LIETUVOS RESPUBLIKOS
RYŠIŲ REGULIAVIMO TARNYBOS
TINKLŲ IR INFORMACIJOS SAUGUMO DEPARTAMENTO
SAUGUMO INCIDENTŲ TYRIMO SKYRIUS (CERT-LT)

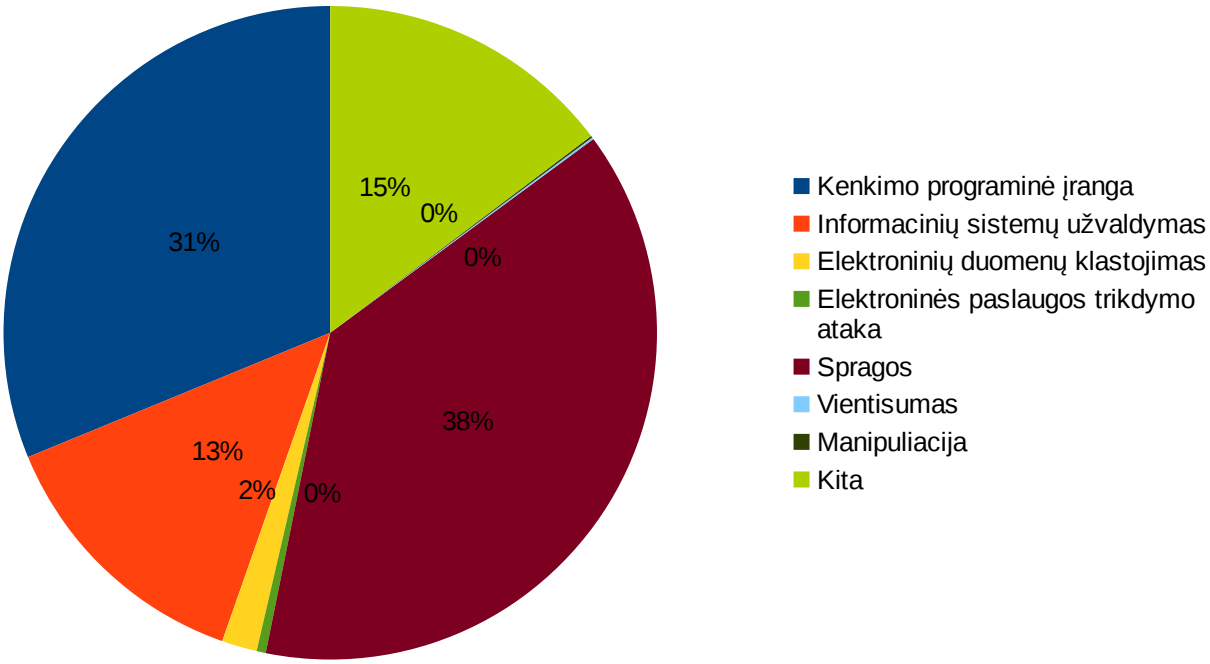
LIETUVOS RESPUBLIKOS NACIONALINIO ELEKTRONINIŲ RYŠIŲ TINKLŲ IR INFORMACIJOS SAUGUMO INCIDENTŲ TYRIMO PADALINIO 2014 METŲ VEIKLOS ATASKAITA

2015-04-02 Nr. LD-665
Vilnius

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2014 metų veiklos rezultatus. 2014 metais CERT-LT ištyrė 36 136 incidentus pagal pranešimus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2013 metais (25 337 pranešimai), pranešimų buvo gauta 43 proc. daugiau. 1-oje lentelėje ir 1-oje diagramoje pateikiamos nagrinėtų pranešimų pagal tipus suvestinės.

1 lentelė. CERT-LT 2014 m. nagrinėti pranešimai pagal jų tipus

Pranešimų pobūdis	**2014 metų laikotarpis**				
	I ketv.	**II ketv.**	**III ketv.**	**IV ketv.**	**iš viso**
Apie kenkimo programinę įrangą	2 820	2 412	2 807	3 237	11 276
Apie informacinių sistemų užvaldymą	1836	526	1 122	1 369	4 853
Apie elektroninės paslaugos trikdymo atakas	43	35	45	42	165
Apie elektroninių duomenų klastojimą	121	81	220	208	630
Apie vientisumo pažeidimus	19	11	5	0	35
Apie įrenginių saugumo spragas	1 673	3 310	3 647	5 197	13 827
Apie manipuliaciją elektroniniais duomenimis	13	5	8	6	32
Kita	850	993	1 712	1 763	5 318



1 diagrama. CERT-LT 2014 m. gautų ir siųstų pranešimų tipai

Didelė Lietuvos kibernetinio saugumo problema (13 827 pranešimai per 2014 m.) buvo ir yra įrenginiai, kurie paprastai priklauso fiziniams asmenims ir turi saugumo spragų. Reikėtų pažymėti, kad dažniausiai tokios spragos nekelia tiesioginės grėsmės įrenginių savininkų duomenų saugumui, tačiau sudaro sąlygas piktavaliams naudoti įrenginius paskirstytųjų paslaugos trikdymo (angl. *Distributed Denial of Service, DDoS*) atakų metu kaip atakų stiprintuvus.

2014 m. CERT-LT organizavo susitikimus su interneto paslaugų teikėjais, kurių metu buvo pristatoma esama padėtis, aptariamos kliūtys kovai su įrenginių saugumo spragomis, nagrinėjami pasiūlymai ir teikėjų patirtis. 2015 m. CERT-LT siekia sustiprinti kovą su įrenginių saugumo spragomis: planuojama dar aktyviau bendradarbiauti su interneto paslaugų teikėjais, plėsti šviečiamąją veiklą raginant vartotojus pasirūpinti turimų tinklo įrenginių saugumu.

Kaip ir 2013 m., 2014 m. užfiksuota daug incidentų, susijusių su kenkimo programine įranga. CERT-LT ištyrė 11 276 kenkimo programinės įrangos panaudojimo atvejus (2013 m. – 11 125). Dažniausiai kenkimo programinė įranga naudota siekiant naudotojų kompiuterius įtraukti į botnetu . Apie įtraukimą į botų tinklą kompiuterio savininkas ilgą laiką gali nieko nežinoti (kompiuteris veikia iš esmės normaliai, kartais gali sulėtėti interneto ryšys). Antivirusinės programos turi vadinamuosius euristinius analizatorius (kurių veikimo tikslas – aptikti žalingą kodą net jei jo nėra antivirusinės programos duomenų bazėje, analizuojant kodo „elgesį“, jei jis būtų vykdomas). Tačiau CERT-LT pažymi, kad neretai būna taip, kad pavojingą kodą antivirusinės programos atpažįsta tik po kelių dienų (pvz., taip buvo su „Geodo“ ir „Feodo“ virusu). Manytina, kad 2015 m. virusų kūrėjai dar aktyviau kurs žalingus kodus išmaniesiems telefonams ir planšetiniams kompiuteriams.

2014 metais CERT-LT ištyrė 165 pranešimus apie paslaugos trikdymo atakas (angl. *Denial of Service, DoS*). Palyginti su 2013 m. (130 pranešimų), pranešimų skaičius padidėjo 27 proc. Paprastai šios atakos vykdomos automatizuotomis priemonėms, pasitelkiant botnetų išteklius. Siekdamas nutraukti vykdomas DoS atakas, CERT-LT teikė rekomendacijas svetainių savininkams ar elektroninės informacijos prieglobos paslaugas teikiančioms įmonėms, kaip stabdyti šias atakas, koordinavo veiksmus su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

Didelę grėsmę kelia botų tinklai, kuriais vykdoma nusikalstama veika: kenkimo kodo ir brukalo platinimas, paslaugos trikdymo atakos ir pan. CERT-LT duomenimis, 2014 metais Lietuvoje kasdien buvo fiksuojama vidutiniškai 2000 kompiuterių, kurie, savininkams nežinant, buvo valdomi nuotoliniu būdu. 2014 m. gruodžio mėn. tokių kompiuterių per dieną buvo fiksuojama mažiau – apie 1500. Šio skaičiaus sumažėjimą lėmė CERT-LT pritaikytos naujos incidentų sprendimo priemonės.

Prognozuojame, kad 2015 metais Lietuvoje botnetus sudarančių įrenginių skaičius ženkliai svyruos priklausomai nuo:

1) programinės įrangos spragų aptikimo (su aptiktomis ir viešai žinomomis spragomis lengviau kovoti);

2) žalingas programas kuriančių žmonių aktyvumo;

3) interneto naudotojų elgesio ir informuotumo (atsargumo, programinės įrangos atnaujinimų diegimo ir pan.).

2014 m. buvo stebimas labai aktyvus „GameOver ZeuS“ botnetas. Vasaros pradžioje CERT-LT su partnerių pagalba užfiksavo daugiau nei 2000 Lietuvos IP adresų, dalyvaujančių šio botneto veikloje. CERT-LT pastangomis 2014 m. pabaigoje šio botneto „narių“ skaičius sumažėjo iki maždaug 80. CERT-LT registruoja ir skelbia informaciją apie botų tinkluose aptiktų kompiuterių aktyvumą interneto svetainėje https://www.cert.lt/botnet.

2014 m. ne vieną dešimtį iš Lietuvos serverių veikiančių tinklalapių dėl galimų turinio valdymo sistemos saugumo spragų buvo užvaldęs kenkimo kodas „Stealrat“. Jis kuria botnetus ir iš užvaldytų kompiuterių siunčia brukalą, kuriuo stengiamasi įtraukti kitus kompiuterius į botnetą. Išaiškintais atvejais CERT-LT pateikė šio kodo šalinimo rekomendacijas svetainių savininkams ar elektroninės informacijos prieglobos paslaugas teikiančioms įmonėms ir tokių tinklalapių skaičius sumažėjo iki vienetų.

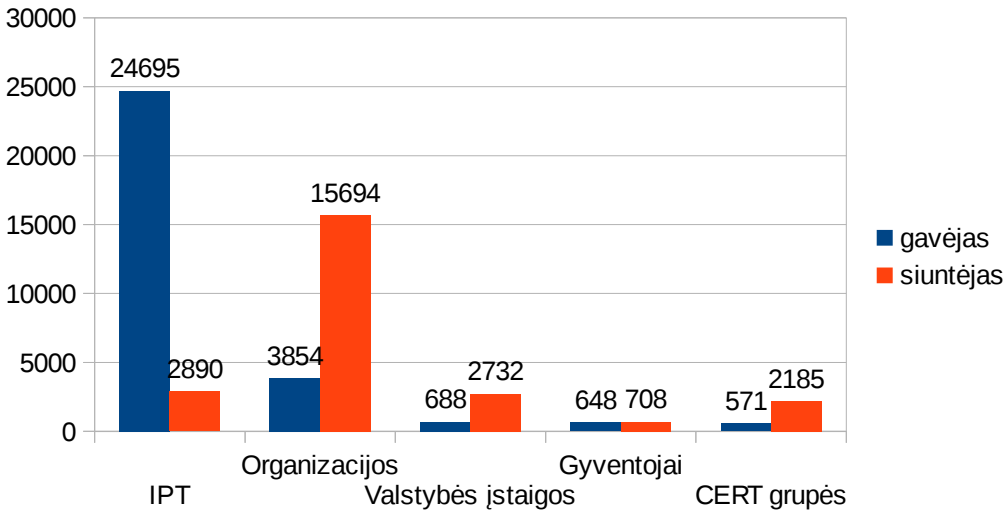
Nuo 2014 m. vidurio internete plito apgaulingas brukalas (angl. *spam*), kuriame buvo siūloma atidaryti failą, kuris neva yra judriojo ryšio operatoriaus atsiųsta arba kitokia sąskaita. Dažniausiai po nuorodą į PDF failą slėpėsi ZIP failas su viruso EXE failu, kurį pirmomis dienomis atpažindavo anaiptol ne kiekviena antivirusinė programinė įranga. Laiškus siųsdavo botneto, pavadinto „Geodo“, užvaldyti kompiuteriai. „Geodo“ naudoja tą pačią užkrėstų kompiuterių infrastruktūrą ir savęs platinimo būdą kaip ir jo pirmtakas „Feodo“. CERT-LT primena, kad net jei laišką gavote iš patikimo šaltinio, su priedais reikia elgtis atsargiai (pvz., juos galima patikrinti svetainėse www.cert.lt/antivirus/ arba www.virustotal.com). Nerekomenduojama atidaryti el. laiško priedų, jei siuntėjas jums nežinomas.

2014 m. CERT-LT ištyrė 630 klastojimo (angl. *phishing*) pranešimų (2013 m. – 558 pranešimus). Piktavaliai kuria internetinių svetainių klastotes siekdami arba išgauti internetinių paskyrų duomenis, arba iš to pasipelnyti. Kiekvieną savaitę gaunama pranešimų apie suklastotus elektroninių mokėjimo sistemų puslapius (dažniausiai – „Paypal“). Taip pat dažnai susidurta su pranešimais apie suklastotas „Facebook“, „Gmail“, „Yahoo“, „VK.com“ interneto svetaines. 2014 m. pabaigoje vėl suaktyvėjo policijos ir Interpolo interneto svetainių klastočių kūrėjai. Pastaroji klastotė pavojinga tuo, kad tinklalapis veikia taip, kad naudotojui būna sunku uždaryti naršyklės langą, o kompiuteris atrodo lyg būtų „užblokuotas“. Apie klastotes CERT-LT informuoja Lietuvos ar užsienio interneto paslaugos teikėjus, tarptautinius partnerius ir tarnybinės stoties, iš kurios veikia tokios svetainės, administratorius. Pažymėtina, kad šios klastotės, CERT-LT operatyviai veikiant, buvo greitai likviduojamos.

Daugiau nei dvigubai sumažėjo informacinių sistemų užvaldymų. 2013 m. šių incidentų buvo 10 924. Dėl CERT-LT aktyvių veiksmų 2014 m. užvaldymų sumažėjo iki 4 853. Atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant botų tinklus, įterpiant kenkimo kodą į prastai apsaugotas interneto svetaines.

Dideliu pasiekimu tapo 2014 m. rugsėjo mėn. CERT-LT organizuotos nacionalinės kibernetinės pratybos „X14“. Tai jau antrosios CERT-LT organizuotos pratybos Lietuvoje, prie kurių šį kartą prisijungė ir 4 šalys iš ES. Šiose pratybose buvo siekiama patikrinti tarpinstitucinio bendradarbiavimo efektyvumą, galimybes kritinėse situacijose rasti atsakingų institucijų atstovų kontaktus ir reaguoti į kibernetinius incidentus. Buvo tikrinami įgūdžiai operatyviai keistis informacija galimų kibernetinių incidentų metu, pasirengimas naudoti šifravimo priemones duomenims perduoti viešaisiais tinklais, įstaigų IT administratorių sugebėjimai atlikti nesudėtingas užduotis, pvz., atlikti greitą automatizuotą įvykių žurnalo (angl. *log*) analizę. Pratybose dalyvavo 25 valstybės institucijos, 8 bankų atstovai, 5 nacionalinės saugumo incidentų tyrimo CERT grupės (Lietuvos, Latvijos, Ukrainos, Bulgarijos, Rumunijos) ir 5 vietinės CERT grupės (LITNET, SVDPT, Krašto apsaugos ministerijos, TEO ir NRD CERT).

Svarbus CERT-LT veiklos faktorius yra aktualios kibernetinio saugumo informacijos apsikeitimas naudojant ryšio technologijas. Paminėtina, kad 2014 m. CERT-LT suteikė 241 konsultaciją Lietuvos gyventojams ir valstybės įstaigoms. 2-oje diagramoje pateikiami 5 pagrindiniai žinučių gavėjai ir siuntėjai.



2 diagrama. CERT-LT 2014 m. žinučių pagrindiniai siuntėjai ir gavėjai

Interneto svetainėje www.cert.lt, kuri pasiekiama ir naudojant IPv6 protokolą, galima:

1) skaityti naujienas, susijusias su IT saugumu;

2) peržiūrėti ilgai kaupiamą statistiką (tiek grafikus, tiek ataskaitas);

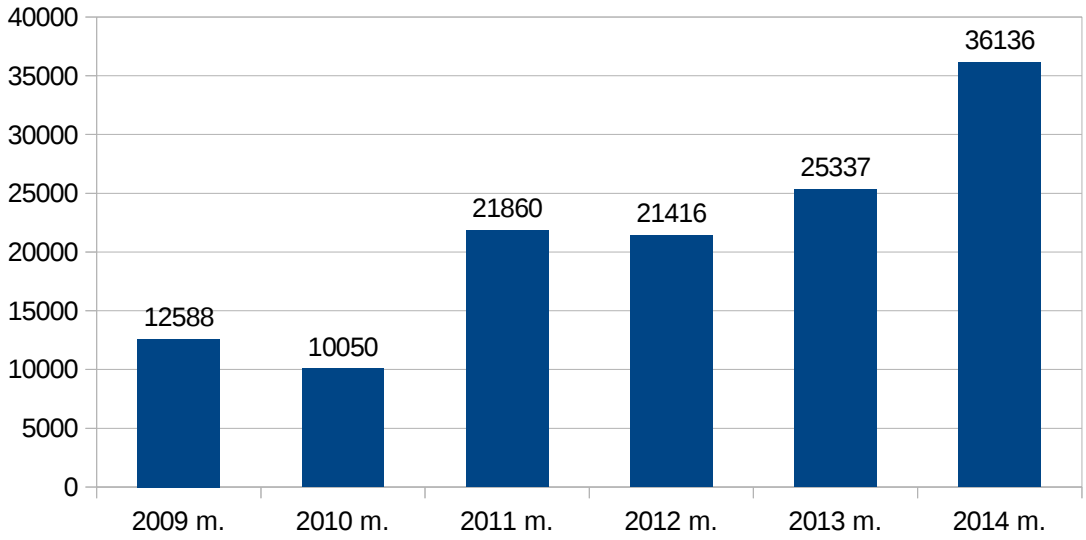
3) sužinoti pagrindinius CERT-LT veiklos uždavinius;

4) susipažinti su teisės aktais, reglamentuojančiais saugumą viešųjų ryšių tinkluose;

5) pasinaudoti vienu iš 6 tikrinimo įrankių (pvz., patikrinti, ar turimas tinklo įrenginys nenaudoja pažeidžiamo UPnP 1.0 protokolo, ar kompiuteris nėra įtrauktas į botneto veiklą, ar turimas IP adresas nėra užfiksuotas CERT-LT duomenų bazėje kaip dalyvaujantis kenkimo veikloje ir pan.).

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 formą tinklalapyje www.cert.lt/pranesti. Daugiau informacijos interneto naudotojams apie saugumą internete prieinama tinklalapyje www.esaugumas.lt.

Apibendrindami pateikiame CERT-LT apdorotų pranešimų suvestinę nuo 2009 iki 2014 m.



3 diagrama. CERT-LT 2009–2014 m. apdorotų žinučių suvestinė