CERT-LT apibendrina 2012 m. I ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2012 m. I ketvirčio veiklos rezultatus. CERT-LT 2012 m. I ketvirtį ištyrė 4 748 iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su 2011 m. IV ketvirčiu (5 815 pranešimų), pranešimų sumažėjo 18 procentų. CERT-LT ištyrė visus gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti jų padarinius ar sustabdyti jų plitimą.

Daugiausia ištirta pranešimų apie kenkėjišką programinę įrangą, kompiuterių ir informacinių sistemų užvaldymo atvejus. Per šį laikotarpį CERT-LT ištyrė 3 274 pranešimus apie kenkėjišką programinę įrangą – 2 proc. mažiau nei 2011 m. IV ketvirtį, ir 1 344 pranešimus apie kompiuterių užvaldymo atvejus – 43 proc. mažiau nei 2011 m. IV ketvirtį. CERT-LT atliktų tyrimų duomenys parodė, kad tarp kenkėjiškos programinės įrangos incidentų daugiausia buvo susijusių su kenkėjiška programine įranga, kuri veikdama pažeidžia kompiuterio valdymą ir įtraukia jį į *botnet* tinklą, ir kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėms, pasitelkiant *botnet* tinklus.

Pirmąjį šių metų ketvirtį Lietuvoje kenkėjiška programinė įranga aktyviai plito per pokalbių programą „Skype“ ir socialinius tinklus. Kenkėjiškos programos siuntinėjo žinutes „Skype“ ir „Facebook“ naudotojų adresatams, siūlančias aplankyti kenkėjišką svetainę, kurioje buvo virusas. CERT-LT išnagrinėjo kenkėjiškos programinės įrangos pavyzdį ir išsiuntė antivirusinių programų gamintojams, kad jie atnaujintų virusų aprašų duomenų bazes. Taip pat CERT-LT nurodė svetainės prieglobos teikėjui, kad pašalintų iš jos kenkėjišką programinę įrangą, įspėjo interneto naudotojus ir pateikė rekomendacijas.

Šį ketvirtį padidėjo pranešimų skaičius (24 pranešimai) apie elektronines paslaugos trikdymo atakas (DDoS). Palyginti su 2011 m. IV ketvirčiu (12 pranešimų), pranešimų skaičius padidėjo 2 kartais. CERT-LT tyrimų duomenimis, šios atakos buvo vykdomos automatizuotomis priemonėms, pasitelkiant *botnet* resursus. CERT-LT teikė rekomendacijas, kaip stabdyti šias atakas, tinklalapių savininkams ar tinklalapių prieglobos

paslaugas teikiančioms įmonėms bei koordinavo veiksmus su interneto paslaugų teikėjais ir CERT tarnybomis siekiant nutraukti vykdomas atakas.

2012 m. sausio 27 d. – vasario 9 d. vyko elektroninės paslaugos trikdymo atakos (DDoS) prieš Lietuvos banko informacines sistemas. CERT-LT atlikti tyrimai parodė, kad DDoS atakų metu buvo naudojamas *botnet* tinklas, o atakų tipas kelis kartus keitėsi, dėl ko šis incidentas turėjo reikšmingos įtakos. Susidurta informacinių sistemų paslaugų trikdymu, ryšio kanalo perpildymu, IP adresų klastojimu ir pan. Nustatyti 9219 unikalūs atakos šaltinių IP adresai iš 87 šalių, tarp jų – 15 iš Lietuvos. Glaudus bendradarbiavimas šio incidento metu tarp CERT-LT, Lietuvos banko darbuotojų, interneto paslaugų teikėjų bei užsienio CERT tarnybų leido efektyviai kovoti su ataka bei išvengti didesnių nuostolių.

Taip pat gauti ir tirti pranešimai apie manipuliaciją elektroniniais duomenimis – 3 (2011 m. IV ketvirtį – 4) ir elektroninių duomenų klastojimą – 29 (2011 m. IV ketvirtį – 38).

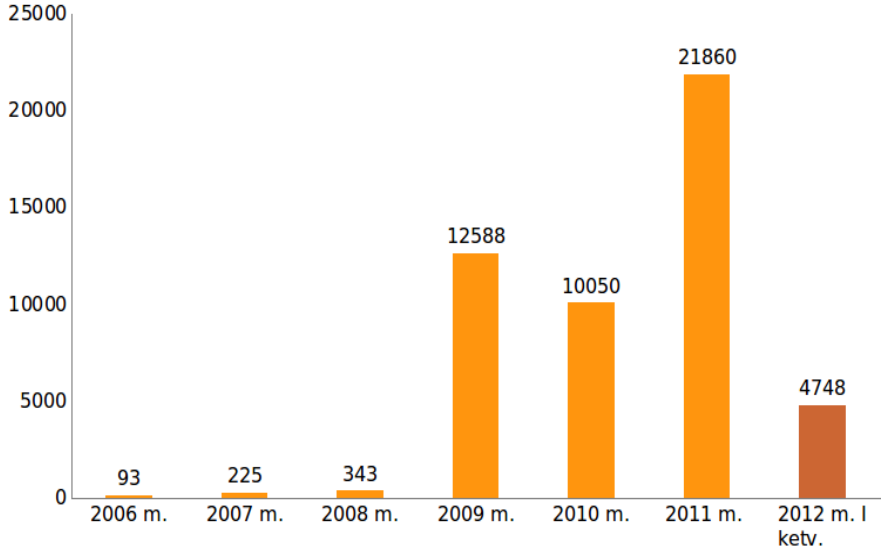
CERT-LT registruoja ir skelbia informaciją apie botnet tinkluose aptiktų kompiuterių aktyvumą. Naudotojas, kilus įtarimui, kad jo kompiuteris gali būti įtrauktas į *botnet* tinklo veiklą, gali pasitikrinti CERT-LT tinklalapyje https://www.cert.lt/tikrinti, ar kompiuterio interneto protokolo (IP) adresas nėra užfiksuotas CERT-LT duomenų bazėje kaip dalyvaujantis kenkėjiškoje veikloje. CERT-LT, bendradarbiaudama su Lietuvos interneto paslaugų teikėjais bei su kitomis CERT grupėmis, kovoja su šiais tinklais, informuoja interneto naudotojus, jei jų kompiuteriai buvo įtrauktį į šį tinklą, pateikia rekomendacijas, kaip išvalyti kompiuterį bei apsaugoti jį ateityje.

Naudotojams, susidūrusiems su tinklų ir informacijos saugumo problemomis, patariama nedelsiant kreiptis į savo interneto paslaugų teikėją, o jei šis problemų išspręsti negali, informuoti apie tai CERT-LT užpildant specialią formą tinklalapyje www.cert.lt/pranesti.html.

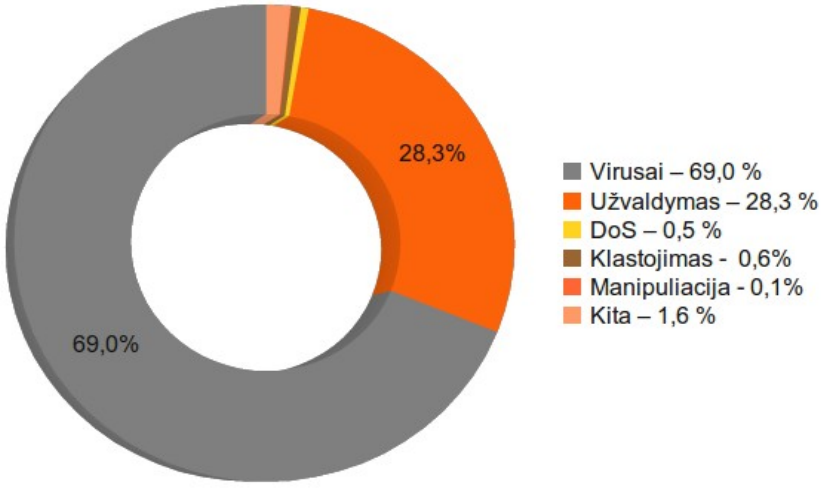
Lentelė. Tirtų pranešimų apie incidentus skyrimas pagal tipus

Incidentų tipas	Incidentų skaičius 2012 m. I ketv. (vnt.)	Procentinė dalis nuo visų incidentų
Virusas	3 274	69
Užvaldymas	1 344	28,3
Klastojimas	29	0,6
Manipuliacija	3	0,1
DoS	24	0,5
Kiti	74	1,6

2006–2012 m. CERT-LT incidentų statistika



2012 m. I ketvirčio CERT-LT incidentų statistika



Visas CERT-LT incidentų statistikos ataskaitas galite rasti internetinėje svetainėje https://www.cert.lt/statistika.html.