2017 METŲ II KETVIRČIO CERT-LT VEIKLOS ATASKAITA

Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2017 m. II ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 13 530 pranešimų apie incidentus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų.** Pažymėtina, kad beveik 14 proc. pranešimų apie incidentus (arba 1 840) buvo detaliai tiriami CERT-LT specialistų. Daugiausia tai – informacinių sistemų užvaldymai, paslaugų trikdymo atakos bei kiti išskirtiniai atvejai, įskaitant incidentus, apie kuriuos pranešta mūsų interneto svetainėje (www.cert.lt/pranesti.html) užpildžius specialią formą arba elektroniniu paštu. Likusioji pranešimų apie incidentus dalis apdorota automatiniu būdu, perduodant informaciją apie incidentą bei rekomendacijas paslaugų teikėjams, kuriems priklauso su incidentu susiję IP adresai. Palyginti su 2016 m. II ketv. (10 991 incidentas), incidentų padaugėjo 23,1 procento. Palyginti su 2017 m. I ketvirčiu (14 643 incidentai), incidentų sumažėjo 7,6 procento.

Kenkimo programinė įranga, įrenginių saugumo spragos ir informacinių sistemų užvaldymai kartu sudaro maždaug 85 proc. visų incidentų. Beveik 44 procentus visų incidentų buvo susiję su tinklo įrenginiais (įskaitant ir „*Internet of Things*“ tipo), turinčiais saugumo spragų – 5 905. Penktadalį visų incidentų (arba 2 755 pranešimus) sudarė kenkimo programinė įranga: virusai (įskaitant išpirkos reikalaujančius „*ransomware*“), Trojos arkliai ir pan. Informacinių sistemų užvaldymų skaičius buvo panašus – 2 775. Atliktų tyrimų duomenys rodo, kad dauguma aptiktų užvaldymo atvejų atliekami automatizuotomis priemonėmis, pasitelkiant botų tinklus, įterpiant kenkimo kodą į prastai apsaugotas ar seniai naujintas interneto svetaines, išnaudojant pasenusių turinio valdymo sistemų saugumo spragas ar pasinaudojant nesaugiu, dažnai – gamykliniu (angl. *default*) slaptažodžiu.

Svetainių klastojimų buvo 376, net 2,5 karto daugiau nei prieš metus. Kaip ir anksčiau, piktavaliai daugiausia klastojo socialinio tinklo svetainę *facebook.com*, el. pašto sistemas (*gmail.com*, *yahoo.com*), el. atsiskaitymų svetainę *paypal.com*, kartais – užsienio bankų svetaines ir užsienio el. parduotuves. Gegužės mėn. pabaigoje ir birželio mėn. pabaigoje stebėtas 2-jų Lietuvoje veikiančių bankų svetainių klastočių „pliūpsnis“. Intervale nuo 06-27 iki 07-03 CERT-LT darbuotojų pastangomis buvo uždaryti 9 piktavalių sukurti tinklalapiai, veikę Prancūzijos, Portugalijos ir JAV tarnybinėse stotyse.

Įvairaus pobūdžio pranešimų sumažėjo iki 1 672. Užfiksuoti 7 vientisumo pažeidimai ir 7 elektroninių paslaugų trikdymo atvejai. Kiti ketvirčio įvykiai ir tendencijos (taip pat žr. https://www.cert.lt/naujienos.html):

1) Gegužę piktavalių buvo įvykdyta didžiulė kibernetinė ataka, panaudojant duomenis šifruojantį ir išpirkos reikalaujantį virusą „WannaCry“. Virusas išnaudojo „SMB/Samba“ protokolo spragą. Žr. https://www.cert.lt/naujienos/didziausia_istorijoje_ransomware_ataka_plinta_wind.html.

2) Birželio pabaigoje pradėjo siautėti kitas duomenis šifruojantis virusas – „Petya“/ „NotPetya“. Jis irgi išnaudojo „SMB/Samba“ spragą.

3) Balandžio viduryje buvo aprašytas naujas svetainių klastojimų būdas, susijęs su „Unicode“ simbolių naudojimu domeno varde. Saugumo tyrinėtojų sukurta pavyzdinė svetainė – appĮe.com, kurios domenas labai panašus į garsiosios korporacijos „Apple Inc.“ svetainę.

4) CERT-LT įvėdė naują IT saugumo pranešimų tipą – „grėsmė“. Grėsmė – tai didelio pavojaus saugumo spraga, kuria nepasirūpinus pasekmės gali būti itin liūdnos (pvz., į kompiuterį ar tarnybinę stotį gali patekti pavojingas kenkimo kodas).

Pavojingų virusų plitimas paprastai susijęs su viena ar kita programinės įrangos saugumo spraga. Todėl CERT-LT ragina fizinius asmenis ir įmonių IT darbuotojus domėtis IT saugumo naujienomis bei rūpintis kompiuterine higiena: tikrinti savo informacinių sistemų konfigūraciją, daryti svarbių duomenų kopijas į nepriklausomą laikmeną, laiku diegti programų naujinius.

Lentelėse ir diagramoje pateikiame incidentų suvestines. Visas CERT-LT apdorotų incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.html. CERT-LT skelbia įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas socialiniame tinkle „Twitter“. Jeigu norite sužinoti naujausias IT saugumo aktualijas, prisijunkite (angl. *follow*) prie mūsų adresu https://twitter.com/cert_lt. Surikiuotos pagal temą rekomendacijos pateikiamos https://www.cert.lt/rekomendacijos.html.

1 lentelė. CERT-LT 2016 m. II, 2017 m. I ir II ketv. apdorotų incidentų skaičiaus palyginimas

Incidentų tipas	**Incidentų skaičius**			**Pokytis, proc.**	
	2016 II	**2017 I**	**2017 II**	**2017 II / 2016 II**	**2017 II / 2017 I**
Grėsmė	n/d	n/d	33	n/d	n/d
Kenkimo programinė įranga	2 531	2 580	2 755	+8,9	+6,8
Informacinių sistemų užvaldymas	2 290	2 962	2 775	+21,2	-6,3
El. paslaugų trikdymas	36	12	7	-80,6	-41,7
El. duomenų klastojimas	147	340	376	+155,8	+10,6
Vientisumo pažeidimai	11	2	7	-36,4	+133,3
Įrenginių saugumo spragos	4 417	5 848	5 905	+33,7	+1
Įvairaus pobūdžio	1 559	2 899	1 672	+7,2	-42,3
Iš viso	10 991	14 643	13 530	+23,1	-7,6

1 pav. 2017 m. II ketvirtį CERT-LT tirtų incidentų diagrama (proc. nuo 100)