

CERT-LT apibendrina II ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys **CERT-LT** apibendrina 2009 m. II ketvirčio veiklos rezultatus. **CERT-LT** per 2009 metų II ketvirtį tyrė 3 886 iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, vykdančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su 2008 m. II ketvirčiu (92 pranešimai), incidentų skaičius išaugo 4 124 proc. – beveik keturiasdešimt trim kartais. Palyginti su 2009 m. I ketvirčiu, incidentų skaičius išaugo 278 proc.

Daugiausia pranešimų (3 817 pranešimų) užregistruota apie kenkėjišką programinę įrangą. Tokį didelį skaičių įtakoją visame pasaulyje išplitęs kirminas *Win32/Conflicker/Downadup*, kuris veikdamas 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. Taip pat pastebėtas didelis kenkėjiškos programinės įrangos plitimas socialiniuose tinklalapiuose. CERT-LT registruoja ir skelbia informaciją apie *botnet* tinkluose aptiktų kompiuterių aktyvumą tinklalapyje www.esaugumas.lt.

Dalyvaujantis projekte „Draugiškas internetas“ (www.draugiskasinternetas.lt), CERT-LT per 2009 metų II ketvirtį gavo ir išnagrino 110 pranešimų apie neteisėtą turinį internete. CERT-LT nustatė 20 atvejų, kuomet buvo pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete (pornografijos, pedofilijos, rasizmo), o visa surinkta medžiaga buvo perduota atsakingoms institucijoms tolimesniai tyrimui.

Išaugo klastojimo (angl. *Phishing*) incidentų skaičius. Per 2009 metus užregistruoti 27 incidentai – tai 8 proc. daugiau nei per visus 2008 metus (25 incidentai). Piktavaliai, pasinaudodami nepageidaujamos elektroninio pašto žinutėmis (angl. *Spam*) ar falsifikuotais internetiniais tinklalapiais, siekia išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis.

Kitų incidentų skaičius šį ketvirtį sumažėjo: *Spam* – 11 incidentų (2009 m. I ketvirtį – 24); *DoS* atakų – 7 (2009 m. I ketvirtį – 20); užvaldymų – 5 (2009 m. I ketvirtį – 17);

manipuliacija – 1 (2009 m. I ketvirtį – 4). Gautus pranešimus apie incidentus iš naudotojų ir teikėjų CERT-LT ištyrė ir pateikė rekomendacijas, kaip pašalinti incidentų pasekmes ar sustabdyti jų plitimą.

Pastebimas padidėjęs elektroninių ryšių tinklų ir informacijos saugumo incidentų aktyvumas, todėl CERT-LT nori atkreipti į tai visų dėmesį ir rekomenduoja įsidięgti apsaugos programas, reguliariai atnaujinti jas, taip pat atnaujinti operacines sistemas bei kitas naudojamąs programas, atsisiunčiant naujausias programų atnaujinimus iš oficialaus gamintojo tinklalapio. Taip pat patariama būti atidiems naudojantis elektroninės bankininkystės sistemomis, bei atminti, kad niekas ir jokiais aplinkybėmis neturi teisės reikalauti pateikti prisijungimo slaptažodžius bei kitus konfidencialius duomenis – nei telefonu, nei el. paštu ar kitais būdais. Daugiau informacijos kaip saugiai naudotis el. paslaugomis internete – www.esaugumas.lt.

Užfiksuotų incidentų pasiskirstymas pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2009 m. II ketv.	Incidentų Skaičius 2009 m. II ketv. (proc.)
Virusai	Kenkėjiška programinė įranga (angl. <i>Virus, Worm</i>) – 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 panaudoti neviešus elektroninius duomenis	3 817	98,22
Spam	Nepageidaujamas elektroninis paštas (angl. <i>spam</i>) – 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.	11	0,28
DoS	Elektroninės paslaugos trikdymo ataka (angl. <i>DoS</i>) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar)	7	0,18

	informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas.		
Neteisėtas turinys	Neteisėtas turinys – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	20	0,51
Užvaldymas	Neleidžiamasis naudojimas informacinės sistemos ištekliais (angl. <i>Web Site Defacement</i>) – neteisėtas informacinės sistemos išteklių naudojimas. ir Neleidžiamasis prisijungimas (angl. <i>System Compromise/Intrusion</i>) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.	5	0,13
Klastojimas	Elektroninių duomenų klastojimas (angl. <i>Phishing</i>) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	15	0,39
Manipuliacija	Manipuliacija elektroniniais duomenimis (angl. <i>Spyware</i>) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	1	0,03
Kita		10	0,26

2009 m. II ketvirčio CERT-LT incidentų statistika

