CERT-LT apibendrina II ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2011 m. II ketvirčio veiklos rezultatus. CERT-LT 2011 m. II ketvirtį tyrė 5 758 iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, tiriančių tarptautinius incidentus, ir iš Lietuvos interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su 2011 m. I ketvirčiu (2 508 pranešimų), tirtų pranešimų apie incidentus padaugėjo 130 procentų. CERT-LT ištyrė visus gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti jų padarinius ar sustabdyti jų plitimą.

Antrąjį 2011 m. ketvirtį itin padaugėjo pranešimų apie kompiuterių užvaldymo incidentus ir kenkėjišką programinę įrangą. Per šį laikotarpį CERT-LT ištyrė 1 551 pranešimą apie kompiuterių užvaldymo incidentus, 3 160 pranešimų apie kenkėjišką programinę įrangą – 2 kartais daugiau nei 2011 m. I ketvirtį. Tokį didelį ištirtų pranešimų skaičių lėmė bendradarbiavimas su naujais tarptautiniais partneriais, tiriančiais tarptautinius incidentus. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėms, pasitelkiant *botnet* tinklus. CERT-LT ir toliau fiksuoja šių incidentų augimo tendencijas.

Antrąjį metų ketvirtį Lietuvoje suaktyvėjo „Zeus“ atmainos kenkėjiška programinė įranga. Ją pasitelkiant galima perimti interneto naudotojų prisijungimų duomenis prie įvairių tinklalapių, tarp jų ir elektroninės bankininkystės, socialinių tinklų bei elektroninio pašto. Taip pat šį ketvirtį padaugėjo nepageidaujamų el. pašto pranešimų (SPAM) – jie dešimtis kartų viršijo įprastus kiekius Lietuvoje. CERT-LT užfiksavo, kad suaktyvėjusio SPAM laiškai pasižymėjo kirilicos simboliais žinutės tekste ir atitinkama koduote antraštėse. Dažniausiai tokie SPAM pranešimai siunčiami pasitelkiant kenkėjišką programinę įrangą ir kompiuterių tinklą *botnet*. CERT-LT nuolatos registruoja ir skelbia informaciją apie botnet tinkluose aptiktų kompiuterių aktyvumą. Apie minėtus atvejus CERT-LT birželio mėnesį įspėjo interneto naudotojus ir pateikė rekomendacijas.

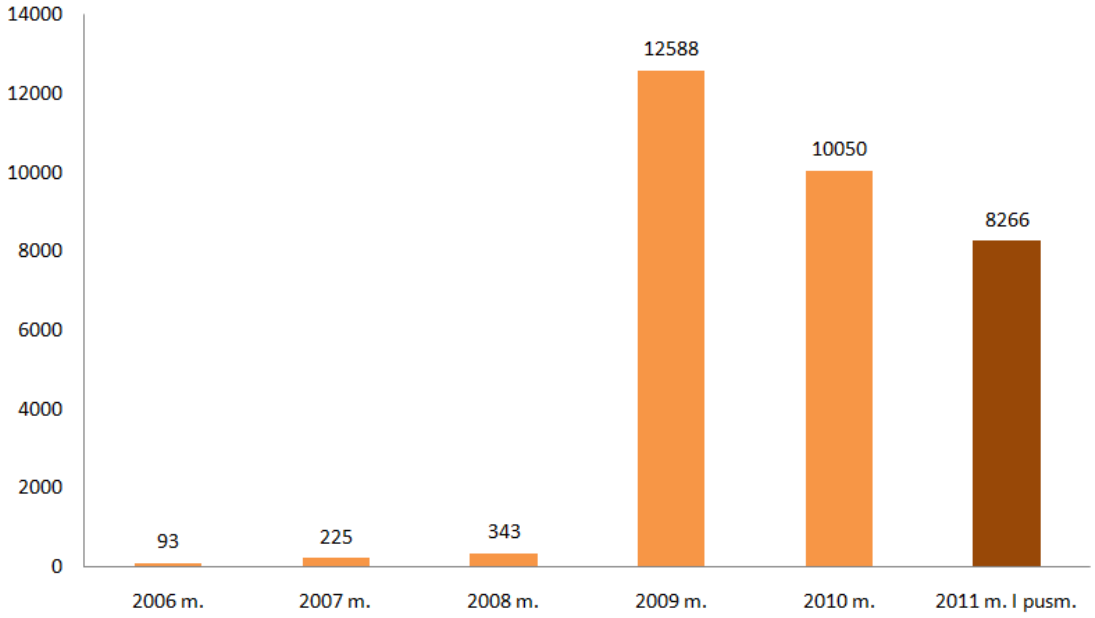
Taip pat gauti ir tirti pranešimai apie šiuos incidentus: dėl elektroninės paslaugos trikdymo atakų (angl. *Denial of Service*, DoS) – 49 (2011 m. I ketvirtį – 12); dėl klastojimo – 38 (2011 m. I ketvirtį – 6); dėl manipuliacijos – 5 (2011 m. I ketvirtį – 5).

Tirti pranešimai apie incidentus pagal tipus:

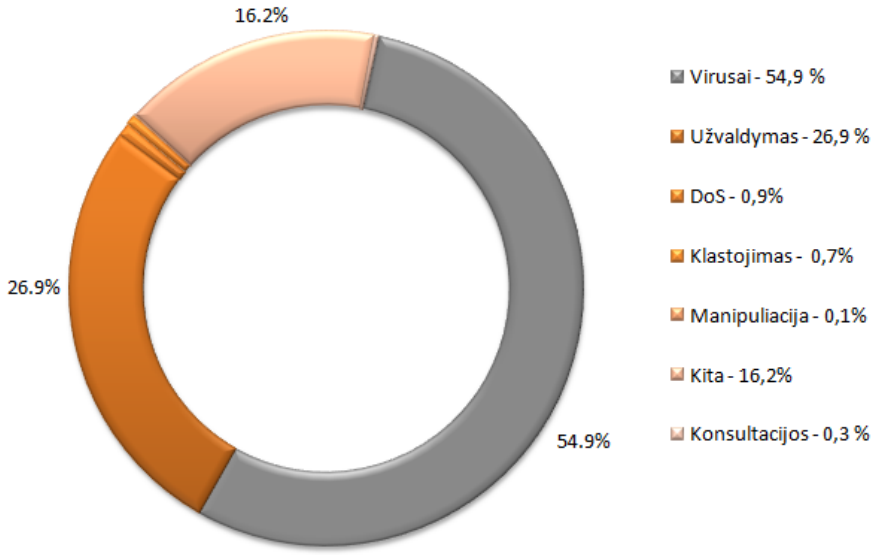
Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2011 m. II ketv.	Incidentų skaičius 2011 m. II ketv. (proc.)
Virusai	Kenkėjiška programinė įranga (angl. *Virus, Worm)* – programinė įranga ar jos dalis, specialiai sukurta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (taip pat perimti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.	3 160	54,9
DoS	Elektroninės paslaugos	49	0,9

	trikdymo ataka (angl. *DoS*) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar) informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas.		
Užvaldymas	Neleidžiamasis naudojimasis informacinės sistemos ištekliais (angl. *Web Site Defacement*) – neteisėtas informacinės sistemos išteklių naudojimas. Neleidžiamasis prisijungimas (angl. *System Compromise/Intrusion*) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.	1 551	26,9
Klastojimas	Elektroninių duomenų klastojimas (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	38	0,7
Manipuliacija	Manipuliacija elektroniniais duomenimis (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	5	0,1
Kiti		935	16,2
Konsultacijos		20	0,3

2006–2011 m. CERT-LT incidentų statistika



2011 m. II ketvirčio CERT-LT incidentų statistika



Incidentų statistikos ataskaitas galite rasti internetinėje svetainėje https://www.cert.lt/statistika.html