GOLJUFIJE V 2018

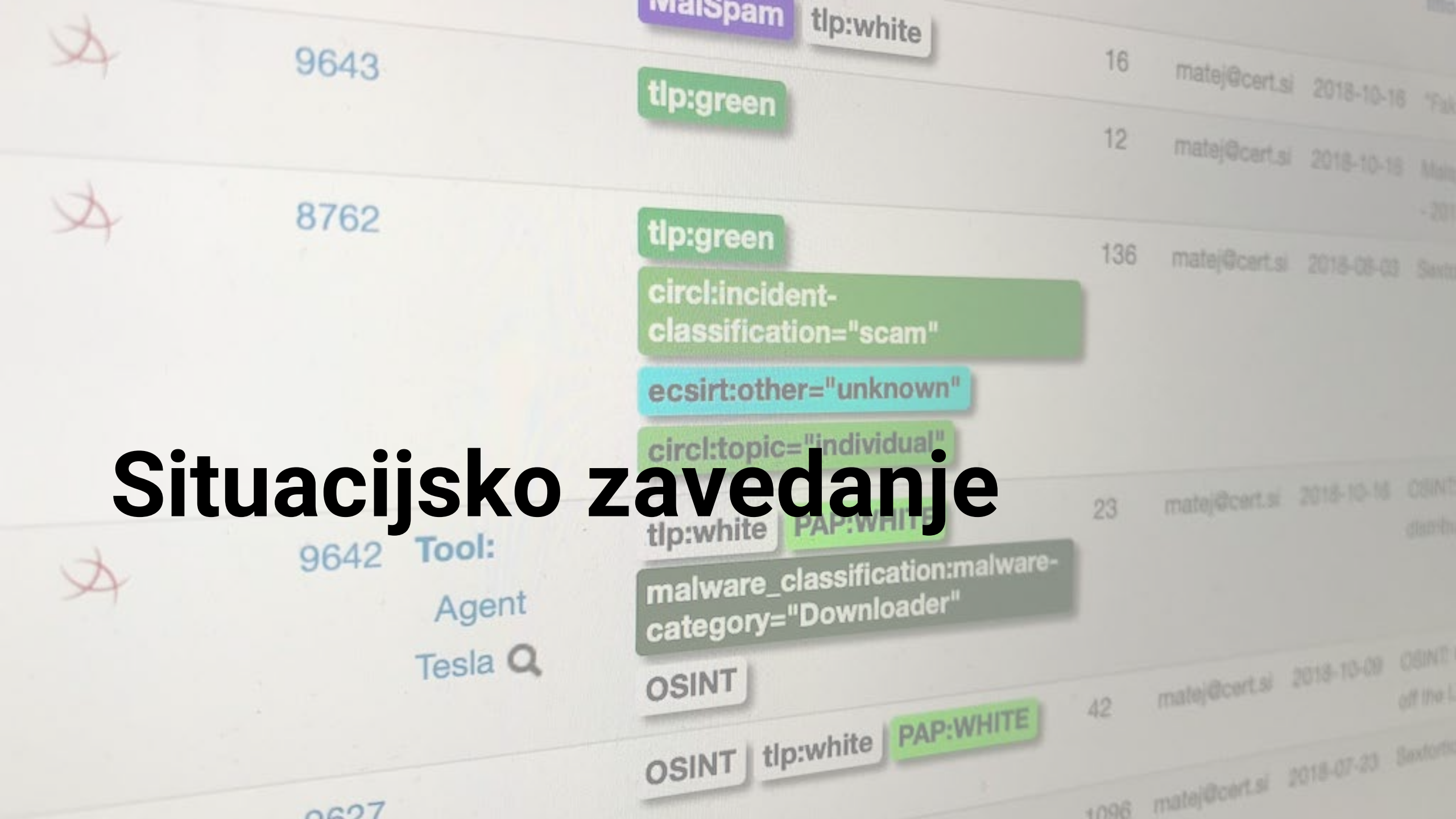
Gorazd Božič, SI-CERT

Mreža znanja 2018, 21. in 22. november

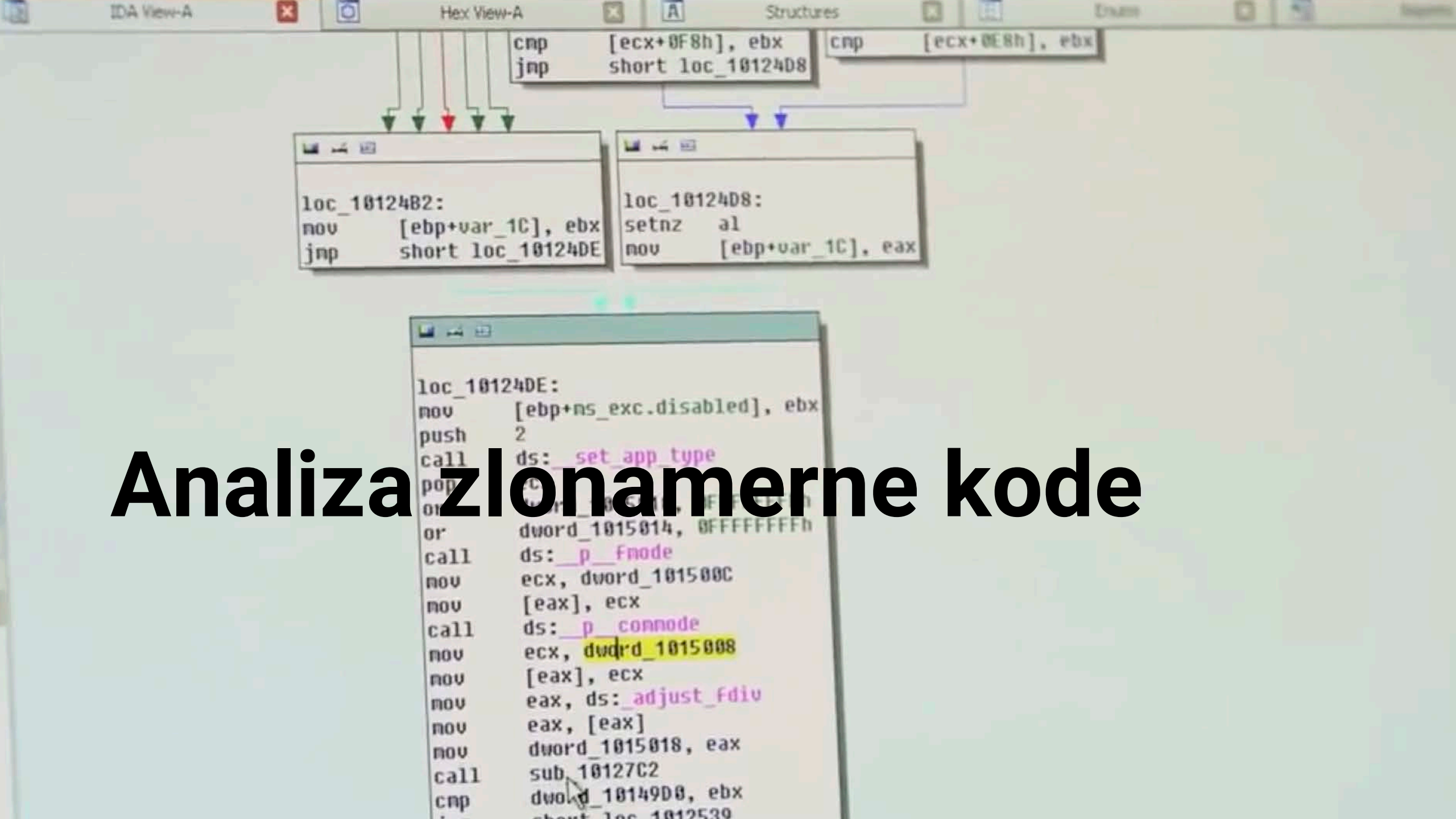
Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj.

si·cert

- nacionalna kontaktna točka
- javni zavod ARNES
- preiskovanje, svetovanje, koordinacija
- ozaveščanje
- pričetek delovanja: 1995



Situacijsko zavedanje

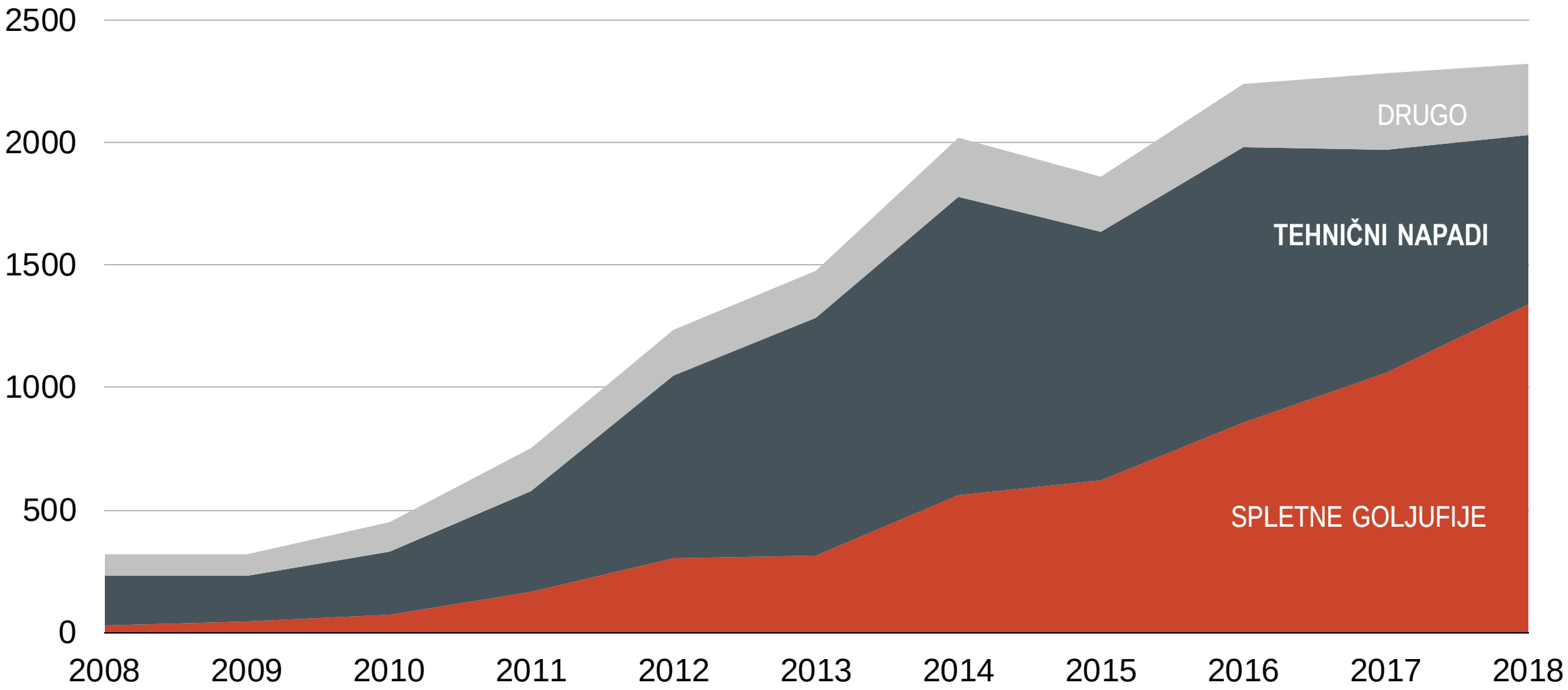


Analiza zlonamerne kode

Mednarodno sodelovanje

INCIDENTI

Število letno obravnavanih incidentov na SI-CERT (s projekcijo za 2018)



2016/17


bolha.com
facebook
wordpress
prodaja
cryptolocker
ponaredki
locky
email
gmail
ssh
westernunion
vdor
cerber
avalanche
kredit
probe
nakup
goljufija
javascript
google
amazon
sqli
crysis
apple
419
izsiljevanje
defacement
spam
ebn
sms
scam
ceofraud
avto.net
disclosure
ransomware
ddos
sms
airbnb
instagram
ebay
rdp
poskus
virus
zloraba
malware
prevara
dharma
paypal
okužba
oglas
mali
kitajska
trojanec
sporočilo
loterijska
phishing
sextortion
lažna_trgovina

2018


fake_sextortion
spletna_trgovina
izsiljevanje
trojanski_konj
spletni_nakup
phishing
bitcoin
malware
email
scan
prodaja
probe
sms
ceo_fraud
ssh
cimbl
419_scam
tcp/22
izsiljevalski_virus
nakup
prevara
geslo
facebook
paypal
spam
sextortion
ransomware
mali_oglasi
bolha.com
nigerijska_prevara

KAJ RAZKRIVAJO ŠTEVILKE?

Statistika obravnavanih incidentov

Vrsta incidenta	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
phishing	23	38	50	61	139	209	279	283	296	222
skeniranje in tipanje naprav	86	39	44	62	51	43	65	65	87	127
botnet	9	3	11	12	12	16	13	17	50	16
napad z onemogočanjem (DDoS)	22	10	18	28	47	76	124	94	78	26
škodljiva koda	18	53	68	126	258	417	438	418	462	360
zloraba storitve	16	15	12	28	9	8	9	15	16	20
vdor v sistem	32	25	56	93	76	61	32	43	42	36
zloraba uporabniškega računa				1	9	37	60	40	60	43
razobličenje					125	80	167	33	13	20
napad na aplikacijo					17	22	33	7	22	41
Tehnični napadi	183	145	209	350	604	760	941	732	830	911
kraja identitete			10	52	67	56	77	70	103	106
nigerijska (419) prevara							38	26	73	119
spletno nakupovanje							68	88	183	258
druge goljufije	5	24	26	89	161	210	309	322	354	492
neželena pošta (spam)	21	22	36	25	74	50	63	112	140	80
dialler in neznani klici na mobilne telefone					1		3		1	3
Goljufije in prevare	26	46	72	166	303	316	558	618	854	1058
zahtevek sodišča	11	6	11	11	9	6	4	2	2	
avtorske pravice	2	4	2	5	9	1	4	4	8	5
interno	3	4	16	38	25	25	31	23	33	19
novinarska vprašanja					18	16	21	12	14	10
splošna vprašanja	70	74	92	120	128	145	179	184	201	278
Vprašanja in zahtevki	86	88	121	174	189	193	239	225	258	312

OŠKODOVANJA

NAJVIŠJA IZPLAČANA ODŠKODNINA ZA IZSILJEVALSKI VIRUS

2016 **10.000 €**
2017 **14.800 €**

POVPREČNO OŠKODOVANJE Z VRIVANJEM V POSLOVNE KOMUNIKACIJE

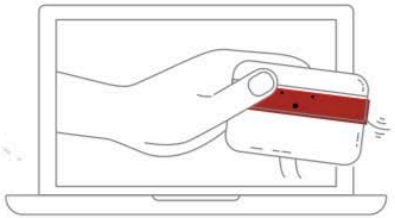
2016 **19.200 €** (največje: 35.000 €)
2017 **13.640 €** (največje: 40.000 €)

NAJVIŠJE OŠKODOVANJE V NIGERIJSKI PREVARI

2016 **100.000 €**
2017 **20.000 €**

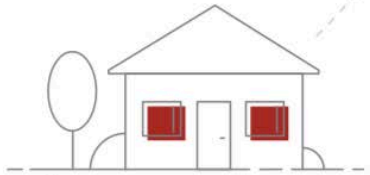
NAJVIŠJE OŠKODOVANJE PRI GOLJUFIJI PO AIRBNB

2016 **1.000 €**
2017 **2.100 €**



POVPREČNO OŠKODOVANJE PRI SPLETNEM NAKUPU

2016 **422 €**
2017 **281 €**



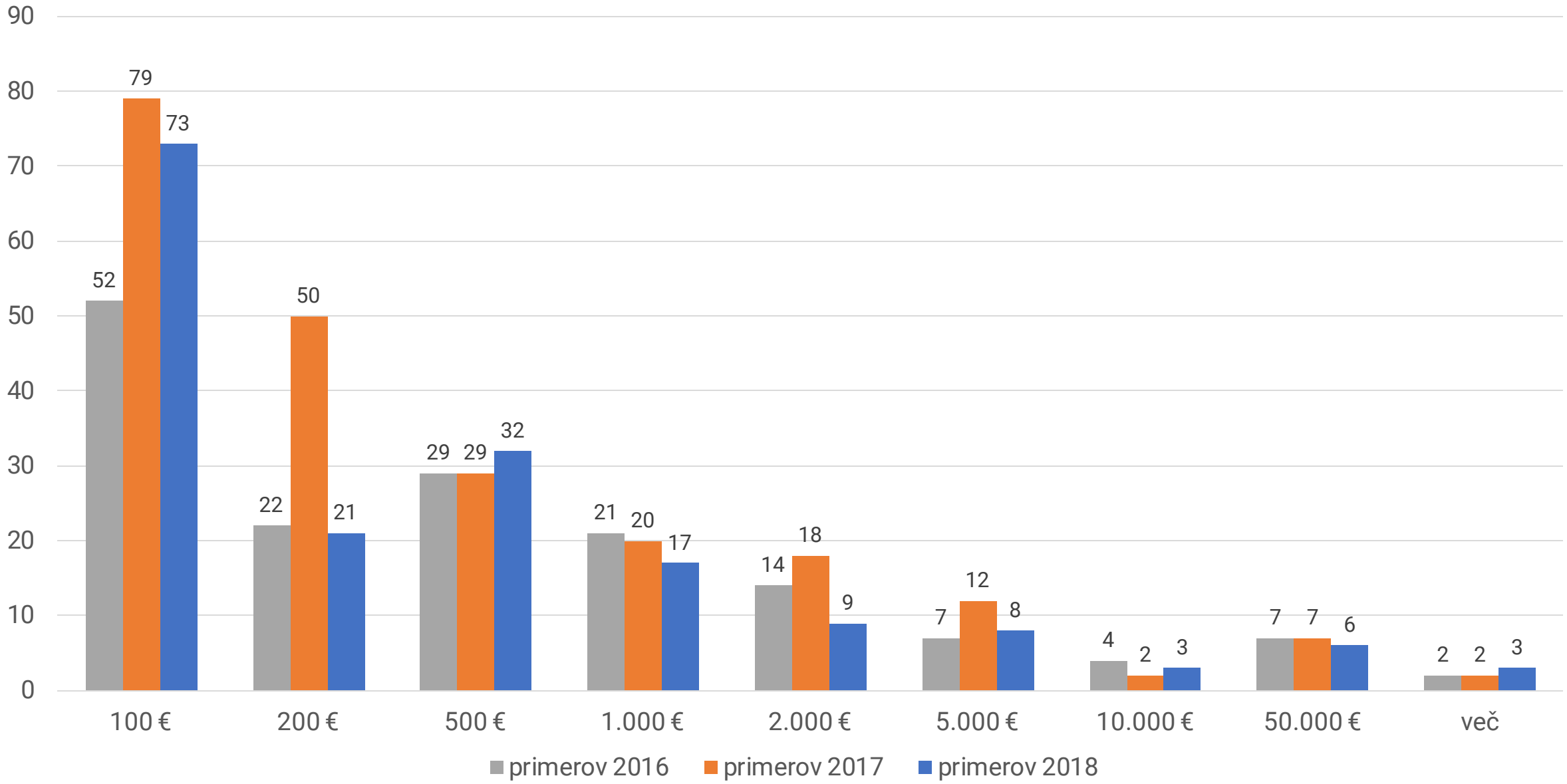
OŠKODOVANJE PRI PRODAJI NEPREMIČNINE

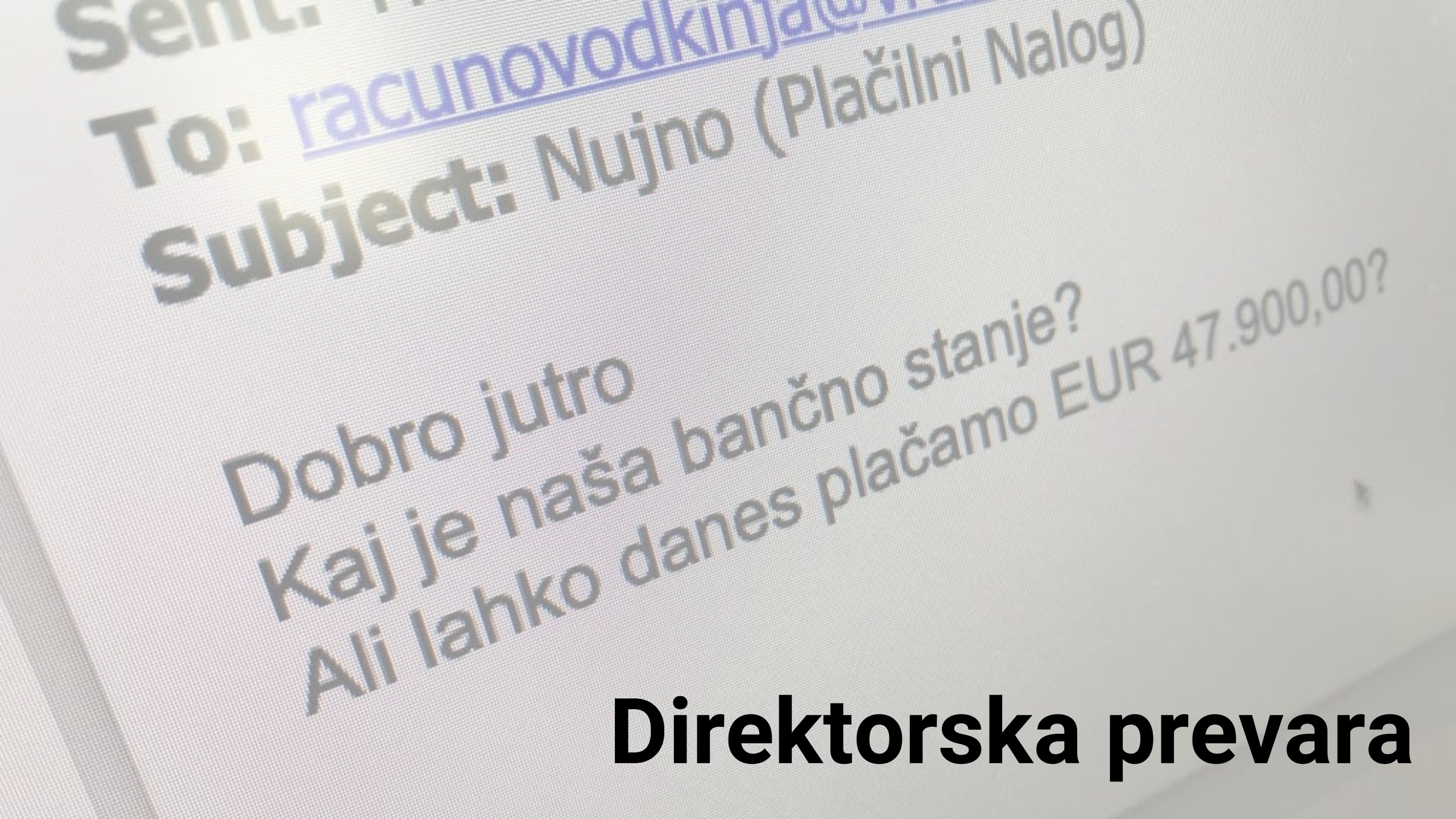
2016 **7.500 €**

POVPREČNO OŠKODOVANJE PRI DRUGIH GOLJUFIJAH

2016 **3.556 €**
2017 **3.730 €**

Porazdelitev oškodovanj v 2016-2018





Direktorska prevara

From [redacted] <mail.mgt@aol.com>

Subject **Re: (Plačilni nalog) Nujno**

To [redacted]

V redu. Prosim Plačaj zdaj. Poslal bom dokumentacijo kasneje.

Podjetje / prejemnik: MERSIN DISANG S.L
Naslov: AV CONSTITUCION 52,2, 33207 GIJON ASTURIAS, ŠPANIJA
IBAN: ES56 1465 0100 9319 0048 6847
Swift: INGDESMMXXX
Banka: ING DIRECT
Sklic: INV. 0043291826
Namen plačila: Nakup kapitala
Znesek: 55.000 EUR

Prosim, pošljite plačila potrditev slip.

LP,
[redacted]

From: [redacted] International [mailto:info@starlinetrading.com]
Sent: Thursday, August 02, 2018 3:40 PM
To: fatemeh[redacted]
Subject: PI NO. EX-06-18/TOP URGENT

Hi Fatemeh,

Please stop any payment to the previous bank details provided as a result of bad payment issued buy our customer and the account is being investigated.
please confirm as this is a top urgent here.

Lep pozdrav/Kind regards,
[redacted]

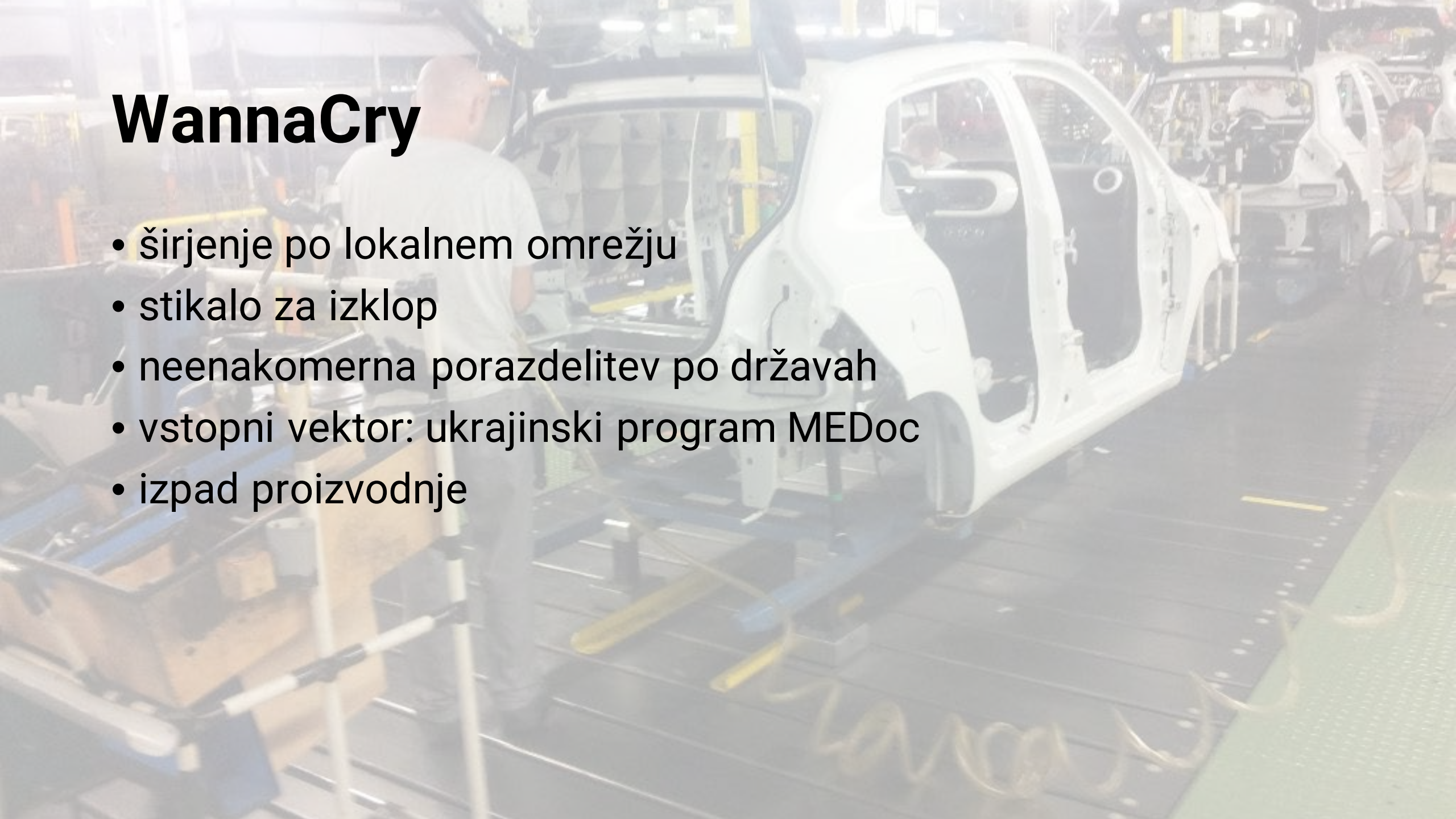
Vrivanje v komunikacijo

Vrivanje v komunikacijo

- vdor v poštni predal enega od partnerjev
- spremljanje komunikacije
- podtaknjen TRR denarne mule
- najvišje oškodovanje v 2018: ~ **450.000 EUR!**

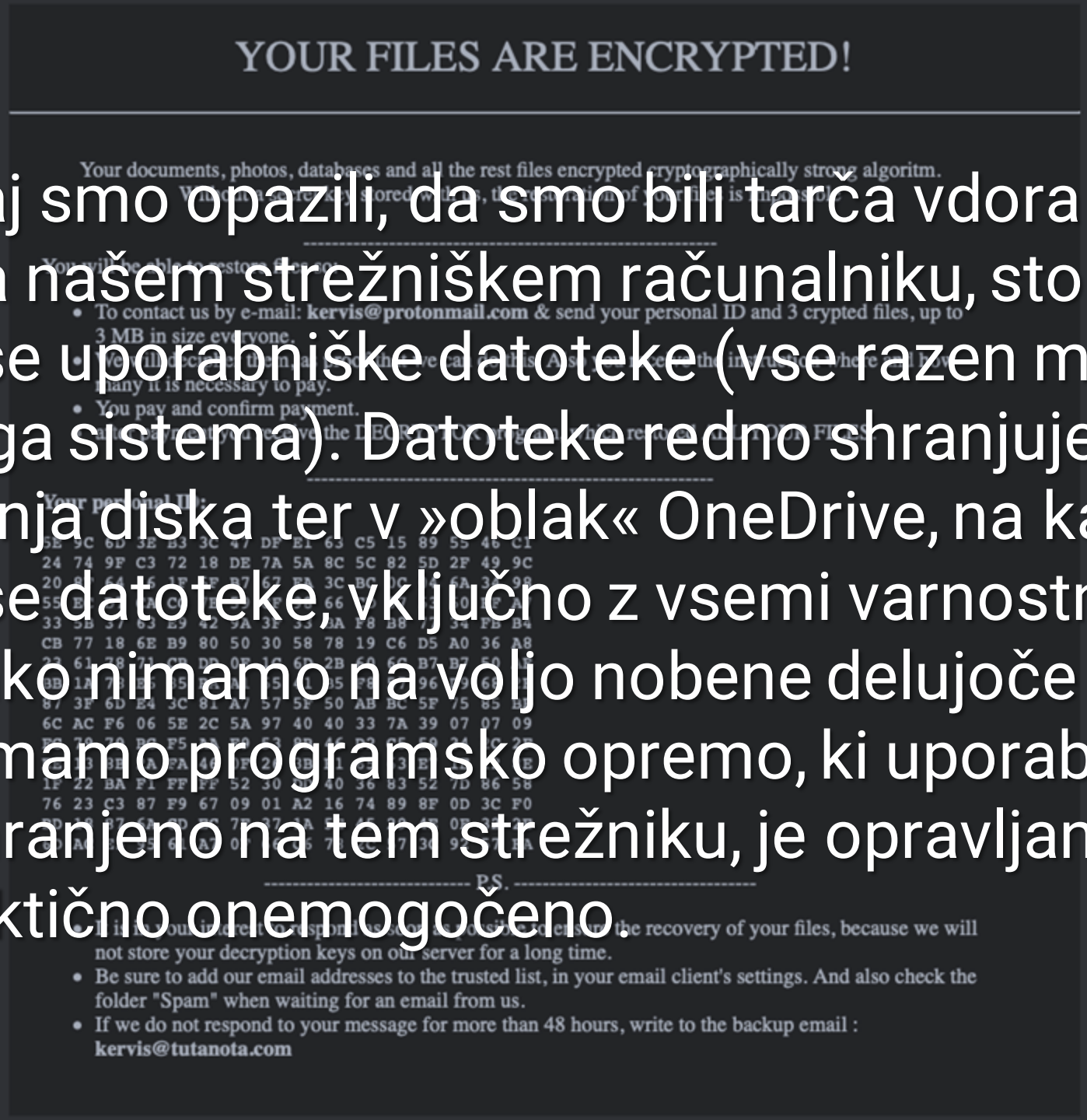
Izsiljevalski virusi

Slika je simbolična. CC-BY Chesapeake Bay Program @ flickr.com



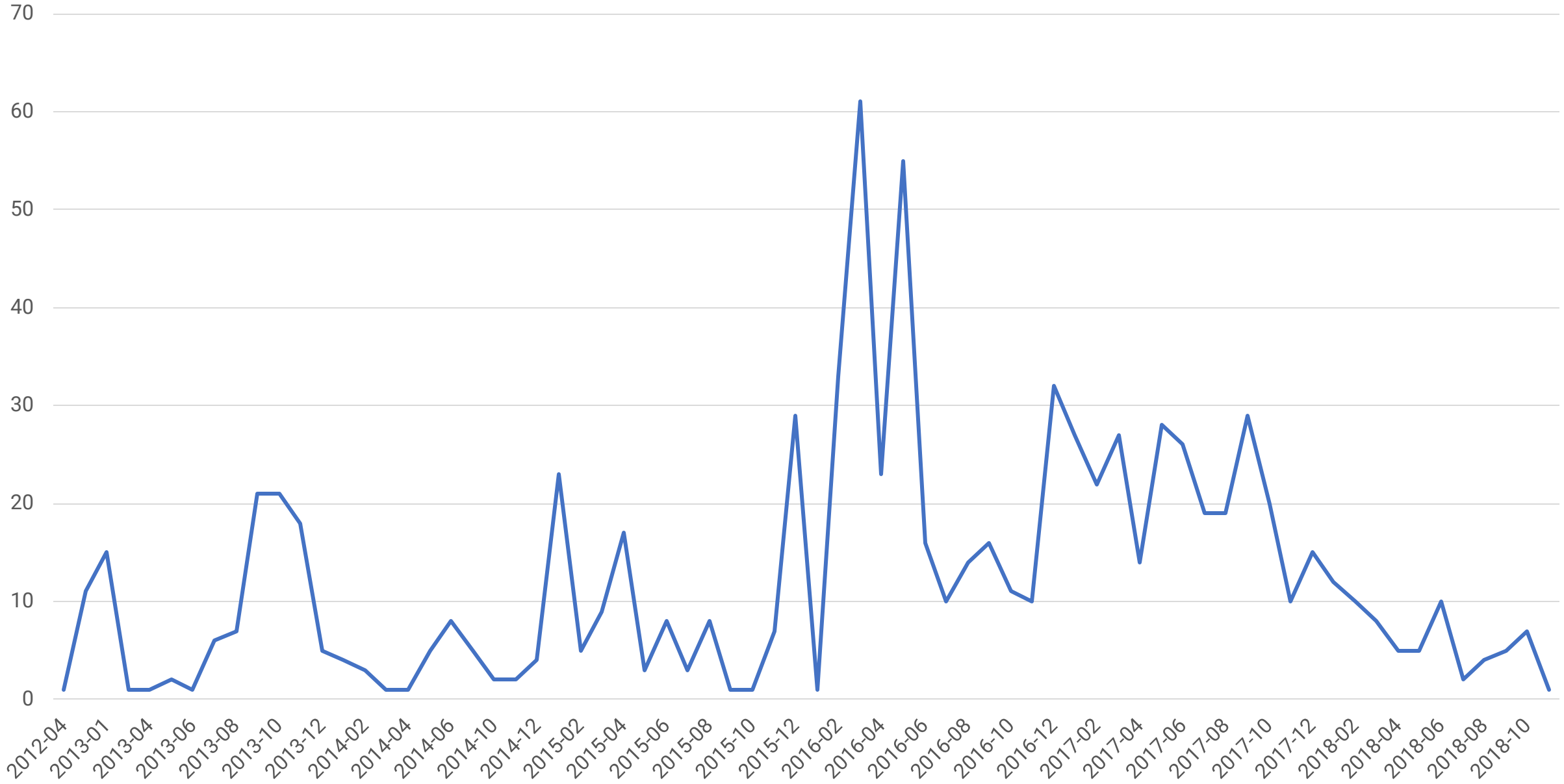
WannaCry

- širjenje po lokalnem omrežju
- stikalo za izklop
- neenakomerna porazdelitev po državah
- vstopni vektor: ukrajinski program MEDoc
- izpad proizvodnje

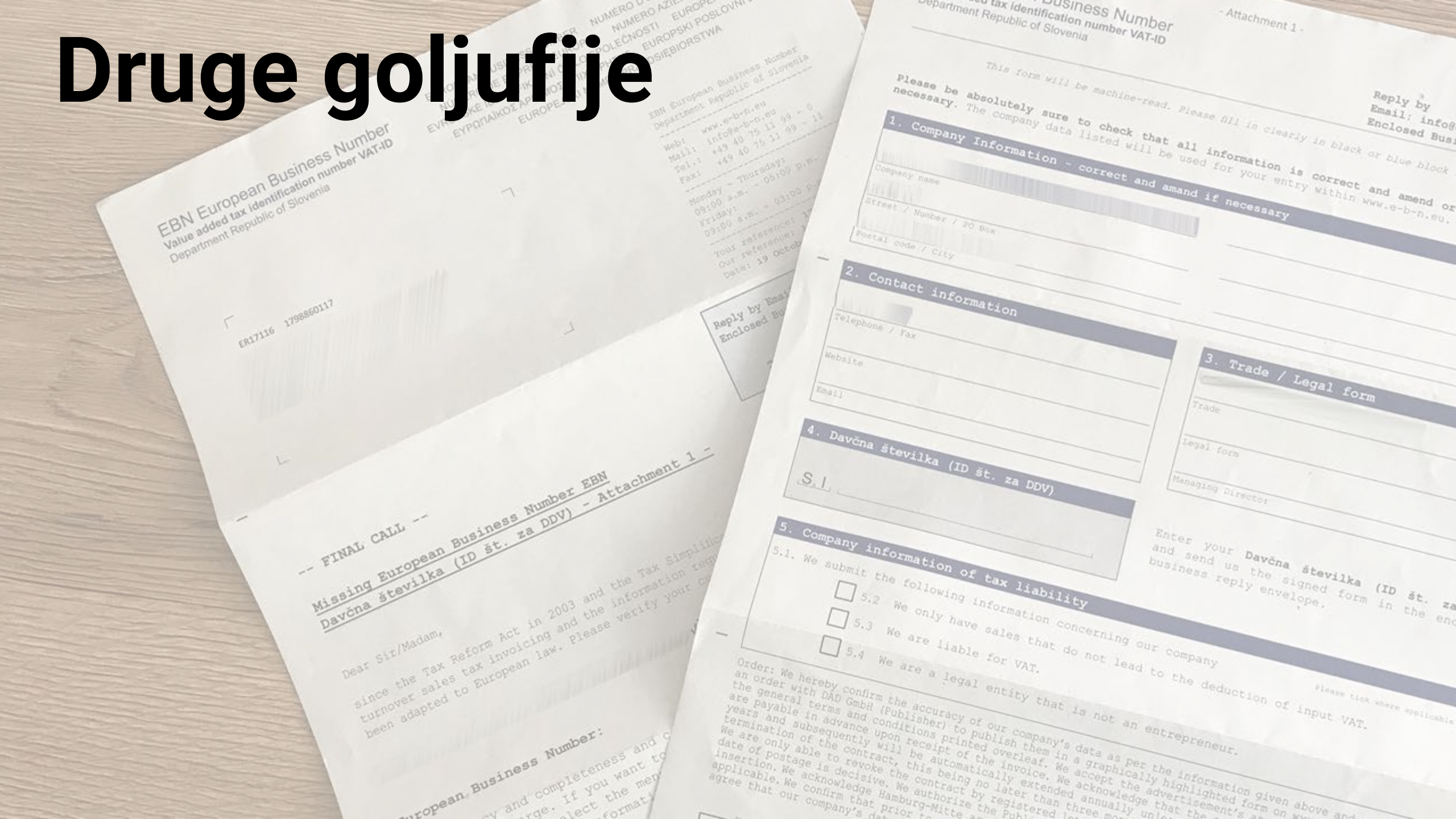


Danes zjutraj smo opazili, da smo bili tarča vdora preko RDP protokola na našem strežniškem računalniku, storilci pa so zakodirali vse uporabniške datoteke (vse razen mape operacijskega sistema). Datoteke redno shranjujemo na dva ločena zunanja diska ter v »oblak« OneDrive, na katerih so tudi zakodirali vse datoteke, vključno z vsemi varnostnimi kopijami. Tako nimamo na voljo nobene delujoče varnostne kopije. Ker imamo programsko opremo, ki uporablja bazo podatkov shranjeno na tem strežniku, je opravljanje dejavnosti podjetja praktično onemogočeno.

Mesečno št. prijav izsiljevalskih virusov



Druge goljufije



THE ISLAMIC STATE OF QATAR
MINISTRY OF ENDOWMENTS AND ISLAMIC AFFAIRS
PROJECT PROCUREMENT DIVISION
Al Funduq St., Doha, Qatar P. O. Box 422
Website: http://www.islam.gov.qa
Phone/Fax: +97444470777, 974 4470700

Our Ref:.....DPP/CTC/005..... *Doha:*.....05/05/2014.....

[redacted]

Attn:The President,

PROFORMA INVOICE APPROVAL

By the power vested upon me as the Honourable Chairman of the Public Procurement Division of the Ministry of Endowments and Islamic Affairs, Islamic State of Qatar, I hereby unequivocally approved the items as expressed in Proforma Invoice Number: 10337/14 dated April, 15th 2014 to the Department of Public Procurement.

We have adequately carried out a thorough study on your products and came to a conclusion that it is indeed in conformity with the required Ministerial need.

The Items are as specified in your Proforma Invoice Number: 10337/14 dated April, 15th 2014 respectively.

The total value of the said Proforma Invoices is €1,843,000.00 (One Million Eight Hundred and Forty Three Thousand Euro) only.

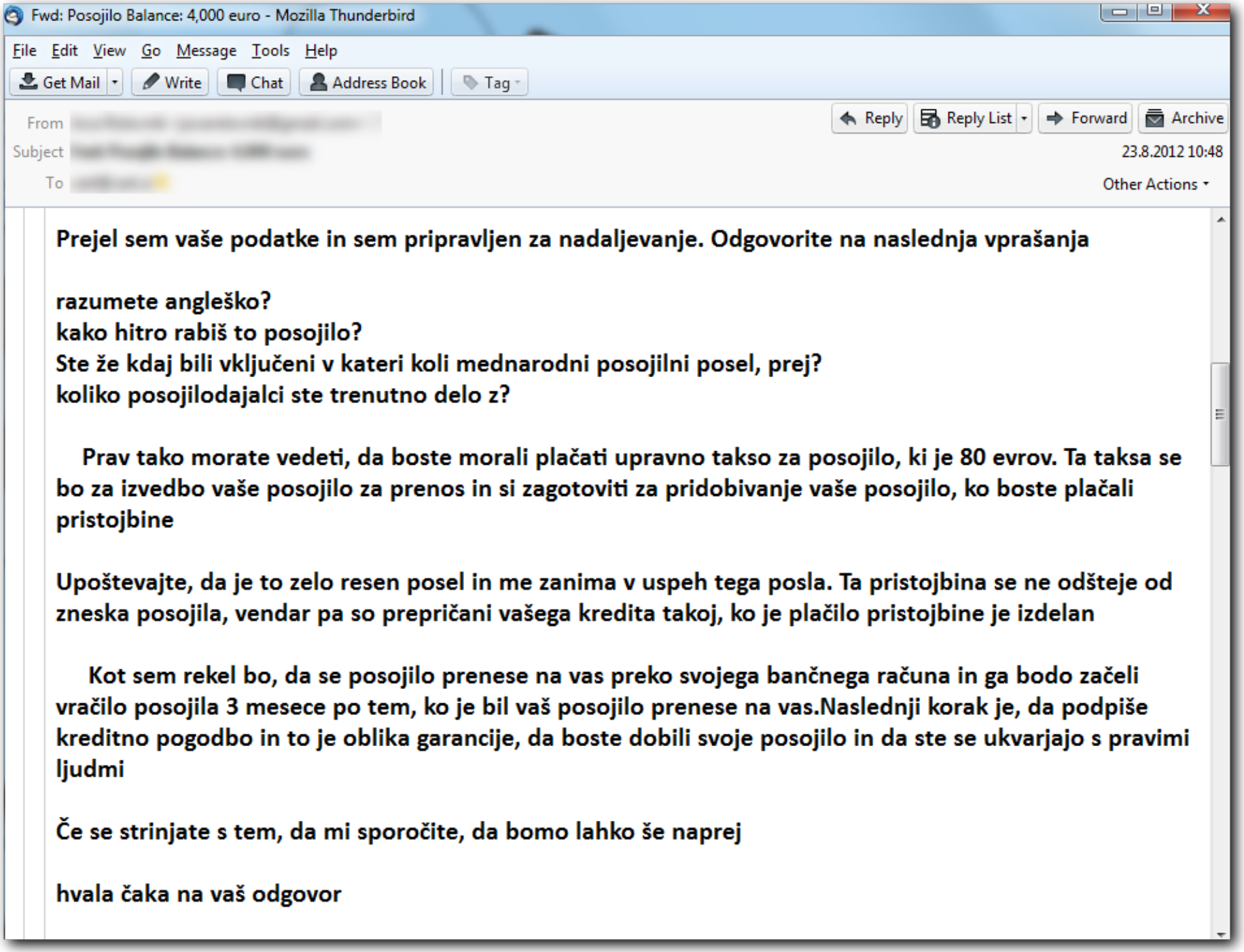
Subsequent upon this Proforma Invoices Approval, the Legal Department of this Board is processing the Contract Agreement, which shall be signed by both parties before the execution of the payment into your bank account.

The Contract Amount will be transferred to your nominated bank account when all requisite procedures are completed. The Honourable Chairman of Public Procurement Department hereby approved your Invoice.

C O N G R A T U L A T I O N S!!!

Yours faithfully,

Dr. Muhammed IBN Hussein
Executive Chairman
Central Tender Committee


Fwd: Posojilo Balance: 4,000 euro - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Chat
Address Book
Tag
From
Subject
To
Reply
Reply List
Forward
Archive
23.8.2012 10:48
Other Actions
Prejel sem vaše podatke in sem pripravljen za nadaljevanje. Odgovorite na naslednja vprašanja
razumete angleško?
kako hitro rabiš to posojilo?
Ste že kdaj bili vključeni v kateri koli mednarodni posojilni posel, prej?
koliko posojilodajalci ste trenutno delo z?
Prav tako morate vedeti, da boste morali plačati upravno takso za posojilo, ki je 80 evrov. Ta taksa se bo za izvedbo vaše posojilo za prenos in si zagotoviti za pridobivanje vaše posojilo, ko boste plačali pristojbine
Upoštevajte, da je to zelo resen posel in me zanima v uspeh tega posla. Ta pristojbina se ne odšteje od zneska posojila, vendar pa so prepričani vašega kredita takoj, ko je plačilo pristojbine je izdelan
Kot sem rekel bo, da se posojilo prenese na vas preko svojega bančnega računa in ga bodo začeli vračilo posojila 3 mesece po tem, ko je bil vaš posojilo prenese na vas.Naslednji korak je, da podpiše kreditno pogodbo in to je oblika garancije, da boste dobili svoje posojilo in da ste se ukvarjajo s pravimi ljudmi
Če se strinjate s tem, da mi sporočite, da bomo lahko še naprej
hvala čaka na vaš odgovor

From Me <tadej.hren@arnes.si>

Reply | Forward | Redirect | More

Subject **Ticket#672942426 <tadej.hren@arnes.si> 19-10-2018 05:46:26 Evidence against you**

18. 10. 2018 18:07

To Me <tadej.hren@arnes.si>

Hello!

My nickname in darknet is hogan49.
I hacked this mailbox more than six months ago,
through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

So, your password from tadej.hren@arnes.si is [redacted]

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!

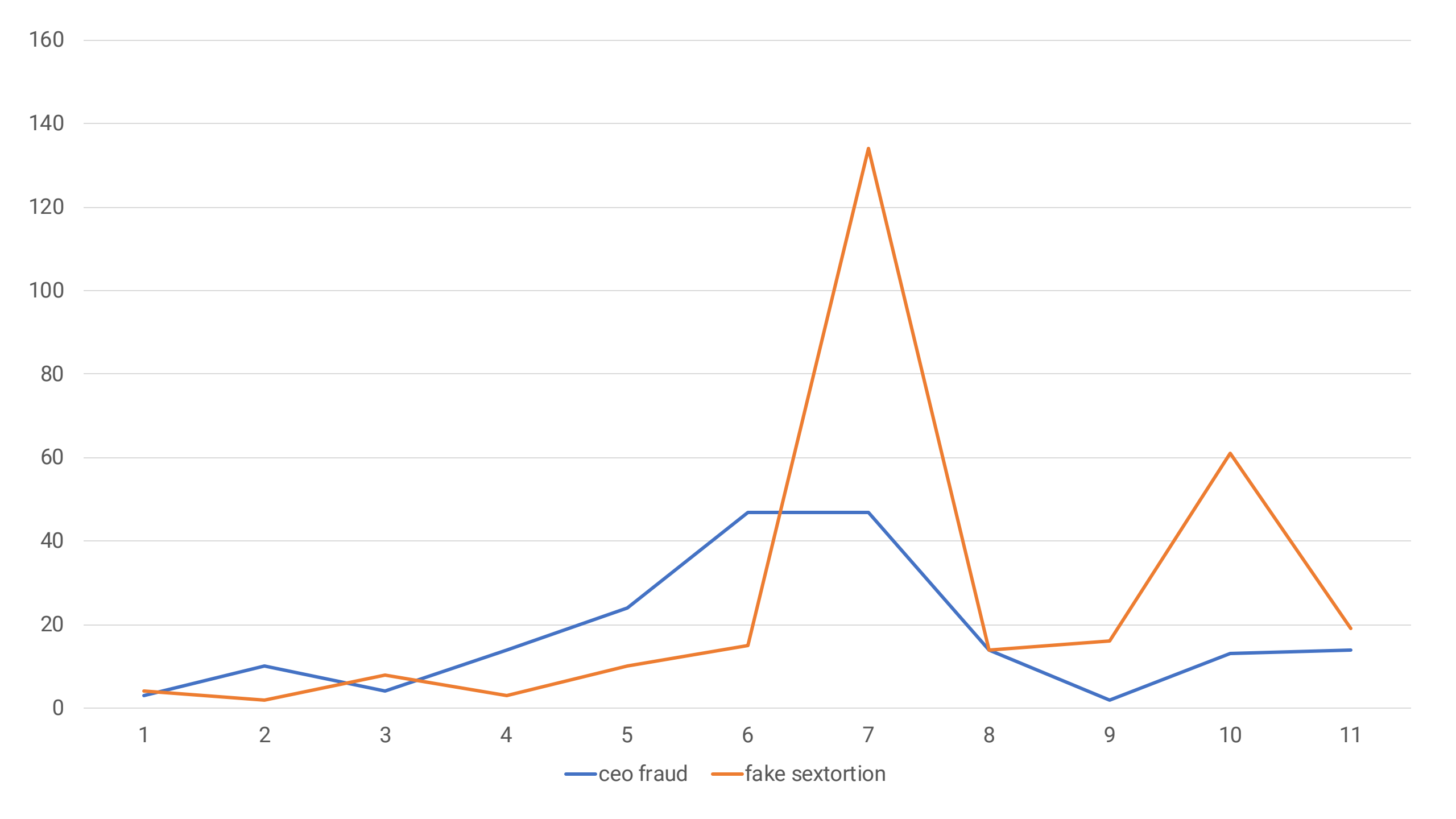
I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $851 is quite a fair price to destroy the dirt I created.

Send the above amount on my BTC wallet (bitcoin): 1EZS92K4xJbymDKwG4F7PNF5idPE62e9XY
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

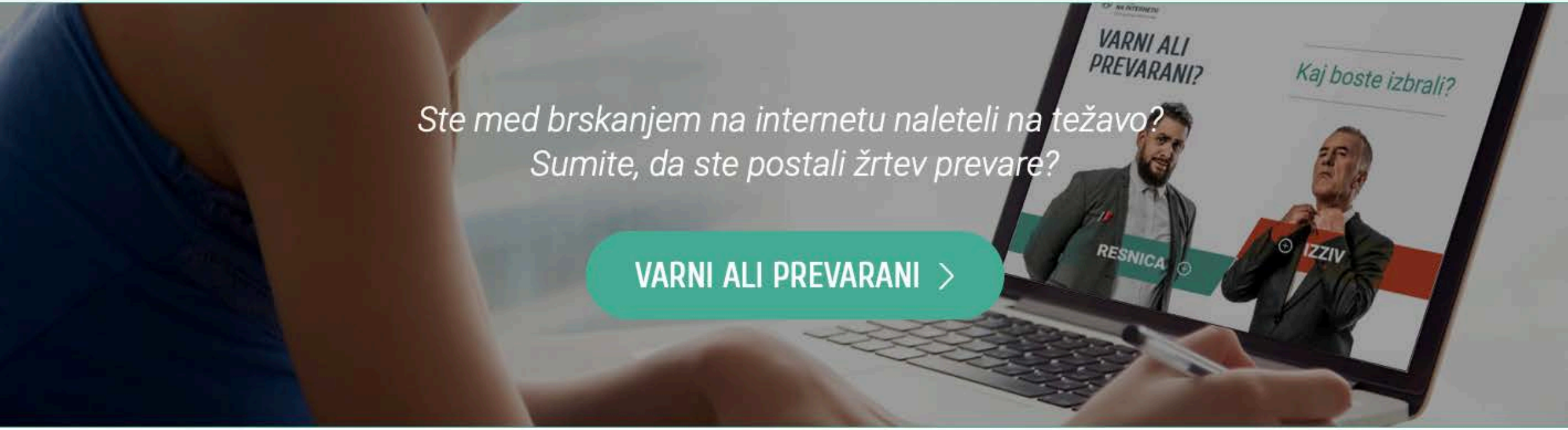

160
140
120
100
80
60
40
20
0
1
2
3
4
5
6
7
8
9
10
11
ceo fraud
fake sextortion

VARNI
NA INTERNETU
Od mene je odvisno vse.

POMOČ IN PRIJAVA

Išči...

PODROČJA ZLORAB | KAKO SE ZAŠČITITI | NASVETI ZA PODJETNIKE | KNJIŽNICA | NOVICE | ZA MEDIJE



Ste med brskanjem na internetu naleteli na težavo?
Sumite, da ste postali žrtev prevare?

VARNI ALI PREVARANI >

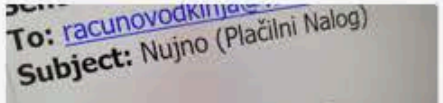
PREPREČIMO PREVARO PREDEN SE ZGODI!

Prijavite se na Varne novice in bodite obveščeni o aktualnih spletnih goljufijah in nasvetih kako se zaščititi pred prevarami na internetu.

Vpišite vaš e-naslov

ODDAJ >

Zadnje novice



13.07.2018

Ali lahko danes

Najpogostejše prevare

Podjetja pozor:

NAJSTRAŠNEJŠA ŽIVAL JE ... MIŠ!

Kažipot za varnost na spletu

10 NASVETOV

ZA MALA PODJETJA

Vsebina

Zakon o informacijski varnosti

- Implementacija EU NIS direktive
- Sprejet na seji DZ 17. aprila 2018, objavljen v UL 26. aprila
- Določa obvezno poročanje o incidentih za *zavezance*
- Določa *pristojni nacionalni organ za kibernetsko varnost*
- *“Nacionalni CSIRT je odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri javnem zavodu Akademska in raziskovalna mreža Slovenije.“*
- **https://cert.si/ZIV**

si·cert

Nacionalni odzivni center
za kibernetsko varnost

VARNI NA INTERNETU

Od mene je odvisno vse.

www.varninainternetu.si