CERT-LT apibendrina 2011 metų veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2011 metų veiklos rezultatus. CERT-LT 2011 metais ištyrė 21 860 iš elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su 2010 metais (10 050 pranešimai), pranešimų padaugėjo daugiau nei du kartus. Tokį didelį ištirtų incidentų skaičių lėmė CERT-LT taikytos naujos aktyvios priemonės saugumo incidentams fiksuoti ir analizuoti bei pasirašyti nauji bendradarbiavimo susitarimai su tarptautiniais partneriais, atliekančiais tarptautinius incidentų tyrimus.

Didžiausia problema, su kuria, CERT-LT duomenimis, 2011 metais susidūrė Lietuvos interneto naudotojai, buvo kenkėjiška programinė įranga – ji sudarė 53,9 proc. visų tirtų pranešimų. Tarp jų daugiausia incidentų buvo susiję su kenkėjiška programine įranga, kuri veikdama pažeidžia kompiuterio valdymą ir įtraukia jį į *botnet* tinklą. 2011 metais Lietuvoje itin suaktyvėjo „Zeus“ atmainos kenkėjiška programinė įranga, kurią pasitelkus galima perimti interneto naudotojų prisijungimų duomenis prie įvairių tinklalapių, ir „DNSChanger“ kenkėjiška programinė įranga, kuri užkrėstame kompiuteryje pakeičia srities vardų struktūros (*angl.* DNS − *Domain Name System*) nustatymus ir nukreipia naudotojo duomenų srautą į kenkėjiškas sistemas − tokiu būdu gali būti atskleisti naudotojo asmeniniai duomenys arba pateikta pakeista tinklalapio informacija.

2011 metais itin padaugėjo incidentų, susijusių su informacinių sistemų užvaldymu. CERT-LT ištyrė 8 507 tokio pobūdžio incidentus – 18 kartų daugiau nei 2010 m. (477 atvejai). CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, tarp jų pasitelkiant *botnet* tinklus. CERT-LT koordinavo veiksmus su elektroninių ryšių paslaugų teikėjais bei informacinių sistemų savininkais dėl tokių incidentų šalinimo. CERT-LT ir toliau fiksuoja šių incidentų augimo tendencijas.

2011 metais daugėjo klastojimo (angl. *Phishing*) pranešimų skaičius. CERT-LT ištyrė 133 pranešimus – 4 kartus daugiau nei 2010 m. (30 pranešimai). Didžiąją šių pranešimų dalį sudarė pranešimai apie Lietuvoje veikiančių bankų suklastotas interneto svetaines. Piktavaliai, pasinaudodami nepageidaujamomis elektroninio pašto žinutėmis (angl. *Spam*),

kuriomis imituodavo banko žinutes, siūlydavo aplankyti suklastotas internetinės bankininkystės svetaines, siekdami išgauti prisijungimo slaptažodžius ir (ar) kitus konfidencialius duomenis. CERT-LT, bendradarbiaudamas su valstybių, dažniausiai ne Europos Sąjungos, kuriose šie tinklalapiai buvo skelbiami, atsakingomis institucijomis ir tų šalių CERT tarnybomis, ėmėsi veiksmų šalinant iš interneto šias falsifikuotas internetinės bankininkystės svetaines. Apie šiuos atvejus CERT-LT viešai įspėjo interneto naudotojus ir pateikė rekomendacijas www.rrt.lt bei www.esaugumas.lt svetainėse.

Taip pat praėjusių metų II ketvirtyje padaugėjo nepageidaujamų el. pašto pranešimų (*Spam*) – jie dešimtis kartų viršijo įprastus kiekius Lietuvoje, palyginti su praeitais šių metų ketvirčiais. CERT-LT užfiksavo, kad suaktyvėjusio SPAM laiškai pasižymėjo kirilicos simboliais žinutės tekste ir atitinkama koduote antraštėse. Atsižvelgdamas į tai, CERT-LT www.esaugumas.lt svetainėje pateikė rekomendacijas el. pašto tarnybinių stočių administratoriams.

2011 metais (panaši tendencija numatoma ir 2012-iesiems) viena iš didžiausių tinklų ir informacijos saugumo grėsmių pasaulyje bei Lietuvoje išlieka *botnet* tinklai, kuriuos pasitelkiant vykdoma nusikalstama veikla, tokia kaip kenkėjiško kodo, nepageidaujamų elektroninių pašto laiškų platinimas, paslaugos trikdymo atakos ir kitos nusikalstamos veikos. CERT-LT tyrimo duomenimis, 2011 metais Lietuvoje kasdien buvo fiksuojama vidutiniškai 8000 aktyvių kompiuterių „zombių“. CERT-LT registruoja ir skelbia informaciją apie botnet tinkluose aptiktų kompiuterių aktyvumą. Naudotojas, kilus įtarimui, kad jo kompiuteris gali būti įtrauktas į *botnet* 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. CERT-LT, bendradarbiaudamas 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 ir ateityje apsaugoti kompiuterį.

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.html.

Apie CERT-LT

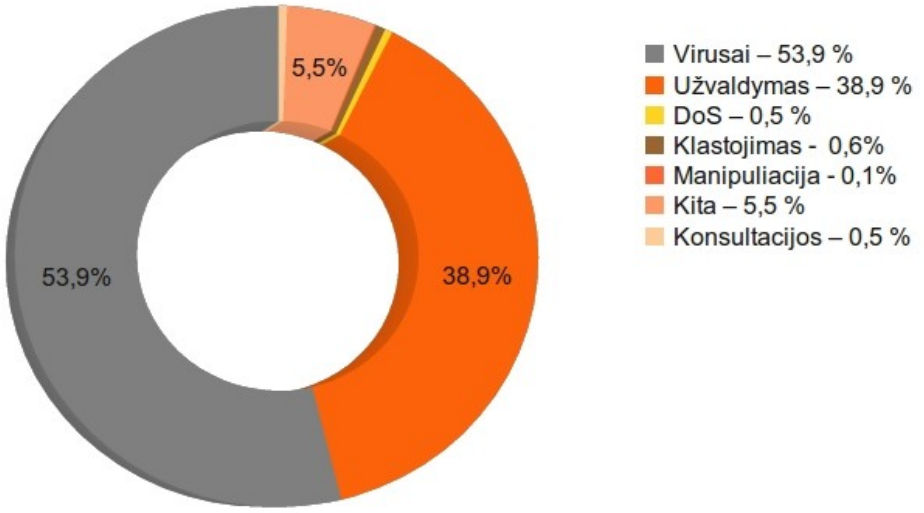
CERT-LT – tai Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, kurio misija yra užtikrinti elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, koordinuoti veiksmus stabdant incidentų plitimą ir vykdyti incidentų prevenciją. 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.

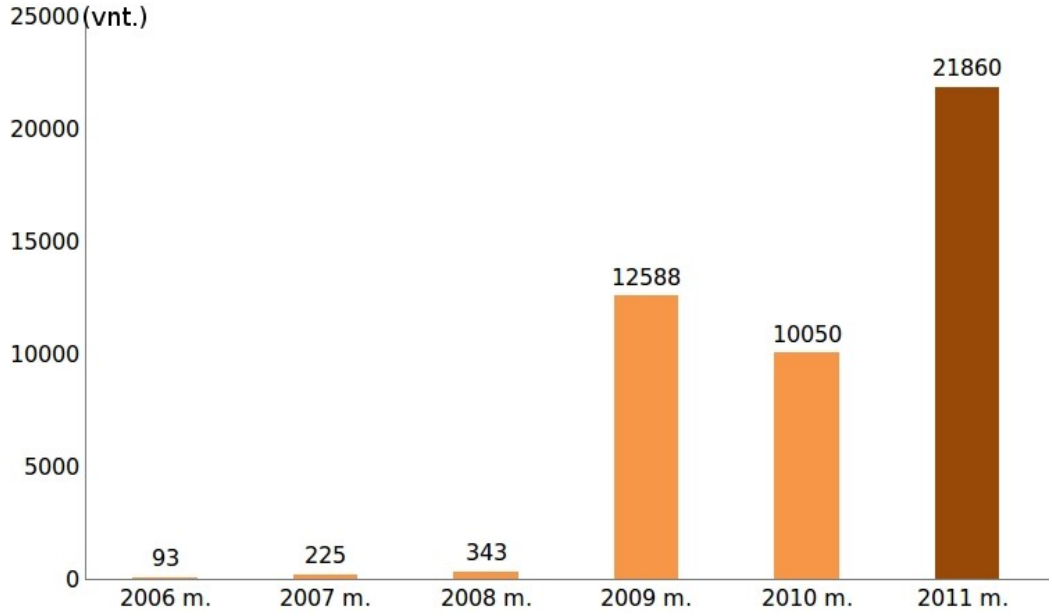
Tirti pranešimai apie incidentus pagal tipus:

Incidentų tipas	**Incidentų skaičius 2011 m. (vnt.)**	**Incidentų skaičius 2011 m. (proc.)**
Virusas	11 777	53,9%
Užvaldymas	8 507	38,9%
Klastojimas	133	0,6%
Manipuliacija	23	0,1%
DoS	103	0,5%
Konsultacijos	120	0,5%
Kiti	1 197	5,5%

2011 m. CERT-LT incidentų statistika



2006–2011 m. CERT-LT incidentų statistika



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