

CERT-LT apibendrina 2013 m. II ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2013 m. II ketvirčio veiklos rezultatus. CERT-LT 2013 m. II ketvirtį ištyrė 6 115 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 2013 m. I ketvirčiu (5 739 pranešimų), pranešimų padaugėjo 7 procentais. II ketvirtį padaugėjo pranešimų apie elektronines paslaugos trikdymo atakas (DDoS).

Daugiausia ištirta incidentų, susijusių su kompiuterių ir informacinių sistemų užvaldymo atvejais ir kenkėjiška programine įranga. Per šį laikotarpį CERT-LT ištyrė 2 840 kenkėjiškos programinės įrangos panaudojimo atvejų – 4 proc. daugiau nei 2013 m. I ketvirtį, ir 2 404 kompiuterių užvaldymo atvejus – 13 proc. mažiau nei 2013 m. I ketvirtį. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis įterpiant kenkėjišką kodą į prastai apsaugotas interneto svetaines, o tarp kenkėjiškos programinės įrangos incidentų daugiausia buvo susijusių su [botnet](#) (kompiuterių robotų) tinklų veikla.

Antrąjį ketvirtį ištirti du kenkėjiškos programinės įrangos incidentai išmaniuosiuose telefonuose. Abiem atvejais kenkėjiška programa pažeistame telefone įrašytiems adresatams išsiuntinėdavo SMS žinutes su nuorodomis, kurias aktyvinus buvo užkrečiamas įrenginys. Taip buvo siekiama užvaldyti telefoną ir išsekvoti pažeisto įrenginio abonento sąskaitą. CERT-LT, bendradarbiaudama su užsienio partneriais, uždarė kenkėjišką programinį kodą platinančias svetaines, todėl grėsmė užvaldyti naujus įrenginius buvo sumažinta.

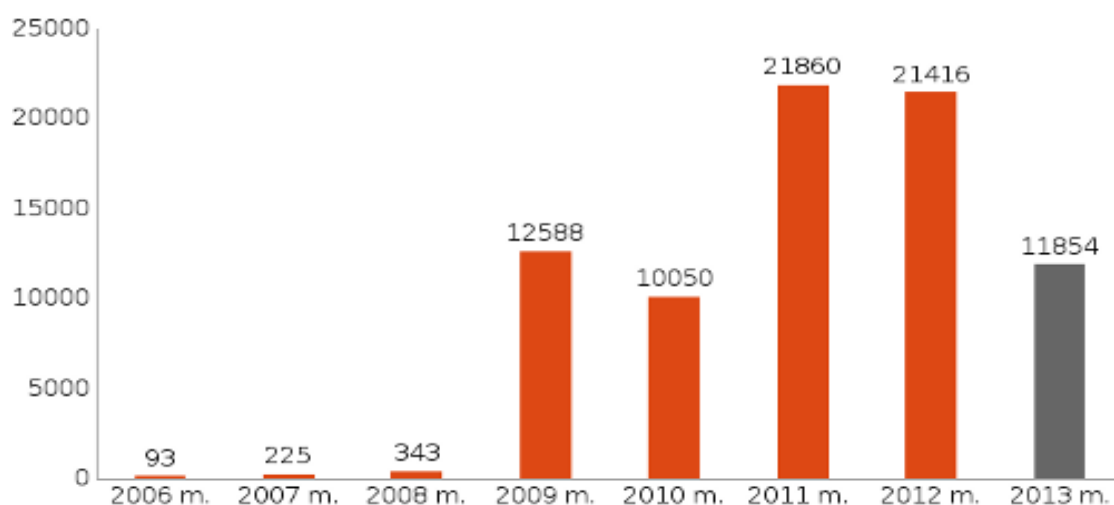
Taip pat padidėjo pranešimų skaičius (36 pranešimai) apie elektronines paslaugos trikdymo atakas (DDoS). Palyginti su 2013 m. I ketvirčiu (28 pranešimai), pranešimų skaičius padidėjo 29 proc. CERT-LT tyrimų duomenimis, šios atakos buvo vykdomos automatizuotomis priemonėmis, pasitelkiant botnet resursus. Siekiant nutraukti vykdomas atakas, CERT-LT teikė rekomendacijas tinklalapių savininkams ar tinklalapių prieglobos paslaugas teikiančioms įmonėms kaip stabdyti šias atakas, koordinavo veiksmus su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

Kiti gauti ir tirti pranešimai apie manipuliaciją elektroniniais duomenimis – 20 (2013 m. I ketvirtį – 12), ir elektroninių duomenų klastojimą – 147 (2013 m. I ketvirtį – 171).

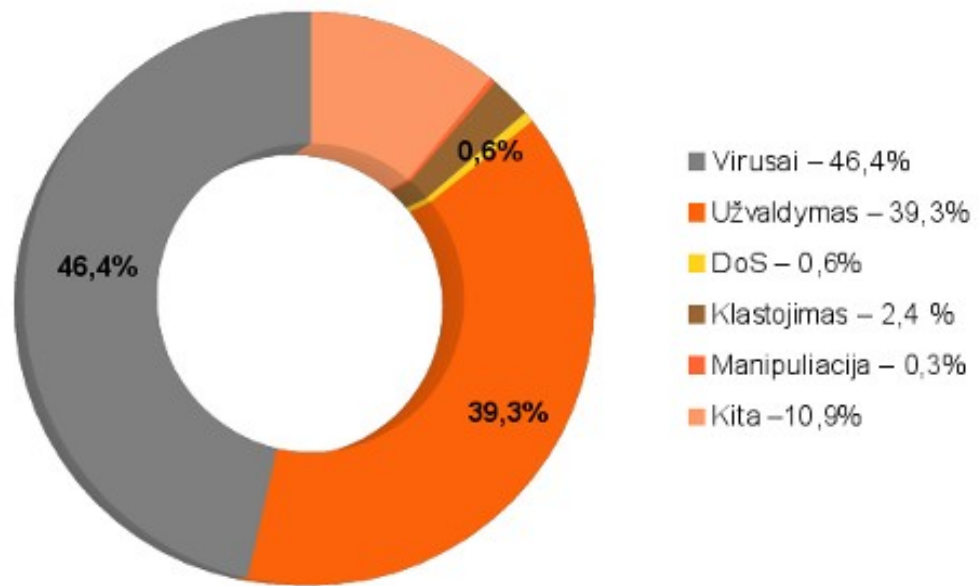
Taip pat II-ojo ketvirčio pabaigoje CERT-LT organizavo ir vykdė tarpinstitucines kibernetines pratybas „X1306“. Šiose pratybose buvo siekiama patikrinti tarpinstitucinio bendradarbiavimo efektyvumą, tarpusavio komunikacijos spartą, galimybes kritinėse situacijose rasti atsakingų institucijų atstovų kontaktus. Buvo tikrinamas pasirengimas naudoti lengvai prieinamas šifravimo priemones duomenims perduoti viešaisiais tinklais, įgūdžiai operatyviai keisti informacija galimų kibernetinių incidentų metu. Pratybose dalyvo 10 valstybinių institucijų ir 4 saugumo incidentų tyrimo CERT grupės.

Lentelė. 2013 metais II ketv. tirti pranešimai apie incidentus pagal tipus

Incidentų tipas	Incidentų skaičius 2013 m. II ketv. (vnt.)	Procentinė visų incidentų dalis (proc.)
Virusas	2 840	46,4
Užvaldymas	2 404	39,3
Klastojimas	147	2,4
Manipuliacija	20	0,3
DDoS	36	0,6
Kiti	668	10,9



1 pav. 2006–2013 m. CERT-LT užfiksuotų incidentų statistika, vnt.



2 pav. 2013 m. II ketvirtį CERT-LT užfiksuotų incidentų statistika, proc.

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