

GOLJUFIJE V 2018

Gorazd Božič, SI-CERT

Mreža znanja 2018, 21. in 22. november





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

Situacijsko zavedanje

9643

MalSpam tlp:white
tlp:green

16 matej@cert.si 2018-10-16 "Fak"

8762

tlp:green

tlp:green
circl:incident-classification="scam"

ecsirt:other="unknown"

circl:topic="individual"

136 matej@cert.si 2018-08-03 Sixt

tlp:white PAP:WHITE

malware_classification:malware-category="Downloader"

23 matej@cert.si 2018-10-16 OSINT

9642

Tool:

Agent

Tesla 🔍

OSINT

OSINT

tlp:white

PAP:WHITE

42 matej@cert.si 2018-10-09 OSINT

9627

1096 matej@cert.si 2018-07-23 Sixtork

Analiza zlonamerne kode

```
IDA View-A Hex View-A Structures  
cnp [ecx+0F8h], ebx  
jnp short loc_10124D8  
cnp [ecx+0E8h], ebx  
loc_10124B2:  
nov [ebp+var_1C], ebx  
jnp short loc_10124DE  
loc_10124D8:  
setnz al  
mov [ebp+var_1C], eax
```

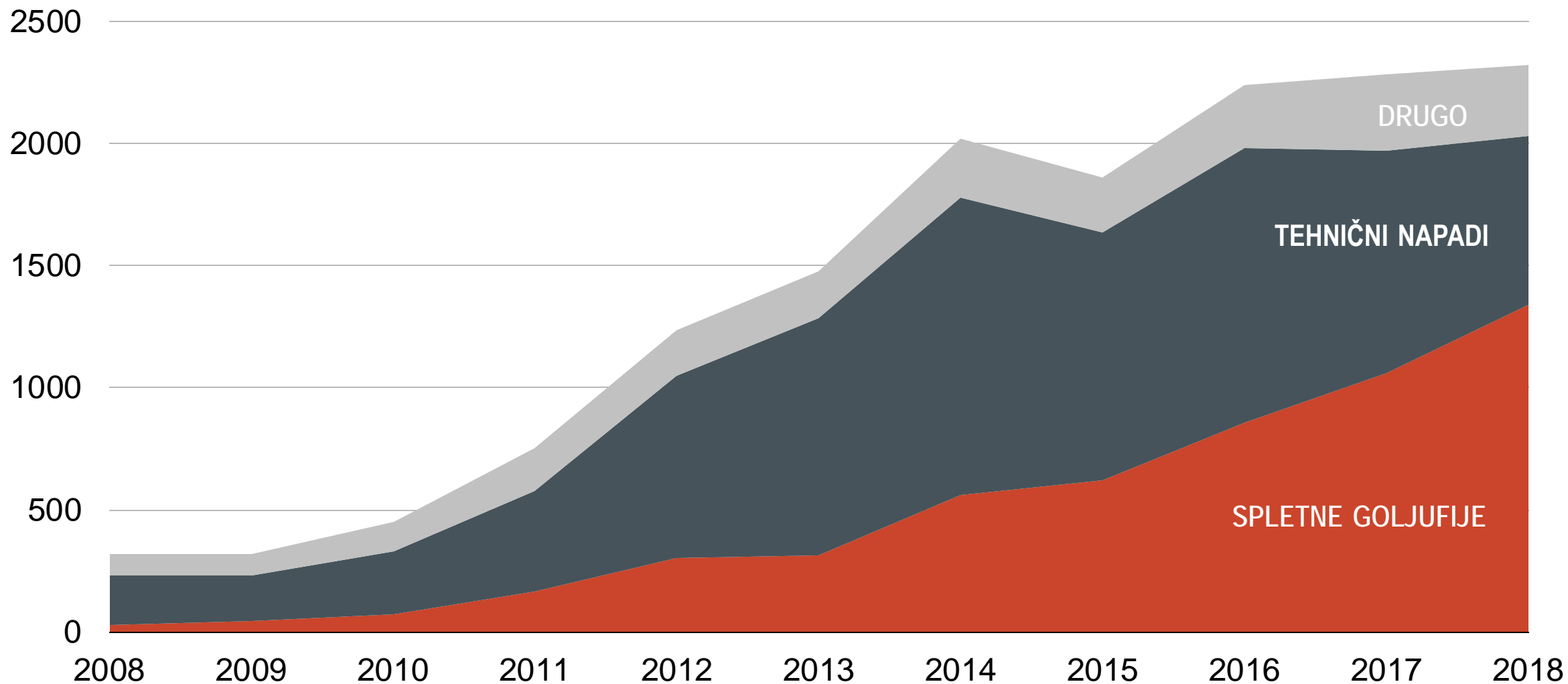
```
loc_10124DE:  
mov [ebp+ns_exc.disabled], ebx  
push 2  
call ds: __set_app_type  
pop [ebp+var_1C], ebx  
or dword_1015014, 0FFFFFFFFh  
call ds: __p_fnode  
mov ecx, dword_101500C  
mov [eax], ecx  
call ds: __p_connnode  
mov ecx, dword_1015008  
mov [eax], ecx  
mov eax, ds: adjust_fdiv  
mov [eax], eax  
mov dword_1015018, eax  
call sub_10127C2  
cnp dword_10149D0, ebx  
jnp short loc_1012530
```

Mednarodno sodelovanje



INCIDENTI

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





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

NAJVIŠJE OŠKODOVANJE
V NIGERIJSKI PREVARI

2016	2017
100.000 €	20.000 €

POVPREČNO OŠKODOVANJE
Z VRIVANJEM V POSLOVNE
KOMUNIKACIJE

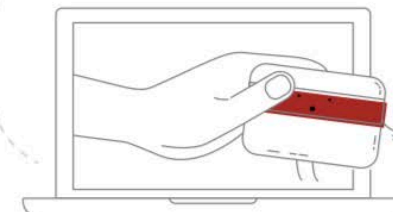
2016	2017
19.200 € (največje: 35.000 €)	13.640 € (največje: 40.000 €)

NAJVIŠJE OŠKODOVANJE
PRI GOLJUFIJI PO AIRBNB

2016	2017
1.000 €	2.100 €

OŠKODOVANJE PRI
PRODAJI NEPREMIČNINE

2016
7.500 €

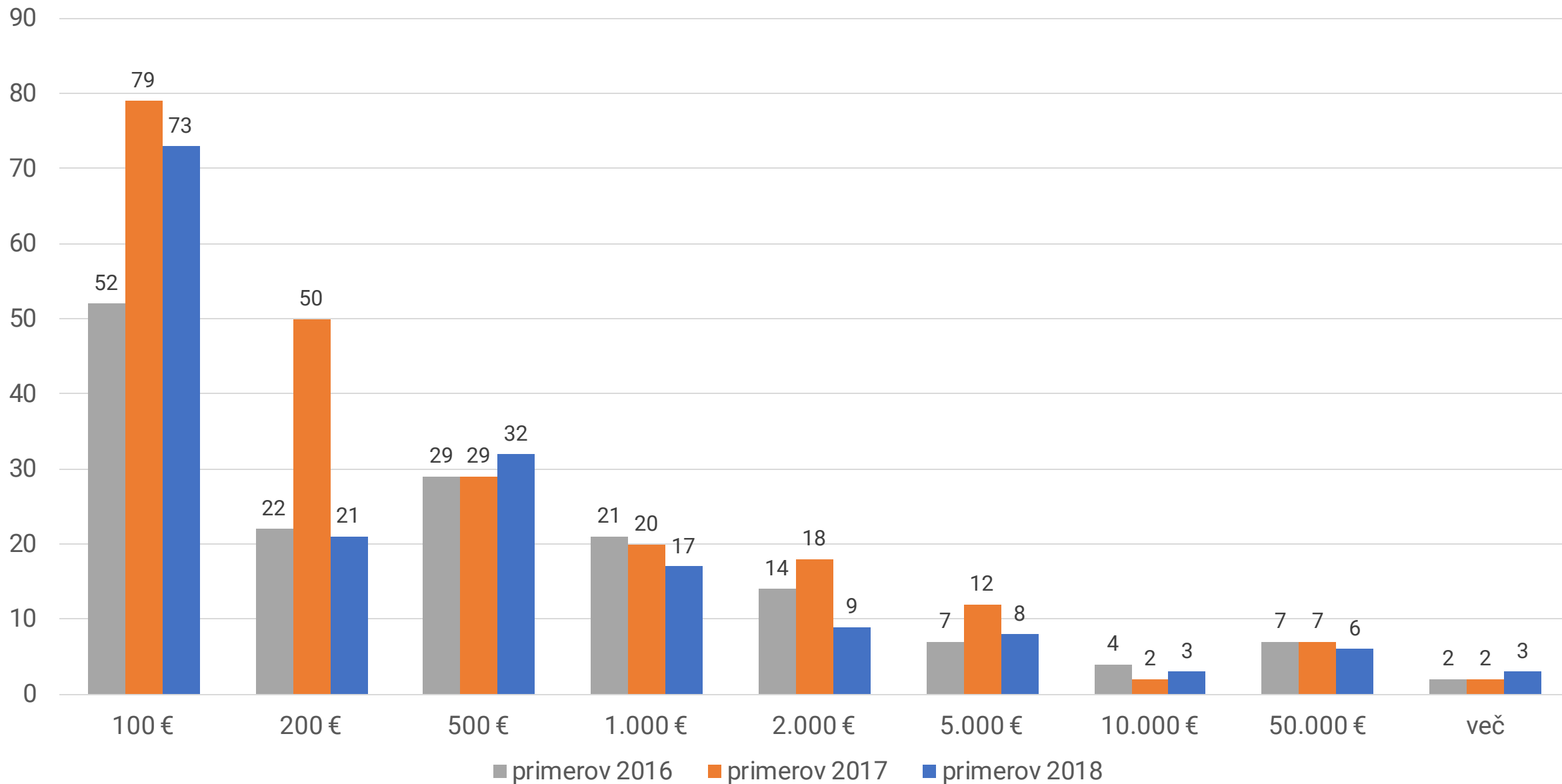
POVPREČNO
OŠKODOVANJE PRI
SPLETNEM NAKUPU

2016	2017
422 €	281 €

POVPREČNO
OŠKODOVANJE PRI
DRUGIH GOLJUFIJAH

2016	2017
3.556 €	3.730 €

Porazdelitev oškodovanj v 2016-2018



Send:

To: racunovodkinja@v...

Subject: Nujno (Plačilni Nalog)

Dobro jutro

Kaj je naša bančno stanje?

Ali lahko danes plačamo EUR 47.900,00?

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: INGDESMXXX

Banka: ING DIRECT

Sklic: INV. 0043291826

Namen plačila: Nakup kapitala

Znesek: 55.000 EUR

Prosim, pošljite plačila potrditev slip.

LP,

[redacted]

From: ██████████ International [<mailto:info@starlinetrading.com>]

Sent: Thursday, August 02, 2018 3:40 PM

To: [fatemeh](#) ██████████

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 by our customer and the account is being investigated.
please confirm as this is a top urgent here.

Lep pozdrav/Kind regards,

██████████

Vrivanje v komunikacijo

Vrivanje v komunikacijo

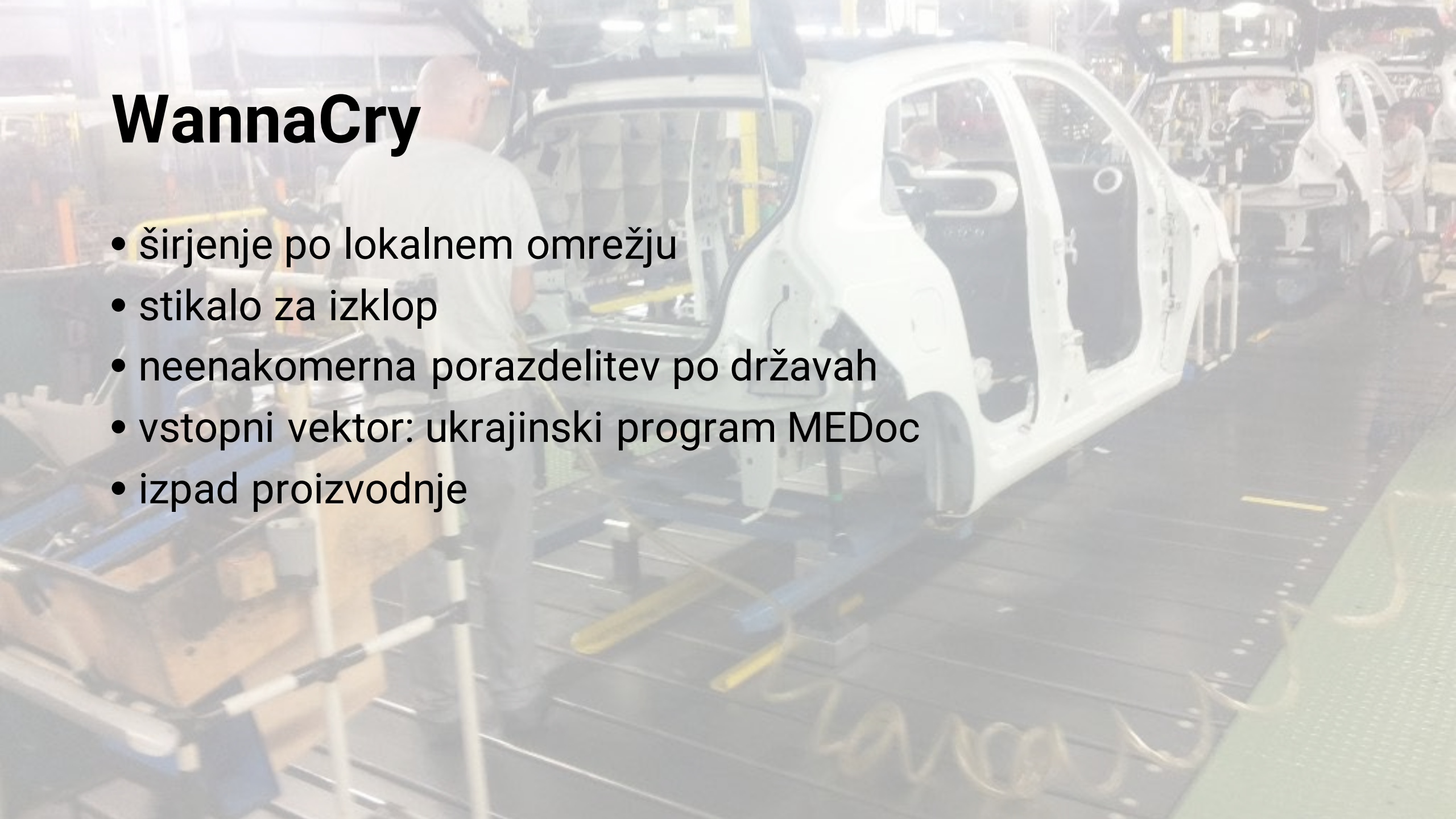
- vdor v poštne predalecne od partnerjev
- spremljanje komunikacije
- podtaknjen TRR denarne mule
- najvišje oškodovanje v 2018: ~ **450.000 EUR!**



Izsiljevalski virusi

WannaCry

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



YOUR FILES ARE ENCRYPTED!

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.

Your documents, photos, databases and all the rest files encrypted cryptographically strong algorithm.

We do not store any decryption keys on our server, the restoration of your files is done as follows:

You will be able to restore files as follows:

- To contact us by e-mail: kervis@protonmail.com & send your personal ID and 3 crypted files, up to 3 MB in size everyone.
- We will decrypt the files and we will send you the originals. As you can see, the instructions where you have to pay many it is necessary to pay.
- You pay and confirm payment.

and you can only receive the DECRYPTED files and not the original files.

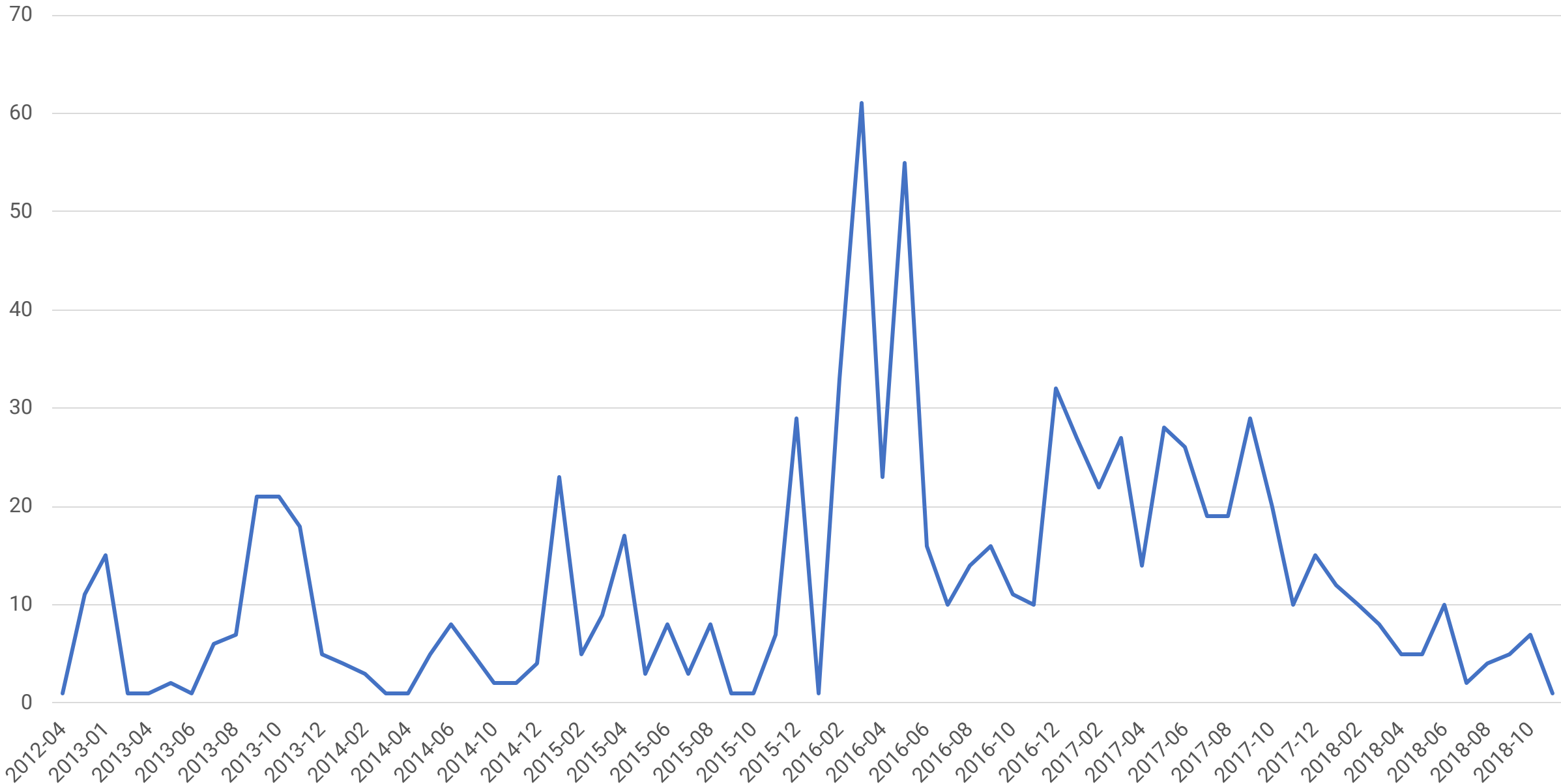
Your personal ID:

```
5E 9C 6D 3E B3 3C 47 DF E1 63 C5 15 89 55 46 C1
24 74 9F C3 72 18 DE 7A 5A 8C 5C 82 5D 2F 49 9C
20 87 64 66 1F 7F B7 67 FA 3C BC 0C 6A 30 98
55 E1 7A C0 E1 7E 66 7A 43 0F A
33 5B 57 63 E9 42 5A 3F 53 9A F8 B8 71 34 FB B4
CB 77 18 6E B9 80 50 30 58 78 19 C6 D5 A0 36 A8
23 61 28 71 CB DB 0F 16 6D 2B 68 68 B7 B7 50 1F
0B 1A 79 E1 95 F8 A1 51 L 05 F8 96 93 68 1E
87 3F 6D E4 3C 81 A7 57 5F 50 AB BC 5F 75 85 1D
6C AC F6 06 5E 2C 5A 97 40 40 33 7A 39 07 07 09
F8 78 78 BC F5 5A F8 53 B8 46 D3 0F 59 24 C 2E
03 3B E1 AFA 4F 0F 2B 1B 11 C 3E 55 5E
1F 22 BA F1 FF FF 52 30 8D 40 36 83 52 7D 86 58
76 23 C3 87 F9 67 09 01 A2 16 74 89 8F 0D 3C F0
DD 18 87 6A 8D 76 7F 37 1A 14 45 28 45 0E 31 2F
8D A1 85 61 A7 01 66 66 71 73 92 57 8E
```

PS:

- It is not our direct responsibility as we do not store the recovery of your files, because we will not store your decryption keys on our server for a long time.
- Be sure to add our email addresses to the trusted list, in your email client's settings. And also check the folder "Spam" when waiting for an email from us.
- If we do not respond to your message for more than 48 hours, write to the backup email : kervis@tutanota.com

Mesečno št. prijav izsiljevalskih virusov



Druge goljufije

EBN European Business Number
Value added tax identification number VAT-ID
Department Republic of Slovenia

ER17116 1798860117

Numero d. az. EUROSPOLEČNOSTI
EUROPSKI POSLOVNI
PSIEBIORSTWA

EBN European Business Number
www.e-b-n.eu
Department Republic of Slovenia

Web: www.e-b-n.eu
Mail: info@e-b-n.eu
Tel.: +49 40 75 11 99 - 0
Fax: +49 40 75 11 99 - 11

Monday - Thursday:
09:00 a.m. - 05:00 p.m.
Friday:
09:00 a.m. - 03:00 p.m.

Your reference: 1
Our reference: 1
Date: 19 October

Reply by Email
Enclosed Bu

FINAL CALL

Missing European Business Number EBN
Davčna številka (ID št. za DDV) - Attachment 1 -

Dear Sir/Madam,

since the Tax Reform Act in 2003 and the Tax Simplification Act in 2004, all tax invoices issued by your company are payable in advance upon receipt of the invoice and the information required for the deduction of input VAT has been adapted to European law. Please verify your company's European Business Number:

accuracy and completeness and correct the information. If you want to correct the information, please select the appropriate information.

Business Number
Value added tax identification number VAT-ID
Department Republic of Slovenia

This form will be machine-read. Please fill in clearly in black or blue block letters. Please be absolutely sure to check that all information is correct and amend or amend if necessary. The company data listed will be used for your entry within www.e-b-n.eu.

Reply by Email
Enclosed Bu

1. Company Information - correct and amend if necessary

Company name

Street / Number / PO Box

Postal code / City

2. Contact information

Telephone / Fax

Website

Email

3. Trade / Legal form

Trade

Legal form

Managing Director

4. Davčna številka (ID št. za DDV)

S.I. _____

5. Company information of tax liability

5.1. We submit the following information concerning our company

5.2 We only have sales that do not lead to the deduction of input VAT.

5.3 We are liable for VAT.

5.4 We are a legal entity that is not an entrepreneur.

Please tick where applicable.

Order: We hereby confirm the accuracy of our company's data as per the information given above and we accept the advertisement's liability for the information provided in this order with DAD GmbH (Publisher) to publish them in a graphically highlighted form on www.dad.de. We accept the advertisement's liability for the information provided in this order with DAD GmbH (Publisher) to publish them in a graphically highlighted form on www.dad.de. We accept the advertisement's liability for the information provided in this order with DAD GmbH (Publisher) to publish them in a graphically highlighted form on www.dad.de. We accept the advertisement's liability for the information provided in this order with DAD GmbH (Publisher) to publish them in a graphically highlighted form on www.dad.de.



لجنة المناقصات المركزية

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.....



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 [redacted] Reply Reply List Forward Archive
Subject [redacted] 23.8.2012 10:48
To [redacted] 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 ██████████

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!

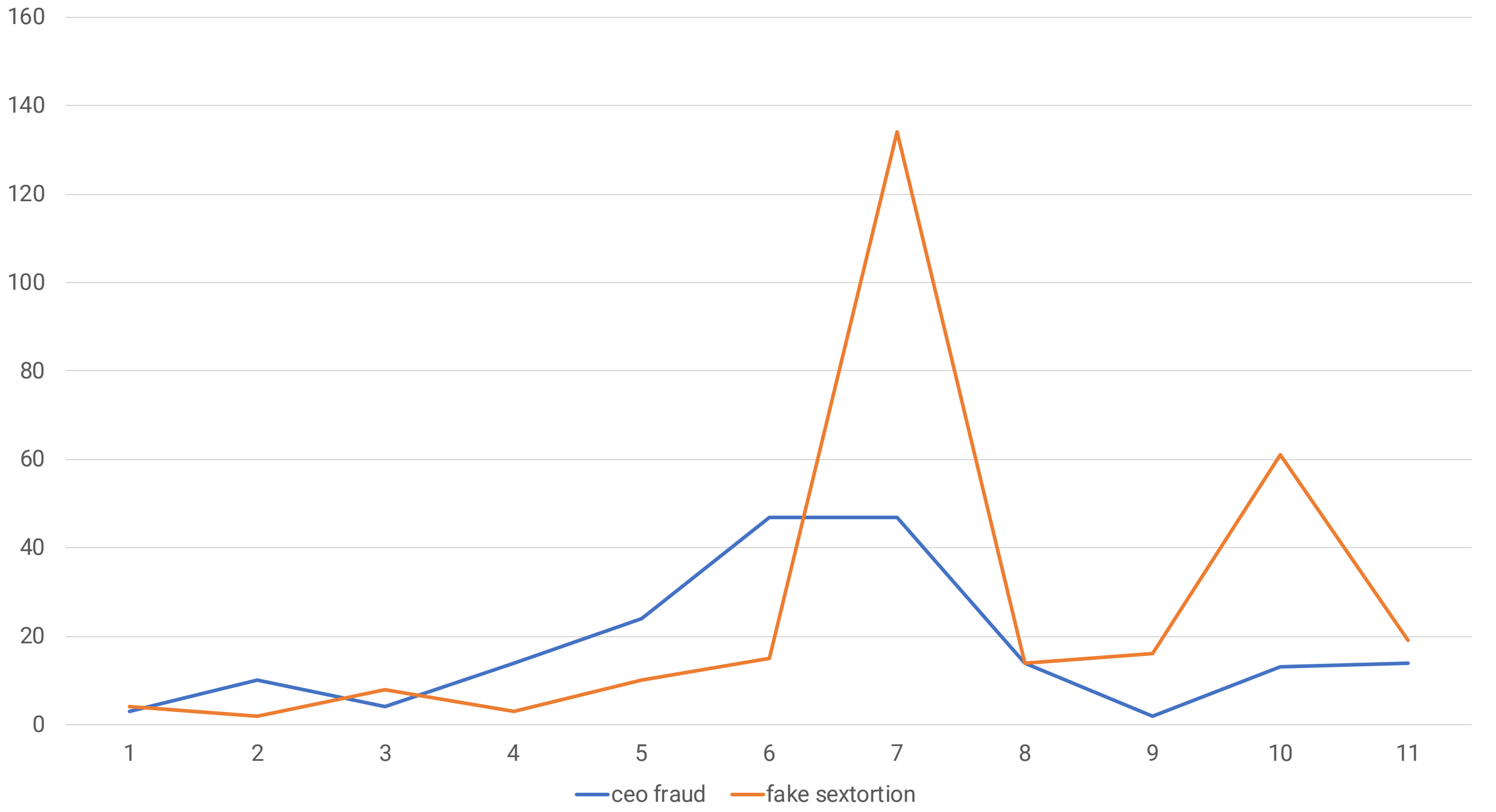
I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that \$851 is quite a fair price to destroy the dirt I created.

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!





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

To: [racunovodkinje](#)
Subject: Nujno (Plačilni Nalog)

13.07.2018

Ali lahko danes

Najpogostejše prevare



Podjetja pozor:

NAJSTRAŠNEJŠA ŽIVAL JE ... MIŠ!

Kažipot za varnost na spletu

10
NASVETOV
ZA MALA PODJETJA

2

Vsebina

- 3 — 1. Previdno ravnajte z elektronsko pošto
- 4 — 2. Nastavite zapletena in močna gesla
- 5 — 3. Varno uporabljajte spletno banko
- 6 — 4. Poskrbite za varnost spletnih strani
- 7 — 5. Varnostno kopirajte, kopirajte in še enkrat kopirajte
- 8 — 6. Vodite popis osnovnih sredstev
- 9 — 7. Previdno uporabljajte službene prenosnike in telefone
- 10 — 8. Programsko opremo redno posodablajte
- 11 — 9. Poskrbite za varno delo od doma
- 12 — 10. Ne pozabite na varnost brezžičnega omrežja
- 13 — Je za varstvo podatkov v vašem podjetju dobro poskrbljeno?

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 kibernetško 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 kibernetško varnost



VARNI NA INTERNETU

Od mene je odvisno vse.

www.varninainternetu.si