Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2017

2017. gada 4. ceturksnis (01.10.2017. – 31.12.2017.)

Pārskatā iekļauta vispārpieejama informācija, tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Saturs

Kopsavilkums

Pārskata periodā iezīmējās jauna tendence. Virkne incidentu bija saistīti ar dažādām kriptovalūtām. Dažos incidentos tika konstatēta neautorizēta resursu izmantošana kriptovalūtu ģenerēšanai, bet vairāki incidenti bija saistīti ar finansiāliem zaudējumiem no 3000 līdz 34 000 eiro apmērā, kas radušies no uzbrukumiem lietotāju kriptovalūtas kontiem.

Tika saņemti arī vairāki ziņojumi par uzņēmumu e-pasta sarakstes pārtveršanu, kurās pārtvērēji sekoja uzņēmuma sarakstei un veica tās modifikāciju, lai no uzņēmuma partneriem izkrāptu maksājumus uz pārtvērējiem piederošiem banku kontiem.

Pirmssvētku periodā raksturīgi bija arī ziņojumi par krāpnieciskiem interneta veikaliem. Lietotāji lūdza palīdzību gan līdzekļu atgūšanā, kad bija kļuvuši par krāpniecības upuri, gan padomus krāpniecisku vietņu atpazīšanā, lai iepirkumus veiktu droši.

Oktobris jau sesto gadu bija Eiropas Kiberdrošības mēnesis. Latvijā Kiberdrošības mēnesi ievadīja CERT.LV un ISACA Latvijas nodaļas rīkotā starptautiskā kiberdrošības konference „Kiberšahs 2017". Konferenci klātienē apmeklēja 512 dalībnieki, bet tiešraidē vēroja vairāk nekā 3000 interesenti.

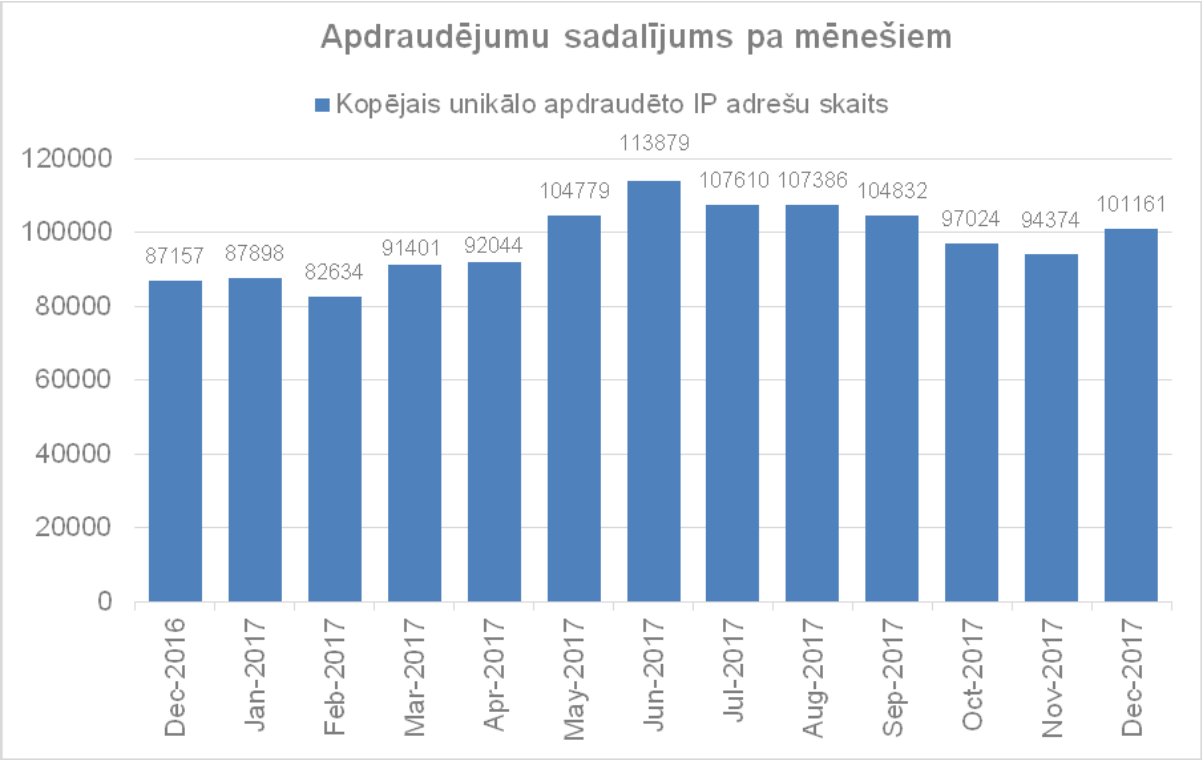
2017.gada 4.ceturksnī CERT.LV apkopoja informāciju par 192 284 apdraudētām IP adresēm. Pārskata periodā izplatītākais apdraudējums bija konfigurācijas nepilnības (137 805 unikālas IP adreses) ar kritumu 2.5%, salīdzinot ar iepriekšējo ceturksni. Nākamais izplatītākais apdraudējums bija ļaundabīgs kods (40 629 unikālas IP adreses) ar kritumu 29%. Trešo vietu ieņēma ielaušanās mēģinājumi (206 unikālas IP adreses) ar pieaugumu 13% attiecībā pret iepriekšējo ceturksni.

Pārskata periodā CERT.LV par IT drošību izglītoja 2458 cilvēkus, iesaistoties 37 izglītojošos pasākumos, ievietoja 16 jaunas ziņas vietnē www.cert.lv, sniedza komentārus 7 radio pārraidēs un 5 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, no 2017. gada 1. janvāra apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Turpmāk statistikā visi CERT.LV reģistrētie apdraudējumi tiks uzskaitīt vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, *Confiker*, *Zeus*, *Mirai*) un ievainojamību (piemēram, *Opendns*, *Openrdp*) tipiem.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 90 000 – 100 000 ievainojamu unikālu IP adrešu.

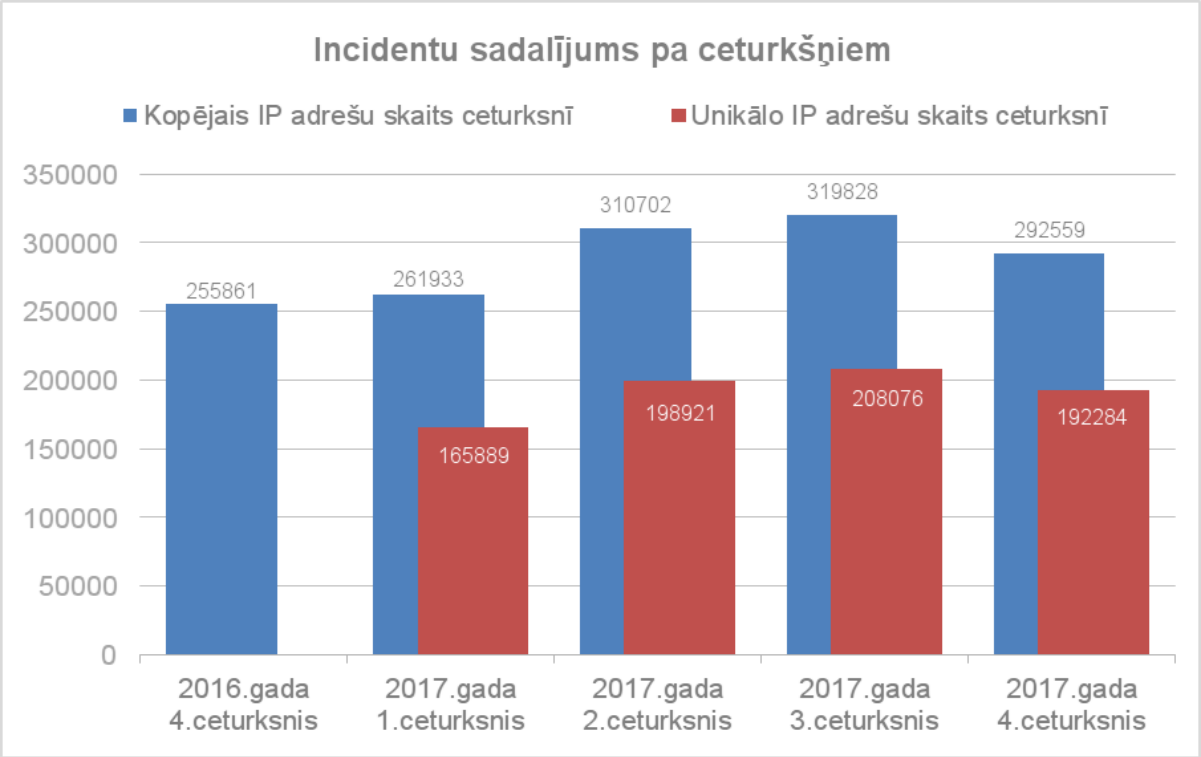


1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā.

Līdz 2016. gada beigām CERT.LV apkopoja informāciju par ceturksnī apdraudētajām IP adresēm, summējot katrā mēnesī apdraudētās IP adreses (2. attēls – zilie stabiņi). No 2017. gada janvāra CERT.LV veic uzskaiti pa unikālām IP adresēm ceturksnī, novēršot to, ka viena un tā pati IP adrese tiek pieskaitīta vairākas reizes (2. attēls – sarkanie stabiņi).

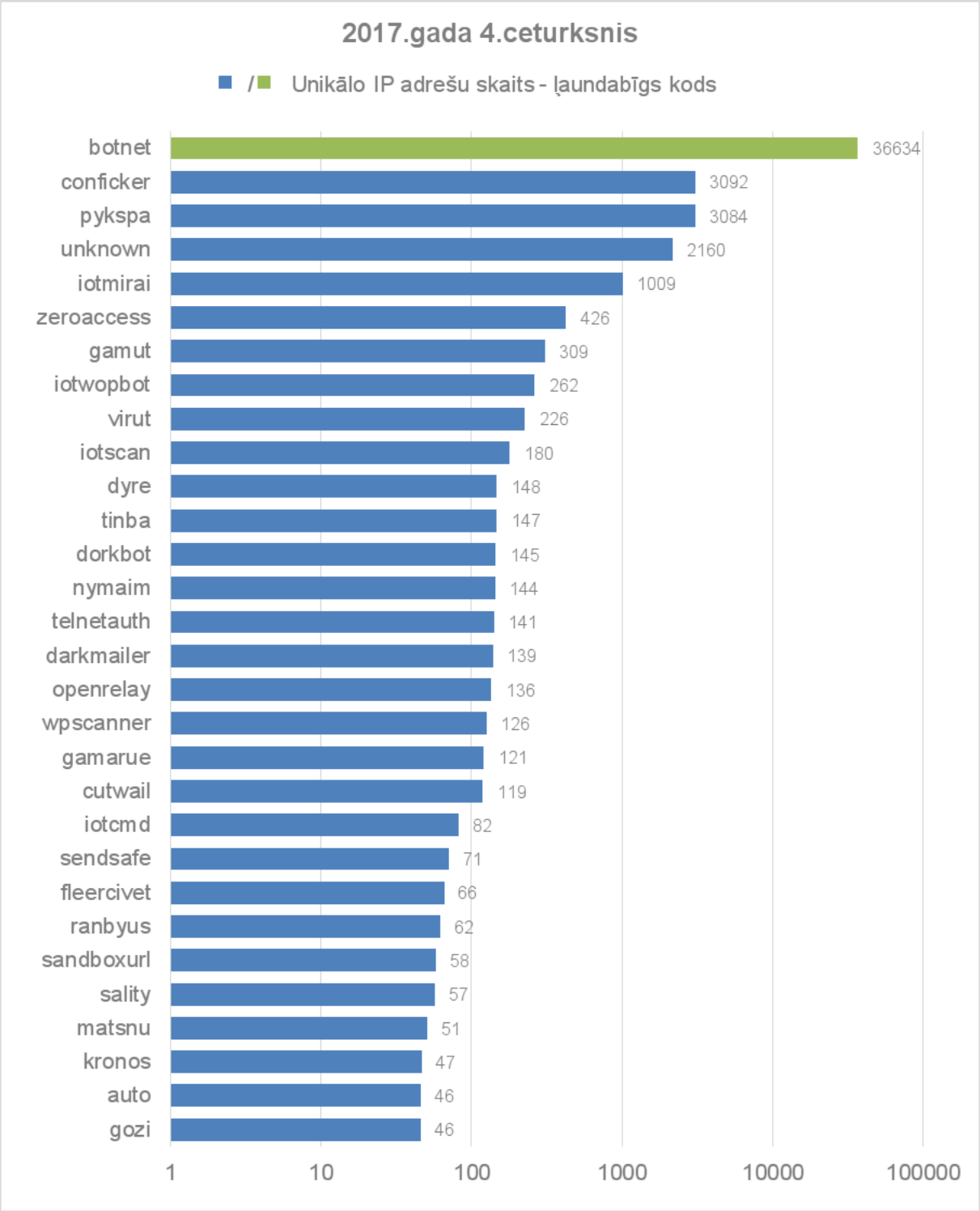
2017. gada 4. ceturksnī tika reģistrētas 192 284 unikālas apdraudētas IP adreses (izmantojot iepriekšējo metodi, tās būtu 292 559 IP adreses). Skaita atšķirība norāda uz to, ka vienas un tās pašas adreses tiek reģistrētas kā apdraudētas vairāku mēnešu garumā, jo apdraudējums netiek ilgstoši novērsts vai atkārtojas.



2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2016. un 2017. gadā.

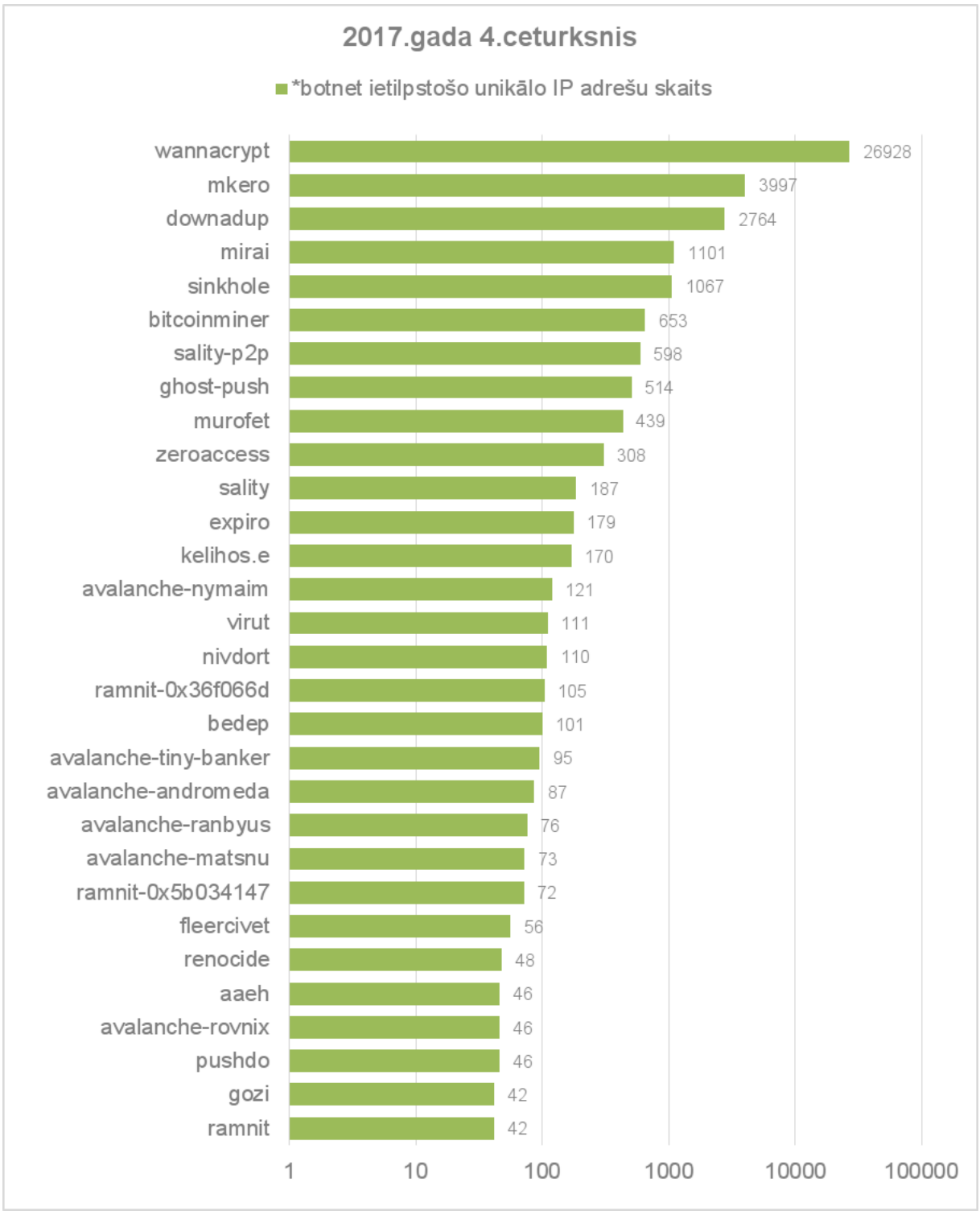
3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 4. ceturksnī pa apdraudējumu veidiem.

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais - ielaušanās mēģinājumi.



4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 4. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

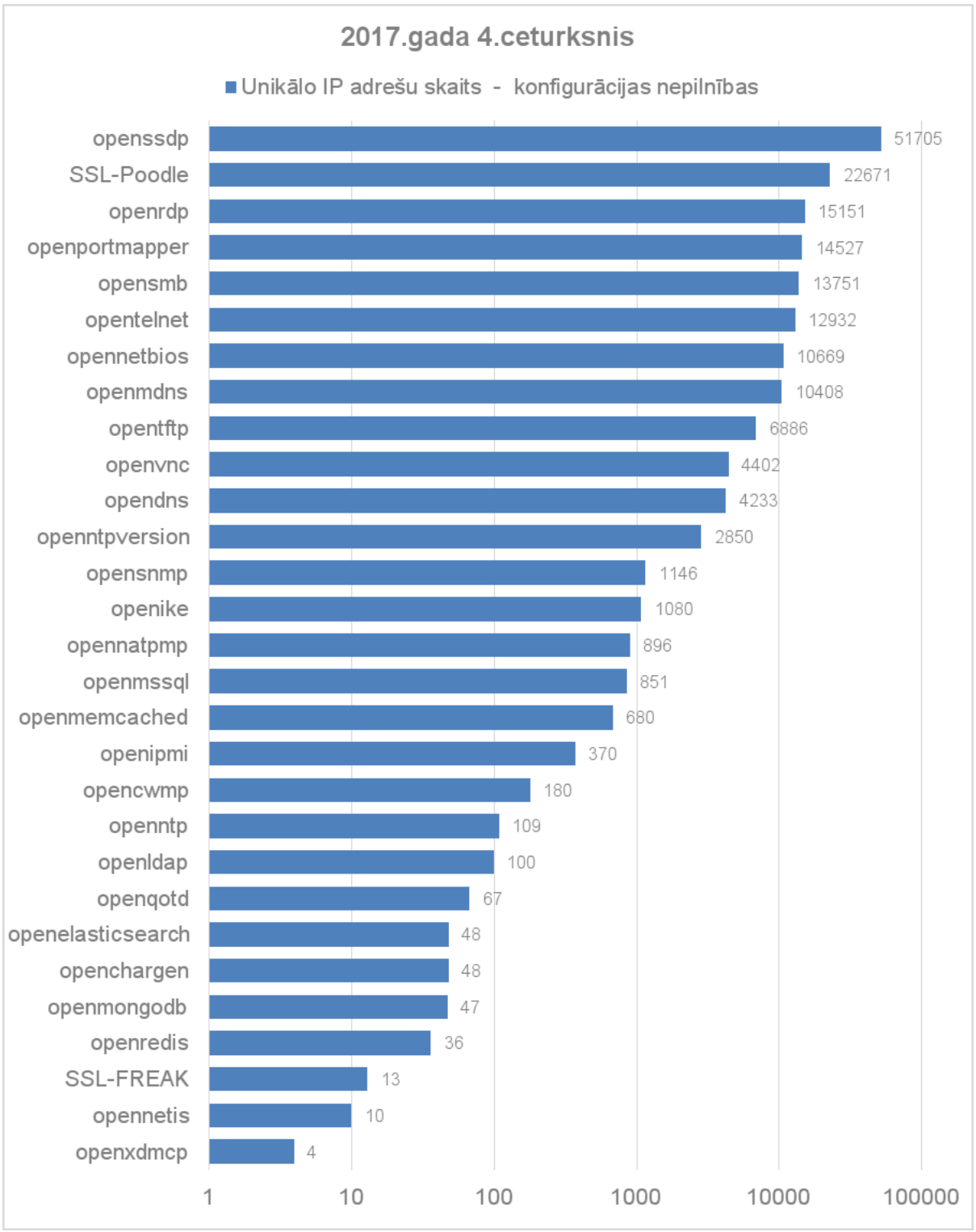
Pirmo vietu ļaunatūras izplatības topā šajā ceturksnī stabili ieņem *botnet* ļaundabīgā koda grupa; tās detalizēts atšifrējums redzams 4.1.grafikā.



4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 4. ceturksnī ar apdraudējuma veidu - Ļaundabīgs kods.

4.1. attēls parāda, ka augsti izplatības rādītāji joprojām ir ļaunatūrai *WannaCry* jeb *WannaCrypt*. Arī šajā ceturksnī otro vietu ļaunatūras izplatības topā ieņēma *MKero Android* trojānis, kas spēj apiet *CAPCHA* autentifikācijas sistēmu un, lietotājam nezinot, veic lietotāja parakstīšanos uz dažādiem maksas servisiem.

Vietu ļaunatūras topa augšgalā nemainīgi saglabā *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Opensmb, kas 2. ceturksnī konfigurācijas nepilnību topā bija jaunpienācēja, no sestās vietas pakāpusies uz piekto. Šī diezgan plaši izplatītā konfigurācijas nepilnība bija vainojama tādu šifrējošo izspiedējvīrusu kā *WannaCry* un *NotPetya* straujajā izplatībā.

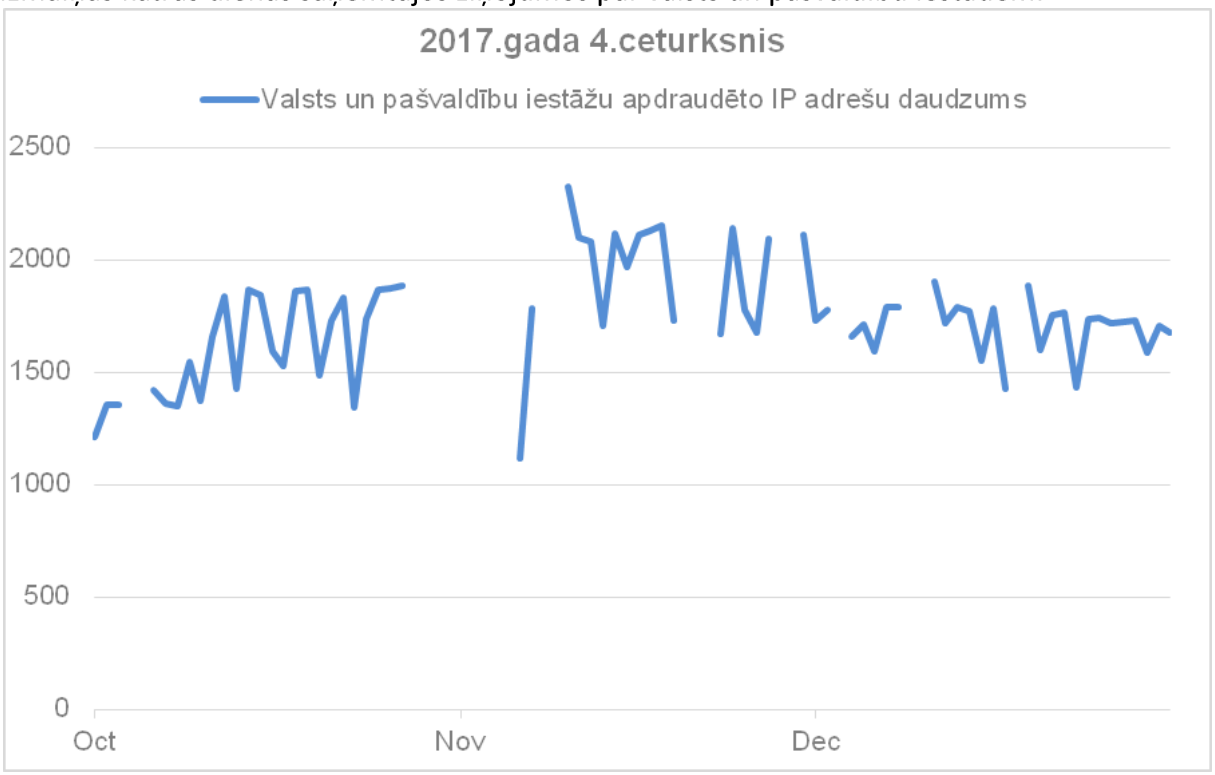
Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar interneta pakalpojumu sniedzējiem (IPS), kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus klientus par to iekārtās

konstatētajiem apdraudējumiem. Atbildīgo IPS kopskaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

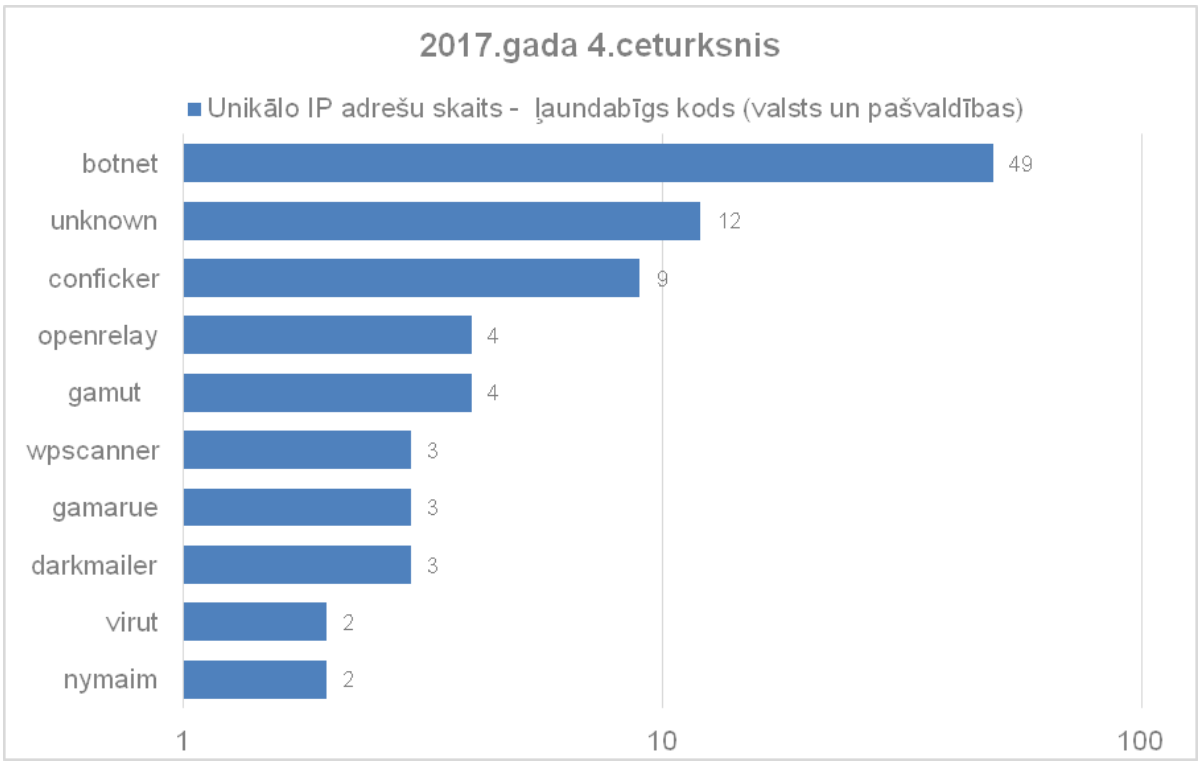
CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā apdraudētas.

Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

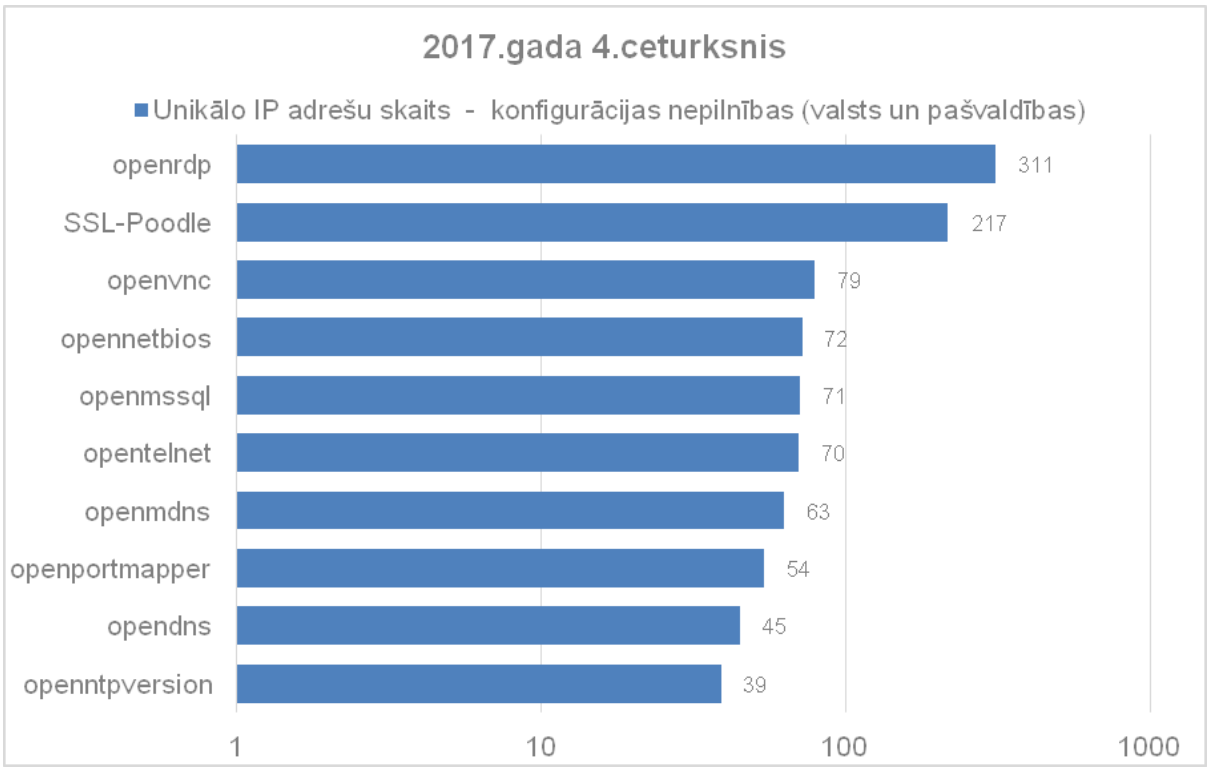


6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2017. gada 4. ceturksnī.

Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 1500 unikālas IP adreses dienā. Būtiskas izmaiņas šajos datos pārskata periodā nebija novērojamas.



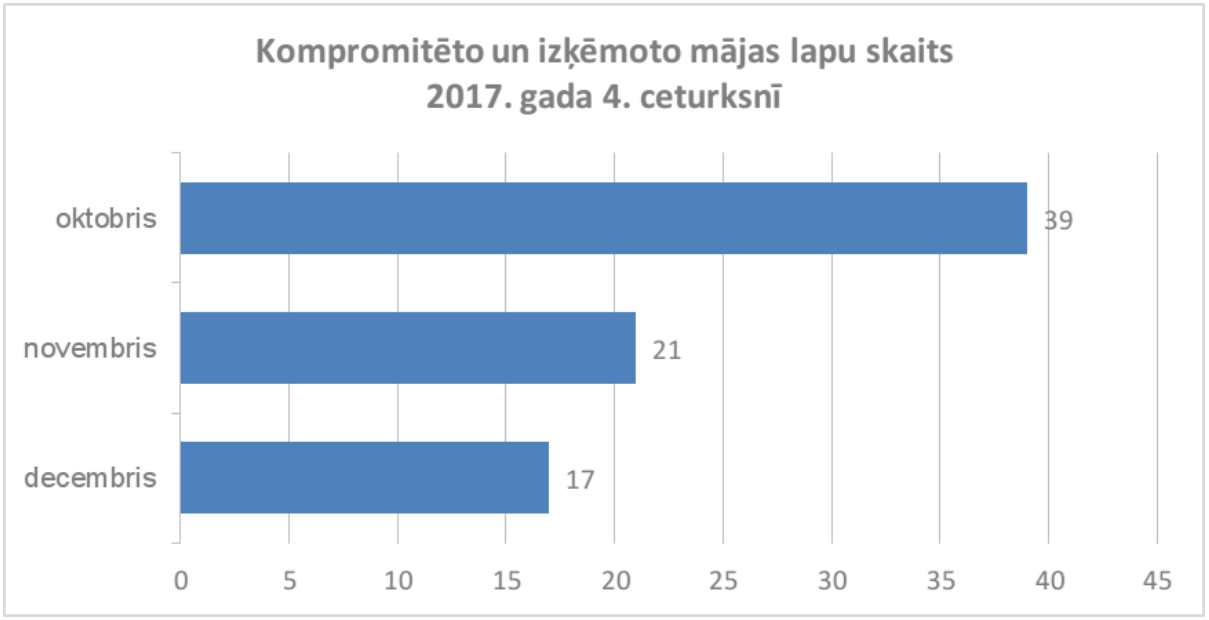
7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 4. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods (TOP 10 ļaundabīgs kods).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10 konfigurācijas nepilnības).

Salīdzinoši lielais konfigurācijas nepilnību apjoms ir tādēļ, ka vienā ievainojamā IP adresē bieži vien ir sastopami vairāki apdraudējumi – vienā iekārtā vienlaicīgi esošas dažādas konfigurācijas nepilnības.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 79 kompromitētas un izķēmotas tīmekļa vietnes. No visām izķēmotajām vietnēm 77 gadījumos vietnes uzturēšanai tika izmantota Linux operētājsistēma, 2 gadījumos Windows. Divpadsmit no visām pārskata periodā izķēmotajām tīmekļa vietnēm pēdējā gada laikā izķēmotas atkārtoti.



9.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2017. gada 4. ceturksnī.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā.

Svarīgākie CERT.LV risinātie drošības incidenti pārskata periodā:

- 03.10. Tika saņemts lūgums no kādas valsts iestādes veikt tai piederošas tīmekļa vietnes testēšanu. Testēšana tika veikta, un kritiskas ievainojamības vietnē netika konstatētas. Vietnes uzturētājiem tika nosūtīts ieteikums ierobežot piekļuvi no interneta vietnes administrācijas panelim un datņu sarakstam, lai mazinātu vietnes potenciālo apdraudējumu.
- 06.10. No kādas pašvaldības iestādes tika saņemts ziņojums par problēmu ar vienu no serveriem, uz kura esošās datnes ir tikušas sašifrētas. Sašifrēto datņu paplašinājums bija .needdecrypt. CERT.LV konstatēja, ka tas ir šifrējošais izspiedējvīruss *Globelmposter*, un ieteica izmantot vietnē nomoreransom.org pieejamo atbilstošo atšifrēšanas rīku.
- 07.10. Tika saņemta ziņa no kāda lietotāja, kurš bija cietis krāpniecībā. Paļaujoties uz reklāmu sociālajā tīklā *Facebook*, lietotājs bija veicis pasūtījumu reklamētajā tīmekļa vietnē, veicot apmaksu 130 eiro apmērā ar bankas karti. Tīmekļa vietne piedāvāja izveidot savu profilu, ievadot dažādus personas datus, lai nodrošinātu iespēju izsekot preces piegādei. Pēc mēnesi ilgas gaidīšanas profila statusā parādījās informācija, ka prece esot piegādāta "līdz durvīm", kaut arī lietotājs nekādu preci nesaņēma. Lietotājs saprata, ka ir "iekritis" uz pievilcīgi zemo cenu un ir ticis apkrāpts. CERT.LV ieteica uzrakstīt iesniegumu policijā un pārbaudīt bankas kartes maksājumu vēsturi, vai ar to nav veikti maksājumi no ārzemju IP adresēm, kā arī veikt bankas kartes nomaiņu, lai novērstu tās ļaunprātīgas izmantošanas iespējas. Turpmākiem

pirkumiem CERT.LV ieteica izmantot arī tīmekļa vietni scamadviser.com, kurā pārbaudīt izvēlētā interneta veikala uzticamību, kā arī nepaļauties uz SSL sertifikāta esamību, kas nodrošina datu šifrētu pārraidi, bet neapliecina pārdevēju godprātīgumu.

- 10.10. Tika saņemti vairāki ziņojumi par ļaunatūru reklāmas baneros vienā no Latvijas interneta ziņu portāliem. Izpētes rezultātā tika konstatēts, ka vietnē izvietotie reklāmas baneri satur ļaundabīgu kodu, kas ģenerē kriprovalūtu, noslogojot apmeklētāju datorus. Vietnes uzturētāji tika informēti un aicināti izņemt ļaundabīgo kodu no reklāmas baneru sistēmas. Baneru sistēma tika salabota.
- 10.10. Tika saņemts ziņojums par 87 IP adresēm, kuras tika izmantotas piekļuves atteices (DDoS) uzbrukumā. Šajās adresēs tika konstatēta *OpenResolver* konfigurācijas nepilnība, par kuru tika brīdināti atbilstošie resursu turētāji. Uz pārskata perioda beigām problēma bija novērsta 12 adresēs no 87.
- 13.10. Tika saņemta informācija no kādas valsts iestādes par uzbrukumu tās e-pasta serverim. Uzbrukums ilga no 12.10. vakarpuses līdz 13.10. agram rītam. Ugunssienas risinājums visus kaitīgos e-pastus bloķēja.
- 14.10. Tika saņemta ziņa no kāda lietotāja par uznirstošu brīdinājumu, ka dators tikko ir ticis inficēts un nepieciešams izmantot papildu rīku datora skenēšanai, lai atklātu un novērstu infekciju. CERT.LV paskaidroja, ka lietotājs, visticamāk, ir apmeklējis inficētu tīmekļa vietni, kura tiek ļaunprātīgi izmantota tālākai ļaunatūru izplatīšanai, iebiedējot apmeklētājus, lai viņi piekrīt programmatūras lejupielādei savā datorā. Lietotājs iebiedēšanai nepakļāvās, un dators inficēts netika.
- 16.10. Tika saņemts ziņojums no kādas valsts iestādes par inficētu e-pasta pielikumu. Iestādes e-pastu filtrs nebija atpazinis kaitīgo sūtījumu. Pielikumā tika konstatēts šifrējošais izspiedējvīruss *Locky*. Lietotājs bija piesardzīgs un pielikumu neatvēra, datnes nošifrētas netika.
- 19.10. Tika saņemta informācija par kādu interneta vietni, kuras darbības lietotājam šķita krāpnieciskas. Pēc pasūtījuma izdarīšanas un apmaksas veikšanas, vietne pieprasījusi lietotājam adreses un pasūtītāja vārda apliecinājumu, nosūtot telefona rēķina kopiju. Rēķina kopija tika nosūtīta. Tam sekoja aizbildinājums par nepietiekamu verifikāciju un tika lūgts nosūtīt arī bankas kartes trīs mēnešu izdruku. CERT.LV ieteica vērsties DVI un rūpīgi apsvērt personīgās informācijas atklāšanas nepieciešamību. Lietotājs pasūtījumu vietnē anulēja.
- 20.10. Tika saņemts ziņojums no kāda lietotāja par krāpniecisku e-pastu it kā Starptautiskā valūtas fonda vārdā par kompensācijām krāpniecību upuriem. E-pasts aicināja nosūtīt vārdu, uzvārdu un pases kopiju, lai ar *Western Union* starpniecību varētu saņemt kompensācijas maksājumu. Lietotājs krāpniecību atpazina un tajā necieta.
- 26.10. Tika saņemta ziņa no kāda lietotāja par aizdomīgu e-pastu no kādas ātro kredītu tīmekļa vietnes. E-pasts informēja par veiksmīgu kredīta pieteikuma formas aizpildīšanu kredīta saņemšanai 900 eiro apmērā, un aicināja apstiprināt kredīta pieprasījumu, kaut arī lietotājs kredītam nebija pieteicies. CERT.LV aicināja sazināties ar kredīta izsniedzējiem un informēt, ka notikusi kļūda vai arī ļaunprātīga darbība, pieprasot kredītu svešā vārdā, kā arī noskaidrot, vai krāpnieciskos nolūkos kompānijai nav iesniegti arī citi šī lietotāja personas dati, un tālāk pieņemt lēmumu, vai rakstīt

iesniegumu policijā.

- 27.10. Tika saņemta ziņa no kāda lietotāja par svešu IP adrešu pieslēgšanos viņa e-pasta kontam. Pēc pārbaužu veikšanas CERT.LV ieteica vērsties ar iesniegumu policijā par korespondences un elektronisko sakaru tīkliem pārraidāmās informācijas noslēpuma pārkāpšanu un nelikumīgām darbībām ar fiziskās personas datiem.
- 08.11. Tika saņemts ziņojums par ievainojamību kādā vietnē. Tika konstatēts, ka vietne padara pieejamu informāciju par uz servera esošo programmatūru, kā arī kļūdu paziņojumos parāda pilnu kļūdas informāciju, kas ļautu potenciālajam uzbrucējam iegūt būtisku informāciju par serveri un veiksmīgāk pielāgot uzbrukumu. CERT.LV ieteica informāciju par programmatūru novākt, bet kļūdu paziņojumos iekļaut tikai identifikatorus, ja tādi nepieciešami kļūdu risināšanai.
- 12.11. Tika saņemts ziņojums no kāda lietotāja, ka no viņa *bitcoin* kriptovalūtas maciņa kādā vietnē ir nozagti 0.52374834 *bitcoin* jeb 2750 eiro. Lietotājs vērsies pēc palīdzības pie vietnes uzturētājiem, bet saņēmis atbildi, ka transakciju atgriezeniskums netiek nodrošināts, pārskaitījums nevar tikt atgriezts, ja saņēmējs nevēlas to atmaksāt atpakaļ. Vietnes uzturētāji bija gatavi sadarboties ar likumsargājošajām iestādēm. CERT.LV ieteica lietotājam vērsties policijā, kā arī veikt datora, no kura veikta piekļuve bitcoin maciņam, pārbaudi uz ļaunatūru.
- 15.11. No kāda lietotāja saņemta ziņa par neautorizētiem lietotāju diskreditējošiem ierakstiem viņa *Facebook* profilā, kā arī ar šo informāciju izveidots pasākums *Facebook*. CERT.LV ieteica pārbaudīt datoru, vai tajā nav vīruss, kā arī izmantot facebook.com/hacked, lai noskaidrotu, vai nav kāda ļaunprātīga aplikācija, kurai ir piešķirtas tiesības publicēt ziņas lietotāja profilā.
- 15.11. Tika saņemts ziņojums par piekļuves atteices (DDoS) uzbrukumu kādai valsts iestādes tīmekļa vietnei. Uzbrukums ilga 23 minūtes. Uzbrukums tika veiksmīgi atvairīts.
- 16.11. Tika saņemts ziņojums no kādas organizācijas par neautorizētu piekļuvi tās tīmekļa vietnes administrācijas panelim. CERT.LV konstatēja paneļa brīvu pieejamību no interneta un ieteica organizācijai piekļuvi panelim ierobežot.
- 21.11. Tika saņemta informācija par kompromitētu tīmekļa vietni, kurā tika izvietots lietotāju datu izkrāpšanai (pikšķerēšanai) paredzēts saturs. Tīmekļa vietnes uzturētāji tika brīdināti, kaitīgais saturs tika dzēsts.
- 22.11. Tika saņemts ziņojums no kādas valsts iestādes par kaitīgu e-pastu ar .iso pielikumu. Tika konstatēts *Kryptik* ļaunatūras iesūtīšanas mēģinājums. Antivīruss pielikuma skenēšanā ļaunatūru atpazina.
- 23.11. Tika saņemts ziņojums par kaitniecisku kodu kādā uzņēmuma tīmekļa vietnē. Tas veica vairākkārtēju secīgu lietotāja pārvirzi uz dažādām reklāmas vietnēm. CERT.LV centās sazināties ar kompromitētās vietnes uzturētājiem un aicināt atjaunot satura vadības sistēmu *WordPress* un tās spraudņus uz jaunāko versiju, taču ar uzturētājiem sazināties neizdevās.
- 23.11. Tika saņemts iesniegums no kādas izglītības iestādes, kas nosūtīts arī Valsts policijai, par iestādes koplietojamā datora kompromitēšanu, kā rezultātā riskam tika pakļauta datora lietotāju personīgā informācija. Uz iesnieguma brīdi visi publiskie datori tikuši atslēgti. CERT.LV sniedza ieteikumus, kā nepieļaut līdzīgu situāciju

nākotnē.

- 27.11. Tika saņemta ziņa no kādas pašvaldības par šifrējošo izspiedējvīrusu *Cryakl* pašvaldību serveros. No vīrusa cieta Windows 2012 R2 un Windows 2008 serveri. Neviena no pašvaldības izmantotajām antivīrusa programmām vīrusu neatpazina, bija aizdomas par inficētu administratora kontu. Saturu izdevās atjaunot no rezerves kopijām.
- 29.11. No kāda uzņēmuma tika saņemts ziņojums par krāpnieciskām darbībām, kas vērstas pret uzņēmumu, izmantojot uzņēmuma e-pasta saraksti. Krāpnieki veikuši vairākas sarakstes ar uzņēmuma ārvalstu klientiem, izmantojot uzņēmuma e-pastu, lai pārliecinātu klientus veikt uzņēmumam pienākošos maksājumus uz viltus bankas kontiem. Krāpnieciskos nolūkos ticis piereģistrēts arī uzņēmumam līdzīga nosaukuma domēns. Uzņēmumam ieteikts nomainīt e-pastu paroles, pārbaudīt datorus uz vīrusiem, pārbaudīt e-pastu filtrus uzturētāja serverī, vai tajos nav pievienoti jauni ieraksti, kas sūta sarakstes kopiju krāpniekiem, kā arī brīdināt sadarbības partnerus. Uzņēmums izpildīja ieteikumus un ieviesa arī e-pastu divpakāpju autentifikāciju.
- 29.11. Tika saņemts ziņojums no kāda lietotāja par iespējamu krāpniecības mēģinājumu. Lietotāja sludinājumam par nekustamā īpašuma pārdošanu atsaucās ārvalstu persona, kas izrādīja vēlmi veikt īpašuma iegādi, un pārdevējam e-pastā nosūtīja it kā maksājuma apstiprinājumu, kas pārvirzīja lietotāju uz datu izkrāpšanai paredzētu vietni. Lietotājam pircēja uzvedība šķita aizdomīga un komunikācija tika pārtraukta.
- 30.11. Tika saņemta ziņa no kāda uzņēmuma par šifrējošā izspiedējvīrusa uzbrukumu lietotāju datnēm. Serveri uzbrukumā necieta. Uzņēmums bija spiests vienoties ar uzbrucējiem, lai iegūtu atšifrēšanas atslēgas un atgūtu datus. CERT.LV ieteica uzņēmumam nākotnē nodrošināt pieslēgšanās iespēju RDP (Remote Desktop Protocol) servisam tikai izmantojot VPN (Virtual Private Network).
- 30.11. Tika saņemta ziņa no kāda uzņēmuma par iejaukšanos biznesa sarakstē un, iespējams, kompromitētu e-pastu. Krāpnieciskie e-pasti tika sūtīti no *Gmail*, izmantojot līdzīgu domēnvārdu. CERT.LV ieteica uzņēmumam izveidot domēna SPF ierakstu, kas liegtu kompānijas vārdā izsūtīt e-pastus no neautorizētiem serveriem, kā arī brīdināt sadarbības partnerus par iespējamu krāpniecisku saraksti.
- 30.11. No kāda uzņēmuma tika saņemta ziņa par serverī konstatētu kriptovalūtas ražošanas procesu, kas neautorizēti tiek palaists no nezināma avota. Ražošanas rezultāti tika sūtīti uz kādu svešu e-pastu, izmantojot 3333 portu. Uz servera atradās vairākas tīmekļa vietnes. Aizdomās tika turēta uz servera esoša tīmekļa vietne ar novecojušu satura vadības sistēmu *Joomla* v1.5, kuru neesot iespējams atjaunināt. CERT.LV ieteica veidus, kā iespējams iegūt izsmeļošāku informāciju par kaitīgo procesu palaišanas mehānismu, kā arī ieteica izolēt potenciāli nedrošo tīmekļa vietni, lai neradītu nevajadzīgu apdraudējumu pārējam servera saturam.
- Novembrī un decembrī no lietotājiem tika saņemti lūgumi palīdzēt noskaidrot, vai tīmekļa vietne ir uzticama? Visos gadījumos CERT.LV norādīja uz neseno domēna reģistrācijas laiku un īso internetveikala pastāvēšanas vēsturi, kas kopā ar neticami zemajām cenām pirmssvētku periodā ir nopietns brīdinājuma signāls par iespējamu krāpšanu. Arī kontaktinformācijas trūkums vietnē ir būtisks pamats neuzticībai, jo nepastāv nekādas iespējas sazināties ar pārdevēju neskaidrību vai problēmu gadījumā. Visi šie aspekti norāda uz augsta riska vietni, kas visticamāk ir krāpnieciska.

- 01.12. Tika saņemts ziņojums no kādas valsts iestādes par darbiniekam iesūtītu e-pastu ar inficētu datni pielikumā. Datne saturēja spiegojošo vīrusu, kurš apkopo datorā ievadītās paroles un citus lietotāju datus, un nosūta tos trešajām pusēm. E-pasts tika atpazīts kā kaitīgs un netika atvērts.
- 04.12. Tika saņemta ziņa no kāda lietotāja par krāpniecisku īsziņu it kā sociālā tīkla konta papildināšanai. Lietotājs veicis pieprasīto konta papildināšanu ar īsziņu un dažu minūšu laikā ar maksas īsziņu palīdzību viņa telefona rēķins par pakalpojumiem pieaudzis vairāku simtu eiro apmērā.
- 06.12. Kāda pašvaldība lūdza veikt padziļinātu drošības pārbaudi tai piederošai tīmekļa vietnei. Pārbaudes rezultātā tika atklāta viena kritiska ievainojamība un četras būtiskas ievainojamības, bet ar vidēja vai zema līmeņa risku. CERT.LV sniedza ieteikumus ievainojamību novēršanai.
- 11.12. Saņemts ziņojums no kādas pašvaldības par krāpniecisku e-pastu pašvaldības grāmatvedei izpilddirektora vārdā ar jautājumu par steidzamu starptautisku bankas pārskaitījumu. E-pasts noformēts ne pārāk labā latviešu valodā ar neatbilstošu *Reply-to* adresi, kas ļāva saņēmējam atpazīt krāpniecību.
- 12.12. Tika saņemts ziņojums no kāda lietotāja par e-pastu, kurā bija aicinājums iepazīties ar ļoti svarīgu pielikumā esošu dokumentu. E-pastam pievienotajā PDF dokumentā tika norādīta saite uz e-pasta piekļuves datu izkrāpšanai paredzētu pikšķerēšanas vietni. Lietotājs tika brīdināts un, tā kā vietnē ievadījis savus datus, aicināts nomainīt e-pasta paroli. Kaitnieciskās vietnes uzturētāji informēti un aicināti vietni aizvērt.
- 15.12. Tika saņemts ziņojums no kāda uzņēmuma par krāpniecisku e-pastu Eiropas Komisijas vārdā par it kā piešķirtu 1,2 miljoni eiro lielu atbalsta grantu, kas tiek piešķirts maziem un vidējiem uzņēmumiem, kā arī akadēmiskajām un zinātniskajām aktivitātēm. E-pastā norādītas leģitīmas saites uz Eiropas Komisijas tīmekļa vietni, bet piekodināts drošības nolūkos turēt e-pasta saņemšanu slepenībā un sazināties rakstiski par tālākām instrukcijām granta saņemšanai. *Reply-to* adrese @ec-europa.eu atšķīrās no leģitīmās @ec.europa.eu. Tā kā uzņēmums papildu finansējumam pieteicies nebija, saņemtais e-pasts tika atpazīts kā krāpniecība.

CERT.LV pasākumi incidentu novēršanā:

- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV sagatavotajās ziņās un sociālā tīkla Twitter kontā (@certlv).

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 6. punktā.

3. Mobilo ierīču ļaunatūras pētniecība.

Mobilā ļaunatūra kļūst arvien aktuālāks apdraudējums. Par to liecina gan CERT.LV saņemtie ziņojumi, gan sabiedrības un mediju interese par mobilo ierīču drošības jautājumiem, gan arvien pieaugošais mobilo ierīču skaits, kas pie CERT.LV speciālistiem nonāk Datorologa akciju laikā.

Tika saņemtas vairākas ziņas par viltus loteriju *AirBaltic* vārdā. Saite uz krāpniecisko vietni tika izplatīta sociālajā tīklā *Facebook*. Lai saņemtu it kā laimētās biļetes, bija jāatzīmē, ka šī ziņa patīk, un jādalās ar ziņu par loteriju ar saviem draugiem.

Tika saņemts ziņojums par iespējams no telefona nopludinātiem adrešu grāmatiņas kontaktiem. Vairākas personas, kuru telefona numurs atradies šajā kontaktu sarakstā, vēlāk saņēmušas zvanu no nezināma numura. Izpētes rezultātā tika konstatēts, ka norādītais nezināmais numurs patiesībā neeksistē, un zvanot, visticamāk, tika viltots jeb *spoofots*. Neviens zvana saņēmējs uz aizdomīgo zvanu neatbildēja.

No kāda lietotāja tika saņemta ziņa par krāpniecisku īsziņu it kā odnoklasniki.ru konta papildināšanai. Lietotājs veicis pieprasīto konta papildināšanu ar īsziņu un dažu minūšu laikā ar maksas īsziņu palīdzību viņa telefona rēķins par pakalpojumiem pieaudzis vairāku simtu eiro apmērā.

CERT.LV saņēma arī ziņojumus par *MKero Android* trojāni, kas, apejot *Google* drošības pasākumus, ar dažādām spēlēm un lietotnēm nokļuva oficiālajā *Google Play*. *MKero* spēj apiet CAPCHA autentifikācijas sistēmu un, nonākot lietotāja ierīcē, veic lietotāja parakstīšanos uz dažādiem maksas servisiem.

4. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību).

Informācija par CERT.LV sadarbību ar medijiem

Pirmssvētku periodā bija vērojama pastiprināta lietotāju saskarsme ar krāpnieciskām tīmekļa vietnēm un krāpnieciskiem e-pastiem. Tas izraisīja arī palielinātu mediju interesi par šiem jautājumiem.

Informācija par CERT.LV tīmekļa vietnēm:

Pārskata periodā vietnē https://www.cert.lv publicētas 16 ziņas. Populārākā bija ziņa par kiberdrošības konferenci "Kiberšahs 2017" ar 3569 unikāliem skatījumiem. Otra populārākā bija ziņa par ievainojamību WPA2 protokolā, kuru skatījuši 2073 unikāli apmeklētāji. Trešā populārākā bija ziņa par IT drošības semināru „Esi drošs" ar 1732 unikāliem skatījumiem. Kopā CERT.LV mājas lapai bijuši 16 932 lapu skatījumi, kurus veido 9 768 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 12 691 apmeklējums, no tiem 9 882 unikāli apmeklējumi. CERT.LV turpina tulkot un portālā www.esidross.lv publicēt OUCH! ikmēneša izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts).

Portālā esidross.lv publicētie raksti:

- Palīdzēt citiem būt drošībā
- Droša tiešsaistes iepirkšanās
- Sargājiet savus lietotāja datus

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1853.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 762.
- CERT.LV draugiem.lv profila http://www.draugiem.lv/certlv sekotāju skaits pārskata perioda beigās bija 73.

5. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

Oktobris jau sesto gadu bija Eiropas Kiberdrošības mēnesis. Latvijā Kiberdrošības mēnesi ievadīja CERT.LV un ISACA Latvijas nodaļas **5. oktobrī** rīkotā starptautiskā kiberdrošības konference „Kiberšahs 2017". Konferenci klātienē apmeklēja 512 dalībnieki, bet tiešraidē vēroja vairāk nekā 3000 interesenti.

12. oktobrī CERT.LV pārstāvis piedalījās *Bite Bizness* rīkotajā tiešsaistes kiberdrošības seminārā uzņēmumiem un ikvienam interesentam, un sniedza prezentāciju par mobilo ierīču un lietu interneta (IoT) drošību. Seminārs notika Eiropas Kiberdrošības mēneša ietvaros.

18. oktobrī CERT.LV pārstāvis piedalījās NetSafe drošāka interneta centra un CERT.LV apvienotajā preses konferencē „Mediju brokastis", kurā Kiberdrošības mēneša ietvaros informēja mediju pārstāvjus par kiberdrošības aktualitātēm.

19. oktobrī Kiberdrošības mēneša ietvaros notika DSS organizētā konference „ITSEC 2017", kurā CERT.LV pārstāvis uzstājās ar prezentāciju „Firmware over the air: Case study of Adups FOTA".

23. oktobrī CERT.LV speciālists prezentēja divas tehnisko pētījumu publikācijas IEEE MILCOM 2017 konferencē, Baltimorā, ASV - " Bbuzz: A Bit-aware Fuzzing Framework for Network Protocol Systematic Reverse Engineering and Analysis" un "Frankenstack: Toward Real-time Red Team Feedback."

25. oktobrī Kiberdrošības mēneša ietvaros norisinājās kārtējā Datorologa akcija, kurā visiem interesentiem bija iespēja bez maksās pārbaudīt savu datoru, planšetdatoru vai mobilo telefonu pie CERT.LV speciālista – datorologa vai saņemt konsultāciju par iekārtas drošību.

30.oktobrī CERT.LV pārstāvis piedalījās Bite organizētajās kiberdrošības brokastīs medijiem un informēja klātesošos par krāpnieciskajiem gadījumiem digitālajā vidē.

1. novembrī CERT.LV pārstāvis piedalījās *Digital Freedom Festival* organizētā diskusijā "Money and cybersecurity".

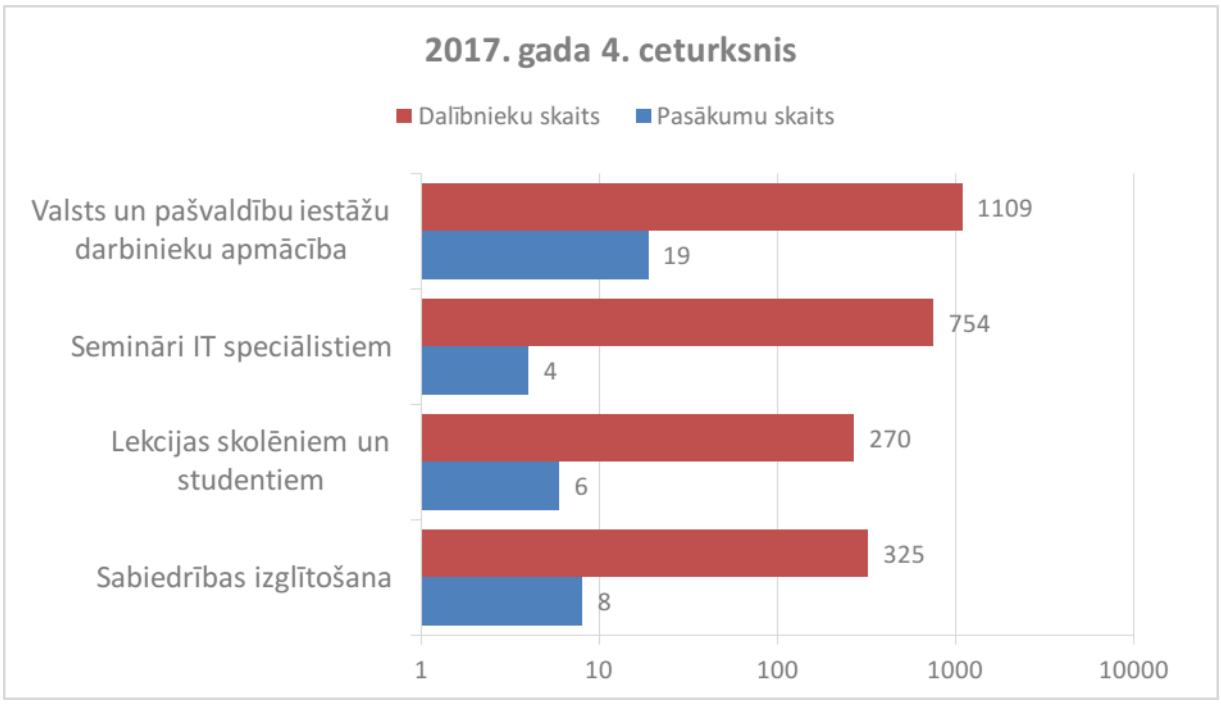
24. novembrī CERT.LV pārstāvis sniedza prezentāciju "IKT drošības apdraudējumu aktualitātes - skats uz privāto sektoru" Tieslietu ministrijas un LU Juridiskās fakultātes rīkotajā konferencē "Komerctiesības un mākslīgais intelekts: qou vadis?".

6. decembrī CERT.LV pārstāvis piedalījās valsts prezidenta rosinātajā diskusijā par viltus ziņām "Latvijas drošība 21. gadsimtā. Viltus ziņas kā sabiedrības viedokļa ietekmes instruments".

13. decembrī ar CERT.LV atbalstu Datorologa akcija norisinājās Zemgales reģiona kompetenču attīstības centrā (ZRKAC), Jelgavā.

28. decembrī CERT.LV pārstāvis piedalījās jauniešiem domātās Valsts policijas izstrādātās mobilās aplikācijas par digitālo drošību testēšanā.

Pārskata periodā CERT.LV par IT drošību izglītoja 2458 cilvēkus, iesaistoties 37 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2017. gada 4. ceturksnī

6. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā.

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 12.10., 09.11. DEG sanāksme.
- 08.11. CERT.LV pārstāvis piedalījās Saeimas Aizsardzības, iekšlietu un korupcijas novēršanas komisijas sēdē par pamatnostādņu „Latvijas kiberdrošības stratēģija 2014. – 2018. gadam" izpildes gaitu.

Sadarbība ar valsts iestādēm incidentu risināšanā aplūkota atskaites 2. punktā.

7. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu.

IT drošības likums nosaka, ka valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību. Līdz 2017. gada 31. decembrim CERT.LV apkopojusi informāciju par 1314 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību vai ar to saistītas.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem (turpmāk – ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai.

Šī pārskata perioda beigās rīcības plānu statistika ir šāda:

- saņemti 36 ESK rīcības plāni;
- 15 ESK rakstiski apliecināja, ka neuztur publisko elektronisko sakaru tīklu.

Pārskata periodā CERT.LV nav saņēmis nevienu ziņojumu no ESK par drošības vai integritātes pārkāpumiem, kas būtiski ietekmējuši elektronisko sakaru tīkla darbību vai pakalpojumu sniegšanu un atbilst Informācijas tehnoloģiju drošības likuma (ITDL) 9.panta pirmās daļas 2.punktam.).

Pārskata periodā CERT.LV nav konstatējis apdraudējumus, kuru atrisināšanai būtu nepieciešams slēgt galalietotājam piekļuvi elektronisko sakaru tīklam (ITDL 9.panta pirmās daļas 5.punkts).

ITDL 6.^{1} pantā minētie gadījumi aplūkoti atskaites 2. punktā.

8. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 09.-15.10. CERT.LV pārstāvis apmeklēja EUNITY projekta semināru „Cybersecurity and Privacy Dialogue between Europe and Japan" Tokijā, Japānā.
- 20.-28.10. CERT.LV pārstāvis piedalījās „IEEE MILCOM 2017" konferencē Baltimorā, ASV, un prezentēja tehniskos pētījumus „Bbuzz: A Bit-aware Fuzzing Framework for Network Protocol Systematic Reverse Engineering and Analysis" un „Frankenstack: Toward Real-time Red Team Feedback".
- 23.-26.10. CERT.LV pārstāvis piedalījās „Secure" konferencē Varšavā, Polijā.
- 23.-28.10. CERT.LV pārstāvis piedalījās „eCrime.EU Symposium" konferencē Porto, Portugālē.
- 01.11. CERT.LV pārstāvis sniedza interviju Apvienoto Nāciju Organizācijas Informācijas un komunikāciju tehnoloģiju aģentūras portālam (ITU News) „Q&A: How Computer Security Incident Response Teams respond to cyber threats".
- 29.10.-02.11. CERT.LV pārstāvji piedalījās Rumānijas CERT.RO organizētajā konferencē „The New Global Challenges in Cyber Security" Bukarestē, Rumānijā.
- 20.-24.11. CERT.LV pārstāvis piedalījās Eiropas Komisijas TAIEX (Technical Assistance and Information Exchange) programmas ietvaros organizētajā seminārā „TAIEX Workshop on Public- Private Partnership in Cyber-security" Kijevā, Ukrainā, un sniedza vairākas prezentācijas, daloties CERT.LV pieredzē par sadarbību ar privāto un valsts sektoru.
- 28.-30.11. CERT.LV pārstāvis piedalījās sanāksmē „Coordinated Vulnerability Disclosure" Briselē, un sniedza prezentāciju par Latvijas pieredzi atbildīgas ievainojamību atklāšanas jomā.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

- 18.10. Tikšanās ar Lielbritānijas vēstniecības pārstāvi par sadarbības iespējām projekta „Idea Garage: Cyber Security" ietvaros.
- 08.-09.11. CERT.LV pārstāvji apmeklēja *Microsoft* kursus par kiberdrošības jautājumiem.
- 08.11. CERT.LV pārstāvis piedalījās StratCom pasākumā, kurā tika prezentēts centra veiktais pētījums par interneta troļļiem.
- 10.11. CERT.LV pārstāvis piedalījās LIKTA balvas „Platīna pele" žūrijas komisijā.
- 24.11. CERT.LV pārstāvis piedalījās DVI seminārā personas datu aizsardzības speciālistiem.
- 07.12. CERT.LV pārstāvis piedalījās LIKTA ikgadējā konferencē, kurā tika pasniegta arī balva „Platīna pele", t.sk., balva „Labākā kiberdrošības iniciatīva".
- 08.12. CERT.LV pārstāvji apmeklēja *Microsoft* kursus par personas datu aizsardzības regulas (GDPR) ieviešanu.
- 28.12. Sanāksme VRAA par informācijas ievietošanu portālā latvija.lv.

10. Ar Elektroniskās identifikācijas uzraudzību saistīto pienākumu izpilde.

Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums "Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību" noteikto CERT.LV pārskata periodā turpināja noteikto funkciju veikšanu.

Iepriekšminēto funkciju izpildei veikto darbu uzskaitījums:

- CERT.LV pārstāvji tikās ar Latvijas Valsts radio un televīzijas centra (LVRTC) pārstāvi par Fizisko personu elektroniskās identifikācijas likuma Ministru kabineta noteikumiem Nr. 560. "Noteikumi par kvalificēta un kvalificēta paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzēja un tā sniegtā pakalpojuma tehniskajām un organizatoriskajām prasībām"
- CERT.LV pārstāvji piedalījās vebinārā par digitālā paraksta pakalpojumiem.
- CERT.LV pārstāvji piedalījās sanāksmē ar Aizsardzības ministrijas pārstāvjiem par LVRTC sertifikāciju.
- CERT.LV pārstāvji piedalījās sanāksmē ar LVRTC pārstāvi par uzticamības sarakstiem.
- CERT.LV pārstāvji iesaistījās komitejas darbā un sadarbībā ar Aizsardzības ministrijas pārstāvjiem sagatavoja lēmumu par LVRTC atbilstības apstiprināšanu.
- CERT.LV pārstāvji piedalījās Digitālās drošības uzraudzības komitejas sēdē, kurā lēma par LVRTC pakalpojumu iekļaušanu uzticamības sarakstos, par vēstuli Latvijas Valsts radio un televīzijas centram, kā arī Digitālās drošības uzraudzības komiteja apstiprināja ekspertu sarakstu, kurā iekļauti eksperti, kuri atbilst Fizisko personu elektroniskās identifikācijas likuma 11. panta otrajā daļā noteiktajām prasībām.

11. Papildu pasākumu veikšana.

Atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību.

Latvijas Interneta asociācijas „Net-Safe Latvia" drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.10.2017. līdz 31.12.2017. ir saņēmusi un izvērtējusi 106 ziņojumus. No tiem 37 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 7 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 14 ziņojumos konstatēta personas goda un cieņas aizskaršana, 4 gadījumos konstatēti vardarbīga rakstura materiāli un 1 ziņojums saņemts par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 8 ziņojumi, 10 ziņojumu saturs nav bijis pretlikumīgs, 25 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 9 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 24 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Sagatavotājs – Līga Besere,
tālrunis 67085888
e-pasts liga.besere@cert.lv