CERT-LT apibendrina 2009 metų veiklą ir teikia prognozes 2010 metams

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT 2009 metais ištyrė 12 588 pranešimus apie incidentus elektroninėje erdvėje, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, vykdančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2008 metais, CERT-LT ištirtų panešimų apie incidentus skaičius išaugo 37 kartus. Didžiausia problema, su kuria, CERT duomenimis, 2009 susidūrė interneto naudotojai, buvo kenkėjiška programinė įranga, sudariusi 95,2 proc. visų tirtų pranešimų.

Didžiąją dalį pranešimų sudarė pranešimai apie „kirminą“ *Win32/Conflicker/Downadup,* kuris labai sparčiai plito 2009 metų pradžioje. „Kirminas“ gali perimti kompiuterio valdymą ir įtraukti jį į *botnet* tinklą, t. y. pasitelkus kenkėjišką programinę įrangą, valdomų kompiuterių tinklas dažnai panaudojamas kaip priemonė kitoms saugumo atakoms vykdyti. CERT-LT registruoja ir tinklalapyje www.esaugumas.lt skelbia informaciją apie *botnet* tinkluose aptiktų kompiuterių aktyvumą. Taip pat 2009 metais pagausėjo kenkėjiškos programinės įrangos, plintančios per interneto pokalbių programas, socialinius tinklalapius. Apie jas interneto naudotojai būdavo įspėjami ir jiems pateikiamos saugumo rekomendacijos tinklalapyje www.esaugumas.lt.

2009 metais ypač padaugėjo pranešimų apie užvaldymo incidentus (180 pranešimų), t. y. 3 kartus daugiau nei 2008 metais. Didžiąją šių pranešimų dalį sudarė neteisėtas prisijungimas prie interneto svetainių, naudojant vogtus arba specialiomis programomis parinktus administratoriaus slaptažodžius. Dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėms, pasitelkiant *botnet* resursus. Kitaip nei ankstesniais metais, daugeliu atveju užvaldytos svetainės vizualiai nebuvo keičiamos, tačiau į jas įterpiamas kenkėjiškas kodas. Interneto naudotojas, aplankęs tokią interneto svetainę, būdavo nukreipiamas į tarnybines stotis, kuriose laikomi interneto naršyklių pažeidžiamumo (angl.

exploit) įrankiai. Tokiu būdu, pasinaudojant vartotojo naudojamų kompiuterinių programų saugumo spragomis, kompiuterį galima užkrėsti kenkėjišku kodu. Toliau jau vartotojo kompiuteryje veikiantis kenkėjiškas kodas atsisiųsdavo kitas kenkėjiškas programas, tokias kaip „Password Stealers“, „Backdoor“,„Downloader“ ir pan.

Kaip ir 2008, taip ir 2009 metais pranešimų apie duomenų klastojimo incidentus skaičius augo. Piktavaliai, pasinaudodami nepageidaujamomis elektroninio pašto žinutėmis (angl. *Spam*) ar suklastotais interneto tinklalapiais, siekdavo išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis. Dažniausiai piktavaliai siekė išgauti duomenis apie prisijungimus prie el. bankininkystės sistemų. Šiais metais buvo tirti 37 tokie pranešimai, t. y. 48 proc. daugiau nei 2008 metais (25 pranešimai).

Viena iš didžiausių tinklų ir informacijos saugumo problemų pasaulyje bei Lietuvoje išlieka *botnet* tinklai. Kiekvienais metais jų vis daugėja sujungiant milijonus užkrėstų kompiuterių. Vis daugiau saugumo atakų įvykdoma pasinaudojant jais. Šiais metais buvo įvykdytos 42 *DoS* atakos prieš Lietuvos elektroninių ryšių tinklus, informacines sistemas ar elektroninių ryšių tinklais teikiamas paslaugas – t. y. 1,63 karto daugiau nei 2008 metais. Dažniausiai naudotojas net nežino, kad jo kompiuteris veikia *botnet* tinkle kaip „kompiuteris zombis“. Tačiau, kilus įtarimams, naudotojas tinklalapyje www.esaugumas.lt/botnet gali pasitikrinti, ar kompiuterio IP adresas (angl. *Internet Protocol*) nėra užfiksuotas *botnet* duomenų bazėje. CERT-LT, bendradarbiaudama su Lietuvos interneto paslaugų teikėjais bei su kitomis CERT grupėmis, kovoja su šiais tinklais, informuoja interneto naudotojus apie pastebėtą jų kompiuterių dalyvavimą šioje veikloje, pateikia rekomendacijas, kaip išvalyti kompiuterį bei apsaugoti jį ateityje. Pastebėta, kad užkrėsti kompiuteriai Lietuvoje ne tik būna tarptautinio *botnet* tinklo dalimi, bet ir formuoja lietuvišką *botnet* tinklą, sudarytą tik iš Lietuvos interneto naudotojų užkrėstų kompiuterių.

Dalyvaudamas projekte „Draugiškas internetas“ (www.draugiskasinternetas.lt) CERT-LT per 2009 metus priėmė ir išnagrinėjo 411 pranešimų apie nelegalų ir žalingą turinį internete. 73 (55 proc. daugiau nei 2008) atvejais CERT-LT pagal suderintus kriterijus identifikavo, kad galbūt buvo pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete. Visa surinkta medžiaga buvo perduota atsakingoms institucijoms tolimesniam tyrimui. CERT-LT duomenimis, dėl 4 incidentų atvejų pradėtos bylos teismuose.

Siekdamas didinti IT saugumo supratimą Lietuvoje, CERT-LT 47 kartus konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

Prognozės 2010 metams

- Tikėtina, kad šiais metais **pagausės kenkėjiškos programinės įrangos**, tokios kaip „Trojos arkliai“ (angl. *Trojan*), kurie vagia iš interneto naudotojų konfidencialius duomenis; „kirminai“ (angl. *worms*), plintantys per socialinius tinklalapius, pasinaudodami užkrėstais vartotojų draugų profiliais. Šio tipo kenkėjiškos programinės įrangos iš lėto išstums klasikinius virusus ar duomenų klastojimo atakas. Pasaulyje pastebima tendencija, kad įvykdyti klastojimo atakas tampa vis sudėtingiau, vartotojai yra daugiau informuoti ir budresni, naudojamos vis sudėtingesnės apsaugos technologijos, todėl manoma, kad šias atakas pakeis „Trojos arkliai“, kurie pasinaudodami naujais metodais, pasieks tuos pačius rezultatus.
- IT saugumo specialistai spėja, kad 2010 metais pati **didžiausia problema bus socialiniai tinklalapiai**, nes jie jungia milijonus vartotojų ir platinti kenkėjišką programinę įrangą nėra sudėtinga.
- Spėjama, kad **daugės kenkėjiškos programinės įrangos, sugebančios automatizuotai keisti savo pačios kodą** kelis kartus per dieną, o tai apsunkins apsaugos priemonių veikimą bei jų aptikimą.
- Vis labiau populiarės **kenkėjiška programinė įranga, sugebanti prisitaikyti prie naudotojo šalies geografinės padėties** (parinkdama vartotojui tinkamą

kalbą, naudodama pranešimuose aktualias tos šalies naujienas, bankų pavadinimus ir pan.).

- Taip pat, sparčiai augant išmaniųjų telefonų populiarumui, tikėtinas **mobilaus tinklo *botnet* augimas bei virusų plitimas šiuose įrenginiuose**, pasinaudojant operacinės sistemos ar trečiųjų šalių programinės įrangos pažeidžiamumais.
- **Piktavaliai šiais metais sieks dar labiau pasinaudoti** interneto naršyklių, PDF bylų redaktorių, *Flash* grotuvų bei kitų populiarių programų **pažeidžiamumais**.
- 2010 metais tikimasi didelio kenkėjiškos programinės įrangos pagausėjimo, suklastotų el. bilietų parduotuvių, nepageidaujamo pašto pranešimų bei kitų **incidentų, susijusių su didelio ažiotažo sulaukiančiu Pasaulio futbolo čempionatu**.

Naudotojams, susidūrusiems su tinklų ir informacijos saugumo problemomis, patariama nedelsiant kreiptis į savo interneto paslaugų teikėją, o jei šis atsisako spręsti problemą, informuoti apie tai ir pranešti apie incidentą CERT-LT. Naudotojas gali užpildyti specialią formą tinklalapyje www.cert.lt/pranesti.html arba siųsti incidento aprašą el. pašto adresu cert@cert.lt

Apie CERT-LT

CERT-LT – tai 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 pavesti nacionalinio CERT funkcijas Lietuvos Respublikos ryšių reguliavimo tarnybai (RRT).

CERT-LT vykdo koordinuojančius veiksmus, įgyvendina programinius sprendimus, susijusius su tinklų ir informacijos saugumu. CERT-LT atlieka prevencinę veiklą, teikdamas informaciją apie naujausias grėsmes kompiuterių naudotojams. Informacija skelbiama specializuotame tinklalapyje

www.esaugumas.lt, kuriame kompiuterių vartotojams taip pat pateikiamos rekomendacijos ir įspėjimai, kaip išvengti didesnio mąsto pavojų. Sprendžiant tarptautinius incidentus, CERT-LT bendradarbiauja su kitose valstybėse veikiančiais CERT padaliniais.

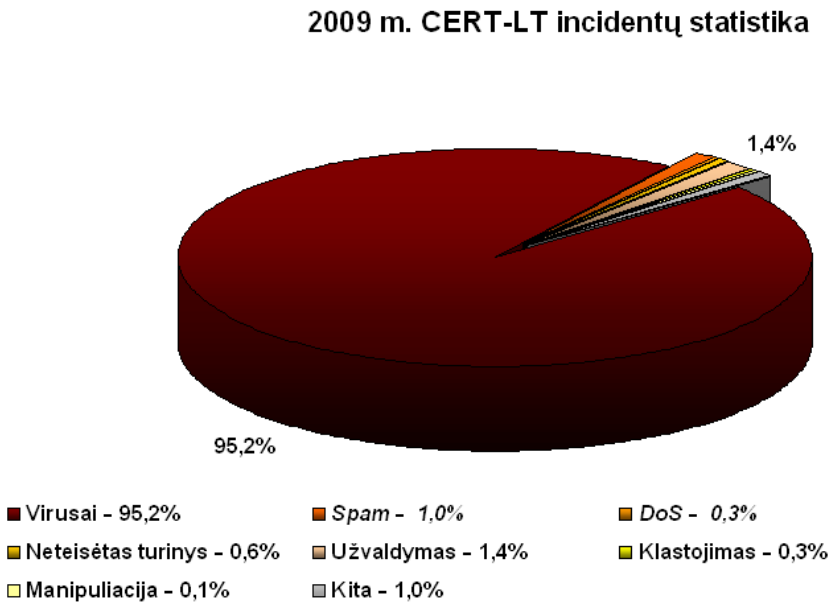
2009-ais metais CERT-LT gavo „Trusted Introducer“ tinklo, vienijančio daugumos Europos valstybių CERT grupes, akreditaciją, taip pat, įgyvendinęs visus reikalavimus, tapo FIRST (angl. Forum of Incident Response and Security Teams) organizacijos pilnateisiu nariu.

Gautų pranešimų apie incidentus pasiskirstymas pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2009 m.	Incidentų Skaičius 2009 m. (proc.)
Virusai	**Kenkėjiška programinė įranga** (angl. *Virus, Worm)* – programinė įranga ar jos dalis, specialiai sukurta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (taip pat perimti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip	**11 989**	**95,2**

	panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.		
Spam	**Nepageidaujamas elektroninis paštas** (angl. *spam*) – elektroninio pašto laiškų tiesioginės rinkodaros tikslais siuntimas be elektroninio pašto naudotojo ir (ar) abonento išankstinio sutikimo, galintis turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui Lietuvos Respublikoje.	**129**	**1,0**
DoS	**Elektroninės paslaugos trikdymo ataka** (angl. *DoS*) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar) informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas.	**42**	**0,3**
Neteisėtas turinys	**Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	**73**	**0,6**
Užvaldymas	**Neleidžiamasis naudojimasis informacinės sistemos ištekliais** (angl. *Web Site Defacement*) – neteisėtas informacinės sistemos išteklių naudojimas. ir **Neleidžiamasis prisijungimas** (angl. *System Compromise/Intrusion*) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.	**180**	**1,4**
Klastojimas	**Elektroninių duomenų klastojimas** (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais	**37**	**0,3**

	duomenimis.		
Manipuliacija	**Manipuliacija elektroniniais duomenimis** (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	**16**	**0,1**
Kiti		**122 (49 konsultacijų)**	**1,0**



Incidentų statistikos ataskaitas galite rasti čia