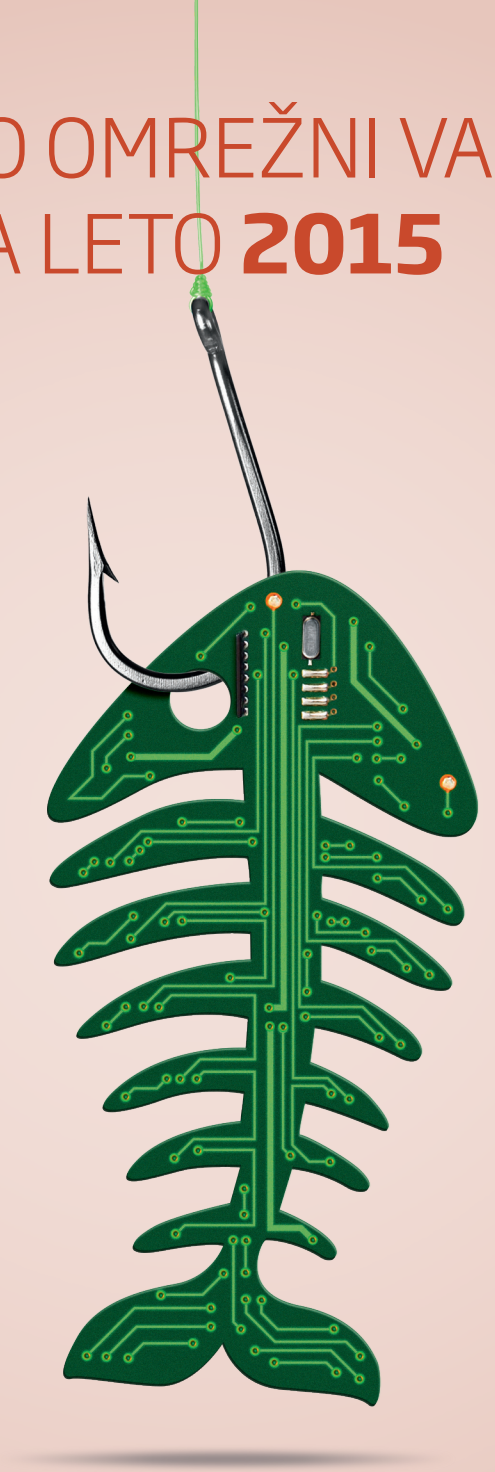
POROČILO O OMREŽNI VARNOSTI ZA LETO **2015**



arnes si·cert 20 LET VARNI NA INTERNETU

KAZALO

OMREŽNA VARNOST V LETIH 1995-2006

Javni zavod Arnes po letu priprav ustanovi SI-CERT, Slovenian Computer Emergency Response Team, in začne obravnavati prijave varnostnih incidentov.

1995

1996

Mladi hekerji začnejo vdirati v tuje sisteme. V Mariboru se oblikuje skupina, ki se druži v popularni internetni kavarni; honorarno jih kot sistemce zaposlujejo po lokalnih podjetjih, kjer se tudi ne morejo upreti hekanju. Lastniki podjetij in upravljavci internetnih kavarn imajo v naslednjih letih zaradi tega kar nekaj težav.

Študent vdre v račun dekana fakultete Univerze v Ljubljani in v njegovem imenu pošlje senatu fakultete pismo z grožnjami.

Pri preiskovanju vdora v sistem v Sloveniji odkrijemo zbirko gesel uporabnikov računalnika v lasti ameriške vojne mornarice (navy.mil). Obvestimo njihov "Information Warfare Center".

1997

1998

Ker SiOL na številki 0880 zaračunava telefonske impulze prijavljenemu uporabniku (in ne lastniku telefonskega priključka), postanejo ti uporabniški računi predmet kraje in preprodaje, saj omogočajo uporabo interneta na tuj (telefonski) račun. Levjesrčni najde napako v sistemu SiOL, s katero lahko masovno prestreza gesla in to objavi; izbruhne preprodaja gesel. Primer začnemo preiskovati skupaj s policijo in identificiramo vpletene.

Obravnavamo prve napade onemogočanja (denial-of-service) na cilje v Sloveniji.

Izbruh okužb z NetBus in BackOrifice trojanskima konjema, izdanima leto prej. Omogočata pritajen dostop in nadzor tujega računalnika. Postavimo spletno stran, na kateri lahko uporabniki preverijo, ali imajo trojanca na svojem računalniku.

Na internetu so na voljo orodja za izvedbo porazdeljenih napadov onemogočanja: trin00, Tribal Flood Network in Stacheldraht.

Ameriška vojska zablokira promet tudi iz Slovenije do .mil domene pred bombardiranjem Zvezne republike Jugoslavije.

1999

2000

Skeniranja naslovnega prostora, vdori pri nas in v tujini ter številni napadi onemogočanja nas polno zaposlujejo.

SI-CERT postane član združenja FIRST (Forum of Incident Response and Security Teams), vodja SI-CERT Gorazd Božič je izbran za predsednika delovne skupine evropskih odzivnih centrov TF-CSIRT, ki jo nato vodi osem let.

Medijsko pozornost ugrabi "I love you" črv, ki se širi prek elektronske pošte. Problem Y2K ob prehodu v novo tisočletje se izkaže za nepotrebno paniko.

Čez leto se rojevajo internetni črvi, ki se samodejno širijo po računalnikih na omrežju. Najodmevnejši je kitajski Code Red, sledijo mu Nimda, Sircam, Klez in Frethem. Obravnavamo prva razobličenja spletnih strani in uporabo rootkitov. V enem incidentu najdemo nekaj sto zlorabljenih sistemov v tujini.

SI-CERT gosti kolege iz evropskih odzivnih centrov, združenih v delovni skupini TF-CSIRT.

2001

2002

Prek nezaščitenih posredniških proxy in SOCKS-strežnikov tujci razpošiljajo velike količine neželene elektronske pošte. Izkorišča se slaba zaščita NetBIOS-protokola na Windowsovih računalnikih za številne vdore in okužbe.

Luknja v poštnem programu PINE je omogočila dostop do seznama uporabniških imen Arnesovih uporabnikov guest.arnes.si, na srečo samo do okleščene kopije brez imen in gesel v zaprtem (chroot) okolju.

Microsoftove spletne strežnike IIS napade Code Red II črv.

2003

2004

IRC-vojne (spopadi slovenskih hekerskih skupin) kulminirajo v napadu na DNS-strežnike SiOLa novembra 2004, kar ohromi vse SiOLove uporabnike. Telekom Slovenije prekine politiko molka glede prijav s SI-CERT in začne se sodelovanje, ki bo v naslednjih letih pomagalo korenito zmanjšati število zlorab in omrežnih napadov v Sloveniji.

"Dialler" virusi po okužbi kličejo na drage plačljive telefonske številke v tujini.

Pojavi se nova vrsta omrežne zlorabe: phishing.

Vrstijo se napadi z ugibanjem gesel iz slovarja preko Secure Shell protokola – slovenski hekerji kot za stavo poskušajo vdreti v čimveč tujih računalnikov. Po večmesečnem zbiranju prijav podatke posredujemo policiji, ki nato opravi okoli 20 hišnih preiskav.

Plačljivi igralni strežniki za igro Call of Duty v Sloveniji povzročijo vrsto medsebojnih napadov onemogočanja med posamezniki v Sloveniji, s katero želijo eden drugega izriniti s "tržišča".

2005

2006

Prva phishing stran v tujini, ki meri na komitente slovenske banke.

OMREŽNA VARNOST V LETIH 2007-2016

2007

V seriji napadov onemogočanja na spletna mesta nekaterih ameriških medijev v botnetu sodeluje tudi nekaj računalnikov iz Slovenije. Na SI-CERT opravimo analizo zlonamerne kode, ki FBI omogoči prijetje Bruca Raisleya, nekaj let kasneje obsojenega pred sodiščem v ZDA.

Pred prvomajskimi prazniki v Estoniji odstranijo spomenik vojaku iz sovjetskih časov, kar sproži obsežne omrežne napade onemogočanja na državno infrastrukturo, banke in spletne medije. Evropska skupina odzivnih centrov TF-CSIRT ustanovi "ad-hoc" skupino za pomoč, ki jo skupaj vodita finski CERT-FI in SI-CERT.

2008

Čez leto se borimo z okužbami Conficker. Ta napredni črv izkorišča za širjenje več kanalov in se izkaže za trdovratnega nasprotnika, posamezne okužbe so zaznane še v obdobju naslednjih petih let.

Evropski potrošniški center nas prosi za pomoč v primeru specialphones.eu, pri katerem nekdo goljufa s fiktivno prodajo telefonov iPhone po polovični ceni. S pomočjo estonskega CERT-EE dosežemo hiter umik strani. Za leto 2009 kasneje ugotovimo, da je prelomno pri porastu spletnih goljufij.

2009

Začnemo z nacionalnim programom ozaveščanja na področju informacijske varnosti, Varni na internetu. Odziv javnosti je zelo dober, program v naslednjih letih prejme nekaj nagrad.

Ugotovimo, da ima ena od slovenskih elektrarn javno dostopen vmesnik na spletu in vprogramirana stranska vrata, ki lahko omogočijo nepooblaščen vstop in pregled nadzornih sistemov elektrarne. Številne toplotne postaje imajo privzeta gesla na spletnih vmesnikih, ki prav tako omogočajo nepooblaščeno spreminjanje nastavitev.

Na Youtube kanalu se znajdejo posnetki zaprtih sej Vlade RS. Google naše zahtevke za odstranitev ignorira, dokler se ne domislimo alternativnega pristopa: lastnik posnetkov je vlada, torej gre za kršitev avtorskih pravic. Pošljemo DMCA-zahtevke pooblaščeni odvetnici v ZDA in problem je hitro rešen.

2010

Slovenija prevzame predsedovanje EU, zato postane zanimivejša za usmerjene napake na zaposlene v državni upravi. Opravimo analize poskusov podtaknjenih virusov v teh napadih; sledi se končajo na Kitajskem.

Dan Kaminsky odkrije resno napako v delovanju DNS-infrastrukture interneta. 82 skrbnikov omrežij obvestimo, da imajo ranljive strežnike, ki omogoča t. i. "zastrupljanje predpomnilnika".

2011

SI-CERT podpiše sporazum z Ministrstvom za javno upravo RS, po katerem prevzame koordinacijo obravnavanja varnostnih incidentov na omrežju javne uprave in pomaga pri vzpostavljanju samostojnega vladnega odzivnega centra za državno infrastrukturo.

Spomladi se med slovenskimi uporabniki Facebooka začne širiti črv, ki ga je napisal Slovenec. V Mariboru policija aretira Matjaža Škorjanca - Iserda, ki je avtor Butterfly Bota (primer Mariposa).

2012

Zaradi podpisa sporazuma ACTA skupina Anonymous najavi napade na državno infrastrukturo in druge tarče. Prevzamemo koordinacijo, postavimo ovire za napade onemogočanja in obvestimo ponudnike o pričakovanih vrstah napadov. Napadi na gov.si ne uspejo, nekaj je spletnih razobličenj drugih spletnih mest, medijsko pa je kampanja Anonymousa zelo odzivna.

Hekerska skupina z Bližnjega vzhoda napada banke v ZDA, pri čemer uporabi tudi 63 strežnikov v Sloveniji. Napadi z odbojem izkoriščajo ranljive DNS-strežnike. V Sloveniji jih je skoraj 9.000; začnemo z rednim obveščanjem skrbnikov.

Slovenija prvič sodeluje v vseevropski vaji Cyber Europe 2012 - scenarij vključuje napade na e-banke in omrežno infrastrukturo, odzivni centri pa imajo v vaji osrednjo vlogo.

SI-CERT prejme za sodelovanje v primeru Raisley uradno priznanje direktorja ameriškega preiskovalnega urada FBI. Število obravnavanih incidentov preseže številko 1000.

Razobličenih je čez 1500 strežnikov malih podjetij, šol in drugih ustanov, ki uporabljajo Joomla sistem za upravljanje vsebin. Ob sprotnem obveščanju skrbnikov pripravimo tudi brošuro "ABC varnosti za lastnike spletnih mest".

S policijo in Uradom RS za preprečevanje pranja denarja 6 mesecev preiskujemo napade na mala podjetja, prek katerih so storilci ukradli 1,8 mio EUR. Analiza škodljive kode, ki jo opravimo na SI-CERT, policijo pripelje do avtorja, Sebastijana Mihelčiča.

"Policijski virus" izsiljuje tudi slovenske uporabnike; na srečo obstaja hiter odklep, s katerim pomagamo čez 300 posameznikom. Na festivalu vsebinskega marketinga POMP 2013 prejmemo nagrado za najboljše letno poročilo in nepričakovano tudi veliko nagrado za projekt leta na področju vsebinskega marketinga.

2013

2014

Leto zaznamuje ranljivost Heartbleed v knjižnici OpenSSL. Ranljivi so okoli 3 % spletnih strežnikov v Sloveniji. Napadi z odbojem se preselijo na protokol NTP. Izsiljevalski virusi postanejo močnejši in šifrirajo podatke uporabnika. Širijo se s pomočjo lažnih računov v nemškem jeziku po elektronski pošti.

Sodelujemo na Cyber Europe 2014 in NATO vaji Cyber Coalition 14. Začnemo z usposabljanjem pripadnikov Slovenske vojske za namene odzivanja na kibernetske grožnje in incidente. Prebijemo mejo 2000 obravnavanih incidentov.

Takoj januarja se začne do sedaj najdolgotrajnejši "phishing" napad na komitente šestih bank v Sloveniji. Ocenjujemo, da je bilo poslanih okoli 100.000 lažnih sporočil in postavljenih okoli 40 lažnih kopij spletnih mest bank. Teden dni oviramo storilce, nato ti obupajo in se usmerijo na druge države.

Jeseni mine 20 let od prve prijave incidenta na SI-CERT.

2015

si·cert 20 LET

arnes

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Poročilo centra SI-CERT

SVET JE SPET EDEN

Informacijska varnost je tema, ki se je začela konec osemdesetih let s hekerji, ki so vdirali po telefonskih in takrat nastajajočih računalniških omrežjih v ZDA. Radi smo brali zgodbe, ki so dobivale že prav mitološki obris, recimo tisto o izmuzljivem spretnežu Kevinu Mitnicku, zaradi katerega se je tudi FBI zavedel, da se začenja nova doba. Pri nas se lahko pohvalimo, da takrat tehnološko na področju omrežij nismo bistveno zaostajali in zgodbo razvoja smo zato uspešno nadaljevali v devetdeseta leta, ko je na javnem zavodu Arnes začel delovati tudi SI-CERT. Z rastjo omrežja je namreč hitro prišlo do vdorov in izkoriščanj različnih lukenj. Naivno smo takrat razmišljali o tem, kako bomo enkrat za vselej končali »buffer overflow« probleme, gledali smo rast botnetov, s katerimi so rivalske hekerske skupine izvajale napade onemogočanja, in skupaj s policijo preiskovali prva kazniva dejanja na internetu. Danes se borimo z močnimi napadi onemogočanja, ki izkoriščajo pomanjkljivosti internetne infrastrukture, raziskujemo sofisticirane napade s strani tujih držav, pri katerih se uporabljajo napredni računalniški virusi, in opozarjamo na širok razrast spletnih goljufij, ki so usmerjene predvsem na posameznike. Države se začenjajo zavedati, da je zaščita moderne informacijske infrastrukture nujna, in upamo lahko, da bomo pri tem zmogli v korak tudi z večjimi in bolj pripravljenimi. Ob vsem tem pa se ne sme čakati samo na ukrepanje države, saj lahko svoje prispevajo tudi velika podjetja s področja elektronskih komunikacij, ponudniki gostovanja in še mariskdo. Prepletenost digitalnega in fizičnega sveta pomeni, da je informacijska varnost bistven del dobro delujočega okolja za celotno gospodarstvo. Zato se mora tudi slednje zavedati njenega pomena.

Gorazd Božič, vodja SI-CERT

PREDSTAVITEV CENTRA SI-CERT

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, ki deluje od leta 1995 v okviru javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije). Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT od leta 2011 samostojno izvaja nacionalni program ozaveščanja in izobraževanja ***Varni na internetu.***

Javni zavod Arnes in Ministrstvo za notranje zadeve RS sta na podlagi sklepa Vlade Republike Slovenije št. 38600-3/2009/21 z dne 8. 4. 2010 podpisala sporazum, po katerem SI-CERT opravlja naloge vladnega centra za odzivanje na omrežne incidente in pomaga pri vzpostavitvi samostojnega centra, ki bo skrbel za zaščito infrastrukture državne uprave.

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

Storitve odzivnega centra SI-CERT so na voljo širši javnosti. SI-CERT se financira iz sredstev, ki jih za javni zavod Arnes zagotavlja Direktorat za informacijsko družbo Ministrstva za izobraževanje, znanost in šport RS. V primeru vdora, okužbe računalnika ali druge omrežne zlorabe lahko pošljete sporočilo z opisom incidenta na naslov cert@cert.si, prek telefona na številko (01) 479 88 22 ali prijavnega obrazca na spletni strani www.varninainternetu.si. Strokovnjaki centra pomagamo prizadetim ob pozameznih 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 pospešijo razreševanje aktualnih primerov.

PRENOS ZNANJA

Sodelavci SI-CERT smo v letu 2015 opravili kar 40 predavanj in predstavitev o kibernetski varnosti in varni uporabi interneta. Predavanja smo izvajali v sodelovanju z univerzama v Ljubljani in Mariboru, Gospodarsko zbornico Slovenije, Informacijskim pooblaščencem RS, Združenjem bank Slovenije, Novo Ljubljansko Banko, d. d., Institutom Jožef Stefan in drugimi. Posebej pa bi še izpostavili:

- predavanja za Generalštab Slovenske vojske,
- predstavitev slovenskih izkušenj odzivanja na informacijske grožnje pred odborom za obrambo in notranje zadeve Skupščine Republike Srbije,
- predavanje o regijskem spodbujanju oblikovanja odzivnih centrov na NATO-delavnici v Skopju,
- vabljeno predavanje o evropskem sodelovanju CERT-centrov na belgijskem B-CCENTRE,
- predstavitev aktivnosti SI-CERT na delavnici Europolovega EC^3-centra.

DOKUMENTARNI FILM #HEKERJI.SI

»Duhoviti filmski pregled zgodovine slovenskega hekerstva je na četrtkovi premieri večkrat nasmejal polno dvorano ljubljanskega Kina Šiška in pokazal, da so lahko tudi računalniške teme »televizične«.

Lenart J. Kučić, Sobotna priloga, Delo

Imamo Slovenci hekerje? Kdo so, zakaj vdirajo v tuje računalnike in se prosto sprehajajo po internetu? Kaj jih žene in ali je danes kaj drugače, kot je bilo pred na primer dvajsetimi leti?

Okrogle obletnice je treba seveda proslaviti, poleg tega pa nas nujno odnesejo še v nekakšno inventuro in razmislek o vsem, kar se je zgodilo do sedaj. Ko smo šli čez vtise in spomine, se nam je zazdelo, da bi lahko bili nekateri zanimivi tudi širši javnosti oziroma da se v ozadju kaže zgodba, ki jo lahko povemo in trajno tudi zapišemo. Film prikaže razvoj hekerske skupnosti v štirih poglavjih, temelji pa na gradivih iz arhiva SI-CERT. V njem poleg hekerjev nastopajo tudi kriminalisti, tožilci, skrbniki omrežij in računalnikov, raziskovalci s področja informacijske varnosti, drugi poznavalci in zaposleni na SI-CERT.

Film je nastal v režiji Blaža Završnika, v sodelovanju s produkcijsko hišo Sever & Sever in RTV Slovenija. Sofinanciran je iz sredstev programa za ozaveščanje Varni na internetu, ki jih zagotavlja Direktorat za informacijsko družbo MIZŠ, in sredstev Register.si, ki upravlja slovenski domenski prostor na internetu.

Celoten projekt je bil izpeljan v prvih devetih mesecih leta 2015, premierno pa je bil film prikazan na projekciji v polni dvorani Kina Šiška 22. oktobra, nato pa še 17. decembra na TV Slovenija 2. Odzivi na film so bili zelo pozitivni in vzpodbudni, med njimi pa je bila velikokrat izražena želja po tem, da bi bilo tovrstnih izdelkov še več. Izvedba projekta je vključevala tudi prevod v angleški jezik in prejeli smo dobre odzive tudi od kolegov iz tujine.

Film je v HD-različici prosto dostopen za ogled prek spletne strani hekerji.si.

Režija: Blaž Završnik
Ideja in koncept: Gorazd Božič
Scenarij: Gorazd Božič, Blaž Završnik
Svetovalec: Vuk Ćosić

Direktor fotografije: Darko Herič, ZFS
Montažerja: Katja in Blaž Završnik
Animacija: Maja Andlovic
Snemalka zvoka: Nina Bučuk
Grafika: Darko Miladinovič
Producenta: Nina Jeglič, Jani Sever
Produkcija: Sever & Sever, 2015

»#Hekerji.si – bili smo na premieri dokumentarnega filma o slovenski hekerski sceni. #priporočamo«

Luna\TBWA

»Ogled filma je obvezen.«

Domen Savič, The L Files

RAČUNALNIŠKI INCIDENTI

Potek obravnave varnostnega incidenta

OD PRIJAVE DO RAZREŠITVE

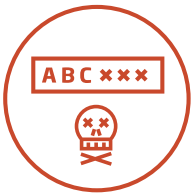
Računalniški incidenti so *nizi dogodkov, ki vplivajo na varnost omrežja, naprave ali podatkov*. Preprečujemo jih z ustrezno zaščito in preventivnimi ukrepi, vendar pa je bistveno spoznanje, da vseh nikoli ne bomo mogli preprečiti. Odzivanje na incidente temelji na **pripravi** nanje. Ko incident **zaznamo**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

DEJAVNOSTI SI-CERT

DEJAVNOST	OPIS
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 vzpostavi kontakt 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 preko programa usposabljanja

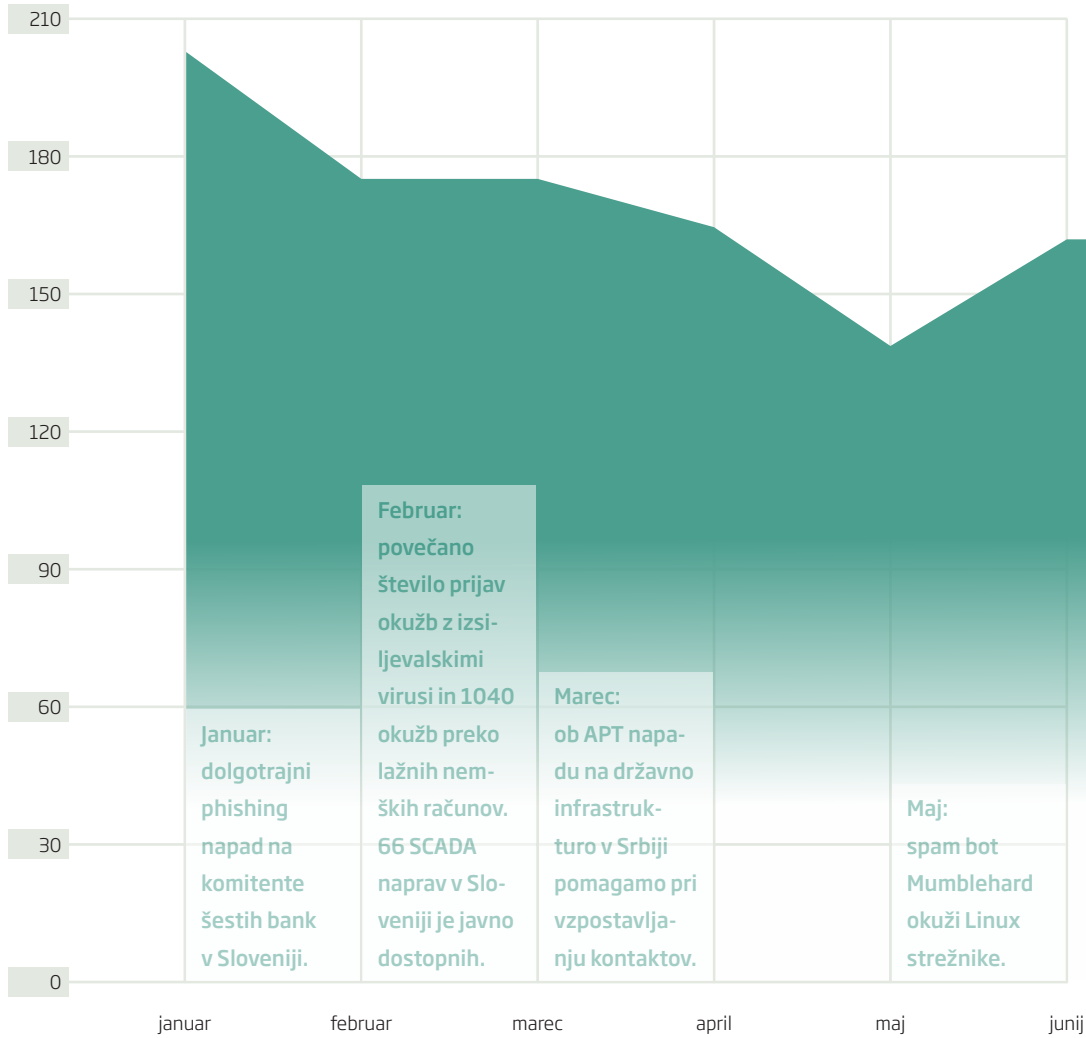
KDAJ PRIJAVITI INCIDENT

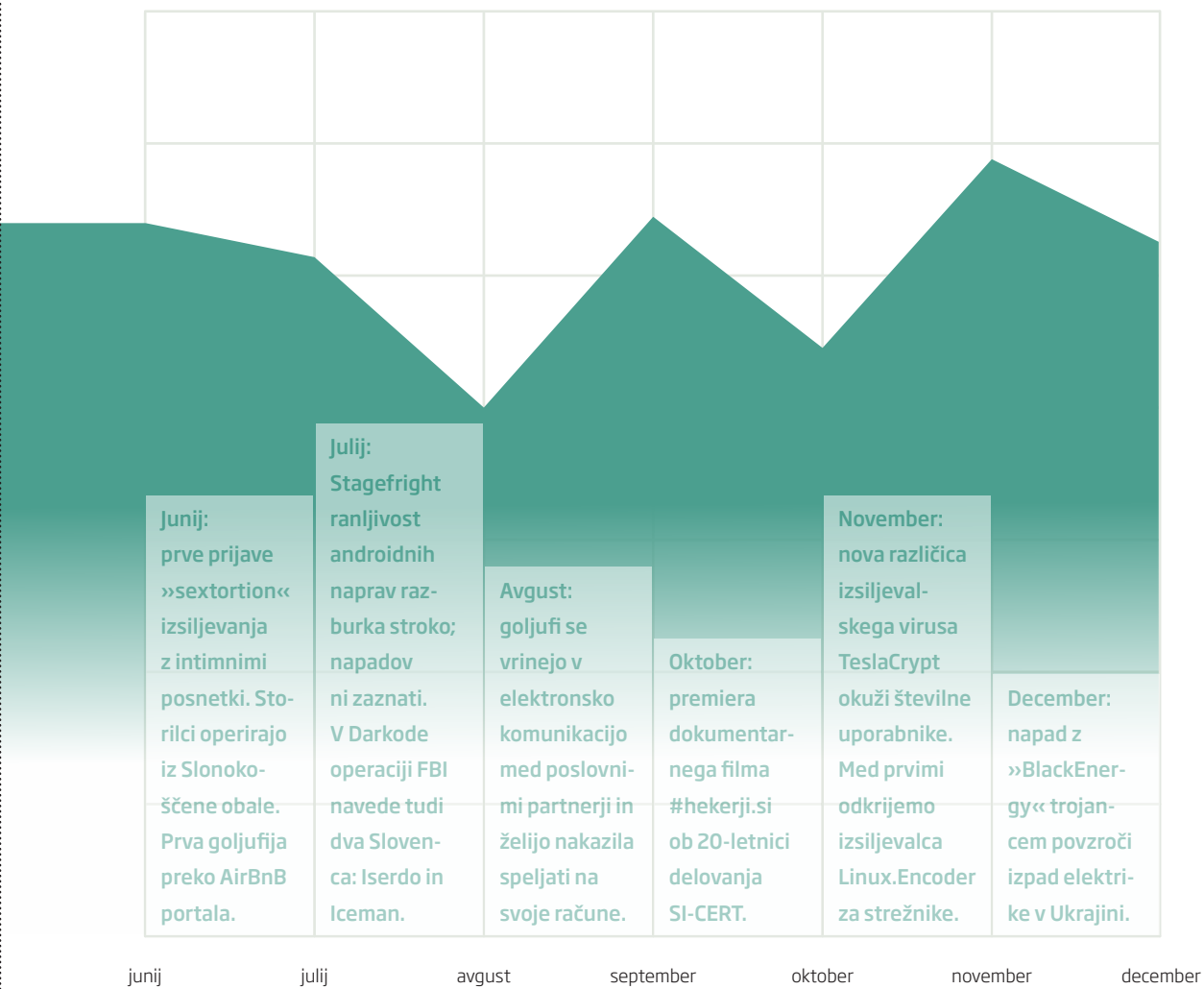
	DOGODEK (PRIMERI)	NA SI-CERT NUDIMO
	**OKUŽBA RAČUNALNIKA** (izsiljevalski virusi, bančni trojanci, agenti za pošiljanje nezaželene elektronske pošte)	pomoč pri odstranjevanju okužbe in njenih posledic, posredovanje vzorca v analizo
	**OPAŽEN VDOR V STREŽNIK** (razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca)	iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, nasveti za odstranjevanje škode
	**SUMLJIVA ELEKTRONSKA SPOROČILA** (phishing sporočila, ponudbe o hitrem zaslužku ali kreditih)	svetovanje in ocena tveganja, zbiranje podatkov o lokacijah goljufivih spletnih mest ter njihovo odstranjevanje in označevanje
	**NAPAD ONEMOGOČANJA** (poplava s prometom, napad na storitev ali spletno aplikacijo z namenom, da jo onemogoča)	ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta in obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti

	DOGODEK (PRIMERI)	NA SI-CERT NUDIMO
	**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 iskanju storilca
	**SPLETNA GOLJUFIJA** (lažne spletne prodajalne, prevare pri prodaji in nakupih prek spletnih posrednikov, lažni krediti, nigerijske in loterijske prevare)	ocena tveganja, odstranjevanje lažne spletne trgovine s spleta, ozaveščanje javnosti

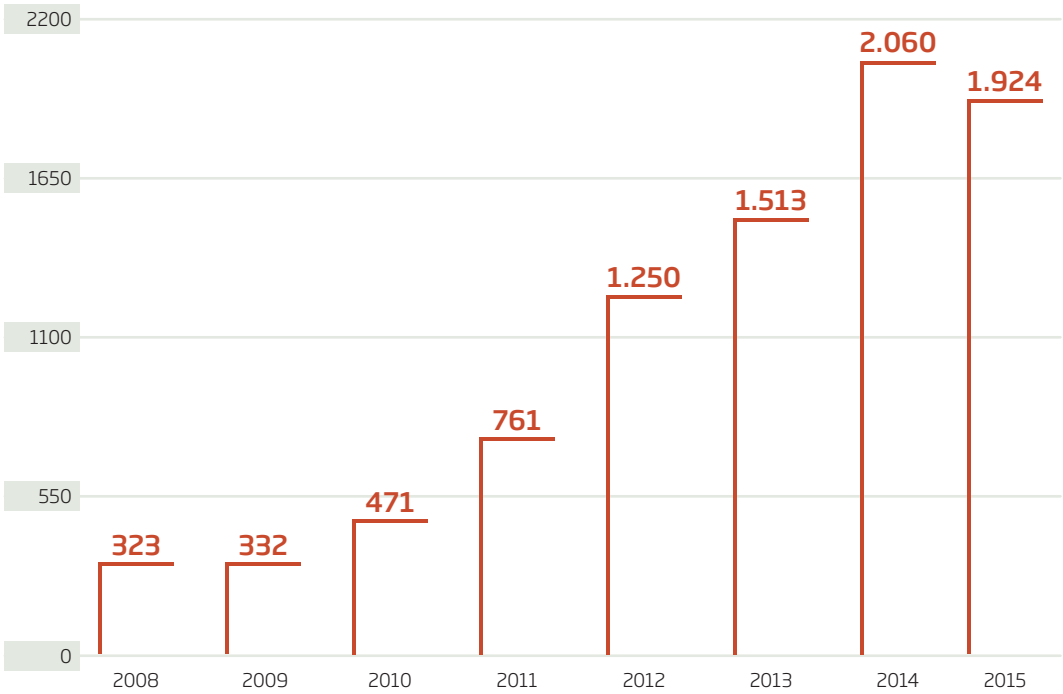
STATISTIKA

Število mesečno obravnavanih incidentov




Junij: prve prijave »sextortion« izsiljevanja z intimnimi posnetki. Storilci operirajo iz Slonokoščene obale. Prva goljufija preko AirBnB portala.
Julij: Stagefright ranljivost androidnih naprav razburka stroko; napadov ni zaznati. V Darkode operaciji FBI navede tudi dva Slovenca: Iserdo in Iceman.
Avgust: goljufi se vrinejo v elektronsko komunikacijo med poslovnimi partnerji in želijo nakazila speljati na svoje račune.
Oktober: premiera dokumentarnega filma #hekerji.si ob 20-letnici delovanja SI-CERT.
November: nova različica izsiljevalskega virusa TeslaCrypt okuži številne uporabnike. Med prvimi odkrijemo izsiljevalca Linux.Encoder za strežnike.
December: napad z »BlackEnergy« trojancem povzroči izpad elektrike v Ukrajini.
junij
julij
avgust
september
oktober
november
december

Število obravnavanih incidentov na leto (SI-CERT)



Delež incidentov

Tehnični napadi
732

Goljufije
618

Phishing
283

Vprašanja in poizvedbe
225

KAJ RAZKRIVAJO ŠTEVILKE?

STATISTIKA OBRAVNAVANIH INCIDENTOV

VRSTA INCIDENTA	2008	2009	2010	2011	2012	2013	2014	2015
skeniranje in poskušanje	86	39	44	62	51	43	65	65
botnet	9	3	11	12	12	16	13	17
napad onemogočanja (DDoS)	22	10	18	28	47	76	124	94
škodljiva koda	18	53	68	126	258	417	438	418
zloraba storitve	16	15	12	28	9	8	9	15
vdor v sistem	32	25	56	93	76	61	32	43
zloraba up. računa				1	9	37	60	40
razobličenje					125	80	167	33
napad na aplikacijo					17	22	33	7
Tehnični napadi	**183**	**145**	**209**	**350**	**604**	**760**	**941**	**732**
kraja identitete			10	52	67	56	77	70
nigerijska (419) prevara							38	26
spletno nakupovanje							68	88
druge goljufije	5	24	26	89	161	210	309	322
spam	21	22	36	25	74	50	63	112
phishing	23	38	50	61	139	209	279	83
dialler					1		3	
Goljufije in prevare	**49**	**84**	**122**	**227**	**442**	**525**	**837**	**901**
zahtevek sodišča	11	6	11	11	9	6	4	2
avtorske pravice	2	4	2	5	9	1	4	4
interno	3	4	16	38	25	24	31	23
novinarsko vprašanje					18	16	21	12
druga vprašanja	70	74	92	120	128	145	179	184
Vprašanja in zahtevki	**86**	**88**	**121**	**174**	**189**	**192**	**239**	**225**

11

prijav incidentov vsak dan v letu (v povprečju)

400+

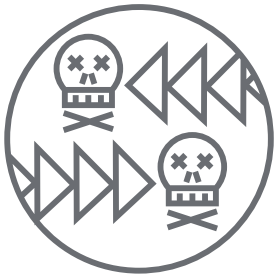
primerov škodljive kode v letu 2015

283

phishing incidentov

18.000 €

Največje posamezno oškodovanje v nigerijski prevari



1.140 €

Povprečno oškodovanje pri spletni goljufiji

720 €

Povprečno oškodovanje pri spletnem nakupovanju

PREGLED IZBRANIH INCIDENTOV

PHISHING NAPAD NA SLOVENSKE BANKE

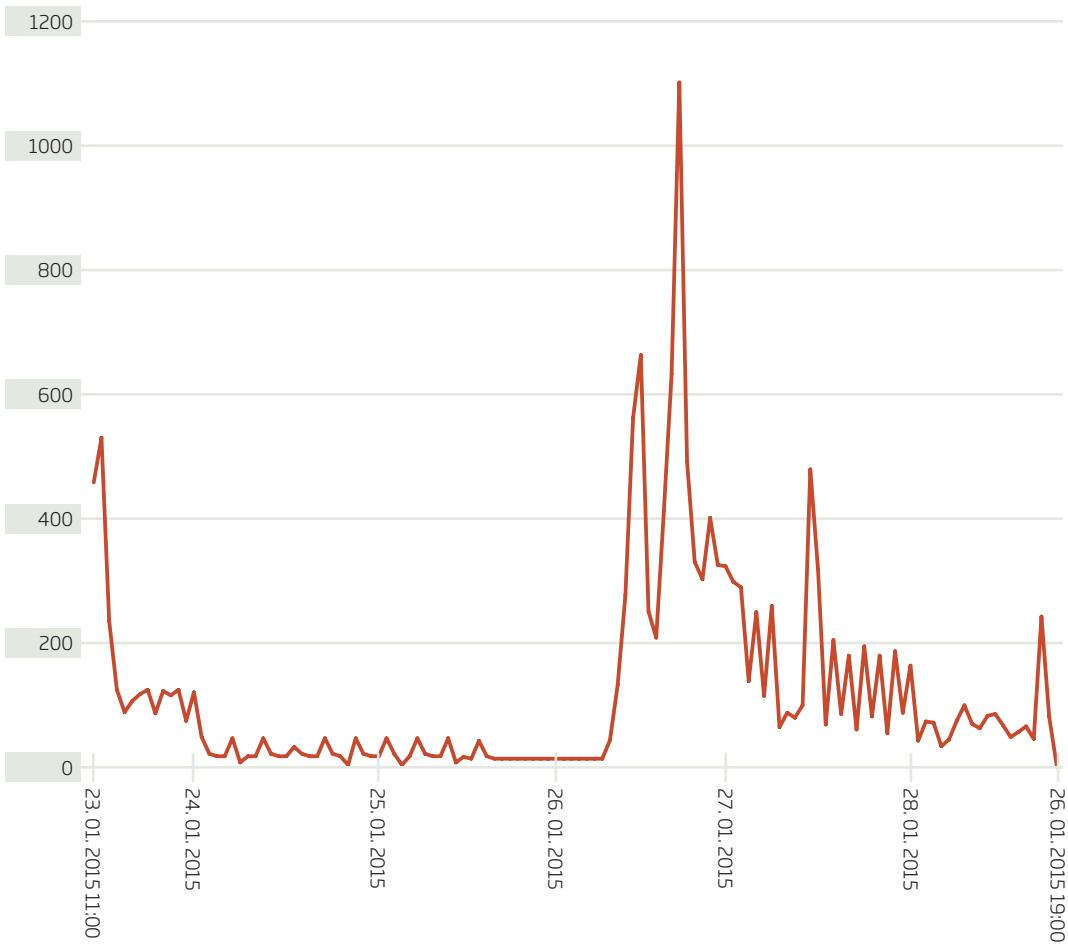
V petek, 23. januarja 2015, smo prejeli prijave o elektronski pošti, ki je naslovnike usmerjala na lažno spletno stran banke NKBM. Sprva je kazalo, kot da gre za le še en phishing poskus, usmerjen na komitente ene od bank v Sloveniji. Nekatera phishing sporočila so vsebovala okvarjene povezave, prijave pa so kmalu usahnile. Že v ponedeljek dopoldne pa se je pokazalo, da je šlo le za preizkušanje terena, saj se je napad nadaljeval in razširil na komitente šestih bank v Sloveniji.

SPOROČILA

Napadalci so pošiljali sporočila z izmišljenih elektronskih naslovov, domene so bile sicer podobne imenu banke, a neregistrirane. Napadalci namreč na črnem trgu pridobijo zbirko elektronskih naslovov slovenskih uporabnikov, ki pa ni preverjena, nekateri naslovi pa morda niti več ne delujejo. Ko se phishing sporočila razpošljejo, se nekatera zaradi tega (ali drugih napak) odbijejo in pošljejo nazaj na strežnik za domeno, navedeno v naslovu pošiljatelja. Tako bi banke naenkrat začele prejemati sporočila o nedostavljeni pošti in kmalu ugotovile, da gre za napad na njihove komitente.

Pošiljanje z neveljavno domeno pa ima drugo pomanjkljivost: bolj striktno nastavljeni poštni strežniki takšno pošto takoj zavrnejo kot neveljavno in tako le-ta niti ne prispe do tarč. S pomočjo dnevniških zapisov poštnega strežnika za Arnesove @guest.arnes.si smo lahko spremljali potek kampanje in izločili nekaj pomembnih informacij o samem napadu.

Količina zavrnjenih sporočil januarske phishing kampanje na Arnesovih potnih strežnikih



Vsa phishing sporočila so se pošiljala s samo nekaj poštnih strežnikov. Vsem internet ponudnikom v Sloveniji smo svetovali omejitev sprejema pošte s teh strežnikov kot tudi razmislek o zavračanju pošte, ki prihaja z neregistriranih domen.

ODSTRANJEVANJE IN BLOKIRANJE

Skozi potek phishing kampanje smo na SI-CERT skrbeli za čim hitrejše odstranjevanje postavljenih lažnih spletnih mest s pomočjo odzivnih centrov CERT v tujini, naslove spletnih »limanic« pa smo sproti sporočali tudi na brskalniške sezname, ki uporabnike opozarjajo pred nevarnimi spletnimi mesti (Safe Browsing Lists).

Našteli smo nekaj čez 30 lažnih spletnih mest, katere storilci postavijo na zlorabljenih strežnikih, kjer izkoristijo nezakrpane sisteme za upravljanje z vsebinami (CMS), najpogosteje so to slabo vzdrževani strežniki Joomla in Wordpress.

OBVEŠČANJE JAVNOSTI

Twitter: @sicert
Facebook: fb.com/sicert

Kot je za večje incidente običajno, javnost prek družbenih omrežij, obvestil na spletni strani cert.si in sporočil medijem sprotno obveščamo o lastnostih napada in zaščiti. Sprotno obveščanje je pomembno, saj lahko z njim dosežemo uporabnike, ki bodo v bližnji prihodnosti tarča napada in se bodo lahko neželenim posledicam izognili. Le-to je bilo zelo jasno vidno potem, ko smo ob preiskovanju pridobili datoteko storilcev z ukradenimi gesli. V začetku so vidna avtentična gesla, čez nekaj dni pa so uporabniki začeli vpisovati očitno neveljavna gesla in uporabniška imena, ki so bila pravzaprav namenjena storilcem in so odslikovala, kaj si uporabniki mislijo o njih. Ta sprememba je bila gotovo tudi posledica poročanja medijev o tem incidentu.

EPILOG

Napad se je do naslednjega petka umiril in razen osamljenih poskusov v naslednjih dneh nismo več zasledili novih lažnih spletnih mest. Na bankah so njihove strokovne ekipe preverjale in ustavljale sumljive transakcije denarnim mulam. Denarni tok je bil prek denarnih mul usmerjen v Rusijo in domnevamo, da so storilci prihajali od tam. Kmalu po koncu »kampanje« pri nas so se ti usmerili na hrvaške banke, zato smo kolegom na HR-CERT poslali kratek povzetek naših izkušenj.

Pri odzivu na incident so sodelovali IT-strokovnjaki prizadetih bank, kriminalistična policija in ekipa SI-CERT. Kmalu po zaključku incidenta smo opravili pregled aktivnosti na Združenju bank Slovenije in na Centru za računalniško preiskovanje Generalne policijske uprave.

OBLIKE IZSILJEVANJA

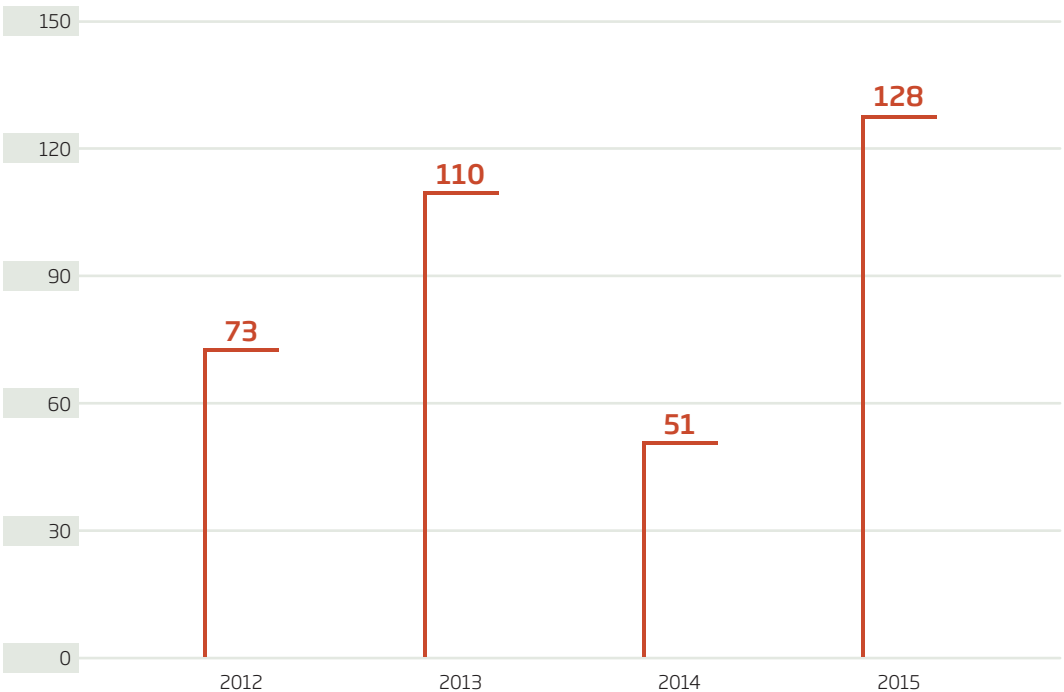
IZSILJEVALSKI VIRUSI

O izsiljevalskih virusih smo prvič pisali v poročilu za leto 2012. Začelo se je z Ransomcrypt virusom, sledil je »policijski virus«, ki je zaklenil računalnik, a podatkov ni poškodoval. A kmalu mu je sledil Ransomcrypt, ki je podatke na računalniku zašifriral, in to dovolj spretno, da ni bilo bližnjice, podatke ste lahko povrnili z varnostne kopije ali pač plačali odkupnino. V nekaj letih se je ta izsiljevalski »poslovni model« kiberkriminalcem očitno izplačal, saj smo v naslednjih letih spremljali pojavljanje vedno novih izsiljevalskih programov.

Izsiljevalski virusi v letu 2015:

bitlocker
synolocker
cryptolocker
cryptowall
ctb-locker
teslacrypt
linux.encoder.1

Število prijav okužb z izsiljevalskimi virusi po letih



IZSILJEVANJE Z NAPADI ONEMOGOČANJA (DD4BC IN ARMADA COLLECTIVE)

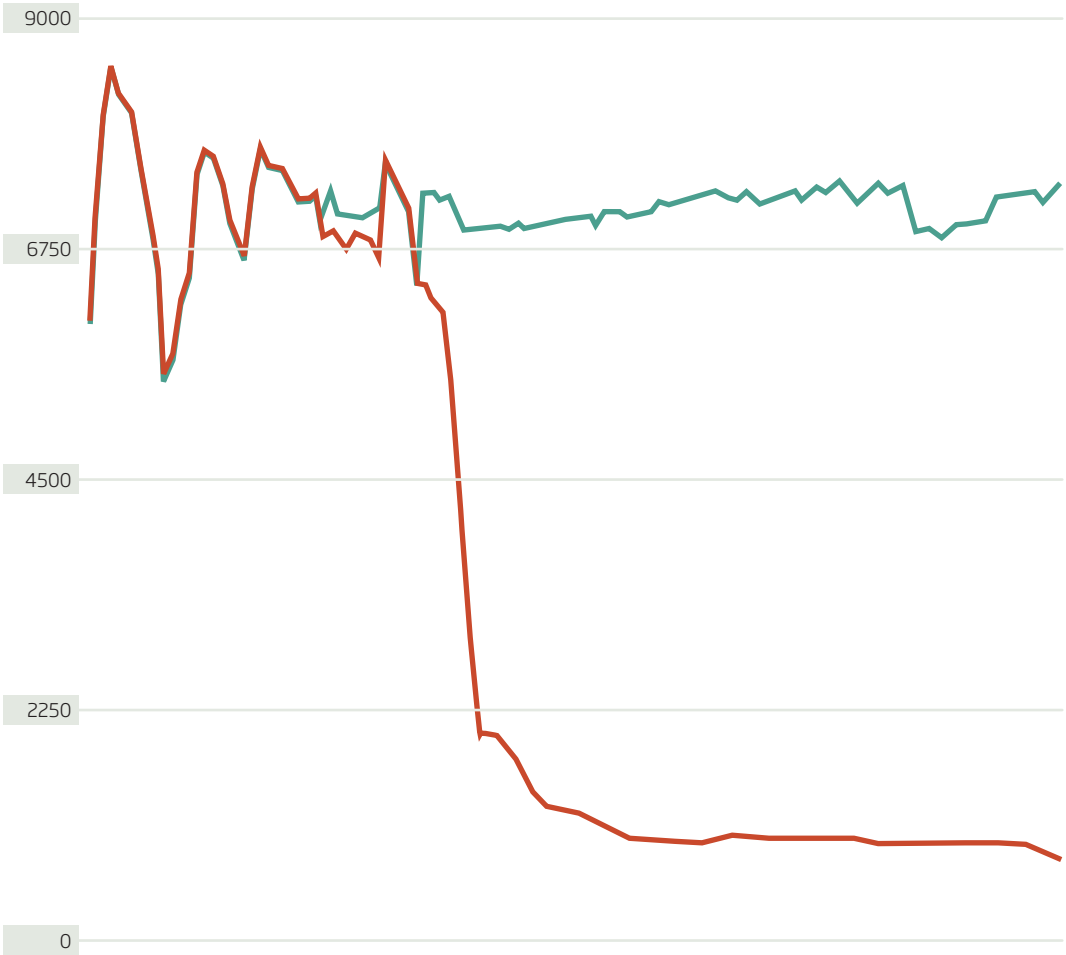
Izsiljevanje z napadi onemogočanja smo v prejšnjih letih na SI-CERT že obravnavali, šlo je za posamezne primere, pri katerih so sledi za storilci kazale v Libijo in Alžir. Leta 2015 je skupina **DD4BC** (Distributed Denial-of-service for Bitcoin) izvajala napade na različne tarče po vsem svetu in grozila s še močnejšimi napadi, če odkupnina (v začetku 25 BTC) ne bo plačana. Skupina je nato dobila posnemovalce, med katerimi je izstopala skupina z imenom **Armada Collective**, proti koncu leta pa smo bili obveščeni, da se napadi izvajajo tudi v sosednjih državah. Preventivno smo izdali obvestilo, namenjeno operaterjem, ponudnikom gostovanja, bančnemu sektorju in upravljavcem državne informacijske infrastrukture, ki so najpogosteje bili tarča tovrstnega izsiljevanja. V obvestilu smo opisali priporočene preventivne ukrepe in dali navodila za ukrepanje ob morebitnem napadu.

12. januarja 2016 je Europol objavil, da je v sodelovanju s policijami Avstrije, Bosne in Hercegovine, Nemčije in Velike Britanije zaključil akcijo, v kateri so izvedli aretacije in prekinili delovanje kriminalne združbe DD4BC, glavna osumljenca pa sta se nahajala v Bosni in Hercegovini (Republika Srpska). Vsaj začasno so se tudi posnemovalci potuhnili.

ZDRAVJE INFRASTRUKTURE

Internet je zgrajen na infrastrukturi, ki ni odporna proti zlorabam in različnim varnostnim ranljivostim. Že od leta 2012 dalje se npr. ukvarjamo z izrabo odprtih rekurzivnih DNS-strežnikov, a kot lahko vidimo po gibanju števila strežnikov, ki so na voljo v Sloveniji in se lahko izrabljajo za izvedbo porazdeljenih napadov onemogočanja (DDOS), je tudi tovrstne probleme mogoče obvladovati. Z nenehnim obveščanjem internet ponudnikov smo pripomogli k temu, da se je število teh strežnikov bistveno zmanjšalo. Napačno pa je zaspati ob uspešnih kampanjah, saj primerjalni graf odprtih NTP-strežnikov kaže, da bomo kmalu morali nasloviti tudi ta problem.

Gibljivo tedensko povprečje števila dostopnih DNS in NTP strežnikov v Sloveniji, ki se lahko izrabljajo v porazdeljenih napadih onemogočanja



Kritična infrastruktura

Obravnavali smo 60 primerov sistemov, ki so uporabljali ModBus- protokol (uporablja se za nadzor industrijskih naprav) in so bili dostopni brez mehanizmov nadzora dostopa.

SPLETNI STREŽNIKI

Leta 2013 smo skušali v sodelovanju s ponudniki gostovanja s pomočjo kampanje obveščanja lastnikov spletnih mest dvigniti zavedanje o tem, zakaj je pomembno tudi manjšim podjetjem nameniti nekaj pozornosti pri vzdrževanju lastnega spletnega mesta. Takrat smo opozarjali na večje število razobličenj (angl. defacement) spletnih strani, v letu 2015 pa so se zlorabljena spletna mesta v Sloveniji izkoriščala za širjenje okužb. Storilci z vdorom na spletno stran vrinejo obiskovalcu sicer nevidno programsko kodo, ki je del t. i. orodja »exploit kit«. Vrinjena koda zbere podatke o obiskovalčevemu brskalniku in vtičnikih, jih sporoči nadzornemu strežniku, ki vrne kodo za izrabo varnostnih ranljivosti, če te obstajajo. Obravnavali smo primere nameščenih **Angler** in **Orange Exploit Kit** orodij, na srečo pa nismo obravnavali nobenega bolj obiskanega spletnega mesta, ki bi lahko zaradi svoje popularnosti okužil večje število uporabnikov.

NoSQL

Zbirke podatkov v NoSQL-obliki so namenjene veliki količini podatkov, ki imajo fleksibilno strukturo in uporabljajo inovativne metode iskanja po zbirki. Veliko implementacij pa žal obravnava varnostne mehanizme kot manj potrebne, zato so različne MongoDB in Redis zbirke žal kar prosto dostopne vsakomur na internetu. V nekaterih primerih so te zbirke uporabljala slovenska podjetja tudi za hrambo osebnih podatkov.

STAGEFRIGHT

Varnostni strokovnjaki podjetja Zimperium so v programski knjižnici Stagefright, ki je ena izmed osnovnih sistemskih knjižnic sistema Android, našli več kritičnih ranljivosti, katerih izraba napadalcu omogoča oddaljeno izvajanje poljubne kode. Ob uspešni izrabi ranljivosti lahko napadalec zgolj s poznavanjem telefonske številke žrtve pridobi vsaj neposreden dostop do mikrofona, kamere in medija za shranjevanje, z izkoriščanjem katere od ranljivosti eskalacije privilegijev pa lahko v nadaljevanju pridobi tudi dostop do jedra sistema (t. i. root). Ranljiva koda se sproži ob predogledu video posnetkov, načinov izkoriščanja ranljivosti (t. i. vektorjev napada) pa je več: npr. prek MMS-sporočil, brskalnika, elektronske pošte, prenosov preko NFC in Bluetootha ipd.

Pri scenariju napada prek MMS-sporočil napadalec žrtvi pošlje zlonamerno MMS-sporočilo s posebej prirejenim posnetkom (exploit), ki izkoristi omenjeno ranljivost. V primeru uporabe aplikacije Hangouts se ranljivost aktivira brez kakršnekoli interakcije uporabnika, v primeru uporabe privzete aplikacije za sporočila pa se ranljivost aktivira ob ogledu sporočila.

Ranljivost je povzročila veliko razburjenja, tudi zaradi razširjenosti platforme Android in razdrobljenega tržišča, kjer ima vsak ponudnik telefonov svoje kanale za upravljanje z nadgradnjami telefonov. Kljub temu pa na SI-CERT nismo prejeli nobenega obvestila o primeru napada prek te ranljivosti.

Upravljanje z ranljivostmi

V letu 2015 smo prejeli nekaj obvestil, ki so se nanašala na ranljivosti spletnih aplikacij na strežnikih v Sloveniji. Šlo je za programske rešitve, razvite v Sloveniji, napake so bile enkrat enostavne, drugič bolj kompleksne, temu ustrezne pa so bile tudi posledice. Poleg bolj sistematičnega pristopa k upravljanju z ranljivostmi na SI-CERT se kot koristna zopet izkažeta neodvisni varnostni pregled kode in penetracijski testi še pred splovitvijo aplikacije.

USMERJENI NAPADI

VRIVANJE V POSLOVNO KOMUNIKACIJO

Omrežni napadi so lahko tudi tehnično zelo enostavni, kar je seveda razvidno tudi v drugem delu našega poročila, kjer pri programu ozaveščanja Varni na internetu veliko pozornosti namenjamo različnim goljufijam.

Koliko mislite, da je vreden dostop do vašega poštnega predala? Lahko zelo veliko, sploh če gre za račun, s katerega opravljate večino poslovne komunikacije svojega podjetja. Storilci lahko po vdoru vso vašo korespondenco pregledajo in se tako seznanijo s tem, kdo so vaše stranke ali dobavitelji ter kako in v kakšnih časovnih obdobjih poteka nabava in plačilo blaga oziroma storitev. V primernem trenutku se nato vrinejo v komunikacijo in skušajo preusmeriti nakazila na bančne račune pod njihovim nadzorom.

NAPAD PREKO NAPAJALIŠČA

Kot je usmerjeno zvabljanje (spear phishing) različica napada, ki je usmerjena na točno določeno skupino uporabnikov ali celo na posameznika, je napad prek napajališča (watering hole) različica okužbe v mimohodu (drive-by download), namenjena določenemu profilu uporabnikov. Napadalci izberejo spletno mesto (npr. proizvajalca vojaške opreme ali ponudnika strojnih in programskih rešitev za energetske sisteme), ki ga redno obiskujejo ti uporabniki, in z vdorom nanj podtaknejo trojanskega konja, ki okuži obiskovalce.

Poskus goljufije s preusmeritvijo nakazila v vrednosti skoraj 88.000 €

Dear Max

Thank you for the payment.
please kind cancel the payment you made to (SI562900[redacted] because we got a call that our company account has been overdraft and currently undergoing auditing,please kindly call off back your money and repay it to our united kingdom bank account below because we can receive money with this now.we will bear the charges for cancellation

BENEFICIARY NAME: [redacted] d.o.o.
ACCOUNT NUMBER:15223969
SORT CODE: 117180
IBAN NUMBER: GB98HLFX11718015223969
BIC\ SWIFT: HLFXGB21Z02
ADDRESS:3A Blackeen parade Blackeen road Sidcup Da15 9lu
BANK NAME: Halifax bank

Note that NTSH Jonathan also going to pay this week? I would appreciate if you could close also his due invoices.
The amount of its due invoices by end of February is 87.850,35 eur

I see that invoice nr. 15-310-00083 for Agripro is still not paid.
Could you please let me know why? It is about 200 pcs of Lezaforte 500 seeds from end of June 2015.

Please keep me informed.

Thank you and best regards,

VLOGA DRŽAVE

USPOSABLJANJE PRIPADNIKOV SLOVENSKE VOJSKE

SI-CERT izvaja usposabljanje pripadnikov Slovenske vojske na področju obravnavanja in preiskovanja računalniških incidentov v skladu s pogodbo, podpisano med Ministrstvom za obrambo RS in javnim zavodom Arnes. Zaradi ustanavljanja kapacitet za odzivanje na omrežne incidente v vojski ta seveda potrebuje kader, ki bo imel praktična znanja pri spopadanju s poskusi zlorabe obrambne informacijske infrastrukture. Ekipa SI-CERT na drugi strani s tem pridobi začasno kadrovsko okrepitev, ki je zaradi vsakoletnega povečanja obravnavanih incidentov nujna. Na ta način tudi skušamo omiliti posledice administrativnih ovir pri zaposlovanju v javnem sektorju.

ZAKONODAJA

Na podlagi Zakona o elektronskih komunikacijah (ZEKom-1, Ur. l. RS, št. 109/2012) in Splošnega akta o varnosti omrežij in storitev Agencije za komunikacijska omrežja in storitve AKOS (Ur. l. RS, št. 75/2013) so operaterji elektronskih komunikacij dolžni o varnostnih incidentih poročati agenciji, ta pa operativno razreševanje incidenta po potrebi in glede na kršitev preda SI-CERT z namenom, da slednji strokovno pomaga in svetuje operaterju, usklajuje udeležence znotraj države ter koordinira odzivne CERT-centre in druge sorodne službe v tujini.

VAJE IZ KIBERNETSKE VARNOSTI

SI-CERT je v letu 2015 sodeloval v vaji iz kibernetske varnosti Cyber Coalition 15, ki jo organizira zveza NATO in je vključevala nacionalne odzivne centre, saj se je preverjalo zmožnost odzivanja na ravni države.

STRATEGIJA KIBERNETSKE VARNOSTI

Leta 2015 je bila dokončana Strategija kibernetske varnosti. Pri pripravi so sodelovala skoraj vsa ministrstva, sami pa smo podali predloge s stališča učinkovite obravnave omrežnih incidentov. Zagovarjali smo sistem postopne nadgradnje obstoječih kapacitet in krepitev tam, kjer že imamo učinkovite mehanizme izboljševanja omrežne in informacijske varnosti. Strategija je bila tudi sprejeta v začetku leta 2016 in bo prispevala k več kot potrebnemu kadrovskemu reševanju na področju odzivanja na omrežne incidente na ravni države.

SLOVAR POJMOV

APT - Advanced Persistent Threat

Množica dolgotrajnih in prikritih omrežnih napadov, običajno organiziranih za vdor v posamezno ustanovo. Pogosto se tem napadom pripisuje politične ali gospodarske motive in ozadja, odkriti pa so lahko šele po nekaj mesecih ali celo letih.

Drive-by Download

Okužba v mimohodu je način okužbe, pri kateri se škodljiva koda podtakne na popularna spletna mesta, s čimer so ogroženi vsi obiskovalci, ki uporabljajo brskalnike ali dodatke zanje, le-ti pa vsebujejo varnostne ranljivosti. Z rednim posodabljanjem programske opreme bistveno zmanjšamo tovrstno ogroženost.

Exploit kit

Programski paket, ki izvaja okužbe v mimohodu in se v najem ponuja na črnem trgu. Predstavlja mehanizem okužbe, »tovor« pa so različni boti, izsiljevalski virusi, bančni trojanci in podobno. Trenutno najbolj razširjena sta »Angler« in »Nuclear«, v preteklosti pa »Blackhole«.

Ransomware

Izsiljevalski virusi ali druga škodljiva koda, ki zaklene računalnik ali šifrira podatke na njem in od žrtve zahteva plačilo odkupnine v zameno za ključ za povrnitev podatkov.

Sextortion

Prevara, v kateri se z lažnim profilom privlačnega dekleta prepriča žrtev (običajno moškega v srednjih letih), da posname in nato pošlje intimne posnetke, storilci pa mu zagrozijo z njihovo objavo na spletu in družbenih omrežjih. Kot rešitev zagate ponudijo odkupnino.

SCADA – Supervisory Control And Data Acquisition

Računalniški sistem za oddaljeni nadzor in spremljanje stanja naprav, ki se uporabljajo v različnih industrijskih procesih ter sistemih za proizvodnjo in prenos energije.

Social Engineering

Družbeni inženiring je psihološka manipulacija žrtve z namenom razkriti informacije ali izvedbo nalog, ki omogočijo nepooblaščen dostop v sistem ali neko neposredno oškodovanje.

Stagefright

Ranljivost v multimedijski knjižnici operacijskega sistema Android, ki napadalcu omogoča izvedbo poljubne programske kode brez uporabnikove vednosti ali potrditve. Raziskovalci so demonstrirali prevzem nadzora nad mobilno napravo že s pošiljanjem MMS-sporočila.

Vulnerability Management

Upravljanje z ranljivostmi je proces njihove identifikacije v programski opremi, omejevanje njihovega vpliva in običajno na koncu tudi odstranjevanja.

Watering Hole Attack

Strategija omrežnega napada, ki meri na določeno skupino uporabnikov (organizacijsko, regijsko ali po poslovnem področju). Z usmerjenimi napadi na spletne strežnike, ki jih skupina redno obiskuje, se poskuša okužiti obiskovalce (»okužba v mimohodu«).

VARNI NA INTERNETU

Od mene je odvisno vse.

Poročilo projekta Varni na internetu

ZDI SE, DA NAS INTERNET PREHITEVA

Postali smo navdušeni sledilci, uporabniki in glasniki spletnih servisov. Tako se veselimo novih storitev in hkrati pozabljamo, da z velikimi tehnološkimi koraki, ki poenostavljajo naše delovne procese, prihajajo tudi velike odgovornosti. Spletni ponudniki in posredniki so odgovorni, da dostavijo storitve in omogočijo njihovo varno delovanje, na nas uporabnikih pa je, da spletne storitve uporabljamo v skladu s pravili in pogoji uporabe ter z nič manj previdnosti, kot smo doslej njihove nedigitalne predhodnike. Za primer vzemimo kartično poslovanje; na POS-terminalu zaščitniško zakrivamo PIN-številko, a takoj zatem svojo kreditno kartico zaupamo spletni trgovini sumljivega izvora.

Ogoljufani niso računalniški analfabeti, ampak povprečni uporabniki, ki ne upoštevajo priporočil za varno uporabo spletnih storitev, saj zase verjamejo, da se jim ne more nič zgoditi. V letu 2015 se je prvič, kar od leta 2008 na SI-CERT beležimo statistiko prijav, zgodilo, da je število prijavljenih spletnih goljufij preseglo število prijavljenih tehničnih incidentov; izsiljevalski virusi, phishing napadi, prevare pri spletnem nakupovanju, izsiljevanja s skrivaj pridobljenimi intimnimi posnetki in ostale goljufije, ki se širijo prek družbenih omrežij. Ti incidenti samo pritrjujejo strokovnjakom za kibernetsko varnost po celem svetu, ki tudi v letu 2016 kot največjo grožnjo izpostavljajo spletne goljufije in izsiljevalske viruse. Skrbi pa nas lahko dejstvo, da za izpeljavo večine teh goljufij napadalci niso potrebovali naprednega računalniška znanja, zadostovale so že preproste tehnike socialnega inženiringa. Davek za našo neozaveščenost, naivnost in nepoznavanje spletnih mehanizmov torej že plačujemo.

Upanje na pregon kriminalcev je skoraj brezpredmetno. Pristojnosti institucij pri reševanju spletnega kriminala se končajo na meji Evropske unije, kar s pridom izkoriščajo goljufi. Ti svoje spletne strani postavljajo na tujih strežnikih, skrivajo se za generičnimi elektronskimi naslovi, uporabljajo kriptirane plačilne valute in nas kontaktirajo iz lažnih profilov. Ne nazadnje je spletne kriminalce praktično nemogoče izslediti tudi zato, ker pogosto prihajajo iz držav tretjega sveta, kjer njihova zakonodaja močno šepa in na možnost pregona lahko računamo le izjemoma. Anonimnost, ki jo omogoča internet, v svetu kiberkriminala igra na strani slabih fantov.

Nekatere številke so nas v letu 2015 razveselile bolj kot druge. Porast spletnih goljufij je ob internetnem razmahu neizbežen, vendar številke na družbenih omrežjih in obiskovalci na spletni strani potrjujejo naše dobro delo in program Varni na internetu postavljajo na čelo vseh aktivnosti ozaveščanja o spletnih nevarnostih v Sloveniji, naša prizadevanja pa prepoznavajo tudi ostale organizacije in podjetja. Naša pot se tukaj ne zaključi; če smo se približali svojim ciljem, je sedaj čas, da postavimo nove!

Marta Štefanič, program Varni na internetu 

O PROGRAMU VARNI NA INTERNETU

Nacionalni program Varni na internetu smo v letu 2011 na SI-CERT zasnovali prav z namenom pomagati, ozaveščati in izobraževati širšo javnost glede varne uporabe interneta in prepoznavanja tveganj. Portal je zasnovan kot bogata zbirka jasnih in natančnih navodil, kako lahko uporabniki zavarujejo svojo spletno identiteto, računalniško opremo in ne nazadnje tudi svoj bančni račun. Celostno platformo dopolnjujejo izobraževalni članki in opozorila ter navodila za ukrepanje ob težavah.

Cilji programa so:

- poučiti spletne uporabnike, kako naj prepoznajo različne oblike spletnih goljufij,
- informirati o varni uporabi storitev elektronskega bančništva in varnem spletnem nakupovanju,
- poučiti spletne uporabnike, kako naj zavarujejo svojo osebno identiteto na spletu, zlasti na družbenih omrežjih.

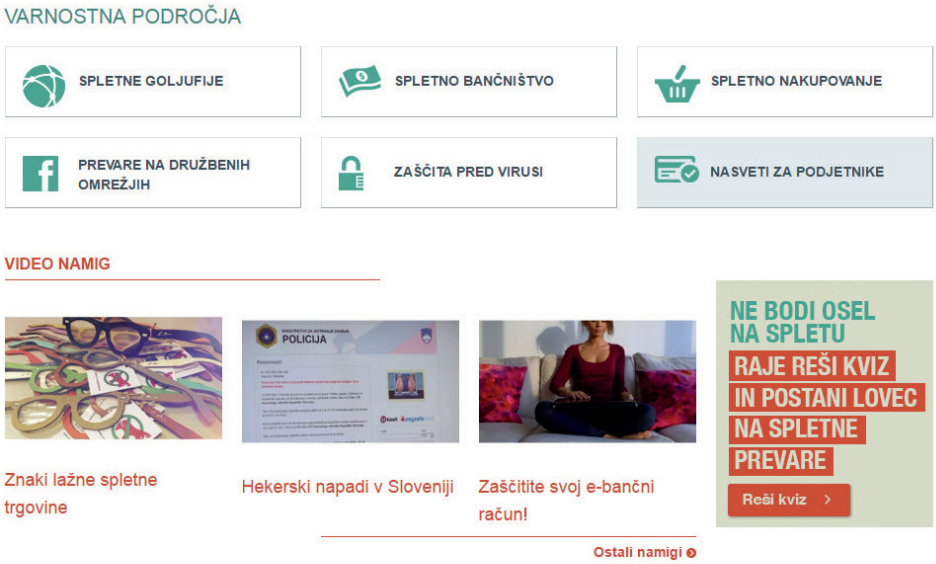
Vsebine programa Varni na internetu naslavljajo široko slovensko spletno javnost, merimo pa predvsem na odraslega spletnega uporabnika, ki uporablja storitve spletnega bančništva, redno uporablja družbena omrežja, elektronsko pošto, nakupuje in na spletu opravlja počitniške rezervacije. Številni opisani primeri prevar in podani nasveti so dobrodošli tudi za manjša podjetja, ki prav tako potrebujejo informacije, kako naj zagotovijo varno spletno poslovanje.

Slogan "Od mene je odvisno vse" prinaša osnovno sporočilo programa ozaveščanja; ravno uporabniki sami lahko največ storijo za svojo varnost na spletu.

Naše svetovanje je brezplačno za vse slovenske uporabnike, tako posameznike kot tudi podjetja. Z nami lahko vzpostavite kontakt prek vseh komunikacijskih kanalov: elektronske pošte, na Facebooku ali Twitterju. Za učinkovitejšo obravnavo prijav se na spletni strani www.varninainternetu.si nahaja kontaktni obrazec, aktualni elektronski naslov za prijavo incidentov pa je cert@cert.si.

1 PREVENTIVA

Središče vseh aktivnosti programa je spletni portal. Zasnovali smo ga z namenom, da postane ključen vir informacij s področja informacijske varnosti in **prvi naslov, ko spletni uporabnik ali uporabnica potrebuje nasvet oziroma pomoč**. Na vstopni strani tako uporabnike pričakajo tematski sklopi: Spletne goljufije, Spletno bančništvo, Spletno nakupovanje, Prevare na družbenih omrežjih, Zaščita pred virusi in Nasveti za podjetnike.



2 AKTUALNO

Redno obveščanje o novoodkritih spletnih goljufijah je ključnega pomena za zajezitev števila žrtev. Uporabnike obveščamo o prevarah, phishing straneh, virusih, lažnih spletnih trgovinah, prevarah na družbenih omrežjih itd.

3 ELEKTRONSKI NOVIČNIK VARNE NOVICE

Dodaten komunikacijski kanal predstavlja elektronski novičnik, ki ga 2x mesečno oz. ob zaznani povečani intenzivnosti spletnih tveganj prek elektronske pošte pošiljamo prejemnikom, ki so se pred tem registrirali na našem portalu.

4 DRUŽBENA OMREŽJA

Kot se je izkazalo, družbena omrežja niso zgolj vir težav, ampak predstavljajo tudi izjemno učinkovit kanal za obveščanje o aktualnih spletnih grožnjah.

Facebook stran Varni na internetu in Twitter račun sta zaživela kot čisto samostojna 'svetovalca'. V letu 2015 je število oboževalcev na Facebook strani preseglo 20.000, številka pa se je ustavila pri 21.700. Na Twitterju nam sledi 1250 uporabnikov, dejavni pa smo tudi na YouTube, na našem kanalu smo zbrali že več kot 40 izobraževalnih avtorskih video posnetkov.

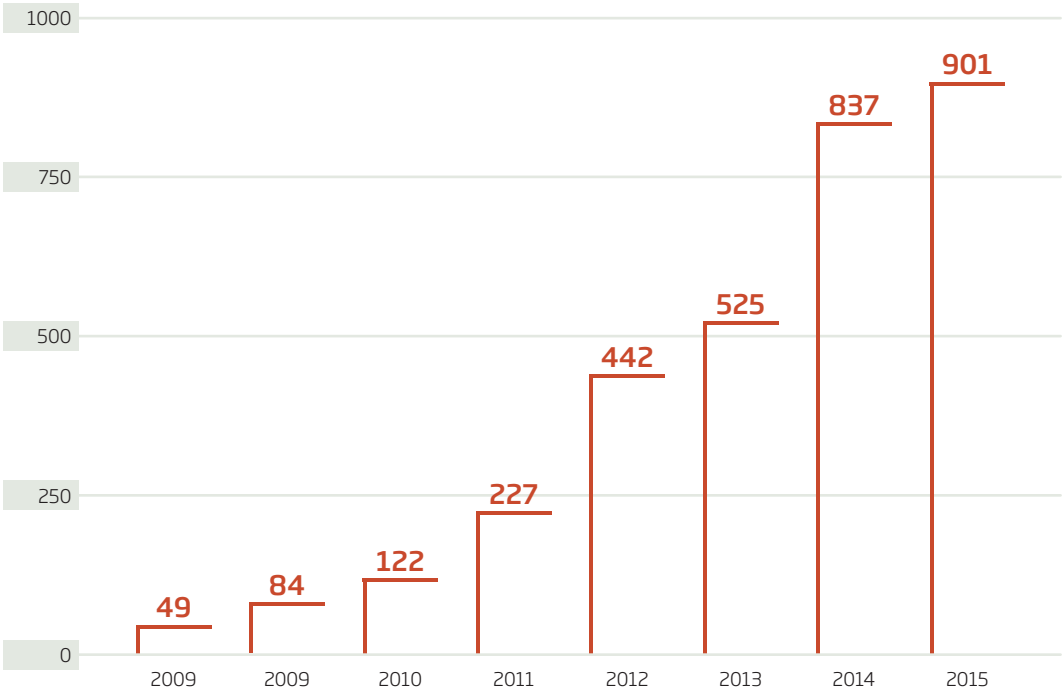
VARNI
NA INTERNETU
Od mene je odvisno vse.

5 NACIONALNA PRIJAVNA TOČKA

Da bi spletni uporabniki v Sloveniji čim hitreje prejeli odgovore na vprašanja in pomoč, ko to najbolj potrebujejo, smo uvedli spletno prijavno točko. Na portalu se nahaja izpostavljen gumb 'Prijavi prevaro', ki vodi do spletnega obrazca, s katerim lahko oškodovanci prijavijo omrežni incident (okužbo z zlonamerno kodo, spletno goljufijo, krajo gesla itd.).

Pomagamo in svetujemo strokovnjaki nacionalnega centra SI-CERT, naše znanje pa je vsem spletnim uporabnikom na voljo brezplačno, saj so vse aktivnosti programa financirane s strani Ministrstva za izobraževanje, znanost in šport RS. Od začetka programa ozaveščanja je najopaznejši porast prijav spletnih prevar. Številke so zelo zgovorne – leta 2010 smo obravnavali 122 primerov spletnih prevar, leta 2015 pa kar 901, v povprečju 2,5 primera na dan.

PORAST PREVAR



KLJUČNA TVEGANJA V LETU 2015

PREVARE NA DRUŽBENIH OMREŽJIH

Od nagradnih iger z iPhoni ter vinjetami, lažnih oglasov za delo, goljufivih ponudnikov športnih stav do ljubezenskih prevar in porno virusov. Uporaba družbenih omrežij očitno ni tako enostavna, kot mnogi mislijo, vsaj glede na statistko goljufij ne. Politika uporabe upravljavcem omrežja zapoveduje dosledno umikanje samo skrajno spornih vsebin, kar pomeni, da številne manjše goljufije ostanejo nekaznovane. Pregon takšnih kriminalcev je praktično nemogoč. Facebook je ameriško zasebno podjetje, ki podatkov o svojih uporabnikih ne izdaja kar tako; vpogled imajo samo organi pregona, pa še to v izjemnih primerih – če gre za preprodajo drog, orožja, otroško pornografijo itd. Resnično identiteto uporabnika, ki se skriva za lažnim uporabniškim računom, je praktično nemogoče odkriti. Da, družbena omrežja se goljufom izplačajo.

LAŽNE SPLETNE TRGOVINE

V letu 2015 so slovenski potrošniki zaupali številnim spletnim trgovinam s poceni izdelki blagovnih znamk Michael Kors, Ugg, Longines, RayBan, Salomon, Nike LeBron in mnogih drugih, ki so se oglaševale kar na družbenih omrežjih. Čeprav so spletne trgovine stale na nemški (.de) ali italjanski (it.) domeni, je izdelek do kupca potoval precej časa. Trgovine so bile locirane nekje na Kitajskem, poceni izdelki pa so se izkazali za ponaredke. Slednje predstavlja težavo samo za evropskega potrošnika in ne kitajskega proizvajalca. Tam so namreč uveljavljena neka čisto drugačna pravila o zaščiti intelektualne lastnine, pri nas pa je prodaja in kupovanje ponaredkov prepovedano; zasežejo jih na carini in pošljejo v uničenje. Oškodovani potrošniki z oddaljenim podjetjem niso mogli doseči nobene poravnave in zopet se je izkazalo, da za svojo varnost na spletu lahko največ storimo prav mi sami!

IZSILJEVANJE Z INTIMNIMI POSNETKI

Vrsta spletnega kriminala, poznanega tudi pod izrazom sextortion, je bila dolga leta samo tema na tujih naslovnicah, pri nas pa so bili posamezni primeri vezani na razprtije med bivšima partnerjema. Meseca maja je našo dejavnost zadel popolnoma drugačen primer. S slovenskimi uporabniki so na družbenem omrežju vzpostavile kontakt privlačne neznanke in jih vabile k videoklepetu na Skype. Za ženskimi profili so delovale kriminalne združbe, njihov edini cilj pa je bil pripraviti sogovornike h kočljivim položajem, jih ob tem posneti in tako pridobiti material za izsiljevanje. Žrtvam so grozili z objavo posnetkov na družbenih omrežjih, zneski izsiljevanj pa dosegajo višino tudi po 1000 in več EUR. Uporabnikom smo svetovali popolno prekinitev komunikacije, kar se je izkazalo za najučinkovitejši ukrep, večkrat je bila potrebna tudi pomoč pri umiku spornih posnetkov s spleta. V večini obravnavanih primerov so plačila izsiljevalcem prek sistema Western Union romala na Slonokoščeno obalo, kar je dvojna slaba novica za žrtve. Plačilni sistem ne omogoča sledljivosti denarnega toka pa tudi evropska zakonodaja in naši organi pregona v zahodnih državah podsaharske Afrike nimajo prav nobenega vpliva.

AIRBNB PREVARA

Za svoje delovanje spletni prevaranti pogosto izkoriščajo priljubljen in zaupanja vreden spletni portal za posredovanje in najem nepremičnin popotnikom. Na sicer popolnoma legitimni in dobro delujoči spletni platformi naredijo svoj profil, iskalce namestitve pa opozorijo nase z izjemno lokacijo, ugodno ceno, dobro opremo. Ravno 'neverjetna ponudba' je njihov glavni adut, s katerim uporabnike prepričajo, da za trenutek pozabijo na pogoje uporabe spletne platforme, in jih skušajo zavesti k neupoštevanju pravil. Ko so uporabniki zavedeni k rezervaciji in plačilu zunaj spletnega mesta AirBnb in gre nekaj hudo narobe, niso več upravičeni do povračila denarja. Goljufi so v svoji komunikaciji izredno prepričljivi. Z vami delijo svojo življenjsko zgodbo: razložijo, da je to stanovanje njihove hčerke, ki je zanosila in se s svojim izbrancem preselila v drugo državo in sedaj iščejo zanesljivega najemnika, saj so sami zboleli za rakom. Zgodbe so sicer različne in zastavljene z veliko domišljije, a vsem je skupno eno: s potencialno žrtvijo skušajo vzpostaviti zaupljiv odnos in jo čim prej prepričati, da jim nakaže svoj denar. Na naši spletni strani smo pripravili seznam ključnih znakov, ki kažejo na prevaro, in nasvete, kako ravnati, ko z vami na spletni platformi Airbnb vzpostavi kontakt goljufiv ponudnik.

KIBERNETSKA VARNOST JE NAŠA SKUPNA ODGOVORNOST!

Tako se je glasilo geslo vseevropske akcije Oktober – mesec kibervarnosti (European Cyber Security Month), ki je pod okriljem Agencije Evropske unije za varnost omrežij in informacij (ENISA) potekala v mesecu oktobru že peto leto zapored. Namen akcije je bil izpostaviti, kako nujno je, da spremenimo dojemanje in naš odnos do informacijske varnosti ter kibernetskih groženj. Akcije se je udeležilo 27 evropskih držav, Slovenijo je že četrtič zapored zastopal SI-CERT z nacionalnim programom ozaveščanja Varni na internetu.

Oktobra smo javnost nagovorili s kampanjo, ki je opozarjala na spletne prevare **z resnimi finančnimi posledicami**, njeno snovno sporočilo je bilo 'Neverjetne ponudbe ne obstajajo'. Z različnimi komunikacijskimi aktivnostmi smo opozarjali na najbolj pereče teme: **lažne spletne trgovine s traktorji in gradbeno mehanizacijo, goljufive spletne ponudbe za kredit, lažne nagradne igre na Facebooku in izsiljevanje na spletu.**

Glavno komunikacijsko orodje kampanje ozaveščanja so bili **privlačni oglasi** na družbenih omrežjih in pasice na najbolj obiskanih novičarskih portalih. Oglasi so posnemali tipične vabe, ki jih goljufi v vsakdanjem življenju uporabljajo, da naivne uporabnike zvabijo k sodelovanju. Neverjetna ponudba, ugodni pogoji, nizka cena, visoki popusti.

Namesto neverjetne ponudbe je uporabnika po kliku na oglas pričakala prevara. Oglas je vodil na pristajalno stran, kjer smo z zgovornimi statističnimi podatki, resnično zgodbo slovenskega uporabnika in videovodičem bralce podučili, kako prevara poteka in na katere znake naj bodo pozorni, da ji tudi sami ne bodo nasedli.

VARNI NA INTERNETU

NAJVEČJE OŠKODOVANJE Z LAŽNIMI KREDITI V LETU 2014 JE ZNAŠALO 9000 EUR.

Mateja je iskala ugoden premostitveni kredit. Preverila je vse ponudbe bank, a je najugodnejšega ponudnika našla kar v svojem elektronskem poštnem predalu:

"Ali ste v finančni krizi? Ali ste že zavrnili banke za posojilo? Ali potrebujete denar nujno? Ali potrebujete posojilo za širitev vašega podjetja? Ste iskali posojilo? Ste prišli na pravo mesto. To posojilo je 100 % zagotovljena. Contact me zdaj in dobili kakovostne storitve. Gospa Ebis Vivian (finaid45@hotmail.com)".

Prijazna gospa Vivian, ki se je predstavila kot direktorica Scottish National Bank, je Mateji odobrila 10.000 EUR kredita. Mateja je gospe Vivian za odobritev kredita plačala 320 EUR prek sistema Western Union. Kmalu, ko o 10.000 EUR ni bilo ne duha ne sluha, je poprej prijazna gosta Vivan nehala odgovarjati na Matejina elektronska plačila.

Mateja Novak

KAKO SE ZAVAROVATI?

Prepoznajte prevaro:

1. Oglas za hitri spletni kredit ste našli na forumu, Facebooku ali pa ste ga dobili kar v elektronskem sporočilu!
2. Od vas želijo, da različne stroške (odobritev kredita, odprtje računa, davek itd.) poravnate prek sistema Western Union. Ta namreč ne omogoča sledljivosti denarja in je ravno zato priljubljeno orodje spletnih goljufov.
3. ''Contanct me zdaj.'' - ne verjemite oglasom v polomljeni slovenščini.
4. NAMIG: Nikoli in pod nobenimi pogoji se ne dogovarjajte za kredit prek spleta!

SODELUJOČI V MESECU OKTOBRU

V oktobrski kampanji ozaveščanja so se nam pridružili: Urad informacijske pooblaščenke, Laboratorij za odprte sisteme in mreže na Institutu Jožefa Stefana in Ministrstvo za obrambo RS. V letu 2015 je v kampanji prvič sodeloval tudi medijski sponzor, Salomon. Veseli nas, da pomen ozaveščanja prepoznavajo tudi ostale institucije in podjetja v Sloveniji.

TOP 5 NASVETOV ZA SPLETNO VARNOST

Spletnim goljufom ne nasedajo vedno samo naivneži in računalniški analfabeti. Sodobnih spletnih groženj ne moremo zožiti na nigerijske prevare, klikanje sumljivih gumbov na straneh za odrasle in prenašanje igric neznanega izvora. Tarča goljufov so tudi naši podatki in ni res, da nimamo česa za skrivati. Z vdorom v uporabniški profil se začnejo številne spletne goljufije in zlorabe, ki smo jih uporabniki omogočili kar sami – s slabimi varnostnimi in drugimi nastavitvami. Zato smo v začetku leta pripravili infografiko Top 5 nasvetov za spletno varnost, ki uporabnika zavarujejo pred najpogostejšimi zlorabami in prevarami na spletu. Za vse nastavitve lahko poskrbijo sami, saj nobena od njih ne zahteva naprednega računalniškega znanja.

TOP 5 NASVETOV ZA SPLETNO VARNOST

1 DVOSTOPENJSKA AVTENTIKACIJA

Aktiviraj jo danes! Gre za preverjanje v dveh korakih in mnogo ponudnikov jo že omogoča (Google račun, Outlook, Facebook, Twitter, Dropbox itd.) Ko se prijavljaš v račun, dobiš na mobilni telefon še dodatno, enkratno kodo ali pa dodatno kodo generiraš z aplikacijo na pametnem telefonu. To bistveno zmanjša možnost zlorabe, saj če ti nekdo ukrade geslo, se vseeno ne bo mogel prijaviti v tvoj račun.

2 MOČNO UNIKATNO GESLO

Poskrbi za močna gesla. Danes takoj zamenjaj gesla 123456, password, geslo123, kombinacije imena in priimka, letnice rojstva itd. In ne uporabljaj enega gesla za vse storitve.

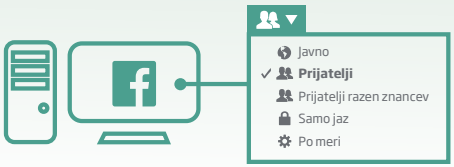
Več nasvetov in pomoč, če pride do težav, najdeš na portalu **VARNI NA INTERNETU**.

3 BACKUP

Ustvari si varnostno kopijo pomembnih dokumentov, shranjenih na osebnem računalniku, pametnem telefonu ali tablici. Močno priporočamo, da za backup uporabiš medij, fizično ločen od računalnika in omrežja, npr. zunanji disk, ki ga po izdelavi backupa iztakneš iz računalnika.

4 OMEJI VIDNOST FACEBOOK OBJAV

V zavihku Nastavitve – Zasebnost izberi možnost Prijatelji. To pomeni, da bodo statusi, fotografije, video posnetki vidni le Facebook prijateljem.



5 ZAKLENI TELEFON

Ker je fizični dostop do mobilne naprave veliko lažji, so tudi vsi shranjeni podatki bolj izpostavljeni. Zato je nujno, da uporabljaš PIN-kodo za zaklep SIM kartice in kodo za zaklep zaslona (vzorec na tipkovnici, še bolje pa PIN ali geslo).

VARNI NA INTERNETU – KOLUMNA V DELU

V letu 2015 smo se pridružili Delovi angažirani rubriki Zaženi se, ki obravnava problematiko, zanimivo širokemu krogu bralcev, ponuja rešitve, spodbuja ljudi k večji družbeni in individualni aktivnosti. Bralce ozaveščamo s članki o varnem nakupovanju, varnem spletnem bančništvu, varovanju digitalne identitete in nenehno poudarjamo, kako pomembno je, da spremenijo dojemanje pomembnosti spletne (ne)varnosti. Sodelovanje nadaljujemo tudi v letu 2016.

DELO

četrtek, 21.01.2016

Novice | Svet | Gospodarstvo | Mnenja | Šport | Kultura | Znanje | Prosti čas | Multimedija | Naroči se

Znanje › Potrošnik › Varni na internetu: Kako hudo je, če vam vdrejo v elektronsko pošto?

Sobotna | Ozadja | NeDelo

Tweet | G+1 1 | Recommend 60

Varni na internetu: Kako hudo je, če vam vdrejo v elektronsko pošto?

Tudi nenavadna pošta, ki smo jo prejeli od znancev in prijateljev, je lahko draga šola za našo denarnico in zasebnost.

Marta Štefanič
tor, 05.01.2016, 10:00

Ključne besede: Varni na internetu, elektronska pošta, E-pošta, vdor, zaščita

Podobne vsebine, ki jih zdaj berejo drugi

Varni na internetu: Vsi obrazi spletnega izsiljevanja
15. december ob 10:00

Varni na internetu: 9 top prevar na družbenih omrežjih
3. november ob 10:00

Varni na internetu: Spletno bančništvo
22. september ob 10:00

Varni na internetu: Kaj delajo računalniški hekerji?
24. november ob 10:00

Varni na internetu: Kibernetska varnost je naša skupna odgovornost!
13. oktober ob 10:00

Varni na internetu: Goljufive ponudbe za hitri kredit prek spleta
1. september ob 10:00

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