

2008 m. IV ketvirčio CERT-LT incidentų statistika

CERT-LT apibendrina IV ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys [CERT-LT](#) apibendrina 2008 m. IV ketvirčio veiklos rezultatus.

[CERT-LT](#) per 2008 metų IV ketvirtį ištyrė 41 pranešimą apie incidentus elektroninėje erdvėje, kurie buvo gauti iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, vykdančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų.

Daugiausia pranešimų (11 pranešimų) užregistruota apie paskirstytąsias atsisakymo aptarnauti (DDoS) atakas. Palyginti su III ketvirčiu, per IV ketvirtį pranešimų apie DDoS atakas skaičius padidėjo 120 proc. (III ketvirtyje – 5 pranešimai). Šios atakos dažniausiai buvo vykdomos iš užkrėstų kenkėjišku kodu kompiuterių (kompiuterių zombių). CERT-LT koordinavo veiksmus su interneto paslaugų teikėjais, kad būtų nutrauktos vykdomos atakos, bei būtų informuoti interneto naudotojai apie pažeistus jų valdomus kompiuterius.

Toliau dalyvaudama projekte „[Draugiškas internetas](#)“, CERT-LT 2008 m. IV ketvirtį priėmė ir išnagrinėjo 59 pranešimą apie neteisėtą turinį. Iš jų pagrįstais buvo pripažinti 8 ir perduoti tirti atsakingoms institucijoms. Nuo projekto pradžios jau priimta 772 pranešimai apie neteisėtą turinį internete.

CERT-LT toliau registruoja ir skelbia informaciją apie „[botnet](#)“ tinkluose aptiktų kompiuterių [aktyvumą](#). Per 2008 m. IV ketvirtį buvo užregistruoti 411 pažeisti ir nuotoliniu būdu valdomi kompiuteriai zombiai („botai“). Nuo stebėjimo pradžios jau užregistruoti 5443 unikalūs lietuviški IP (*angl.* Internet Protocol) adresai, veikiantys „botnet“ tinkluose. Nuo 2008 m. II ketvirčio CERT-LT siunčia pranešimus interneto paslaugų tiekėjams apie jų tinkluose aptiktus kompiuterius zombius.

Kitų incidentų skaičius šį ketvirtį: *Spam* – 9 incidentai (skaičius sumažėjo lyginant su III ketvirčiu, 53 pranešimais, nes CERT-LT nuo šiol vykdo tyrimus tik tų elektroninio pašto pranešimų, kurių siuntimas dideliais kiekiais gali turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui, Lietuvos Respublikoje); *phishing* atakos – 1 incidentas (III ketvirtį – 2); kompiuterių virusų – 5 (III ketvirtį – 11); įsilaužimų – 5 (III ketvirtį – 20). Gautus pranešimus apie incidentus iš naudotojų ir tiekėjų CERT-LT ištyrė ir pateikė rekomendacijas, kaip pašalinti incidentus ar sustabdyti jų plitimą.

Užfiksuotų incidentų pasiskirstymas pagal tipus:

<i>Spam</i>	<i>Phishing</i>	Virusai	Įsilaužimai	Neleg. turinys	DDoS	Kita
9	1	5	5	8	11	2

2008 m. IV ketvirčio CERT-LT incidentų statistika

