

CERT-LT apibendrina IV ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys **CERT-LT** apibendrina 2010 m. IV ketvirčio veiklos rezultatus. **CERT-LT** per 2010 m. IV ketvirtį tyrė 2 620 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 2009 m. IV ketvirčiu (3 276 pranešimai), tirtų pranešimų sumažėjo 20 procentais. Palyginti su 2010 m. III ketvirčiu (2 375 pranešimų), tirtų pranešimų apie incidentus padaugėjo 10 procentų.

Daugiausia ištirta pranešimų (2 503) apie kenkėjišką programinę įrangą, kuri veikdama gali pažeisti kompiuterio valdymą ir įtraukti jį į *botnet* tinklą, t. y. pasitelkus kenkėjišką programinę įrangą valdomų kompiuterių tinklas dažnai panaudojamas kaip priemonė kitoms saugumo atakoms vykdyti. Glaudžiai bendradarbiaujant su tarptautiniais partneriais, gaunama vis daugiau pranešimų apie Lietuvoje plintančius kompiuterių „zombius“, dalyvaujančius *botnet* tinklo veikloje. CERT-LT ir toliau registruoja ir skelbia informaciją apie *botnet* tinkluose aptiktų kompiuterių aktyvumą. Naudotojui kilus įtarimų, kad jo kompiuteris gali būti įtrauktas į *botnet* tinklo veiklą, gali pasitikrinti tinklalapyje www.esaugumas.lt/botnet, ar jo kompiuterio IP adresas (angl. Internet Protocol) nėra užfiksuotas *botnet* duomenų bazėje.

Dalyvaudamas projekte „Draugiškas internetas“ (www.draugiskasinternetas.lt) CERT-LT 2010 m. IV ketvirtį gavo ir išnagrinėjo 151 pranešimą apie neteisėtą ir žalingą turinį internete. CERT-LT pagal suderintus kriterijus nustatė 16 (tiek pat kaip ir 2010 m. III ketvirtį) atvejų, kai galbūt buvo pažeisti Lietuvos Respublikos įstatymai dėl neteisėto turinio internete. Su šiais atvejais susijusi medžiaga ir duomenys perduoti atsakingoms institucijoms tolesniam tyrimui.

CERT-LT šį ketvirtį gavo 84 pranešimus apie nepageidaujamus elektroninio pašto laiškus (angl. spam). Išsamesniam tyrimui jie perduoti *spam* atvejus nagrinėjančioms kompetentingoms institucijoms, nes juose nebuvo aptikta saugumo spragų, kurios galėtų turėti neigiamos įtakos elektroninio pašto informacinių sistemų veikimui Lietuvos Respublikoje.

Be minėtų, tirti pranešimai apie šiuos incidentus: dėl užvaldymo – 33 (2010 m. III ketvirtį – 61); dėl elektroninės paslaugos trikdyto atakų (angl. Denial of Service, DoS) – 10 (2010 m. III ketvirtį – 7); dėl klastojimo – 8 (2010 m. III ketvirtį – 7); dėl manipuliacijos – 8 (2010 m. III ketvirtį – 6). CERT-LT ištyrė visus iš interneto naudotojų ir interneto paslaugų teikėjų gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti jų padarinius ar sustabdyti jų plitimą.

CERT-LT 11 kartų konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

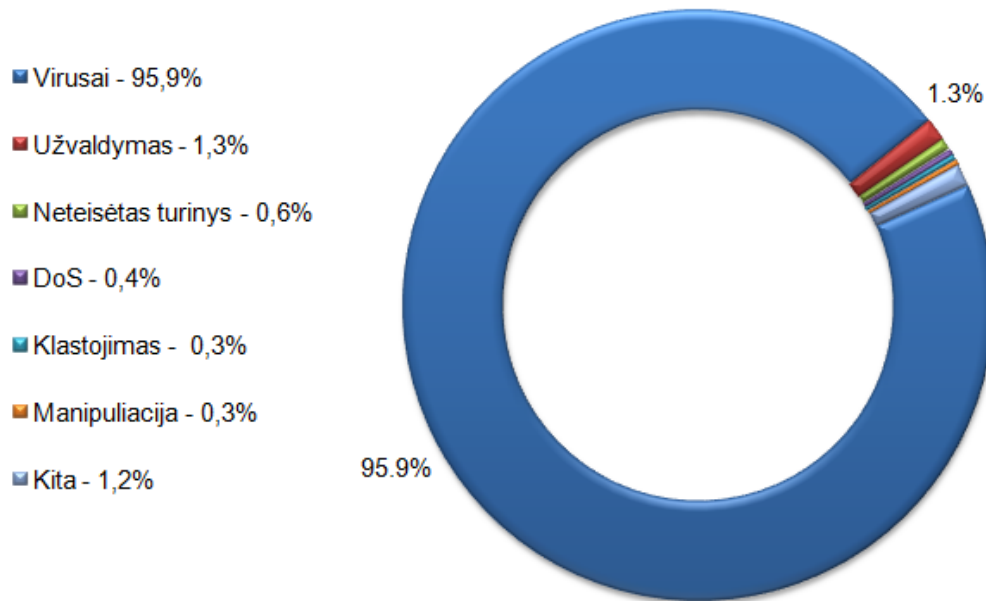
Tirti pranešimai apie incidentus pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2010 m. IV ketv.	Incidentų Skaičius 2010 m. IV 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	2 503	95,9

	duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.		
Spam	Nepageidaujamas elektroninis paštas (angl. <i>spam</i>) – elektroninio pašto laiškų tiesioginės rinkodaros tikslais siuntimas be elektroninio pašto naudotojo ir (ar) abonento išankstinio sutikimo, galintis turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui Lietuvos Respublikoje.	0 (gauta 84 pranešimai apie pavienį nepageidaujamą elektroninį paštą)	0
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.	10	0,4
Neteisėtas turinys	Neteisėtas turinys – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	16	0,6
Užvaldymas	Neleidžiamasis	33	1,3

	<p>naudojimas informacinės sistemos ištekliais (angl. <i>Web Site Defacement</i>) – neteisėtas informacinės sistemos išteklių naudojimas.</p> <p>ir</p> <p>Neleidžiamasis prisijungimas (angl. <i>System Compromise/Intrusion</i>) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.</p>		
Klastojimas	<p>Elektroninių duomenų klastojimas (angl. <i>Phishing</i>) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.</p>	8	0,3
Manipuliacija	<p>Manipuliacija elektroniniais duomenimis (angl. <i>Spyware</i>) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.</p>	8	0,3
Kiti		31	1,2

2010 m. IV ketvirčio CERT-LT incidentų statistika



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