2013 metais CERT-LT ištyrė 25 337 incidentus elektroninėje erdvėje

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2013 metų veiklos rezultatus. CERT-LT 2013 metais ištyrė 25 337 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 2012 metais (21 416 pranešimų), pranešimų buvo gauta 18 procentų daugiau.

Didžiausia problema, su kuria, CERT-LT duomenimis, 2013 metais susidūrė Lietuvos interneto naudotojai, buvo kenkimo programinė įranga ir informacinių sistemų užvaldymai. Per šį laikotarpį CERT-LT ištyrė 11 125 kenkimo programinės įrangos panaudojimo atvejus – tai sudarė 43,9 proc. visų tirtų incidentų. Dažniausiai kenkimo programinė įranga buvo naudojama kompiuterio valdymui pažeisti, siekiant jį įtraukti į botnetų tinklą. Taip pat 2013 m. kenkimo programos aktyviai plito mobiliuosiuose įrenginiuose (išmaniuosiuose telefonuose, planšetiniuose kompiuteriuose ir pan).

2013 metais ir toliau daugėjo incidentų, susijusių su informacinių sistemų užvaldymu. CERT-LT ištyrė 10 924 tokio pobūdžio incidentus – 19 proc. daugiau nei 2012 m. (9 148 atvejai), ir tai sudarė 43,1 proc. visų tirtų incidentų. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant botnetų tinklus, įterpiant kenkimo kodą į prastai apsaugotas interneto svetaines. CERT-LT ir toliau fiksuoja šių incidentų skaičiaus augimo tendencijas.

2013 metais daugėjo ir klastojimo (*angl*. phishing) incidentų skaičius. CERT-LT ištyrė 558 pranešimus – 3 kartus daugiau nei 2012 m. (185 pranešimai). Didžiąją šių pranešimų dalį sudarė pranešimai apie suklastotas finansinių atsiskaitymų paslaugų ir bankų interneto svetaines, kurios veikdavo dažniausiai ne Europos Sąjungos tarnybinėse stotyse. Pasinaudodami nepageidaujamomis elektroninio pašto žinutėmis (*angl*. spam) ar kitomis apgaulės priemonėmis, piktavaliai siūlydavo aplankyti suklastotas interneto svetaines siekdami išgauti prisijungimo slaptažodžius ir (ar) kitus konfidencialius duomenis. Apie tai CERT-LT informuoja Lietuvos ar užsienio interneto paslaugos teikėjus, tarptautinius partnerius ir tarnybinės stoties, iš kurios veikia tokios svetainės, administratorius.

2013 metais CERT-LT ištyrė 130 pranešimų apie elektronines paslaugos trikdymo atakas (*angl*. denial of service, DoS). Palyginti su 2012 m. (61 pranešimas), pranešimų

skaičius padidėjo daugiau nei 2 kartus. Šios atakos buvo vykdomos automatizuotomis priemonėms, pasitelkiant botnetų resursus. Tarp tokių incidentų buvo fiksuotos daugiau kaip 6 Gb/s srauto atakos prieš taikinius Lietuvoje. Siekiant nutraukti vykdomas atakas, CERT-LT teikė rekomendacijas svetainių savininkams ar svetainių prieglobos paslaugas teikiančioms įmonėms, kaip stabdyti šias atakas, koordinavo veiksmus su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

2013 metais (panaši tendencija numatoma ir 2014-iesiems) viena iš didžiausių tinklų ir informacijos saugumo grėsmių pasaulyje ir Lietuvoje toliau išlieka botnetų tinklai, kuriais vykdoma nusikalstama veika – kenkimo kodo, nepageidaujamų elektroninio pašto laiškų platinimas, paslaugos trikdymo atakos ir kitos nusikalstamos veikos. CERT-LT tyrimo duomenimis, 2013 metais Lietuvoje kasdien buvo fiksuojama vidutiniškai 7000 aktyvių kompiuterių „zombių“. CERT-LT registruoja ir skelbia informaciją apie botų tinkluose aptiktų kompiuterių aktyvumą interneto svetainėje https://www.cert.lt/botnet.

CERT-LT, bendradarbiaudama su užsienio partneriais, 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.

Taip pat 2013 m. II 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 keistis informacija galimų kibernetinių incidentų metu. Pratybose dalyvavo 10 valstybinių institucijų ir 4 saugumo incidentų tyrimo CERT grupės.

Atsižvelgdamas į vis didėjantį incidentų, susijusių su naudotojų tinklo įrenginių saugumo spragomis, kurios leidžia užvaldyti įrenginius ir išnaudoti juos asmens duomenų vagystėms, paskirstytoms paslaugos trikdymo atakoms (*angl*. DDoS) ir kitoms kenkimo veikoms internete, CERT-LT savo svetainėje sukūrė papildomus įrankius interneto naudotojams. Tinklalapyje https://www.cert.lt/irankiai galima patikrinti, ar tinklo įrenginiai, per kuriuos jungiamasi į internetą, nenaudoja pažeidžiamo UPnP 1.0 protokolo ir ar

maršrutų parinktuve nėra palikta *Open resolver* tipo saugumo spragų. Taip pat galima pasitikrinti, ar kompiuteris nėra įtrauktas į botneto veiklą ir ar kompiuterio interneto protokolo (IP) adresas nėra užfiksuotas CERT-LT duomenų bazėje kaip dalyvaujantis kenkimo veikloje.

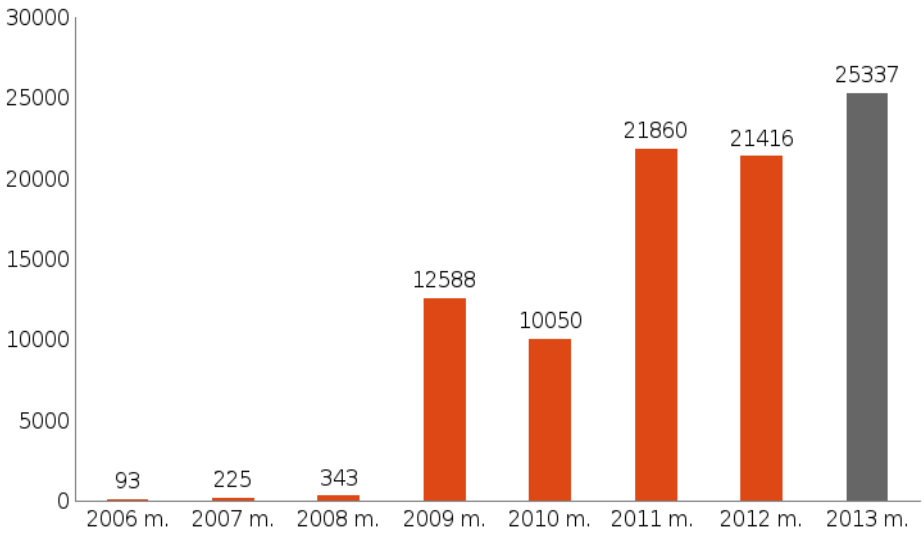
Naudotojams, susidūrusiems su tinklų ir informacijos saugumo problemomis, patariama nedelsiant kreiptis į savo interneto paslaugų teikėją, o jei šis problemų išspręsti negali, informuoti apie tai CERT-LT užpildant specialią formą tinklalapyje www.cert.lt/pranesti.

Taip pat nuo 2013 metų pabaigos Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT-LT svetainę www.cert.lt galima pasiekti ir naudojantis IPv6 protokolu.

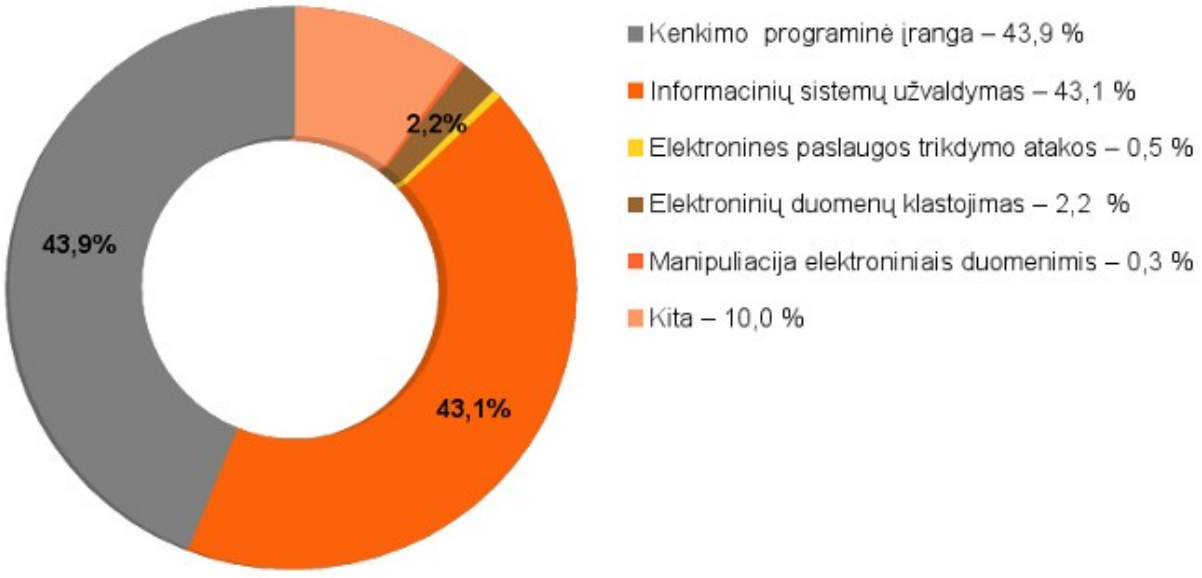
Lentelė. 2013 metais tirti pranešimai apie incidentus pagal tipus

Incidentų tipas	Incidentų skaičius 2013 m. (vnt.)	Procentinė visų incidentų dalis (proc.)
Kenkimo programinė įranga	11 125	43,9
Informacinių sistemų užvaldymas	10 924	43,1
Elektroninių duomenų klastojimas	558	2,2
Manipuliacija elektroniniais duomenimis	69	0,3
Elektroninės paslaugos trikdymo atakos	130	0,5
Kiti	2 531	10,0

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



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



Apie CERT-LT

CERT-LT – 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 specializuotose svetainėse www.cert.lt ir www.esaugumas.lt, kuriose kompiuterių naudotojams taip pat pateikiamos rekomendacijos ir įspėjimai, kaip išvengti didesnių pavojų. Sprendžiant tarptautinius incidentus, CERT-LT bendradarbiauja su kitose valstybėse dirbančiais CERT padaliniais. CERT-LT yra visateisis „Trusted Introducer“ ir FIRST (angl. Forum of Incident Response and Security Teams) organizacijų narys.

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