si·cert
p.p. 7, SI-1001 Ljubljana
T +386 1 479 88 22, **F** +386 1 479 88 23
E cert@cert.si, www.cert.si

Obravnavani varnostni incidenti v letu 2010

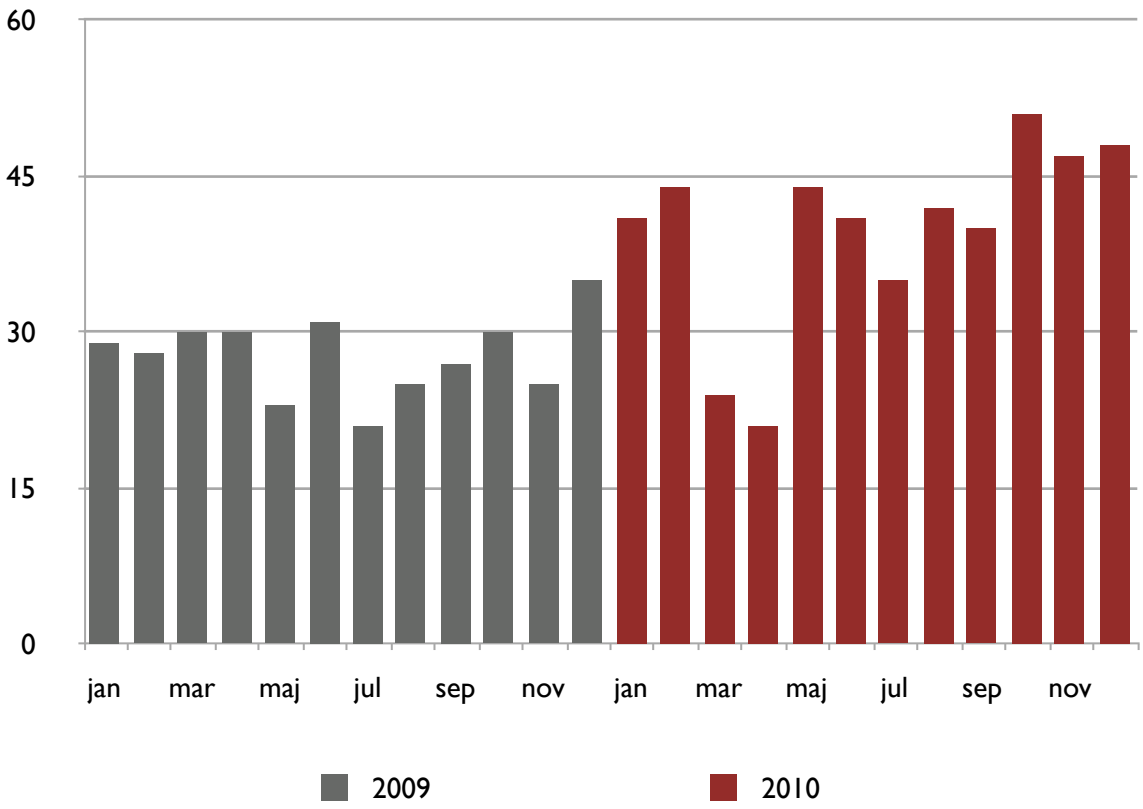
Poročilo Slovenskega centra za obravnavo omrežnih incidentov SI-CERT

Akademska in raziskovalna mreža Slovenije, februar 2011

Število obravnavanih incidentov

SI-CERT je v letu 2010 prejel 1.959 sporočil, od katerih je bilo 861 utemeljenih prijav incidentov (ostalo je predstavljalo vprašanja in sporočila, ki se ne nanašajo na varnostne incidente na omrežju). Na podlagi prijav smo odprli 478 incidentov, kar predstavlja kar 43 % porast v primerjavi z letom 2009.

Število obravnavanih incidentov na mesec v letih 2009 in 2010



Vrste incidentov

Obravnavane incidente razvrščamo v 14 kategorij. Na začetku leta 2010 je bila dodana nova: *kraja omrežne identitete*.

Vprašanja in svetovanja

Raznovrstne poizvedbe. Te vključujejo tudi novinarska vprašanja, največ pa je vprašanj uporabnikov, ki želijo nasvet pri določenem ravnanju ali situaciji na omrežju, lahko tudi hipotetični.

Preiskava zlonamerne kode

Kadar ob obravnavi incidenta naletimo na zlonamerno kodo (angl. *malware*), opravimo njeno analizo v SI-CERT laboratoriju. Običajno gre za *bote*, podtaknjeno javascript kodo, ali zlonamerne priponke (v zadnjem času najpogosteje PDF priponke, ki izkoriščajo ranljivost Acrobat Reader bralnika).

Poskus vdora

Pri poskusu vdora gre lahko za pregledovanje tujih računalnikov na omrežju (t.i. *skeniranje*), ali poskušanje s kombinacijami uporabniških imen in gesel (napad s slovarjem). V splošnem gre za "tipanje" in preizkušanje receptov za izrabo različnih ranljivosti.

Vdor v računalnik

Nepooblaščen vstop v računalniški sistem.

Phishing

Lažne spletne strani za storitev (pogosto za e-bančne storitve), preko katerih napadalec skuša pridobiti identifikacijske podatke uporabnikov.

Spam

Masovno razpošiljanje neželene elektronske pošte, navadno preko zlorabljenih domačih računalnikov ali strežnika. SI-CERT ne obravnava pritožb za posamezno neželeno (spam) sporočilo, ampak le primere, kjer gre za zlorabo oz. nepooblaščeno uporabo računalnika.

Goljufija

Različne vrste spletnih goljufij, od klasične nigerijske "419" prevare, lažnih loterijskih dobitkov in goljufij pri spletnih prodajah in nakupih blaga in storitev.

Botnet

Preiskava botneta, ki združuje večje število zlorabljenih računalnikov, upravljanih preko centralnega nadzornega sistema.

DOS napad

Napad preko omrežja, ki ima za posledico izpad storitve ali resno degradacijo njene kvalitete. Običajno napad poteka s poplavo podatkov, možen pa je tudi napad s posebej prirejeno komunikacijo, ki povzroči izpad storitve.

Zloraba storitve

Uporaba omrežne storitve v namen, za katerega ni bila načrtovana.

Odredba sodišča

Odredba sodišča ali zaprosilo policije za podatke.

Kraja omrežne identitete

Lažno predstavljanje preko storitev na omrežju. Najpogosteje gre za krajo ali nepooblaščeno uporabo gesla za dostop do računa elektronske pošte ali Facebook profila.

Kršitev avtorske pravice

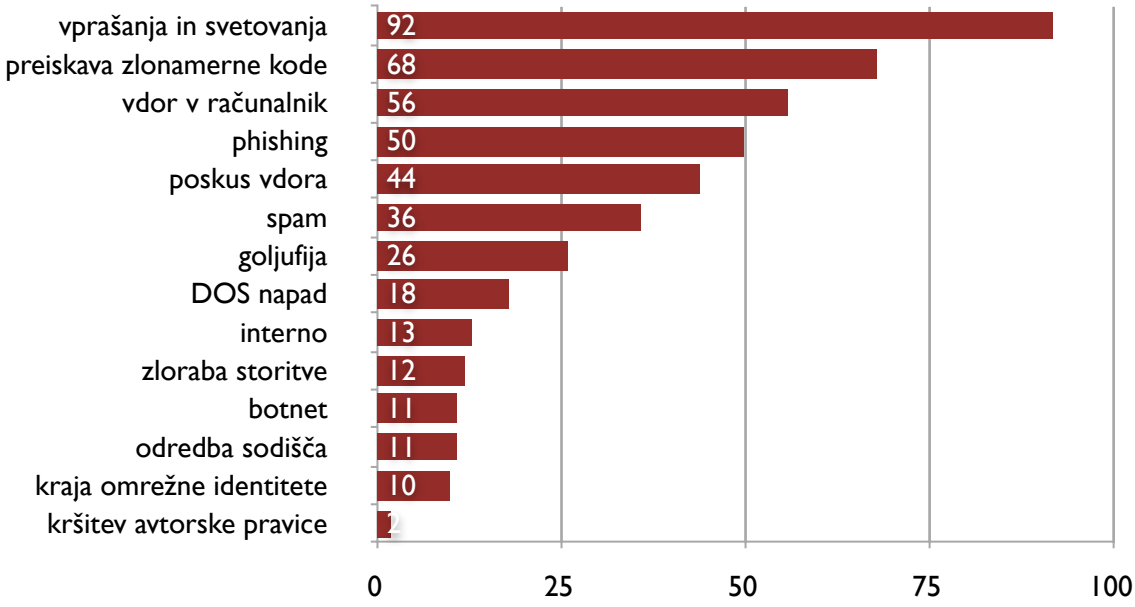
Prijava kršitve avtorske pravice.

Interno

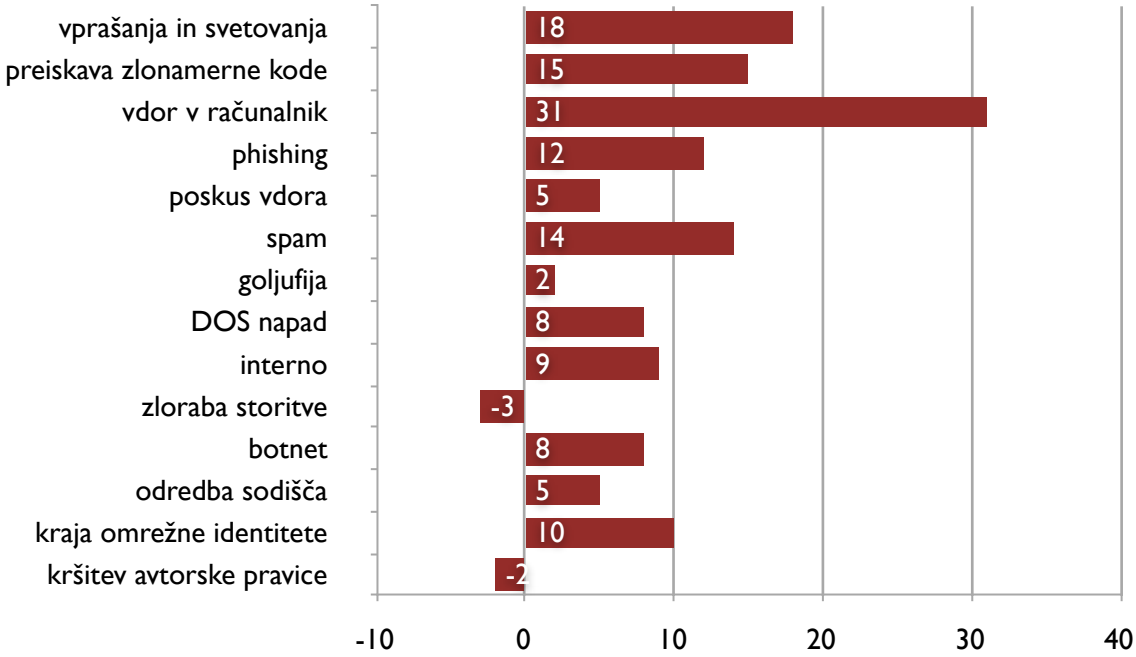
Interna komunikacija in koordinacija z drugimi oddelki Arnesa.

Na prvem mestu po vrsti incidenta se nahajajo različna vprašanja in splošno svetovanje. Iz tega sklepamo, da se lahko z ustreznim izobraževanjem in ozaveščanjem širše javnosti pripomore k bolj varni uporabi omrežja.[1] Sledijo preiskave zlonamerne kode, vdori v računalniške sisteme in phishing. Še vedno torej prednjači "klasično" računalniško vdiranje, čeprav smo porast spletnih goljufij opazili že leta 2009. 29 incidentov ni bilo razvrščenih v nobeno od kategorij.

Število obravnavanih incidentov po kategorijah



Prirast števila incidentov po kategorijah v primerjavi z letom 2009

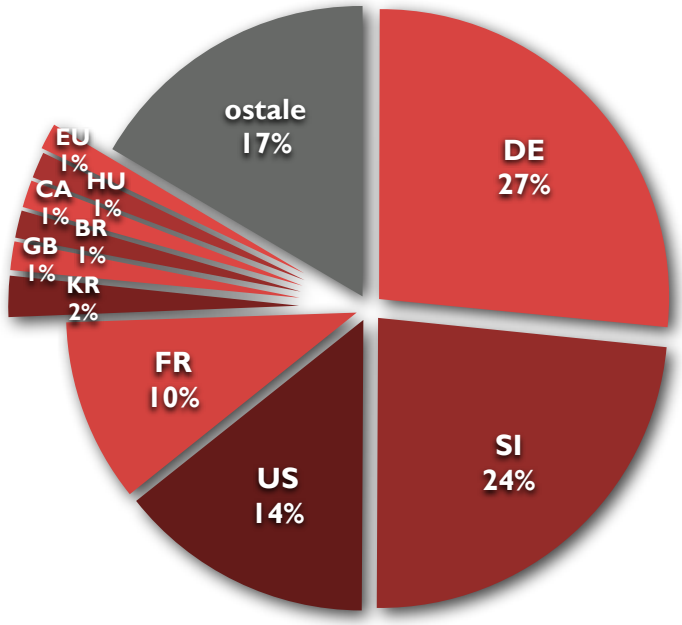


[1] 9. februarja 2011 smo lansirali spletno mesto **varninainternetu.si**, ki je namenjeno izobraževanju in ozaveščanju odraslih domačih uporabnikov in malih podjetij oz. samostojnih podjetnikov.

IP naslovi

Ob obravnavi posameznega incidenta lahko zabeležimo različne IP naslove. Lahko gre za napaden strežnik, za IP naslov napadalca, ali pa za velik spisek naslovov, ki so bili tarča t.i. omrežnega *skeniranja*. Zbranim naslovom na podlagi javno dostopnih whois imenikov določimo državo (ki je običajno država, kjer ima ponudnik svoj sedež). Ker pa gre za IP naslove, ki so se pojavljali v različnih vlogah in razmerjih, ne moremo prehitro sklepati na prava razmerja med različnimi državami, ki so bile izvor ali cilj nekega incidenta, vseeno pa lahko v grobem vidimo, katera območja se nas pri varnostnih incidentih bolj dotikajo in katera manj.

Prvih 10 držav po številu IP naslovov v obravnavanih incidentih



Število različnih IP naslovov v obravnavanih incidentih po državah

število	država	število	država	število	država	število	država
804	DE	16	UA	5	VE	1	AT
711	SI	14	BY	4	MY	1	BA
429	US	13	HK	4	PR	1	BD
307	FR	13	IT	4	TH	1	DO
65	KR	12	BE	3	CR	1	EE
44	GB	12	VN	3	HR	1	IE
42	BR	10	ES	3	IL	1	KW
42	CA	10	SE	3	LU	1	KZ
40	HU	9	NG	3	NO	1	LB
40	EU	8	BG	3	NZ	1	MK
38	NL	8	CH	3	RS	1	MR
28	PL	8	LT	3	SK	1	MX
27	CN	7	IN	3	SN	1	PA
27	RO	7	QA	2	AR	1	PK
25	TW	6	LV	2	BS	1	SA
22	JP	5	AU	2	LY	1	SG
22	RU	5	CO	2	ME	1	TN
22	TR	5	DK	2	PT		
20	PE	5	EG	1	AE		
18	CZ	5	IR	1	AG		

Nekaj izpostavljenih primerov

Analiza slovenskega Facebook botneta 16. 3. 2010

http://www.cert.si/obvestila/obvestilo/browse/2/article/analiza-slovenskega-facebook-botneta/44.html

Analizirali smo programskega črva, ki se je širil preko facebook omrežja in je zlorabljene računalnike povezal v botnet. O dogodku so poročali tudi nekateri tuji in slovenski mediji, ki so ugotavljali, da napad morda izvira iz Hrvaške. Naša analiza je pokazala, da napad izvira kar iz Slovenije. V kodi enega izmed programov smo celo našli podatek, kje se je nahajala projektna datoteka na avtorjevem sistemu. Čeprav smo avtorja identificirali, je ta zaradi sporočila finskega protivirusnega podjetja F-Secure hitro pobrisal sledove na svojem računalniku in Facebook profilu.

Stuxnet virus 25. 7. 2010

http://www.cert.si/obvestila/obvestilo/article/si-cert-2010-04-windows-lnk-kriticna-ranljivost/35.html
http://www.cert.si/obvestila/obvestilo/browse/1/article/najnevarnejsi-virus-doslej/44.html

Stuxnet je virus, ki se širi preko USB ključev in omrežnih diskovnih pogonov, namenjen pa je motenju Siemens SCADA industrijskih sistemov za proizvodnjo obogatenega urana. Podpisan je bil kot Microsoft gonilnik z veljavnimi šifrirnimi ključi tajvanskih podjetij, domnevna tarča pa je iranski jedrski program. Ob incidentu smo izpeljali koordinacijo obveščanja preko slovenskega predstavništva Siemens podjetja in v sodelovanju z Direktoratom za e-upravo in upravne procese pri Ministrstvu za javno upravo Republike Slovenije.

Sodelavec SI-CERT pričal na ameriškem sodišču 20. 9. 2010

http://www.cert.si/obvestila/obvestilo/article/sodelavec-si-cert-pricel-na-ameriskem-sodiscu/44.html

15. novembra 2007 smo na SI-CERT prejeli več prijav, ki so se nanašale na sklop distribuiranih napadov na strežnik www.rickross.com. Napadalec je okužil tuje računalnike in z njih bombardiral spletni strežnik s pogostimi zahtevki. Okuženi računalniki, med njimi tudi slovenski, so bili povezani v botnet, preko katerega je napadalec izdajal ukaze.

Takrat smo se z lastnikom enega od okuženih računalnikov dogovorili, da smo lahko na sistemu opravili analizo in našli zlonamerno kodo, ki je napade izvajala. V SI-CERT laboratoriju smo nato opravili analizo bota, ter popisali njegove značilnosti in delovanje. Naši izsledki so pripomogli k temu, da je ameriški FBI 30. junija 2009 aretiral Bruca Raisleya, ki je bil nato obtožen napada na več spletnih strežnikov.

15. septembra, se je Camdenu v New Jerseyu pričelo sojenje Brucu Raisleyu, kjer je na povabilo ameriškega okrožnega tožilstva nekaj dni kasneje pričal tudi Tadej Hren iz Arnesovega centra SI-CERT, ki je leta 2007 vodil obravnavo tega incidenta in v SI-CERT laboratoriju opravil analizo zlonamerne kode, ki je omogočila identifikacijo storilca.

Raisley je bil obtožen, da je uporabljal DDoS (distributed denial-of-service) napade proti spletnim stranem medijev, ki so objavili zgodbo o njegovem razkritju. Sodeloval je namreč s skupino Perverted Justice, ki je za televizijsko hišo NBC snemala serijo "To Catch a Predator." V njej so pred kamero razkrivali ljudi, ki so se za zmenke dogovarjali z mladoletnimi osebami. Med Raisleyem in skupino je prišlo do konflikta, po katerem so Raisleya na podoben način ujeli in razkrinkali, ter zgodbo dali v javnost. Raisley se je maščeval z napadom na strežnike, ki so zgodbo objavili.

22. septembra 2010 je bil Bruce Raisley spoznan za krivega.