POROČILO O KIBERNETSKI VARNOSTI ZA LETO 2022

si·cert

Nacionalni odzivni center za kibernetsko varnost

POROČILO O KIBERNETSKI VARNOSTI ZA LETO 2022

SI-CERT

Nacionalni odzivni center za kibernetsko varnost

Nacionalni odzivni center za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team) opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost

www.cert.si

Facebook:
facebook.com/sicert

Twitter:
@sicert

Ozaveščanje javnosti na področju informacijske varnosti

www.varninainternetu.si

Facebook:
facebook.com/varninainternetu

Twitter:
@varninanetu

Instagram:
instagram.com/varninainternetu

URSIV

Vse dejavnosti centra SI-CERT financira Urad Vlade Republike Slovenije za informacijsko varnost.

POROČILO O KIBERNETSKI VARNOSTI ZA LETO 2022

si·cert

Nacionalni odzivni center za kibernetsko varnost

Uvodni nagovor 8

Pregled leta 2022
v številkah 10

Pregled leta 2022
po ključnih besedah
v obravnavanih incidentih 12

1. PREDSTAVITEV ODZIVNEGA CENTRA SI-CERT 14

Nacionalni okvir kibernetske varnosti 16

Kdaj incident prijaviti centru SI-CERT? 18

Organizacijske spremembe - uvedba prvolinijske pomoči 20

Mednarodno sodelovanje 22

Platforma za izmenjavo informacij o kibernetskih grožnjah MISP 23

2. VRSTE, ŠTEVILO INCIDENTOV IN KLJUČNI KAZALCI 25

Statistika oškodovanj 30

3. POMEMBNEJŠI INCIDENTI IN OPAŽANJA 31

Vojna v Ukrajini - ko kibernetsko bojevanje prestopi geografske meje 32

Obveščanje o ranljivostih 35

Zlonamerna koda 36

Napadi na podjetja 40

Spletne goljufije 42

Phishing napadi ne pojenjajo 45

4. PROGRAM OZAVEŠČANJA VARNI NA INTERNETU 50

Širok splet komunikacijskih orodij za doseganje uporabnikov 51

Evropski mesec kibernetske varnosti - postani ambasador kibervarnosti! 53

Izognite se najslabšemu scenariju - izobražujte zaposlene 55

Nova videoserija
A si vedu? - zanimiva dejstva s področja kibernetske varnosti 57

UVODNI NAGOVOR

Leto 2022 se je začelo z vojno v Ukrajini. Mesec dni pred vojaškim napadom smo že lahko zaznali povečano dejavnost v kibernetskem prostoru. V mreži CSIRT Evropske unije, v kateri sodelujejo odzivni centri iz držav članic EU in CERT-EU, smo takoj začeli intenzivno spremljati dogajanje. Nabor kibernetskih napadov, ki so bili sproženi tik pred invazijo, je bil dokaj pričakovan in precej omejen na območje Ukrajine (podrobneje o tem v nadaljevanju poročila). Mednarodno sodelovanje v omenjeni mreži CSIRT temelji na zaupanju med odzivnimi centri za kibernetsko varnost CSIRT znotraj EU. Tako namreč dosežemo hitro izmenjavo informacij ob znanih pravilih, kaj lahko z njimi storimo in s kom jih lahko dalje delimo. Tudi znotraj države velja isto pravilo: zaupanje se ne daje, temveč se v praksi gradi mesece in leta. Zato je bilo neprijetno spremljati, kako se je v javnosti pojavilo interno poročilo centra SI-CERT o kibernetskem napadu na Upravo RS za zaščito in reševanje. V centru SI-CERT se seveda dobro zavedamo pomembne vloge, ki jo imajo mediji pri uresničevanju pravice javnosti do obveščenosti, o tem pričajo tudi številke o izjavah, ki jih

dajemo za različne medije. Iskanje motiva, ali je tu bil primarni interes javnosti ali pa kaj veliko bolj banalnega, je naloga koga drugega. A vseeno nas skrbi učinek na raven zaupanja, ki ga bomo kot država na področju kibernetske varnosti ohranili dolgoročno, saj so v poročilu tudi podatki tujih partnerjev, ki so nam jih poslali v zaupanju. Ne želimo si namreč, da bi kolegi iz skupnosti CSIRT zastali in razmišljali, ali naj res pošljejo podatke, ključne za preiskavo, v državo, od koder curljajo zaupne informacije. Članke o tem, kaj smo namreč v preiskavi odkrili, berejo seveda tudi napadalci.

Gorazd Božič,
vodja centra SI-CERT

PREGLED LETA 2022 V ŠTEVILKAH

4123

- obravnavanih incidentov (30-odstotni porast glede na leto 2021)

133

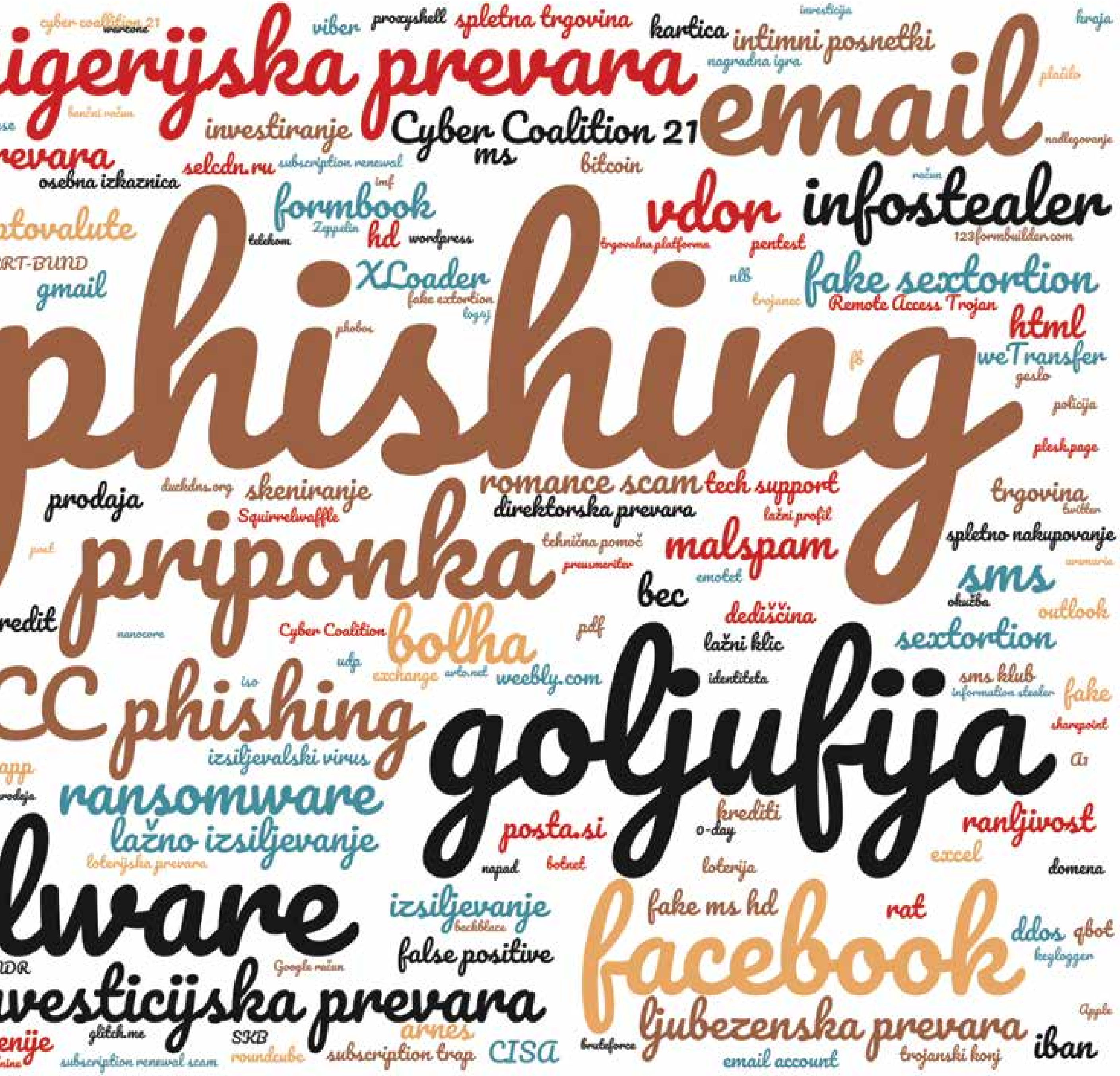
- novinarskih vprašanj

375

- preiskanih vzorcev zlonamerne kode


6100
izdanih potrdil o uspešno opravljenem spletnem tečaju Varni v pisarni
5800
poslanih odgovorov
1432
phishing incidentov
10.
obletnica kampanje Evropski mesec kibervarnosti
20
novih videov z nasveti o prepoznavanju spletnih nevarnosti
2
večji spletni oglaševalski kampanji, ki sta zbrali več kot 357.000 ogledov na platformah Facebook, LinkedIn in YouTube

PREGLED LETA 2022 PO KLJUČNIH BESEDAH V OBRAVNAVANIH INCIDENTIH


phishing
goljufija
email
priponka
facebook
infostealer
vdor
fake sextortion
ransomware
Cyber Coalition 21
formbook
XLoader
lažno izsiljevanje
izsiljevanje
ljubezenska prevara
malspam
romance scam
tech support
sextortion
bolha
posta.si
ranljivost
sms
html
weTransfer
spletna trgovina
intimni posnetki
kartica
investiranje
bitcoin
skeniranje
direktorska prevara
spletno nakupovanje
bec
dediščina
lažni klic
weebly.com
false positive
fake ms hd
email account
subscription trap
iban
CISA
ddos
qbot
trgovina
prodaja
gmail
osebna izkaznica
selcdn.ru
Remote Access Trojan
izsiljevalski virus
krediti
loterija
excel
rat
outlook
domena
Squirrelwaffle
Cyber Coalition
exchange
sms klub
fake
trojanski konj
roundcube
arnes
botnet
napad
o-day
identiteta
pentest
wordpress
hd
telekom
viber
proxyshell
pdf
policija
geslo
plesk.page
twitter
okužba
emotet
tehnična pomoč
preusmeritev
lažni profil
duckdns.org
prodaja
trgovalna platforma
123formbuilder.com
nagradna igra
plačilo
nadlegovanje
keylogger
Apple
bruteforce
SKB
glitch.me
Google račun
sharepoint
information stealer
A1
subscription renewal scam
subscription renewal
loterijska prevara
nanocore
udp
iso
phobos
log4j
fake extortion
trojanec
nlb
fb
Zeppelin
imf
račun
kraja
investicija
bančni račun

1. PREDSTAVITEV ODZIVNEGA CENTRA SI-CERT

si·cert
Nacionalni odzivni center za kibernetsko varnost

URSIV

VARNI NA INTERNETU
Od mene je odvisno vse.

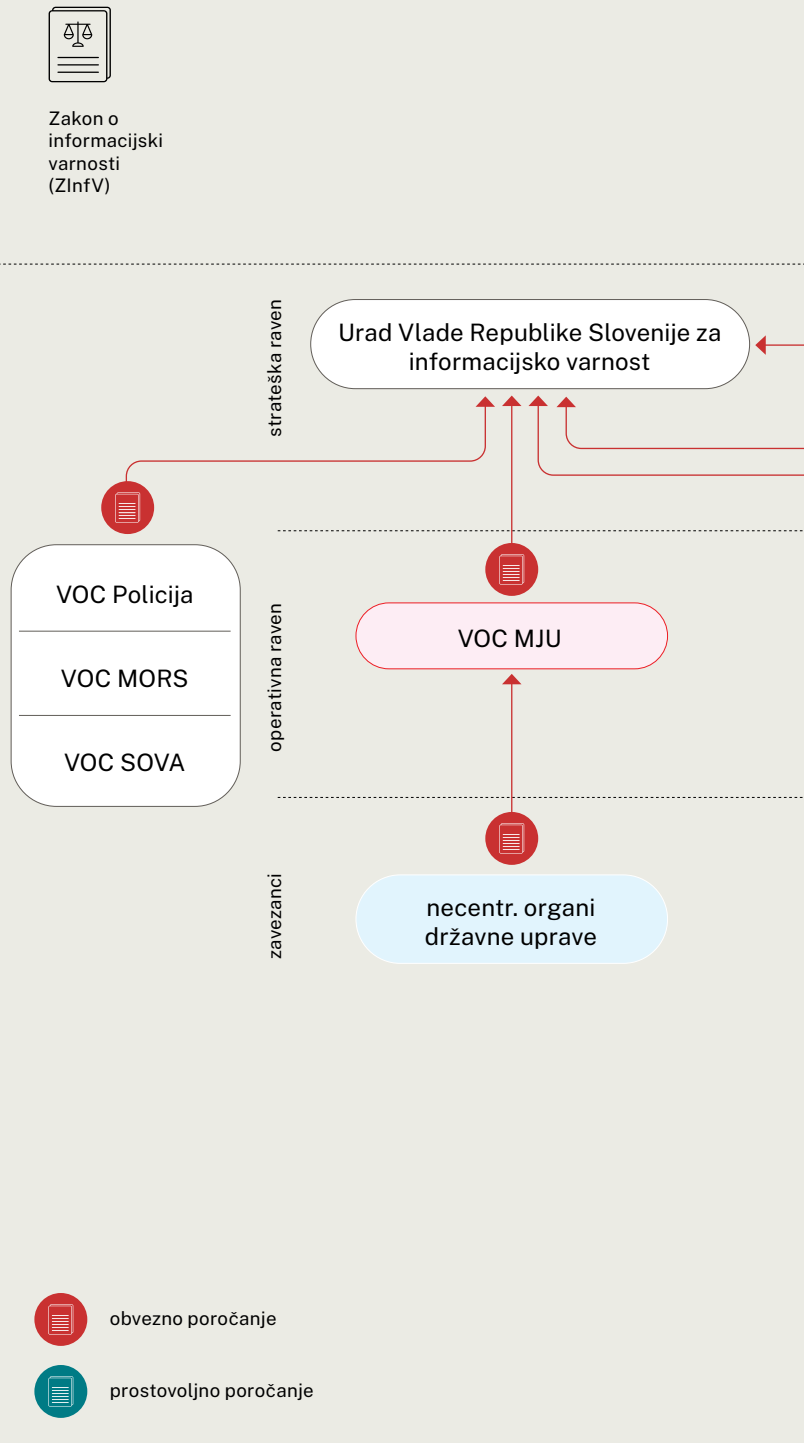
Nacionalni odzivni center za kibernetsko varnost SI-CERT je odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Ustanovljen je bil leta 1995 in deluje pod okriljem Javnega zavoda Arnes. Njegove primarne naloge so strokovna pomoč pri preiskovanju incidentov, 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.

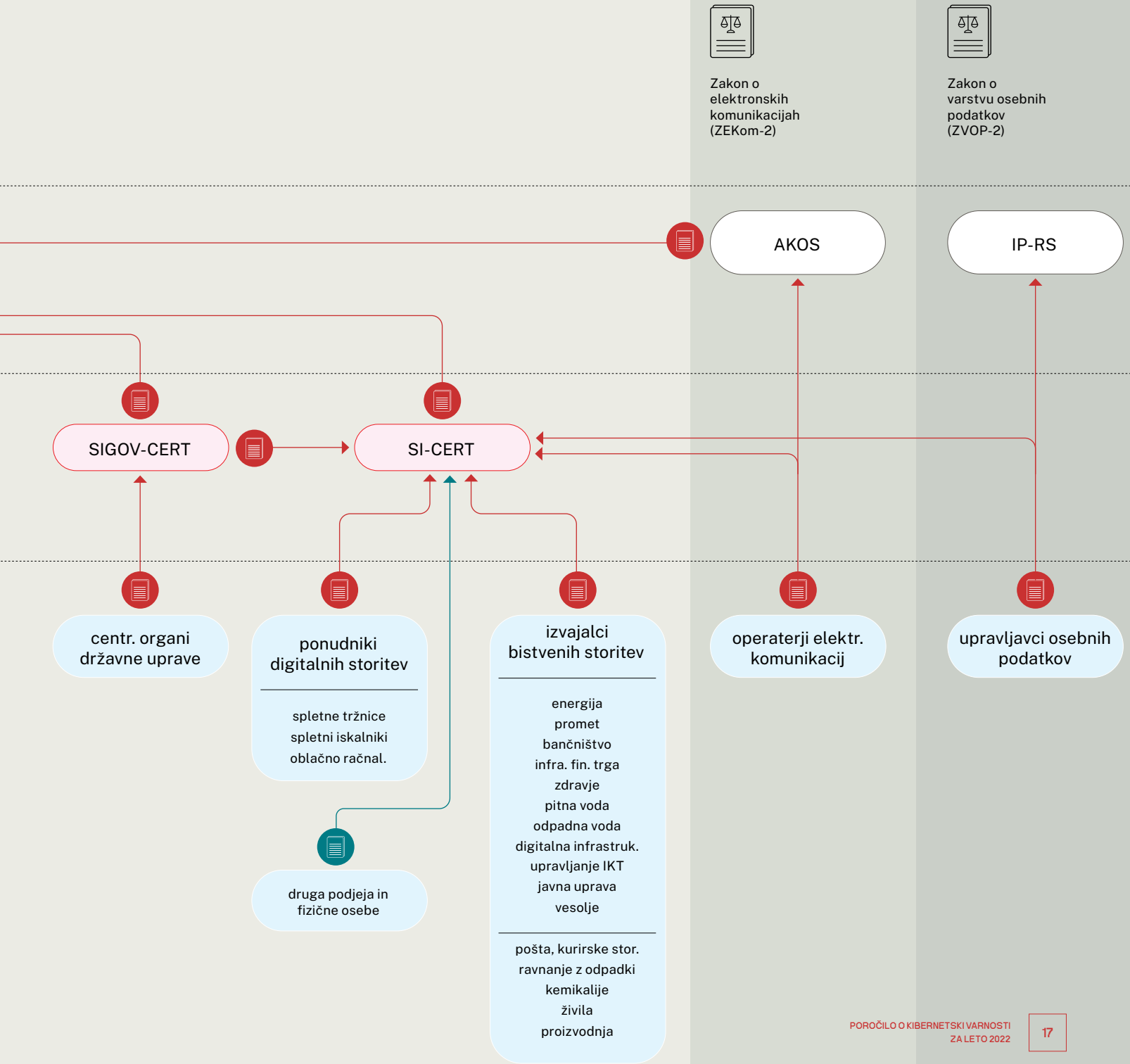
S sprejetjem Zakona o informacijski varnosti (ZInfV) leta 2018 je SI-CERT prepoznan kot nacionalna skupina CSIRT, katere naloge so opredeljene v 28. členu ZInfV. Kot ključne naloge v vlogi nacionalne skupine CSIRT izpostavljamo sprejem incidentov, ki jih priglasijo zavezanci, in nudenje metodološke pomoči pri obvladovanju incidentov. Dejavnosti centra SI-CERT v celoti financira Urad Vlade Republike Slovenije za informacijsko varnost, pristojni nacionalni organ za informacijsko varnost.

SI-CERT od leta 2011 koordinira tudi nacionalni program ozaveščanja javnosti o informacijski varnosti **Varni na internetu**. Program je zasnovan z namenom izobraževanja širše slovenske javnosti o osnovah varne uporabe interneta ter prepoznavanju aktualnih spletnih tveganj in obveščanju o njih. Opozarjamo na najrazličnejše spletne prevare ter svetujemo, kako varno nakupovati na spletu ter kako zaščititi uporabniške račune, podatke in naprave. **Poseben sklop vsebin je namenjen izobraževanju o informacijski varnosti v poslovnem okolju**.

NACIONALNI OKVIR KIBERNETSKE VARNOSTI

Storitve odzivnega centra SI-CERT so na voljo širši javnosti; po strokovno pomoč pri obravnavi kibernetskih incidentov se lahko obrnejo subjekti, ki jim to predpisuje zakon, prav tako tudi druge pravne in fizične osebe. Umeščenost centra SI-CERT v nacionalni okvir kibernetske varnosti in sistem odzivanja na incidente je razviden iz shematskega prikaza.




Zakon o elektronskih komunikacijah (ZEKom-2)
Zakon o varstvu osebnih podatkov (ZVOP-2)
AKOS
IP-RS
SIGOV-CERT
SI-CERT
centr. organi državne uprave
ponudniki digitalnih storitev
spletne tržnice
spletni iskalniki
oblačno računal.
druga podjeja in fizične osebe
izvajalci bistvenih storitev
energija
promet
bančništvo
infra. fin. trga
zdravje
pitna voda
odpadna voda
digitalna infrastruk.
upravljanje IKT
javna uprava
vesolje
pošta, kurirske stor.
ravnanje z odpadki
kemikalije
živila
proizvodnja
operaterji elektr. komunikacij
upravljavci osebnih podatkov

KDAJ INCIDENT PRIJAVITI CENTRU SI-CERT?

Primer incidenta	Pričakovane dejavnosti centra SI-CERT
OKUŽBA RAČUNALNIKA: izsiljevalski virusi, bančni trojanski konji, ciljani napadi, agenti za pošiljanje neželene elektronske pošte	Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami. Svetovanje o ukrepih za sanacijo stanja.
OPAŽEN VDOR V STREŽNIK: razobličenje, zloraba podatkovnih zbirk, namestitev prikritih orodij storilca	Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.
PHISHING ELEKTRONSKA SPOROČILA: potvorjena elektronska sporočila, ki vas napeljujejo, da geslo vpišete na lažni spletni strani	Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.

Primer incidenta	Pričakovane dejavnosti centra SI-CERT
NAPAD ONEMOGOČANJA: poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja	Ocena o uporabljenih sredstvih za napad, opredelitev mogočih zaščitnih ukrepov, poskus onemogočanja botneta ter obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti.
RANLJIVE ALI IZPOSTAVLJENE STORITVE: vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja	Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.
IZGUBA GESEL ALI KRAJA OMREŽNE IDENTITETE: zloraba prek phishing napada ali okužbe računalnika	Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in možni identifikaciji storilca.

ORGANIZACIJSKE SPREMEMBE – UVEDBA PRVOLINIJSKE POMOČI

V centru SI-CERT sprejemamo prijave, na podlagi katerih lahko nato odpremo vodenje incidenta. Nanj se lahko nanaša več prijav, zato je pomembno spremljati tudi trende prejetih prijav, ne le odprtih incidentov. Ker je pravočasno podajanje informacij prijaviteljem zelo pomembno, moramo ob povečanju števila prijav na daljši rok razmisliti, kako lahko poskrbimo za obvladovanje povečanja.

Odzivni čas centra SI-CERT v letu 2022

Odstotek	Čas prvega odgovora na prijavo
25 %	odgovor poslan v roku **ene ure**
39 %	odgovor poslan v roku **dveh ur**
70 %	v **12 urah**
86 %	v **24 urah**

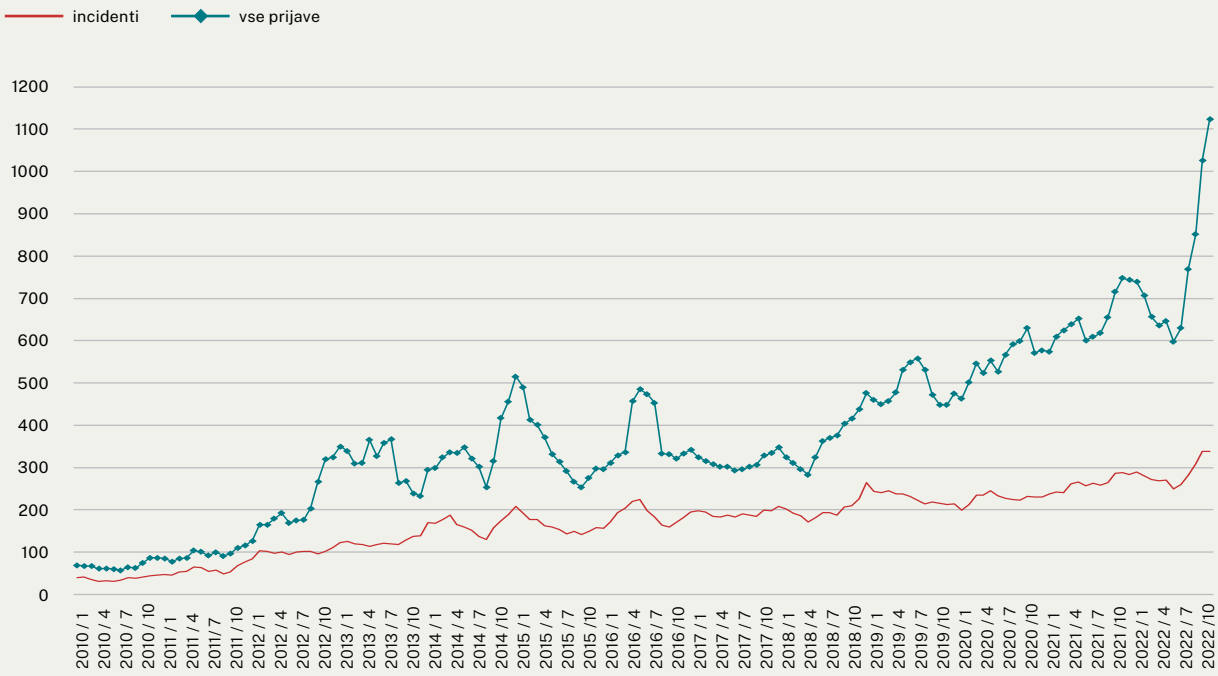
Veliko prijav, en incident.

Nekatere goljufije prihajajo v valovih. Klici lažne Microsoftove tehnične podpore ali lažna sporočila o grožnji s kazenskim pregonom oziroma s podpisom direktorja policije sta značilna primera. Takrat ob številnih prejetih prijavah različnih uporabnikov omrežja v centru SI-CERT odpremo samo en incident, ki združuje vse prijave. Podobno se zgodi, ko gre za zlorabljen sistem v Sloveniji, ki ga storilci uporabijo za pregledovanje omrežja in iskanje ranljivosti. To »skeniranje« običajno opazi več skrbnikov drugih sistemov na internetu in nam pošljejo več prijav, ki pa se nanašajo na isti incident.

V centru SI-CERT smo se v letu 2022 odločili za uvedbo prvolinijske pomoči (PLP), kamor usmerimo vsa vprašanja in prijave, ki nimajo zahtevnejše tehnične komponente. S to preusmeritvijo lahko razbremenimo specializiran kader, analitike, ki se bodo lahko vedno bolj posvečali naprednejšim kibernetskim napadom in obravnavi ranljivosti.

Pričakovati je, da bo kader za prvolinijsko pomoč lažje najti, prvi razgovori s kandidati pa so pokazali, da predstavlja zaposlitev na PLP tudi dobro možnost za nadgradnjo znanja in dobro izhodišče za karierno pot na področju obravnave kibernetskih incidentov. Prvolinijsko pomoč smo v centru SI-CERT uvedli s septembrom 2022.

Obravnavani incidenti in prejete prijave, 2010-2022 (gibljivo štirimesečno povprečje)



MEDNARODNO SODELOVANJE

Vpetost v mednarodno okolje in desetletja povezovanj s kolegi iz tujine so pogosto ključni za hitro ukrepanje, izmenjavo informacij in posledično zamejitev incidenta. SI-CERT je akreditiran skozi program Trusted Introducer (TI), ki od leta 2000 povezuje odzivne centre po vsem svetu. Trusted Introducer predstavlja koordinacijsko središče za izmenjavo informacij in dobrih praks ter upravlja seznam akreditiranih odzivnih centrov za obravnavo incidentov s področja kibernetske varnosti.

Skladno z Direktivo NIS2 je SI-CERT član mreže CSIRT; gre za povezavo, v kateri sodelujejo skupine CSIRT iz držav članic EU in CERT-EU.

Je tudi 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.

PLATFORMA ZA IZMENJAVO INFORMACIJ O KIBERNETSKIH GROŽNJAH MISP

MISP (Malware Information Sharing Platform) je odprtokodna platforma za izmenjavo informacij o kibernetskih grožnjah. Prek platforme MISP partnerji izmenjujemo informacije o indikatorjih zlorab (ang. indicators of compromise, IoC), pridobljenih z analizo škodljive kode ali zajemom in analizo sumljive omrežne dejavnosti. Tako pridobljeni indikatorji so ključnega pomena pri pravočasnem odkrivanju in proaktivni zajezitvi omrežnih zlorab ter tudi za povezovanje posameznih, z analizo pridobljenih indikatorjev z že znanimi omrežnimi zlorabami in okužbami.

SI-CERT se je globalni skupnosti MISP aktivno pridružil pred skoraj desetimi leti. V preteklih desetih letih smo skrbeli za vpeljavo platforme MISP v lokalni skupnosti in pri širitvi platforme MISP v druge države bližnje regije, kjer predstavljamo stičišče za izmenjavo s skupinami CSIRT na območju Zahodnega Balkana. Predstavitev in promocija platforme sta bili opravljeni tudi na regijskem tehničnem kolokviju FIRST, ki je bil leta 2019 organiziran v Ljubljani.

Prek vzpostavljenih partnerskih povezav navzven z evropsko skupnostjo CSIRT, globalno mrežo FIRST, agencijami EU in posameznimi tujimi skupinami CSIRT na podlagi medsebojnih sporazumov ima SI-CERT možnost pridobivanja kakovostnih virov informacij o grožnjah kot tudi dostop do široke mednarodne skupnosti MISP. Vendar informacije ne tečejo zgolj v eni smeri, saj je SI-CERT aktiven partner in je samo v letu 2022 prispeval več kot 200 regionalnih dogodkov, nastalih kot posledica napadov na informacijske sisteme uporabnikov v slovenskem prostoru. Skupno je bilo v letu 2022 prenesenih več kot 24.000 dogodkov, ki so vsebovali več kot 5 milijonov novih atributov. Omeniti velja tudi več kot 2 milijona novih atributov oz. indikatorjev zlorab, ki jih lahko povezane organizacije ob pomoči pravil za napredne požarne pregrade neposredno uporabijo pri zaščiti.

Pri hranjenih informacijah SI-CERT seveda nima interesa, da bi jih zadrževal zgolj zase, zato jih neokrnjene delimo z lokalno skupnostjo v Sloveniji. Med organizacije z možnostjo pridobivanja podatkov prek storitve MISP štejemo že:

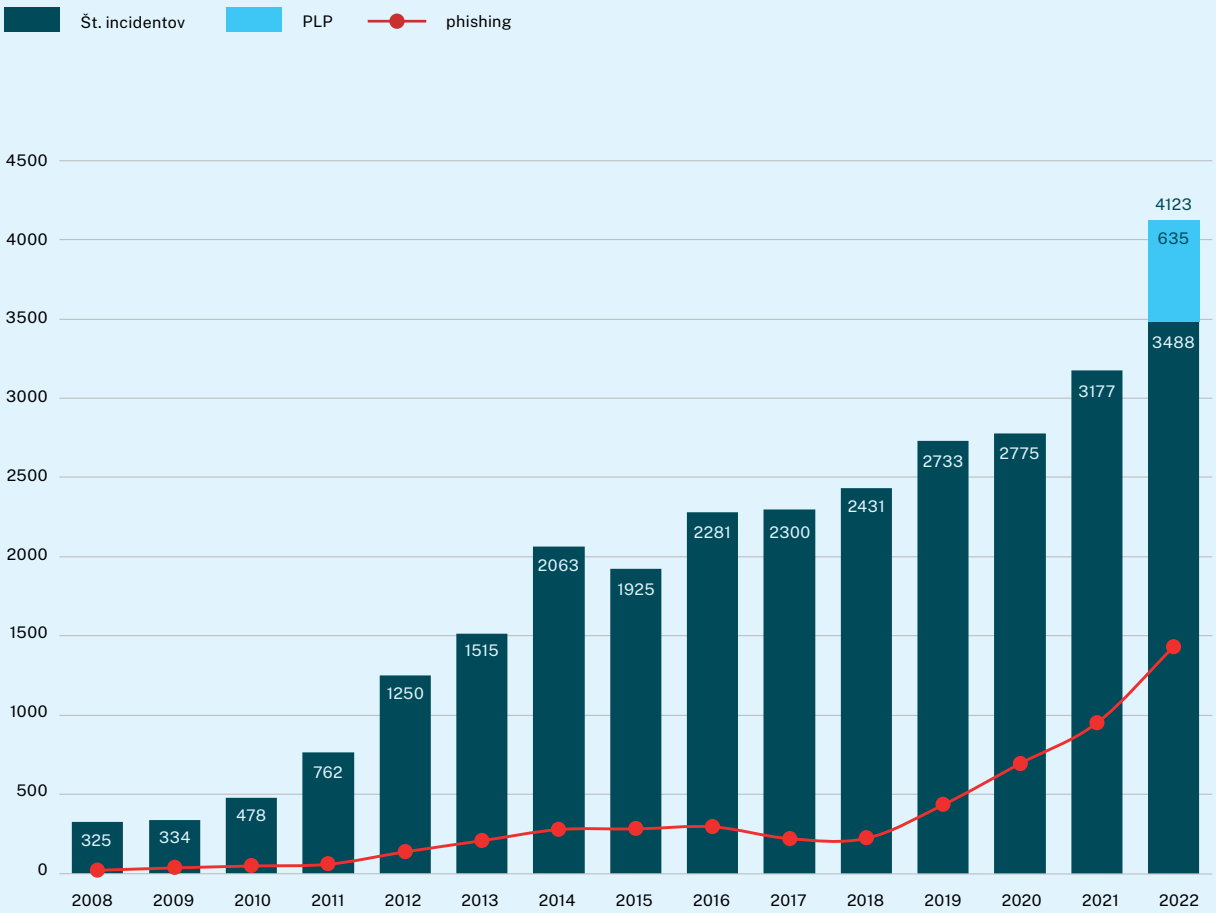
- izvajalce bistvenih storitev, kot jih opredeljuje ZInfV,
- operaterje elektronskih komunikacij,
- državne organe, z vlogo zagotavljanja kibernetske varnosti,
- banke.

Vsem izvajalcem bistvenih storitev SI-CERT omogoča brezplačen priklop v skupnost MISP ter s tem dostop do regionalnih dogodkov in tistih, ki jih zaznajo tuji partnerji. S priklopom pridobijo brezplačen dostop do širokega nabora indikatorjev zlorab, ki jih lahko uporabijo za iskanje korelacij znotraj sistema SIEM ali pa zgolj kot dodatna pravila na požarni pregradi ali obogatitev filtrov poštnega strežnika.

2. VRSTE, ŠTEVILO INCIDENTOV IN KLJUČNI KAZALCI

Število incidentov v letih 2008–2022, s poudarkom na phishing prevarah.

Iz grafa je razvidno število incidentov, ki jih je obravnavala prvolinijska pomoč.



Vrste in število incidentov v obdobju 2019–2022

V tabeli Razvrstitev incidentov je razviden velik upad novinarskih vprašanj, ki pa je samo navidezen in je posledica tega, da smo v začetku leta 2021 spremenili njihovo obravnavo: uvedli smo naslov press@cert.si in ločeno linijo za odgovore. Skupaj smo (vključno z zgoraj navedenim) **v letu 2022 prejeli 133 novinarskih vprašanj**.

Skupina	Vrsta incidenta	2019	2020	2021	2022
Neprimerna vsebina	neželena sporočila	57	72	120	97
	žaljiva vsebina	9	22	13	9
	nasilna vsebina	1	3	0	1
Zlonamerna koda	virus	53	46	29	8
	črv	0	0	2	0
	trojanski konj	166	141	171	278
	vohunska programska oprema	3	1	2	2
	samodejni izbirnik (ang. dialler)	0	0	0	0
	korenski komplet (ang. rootkit)	0	1	0	0
	boti in botneti	17	16	9	8
	nadzorni strežnik	6	7	0	1
	izsiljevalski virus	53	69	64	45
	orodje za oddaljeni nadzor (RAT)	6	14	29	33

Skupina	Vrsta incidenta	2019	2020	2021	2022
Zbiranje informacij	odkrivanje potencialnih tarč in ranljivosti (skeniranje)	33	28	41	42
	prestrezanje komunikacije	5	1	1	0
	socialni inženiring	2	2	0	3
Poskusi vdora	izkoriščanje znane ranljivosti	5	4	1	3
	poskusi prijav, napad z grobo silo (ang. brute force attack) in napadi s slovarjem	46	16	32	18
	nova vrsta napada	0	0	0	0
Vdori	zloraba privilegiranega uporabniškega računa	6	7	6	0
	zloraba neprivilegiranega uporabniškega računa	35	82	105	112
	napad na aplikacijo	4	4	5	6
Razpoložljivost	napad onemogočanja	2	7	6	5
	porazdeljen napad onemogočanja	31	31	27	17
	sabotaža	4	0	0	0
	izpad delovanja naprav ali omrežja	3	2	4	1
Varnost informacijskih virov	nepooblaščen dostop do podatkov	15	13	12	8
	nepooblaščeno spreminjanje podatkov	5	8	22	15
	odtekanje informacij	4	5	6	5
Goljufije	nepooblaščeno izkoriščanje virov	8	4	5	6
	intelektualna lastnina in avtorske pravice	13	10	10	12
	kraja identitete	96	67	68	48
	phishing sporočilo	301	488	765	1221

Skupina	Vrsta incidenta	2019	2020	2021	2022
Goljufije	phishing spletno mesto	134	202	185	211
	spletno nakupovanje	164	97	86	113
	goljufija z vnaprejšnjim plačilom	149	168	182	181
	izsiljevanje	291	144	138	346
	druge goljufije	684	668	655	762
Ranljivosti	odgovorno razkrivanje	25	14	12	4
	razkritje ranljivosti	1	2	12	53
	ranljivi sistemi in naprave	24	20	33	15
Drugo	drugo	243	226	301	320
	novinarsko vprašanje	17	53	9	1
Test	namenjeno preizkusom	3	1	1	1
Skupaj		2724	2766	3169	4011
Nerazvrščenih		9	9	8	112
Vseh primerov skupaj		2733	2775	3177	4123

Opomba: Pri primerih, ki jih je obravnavala PLP, je bilo naknadno uvedeno določanje vrste incidenta, zato je vidno veliko število nerazvrščenih incidentov.

Ali je število incidentov primerljivo s številom dogodkov v sistemu za upravljanje varnostnih informacij in dogodkov (SIEM)?

V centru SI-CERT razvrščamo incidente na osnovi referenčne taksonomije, ki jo je predpisala agencija ENISA. Taksonomijo smo dopolnili z nekaterimi vrstami zlorab, s katerimi se prvenstveno srečujemo pri ozaveščanju javnosti. Tovrstno razvrščanje ni primerljivo s številom dogodkov oz. dnevniškimi zapisi iz sistemov SIEM.

STATISTIKA OŠKODOVANJ

Ob prijavi incidenta lahko prijavitelj prostovoljno sporoči tudi finančno škodo, ki jo je utrpel zaradi incidenta. Žrtve napadov z izsiljevalskim virusom pogosto denimo ne želijo razkriti višine zahtevane odkupnine za podatke. Ker tako SI-CERT ne razpolaga z vsemi oškodovanji (kot je to pri prijavi suma kaznivega dejanja policiji), teh podatkov ne moremo vedno jemati kot statistično relevantnih. Vseeno pa z njimi dobimo dober uvid v razpon oškodovanj pri določenih incidentih.

Oškodovanje	Opis
najvišja oškodovanja	
3.000.000 EUR	Najvišji znesek, na srečo neuspešnega, oškodovanja v letu 2022 (šlo je za vrivanje v poslovno komunikacijo, ang. business email compromise oz. BEC fraud) – prenos denarja je bil pravočasno zaustavljen zaradi nadzornih mehanizmov bank in Urada RS za preprečevanje pranja denarja.
400.000 EUR	Najvišje oškodovanje fizične osebe (izsiljevanje z lažnimi grožnjami o pregonu).
povprečna oškodovanja	
58.000 EUR	Povprečno oškodovanje v nigerijski prevari (vnaprejšnje plačilo).
31.000 EUR	Povprečno oškodovanje v ljubezenski prevari.
19.000 EUR	Povprečno oškodovanje zaradi lažne tehnične pomoči Microsofta.
3.400 EUR	Povprečno oškodovanje pri phishing napadu (zloraba kreditne kartice).
780 EUR	Povprečno oškodovanje pri spletnem nakupovanju.

3. POMEMBNEJŠI INCIDENTI IN OPAŽANJA

VOJNA V UKRAJINI – KO KIBERNETSKO BOJEVANJE PRESTOPI GEOGRAFSKE MEJE

Konec januarja 2022 je mreža CSIRT, katere član je tudi SI-CERT, prešla v višjo stopnjo pripravljenosti. Že mesec dni pred začetkom spopadov so namreč različni dogodki na internetu kazali na povečano dejavnost na področju Ukrajine. Neposredno pred vojaško invazijo smo lahko spremljali napade onemogočanja (DDoS) na spletna mesta organov državne uprave Ukrajine, banke in medije v tej državi. Na več sto sistemov v Ukrajini so bili predhodno nameščeni destruktivni virusi (t. i. wipers), ki na videz delujejo kot izsiljevalski virus (kar zelo spominja na napada WannaCry in NotPetya iz leta 2017). Uničenje podatkov je bilo sproženo neposredno pred vojaško invazijo.

Po začetku vojaških operacij je bil izdan poziv podpredsednika ukrajinske vlade Mihajla Fedorova, da oblikujejo t. i. IT Army, v katero vabijo strokovnjake za kibernetsko varnost, koordinacija pa naj bi potekala po kanalu aplikacije za hipno sporočanje Telegram. Na drugi strani se je najopazneje v podporo ruski vladi oglasila kiberkriminalna skupina Conti4, znana po izvedbi napadov z izsiljevalskimi virusi. Pozneje je bila največ medijske pozornosti deležna hektivistična skupina **KillNet**, ki je objavljala nove in nove sezname tarč za napade onemogočanja.

SI-CERT je podal oceno stanja in priporočila (prvo poročilo je bilo izdano 3. marca 2022, zadnje 3. maja 2023) Uradu Vlade Republike Slovenije za informacijsko varnost, vsem izvajalcem bistvenih storitev po Zakonu o informacijski varnosti, operaterjem elektronskih komunikacij (prek

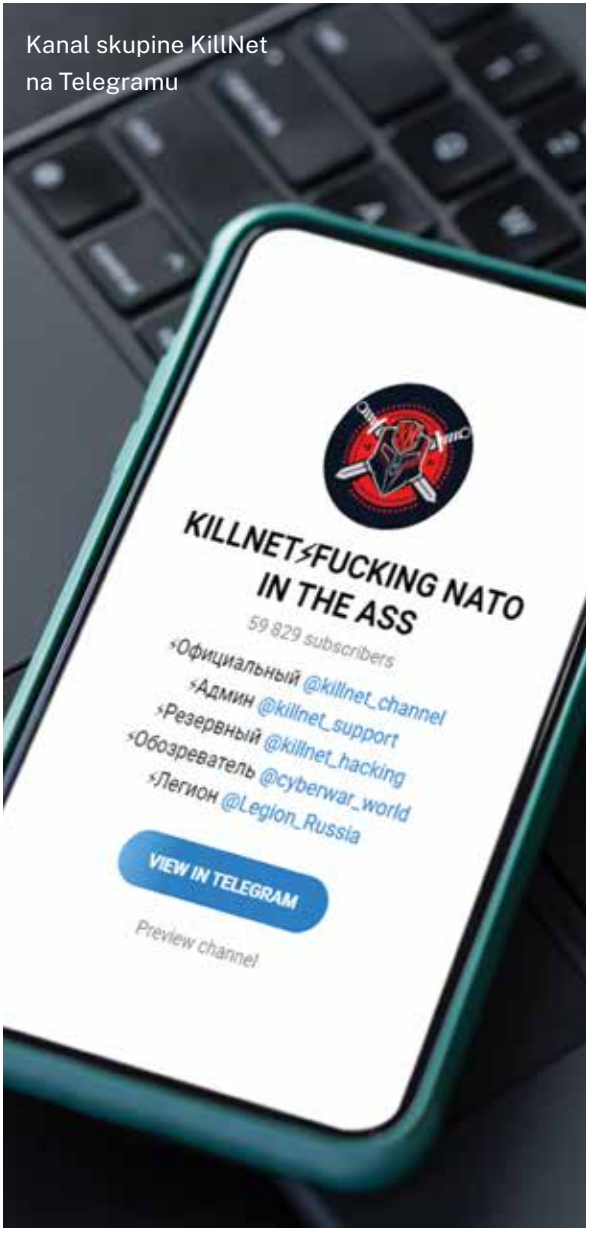
Agencije za komunikacijska omrežja in storitve AKOS) in članicam Združenja bank Slovenije. Poročila so vsebovala trenutno oceno ogroženosti na osnovi podatkov SI-CERT in izmenjave v mreži CSIRT, možne vrste pričakovanih napadov in priporočene ukrepe.

STANJE V SLOVENIJI

Razen posamičnih napadov onemogočanja, ki bi jih morda lahko povezali z vojno v Ukrajini (vendar tega ni bilo mogoče potrditi), in redkih poskusov podtikanja zlonamerne kode večjih dejavnosti na območju kibernetskega prostora, ki ga pokriva SI-CERT, nismo opazili. Podobno je bilo opažanje tudi pri več drugih članicah EU, z izjemo baltskih republik, Poljske in Finske ter občasno tudi Slovaške. Te države imajo pri podpori Ukrajine vidnejšo vlogo, zato so tudi pogosteje tarča povezanih kibernetskih napadov.

DEZINFORMACIJE IN PROPAGANDA

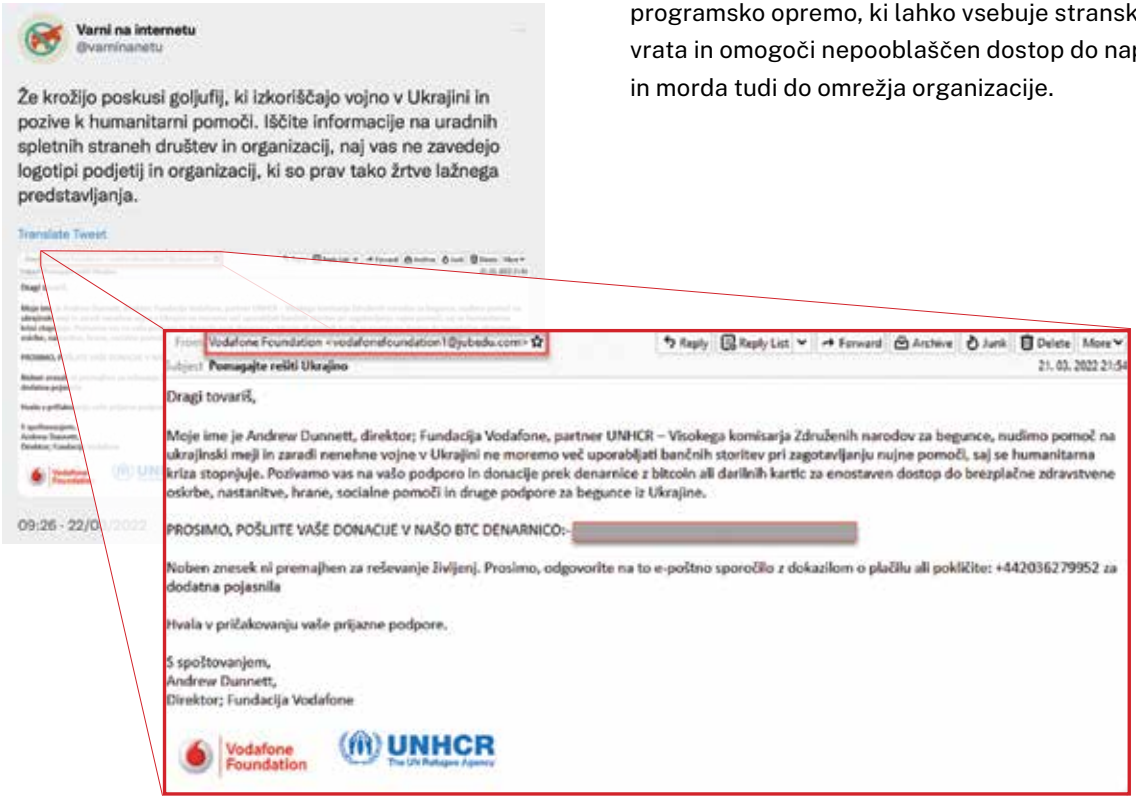
Veliko informacij na internetu, zlasti na družbenih omrežjih, se je pozneje izkazalo za neresnične. Dezinformacije so v vojni uporabljene kot eno od sredstev za doseganje ciljev, zato smo opozorili na previdnost pri obravnavi podatkov, ki se nanašajo na stanje v kibernetskem prostoru in razglašene uspehe kibernetskih napadov. Preverjanje teh informacij pogosto ni preprosto.



Kanal skupine KillNet na Telegramu

IZRABA VOJNEGA STANJA ZA IZVEDBO SPLETNIH GOLJUFIJ

Kot smo napovedali, se je vojna v Ukrajini uporabila tudi v nekaterih poskusih spletnih goljufij, kar ne preseneča, saj goljufi izrabljajo vse izredne dogodke – vojne, naravne nesreče, pandemijo covida-19 itd. – za poskuse oškodovanja posameznikov in podjetij.



NAPADI ONEMOGOČANJA

Opozorili smo tudi na problematičnost sodelovanja posameznikov v napadih, če bi se ti pridružili kateri od hektivističnih skupin, še zlasti kadar bi bile uporabljene službene naprave in službena omrežja. Za izvedbo omenjenih napadov hektivističnih skupin se pogosto uporabljajo orodja, ki jih morajo posamezniki namestiti v svoje naprave (v nekaterih primerih pa z obiskom spletne strani, prek katere se v brskalniku izvede ustrezna programska koda javascript). Gre za tujo programsko opremo, ki lahko vsebuje stranska vrata in omogoči nepooblaščen dostop do naprave in morda tudi do omrežja organizacije.

OBVEŠČANJE O RANLJIVOSTIH

Ranljivost je niz različnih pogojev, ki omogočajo kršitev varnostne politike. Gre za pomanjkljivosti v informacijskem sistemu, aplikacijah, omrežnih napravah, varnostnih postopkih sistema, notranjem nadzoru ali izvajanju postopkov, ki so lahko predmet izkoriščanja ali zlorabe. Ranljivost lahko povzročijo napake v programski opremi, napačna konfiguracija ali nepričakovane interakcije med različnimi sistemi. Uspešno izkoriščanje ranljivosti ima lahko za posledico tehnična tveganja in tudi tveganja, ki lahko ogrozijo celoten sistem. Skoraj celotna panoga proizvajalcev digitalnih rešitev je sprejela model odgovornega ali koordiniranega razkrivanja ranljivosti, s katerim se zmanjša škodljiv vpliv ranljivosti na prizadete uporabnike. Med razkrivanjem informacij o varnostnih ranljivostih različni deležniki včasih sledijo nepisanim pravilom ali neformalnim smernicam o medsebojnem povezovanju in izmenjavi informacij.

SI-CERT ob koordinaciji razreševanja incidentov ter 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 v elektronskih omrežjih. Skrbnike sistemov in uporabnike o znanih ranljivostih in drugih zlorabah obvestimo neposredno, ob pomoči ponudnikov gostovanja ali operaterjev elektronskih komunikacij.

Objavljena varnostna obvestila v letu 2022

SI-CERT 2022-01
Kibernetski napadi, povezani z vojno v Ukrajini

SI-CERT 2022-02
Ranljivost MSDT (Microsoft Support Diagnostic Tool)

SI-CERT 2022-03
Več ranljivosti v produktih podjetja Siemens

SI-CERT 2022-04
Ranljivost strežnika Microsoft Exchange

SI-CERT 2022-05
Ranljivosti knjižnice OpenSSL 3

SI-CERT 2022-06
Ranljivost FortiOS SSL-VPN

SI-CERT 2022-07
Ranljivost Citrix ADC in Citrix Gateway

ZLONAMERNA KODA

PREGLED OBRAVNAVANE ZLONAMERNE KODE

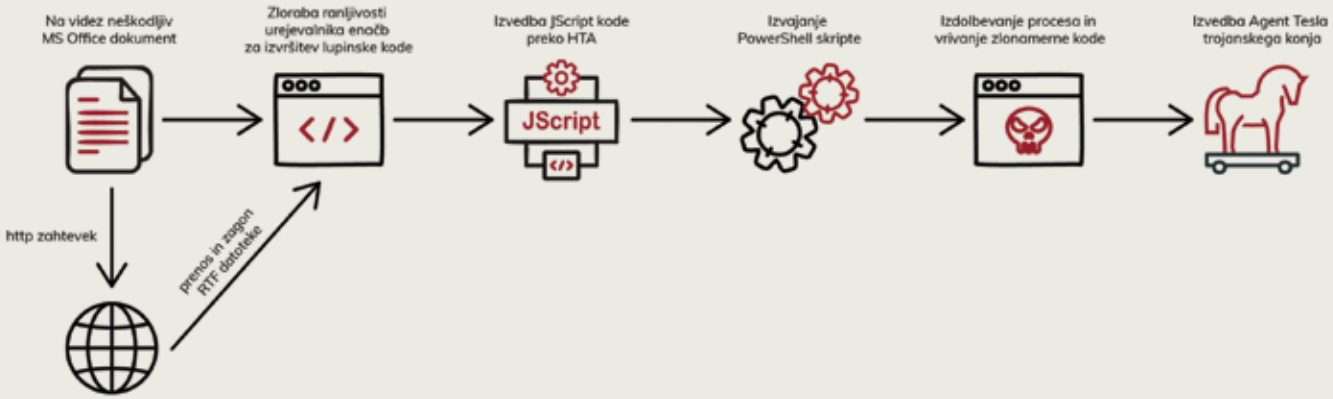
Na področju zlonamerne kode leto 2022 ni prineslo večjih sprememb. Še vedno smo se največkrat ukvarjali z različnimi trojanskimi konji, izsiljevalskimi kriptovirusi in orodji za oddaljeni dostop. Pri trojanskih konjih so prednjačile različice FormBooka (nekateri ga označujejo tudi kot xLoader) in AgentTesle. Sledi jima Emotet s sestrskim QBotom, ki kljub onesposobitvi infrastrukture s strani organov pregona leta 2021 še vedno prihaja v občasnih valovih. Trojanski konji se najpogosteje širijo v obliki priponk elektronske pošte s sporočili, ki želijo naslovnika prepričati, da nanjo klikne in s tem nevede v računalnik namesti zlonamerno kodo. Lažna sporočila, tudi s pomočjo orodij umetne inteligence, postajajo čedalje prepričljivejša, lahko vsebujejo elemente pretekle (legitimne) korespondence, z različnimi tehnikami pa tudi preslepijo filtre poštnih strežnikov. Taka lažna sporočila običajno predstavljajo prvi korak pri nepooblaščenem dostopu do omrežja podjetja skozi okužbo računalnika enega od zaposlenih. Proces okužbe praviloma vsebuje več stopenj, od prenosa dodatne kode iz oddaljenega strežnika do izvedbe različnih vmesnih skript.

Večina trojanskih konjev spada v kategorijo t. i. infostealerjev. V prvi fazi po zagonu ukradejo vse avtentikacijske elemente v sistemu (shranjena gesla, poverilnice VPN, kriptodenarnice itd.). V nadaljevanju storilci to izkoristijo za lateralno širjenje po omrežju, pridobitev administratorskih pravic, onemogočanje varnostnih aplikacij (protivirusni programi ipd.) ter v končni fazi zagon izsiljevalskih virusov.

Vrste zlonamerne kode v letu 2022, ki jih je obravnaval SI-CERT

Vrsta	Število
Virus	8
Trojanski konj	278
Vohunska programska oprema	2
Boti in botneti	9
Izsiljevalski virus	45
Orodje za oddaljeni dostop (RAT)	33

Grafični prikaz večstopenjskega procesa okužbe računalnika



Vrste trojanskih konjev, ki jih je v letu 2022 obravnaval SI-CERT

Vrsta	Število
Agent Tesla	67
FormBook/xLoader	90
Emotet/QBot	40
Lokibot	9
Drugo	72

Vrste orodij za oddaljeni dostop, ki jih je v letu 2022 obravnaval SI-CERT

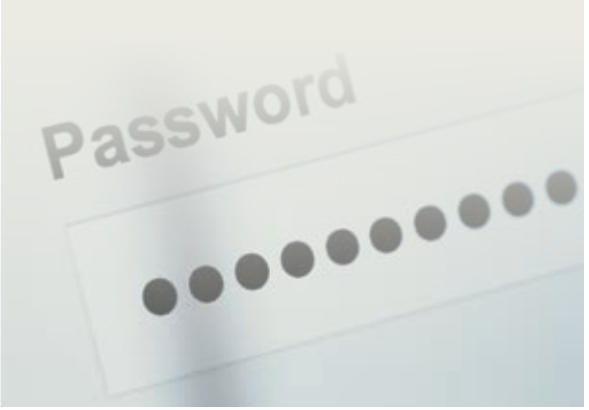
Orodje	Število
Remcos	12
NanoCore	5
SystemBC	3
Guloader	5
Drugo	8

AgentTesla in FormBook skozi leta

Leto	AgentTesla	FormBook/xLoader
2019	1	1
2020	4	4
2021	33	39
2022	67	90

Zgodovina FormBooka sega v leto 2016. Temelji na poslovnem modelu malware-as-a-service (MaaS), pri katerem avtorji virusa sami ne izvajajo napadov, ampak zgolj prodajo binarno kodo in dostop do nadzornih strežnikov (ang. command and control, tudi C&C oz. C2). FormBook je priljubljenost pridobil zlasti zaradi nizke cene. Napadalci po nakupu storitve na črnem trgu običajno najamejo še različne storitve za distribucijo, pri čemer lahko z napadom ciljajo na posamezno državo ali organizacijo. Običajno se širi v priponkah elektronskih sporočil v dokumentih MS Office (.rtf, .doc, .xls), ki vsebujejo škodljive makre ali kodo, ki izrablja različne ranljivosti. Po zagonu svojo kodo injicira v različne legitimne procese, beleži pritiske na tipke, spremlja vsebino odložišča in vsebino sej http, zajema posnetke zaslona, v nadzorni strežnik napadalca pošlje shranjena gesla iz spletnih brskalnikov in aplikacij za elektronsko pošto ter izvaja dodatne škodljive kode v skladu z ukazi, ki jih prejema iz nadzornega strežnika. Avtor FormBooka je leta 2020 ustavil prodajo, vendar se je kmalu spet pojavil, takrat z imenom xLoader, ki ima sposobnost delovanja tudi v operacijskem sistemu macOS. V centru SI-CERT v letu 2022 sicer nismo obravnavali nobenega primera zlorabe sistema macOS s tem virusom.

Proti koncu leta 2022 smo obravnavali več primerov okužb sistemov s programi za goljufanje v igrah in razbijanje zaščit licenčne programske opreme (t. i. cracki). Virus je takoj po zagonu napadalcem poslal shranjena gesla za elektronsko pošto in posnetek zaslona. Uporabniki so pozneje prejeli izsiljevalsko sporočilo s svojimi gesli in posnetkom zaslona ter sporočilom z grožnjo po objavi intimnih posnetkov in zahtevo za plačilo okoli 1000 evrov v kriptovaluti.



IZSILJEVALSKI KRIPTOVIRUSI – RANSOMWARE

Prevladujoči trend odmika napadov z izsiljevalskimi virusi od individualnih uporabnikov k bolj dobičkonosnim napadom na podjetja je bilo zaznati tudi v letu 2022. Poglavitni vstopni vektorji še vedno ostajajo škodljive priponke, neprimerno zaščiten oddaljeni dostop ali izkoriščanje znanih ranljivosti omrežnih naprav. Prav slednje je v začetku leta 2022 bilo vzrok za globalno širjenje izsiljevalskega virusa DeadBolt, ki je ciljal na priljubljene naprave za lastno oblačno/omrežno shranjevanje proizvajalca QNAP. Virus se je z izrabo novoodkritih ranljivosti naprav QNAP NAS v več valovih širil praktično vse leto.

V Sloveniji se je v začetku februarja zgodil medijsko precej odmeven incident, povezan z izsiljevalskim virusom. Napadalci so namreč izvedli uspešen napad na našo največjo komercialno televizijo POP TV. Posledica reševanja težav in odprave posledic je bilo obdobje, ko je televizija imela opazno okrnjene programske in tudi spletne vsebine, prišlo pa je tudi do odtekanja podatkov, kar seveda ni ostalo neopaženo.

Vpogled v ustroj in delovanje tovrstnih napadov ter kriminalnih združb, ki stojijo za njimi, smo imeli priložnost spoznati kmalu za tem. V kontekstu burnega geopolitičnega dogajanja (tragična vojna v Ukrajini) so se namreč na spletu pojavili t. i. Conti leaks, tj. vsebina interne komunikacije, datotek, načrtov ter tudi šifrirnih ključev ruske izsiljevalske skupine (operaterjev virusa) z imenom Conti. Strokovna javnost je tako dobila možnost resnično podrobnega vpogleda v način delovanja tovrstnih skupin, saj so prepisi internih pogovorov pokazali praktično vse: od kadrovanja članov, plačnega sistema, načina razvoja zlonamerne programske opreme in strategije poteka pogajanj z žrtvami do ne nazadnje povezav tovrstnih skupin z državnimi (ruskimi) obveščevalnimi strukturami.

NAPADI NA PODJETJA

Napadi na podjetja se nadaljujejo. Pogosta tarča kibernetskih napadov so mala in srednje velika podjetja, saj ta velikokrat nimajo možnosti zagotavljanja zadostnih virov za povečevanje odpornosti na kibernetska tveganja. Hkrati je njihovo celotno poslovanje zelo odvisno od nemotenega delovanja informacijskih sistemov. Ob uspešni izvedbi kibernetskega napada se lahko poslovanje podjetja popolnoma ustavi za daljše časovno obdobje, kar pomeni izredno velike izgube.

Podjetja so zelo izpostavljena napadom z izsiljevalskimi virusi, ki po vdoru v informacijski sistem zašifrirajo vse dosegljive datoteke. Napadalci žrtvam ponudijo možnost odkupa šifrirnega ključa, pri čemer znesek odkupnine prilagodijo velikosti podjetja. Običajni zneski odkupnine so od nekaj 10.000 EUR do več milijonov evrov.

V 78 % vseh obravnavanih incidentov z izsiljevalskimi virusi je bil tarča napada poslovni subjekt.

Direktorska prevara (ang. CEO fraud) je preprosta oblika napada, pri kateri napadalci na različne načine prevzamejo identiteto člana vodstvenega kadra (običajno direktorja) ter v njegovem imenu od drugih zaposlenih zahtevajo izvedbo določenih nalog, ki pa so v škodo podjetja. Značilen primer direktorske prevare je pošiljanje elektronskega sporočila na naslov računovodstva z zahtevo po nujnem plačilu fiktivne fakture na nek tuj bančni račun. Napadalci pri tem registrirajo elektronski naslov, ki vsebuje ime in priimek direktorja, ali pa pri pošiljanju sporočila ponaredijo pošiljatelja

Najvišji zabeleženi znesek preusmerjenega nakazila v letu 2022 iz kategorije napadov BEC je bil 3.000.000 evrov. Na srečo je bil prenos denarja zaradi nadzornih mehanizmov bank in Urada RS za preprečevanje pranja denarja pravočasno zaustavljen.

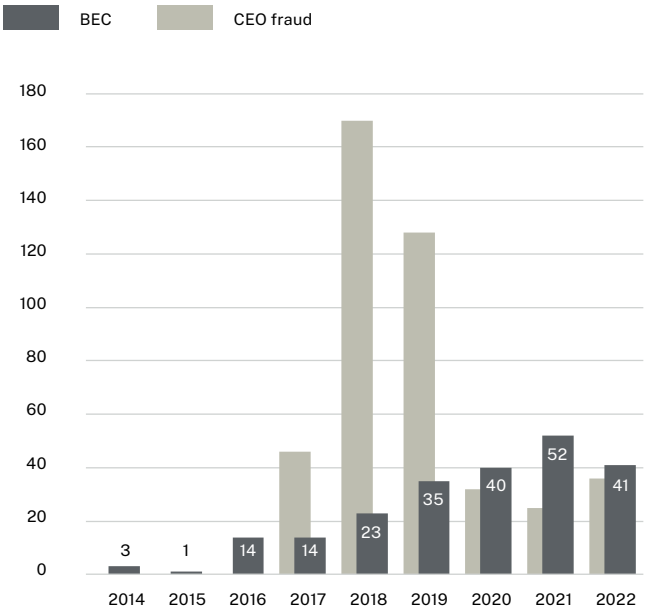
(t. i. email spoofing). Naprednejši napadi te vrste lahko vsebujejo tudi avdio- in videoposnetke, ustvarjene z orodji umetne inteligence.

Vrhunec teh napadov smo zaznali leta 2018, ko je v mnogih primerih prišlo tudi do oškodovanj. Zadnja leta je, zlasti zaradi pogostega opozarjanja v medijih in boljše obveščenosti zaposlenih v finančnih in IT-službah, tovrstnih uspešnih napadov precej manj.

Vrivanje v poslovno komunikacijo (ang. BEC, business email compromise) je naprednejša oblika kibernetskega napada, ki zahteva predhodni vdor v poštni sistem podjetja. Ta je običajno posledica uspešnega phishing napada na zaposlene. Z vdorom v poštni predal napadalci spremljajo komunikacijo v podjetju in ob pošiljanju fakture v njej zamenjajo podatek o bančnem računu in tako preusmerijo nakazilo denarja. Zneski oškodovanja so praviloma zelo visoki.

Vsako spremembo bančnih podatkov poslovnega partnerja vedno dodatno preverite po neodvisnem kanalu (osebno, po telefonu ipd.).

Primerjava števila prevar z vrivanjem v komunikacijo in direktorskih prevar skozi čas



leto	BEC	CEO fraud
2014	3	
2015	1	
2016	14	
2017	14	46
2018	23	170
2019	35	128
2020	40	32
2021	52	25
2022	41	36

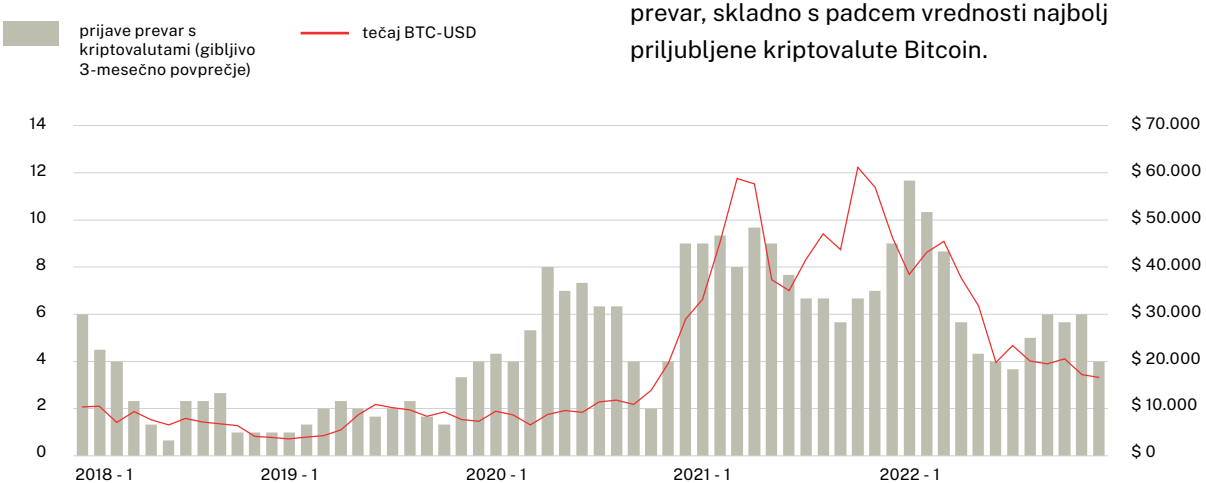
SPLETNE GOLJUFIJE

INVESTICIJSKE KRIPTOPREVARE DOBIJO ŠE DODATEN ZAPLET

Investicijske prevare ostajajo stalnica obravnavanih spletnih goljufij. Modus operandi tovrstnih prevar ostaja še vedno isti: začetni minimalni vložki, ki na lažnih portalih narastejo do neverjetnih zneskov. Zaplete se seveda pri izplačilu, ki je pogojevano z vedno novimi izmišljenimi davki ali stroški, vse zgolj z namenom dodatnega finančnega izčrpavanja žrtve. Temu se pridružuje tudi opazen porast prijav incidentov, kjer (lažna) podjetja nagovarjajo žrtve tovrstnih prevar in jim obljubljajo povrnitev vloženih finančnih sredstev.

Leto 2022 je bilo polno nihanj vrednosti kriptovalut. Posledično smo, kljub razmeroma majhnemu vzorcu, opazili trend zmanjšanja prijav tovrstnih prevar, skladno s padcem vrednosti najbolj priljubljene kriptovalute Bitcoin.

Primerjava števila prijav prevar s kriptovalutami in mesečnega povprečja tečaja Bitcoina



OGLAŠEVANJE SPLETNIH GOLJUFIJ – OBIČAJNA POSLOVNA PRAKSA?

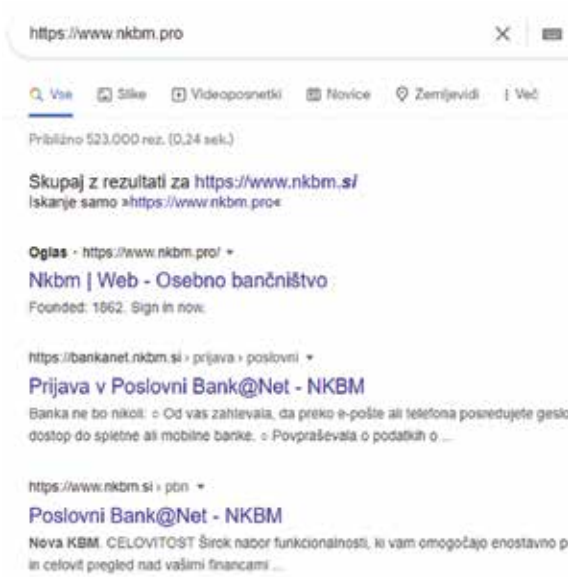
Vsako novo tehnologijo, spletno storitev ali vsaj funkcionalnost slej kot prej izkoristijo napadalci. Zato ne presenečajo goljufive kriptosheme ali zlonamerne razširitve ChatGPT za brskalnik, ki napadalcu omogočijo prestrezanje gesel. Goljufi sledijo trendom in tehnološkemu razvoju, izkoriščajo trenutno pozornost uporabnikov in jo preusmerjajo v svoj lasten posel. Podobno je tudi z digitalnimi oglaševalskimi platformami, ki so jih spletni napadalci popolnoma usvojili in so, če karikiramo, postale že del običajne poslovne prakse.

Uporaba (oz. natančneje zloraba) legitimnih oglaševalskih orodij za zvabljanje uporabnikov v različne spletne prevare ni novost leta 2022. Presenetljivo pa je, kako pogosto smo v preteklem letu zaznali tovrstne oglase, kako dobro so ciljali uporabnike in kako malo vzvodov je na voljo, da bi se zaščitili tako spletni uporabniki, ki so nasedli prevari, kot tudi posamezniki, katerih identiteta je zlorabljena v takšnih oglasih. Najočitnejši so bili oglasi za goljufive kriptosheme, ki se prek široko razpredenih oglaševalskih mrež umeščajo na različne spletne strani in medijske portale, med njimi so tudi številni slovenski.

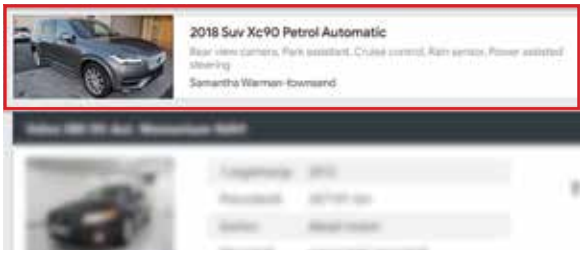
Na več inšpekcijskih služb smo naslovili problematiko oglaševanja in zvabljanja obiskovalcev slovenskih medijskih portalov v različne goljufive kriptosheme in tudi oglaševanja dvomljivih prehranskih dodatkov in zdravil, kjer so zlorabili identiteto slovenskih zdravnikov. Vprašanji, kdo je odgovoren za tovrstne, očitno škodljive in zavajajoče oglase (oglaševalec, oglaševalska mreža ali ponudnik oglasnega prostora) in kdo je pristojen za sankcioniranje kršitev, ostajata neodgovorjeni. Pristojnosti nadzornih organov so omejene, saj naročniki oglasov niso podjetja s sedežem v Sloveniji. Oglaševalske mreže prav tako ne, hkrati pa celotno odgovornost za vsebino oglasov prelagajo izključno na naročnika oz. oglaševalca.

Podoben odziv je tudi pri ponudnikih medijskega prostora, ki prav tako ne odgovarjajo za vsebino oglasov, ki se pojavljajo v njihovem inventarju. Začarani krog je sklenjen in ostane nam zgolj čakanje na implementacijo Akta o digitalnih storitvah, ki bo razmejil odgovornosti, določil pristojne organe za nadzor in tudi definiral postopke, kako sankcionirati kršitve.

Na podoben način napadalci zlorabljajo tudi oglase Googla in Facebooka. Obravnavali smo primer uporabe oglaševalske storitve Google Ads, kjer so napadalci zakupili iskalni pojem, ki je vodil na phishing spletno stran, namenjeno kraji prijavnih podatkov bančnih komitentov. Vložek v oglaševanje je najverjetneje ničen, saj gre za zlorabljene kreditne kartice.



Na podoben način so oglaševali tudi lažno spletno trgovino z avtomobili. Na znanem avtomobilističnem portalu so bili umeščeni oglasi, ki so vodili neposredno na spletno mesto, ki so ga postavili napadalci. To je primer kontekstualno zelo dobro umeščenega oglasa, ki natančno cilja uporabnike, ki že iščejo rabljeno vozilo, hkrati pa ima obiskovalec, ki oglas vidi na poznanem spletnem mestu, še dodaten občutek zaupanja.



Uporaba digitalnih oglaševalskih orodij tako napadalcem omogoča doseg večjih množic in natančno ciljanje glede na interese, kar je ključno za uspešen napad z družbenim inženiringom. Oglasi tudi vzbujajo občutek, da na drugi strani stoji legitimno podjetje. Čeprav uporabniki vedno manj verjamemo obljubam oglaševalcev, še vedno zaupamo, da je vsaj naročnik oglasa resnično podjetje in da obstajajo določene varovalke, da ne bomo kliknili neposredno na spletno prevaro. Varovalk očitno ni, vse, kar napadalci potrebujejo, je kreditna kartica in malo marketinških veščin.

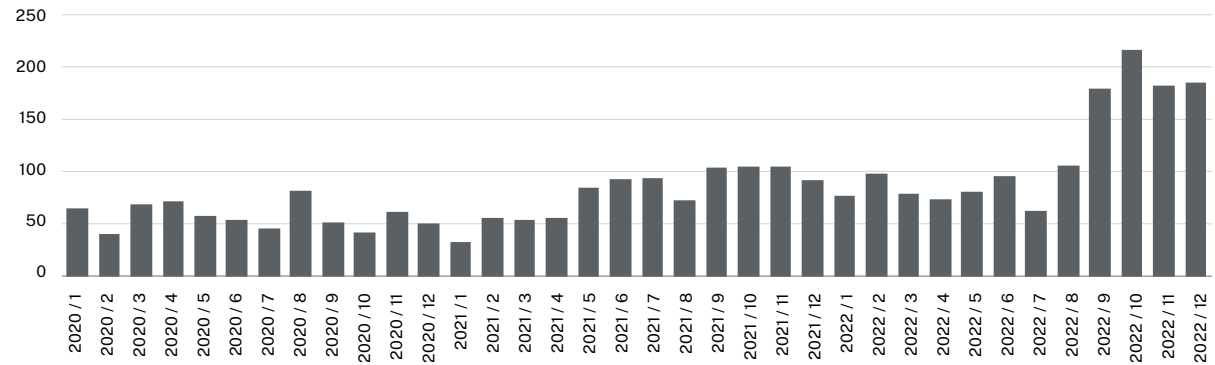
PHISHING NAPADI NE POJENJAJO

Phishing ali ribarjenje za podatki je vrsta napada z lažnim predstavljanjem, najpogosteje v elektronskih sporočilih, ki poskušajo prejemnika prepričati v razkritje občutljivih podatkov. Najpogostejši cilji napadov so gesla za elektronsko pošto, prijavni podatki za spletne banke in podatki o kreditnih karticah. Phishing sporočilo prejemnika nagovarja h kliku na povezavo v sporočilu, običajno pod krinko nekega nepredvidenega dogodka, ki zahteva hitro ukrepanje. Povezava vodi na potvorjeno spletno stran, ki zahteva vpis uporabniškega imena, gesla in drugih osebnih podatkov. Sporočilo in spletna stran po navadi vsebujeta grafične elemente in posnemata podobo ciljane storitve.

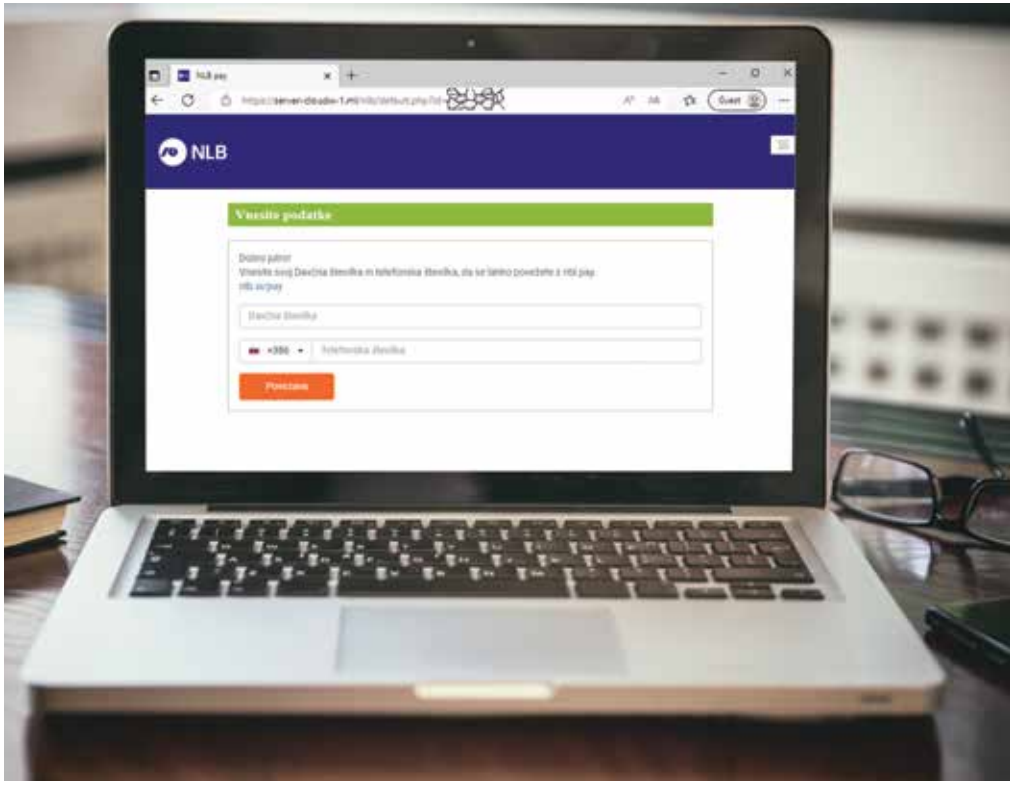
Nekatere organizacije med phishing uvrščajo tudi druge vrste napadov, npr. elektronsko sporočilo z okuženo priponko ali vabe v SMS-klube, v centru SI-CERT in večini drugih sorodnih organizacij pa je kategorija phishing incidentov omejena zgolj na neposreden poskus kraje osebnih podatkov ali poverilnic.

V letu 2022 smo v centru SI-CERT obravnavali 1432 phishing incidentov. V največ primerih je vektor napada elektronska pošta, čedalje bolj pa so v porastu phishing napadi s sporočili SMS in drugimi zasebnimi sporočili.

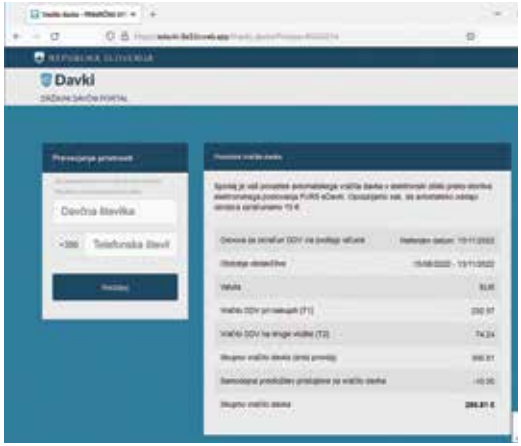
Phishing incidenti po mesecih od 2020 do 2022



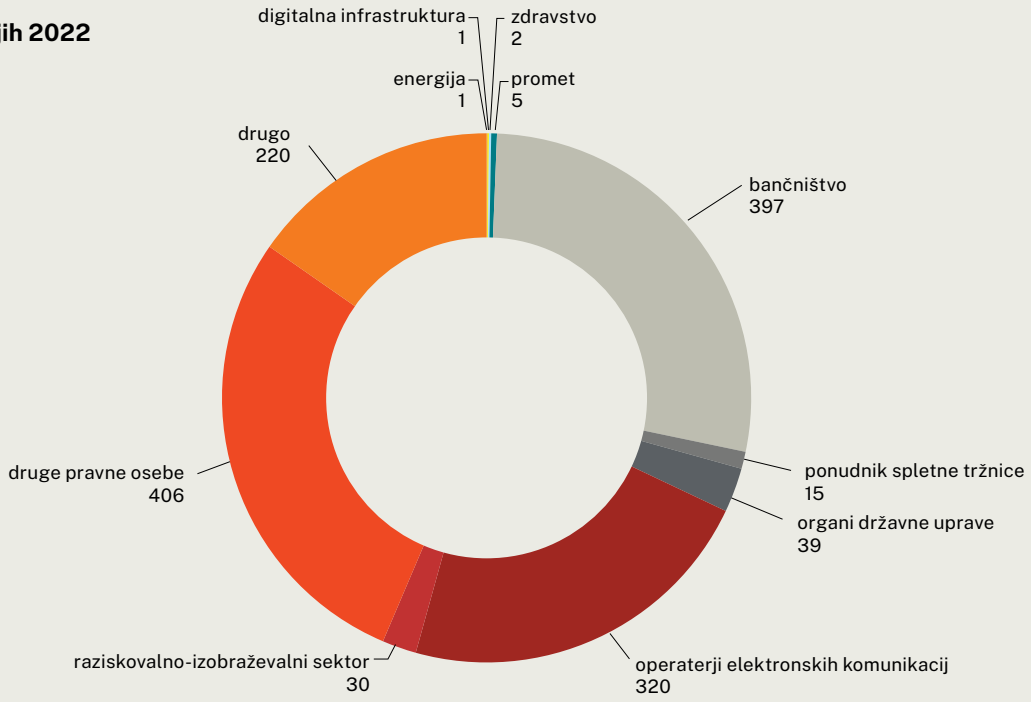
Konec avgusta se je začel zelo obsežen val phishing napadov na komitente različnih slovenskih bank, katerih cilj je bil pridobiti avtentikacijske podatke za aktiviranje mobilne denarnice. Trajal je vse do začetka leta 2023. Val teh napadov je bil tako obsežen, da smo v povprečju vsak dan obravnavali približno šest različnih napadov te vrste, v konicah pa tudi več kot 15 dnevno.



Napadi so potekali po elektronski pošti in sporočilih SMS, tudi v imenu Finančne uprave Republike Slovenije pod krinko vračila davka. Phishing spletne strani so zahtevale vpis telefonske številke, davčne številke, enkratne kode iz sporočila SMS ter številke PIN bančne kartice. S temi podatki so lahko napadalci v imenu žrtve na svojem telefonu aktivirali mobilno denarnico ter prek nje opravljali različne spletne nakupe.



Phishing po sektorjih 2022



Ob zaznavi phishing napada v centru SI-CERT izvedemo različne ukrepe, s katerimi poskušamo napad zaustaviti ali ga omejiti. Med te ukrepe lahko spadajo:

- uvrstitev phishing spletnega mesta na različne zadrževalne sezname,
- obveščanje ponudnika gostovanja spletne strani oz. domene,
- obveščanje drugih deležnikov v Sloveniji in tujini,
- obveščanje javnosti,
- obveščanje posameznih žrtev napada.

Prvič smo v centru SI-CERT o phishingu pisali pred skoraj dvajsetimi leti.

SPLETNI SEMINAR O IZVAJANJU PHISHING PREIZKUSOV

Naročeno izvajanje phishing preizkusov je uveljavljena praksa preverjanja prepoznavanja te vrste groženj pri zaposlenih v bankah, državnih ustanovah in drugih podjetjih. Ti preizkusi so lahko pripravljeni interno ali pa se jih naroči pri zunanjem izvajalcu. V literaturi lahko najdemo primere dobrih praks in tudi obravnavo vprašanja etičnosti tovrstnih preizkusov. V letu 2022 smo v centru SI-CERT lahko opazovali številne preizkuse v slovenskih podjetjih in organizacijah, zato smo se odločili izvesti spletni seminar za ozaveščanje izvajalcev o tem, kako dobro pripraviti preizkus. Kadar ta denimo ni ustrezno najavljen pri centru SI-CERT, lahko do nas prispejo prijave incidenta. S preiskovanjem izgubljamo resurse, kjer nato ugotovimo, da ne gre za dejanski incident, ampak naročeno preizkušanje zaposlenih.

Spletni seminar je potekal 25. oktobra 2022 in je bil del kampanje v okviru evropskega meseca kibervarnosti. Izraženo zanimanje je preseglo naša pričakovanja, prav tako udeležba na seminarju, ki ga je praktično od začetka do konca spremljalo 177 udeležencev. Pozitivne povratne informacije ter aktivno in konstruktivno sodelovanje udeležencev so signal, da so tovrstni dogodki dobrodošli. Posnetek seminarja je na voljo na spletni strani centra SI-CERT, skupaj s povezavami na vire, ki so bili podlaga za pripravo seminarja.

Ključni poudarki za izvajalce preizkusov:

- preizkus naj sledi izobraževanju zaposlenih in ne obratno;
- zaposleni naj bodo seznanjeni s tem, da se bo v prihodnosti izvedel preizkus prepoznavanja phishing sporočil;
- preizkus je treba pravočasno priglasiti pri centru SI-CERT;
- kadar se v preizkusu uporablja tuja intelektualna lastnina (logotipi, domene blagovnih znamk, uporaba identitete državnih organov), je treba preveriti zakonitost tako oblikovanega preizkusa;
- izogibajte se izpostavljanju zaposlenih ali celo sramotenju;
- jasno določite, kateri podatki iz rezultatov bodo razkriti in komu.

4. PROGRAM OZAVEŠČANJA VARNI NA INTERNETU

ŠIROK SPLET KOMUNIKACIJSKIH ORODIJ ZA DOSEGANJE UPORABNIKOV

VARNI NA INTERNETU
Od mene je odvisno vse.

Nacionalni program ozaveščanja Varni na internetu je še ena izmed zakonsko opredeljenih nalog, ki jih izvaja odzivni center SI-CERT. Ozaveščanje javnosti na področju informacijske varnosti je opredeljeno v 5. točki drugega odstavka 28. člena Zakona o informacijski varnosti, SI-CERT pa naloge izpolnjuje s številnimi dejavnostmi programa Varni na internetu. Vse izpeljane dejavnosti so v celoti financirane s sredstvi Urada Vlade Republike Slovenije za informacijsko varnost.

Program Varni na internetu je bil leta 2011 zasnovan z namenom ozaveščanja in izobraževanja odraslih spletnih uporabnikov o varni uporabi interneta in prepoznavanju tveganj. Program pokriva ključne problematike: okužbe z zlonamerno kodo, vdore v uporabniške račune, lažne spletne trgovine, različne oblike spletnih goljufij, phishing kraje gesel itd. Zaupanje v programske rešitve pred takšnimi zlorabami ne obvaruje – edina rešitev je kontinuirano izobraževanje spletnih uporabnikov.

Vsebine programa so namenjene vsem, ki se povezujejo v internet doma, na poti ali v službi. Naslavljamo zlasti uporabnike, starejše od 25 let, saj ta populacija že uporablja storitve spletnega bančništva in tudi opravi največji delež spletnih nakupov. **Druga ciljna skupina, ki vedno bolj prihaja v ospredje, so zaposleni, vodstva podjetij in IT-kader, ki potrebujejo bolj specifične napotke in priporočila.**

Osrednjo vlogo v okviru programa Varni na internetu ima portal **www.varninainternetu.si**, kjer je trenutno največja zbirka gradiv in nasvetov

s področja informacijske varnosti ter opisov spletnih goljufij v Sloveniji. Na kanalih družbenih omrežij praktično vsakodnevno objavljamo vsebine (nasvete in opozorila) in odgovarjamo na vprašanja uporabnikov. Prijave zlorab sprejemamo tudi prek prijavne točke na spletnem portalu, ob zaznanih grožnjah širših razsežnosti pa pripravimo obvestila za medije.

Ključne komunikacijske dejavnosti v letu 2022: poslanih je bilo 21 izdaj elektronskega novičnika Varne novice, ki v povprečju dosega 42-odstotno stopnjo odprtja, kar je izjemno dober rezultat. Konec leta 2022 je bilo 9018 naročnikov e-novic. Zabeleženih je bilo več kot 500 medijskih objav o programu in pripravljenih osem sporočil za javnost. Posnetih je bilo kar 20 novih kratkih videov z nasveti o prepoznavanju spletnih nevarnosti, uporabi dodatnih varnostnih nastavitev, zaščiti uporabniških računov in pomenu izobraževanja zaposlenih o osnovah informacijske varnosti. Izpeljani sta bili dve večji spletni oglaševalski kampanji, ki sta temeljili na promociji videovsebin in sta zbrali več kot 357.000 ogledov na platformah Facebook, LinkedIn in YouTube. Brezplačni spletni tečaj Varni v pisarni, namenjen usposabljanju zaposlenih, je od postavitve platforme leta 2021 do konca leta 2022 izobrazil 5918 tečajnikov, ki so skupaj opravili skoraj 10.000 izobraževalnih modulov. V letu 2022 je bilo izdanih 6156 certifikatov oz. potrdil o opravljenih modulih.

Prepoznavnost med slovenskimi uporabniki: v več kot desetih letih delovanja je program Varni na internetu postal prepoznaven tako med spletnimi uporabniki kot mediji in strokovno javnostjo. Aprila 2022 so bili objavljeni izsledki raziskave, ki je med drugim vsebovala tudi vprašanja o mnenjih o organizacijah, ki se ukvarjajo z varno rabo interneta. Raziskavo je opravil Center za raziskovanje javnega mnenja in množičnih komunikacij (CJMMK) Fakultete za družbene vede. Odgovori respondentov so pokazali, da sta med organizacijami, ki želijo izboljšati varno uporabo interneta, najbolj prepoznavna Arnes in Varni na internetu. Pri ocenjevanju vloge, ki jo imajo organizacije v slovenski družbi pri izobraževanju o varni uporabi interneta, je bil z najvišjo povprečno oceno ocenjen program Varni na internetu.

EVROPSKI MESEC KIBERNETSKE VARNOSTI – POSTANI AMBASADOR KIBERVARNOSTI!

Evropski mesec kibervarnosti, ki ga organizira Agencija EU za kibernetsko varnost ENISA v sodelovanju z državami članicami, je v letu 2022 praznoval deseto obletnico. V vseevropski pobudi že od začetka sodeluje tudi Slovenija, ki jo zastopa SI-CERT s programom Varni na internetu. Ob obletnici so bile tudi prvič podeljene nagrade za najboljša gradiva, ki so nastala v teh letih. **Video o počitniških prevarah, ki je bil pripravljen v okviru programa Varni na internetu, je prejel nagrado za najboljši video. Zmagovalni video je dostopen v vseh jezikih EU.**

Namen evropskega meseca kibernetske varnosti je okrepiti odpornost sistemov in storitev EU, opolnomočiti državljane ter narediti korak naprej k bolj kibernetsko varni in ozaveščeni družbi. **V letu 2022 sta bili v ospredju dve temi, izsiljevalski virusi in phishing.** Gre za globalna varnostna izziva, ki sta že nekaj let na zemljevidu najpogostejših kibernetskih nevarnosti.

Za prepoznavanje in preprečevanje zlorab so bila pripravljena izobraževalna gradiva, prilagojena delovno aktivni populaciji, saj so zaposleni pri

svojem delu v vedno večji meri odvisni od digitalnih tehnologij in orodij. Zaposleni v podjetjih, zlasti pa vodstvo, so bili med kampanjo pozvani, naj postanejo ambasadorji kibervarnosti in izvedejo vsaj eno dejavnost v podjetju. Če podjetje ni imelo lastnih gradiv, so jim bili na voljo že pripravljeni plakati, letaki in video, ki so nastali v kampanji.

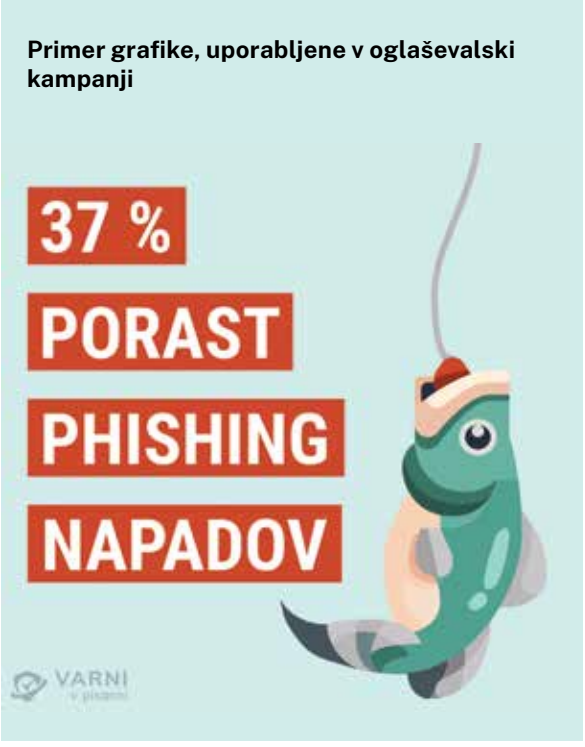
Splošna javnost je bila o pomenu varnosti na spletu opozorjena s serijo videoposnetkov, ki so bili pripravljeni v sodelovanju z mladima ustvarjalcema vsebin na omrežju TikTok. Prikazane so nekatere značilne napake, ki jih uporabniki počnejo na spletu, tako mlajši kot tudi predstavniki t. i. boomer generacije. Cilj kampanje na omrežju TikTok je bil nagovoriti mlajše uporabnike. Z zabavnimi videi so prikazane situacije, v katerih se lahko vsakodnevno znajdejo uporabniki spleta. Želja je bila, da bi mladim predali informacije o prevarah na internetu in o tem, kje lahko najdejo konkretne nasvete za starejše – svoje starše, dedke, babice in tudi svoje prijatelje. Videi imajo skupno nekaj manj kot 180.000 ogledov.

IZOGNITE SE NAJSLABŠEMU SCENARIJU – IZOBRAŽUJTE ZAPOSLENE

Še vedno je pogosto prepričanje, da manjša podjetja niso zanimiva za spletne napadalce, vendar to ne drži. Zaradi omejenih finančnih in kadrovskih virov so vlaganja v informacijsko varnost omejena, zato so manjša podjetja lažja tarča. Tudi v večjih podjetjih in organizacijah, kjer je stopnja zavedanja o kibernetski varnosti mnogo višja, težavo še vedno predstavlja nezadostno izobraževanje zaposlenih. Ker zaposleni nimajo ustreznih znanj in veščin, da bi prepoznali nevarnost, so napadalci pogosto uspešni. Značilen primer so phishing napadi. Čeprav gre za eno najstarejših vrst spletnih napadov, ki so tehnično zelo preprosti, so še vedno uspešni, saj jih zaposleni enostavno ne prepoznajo.

V letu 2022 je bilo več virov namenjenih promociji izobraževalnih vsebin, namenjenih zaposlenim, zlasti pa IT-kadru in vodstvu, ki ima možnost, da s svojim delovanjem in vlaganjem v izobraževanje pomembno zmanjša tveganja.

Primer grafike, uporabljene v oglaševalski kampanji



Septembra 2022 je bila v okviru komunikacijske akcije Izognite se najslabšemu scenariju! predstavljena širša oglaševalska kampanja, ki je nagovarjala različne skupine zaposlenih in njihove šibke točke. Akcija je ob štirih novih videih vključevala še infografike, oglaševalsko videokampanjo na omrežjih LinkedIn in YouTube, zakup ključnih besed v iskalniku Google ter obveščanje medijev in drugih deležnikov. Cilja kampanje sta bila dvig zavedanja o kibernetskih napadih na zaposlene v podjetjih in promocija brezplačnega spletnega tečaja Varni v pisarni.

Spletni tečaj Varni v pisarni je še ena od izobraževalnih dejavnosti, ki se izvajajo v okviru programa Varni na internetu. Platforma, ki temelji na videopredavanjih, na preprost, razumljiv in vizualno privlačen način zaposlenim predstavi osnove informacijske varnosti. Spletni tečaj je brezplačen, poteka kadarkoli na zahtevo, traja 30 minut in je prilagojen različnim delovnim mestom. Učne teme so razdeljene na module in prilagojene različnim delovnim procesom (splošne vsebine za vse zaposlene, za računovodje in poslovne sekretarje, za marketing in nabavo ter za IT-kader), zato je tečaj primeren tudi za vse organizacije, kjer ni sistematičnega pristopa k izobraževanju o informacijski varnosti.

Oglaševalska kampanja je trajala štiri mesece, od septembra do konca leta 2022, z glavnim ciljem pritegniti nove uporabnike, ki bodo opravili spletni tečaj Varni v pisarni. S spletnim oglaševanjem je bilo doseženih 138.311 uporabnikov, videooglasi so skupaj zabeležili 177.888 ogledov v celoti (na vseh oglasnih platformah). Po zaključeni kampanji je tako 4360 novih tečajnikov pridobilo certifikat o opravljenem izobraževanju, skupaj pa je bilo rešenih 7532 različnih modulov. Največ opravljenih modulov, poleg splošnega, obveznega dela, je bilo s področja, namenjenega računovodjem.

Spletni tečaj Varni v pisarni je brezplačen, poteka kadarkoli na zahtevo, traja 30 minut in je prilagojen različnim delovnim mestom v organizaciji.

NOVA VIDEOSERIJA A SI VEDU? – ZANIMIVA DEJSTVA S PODROČJA KIBERNETSKE VARNOSTI

Z ustvarjalcem videovsebin Petrom Jenkom smo posneli videoserijo A si vedu?, ki uporabnikom približa zanimiva dejstva s področja kibernetske varnosti. V osmih epizodah smo zajeli najpogostejše spletne prevare in načine, kako jih prepoznati in se pred njimi zavarovati. Videoserija je bila objavljena na vseh spletnih kanalih Varni na internetu, kjer si jo je do zdaj ogledalo že več kot 20.000 uporabnikov, pri čemer je najbolj gledana epizoda z naslovom Kako dobijo tvoj mail.

Naslov publikacije: Poročilo o kibernetski varnosti za leto 2022

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

Leto izida: 2023

Naklada: 520 izvodov

Založnik: Akademska in raziskovalna mreža Slovenije

Oblikovanje in prelom: KOFEIN dizajn

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

Ob zaznanem varnostnem incidentu pošljite prijavo z elektronskim sporočilom in nudili vam bomo pomoč pri preiskavi incidenta.

cert@cert.si