Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi 2017. gadā

2018

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

2017. gadu raksturo būtisks pavērsiens šifrējošo izspiedējvīrusu jomā, kas neizbēgami ietekmēja arī Latviju. Ja līdz šim šifrējošie vīrusi tika izmantoti finansiāla labuma gūšanai, lai izspiestu no upuriem izpirkuma maksu par datu atgūšanu, tad pagājušajā gadā tika novērotas vairākas šifrējošo izspiedējvīrusu kampaņas (piem., WannaCry, NotPetya), kurām, visticamāk, tika nodrošināts valsts līmeņa atbalsts politisku mērķu sasniegšanai.

Straujus apgriezienus uzņēma lietu interneta (IoT) attīstība, un paredzams, ka tā nemazinās tempus arī nākamajos piecos gados. Arvien palielinās internetam pievienojamo lietu klāsts, bet ražotāji ne vienmēr rūpējas par pietiekamu drošības līmeni savos produktos. Lai arī industrijā ir izstrādāti drošības standarti, tie ne vienmēr tiek ievēroti, un šobrīd trūkst mehānismu, kā cīnīties ar ražotājiem, kas neseko noteikumiem. Rezultātā pieaug lietu interneta ļaunprātīgas izmantošanas iespējas. Drošības standartu neievērošana rada bažas arī kritiskās infrastruktūras turētājos, kuru objektos tiek izmantotas viedās komponentes.

Daļa no 2017. gadā globālajā kibertelpā piedzīvotajām datu noplūdēm ir notikušas lietotāju nepietiekamas informētības dēļ par mākoņpakalpojumu lietošanu un drošības līmeni. Minētā lietotāju neizpratne par pakalpojuma nosacījumiem un neiedziļināšanās izmantojamā pakalpojuma iespējās, tajā skaitā drošības mehānismos, pēc CERT.LV domām ir nopietna un risināma problēma. Līdz ar to ir paredzams, ka 2018. gadā arvien aktuālāks kļūst mākoņpakalpojumu izmantošanas jautājums gan privātajā, gan valsts sektorā.

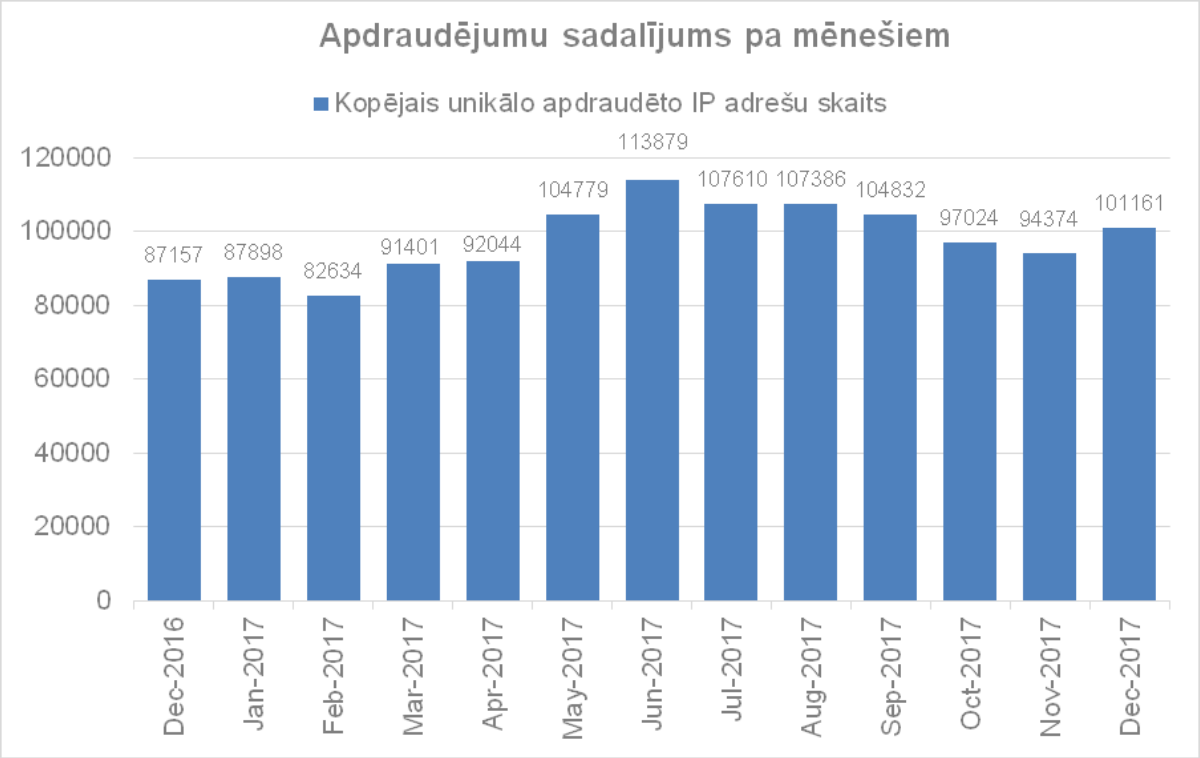
Viens no gada pozitīvajiem notikumiem: ar 2017.gada janvāri spēkā stājās Ministru kabineta noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”. Valsts iestādes sāka pielāgot procedūras un informācijas sistēmas, kā arī sagatavot iepirkumu specifikāciju atbilstoši noteikumu prasībām, kas savukārt paaugstina kopējo drošības līmeni valstī.

Kopumā pārskata periodā CERT.LV reģistrēja 477 252 apdraudētas unikālās IP adreses, veica ielaušanās testus 13 valsts un pašvaldību iestāžu tīmekļa vietnēs, kurās konstatēja 3 kritiskas un 11 augstas bīstamības ievainojamības, sniedza nepieciešamo atbalstu gan publiskajam, gan privātajam sektoram, gan arī tiesībsargājošajām iestādēm incidentu risināšanā, piedalījās 125 dažādos pasākumos un izglītoja gandrīz 8000 cilvēkus.

1. Incidentu apstrāde

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 vidēji 90 000 – 100 000 ievainojamu unikālu IP adrešu.

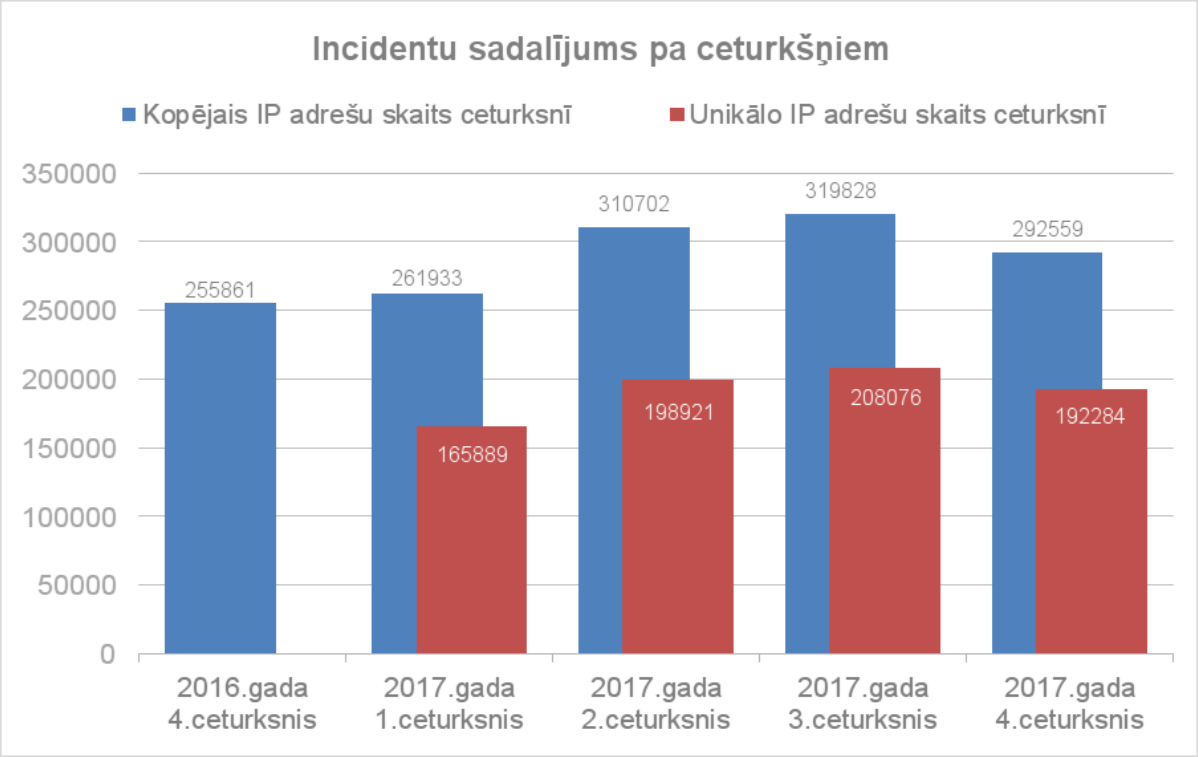


1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 2017. gadā.

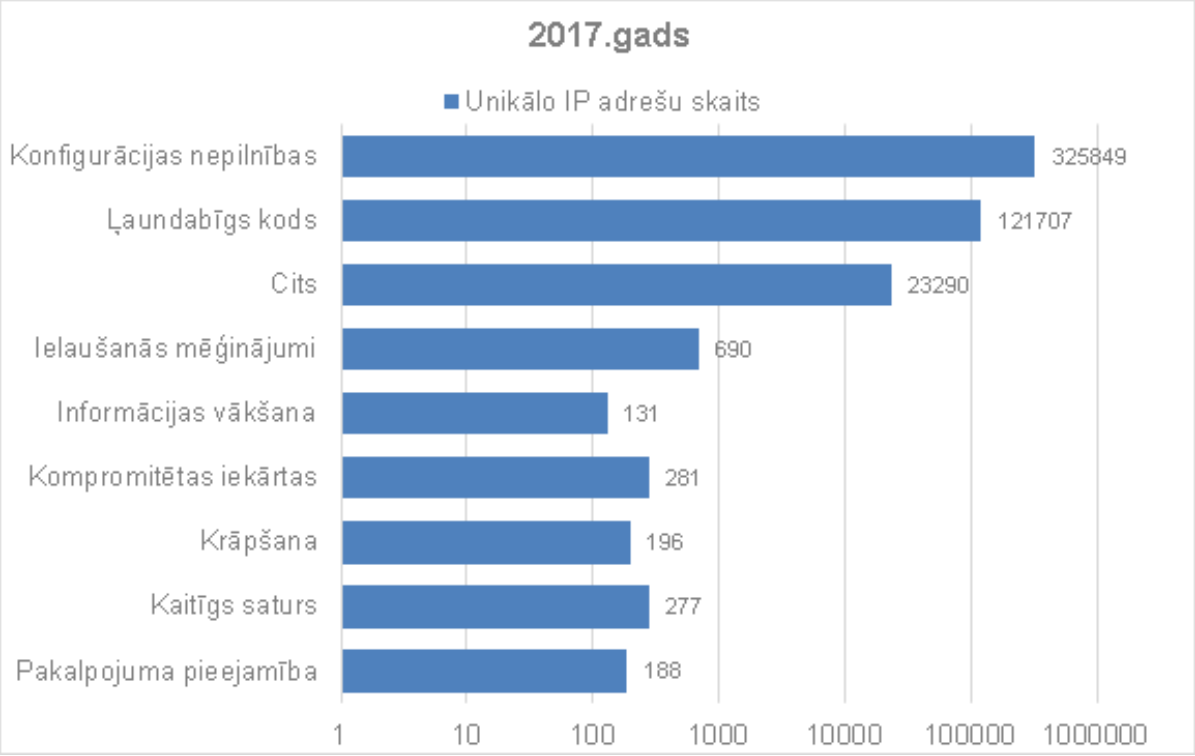
Notikušās *WannaCry* un *NotPetya* globālās kampaņas atspoguļojās arī CERT.LV apkopotajā statistikā ar kāpumu maijā un jūnijā (1. attēls).

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).

Piemēram, 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.

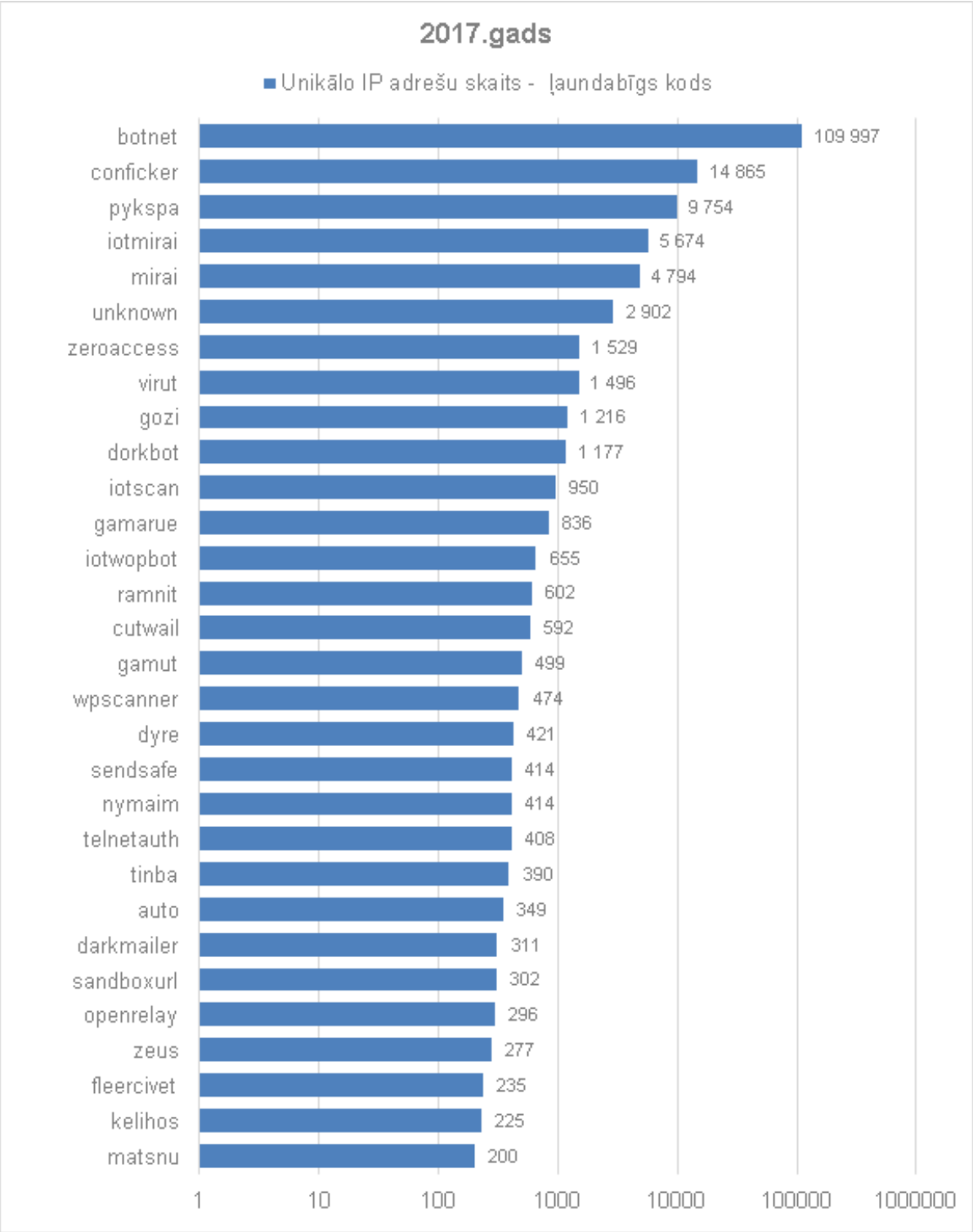


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2017. gadā.



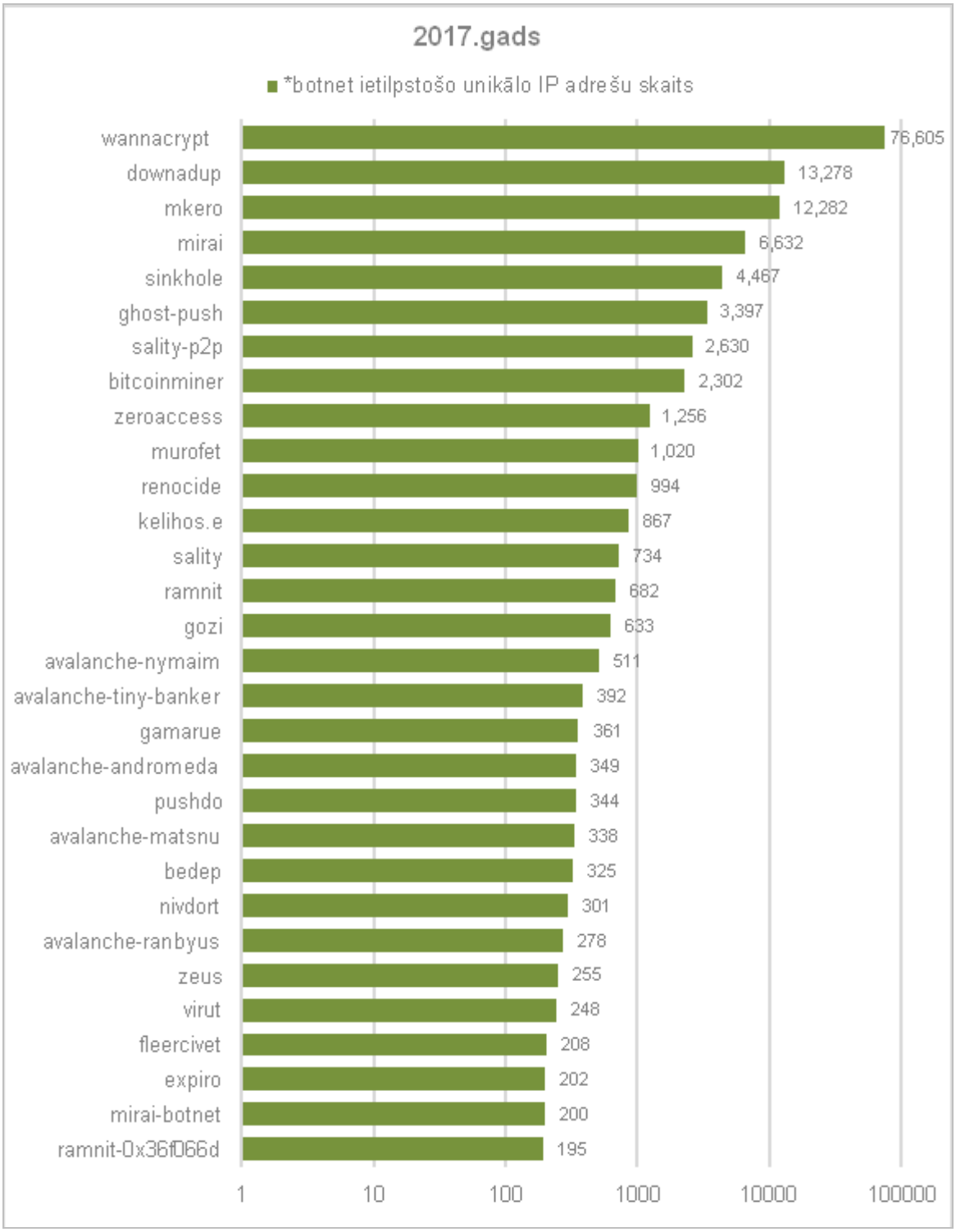
3.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa apdraudējuma veidiem 2017. gadā.

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



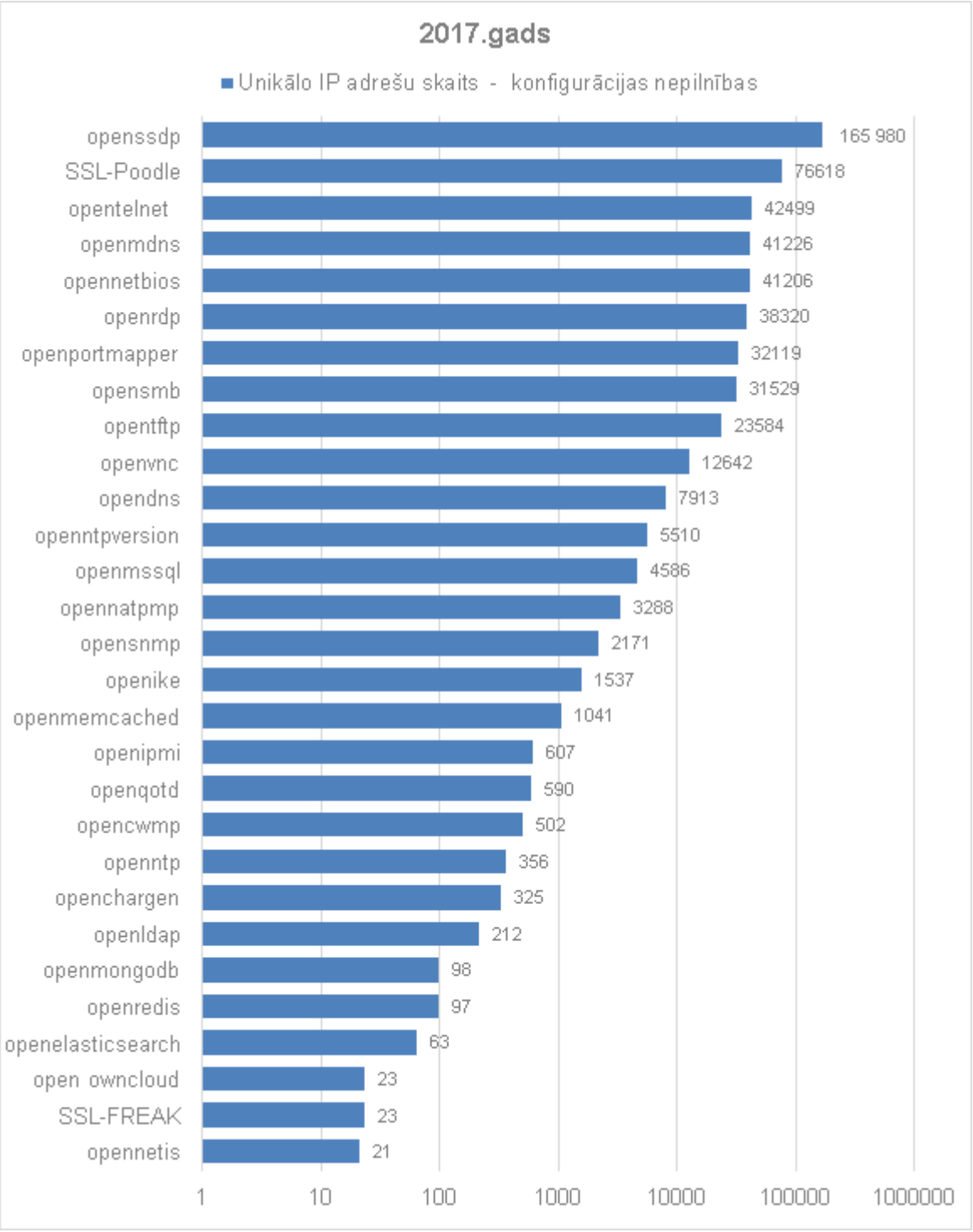
4.attēls – CERT.LV kopējais reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gadā ar apdraudējuma veidu - ļaundabīgs kods.

Pirmo vietu ļaunatūras izplatības topā šajā gadā 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. gadā ar apdraudējuma veidu - ļaundabīgs kods.

4.1. attēlā redzams, ka visaugstākie izplatības rādītāji pērn bijuši ļaunatūrai *WannaCry* jeb *WannaCrypt*. Otro vietu ļaunatūras izplatības topā 2017. gadā ieņēma *Conficker* jeb *downadup*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra. TOP3 noslēdz *MKero Android* trojānis, kas spēj apiet *CAPCHA* autentifikācijas sistēmu un, lietotājam nezinot, veic lietotāja parakstīšanos uz dažādiem maksas servisiem.

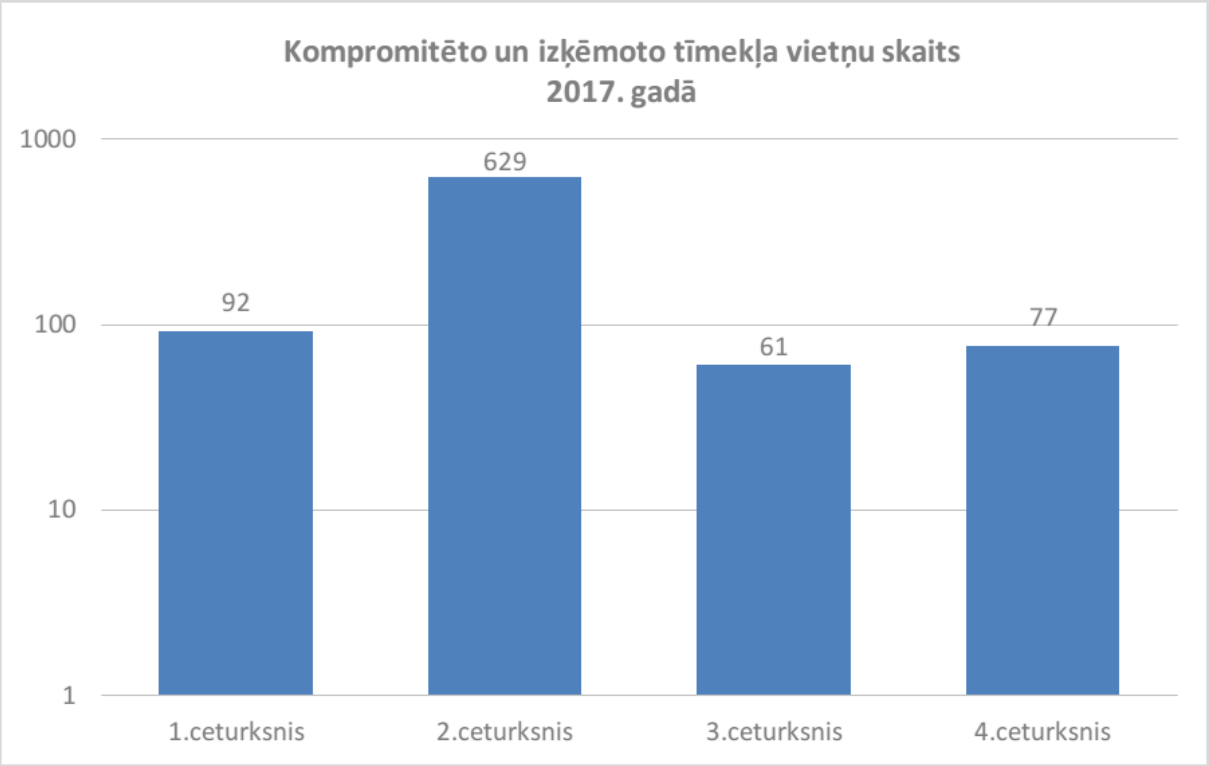


5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gadā ar apdraudējuma veidu – konfigurācijas nepilnība.

Opensmb, kas 2017. gada pirmajā pusē konfigurācijas nepilnību topā bija jaunpienācēja, gada šķērsgriezumā ieņem 8. vietu. Šī diezgan plaši izplatītā konfigurācijas nepilnība bija vainojama tādu šifrējošo izspiedējvīrusu kā *WannaCry* un *NotPetya* straujajā izplatībā.

Kompromitētas vietnes

CERT.LV uzskaita uzlauzto un izķēmoto mājaslapu gadījumus. 2017. gadā tika uzlauztas un izķēmotas 859 mājaslapas, kas ir par 35% vairāk kā 2016. gadā. Divdesmit deviņos gadījumos tīmekļa vietne gada laikā tika uzlauzta atkārtoti.



3. attēls – Kompromitēto tīmekļa vietņu skaits pa ceturkšņiem 2017. gadā.

2. Nozīmīgākie incidenti 2017. gadā

Pārskata periodā CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Pārskatā apkopoti nozīmīgākie incidenti, kas iezīmē gada tendences.

2.1. Izspiedējvīrusi

CERT.LV pārskata periodā regulāri saņēma ziņojumus par dažādiem šifrējošajiem izspiedējvīrusiem, piemēram, *Cerber, WannaCry, BTCWare, NotPetya, Scarab ransomware, Locky, Kryptik* u.c. Salīdzinoši biežāk ziņojumi tika saņemti no privātpersonām un mazajiem uzņēmumiem, nevis pašvaldībām un valsts iestādēm.

Gada laikā iezīmējās divas lielākas šifrējošo vīrusu kampaņas, kas piesaistīja arī pastiprinātu mediju uzmanību - maijā tā bija *WannaCry* kampaņa, bet jūnijā *NotPetya.*

WannaCry kampaņas laikā tika inficētas vairāk kā 200 000 Windows iekārtas 150 valstīs. CERT.LV saņēma ziņas par 20 cietušajiem Latvijā, bet atšķirībā no ārvalstīm, kur starp cietušajiem bija gan slimnīcas, gan telekomunikāciju kompānijas, Latvijā cietušas bija privātpersonas un daži mazie uzņēmumi.

Savukārt vīruss *NotPetya* vissmagāk skāra Ukrainu, būtiski ietekmējot arī tās kompānijas, kuru darbība ir saistīta ar šo valsti. Līdz CERT.LV nonāca informācija par četriem upuriem Latvijā – 3 tirdzniecības uzņēmumiem un vienu privātpersonu.

Lielākajā daļā gadījumu dati tika atgūti no rezerves kopijām vai izmantojot bezmaksas projekta *„No More Ransom"* piedāvātos atšifrēšanas rīkus. Retos gadījumos cietušajam nācās vienoties ar ļaundariem.

CERT.LV iesaka uzbrucējiem nemaksāt, jo pretējā gadījumā cietušie, paši nepazinoties, nodrošina uzbrucējiem resursus jaunu šifrējošo vīrusu kampaņu izstrādei. Kā arī nav garantēts, ka pēc apmaksas veikšanas, cietušā dati tiks atšifrēti.

2.2. Nesankcionēta iejaukšanās biznesa sarakstē (Business e-mail compromise)

2017. gada laikā CERT.LV saņēma vairākus ziņojumus gan no valsts un pašvaldību iestādēm, gan uzņēmumiem par krāpnieciska rakstura e-pastiem, kas plašāk pazīstami kā *Business e-mail compromise* jeb kā nesankcionēta iejaukšanās biznesa sarakstē.

Šāda veida e-pastus visbiežāk saņem vai nu grāmatvedības nodaļas vai darbinieki, kas atbild par organizācijas finansēm. E – pasta sūtītājs šķietami ir kāds no uzņēmuma vadības – valdes loceklis, valdes priekšsēdētājs, direktors vai direktora vietas izpildītājs u.c. E-pastā parasti tiek pieprasīts veikt maksājumu par konkrētu summu uz it kā kādu no uzņēmuma sadarbības partneru kontiem, kas patiesībā pieder krāpniekam. Šī krāpšanas shēma satur sociālās inženierijas elementus, kur tiek manipulēts ar cilvēka emocijām, piemēram, e-pasta saturs parasti pieprasa steidzamu vai ārkārtas rīcību no darbinieka. Tāpat CERT.LV ir konstatējis, ka krāpnieciskos e-pastus aizvien ticamākus padara tajos izmantotā korektā un gramatiski pareizā latviešu valoda.

Lielākās šāda veida kampaņas konstatētas aprīlī un augustā. Visos gadījumos e-pastiem bija neatbilstoša *Reply-To* adrese, kas ļāva tos atpazīt kā krāpnieciskus.

CERT.LV rīcībā nav informācijas, ka kāds no fiksēto e-pastu saņēmējiem būtu cietis finansiālus zaudējumus.

Lai novērstu šāda tipa uzbrukumus, CERT.LV iesaka izmantot rīkus, kas slēpj uzņēmuma vai iestādes tīmekļa vietnē izvietotās e-pasta adreses no skeneriem, kā arī izveidot SPF ierakstus, kas noteiktu, no kādiem serveriem atļauts sūtīt e-pastus ar noteiktiem domēna vārdiem, lai novērstu krāpniecisku e-pastu izplatīšanu.

2.3. Krāpšana

Pārskata periodā reģistrētie krāpšanas mēģinājumi visbiežāk bija saistīti ar krāpnieciskām interneta vietnēm, t.sk. oriģinālo vietņu viltus versijām, kurās integrēta arī, piemēram, valsts iestāžu simbolika. Šādu interneta vietņu mērķis parasti ir izkrāpt uzņēmuma vai iestādes klientu datus.

2017. gada nogalē, pirmssvētku periodā, no vairākiem 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.

CERT.LV saņēma arī informāciju par krāpniecisku telefona zvanu, kurā zvanītājs uzdevās par Microsoft pārstāvi un teica, ka datoram vajag apmaksāt sertifikātu, lai dators nesūtītu kļūdu paziņojumus. Lietotājam tika norādīts, ka nelielā samaksa par sertifikātu jāveic konkrētā tīmekļa vietnē. Lietotājs ievadīja krāpnieciskajā vietnē savus bankas datus.

Pēc telefonsarunas no lietotāja konta tika aizskaitīti 3000 eiro. Cietušajam tika ieteikts rakstīt iesniegumu policijā.

2.4. Pikšķerēšanas kampaņas

Pikšķerēšanas kampaņu mērķis ir izvilināt no interneta lietotāja sensitīvus datus, piemēram, kredītkaršu informāciju, sociālo tīklu un e-pastu paroles, pases datus u.c. Pārskata periodā visbiežāk pikšķerēšanas kampaņām tika izmantoti krāpnieciski e-pasti ar lūgumu atjaunot piekļuvi e-pasta kontam un lūgumi (it kā no e-pasta uzturētāja) atjaunot e-pastu paroles.

Zemāk pāris pikšķerēšanas kampaņu piemēri:

- Aprīlī tika saņemta informācija, ka no daudziem e-pastiem .LV domēna zonā pienāk paziņojumi par it kā pārsniegtu pastkastes limitu un lūgts klikšķināt uz saites, lai sniegtu prasītos datus pakalpojuma atjaunošanai, pretējā gadījumā draudot ar e-pasta pakalpojuma izbeigšanu. CERT.LV informēja saitē norādītās tīmekļa vietnes uzturētājus par vietnes kaitīgo raksturu un lūdza vietni dzēst.
- Aprīlī tika saņemta informācija arī par kaitniecisku Google Chrome pārlūka spraudni, kas bija paredzēts it kā konkrētas lietotnes autorizācijas atvieglošanai, piedāvājot lietotāju turpmāk autorizēt ar vienu klikšķi, ja lietotājs saglabā spraudnī savu lietotājvārdu, paroli un visus kodu kartes kodus, bet visi spraudnī ievadītie dati tika nosūtīti krāpniekiem. Spraudnis tika pieteikts Google kā kaitniecisks.

2.5. Piekļuves atteices uzbrukumi (DoS un DDoS)

Pārskata periodā CERT.LV saņēma ziņojumus par DoS un DDoS uzbrukumiem gan no valsts un pašvaldību iestādēm, gan arī kādas Latvijas komercbankas. Periodiski tika saņemti ziņojumi arī no citām Eiropas valstu CERT vienībām par Latvijas IP adresēm, kurās konstatētas dažādas konfigurāciju nepilnības (*openDNS, OpenResolver u.c.*) un kuras tikušas izmantotas DDoS uzbrukumos. Adrešu turētāji tika apzināti un informēti.

Lielākā daļa uzbrukumu tika veiksmīgi atvairīti, tomēr dažos gadījumos uzbrukuma rezultātā interneta resurss uz īsu brīdi kļuva nepieejams. Visos gadījumos CERT.LV sniedza ieteikumus interneta vietņu drošības uzlabošanai, piemēram, iesakot robotu darbības ierobežošanu vietnē.

CERT.LV zemāk piedāvā ieskatu dažos no DoS un DDoS gadījumiem:

- Janvāra beigās kāda komercbanka informēja CERT.LV par pārdomātu SPAM uzbrukumu ar naudas izspiešanas mērķi. Iestādei tika nosūtīti ap 60 tūkstošiem e-pastu un tika veikts neliels demonstratīvs DDoS uzbrukums, izmantojot UDP Flood. Izsūtītie e-pasti bija no leģitīmiem serveriem, piemēram, scientificamerican.com, robly.com, u.t.t. No katra e-pasta izsūtīšanas servera tika nosūtītas ne vairāk par 20-30 vēstulēm. Pamatā tika izmantoti dažādi ziņu un mediju portāli, kuriem ir iespēja pierakstīties uz paziņojumiem par kādu raksta tēmu. CERT.LV sniedza ieteikumus, kā rīkoties šādos izspiešanas gadījumos – nekomunicēt ar izspiedējiem un nemaksāt. Tika pieprasīts slēgt uzbrucēju Google e-pasta adresi. Reāls pilna apjoma uzbrukums nesekoja.
- Maijā tika saņemta informācija par uzbrukumu kādam valsts iestādes portālam. Žurnālfailu analīze atklāja, ka portālam tika veikts plānots uzbrukums, izmantojot speciālus rīkus, kas paredzēti ievainojamību meklēšanai. Attiecīgās dienas vakarā uzbrukums iegāja DoS fāzē un izraisīja portāla nepieejamību. Nepilnas stundas laikā portāla darbība tika atjaunota.
- Oktobrī tika saņemts ziņojums par 87 Latvijas IP adresēm, kuras tika izmantotas piekļuves atteices (DDoS) uzbrukumā. Šajās adresēs tika konstatēta *OpenResolver* konfigurācijas nepilnība, par kuru tika brīdināti atbilstošie resursu turētāji.

2.6. Finanšu platformas

Vairāki lietotāji izmantoja nelicenzētas akciju tirdzniecības platformas un kļuva par krāpniecības upuriem, ciešot zaudējumus no 2000 līdz pat 100 000 EUR apmērā.

Pirms finanšu pakalpojumu izmantošanas CERT.LV aicina pārliecināties, ka izvēlētais pakalpojuma sniedzējs ir saņēmis Finanšu un kapitāla tirgus komisijas (FKTK) licenci, jo tikai pie šādiem noguldījumu piesaistītājiem klientu aizsargā valsts. Informācija par licencētiem ieguldījumu pakalpojumu sniedzējiem Latvijā ir pieejama FKTK mājas lapā.

Kriptovalūtai iegūstot popularitāti, kļūst aktuāli arī uzbrukumi lietotāju kriptovalūtas maciņiem. Atgūt nozagtu kriptovalūtu ir vēl grūtāk nekā zaudētu naudu, jo kriptovalūtai pagaidām trūkst regulējuma un pienācīgas lietotāju aizsardzības. Lietotājiem ir rūpīgi jāseko atbilstošu drošības līdzekļu izmantošanai un vietņu autentiskumam, kurās tiek veiktas darbības.

2.7. Mobilā ļaunatūra

CERT.LV ir saņēmusi informāciju par atsevišķiem mobilās ļaunatūras gadījumiem, bet lielākoties mobilo iekārtu lietotāji cieš zaudējumus, neuzmanīgi parakstoties uz maksas pakalpojumiem vai atbildot uz krāpnieciskiem ziņojumiem ar īsziņu nosūtīšanu, kas izrādās maksas pakalpojums. Uz Latvijas lietotājiem mērķētas mobilās ļaunatūras kampaņas pagaidām nav fiksētas.

2.8. Sociālie tīkli

2017.gadā CERT.LV saņēma ziņas par dažāda veida incidentiem sociālo tīklu vidē.

- Tika konstatēti vairāki *Twitter* un *Facebook* viltus konti, kas izveidoti valsts iestāžu vārdā. Tajos tika publicētas neatbilstoša satura ziņas. Iestādes tika aicinātas pieprasīt viltus kontu slēgšanu. Visi konstatētie viltus konti pāris dienu laikā tika slēgti.
- No vairākiem lietotājiem tika saņemtas ziņas par mēģinājumiem izkrāpt sociālā tīkla *Facebook* lietotāja datus, izsūtot brīdinājumus par konta slēgšanu vai piedāvājot aplūkot konta statistiku. Ja lietotājs sekoja saņemtajai saitei, tas tika pārvirzīts uz krāpniecisku vietni ar aicinājumu ievadīt savu e-pastu un *Facebook* paroli.
- Vairākiem lietotājiem iepazīšanās mēģinājumi sociālajā tīklā *Facebook* beidzās ar šantāžu un izspiešanas mēģinājumiem, sākot ar centieniem iežēlināt ar atrašanos kara zonā un lūgumu pārskaitīt naudu vai aicinājumiem pāriet uz videosaziņu, pēc kuras pieprasīta izpirkuma maksa, lai ieraksts netiktu publicēts. CERT.LV iesaka šantāžas gadījumos ar izspiedējiem nekomunicēt un nekādā gadījumā pieprasīto maksu nemaksāt, jo izspiedēji visticamāk draudēs atkārtoti, pieprasot arvien lielāku summu. Ar iesniegumu par izspiešanu jāvēršas policijā.
- Krāpniecībai tika pakļauti arī tērzētavas *WhatsApp* lietotāji. Aicinot piedalīties viltus loterijā vai draudot ar pakalpojuma pārtraukšanu, krāpnieki centās panākt maksas īsziņu nosūtīšanu vai maksājumu kartes datu ievadīšanu krāpnieciskā vietnē.
- Tika saņemtas arī vairākas sūdzības par neautorizētiem ierakstiem lietotāju *Facebook* profilos. Šādā gadījumā CERT.LV aicina pirmkārt izmantot facebook.com/hacked, lai noskaidrotu, vai nav kāda ļaunprātīga aplikācija, kurai ir piešķirtas tiesības publicēt ziņas lietotāja profilā, kā arī pārbaudīt iekārtu, vai tajā nav vīruss.

2.9. Ielaušanās/ kompromitētas iekārtas

- CERT.LV apzināja vairākas kompromitētas tīmekļa vietnes, kurās tika konstatēta SQL injekcijas ievainojamība, to starpā vairākas pašvaldību vietnes. Ievainojamība padarīja iespējamu datu neautorizētu izgūšanu. CERT.LV sazinājās ar vietņu uzturētājiem un informēja par atklāto ievainojamību un ieteica, kā to novērst.
- Tika konstatēti vairāki gadījumi ar kompromitētiem maršrutētājiem. Vienā gadījumā tie sūtīja lietotāju datus uz komandu un kontroles serveri. Citā gadījumā uzlauzts maršrutētājs tika izmantots kā komandu- un kontroles centrs ļaunatūras Trickbot izplatīšanai, kas ir banku trojānis un tiek izmantots finanšu datu izkrāpšanai. CERT.LV veica iekārtu turētāju apziņošanu un ieteica, kā novērst ievainojamības.
- Vairākas valsts iestāžu tīmekļa vietnes tika kompromitētas un izķēmotas. CERT.LV

sniedza rekomendācijas vietņu drošības uzlabošanai.

- Gada nogalē tika saņemti vairāki ziņojumi par ļaunatūru reklāmas baneros vienā no Latvijas interneta ziņu portāliem. Baneri saturēja ļaundabīgu kodu, kas ģenerēja kriprovalūtu, noslogojot apmeklētāju datorus. Vietnes uzturētāji tika informēti, baneru sistēma tika salabota.

2.10. Dati

Apjomīgas datu noplūdes pārskata periodā netika konstatētas, bet tika saņemta informācija par vairākiem gadījumiem, kuros no interneta bija publiski pieejama sensitīva tīmekļa vietņu informācija, kas radīja datu noplūdes risku. CERT.LV informēja vietņu uzturētājus un aicināja ierobežot attiecīgo piekļuvi no publiskā tīkla.

2.11. Ievainojamības

- LVRTC speciālisti veica eParaksta un saistīto sistēmu drošības auditu un izstrādāja programmatūras atjauninājumu, izmantojot jaunākas paaudzes kriptogrāfijas algoritmu SHA256.
- Tika saņemta informācija par kritiskām ievainojamībām vairākās tīmekļa vietnēs. Dažādi tīmekļa vietņu parametri tika pakļauti SQL injekcijas tipa uzbrukumam, kas ļautu uzbrucējam pārņemt kontroli pār vietni un serveri. Vietņu uzturētāji tika informēti un saņēma ieteikumus, kā ievainojamības novērst.

3. Informatīvie komunikācijas pasākumi

CERT.LV eksperti arī 2017. gadā turpināja sniegt intervijas un atbildēt uz mediju jautājumiem gan TV, gan presē un radio par dažādām aktuālām ar kiberdrošību saistītām tēmām. Pārskata periodā mediju interese visbiežāk bija saistīta ar tādām tēmām kā mobilo iekārtu drošība, jaunā banku autentifikācija, kiberdrošības situācija Latvijā, sociālo tīklu drošība, šifrējošie vīrusi, krāpnieciski interneta veikali u.c.

3.1. Informatīvie pasākumi medijiem

15. maijā CERT.LV rīkoja preses konferenci, kurā informēja medijus par WannaCry izspiedējvīrusu un tā radīto ietekmi Latvijā.

28. jūnijā CERT.LV aicināja preses pārstāvjus uz preses konferenci, kurā sniedza atbildes uz mediju jautājumiem par izspiedējvīrusu NotPetya un tā izplatību Latvijā.

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.

3.2. Komunikācija digitālajā vidē

2017. gada laikā stabili pieauga sekotāju skaits populārajās sociālo tīklu platformās *Twitter* un *Facebook*:

- *Twitter* konta twitter.com/certlv sekotāju skaits pārskata perioda beigās bija **1853.**
- *Facebook* profila facebook.com/certlv sekotāju skaits pārskata perioda beigās bija **762.**

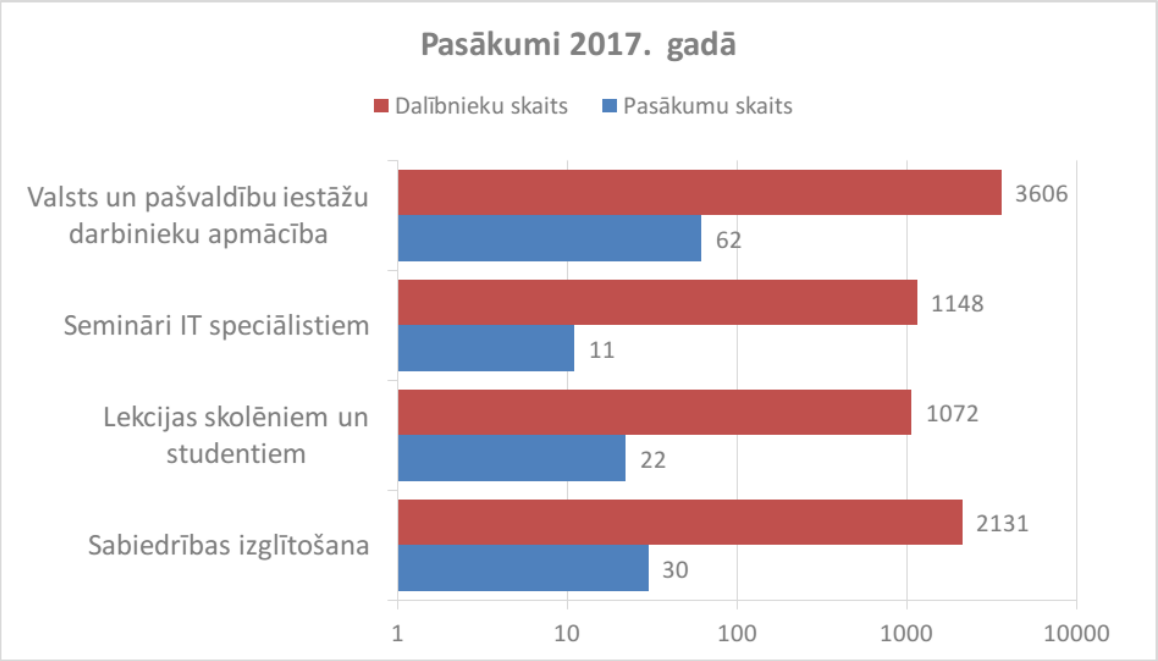
CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. **Kopā gada laikā CERT.LV lapai bijuši 67,855 unikāli apmeklējumi jeb sesijas.**

CERT.LV turpināja uzturēt arī lietotāju izglītošanas portālu www.esidross.lv, regulāri publicējot jaunus rakstus un atbildot uz lietotāju komentāriem.

Pārskata periodā katru mēnesi sadarbībā ar SANS institūtu tika izdoti informatīvie kiberdrošības biļeteni „OUCH!" ikvienam interneta lietotājam.

4. Izglītojošie pasākumi

2017. gadā CERT.LV turpināja rīkot izglītojošus pasākumus par drošības jautājumiem IT drošības speciālistiem, valsts un pašvaldību iestāžu darbiniekiem, studentiem, skolēniem un citiem interesentiem. Pārskata periodā CERT.LV piedalījās 125 pasākumos un izglītoja 7957 klausītājus.



4.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2017. gadā.

Gada lielākais pasākums bija ikgadējā IT drošības konference „Kiberšahs 2017", kas notika 5. oktobrī *Radisson Blu Hotel Latvija* telpās. Konferenci klātienē apmeklēja vairāk nekā 500 dalībnieku, savukārt tiešsaistē tai bija 3000 unikālu skatījumu.

Konference tika organizēta sadarbībā ar *ISACA Latvijas nodaļu*. Pasākumu atbalstīja *LMT, SQUALIO cloud consulting* un *Accenture Latvia.*

4.1. CERT.LV organizētie pasākumi IT drošības speciālistiem

6. aprīlī CERT.LV rīkoja semināru IT drošības speciālistiem „Esi drošs", kurā iepazīstināja klātesošos ar IT drošības aktualitātēm un aplūkoja tādas tēmas kā mobilo iekārtu drošības aspekti, lietu interneta drošība, uzbrukuma vektori sociālajos tīklos un open-source informācijas riski.

5. oktobrī CERT.LV sadarbībā ar *ISACA Latvija nodaļu* rīkoja IT drošības konferenci „Kiberšahs 2017". Nozīmīgākās tēmas bija lietu internets un tā drošība, mākslīgais intelekts, DDoS, IKT piegādes ķēdes riski, digitālā valsts, NIS direktīvas ieviešana, kiberdrošība kā daļa no valsts drošības, kiber-neatkarība u.c.

13. novembrī NIC sadarbībā ar CERT.LV un ICANN rīkoja praktisku semināru IT drošības speciālistiem „DNS ļaunprātīga izmantošana: izmeklēšanas rīki un metodes".

11. decembrī CERT.LV rīkoja semināru IT drošības speciālistiem „Esi drošs", kurā iepazīstināja klātesošos ar CERT.LV aktualitātēm un aplūkoja tādas tēmas kā šifrējošo vīrusu apdraudējumi, būtiskākās ievainojamības, interneta lietotāja biežāk pieļautās kļūdas, domēnvārda pārdomāta un droša izvēle, drošība sociālajos tīklos u.c.

4.2. CERT.LV prezentācijas par IT drošību sabiedrības izglītošanai

No 27. marta līdz 2. aprīlim Latvijā un visā Eiropā notika jau astotā E-prasmju nedēļa. 2017.gadā pasākumā uzsvars tika likts ne tikai uz e-prasmju apgūšanu, bet arī uz kiberdrošību, tādēļ 28. marts tika izvēlēts par Digitālās drošības dienu. Šajā dienā tika organizēti trīs semināri-diskusijas, kas veltīti dažādām kiberdrošības tēmām: kiberdrošības politikai Latvijā, mobilai drošībai un lietu internetam un tā drošībai. CERT.LV pārstāvji piedalījās visās trijās diskusijās.

29. martā E-prasmju nedēļas ietvaros CERT.LV telpās norisinājās kārtējā Datorologa akcija, kuras laikā katrs interesents bez maksas varēja atnest uz pārbaudi pie IT speciālista savu datoru, planšetdatoru vai viedtālruni un saņemt padomus savas iekārtas un datu aizsardzībai.

31. martā CERT.LV pārstāvis E-prasmju nedēļas ietvaros piedalījās VARAM organizētajā seminārā-tiešraidē "Tavas e-iespējas" un uzstājās ar prezentāciju „Realitāte virtuālajā vidē".

26. aprīlī CERT.LV pārstāvis uzstājās ar prezentāciju „Lietu internets – kā lietu internets ietekmē mūsu ikdienu šodien un kas mūs varētu sagaidīt nākotnē" pasākumā „Digitālā ēra 2017".

26. maijā CERT.LV piedalījās Microsoft un VARAM organizētajā akcijā „Strādā jebkur", informējot pasākuma dalībniekus par IT drošības aspektiem, kas jāievēro, atrodoties ceļā un publiskās vietās.

12. septembrī CERT.LV pārstāvis piedalījās Erasmus+ programmas stratēģisko skolu sadarbības partnerības projekta "The ICT road to STEM through TCC" sanāksmē un sniedza prezentāciju par CERT.LV izmantotajiem materiāliem 1.-6. klašu skolēnu izglītošanai par IT drošību. CERT.LV pārstāvis piedalījās arī diskusijā un informācijas apmaiņā par mazāko klašu skolēnu izglītošanu.

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.

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".

25. oktobrī kiberdrošības mēneša ietvaros CERT.LV telpās norisinājās Datorologa akcija, kuras laikā katrs interesents bez maksas varēja atnest uz pārbaudi pie IT speciālista savu datoru, planšetdatoru vai viedtālruni un saņemt padomus savas iekārtas un datu

aizsardzībai.

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".

5. Sadarbība ar valsts iestādēm

Pārskata periodā CERT.LV veica ielaušanās testus 13 valsts un pašvaldību iestāžu tīmekļa vietnēm, kurās konstatēja 3 kritiskas un 11 augstas bīstamības ievainojamības.

2017. gadā kopumā bija novērojama pozitīva tendence - jūtami palielinājusies valsts un pašvaldību iestāžu interese par CERT.LV piedāvātajiem ielaušanās testiem jeb audzis pieprasījums pēc tiem. Tas nozīmē, ka līdz ar interesi augusi arī pašu iestāžu atbildības sajūta par to uzturētajiem interneta resursiem un to drošību.

5.1. Sadarbība ar Aizsardzības ministriju

Regulāri notika tikšanās ar ministrijas Valsts sekretāru un komunikācija ar Nacionālās kiberdrošības politikas koordinācijas nodaļu.

CERT.LV regulāri piedalījās Aizsardzības ministrijas darba grupā par NIS direktīvas ieviešanu.

5.2. Citi sadarbības partneri

CERT.LV sadarbojās ar *Zemessardzes Kiberaizsardzības vienību*, kopīgi piedaloties dažādās tehniskajās mācībās, kā arī nodrošinot vienībai virtuālu treniņu vidi drošības incidentu risināšanas pilnveidei.

CERT.LV turpināja atbalstīt *Drošības ekspertu grupas (DEG)* darbību, kas nodrošina diskusiju forumu IT drošības speciālistiem gan no privātā, gan valsts sektora. *DEG* sanāksmes notika reizi mēnesī.

6. Starptautiskā sadarbība

Pārskata periodā CERT.LV stiprināja sadarbību ar citu valstu IT drošības incidentu novēršanas vienībām un starptautiskām organizācijām. CERT.LV speciālisti uzstājās ar prezentācijām starptautiskās konferencēs, semināros un apguva jaunas prasmes tehniskajās mācībās.

6.1. Sadarbība ar CERT kopienu

CERT.LV pārstāvji pārskata periodā piedalījās *TF-CSIRT* un *FIRST* tehniskajos semināros un sanāksmēs.

No 23. līdz 25. janvārim CERT.LV pārstāvji piedalījās TF-CSIRT sanāksmē un FIRST reģionālajā simpozijā Valensijā, CERT.LV pārstāvis prezentēja „Firmware over the air, case study of ADUPS Fota".

No 8. līdz 10. maijam Eiropas Komisijas TAIEX programmas ietvaros CERT.LV sadarbībā ar Aizsardzības ministriju uzņēma Melnkalnes CERT pārstāvjus.

Viesi no Melnkalnes uzzināja par CERT.LV labo praksi incidentu risināšanā, starptautiskās sadarbības veidiem, izglītošanas aktivitātēm u.c. CERT.LV darbības jomām. Vizītes mērķis bija apmainīties ar pieredzi un informāciju, lai stiprinātu Melnkalnes CERT kapacitāti.

6.2. Sadarbība ar ENISA

Daudzveidīga sadarbība notika ar Eiropas Tīkla un informācijas drošības aģentūru, piemēram, gatavojoties konferencei utt.

21. martā CERT.LV pārstāvis piedalījās seminārā Briselē, Beļģijā, kurā tika vērtēta ENISA aģentūras darbība pēdējos 8 gados un diskutēts par ENISA nākotnes uzdevumiem, mandātu un stratēģiju.

No 9. līdz 10. maijam norisinājās Eiropas Tīkla un informācijas drošības aģentūras (ENISA) Eiropas Kiberdrošības mācību „Cyber Europe 2016" noslēguma ziņojuma konference, kā arī nākamo mācību („Cyber Europe 2018" un „EUROSOPEx 2017") plānošana.

6.3. Sadarbība ar NATO CCDCoE

CERT.LV pārstāvji sadarbojās ar *NATO Cooperative Cyber Defence Centre of Exelence*.
Viens no nozīmīgākajiem pasākumiem bija starptautiskās kiberdrošības mācības "Locked Shields 2017", kuras notika no 24. līdz 29. aprīlim. CERT.LV piedalījās gan organizatoru (baltajā), gan aizstāvju (zilajā), gan uzbrucēju (sarkanajā) komandā. CERT.LV un US EUCOM apvienotā komanda mācībās ieguva 5. vietu.

2017. gada augustā ar NATO CCDCoE tika noslēgts sadarbības līgums par kopīgu tehnisko kiberaizsardzības mācību „Crossed Swords„ organizēšanu. Tika uzsākta gatavošanās mācībām, kuras notika 2018. gada janvārī.

Atskaiti sagatavoja:
CERT.LV sabiedrisko attiecību projektu vadītāja Madara Grinvalde, tālrunis 67085888,
e-pasts madara.grinvalde@cert.lv

2018. gada 23. martā