# CERT-LT apibendrina 2010 metų veiklą

**Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2010 metų veiklos rezultatus. CERT-LT 2010 metais tyrė 10 050 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 metais (12 588 pranešimai), pranešimų sumažėjo 20 procentų.**

Didžiausia problema, su kuria, CERT-LT duomenimis, 2010 metais susidūrė Lietuvos interneto naudotojai, buvo kenkėjiška programinė įranga, sudariusi 92,8 proc. visų tirtų pranešimų.
Tarp jų daugiausia incidentų, susijusių su kenkėjiška programine įranga, kuri veikdama gali pažeisti kompiuterio valdymą ir įtraukti jį į *botnet* tinklą. Nustatyta, kad ir 2010 metais kenkėjiška programinė įranga buvo platinama per nešiojamas duomenų laikmenas, socialinius tinklus ir internetinių pokalbių programas.

2010 metais itin padaugėjo pranešimų apie kompiuterių užvaldymo incidentus. CERT-LT ištyrė 477 pranešimus –2.65 karto daugiau nei 2009 metais (180 pranešimų). Didžiąją šių tirtų pranešimų dalį sudarė pranešimai apie neteisėtus prisijungimus prie interneto svetainių, įterpiant į jas kenkėjišką kodą, galintį paveikti jų lankytojų kompiuterių programinę įrangą. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma tinklalapių buvo užvaldyti dėl to, kad teisėtų savininkų prisijungimo duomenis atiteko piktavaliams. Dažnas piktavalių taikinys − pasitelkiant kenkėjiškas programas pasisavinti įvairiose programose, elektroninio pašto žinutėse ar kituose elektroniniuose tekstuose saugomus prisijungimo duomenis. CERT-LT informavo tinklalapių savininkus ar tinklalapių prieglobos paslaugas teikiančias įmones apie pastebėtus kenkėjiškus programos kodus ir paprašė juos pašalinti, nes per pažeistus tinklalapius toliau platinamas kenkėjiškas programos kodas. CERT-LT ir toliau stebi šių incidentų skaičiaus didėjimo tendencijas.

Dalyvaudamas projekte „Draugiškas internetas“ (www.draugiskasinternetas.lt), CERT-LT 2010 metais gavo ir išnagrinėjo 451 pranešimą apie neteisėtą ir žalingą turinį internete. CERT-LT pagal suderintus kriterijus nustatė 63 (14 proc. mažiau nei 2009 m.) atvejus, kai

buvo požymių, jog gali būti pažeisti Lietuvos Respublikos įstatymai dėl neteisėto turinio internete. Visa surinkta medžiaga perduota atsakingoms institucijoms tolesniam tyrimui.

Viena iš didžiausių tinklų ir informacijos saugumo grėsmių pasaulyje bei Lietuvoje ir toliau išlieka *botnet* tinklai, kuriuos pasitelkiant vykdoma kita nusikalstama veikla, tokia kaip kenkėjiško kodo, nepageidaujamų elektroninių pašto laiškų platinimas, paslaugos trikdymo atakos ir kitos nusikalstamos veiklos. CERT-LT, glaudžiai bendradarbiaudama su tarptautiniais partneriais, gauna vis daugiau pranešimų apie Lietuvoje plintančius kompiuterių „zombius“, dalyvaujančius *botnet* tinklo veikloje. 2010 metais Lietuvoje kasdien buvo vidutiniškai 10000 aktyvių kompiuterių „zombių“. 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. CERT-LT, bendradarbiaudama su Lietuvos interneto paslaugų teikėjais bei su kitomis CERT grupėmis, kovoja su šiais tinklais, informuoja interneto naudotojus apie pastebėtą jų kompiuterių dalyvavimą šioje veikloje, pateikia rekomendacijas, kaip išvalyti kompiuterį bei apsaugoti jį ateityje.

2010 metais CERT-LT gavo 381 pranešimą 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.

Siekdamas didinti IT saugumo supratimą Lietuvoje, CERT-LT 61 kartą konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

**2011 metų prognozės**

Auga išmaniųjų telefonų populiarumas net tik tarp vartotojų, bet ir tarp įmonės darbuotojų, kurie juos naudoja prisijungti prie interneto, el. pašto bei įmonės tinklo. Šių įrenginių naudotojai saugumu rūpinasi nepakankamai, retas naudoja saugumo priemones. Todėl tikėtina, kad 2011 metais kenkėjiška programinė įranga dar labiau plis šiuose įrenginiuose,

išnaudojant įrenginių naudotojų patiklumą, operacinės sistemos ar trečiųjų šalių programinės įrangos pažeidžiamumus bei klaidas.

Taip pat spėjama, kad dar labiau plis kenkėjiška programinė įranga MAC OS sistemose, daugės kenkėjiškos programinės įrangos, sugebančios pažeisti ar sutrikdyti kritinių infrastruktūrų sistemų darbą.

2011 metais, tikėtina, atsiras dar sudėtingesnis kenkėjiškas programinis kodas, kuris išnaudos ne vieną, o kelias programinės įrangos spragas. Dėl to ne taip efektyviai veiks apsaugos programos, bus sunkiau aptikti tas spragas.

2011 metais kenkėjiško kodo plitimas ir privačios bei konfidencialios informacijos vagystės socialiniuose tinkluose turėtų didėti, nes vartotojų skaičius juose smarkiai auga.

Prognozuojama, kad ir toliau augs bei sudėtingės *botnet* tinklai, į kuriuos įsitrauks vis daugiau interneto naudotojų. Todėl šiais metais reikėtų laukti dar sudėtingesnių ir aktyvesnių saugumo atakų, organizuotų šiais tinklais.

Kaip ir paskutiniais keleriais metais, taip ir šiemet pagrindinė saugumo atakų, incidentų priežastis bus ekonominė piktavalių motyvacija, tad saugumo atakų padaroma žala gali didėti.

Naudotojams, susidūrusiems su tinklų ir informacijos saugumo problemomis, patariama nedelsiant kreiptis į savo interneto paslaugų teikėją, o jei šis atsisako spręsti problemą, informuoti apie tai CERT-LT. Naudotojas gali užpildyti specialią formą tinklalapyje www.cert.lt/pranesti.html.

**Apie CERT-LT**

CERT-LT – tai Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, kurio misija yra užtikrinti elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, koordinuoti veiksmus stabdant incidentų plitimą ir vykdyti incidentų prevenciją. Padaliniui nacionalinio CERT statusas suteiktas 2008 m. liepos 9 d. Lietuvos Respublikos Vyriausybei priėmus nutarimą patikėti nacionalinio CERT funkcijas Lietuvos Respublikos ryšių reguliavimo tarnybai (RRT).

CERT-LT koordinuoja ir įgyvendina IT sprendimus, susijusius su tinklų ir informacijos saugumu, atlieka prevencinę veiklą, teikdamas informaciją apie naujausias grėsmes kompiuterių naudotojams. Informacija skelbiama specialiame tinklalapyje www.esaugumas.lt, kuriame kompiuterių vartotojams taip pat pateikiamos rekomendacijos ir įspėjimai, kaip išvengti didesnio masto pavojų. Sprendžiant tarptautinius incidentus, CERT-LT bendradarbiauja su kitose valstybėse dirbančiais CERT padaliniais. CERT-LT yra pilnateisis „Trusted Introducer“ ir FIRST (angl. *Forum of Incident Response and Security Teams*) organizacijų narys.

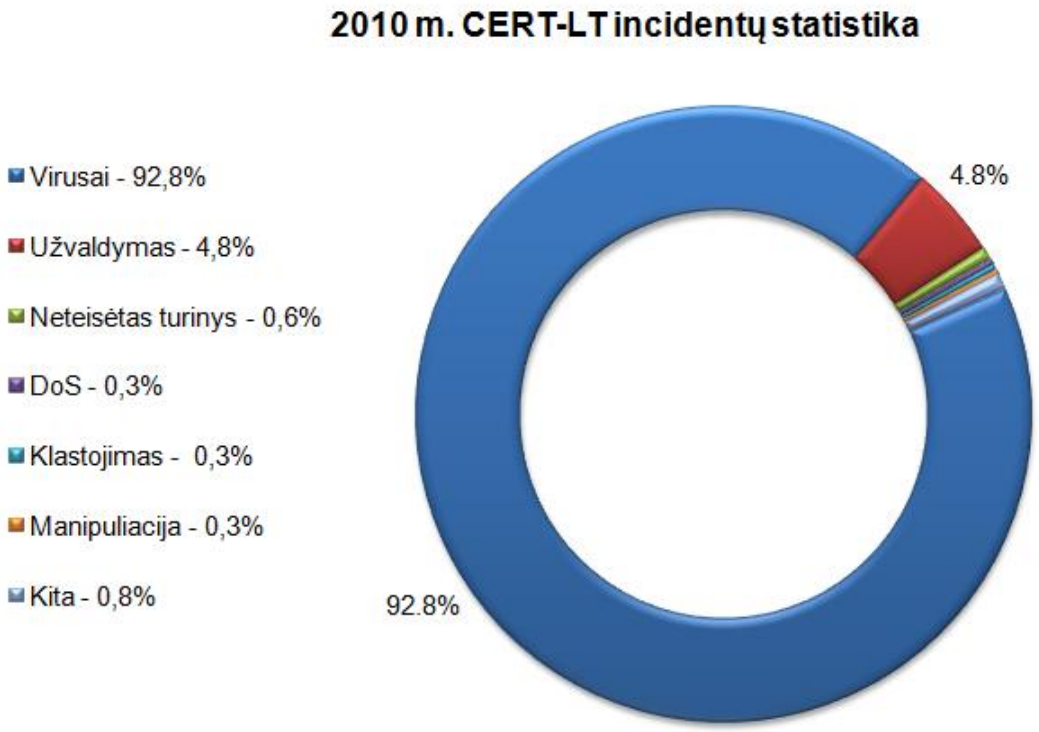
2010 m. CERT-LT dalyvavo pirmose Europos kibernetinėse pratybose „Kibernetinė Europa 2010“. Per šias pratybas ekspertai bandė atremti programišių mėginimus paralyžiuoti kelių ES valstybių narių svarbiausių paslaugų teikimo internetu svetainių darbą. ES masto elektroninio saugumo parengties pratybomis siekiama didinti interneto patikimumą ir saugumą.

**Tirti pranešimai apie incidentus pagal tipus:**

| Incidentų tipas (sutrumpinimas) | Incidentų tipo paaiškinimas | Incidentų skaičius 2010 m. | Incidentų Skaičius 2010 m. (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 pažeisti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę | **9273** | **92,8** |

| | | | |
|---|---|---|---|
| | naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims. | | |
| ***Spam*** | **Nepageidaujamas elektroninis paštas** (angl. *spam*) – 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 381 pranešimai apie pavienį nepageidaujamą elektroninį paštą) | **0** |
| ***DoS*** | **Elektroninės paslaugos trikdymo ataka** (angl. *DoS*) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar) informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas. | **33** | **0,3** |
| **Neteisėtas turinys** | **Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus. | **63** | **0,6** |
| **Užvaldymas** | **Neleidžiamasis naudojimasis informacinės sistemos ištekliais** (angl. *Web Site Defacement*) – neteisėtas informacinės sistemos išteklių naudojimas.<br>ir<br>**Neleidžiamasis prisijungimas** (angl. *System Compromise/Intrusion*) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo. | **477** | **4,8** |
| **Klastojimas** | **Elektroninių duomenų klastojimas** (angl. *Phishing*) – | **30** | **0,3** |

| | | | |
|---|---|---|---|
| | sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis. | | |
| **Manipuliacija** | **Manipuliacija elektroniniais duomenimis** (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas. | **29** | **0,3** |
| **Kiti** | | **84** | **0,8** |




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