2016 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 2016 m. II ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 10 991 incidentą pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus.** Pažymėtina, kad 17 proc. visų incidentų buvo detaliai tiriami CERT-LT specialistų, įskaitant paskirstyto paslaugos trikdymo (angl. *Distributed Denial of Service*, *DDoS*) atakas, informacinių sistemų užvaldymo ir kitokius išskirtinius incidentus, taip pat incidentus, apie kuriuos pranešta CERT-LT interneto svetainėje užpildžius specialią formą (www.cert.lt/pranesti.html) arba elektroniniu paštu. Likusioji incidentų dalis yra apdorojama automatiniu būdu, perduodant informaciją apie incidentą bei rekomendacijas paslaugų teikėjams, kuriems priklauso su incidentu susiję IP adresai. Palyginti su 2015 m. II ketv. (9 527 incidentai), incidentų padaugėjo 15,4 procento. Palyginti su 2016 m. I ketvirčiu (12 035 incidentai), incidentų sumažėjo 8,7 procento.

Dviejų pagrindinių incidentų tipų procentinės dalys nuo bendro incidentų skaičiaus mažai keitėsi. 40 procentų visų incidentų buvo susiję su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų – 4 417. Beveik ketvirtadalį visų incidentų sudarė kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 2 531 atvejis. Tačiau informacinių sistemų užvaldymų (2 290) ir elektroninių duomenų klastojimų (147) skaičius auga ne pirmą ketvirtį: abiejų tipų incidentų buvo kone 80 proc. daugiau nei prieš metus. CERT-LT tyrimų duomenys rodo, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis ir susiję su pažeidžiama įranga internete. Kaip ir anksčiau, daugiausia buvo klastojamos socialinio tinklo svetainė *facebook.com*, el. pašto sistemos (*gmail.com*, *yahoo.com*), el. atsiskaitymų svetainė *paypal.com*, kai kada – užsienio bankų svetainės.

Žymiai padaugėjo elektroninių paslaugų trikdymo atvejų – 36. Aptariamojo ketvirčio balandžio ir gegužės mėn. vyko nuolatinės paslaugų trikdymų atakos (DDoS), nukreiptos prieš Lietuvos Respublikos institucijų, žiniasklaidos, bankų ir privačiojo sektoriaus svetaines. Šių atakų metu piktavaliai naudojo įvairius atakų būdus, apsunkindami svetainių administratorių gynybą ir šių atakų valdymą. CERT-LT atkreipia dėmesį, kad šiuolaikinės kibernetinės atakos yra sudėtingos ir skiriasi pagal naudojamus atakų metodus, todėl yra naudojamos skirtingos kibernetinių incidentų valdymo priemonės. Dauguma šiuolaikinėse atakose naudojamų metodų neleidžia nustatyti tikrojo atakos šaltinio. Atakų vykdytojai naudoja IP adresų klastojimo technologijas (angl. *spoofing*), todėl iš sukauptos tarnybinių įrašų informacijos ne visada pavyksta nustatyti tikruosius IP adresus, taip pat išlieka klaidos tikimybė ir dideli vėlinimai stabdant atakas. Efektyvi gynyba nuo tokių atakų įmanoma tik lanksčiai derinant kibernetinių incidentų valdymo metodus tiek su turinio prieglobos, tiek su interneto paslaugų teikėjais, tiek su informacinių sistemų valdytojais.

Kiti gauti ir tirti pranešimai:

1) apie neteisėtą elektroninių duomenų naudojimą – 0;

2) apie vientisumo pažeidimą – 11;

3) įvairaus pobūdžio – 1 559.

Kiti įvykiai:

1) Nuo pirmo šių metų ketvirčio tęsiasi brukalo su „JavaScript“ kenkimo kodu plitimas. Šio kenkimo kodo paskirtis – užmegzti ryšį su vienu arba keliais nutolusiais kompiuteriais (kontroleriais), iš jų į aukos įrenginį atsiųsti kenkimo kodą ir jį paleisti. Atsiųstas kenkimo kodas – išpirkos reikalaujantis (angl. *ransomware*) virusas, aukos kompiuteryje užšifruojantis kone visą svarbią informaciją. Tokį brukalą atpažinti nesunku: labai mažas (keli KB) ZIP formato priedas. Laiškų antraštės paprastai yra angliškos, dviejų tipų: apie neva gautą sąskaitą ir apie neva skenuotą dokumentą.

2) Nustatyta tūkstančiai svetainių, kuriose veikianti populiariosios turinio valdymo sistemos „Wordpress“ funkcija „pingback“ buvo netinkamai sukonfigūruota. Ši funkcija leido piktavaliams, turintiems nesaugių „Wordpress“ svetainių sąrašą, kurti didelį dirbtinį „pingback“ srautą ir naudoti jį paslaugos trikdymo atakose prieš pasirinktą svetainę.

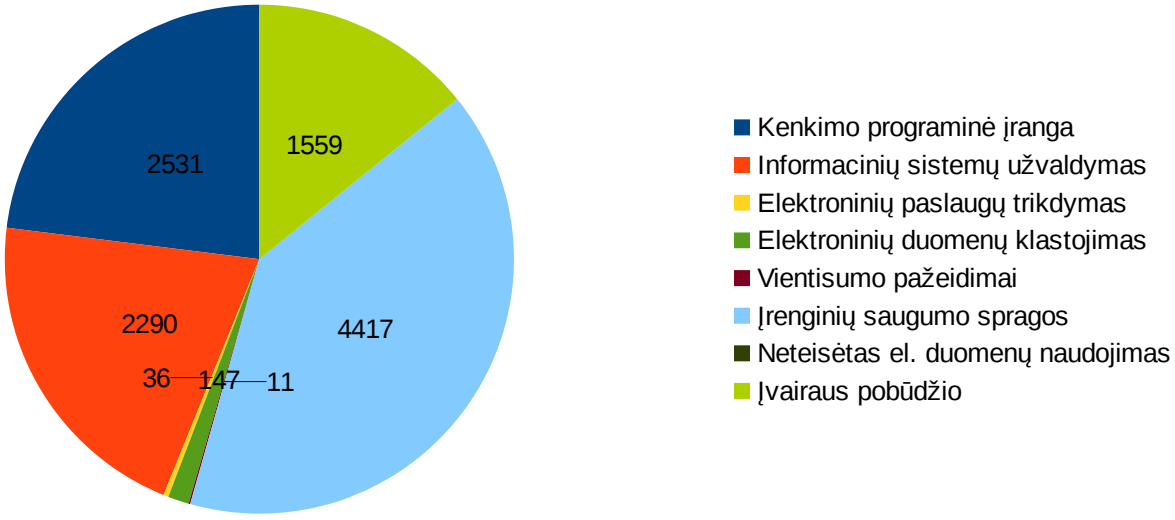
Lentelėse ir diagramoje pateikiame incidentų suvestines. Visas CERT-LT apdorotų incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.html. CERT-LT skelbia įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas socialiniame tinkle „Twitter“.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

1 lentelė. CERT-LT 2016 m. II ketv. apdorotų incidentų suvestinė

Incidentų tipas	Incidentų skaičius	Procentinė dalis nuo visų
Kenkimo programinė įranga	2 531	23
Informacinių sistemų užvaldymas	2 290	20,8
Elektroninių paslaugų trikdymas	36	0,3
Elektroninių duomenų klastojimas	147	1,3
Vientisumo pažeidimai	11	0,1
Įrenginių saugumo spragos	4 417	40,2
Neteisėtas el. duomenų naudojimas	0	0
Įvairaus pobūdžio	1 559	14,2

2 lentelė. CERT-LT 2015 m. II ketv., 2016 m. I ir 2016 m. II ketv. apdorotų incidentų skaičiaus palyginimas

Incidentų tipas	Incidentų skaičius		Pokytis, proc.	
	2016 I	2015 II	2016 II / 2016 I	2016 II / 2015 II
Kenkimo programinė įranga	2 887	2 579	–12,3	–1,9
Informacinių sistemų užvaldymas	2 902	1 278	–21,1	79,2
El. paslaugų trikdymas	10	14	260	157,1
El. duomenų klastojimas	112	83	31,3	77,1
Vientisumo pažeidimai	6	2	83,3	450
Įrenginių saugumo spragos	4 963	4 698	–11	–6
Neteisėtas el. duomenų naudojimas	2	8	–100	–100
Įvairaus pobūdžio	1 154	865	35,1	80,2



1 pav. 2016 m. II ketvirtį CERT-LT tirtų incidentų statistika