CERT-LT apibendrina 2014m. II k. veiklą

Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2014 m. II ketvirčio veiklos rezultatus. CERT-LT 2014 m. II ketvirtį ištyrė 7 373 incidentus pagal 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 tuo pačiu 2013 m. laikotarpiu (6115 incidentų), incidentų padaugėjo 21 proc. Šių metų II-ame ketvirtyje CERT-LT atliktų tyrimų metu buvo užregistruoti 3310 incidentai, susiję pavojingomis interneto įrenginių saugumo spragomis.

Daugiausia užregistruota incidentų, susijusių su kompiuterių naudotojų įrenginiais, tokiais kaip tinklo maršruto parinktuvai ir pan., skirtais prisijungti prie interneto ir turinčiais pavojingų saugumo spragų. Per šį laikotarpį CERT-LT užregistravo 3310 pavojingas saugumo spragas – dvigubai daugiau nei 2014 m. I ketvirtį, ir 526 kompiuterių užvaldymo atvejus – 71 proc. mažiau nei 2014 m. I ketvirtį. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, jie susiję su prastai apsaugota įranga internete.

2014 II ketvirtį aktyviai plito kenkimo programa - kirminas *„Turla“*. Šis *Trojos arklys* surenka ir į komandinį serverį išsiunčia pažeistuose kompiuteriuose esančią tam tikrą informaciją bei komandinio serverio valdytojui suteikia teisę pilnai kontroliuoti tokį kompiuterį. Kenkimo programa atidaro *galines duris* (*angl. Back door*), kad galėtų kontroliuoti aukų kompiuterius sudarant galimybes nukopijuoti kompiuteriuose esančią informaciją ir naudoti tokį įrenginį naujų kompiuterių naudotojų užkrėtimui, kenkimo programos plitimui.

Antrąjį ketvirtį buvo užfiksuotas pirmasis išmanusis televizorius, dalyvavęs kenkėjiškoje botnet veikloje. Taip pat šį ketvirtį buvo užfiksuota daugiau nei 2000 IP adresų, Lietuvoje dalyvaujančių „GameOver ZeuS“ botneto veikloje. „GameOver Zeus“ dažniausiai naudojamas siekiant perimti vartotojų asmens duomenis, gauti slaptažodžius ar prisijungimus prie elektroninės bankininkystės.

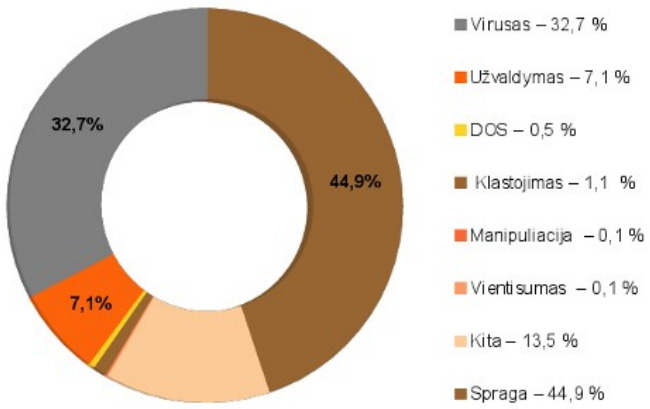
2014 II ketvirtį CERT-LT užregistravo daugiau nei 38000 unikalių Lietuvos IP adresų, turinčių *SSDP, DNS, NTP, SNMP, NetBIOS* paslaugų saugumo spragas, kurios gali būti naudojamos paslaugos trikdymo atakoms ar kitai kenkimo veiklai vykdyti. CERT-LT apie Lietuvos tinkle pastebėtus įrenginius, galinčius turėti šią spragą, informavo interneto paslaugų teikėjus ir pateikė rekomendacijas www.cert.lt svetainėje.

Antrąjį ketvirtį sumažėjo pranešimų skaičius (35 pranešimai) apie paskirstytosios paslaugos trikdymo atakas (DDoS). Palyginti su 2014 m. I ketvirčiu (45 pranešimai), pranešimų skaičius sumažėjo 23 proc. CERT-LT tyrimų duomenimis, šios atakos buvo vykdomos automatizuotomis priemonėms, pasitelkiant botnetų resursus ir pažeidžiamus įrenginius internete. Siekiant nutraukti vykdomas atakas, CERT-LT teikė rekomendacijas atakuojamų tarnybinių stočių savininkams ar svetainių prieglobos paslaugas teikiančioms įmonėms, kaip stabdyti šias atakas, koordinavo veiksmus su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

Kiti gauti ir tirti pranešimai: apie manipuliaciją elektroniniais duomenimis – 5 (2014 m. I ketvirtį – 13), vientisumo pažeidimus – 11 ir elektroninių duomenų klastojimą – 81 (2014 m. I ketvirtį – 130).

Šių metų antrąjį ketvirtį CERT-LT ištyrė 2 412 kenkimo programinės įrangos panaudojimo atvejų.

Incidentų tipas	**Incidentų skaičius 2014m. II ketv. (vnt.)**	**Procentinė visų incidentų dalis (proc.)**
Spraga	3310	44,9
Virusas	2412	32,7
Užvaldymas	526	7,1
Klastojimas	81	1,1
DOS	35	0,5
Vientisumas	11	0,1
Manipuliacija	5	0,1
Kita	993	13,5



1 pav. 2014 m. II ketvirtį CERT-LT užfiksuotų incidentų statistika, proc.