CERT-LT apibendrina 2013 m. III ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2013 m. III ketvirčio veiklos rezultatus. CERT-LT 2013 m. III ketvirtį ištyrė 5 907 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. II ketvirčiu (6115 pranešimų), pranešimų buvo gauta 3 procentais mažiau.

Daugiausia ištirta incidentų, susijusių su kenkėjiškos programinės įrangos naudojimu ir kompiuterių bei informacinių sistemų užvaldymu. Per šį laikotarpį CERT-LT ištyrė 2 889 kenkėjiškos programinės įrangos panaudojimo atvejus – 2 proc. daugiau nei 2013 m. II ketvirtį, ir 2 341 kompiuterių užvaldymo atvejį – 3 proc. mažiau nei 2013 m. II 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 botnetų veikla.

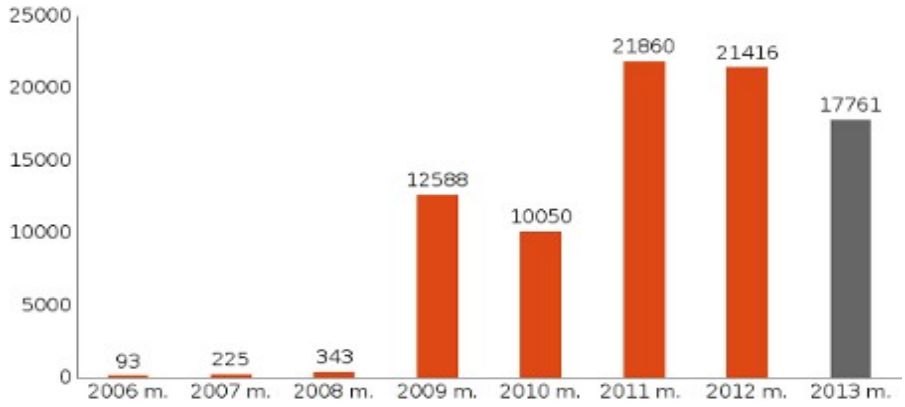
Taip pat III ketvirtį CERT-LT, bendradarbiaudama su Vokietijos nacionaliniu CERT (CERT-Bund), aptiko ir neutralizavo Lietuvoje veikiančią botneto valdymo tarnybinę stotį, kuri buvo naudojama užvaldytiems kompiuteriams (botams) kontroliuoti ir valdyti. Tyrimo metu buvo nustatyta, kad nuo 2013 m. gegužės mėn. šis botneto valdymo centras galėjo valdyti 5400 kompiuterių visame pasaulyje. HTTP protokolo pagrindu veikiantis valdiklis uždarymo metu kontroliavo daugiau kaip 600 aktyvių užvaldytų įrenginių, tarp jų – 75 iš Lietuvos. CERT-LT informavo Lietuvos ir užsienio interneto paslaugos teikėjus, tarptautinius partnerius, kurių priežiūroje yra užvaldytų kompiuterinių įrenginių IP adresai.

Kiti gauti ir tirti pranešimai buvo susiję su elektroninių paslaugų trikdymo atakomis (DoS) – 40 (2013 m. II ketvirtį – 36), manipuliacija elektroniniais duomenimis – 16 (2013 m. II ketvirtį – 20), ir elektroninių duomenų klastojimu – 65 (2013 m. II ketvirtį – 147).

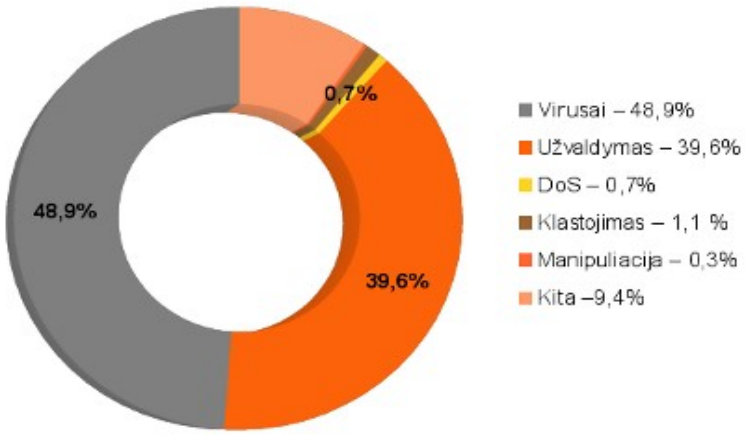
Lentelė. 2013 metų III ketvirtį tirti pranešimai apie incidentus pagal tipus.

Incidentų tipas	Incidentų skaičius 2013 m. III ketv. (vnt.)	Procentinė visų incidentų dalis (proc.)
Virusas	2 889	48,9
Užvaldymas	2 341	39,6
Klastojimas	65	1,1
Manipuliacija	16	0,3
DDoS	40	0,7
Kiti	556	9,4

1 pav. 2006–2012 m. ir 2013 m. III ketv. CERT-LT užfiksuotų incidentų statistika, vnt.



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



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