POROČILO O OMREŽNI VARNOSTI ZA LETO 2013

SKOZI RAČUNALNIK V VAŠO DENARNICO

arnes si·cert VARNI NA INTERNETU

si·cert

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni center za obravnavo omrežnih incidentov.
Na elektronskem naslovu cert@cert.si ali telefonski številki (01) 479 88 22 lahko prijavite vdor v računalnik ali poskus druge zlorabe prek omrežja. Po sklepu Vlade Republike Slovenije št. 38600-3/2009/21 z dne 8. 4. 2010 ter v skladu s sporazumom med Ministrstvom za javno upravo (sedaj Ministrstvo za notranje zadeve) z dne 31. 5. 2010 SI-CERT opravlja naloge vladnega centra za odzivanje na omrežne incidente.

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

Dejavnosti centra SI-CERT financira Direktorat za informacijsko družbo Ministrstva za izobraževanje, znanost in šport.

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

KAZALO

OMREŽNA VARNOST V LETU 2013

V prvem tednu januarja prejmemo *obvestilo o vdorih* v kar 200 Joomla spletnih strežnikov. Nekateri od teh so uporabljeni za napade na banke v ZDA.

Skupaj z uradom Informacijskega pooblaščenca izdamo priročnik *ABC varnosti in zasebnosti na mobilnih napravah*.

Policija v sodelovanju z Uradom za preprečevanje pranja denarja in SI-CERT razkrinka kriminalno združbo, ki je vdirala v elektronske bančne račune in skupaj prenakazala kar 2 milijona evrov (*primer Balkanboy*).

18 slovenskih internet ponudnikov obvestimo o približno 5.200 DNS-strežnikih njihovih strank, ki se uporabljajo za napade onemogočanja z odbojem.

Število novih razobličenj slovenskih spletnih mest ta mesec pade malo pod 200. Slovenskim ponudnikom gostovanja ob pomoči registra slovenskih domen predstavimo *predlog kampanje o varnem spletnem mestu* za njihove lastnike in jih pozovemo k sodelovanju.

Skupina Anonymous v operaciji #OpUSA izvede napade na strežnike v ZDA, tudi s pomočjo brbot botneta, v katerem se znajde 14 slovenskih strežnikov.

Prejmemo več prijav glede sumljivih klicev na stacionarne telefonske številke v Sloveniji. *Klicatelj se v polomljeni angleščini predstavi kot Microsoftova tehnična pomoč* in razloži, da nujno kliče, ker je njegov računalnik okužen. Gre za goljufijo, ki je že dolgo znana, tokrat pa so goljufi prvič klicali v Slovenijo.

JANUAR

Nekaj strežnikov v Sloveniji je okuženih z Linux SSHD rootkitom. Prejmemo podatke *o ciljanih napadih* na državne ustanove z MiniDuke trojancem.

Med Facebook uporabniki se hitro širi *lažna nagradna igra*. Seveda, saj obljubljajo kar 100 MacBook Pro prenosnikov.

FEBRUAR

MAREC

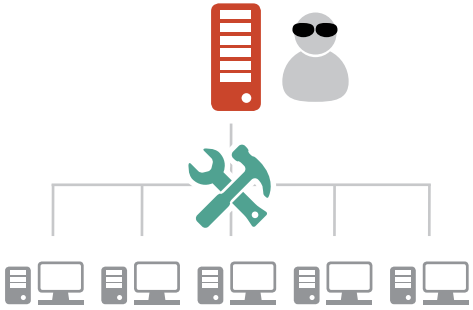
Izdamo *Poročilo o omrežni varnosti za leto 2012*. Med poglavitnimi temami je "hektivizem", pomembna novost lanskega leta so tudi prvi resni napadi na komitente slovenskih bank.

V napadu onemogočanja zasledimo, da sodelujejo tudi tiskalniki oz. multifunkcijske naprave. Na SI-CERT menimo, da se jim bodo v prihodnosti pridružile tudi druge naprave, povezane v internet stvari.

APRIL

MAJ

Microsoft sporoči, da v sodelovanju z FBI začenja z operacijo b54 za "demontažo" Citadel botneta in prosi nacionalne odzivne centre za pomoč. V Sloveniji sta dva nadzorna strežnika botneta.



JUNIJ

Nenavaden *porast prijav o okužbah z Ukash* (tudi Reveton ali Urausy) izsiljevalskim virusom, ki v imenu policije zaklene računalnik in zahteva odkupnino. Kasneje bomo videli, da je to le začetek velikega vala okužb, ki bo trajal vse do konca leta.

Izdamo kratek vodič Varni na internetu, tudi na počitnicah, ki opisuje *najpogostejše počitniške goljufije*; vse na enem mestu, od lažnih apartmajev, brezžičnega povezovanja do varnega plačevanja s kreditno kartico.

Zaznamo prve okužbe z izsiljevalskim virusom Cryptolocker, ki zašifrira datoteke na disku in za odšifriranje zahteva odkupnino.

Prejmemo mali in veliki POMP – nagradi s področja vsebinskega marketinga za naj letno poročilo in naj projekt s področja vsebinskega marketinga.

Na dogodku Posvetovanje o informatiki v energetiki Slovenije predstavimo slabo zaščito ene od slovenskih hidroelektrarn ter težave toplotnih postaj in pametnih števcev.

SI-CERT sodeluje na vaji NATO Cyber Coalition 2013.

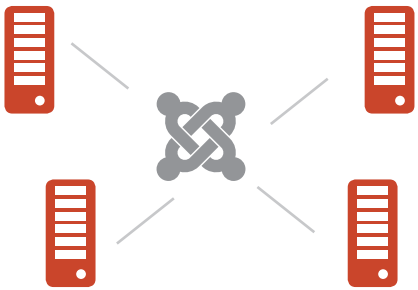
20 let Slovenije na spletu! Novembra 1993 je Mark Martinec na Institutu Jožef Stefan vzpostavil spletni strežnik s prvimi slovenskimi stranmi in spletno predstavitvijo Slovenije.

Portal *www.varninainternetu.si* dobi novo podobo. Preglednejša organizacija vsebin, nove funkcionalnosti, enostavnejše iskanje glede na uporabo različnih spletnih storitev.

JULIJ

30 zlorabljenih Joomla strežnikov je povezanih v botnet in sodeluje v izvajanju napadov onemogočanja, nam sporoči US-CERT.

Si.mobil skupaj s Fakulteto za varnostne vede, SI-CERT ter Zavodom Ypsilon in njegovim projektom Simbioza pripravi *brošuro o varni in brezskrbni uporabi mobilnikov* tudi v tretjem življenjskem obdobju.



AVGUST

SEPTEMBER

V 25 državah EU se začne prvi celovit *evropski mesec kibervarnosti*. Slovenija sodeluje s programom Varni na internetu, več pozornosti namenjamo manjšim podjetjem oz. lastnikom spletnih strani. Predstavimo še 3 nove video vodiče.

Kdo bo plačal varnostno luknjo? Skupaj s podjetjem Domovanje organiziramo *prvo srečanje slovenskih spletnih razvijalcev*, ključna beseda pa je varnost.

Mesec končamo z več kot 150 obravnavanimi incidenti in prve projekcije kažejo, da bomo konec leta dosegli številko 1500.

OKTOBER

NOVEMBER

Na Okrožnem sodišču v Mariboru je na štiri leta in deset mesecev zapora obsojen avtor Butterfly bota, Matjaž Škorjanc – Iserdo (primer Mariposa).

Prejmemo prve prijave napadov onemogočanja z odbojem prek NTP-strežnikov, ki na omrežju skrbijo za sinhronizacijo računalniških ur.

Prek Facebook nagradne igre *"Spletni goljufi ne poznajo praznikov"* širimo koristne napotke o varnem spletnem nakupovanju.

DECEMBER

si·cert

Poročilo centra SI-CERT

POT DO VAŠEGA DENARJA SE ZAČNE NA VAŠEM RAČUNALNIKU

Kako se kaj slovenski hekerji primerjajo s tistimi drugod po svetu? To je dokaj pogosto vprašanje, ki ga slišimo na SI-CERT. V letu 2013 sta dva dogodka pritegnila zanimanje tuje strokovne javnosti in medijev: obsodba avtorja Butterfly bota Matjaža Škorjanca na Okrožnem sodišču Maribor (primer Mariposa) in aretacija kriminalne združbe, ki je prek spletnega bančništva slovenskim podjetjem skušala ukrasti 2 milijona evrov.

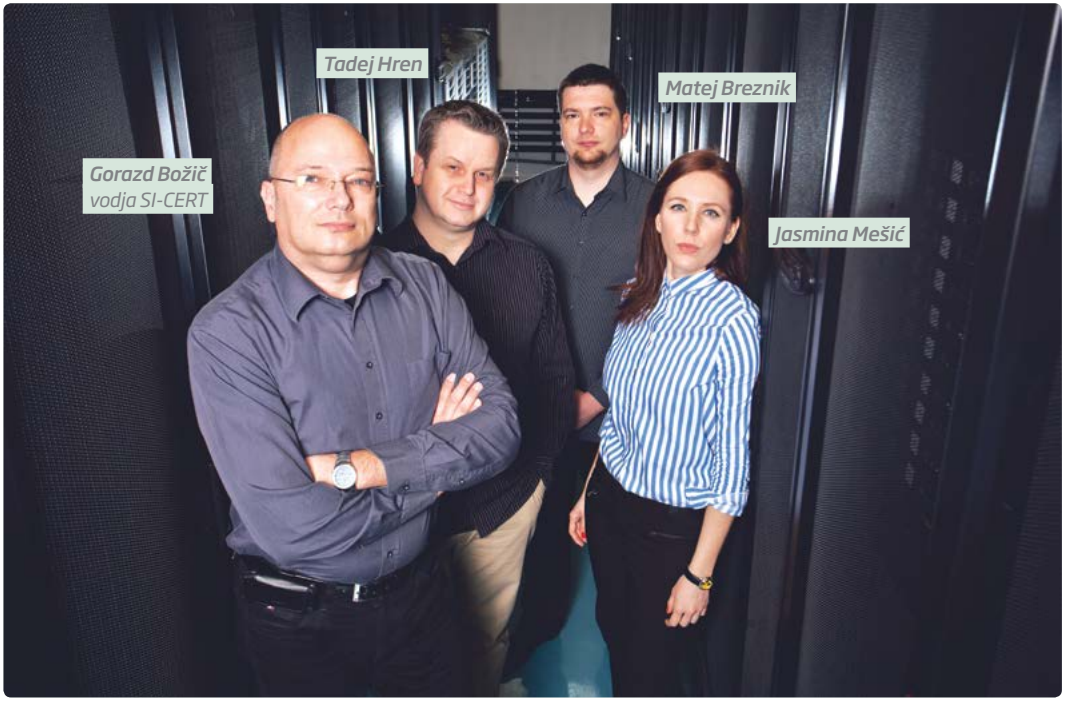
Medijsko pozornost je lani sicer ukradel Edward Snowden, ki je v sodelovanju z Glennom Greenwaldom iz časopisa The Guardian prikazal neslutene razsežnosti programov ameriške obveščevalne službe NSA, usmerjenih na zbiranje podatkov na elektronskih omrežjih. V tem kontekstu se je pri nas konec leta sprožila polemika o spremembah Zakona o kazenskem postopku, po katerem bi policija imela možnost nameščanja pritajenega "državnega trojanca" na računalnike osumljencev.

Ob tem so nam na SI-CERT brez resničnih presenečenj čas zapolnjevali problemi internetne infrastrukture, ki se kažejo v zlorabah razprostranjene mreže DNS-strežnikov, izkoriščanih za močne napade onemogočanja, številna slabo vzdrževana spletna mesta slovenskih podjetij, ki so jih napadalci zlorabili v svoje namene, ter še več primerov škodljive programske kode, ki je bila vstavljena na spletne strani istih strežnikov ali pa je s pomočjo okužb poskusila izsiliti denar domačih uporabnikov in podjetij.

V našem poročilu najdete opis lanskoletne dejavnosti SI-CERT s pomočjo statistike in izpostavljenih primerov. Glede na to, da smo lani za letno poročilo prejeli nagrado na konferenci za vsebinski marketing POMP 2013, hkrati pa kot SI-CERT še veliko nagrado za projekt leta, upam, da bo tudi letošnje poročilo o omrežni varnosti vredno vašega časa.

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 od leta 1995 deluje v okviru javnega zavoda Arnes (Akademska in raziskovalna mreža Slovenije). Opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih.

SI-CERT od leta 2011 samostojno izvaja nacionalni program ozaveščanja in izobraževanja Varni na internetu.

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. V primeru vdora, okužbe računalnika ali druge omrežne zlorabe lahko pošljete sporočilo z opisom incidenta na e-naslov *cert@cert.si*, prek telefonske številke (01) 479 88 22 ali prijavnega obrazca na spletni strani *www.varninainternetu.si*. Strokovnjaki centra pomagamo prizadetim ob posameznih incidentih s specializiranim znanjem in izkušnjami. Kot nacionalna kontaktna točka imamo vpogled v trende, podatki o sorodnih incidentih doma in v tujini pa izboljšajo ter pospešijo razreševanje aktualnih primerov.

Sodelavci SI-CERT smo v letu 2013 opravili čez 30 predavanj na različnih srečanjih, konferencah in delavnicah. Izpostavili bi predavanja na Ministrstvu za obrambo, vabljeno predavanje o evropskem sodelovanju odzivnih centrov na srečanju Global Corporate Executive Programe, predavanje o varnosti SCADA-sistemov na podjetju Eles, d. d., in predstavitev aktivnosti ozaveščanja Varni na internetu na delavnici združenja evropskih domenskih registrov CENTR.

RAČUNALNIŠKI INCIDENTI

OD PRIJAVE DO RAZREŠITVE

Potek obravnave varnostnega incidenta

Faze obravnave varnostnega incidenta na omrežju

Računalniški incident je ***niz 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 s prijavo nekega dogodka), se najprej opravi **analiza** in klasifikacija, nato pa 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. V njih zberemo izkušnje in jih povežemo z drugimi obravnavanimi incidenti. Tako zaznavamo trende, opazimo nove ranljivosti in dopolnjujemo lastno znanje ter izkušnje. Celoten proces zaokrožijo javno objavljena priporočila in opozorila.


User
Pass
4160
zavrnjenih
3649
prijav
klasifikacija
incidenta
Incident
#51723
Mediji
CERT
sysadmin
ISP
2380
preiskav

KAJ RAZKRIVAJO ŠTEVILKE?

STATISTIKA OBRAVNAVANIH INCIDENTOV

VRSTA INCIDENTA	2008	2009	2010	2011	2012	2013
skeniranje in poskušanje	86	39	44	62	51	43
botnet	9	3	11	12	12	16
napad onemogočanja (DDoS)	22	10	18	28	47	76
škodljiva koda	18	53	68	126	258	417
zloraba storitve	16	15	12	28	9	8
vdor v sistem	32	25	56	93	76	61
zloraba up. računa				1	9	37
razobličenje					125	80
napad na aplikacijo					17	22
Tehnični napadi	**183**	**145**	**209**	**350**	**604**	**760**
kraja identitete			10	52	67	56
goljufija	5	24	26	89	161	210
spam	21	22	36	25	74	50
phishing	23	38	50	61	139	209
dialler					1	
Goljufije in prevare	**49**	**84**	**122**	**227**	**442**	**525**
zahtevek sodišča	11	6	11	11	9	6
avtorske pravice	2	4	2	5	9	1
interno	3	4	16	38	25	24
novinarsko vprašanje					18	16
druga vprašanja	70	74	92	120	128	145
Vprašanja in zahtevki	**86**	**88**	**121**	**174**	**189**	**192**

HITRA PRIMERJAVA Z LETOM 2012

30% porast goljufij

50% porast phishinga

60% porast škodljive kode

VREDNO OMEMBE

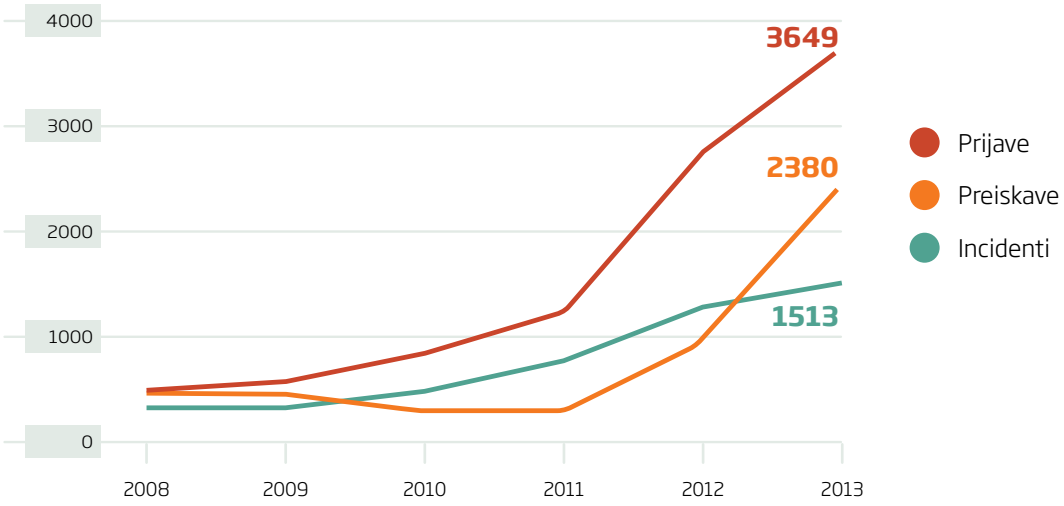
417 primerov škodljive kode

209 vdorov v spletna mesta z namestitvijo phishing strani

1152 razobličenih slovenskih spletnih mest (80 incidentov)

4912 poslanih sporočil

Primerjava števila obravnavanih incidentov



ZAŠČITA INFRASTRUKTURE

Internet je univerzalno omrežje za komunikacijo, ki ga posamezniki poznamo predvsem prek brskanja po spletnih straneh, družabnih omrežjih in elektronske pošte. Vse bolj pa povezujemo v isto omrežje širok nabor različnih naprav: vse od merilnih sistemov, medicinskih aparatov pa tja do nadzornih sistemov naših elektrarn. Naslednji val razvoja bo po napovedih predstavljal ***internet stvari (internet of things)***, omrežje številnih naprav povsod okoli nas. Navdušenje nad možnostmi, ki bi jih internet stvari prinesel, pa pričakovano preglasi varnostne pomisleke. Danes je sprejeto dejstvo, da moramo na računalnike redno nameščati popravke, ki odpravljajo varnostne pomanjkljivosti, če se želimo izogniti zlorabam. S pametnimi napravami ni nič drugače, saj na njih teče enaka ali sorodna programska oprema, vendar jih običajno nastavimo in pozabimo, kar jih pušča na voljo vdiralcem.

Srečali smo se že s tiskalniki in TV-snemalniki, ki so izvajali napade onemogočanja, in z ogrevalnimi sistemi, ki so bili prosto dostopni vsakomur na omrežju, zato lahko v prihodnosti pričakujemo podobne zlorabe tudi na "stvareh", povezanih v internet. Toda danes je središče dogajanja še vedno na "stari" omrežni infrastrukturi: internetnih strežnikih.

ZOMBIJI NAPADAJO

30. marca 2013 smo 18 slovenskih internet ponudnikov obvestili o skupaj 5.198 odprtih DNS-strežnikih, ki so se uporabljali v porazdeljenih napadih. Večji operaterji so takoj sprejeli ukrepe za omejitev dostopa.

PORAZDELJENI NAPADI ONEMOGOČANJA (DDOS)

Napadi onemogočanja z odbojem so se redno vrstili tudi v letu 2013. Ker napadalec v poizvedbo vstavi naslov žrtve kot naslov vira komunikacije, strežnik odgovor pošlje žrtvi (zato govorimo o odboju). Napad je mogoč na storitvah, ki temeljijo na protokolu UDP, učinkovit pa je lahko le, če strežnik vprašanje ojača – to pomeni, da je odgovor daljši, kot je bilo vprašanje.

Najpogosteje se za tovrstne napade izrablja protokol DNS, ki je za delovanje interneta bistvenega pomena, z uvedbo DNSSEC-razširitve pa lahko napadalci z ustreznimi poizvedbami dosežejo zelo velika ojačenja. Številčno so Windows DNS-strežniki predstavljali največjo težavo, saj na njih rekurzivnih poizvedb ni mogoče omejiti na lokalna omrežja in tako ostanejo odprti tudi za napadalce.

Druga zlorabljena storitev za tovrstne napade je bil ***chargen***. Gre za testno storitev, ki se lahko uporabi za preverjanje delovanja omrežja. Nekateri tiskalniki imajo storitev ***chargen*** privzeto omogočeno in napadalci prek njih izvajajo napade. Vseeno pa je bilo teh napadov razmeroma malo.

Več pozornosti je bil deležen tretji protokol v vrsti napadov z odbojem: NTP, Network Time Protocol. Le-ta se uporablja za sinhronizacijo računalniških ur, v napadih pa se izkoristi nadzorno poizvedbo 'monlist', ki vrne spisek IP-naslovov, sinhroniziranih s strežnikom. Pogostejši napadi prek NTP-strežnikov so se začeli decembra 2013, vendar pa pričakujemo dokaj hitro reševanje tega problema, medtem pa se bo verjetno odpravljanje odprtih rekurzivnih strežnikov DNS zavleklo tudi v 2014 ali pa še v poznejši čas.

Posledice DDoS-napada – napad z odbojem prek NTP-strežnikov. Eden od teh je stikalo za diskovno polje, ki pod obremenitvijo izpade. Na tem temelji okolje virtualnih strežnikov ponudnika gostovanja, zato preneha delovati nekaj deset spletnih strežnikov slovenskih podjetij.

SPLETNI GRAFITI

(NE)VARNOST SPLETNIH MEST V SLOVENIJI

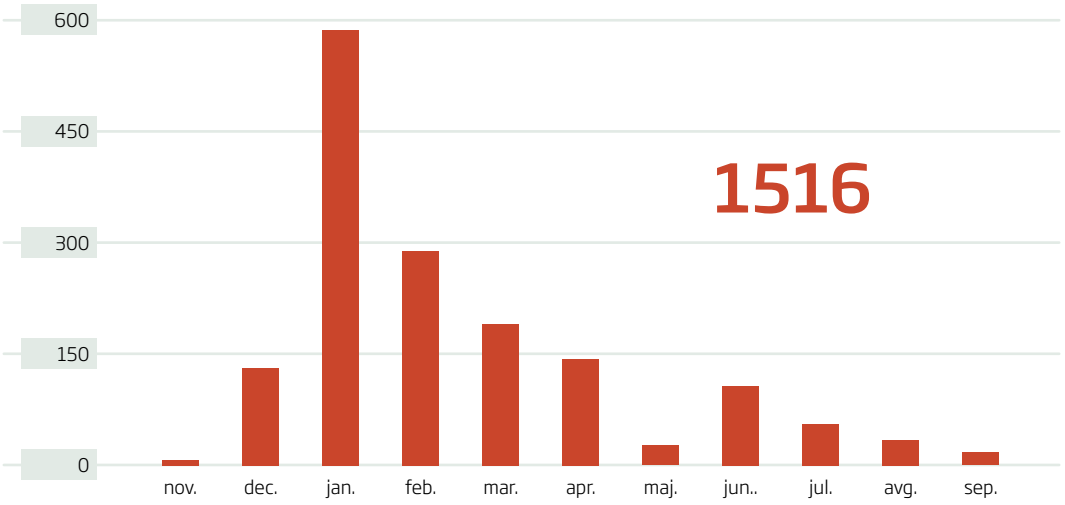
Tik pred koncem leta 2012 se je zvrstilo večje število vdorov v spletne strežnike po Sloveniji. V večini primerov je bilo spletno mesto ***razobličeno:*** napadalec je spletno stran nadomestil s svojim sporočilom ali podpisom (angl. defacement). V nekaterih primerih pa ni šlo samo za spletno "grafitiranje", ampak je napadalec na strežnik namestil svoja orodja, ki so mu omogočala izvedbo napadov onemogočanja. Tarče teh so bile ameriške banke, napadalci pa so bili z Bližnjega vzhoda (Cyber Fighters of Izz ad-Din al-Qassam).

Napadi so si delili enak vstopni podpis: zastarel sistem za upravljanje z vsebinami Joomla, ki je napadalcem omogočil podtikanje programskih skript in spletna mesta. Glede na število prizadetih spletnih mest smo se ob nenehnem obveščanju lastnikov domen in skrbnikov strežnikov odločili tudi, da poskusimo dvigniti zavedanje o pomenu ustreznega vzdrževanja spletnega mesta. V sodelovanju z registrom slovenskih domen, ki upravlja vrhnjo strežniško infrastrukturo DNS-sistema za domeno .si, smo problematiko predstavili registrarjem domen, ki so velikokrat tudi ponudniki gostovanja. Rezultat je bil vodič ***ABC varnosti za lastnike spletnih strani***.

register.si

Register.si upravlja z vrhnjo državno domeno .si. Razvija in vzdržuje centralni sistem za registracijo domen, prek katerega za končne stranke registrirajo domene registrarji (teh je približno 100). Register.si skrbi za nemoteno delovanje vrhnjih DNS-strežnikov za slovensko domeno na različnih lokacijah, tako doma kot v tujini. Vrhnja domena .si je podpisana z DNSSEC-tehnologijo od 30. 11. 2011.

Število razobličenj spletnih mest v Sloveniji, obravnavanih na SI-CERT



Vdori in zlorabe so realnost, ki se je morajo zavedati tako lastniki spletnih mest kot tudi spletni razvijalci. Zato smo skupaj s podjetjem Domovanje, d. o. o., organizirali **prvo srečanje slovenskih spletnih razvijalcev,** ki smo ga naslovili **Kdo bo plačal varnostno luknjo**. Poudarek srečanja je bil na konkretnih primerih zlorab iz prakse in nasvetih, kako se je pred zlorabami mogoče zaščititi.

Po delavnici je sledila tudi okrogla miza z naslovom A**li veste, da ste odgovorni za varnost na spletu**, na kateri so svoje poglede na omrežno varnost poleg vodje **SI-CERT Gorazda Božiča** in **Uroša Čimžarja** iz podjetja **Domovanje** podali še IT-novinar **Miran Varga**, novinar in urednik 24ur **Denis Oštir**, direktorica Mimovrste **Lea Benedejčič** in pravnik, specialist za informacijsko pravo iz JK Skupine **Matija Jamnik**. Sogovorniki so se strinjali, da stanje "na terenu" jasno kaže, da za varnost ni dobro poskrbljeno. Kot je izpostavil Denis Oštir, se lastniki podjetij pomena varnosti na spletnih straneh ne zavedajo oz. se zavedajo šele takrat, ko se kaj zgodi. Kmalu po antivirusnih programih pa se vse neha. Kot je dejal: "***Spletna varnost je podobna poplavni varnosti. Aktualna je le, ko je pol države pod vodo.***"

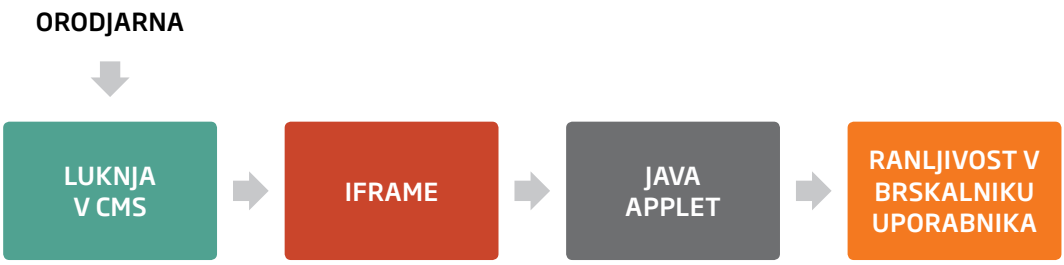
TOP 10 LEKCIJ ALI KAJ SMO ODNESLI OD SREČANJA SPLETNIH RAZVIJALCEV?

1. Čas garažnih internet mojstrov je minil, spletnega mesta se je treba lotiti z ustrezno profesionalno podporo, kar bodo morali spoznati predvsem lastniki spletnih mest!
2. Najpogostejše posledice vdorov v spletna mesta so phishing, razobličenje, okužbe v mimohodu (drive-by-download).
3. Ponudnik gostovanja ni odgovoren za uporabnikove vsebine na strežniku do tistega trenutka, ko je o protipravnosti obveščen. Nato mora ukrepati!
4. Spletni razvijalec ni strokovnjak za šifriranje, zato ne izumljajte svojih šifrirnih algoritmov, ampak uporabite že preverjene.
5. Top tehnike varnosti so: konfiguracija, preverjanje vhodnih podatkov, obravnava napak, šifriranje podatkov, ločitev kode od podatkov, varnostne kopije. Predvsem na slednje razvijalci pogosto pozabljajo!
6. Vsak spletni razvijalec bi moral poznati ranljivosti spletnih aplikaciji, ki so navedene v dokumentu *OWASP TOP 10*.
7. Vsak osnovni paket vzdrževanja spletnih strani bi moral že vsebovati varnostne popravke. Naj ti ne bodo ponujeni šele kot dodatna storitev!
8. Varnost strežnika lahko povečate, če na strežniku izklopite storitve, ki so privzeto nameščene, a jih ne potrebujete.
9. Ko kupujete VPS, vedno preverite, kakšen način virtualizacije omogoča. Pomembno je, da omogoča tudi "live migration", sicer bo ob kakršnih koli spremembah (selitve, nadgradnje itd.) strežnik po nepotrebnem nedosegljiv.
10. Vedno preverite, kateri postopek nadgradenj vam omogoča kupljeni VPS. Že ob nakupu mora biti jasno, kdo bo vaš VPS vzdrževal.

ŠKODLJIVA KODA

Škodljiva ali zlonamerna koda (angl. "malware") je eno od osnovnih orodij za izvajanje napadov na omrežju. Lahko se odloži v obliki majhnega trojanca, ki z omrežja naloži dodatne komponente, v obliki bota razpošilja neželeno pošto in izvaja porazdeljene napade onemogočanja (angl. "distributed denial-of-service"), pritajeni nadzorni programi pa na stežaj odprejo vrata vašega računalnika in omrežja, medtem ko se napredni trojanec umesti v vaš brskalnik in prestreza bančna plačila.

Škodljiva programska koda se lahko širi na različne načine: samodejno prek omrežja z ***izrabo znanih ranljivosti*** v strežnikih ali spletnih aplikacijah (t. i. omrežni črvi), prek izmenljivih ***USB-naprav***, v obliki ***priponk elektronske pošte*** ali prek ***okužb v mimohodu*** (angl. drive-by download). Da zaobidejo zaščitne mehanizme, avtorji uporabljajo številne prijeme za zakrivanje in preoblačenje svojih programov. Na črnem trgu lahko najamete ali kupite napredne orodjarne za izvajanje masovnih okužb (angl. "exploit toolkit"). V jeziku oblačnega računalništva zato že govorimo o ***MaaS - Malware as a Service***.



Primer zakrite kode bot programa

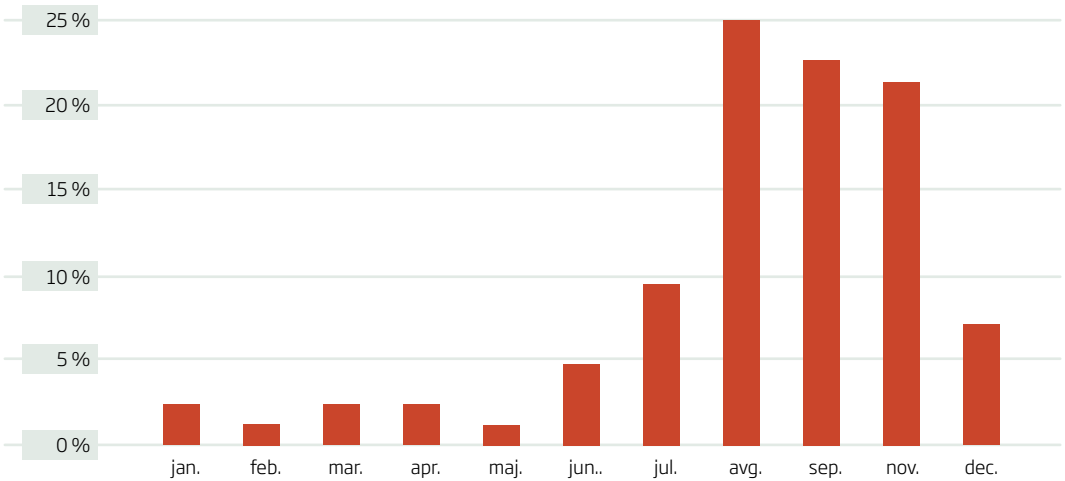
VAŠI PODATKI SO VREDNI 100 €

IZSILJEVALSKI PROGRAMI NA POHODU

Aprila 2012 smo na SI-CERT prejeli prva obvestila o okužbah z virusom **Ransomcrypt**, ki je zašifriral uporabnikove datoteke in prikazal obvestilo o plačilu 50 € globe. Jeseni 2012 se je pojavil nov izsiljevalec (**Ukash/Reveton/Urausy**), ki je zaklenil računalnik, ni pa okvaril podatkov na njem. S posegom v Windows register je onemogočil prijavo uporabnika in prek interneta prenesel lažno opozorilo s pripadajočim slikovnim gradivom glede na državo, v kateri se je žrtev nahajala. Žrtev je obtožil kršitve zakona zaradi prenosa nelegalnih vsebin in zahteval plačilo globe v imenu policije. Pri nas so uporabili oznake Nacionalnega preiskovalnega urada in dodali sliko predsednika republike.

Okužbe so se vrstile čez celo leto in doživele vrhunec jeseni 2013. Vseh okuženih v Sloveniji v tem letu je bilo okoli 300, virus pa je bilo dokaj enostavno odstraniti. Kljub temu je nekaj žrtev odkupnino plačalo.

Graf za delež od približno 300 primerov obravnavanih okužb z Ukash izsiljevalskim virusom kaže na izrazit jesenski izbruh.



CryptoLocker je naslednji ransomware primerek, ki pomeni pomemben mejnik. Šifrirne postopke uporabi na pravi način, kar pomeni, da prizadeti nima na voljo bližnjice (kot pri Ukash) ali orodja za povrnitev podatkov (kot pri Ransomcryptu). CryptoLocker po okužbi najprej kontaktira s svojim nadzornim strežnikom. Ta se lahko nahaja na katerikoli od 1000 domen, ki se dnevno na novo zgenerirajo po določenem algoritmu. Virus poskuša eno za drugo, dokler ne pride do delujoče. Ko se virus tako javi "domov", nadzorni strežnik ustvari unikaten javno-zasebni par RSA-ključev in javni del pošlje nazaj okuženemu računalniku. CryptoLocker nato za posamezno datoteko ustvari vsakič nov AES-ključ, jo z njim zašifrira, nato pa z javnim RSA-ključem, ki ga je prejel z nadzornega strežnika, zašifrira še sam AES-ključ. Tako lahko povrne podatke le tisti, ki ima v roki zasebni del RSA-ključa, ta pa se nahaja samo na strežniku, ki ga nadzirajo avtorji virusa. Poleg tega vam je na voljo zgolj 72 ur časa, da plačate 2 bitcoina (BTC) oziroma 300 evrov prek MoneyPak sistema. Po izteku tega časa pa grozijo, da bodo zasebni del RSA-ključa izbrisali in tako bo odšifriranje vaših podatkov popolnoma onemogočeno.

Veriga okužbe za CryptoLocker

Storilci uporabijo Cutwail botnet, omrežje zlorabljenih računalnikov, ki se uporablja za pošiljanje neželene pošte. Z njegovo pomočjo razpošljejo elektronska sporočila, ki v priponki vsebujejo trojanca Upatre, tj. odlagalec (angl. trojan dropper), ki z interneta potegne GameOver, P2P-različico naprednega trojanca ZeuS. Ta nima centralnega nadzornega strežnika in je zato odpornejši proti razkuževalnim akcijam na internetu. GameOver poskrbi za okužbo s CryptoLocker virusom.

Druge oblike izsiljevanja na omrežju

Okužbe z virusi pa niso edini način izsiljevanja. Storilci izberejo žrtev, ki svoje storitve nudi na spletu in proti njej sprožijo porazdeljen napad onemogočanja (DDoS, distributed denial-of-service). Kasneje z žrtvijo kontaktirajo in razložijo, da je napade naročila in plačala konkurenca, vendar bodo z napadi prenehali, če žrtev plača odkupnino. V nekaj obravnavanih primerih so sledi za napadalci vodile v Alžirijo in Libanon.

Storilci so kasneje na anonimnem Tor omrežju lansirali podporno storitev, prek katere so omogočili plačevanje tistim, ki so zamudili 72-urno priložnost za plačilo. Zahtevana odkupnina je bila tam 10-krat višja! Na SI-CERT smo prejeli le tri obvestila o okužbah v Sloveniji.

Žrtev okužbe ima v praksi dve možnosti: povrnitev podatkov iz varnostnih kopij, kadar le-te obstajajo, ali plačilo odkupnine.

BALKANBOY – HEKERSKA AKCIJA, TEŽKA 2 MILIJONA EVROV

NAJOBSEŽNEJŠI VDORI V E-BANČNE RAČUNE V SLOVENIJI

Sredi leta 2012 smo dobil prve prijave v vrsti napadov, ki so imeli nekatere skupne lastnosti. Računovodje manjših podjetij in samostojni podjetniki so prejeli elektronsko sporočilo v imenu finančne ustanove: banke, hranilnice ali Davčne uprave RS, ki je govorilo o zapadlih obveznostih izmišljenega posojila. Sporočilu je bila pripeta škodljiva koda, ki je po okužbi računalnika nanj naložila komponento za neposreden dostop do računalnika (RAT, remote administration toolkit) in začela s prestrezanjem gesel.

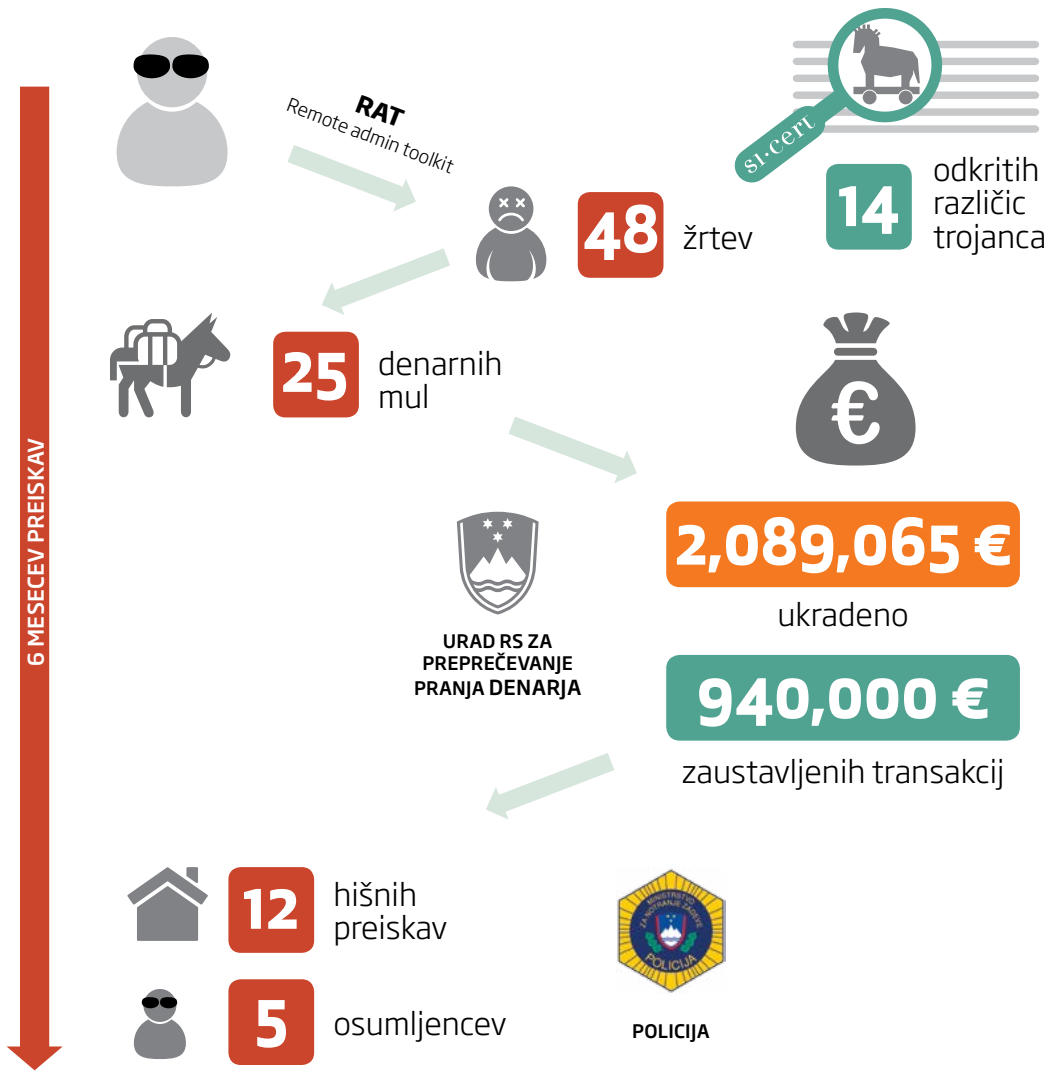
Podtaknjeni program se je nato javil svojemu nadzornemu strežniku, ki je pogosto menjal lokacijo na omrežju. Storilci so lahko prek nameščenega RAT-programa prikrito spremljali dogajanje na okuženem računalniku. Z ukradenim geslom za dostop do bančnih storitev podjetja so nato lahko opravili prenose denarja, seveda ob pogoju, da so v podjetju računalnik pustili vklopljen čez noč, pametno kartico s certifikatom pa v čitalcu.

Napadi so se začeli ob petkih ali dan pred praznikom, kar je napadalcem dalo dovolj časa za to, da so prenose denarja vnesli v e-bančni spletni vmesnik. Za prenose denarja so novačili t. i. "denarne mule", in sicer pod pretvezo britanskega zavarovalniškega podjetja, ki naj bi iskalo agente tudi v Sloveniji. Ukradenega denarja je bilo za skoraj dva milijona evrov, približno polovico nakazil pa je Uradu za preprečevanje pranja denarja uspelo zaustaviti in na ta način oškodovanje preprečiti.

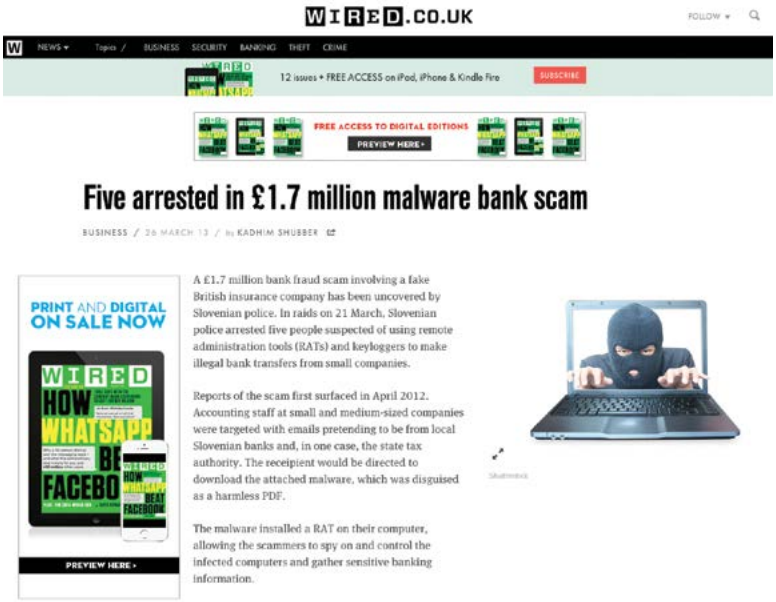
Večmesečno preiskavo je koordinirala policija, na SI-CERT pa smo **opravljali laboratorijsko preiskovanje značilnosti podtaknjene škodljive kode in analizo njenega omrežnega prometa**. Po aretacijah in opravljenih hišnih preiskavah pri osumljencih na SI-CERT nismo prejeli nobenega obvestila več, ki bi se nanašal na ta primer.

AKCIJA BALKANBOY V ŠTEVILKAH

Incident smo poimenovali Balkanboy, ker smo na to ime naleteli ob opazovanju omrežne komunikacije podtaknjene škodljive kode z nadzornim strežnikom v našem laboratoriju.



***Tadej Hren**, SI-CERT (levo), **Dušan Florjančič**, vodja Sektorja za gospodarski kriminal v Upravi kriminalistične policije (sredina), in **Damjan Režek**, namestnik direktorja Urada za preprečevanja pranja denarja (desno), na tiskovni konferenci 22. marca 2013 (foto: Slovenska policija)*



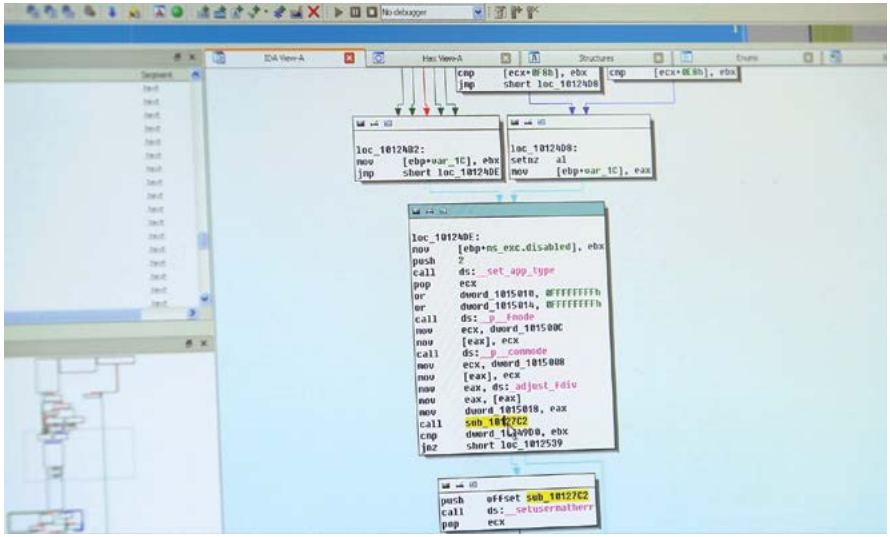
*Izmišljeno britansko zavarovalniško podjetje, ki je služilo kot vaba za denarne mule, je pritegnilo pozornost angleške edicije revije **WIRED** - vni.si/wired.*

TARČA: DRŽAVNI URADNIK

NAPREDNI TROJANEC MINIDUKE

Laboratorij protivirusnega podjetja Kaspersky je v sodelovanju z madžarskim raziskovalnim centrom CrySys 27. februarja 2013 objavil izsledke analize naprednega virusa MiniDuke. Ta je sodeč po podatkih o okužbah ciljal na državne ustanove in v njih zaposlene uradnike. Med državami, v katerih so zaznali okužbo, je bila navedena tudi Slovenija.

SI-CERT je dan pozneje prek mednarodne mreže odzivnih centrov res prejel obvestilo o enem IP-naslovu v Sloveniji, ki kaže promet, značilen za okužene sisteme. IP-naslov je del naslovnega prostora komercialnega internet operaterja. S pomočjo operaterja smo takoj stopili v kontakt z njihovim naročnikom in opravili ustrezne ukrepe za odstranjevanje posledic incidenta. Okužba z virusom MiniDuke je bila omejena samo na en sistem, prizadeti sistem in sama ustanova pa nista del slovenske javne oz. državne uprave.



VLOGA DRŽAVE

SPREMEMBE ZEKOM-1

Na podlagi Evropske direktive 2009/140/ES so bile sprejete spremembe Zakona o elektronskih komunikacijah (ZEKom-1, Ur. l. RS, št. 109/2012), ki v 7. poglavju operaterjem nalaga sprejem ukrepov za obvladovanje tveganj za varnost omrežij in storitev. Operaterji so o varnostnih incidentih tudi dolžni poročati Agenciji za komunikacijska omrežja in storitve (AKOS), ta pa operativno razreševanje incidenta preda po potrebi in glede na kršitev SI-CERT z namenom strokovne pomoči in svetovanja operaterju, usklajevanja z udeleženci znotraj države ter koordinacijo z odzivnimi CERT-centri in drugimi sorodnimi službami v tujini. Postopek je opredeljen v Splošnem aktu o varnosti omrežij in storitev (Ur. l. RS, št. 75/2013).

VAJE IZ KIBERNETSKE VARNOSTI

Konec novembra 2013 je potekala NATO-vaja kibernetske varnosti Cyber Coalition 2013, v kateri je sodelovala tudi Slovenija. Ministrstvo za obrambo Republike Slovenije je koordiniralo aktivnosti v zvezi z vajo znotraj države, SI-CERT pa je sodeloval kot nacionalna kontaktna točka in pomagal z izkušnjami pri vodenju incidentov in njihovem preiskovanju.

Začele so se pripravljalne aktivnosti za evropsko vajo Cyber Europe 2014, ki bo potekala pod okriljem Evropske agencije za varnost omrežij in informacij ENISA. SI-CERT bo tudi tu odigral podobno vlogo, sodeluje pa tudi pri pripravi scenarija same vaje.

STRATEGIJA INFORMACIJSKE VARNOSTI

V drugi polovici leta 2013 so se začele aktivnosti za oblikovanje nacionalne strategije informacijske oz. kibernetske varnosti, ki jih po sklepu Vlade RS koordinira Direktorat za informacijsko družbo Ministrstva za izobraževanje, znanost in šport. Bistven del strategije bo tudi sistem odzivanja na omrežne incidente na državni ravni.

SLOVAR UPORABLJENIH IZRAZOV

DNSSEC

DNSSEC je razširitev DNS-a, ki je ustvarjena z namenom, da zagotavlja avtentičnost in celovitost podatkov. Računalnik, ki poizveduje po določenem IP-naslovu, lahko z DNSSEC-tehnologijo preveri, ali je bil DNS-odgovor spremenjen med potovanjem po omrežju. DNSSEC zagotavlja, da je obiskovalec dejansko na spletni strani, na katero je imel namen priti. To jamstvo je ustvarjeno s pomočjo digitalnega podpisovanja.

Okužba v mimohodu, drive-by-download

Storilci prek luknje v spletnem strežniku podtaknejo zlonamerno programsko kodo na spletno mesto. Uporabniki, ki si na njem ogledujejo spletne strani, so izpostavljeni možni okužbi. Le-ta izkorišča ranljivosti v spletnem brskalniku ali njegovih vtičnikih (plugin). Najpogosteje se izkorišča vtičnik za Javo.

Porazdeljen napad onemogočanja, distributed denial-of-service (DDoS)

Porazdeljen napad onemogočanja se izvaja prek posredniških sistemov, ki so pod nadzorom napadalca. Na njih napadalec običajno namesti bot program in posredniške sisteme (včasih imenovane tudi zombiji) poveže v botnet. Ob usklajenem napadu botneta se učinki napada seštevajo, zato so ti napadi zelo učinkoviti. Stranski učinek je lahko izpad dela omrežja ali prenosnih sistemov na njem. Najobičajnejši so porazdeljeni napadi z odbojem, poplava velikih UDP-paketov, TCP SYN-napad in ***slowloris*** napad na spletne strežnike.

Napad z odbojem/ojačanjem, reflection/amplification attack

Napad temelji na možnosti potvarjanja izvornega naslova v UDP-paketih. Napadalec pošlje vprašanje strežnikom na omrežju, pri čemer spremeni izvorni naslov tako, da ga zamenja z IP-naslovom žrtve. Zato strežniki odgovore pošljejo žrtvi (od tu poimenovanje odboj). Napad je mogoč na storitvah, ki temeljijo na protokolu UDP, učinkovit pa je lahko le, če strežnik vprašanje ojača – to pomeni, da je odgovor daljši, kot je bilo vprašanje. Za napade z odbojem se uporabljajo strežniki DNS (Domain Name System) in NTP (Network Time Protocol).

RAT, remote administration toolkit

Je program, ki omogoča oddaljeno delo na računalniku. Da se izogne omejitvam na požarnih zidovih in NAT-pregradam, se poveže na posredniški strežnik, prek katerega do ciljnega sistema pride tudi upravljavec. Nekateri RAT-programi se uporabljajo kot komponente pri omrežnih napadih (najpogosteje Blackshades RAT).

Razobličenje, defacement

Le-to pomeni vdor v spletni strežnik z namenom spremeniti spletne strani, pogosto za objavo sporočila. Govorimo tudi o "grafitiranju" spletnega mesta, prek katerega želi napadalec izraziti svoje mnenje, bodisi osebno bodisi politično ali pa le želi pustiti svoj podpis.

Izsiljevalski programi, ransomware

Računalniški virusi ali trojanski konji, ki z zaklepom ali šifriranjem uporabnikovih podatkov od njega zahtevajo denarno odkupnino.

Network Time Protocol (NTP)

Protokol za zelo natančno sinhronizacijo računalniških ur prek omrežja internet. V napadih z odbojem se izkorišča nadzorno poizvedba 'monlist', ki vrne spisek IP-naslovov, ki so se z NTP-strežnikom sinhronizirali.

Phishing

Napadalec izkoristi vaše spletno mesto za postavitev lažne kopije npr. spletne strani banke in skuša prek vašega strežnika ukrasti gesla ter nato tudi denar njenih komitentov. Napadalci uporabljajo phishing tehniko tudi za krajo drugih podatkov: gesel elektronske pošte, številk kreditnih kartic, uporabniških računov ipd.

VARNI
NA INTERNETU
Od mene je odvisno vse.

Poročilo projekta Varni na internetu

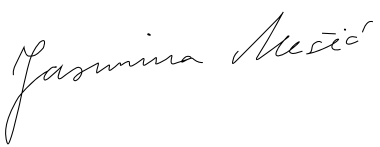
LETO 2013 V ZNAMENJU SODELOVANJA

Statistika obravnavanih incidentov je ponovno pokazala porast spletnih goljufij, v letu 2013 "le" za 30 %. Zadnjih nekaj let beležimo jasen trend naraščanja spletnih prevar, še posebej izrazit je bil skok leta 2012, ko smo obravnavali več prijav kot poprejšnji leti skupaj. Razlogov za to je nedvomno več. Vse pogosteje nakupujemo in prodajamo prek spleta, uporabljamo storitve elektronskega bančništva, se povezujemo in komuniciramo prek kopice družbenih omrežij, obenem se pojavljajo vedno novi spletni servisi, da aplikacij za naše pametne telefone sploh ne omenjamo. In vse je na voljo takoj in kjerkoli, kajti internet je vseskozi v našem žepu. Hkrati se izkaže, da vsako spletno novost goljufi prej ali slej izkoristijo v svoj prid, obenem pa sta program Varni na internetu in prijavna točka bolj prepoznavna in vedno več uporabnikov nam sporoča svoje težave. Vsi ti dejavniki so prispevali svoj delež v našo statistiko. Internet je prisoten v skoraj vsakem trenutku in na vsaki točki komunikacije in jasno je, da če želimo izobraževati in svetovati o varnosti, moramo spletne uporabnike nagovoriti vsi udeleženci, katerih skupni imenovalec je http (raje https). Naš skupni cilj mora biti zmanjšati tveganja, ki smo jim spletni uporabniki izpostavljeni, in tako omogočiti, da v polni meri izkoristimo vse prednosti, ki jih internet prinaša.

Za leto 2013 lahko brez obotavljanja rečemo, da je bilo leto sodelovanja in povezovanja. V začetku leta smo skupaj **z Uradom informacijskega pooblaščenca** predstavili priročnik ***ABC varnosti in zasebnosti na mobilnih napravah***, v katerem opozarjamo na možnosti zlorab na mobilnih platformah ter hkrati podamo osnovna načela varne rabe pametnih telefonov in tablic. Si.mobil nas je skupaj s Fakulteto za varnostne vede Univerze v Mariboru in Zavodom Ypsilon ter njegovim projektom Simbioza povabil k sodelovanju pri pripravi brošure z nasveti in informacijami o varni uporabi mobilnih telefonov za starejše. Akcijo ob vseevropskem mesecu kibervarnosti smo zaokrožili z nasveti, ki so jih prispevali na **Združenju bank Slovenije** in največjem spletnem oglasniku **Bolha.com**. Skupaj z nacionalnim registrom slovenskih domen **Register.si** smo zagrizli v trd oreh – množico slabo vzdrževanih spletnih mest in izdali izčrpen priročnik za lastnike spletnih strani.

In kaj bomo počeli prihodnje leto? Januar 2014 je prinesel množično "spamanje" slovenskih uporabnikov z lažnim računom, ki je v priponki skrival virus. Če sodimo leto po prvem mesecu, nam dela zlepa ne bo zmanjkalo.

Jasmina Mešić, *koordinatorka programa Varni na internetu*



O PROJEKTU VARNI NA INTERNETU

Nacionalni program ozaveščanja Varni na internetu smo v SI-CERT zasnovali z namenom izobraževanja širše slovenske javnosti o varni uporabi interneta in prepoznavanja spletnih tveganj. S številnimi komunikacijskimi aktivnostmi opozarjamo na nujnost ustrezne tehnične zaščite, ki pa danes zagotavlja le minimum omrežne higiene. Naše delo temelji predvsem na preventivnem delovanju – opozarjanju in izobraževanju spletnih uporabnikov, kako naj prepoznajo različne oblike spletnih goljufij. Pri mnogih primerih spletnih prevar, ki smo jih obravnavali, še tako napreden antivirusni program ne bi preprečil škode in zagotovil varnosti. Za najboljšo rešitev se še vedno izkaže preudarno spletno vedenje.

Cilj programa Varni na internetu je zagotoviti celostno platformo za spletne uporabnike, ki sega od preventivnih nasvetov in napotkov do strokovne pomoči, ko že pride do omrežnega incidenta. Z našo aktivnostjo želimo ponuditi odgovore na ključna vprašanja:

- Kako prepoznam goljufije na spletu in se pred njimi zavarujem?
- Kako varno uporabljam storitve elektronskega bančništva in varno nakupujem prek spleta?
- Kako naj zavarujem svojo spletno osebno identiteto?

Od izobraževanja do pomoči žrtvam spletnih goljufov

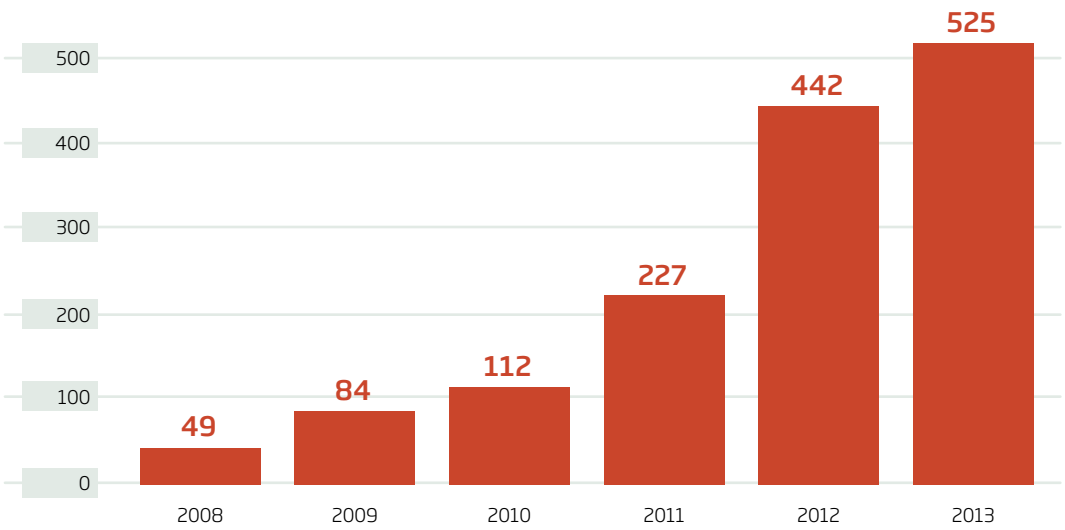
Izobraževalni portal www.varninainternetu.si

Izobraževalni portal *www.varninainternetu.si* smo zasnovali s ciljem, da postane ključen vir informacij s področja informacijske varnosti in **prvi naslov, ko spletni uporabnik ali uporabnica potrebuje nasvet ali pomoč**. Na portalu ažurno obveščamo o odkritih goljufijah in ostalih zaznanih nevarnostih, tudi v obliki video prispevkov, opisujemo najpogostejše spletne prevare, analiziramo konkretne primere, usmerjamo na relevantne zunanje vire. Da bi obiskovalci čim hitreje našli odgovore na vprašanja in pomoč, ko jo najbolj potrebujejo, smo portal v letu 2013 temeljito prenovili.

Prijavi prevaro!

Na portalu je vzpostavljena prijavna točka, prek katere lahko oškodovanci prijavijo omrežni incident (vdor, goljufija, kraja identitete itd.). Pomagamo in svetujemo strokovnjaki nacionalnega centra SI-CERT, **naše znanje je vsem spletnim uporabnikom na voljo brezplačno**. V primerjavi z letom pred začetkom programa ozaveščanja (2010) opazimo kar štirikraten porast prijav spletnih goljufij.

Prikaz porasta spletnih goljufij in prevar



Družbena omrežja so naš zaveznik

Izkazalo se je, da družbena omrežje nikakor niso zgolj vir težav, ampak so tudi najhitrejši in najučinkovitejši kanal za obveščanje o aktualnih spletnih prevarah. ***Facebook stran Varni na internetu in Twitter račun @varninanetu*** sta zaživela kot čisto samostojna "svetovalca", v letu 2013 smo zabeležili že 13.800 oboževalcev na Facebook strani in 600 sledilcev na Twitter omrežju.

KLJUČNA TVEGANJA V LETU 2013

ODRASLI UPORABNIKI

(uporabljajo spletno banko, nakupujejo prek spleta)

prevare pri spletnem nakupovanju, predvsem lažne spletne trgovine in trgovine s ponaredki

izsiljevalski virusi, ki zaklenejo računalnik in zahtevajo odkupnino

nepremišljeni kliki na družbenem omrežju Facebook

POSLOVNI UPORABNIKI

(samostojni podjetniki, manjša podjetja, društva)

slabo vzdrževane spletne strani predstavljajo lahke tarče za hekerje

neupoštevanje osnovnih načel varne rabe elektronskega bančništva

premalo zavedanja, kako pomembne so varnostne kopije (backup) ključnih poslovnih podatkov

KAJ JE ODMEVALO V LETU 2013?

MALI IN VELIKI POMP!

Nagradi za naj letno poročilo in projekt leta s področja vsebinskega marketinga

POMP Forum je mednarodna strokovna konferenca s področja vsebinskega marketinga, v sklopu katere podelijo nagrade za učinkovitost in kreativnost v sedmih kategorijah ter glavno nagrado VELIKI POMP za projekt leta na področju vsebinskega marketinga.

V letu 2013 je ekipa SI-CERT prejela nagrado POMP za naj letno poročilo – ***Poročilo o omrežni varnosti 2012.***

Odzivi na prejeto nagrado so bili zelo pozitivni, veseli nas, da je komisija POMP opazila trud, ki smo ga vložili v ***Poročilo o omrežni varnosti za leto 2012***, tako v pripravo samih besedil kot tudi infografik, domiselne naslovnice in nenavadne embalaže (*vni.si/2012*).

OBRAZLOŽITEV NAGRADE

Dileme ni. Letno poročilo, ki se ne omejuje le na pregled organizacije in njenega dela v minulem letu, temveč se celotne panoge oz. problematike, ki jo pokriva, loteva širše. Cilj ni bil le podati pregled ključnih dogodkov, temveč tudi pogledati v prihodnost. Predvsem pa to letno poročilo izstopa po bogati vsebini, ki pritegne pozornost bralca. Še več. Ta publikacija ima dolgotrajno vrednost. Da niti ne omenjamo, da gre za tiskano letno poročilo o spletni problematiki.

Nagrada za projekt leta s področja vsebinskega marketinga pa je bila kar veliko presenečenje, saj je v konkurenci res odličnih komunikatorjev – Petrol, Akrapovič, Telemach – glavno nagrado prejel naš program ozaveščanja Varni na internetu. Postavljeni smo bili ob bok velikim in uveljavljenim podjetjem ter blagovnim znamkam, ki upravljajo z večjimi kadrovskimi resursi in oglaševalskimi sredstvi, zato je bilo presenečenje ob izboru zmagovalca precejšnje. Naše najmočnejše orožje v boju z "velikimi" je odlično poznavanje svojega področja in vsakodnevno relevantno, zanimivo, uporabno, bralcu prilagojeno komuniciranje na več komunikacijskih kanalih.

OBRAZLOŽITEV NAGRADE

SI-CERT s programom Varni na internetu predstavlja primer odlične prakse vsebinskega komuniciranja in njene izvedbe. Z izbiro ustreznih medijev in orodij, med katerimi ne manjkajo niti tiskana, učinkovito komunicirajo s splošno javnostjo in drugimi vplivnimi javnostmi, ki so pomembne za podporo oz. izvajanje osveščanja o nevarnostih na spletu. Video vsebine, blog, odlična uporaba družbenih medijev s hitrimi odzivi in cela vrsta drugih komunikacijskih aktivnosti sestavljajo celovit sveženj vsebin, ki je redko razvit v tolikšni meri. Posebej prilagojeni nagovori za podjetja in posebne vsebine za domače uporabnike pa potrjujejo, da si ekipa SI-CERT zasluži VELIKI POMP 2013 za svoje dozdajšnje dosežke kot spodbudo za naprej in kot zgled drugim.

IZPOSTAVLJENI DOGODKI

NAPRAVA JE PAMETNA TOLIKO, KOLIKOR JE PAMETEN NJEN UPORABNIK!

SKUPNA AKCIJA Z URADOM INFORMACIJSKEGA POOBLAŠČENCA

Če govorimo o varnosti in zasebnosti na spletu, ne moremo mimo dejstva, da se je korenito spremenil način dostopanja do spleta. Pametni telefoni in tablice omogočajo povezljivost kjerkoli in kadarkoli, hkrati pa se spletna tveganja, na katere opozarjamo uporabnike, ko sedijo za svojim domačim računalnikom, selijo tudi na njihove mobilne naprave.

Uporabniki pametnih telefonov in tablic, ste že kdaj pomislili, da v žepu pravzaprav nosimo dokaj zmogljiv računalnik, ki pa mu še vedno rečemo "telefon". Le-to pomeni, da smo prav tako izpostavljeni kraji identitete oz. kraji gesla, izgubi podatkov ali okužbi z virusi.

Vodič smo predstavili na skupni tiskovni konferenci ob evropskem dnevu varstva osebnih podatkov.

V vodiču smo na enem mestu strnili ključna tveganja in nasvete, kako varno shranjevati in prenašati podatke ter kako zaščititi našo zasebnost pred podatkov lačnimi aplikacijami. abc.vni.si

Zato smo skupaj z uradom Informacijskega pooblaščenca pripravili vodič **ABC varnosti in zasebnosti na mobilnih napravah**. Priročnik enostavno in razumljivo odgovarja na najpogostejša vprašanja uporabnikov. Kako varno shranjujem podatke (fotografije, kontakte, koledar)? Kako se varno povežem na internet? In če mi kdo ukrade telefon? Kaj pa mobilne aplikacije, kakšna so tu tveganja? Dodatni napotki so namenjeni **poslovnim uporabnikom**. Le-ti se srečujejo z drugačnimi varnostnimi izzivi, predvsem kraja podatkov lahko ima v poslovnem okolju veliko hujše posledice

Zaslon na pametnem telefonu ali tablici pa postane med dopustovanjem praktično nepogrešljiv. Da bi počitnice minile čim bolj brezskrbno, smo pripravili še kratek e-priročnik **Varni na internetu, tudi na počitnicah**. V vodiču so opisane **najpogostejše počitniške goljufije**, na katere uporabniki lahko naletijo, ko brskajo za turističnimi ponudbami – od fantomskih apartmajev do lažnih turističnih agencij.

V vodiču so zbrane najpogostejše goljufije, na katere lahko naletite, ko brskate za apartmaji, turističnimi agencijami ali vstopnicami za različne prireditve. Ko boste prispeli na vašo destinacijo, bo verjetno na voljo več možnosti dostopa do interneta (javni računalniki, Wi-Fi, mobilni internet), vendar ***niso vse enako varne****. Zato preverite tudi nasvete, kako varno pregledovati e-pošto, uporabljati družbena omrežja in plačevati s kreditno kartico. vni.si/počitnice*

VAŠA SPLETNA STRAN POTREBUJE VAŠO POZORNOST

IZOBRAŽUJMO LASTNIKE SPLETNIH STRANI

Težava, s katero se skoraj vsakodnevno srečujemo na SI-CERT, so neposodobljena in ranljiva spletna mesta, ki predstavljajo lahke tarče za hekerje. Ne le spletna stran, pomemben inventar podjetja ali društva, na katerega se (pre)pogosto pozablja, je tudi domena oz. naslov spletne predstavitve. Tudi na nacionalnem registru slovenskih domen Register.si opažajo, da **lastniki spletnih strani preprosto pozabijo, da domeno sploh imajo, vse dokler ne nastopijo težave**.

Lastniki spletnih strani v Sloveniji se še premalo zavedajo nevarnosti – če za spletno mesto ne poskrbijo, je samo vprašanje časa, kdaj bo prišlo do takšnega ali drugačnega zapleta. Odpravljanje posledic zlorabe terja določen čas in denar, nedostopnost strani ali spletne trgovine pa povzroči tudi izgubo strank, poslovno škodo in prav gotovo ne prispeva k dobri podobi podjetja.

Trend naraščanja števila zlorabljenih slovenskih spletnih mest je razlog, da smo več pozornosti namenili ozaveščanju manjših podjetij, obrtnikov, blogerjev in društev, kako **pomembno je redno vzdrževanje spletnih strani**. Le-ti pogosto zaradi pomanjkanja tako finančnih kot človeških virov **zanemarjajo svoje spletne strani in tako nevede odpirajo vrata zlorabam**. Skupaj z nacionalnim registrom slovenskih domen Register.si smo izdali vsebinsko izčrpno knjižico, ki na **enem mestu podaja vse informacije, ki jih vsak odgovoren lastnik spletne strani mora poznati**. Vodič **ABC varnosti za lastnike spletnih strani** opisuje najpogostejša varnostna tveganja slabo vzdrževanih spletišč, podaja ključne nasvete lastnikom in vzdrževalcem spletnih mest ter kontaktne naslove, kamor se lahko obrnejo v primeru težav.

Vsebine, ki smo jih razdelali v priročniku, so zastavljene širše. Lastniki spletnih mest najdejo tako napotke za varno ravnanje z domeno kot tudi za druge faze – od načrtovanja, postavitve do vzdrževanja spletne strani.
vni.si/www

Pobudo za projekt ozaveščanja o varni spletni predstavitvi smo naslovili tudi na vse slovenske registrarje, ki velikokrat nastopajo tudi v vlogi ponudnikov gostovanja. Povabili smo jih k sodelovanju, da s svojim znanjem in izkušnjami prispevajo k vsebinski pripravi vodiča in pomagajo pri distribuciji priročnika do svojih strank. Vsem registrarjem, ki so se odzvali pobudi, se še enkrat zahvaljujemo.

OKTOBER V ZNAMENJU KIBERVARNOSTI

VSEEVROPSKA SKUPNA AKCIJA "SPLETNA VARNOST JE ZA TVOJE DOBRO!"

Oktobra 2013 se je prvič v polnem obsegu odvil evropski mesec kibervarnosti (European Cyber Security Month) – vseevropska kampanja ozaveščanja, ki jo je organizirala Evropska unija. Članice EU so pod skupnim geslom ***"Spletna varnost je za tvoje dobro!"*** ves oktober sodelovale z različnimi dejavnostmi in prireditvami z namenom izboljšati obveščenost svojih državljanov o informacijski varnosti. V kampanjo je bilo vključenih več kot 60 različnih udeležencev iz 25 evropskih držav, ki so skupaj pripravili več kot 50 različnih aktivnosti.

Dejavnosti v okviru evropskega meseca kibervarnosti so potekale v 22 državah članicah EU in 3 državah partnericah. Slovenijo je v evropski kampanji zastopal nacionalni program ozaveščanja Varni na internetu, ki ga izvajamo na SI-CERT.

Na SI-CERT smo bili tudi leta 2012 del prvega poskusa vseevropskega sodelovanja, ko je bil uspešno izpeljan pilotski evropski mesec kibervarnosti. Takrat nas je sodelovalo le 8 članic EU, v sklopu programa Varni na internetu pa smo javnost nagovorili z odmevno kampanjo *"Ne bodi osel na spletu"*.

Odzivi iz leta 2012 so bili zelo pozitivni, zato smo ob mesecu kibervarnosti ponovno postavili v ospredje video vodiče. Če smo ob takratni vseevropski akciji spletnim prevaram pristopili na zabaven način, smo se v letu 2013 odločili za resnejši pogled. Čeprav smo ubrali drugačen pristop, so vsebine in problematike, ki smo jih izpostavili, ostale enake, prav tako tudi posledice – **slabe odločitve v virtualnem svetu lahko povzročijo finančno izgubo v realnem svetu**.

Vsak teden v mesecu oktobru smo predstavili nov video vodič, v katerem smo raziskali določeno temo s področja spletne varnosti: prevare pri spletnem nakupovanju, zlorabe elektronskega bančništva in hekerske napade na podjetja in posameznike. Z izjemo animiranega videa, ki nagovarja lastnike spletnih strani, smo v video prispevkih zasledovali novinarski žanr z uporabo tipičnega novinarskega diskurza, ki so ga gledalci vajeni iz televizijskih informativnih oddaj. V vsakem video vodiču predstavimo resnične primere, ki smo jih obravnavali na SI-CERT in s katerimi se povprečen gledalec in spletni uporabnik lahko poistoveti – "lahko bi se zgodilo tudi vam" pristop. Pred kamero smo povabili tudi **predstavnika največjega spletnega oglasnika Bolha.com in Združenja bank Slovenije**, ki prispevata še dodaten nasvet, kako lahko uporabniki varno in brezskrbno nakupujejo ali opravljanje bančne storitve prek spleta. Rdeča nit, ki povezuje vse obravnavane teme, je dejstvo, da spletni goljufi lahko nepozornega uporabnika tudi finančno oškodujejo.

Tvegani spletni nakupi

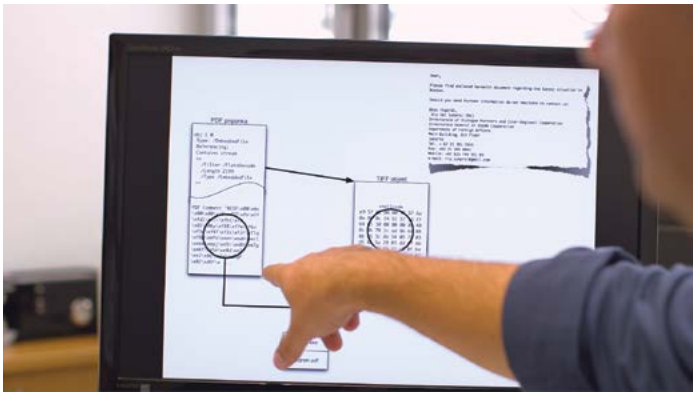
Prvi video, ki smo ga predstavili, obravnava različne oblike spletnih nakupov in povezana tveganja – nakup v lažni spletni trgovini, trgovine s ponarejenimi izdelki in goljufije, ki prežijo na uporabnike spletnih oglasnikov. V letu 2013 smo na SI-CERT zaznali predvsem velik porast spletnih trgovin s ponaredki. V lovu za dobro ceno se kupci pogosto odločijo za nakup ponaredkov znanih in prestižnih blagovnih znamk, vendar je promet s ponaredki v EU prepovedan, zato so takšni paketi na slovenski carini zaseženi in uničeni. V nekaterih primerih morajo celo kupci sami poravnavati stroške uničenja.

Video vsebine si lahko pogledate na vni.si/video.

Zlorabe elektronskega bančništva

V videu svetujemo, kako ustrezno zaščitimo svoj e-bančni račun. Žal smo najšibkejši člen sami uporabniki, ki nevede odpremo vrata zlorabam. Vse večkrat pa so tarče spletnih kriminalcev tudi podjetja. Marca 2013 je kriminalistična policija ob sodelovanju SI-CERT in Urada RS za preprečevanja pranja denarja uspešno preiskala vdore v e-bančne račune, s katerih so kriminalci skupaj prenakazali kar 2 milijona evrov.

Hekerski napadi v Sloveniji



V tretjem videu izpostavljamo nekatere vrste hekerskih napadov, ki smo jih na SI-CERT obravnavali v zadnjem letu. Škodljiva ali zlonamerna koda je tisto orodje, ki na veliko odpira naše računalnike. Resda okužen računalnik ne zveni tako zanimivo kot zgodbe o kiberspopadih med ZDA in Kitajsko, vendar če smo spletni uporabniki sami žrtev okužbe in zato izgubimo vse dokumente ali pa je našemu podjetju heker onemogočil spletno trgovino, potem je za nas ta težava nedvomno pomembnejša.

Akcijo vseevropskega meseca kibervarnosti smo podprli tudi s televizijskimi spoti, spletnimi pasicami in objavami na najbolj obiskanih slovenskih medijskih portalih.

VIRUS TI JE ZAKLENIL RAČUNALNIK POD PRETVEZO, DA SI PRENAŠAL NELEGALNE VSEBINE S SPLETA. ZAHTEVA 100 EVROV. KAJ BOŠ NAREDIL?

Tudi v TV-spotih, ki so se predvajali na slovenskih televizijah, smo izpostavili vedno prisotno finančno komponento. Enkrat kot mamljivo vabo v past, drugič kot škodljivo posledico.

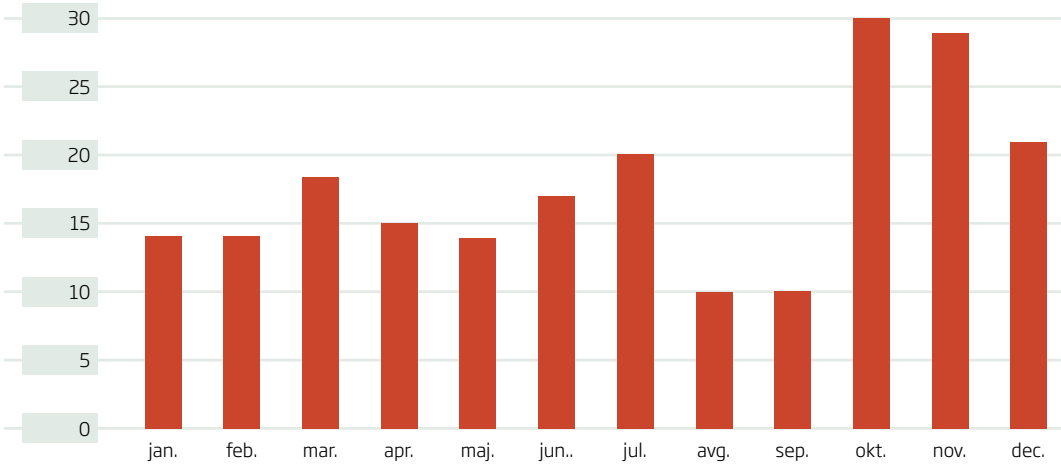
ČESTITKE! TO JE URADNO VAS OBVESTITI, DA JE BIL VAŠ E-MAIL NASLOV IZŽREBAN IN ZADETI 760.000 FUNTOV OB OBLETNICA NAŠEGA PODJETJA.

ORIGINALNA RAYBAN OČALA. LE 35 EVROV. VSI MODELI NA ZALOGI. BREZPLAČNA DOSTAVA. KLIKNI ZDAJ!

In kakšni so bili rezultati celomesečnega dela?

Najočitnejši znak, da so naša sporočila dosegla spletne uporabnike, je velik porast števila prijavljenih incidentov, telefonskih klicev, prošenj za pomoč ali nasvet. Oktobra in novembra smo zabeležili največji skok ravno v številu prijavljenih spletnih goljufij, kar je posledica jasnega poziva uporabnikom, da se lahko v primeru težav obrnejo na našo prijavno točko.

Število obravnavanih spletnih goljufij v letu 2013



Prav tako je oktobra močno narasel obisk portala, število Facebook oboževalcev se je povečalo za 1000, do konca meseca pa smo zabeležili 17.400 ogledov video vodičev na našem YouTube kanalu. Kampanjo ob mesecu kibervarnosti so opazili tudi slovenski mediji, našteli smo 16 objav v medijih, med katerimi so bili vsi največji slovenski novičarski portali. Predvsem bi izpostavili radijsko oddajo **Petkova izvidnica na radiu VAL 202, ki je bila v celoti posvečena temi (ne)varnosti na spletu, oddajo smo uspešno izpeljali v živo kar iz pisarne SI-CERT**.

VESELI DECEMBER TUDI ZA SPLETNE GOLJUFE

AKCIJA OZAVEŠČANJA O VARNEM SPLETNEM NAKUPOVANJU

V poplavi akcijskih ponudb, podkrepljenih z naglico nakupovanja še zadnjih daril, lahko hitro nasedemo velikim obljubam spletnih goljufov. Zato smo tik pred iztekom leta izvedli komunikacijsko akcijo, v sklopu katere smo opozorili na nekaj najpogostejših spletnih prevar, ki smo jim uporabniki izpostavljeni ravno v prazničnem decembru.

Na naši Facebook strani smo organizirali praznično obarvan nagradni izziv. Simpatična nagradna igra **"Spletni goljufi ne poznajo praznikov"** je od tekmovalcev zahtevala, da se sprehodijo med božičnimi stojnicami, ki so predstavljale različno vrsto in stopnjo tveganja: nakup v lažni spletni trgovini, nakup ponaredkov in nakup pri povsem zanesljivem spletnem trgovcu. Na vsaki stojnici so bili različni indici, ki so kazali na varen oz. nevaren nakup, tekmovalci pa so morali prepoznati skrite trike spletnih goljufov.

Prepoznate znake na stojnici, ki kažejo na tvegan nakup?

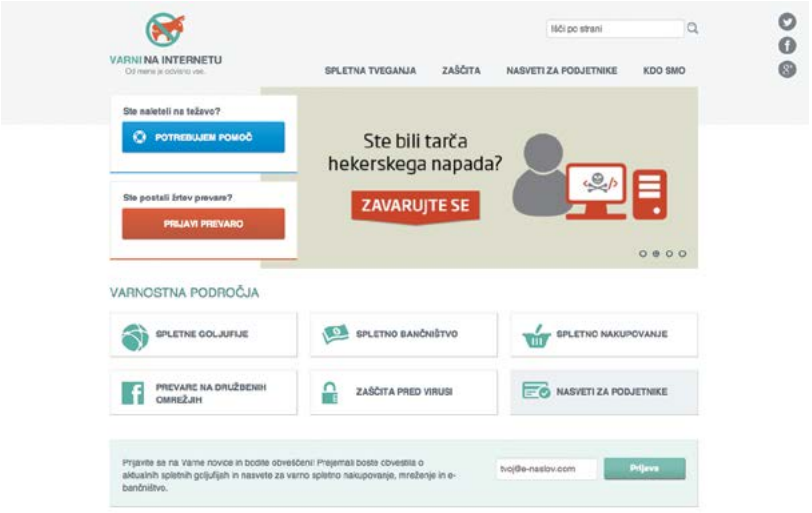
PODOBA NAJ SLEDI VSEBINI

PRENOVA PORTALA VARNI NA INTERNETU

Portal *www.varninainternetu.si* je bil v letu 2013 temeljito prenovljen. Po dveh letih in pol, kolikor je vztrajala stara podoba portala, smo se odločili za spremembo, o kateri smo razmišljali že dlje časa.

Čeprav se dve leti in pol ne sliši veliko, smo v tem času spisali **114 člankov in obvestil, 4 obsežnejše priročnike, posneli 18 video prispevkov**. Portal je bil dobesedno zasut z vsebinami, ta priliv pa je zahteval premislek o informacijski arhitekturi spletnega mesta, ki v stari obliki obiskovalcem ni več omogočal, da bi na preprost način našli vsebine za rešitev svojih težav. Prav tako na portalu ni bilo jasne kategorizacije različnih vrst spletnih tveganj, ki bi olajšale iskanje odgovora na določeno težavo, na katero je uporabnik naletel. Na neustrezno organizacijo vsebin sta kazali tudi visoka stopnja odboja v kombinaciji s precej časa, kolikor se je obiskovalec zadržal na strani, iz česar smo sklepali, da so vsebine zanimive in obiskovalci berejo naše članke, vendar ne obiščejo še drugih strani na portalu.

Prenovljen portal na prvi strani ponudi obiskovalcu šest ključnih kategorij oz. vsebinskih področij, ki so poimenovana enostavno in nedvoumno. Tako obiskovalec že na prvi strani ve, kje iskati odgovor na vprašanje oz. težavo. Do osnovnih vsebinskih področij lahko dostopa iz katerekoli strani tudi prek glavnega menija. Izpostavili smo možnost prijave prevare in najpogostejše težave združili pod kategorijo "Potrebujem pomoč!".



Portal Varni na internetu po prenovi

VARNI
NA INTERNETU

Nacionalni program Varni na internetu smo zasnovali z namenom pomoči, ozaveščanja in izobraževanja širše slovenske javnosti o varni uporabi interneta in prepoznavanja tveganj.

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

KOLOFON

Naslov publikacije:
Poročilo o omrežni varnosti za leto 2013

Avtor publikacije:
Nacionalni center za posredovanje pri omrežnih incidentih SI-CERT

Leto izzida: 2014

Natis: 200 izvodov
Založnik: Javni zavod Arnes

POROČILO O OMREŽNI VARNOSTI ZA LETO 2013

arnes si·cert VARNI NA INTERNETU