CERT-LT apibendrina II ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2010 m. II ketvirčio veiklos rezultatus. CERT-LT per 2010 m. II ketvirtį tyrė 2 706 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 2009 m. II ketvirčiu (3 886 pranešimai), tirtų pranešimų sumažėjo 30 procentais. Palyginti su 2010 m. I ketvirčiu (2 313 pranešimų), tirtų pranešimų apie incidentus padaugėjo 17 procentų.

Daugiausia ištirta pranešimų (2 536) apie kenkėjišką programinę įrangą. Didžiąją jų dalį sudarė incidentai dėl „kirmino“ Win32/Conflicker/Downadup, kuris ypač sparčiai plito 2009 m. pradžioje. Nors šis „kirminas“ jau mažiau plinta, tačiau dar yra daug pažeistų kompiuterių sistemų, kurios ir toliau platiną šią kenkėjišką programą. Ji gali pažeisti kompiuterio valdymą ir įtraukti jį į botnet tinklą, t. y. pasitelkus kenkėjišką programą valdomų kompiuterių tinklas dažnai panaudojamas kitoms saugumo atakoms vykdyti. CERT-LT nuolat registruoja ir tinklalapyje www.esaugumas.lt skelbia informaciją apie botnet tinkluose aptiktų kompiuterių aktyvumą.

Dalyvaudamas projekte „Draugiškas internetas“ (www.draugiskasinternetas.lt) CERT-LT 2010 m. II ketvirtį gavo ir išnagrinėjo 18 pranešimų apie neteisėtą ir žalingą turinį internete. CERT-LT pagal suderintus kriterijus nustatė 6 (45 proc. mažiau nei 2010 m. I ketvirtį) atvejus, kai galbūt buvo pažeisti Lietuvos Respublikos įstatymai dėl neteisėto turinio internete. Su šiais atvejais susijusi medžiaga ir duomenys perduoti atsakingoms institucijoms tolesniam tyrimui.

Šį ketvirtį, kaip ir ankstesniais ketvirčiais, ir toliau daugėjo pranešimų apie kompiuterių užvaldymo incidentus: CERT-LT ištyrė 111 pranešimų – tai 22 kartais daugiau nei 2009 m. II ketvirtį (5 pranešimai) ir 57 proc. mažiau nei 2010 m. I ketvirtį (261 pranešimas). CERT-LT tyrimų duomenimis, dauguma tinklalapių buvo užvaldyta ne dėl programinių ar laiku neištaisytų spragų, bet dėl to, kad teisėti savininkai prarado prisijungimo duomenis. Įvairiose programose, elektroniniame pašte ar kituose elektroniniuose tekstuose saugomus prisijungimo duomenis dažnai gali pasisavinti ir naudoti piktavaliai – tai dažnas kenkėjiškų programų taikinys. CERT-LT informavo tinklalapių savininkus ar tinklalapių

prieglobos paslaugas teikiančias įmones apie pastebėtus kenkėjiškus programos kodus ir paprašė juos pašalinti, nes per pažeistus tinklalapius toliau platinamas kenkėjiškas programos kodas. CERT-LT ir toliau stebi šių incidentų skaičiaus didėjimo tendencijas.

CERT-LT šį ketvirtį gavo 56 pranešimus apie nepageidaujamus elektroninio pašto laiškus (angl. spam). Išsamesniam tyrimui jie perduoti spam atvejus nagrinėjančioms kompetentingoms institucijoms, nes juose nebuvo aptikta saugumo spragų, kurios galėtų turėti neigiamos įtakos elektroninio pašto informacinių sistemų veikimui Lietuvos Respublikoje.

Be minėtų, tirti pranešimai apie šiuos incidentus: dėl elektroninės paslaugos trikdymo atakų (angl. Denial of Service, DoS) – 6 (2010 m. I ketvirtį – 7); dėl klastojimo – 6 (2010 m. I ketvirtį – 8); dėl manipuliacijos – 6 (2010 m. I ketvirtį – 9). CERT-LT ištyrė visus iš interneto naudotojų ir interneto paslaugų teikėjų gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti jų pasekmes ar sustabdyti jų plitimą.

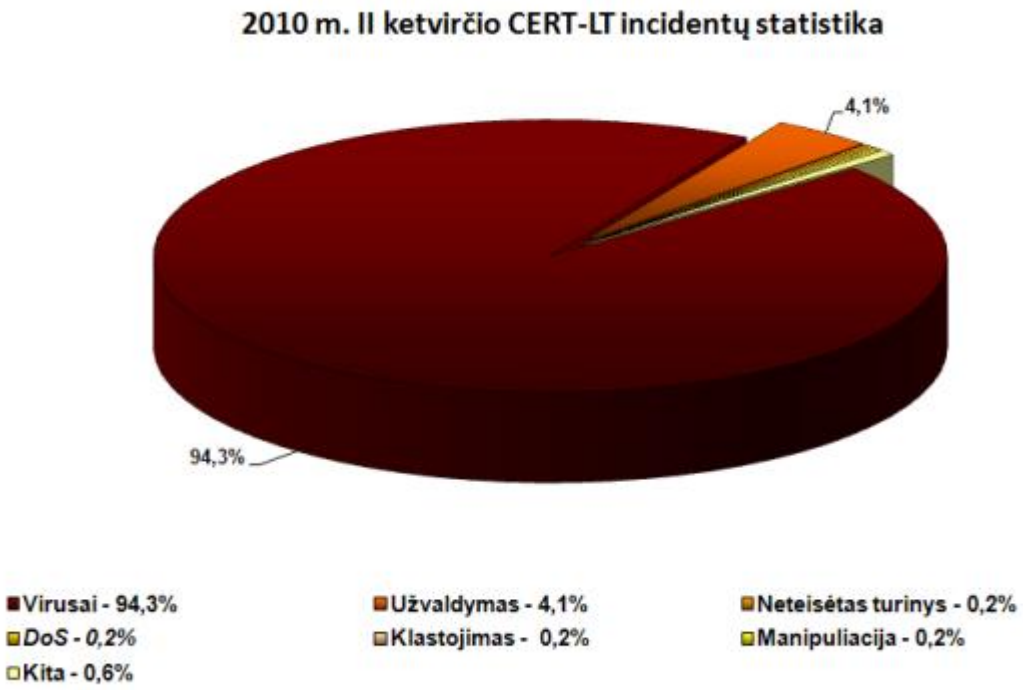
CERT-LT 18 kartų konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

Tirti pranešimai apie incidentus pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2010 m. II ketv.	Incidentų Skaičius 2010 m. II ketv. (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,	**2 536**	**94,3**

	panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip 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.	**0** (gauta 56 pranešimai apie pavienį nepageidaujamą elektroninį paštą)	**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.	**6**	**0,2**
Neteisėtas turinys	**Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	**6**	**0,2**
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.	**111**	**4,1**
Klastojimas	**Elektroninių duomenų**	**6**	**0,2**

	klastojimas (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.		
Manipuliacija	**Manipuliacija elektroniniais duomenimis** (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	**6**	**0,2**
Kiti		**17**	**0,6**



Incidentų statistikos ataskaitas galite rasti internetinėje svetainėje https://www.cert.lt/statistika.html