2017 METŲ I 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. I ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 14 643 pranešimus apie incidentus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų.** Pažymėtina, kad 20 proc. pranešimų apie incidentus (arba 2 968) buvo detaliai tiriami CERT-LT specialistų. Daugiausia tai – informacinių sistemų užvaldymai, paslaugų trikdymo atakos bei kiti išskirtiniai atvejai, taip pat – visų tipų incidentai, apie kuriuos pranešta CERT-LT interneto svetainėje (www.cert.lt/pranesti.html) užpildžius specialią formą arba elektroniniu paštu. Likusioji pranešimų apie incidentus dalis apdorota automatiniu būdu su CERT-LT specialiai sukurtais programiniais įrankiais, perduodant informaciją apie incidentą bei rekomendacijas paslaugų teikėjams, kuriems priklauso su incidentu susiję IP adresai. Palyginti su 2016 m. I ketv. (12 035 incidentai), incidentų padaugėjo 21,7 procento. Palyginti su 2016 m. IV ketvirčiu (13 874 incidentai), incidentų padaugėjo 5,5 procento.

Kaip ir anksčiau, kenkimo programinė įranga, įrenginių saugumo spragos ir informacinių sistemų užvaldymai kartu sudaro maždaug 3 ketvirtadalius visų incidentų. 40 procentų visų incidentų buvo susiję su tinklo įrenginiais, įskaitant ir daiktų interneto (angl. „*Internet of Things*“), turinčiais saugumo spragų – 5 848. 17,6 procento visų incidentų (arba 2 580 pranešimų) sudarė kenkimo programinė įranga: virusai (įskaitant išpirkos reikalaujančius „*ransomware*“), Trojos arkliai ir pan. – 2 580 atvejų. Informacinių sistemų užvaldymų skaičius, augęs kelis ketvirčius, stabilizavosi ties 2 962: jų buvo 2,1 proc. daugiau nei prieš metus. 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 klastojimo incidentų skaičius smarkiai šoktelėjo į viršų: jų buvo net 340. 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. Sausio mėn. stebėtas Lietuvoje veikiančių bankų svetainių klastočių „pliūpsnis“. Užfiksuoti 2 vientisumo pažeidimai ir 12 elektroninių paslaugų trikdymo atvejų.

Kiti ketvirčio įvykiai ir tendencijos (taip pat žr. https://www.cert.lt/naujienos.html):

1) CERT-LT duomenimis, sumažėjo tinklo įrenginių, esančių Lietuvoje ir įtrauktų į didžiulį pasaulinį botnetą „*Mirai*“. 2016 m. pabaigoje užkrėstų įrenginių (unikalių IP adresų) buvo beveik 150, o 2017 m. I ketv. pabaigoje – apie 90. Naudodami šį botnetą, piktavaliai vykdo itin galingas paslaugos trikdymo atakas.

2) Buvo atakuoti tūkstančiai „MongoDB“ valdytojų. „MongoDB“ yra duomenų bazių valdymo sistema, naudojama saugant didelius duomenų masyvus. Dėl neteisingo konfigūravimo tokios sistemos būna prieinamos iš išorės (iš interneto) ir pažeidžiamos. Piktavaliai, suradę pažeidžiamas „MongoDB“ duombazes, automatizuotu būdu jas užvaldydavo ir užšifruodavo duomenis. Ketvirčio pabaigoje pažeidžiamų „MongoDB“ duombazių pasaulyje buvo beveik 28 000, Lietuvoje – apie 50.

3) Plito suklastotos žinutės iš neva Valstybinės mokesčių inspekcijos atstovų. Žinutėje-klastotėje buvo pateikiamas gramatiškai netaisyklingas tekstas ir nuoroda į suklastotą interneto svetainę, kurioje buvo prašoma suvesti asmeninius duomenis.

4) Piktavaliai vėl vykdė kibernetinio sukčiavimo kampanijas, apsimesdami įmonės direktoriumi ir el. paštu prašydami tos įmonės buhalterio „greitai apmokėti sąskaitą“. CERT-LT ragina įmonių finansininkus būti budriems ir atidžiai nagrinėti tokius „prašymus“.

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.

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

Incidentų tipas	**Incidentų skaičius**			**Pokytis, proc.**	
	2016 I	**2016 IV**	**2017 I**	**2017 I / 2016 I**	**2017 I / 2016 IV**
Kenkimo programinė įranga	2 887	2 989	2 580	-10,6	-13,7
Informacinių sistemų užvaldymas	2 902	3 098	2 962	+2,1	-4,4
El. paslaugų trikdymas	10	4	12	+20	+200
El. duomenų klastojimas	112	143	340	+203,6	+137,8
Vientisumo pažeidimai	6	1	2	-66,7	+100
Įrenginių saugumo spragos	4 963	5 801	5 848	+17,8	+0,8
Neteisėtas elektroninių duomenų naudojimas	1	0	0	-100	n/d
Įvairaus pobūdžio	1 154	1 838	2 899	+151,2	+57,7
Iš viso	12 035	13 874	14 643	+21,7	+5,5

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