

CERT-LT apibendrina I ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys [CERT-LT](#) apibendrina 2011 m. I ketvirčio veiklos rezultatus. [CERT-LT](#) per 2011 m. I ketvirtį tyrė 2 508 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 2010 m. I ketvirčiu (2 313 pranešimų), tirtų pranešimų apie incidentus padaugėjo 8 procentais.

Pirmąjį metų ketvirtį itin padaugėjo pranešimų apie kompiuterių užvaldymo incidentus. CERT-LT ištyrė 707 pranešimus – 22 kartais daugiau nei 2010 m. IV ketvirtį (33 pranešimai). Tokį didelį ištirtų pranešimų skaičių lėmė bendradarbiavimas su naujais tarptautiniais partneriais, atliekančiais tarptautinius incidentų tyrimus. Pasirašyti bendradarbiavimo susitarimai dėl informacijos teikimo, susijusios su tinklų ir informacijos saugumo pažeidimais, užfiksuotais Lietuvos Respublikos viešuosiuose elektroninių ryšių tinkluose ir informacinėse sistemose. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant botnet tinklus. CERT-LT ir toliau stebi šių incidentų augimo tendencijas.

Daugiausia ištirta pranešimų (1 588) apie kenkėjišką programinę įrangą, kuri veikdama gali pažeisti kompiuterio valdymą ir įtraukti jį į *botnet* tinklą. Glaudžiai bendradarbiaujant su tarptautiniais partneriais, gaunama vis daugiau pranešimų apie Lietuvoje plintančius kompiuterių „zombius“, dalyvaujančius *botnet* tinklo veikloje. Pasitelkus kenkėjišką programinę įrangą valdomų kompiuterių tinklas dažnai naudojamas kaip priemonė kitoms saugumo atakoms vykdyti. CERT-LT nuolat registruoja ir skelbia informaciją apie [botnet tinkluose aptiktų kompiuterių aktyvumą](#).

Taip pat gauti ir tirti pranešimai apie šiuos incidentus: dėl elektroninės paslaugos trikdymo atakų (angl. *Denial of Service*, DoS) – 12 (2010 m. IV ketvirtį – 10); dėl klastojimo – 6 (2010 m. IV ketvirtį – 8); dėl manipuliacijos – 5 (2010 m. IV ketvirtį – 8).

CERT-LT ištyrė visus gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti jų padarinius ar sustabdyti jų plitimą.

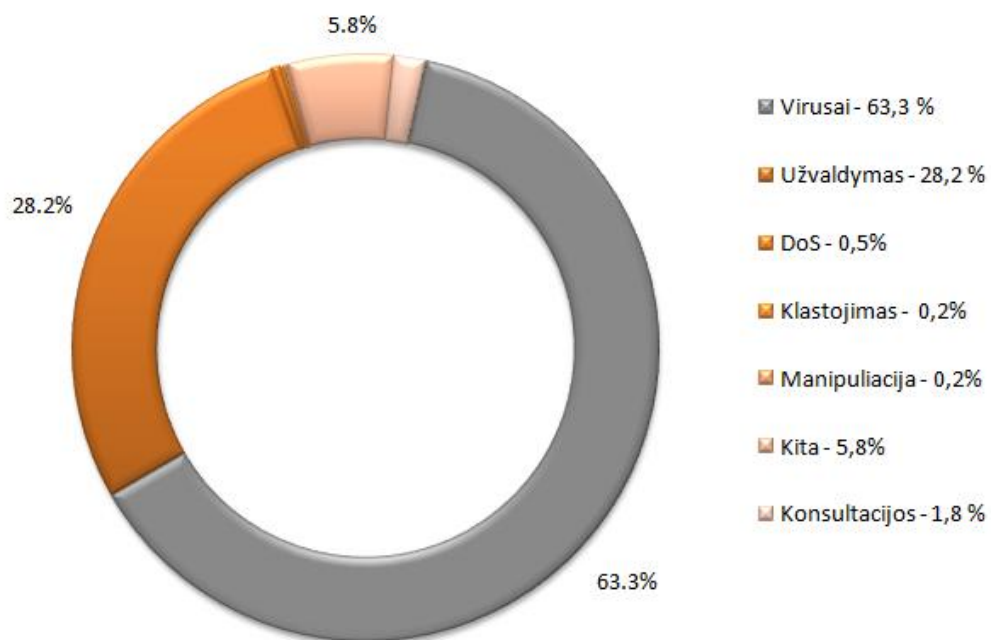
Pirmąjį ketvirtį CERT-LT 44 kartus konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

Tirti pranešimai apie incidentus pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2011 m. I ketv.	Incidentų Skaičius 2011 m. I ketv. (proc.)
Virusai	Kenkėjiška programinė įranga (angl. <i>Virus, Worm</i>) – 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.	1 588	63,3

DoS	Elektroninės paslaugos trikdymo ataka (angl. <i>DoS</i>) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar) informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas.	12	0,5
Užvaldymas	Neleidžiamasis naudojimas informacinės sistemos ištekliams (angl. <i>Web Site Defacement</i>) – neteisėtas informacinės sistemos išteklių naudojimas. ir Neleidžiamasis prisijungimas (angl. <i>System Compromise/Intrusion</i>) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.	707	28,2
Klastojimas	Elektroninių duomenų klastojimas (angl. <i>Phishing</i>) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	6	0,2
Manipuliacija	Manipuliacija elektroniniais duomenimis (angl. <i>Spyware</i>) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	5	0,2

Kiti		146	5,8
Konsultacijos		44	1,8



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