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 2. ceturksnis (01.04.2017. – 30.06.2017.)

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

Maijā gan pasauli, gan Latviju spēcīgi ietekmēja šifrējošo izspiedējvīrusu WannaCry un NotPetya izplatīšanas kampaņas. WannaCry inficēja 200 000 iekārtas 150 pasaules valstīs. Cietušo vidū bija gan veselības aprūpes iestādes, gan telekomunikāciju uzņēmumi. Neskatoties uz to, ka Latvijā WannaCry upuru skaits bija neliels (CERT.LV saņēma 20 ziņojumus par privātpersonām un dažiem mazajiem uzņēmumiem), apdraudējuma raksturs bija nopietns. Vīrusu izmantotā ievainojamība norādīja uz virkni tīklam pieslēgtu iekārtu, kuru aizsardzība nebija pietiekama, pakļaujot šīs iekārtas līdzīgiem uzbrukumiem arī nākotnē. Papildu apdraudējuma aspekts šajās šifrējošo izspiedējvīrusu kampaņās bija tajās izmantotais uzbrukuma vektors - ja agrāk šādus vīrusus izplatīja, izsūtot kaitnieciskus pielikumus vai saites, tad šajā gadījumā uzbrukumi notika bez lietotāju līdzdalības.

Aprīļa sākumā vairākas valsts un pašvaldību iestādes saņēma krāpnieciskus e-pastus, kas sūtīti grāmatvedei iestādes vadītāja vārdā ar lūgumu veikt steidzamu bankas pārskaitījumu. Visos gadījumos e-pasti tika identificēti kā krāpnieciski (CEO fraud) un zaudējumi netika nodarīti. Iestādēm tika sniegti ieteikumi, kā mazināt krāpšanas mēģinājumus un nodrošināt kontroli pār iestādes domēna vārda izmantošanu.

Visā pārskata periodā bija novērojamas arī sociālā tīkla Facebook un tērzēšanas lietotnes WhatsApp vārdu izmantojošas krāpšanas, gan viltus loteriju, gan krāpniecisku brīdinājumu formā, cenšoties izkrāpt lietotāju piekļuves vai bankas datus, vai panākot maksas pakalpojumu pieslēgšanu. Šādi gadījumi notiek regulāri, un CERT.LV brīdina lietotājus, ja tiek konstatētas jaunas kampaņas.

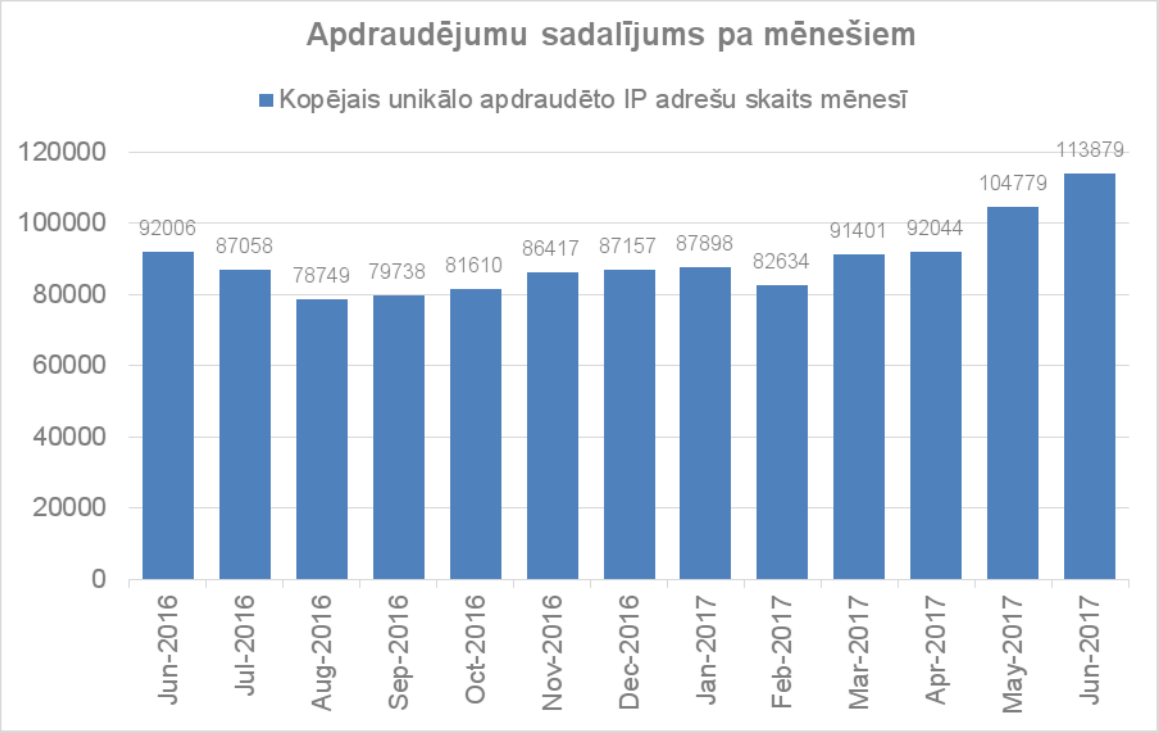
2017.gada 2.ceturksnī CERT.LV apkopoja informāciju par 198 921 apdraudētu IP adresi. Izplatītākais apdraudējums bija konfigurācijas nepilnības (150 624 unikālas IP adreses), tam sekoja ļaundabīgs kods (41 578 unikālas IP adreses) un ielaušanās mēģinājumi (182 unikālas IP adreses).

Pārskata periodā CERT.LV par IT drošību izglītoja 2380 cilvēkus, iesaistoties 38 izglītojošos pasākumos.

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 – 110 000 ievainojamu unikālu IP adrešu.

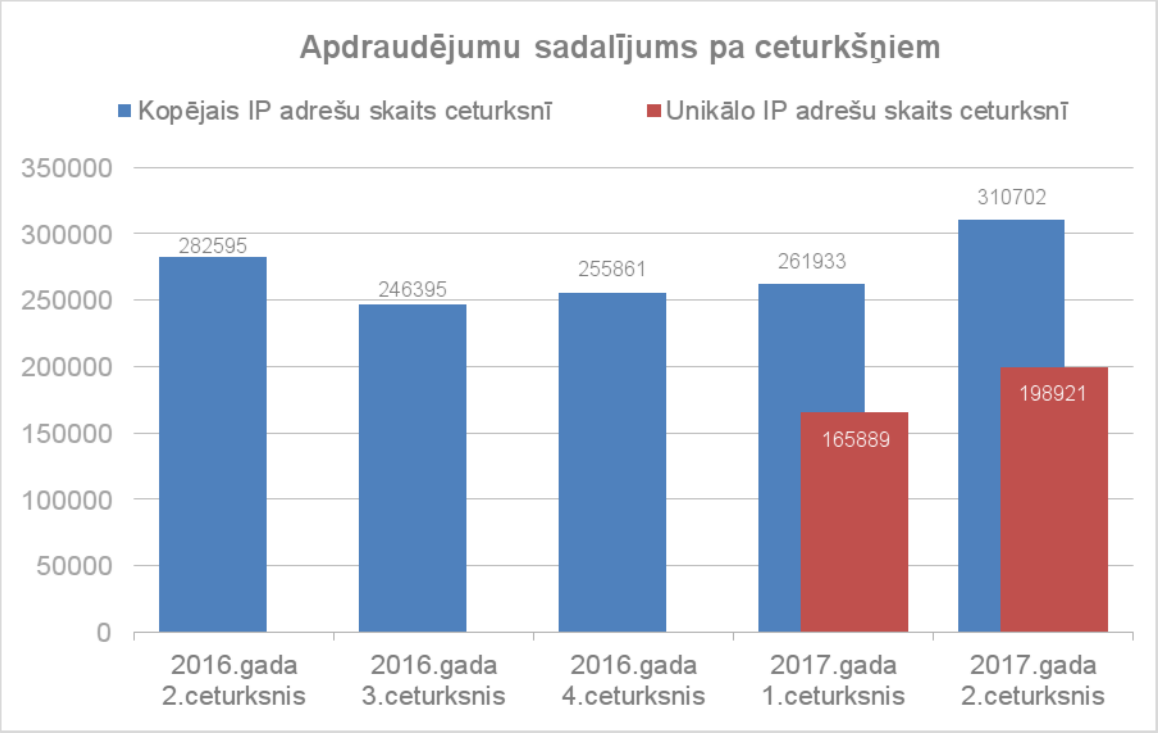


1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

Pārskata perioda beigās novērotais kāpums skaidrojams ar starptautiskajām izspiedējvīrusu kampaņām, kas skāra arī Latviju. Jūnijā liels apdraudēto IP adrešu daudzums saistīts ar WannaCry jeb WannaCrypt izspiedējvīrusa kampaņu.

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 2. ceturksnī tika reģistrēta 198 921 unikāla apdraudēta IP adrese (izmantojot iepriekšējo metodi, tās būtu 310 702 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.

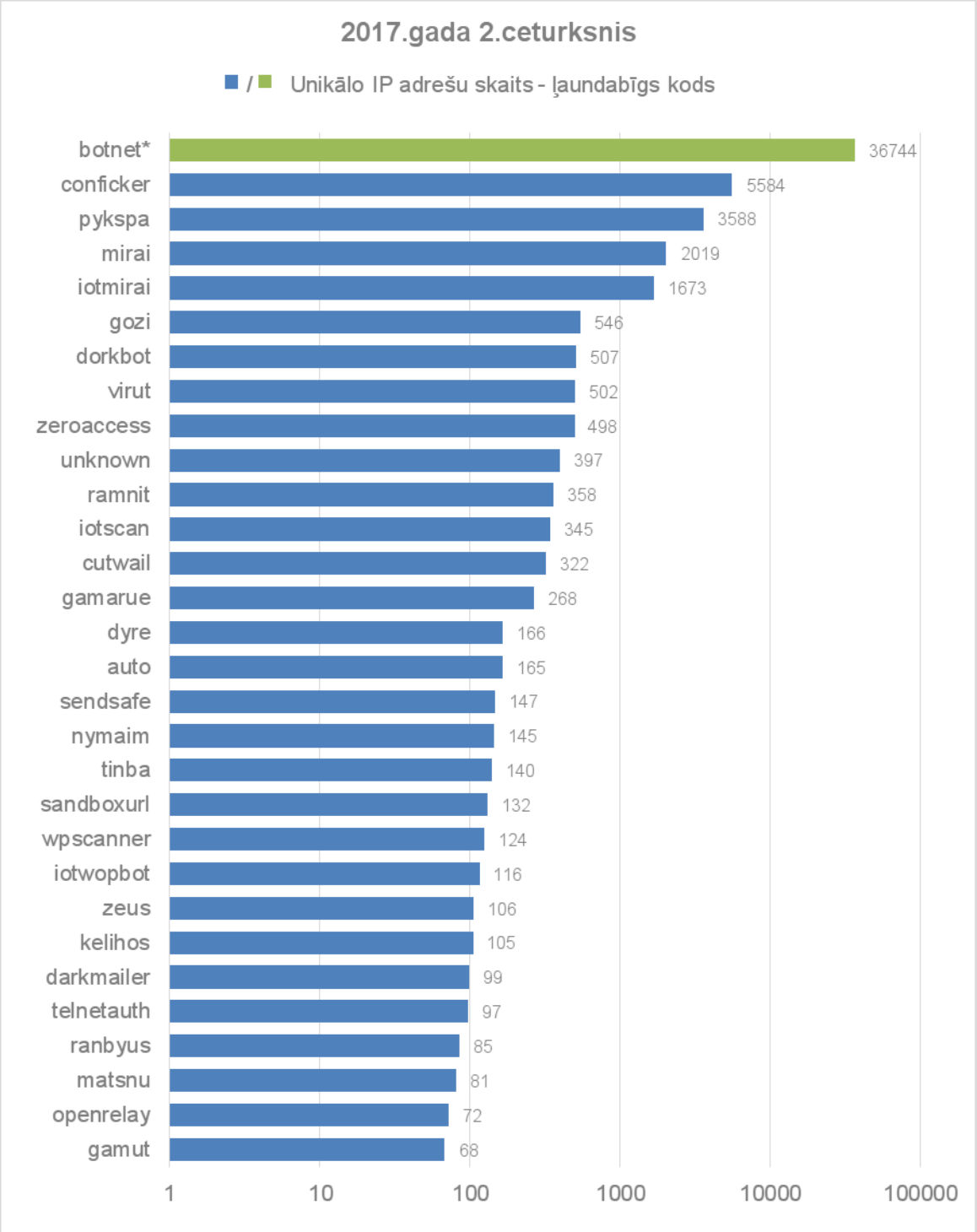


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2016. un 2017. gadā.

3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 2. ceturksnī pa apdraudējumu veidiem.

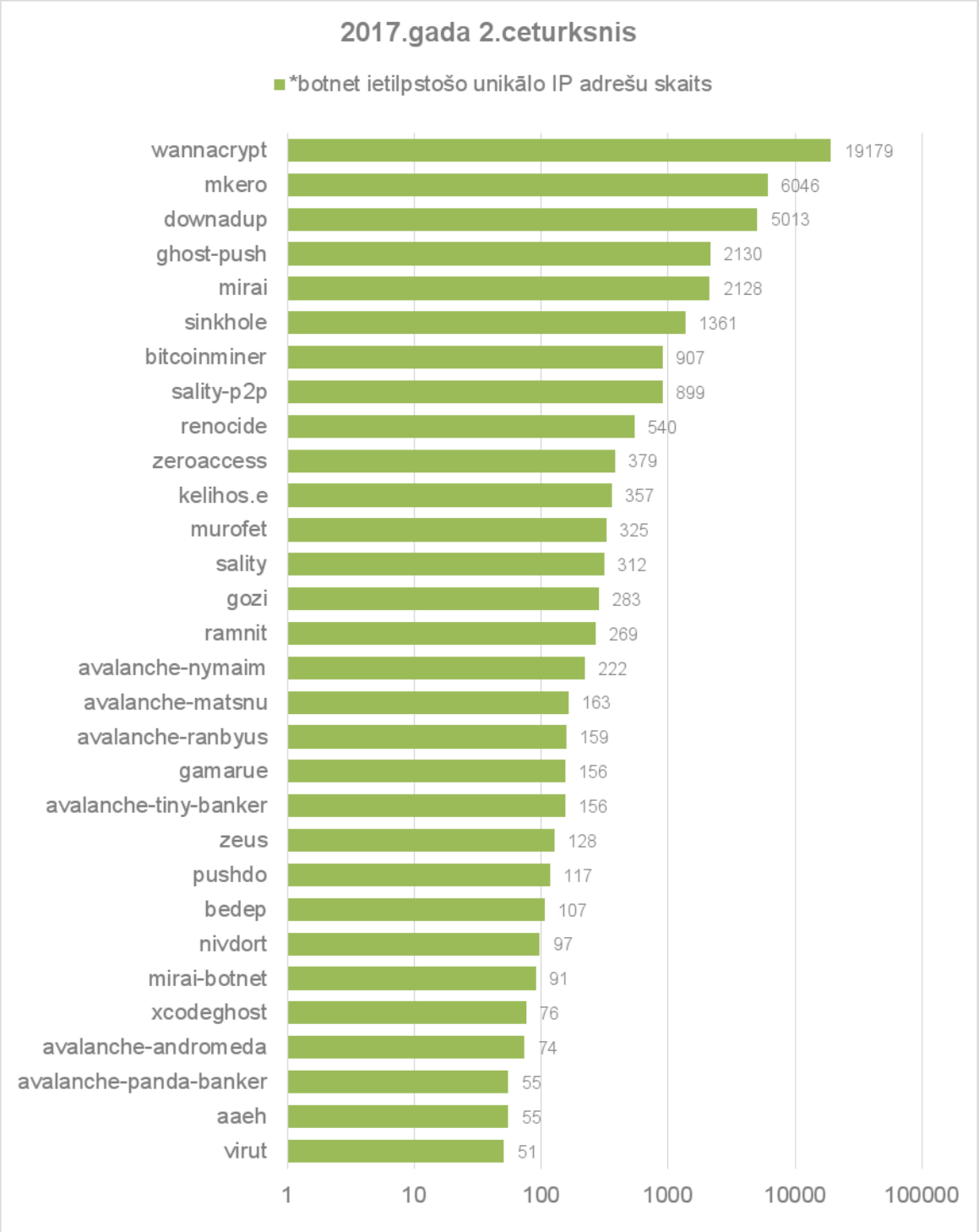
Izplatītākais apdraudējuma veids pārskata periodā bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais - ielaušanās mēģinājumi.

Pārskata periodā, salīdzinot ar iepriekšējo periodu, lielāko apdraudēto IP adrešu daudzuma pieaugumu radīja ļaundabīgs kods. Rādītājs palielinājās par 128%.



4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 2. 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.

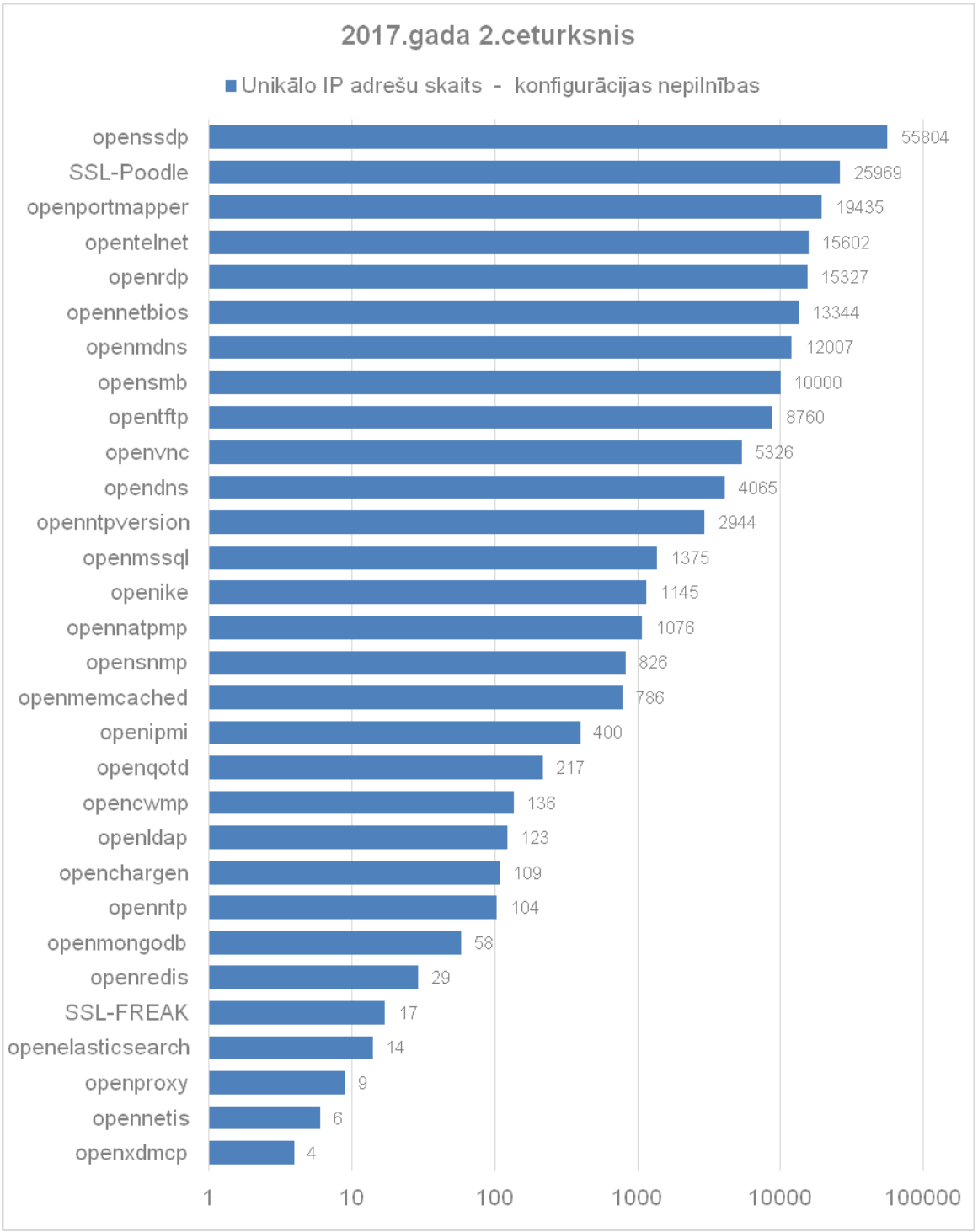


4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 2. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods/ *botnet*.

4.1. attēls parāda, ka maija vidū aizsākusies globālā izspiedējvīrusa WannaCry jeb WannaCrypt kampaņa radīja būtiskāko apdraudēto IP adrešu pieaugumu 2017. gada 2. ceturksnī. Neskatoties uz nelielo sašifrēto darbstaciju daudzumu (CERT.LV saņēma informāciju par 20 gadījumiem), inficēts tika daudz lielāks iekārtu skaits, bet, pateicoties atklātajam drošības slēdzim (killswitch), nenotika inficēto darbstaciju šifrēšana. Neskatoties uz to, ka ļaunatūra neveica datu šifrēšanu, tā no inficētās iekārtas turpināja izplatīties uz citām iekārtām, veicot iekārtu inficēšanu arī atkārtoti.

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 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 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Konfigurācijas nepilnību topā ir jaunpienācējs, kas uzreiz ierindojas astotajā vietā – tā ir

ievainojamība opensmb. Šī diezgan plaši izplatītā konfigurācijas nepilnība bija vainojama šifrējošo izspiedējvīrusu WannaCry un NotPetya straujajā izplatībā. Pēc WannaCry izplatības viļņa CERT.LV izsūtīja paziņojumus par nepieciešamību aizvērt uz internetu atvērto SMB protokola izmantoto 445. portu. Mēneša laikā bija vērojama konkrētās ievainojamības samazināšanās par 27%.

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.

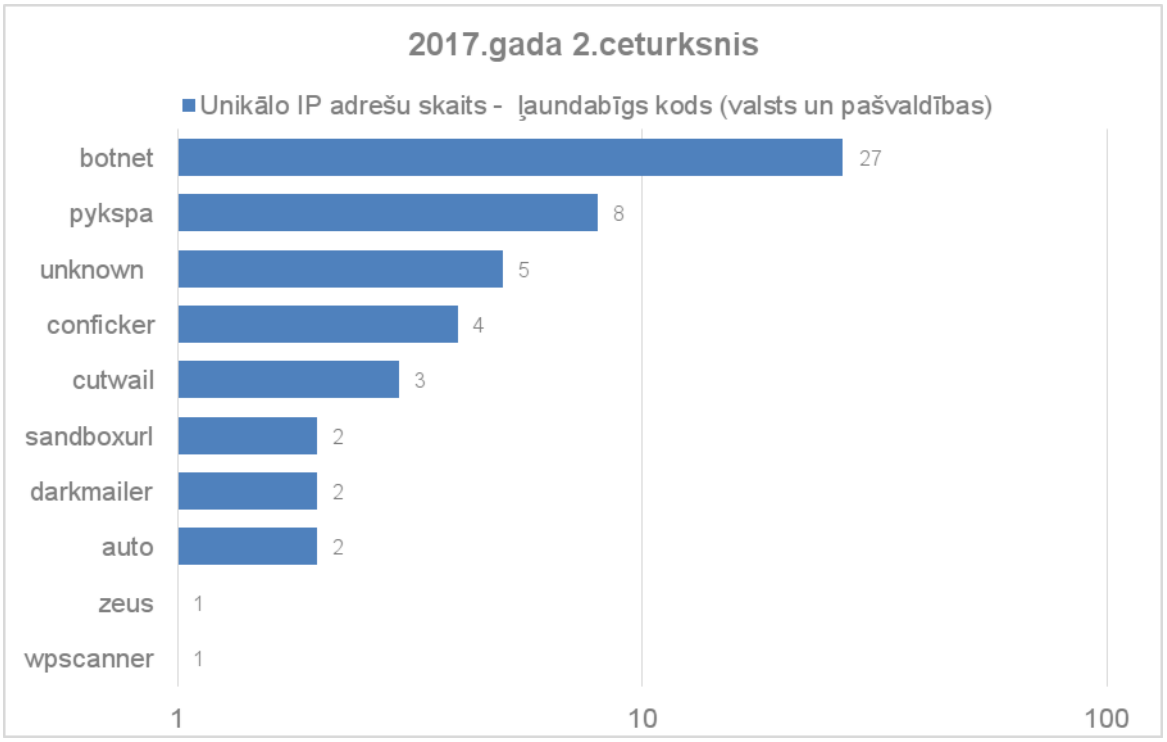
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

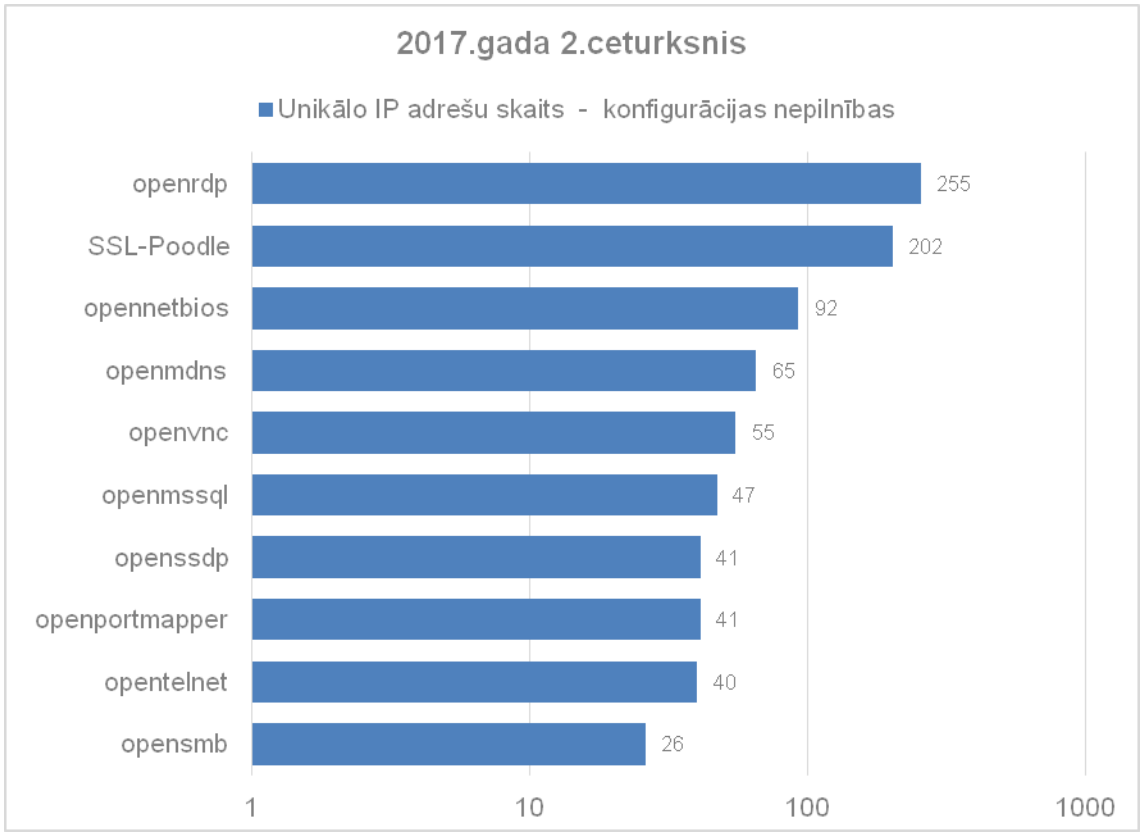
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2017. gada 2. ceturksnī.

Palielinoties ziņojumu avotu skaitam, ir palielinājies arī katras dienas ziņojumos reģistrēto apdraudēto valsts un pašvaldību iestāžu IP adrešu skaits. Tādējādi CERT.LV iegūst pilnvērtīgāku ainu par valsts un pašvaldību iestāžu kibertelpā notiekošo.



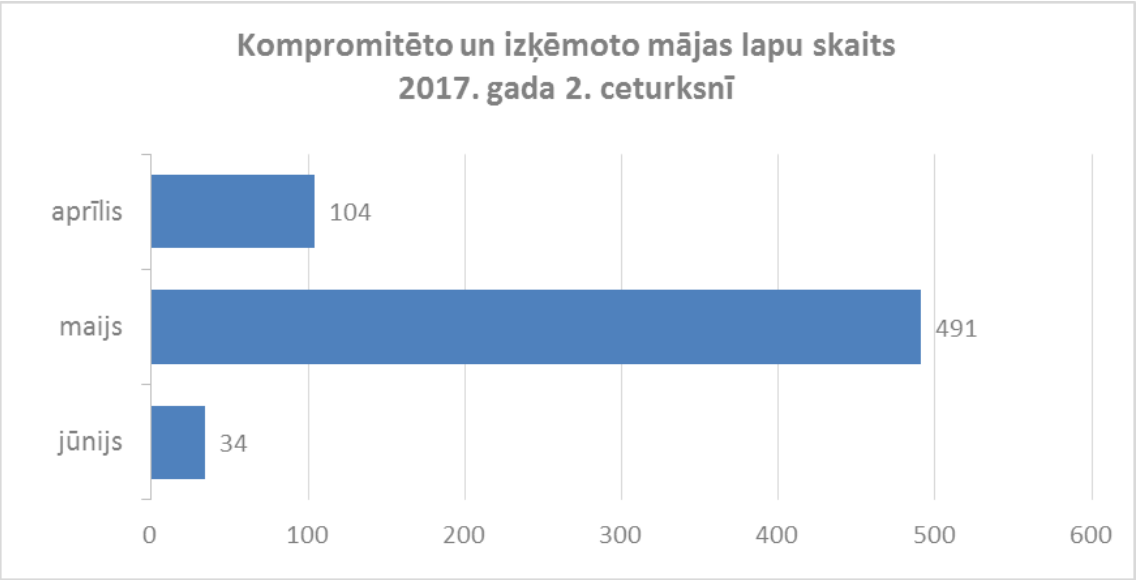
7.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 2. ceturksnī ar apdraudējuma veidu – Ļaundabīgs kods (TOP 10).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10).

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 629 kompromitētas un izķēmotas tīmekļa vietnes. No visām izķēmotajām vietnēm 622

gadījumos vietnes uzturēšanai tika izmantota Linux operētājsistēma, 3 gadījumos Windows, 3 gadījumos FreeBSD, bet 1 gadījumā par izmantoto operētājsistēmu nav informācijas. Sešas no visām pārskata periodā izķēmotajām tīmekļa vietnēm pēdējā gada laikā izķēmotas atkārtoti.



9.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2017. gada 2. ceturksnī.

Lielais maijā izķēmoto tīmekļa vietņu skaits skaidrojams ar to, ka maija vidū automatizēts uzbrukums tika vērsts pret tīmekļa vietnēm, kas izmantoja kāda mitinātāja sniegto bezmaksas mitināšanas pakalpojumu un netika pienācīgi uzturētas un atjauninātas. Tādas bija 2/3 no visām attiecīgo pakalpojumu izmantojošām vietnēm. Otrs pieauguma iemesls ir kāda mitinātāja serverim notikušais uzbrukums, kurā izķēmotas tika vairāk kā 300 tīmekļa vietnes.

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:

- 06.04. CERT.LV saņēma ziņu par publiski paziņotu ievainojamību kādas valsts iestādes tīmekļa vietnē. Informācija par XSS ievainojamību tika publicēta vietnē openbugbounty.org
- 07.04. Tika saņemta informācija 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.
- 10.04. Tika saņemts ziņojums par izspiešanas mēģinājumu sociālajā tīklā Facebook. Upura vārdā tika izveidots viltots sociālā tīkla konts, kurā izvietota dažāda rakstura informācija, par kuras dzēšanu tika prasīta samaksa. CERT.LV ieteica ar izspiedējiem nekomunicēt un nekādā gadījumā pieprasīto summu nemaksāt, jo tas, visticamāk, novestu pie atkārtotiem izspiešanas mēģinājumiem. CERT.LV ieteica vērsties arī policijā ar iesniegumu par izspiešanas mēģinājumu.

- Aprīlī vairāku pašvaldību grāmatvedes saņēma krāpniecisku e-pastu it kā pašvaldības vadītāja vārdā ar aicinājumu veikt steidzamu bankas pārskaitījumu. Pārbaudot Reply-To adresi, bija redzams, ka tā ir CEO fraud (CEO krāpšanas) tipa vēstule, jo pašvaldības domēna vārda vietā parādījās @privatceomail.com. Krāpnieki informāciju par pašvaldību darbiniekiem bija ieguvuši no pašvaldību tīmekļa vietnēm. CERT.LV ieteica pašvaldībām izmantot kādu rīku, kas slēpj tīmekļa vietnēs 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. Grāmatvedes uz krāpnieciskajiem e-pastiem neatbildēja, zaudējumi nodarīti netika.
- 11.04. 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.
- 19.04. Kāda pašvaldība lūdza drošības pārbaudi pašvaldības jaunajai tīmekļa vietnei pirms tā tiek padarīta publiski pieejama. Maijā tika veikta jaunās tīmekļa vietnes testēšana, kuras rezultātā tika atklātas divas būtiskas ievainojamības – openredirect un uz servera pieejami faili, kas atklāj informāciju par vietnē izmantoto programmatūru. Pašvaldībai tika nosūtīti drošības pārbaužu rezultāti un ieteikumi nepilnību novēršanai.
- 20.04. Tika saņemta ziņa par krāpniecisku loteriju WhatsApp vārdā, kura izmantoja domēnu " whatsappp.win". Vietne nesaturēja kaitīgu kodu, bet lietotājus, kas piedalījās "loterijā", aicināja sūtīt maksas sms, lai saņemtu balvu. CERT.LV informēja vietnes uzturētājus par vietnes kaitniecisko raksturu un lūdza vietni slēgt. Vietne tika slēgta.
- 25.04. Tika saņemta informācija par Facebook sociālā tīkla lietotāju datu pikšķerēšanas kampaņu, izmantojot saīsinātas saites, kas lietotājiem tiek nosūtītas paziņojumos (notifications). Lietotāji saņēma paziņojumus par konta bloķēšanu tuvāko 24h laikā, ja netiks veikta atkārtota autentifikācija, izmantojot paziņojumā norādīto saīsināto saiti. Saite lietotāju aizveda uz lietotāja datu izkrāpšanas vietni. CERT.LV pieprasīja vietnes aizvēršanu.
- 02.05. Tika saņemts ziņojums par kāda uzņēmuma tīmekļa vietnes neautorizētu klonu, kas izveidots, visticamāk, ar mērķi izkrāpt kompānijas klientu informāciju. Krāpnieciskā tīmekļa vietne tika izveidota ļoti līdzīga oriģinālajai, un lietotāji pēc reģistrācijas šajā vietnē tika piereģistrēti arī oriģinālajā. Krāpnieciskā vietne darbojās neilgu laiku un pēc tam tika atslēgta. Kompānija brīdināja savus klientus, lai pievērš pastiprinātu uzmanību tam, vai vietne, kurā tiek vadīta lietotāja informācija, ir oriģinālā. CERT.LV ieteica arī sazināties ar krāpnieciskās vietnes uzturētājiem un palūgt žurnālfailus, kas palīdzētu analizēt notikušo.
- 02.05. 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.
- 03.05. Kāda uzņēmuma darbinieki saņēma e-pastus par steidzama maksājuma veikšanu. Neskatoties uz labo noformējumu, e-pasti tika identificēti kā CEO krāpniecība, jo sūtītāja

adrese neatbilda līdzšinējiem sadarbības partneriem un izskatījās aizdomīga. Zaudējumi nodarīti netika.

- 06.05. Tika saņemts ziņojums par Latvijas IP adresi, kurā tika uzturēta nelegāla informācija par maksājumu karšu datiem. Incidents nodots Valsts policijai.
- 08.05. Tika saņemta informācija par krāpnieciskiem e-pastiem Swedbank vārdā. E-pastā lietotājs tika brīdināts par it kā veiktu neautorizētu pieslēgšanos un aicināts veikt konta verifikāciju, sekojot e-pastā norādītajai saitei, un ievadīt savus datus. Krāpnieciskā vietne tika slēgta. CERT.LV nav ziņu, ka kāds būtu cietis šajā krāpniecībā.
- 09.05. Kāda valsts iestāde lūdza atbalstu drošības pārbaužu veikšanai kādai informācijas sistēmai, kurai noteikts paaugstinātas drošības sistēmas statuss. Maija otrajā pusē tika veikti ielaušanās testi, ievainojamības vietnē netika atrastas. Iestādei tika nosūtīti ielaušanās testu rezultāti.
- 12.05. Tika saņemta informācija par uzbrukumu kādam valsts iestādes portālam. Žurnālfailu analīze atklāja, ka 8. maijā 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.
- 13.05. Visā pasaulē strauji izplatījās šifrējošais izspiedējvīruss WannaCry, inficējot 200 000 Windows iekārtas 150 valstīs. CERT.LV saņēma ziņas par 20 cietušajiem Latvijā, bet atšķirībā no ārvalstīm, kur starp cietušajiem ir gan slimnīcas, gan telekomunikāciju kompānijas, Latvijā cietušas bija privātpersonas un daži mazie uzņēmumi.
- 16.05. Tika saņemts ziņojums par uzbrukumu kādas valsts iestādes tīmekļa vietnei. Uzbrukums tika veikts no Turcijas IP adreses ar mēģinājumu uzlauzt iestādes e-pakalpojumu un datu publicēšanas vietni. Uzbrukumā izmantotā adrese tika bloķēta.
- 19.05. Tika saņemta informācija par iespējami kaitniecisku e-pastu no it kā lokālas kompānijas, kas izsaka biznesa sadarbības piedāvājumu. E-pasts bija profesionāli sagatavots, bet, neskatoties uz to, ka komunikācija notika starp vietējām kompānijām, tika rakstīts angļu valodā. Pielikumā atradās .ZIP arhīva fails, kura analīze, diemžēl, nebija iespējama faila bojājumu dēļ.
- 24.05. Tika saņemts ziņojums no kāda uzņēmuma par viltotu e-pasta saraksti. Aplūkojot incidenta materiālus, varēja secināt, ka uzbrucējs ir kompromitējis kompānijas e-pastu un tādējādi iejaucas kompānijas sarakstē un lūdz kompānijas partneriem mainīt pārskaitījumiem paredzētos bankas kontus. CERT.LV ieteica veikt e-pasta serveru pārbaudi, kā arī izveidot SPF ierakstus, kas ļautu e-pastus ar kompānijas domēnu izsūtīt tikai no kompānijas e-pasta servera.
- 31.05. Tika saņemta ziņa par WannaCry izspiedējvīrusa pārlūka versiju, kas lietotājam parāda brīdinājumu, ka dators ir inficēts ar WannaCry vīrusu un visi faili ir šifrēti, bet patiesībā ir viltus paziņojums un tiek parādīts tikai interneta pārlūkā.
- 02.06. Kādas valsts iestādes tīmekļa vietne piedzīvoja DDoS tipa uzbrukumu, kurā bija iesaistītas daudzas ārvalstu IP adreses. Iestāde lūdza palīdzību CERT.LV uzbrukuma novēršanā un incidenta risināšanā. Uzbrukuma ietekmi izdevās novērst vietnes uzturētājam, atslēdzot ārvalstu tīkla plūsmu. CERT.LV veica žurnālfailu analīzi un sniedza

ieteikumus vietnes drošības uzlabošanai, piemēram, iesakot robotu darbības ierobežošanu vietnē.

- 05.06. Kāds lietotājs ziņoja par aizdomīgiem procesiem savā datorā un lūdza palīdzību situācijas risināšanā. CERT.LV identificēja vīrusu, kas pārvirza lietotāju uz reklāmas lapām, un ieteica soļus, kā atbrīvot datoru no infekcijas.
- 05.06. Tika saņemts ziņojums no kādas valsts iestādes par vienas dienas laikā saņemtiem 112 e-pastiem ar sociālās inženierijas elementiem no vienas konkrētas e-pasta adreses. Iestāde bloķēja sūtītāja e-pasta adresi un piekļuvi e-pastā norādītajai saitei. CERT.LV sazinājās ar saitē norādītās vietnes uzturētājiem un lūdza kaitīgo vietni bloķēt. Vietne tika dzēsta.
- 05.06. Tika saņemts ziņojums par maldinoša izskata tīmekļa vietni, kas līdzinās kādas valsts iestādes uzturētajai vietnei. Vietnē tika pretlikumīgi izmantots valsts ģerbonis, un vietne tika izveidota, lai reklamētu medikamentus. CERT.LV sazinājās ar viltotās vietnes uzturētājiem un lūdza to slēgt.
- 06.06. Tika saņemta informācija no kāda uzņēmuma, ka vairāku mēnešu garumā uzņēmuma klienti saņēmuši it kā uzņēmuma vārdā sūtītus piedāvājumus, bet uzņēmuma nosaukums bija neatbilstošs un kā kontaktpersona tika norādīts darbinieks, kas uzņēmumā vairs nestrādā. Vēstules saturs nesaturēja specifisku informāciju, kas liecinātu par uzņēmuma e-pasta kompromitēšanu, taču CERT.LV ieteica uzņēmumam brīdināt savus klientus par viltotu e-pastu izplatīšanos.
- 08.06. Tika konstatēta kādas valsts iestādes tīmekļa vietnes izķēmošana. CERT.LV konstatēja vietnē SQL injekcijas ievainojamību. Tika informēti vietnes uzturētāji.
- 08.06. Tika saņemts ziņojums par lietotni, kas it kā piedāvā Facebook lietotājiem aplūkot sava profila statistiku, bet rezultātā pārvirza tos uz krāpniecisku vietni ar mērķi izkrāpt Facebook lietotāja datus. Krāpnieciskās vietnes uzturētāji tika brīdināti, vietne tika dzēsta.
- 08.06. Tika saņemta ziņa no kādas valsts iestādes par kaitīgu e-pastu, kuru neatpazina izmantotā antivīrusu programmatūra. E-pasts tika sūtīts kā darba pieteikums un pielikumā saturēja failu ar Macros kodu, kas dokumentā bija maskēts. CERT.LV ieteica iestādei bloķēt IP adresi, ar kuru koda izpildes gadījumā tiktu izveidots savienojums.
- 09.06. Tika saņemts ziņojums par viltotu kādas valsts iestādes lapu sociālajā tīklā Facebook. Viltotājā lapā tika gan pārpublicētas ziņas no oficiālā iestādes profila, gan arī ievietotas ziņas ar neatbilstošu saturu. Iestāde lūdza CERT.LV palīdzību viltus lapas slēgšanā. Šis bija jau otrais gadījums, kad sociālajā tīklā Facebook parādās iestādes lapas viltojums. CERT.LV sazinājās ar sociālo tīklu un lūdza viltus lapu aizvērt.
- 09.06. Tika saņemta informācija par vairākiem kādas valsts iestādes resursiem, kuri 3. jūnijā piedzīvojuši uzbrukumus. Kopā tikuši atvairīti aptuveni 3.5 miljoni pieprasījumu. CERT.LV saņēma detalizētu informāciju par incidentu.
- 12.06. Tika saņemta informācija no kāda lietotāja par datorā konstatēto šifrējošo izspiedējvīrusu BTCWare. Konkrētajam vīrusa variantam pirms dažām dienām nopublicētā atšifrēšanas atslēga nederēja. Lietotājam nebija sagatavotas failu rezerves kopijas.

- 12.06. Saņemta informācija par pikšķerēšanas kampaņu Facebook datu izkrāpšanai. Lietotāji saņēma it kā Facebook vārdā sūtītus e-pastus ar paziņojumiem par jauniem draudzības uzaicinājumiem ar saiti uz krāpniecisku vietni. Krāpnieciskā vietne aizvērta.
- 12.06. Tika saņemta informācija par uzlauztu Ubiquiti maršrutētāju, kurš tika izmantots kā komandu- un kontroles centrs ļaunatūras Trickbot izplatīšanai, kas ir banku trojānis un tiek izmantots finanšu datu izkrāpšanai. CERT.LV sazinājās ar interneta pakalpojumu sniedzēju, kas nodrošināja maršrutētāja programmatūras atjaunināšanu, lai novērstu ievainojamību.
- 12.06. Tika saņemts ziņojums par pikšķerēšanas vietni Google datu izkrāpšanai. Labi sagatavots pikšķerēšanas e-pasts tika nosūtīts kā rezervācijas pieteikums viesu namam. E-pastā tika norādīta saite it kā uz dokumentu ar informāciju par rezervācijas datumiem un personām, bet tika atvērta tīmekļa vietne Google datu izkrāpšanai. CERT.LV informēja vietnes uzturētājus par kaitīgo saturu, vietne tika slēgta.
- 14.06. Tika saņemta informācija par DDoS uzbrukumu spēļu serverim. Kāds spēles lietotājs pēc kaitniecisku darbību veikšanas, kas izdarītas, apejot servera aizsardzību, tika uz laiku bloķēts. Pēc nobloķēšanas konkrētais lietotājs no dažādām IP adresēm veica īslaicīgu DDoS uzbrukumu, kas uz laiku paralizēja servera darbību. CERT.LV ieteica servera uzturētājam pasākumus DDoS uzbrukumu ietekmes mazināšanai, kā arī zaudējumu gadījumā vērsties ar iesniegumu policijā.
- 16.06. Tika saņemta informācija par ievainojamību kādā tīmekļa vietnē. Tika konstatēts, ka FTP serverim iespējams piekļūt bez autorizācijas. Uz konkrētā servera atradās arī kompānijas klientu datu bāze, kas saturēja fizisku personu datus. CERT.LV brīdināja vietnes uzturētāju.
- 22.06. Tika saņemta informācija par WhatsApp krāpšanu. Lietotāji saņēma paziņojumu, ka 48 stundu laikā pakalpojums tiks pārtraukts un visi dati, ieskaitot fotogrāfijas un video, dzēsti, ja lietotājs neveiks pakalpojuma atjaunošanu, nospiežot uz saites. Saite aizveda uz krāpniecisku vietni, kurā lietotājam bija jāievada kredītkartes dati, lai veiktu maksu par WhatsApp pakalpojuma pagarināšanu. Uzlauztās un krāpniecībai izmantotās vietnes uzturētāji brīdināti par kredītkaršu datu izkrāpšanu vietnē, kaitīgais kods no vietnes dzēsts.
- 27.06. Tika saņemts ziņojums par krāpšanas mēģinājumu, izsludinot krāpniecisku loteriju kādas kompānijas vārdā. Kaitnieciskās vietnes uzturētāji brīdināti. CERT.LV nav ziņu, ka kāds krāpšanā būtu cietis.
- 27.06. Pasaule piedzīvoja vēl vienu šifrējošā izspiedējvīrusa izplatības vilni. 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.
- 28.06. Tika saņemts ziņojums par uzbrukumu kādas pašvaldības tīmekļa vietnei. Tika konstatēts, ka uzbrucēji ielauzušies serverī un izdzēsuši tīmekļa vietni un žurnālfailus. Tīmekļa vietne tika atjaunota no rezerves kopijas. CERT.LV iesaistījās incidenta analīzē. Informācija nodota policijai.

CERT.LV pasākumi incidentu novēršanai:

- 16.05. CERT.LV apzināja vīrusa WannaCry apdraudētās valsts un pašvaldību iestādes un apdraudētajām iestādēm izsūtīja brīdinājumu un ieteikumus tālākai rīcībai. Pēc izsūtītā brīdinājuma un publiskiem aicinājumiem medijos aizvērt uz internetu atvērto apdraudēto TCP 445. portu, kļūdaini konfigurēto apdraudēto iekārtu skaits mēneša laikā saruka par 27%.
- 15.06. CERT.LV izsūtīja informāciju elektronisko sakaru komersantiem par būtisku ievainojamību plaši izmantotajā Ubiquiti AirOS.
- 28.06. CERT.LV izsūtīja informāciju valsts un pašvaldību iestāžu par IT drošību atbildīgajiem par izspiedējvīrusa NotPetya izplatīšanas mehānismiem un apdraudējuma novēršanu.
- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV sagatavotajās iknedēļas 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.

Pārskata periodā tika saņemti daudzi ziņojumi, kas bija saistīti ar plaši izmantoto mobilo tērzēšanas lietotni WhatsApp. Lietotnes vārdā tika izplatīta krāpnieciska ziņa par „loteriju", kura neuzmanīgiem lietotājiem beidzās ar paaugstinātas maksas īsziņu sūtīšanu. Lietotāji saņēma arī krāpnieciskus „brīdinājumus" par pakalpojuma pārtraukšanu, ja netiks veikta pakalpojuma apmaksa, izmantojot maksājumu karti. Lietotājam, veicot maksājumu norādītajā vietnē, tika izkrāpts gan maksājums, gan viņa kartes dati.

Krāpnieki izmantoja arī globālo ažiotāžu, kas bija saistīta ar WannaCry šifrējošā izspiedējvīrusa vilni. Mobilo lietotņu lejuplādēšanas vietnēs parādījās lietotnes, kas piedāvāja pasargāt Android mobilās ierīces no WannaCry draudiem, neskatoties uz to, ka WannaCry vīruss radīja reālu apdraudējumu tikai Windows iekārtām.

Pārskata periodā tika saņemti arī ziņojumi par SlemBunk Android trojāņa gadījumiem. Šis trojānis paredzēts banku mobilo lietotņu datu pārtveršanai un lietotņu sagatavotās informācijas modificēšanai. Šobrīd trojānis nav ticis pielāgots Latvijas „tirgum" un, neskatoties uz to, ka inficējis mobilās iekārtas, neveic ļaundabīgas darbības, jo nav pielāgots Latvijā lietoto banku lietotnēm. Taču uz šādu mobilo iekārtu aizsardzības metodi kā vienīgo nevajadzētu paļauties ilgtermiņā, jo ļaundari ar laiku atrod veidus kā ātri un lēti pielāgot savu "produktu" nepieciešamajam "tirgum".

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

Pārskata perioda aktuālākās tēmas bija izspiedējvīrusu WannaCry un NotPetya globālās izplatīšanas kampaņas, par kuru upuriem citās pasaules valstīs kļuva gan lidostas, gan slimnīcas, gan bankas un valsts pārvaldes iestādes, gan virkne citu uzņēmumu un institūciju.

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.

Plašāko mediju interesi pārskata periodā izraisīja tēmas par WannaCry un NotPetya izspiedējvīrusiem, kā arī tiesībām pieprasīt domēnu vārdu bloķēšanu.

Informācija par CERT.LV tīmekļa vietnēm:

https://www.cert.lv populārākā bija ziņa par WannaCry izspiedējvīrusa kampaņu, kurai bija 4490 unikāli skatījumi. Otra populārākā bija ziņa par izspiedējvīrusa NotPetya pazīmēm un aizsardzību, kuru skatījuši 2461 unikāls apmeklētājs. Trešā populārākā bija Kontaktu sadaļa ar 1454 unikāliem skatījumiem. Kopā CERT.LV mājas lapai bijuši 21 063 lapu skatījumi (pieaugums par 37,73% pret pagājušo ceturksni), kurus veido 13 517 unikāli lapu skatījumi (pieaugums par 51,94% pret pagājušo ceturksni).

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 14 389 apmeklējumi (pieaugums par 3,17% pret iepriekšējo ceturksni), no tiem 10 712 unikāli apmeklējumi (kritums par 6,21% pret iepriekšējo ceturksni). CERT.LV turpina tulkot un portālā a izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts).

Portālā esidross.lv publicētie raksti:

- Ko var mācīties no WannaCry
- Mūsdienu tiešsaistes bērnu drošība
- Paroļu frāzes

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1780.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 680.
- 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.

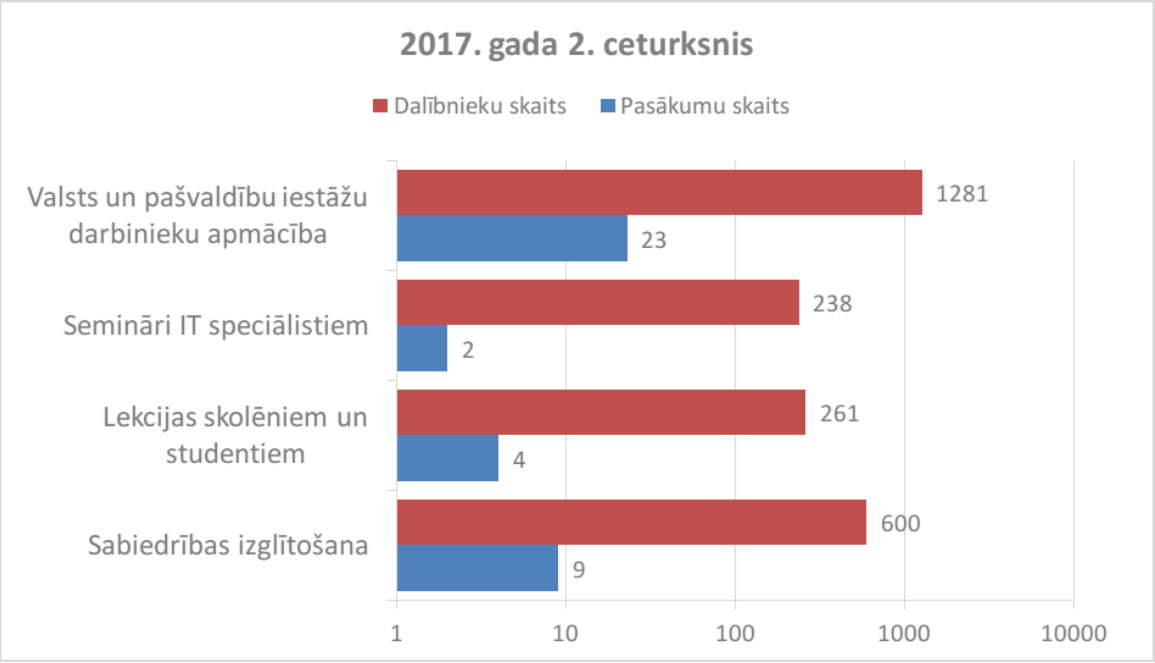
6. aprīlī CERT.LV rīkoja semināru IT drošības speciālistiem „Esi drošs", kurā iepazīstināja klātesošos ar IT drošības aktualitātēm un aplūkoja tādas tēmas kā mobilo iekārtu drošības aspekti, lietu interneta drošība, uzbrukuma vektori sociālajos tīklos un open-source informācijas riski.

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.

2. jūnijā CERT.LV sniedza atbalstu Accenture „Night Hack 2017" pasākuma tapšanā gan informatīvi, gan sagatavojot pasākumam paredzētu uzdevumu.

Pārskata periodā CERT.LV par IT drošību izglītoja 2380 cilvēkus, iesaistoties 38 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2017. gada 2. ceturksnī.

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

15. jūnijā tika pieņemti grozījumi Informācijas tehnoloģiju drošības likumā, kas paredz CERT.LV tiesības pieprasīt ".lv" domēna vārda atslēgšanu, ja tas ir iesaistīts drošības incidentā, kas būtiski apdraud lietotāju, informācijas sistēmu vai elektronisko sakaru tīklu drošību, un drošības incidentu nav iespējams novērst citā veidā.

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 02.05. Tikšanās Aizsardzības ministrijā par pamatpakalpojumu operatoru identifikāciju saistībā ar NIS direktīvu.
- 03.05. CERT.LV pārstāvis piedalījās Saeimas sēdē, kurā tika izskatīti grozījumi IT drošības likumā.
- 11.05. DEG sanāksme.
- 22.05. Tikšanās Aizsardzības ministrijā ar Sabiedrisko pakalpojumu regulēšanas komisiju un NIC par digitālo pakalpojumu sniedzēju identifikāciju saistībā ar NIS direktīvu.
- 24.05. Tikšanās ar Aizsardzības ministriju par MK noteikumu Nr.442 ieviešanu.
- 06.06. CERT.LV pārstāvis piedalās Saeimas sēdē, kur 3.lasījumā tiek izskatīti IT drošības likuma grozījumi.
- 07.06. Tikšanās ar Aizsardzības ministriju un LIX saistībā ar NIS direktīvu.

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta 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 30. jūnijam CERT.LV apkopojusi informāciju par 1312 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.

Iepriekšējā pārskata periodā CERT.LV izsūtīja 153 elektroniskās vēstules Elektronisko sakaru komersantiem par rīcības plānu atjaunošanu un izveidošanu. Šī pārskata perioda beigās rīcības plānu statistika ir šāda:

- saņemti 14 atjaunoti ESK rīcības plāni;
- saņemts 21 jauns ESK rīcības plāns;
- 15 ESK rakstiski apliecināja, ka neuztur publisko elektronisko sakaru tīklu;
- 17 komersantiem, kas bija atbildējuši par vēstules saņemšanu, bet neiesnieguši plānus, tika atkārtoti nosūtīta vēstule par rīcības plāna sastādīšanu. No tiem 2 atbildēja, ka neuztur publisko elektronisko sakaru tīklu, un 1 plāns tika iesniegts.

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 61 pantā minētie gadījumi aplūkoti atskaites 2. punktā.

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

Pārskata periodā notika NATO CCDCOE organizētās kiberdrošības mācības „Locked Shields 2017". CERT.LV piedalījās gan organizatoru (baltajā), gan aizstāvju (zilajā), gan uzbrucēju (sarkanajā) komandā. CERT.LV un US EUCOM apvienotā komanda mācībās ieguva 5. vietu.

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. Melnkalnes pārstāvji viesojās arī Aizsardzības ministrijā, Kiberaizsardzības vienībā, tikās ar LIKTA un citām nevalstiskajām organizācijām, uzzināja par IT drošības likumdošanu, NIS ieviešanu un citām ministrijas iniciatīvām.

Vizītes mērķis bija apmainīties ar pieredzi un informāciju, lai stiprinātu Melnkalnes CERT kapacitāti.

Šādu vizīti CERT.LV sadarbībā ar Aizsardzības ministriju rīkoja pirmo reizi. Vizītes rezultātā tika stiprināta sadarbība starp Latvijas un Melnkalnes CERTiem un izstrādāti vairāki informatīvi materiāli, kurus var pielietot CERTu apmācību vizītēm arī nākotnē

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 05.-07.04. CERT.LV pārstāvis piedalījās ar NIS direktīvas ieviešanu Eiropas Savienības dalībvalstīs, tostarp drošības īstenošanas akta izstrādi digitālo pakalpojumu sniedzējiem, saistītos pasākumos „NIS Security Measures workshop" Briselē.
- 05.04. Devītā trīs Baltijas valstu kiberdrošības politikas koordinēšanas sanāksme Viļņā.
- 20.04. Portugāles CERT vienība lūdza atbalstu iespējamas paaugstinātas haktīvistu aktivitātes gadījumā. CERT.LV apliecināja gatavību sadarboties.
- 24.-29.04. Kiberdrošības mācību "Locked Shields 2017" norise.
- 25.04. CERT.LV pārstāvis piedalās FI-ISAC sanāksmē Barselonā, Spānijā.
- 08.-10.05. Melnkalnes CERT pārstāvju vizīte.
- 09.05. Tikšanās ar Dānijas Kiberdrošības centra vadību.
- 09.-10.05. 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.
- 12.-19.05. CERT.LV pārstāvis vadīja TF-CSIRT sanāksmi Hāgā un vairāki CERT.LV pārstāvji piedalījās NCSC-NL organizētajā „One Conference", kā arī TF-CSIRT sanāksmē.
- 22.-24.05. Kiberdrošības mācību "Locked Shields 2017" pēcpasākuma sanāksme Tallinā, Igaunijā.
- 29.-30.05. CERT.LV pārstāvji piedalījās "CERT-EE Symposium" Tallinā, Igaunijā. CERT.LV pārstāvji piedalījās arī Capture the Flag sacensībās, iegūstot 2. vietu.
- 29.05.-03.06. CERT.LV pārstāvis piedalījās un vadīja vairākas sesijas "The Networking Conference" Lincā, Austrijā.

- 30.-31.05. CERT.LV pārstāvis piedalījās "2nd CSIRT Network Meeting" Tallinā, Igaunijā.
- 01.06. CERT.LV pārstāvis piedalījās CEF projekta CERTu sadarbības platformas ieinteresēto pušu sanāksmē Tallinā, Igaunijā.
- 11.-19.06. CERT.LV pārstāvji piedalījās FIRST konferencē Puertoriko. CERT.LV pārstāvis sniedza prezentāciju par CERTu darbības pilnveidošanu "Non-Formal - Everything Out of Normal", kā arī tika vadītas konferences sesijas.
- 13.06. Telefonintervija ar Rumānijas CERT saistībā ar pētījumu par CERTu sadarbību ar tiesībsargājošajām institūcijām.

Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

- 19.04. CERT.LV pārstāvis tiekas ar studentu, lai atbildētu uz jautājumiem, kas saistīti ar bakalaura darba izstrādi.
- 28.04. Tikšanās ar LIKTA par balvas „Platīna pele" nolikumu, lai pārrunātu iespēju apbalvot arī labāko kiberdrošības iniciatīvu.
- 09.05. CERT.LV pārstāvji tikās ar studentu, lai atbildētu uz jautājumiem, kas saistīti ar bakalaura darba izstrādi par lietu internetu.
- 25.05. CERT.LV pārstāvis piedalījās Net-Safe konsultatīvās padomes sēdē.
- 07.06. CERT.LV pārstāvis piedalījās Latvijas Universitātes studentu kvalifikācijas darbu aizstāvēšanā.

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 piedalījās sanāksmē ar VAS Latvijas Valsts radio un televīzijas centra (turpmāk – LVRTC), Valsts reģionālās attīstības aģentūras un ISACA pārstāvjiem, lai vienotos par noslēdzošajiem jautājumiem, kas skāra Ministru kabineta noteikumus, kuri tika izstrādāti uz Fizisko personu elektroniskās identifikācijas likuma pamata.
- CERT.LV pārstāvji tikās ar LVRTC pārstāvjiem, lai pārrunātu klātienes auditu, darbības izbeigšanas plānu, gaidāmo tikšanos ar auditoriem un prasībām, ko noteikt LVRTC, kā arī par ielaušanās testu veikšanas kārtību. Sanāksmes laikā CERT.LV un LVRTC pārstāvji vienojās, ka Elektroniskās identifikācijas uzraudzības komitejas (turpmāk – Uzraudzības iestāde) pārstāvji tiksies ar LVRTC auditoriem.

- CERT.LV pārstāvis apmeklēja sanāksmi Briselē, kuras laikā noteica Vācijas pieteiktās nacionālās elektroniskās identifikācijas shēmas pārbaužu apjomu un definēja pienākumus pārbaužu veicējiem. Tās laikā definēja arī Latvijas pozīciju Vācijas eID shēmas peer review uz konkrēto brīdi. CERT.LV pārstāvis novērotāja lomā līdzdarbojās peer review grupā no Latvijas.
- CERT.LV pārstāvis piedalījās LVRTC audita novērošanā, kuru veica Vācijas auditori. Audita gaitā novērotais tika apkopots vienā dokumentā, kas nodots Aizsardzības ministrijas rīcībā.
- CERT.LV pārstāvji piedalījās sanāksmē ar Latvijas komercbanku asociāciju, lai apspriestu izstrādāto Ministru kabineta noteikumu projektu redakcijas.
- CERT.LV pārstāvji piedalījās sanāksmē ar Datu valsts inspekcijas pārstāvjiem, lai vienotos par Uzraudzības iestādes funkciju pārņemšanu attiecībā uz uzticamiem sertifikācijas pakalpojuma sniedzējiem, tostarp uzticamības sarakstu pārvietošanai uz Elektroniskās identifikācijas uzraudzības komitejas tīmekļa vietni.

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 01.04.2017. līdz 30.06.2017. ir saņēmusi un izvērtējusi 103 ziņojumus. No tiem 40 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 9 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 9 ziņojumos konstatēta personas goda un cieņas aizskaršana, 1 gadījumā konstatēti vardarbīga rakstura materiāli un 1 ziņojums saņemts par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 12 ziņojumi, 12 ziņojumu saturs nav bijis pretlikumīgs, 19 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 24 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 9 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.

2017. gada 19. jūlijā
Sagatavotājs – Līga Besere
Tālrunis: 67085888
E-pasts: liga.besere@cert.lv