

CERT-LT apibendrina IV ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys ([CERT-LT](#)) apibendrina 2011 m. IV ketvirčio veiklos rezultatus. [CERT-LT](#) 2011 m. IV ketvirtį ištyrė 5 815 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 2011 m. III ketvirčiu (7 781 pranešimu), pranešimų sumažėjo 25 procentais. CERT-LT ištyrė visus gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti jų padarinius ar sustabdyti jų plitimą.

Daugiausia ištirta pranešimų apie kenkėjišką programinę įrangą ir kompiuterių bei informacinių sistemų užvaldymo incidentus. Per šį laikotarpį CERT-LT ištyrė 3 324 pranešimus apie kenkėjišką programinę įrangą – 10 proc. mažiau nei 2011 m. III ketvirtį, ir 2 363 pranešimus apie kompiuterių užvaldymo incidentus – 39 proc. mažiau nei 2011 m. III ketvirtį. CERT-LT atliktų tyrimų duomenys parodė, kad tarp kenkėjiškos programinės įrangos daugiausia incidentų buvo susijusių su kenkėjiška programine įranga, kuri veiksma pažeidžia kompiuterio valdymą bei įtraukia jį į *botnet* tinklą, ir kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant *botnet* tinklus. CERT-LT ir toliau fiksuoja šių incidentų augimo tendencijas.

Ketvirtąjį metų ketvirtį Lietuvoje buvo padidėjęs „DNSChanger“ kenkėjiškos programinės įrangos aktyvumas – jis šimtus kartų viršijo įprastinius kiekius Lietuvoje. Užkrėstame kompiuteryje „DNSChanger“ pakeičia srities vardų struktūros (*angl. Domain Name System, DNS*) nustatymus ir nukreipia naudotojo duomenų srautą – tokiu būdu gali būti atskleisti naudotojo asmeniniai duomenys (pavyzdžiui, prisijungimo prie elektroninės bankininkystės) arba pateikta pakeista tinklalapio informacija. Apie minėtą atvejį CERT-LT lapkričio mėnesį įspėjo interneto naudotojus ir pateikė rekomendacijas.

Taip pat gauti ir tirti pranešimai apie šiuos incidentus: dėl elektroninės paslaugos trikdymo atakų (*angl. Denial of Service, DoS*) – 12 (2011 m. III ketvirtį – 30); dėl manipuliacijos – 4 (2011 m. III ketvirtį – 9); dėl klastojimo – 38 (2011 m. III ketvirtį – 51).

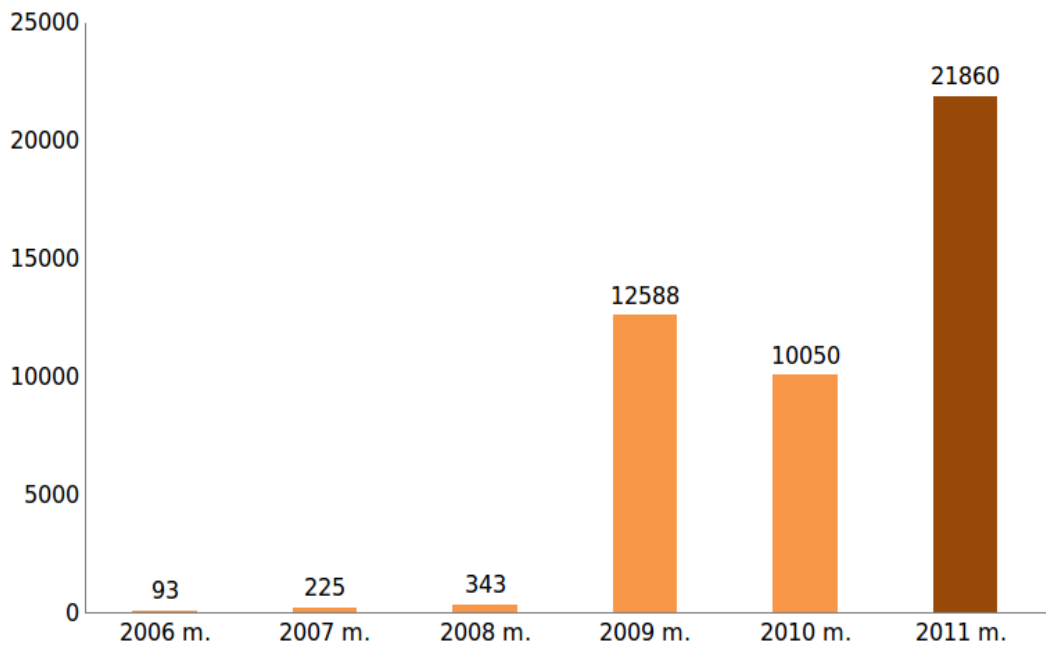
CERT-LT registruoja ir skelbia informaciją apie [botnet tinkluose aptiktų kompiuterių aktyvumą](#). Naudotojas, kilus įtarimui, kad jo kompiuteris gali būti įtrauktas į *botnet* tinklo veiklą, gali pasitikrinti CERT-LT tinklalapyje <https://www.cert.lt/tikrinti>, ar kompiuterio interneto protokolo (IP) adresas nėra užfiksuotas CERT-LT duomenų bazėje kaip dalyvaujantis kenkėjiškoje veikloje. CERT-LT, 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.

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.

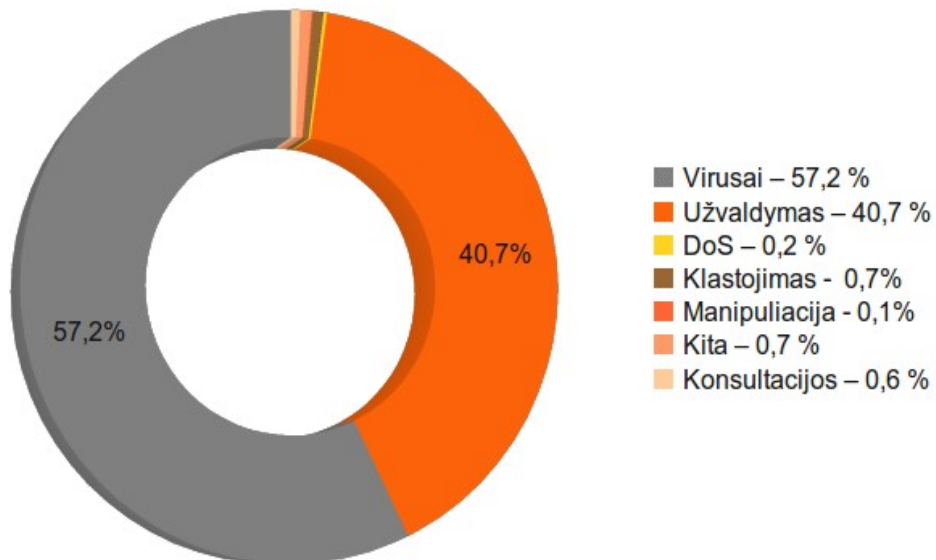
Tirti pranešimai apie incidentus pagal tipus:

Incidentų tipas	Incidentų skaičius 2011 m. IV ketv.	Incidentų skaičius 2011 m. IV ketv. (proc.)
Virusas	3 324	57,2
Užvaldymas	2 363	40,7
Klastojimas	38	0,7
Manipuliacija	4	0,1
DoS	12	0,2
Konsultacijos	32	0,6
Kiti	42	0,7

2006–2011 m. CERT-LT incidentų statistika



2011 m. IV ketvirčio CERT-LT incidentų statistika



Visas CERT-LT incidentų statistikos ataskaitas galite rasti internetinėje svetainėje

<https://www.cert.lt/statistika.html>