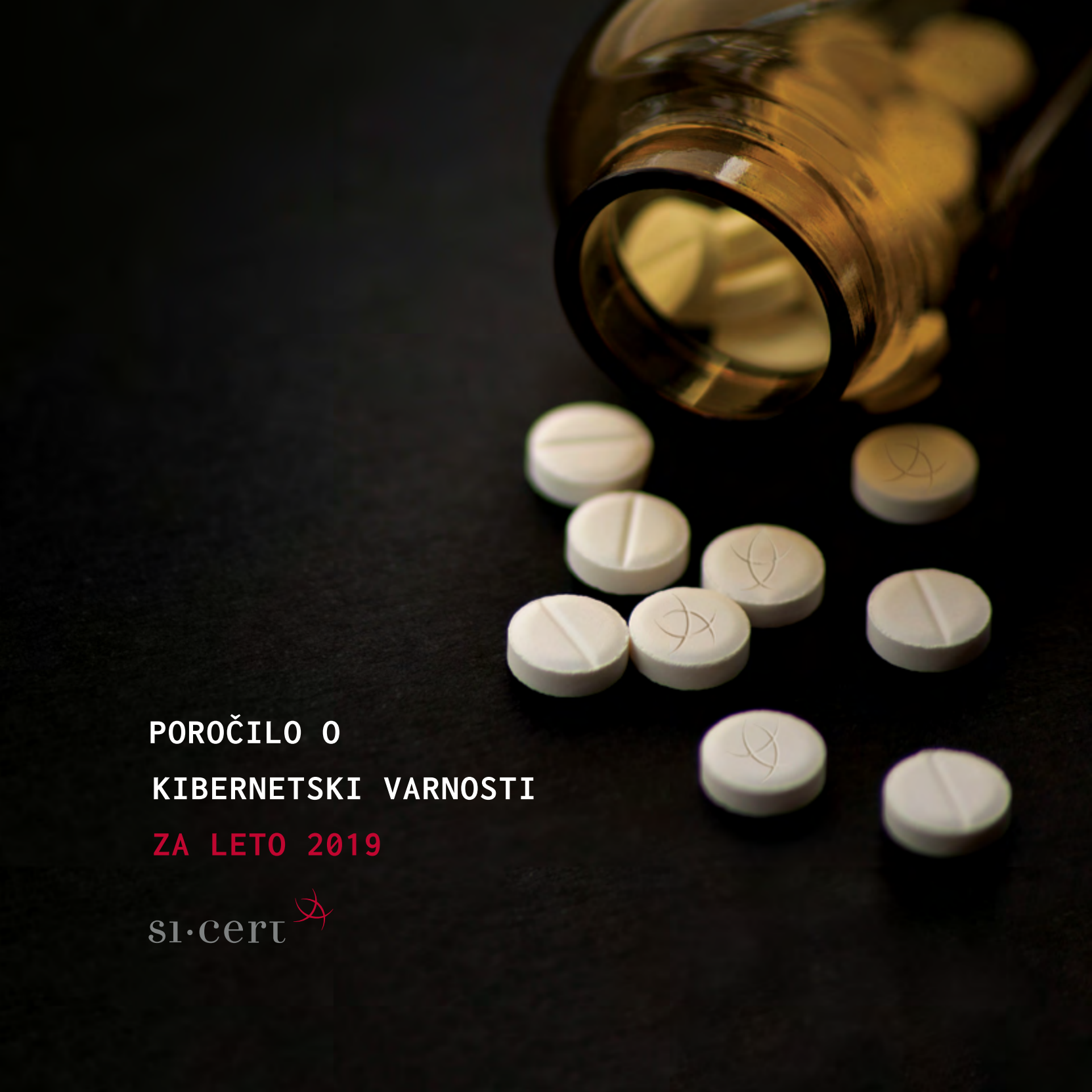


POROČILO O KIBERNETSKI VARNOSTI ZA LETO 2019

si·cert

POROČILO O KIBERNETSKI VARNOSTI

ZA LETO 2019

si·cert

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 Uprava RS za informacijsko varnost Ministrstva za javno upravo.

URSIV

Leto sprememb

Kdor se ukvarja s kibernetsko varnostjo, ve, kako dinamično je to področje. Vendar pa je leto 2019 vseeno izstopalo po tem, koliko stvari se je zgodilo in na koliko stvari smo morali postati pozorni. Res je, Zakon o informacijski varnosti je bil sprejet že leta 2018, ampak kot pravi pregovor, hudič je v detajlih, ki smo jih morali opredeliti sami.

Večje pristojnosti so zahtevale razmisleke o postopkih, označevanju incidentov, vodenju statistike in poročanju Upravi RS za informacijsko varnost. Odločili smo se, da sami prevzamemo pobudo in smo zato posvojili osnutek evropskega referenčnega modela taksonomije incidentov, ki ga pripravlja agencija ENISA. Pri odločanju o tem, kdaj je incident manjše in kdaj večje stopnje, smo v svojih postopkih na začetku leta 2019 pilotno prevzeli model britanskih kolegov in nato pozitivne izkušnje predstavili evropskim kolegom, ki so potrdili, da bodo šli v podobni smeri.

Hkrati smo se obrnili tudi na nam bližnjo regijo, Zahodni Balkan. Naše dejavnosti pri podpori vzpostavitve novih skupin CSIRT v tamkajšnji regiji segajo nazaj v leto 2011, smo pa lani še posebej izstopali pri prenosu znanja skozi tehnični kolokvij FIRST, ki je bil odprt za vse novonastale strukture v regiji, ki bodo operativno delovale pri obravnavi incidentov. To vidimo kot enkratno priložnost za prenos znanja in možnost vzpostavitve Slovenije kot središča za izmenjavo izkušenj na področju kibernetske varnosti.

To vlogo pa bomo lahko izpolnili le, če bomo vedno sami skrbeli za lastne zmogljivosti in znanje. Zato na SI-CERT-u s pomočjo evropskih sredstev gradimo nov laboratorij za analizo zlonamerne kode in vozlišče za enotno izmenjavo informacij med nacionalnimi skupinami CSIRT članic EU. Vse investicije v zmogljivo opremo pa nimajo prav nobenega smisla, če je ne uporabljajo strokovnjaki, ki svoje izkušnje gradijo z večletnim operativnim delom. Naša usmeritev je jasna: zainteresiran in izkušen kader mora biti vedno na prvem mestu.

Gorazd Božič,
vodja SI-CERT

Predstavitev centra SI-CERT

SI-CERT *(Slovenian Computer Emergency Response Team)* je nacionalni odzivni center za kibernetsko varnost. Ustanovljen je bil leta 1995, primarna naloga centra pa je strokovna pomoč pri preiskovanju incidentov, koordinacija njihovega razreševanja, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdajanje opozoril upraviteljem omrežij in širši javnosti o trenutnih grožnjah v kibernetskem prostoru.

SI-CERT izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu. Delovanje centra SI-CERT opredeljuje 28. člen Zakona o informacijski varnosti (ZInfV). Bogate izkušnje, osredotočenost na specializirana strokovna znanja preiskovanja računalniških incidentov in dobra mednarodna vpetost postavljajo SI-CERT v središče operativnega delovanja pri odzivu na kibernetske incidente v državi.

SI-CERT je član Mreže CSIRT po direktivi NIS in je akreditiran skozi program 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.

CERT ali CSIRT?

CSIRT = Computer Security Incident Response Team
CERT = Computer Emergency Response Team

Obe kratici označujeta odzivni center za obravnavo incidentov s področja kibernetske varnosti in sta sinonima. V obdobju pred letom 2000 se je uporabljal pojem CERT, potem pa vedno bolj CSIRT.

SI-CERT je financiran iz sredstev, ki jih zagotavlja Uprava Republike Slovenije za informacijsko varnost Ministrstva za javno upravo, ki je pristojni nacionalni organ za kibernetsko varnost. 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.

si·cert

ZAVEDANJE O STANJU

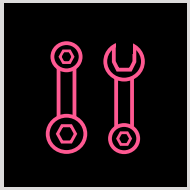
Na podlagi priglašenih incidentov, podatkovnih virov o okužbah in ranljivostih, izmenjave podatkov o aktualnih grožnjah z drugimi centri, se izdela slika stanja in ocene ogroženosti, ki je podlaga za odločitev o primernih ukrepih za zmanjševanje tveganj.

ZDRAVJE KIBERNETSKEGA PROSTORA

Podatki o ranljivih sistemih in videnih okužbah prek zaseženih omrežij botnet kažejo na zdravje omrežij in sistemov v Sloveniji in omogočajo distribucijo opozoril in navodil upraviteljem in končnim uporabnikom prek stikov pri operaterjih.

MEDNARODNO SODELOVANJE

Redno operativno sodelovanje in izmenjava podatkov o opravljenih analizah in indikatorjih zlorab (IoC) krepi bazo znanja, potrebnega pri preiskovanju incidentov.



STROKOVNA PODPORA

Specializirana znanja preiskovanja vdorov, omrežne forenzike in analize zlonamerne kode omogočajo učinkovit in ustrezen odziv na zaznane varnostne incidente.

SODELOVANJE ZNOTRAJ DRŽAVE

Preiskovanje incidenta lahko poteka iz različnih pogledov, zato je pomembno sodelovanje z organi pregona, inšpekcijskimi službami in sektorskimi regulatornimi organi.

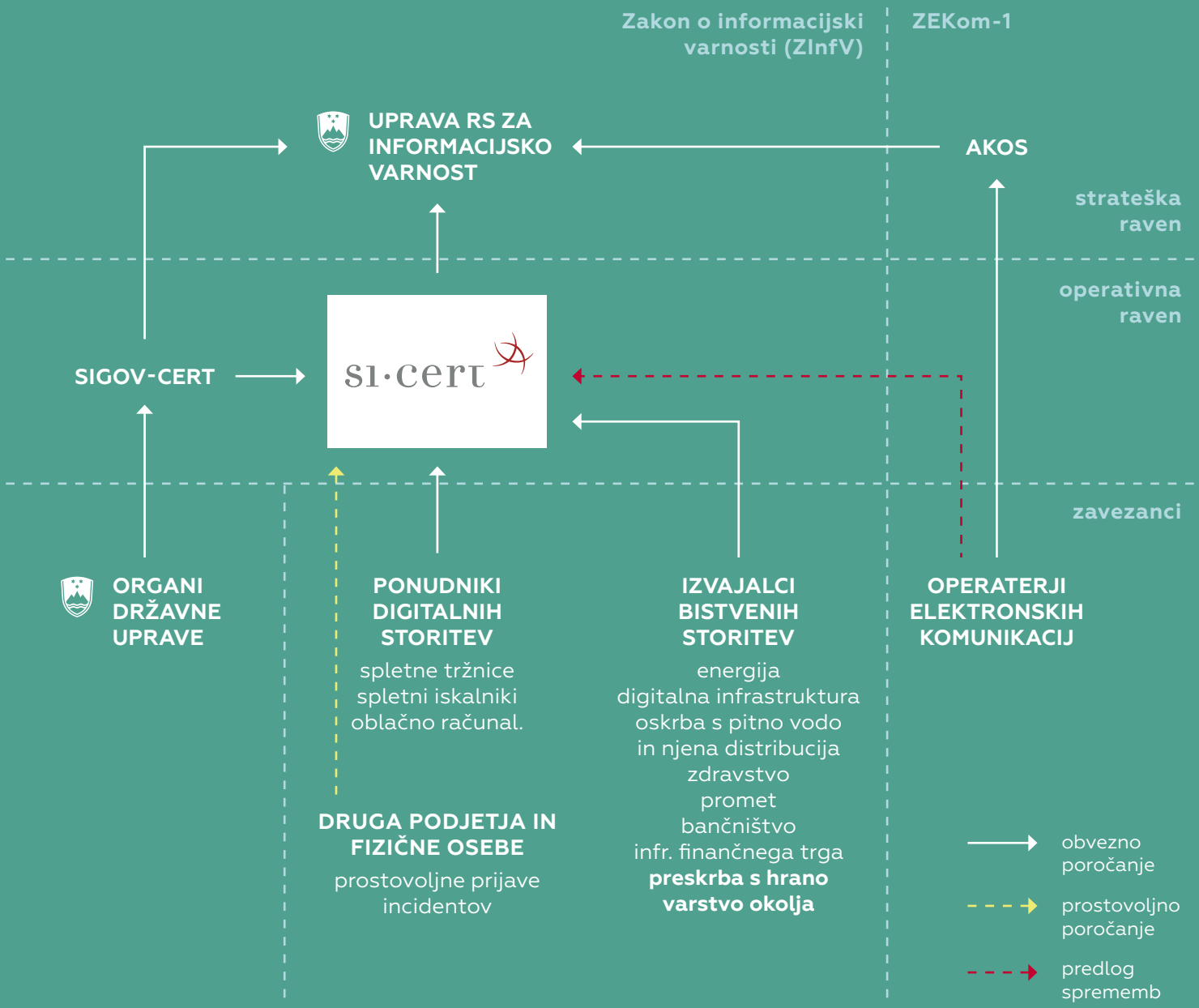
OBVEŠČANJE JAVNOSTI

Obvestila za strokovno javnost, program ozaveščanja Varni na internetu, sodelovanje z mediji, koordinacija odgovornega razkrivanja ranljivosti zaokroža funkcije odzivnega centra.

Kibernetski incidenti

Odzivni center SI-CERT je pristojen za obravnavo incidentov vseh zavezancev po Zakonu o informacijski varnosti (28. člen). Na SI-CERT lahko priglasijo incident tudi vsa druga podjetja, javne ustanove ali fizične osebe.

V primeru vdora, okužbe računalnika ali druge omrežne zlorabe se prijavo z opisom incidenta pošlje na elektronski naslov cert@cert.si, sporoči po telefonu na številko (01) 479 88 22 ali izpolni prijavni obrazec na spletni strani www.varninainternetu.si. Državni organi incidente sporočajo SIGOV-CERT, ki je CSIRT državnih organov (29. člen zakona).

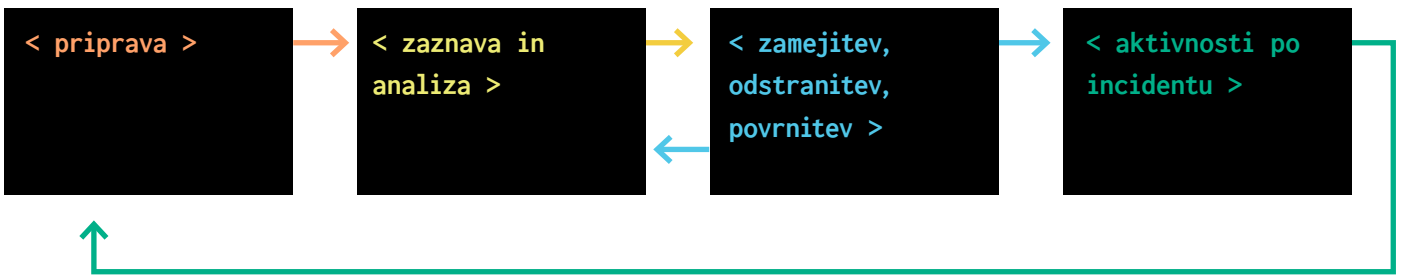

Zakon o informacijski varnosti (ZInfV)
ZEKom-1
UPRAVA RS ZA INFORMACIJSKO VARNOST
AKOS
strateška raven
operativna raven
SIGOV-CERT
si·cert
zavezanci
ORGANI DRŽAVNE UPRAVE
PONUDNIKI DIGITALNIH STORITEV
spletne tržnice
spletni iskalniki
oblačno računal.
IZVAJALCI BISTVENIH STORITEV
energija
digitalna infrastruktura
oskrba s pitno vodo in njena distribucija
zdravstvo
promet
bančništvo
infr. finančnega trga
preskrba s hrano
varstvo okolja
OPERATERJI ELEKTRONSKIH KOMUNIKACIJ
DRUGA PODJETJA IN FIZIČNE OSEBE
prostovoljne prijave incidentov
obvezno poročanje
prostovoljno poročanje
predlog sprememb

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 prek 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. Dejavnosti 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.

FAZE OBRAVNAVE VARNOSTNEGA INCIDENTA NA OMREŽJU



Dejavnosti SI-CERT

OBRAVNAVA PRIJAV VARNOSTNIH INCIDENTOV

Kdorkoli lahko pošlje prijavo ob zaznanem incidentu: vdor v sistem, okužba, zloraba ali goljufija; 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 skuša ranljivosti čim hitreje odpraviti ali vsaj zmanjšati posledice.

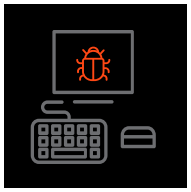
ANALIZA ŠKODLJIVE KODE

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 s programom 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 posojilih)

Kaj storimo na SI-CERT

Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami; svetovanje o ukrepih za sanacijo stanja.

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

Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.

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 prek phishing napada ali napada okužbe računalnika)

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

SPLETNA GOLJUFIJA
(lažne spletne trgovine, prevare pri prodaji in nakupih prek spletnih posrednikov, lažna posojila, nigerijske, loterijske in ljubezenske prevare)

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

Vrste incidentov

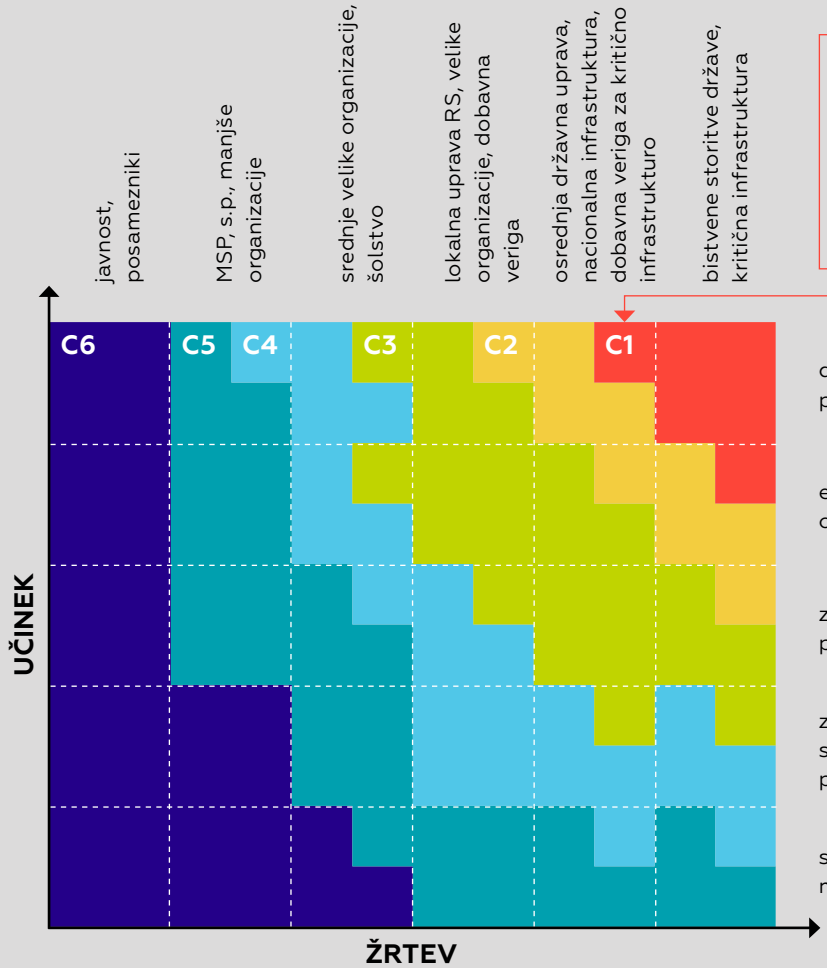
Na SI-CERT-u smo razvrščanje incidentov v kategorije uvedli že leta 2004. Kot mnogi odzivni centri takrat smo se sami odločili, kako bomo opredelili vrste incidentov. Kasneje se je pokazala potreba po poenotenju taksonomije incidentov in začeli so se pogovori v različnih skupinah CSIRT (TF-CSIRT: skupina vseh evropskih skupin CSIRT) in projektih (kot je eCSIRT.net). Z implementacijo direktive NIS po državah članicah EU pa so se dejavnosti glede usklajevanja taksonomije preselile tudi v Mrežo CSIRT, koordinacijo dejavnosti pa izvaja agencija ENISA.

Na SI-CERT-u od 1. 1. 2019 uporabljamo novo razvrščanje incidentov, narejeno na osnovi referenčne taksonomije, ki jo je predpisala agencija ENISA (https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/). Taksonomijo smo dopolnili z nekaterimi vrstami zlorab, s katerimi se prvenstveno srečujemo pri ozaveščanju javnosti. Opravljena je bila preslikava stare kategorizacije od leta 2016 naprej v novo taksonomijo, kar omogoča pregled nad številčnimi trendi obravnavanih incidentov.

Stopnje incidentov

Poleg vrste incidenta lahko določimo tudi njegovo stopnjo. Zakon o informacijski varnosti v 21. členu določa vrednotenje incidenta v tri stopnje (lažji, težji, kritičen) in podaja opisno razlago kot pomoč pri vrednotenju. Pri triaži incidenta pa potrebujemo sistem, ki bo preiskovalcu s preprosteje določljivimi parametri omogočil določanje stopnje. Novembra 2018 je na sestanku Mreže CSIRT predstavnik britanskega centra za kibernetsko varnost NCSC-UK predstavil matriko stopnjevanja, ki je vzbudila veliko zanimanje drugih članov. Na njeni osnovi je bilo vpeljano tudi stopnjevanje incidentov na SI-CERT-u in predstavljeno Upravi RS za informacijsko varnost.

Stopnja incidenta se v matriki opredeli tako, da se določi učinek incidenta (E, Effect) in žrtev incidenta (V, Victim). Za posamični incident se lahko uporabi tudi oznako pomemben incident, ki stopnjo lahko zviša.



Oznaka POMEMBNO

- zelo razširjena zloraba ali ranljivost
- velik vpliv na žrtev
- strateško pomemben akter
- velika javna izpostavljenost

Oznaka KRITIČNO

- dejanske posledice se vrstijo
- potreba po takojšnji zamejitvi
- ogroženost življenja

dlje trajajoče motnje bistvenih storitev in povezanih sistemov

eksfiltracija, poškodovanje ali izguba ključnih in občutljivih podatkov in intelektualne lastnine

zlonamerna koda, C2 komunikacija, aktivni vdor preko omrežja, zač. motnja storitev in sistemov

zlonameren napad nižje pomembnosti, ciljano skeniranje, phishing, izguba manj občutljivih podatkov

skeniranje in pregledovanje, identifikacija možnih tarč ali žrtev, goljufije

C1: Kritičen incident
povzročanje resne motnje delovanja osrednjih državnih storitev, motnja stabilnosti države

C2: Zelo pomemben incident
zaznan ali zelo možen vpliv na občutljive podatke in delovanje državne in kritične infrastrukture

C3: Pomemben incident
zaznan ali možen vpliv na gospodarstvo, dele državne infrastrukture in dobavno verigo za kritično infrastrukturo

C4: Incident višje stopnje
zaznan ali možen vpliv na srednja podjetja ali nižji vpliv na gospodarstvo in dele države ali dobavno verigo

C5: Incident srednje stopnje
zaznan ali možen vpliv na mala podjetja, nizek vpliv na srednja, priprrave na napad na gospodarstvo ali državno infrastrukturo

C6: Rutinski incident
vpliv na javnost ali priprave in poskusi, ki bi vplivali na posameznike in MSP

Matrika povzeta po dokumentu »National Cyber Incident Categorisation« britanskega centra za kibernetsko varnost NCSC-UK, UK Crown Copyright ©, predstavljenega na Mreži CSIRT. Prevod in prilagoditev: SI-CERT.

TLP: semafor za posredovanje informacij

Skupine CSIRT uporabljamo poseben protokol za označevanje vsebine, ki določa, s kom lahko vsebino delimo. Gre za TLP, Traffic Light Protocol, ki je postal standard pri izmenjavi informacij, zato se od vsake nove skupine CSIRT pričakuje, da bo dobro seznanjena z lestvico TLP in bo pravila označevanja strogo upoštevala. Pošiljatelj, ki označi vsebino po lestvici TLP, se mora prepričati, da vsi naslovniki razumejo, kaj oznaka pomeni.

TLP IN TAJNI PODATKI

Vsaka država z zakonom določa označevanje tajnih podatkov in načine njihovega širjenja. Tako se že pri stopnji INTERNO mora uporabljati državno odobren sistem za šifriranje, višjih stopenj (ZAUPNO, TAJNO in STROGO TAJNO) pa v nobenem primeru ni dovoljeno izmenjevati po javnih elektronskih omrežjih. Pri obravnavi incidentov podatki niso uradno označeni s stopnjo tajnosti in se praviloma morajo izmenjevati po javnem omrežju (internet), pri čemer je seveda pomembno, da se uporabljajo ustrezni postopki, ki zagotavljajo integriteto in zaupnost podatkov. Lahko gre recimo za občutljive podatke o novoodkritih ranljivostih ali pa za osebne podatke, ki jih moramo čim prej razširiti znotraj skupnosti CSIRT, da se obvesti končne uporabnike o možni zlorabi. V teh primerih se uporablja sistem šifriranja podatkov PGP/GPG in označevanje po lestvici TLP. Zakonsko določeni tajni podatki in TLP sta torej za dva ločena sistema (lahko bi rekli na ločenih oseh, ortogonalna), z drugačnimi nameni in drugačnimi zahtevami pri pretoku podatkov.

INFORMACIJA NI ZA RAZKRITJE, OMEJENO LE NA PRISOTNE

Naslovniki ne smejo deliti informacije izven okvirja samega sestanka ali pogovora, v katerem je bila informacija posredovana. Informacija TLP:RED se mora posredovati ustno ali osebno.

RAZKRITJE OMEJENO NA ORGANIZACIJE UDELEŽENIH

Naslovniki lahko delijo informacijo samo znotraj svoje organizacije. Pošiljatelj lahko dovoli izmenjavo tudi s partnerskimi organizacijami naslovnika, ko je poznavanje informacije nujno pri zaščiti in preprečevanju nadaljnje škode.

RAZKRITJE OMEJENO NA SKUPNOST ALI SEKTOR

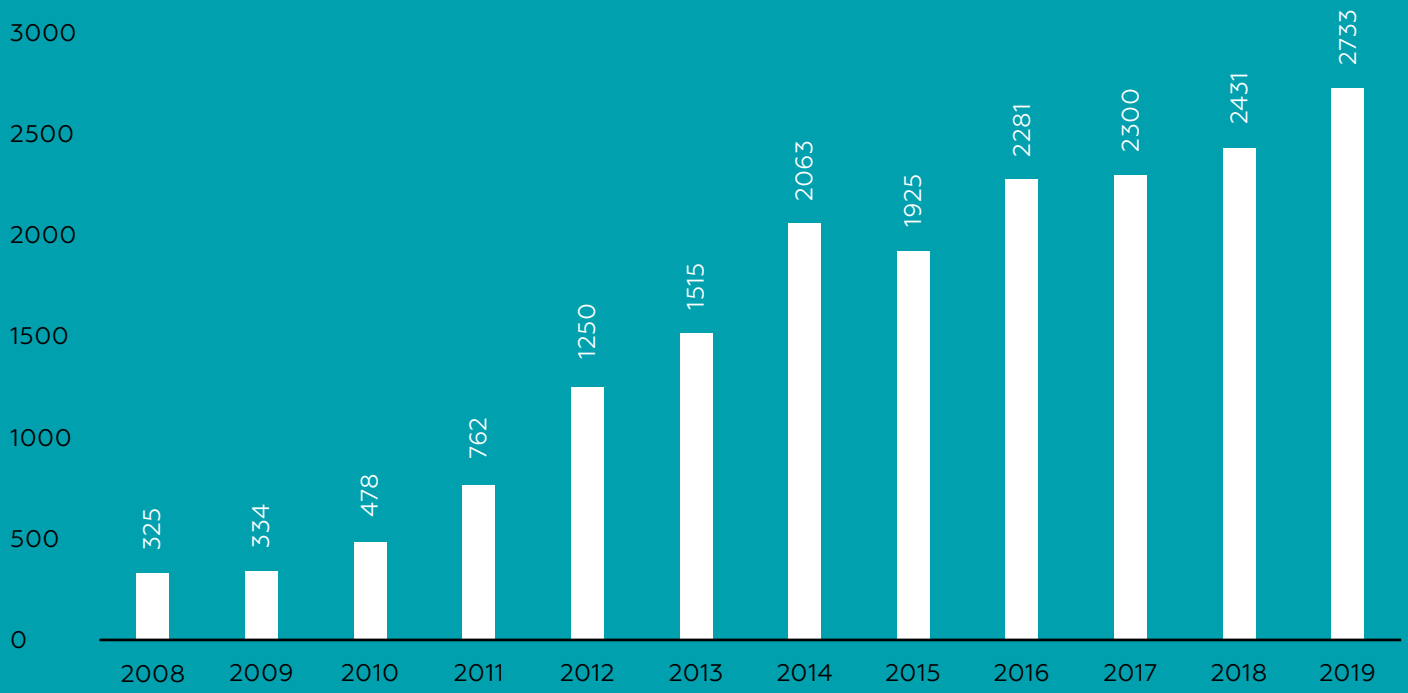
Naslovniki lahko delijo informacijo po potrebi znotraj svoje organizacije ter znotraj svoje skupnosti ali sektorja, vendar pa ne po komunikacijskih kanalih, ki so dostopni tudi širši javnosti (objava na javno dostopnih mestih).

RAZKRITJE NI OMEJENO

Naslovniki lahko informacijo prosto delijo naprej.

Kibernetska varnost v številkah

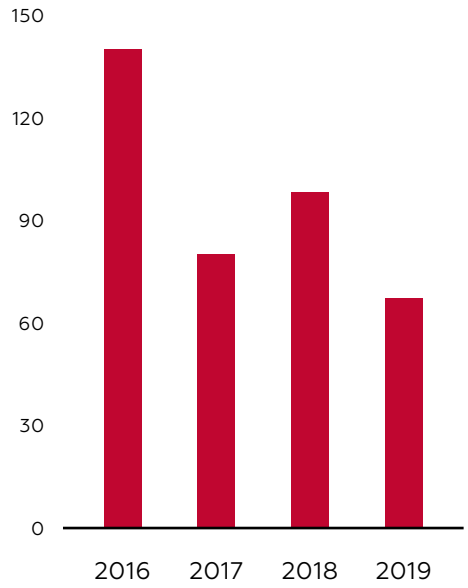
ŠTEVILO OBRAVNAVANIH INCIDENTOV PO LETIH



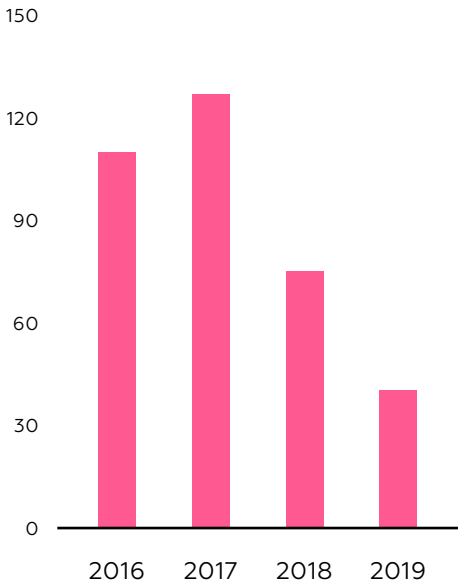
Podrobno razčlenitev glede na vrsto incidentov za obdobje 2016–2019 si lahko ogledate na straneh 24–27.

Za incidente v letih 2016–2018 je bila opravljena večfazna preslikava v novo taksonomijo, pri čemer je ostalo nekaj incidentov po novi shemi nerazvrščenih, kar nima bistvenega vpliva na prikaz trendov.

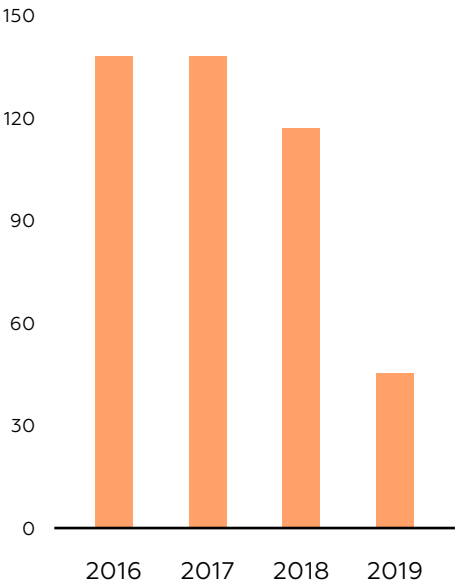
NEPRIMERNA VSEBINA



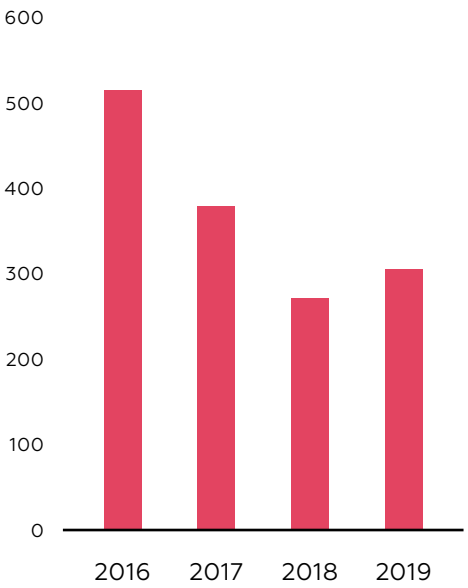
ZBIRANJE INFORMACIJ



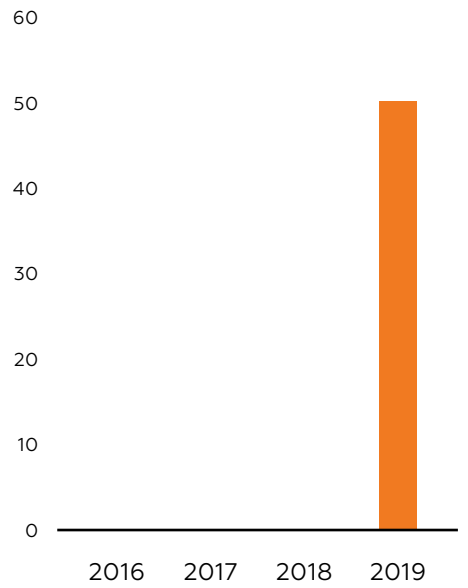
VDORI



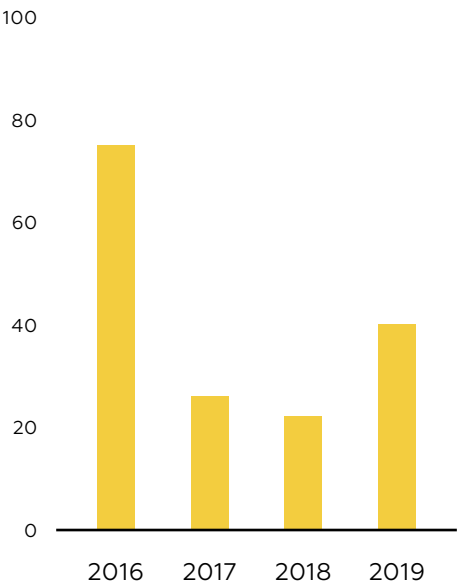
ZLONAMERNA KODA

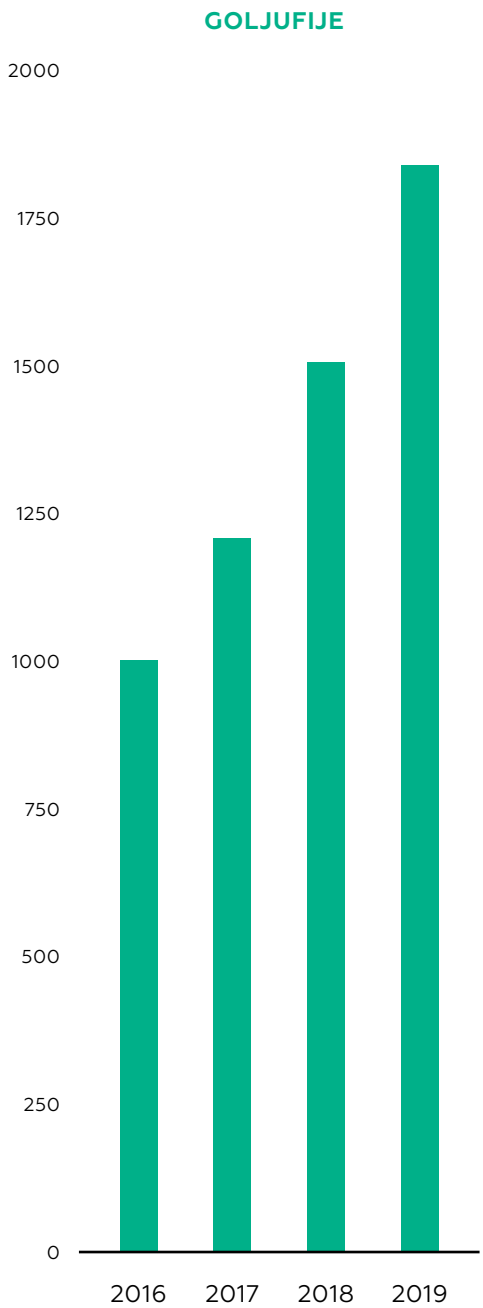


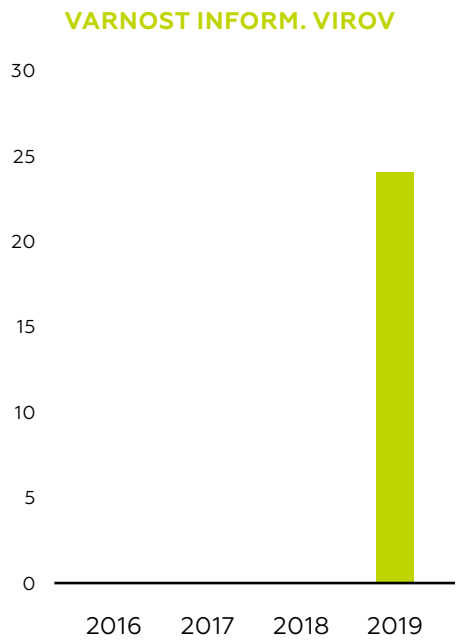
POSKUSI VDORA

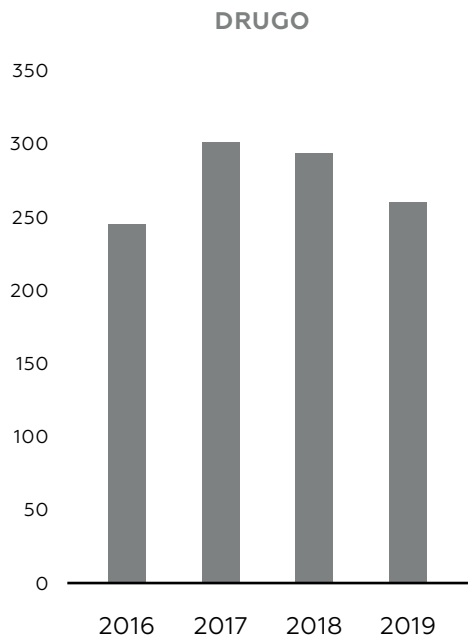


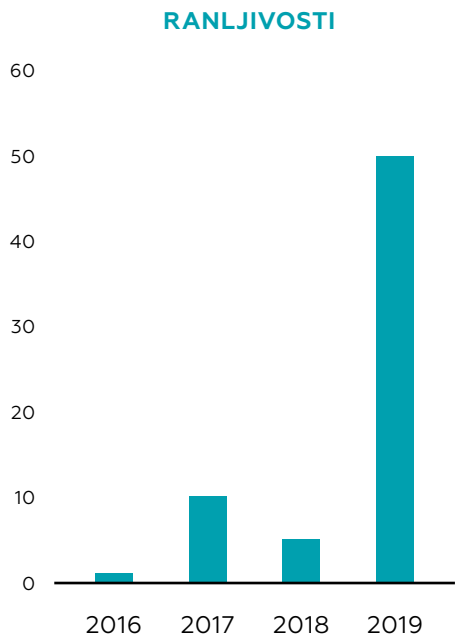
RAZPOLOŽLJIVOST

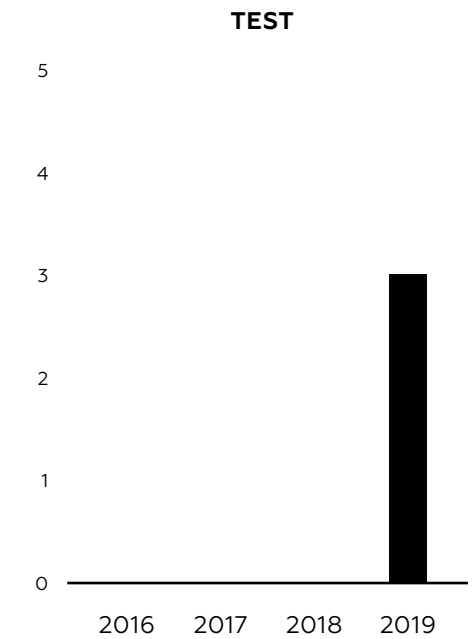



GOLJUFIJE
2000
1750
1500
1250
1000
750
500
250
0
2016
2017
2018
2019


VARNOST INFORM. VIROV
30
25
20
15
10
5
0
2016
2017
2018
2019


DRUGO
350
300
250
200
150
100
50
0
2016
2017
2018
2019


RANLJIVOSTI
60
50
40
30
20
10
0
2016
2017
2018
2019


TEST
5
4
3
2
1
0
2016
2017
2018
2019

VRSTE INCIDENTOV	2016	2017	2018	2019
NEPRIMERNA VSEBINA	**140**	**80**	**98**	**67**
Neželena sporočila	140	80	98	57
Žaljiva vsebina	0	0	0	9
Nasilna vsebina	0	0	0	1
ZLONAMERNA KODA	**514**	**378**	**270**	**304**
Virus	236	144	111	53
Črv	0	0	0	0
Trojanski konj	8	39	73	166
Vohunska programska oprema	0	0	0	3
Dialler	1	3	0	0
Rootkit	0	0	0	0
Boti in botneti	56	18	17	17
Nadzorni strežnik	0	0	0	6
Izsiljevalski virus	212	171	64	53
Orodje za oddaljen nadzor (RAT)	1	3	5	6

	2016	2017	2018	2019
ZBIRANJE INFORMACIJ	**110**	**127**	**75**	**40**
Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	86	126	75	33
Prestrezanje komunikacije	0	0	0	5
Družbeni inženiring	24	1	0	2
POSKUSI VDORA	**0**	**0**	**0**	**51**
Izkoriščanje znane ranljivosti	0	0	0	5
Poskusi prijav, bruteforce in napadi s slovarjem	0	0	0	46
Nova vrsta napada	0	0	0	0
VDORI	**138**	**138**	**117**	**45**
Zloraba privilegiranega uporabniškega računa	41	35	42	6
Zloraba neprivilegiranega uporabniškega računa	75	67	62	35
Napad na aplikacijo	22	36	13	4

	2016	2017	2018	2019
RAZPOLOŽLJIVOST	**75**	**26**	**22**	**40**
Napad onemogočanja	2	1	0	2
Porazdeljen napad onemogočanja	73	25	22	31
Sabotaža	0	0	0	4
Izpad delovanja naprav ali omrežja	0	0	0	3
GOLJUFIJE	**1001**	**1207**	**1505**	**1840**
Nepooblaščeno izkoriščanje virov	16	18	13	8
Intelektualna lastnina in avtorske pravice	8	5	8	13
Kraja identitete	103	106	62	96
Phishing sporočilo	157	171	175	301
Phishing spletno mesto	139	49	47	134
Spletno nakupovanje	302	408	339	164
Goljufija z vnaprejšnjim plačilom	87	157	161	149
Izsiljevanje	33	78	359	291
Druge goljufije	156	215	341	684

	2016	2017	2018	2019
VARNOST INFORM. VIROV	**0**	**0**	**0**	**24**
Nepooblaščen dostop do podatkov	0	0	0	15
Nepooblaščeno spreminjanje podatkov	0	0	0	5
Odtekanje informacij	0	0	0	4
RANLJIVOSTI	**1**	**10**	**5**	**50**
Odgovorno razkrivanje	1	10	5	25
Razkritje ranljivosti	0	0	0	1
Ranljivi sistemi in naprave	0	0	0	24
DRUGO	**245**	**301**	**293**	**260**
Drugo	231	291	246	243
Novinarsko vprašanje*	14	10	47	17
TEST	**0**	**0**	**0**	**3**
Namenjeno preizkusom	0	0	0	3

* Predstavljenih je veliko manj novinarskih vprašanj, saj jih beležimo prek različnih poti (dejansko je bilo pripravljenih 67 odgovorov medijem, kot je razvidno na naslednji strani poročila)

ZNANA OŠKODOVANJA 2019

65.000 € Povprečno oškodovanje z **vrivanjem v poslovno komunikacijo**

200.000 € **Največje posamično oškodovanje** z vrivanjem v poslovno komunikacijo

35.000 € Največje oškodovanje v **direktorski prevari**

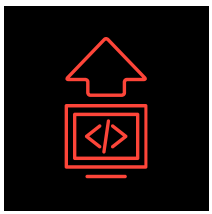
4.700 € Povprečno oškodovanje pri **prevari z vnaprejšnjim plačilom** (tudi »nigerijska prevara«)

520 € Povprečno oškodovanje pri **spletnem nakupovanju**

2.400.000 € Največja znana ocenjena škoda pri **napadu izsiljevalskega virusa**

60.000 € Največja znana škoda pri **kraji kriptovalut**

16.200 € Oškodovanje pri **nakupu stroja**



12 %

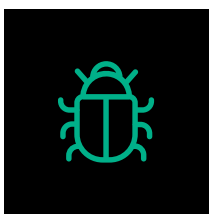
PORAST OBRAVNAVANIH INCIDENTOV

343

PREISKAV ŠKODLJIVE KODE

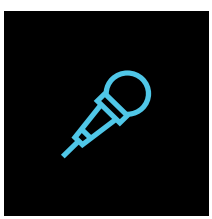
300

PRIJAVLJENIH PHISHING NAPADOV



53

NAPADOV Z IZSILJEVALSKIM VIRUSOM



67

NOVINARSKIH VPRAŠANJ

OBLAK OZNAK ZA INCIDENTE

Dogodki v letu 2019

1

JANUAR

Na SI-CERT-u uvedemo referenčno taksonomijo, ki jo predpiše agencija ENISA in stopnjevanje incidentov po vzoru NCSC-UK. Vladni odzivni center SIGOV-CERT uradno prične z delovanjem, kolegom bomo v tem letu pomagali pri vpeljavi v mednarodno skupnost CSIRT. Obravnavamo več kot 70 prijav lažnega izsiljevanja.

475

prejetih prijav incidentov

FEBRUAR

Partnerjem nekaterih slovenskih podjetij storilci pošiljajo lažna sporočila z namenom izvedbe preusmeritve nakazil denarja. Svetujemo sorodnikom žrtve ljubezenske prevare, ki je do zdaj goljufom nakazala že 62.000 EUR. Primerov je v zadnjih mesecih vedno več, zato organiziramo okroglo mizo.

482

prejetih prijav incidentov

2

3

MAREC

Obravnavamo kar osem primerov odgovornega razkrivanja ranljivosti, ki se nanašajo na možnost odtekanja občutljivih informacij.

465

prejetih prijav incidentov

4

APRIL

Kampanja slovenskega podjetja za zbiranje investicijskih sredstev v obliki kriptovalut je dovolj odmevna, da se nanjo usmerijo tudi storilci z vrsto phishing napadov. Z njimi želijo preusmeriti vložke v svoje denarnice.

409

prejetih prijav incidentov

554

prejetih prijav incidentov

MAJ

Kritična ranljivost storitve za oddaljeni dostop (Windows Remote Desktop) omogoča neprijavljenemu uporabniku zagon programske kode na daljavo brez uporabniškega posredovanja. V Sloveniji je okoli 3.500 izpostavljenih strežnikov, obvestimo njihove ponudnike.

5

6

JUNIJ

Okoli 60 poštnih strežnikov Exim v Sloveniji vsebuje kritično ranljivost, razpošljemo obvestila. Več denarno visokih goljufij na platformah za trgovanje z delnicami.

695

prejetih prijav incidentov

540

prejetih prijav incidentov

JULIJ

Zaznan je krajši DDoS napad na državni organ, delovanje ni ogroženo in operater vključi mehanizme za preusmerjanje in čiščenje zlonamernega prometa.

7

8

AVGUST

Lekarne Ljubljana so žrtev napada z izsiljevalskim virusom Ryuk, ki javnemu zavodu povzroči več kot 2 milijona evrov škode. Konec meseca zaposleni v številnih bankah v Sloveniji prejmejo sumljiva sporočila.

442

prejetih prijav incidentov

450

prejetih prijav incidentov

SEPTEMBER

Zaposleni v bankah so tarča napada s sporočili, ki vsebujejo zlonamerno kodo. Napad se vrsti v več valovih od konca avgusta do sredine oktobra. Na SI-CERT-u bankam nudimo pomoč z analizo uporabljene zlonamerne kode. Neznani storilec »trojanizira« Petrolovo mobilno aplikacijo in jo skuša razširiti uporabnikom s sporočili SMS.

446

prejetih prijav incidentov

NOVEMBER

Organiziramo tehnični kolokvij združenja FIRST za usposabljanje kolegov v Sloveniji in za nove skupine CSIRT območja Zahodnega Balkana. Trojanec Emotet se po novem širi sam: po okužbi ukrade elektronsko korespondenco in se razpošlje kot priponka pod krinko odgovora na predhodno sporočilo. Preiskovanje opravimo v sodelovanju s slovensko policijo.

9 10 11 12

OKTOBER

Skozi Evropski mesec kibernetske varnosti na programu ozaveščanja Varni na internetu želimo doseči čim več spletnih uporabnikov in jim predstaviti aktualna tveganja. Hkrati poudarjamo glavne korake spletne higiene, ki naj postanejo del naše vsakodnevne rutine.

459

prejetih prijav incidentov

DECEMBER

Leto zaključimo z največjim številom obdelanih incidentov do zdaj. Čaka nas veliko dela pri nadgradnji lastne infrastrukture in laboratorija za preiskavo zlonamerne kode.

437

prejetih prijav incidentov

Krepitev kapacitet

SI-CERT je v okviru instrumenta za povezovanje Evrope (Connecting Europe Facility – CEF) leta 2018 pridobil evropska sredstva, ki so namenjena krepitvi kapacitet nacionalnih odzivnih centrov.

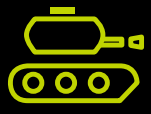
Sofinancirano s pomočjo Instrumenta za povezovanje Evrope Evropske unije

Projekt CEF 2017-SI-IA-0124 je v obdobju izvajanja projekta (oktober 2018 – avgust 2020) razdeljen na več dejavnosti, ki bodo omogočile implementacijo določil iz direktive NIS. Direktiva NIS od nacionalnih skupin CSIRT zahteva vzpostavitev delovnih prostorov za potrebe neprekinjenega delovanja na vsaj dveh varnih lokacijah. Posledično to prinese tudi nadgradnjo obstoječih zmogljivosti SI-CERT-a in vzpostavitev ustrezne strojne in programske opreme, ki bo omogočila delo tudi na zahtevani sekundarni lokaciji.

V sklopu projekta je v letu 2019 zagotovljena strojna oprema, ki bo v letu 2020 omogočila vzpostavitev zahtevane sekundarne lokacije. Leto 2019 sta zaznamovala tudi vzpostavitev in razvoj enotne platforme MeliCERTes, ki se kot gradnik Evropske strategije za kibernetsko varnost razvija pod vodstvom Mreže CSIRT in s pomočjo agencije ENISA. Platforma omogoča sodelovanje evropskih nacionalnih in državnih skupin CSIRT, skupno vodenje incidentov, samodejno izmenjavo opažanj škodljive kode, oblikovanje varnih zaprtih skupin za izmenjavo hipnih sporočil kot tudi platformo konferenčnih klicev. Platforma in sestavna orodja bodo prispevala k boljšemu sodelovanju skupin CSIRT ter omogočila hitrejšo izmenjavo informacij, kar bo posledično prineslo tudi boljšo odpornost na kibernetske grožnje.

Sredstva projekta CEF so zaposlenim na SI-CERT-u v letu 2019 omogočila tudi številna napredna usposabljanja iz področja reverznega inženiringa in analize škodljive kode, med katerimi še posebej izstopajo tečaji SANS. Sredstva projekta so bila namenjena tudi delu podpore dejavnostim Evropskega meseca kibernetske varnosti (European Cyber Security Month), ki jih koordinira SI-CERT.

Vaje kibernetske varnosti



NATO CYBER COALITION 19

SI-CERT že od leta 2013 sodeluje v vajah kibernetske varnosti, ki jih organizira zveza NATO, koordinator vaje v Sloveniji pa je Ministrstvo za obrambo. SI-CERT pomaga z izkušnjami in znanjem pri analizi škodljive kode in naprednejšem preiskovanju incidentov. SI-CERT je v vaji izvedel analizo slike kontrolnega sistema zaseženega brezpilotnega letalnika (dron) ter statično in dinamično analizo zlonamerne kode, ki je bila namenjena prestrezanju in spreminjanju komunikacije igralcev.

KIVA 2019

Uprava RS za jedrsko varnost je januarja 2019 organizirala prvo nacionalno vajo kibernetske varnosti v jedrskem sektorju v Sloveniji, KIVA 2019, na kateri so sodelovali državni organi, ki imajo določene pristojnosti v jedrskem sektorju, sodelavci Nuklearne elektrarne Krško, predstavniki izbranih zunanjih izvajalcev, Fakultete za varnostne vede ter SI-CERT-a.

EU CYBERSOPEX

Vajo CyberSOPEx, ki je potekala sredi maja 2019, je organizirala Agencija Evropske unije za kibernetsko varnost ENISA. V skladu s cilji direktive NIS je bil namen vaje izboljšanje koordinacije in sodelovanja med članicami EU pri obravnavi obsežnejših omrežnih incidentov.

CAA / EUROCONTROL

Septembra 2019 je potekala tridnevna delavnica kibernetske varnosti, namenjena kontrolorjem zračnega prometa in deležnikom, vpletenim v letalsko varnost. Na delavnici so tako sodelovali predstavniki Kontrole zračnega prometa, Agencije RS za okolje, letalski inšpektorji, predstavniki Agencije za civilno letalstvo, letališča Fraport Ljubljana, letalske družbe Adria Airways, vladne skupine CSIRT, Uprave RS za informacijsko varnost in predstavniki SI-CERT-a. Delavnica je bila organizirana s pomočjo evropske kontrole zračnega prometa Eurocontrol, bolj natančno njihovega centra EATM-CERT, ki je tudi ponudil svoje predavatelje za izvedbo dogodka. Na delavnici so bile tako izpostavljene tematike rešitev uporabe javnih ključev za potrebe infrastrukture, samo delo centra EATM-CERT ter postavitev in delo centra SOC oz. operativnega centra za kibernetsko varnost. SI-CERT je na delavnici predstavil svoje delovanje in vlogo v slovenskem prostoru ter večletno sodelovanje s centrom EATM-CERT s poudarkom na samodejni izmenjavi značilnosti zaznane škodljive kode. Delavnica je prinesla veliko novega za vse udeležence in je pozitivno prispevala k boljšemu zavedanju pomena kibernetske varnosti v sektorju civilnega letalstva.

Tehnični kolokvij

FIRST Ljubljana 2019 – Sodelovanje centrov za kibernetsko varnost v regiji Zahodnega Balkana

FIRST je svetovno združenje več kot 500 odzivnih centrov za kibernetsko varnost, proizvajalcev varnostnih rešitev in vseh pomembnih članov industrije IKT, ki kibernetsko varnost jemljejo za pomemben gradnik v svoji dejavnosti. SI-CERT je član združenja od leta 2001.

SI-CERT je v okviru svetovnega združenja odzivnih in varnostnih centrov FIRST ter v sodelovanju z Ženevskim centrom za demokratični nadzor nad oboroženimi silami (DCAF) organiziral mednarodni tehnični kolokvij o kibernetski varnosti. Kolokvij je potekal v Ljubljani, 13. in 14. novembra 2019, in je združil več kot 70 udeležencev iz Evrope. Tehnični kolokviji so namenjeni članom združenja FIRST, SI-CERT pa je v dogovoru z vodstvom FIRST-a udeležbo omogočil tudi gostom iz regije, ki niso člani in še izpopolnjujejo svoje odzivne kapacitete na področju kibernetske varnosti, ter slovenskim državnim organom, ki imajo pomembno operativno vlogo pri odzivanju na področju kibernetske varnosti.

Prvi dan srečanja v Ljubljani je bil namenjen predstavitvi različnih orodij in tehnik za krepitev novoustanovljenih centrov za kibernetsko varnost na Zahodnem Balkanu. Med predavatelji so bili strokovnjaki evropskih odzivnih centrov in predstavniki Agencije Evropske unije za kibernetsko varnost ENISA. Na koncu dneva je potekal posvet o pobudah za krepitev kibernetskih zmogljivosti v regiji. SI-CERT je že več let aktiven na področju podpore pri ustanavljanju odzivnih centrov in izboljšanju njihovega povezovanja v regiji.

Drugi dan je ponudil dve vzporedni celodnevni tehnični usposabljanji: usposabljanje na platformi MISP (Malware Information Sharing Platform), ki ga je izvedel Center za obravnavo incidentov v Luksemburgu CIRCL, in usposabljanje za digitalno forenziko, ki ga je opravil najstarejši CERT na svetu, ameriški CERT/CC (sedaj CERT Division na inštitutu Software Engineering Institute, Carnegie Mellon University, CMU SEI).

SI-CERT je ob podpori vlade ZDA in skupaj z inštitutom CMU SEI po zaključku kolokvija tretji dan organiziral srečanje za posebej povabljeno skupino odzivnih centrov regij Zahodnega Balkana in Kavkaza, sestavljeno iz predavanj in praktičnega usposabljanja.

FIRST TC je prvi tovrstni strokovni kolokvij, ki ga je gostila Slovenija, in predstavlja pomemben vzvod za krepitev ter poglabljanje odnosov v regiji. Z njim SI-CERT in posledično tudi država Slovenija krepita svojo strokovno veljavo v regiji in širše v Evropi.

Obravnavani incidenti

Škodljiva in zlonamerna koda

Škodljiva ali zlonamerna koda je ustvarjena za povzročanje škode na sistemu, omrežju in/ali neposredno uporabniku. Pod ta pojem uvrščamo trojanske konje, viruse, črve, vohunske programe, orodja za oddaljeni nadzor in podobno. Najpogosteje smo izpostavljeni škodljivi kodi, katere namen je kraja občutljivih podatkov (uporabniška imena in gesla, zasebni ključi digitalnih potrdil, podatki kreditnih kartic), prevzem nadzora nad okuženim sistemom za izvajanje drugih zlonamernih dejavnosti (nepooblaščen dostop do e-bančnega računa, razpošiljanje neželenih sporočil, izvajanje DDoS napadov, iskanje ranljivosti na drugih sistemih ...) in šifriranje podatkov (izsiljevalski virusi).

ANALIZA ŠKODLJIVE KODE

Da bi v čim večji meri lahko zamejili širjenje in število okužb, SI-CERT opravlja statično in dinamično analizo škodljive kode v lastnem laboratoriju. Koda je pridobljena v priglašenih incidentih ali pa v drugače opaženih ali posredovanih vzorcih. Pri tem se ugotovita namen in delovanje kode, zraven pa lahko izluščimo kazalnike zlorabe (*angl. IoC, Indicator of Compromise*), ki podajajo lastnosti zlorabe in jih lahko uporabimo za ugotavljanje okuženosti računalniških sistemov. Kazalnike lahko nato delimo z različnimi skupnostmi v državi, skupnostmi CSIRT v EU in širše po svetu. To običajno izvedemo prek sistema MISP (*angl. Malware Information Sharing Platform*).

Opise nekaterih analiz si lahko ogledate v Tehničnih zapisih centra SI-CERT:

SI-CERT TZ002 / Zlonamerna koda na osnovi skriptnega jezika AutoIt
>> www.cert.si/tz002/

SI-CERT TZ003 / Analiza VB5 packed zlonamerne kode
>> www.cert.si/tz003/

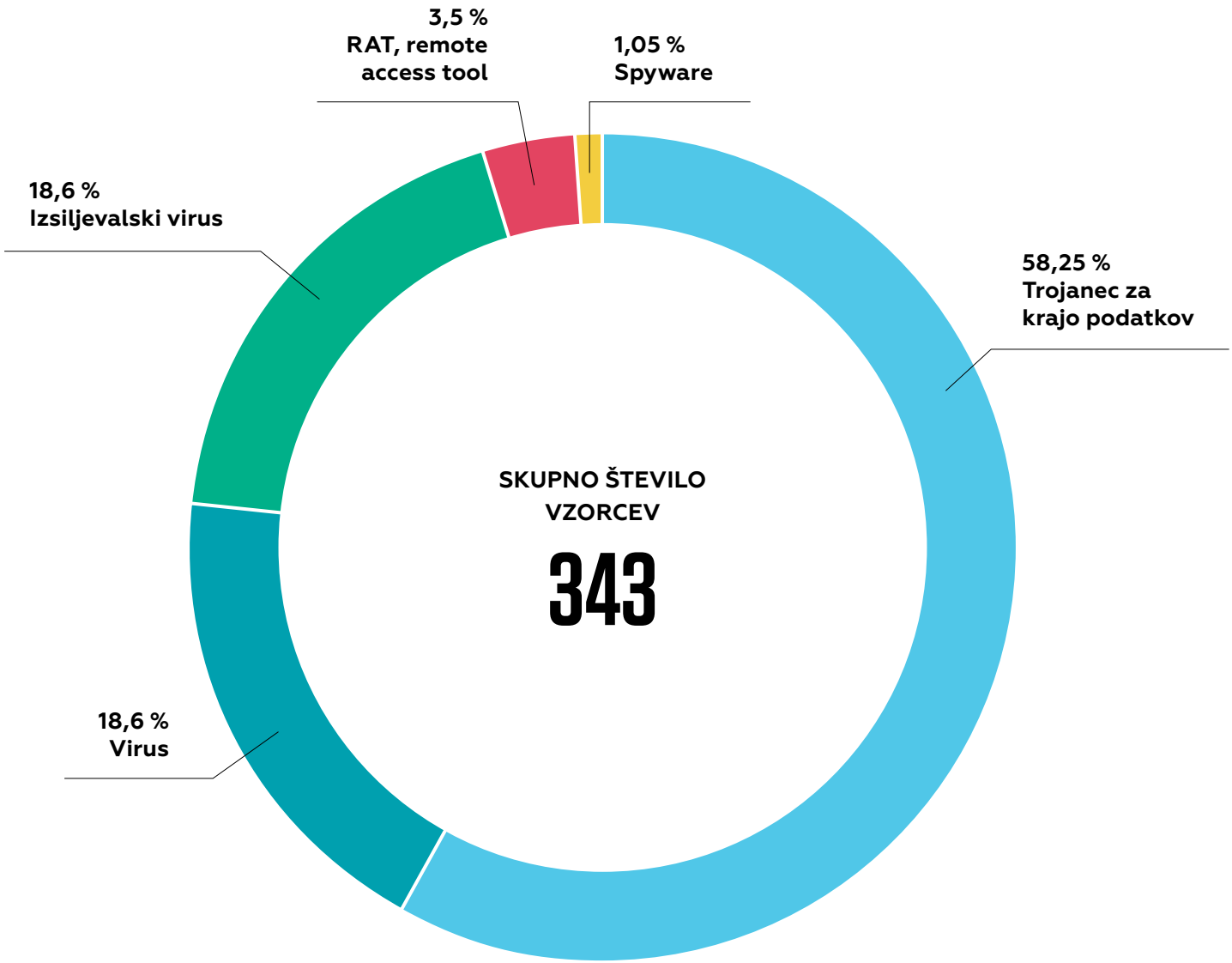
SI-CERT TZ004 / Analiza trojanca za Android mobilne naprave
>> www.cert.si/tz004/

SI-CERT TZ005 / Analiza trojanca za prikriti oddaljeni dostop (RAT)
>> www.cert.si/tz005/

VSTOPNI VEKTOR

Elektronska sporočila še vedno predstavljajo najpogostejšega nosilca računalniških okužb. Sporočila z zanimivo zgodbo, ki naj bi prejemnika prepričala v klik na povezavo, prek katere se prenese zlonamerna koda, strašenje s potvorjenim računom v priponki, obvestila o izvršbah z dokumentom, ki vsebuje zlonamerno kodo: to so priljubljeni pristopi napadalcev. V priponkah najdemo arhivske datoteke (.rar, .zip, .ace, .tar.gz ...) z izvršljivo kodo, datoteke MS Office (.docx, .xlsx) z zlonamerno kodo v obliki makrov. Široko »sejanje« sporočil je preprosto in poceni, napadalcem pa je dovolj že manjši odstotek žrtev, ki kliknejo in okužijo svoj računalnik.

ANALIZE KODE V LETU 2019

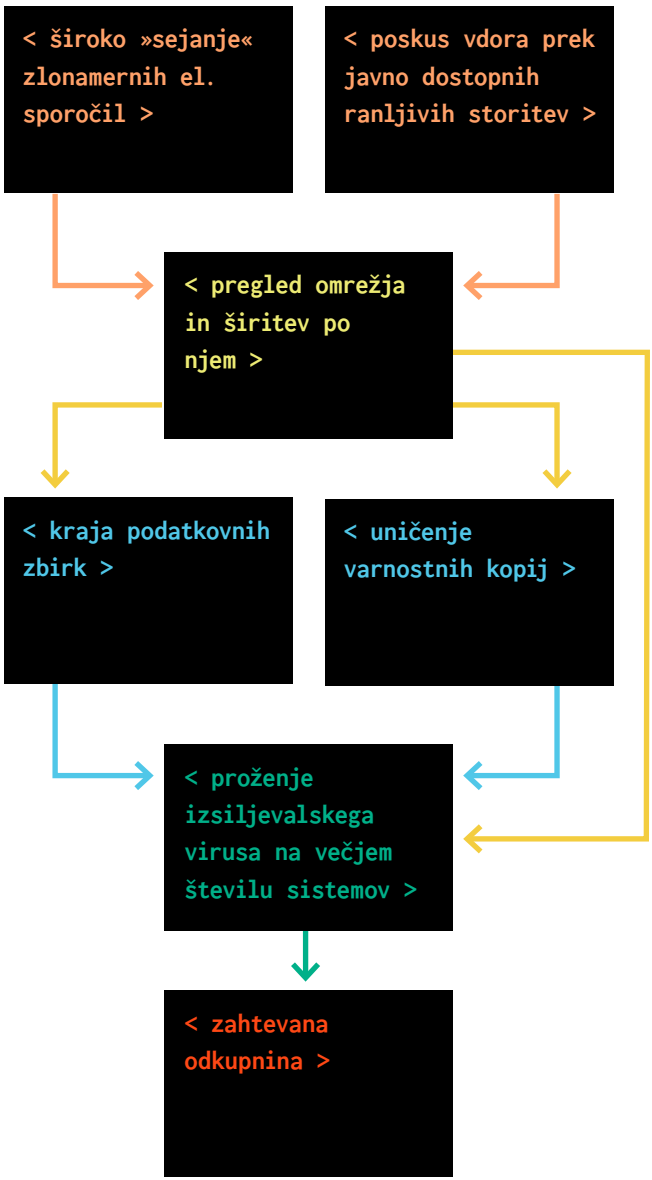


Izsiljevalski virusi

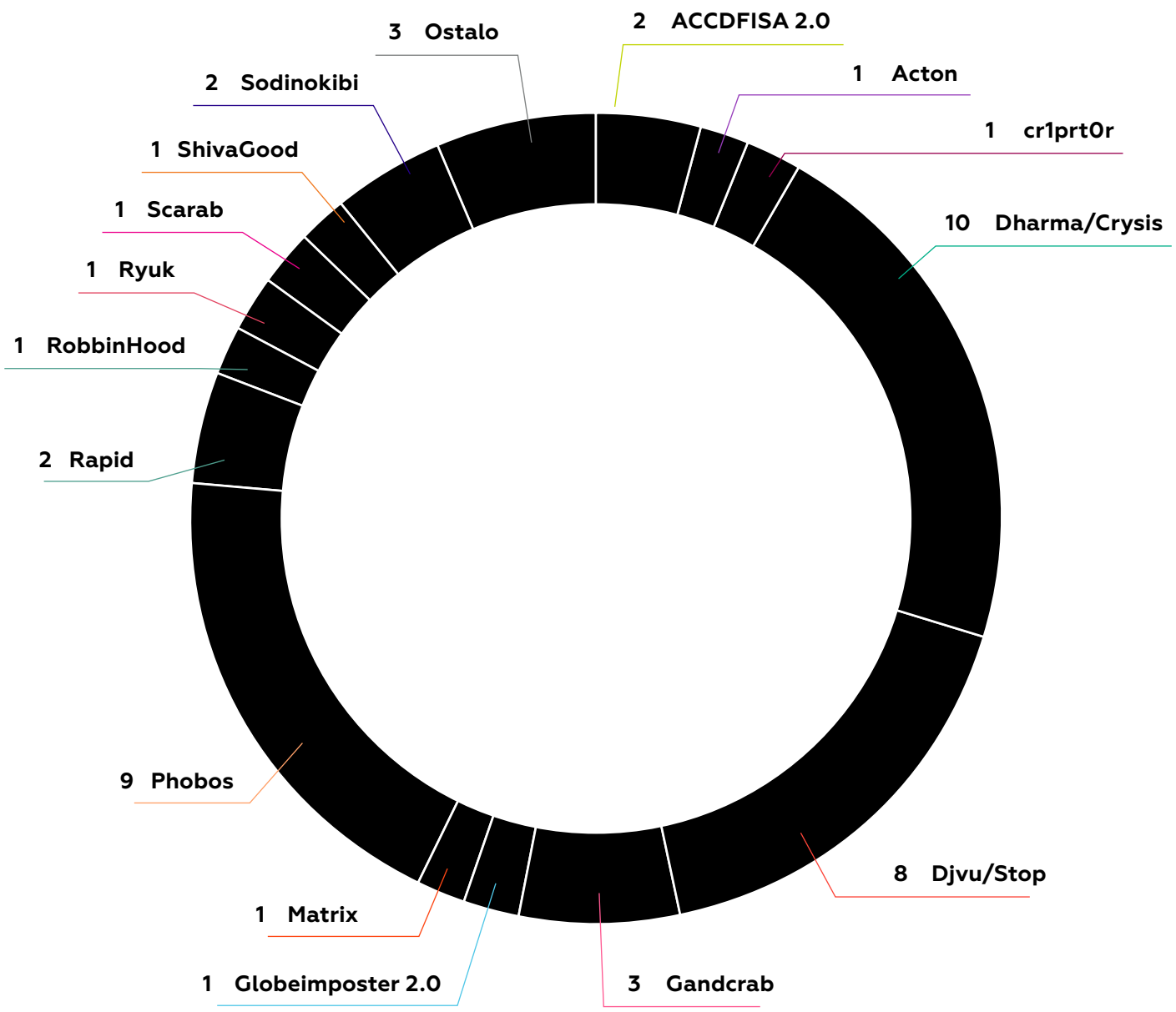
SI-CERT od aprila 2012 redno obravnava prijave okužb z izsiljevalskimi virusi. Pred letom 2018 so bile žrtve vdorov izbrane naključno, kot del širše kampanje širjenja virusov, v zadnjih letih pa so primarna tarča podjetja in javne ustanove. V večini obravnavanih primerov sta bila vektorja okužbe zlonamerna elektronska pošta, ki je vsebovala zlonamerno priponko oz. povezavo do nje, ali pa vdor prek neustrezno zaščitene storitve za oddaljen dostop (Remote Desktop). Storilci pa lahko izkoriščajo tudi nove ranljivosti, ki omogočajo nepooblaščen vstop v omrežje. Potek napada so izpopolnili tudi s krajo podatkovnih zbirk in uničenjem varnostnih kopij, kadar je to mogoče.

ŠTEVILO POTRJENIH OKUŽB Z IZSILJEVALSKIMI VIRUSI NA LETO

POTEK NAPADA Z IZSILJEVALSKIM VIRUSOM

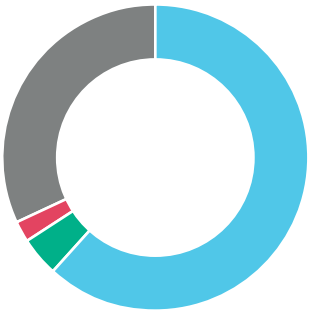


VRSTA VIRUSA



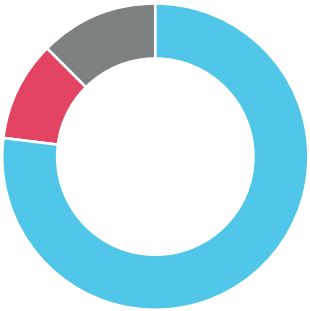
VEKTOR NAPADA

Remote Desktop Protocol	29
Nelegalna programska oprema	2
Elektronska pošta	1
Ni znano	15



VRSTA ŽRTEV

Poslovni	37
Domači	5
Ni znano	6



Več o izsiljevalskih virusih najdete v poročilih centra SI-CERT za leta 2016, 2017 in 2018.

>> www.cert.si/o-nas/letna-porocila-o-omrezni-varnosti/

NAPAD NA JAVNI ZAVOD LEKARNA LJUBLJANA

Delovne postaje na informacijskem sistemu Javnega zavoda Lekarna Ljubljana so 6. avgusta 2019 utrpele okužbo z izsiljevalskim virusom Ryuk. O incidentu so Lekarne neposredno obvestile SI-CERT, v komunikacijo pa so vključili zunanjega izvajalca. V preiskavo sta bila v okviru svojih pristojnosti vključena tudi Urad informacijskega pooblaščenca in Center za računalniško preiskovanje Generalne policijske uprave. Analiza je pokazala prvotno okužbo s trojancem TrickBot nekaj dni prej, v naslednji fazi pa so storilci uporabili Empire Post-Exploatation Framework za širjenje po omrežju organizacije in nameščanje izsiljevalskega virusa. Lekarnam je uspelo sisteme povrniti v prvotno stanje iz varnostnih kopij, vendar je zaradi okužbe prišlo do večdnevnega izpada delovanja sistema, škoda pa je po javnih navedbah vodstva znašala 2,4 milijona evrov. SI-CERT je izsledke analize posredoval kontaktnim osebam v Lekarni Ljubljana ter drugim navedenim pristojnim institucijam.

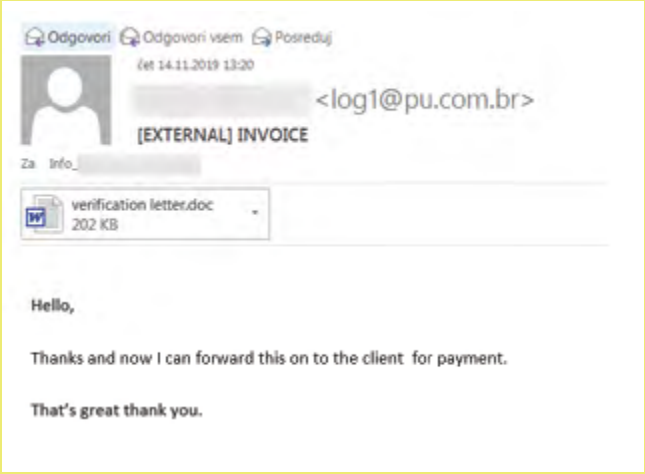
TROJANEC EMOTET SE ŠIRI SAM

Emotet je trojanski konj, ki je v široki uporabi že od leta 2014 in se pogosto uporablja v začetni fazi vdora. Novembra 2019 smo na SI-CERT-u obravnavali novo različico, ki se je razpošiljala s pripetim zlonamernim dokumentom MS Office Word kot odgovor na dejansko obstoječo preteklo korespondenco. Analiza je pokazala, da ne gre za vdore v različne poštne predale, ampak nov način širjenja trojanca z ukradeno poštno korespondenco okuženega.

Trojanec je poiskal poštne mape poštnega programa MS Outlook s ključem v registru HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Search\Catalog ter vso korespondenco ukradel in jo poslal nadzornemu strežniku. Nato je bila uporabljena obstoječa korespondenca za sestavljanje lažnega sporočila, ki naj bi prejemnike zavedlo v odpiranje priponke. Analizirali smo več kot 40 vzorcev, večina naslovnikov so bili zaposleni v zdravstvenem sektorju v Sloveniji. Tudi en od nadzornih strežnikov je bil v Sloveniji, v preiskavo pa je bila vključena slovenska kriminalistična policija.

Storilci seveda uporabljajo omrežje zlorabljenih strežnikov za namene širjenja zlonamerne kode in nadzorovanje okuženih računalnikov.

Na naši spletni strani smo izdali varnostno obvestilo o širjenju trojanskega konja Emotet prek sporočil s preteklo korespondenco (https://www.cert.si/okuzena-sporocila-s-preteklo-korespondenco/), o nadzornih strežnikih pa smo obveščali tuje partnerje.



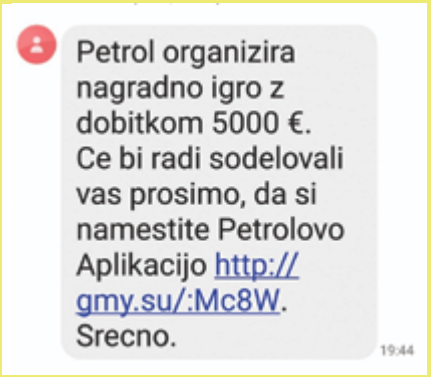
Vsebina sporočila je bila v angleškem jeziku, ta pa prejemnika poziva k pregledu pripetega dokumenta

ZLORABA PETROLOVE MOBILNE APLIKACIJE

Sporočilo SMS je z vabilom v nagradno igro podjetja Petrol z visokim dobitkom prejemnika skušalo prepričati, da klikne na povezavo v sporočilu. Številka pošiljatelja je bila slovenska, a te ni težko potvoriti. Povezava v sporočilu je bila zakrita z uporabo skrajševalnika, vodila pa je do storitve Portmap.io, ki je namenjena posredovanju prometa iz javnega interneta s preslikavami NAT na določeno lokalno omrežje. V tem primeru je storilec to uporabil še za eno raven prikritja svoje lokacije.

Na preusmerjenem naslovu URL je bila spremenjena (trojanizirana) starejša verzija aplikacije Moj Petrol za mobilno platformo Android (APK). V primeru namestitve aplikacije se telefon začne povezovati z nadzornim strežnikom pri ponudniku Amazon AWS prek vrat TCP 11390, napadalec pa ima možnost dostopati do naprave z Metasploit Meterpreterjem.

Metasploit je odprtokodna modularna platforma za izvedbo varnostnih pregledov, ki vsebuje nabor orodij za izkoriščanje ranljivosti za



Lažno Petrolovo sporočilo SMS

številne storitve, aplikacije, operacijske sisteme in platforme, kot tako pa se (in tudi se) lahko uporabi v nelegitimne namene. Meterpreter je tovor (payload) ogrodja Metasploit, ki omogoča interaktivni nadzor zlorabljenega ciljnega sistema.

To se odraža tudi v nekaterih dodatnih pravicah, ki jih zahteva trojanizirani APK.

Aplikacija želi dostop do pravic RECEIVE_SMS, SEND_SMS, READ_CALL_LOG, READ_CONTACTS, WRITE_CALL_LOG, WRITE_CONTACTS, RECORD_AUDIO, READ_SMS, ACCESS_FINE_LOCATION, CAMERA, kar dokaj nazorno kaže na razpon funkcionalnosti, ki jih ima na voljo storilec prek nameščene datoteke APK na napravi žrtve. Preiskavo smo nadaljevali v sodelovanju s policijo, o nadzornem strežniku pa obvestili podjetje Amazon.

ZLONAMERNA KODA CILJA NA ZAPOSLENE V BANKAH

Zaposleni v slovenskih bankah so bili konec poletja in jeseni 2019 tarča ciljanih napadov z zlonamerno kodo. Konec avgusta so bila v prvem valu poslana sporočila, ki so v objektu toka OLE v priponki .doc vsebovale kodo JavaScript ali ki so imele v priponki sporočila .iso izvršljivo datoteko .js.

Primer elektronskega sporočila

Zlonamerna koda JavaScript

Koda po zagonu pošlje osnovne podatke sistema (ime računalnika, domena, seznam procesov, operacijski sistem, uporabniško ime, podatki o disku) nadzornemu strežniku, v odgovoru pa pričakuje seznam naslovov URL, od koder lahko prenese naslednjo fazo okužbe.

DRUGI in TRETJI VAL

Deset dni po prvem valu se je napad ponovil, vendar so tokrat sporočila vsebovala preglednico .xls MS Office z vgrajenim objektom OLE v obliki datoteke PNG, ta pa je vsebovala komponento PE (Portable Executable) tako za arhitekturo x86 kot tudi za arhitekturo x64. Vsebovala je tudi skripto VBS, ki je na podlagi ugotovljene arhitekture sistema (32-bitnega oz. 64-bitnega OS) iz slike PNG izrezala in zagnala ustrezno binarno datoteko.

```
Private Sub CreateGifFile()
TempName = Environ("TEMP") & "\13.xlsx"
ZipName = TempName + ".zip"
ZipFolder = Environ("TEMP") '& "\UnzTmp"
Dim nm As String
Dim size As Long
Dim num As Integer
#If Win64 Then
nm = Environ("APPDATA") + "\carpc2.dll"
size = 64512
num = 2
#Else
nm = Environ("APPDATA") + "\carpc1.dll"
size = 81920
num = 1
#End If
```

Izsek skripte VBS, ki na osnovi arhitekture operacijskega sistema iz objekta OLE »izreže« ustrezno binarno datoteko

Že dan po drugem valu je bil sprožen tretji napad. Tokrat napadalci metode niso spreminjali. Ponovno so uporabili tehnike, ki smo jih spremljali že v drugem valu. Sprememba je bila le v naslovu nadzornega strežnika. Podobno kot v prvem valu zagnana zlonamerna koda povpraša za dodatne lokacije (naslove URL), od koder prenese vsebino, jo odloži v sistem in zažene. Dostop do dodatne zlonamerne kode na strežnikih tudi v tem primeru ni uspel, smo pa v simuliranem okolju to obnašanje lahko potrdili.

ČETRTI VAL

Natanko mesec dni po tretjem valu se je, sicer v manjšem obsegu, pojavil še četrti val sporočil. Tokrat so sporočila vsebovala povezavo, prek katere se izvede prenos datoteke .xls, katere funkcionalnost je identična obravnavanim v drugem in tretjem valu.

```
Public Sub ReplaceCurrentModule()
NameFav = UserForm3.TextBox1.Tag + "\favorite" + ".xlsx"
ZipName = NameFav + ".zip"
ZipFolder = UserForm3.TextBox1.Tag
Dim nm As String
Dim API_LENGTH As Long
Dim d_6 As Integer
nm = UserForm3.TextBox2.Tag + "\libGTPK1"
API_LENGTH = 282624
d_6 = 1

#If Win64 Then
nm = UserForm3.TextBox2.Tag + "\libGTPK2"
API_LENGTH = 201216
d_6 = 2
#End If
nm = nm + ".d" + "ll"
KillArray ZipFolder & "\oleObj" + "ect*.bin", ZipName, nm
```

V vseh obravnavanih napadih je SI-CERT tesno sodeloval s slovenskimi bankami in Združenjem bank Slovenije. Posredovali smo izsledke analiz in kazalnike okužb (*angl. IoC, Indicators of Compromise*). Nobena od slovenskih bank ni zabeležila uspešne okužbe, varnostni mehanizmi, postopki obveščanja in hitre izvedbe zaščitnih ukrepov na njihovih omrežjih so jih uspešno preprečili.

Taktika storilcev se je sicer čez čas spreminjala, vendar pa je osnovna funkcionalnost škodljive programske kode ostala enaka. Vzorci vseh valov napadov kažejo na istega akterja. Vzorce povezuje funkcionalnost sporočanja podatkov o sistemu ter čakanje na seznam datotek za izvršitev in podobnost imena domen nadzornih strežnikov, ti pa so bili pri ponudnikih v Latviji, na Nizozemskem in Finskem. Prijave o nadzornih strežnikih smo podali pristojnim nacionalnim skupinam CSIRT, podali pa smo tudi prijavo suma kaznivega dejanja na Upravo kriminalistične policije in jih zaprosili za sodelovanje ter za ukrepanje prek mehanizmov EUROPOL.

Na spletu se je pojavil zapis z omembo vzorcev, ki je kazal na možnost, da gre za širši napad na banke v regiji Zahodnega Balkana. Skupine CSIRT v regiji smo zato obvestili o naših izsledkih in prosili za informacijo o zaznavi podobnih napadov, ki je bila tudi potrjena.

Phishing

Phishing ali ribarjenje za gesli je vrsta napada z lažnim predstavljanjem, najpogosteje v elektronskih sporočilih, ki skušajo prejemnika prepričati v razkritje občutljivih podatkov. Napadalci si za žrtve izbirajo naključne ali skrbno načrtovane uporabnike, odvisno od samega namena napada. Pri široko zastavljeni kampanji bodo napadalci ciljali na gesla za dostop do elektronske pošte, s katerimi lahko nato prevzamejo tudi druge spletne storitve, vezane na elektronski naslov uporabnika. V bolj ciljanih napadih pa je phishing prva faza, v kateri s krajo gesla zaposlenega v podjetju ali državnem organu napadalci pridobijo začetni dostop do omrežne infrastrukture in storitev ustanove.

94 %

PORAST PHISHING PRIJAV GLEDE NA LETO 2018

301

OBRAVNAVANIH PRIJAV PHISHING SPOROČIL

134

UKREPOV ZOPER VDORE
v spletna mesta za namestitev phishing strani

KRAJA GESEL ELEKTRONSKE POŠTE

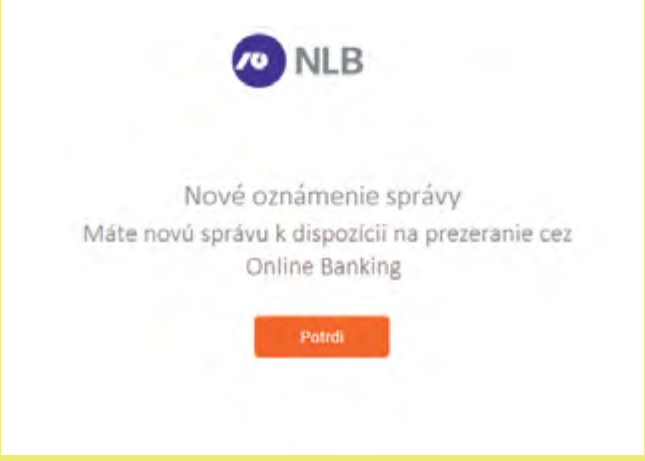
Računi za elektronsko pošto se nam morda vedno ne zdijo toliko pomembni kot izvajalcem phishing napadov. Ker imamo na elektronski naslov vezane druge storitve, lahko tako napadalci poskusijo prevzeti tudi dostop do teh. V letu 2019 smo obravnavali primer, ko so storilci vdrli v oglaševalski račun Facebook slovenskega podjetja in ga z objavo svojih lastnih oglasov finančno oškodovali.

»WHACK-A-MOLE«

SI-CERT zelo hitro prejme obvestilo o phishingu. V kratkem času, včasih lahko samo nekaj minut, razpošljemo naslove lažnih spletnih strani na črne liste brskalnikov, za spletno mesto pa že v nekaj urah dosežemo umik, običajno po obveščanju tuje skupine CSIRT ali neposredno ponudnika gostiteljstva.

NAPADI NA KOMITENTE BANK

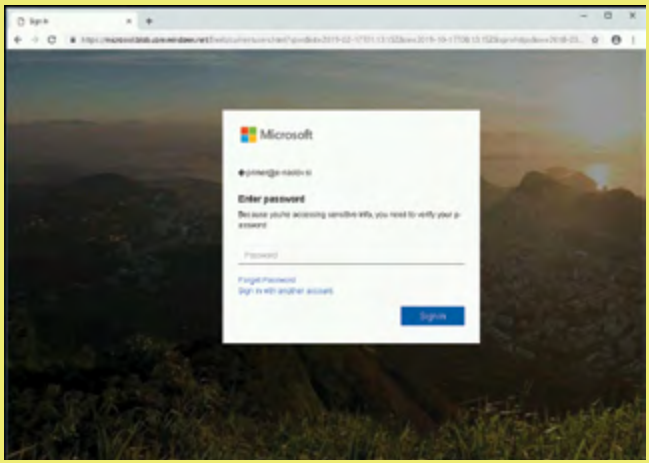
V letu 2019 smo zabeležili 22 različnih phishing napadov na komitente slovenskih bank. Občasno imajo storilci še vedno težave z izbiro ciljnega jezika za strojni prevod sporočila, kar bistveno zmanjša uspešnost njihove kampanje – že kar pregovorno nas zamenjujejo s Slovaki, kar se celo izkaže za koristno. SI-CERT pri obravnavi phishing napadov tesno in uspešno sodeluje z bankami in Združenjem bank Slovenije.



Phishing sporočilo slovenskim uporabnikom v slovaškem jeziku

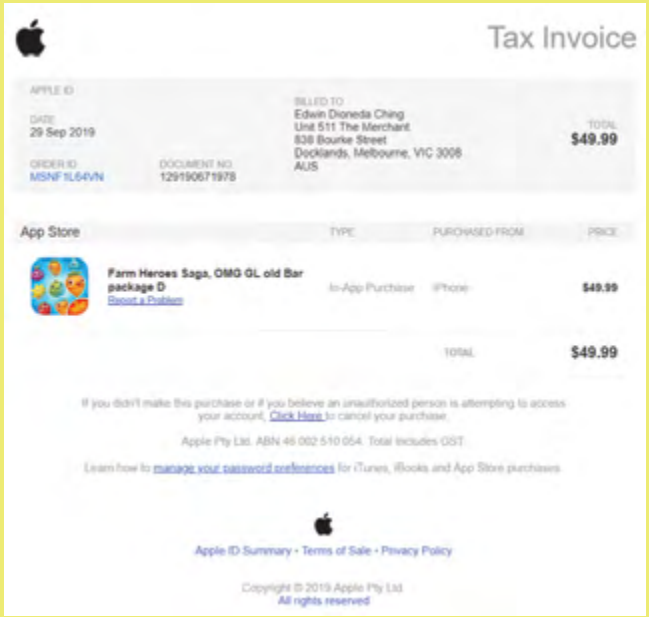
IZKORIŠČANJE OBLAČNIH STORITEV

Microsoftova oblačna platforma Azure dodeljuje uporabnikom imena v domeni .blob.core.windows.net. Napadalci tako na preprost način žrtev zavedejo na sklep, da gre za uradno Microsoftovo storitev in so s tem bolj dovzetni za vpis uporabniškega imena in gesla.



KUPILI STE APLIKACIJO! NISTE? KLIKNITE TU.

V phishing napadu na uporabnike trgovine Apple AppStore je elektronsko sporočilo navajalo nakup aplikacije v vrednosti 50 dolarjev. Priložen je bil dokument PDF, ki je bil oblikovno identičen računu, ki ga prejmete s strani podjetja Apple ob dejanskem nakupu. V njem pa je bilo še navedeno, da lahko nakup prekličete s klikom na povezavo. Ta pa seveda vodi na phishing stran, kjer storilci pridobijo uporabnikov AppleID in nato dostop do povezanih storitev.



Napadi na podjetja

VDOR V POSLOVNO KOMUNIKACIJO

Vrsta napada (*angl. BEC, Business Email Compromise*), 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 fakturo za plačilo storitev ali materiala, e-pošto z računom zadržijo, na fakturi spremenijo podatke o bančnem računu in spremenjeno fakturo 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.

NEPLAČANE FAKTURE

Slovensko podjetje je imelo na spletni strani naveden seznam poslovnih partnerjev v tujini in njihove kontaktne podatke. Napadalci so podatke izkoristili za pošiljanje lažnih sporočil poslovnim partnerjem, z najverjetnejšim namenom preusmeritve neplačanih faktur.

Leto	Skupno oškodovanje*	št. primerov
2016	134.000 €	7
2017	68.000 €	5
2018	530.000 €	15
2019	432.000 €	22

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

DIREKTORSKA PREVARA

Direktorska prevara (*angl. CEO fraud*) je primer družbenega inženiringa, ki cilja primarno na računovodje. Spletni goljufi poiščejo vse potrebne informacije na spletni strani podjetja, nato ponaredijo elektronsko sporočilo, v katerem se lažno predstavijo kot direktor podjetja. Potem računovodji pošljejo elektronsko sporočilo, v katerem prosijo za prenakazilo večje vsote denarja na račun v tujini. To so bančni računi denarnih mul, ki sredstva takoj po prejemu pošljejo po drugi poti, sledenje denarju pa je s tem vedno težje. SI-CERT ima z vsemi bankami, članicami Združenja bank Slovenije, vzpostavljen namenski kanal za izmenjavo podatkov o računih denarnih mul. Preiskave primerov pogosto pokažejo, da napadi izvirajo predvsem iz Nigerije. Napadu so najbolj izpostavljena majhna podjetja, ki nimajo vpeljanih postopkov preverjanja pri spremembah računov. Varne pa so vse ustanove, ki morajo delovati po Zakonu o javnem naročanju, saj zgolj na poziv direktorja računovodstvo ne sme kar nakazati denarja v neznano.

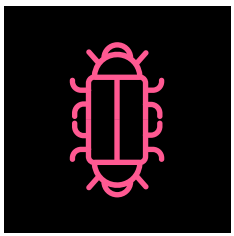
Kriptovalute – stalnica in ne novost

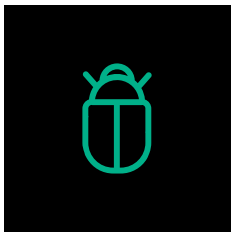
Burno dogajanje v prejšnjih letih na področju kriptovalut in zaledne tehnologije veriženja blokov se je v letu 2019 precej stabiliziralo. Tudi napadalci so kriptovalute »vzeli za svoje« in ostajajo največkrat uporabljeno plačilno sredstvo napadalcev v primerih izsiljevanj, pri čemer je v praktično vseh obravnavanih primerih uporabljena najstarejša in najbolj popularna kriptovaluta Bitcoin, čeprav ta napadalcem ne omogoča absolutne anonimnosti. Lastništvo večine kriptodenarnic res ni znano, so pa vse transakcije javne. Možnost identifikacije storilcev se običajno pokaže, ko ti želijo kriptovaluto na borzi zamenjati v običajen denar (FIAT).
Tudi število obravnavanih primerov napadov na tehnologijo, ki jo lahko povezujemo s kriptovalutami, se je v letu 2019 močno zmanjšalo. Obravnavali smo zgolj nekaj primerov phishing napadov na spletne platforme ter en primer vstavljene kode CoinHive na spletnem strežniku. Ta metoda monetizacije, ki je postala popularna v letu 2018 in temelji na izkoriščanju procesorskega časa računalnika obiskovalca, se je očitno izkazala za neuporabno.

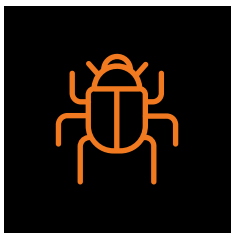
NAPADENE KRIPTODENARNICE

V DDoS napadu na strežnike tujega podjetja, ki izdeluje aplikacijo za kriptodenarnico, je sodelovalo nekaj 10.000 sistemov iz celotnega sveta, med njimi tudi sistem iz Slovenije. Prek skrbnika omrežja in z dovoljenjem lastnika računalnika smo na njem identificirali zlonamerni program, ki je sodeloval v napadu. Napadeno podjetje smo seznanili z našo analizo in informacijami o možnosti blokade virusa.

Nekaj neobičajnih







Včasih se na SI-CERT-u ukvarjamo tudi s primeri, ki ne spadajo v običajne kategorije, znajo pa biti precej zanimivi. Na neki osnovni šoli so učitelji na primer ugotovili, da so v e-redovalnici pri nekaterih učencih vpisane drugačne ocene, kot so jih prejeli, neka druga šola pa je bila tarča popolnoma unikatnega DDoS napada s poplavo podatkov. Je bil krivec morda eden od tehnično bolj nadarjenih dijakov? Obravnavali smo tudi nekaj lažno pozitivnih primerov, ko je tuji CERT slovensko spletno stran neke banke označil kot phishing, na črnih listah brskalnikov pa se je po pomoti znašla tudi spletna stran za prenos programske opreme za zaščito poštnih strežnikov. Slovenskemu podjetju smo pomagali pri odstranitvi odkrivanja njihove programske opreme s strani enega od antivirusov.

V navalu prijav lažnih izsiljevalskih sporočil po elektronski pošti na začetku leta smo dobili tudi nekaj prijav s strani organizacij, pri katerih so napadalci izsiljevalsko sporočilo natisnili neposredno s tiskalniki, saj ti niso bili ustrezno zaščiteni in so bili javno dostopni prek interneta.

Obravnava ranljivosti sistemov

SI-CERT ob koordinaciji razreševanja incidentov, tehničnega svetovanja ob vdorih, računalniških okužbah in drugih zlorabah na svoji spletni strani izdaja tudi opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. Skrbnike sistemov in uporabnike o znanih ranljivosti in drugih zlorabah obvestimo neposredno, s pomočjo ponudnikov gostiteljstva ali operaterjev elektronskih komunikacij.

ZLORABA DOBAVNE VERIGE SHADOWHAMMER

Konec marca 2019 je prišlo do objave o zlorabi pripomočka ASUS Live Update za samodejno posodabljanje nameščenih aplikacij in gonilnikov prenosnih računalnikov ASUS. S tem lahko storilci v posodobitve vrinejo škodljivo kodo. Posodobitve so uporabljale digitalne podpise podjetja ASUS za distribucijo orodja z vgrajenimi stranskimi vrati. Šlo naj bi za usmerjen napad na točno določene uporabnike, njihova identifikacija pa se je izvajala prek naslovov MAC omrežnih vmesnikov. O zlorabi sistema za nadgradnje podjetja ASUS smo obvestili vse organe državne uprave in jih pozvali, da ugotovijo prisotnost ranljivih naprav ASUS in preverijo možnosti okužbe glede na kazalnike okužbe.

RAZMAH RANLJIVOSTI BLUEKEEP V SLOVENIJI

Sredi maja 2019 je bila objavljena ranljivost v storitvi za oddaljeni dostop Windows Remote Desktop Service (RDP), ki oddaljenemu uporabniku brez prijave omogoča zagon programske kode na daljavo (RCE, Remote Code Execution). Ranljivost je bila prisotna v operacijskih sistemih Windows Vista, Windows 7, Windows XP, Windows Server 2003 in Windows Server 2008, znana pa je pod imenom BlueKeep. SI-CERT je o ranljivosti RDP obvestil skrbnike vseh sistemov v Sloveniji, ki imajo prosto dosegljivo storitev RDP. Obveščanje je potekalo neposredno, kadar je bilo to mogoče na podlagi reverznih zapisov DNS, sicer pa prek ponudnikov. V času obveščanja je bilo v slovenskem naslovnem prostoru IP 4000 sistemov z odprtim dostopom RDP. Čeprav niso vsi imeli težave BlueKeep, smo vseeno izkoristili to priložnost za razpošiljanje priporočil o ustrezni zaščiti dostopa.

SISTEMI, RANLJIVI NA BLUEKEEP

Na začetku novembra smo ponovili poizvedbo o ranljivih sistemih, ki uporabljajo storitev za oddaljeni dostop Windows Remote Desktop Service (RDP). Na voljo smo imeli tudi orodje, ki je preverjalo dejansko prisotnost ranljivosti BlueKeep. V času analize in iskanja ranljivosti Bluekeep je bilo v slovenskem naslovnem prostoru IP 3555 sistemov z odprtim dostopom RDP. Raziskava je pokazala, da je imelo od omenjenega števila 383 sistemov prisotno ranljivost BlueKeep. Prek njihovih ponudnikov smo uporabnike sistemov obvestili in jih pozvali k odpravi ranljivosti.

Izvedli smo tudi ponovni pregled ranljivosti, ki je pokazal trend upada dostopnosti sistemov z odprtim dostopom RDP; v slovenskem naslovnem prostoru IP je bilo tako prisotno še 2608 sistemov z odprtim dostopom RDP, kar je pomenilo 27-odstotni padec glede na prvotne podatke. Od tega je imelo v novi raziskavi 342 sistemov prisotno ranljivost BlueKeep, kar je pomenilo 12-odstotni padec glede na prvotno raziskavo. Tudi tokrat smo skrbnike sistemov prek njihovih ponudnikov obvestili o prisotni ranljivosti.

RANLJIVOST V POŠTNEM STREŽNIKU EXIM – CVE-2019-10149

Junija 2019 je sledila javna objava ranljivosti v sistemu za posredovanje elektronske pošte Exim verzij 4.87 do 4.91. Ranljivost je bila posledica nepravilnega preverjanja naslova prejemnika in je omogočala prevzem nadzora nad ranljivim strežnikom ter izvajanje ukazov s povišanimi pravicami na daljavo.

V slovenskem naslovnem prostoru IP je bilo 61 ranljivih poštnih strežnikov Exim, katerih skrbniki so bili obveščeni prek ponudnikov storitev. Ugotovljena je bila zloraba dveh poštnih strežnikov Exim. Napadalci so omenjeno ranljivost izkoristili za podtikanje skripte za rudarjenje kriptovalut, nameščanje posredniškega strežnika (proxy) in nameščanje obratnega posredniškega strežnika (reverse proxy) Onion.sh, ki je omogočal dostop do strežnika tudi prek omrežja TOR. Tako je strežnik za nekaj časa (brez vednosti lastnika, seveda) postal del temnega spleta (angl. dark web).

4000

SISTEMOV Z ODPRTO STORITVIJO RDP V SLOVENIJI

383

SISTEMOV Z RANLJIVOSTJO BLUEKEEP

61

RANLJIVIH STREŽNIKOV EXIM V SLOVENIJI

2

ZLORABLJENA STREŽNIKA EXIM V SLOVENIJI

ODGOVORNO RAZKRIVANJE RANLJIVOSTI

Odgovorno razkrivanje ranljivosti predvideva, da oseba, ki odkrije ranljivost, to sporoči proizvajalcu, skrbniku sistema ali razvijalcu programske opreme. Sporočanje je lahko neposredno ali prek neodvisne tretje osebe koordinatorja. Odgovorno razkrivanje je ustaljen postopek sodelovanja neodvisnih raziskovalcev pri izboljševanju zaščite računalniških sistemov in je postal dobra praksa v tehnologiji IKT in računalniški industriji.
SI-CERT v procesu odgovornega razkrivanja prevzame vlogo koordinatorja. Sama prisotnost ranljivosti tudi še ne pomeni, da je možno to ranljivost izkoristiti v napadu, zato je treba vsako posamezno prijavo skrbno preučiti in preveriti. 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.

PRIMERI OBRAVNAVANIH ODGOVORNO RAZKRITIH RANLJIVOSTI V LETU 2019

- **Dostopni podatki nekaterih bolnikov slovenske bolnišnice, ki so se prek spleta naročili na pregled.**
- **Izdani računi nekaterih slovenskih spletnih trgovin so bili javno dostopni.**
- **Zaradi neustrezne zaščite skrbniškega vmesnika je bil možen vpogled v osebne podatke kupcev spletne trgovine.**
- **Na spletni strani slovenskega društva so bili javno dostopni nekateri osebni podatki članov.**
- **Na spletni strani slovenske šole so bili javno dostopni dokumenti z osebnimi podatki.**
- **Na spletni strani slovenske fakultete so bili javno dostopni dokumenti z osebnimi podatki nekaterih študentov.**

- **Na spletni strani pobude so bili dosegljivi nekateri življenjepisi z osebnimi podatki.**
- **Na spletni strani slovenskega podjetja so bili javno dostopni bančni izpiski podjetja.**
- **Zaradi neustrezne zaščite mape git na strežniku so bile razvidne informacije za dostop do baze podatkov ter najdene dodatne ranljivosti spletne aplikacije.**
- **Na slovenski spletni strani za prodajo vstopnic so bili dosegljivi osebni podatki strank.**
- **V programski opremi za davčne blagajne je bilo najdenih več ranljivosti.**

Program ozaveščanja

Upravljanje nacionalnega programa ozaveščanja o informacijski varnosti Varni na internetu je še ena dejavnost SI-CERT-a, ki je skozi leta postala prepoznavna tako med spletnimi uporabniki kot v strokovni javnosti.

VARNI NA INTERNETU
Od mene je odvisno vse.

Zavedanje, znanje, pomoč

Na začetku 2011 smo na tiskovni konferenci javnosti prvič predstavili program Varni na internetu, v osmih letih pa smo s številnimi spisanimi članki, posnetimi videi in odgovori na konkretne težave spletnih uporabnikov pomembno prispevali k dvigu zavedanja o informacijski varnosti.

Komu so naša sporočila namenjena? Preprosto vsem, ki se povezujejo v internet, doma ali v službi. Napotki o varni uporabi sodobnih spletnih storitev so postali nepogrešljivi, pa vendar so se naše ključne problematike in ciljne javnosti v letih izostrile. Ravno umeščenost programa Varni na internetu med dejavnosti sprejemanja in odzivanja na incidente nam daje vpogled v realnost težav slovenskih spletnih uporabnikov in temu primerno javnost ažurno opozarjamo na zaznane nevarnosti.

Nacionalni program Varni na internetu

Program smo zasnovali za pomoč, ozaveščanje in izobraževanje širše slovenske javnosti o varni uporabi interneta in prepoznavanju tveganj. Opozarjamo na najrazličnejše spletne prevare, svetujemo, kako varno nakupovati prek spleta, kako zaščititi uporabniške račune, podatke in naprave. Poseben sklop vsebin je namenjen izobraževanju o informacijski varnosti v poslovnem okolju.

Ciljamo predvsem na odrasle spletne uporabnike, ki (včasih preveč brezskrbno) uporabljajo kreditno kartico za spletne nakupe, uporabljajo družbena omrežja, rezervirajo počitnice in koncertne vstopnice, vedno pogosteje iščejo priložnosti za zaslužek, včasih tudi večno ljubezen. Kot pomembni prejemniki naših sporočil so se izkazali zaposleni v manjših podjetjih, saj opažamo, da napadi na podjetja in višina finančne škode vztrajno naraščajo. Zato smo tudi ustvarili portal www.varninainternetu.si, kjer so na enem mestu zbrane številne spletne goljufije, nasveti, kvizi, video napotki. Tudi drugje na kanalih družbenih omrežij, na predavanjih in v medijskih izjavah opozarjamo na nujnost ustrezne tehnične zaščite, predvsem pa na preudarno obnašanje na spletu. Naše delo temelji na preventivnem delovanju – opozarjanju in izobraževanju spletnih uporabnikov, kako prepoznajo različna spletna tveganja ter pravočasno zaščitijo svojo digitalno identiteto, računalniško opremo in ne nazadnje tudi svoj bančni račun. 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.

#KLJUČNIKI LETA 2019:

nagradna igra na Facebooku
SMS-klub
lažne grožnje (fake sextortion)
ljubezenska prevara
lažno posojilo

Aprila 2018 je bil sprejet Zakon o informacijski varnosti (ZInfV), ki je jasno definiral naloge odzivnega centra SI-CERT in ob bok drugim dejavnostim postavil tudi ozaveščanje uporabnikov na področju informacijske varnosti. Zakonsko predpisane naloge ozaveščanja javnosti, opredeljene v 5. točki drugega odstavka 28. člena ZInfV, SI-CERT izpolnjuje skozi številne komunikacijske in medijske dejavnosti programa Varni na internetu. Lahko rečemo, da je zakon tudi formalno popisal naloge, ki jih opravljamo že osem let.

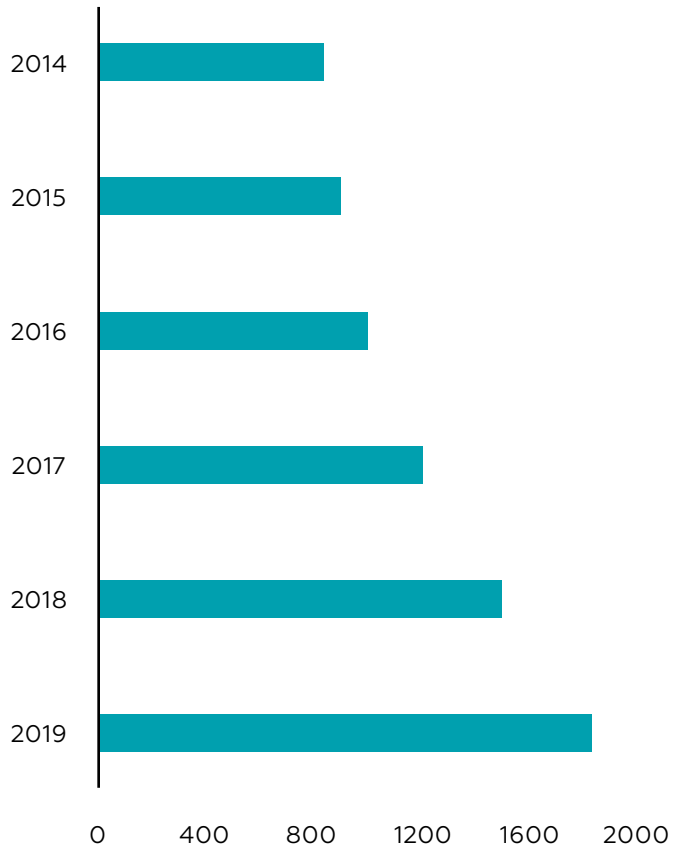
(Ne)slavni rekordi 2019

LETO V ZNAMENJU LAŽI

Na SI-CERT-u smo v letu 2019 obravnavali kar 1840 primerov družbenega inženiringa, med katere uvrščamo različne spletne goljufije in tudi phishing napade, znova pa so tovrstne zlorabe presegle število tehničnih napadov. In ponovno lahko rečemo, da smo podrli lanskoletni rekord v številu vseh obravnavanih incidentov ter podvojili število obravnavanih phishing napadov, teh je bilo kar 435.

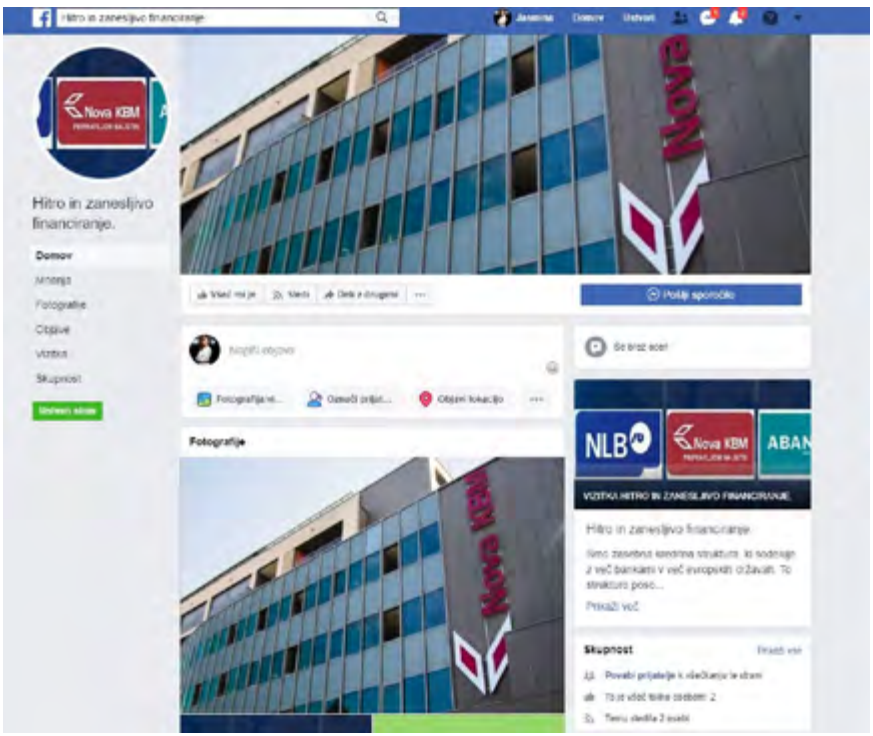
Najpogostejša vprašanja, ki so nam jih zastavljali spletni uporabniki, lahko strnemo v filmski naslov – Sex, Lies, and Videotape (Seks, laži in videotrakovi). Januarja 2019 smo zabeležili val vprašanj uporabnikov, povezanih z lažnimi grožnjami o okužbi računalnika in izsiljevanjem z objavo (neobstoječih) intimnih posnetkov (*angl. fake sextortion*). Podobno kampanjo izsiljevalskih sporočil smo beležili že julija 2018, takrat celo bolj intenzivno, v letu 2019 pa smo prejeli skupaj 291 prijav lažnega izsiljevanja.

ŠTEVILO OBRAVNAVANIH SPLETNIH GOLJUFIJ IN PHISHING NAPADOV



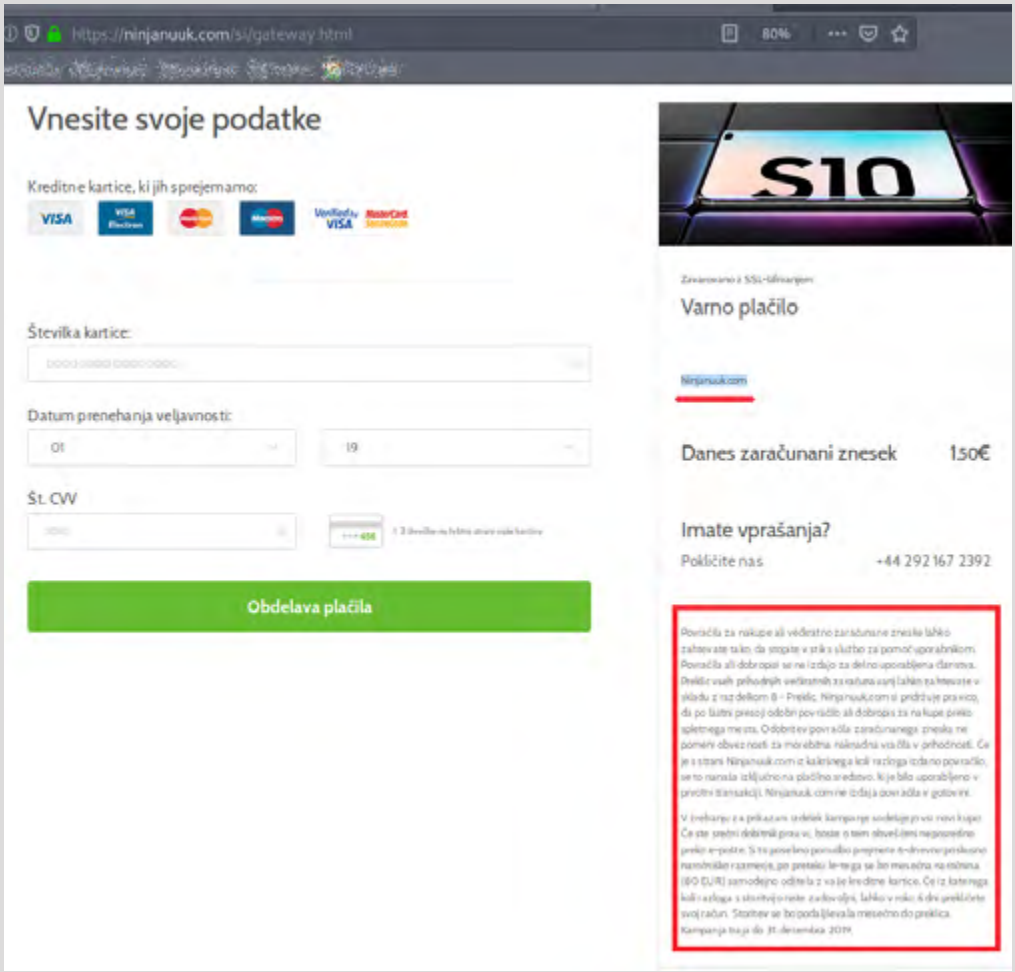
Ponovno smo zaznali rast ponudb za lažna posojila, vendar v sodobnejši različici. Že leta 2012 smo prejemali prijave oškodovanih posameznikov, ki so vzpostavili stik z goljufi na različnih forumih in spletnih oglasnikih. Zdaj pa se lažne ponudbe pojavljajo predvsem na Facebooku, kjer goljufi izkoriščajo logotipe in vizualno podobo slovenskih finančnih ustanov in postavljajo strani Facebook z namenom zavajanja. Oktobra 2019 smo na problematiko opozorili v izjavi za javnost, hkrati je podobno opozorilo objavilo tudi Združenje bank Slovenije.

Zaznali smo tudi občutno več lažnih nagradnih iger, vendar z drugačnim razpletom, kot smo ga bili vajeni. V lažnih nagradnih igrah je največkrat glavni namen zvabiti uporabnike v plačljivi SMS-klub, v obravnavanih primerih pa goljufi želijo izvabiti številko kreditne kartice ter uporabnike naročiti na trivialno storitev. Sprva simbolični znesek en evro se po nekaj dneh spremeni v mesečno naročnino v znesku tudi do 100 evrov, za katerega je bremenjena kreditna kartica.



NAJUČINKOVITEJŠI UKREP? IGNORIRAJTE ODLIČNE PONUDBE!

Če na spletnih straneh zasledite tovrstne oglase, vam svetujemo, da jih preprosto ignorirate in ne klikate povezav ter ne izpolnjujte obrazcev za prejem telefonov v nagradnih igrah ali anketah. Prav tako omejite možnost oz. izklopite sporočanje (*angl. notifications*) za spletne strani, za katere niste prepričani, da so legitimne oz. so vam neznane. Običajno so te strani in njihova obvestila vir zavajajočih oglasov, ki sploh ne pripeljejo do nagradnih iger.



Okrogla miza o problematiki ljubezenskih prevar na spletu

KO REČEM »LJUBIM TE«, MISLIM VSAKO BESEDO. ZDAJ PA NAKAŽI DENAR!

20. februarja 2019 smo v kreativnem centru Poligon organizirali okroglo mizo z naslovom »Ljubezenske prevare na spletu«, s katero smo želeli slovensko javnost opozoriti na velik porast tovrstnih prevar. V razpravi so sodelovali Tadej Hren, vodilni strokovnjak na področju informacijske varnosti in dolgoletni sodelavec SI-CERT-a, dr. David Modic, mednarodno priznan raziskovalec psihologije računalniških prevar iz ljubljanske Fakultete za računalništvo in informatiko, in dr. Veronika Podgoršek, cenjena slovenska psihoterapevtka, ki je svoje znanje izpopolnila na Mednarodnem psihoterapevtskem inštitutu (IPI) v Washingtonu.

Namen okrogle mize je bil opozoriti na trend naraščanja ljubezenskih prevar. Kot je poudaril Tadej Hren, smo na SI-CERT-u zabeležili prvo tovrstno prevaro leta 2013, v naslednjih letih eno ali dve, nato pa je sledil velik skok. Leta 2018 smo obravnavali 40 primerov ljubezenskih prevar in v prvih mesecih 2019 je sledilo kar 14 prijav. Hren je pojasnil, da so ljubezenske prevare specifična oblika spletne goljufije, kjer so žrtve poleg visokega finančnega oškodovanja še hudo čustveno izkoriščane in zavedene. Kriminalci, praviloma iz afriških držav, žrtve iščejo na Facebooku in Instagramu, kjer postavijo lažen profil z lepimi slikami. Pošljejo prošnjo za prijateljstvo, začnejo pogovor in razkrijejo svojo tragično življenjsko zgodbo – so osamljeni

marinci, ovdoveli zdravniki z majhnimi otroki, človekoljubni delavci. Ko vzpostavijo zaupen odnos, začnejo s prošnjami za denar.

»Ko je denar nakazan, sledijo vedno nove prošnje, dokler žrtev ne ugotovi, da je vse popolna laž. Bolj kot dejansko povzročena finančna škoda žrtve prizadene občutek izkoriščenosti, sramu, razočaranja. Laž in zavrnitev jih boli bolj kot izguba denarja,« je poudaril Hren iz centra SI-CERT.

Dr. Modic je v uvodu pojasnil, da gre za že stoletja staro prevaro »španski zapornik« oz. nigerijsko prevaro, le v drugi preobleki. V sodobnem svetu pač dobro usposobljeni spletni kriminalci sledijo preverjenim trženjskim metodam in uporabljajo principe psihologije potrošništva. Poudaril je tudi zanimivo statistiko – ženske v povprečju goljufom nakažejo višje zneske v ljubezenskih prevarah, vendar moški večkrat podležejo takšnim prevaram. Tudi dr. Podgoršek je poudarila, da spletni goljufi izjemno dobro poznajo psihologijo moškega in ženske, njihov način življenja in vrednote, ali pa jim žrtve to same zaupajo. Kot je dejala: *»Vsi hrepenimo po odnosu, osamljenost najbolj boli. Ti prevaranti pa poznajo psihologijo žensk.«*

Statistika SI-CERT-a kaže, da je v letu 2019 žrtev ljubezenske prevare v povprečju nakazala 12.377 evrov, lani je povprečno oškodovanje znašalo 9.120 evrov. In ravno pri tej obliki spletne goljufije smo zabeležili najvišje finančno oškodovanje, kjer je žrtev goljufu v posamičnem primeru nakazala kar 62.000 evrov.

Evropski mesec kibernetske varnosti 2019

SPLETNA VARNOST JE NAŠA SKUPNA ODGOVORNOST

Evropski mesec kibernetske varnosti (*angl.* *European Cyber Security Month*) je vseevropska kampanja ozaveščanja, ki jo s podporo držav članic organizirata Agencija Evropske unije za kibernetsko varnost (ENISA) in Evropska komisija. Kampanja, ki poteka vsako leto v mesecu oktobru, je v ospredje postavila dve pomembni temi, in sicer osnove kibernetske higiene in nove, nastajajoče tehnologije (*angl.* *Emerging technologies*). Poseben poudarek je ENISA namenila potrebi po spremembi vedenja ter načinih, na katere lahko spletni uporabniki prepoznajo tveganja, ki jih prinašajo nove tehnologije.

Prva tema meseca kibernetske varnosti je zajemala osnovno kibernetsko higieno. S to metaforo so organizatorji kampanje predstavili dobre navade v zvezi s kibernetsko varnostjo, ki bi morale biti del naše vsakodnevne rutine.

Ključno sporočilo je, da je kibernetska varnost navada, ki jo pridobimo v mladosti in nas spremlja vse življenje. ENISA je ob začetku kampanje objavila videoposnetek s preprostimi koraki za zagotavljanje kibernetske varnosti, ki jih lahko državljani vključimo v svoj vsakdan.

Slovenija je že osmo leto zaporedoma sodelovala v vseevropski pobudi s programom ozaveščanja Varni na internetu. Spletne uporabnike smo ves oktober opozarjali na osnovne varnostne ukrepe z video kampanjo na družbenih omrežjih, televizijskim oglasom ter tremi namenskimi pristajalnimi stranmi, ki v ospredje postavljajo številke – dejanska finančna oškodovanja, ki jih povzročijo spletne zlorabe. Kampanjo je podprlo tudi predstavništvo Evropske komisije v Sloveniji. Omogočili so nam enotedensko predvajanje videov na vseh predvajalnikih na avtobusih javnega potniškega prometa v Ljubljani in Mariboru ter s tem še večji doseg kampanje.

Na začetku oktobra smo medijem in javnosti posredovali osnovne varnostne napotke na posebni pristajalni strani »Naredi backup!«: uporabljate upravljalnike gesel in aktivirajte preverjanje v dveh korakih. Skrbite, da so vse vaše naprave redno posodobljene, predvsem pa ne pozabite na varnostne kopije pomembnih dokumentov.

Zgolj tehnični ukrepi ne morejo zagotoviti varne rabe sodobnih tehnologij, še vedno je na strani uporabnikov, da prepoznajo znake spletnih goljufij. Vabe, ki jih nastavljajo spletni goljufi, so zelo preproste – nizke cene in velike obljube, pa naj bodo odlični zaslužki, ugodna posojila, milijonske nagrade, zastonj vinjete za en sam »všeček« ali neverjetno poceni izdelki. Druga tematska pristajalna stran »Ne verjemi velikim obljubam!« je tako izobraževala o tipičnih znakih prevar.

Na namenski strani »Za profilno sliko je lahko kdorkoli!« pa smo poudarili statistiko, da se je v enem letu število primerov izsiljevanja z intimnimi posnetki povečalo za kar 400-odstotkov. Tako smo želeli pozornost usmeriti na prevare, ki temeljijo na čustveni manipulaciji, žrtve pa so poleg visokega finančnega oškodovanja še pod hudim psihičnim pritiskom izsiljevalcev.

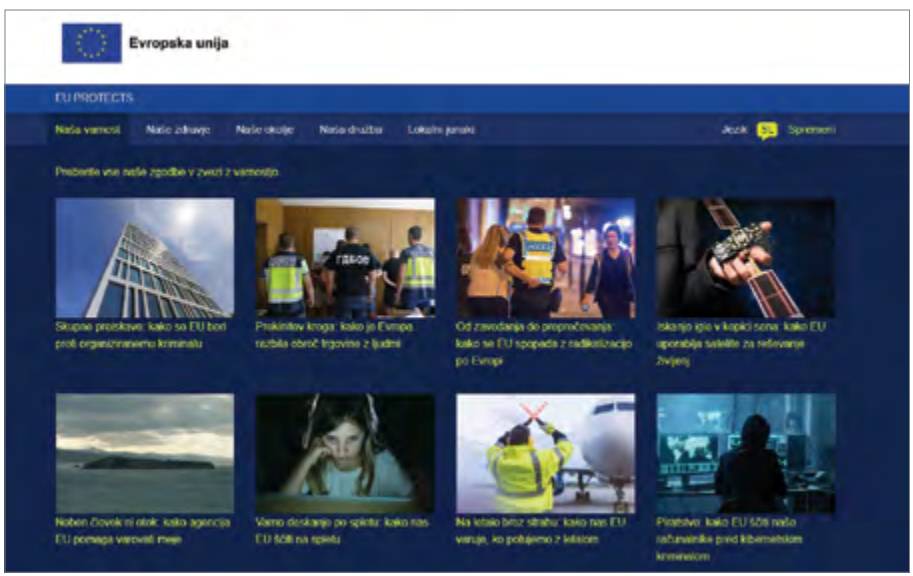
Kriminalci svoje žrtve največkrat iščejo na Facebooku in Instagramu, zato smo tudi video kampanjo umestili na družbena omrežja, da bi dosegli populacijo, ki uporablja družbene platforme za navezovanje stikov, sodelovanje v nagradnih igrah, tudi nakupovanje. Z našimi videi želimo opozoriti na dejstvo, da se za lepo profilno sliko ali obljubami o milijonskih nagradah najverjetneje skrivajo prevaranti.

EUROPEAN CYBER SECURITY MONTH

EU varujemo skupaj

SI-CERT SODELOVAL PRI VSEEVROPSKI KAMPANJI »EU PROTECTS«

Predstavništvo Evropske komisije v Sloveniji nas je povabilo k sodelovanju v kampanji »EU protects« oz. »EU varujemo skupaj«, s katero Evropska unija opozarja na zgodbe posameznikov, ki s svojim delom dnevno skrbijo za zaščito ljudi v Evropi. Veliko se govori o perečih izzivih in nevarnostih, kot so terorizem, trgovina z ljudmi, naravne nesreče ali redke bolezni. Manj pa se govori o ljudeh, ki za te izzive iščejo rešitve. Kampanja »EU protects« opozarja na politike EU za zaščito državljanov in »junake vsakdana«, ki s svojim delom pripomorejo k temu, da smo vsi varnejši, najsi gre za pomoč pri požarih, boj proti organiziranemu kriminalu ali preprečevanje prodaje nevarnih igrač.



Kot eden od strokovnjakov, ki se odziva na nujne primere, je bil izpostavljen tudi vodja SI-CERT-a, Gorazd Božič. Kot je poudaril, je v številnih primerih celotna skupina SI-CERT s hitrim ukrepanjem in odličnim medsebojnim sodelovanjem s partnerji po Evropi in svetu preprečila širitev kibernetskega napada. Preprečili smo ogromno finančno škodo ter vzpostavili primer dobre prakse odličnega sodelovanja med državnimi institucijami in partnerji v mednarodnem okolju.

Naslov publikacije:
Poročilo o kibernetski varnosti za leto 2019

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

Leto izida: 2020

Natis: 600 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

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

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