2017 METŲ III 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. III ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 13 281 pranešimą apie incidentus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2016 m. III ketv. (12 563 incidentai), incidentų padaugėjo 5,7 procento. Palyginti su 2017 m. II ketvirčiu (13 530 incidentai), incidentų sumažėjo 1,8 procento.**

9,5 proc. pranešimų apie incidentus (arba 1 255) buvo detaliai tiriami CERT-LT specialistų. Daugiausia tai – svetainių klastojimo atvejai, paslaugų trikdymo atakos bei kiti išskirtiniai atvejai, įskaitant incidentus, apie kuriuos pranešta 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.

Apie penktadalį visų incidentų (arba 2 898 pranešimai) sudarė kenkimo programinė įranga: virusai (įskaitant išpirkos reikalaujančius „*ransomware*“), Trojos arkliai ir pan. Dažnai kenkimo programinė įranga buvo platinama brukalu. Piktavaliai el. laiške „informuoja“ apie neva gautą sąskaitą ir siekia, kad asmuo paleistų kelių KB dydžio priedą (kuris dažniausiai būna ZIP, 7Z arba RAR formato). Tokio archyvo viduje būna kitas failas (VBS arba JS plėtinio), kurį paleidus, vyksta pagrindinio kenkimo kodo siuntimas į naudotojo kompiuterį.

Susijusių incidentų – informacinių sistemų užvaldymų – skaičius pakito nežymiai: jų buvo 2 704. Buvo užfiksuoti 2 išskirtiniai atvejai, kai svetainės be jas valdančių žmonių žinios buvo išnaudotos ne kenkimo kodo platinimui, o kriptovaliutos gavybai (angl. *mining*). Interneto naudotojas apsilanko svetainėje, kurioje yra „JavaScript“ kalba parašyta komandų seka (skriptas), ir jam nežinant jo kompiuterio procesorius pradeda vykdyti intensyvius skaičiavimus. Skaičiavimų metu išgaunama kriptovaliuta patenka į skaitmeninę piniginę ir persiunčiama kitiems asmenims, o naudotojui apkraunamas įrenginio procesorius, dėl ko sulėtėja kompiuterio ar kito įrenginio veikimas.

Fiksuoti 6 464 incidentai, susiję su tinklo įrenginiais, įskaitant ir daiktų interneto (angl. „Internet of Things“). Spragų turintys tokie įrenginiai vėliau gali būti įtraukti į botnetus (pvz., „Mirai“) arba išnaudoti kitai kenkimo veikai vykdyti.

Svetainių klastojimų buvo 257, t. y. 68 proc. daugiau nei prieš metus, bet trečdaliu mažiau nei užfiksuota 2017 m. II ketvirtyje. Kaip ir anksčiau, piktavaliai daugiausia klastojo socialinio tinklo svetainę *facebook.com*, el. pašto sistemas (*gmail.com*, *yahoo.com*), el. atsiskaitymų svetainę *paypal.com*, failų talpyklą *dropbox.com*, kartais – užsienio bankų svetaines ir užsienio el. parduotuves. Liepos pradžioje ir rugsėjo viduryje stebėtas Lietuvoje veikiančių

bankų svetainių klastočių „pliūpsnis“. Svarbu paminėti, kad nuorodos į klastotas svetaines buvo platinamos ir trumposiomis žinutėmis.

Šį ketvirtį ir toliau plito tikslinės klastotės, angliškai vadinamos „C-level fraud“. Tokiais atvejais piktavaliai pasirenka įmonę, nustato joje sprendimus priimančius asmenis. Vėliau darbuotojams, galintiems daryti piniginius pavedimus, jie siunčia el. laiškus, kuriuose prisistato įmonės vadovu ir paprašo atlikti „skubų pavedimą“.

Lentelėje ir diagramoje pateikiame incidentų suvestines. Visos CERT-LT apdorotų incidentų ataskaitos pateikiamos mūsų svetainės statistikos skiltyje. CERT-LT skelbia įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas socialiniame tinkle „Twitter“. Surikiuotos pagal temą kibernetinio saugumo rekomendacijos pateikiamos čia.

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

Incidentų tipas	**Incidentų skaičius**			**Pokytis, proc.**	
	2016 III	**2017 II**	**2017 III**	**2017 III / 2016 III**	**2017 III / 2017 II**
Kenkimo programinė įranga	2 805	2 755	2 898	+3,3	+5,2
Informacinių sistemų užvaldymas	2 383	2 775	2 704	+13,5	–2,6
El. paslaugų trikdymas	11	7	11	0	+57,1
El. duomenų klastojimas	153	376	257	+68	–31,6
Vientisumo pažeidimai	3	7	4	+33,3	–42,9
Įrenginių saugumo spragos	5 309	5 905	6 464	+21,8	+9,5
Įvairaus pobūdžio	1 899	1 672	943	–50,3	–43,6
Iš viso	12 563	13 530	13 281	+5,7	–1,8

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