Per 2014 m. I ketvirtį CERT-LT ištyrė 7 375 incidentus elektroninėje erdvėje

Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2014 m. I ketvirčio veiklos rezultatus. CERT-LT 2014 m. I ketvirtį ištyrė 7 375 incidentus pagal 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 tuo pačiu 2013 m. laikotarpiu (5 753 incidentai), incidentų padaugėjo 28 procentais. Nuo šių metų pradžios CERT-LT atliktų tyrimų metu buvo užregistruoti 1673 incidentai, susiję pavojingomis įrenginių saugumo spragomis, kurios gali būti išnaudotos kenkimo veiklai internete.

Daugiausia ištirta incidentų, susijusių su kompiuterių ir informacinių sistemų užvaldymu ir kenkimo programine įranga. Per šį laikotarpį CERT-LT ištyrė 2 820 kenkimo programinės įrangos panaudojimo atvejų – 5 proc. daugiau nei 2013 m. IV ketvirtį, ir 1 836 kompiuterių užvaldymo atvejus – 46 proc. mažiau nei 2013 m. IV ketvirtį. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, jie susiję su prastai apsaugota įranga internete, o tarp kenkimo programinės įrangos incidentų daugiausia buvo susijusių su botnetų (kompiuterių robotų tinklų) veikla.

Šį ketvirti aktyviai plito kenkimo programa – kirminas „The Moon“. Šis kirminas, išnaudodamas HNAP (angl. *Home Network Administration Protocol*) protokolo saugumo spragą, pažeidžiamame maršruto parinktuve gauna valdymo galimybes, įkelia į jį vykdomąsias bylas, atidaro įvairius įrenginio prievadus, leidžia piktavaliams įrenginiu manipuliuoti nuotoliniu būdu (*angl. Backdoor*), priima komandas iš piktavalių. Užvaldytas įrenginys vykdo kitų tinklo įrenginių skenavimą ieškodamas daugiau saugumo spragą turinčių įrenginių, kuriuos būtų galima užvaldyti, ir gali būti panaudotas asmens duomenims iš duomenų srauto perimti ir kitoms atakoms prieš taikinius internete. CERT-LT apie Lietuvos tinkle pastebėtus įrenginius, galinčius turėti šią spragą, informavo interneto paslaugų teikėjus ir pateikė rekomendacijas www.cert.lt svetainėje.

Taip pat šį ketvirtį buvo fiksuotas 30 proc. padidėjęs (palyginti su ankstesniu ketvirčiu) *ZeroAcces* ir *Zeus* (dar kitaip vadinamo *Zbot*) botnetų aktyvumas Lietuvos tinkluose.

Šiais metais CERT-LT pradėjo nagrinėti Lietuvos interneto tinkle veikiančių įrenginių spragas, kurios gali būti naudojamos paslaugos trikdymo atakoms ar kitai kenkimo veiklai vykdyti. Per pirmąjį ketvirtį nustatyti 1673 pavojingų spragų egzistavimo atvejai.

Pirmąjį ketvirtį padidėjo pranešimų skaičius (43 pranešimai) apie paskirstytosios paslaugos trikdymo atakas (DDoS). Palyginti su 2013 m. IV ketvirčiu (26 pranešimai), pranešimų skaičius padidėjo 65 proc. CERT-LT tyrimų duomenimis, šios atakos buvo vykdomos automatizuotomis priemonėms, pasitelkiant botnetų resursus ir pažeidžiamus įrenginius internete. Siekiant nutraukti vykdomas atakas, CERT-LT teikė rekomendacijas atakuojamų tarnybinių stočių savininkams ar svetainių prieglobos paslaugas teikiančioms įmonėms, kaip stabdyti šias atakas, koordinavo veiksmus su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

2014 m. I ketvirtį tirti 166 incidentai, susiję su užvaldytais, kenkimo programinį kodą platinančiais ar suklastotais tinklalapiais. Dažniausiai tai buvo atvejai, susiję su prastai apsaugota tinklalapio turinio valdymo sistema.

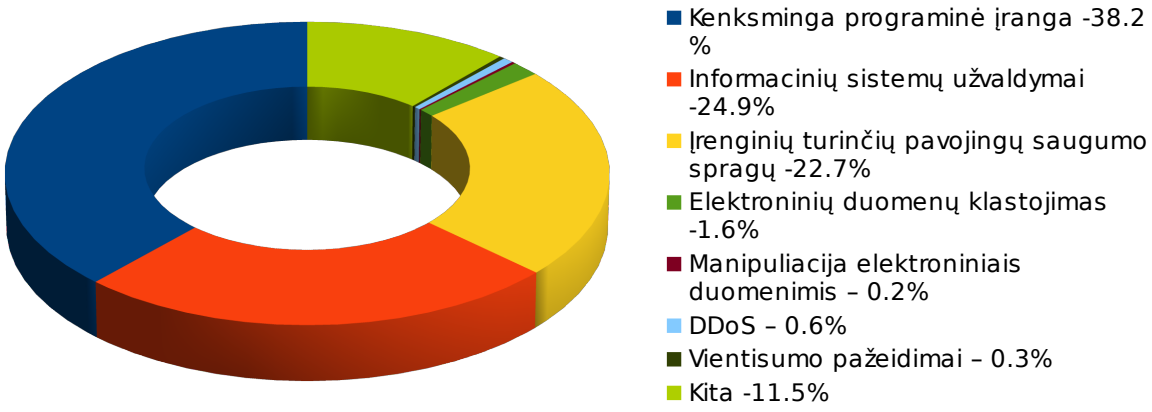
Kiti gauti ir tirti pranešimai: apie manipuliaciją elektroniniais duomenimis – 13 (2013 m. IV ketvirtį – 21), vientisumo pažeidimus – 19 ir elektroninių duomenų klastojimą – 121 (2013 m. IV ketvirtį – 175).

Šių metų pirmąjį ketvirtį CERT-LT atliktų tyrimų metu Lietuvoje buvo užregistruoti 1673 kompiuterių naudotojų įrenginiai, skirti prisijungti prie interneto ir turintys pavojingų saugumo spragų, kurios gali būti išnaudotos kenkimo veiklai internete. Apie tokius įrenginius CERT-LT informavo juos prižiūrinčius Lietuvos interneto paslaugos teikėjus. Atkreiptinas dėmesys, kad šie incidentai yra ypač pavojingi, nes, išnaudodami saugumo spragas, piktavaliai gali užvaldyti įrenginį ir kontroliuoti jį nuotoliniu būdu. Toks įrenginys naudojamas byloms persiųsti, paskirstytosioms paslaugų trikdymo atakoms vykdyti, tinklu siunčiamai informacijai perimti ir kitiems veiksmams atlikti.

Lentelė. 2014 m. I ketv. tirti pranešimai apie incidentus pagal tipus

Incidentų tipas	**Incidentų skaičius 2014 m. I ketv. (vnt.)**	**Procentinė visų incidentų dalis (proc.)**
Virusas	2 820	38,2
Užvaldymas	1 836	24,9

Spragos	1 673	22,7
Klastojimas	121	1,6
Manipuliacija	13	0,2
DDoS	43	0,6
Vientisumas	19	0,3
Kiti	850	14,9



1 pav. 2014 m. I ketvirtį CERT-LT užfiksuotų incidentų statistika, proc.

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

Cituojant pranešimus, šaltinį prašome nurodyti