Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2016

2016. gada 2. ceturksnis (01.04.2016. – 30.06.2016.)

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

2016.gada 2.ceturksnī CERT.LV reģistrēja un apstrādāja 798 augstas prioritātes incidentus un 281 797 zemas prioritātes incidentus.

Būtiska ceturkšņa iezīme ir šifrējošos izspiedējvīrusus saturošu e-pastu izplatīšana gan uzņēmumiem, gan individuāliem datorlietotājiem. Daļā gadījumu, neskatoties uz preventīvajiem pasākumiem, vīrusam izdevās iekļūt datorā un nošifrēt vismaz daļu datora satura, pirms vīruss tika atklāts. Atsevišķos gadījumos lietotājiem bija laicīgi sagatavotas svarīgo dokumentu rezerves kopijas, taču daļa lietotāju par rezerves kopijām nebija parūpējušies un nošifrētos failus atgūt nespēja.

Otrs pārskata periodam raksturīgs incidentu veids ir "CEO krāpšana", kurā izmantoti viltoti e-pasti, kas sūtīti kompānijas vadītāja vai sadarbības partnera vārdā, lai panāktu nozīmīgu naudas summu pārskaitīšanu uz krāpnieku bankas kontiem. Ļaundari bieži piekļūst uzņēmumu e-pastiem, izmantojot sociālo tīklu piekļuves datu noplūdēs iegūto informāciju, jo daudzi lietotāji virknē interneta resursu izmanto identisku paroli. Otrs biežākais paroles iegūšanas veids ir datora inficēšana ar ļaunatūru. Iegūstot kontroli pār e-pastu, ļaundari var precīzi izpētīt situāciju un atbilstošajā brīdī veikt ļoti ticami noformētu uzbrukumu. Lietotās programmatūras regulāra atjaunināšana un atšķirīgu paroļu izmantošana mazina e-pastu uzlaušanas risku.

18.-23. aprīlī CERT.LV piedalījās NATO kiberdrošības mācībās "Locked Shields 2016" gan baltās (organizatoru), gan sarkanās (uzbrucēju), gan zilās (aizstāvju) komandas sastāvā. Mācību laikā tika gūta vērtīga pieredze un atziņas, kuras izmantot tālākā ikdienas darbā.

26. aprīlī CERT.LV organizēja semināru IT drošības speciālistiem "Esi drošs". Seminārs tika veltīts Ministru kabineta noteikumu Nr. 442 ieviešanai, atbildīgai ievainojamību atklāšanai un šifrējošo izspiedējvīrusu jautājumam.

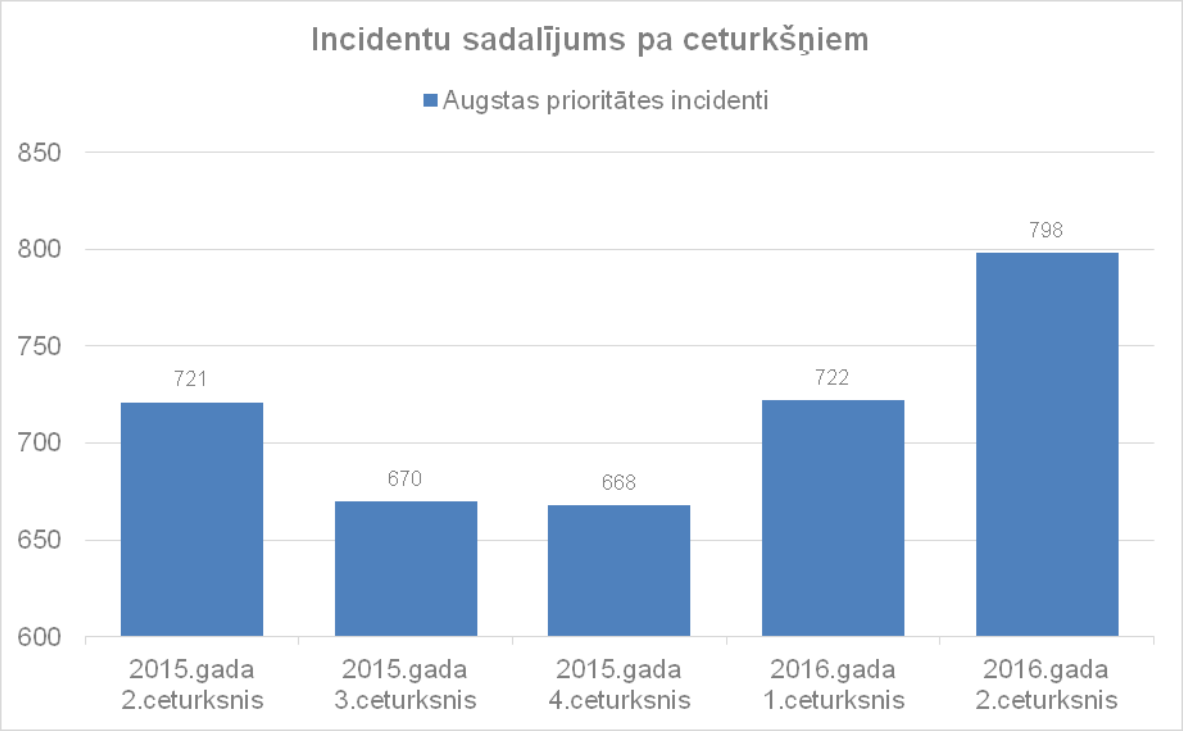
Maijā CERT.LV Rīgā organizēja 48. TF-CSIRT sanāksmi, kurā piedalījās gandrīz 100 pārstāvji no dažādām Eiropas CERTu komandām. Pirms šīs sanāksmes notika arī ES tīklu un informācijas drošības direktīvas (NIS direktīvas) CSIRT tīkla otrā neformālā veidošanas sanāksme, kuras laikā norisinājās diskusijas darba grupās par CSIRT tīkla darbības principiem. Papildus Rīgā notika arī citas sanāksmes – "Incident handling and taxonomies", "11th annual workshop - CSIRTs in Europe", kā arī "Train-the-trainer workshop".

Pārskata periodā CERT.LV par IT drošību izglītoja 1512 cilvēkus, iesaistoties 19 izglītojošos pasākumos, ievietoja 37 jaunas ziņas vietnē www.cert.lv, piedalījās 2 radio pārraidēs un 6 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

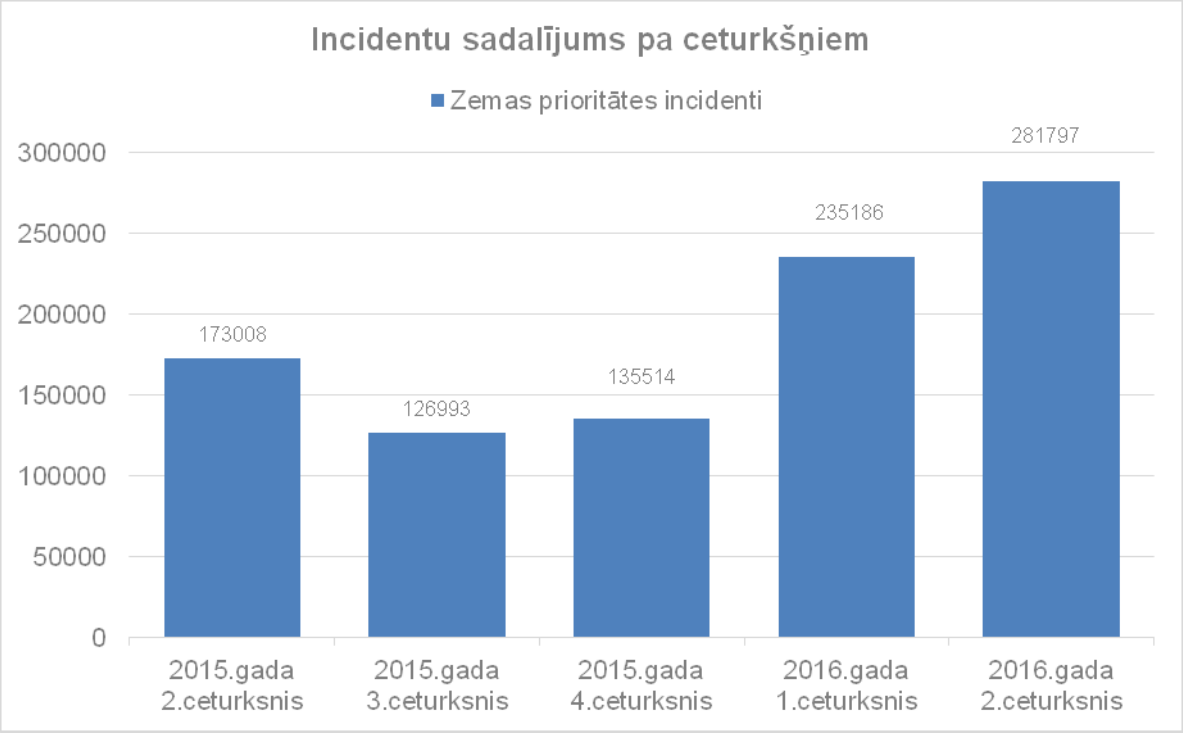
CERT.LV ik mēnesi apkopo informāciju par notikušajiem incidentiem, iedalot incidentus augstas prioritātes (visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas vai ko ir paziņojis cilvēks, nevis automātisks ziņotājs) un zemas prioritātes (galvenokārt inficētas galalietotāju iekārtas, kas kļuvušas par robotu tīklu sastāvdaļām un/vai izsūta mēstules) incidentos.

2016. gada 2. ceturksnī CERT.LV apstrādāja 798 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 722 augstas prioritātes incidenti, bet 2015. gada 2. ceturksnī 721 augstas prioritātes incidents.



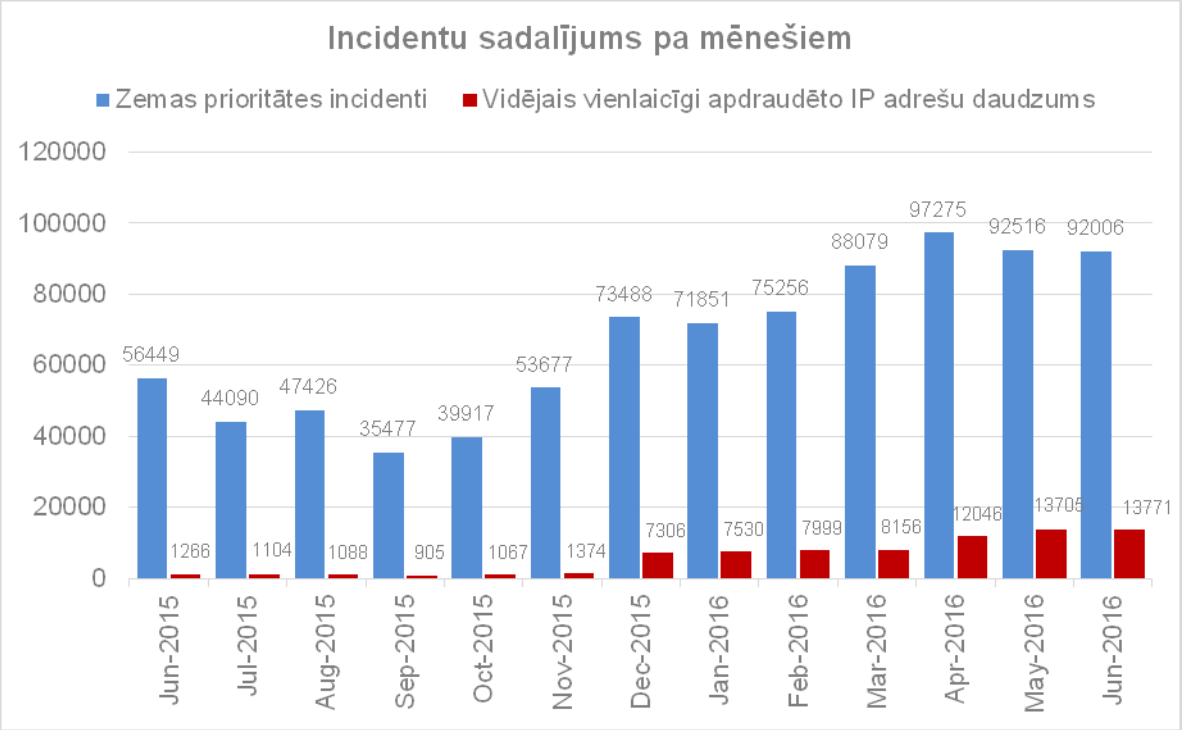
1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2015. un 2016. gadā.

2016. gada 2. ceturksnī CERT.LV reģistrēja 281 797 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 235 186 zemas prioritātes incidenti, bet 2015. gada 2. ceturksnī 173 008 zemas prioritātes incidenti.



2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2015. un 2016.gadā.

Zemas prioritātes incidentu skaita pieaugums skaidrojams ar dažādu informācijas avotu sniegtās informācijas apjoma palielināšanos.



3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi apdraudēto IP adrešu daudzums 2015. un 2016. gadā.

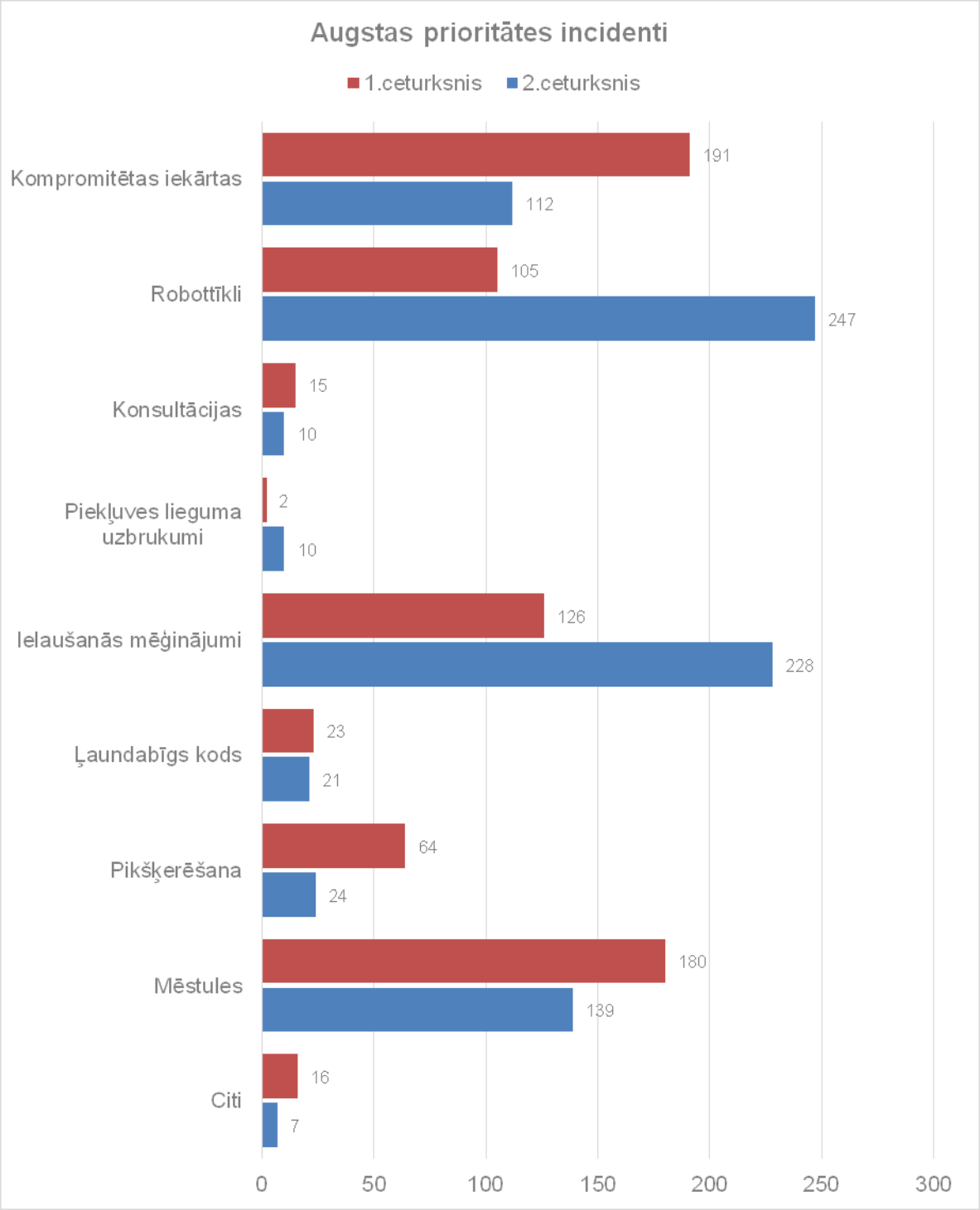
Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi apdraudēto unikālo IP adrešu skaitu Latvijā. Zemas prioritātes incidentu apjoma pieaugums 2016. gada pirmajā pusē un reizē arī CERT.LV fiksēto vienlaicīgi apdraudēto IP adrešu daudzuma pieaugums pārskata periodā skaidrojams

ar saņemtās informācijas apjoma pieaugumu. Secinājums – kopējā situācija nav pasliktinājusies, bet tiek iegūta plašāka informācija par notiekošo.

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 IPS, kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus gala lietotājus 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.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 798 augstas prioritātes incidentus.



4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2016. gada 1. un 2. ceturksnī.

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:

5.attēls - Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2016.gada 2.ceturksnī.

Pārskata periodā CERT.LV ir identificējis vairāk kā 200 Locky un citu šifrējošo vīrusu piegādes mēģinājumus valsts pārvaldes iestādēm gov.lv domēnu zonā un vairāk kā 1500 šifrējošo vīrusu piegādes mēģinājumus privātam sektoram. Kā piegādes mehānismu uzbrucēji galvenokārt izmanto e-pasta ziņojumus, kas noformēti vairāk vai mazāk saņēmējam saistošā formā ar mērķi panākt, lai saņēmējs atver pielikumu.

Kaitīgie pielikumi Locky un citu šifrējošo vīrusu uzbrukumu kampaņās piegādā datoram izpildāmus failus jeb ļaunprātīgas instrukcijas. Lai uzbrucēja instrukcijas izpildītu, saņēmējam pietiek tikai atvērt piegādāto failu.

Kaitīgajos e-pastos biežāk izmantotie arhīva failu formāti: zip, rar, jar.

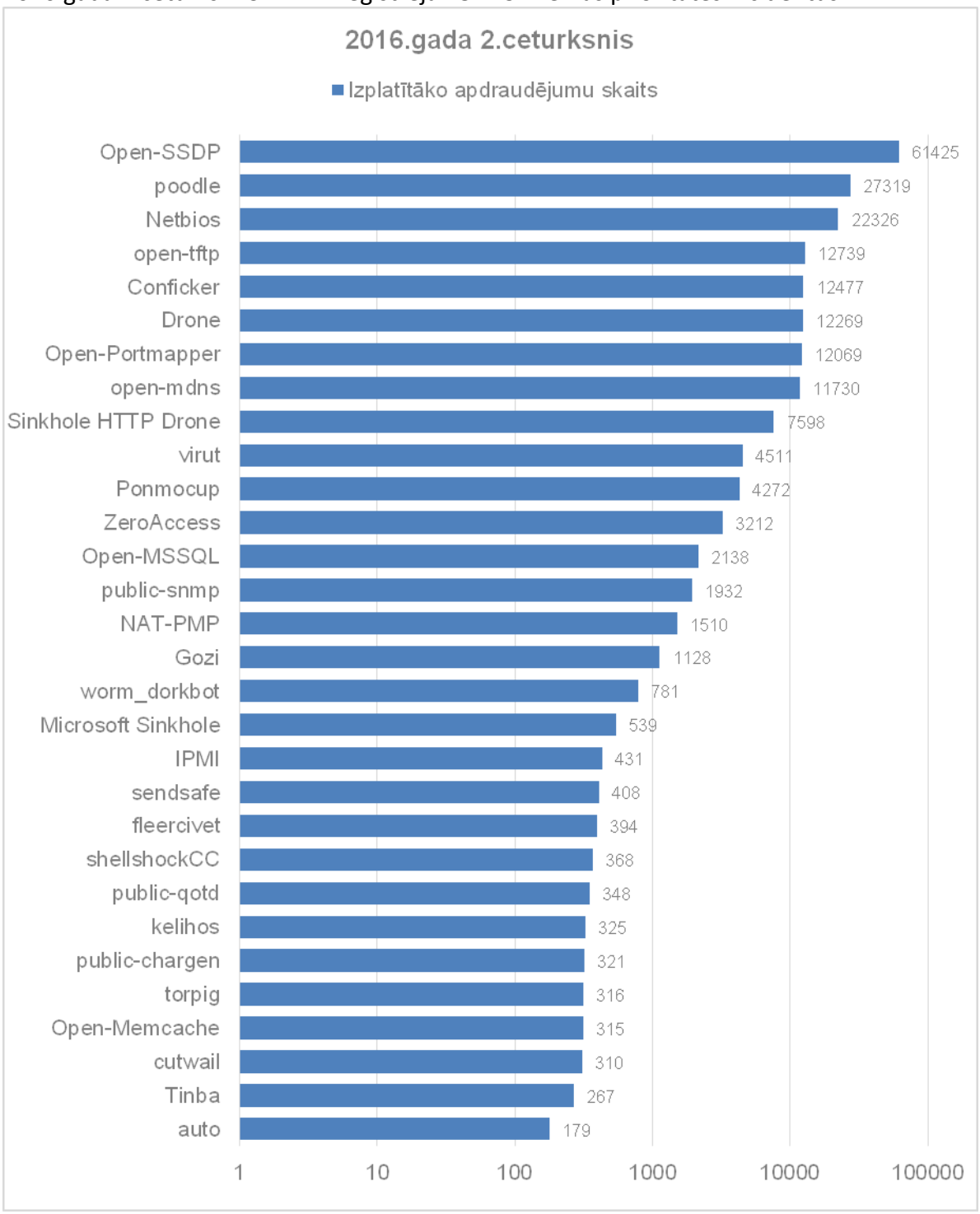
Biežāk izmantotie izpildāmo failu paplašinājumi: .ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .hlp, .ht, .hta, .inf, .ins, .isp, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .pcd, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh, .exe, .pif, un citi.

Lai uzbrucējs panāktu kaitīgā koda izpildi, kas piegādāts ar atsūtīta dokumenta starpniecību (piemēram, kā daļa no .doc dokumenta), ir jābūt ievainojamībai dokumentu apstrādes programmatūrā, vai jāpanāk, ka lietotājs pats aktivizē dokumenta aktīvo daļu jeb Macros.

Dokumentu formāti, kas atbalsta Macros funkcionalitāti: .doc, .xls, .docm, .xlsm, .pptm, un citi.

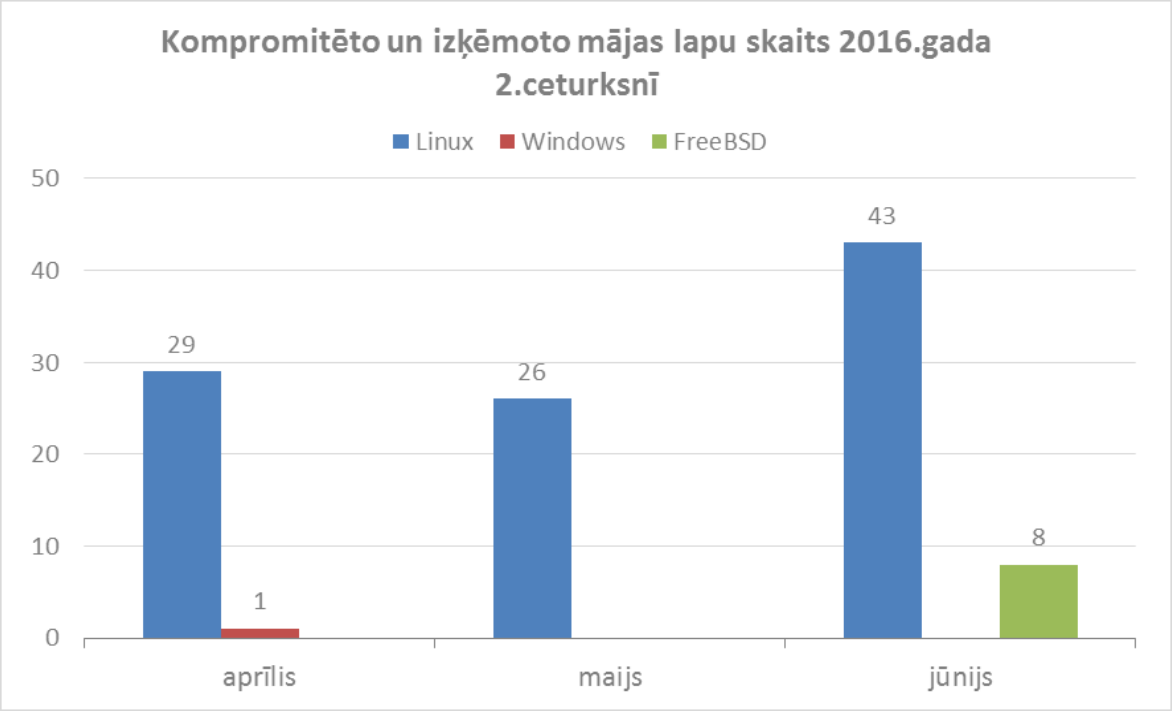
Pēc noklusējuma Microsoft Office produkti nepieļauj automātisku Macros koda izpildi, tāpēc gadījumos, kad redzams paziņojums zem rīku joslas "Security Warning Macros have been disabled", CERT.LV aicina nespiest pogu "Enable Content", lai izvairītos no ļaunatūras nonākšanas datorā.

2016.gada 2.ceturksnī CERT.LV reģistrēja 281 797 zemas prioritātes incidentus.



6.attēls – CERT.LV reģistrētie zemas prioritātes incidenti no 2016. gada 1. aprīļa līdz 30. jūnijam pa apdraudējumu veidiem.

CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus.



7.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2016. gada 2. ceturksnī.

Pārskata periodā kompromitēto un izķēmoto mājas lapu skaits ir būtiski krities, salīdzinot ar iepriekšējo periodu. Tas skaidrojams ar to, ka pārskata periodā nav tikušas atklātas būtiskas jaunas satura vadības sistēmu, piemēram, Joomla un Wordpress, ievainojamības, kas veicinātu automatizētu uzbrukumu izpildi ar mērķi atrast jaunas ievainojamas iekārtas.

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:

- 01.04. Kādā valsts iestādē šifrējošais datorvīruss TeslaCrypt sabojāja datus vienā datorā. Tie atgūti no rezerves kopijām.
- 04.04. CERT.LV saņēma vairāku uzņēmumu incidentu pieteikumus par tā saucamo "CEO krāpniecību" (*CEO scam*), kurā izmantoti viltoti e-pasti, kas sūtīti kompānijas vadītāja vai sadarbības partnera vārdā, lai panāktu nozīmīgu naudas summu pārskaitīšanu uz krāpnieku bankas kontiem. Tā ir klasiska krāpniecība, kas nav pat īsti klasificējama kā kiberuzbrukums, taču diemžēl darbojas ļoti efektīvi. CERT.LV ir zināmi vairāki krāpniecības upuri Latvijā, kuru zaudējumu apmērs katrā gadījumā ir 4 000 EUR - 20 000 EUR. ASV tiesībsargājošās iestādes lēš, ka šādas krāpniecības radītie zaudējumi varētu būt mērāmi vairāk kā 2 miljardos ASV dolāru. Visos "CEO krāpniecības" incidentos, kas nonākuši līdz CERT.LV, ir veikta analīze un detalizēta informācija nodota Valsts Policijai.
- 08.04. CERT.LV veica ievainojamību pārbaudi kādas valsts iestādes datortīklos. Pārbaude ierosināta pēc atbildīga ievainojamības atklāšanas ziņojuma saņemšanas, jo tika konstatēts, ka konkrētajā iestādē ir iegādāti vairāki simti ievainojamu iekārtu.

Pārbaudes rezultātā apstiprinātas kritiskas ievainojamības šajās iekārtās, kā arī šo iekārtu vadības moduļos. CERT.LV uzsāka ievainojamību novēršanas koordinācijas procesu ar ražotāju.

- 11.04. Kādas privātpersonas privātā informācija - CV dokuments, kas iesniegts darba pieteikumam, - izlikts brīvai pieejai internetā. CERT.LV brīdināja servera uzturētājus un Datu valsts inspekciju par šo gadījumu.
- 11.04. CERT.LV konstatēja publiskā tīklā pieejamu Siemens "gudrās mājas" vadības saskarni. Par identificēto apdraudējumu tika informēts sistēmas turētājs un veikti apdraudējuma mazināšanas pasākumi.
- 12.04. Kādas populāras tīmekļa vietnes uzturētāji saņēma draudu vēstuli par DDoS uzbrukumu līdz 1 TB sekundē, ja netiks veikta samaksa. Tiklīdz uzbrukums tiks sākts, samaksa par tā apturēšanu tiks palielināta ar katru uzbrukuma dienu. Draudu vēstulē netika minēts periods, cik dienas ir plānots šis uzbrukums. Sekojot CERT.LV ieteikumam, portāls neveica nekādu komunikāciju ar uzbrucējiem. Reāls uzbrukums nesekoja.
- 14.04. Pret kādu populāru tīmekļa resursu veikts DDoS uzbrukums. Tam izmantotas apmēram 24000 inficētas vietnes, kas izmanto novecojušu satura vadības sistēmas Wordpress versiju. Zināms, ka 33 no uzbrukumā izmantotajām vietnēm bija Latvijā uzturētas. Tīmekļa resursa uzturētājs izveidojis filtrus, kas veiksmīgi atvairīja šo uzbrukumu.
- 16.04. Kāds lietotājs kļuva par upuri Cerber šifrējošajam izspiedējvīrusam. Diemžēl šobrīd nav atrastas kļūdas šī šifrējošā datorvīrusa kodā, lai varētu izstrādāt rīku failu atjaunošanai. Lai pasargātu savu datoru no šādiem vīrusiem, jāatjaunina datorā lietotās programmas, piemēram, Adobe Flash Player, kura ievainojamība ir tiešā mērā saistīta ar Cerber šifrējošā datorvīrusa izplatību, un savlaicīgi jāveido svarīgo dokumentu rezerves kopijas.
- 19.04. Vairākās valsts un pašvaldību iestādēs masveidā izplatīti e-pasti, kas domāti lietotāju e-pasta piekļuves datu izkrāpšanai. Darbinieki brīdināti.
- 21.04. Konstatēts intensīvs paroļu pielasīšanas tipa uzbrukums kādas valsts iestādes e-pasta serverim. Uzbrukums nav bijis sekmīgs.
- 22.04. Kādas valsts iestādes lapā konstatēta ievainojamība, kas ļauj veikt SQL injekcijas tipa uzbrukumu. Lapas uzturētājs brīdināts.
- 22.04. CERT.LV saņēma informāciju par kritisku ievainojamību kādas valsts iestādes tīmekļa vietnē. Lai arī ziņotājs nebija gluži ievērojis visus atbildīgas ievainojamības atklāšanas principus, informācija bija vērtīga un CERT.LV koordinēja ievainojamības novēršanas procesu.
- 25.04. Kāda uzņēmuma klienti kļuva par krāpnieku upuriem, apmaksājot rēķinus par produkciju uz izmainītiem bankas kontiem. CERT.LV ieteica uzņēmumam brīdināt visus savus klientus un nomainīt e-pasta piekļuves paroles.
- 27.04. CERT.LV informē par DHL un PayPal datu izkrāpšanas incidentiem un to iespējamo saistību ar nopludinātiem pasta sistēmu kontiem.

- 28.04. Kādā valsts iestādē lietotājs aktivizējis e-pastā iesūtītu Locky šifrējošo datorvīrusu. Dators ātri atslēgts no tīkla, tāpēc bojātas tikai lokālās datnes, ko izdevies atjaunot no rezerves kopijām. Nozīmīgi dokumenti nav cietuši.
- Maijā kādā uzņēmumā šifrējošais izspiedējvīruss spējis tikt cauri vairākām uzstādītām drošības sistēmām un inficēt vienu datoru, nošifrējot daļu no datnēm. Vīruss tika paslēpts .docm datnē un iesūtīts e-pastā. To nav pamanījis F-secure e-pasta antivīruss, Symantec antivīruss, kā arī ugunsmūra risinājums ar aktīvo aizsardzību, kuram vajadzēja bloķēt vīrusa lejupielādi. Tikai pateicoties tam, ka pats vīruss par sevi paziņoja, pirms šifrēšana tika pabeigta, dators tika atvienots no interneta pieslēguma, tādējādi vīruss bija paspējis nošifrēt tikai daļu no failiem.
- 02.05. Kādas pašvaldības darbiniekiem kolēģu vārdā iesūtīti viltoti e-pasti ar saitēm uz krāpnieciskām lapām. CERT.LV sniedza ieteikumus e-pastu serveru aizsardzības uzlabošanai, lai nepieļautu viltotu e-pastu iesūtīšanu.
- 05.05. Konstatēta masveida Locky datorvīrusa izplatīšanas kampaņa, kas mērķēta galvenokārt uz valsts un pašvaldību iestādēm. Inficētie e-pasti noformēti kā viltus rēķini angļu un spāņu valodā. Vīrusa lejupielādētājs tika ievietots.js (*Java Script*) datnē, kas ZIP arhīva konteinerā tiek izsūtīta e-pastu pielikumos.
- 13.05. Kādas lapas audita pierakstu fails bija brīvi pieejams internetā. Tas saturēja datus par lietotāju migrāciju uz jaunu serveri. Tajā bija redzami lietotājvārdi un nešifrētas paroles, kas ļauj iegūt pilnu kontroli pār šo serveri. CERT.LV brīdināja lapas īpašnieku, šī kļūda tika salabota.
- 13.05. CERT.LV apziņoja Pony botneta upurus Latvijā. Informācija par upuriem tika iegūta botnet kontrolcentra analīzes rezultātā, kas veikta sadarbībā ar Ukrainas kolēģiem. Konkrētā incidenta ietvaros upuru skaits Latvijā mērāms vairākos desmitos.
- 17.05. Kāda uzņēmuma klientiem izkrāpta nauda, izmantojot viltus rēķinus.
- 17.05. Kāda uzņēmuma darbinieki saņēma e-pastus ar kaitīgu pielikumu, kurš pēc atvēršanas mēģināja datorā lejuplādēt Locky šifrējošo izspiedējvīrusu. CERT.LV uzņēmumam ieteica atslēgt WSH, lai pasargātu datoru no .js un citu izpildāmu skriptu palaišanas.
- 16.05. CERT.LV koordinēja ievainojamības/ nedrošas konfigurācijas novēršanas procesu, kas skāra vairākus tūkstošus optiskā interneta klientu kāda uzņēmuma tīklā, kuriem uzstādītas Alcatel-Lucent iekārtas. Par ievainojamību CERT.LV paziņoja IT drošības speciālists, ievērojot atbildīgas ievainojamību atklāšanas pamatprincipus. Uzņēmums nekavējoties uzsāka risku mazināšanas pasākumus, kā arī dažu dienu laikā novērsa ievainojamības izmantošanas iespējas.
- 25.05. CERT.LV saņēma ziņojumu, ka kāda tīmekļa vietne ir kompromitēta ievainojamas Joomla satura vadības sistēmas dēļ un tiek izmantota Locky šifrējošā izspiedējvīrusa izplatīšanai. Vietnes uzturētāji tika brīdināti.
- 25.05. Kāda valsts iestāde piedzīvoja 45 minūšu ilgu uzbrukumu ar intensitāti 3-5 pieprasījumi sekundē – mēģināts veikt POST pieprasījumus mainot URL, izmantots automatizēts ievainojamību meklēšanas rīks. Lapas aizsardzības sistēma šos pieprasījumus bloķēja, informācijas noplūde nav notikusi. Uzbrukumā izmantota

Latvijas IP adrese, kas iesaistīta arī citos mēģinājumos meklēt ievainojamas tīmekļa lapu satura vadības sistēmas.

- 31.05. Kāds uzņēmums saņēma kaitīgus e-pastus, kas domāti lietotāju e-pasta pieejas datu izkrāpšanai. Tie bija jauna tipa krāpnieciski e-pasti, kas noformēti kā produkcijas piedāvājums un ir sagatavoti konkrētajam saņēmējam.
- Maijā Latvijas interneta pakalpojumu sniedzēji kļuva par mērķi datortārpam, kas izmanto ievainojamību neatjauninātā Ubiquiti tīkla maršrutētāju programmatūrā. Lai novērstu šo ievainojamību, jau pirms gada Ubiquiti ir izlaidis atjauninājumus, taču vēl aizvien daudzas no iekārtām tiek lietotas ar novecojušo programmnodrošinājumu. CERT.LV rīcībā ir informācija, ka uzbrukuma rezultātā Latvijā ir vairāki simti sabojātu ievainojamo ierīču, taču šis skaits varētu pieaugt līdz pat vairākiem tūkstošiem.
- 03.06. Kādā skolā konstatēta skolnieku izveidota klaviatūras ievades pārtvērējprogramma, ar kuras palīdzību iegūti piekļuves dati elektroniskajiem klases žurnāliem un mainītas atzīmes. Vainīgie skolnieki atklāti.
- 07.06. Kāds uzņēmums saņēma e-pastus, kuru pielikumā esošais dokuments saturēja *Macro*, kas lejuplādē šifrējošo izspiedējvīrusu saturošu failu.
- 14.06. Kāda uzņēmuma dators inficēts ar Cerber šifrējošo izspiedējvīrusu. Cietušais uzņēmums vērsies pie CERT.LV ar jautājumu, vai ir iespējams atgūt zaudētos failus, ja nav rezerves kopijas. Diemžēl šobrīd tas nav iespējams.
- 15.06. No kāda uzņēmuma klientiem mēģināts izkrāpt naudu, izmantojot viltotu rēķinu. Uzbrucēju kļūdas dēļ pārskaitījums nav izdevies, kas pasargājis klientus no zaudējumiem. CERT.LV ieteica uzņēmumam brīdināt visus savus klientus par šāda veida krāpniecību.
- 29.06. Kāda uzņēmuma partneriem nosūtīti viltus rēķini, kas domāti naudas izkrāpšanai. Zaudējumi nav nodarīti, par notikušo informēta policija.
- Jūnija otrajā pusē gan Latvijā, gan citās valstīs ar jaunu kampaņu atgriezās Locky šifrējošais izspiedējvīruss. Tas novērots galvenokārt uz valsts un pašvaldību iestādēm mērķētos uzbrukumos. Ar e-pastu starpniecību tika izsūtīta Javascript datne, kuru atverot notika mēģinājums savienoties ar kaitīgām tīmekļa vietnēm un ielādēt vīrusu datorā.

CERT.LV pasākumi incidentu novēršanai:

- 05.05. CERT.LV konstatēja inficētu e-pastu izplatīšanu valsts un pašvaldību iestāžu darbiniekiem, ar mērķi inficēt datorus ar šifrējošo izspiedējvīrusu Locky. Kaitīgie e-pasti pielikumā saturēja .zip arhīvu ar Javascript (.js) failu. Ja šis fails tika atvērts, datorā tika lejuplādēts Locky vīruss un visi datorā un tam pievienotajās tīkla koplietošanas mapēs esošie faili tika sašifrēti. Lai bloķētu Javascript pielikumu izpildi, CERT.LV ieteica atslēgt WSH. Tika sagatavota arī video pamācība WSH atslēgšanai. Par kaitīgajiem e-pastiem tika brīdināti valsts un pašvaldību iestāžu par IT drošību atbildīgie.
- 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. un 9.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.

Līdz šim CERT.LV eksperti saskārušies tikai ar tādu mobilo ļaunatūru, kas nav specifiska Latvijai, bet tas ir tikai laika jautājums, līdz parādīsies arī mobilā ļaunatūra, kas tiks mērķēta tieši uz Latvijas mobilo iekārtu lietotājiem. Lai pilnvērtīgi sagatavotos jaunās mobilās ļaunatūras analīzei, CERT.LV turpina darbu pie laboratorijas izveides.

Pārskata periodā ir saņemti vairāki incidentu pieteikumi, kuros iesaistītas mobilās ierīces ar Android OS. Tika uzsākta kāda Android mobilā telefons analīze, pamatojoties uz aizdomām par iekārtas iespējamu kompromitēšanu un iesaistīšanu nelikumīgās naudas transakcijās, taču analīzes rezultātā tika konstatēts, ka kompromitēts ir Google konts, kura autentifikācijas dati ir noplūduši, visticamāk, kādā no sociālo tīklu piekļuves datu noplūdes gadījumiem. Uzbrucēji izmantoja iegūtos autentifikācijas datus, lai piekļūtu Google e-pasta kontam, kas Android ierīcēs tiek piesaistīts arī kā iekārtas servisa konts, un iejaucās uzņēmuma sarakstē, izliekoties par uzņēmuma partneri, ar kuru uzņēmums plānoja veikt darījumu.

Ir veikta vairāku Android lietotņu analīze, balstoties uz aizdomām par to kaitniecisku darbību. Lietotnes ievāca nepamatoti daudz informācijas par lietotāja ierīci. Ievāktā informācija pēc tam, visticamāk, tiek izmantota reklāmas nolūkos. Tiešas Android vīrusam raksturīgas pazīmes netika konstatētas.

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

27. aprīlī CERT.LV pārstāvis piedalījās DDA rīkotajā preses konferencē naudas drošības kampaņas "Internetā dari kā dzīvē?" ietvaros, kas notika Rīgas autoostā. CERT.LV informēja klātesošos par izspiedējvīrusiem un to, kā sevi no šiem vīrusiem pasargāt.

Informācija par CERT.LV sadarbību ar medijiem

1) **Intervijas un ziņas radio:**
   - 27.04. Telefonintervija DDA naudas drošības kampaņas "Internetā dari kā dzīvē?" ietvaros LR4 raidījumam "Домская площадь" par krāpniecību ar viltus rēķiniem.
   - 21.06. Intervija LR4 par bankas pārskaitījumu drošību un kibernoziegumiem saistībā ar internetbanku lietošanu.

2) **Sižeti televīzijā, tiešraides:**
   - 11.04. Intervija Re:TV raidījumam "Re:TV Intervija" par pakalpojumu digitalizāciju un datu drošību.
   - 27.04. Telefonintervija LTV raidījumam "Rīta panorāma" saistībā ar DDA uzsākto naudas drošības kampaņu "Internetā dari kā dzīvē?".
   - 27.04. Intervija TV3 ziņām par šifrējošajiem izspiedējvīrusiem DDA kampaņas "Internetā dari kā dzīvē?" ietvaros.
   - 27.04. Intervija LNT ziņām par izspiedējvīrusiem DDA kampaņas "Internetā dari kā dzīvē?" ietvaros.
   - 29.04. Komentārs Kivi TV par krāpšanu un datu drošību internetā.
   - 09.05. Intervija LTV raidījumam "Rīta panorāma" par vecāku kontroles iespējām datoros.

3) **Informācija par CERT.LV tīmekļa vietnēm:**

Pārskata periodā vietnē https://www.cert.lv publicētas 37 ziņas. Populārākā sadaļa bija par jaunākajiem vīrusiem, kurai ir 6,805 unikāli skatījumi. Otra populārākā bija ziņa par CERT.LV rīkoto IT drošības semināru "Esi drošs", kuru skatījuši 1,394 unikāli apmeklētāji. Trešā populārākā bija jaunumu sadaļa ar 1,222 unikāliem skatījumiem. Pārskata periodā novērojams ievērojams apmeklētāju apjoma kritums (par 20%), salīdzinājumā ar 2016. gada pirmo ceturksni. Tas skaidrojams ar vasaras un atvaļinājumu laika sākumu. Kopā CERT.LV mājaslapai bijuši 13,920 lapu skatījumi, kurus veido 8,161 unikāls lapu skatījums.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 11,607 apmeklējumi, no tiem 9,646 unikāli apmeklējumi. Arī šī portāla apmeklējums ir krities par nepilniem 20%, salīdzinot ar iepriekšējo pārskata periodu.

CERT.LV turpina tulkot un portālā esidross.lv publicēt OUCH! ikmēneša izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts). Pārskata periodā nopublicēti 3 jauni OUCH! numuri.

Portālā esidross.lv publicētie raksti:

- Mani ir “uzlauzuši”, ko darīt?
- Lietiskais internets (IoT)
- Kā rīkoties izspiedējvīrusa gadījumā?
- Šifrēšana

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1519.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 384.
- CERT.LV draugiem.lv profila http://www.draugiem.lv/certlv sekotāju skaits pārskata perioda beigās bija 68.
- Sociālajā tīklā Google+ https://www.google.com/+CertLv ir 26 sekotāji.

Pēdējos divos ceturkšņos stabili pieaug sekotāju skaits populārajās sociālo tīklu platformās Twitter un Facebook, taču draugiem.lv un Google+ tas saglabājas nemainīgs.

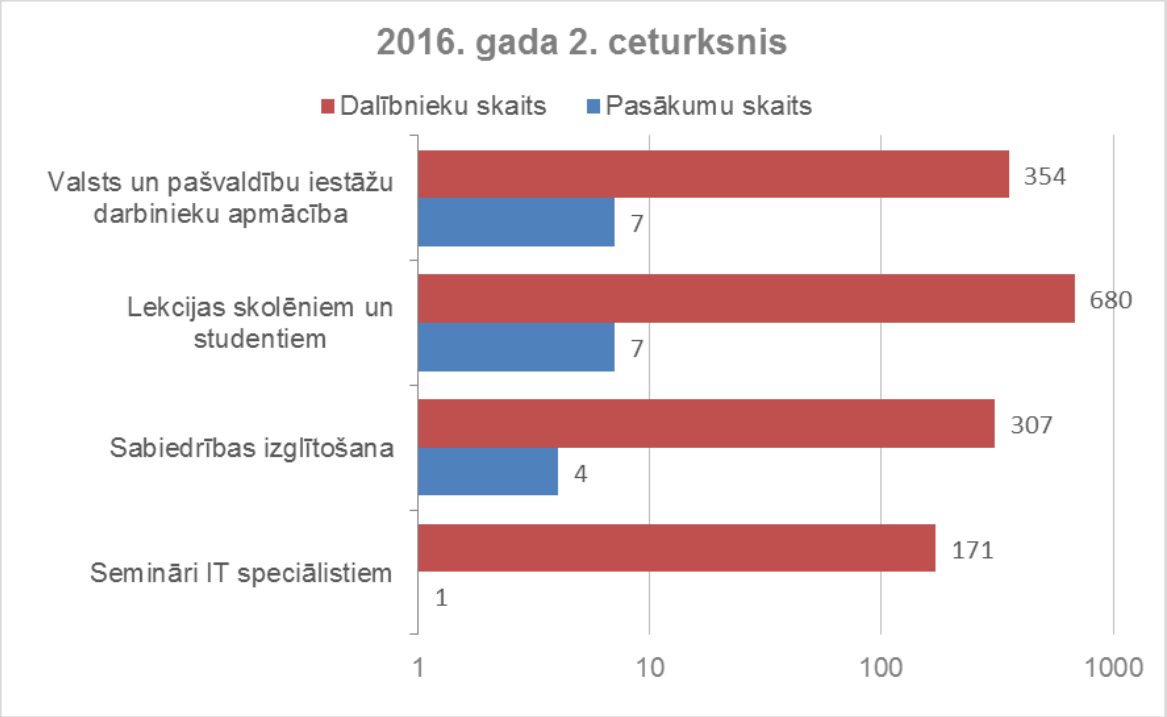
5. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

2. aprīlī CERT.LV pārstāvis sniedza prezentāciju un vadīja diskusiju par IT drošību UNESCO organizētajā starptautiskajā jauniešu forumā Valmierā.

22. aprīlī CERT.LV pārstāvis sniedza prezentāciju LVRTC organizētajā pasākumā "IT izstrādātāju brokastis", aplūkojot jautājumus, kas saistīti ar atbildīgu ievainojamību atklāšanu.

28. aprīlī CERT.LV pārstāvis sniedza prezentāciju Dienas Bizness rīkotajā konferencē "Datu drošība" par aktuāliem apdraudējumiem kibervidē CERT.LV redzējumā: kas tad īsti mūs apdraud kibervidē un kādas ir iespējas ar to cīnīties, kā šie apdraudējumi ir mainījušies pēdējo 5 gadu laikā?

Pārskata periodā CERT.LV par IT drošību izglītoja 1512 cilvēkus, iesaistoties 19 izglītojošos pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2016. gada 2. Ceturksnī.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 14.04. DEG sanāksme.
- 25.04. Informācijas tehnoloģiju drošības likuma grozījumu darba grupas sēde, kurā diskutēja par atbildīgas ievainojamību atklāšanas procesa ieviešanu, domēnu vārdu bloķēšanas iespējām un citiem grozījumiem.
- 26.05. NetSafe konsultatīvās padomes sēde.
- 27.05. Tikšanās ar NBS pārstāvjiem, lai apspriestu 2016. gada NATO mācību plānošanu.
- 01.06. Krimināllikuma darba grupas sanāksme par grozījumiem, kas saistīti ar atbildīgas ievainojamību atklāšanas procesa ieviešanu.
- 09.06. DEG sanāksme.
- 28.06. Tikšanās ar Aizsardzības ministriju par atbildīgas ievainojamību atklāšanas ieviešanu.

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 2016. gada 30. jūnijam CERT.LV apkopojusi informāciju par 1335 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību vai ar to ir 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. CERT.LV ir izstrādājis rīcības plāna paraugu, lai palīdzētu mazajiem ESK izveidot savus plānus, un izsūtījis informāciju par šo paraugu tiem ESK, kuri līdz šim nav izstrādājuši un iesnieguši CERT.LV rīcības plānu elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai.

Uz pārskata perioda beigām informācija ir saņemta no 64 ESK. 59 ESK ir iesnieguši rīcības plānu, bet 5 ESK rakstiski apliecinājuši, ka neuztur publisko elektronisko sakaru tīklu, no tiem 1 ESK nodevis visu ārpakalpojumā citam ESK.

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).

Attiecībā uz ITDL 61 panta izpildi, pārskata periodā nav saņemts neviens ziņojums.

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

Maijā CERT.LV Rīgā organizēja 48. TF-CSIRT sanāksmi, kurā piedalījās gandrīz 100 pārstāvji no dažādām Eiropas CERTu komandām. Pirms šīs sanāksmes notika arī ES tīklu un informācijas drošības direktīvas (NIS direktīvas) CSIRT tīkla otrā neformālā veidošanas sanāksme, kuras laikā norisinājās diskusijas darba grupās par CSIRT tīkla darbības principiem. Papildus notika arī citas sanāksmes – "Incident handling and taxonomies", "11th annual workshop - CSIRTs in Europe", kā arī "Train-the-trainer workshop". Visās šajās sanāksmēs CERT.LV piedalījās gan ar prezentācijām, gan iesaistoties diskusijās. Tika saņemtas ļoti pozitīvas atsauksmes no dalībniekiem par pasākumu organizāciju.

18.-23. aprīlī CERT.LV pārstāvji piedalījās NATO kiberdrošības mācībās "Locked Shields 2016" gan baltās (organizatoru), gan sarkanās (uzbrucēju), gan zilās (aizstāvju) komandas sastāvā. Aizstāvju (zilās komandas) statusā šogad CERT.LV startēja kopā ar ekspertiem no Latvijas Kiberaizsardzības vienības un kolēģiem no ASV.

30.-31. maijā CERT.LV pārstāvji piedalījās CERT-EE simpozijā Tallinā. CERT.LV piedalījās arī vingrinājumā Iegūsti karogu (Capture the Flag) un izcīnīja pirmo vietu.

Pārskata periodā tika uzsākta gatavošanās rudenī notiekošajām ENISA mācībām "Cyber Europe 2016", uzrunāti potenciālie dalībnieki.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 04.-05.04. CERT.LV pārstāvis piedalījās Nīderlandes CERT konferencē "One conference" un NIS direktīvas CSIRT tīkla pirmajā neoficiālajā veidošanas sanāksmē Hāgā, sniedzot prezentāciju par CERT komandu brieduma pakāpēm un to izvērtēšanas mehānismiem.
- 08.04. CERT.LV uzņēma Butānas CERT pārstāvjus Rīgā.
- 12.-15.04. CERT.LV pārstāvji apmeklēja TRANSITS kursu Nīderlandē.
- 13.04. CERT.LV pārstāvji piedalījās starptautisko kiberdrošības mācību "Locked Shields 2016" izmēģinājumā.
- 14.04. CERT.LV konsultēja Lietuvas kolēģus un sniedza atbalstu DDOS aizsardzības risinājuma piemērošanā.
- 18.-23.04. CERT.LV pārstāvji piedalījās "Locked Shields 2016" mācībās gan aizstāvju (zilajā), gan uzbrucēju (sarkanajā), gan organizatoru (baltajā) komandā.
- 09.05. CERT.LV pārstāvis apmeklēja CCDCoE organizētos kursus "Monitoring Course Module 3" Tallinā.
- 10.05. Rīgā notika CERT.LV un ENISA organizētais NIS direktīvas CSIRT tīkla veidošanas otrā neoficiālā sanāksme, kurā piedalījās vairāk nekā 50 pārstāvji no gandrīz visām ES dalībvalstīm.
- 10.05. CERT.LV pārstāvji organizēja un piedalījās ENISA sanāksmē "Incident handling and taxonomies" Rīgā.

- 10.-11.05. CERT.LV pārstāvji organizēja un piedalījās "ENISA's 11th annual workshop - CSIRTs in Europe" Rīgā.
- 11.05. Tikšanās ar Eiropas komisijas pārstāvjiem, lai apspriestu NIS direktīvas ieviešanas gaitu un nepieciešamās izmaiņas likumdošanā Latvijā.
- 11.05. CERT.LV pārstāvji organizēja un piedalījās TRANSITS "Train-the-trainer workshop" Rīgā.
- 12.-13.05. CERT.LV pārstāvji organizēja un piedalījās "48th TF-CSIRT meeting" Rīgā, kā arī uzstājās ar prezentāciju par atbildīgas ievainojamību atklāšanas procesa ieviešanu Latvijas likumdošanā.
- 16.-19.05. CERT.LV pārstāvji piedalījās "Locked Shields Forensic Challenge Workshop" Tallinā.
- 26.05. CERT.LV pārstāvis piedalījās mācību "Locked Shields 2016" pārskata pasākumā Tallinā.
- 30.-31.05. CERT.LV pārstāvji piedalījās CERT-EE simpozijā Tallinā.
- 01.-04.06. CERT.LV pārstāvji piedalījās CyCON konferencē Tallinā.
- 03.06. CERT.LV pārstāvji piedalījās ENISA mācībās par Eiropas līmeņa krīžu novēršanas standarta procedūru īstenošanu.
- 10.-20.06. CERT.LV pārstāvji piedalījās FIRST konferencē un vispasaules nacionālo CERT pārstāvju sanāksmē Seulā, uzstājoties ar prezentāciju "CERT.LV experience - roles far beyond traditional CSIRT activities".
- 14.-18.06. CERT.LV pārstāvis piedalījās ENISA Eiropas kiberdrošības mācību plānošanas konferencē Atēnās.
- 27.-29.06. CERT.LV pārstāvji apmeklēja un piedalījās paneļdiskusijā "UNESCO 2nd Media & Info Literacy forum".

Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

Pārskata periodā CERT.LV pārstāvji recenzēja divus LU kvalifikācijas darbus, vadīja kursa darbu "HTTPS satura inspekcija uzņēmuma starpniekserverī" un bakalaura darbus "Drošības pārbaužu veikšana atbilstoši ASVS standartam" un "Twitter troļļi – statistikas metodes automātiski ģenerēta satura noteikšanai". Kursa darbā paustās tēzes tika pielietotas arī praksē kiberdrošības mācībās "Locked Shields 2016", un rezultāts tika atzinīgi novērtēts.

- 12.05. CERT.LV pārstāvis piedalās seminārā CiscoConnect.
- 20.-21.05. CERT.LV pārstāvis piedalās seminārā ''Latvijas Datortīklu Skola 37.sesija".
- 07., 08.06. CERT.LV pārstāvis piedalās bakalaura darbu aizstāvēšanā.
- 10.06. CERT.LV pārstāvis piedalās LU kvalifikācijas darbu aizstāvēšanā.
- 14.06. CERT.LV sniedza konsultāciju Rīgas Tehniskajai koledžai par apmācību programmas "IT drošības speciālists" izveidi.
- 17.06. Tikšanās ar StratCom COE, lai izvērtētu bakalaura darba "Twitter troļļi – statistikas metodes automātiski ģenerēta satura noteikšanai" ietvaros veiktā pētījuma rezultātus.

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 ir uzsācis gatavošanos noteikto funkciju veikšanai.

Saskaņā ar šobrīd plānoto pienākumu sadalījumu CERT.LV pārstāvji piedalīsies Elektroniskās identifikācijas uzraudzības komitejas darbā un sniegs tehnisko atbalstu, izvērtējot pakalpojumu sniedzējus, tostarp veiks informācijas sistēmu risku analīzi un izvērtēs atbilstību normatīvajiem aktiem, kuros noteiktas informācijas sistēmu drošības tehniskās un organizatoriskās prasības.

Pārskata periodā paveiktais:

- Uzsākta un tiek turpināta standartu izpēte pārbaužu metodikas izstrādei, kā arī veikta ES regulas Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un to pavadošo dokumentu (īstenošanas lēmumu un īstenošanas regulu) izpēte.

- Elektroniskās identifikācijas uzraudzības komitejas pārstāvji no CERT.LV iesaistījās uzticamības sarakstu (*Trusted Lists - TL*) migrācijas jautājumu izpētē un migrācijas

nodrošināšanā - apmeklēja Eiropas Komisijas (EK) organizētas mācības, piedalījās TL izveidē un migrācijā, kā arī organizēja iesaistīto pušu sanāksmes.

- Sagatavoti komentāri par saistītajiem normatīvajiem aktiem un to grozījumiem atbilstoši noteiktajai kompetencei.

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 01.04.2016. līdz 30.06.2016. ir saņēmusi un izvērtējusi 155 ziņojumus. No tiem 56 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 45 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 9 ziņojumos konstatēta personas goda un cieņas aizskaršana un 3 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 5 ziņojumi. 23 ziņojumu saturs nav bijis pretlikumīgs, 14 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 23 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 31 ziņojums 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.

2016. gada 22. jūlijā

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