# CERT-LT apibendrina 2012 metų veiklą

**Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2012 metų veiklos rezultatus. CERT-LT 2012 metais ištyrė 21 416 iš elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su 2011 metais (21 860 pranešimų), pranešimų skaičius sumažėjo 2 proc.**

Didžiausia problema, su kuria, CERT-LT duomenimis, 2012 metais susidūrė Lietuvos interneto naudotojai, buvo kenkėjiška programinė įranga – tai sudarė 54,9 proc. visų tirtų pranešimų. Iš jų daugiausia incidentų buvo susiję su kenkėjiška programine įranga, kuri veikdama pažeidžia kompiuterio valdymą ir įtraukia kompiuterį į „botnet“ tinklą. Taip pat kenkėjiškos programos aktyviai plito per pokalbių programą „Skype“ ir socialinius tinklus. Kenkėjiškos programos siuntinėjo žinutes „Skype“ ir „Facebook“ naudotojų adresatams, ir siūlė aplankyti kenkėjiškas svetaines, kuriose būdavo užkrečiama virusais.

2012 metais daugėjo incidentų, susijusių su informacinių sistemų užvaldymu. CERT-LT ištyrė 9 148 tokio pobūdžio incidentus – 8 proc. daugiau nei 2011 m. (8 507 atvejai). CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant „botnet“ tinklus, įterpiant kenkėjišką kodą į prastai apsaugotas internetines svetaines.

2012 metais daugėjo pranešimų apie klastojimo (angl. phishing) atvejus skaičius. CERT-LT ištyrė 185 pranešimus – 39 proc. daugiau nei 2011 m. (133 pranešimai). Didžiąją šių pranešimų dalį sudarė pranešimai apie finansinių įmonių, įskaitant ir Lietuvoje veikiančių finansinių įmonių ir bankų, suklastotas interneto svetaines. Piktavaliai, pasinaudodami nepageidaujamomis elektroninio pašto žinutėmis (angl. spam), ar kitomis apgaulės priemonėmis, siūlydavo aplankyti suklastotas interneto svetaines, kurios veikdavo dažniausiai ne Europos Sąjungos tarnybinėse stotyse, siekdami išgauti prisijungimo slaptažodžius ir (ar) kitus konfidencialius duomenis. Apie tai CERT-LT informuoja Lietuvos ar užsienio interneto paslaugos teikėjus, tarptautinius partnerius ir tarnybinės stoties administratorius, kurių priežiūroje yra skelbiamos tokios svetainės. Atsižvelgiant į tai, kurios valstybės tarnybinėse stotyse suteikiama priegloba tokio turinio svetainėms, dažniausiai grėsmę pavyksta pašalinti per kelias valandas.

2012 metais CERT-LT ištyrė 61 pranešimą apie elektronines paslaugos trikdymo atakas (DDoS). Nors, palyginti su 2011 m. (103 pranešimai), pranešimų skaičius sumažėjo 41 proc., tačiau šių atakų mastas ir technologinis sudėtingumas išaugo. CERT-LT tyrimų duomenimis, šios atakos buvo vykdomos automatizuotomis priemonėms, ypač dažnai pasitelkiant „botnet“ resursus.

2012 metais (panaši tendencija numatoma ir 2013-iesiems) viena iš didžiausių tinklų ir informacijos saugumo grėsmių pasaulyje ir Lietuvoje toliau išlieka „botnet“ tinklai, kuriais vykdoma nusikalstama veika, tokia kaip kenkėjiško kodo, nepageidaujamų elektroninio pašto laiškų platinimas, paslaugos trikdymo atakos ir kitos nusikalstamos veikos. CERT-LT tyrimo duomenimis, 2012 metais Lietuvoje kasdien buvo fiksuojama vidutiniškai 7000 aktyvių kompiuterių „zombių“.

CERT-LT registruoja ir skelbia informaciją apie „botnet“ tinkluose aptiktų kompiuterių aktyvumą interneto svetainėje https://www.cert.lt/botnet. Naudotojas, kilus įtarimui, kad jo kompiuteris gali būti įtrauktas į tokio 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.

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.

**Apie CERT-LT**

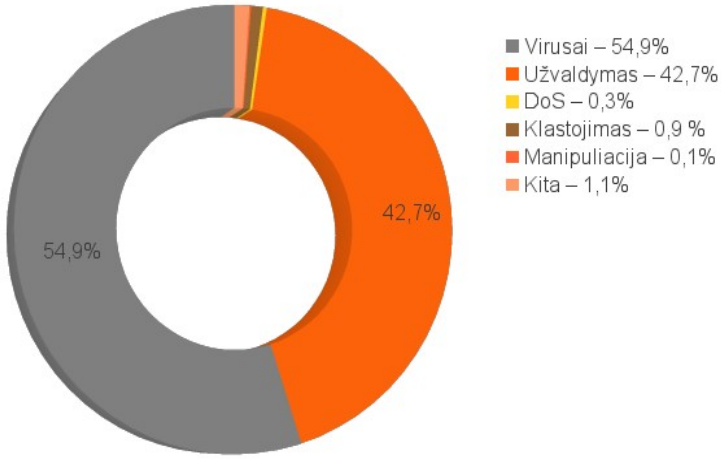
CERT-LT – tai Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, kurio misija yra užtikrinti elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, koordinuoti veiksmus stabdant incidentų plitimą ir vykdyti incidentų prevenciją. 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 specializuotuose tinklalapiuose www.cert.lt ir www.esaugumas.lt, kuriame kompiuterių naudotojams taip pat pateikiamos rekomendacijos ir įspėjimai, kaip išvengti didesnių pavojų. Sprendžiant tarptautinius incidentus, CERT-LT bendradarbiauja su kitose valstybėse dirbančiais CERT padaliniais. CERT-LT yra visateisis „Trusted Introducer“ ir FIRST (angl. Forum of Incident Response and Security Teams) organizacijų narys.

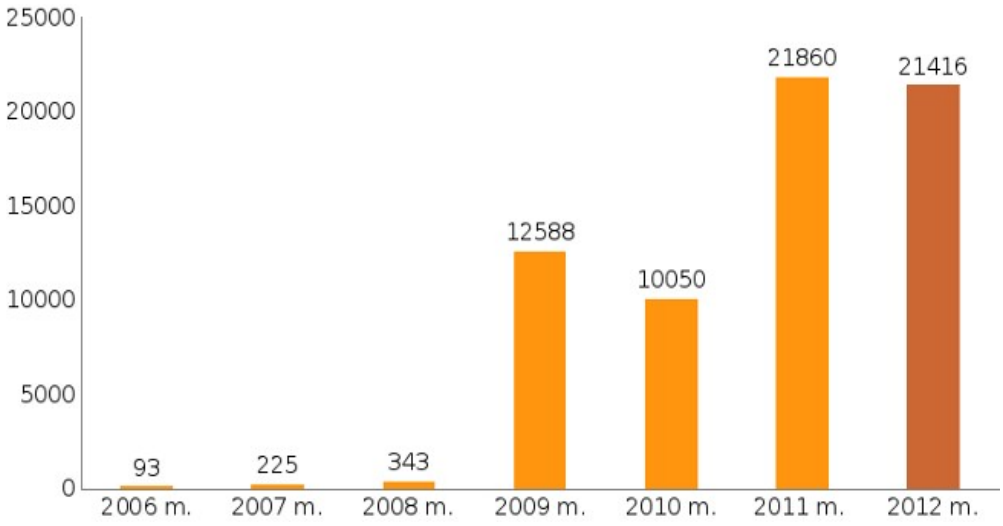
**1 lentelė. 2012 metais tirti pranešimai apie incidentus pagal tipus**

| Incidentų tipas | Incidentų skaičius (vnt.) | Procentinė visų incidentų dalis (proc.) |
|---|---|---|
| Virusas | 11 762 | 54,9 % |
| Užvaldymas | 9 148 | 42,7 % |
| Klastojimas | 185 | 0,9 % |
| Manipuliacija | 29 | 0,1 % |
| DoS | 61 | 0,3 % |
| Kiti | 231 | 1,1 % |

2012 m. CERT-LT incidentų statistika, proc.




2006–2012 m. CERT-LT incidentų statistika, vnt.




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