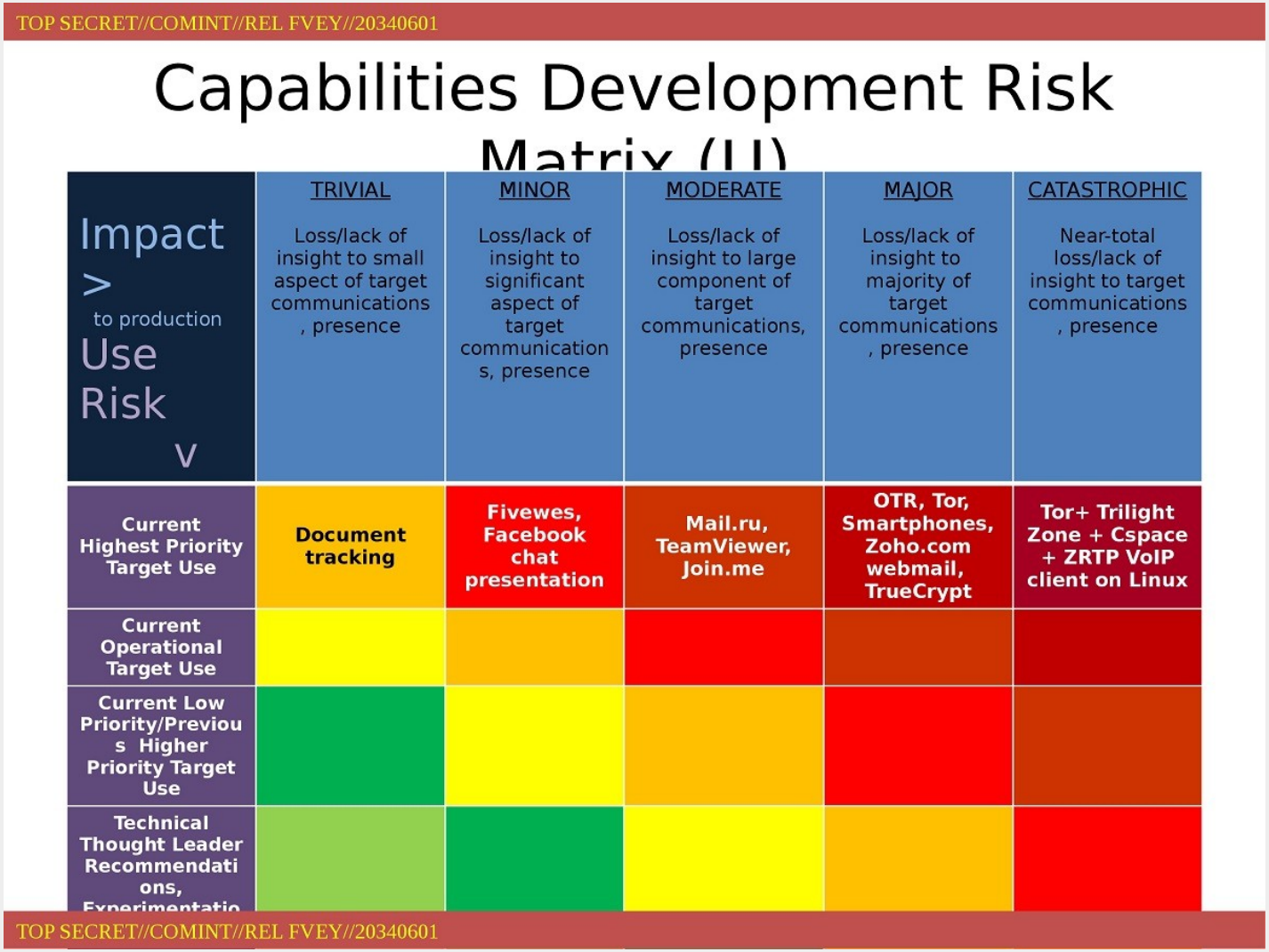
Upravljavec gesel (angl. *password manager*): Keepass, Lastpass, Bitwarden, Lesspass...).

Priporočljivo je, da so varnostni dodatki odprtokodni.

Zakaj šifiriranje?



Šifriranje »priporoča« tudi NSA!



TOP SECRET//COMINT//REL FVEY//20340601

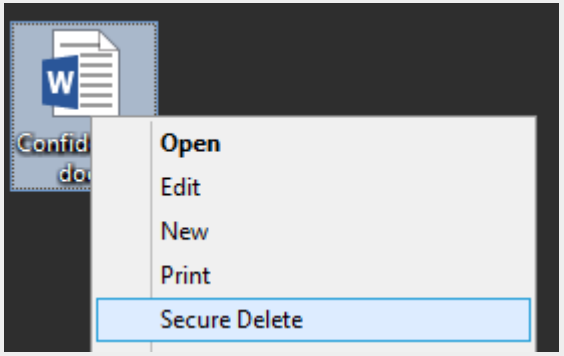
Capabilities Development Risk Matrix (U)

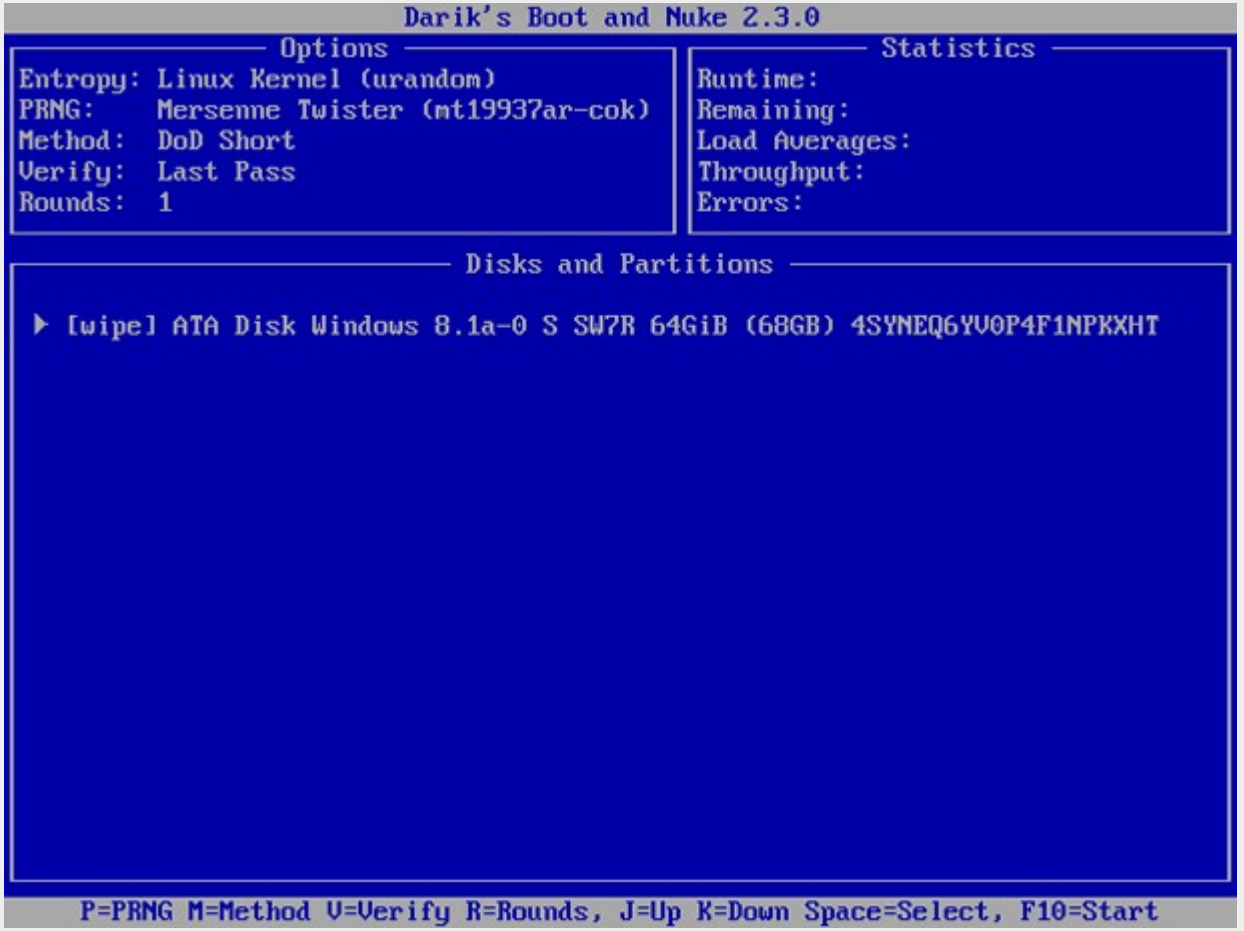
Impact > to production Use Risk v	TRIVIAL Loss/lack of insight to small aspect of target communications, presence	MINOR Loss/lack of insight to significant aspect of target communications, presence	MODERATE Loss/lack of insight to large component of target communications, presence	MAJOR Loss/lack of insight to majority of target communications, presence	CATASTROPHIC Near-total loss/lack of insight to target communications, presence
Current Highest Priority Target Use	**Document tracking**	**Fivewes, Facebook chat presentation**	**Mail.ru, TeamViewer, Join.me**	**OTR, Tor, Smartphones, Zoho.com webmail, TrueCrypt**	**Tor+ Trilight Zone + Cspace + ZRTP VoIP client on Linux**
Current Operational Target Use					
Current Low Priority/Previous Higher Priority Target Use					
Technical Thought Leader Recommendations, Experimentatio					

TOP SECRET//COMINT//REL FVEY//20340601

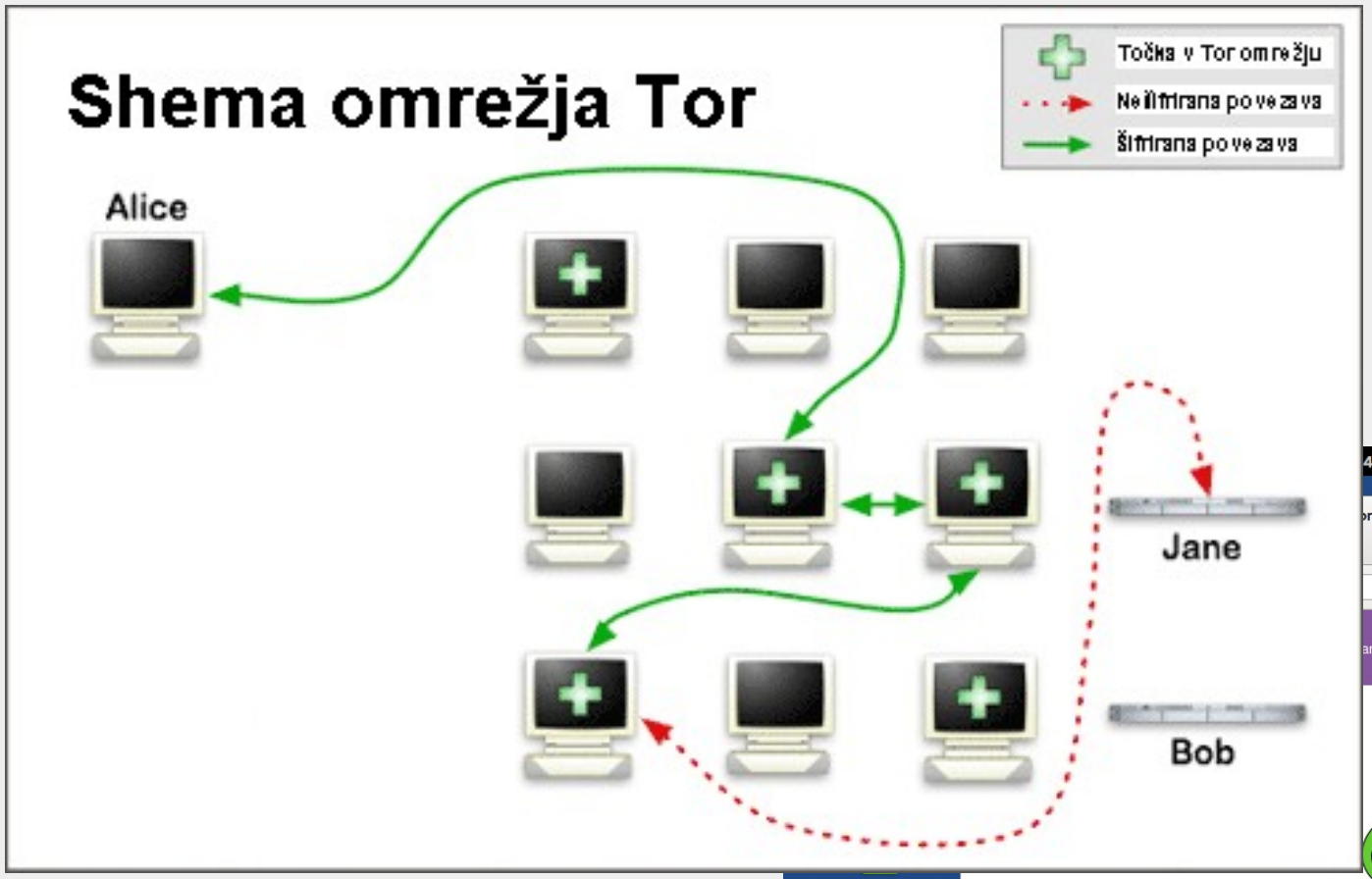
Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states. (Der Spiegel)

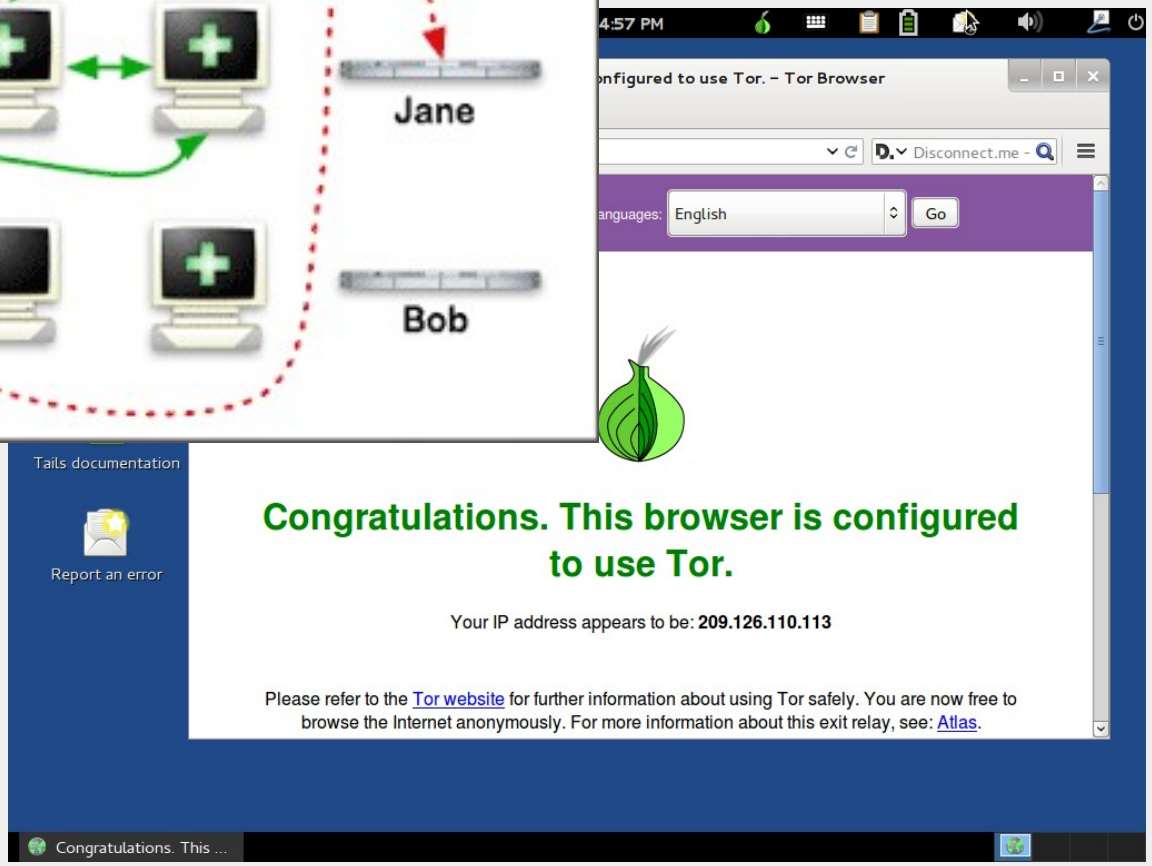
Trajno brisanje podatktov





Anonimizacija





Varnost e-pošte

Poštni strežnik:

- varnostni protokoli za preverjanje pristnosti e-pošte (SPF - Sender Policy Framework, DKIM - DomainKeys Identified Mail in DMARC - Domain-based Message Authentication, Reporting & Conformance),
- strežniški diski so šifrirani,
- protivirusni in protismetni filtri,
- podpora šifriranim protokolom (POP3s/IMAPs/SMTPs).

Poštni odjemalci:

- šifriranje e-pošte (GPG),
- dvofaktorska avtentikacija (Yubikey,...).

Razpoložljivost

Razpoložljivost zagotavlja zanesljiv in pravočasen dostop do informacijskega sistema, ko ga uporabniki potrebujejo. Zanesljiv in razpoložljiv informacijski sistem v organizaciji predstavlja temelj za nemoteno izvajanje delovnih in poslovnih procesov in ima zato ključno vlogo pri učinkovitosti poslovanja.

Delo na daljavo:

- infrastruktura v organizaciji (oddaljeni dostopi, videokonferenčni sistemi),
- infrastruktura pri zaposlenih (strojna in programska oprema (slušalke,...)),
- oddaljeno vzdrževanje,
- varnost terminalne opreme,
- trening.

Delo na daljavo

Digitalizacija poslovanja in delo na daljavo niso možni v vseh gospodarskih panogah v enaki meri.

Kjer pa je to mogoče, pa je priprava na to smiselna.

Spremembe je treba uvajati premišljeno in sistematično.

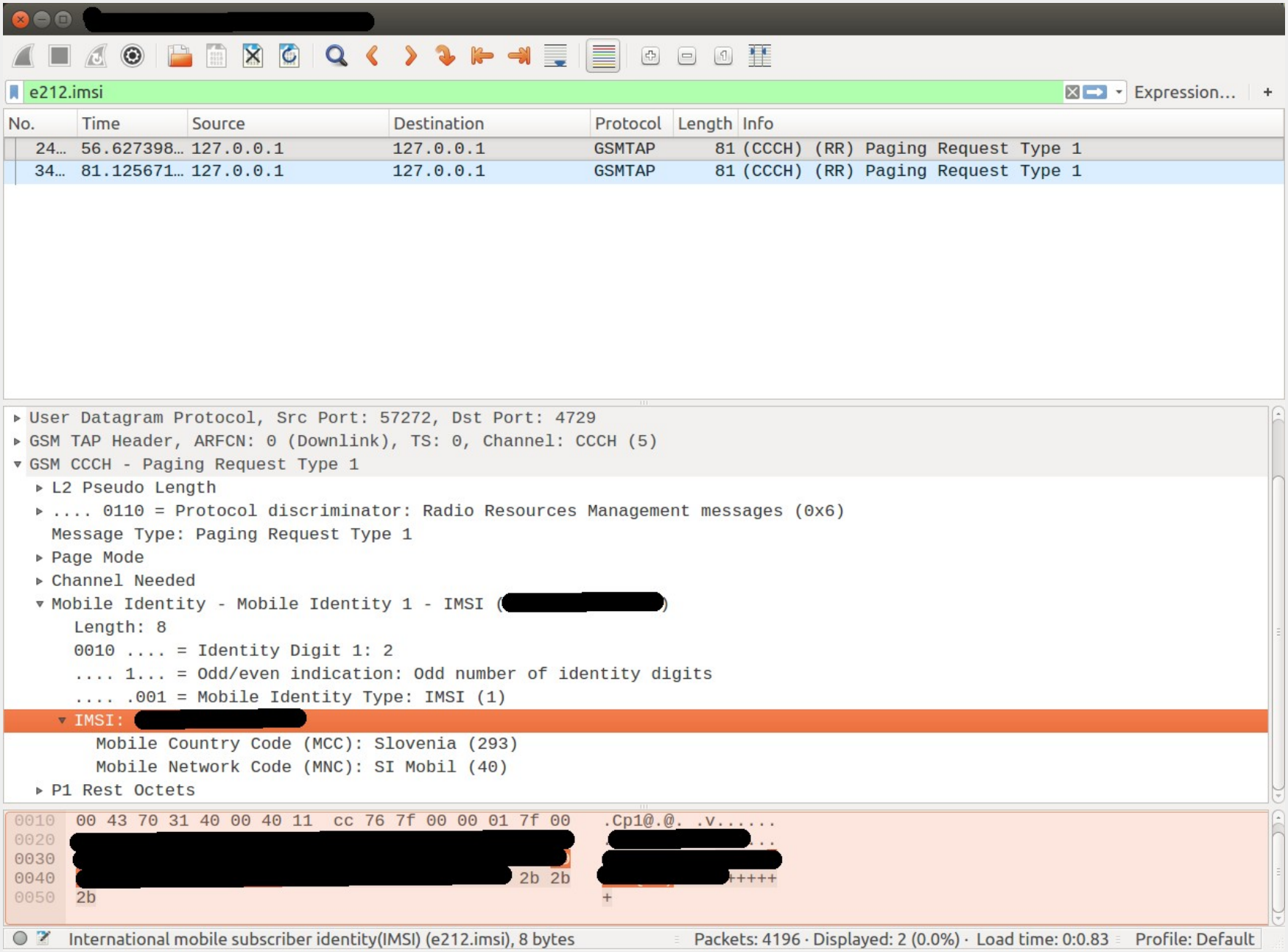
1. Priprava ustrezne infrastrukture na strani organizacije.
2. Zagotovitev podpore delu na daljavo pri zaposlenih.
3. Izobraževanje zaposlenih.
4. Občasno izvajanje dela na domu/na daljavo (trening).

Poseben poudarek na zagotavljanju varnosti.

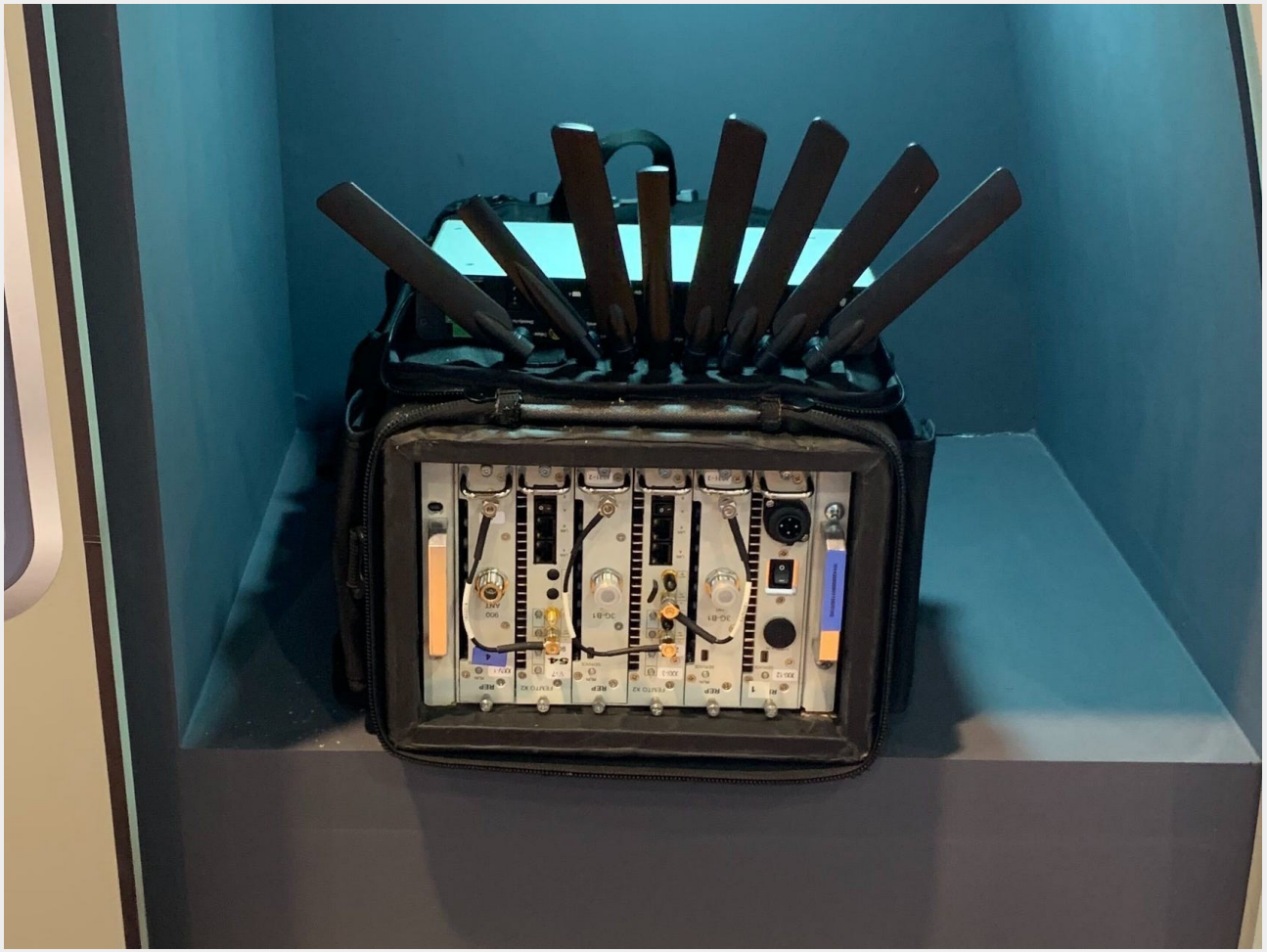
S tem bo organizacija bolje pripravljena na potencialno krizo, kar pa je bistvenega pomena za preživetje v primeru izrednih dogodkov.

Varnost mobilnih komunikacij

Varnost mobilnih komunikacij

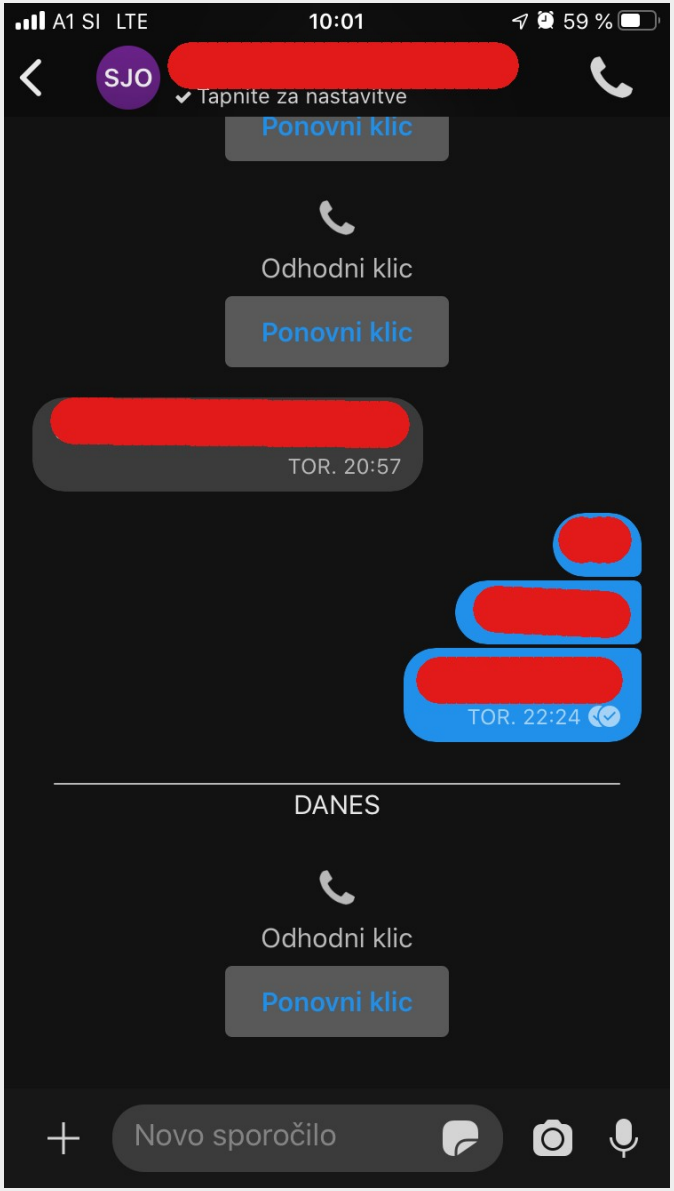


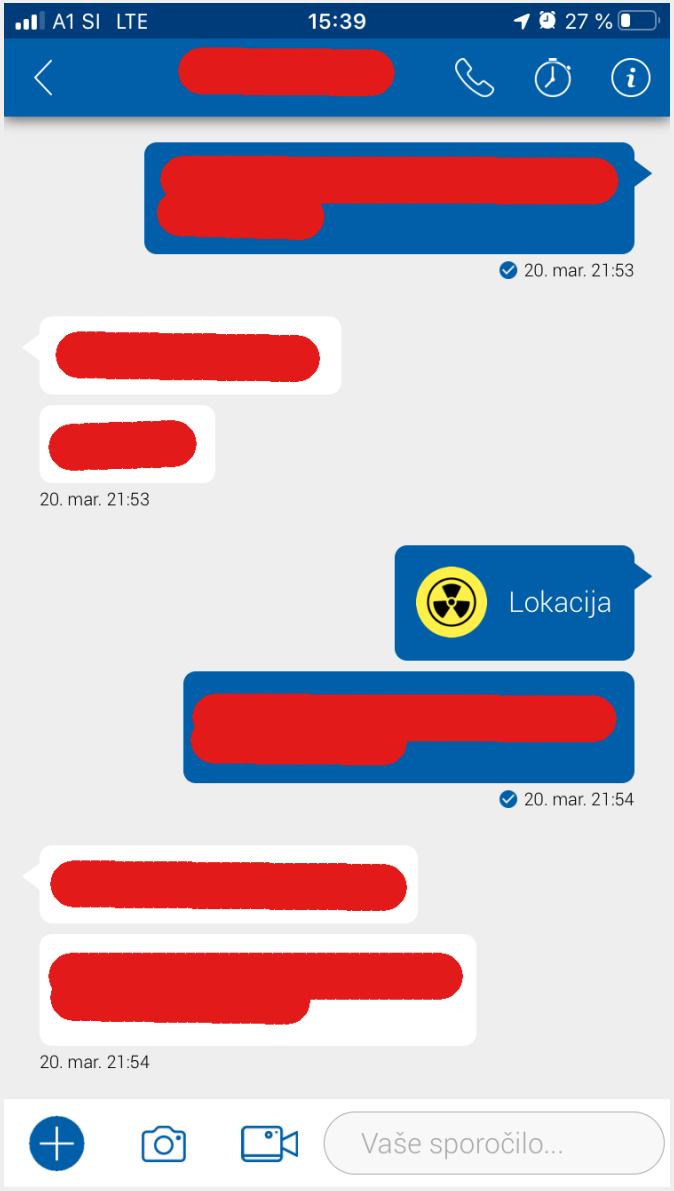
Varnost mobilnih komunikacij



Naprava podjetja NSO namenjena vdorom v mobilne telefone.

Varnost mobilnih komunikacij





Vidiki informacijske varnosti

Gradniki zagotavljanja informacijske varnosti:

- Techologija (pogosto se nanjo daje preveč poudarka, prepričanje, da samo s tehnologijo lahko zagotovimo varnost je napačno).
- Ljudje (pomemben del varnosti smo ljudje).
- Procesi, ki podpirajo tehnologijo in ljudi.
- Družbeni vidiki (širše družbene posledice uporabe informacijskih sistemov).

Ljudje

Ljudje smo pomemben element pri zagotavljanju varnosti.

Ljudje smo nagnjeni h delanju napak.

Ljudje pogosto skušamo zaobiti varnostne protokole, ker nam to olajša življenje.