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 1. ceturksnis (01.01.2016. – 31.03.2016.)

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 3

1. Elektroniskās informācijas telpā notiekošo darbību atainojums. 4

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā. 7

3. Mobilo ierīču ļaunatūras pētniecība 14

4. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību). 15

5. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā. 17

6. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā. 18

7. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu. 19

8. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām. 20

9. Citi normatīvajos aktos noteiktie pienākumi. 21

10. Aģentūras papildu pasākumu veikšana. 21

Kopsavilkums

2016.gada 1.ceturksnī CERT.LV reģistrēja un apstrādāja 722 augstas prioritātes incidentus un 235 186 zemas prioritātes incidentus.

Gada sākumā tika atklātas vairākas ievainojamības E-parakstītājs programmatūrā un saistītās Java bibliotēkās. Ievainojamības atklāja IT drošības speciālists Oskars Veģeris sadarbībā ar SIA BITI. CERT.LV uzsāka ievainojamību novēršanas vadības procesu un reģistrēja tās starptautiskajā CVE ievainojamību reģistrā.

Visa ceturkšņa garumā tika fiksētas vairākas apjomīgas mēstuļošanas kampaņas, kuru mērķis bija izplatīt šifrējošos izspiedējvīrusus Tesla Crypt, Locky vai Crypto Wall. CERT.LV saņēma arī ziņojumus par vīrusu upuriem un nošifrētiem datoriem. Līdz pat pārskata perioda beigām nebija zināms veids, kā nošifrēto informāciju atgūt.

Līdz šim šifrējošie vīrusi skāra tikai Windows lietotājus, bet pārskata periodā tika saņemta informācija arī par pirmajiem šifrējošā vīrusa gadījumiem, kuros vīruss nošifrēja failus Linux operētājsistēmās.

Palielinājās to ļaundabīgo aktivitāšu skaits, kas vērstas uz mobilo iekārtu lietotājiem. Tika fiksēti gan mēģinājumi izkrāpt maksājumus ar uzmanības novēršanas paņēmieniem, gan mobilo iekārtu inficēšana ar ļaunatūru.

18.februārī CERT.LV organizēja semināru IT drošības speciālistiem “Informācijas tehnoloģiju drošības dokumenti”. Seminārs tika veltīts Ministru kabineta noteikumu Nr. 442 ieviešanai un CERT.LV sagatavotajiem dokumentu paraugiem.

Savukārt 9.martā, E-prasmju nedēļas ietvaros, CERT.LV rīkoja Datorologa akciju, kuras laikā jebkuram interesentam bija iespēja atnest savu datoru, planšetdatoru vai viedtālruni uz pārbaudi pie CERT.LV speciālistiem – Datorologiem. Pasākumu apmeklēja 59 interesenti.

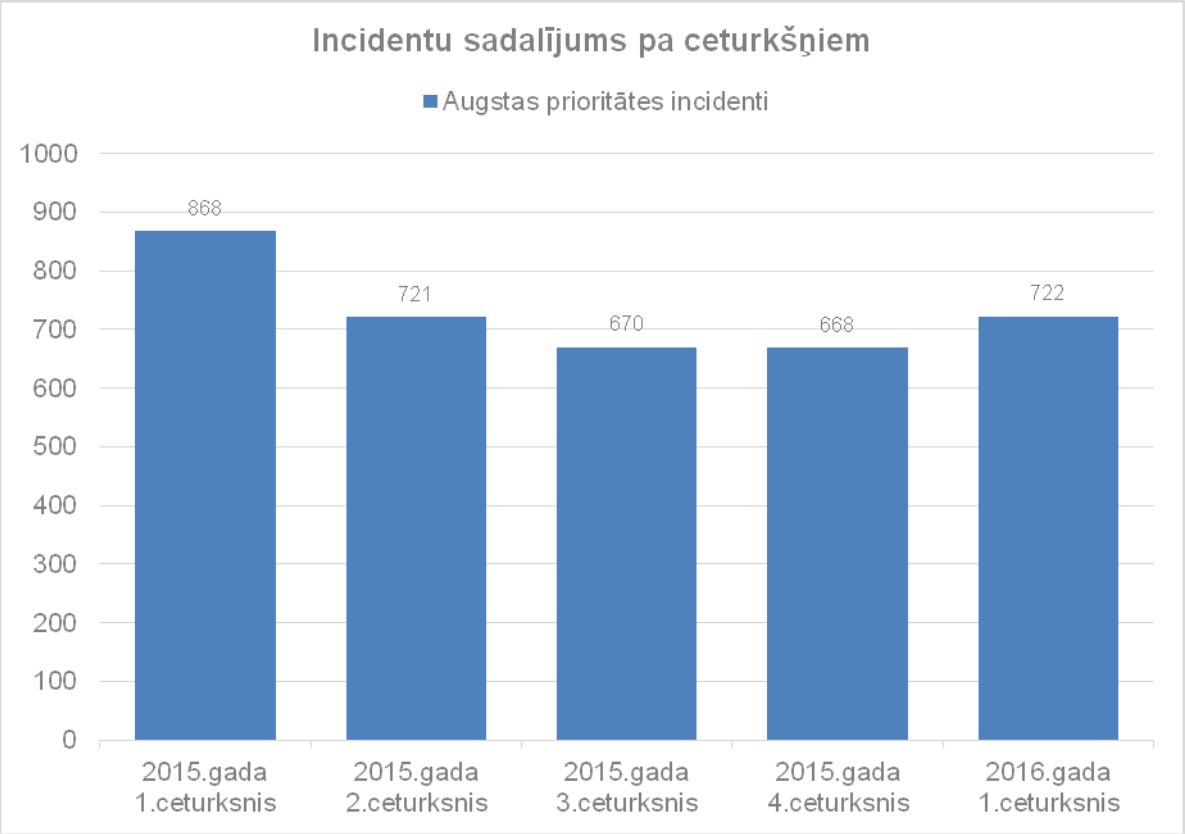
Pārskata periodā CERT.LV par IT drošību izglītoja 2167 cilvēkus, iesaistoties 19 izglītojošos pasākumos, ievietoja 43 jaunas ziņas vietnē www.cert.lv, piedalījās 3 radio pārraidēs un 10 televīzijas sižetos.

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.

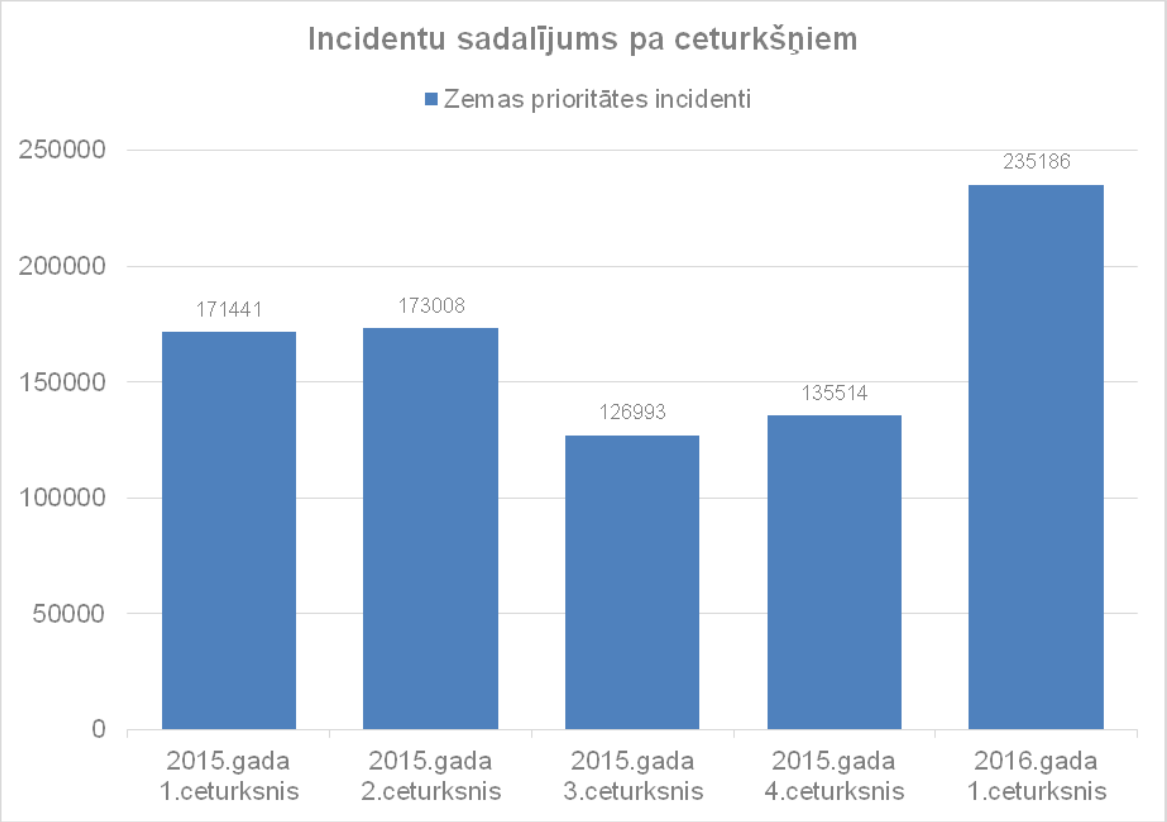
2016. gada 1. ceturksnī CERT.LV apstrādāja 722 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāts 668 augstas prioritātes incidents, bet 2015. gada 1. ceturksnī 868 augstas prioritātes incidenti.

Pēdējo 12 mēnešu periodā augstas prioritātes incidentu apjoms ir bijis stabils.



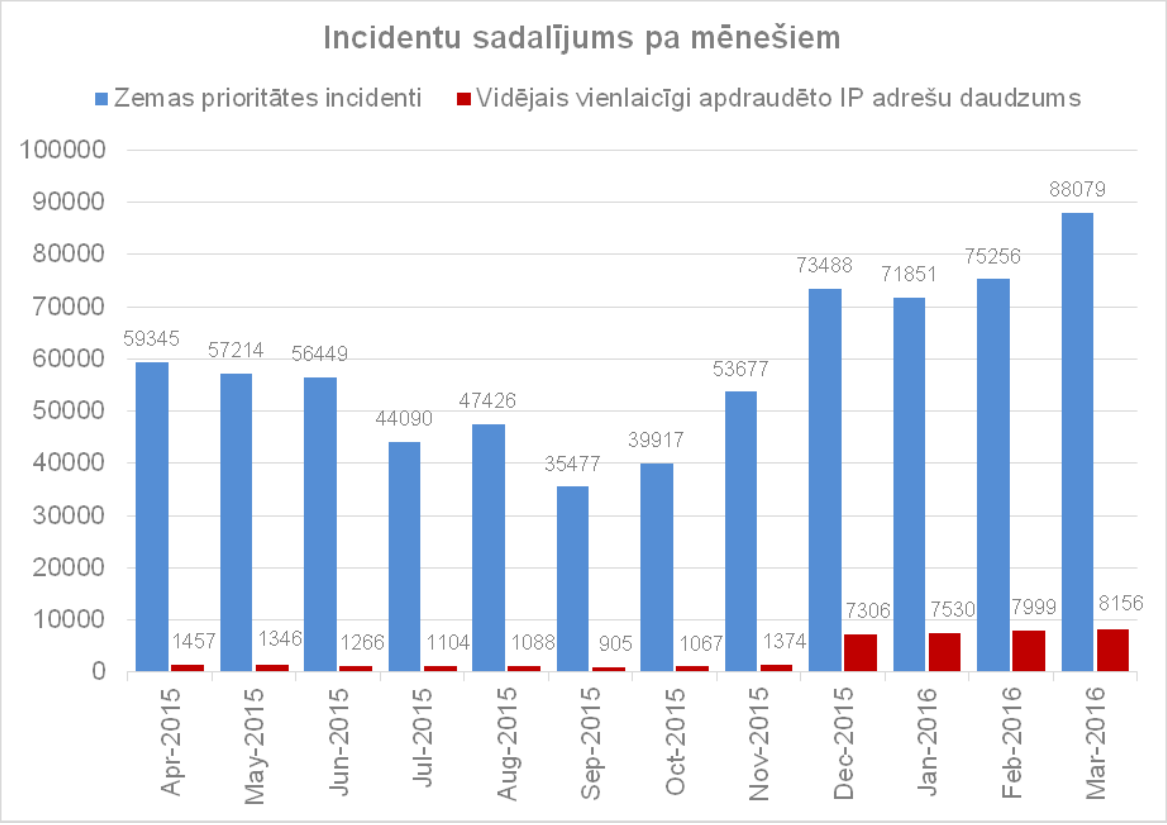
1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2015. un 2016. gadā.

2016. gada 1. ceturksnī CERT.LV reģistrēja 235 186 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 135 514 zemas prioritātes incidenti, bet 2015. gada 1. ceturksnī 171 441 zemas prioritātes incidents.



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

Zemas prioritātes incidentu skaita pieaugums skaidrojams ar apjomīgu Tesla Crypt un Locky šifrējošo vīrusu izplatīšanas kampaņu, kura visaktīvāk noritēja martā.



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

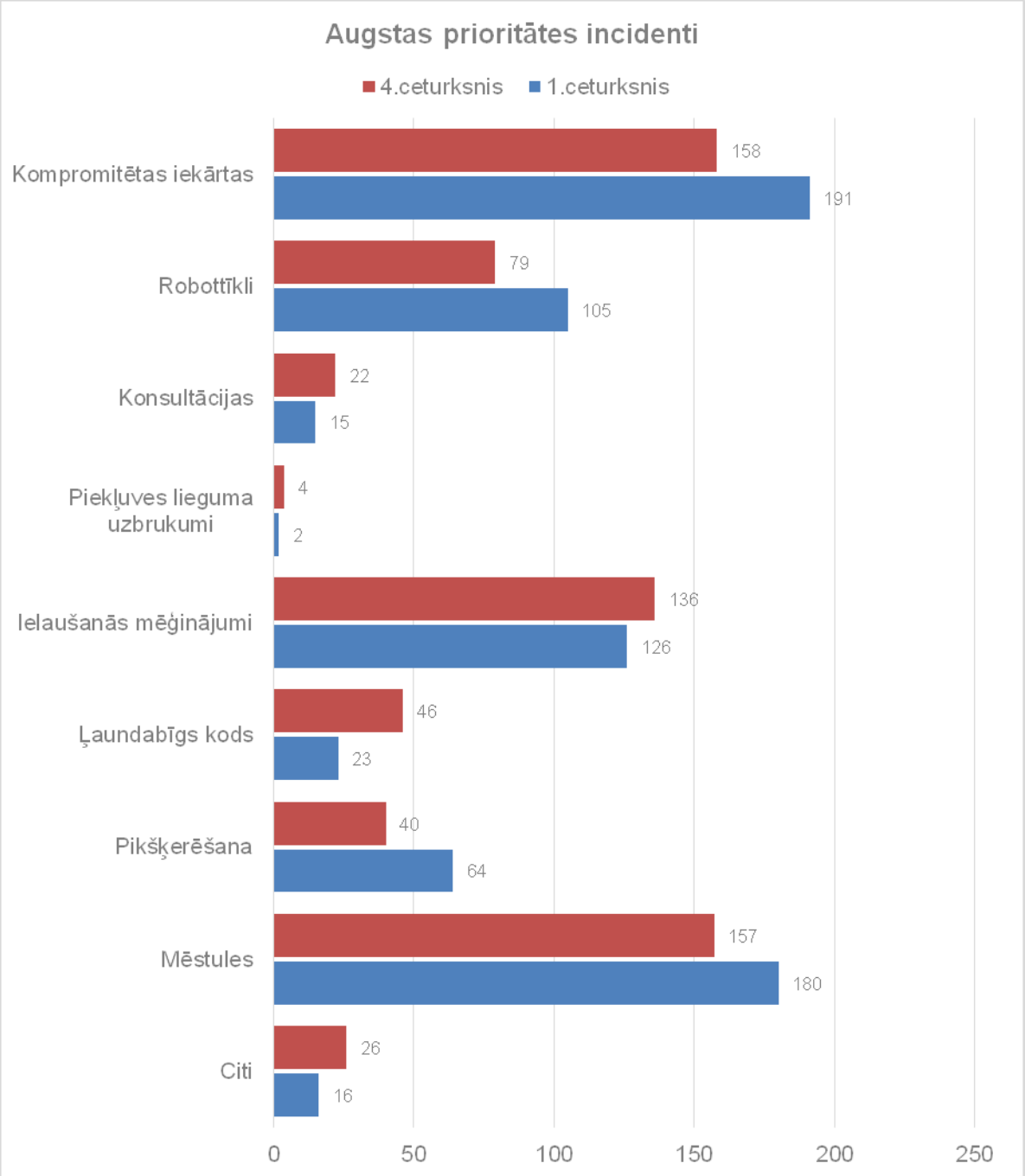
Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi apdraudēto unikālo IP adrešu skaitu Latvijā. Zemas prioritātes incidentu apjoma pieaugums 2015.gada noslēgumā un 2016.gada 1.ceturksnī un reizē arī CERT.LV fiksēto vienlaicīgi apdraudēto IP adrešu daudzuma pieaugums pārskata periodā skaidrojams ar jaunu ziņojumu avotu piesaisti. 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 Latvia 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.

IT drošības eksperti no SIA Latnet Serviss/Stream Networks un SIA Lattelecom, kas ir saņēmuši arī kvalitātes zīmi "Atbildīgs interneta pakalpojumu sniedzējs", iesaistījās CERT.LV organizētajā Datorologa akcijā, kas notika 9.martā E-prasmju nedēļas ietvaros.

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

Pārskata periodā CERT.LV reģistrēja un apstrādāja 722 augstas prioritātes incidentus.

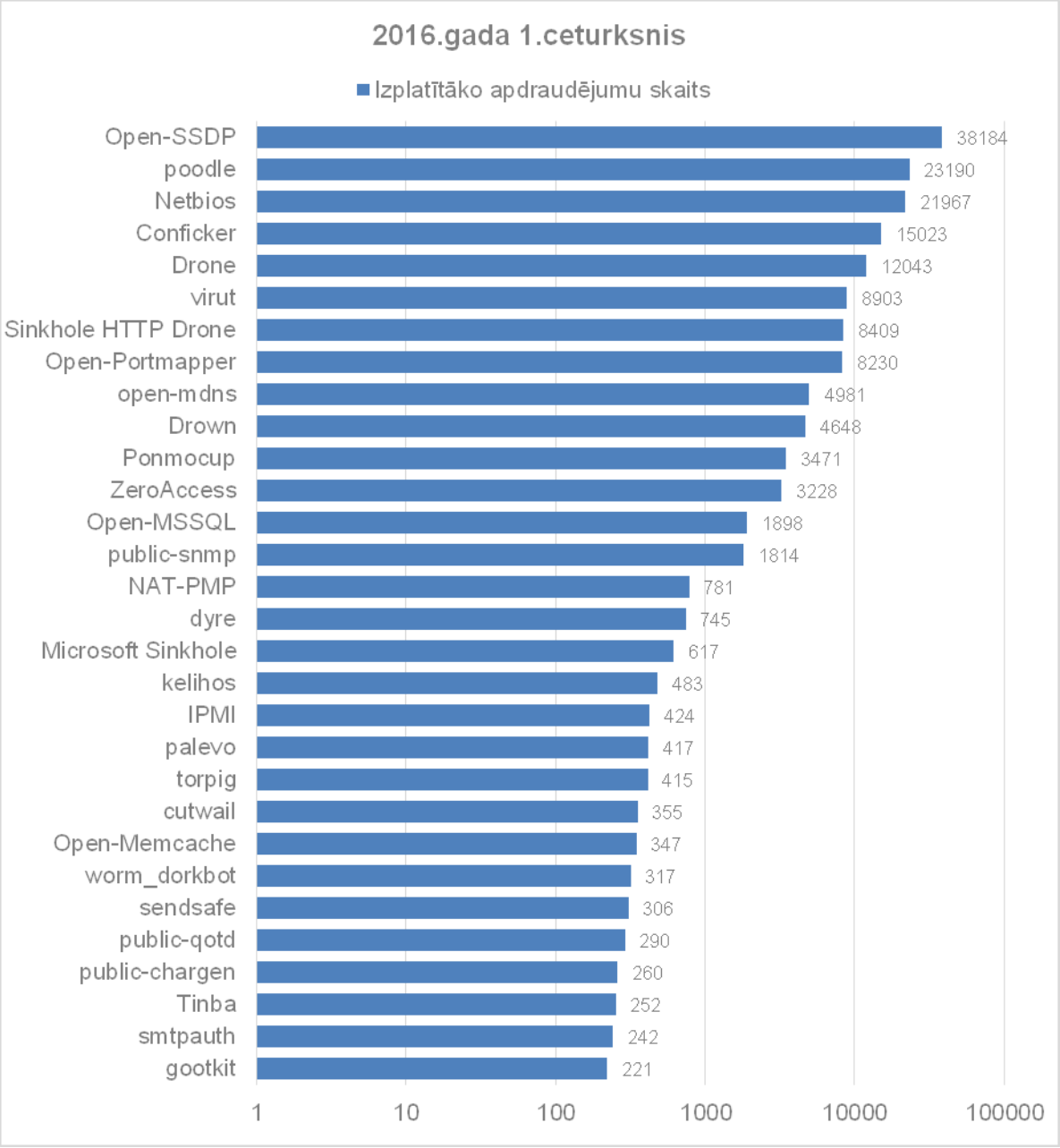


4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2015. gada 4. un 2016. gada 1. ceturksnī.

Lielais kompromitēto iekārtu daudzums lielākoties skaidrojams ar valsts un privātajā sektorā uzturētām mājas lapām, kas izmanto novecojušas un ievainojamas satura vadības sistēmas, galvenokārt Joomla un Wordpress. Uzlauztās mājas lapas pārsvarā tika izmantotas pikšķerēšanas aktivitātēm vai ļaunatūras izplatīšanai.

Pārskata periodā kompromitēto iekārtu apjomu palielināja arī šifrējošo izspiedējvīrusu Locky, Crypto Wall un Tesla Crypt upuri.

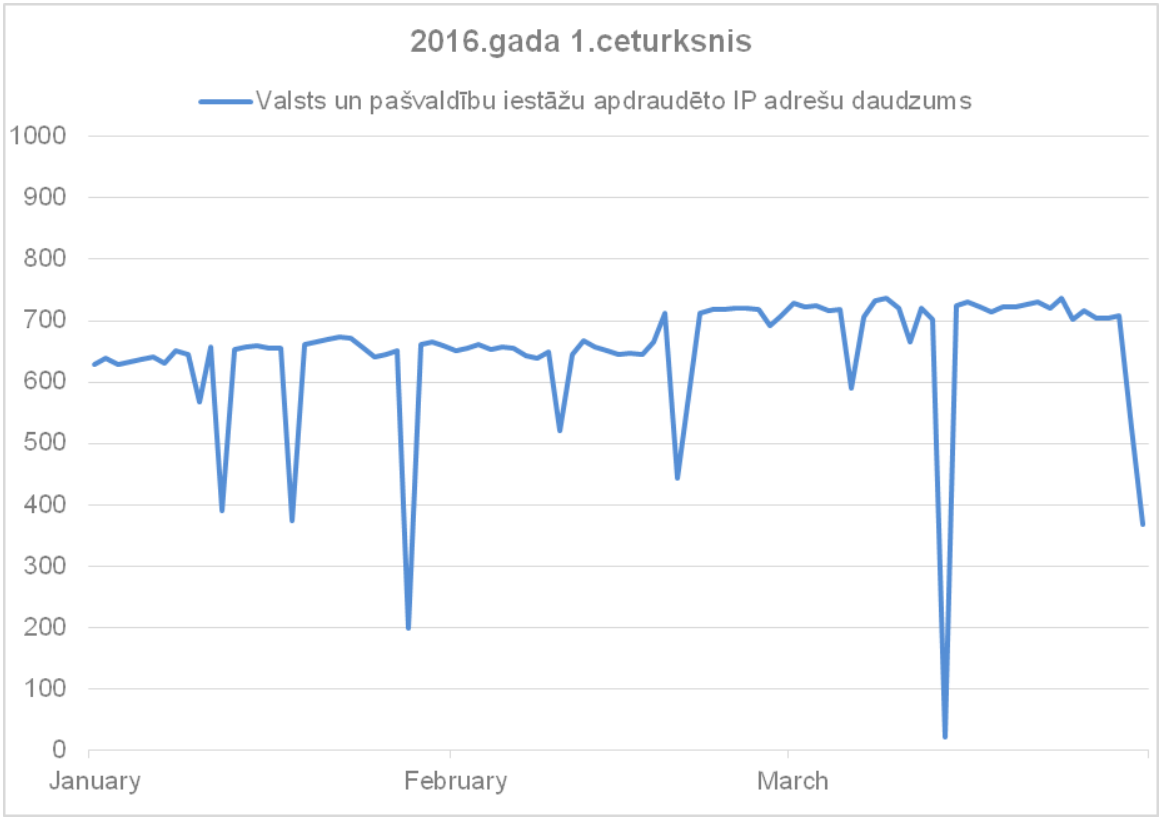
2016.gada 1.ceturksnī CERT.LV reģistrēja 235 186 zemas prioritātes incidentus.



5.attēls - CERT.LV reģistrētie zemas prioritātes incidenti no 2016. gada 1. janvāra līdz 31. martam pa apdraudējumu veidiem.

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.

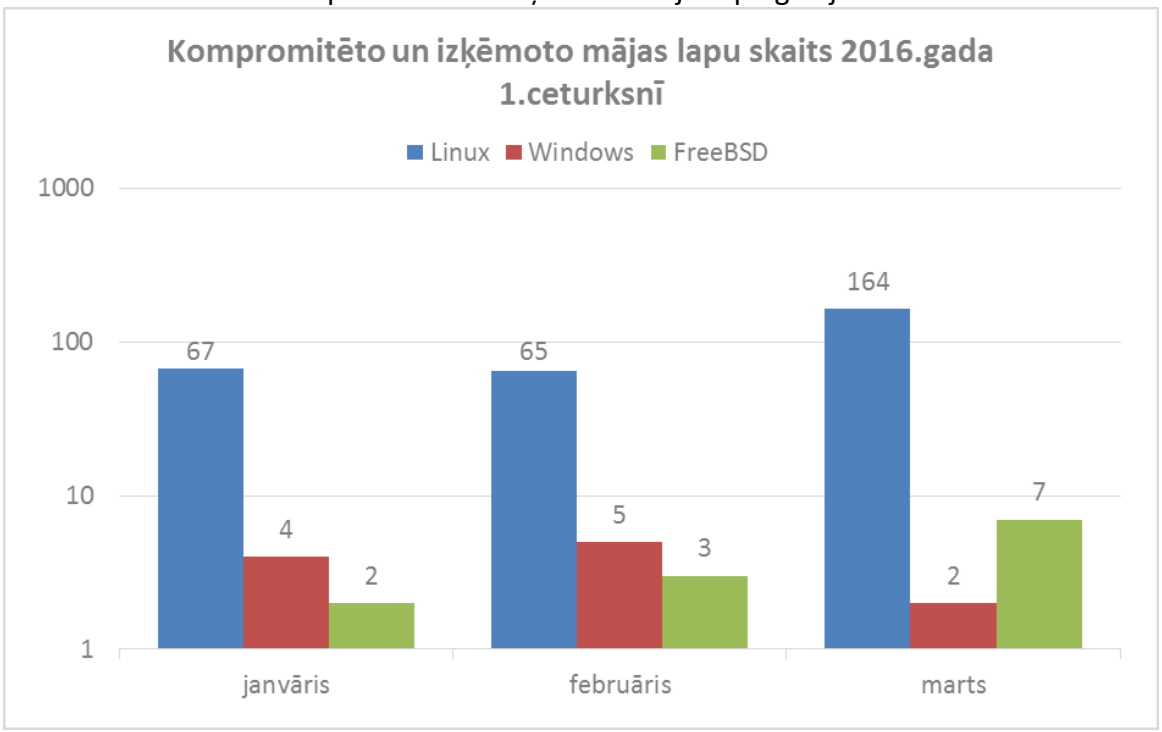
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:



6.attēls –Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2016. gada 1. ceturksnī.

Augstais valsts un pašvaldību iestāžu apdraudēto IP adrešu daudzums arī skaidrojams ar CERT.LV saņemtās un apstrādātās informācijas pieaugumu, jo tiek saņemta informācija no jauniem ziņojumu avotiem.

CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus.



7.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2016. gada 1. ceturksnī.

Salīdzinoši lielais martā izķēmoto lapu apjoms skaidrojams ar to, ka automātiska Joomla ievainojamību skenera redzes lokā nonāca kāds mitinātājs, kura serveros tika uzturētas mājas lapas ar neatjauninātu Joomla satura vadības sistēmu.

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

Svarīgākie CERT.LV drošības incidenti pārskata periodā

- 04.01. Tika atklātas vairākas ievainojamības E-parakstītājs programmatūrā un saistītās Java bibliotēkās. Ievainojamības atklāja IT drošības speciālists Oskars Veģeris sadarbībā ar SIA BITI. CERT.LV uzsāka ievainojamību novēršanas vadības procesu un reģistrēja CVE numurus:

  CVE-2015-8275
  1. Possible to WRITE arbitrary files to the filesystem by creating a specifically crafted EDOC file (versions: EDOC 1.01, EDOC 2.0)

  CVE-2015-8726
  2. Possible to READ arbitrary files from the filesystem by creating a specifically crafted EDOC file (versions: EDOC 1.01, EDOC 2.0)

- Janvāra sākumā kāds dators tika inficēts ar Linux Encoder 1 šifrējošo vīrusu caur Joomla attālinātā koda izpildes ievainojamību. Atšķirībā no jau zināmajiem šifrējošajiem vīrusiem, kas skāra tikai Windows lietotājus, šis vīruss šifrē failus Linux operētājsistēmās. Konkrētajā gadījumā tika nošifrēta tikai daļa no failiem, un tie tika atgūti ar rezerves kopiju un Internetā pieejama antivīrusa kompānijas BitDefender izstrādāta skripta palīdzību.
- 11.01. Kādā valsts iestādes vietnē no iekārtas ar Ukrainas IP adresi veiktas pārdomātas SQL injekcijas. Savukārt no iekārtas ar Latvijas IP adresi kāds lietotājs 1278 reizes mēģinājis izgūt adrešu datus, izmantojot nederīgu tokenu.
- 12.01. vairākās uz CMS Joomla un Wordpress bāzētās lapās ievietots kaitīgs skripts, kas pārvirza apmeklētājus, kuri izmanto Internet Explorer pārlūkprogrammu, uz Angler Exploit kit ļaunatūras izplatīšanas vietni. Konstatētas vairāk kā 10 kompromitētas lapas.
- Janvārī no vairākām uzlauztām e-pasta adresēm tika veikti pikšķerēšanas mēģinājumi ar mērķi izgūt PayPal lietotāju datus. Atbildīgie tika informēti un veiktas nepieciešamās darbības adrešu bloķēšanai.
- Janvārī pikšķerēšanai tika izmantotas arī divas uzlauztas interneta vietnes, kurās pēc uzlaušanas izvietots pikšķerēšanas uzbrukumiem domāts saturs. Pēc atbildīgās puses informēšanas kaitīgais saturs tika nodzēsts.
- 21.01. CERT.LV brīdināja kādu Latvijas uzņēmumu par internetā pieejamu Siemens gudrās mājas vadības kontrolieri. Lai arī pieeja bija aizsargāta ar paroli, tā konfigurācija bija nedroša un kontrolieris nevajadzīgi pakļauts uzbrukuma riskam.
- 28.01. Pēc Ukrainas CERT pieprasījuma slēgta Latvijas IP adresē uzturēta lapa, kas tika izmantota maksājumu karšu datu izkrāpšanā.

- 28.01. Kādā sludinājumu portālā tika konstatēti krāpnieciski sludinājumi, kuros, uzdodoties par "Morgan Machinery Limited" traktortehnikas tirdzniecības uzņēmumu, tika izkrāpta priekšapmaksa par lietotu traktortehniku. Portāla uzturētāji krāpnieciskos sludinājumus operatīvi dzēsuši, bet bija cietušie. Zināms, ka šie paši krāpnieki izvietojuši arī citus sludinājumus ar līdzīgiem uzņēmuma nosaukumiem, izmantojot citu kontaktinformāciju. Sadarbībā ar sludinājumu portālu tika apkopota informācija par šo krāpniecības gadījumu izcelsmi.
- Februārī turpinājās to mājas lapu uzlaušana, kuras izmantoja neatjauninātas un ievainojamas Joomla versijas, par kurām tika brīdināts jau 2015.gada beigās. Vienā no vietnēm tika izvietota pikšķerēšanas lapa ar mērķi iegūt e-pastu piekļuves datus, bet citā mājas lapā apmeklētāji, kas interneta pārlūkošanai izmantoja mobilās ierīces, tika pārvirzīti uz kaitīgu interneta vietni id.nice-dns.ru, kas mēģināja veikt datorvīrusa izpildi apmeklētāju iekārtās. Vairākās vietnēs, kas izmantoja ievainojamas Joomla versijas, tika izvietots kaitīgs Javascript fails, kas saturēja Angler Exploit kit rīku, ar kura palīdzību apmeklētāju datoros tika veikta datorvīrusu lejupielāde un izpilde.
- 04.02. Vairākos ar veļas mazgāšanu saistītos uzņēmumos mērķtiecīgi tika mēģināts iesūtīt datorvīrusus, kas domāti attālinātas piekļuves nodrošināšanai uzņēmumu datortīklam. Patiecoties laicīgai datorsistēmas uzturētāja reakcijai, kaitīgie pielikumi tika identificēti un bloķēti.
- 04.02. CERT.LV sadarbībā ar Lietuvas un Ukrainas kolēģiem izmeklēja banku trojāna izplatīšanas incidentus.
- 10.02. CERT.LV izmeklēja Dridex banku trojāna izplatīšanas kampaņu, kuras mērķu starpā bija liels skaits valsts iestāžu darbinieku e-pasti. Sekmīgu infekciju skaits bija neliels, neskatoties uz uzbrukuma kampaņas agresivitāti.
- 12.02. Kādas kompānijas klientiem tika izkrāpta nauda, aizsūtot tiem viltus rēķinu par datortehniku, kuros norādīts nepareizs maksājuma konts. Krāpšanai izmantots domēns capital-latvia.lv
- 16.02. Ar viltotiem reklāmas baneriem dažādās leģitīmās vietnēs tika reklamēta viltus loterija, kas WhatsApp vārdā aicināja apmeklētājus pieteikt savu mobilā tālruņa numuru paaugstinātas maksas abonēšanas pakalpojumam. Viltus baneri izmantoja informāciju par apmeklētāja IP adresi, lai noformētu viltoto paziņojumu kā datorlietotāja interneta pakalpojumu sniedzēja vārdā organizētu loteriju.
- 02.03. CERT.LV saņēma ziņojumus par masveidā izsūtītiem viltus paziņojumiem par piegādātiem pasta sūtījumiem. Paziņojumiem bija pievienots ZIP formāta arhīvs, kas saturēja Javaskript failu. Atverot pievienoto failu ar interneta pārlūku, tas veica Locky šifrējošā vīrusa lejupielādi.
- Marta sākumā tika reģistrēts ziņojums no kāda sociālā tīkla lietotāja, kurš tajā saņēmis draudu vēstuli, ka tiks publicētas privātas fotogrāfijas, ja netiks samaksāta izpirkuma maksa. Izpirkums ticis samaksāt, bet bilžu publiskošanu tas nav kavējis, papildus pieprasot vēl naudu, lai to pārtrauktu. Cietušajam CERT.LV ieteica vērsties policijā.
- 07.03. E-pastu pielikumos masveidā tika mēģināts izplatīt Tesla Crypt 3 un Locky šifrējošos datorvīrusus. Bija arī vairāki upuri.

- 08.03. Tika konstatēts, ka vairākas komunālo maksājumu pieņemšanas vietnes ir nepareizi konfigurētas un pārsūta klientu piekļuves un reģistrācijas datus nešifrētā veidā. Tika brīdināti serveru īpašnieki.
- Martā tika atklāta viltota mājas lapa, kas uzdevās par kompāniju, kas izsniedz jūrnieku sertifikātus. Tā lūdza iesniegt nepieciešamo informāciju sertifikāta saņemšanai, kas saturēja arī personas datus. Lapa saturēja viltus informāciju un nelikumīgi izmantoja Latvijas Jūras spēku flotiles ģerboni. Pēc izpētes secināts, ka šāda kompānija nepastāv un nav sertificēta izsniegt jūrnieku sertifikātus. CERT.LV informēja šīs vietnes uzturētājus, kā arī attiecīgās valsts CERT komandu, lai novērstu šīs vietnes turpmāku darbību.
- 31.03. Tika konstatēts kādā uzlauztā vietnē ievietots skripts, kas, izmantojot specifiski noformētu URL saiti, pārvirza apmeklētājus uz datorvīrusu izplatīšanas vietnēm. Servera īpašnieki tika brīdināti, lapa salabota.
- Martā kādam uzņēmumam tika kompromitēts Facebook konts, un no tam piesaistītās kredītkartes nozagti apmēram 2000 EUR nepieprasītu reklāmu apmaksai. Pēc Facebook un kredītkartes izdevējbankas informēšanas, nauda kontā atgūta.
- Martā viltus rēķinu veidā tika izsūtīti .ace formāta arhīva pielikumi, kas saturēja KAZY saimes datorvīrusu.
- Marta otrajā pusē aktivizējās jauna Tesla Crypt šifrējošā izspiedējvīrusa versija 3.0, kurai nav izstrādāti rīki failu atšifrēšanai. Nedēļas laikā bija vairāki upuri, kuriem tika sašifrēti datorā esošie faili. Vīruss tika izplatīts ar e-pasta pielikumos sūtītiem failiem .zip formātā, kas saturēja Javascript failu, kuru atverot, tas veica vīrusa lejupielādi no interneta.
- Marta otrajā pusē krāpniekiem, uzdodoties par vācu sadarbības partneri, no Latvijas uzņēmuma izdevās izkrāpt naudu. Krāpšana notika, nosūtot viltus rēķinu it kā no sadarbības partnera par preces piegādes uzsākšanu, kuru uzņēmums arī apmaksāja uz viltus rēķinā norādītajiem konta numuriem. Šādi krāpšanas gadījumi pēdējā gada laikā aktualizējušies, tāpēc, lai izvairītos no šādu viltus dokumentu saņemšanas, CERT.LV iesaka izmantot elektroniski parakstītus dokumentus, lai būtu droši par to izcelsmi.
- Marta beigās konstatēta Adobe Flash Player ievainojamības CVE-2015-7645 izmantošana tādos uzbrukuma (exploit kit) rīkos kā Angler EK. Latvijā tika konstatēta šīs ievainojamības izmantošana, lai izplatītu Vawtrak ļaunatūru ar Angler EK. Ļaunatūras mērķis bija internetbanku lietotāji.
- Marta beigās tika konstatēti arvien jauni inficēšanās gadījumi ar CryptoWall 3.0. vīrusu, kurš lietotāja datorā pieejamo informāciju efektīvi nošifrēja un uzbrucēji pieprasīja izpirkuma maksu par informācijas atšifrēšanu. Šis vīruss dažu gadu laikā ir radījis desmitiem miljonu eiro zaudējumus visā pasaulē.

  Vīrusa izplatīšana lielākajā daļā gadījumu notika caur e-pastu sūtījumiem, kas saturēja kaitīgus pielikumus, taču bija arī virkne gadījumu, kad kaitīgais kods tika piegādāts caur uzlauztām tīmekļa vietnēm. Pielikumi varēja būt gan arhīvs (.ZIP) ar izpildāmo failu .EXE vai .SCR, gan arī kaitīgu kodu saturoši MS Office un PDF dokumenti.

Uzbrucēji kā daļu no uzbrukuma infrastruktūras bieži izmantoja novecojušas, uzlauztas Wordpress tīmekļa vietnes.

- Marta beigās tika konstatēta e-pastu izsūtīšanas kampaņa, kas saistīta ar Dyre banking trojāņa izplatīšanu, kurš tiek izmantots naudas zādzībām no internetbanku kontiem. Kaitīgo e-pastu izplatība notika arī no inficētiem valsts un pašvaldību iestāžu datoriem. Pielikumā atradās izpildāmo failu saturošs .zip fails, kas lietotāju maldināšanai Windows datorsistēmās attēlojās ar PDF dokumentam līdzīgu ikonu. Fails saturēja lejupielādes rīku, kas pēc programmas palaišanas veica datorvīrusa Dyre (zināmu arī kā Dureza.A, Dyreza) lejupielādi un izpildi upura datorā.

Konstatējot būtisku potenciālo apdraudējumu, CERT.LV par to informē valsts un pašvaldību iestāžu par IT drošību atbildīgos un sniedz ieteikumus, kā veicināt iestāžu IT drošību un mazināt draudus.

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 5. un 8.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 uzsāka darbu pie laboratorijas izveides.

Izvēlētais laboratorijas aprīkojums ļaus veikt gan manuālu, gan automatizētu mobilās ļaunatūras analīzi un ļaus operatīvāk identificēt mobilos apdraudējumus, kā arī paaugstinās CERT.LV spēju reaģet incidentu gadījumā.

Nozīmīgākie mobilo iekārtu incidenti:

- 10.01. No vairākiem kāda mobilā operatora klientiem tika saņemtas sūdzības, ka no viņu rīcībā esošām GSM interneta piekļuves iekārtām tiek masveidā izsūtītas maksas īsziņas. Veicot iekārtas analīzi, tika konstatēts, ka iekārtas vadības panelis ir brīvi pieejams no interneta, izmantojot ražotāja standarta paroli. Šāda iekārtas konfigurācija neatbilst noklusējuma uzstādījumiem, īpašnieki vai iekārtu apkalpojušās personas kļūdījušās, veicot iekārtu konfigurācijas maiņu. Sadarbībā ar mobilo operatoru tika apzināti vēl citi iespējamie apdraudētie klienti.
- Februāra beigās tika saņemts ziņojums par kāda lietotāja mobilo telefonu, no kura bez lietotāja ziņas tika izsūtīti apmēram 200 SMS ziņojumi ar tekstu "Let's video chat and text on imo! get the free app http://ww24.getvideocalls.com”
  Apmeklējot norādīto saiti, tā pārvirzīja apmeklētāju uz legālajā Google Play programmatūras centrā piedāvāto aplikāciju Imo IM (https://play.google.com/store/apps/details?id=com.imo.android.imoim), pievienojot savu refereri. ImoIM aplikācija nav zināma kā kaitīga, bet izmantotās reklamēšanas metodes var radīt zaudējumus tālruņa īpašniekam. CERT.LV veica pārbaudi, lai konstatētu, kura no tālrunī uzstādītajām aplikācijām izsūtīja šos SMS.
- Martā kāda sociālā tīkla Androdid aplikācijā tika konstatēta iespēja nesankcionēti iegūt lietotāju identifikācijas datus (vārdu, uzvārdu, attēlu), meklējot pēc zināma telefona numura, ja lietotājs to reģistrējis savā profilā. Meklējamajai personai nebija obligāti jābūt meklētāja draugu lokā.

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

1. Februārī CERT.LV atzīmēja institūcijas 5 gadu pastāvēšanu, atskatoties uz paveikto un tiekoties ar sadarbības partneriem un dibinātājiem.

Iestādes vadība secināja, ka iestādes pastāvēšanas laikā sabiedrības izpratne par kiberdraudiem un spēja tos atvairīt ir būtiski uzlabojusies, taču pieaugošā kiberuzbrukumu kvalitāte joprojām sagādā jaunus izaicinājumus.

9.februārī, Vispasaules drošāka interneta dienā, CERT.LV kopā ar citiem nozares ekspertiem no Komercbanku asociācijas, Swedbank un Draugiem.lv apvienojās Digitālās drošības aliansē, kuras mērķis ir izglītot sabiedrību un uzņēmumus par digitālās drošības jautājumiem.

10.februārī CERT.LV telpās viesojās Aizsardzības ministrijas valsts sekretāra Jāņa Garisona "ēnas" - četri skolēni, kas iepazinās gan ar valsts sekretāra darbu ministrijā, gan arī ar Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV darbību.

2.martā CERT.LV pārstāvis piedalījās Digitālās drošības alianses un Dienas Biznesa rīkotajā diskusijā, kurā tika apskatīti tādi jautājumi kā tipiskās kļūdas no uzņēmumu puses digitālajā vidē, norēķinos; jaunās Eiropas prasības; kā arī iespējas nākotnē plašāk izmantot e-parakstu autentifikācijai.

7.martā CERT.LV pārstāvis piedalījās E-prasmju nedēļas atklāšanas diskusijā par kiberdrošības jautājumiem. Diskusija notika Rīgas radio un televīzijas tornī un tika translēta tiešraidē.

Informācija par CERT.LV sadarbību ar medijiem

1) **Intervijas un ziņas radio:**
   - 01.02. CERT.LV pārstāvis piedalījās LR1 raidījumā "Kā labāk dzīvot" par sociālajiem tīkliem un mūsu drošību Internetā.
   - 08.02. CERT.LV pārstāvis sniedza interviju LR4 par Digitālās drošības alianses (DDA) izveidošanu.
   - 10.03. RadioTev tika sagatavots sižets "Noslēgusies akcija - aizved datoru pie ārsta".

2) **Sižeti televīzijā, tiešraides:**
   - 04.01. CERT.LV pārstāvis sniedza interviju LNT par kiberdrošības tendencēm.
   - 09.02. CERT.LV pārstāvis piedalās LNT raidījumā "900 sekundes".
   - 02.03. CERT.LV pārstāvis sniedza komentāru par mobilo apdraudējumu izplatību LTV raidījumam "Rīta panorāma".
   - 07.03. CERT.LV pārstāvis sniedza interviju LTV1 raidījumam "Rīta panorāma" par drošību digitālajā vidē.
   - 07.03. CERT.LV pārstāvis E-prasmju nedēļas ietvaros sniedza intervijas LNT un TV3 par digitālo drošību.
   - 09.03. Kā cīnīties ar vīrusiem tālrunī? - sižets LTV1 raidījumā "Rīta panorāma".
   - 09.03. Осторожно! Вам угрожают "шифровальщики"! – sižets 1BK ziņu izlaidumā

(Datorologa akcijas ietvaros).
- 13.03. CERT.LV pārstāvis sniedza komentāru LTV raidījumam "De Facto" par Gozi vīrusu.
- 15.03. CERT.LV pārstāvis sniedza komentāru Vidzemes TV par viedierīču drošību.
- 21.03. CERT.LV pārstāvis sniedza komentāru LTV1 par nelicenzētas programmatūras lietošanu

3) Informācija par CERT.LV tīmekļa vietnēm:

Pārskata periodā vietnē https://www.cert.lv publicētas 43 ziņas.

Populārākā sadaļa bija par jaunākajiem vīrusiem, kurai ir 9,805 unikāli skatījumi. Otra populārākā bija ziņa par MK noteikumu nr.442 ieviešanai veltīto semināru ar 2,083 unikāliem skatījumiem. Trešā populārākā bija CERT.LV jaunumu sadaļa, kuru skatījuši 1,830 unikāli apmeklētāji. Pārskata periodā novērojams būtisks apmeklētāju apjoma kritums, salīdzinājumā ar 2015.gada nogali. Tas skaidrojams ar to, ka iepriekšējā pārskata periodā CERT.LV publicēja informācija par inficētu e-pastu izplatīšanas kampaņu, kas guva lielu sabiedrības uzmanību.

Kopā CERT.LV mājaslapai bijuši 17,843 lapu skatījumi, kurus veido 10,588 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 14,295 apmeklējumi, no tiem 11,655 unikāli apmeklējumi. Portāla apmeklējums ir nedaudz pieaudzis, salīdzinot ar iepriekšējo pārskata periodu.

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

Portālā publicētie raksti:
- Kas ir ļaunatūra?
- Pasaka par Antiņu un viņa miljoniem
- Pasaka par Gaišgalvīti
- Mājas tīkla drošība
- Jaunā planšetdatora drošība

4) CERT.LV sociālo tīklu konti:
- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1490.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 337.
- CERT.LV draugiem.lv lapā http://www.draugiem.lv/certlv. Pārskata perioda beigās lapas sekotāju skaits 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 teju nemainīgs.

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

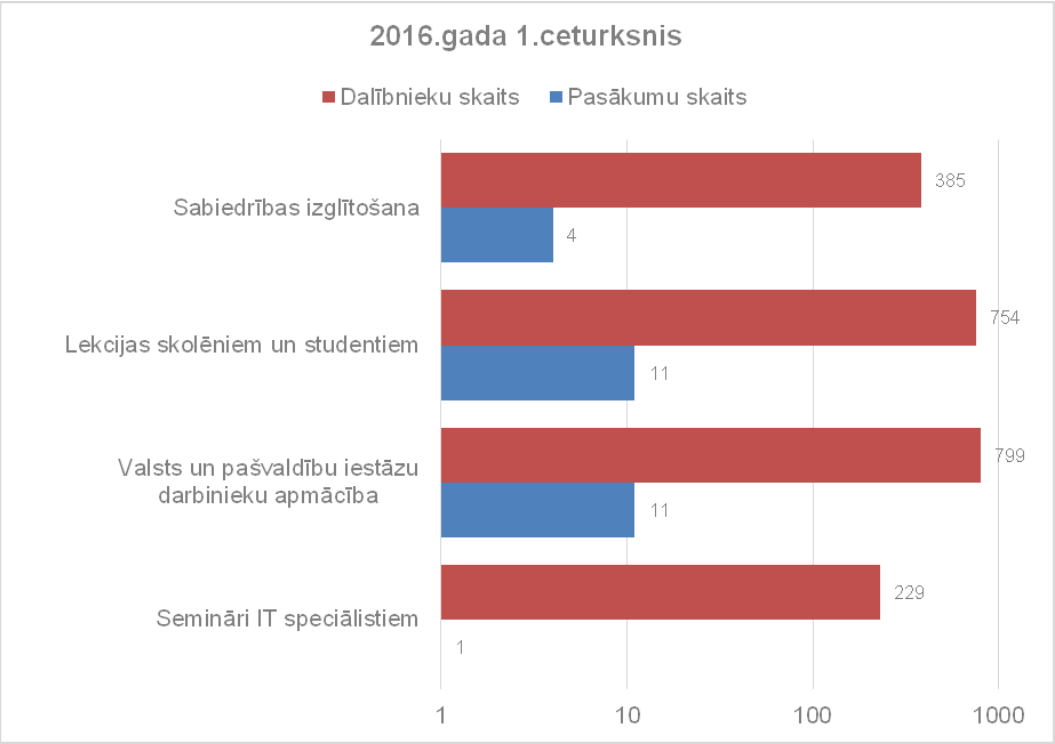
28. janvārī LATA rīkotajā konferencē "Atvērtas tehnoloģijas un viedi risinājumi" CERT.LV pārstāvis uzstājās ar prezentāciju "Internet of Things – kur drošībai nav vietas", kuras pamatā ir neliels CERT.LV pētījums par IoT iekārtām Latvijas internetā. Pasākumu apmeklēja aptuveni 270 dalībnieki.

18. februārī konferenču centrā Citadele notika CERT.LV seminārs IT drošības speciālistiem "Informācijas tehnoloģiju drošības dokumenti". Seminārs tika veltīts Ministru kabineta noteikumu Nr. 442 ieviešanai un CERT.LV sagatavotajiem dokumentu paraugiem. Semināru klātienē apmeklēja 229, bet tiešraidē vēroja gandrīz 500 interesenti.

9. martā E-prasmju nedēļas ietvaros CERT.LV rīkoja Datorologa akciju. Tās laikā jebkuram interesentam bija iespēja atnest savu datoru, planšetdatoru vai viedtālruni uz pārbaudi pie CERT.LV speciālistiem – Datorologiem -, lai noteiktu, vai iekārta nav inficēta, un, infekcijas gadījumā, to "izārstētu". Tika sniegtas arī konsultācijas par drošas interneta lietošanas un privāto datu aizsardzības principiem. Pasākumu apmeklēja 59 interesenti. Šogad akcijā kā Datorologi iesaistījās ar IT drošības eksperti no SIA Latnet Serviss/Stream Networks un SIA Lattelecom. SIA Latnet Serviss un SIA Lattelecom ir saņēmuši arī kvalitātes zīmi "Atbildīgs interneta pakalpojumu sniedzējs".

10. un 11. martā CERT.LV pārstāvji sniedza prezentācijas par IT drošību VARAM rīkotajā seminārā "e-Iespējas pašvaldībās". Seminārs notika E-prasmju nedēļas ietvaros, un to klātienē vēroja 56, bet tiešraidē 400 interesenti.

Pārskata periodā CERT.LV par IT drošību izglītoja 2167 cilvēkus, iesaistoties 19 pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2016. gada 1. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 07.01. Krimināllikuma darba grupas sanāksme Tieslietu ministrijā.
- 12.01. Tikšanās Aizsardzības ministrijā par IT drošības likuma izmaiņām.
- 14.01. un 11.02. DEG sanāksmes.
- 21.01. Konsultācijas ar nozares pārstāvjiem par jauno MK noteikumu ieviešanu.
- 12.02. Tikšanās VARAM par E-prasmju nedēļas organizēšanu.
- 22.02. CERT.LV uzstājās ar prezentāciju "Responsible Disclosure Policy and Latvia CERT collaboration" Aizsardzības ministrijas organizētā seminārā "Baltic Cyber Defense Workshop "Whole-of-Government Cyber Strategy & Policy Development"".
- 22.02. Tikšanās ar Iekšlietu ministriju, lai sagatavotos Latvijas novērtēšanas vizītei par kibernoziegumu prevencijas un apkarošanas jautājumiem.
- 09.03. Tikšanās ar Aizsardzības ministriju par atbildīgas ievainojamību atklāšanas politiku.
- 09.-10.03. Tikšanās Aizsardzības ministrijā par ES dalībvalstu savstarpējo novērtēšanu kibernoziegumu prevencijas un apkarošanas jautājumos.
- 15.03. Tikšanās ar Aizsardzības ministriju par atbildīgas ievainojamību atklāšanas politiku.
- 29.03. CERT.LV pārstāvis piedalās UNESCO rīkotajā "2. Eiropas Mediju un informācijas pratības foruma" koordinācijas darba grupas izveides sanāksmē Rīgā.

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.

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.

Pārskata periodā rīcības plānu iesniedza vēl viens ESK. Uz 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 6^1 panta izpildi, pārskata periodā nav saņemts neviens ziņojums.

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

Pārskata periodā CERT.LV pārstāvji piedalījās ar NATO kiberdrošības mācībām "Locked Shields 2016" saistītās sanāksmēs un pasākumos, gatavojoties piedalīties gan baltās (organizatoru), gan sarkanās (uzbrucēju), gan zilās (aizstāvju) komandas sastāvā. Uz Latviju iepazīšanās vizītē ieradās arī ASV kiberdrošības eksperti, kuri mācībās piedalīsies Latvijas-ASV apvienotajā komandā.

Martā tika uzsākta aktīva gatavošanās ENISA semināram "11th Annual National and Governmental CSIRTs Workshop – CSIRTs in Europe" un 48. TF-CSIRT sanāksmei, kas notiks maija otrajā nedēļā Rīgā.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 13.-15.01. CERT.LV pārstāvji piedalījās NATO kiberdrošības mācību "Locked Shields 2016" sagatavošanas sanāksmē Tallinā.
- 17.-19.01. CERT.LV pārstāvis piedalījās GEANT konferences "The Networking Conference" programmkomitejas sanāksmē Amsterdamā.
- 19.01. Notika tikšanās ar Somijas CERT pārstāvjiem.
- 24.-27.01. CERT.LV pārstāvis vadīja TF-CSIRT sanāksmi un vairāki CERT.LV pārstāvji piedalījās TF-CSIRT sanāksmē un FIRST tehniskajā seminārā Prāgā. CERT.LV pārstāvis uzstājās arī ar prezentāciju "CSIRT maturity and TI certification scheme in details".
- 28.-29.01. CERT.LV pārstāvji apmeklēja Luksemburgas valdības CERT.
- 15.02. CERT.LV uzsāka NATO kiberdrošības mācību "Locked Shields" 2016 komandas veidošanu.
- 07.-11.03. CERT.LV pārstāvis piedalījās Microsoft Digital Crimes Consortium konferencē Vīnē.
- 08.-09.03. CERT.LV pārstāvji piedalījās mācību "Locked Shields 2016" sagatavošanas sanāksmē Tallinā.
- 22.03. ASV komandas iepazīšanās vizīte pirms kopīgas dalības IT drošības mācībās "Locked Shields 2016".
- 22.03. CERT.LV pārstāvis piedalījās GFCE (Global Forum of Cyber Expertise) rīkotajā RDP (Responsible Disclosure Policy) darba grupas sēdē Budapeštā, uzstājoties ar prezentāciju par Latvijas pieeju atbildīgas ievainojamību atklāšanas jautājuma risināšanā un plānotajām izmaiņām likumdošanā.
- 26.03.-1.04. CERT.LV pārstāvji apmeklēja BlackHat konferenci Singapūrā.
- 29.03. CERT.LV pārstāvji piedalījās un uzstājās ar prezentācijām par Latvijas aktualitātēm Baltijas valstu sanāksmē "8th Baltic Cyber Security Coordination Meeting" Tallinā.

Pārskata periodā notika arī CERT.LV gatavošanās Trusted Introducer (TI) sertifikācijai un martā notika sākotnējās novērtēšanas seminārs, kurā Trusted Introducer pārstāvji sniedza CERT.LV darbības novērtējumu un ieteikumus darbības uzlabošanai. Plānots, ka TI sertifikāciju CERT.LV varētu saņemt līdz 2016.gada beigām.

Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

- 20.01. Tikšanās ar Digitālās drošības alianses pārstāvjiem par sadarbību.
- 28.01. CERT.LV pārstāvji apmeklēja Eiropas datu aizsardzības dienas ietvaros organizēto pasākumu "Bērnu un pusaudžu virtuālās dzīves ceļi un neceļi. Kā pasargāt?".

10. Aģentūras 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 01.01.2016. līdz 31.03.2016. ir saņēmusi un izvērtējusi 168 ziņojumus. No tiem 61 ziņojuma saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 25 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 13 ziņojumos konstatēta personas goda un cieņas aizskaršana un 4 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 16 ziņojumi, 31 ziņojuma saturs nav bijis pretlikumīgs, 18 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 7 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 55 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.

2016. gada 29. aprīlī

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