Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi 2016. gadā

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

2016. gadā Latvijas iedzīvotāji cieta no šifrējošo izspiedējvīrusu kampaņām. Savukārt uzņēmumi, apmaksājot krāpnieciskus rēķinus (CEO krāpšana), viena incidenta ietvaros zaudēja no 2 000 līdz pat 78 000 eiro.

Pārskata periodā aktualizējās lietu interneta (IoT) drošības jautājums. Pasaulē notikušais *Mirai* robotu tīkla veiktais uzbrukums, kurā tūkstošiem nedroši konfigurētu tīklam pieslēgtu iekārtu uz laiku padarīja nepieejamas virkni populāru tīmekļa vietņu, liek rūpīgi izvērtēt, kuras ierīces vai mājsaimniecības iekārtas tiešām ir nepieciešams pieslēgt internetam un pārliecināties, vai iekārta ir konfigurēta atbilstoši labajai praksei, ja tomēr to ir nepieciešams pieslēgt pie tīkla, lai neradītu apdraudējumu sev un apkārtējiem.

Pieaug tendence uzbrukumos izmantot mobilās iekārtas un sociālos tīklus. Mobilo iekārtu gadījumos pārsvarā izmanto lietotāju neuzmanību, lai panāktu pieteikšanos paaugstinātas maksas pakalpojumu saņemšanai, bet, palielinoties mobilo iekārtu izmantošanai banku transakciju veikšanai, paredzams, ka mobilo apdraudējumu apjoms un daudzveidība pieaugs. Attiecībā uz sociālajiem tīkliem vērojama lietotāju uzticēšanās informācijai, kas publicēta sociālajā tīklā, kaut arī lietotājs nav veicis padziļinātu informācijas patiesuma pārbaudi. Tādejādi sociālo tīklu lietotāji biežāk kļūst par krāpniecisku sludinājumu un loteriju upuriem.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 3047 augstas prioritātes incidentus un 595 405 zemas prioritātes incidentus.

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.

Decembrī CERT.LV sadarbībā ar Aizsardzības ministriju organizēja kiberdrošības mācības "Kiberdzirnas 2016", kurās piedalījās valsts un pašvaldību iestāžu vadītāji un par informācijas tehnoloģiju drošību atbildīgie darbinieki no 23 institūcijām. Pārskata periodā CERT.LV piedalījās 112 pasākumos, izglītojot 8963 cilvēkus par IT drošības tēmām.

1. Incidentu apstrāde

Pārskata periodā viens no izplatītākajiem incidentu veidiem bija šifrējošie izspiedējvīrusi *Locky*, *TeslaCryptn* un *CryptoWall*, kas lietotājiem tika nogādāti visbiežāk inficētu e-pasta pielikumu veidā. Drošākais veids, kā pasargāties no datu sašifrēšanas, ir nevērt vaļā e-pastu pielikumus no nezināmiem sūtītājiem, bet, ja dati tomēr ir tikuši sašifrēti, reālākais veids tos atgūt ir no rezerves kopijas. Atsevišķos gadījumos tas ir arī vienīgais datu atgūšanas veids, jo izspiedēji pat pēc izpirkuma maksas samaksāšanas vai nu apzināti, vai kļūdas pēc piekļuvi datiem tā arī nesniedz.

Otrs izplatītākais incidentu veids bija "CEO krāpšana", kad uzņēmuma vadītāja vai sadarbības partnera vārdā tiek lūgts veikt maksājumu uz viltus rēķinā norādītu bankas kontu. Parasti šie uzbrukumi ir rūpīgi sagatavoti, uzbrucēji nereti ir ieguvuši piekļuvi arī uzņēmuma e-pastu sarakstei un veikuši detalizētu situācijas izpēti, tāpēc atpazīt šos uzbrukumus ir diezgan sarežģīti. Saņemot e-pastu ar lūgumi veikt pārskaitījumu uz jaunu bankas kontu, drošāk ir sazināties ar sūtītāju telefoniski un pārliecināties, ka e-pasts ir īsts. CERT.LV iesaka izmantot arī elektroniski parakstītus dokumentus, lai mazinātu to viltošanas iespēju.

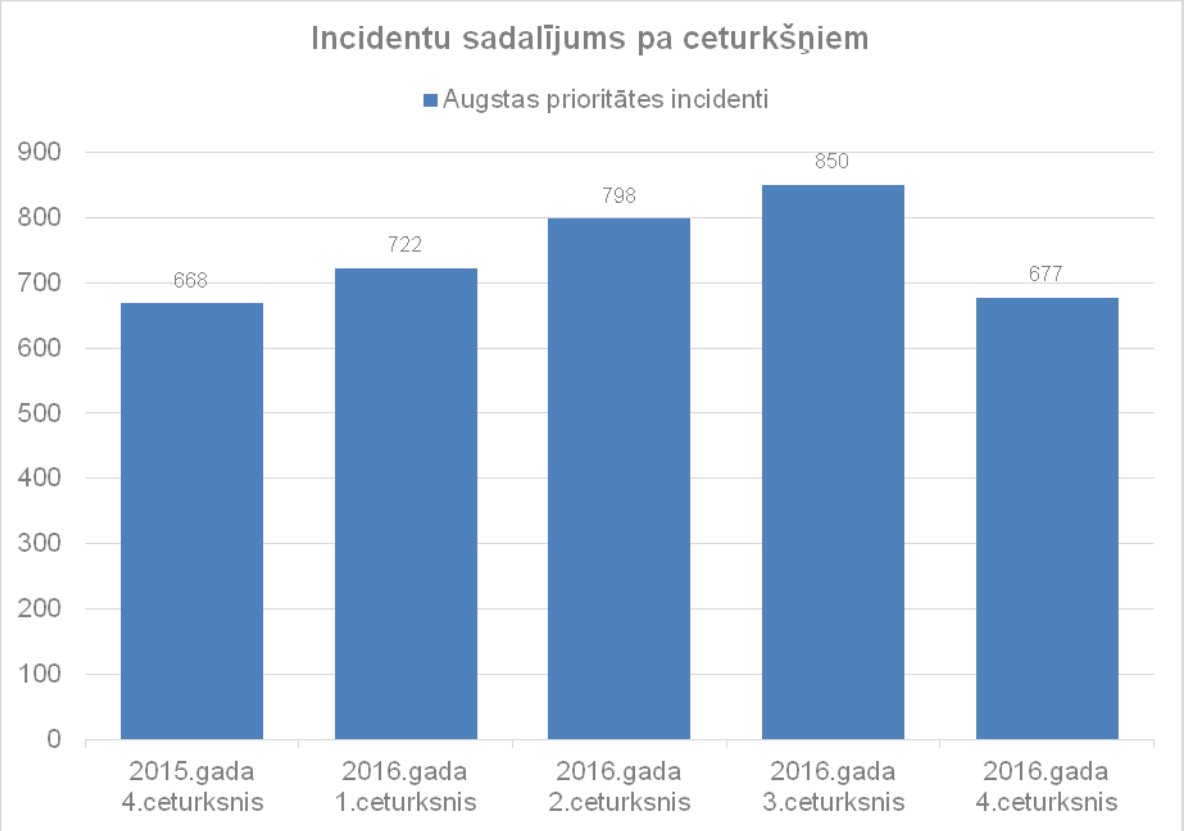
Pārskata periodā aktualizējās lietu interneta (IoT) drošības jautājums. Pasaulē notika lielākais lietu interneta realizētais uzbrukums, kas uz laiku padarīja nepieejamas vairākas globāli populāras tīmekļa vietnes. Virkne nedroši konfigurētu iekārtu, kas varētu būt piedalījušās uzbrukumā, tika konstatēta arī Latvijā. Ir pienācis brīdis, kad lietotājiem ir rūpīgi jāizvērtē, kuras ierīces vai mājsaimniecības iekārtas tiešām ir nepieciešams pieslēgt internetam, lai neradītu draudus sev un apkārtējiem.

1.1. Augstas prioritātes incidenti

CERT.LV apkopo informāciju par notikušajiem augstas prioritātes incidentiem, kas ir visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas vai par ko ir paziņojis cilvēks, nevis automātisks ziņotājs.

2016. gadā CERT.LV apstrādāja 3047 augstas prioritātes incidentus. Apstrādāto augstas prioritātes incidentu apjoms ir palielinājies salīdzinājumā ar iepriekšējo gadu, kad CERT.LV apstrādāja 2927 incidentus.

CERT.LV saņem ziņojumus no iestādēm, sadarbības partneriem, un lietotājiem, kas vēršas pēc palīdzības un konsultācijām, ja kibertelpā pamana ko neparastu. Apstrādāto augstas prioritātes incidentu apjoma pieaugums skaidrojams ar to, ka CERT.LV ir vairojis sabiedrības uzticību un ziņojumi par IT drošības incidentiem tiek saņemti ne tikai no institūcijām, kurām par incidentiem ir pienākums ziņot likumā noteiktajā kārtībā, bet arī no privātā sektora uzņēmumiem un individuālām privātpersonām, gan situācijās, kad ziņotājs ir arī cietušais, gan situācijās, kad novēroti kaitnieciski resursi vai darbības virtuālajā vidē.



1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem.

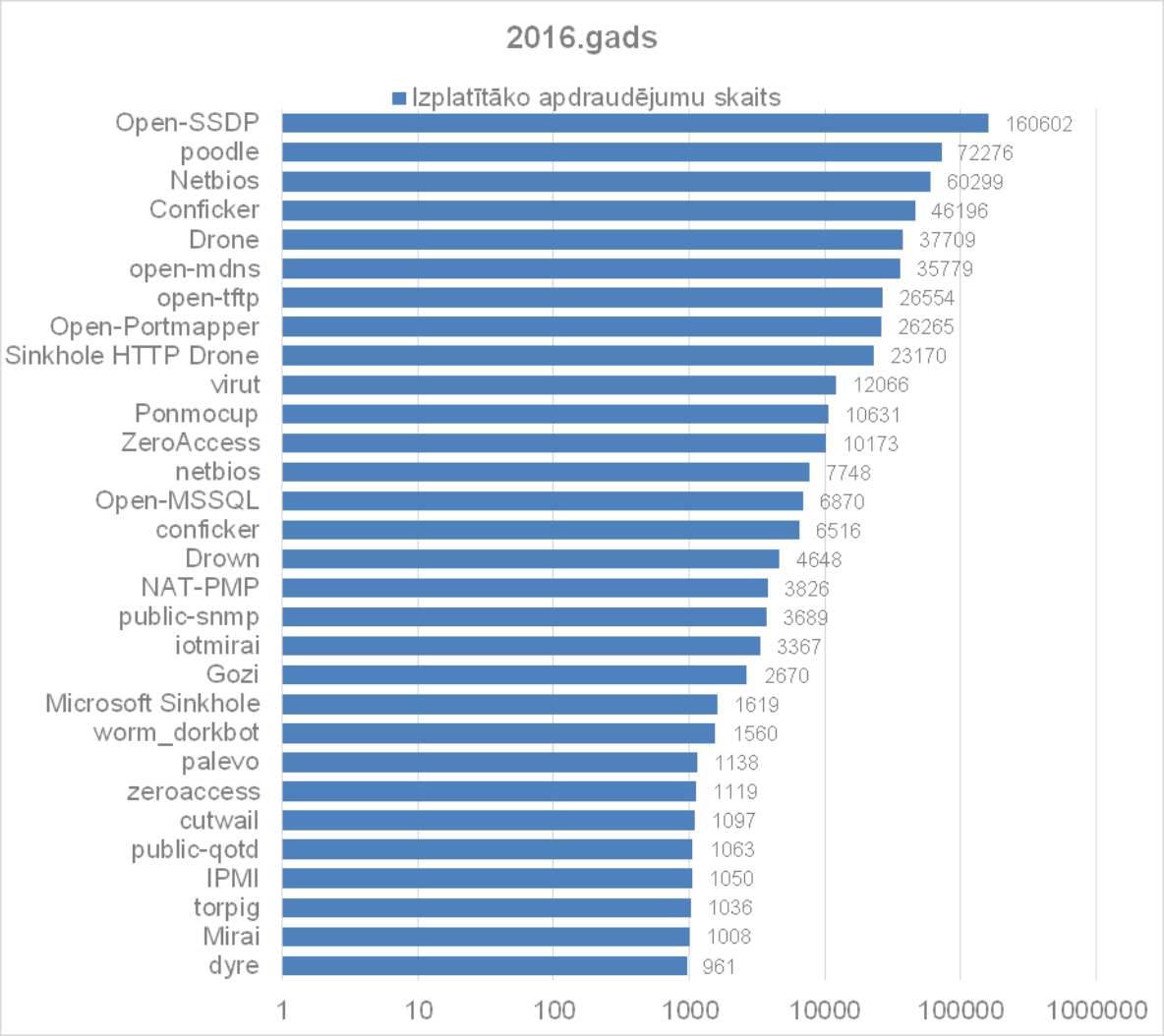
Visa pārskata periodā vērojams lēns, bet stabils augstas prioritātes incidentu kāpums, izņemot gada pēdējo ceturksni. Neskatoties uz to, ka pirmssvētku periodā krāpnieku un ļaundaru aktivitāte pieaug, statistikā tas visticamāk atspoguļosies vēlāk, jo to, ka notikusi krāpšana vai viņu iekārta ir inficēta, incidentos iesaistītie upuri bieži konstatē tikai vairākas nedēļas vai pat mēnešus pēc incidenta, kibernoziedzniekiem prasmīgi slēpjot sava nodarījuma pēdas.

Pirmo vietu augstas prioritātes apdraudējumu topā 2016. gadā ieņēma robottīkli, atstājot aiz sevis ielaušanās mēģinājumus un mēstules.

Lai novērstu sevišķi bīstamus incidentus, CERT.LV regulāri veica valsts un pašvaldību iestāžu brīdināšanu par aktuālajām vīrusu kampaņām, ievainojamībām un politiski nozīmīgiem datumiem, kad iestādēm jāpievērš pastiprināta uzmanība iestādes IT infrastruktūrai.

1.2. Zemas prioritātes incidenti

2016. gadā CERT.LV reģistrēja un apstrādāja 595 405 zemas prioritātes incidentus. Tie ir galvenokārt inficētas galalietotāju iekārtas, kas kļuvušas par robotu tīklu sastāvdaļām un/vai izsūta mēstules, kā arī nedroši nokonfigurētas iekārtas.



2.attēls - CERT.LV reģistrētie zemas prioritātes incidenti 2016.gadā pa apdraudējumu tipiem.

Latvijā joprojām ir salīdzinoši lieli *Conficker* vīrusa infekcijas rādītāji. Statistika liecina, ka lielākā daļa ar šo vīrusu inficētie datori lieto novecojušu *Microsoft Windows XP* operētājsistēmu, turklāt netiek lietota arī pretvīrusu programmatūra. Šis vīruss uzskatāms par novecojušu, kā arī no tā var diezgan vienkārši atbrīvoties, taču inficēto datoru īpašnieki nepūlas to darīt, padarot savu datoru par vīrusu perēkli un apdraudējumu citiem datorlietotājiem.

Nemainīgi augstas izplatības pozīcijas saglabā lielais nedroši konfigurēto ierīču skaits, kas statistikā atzīmēts kā *open-ssdp* un *netbios* servisi (pakalpojumi, kas nodrošina servisu apziņošanu un atpazīšanu tīklā, kā arī saziņas iespējas starp iekārtām lokālā tīkla ietvaros).

Visbiežāk šie servisi atrodas uz nedroši konfigurētiem mājas maršrutētājiem un WiFi iekārtām, kuras tiek lietotas ar ražotāja sagatavoto konfigurāciju, kas ir ērti, taču nebūt ne

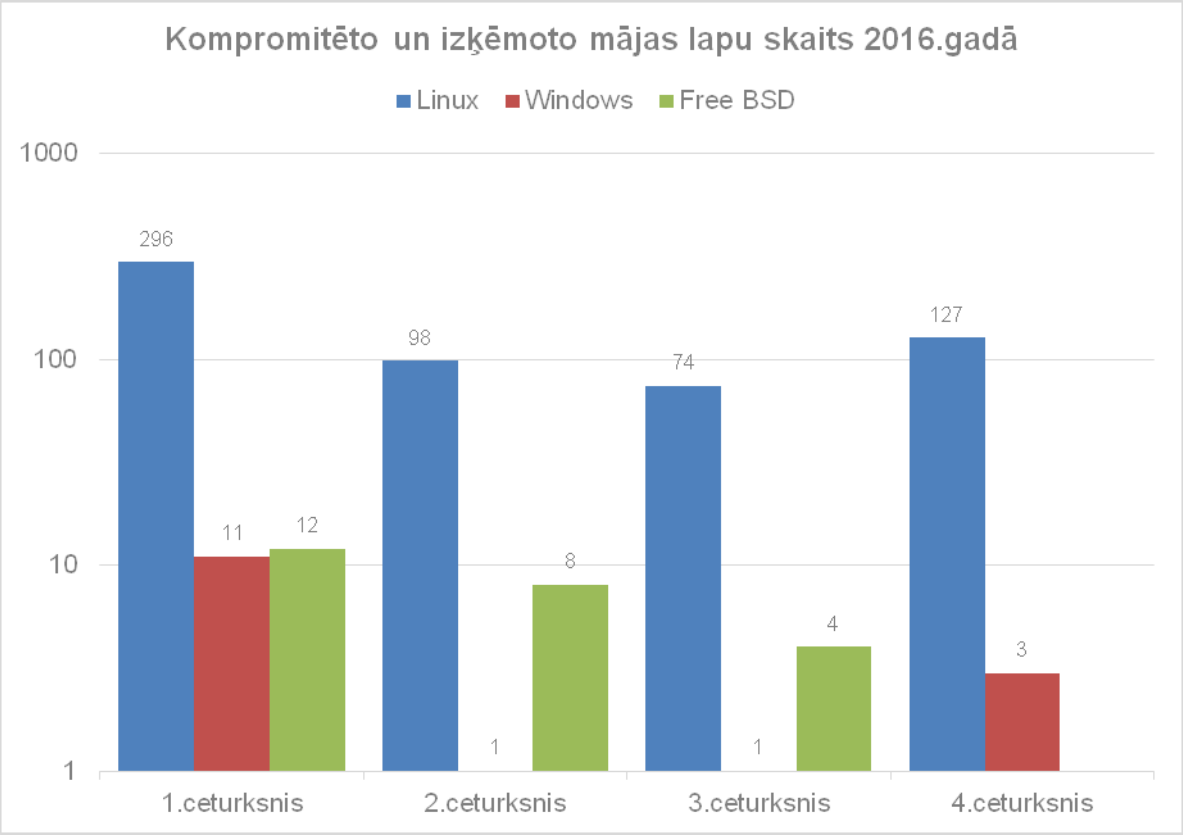
droši, sniedzot potenciālajiem uzbrucējiem ērtu iespēju piekļūt tīklā esošajiem datoriem un izmantot tos tālākās nelikumīgās darbībās vai veikt datu zādzību.

Bieži vien šo iekārtu funkcionalitāte tiek nesankcionēti izmantota, lai veiktu piekļuves lieguma (DDoS) uzbrukumus citiem tīkliem. Nedroši konfigurētas iekārtas arvien vairāk tiek izmantotas kā starpniekserveri noziedzīgu darbību slēpšanai.

CERT.LV sadarbojas ar lielāko daļu Latvijas interneta pakalpojuma sniedzēju un iniciatīvas "Atbildīgs interneta pakalpojuma sniedzējs" ietvaros informē par inficētām iekārtām gala lietotājus. Gandrīz 70% no CERT.LV rīcībā esošās informācijas ar atbildīgo interneta pakalpojuma sniedzēju starpniecību tiek sekmīgi nogādāta līdz gala lietotājam kopā ar instrukcijām, kā atbrīvoties no kaitīgās programmatūras un novērst konfigurācijas kļūdas.

Kompromitētas vietnes

CERT.LV uzskaita uzlauzto un izķēmoto mājaslapu gadījumus. 2016. gadā tika uzlauztas un izķēmotas 635 mājaslapas.



3. attēls – Kompromitēto mājas lapu skaits 2016. gadā.

2. Nozīmīgākie incidenti 2016. gadā

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

Izspiedējvīrusi

- Marta sākumā 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.
- Martā e-pastu pielikumos masveidā tika mēģināts izplatīt *TeslaCrypt* 3 un *Locky* šifrējošos datorvīrusus. Vīrusi tika izplatīti ar e-pasta pielikumos sūtītiem failiem .zip formātā, kas saturēja *Javascript* failu, kuru atverot, tas veica vīrusa lejupielādi no interneta. Kampaņām bija vairāki upuri, kuriem tika sašifrēti datorā esošie faili.
- 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 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.
- Aprīlī vairākas valsts iestādes cieta no *TeslaCrypt* un *Locky* šifrējošajiem datorvīrusiem. Dati tika atgūti no rezerves kopijām.
- Maijā kādā uzņēmumā šifrējošais izspiedējvīruss spēja 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.
- Maijā tika 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.
- 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.

- Augustā CERT.LV nodeva informāciju Valsts policijai par Latvijā uzturētu šifrējošā vīrusa *Zepto* kontrolcentru.
- Augusta beigās vairāki uzņēmumi cieta no šifrējošo datorvīrusu *Zepto* un *Crysis* darbības. Vīrusi aktivizēti, atverot *Microsoft Office Macro* komandas saturošus dokumentus, kas atsūtīti e-pastā.
- Augustā tika novērota arī agresīva *Locky* vīrusa izsūtīšanas kampaņa vairāku nedēļu garumā. Vīruss tika izsūtīts e-pasta ziņojumos, kas saturēja .docm paplašinājuma failus, kas ir *Microsoft Word* dokuments ar *Macros* aktīvā koda funkcionalitāti. Lai arī šī vīrusa aktivitāte vairs nepārsteidz, tā piegādes veidi ir cieši saistīti ar sociālās inženierijas elementiem un nereti tomēr panāk rezultātu neuzmanīgu lietotāju dēļ.
- Oktobrī kāda valsts iestāde saņēma e-pastu it kā pašas iestādes vārdā bez sūtījuma teksta, bet ar arhivētu (.zip) HTML failu pielikumā, kurš saturēja *Cerber* šifrējošo vīrusu. E-pasta filtri kaitīgo sūtījumu bloķēja.
- Novembra beigās kādas valsts iestādes darbiniekam tika atsūtīts e-pasts par rēķinu. E-pasta pielikums saturēja MS Excel failu ar *Macro* komandu, kas pēc atvēršanas datorā lejuplādē šifrējošo vīrusu *Locky*. Darbinieks tika brīdināts par kaitīgo saturu. Vīruss netika aktivizēts.
- Decembrī tika sašifrēts kādas valsts iestādes darbinieka dators. Darbinieks atvēra inficētu e-pastu ar augstas ticamības saturu no reāli eksistējošas e-pasta adreses, kas tika sūtīts, izmantojot eksistējošu pasta grupu. Dators bija pieslēgts pie bezvadu tīkla, kurš bija izolēts no lokālā datortīkla, rezultātā citi datori netika ietekmēti.

CEO krāpšana

- Janvārī un februārī no uzņēmumiem tika izkrāpti maksājumi par lietotu datortehniku, izmantojot krāpnieciskus sludinājumus portālos un viltotus rēķinus.
- Marta otrajā pusē krāpniekiem, uzdodoties par vācu sadarbības partneri, no Latvijas uzņēmuma izdevās izkrāpt naudu, nosūtot viltus rēķinu it kā no sadarbības partnera par preces piegādes uzsākšanu, kuru uzņēmums arī apmaksāja uz viltus rēķinā norādītajiem konta numuriem. Lai izvairītos no šādu viltus dokumentu saņemšanas, CERT.LV ieteica izmantot elektroniski parakstītus dokumentus, lai būtu droši par to izcelsmi.
- Aprīļa sākumā CERT.LV saņēma vairāku uzņēmumu incidentu pieteikumus, kurā izmantoti viltoti e-pasti, kas sūtīti kompānijas vadītāja vai sadarbības partnera vārdā, lai panāktu nozīmīgu naudas summu pārskaitīšanu uz krāpnieku bankas kontiem. 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.
- Arī jūnijā no kāda uzņēmuma klientiem mēģināts izkrāpt naudu, izmantojot viltotu rēķinu. Uzbrucēju kļūdas dēļ pārskaitījums neizdevās, kas pasargājis klientus no zaudējumiem. CERT.LV ieteica uzņēmumam brīdināt visus savus klientus par šāda veida krāpniecību.

- Augustā no kāda uzņēmuma partneriem, izmantojot viltotu rēķinu, izkrāpta samaksa par kokmateriālu sūtījumu. Ziņas par darījumu iegūtas, ielaužoties uzņēmuma e-pastā, kura piekļuves dati iegūti no datora, kas inficēts ar ļaunatūru. Pēc datoru iztīrīšanas un paroļu maiņas atkārtotie uzbrukumi nav bijuši sekmīgi.
- Augusta otrajā pusē identificēts krāpšanas mēģinājums, kura realizācijā uzbrucēji ieguldījuši lielāku izdomu un sagatavošanos nekā parasti. Lai veiktu krāpnieciskas darbības, uzbrucēji piereģistrējuši viltus uzņēmuma domēna vārdu .lv zonā, kas ir līdzīgs Latvijā strādājoša uzņēmuma nosaukumam, kā arī mēnesi pirms uzbrukuma izveidojuši Wikipēdija ierakstus par viltus uzņēmuma identitāti, lai potenciāliem upuriem izskatītos ticamāki. Lieki teikt, ka sarakstē norādītie kontu numuri nepieder patiesajiem partneriem, bet gan uzbrucējiem. Viltus tīmekļa vietnes, kurās norādīti neatbilstoši rekvizīti, uzticamības palielināšanai krāpnieki izmantojuši arī vēlākos incidentos.
- Novembra vidū CERT.LV saņēma vairākus ziņojumus par krāpšanas mēģinājumiem, kuros no uzņēmumiem mēģināja izkrāpt naudu ar uzņēmuma vadītāja vārdā sūtītu viltotu e-pastu. Krāpnieki pirms tam veikuši rūpīgu uzņēmumu mājas lapu izpēti, lai noskaidrotu uzņēmuma struktūru, uzņēmuma vadītāju, vadītāja e-pastu un uzņēmuma grāmatvedi, kuram adresēt viltoto sūtījumu. Lai attaisnotu kļūdaini sagatavoto tekstu, krāpnieki aizbildinājās ar bojātu klaviatūru. CERT.LV aicina būt uzmanīgiem un rūpīgi izvērtēt saņemtos e-pastus pirms tiek veiktas jebkādas finansiālas darbības. Ja e-pasti ir neprofesionāli sagatavoti, tajos ir steidzamības vai slepenības aspekts, drošāk ir veikt telefona zvanu un pārliecināties, vai šāds e-pasts tiešām ir sūtīts.
- Novembra beigās, izmantojot viltus rēķinus, kādam uzņēmumam tika izkrāpti vairāki maksājumi. Krāpnieki izmantoja *backdoor* vienā no uzņēmuma datoriem un pieslēdzās uzņēmuma e-pastam. Informācija par krāpniecību nodota policijai.
- Decembrī tika saņemta informācija no vairākām valsts iestādēm un organizācijām par personalizētiem krāpnieciskiem e-pastiem, kas iestādes vadītāja vārdā tika nosūtīti iestādes grāmatvedim un aicināja veikt steidzamu maksājumu 11 985 EUR apmērā uz Lielbritāniju.

Pikšķerēšanas kampaņas

- Gada sākumā 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.
- Aprīlī vairākās valsts un pašvaldību iestādēs masveidā izplatīti e-pasti, kas domāti lietotāju e-pasta piekļuves datu izkrāpšanai. Darbinieki brīdināti.
- 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 sagatavoti konkrētajam saņēmējam.
- Augustā vairāku finanšu institūciju darbinieki savos pasta kontos saņēma krāpnieku sagatavotus e-pastus, kas sūtīti ar mērķi izkrāpt lietotāja datus, ievilnot saņēmēju apmeklēt interneta vietni, kas noformēta līdzīgi leģitīma pasta pakalpojumu sniedzēja vietnei.

- Kādā valsts iestādē vairāki darbinieki saņēma savu kolēģu vārdā nosūtītus e-pastus ar virsrakstu "Latvijas Stabilitātes programma 2016.-2019.gadam", kas izsūtīti no inbox.lv servera. To pielikums saturēja *Microsoft Office* formāta dokumentu ar *Makro* funkciju, kas lejupielādēja un izpildīja datorvīrusu. *Inbox.lv* portālā sūtītāju e-pasta adreses izveidotas tajā pašā dienā no Korejas IP adresēm. Datoru inficēšana iestādē netika konstatēta.
- CERT.LV kopā ar bankām strādāja pie incidentu risināšanas, kuros Latvijas interneta lietotājiem masveidā tika izsūtītas pikšķerēšnas e-pasta vēstules ar aicinājumiem apmeklēt tīmekļa vietni, kas izskatās līdzīgi internetbanku vietnēm. Uzbrukuma mērķis – izkrāpt lietotāju datus. CERT.LV panāca kaitīgo resursu aizvēršanu dažu stundu laikā. Neviena lietotāja konts necieta uzbrukumā. Uzbrukumā tika iesaistīti inficēti serveri.
- Masveidā tika izsūtīti e-pasti it kā *Paypal* tiešsaistes maksājumu sistēmas vārdā, ziņojot par konta bloķēšanu. Lai apstiprinātu savu identitāti un atrisinātu it kā radušās problēmas, upuris tika aicināts apmeklēt uzbrucēju sagatavotu *Paypal* vietnes līdzinieku un veikt pieslēgšanos sistēmai. Ja upuris veica autentifikācijas mēģinājumu, tad lietotājvārds un parole nonāca uzbrucēju rīcībā.
- CERT.LV saņēma informāciju par viltus loteriju, kas tika nesankcionēti rīkota it kā kādas bankas vārdā izlozējot mobilo telefonu, un bija paredzēta bankas lietotāju datu izkrāpšanai. CERT.LV nav informācijas, ka kāds lietotājs būtu šajā incidentā cietis. CERT.LV sazinājās ar vietnes uzturētājiem un kaitīgais saturs no vietnes tika izņemts.

Piekļuves atteices uzbrukumi (DoS un DDoS)

- 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.
- Pret kādu populāru tīmekļa resursu tika 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
- Kāds Latvijas uzņēmums saņēma draudu vēstuli grupējuma *Armada Collective* vārdā. Tika draudēts veikt apjomīgu DDOS uzbrukumu, kas traucēs uzņēmuma darbību, ja uz e-pastā norādītu *Bitcoin* adresi netiks pārskaitīts 1 BTC. CERT.LV informēja uzņēmumu, ka šis ir krāpšanas mēģinājums, *Armada Collective* nekad neveic reālus uzbrukumus, bet izspiež naudu ar tukšiem draudiem. Līdzīgas draudu vēstules vairāki Latvijas uzņēmumi saņēmuši arī iepriekš.
- Pret kāda uzņēmuma datortīklu no 20. līdz 21. novembrim tika veikts apjomīgs DDoS uzbrukums, kurš tika ierobežots, atslēdzot uzņēmuma tīklu no ārzemju interneta. Uzbrukuma organizatori sazinājušies ar uzņēmuma vadību un izteikuši vēlmi iegūt kontroli pār uzņēmuma daļām. Uzņēmums atteicās ar viņiem komunicēt, taču atkārtoti DDoS uzbrukumi uzņēmumam nesekoja.

- DoS uzbrukuma rezultātā tika traucēta kāda portāla darbība. Incidenta analīzes rezultātā tika konstatēts, ka resursu pārslodzi radīja ievainojamību skenera izmantošana no kaitnieciskas IP adreses. CERT.LV ieteica uzlabot portāla aizsardzību, lai šādu skeneru izmantošana no vienas IP adreses neradītu DoS situācijas.

"Banku" vīrusi

- Februārī CERT.LV izmeklēja *Dridex* banku trojāņa izplatīšanas kampaņu, kuras mērķu starpā bija liels skaits valsts iestāžu darbinieku e-pasti. Sekmīgu infekciju skaits bija neliels, neskatoties uz uzbrukuma kampaņas agresivitāti.
- 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.
- Augustā CERT.LV nodeva uzbrukuma indikatorus Latvijas komercbankām, lai informētu par identificētajiem uzbrukumu mēģinājumiem.
- Septembrī IBM incidentu novēršanas vienība publicēja banku vīrusa *Dridex* analīzi, kurā kā vīrusa mērķis tika identificētas arī liela daļa Latvijā strādājošu komercbanku. CERT.LV informēja par apdraudējumu un izplatīja uzbrukuma indikatorus identificētajām komercbankām. CERT.LV veica arī padziļinātu vīrusa analīzi un nekonstatēja nevienu pilnvērtīgi realizētu šīs kampaņas uzbrukumu, kurā Latvijas banku klientiem būtu sagatavoti pārlūku pārtveršanas skripti. To varētu skaidrot kā iespējamu gatavošanos uzbrukumam, kas nav noticis, vai uzbrucēju pieļautu kļūdu, kas netieši norāda uz uzbrucēju saistību ar Latviju.
- Oktobrī tika atklāti pieci .LV domēnus izmantojoši internetveikali, kuru lapās, izmantojot populārajā interneta veikalu platformā *Magento* esošu ievainojamību, kibernoziedznieki bija ievietojuši kaitīgu kodu, kas vāca maksājuma formās ievadītos kredītkaršu datus. CERT.LV izsūtīja brīdinājumus šo resursu īpašniekiem par lapas koda atjaunināšanu. Kibernoziedznieki kopumā bija kompromitējuši vairāk kā 4900 interneta vietņu dažādās valstīs.

Mobilā ļaunatūra

- Janvārī 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.
- 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.

- 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 *ImoIM* (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.
- Kādā operētājsistēmai *Android* paredzētā sociālā tīkla 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.
- Tika 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.
- Mobilās aplikācijas *Watsapp* lietotāju vidū tika izplatīta saite uz viltus loteriju www.faceb00ks.com/laimesrats. Ja lietotājs izvēlējās iesaistīties piedāvātajās aktivitātēs, viņam tika paziņots, ka ir laimēts un nepieciešams ievadīt tālruņa numuru laimesta saņemšanai. Ievadot tālruņa numuru un neizlasot atrunu zem ievades lauka, lietotājs veica reģistrēšanos maksas pakalpojumam.
- Gada otrajā pusē tika saņemta ziņa par jaunatklātu *Android* ļaundabīgo programmatūru, kas zog finanšu informāciju (kredītkaršu numuri u.c.), un bloķē zvanus uz bankas zvanu centriem, tādējādi traucējot īpašniekam laikus bloķēt maksājumu karti. Nākotnē paredzams, ka ar šādas ļaunatūras palīdzību būs iespējama arī zvanu pāradresēšana uz viltotu zvanu centru, kas radītu papildu riskus. Līdz šim par šīs ļaunatūras upuriem Latvijas iedzīvotāji nav kļuvuši, bet jāatceras, ka mobilās iekārtas savas popularitātes dēļ ir kļuvušas par iekārojamu mērķi ļaundariem, tādēļ vieglprātīga rīcība ar savu viedierīci un izmantojamo programmatūru nav pieļaujama.
- Bieži pārskata periodā bija lietotāju saņemti paziņojumi par it kā konstatētām problēmām mobilajā iekārtā, kuru risināšanai lietotājam tiek piedāvāts lejupielādēt kādu mobilo lietotni, kura, ja lejupielādēta no oficiālā *PlayStore*, var aprobežoties tikai ar reklāmu rādīšanu, bet, ielādēta no neoficiālām tīmekļa vietnēm, var nodarīt būtisku kaitējumu iekārtas un datu drošībai.
- Gada beigās tika reģistrēta lietotāju apkrāpšana ar paaugstinātas maksas pakalpojumu starpniecību. Lietotāji saņēma paziņojumus par laimestu loterijā vai ziņojumu par it kā konstatētu infekciju viņu mobilajā iekārtā, un tika aicināti sūtīt īsziņu (SMS), lai pieteiktos laimestam vai lejupielādētu antivīrusu, bet, neiepazīstoties ar pakalpojuma nosacījumiem, veica paaugstinātas maksas pakalpojuma abonēšanu.

Lietu internets (IoT)

- CERT.LV veica ievainojamību novēršanas koordināciju sadarbībā ar Ķīnas nacionālo *CSIRT* vienību *CNCERT*, IP kameru ražotāju *Milesight* un ievainojamību atklājēju Kirilu Solovjovu. CERT.LV uzstāja uz ražotāja atbilstošu reakciju un nepieciešamību iegūt programmatūras labojumus, jo vairāki simti ievainojamu iekārtu tika atklāti kādā valsts iestādē. Tika panākta atklāto ievainojamību novēršana un ražotājs izsniedza programmatūras ielāpus. Šis process prasīja koordinēšanas darbu 8 mēnešu garumā.
- Oktobrī lietu interneta (IoT) robotu tīkls *Mirai* veica masīvu DDoS uzbrukumu DNS pakalpojuma nodrošinātājam *Dyn*. Uzbrukums uz dažām stundām padarīja nepieejamas daudzas *Dyn* klientu vietnes, tādas kā *Twitter*, *Reddit*, *Github*, *Soundcloud*, *Spotify* u.c.

  Tiek lēsts, ka uzbrukumā piedalījās 100,000 inficētas IoT iekārtas. Latvijā tika identificēti vairāki simti iekārtu, kuras varētu būt piedalījušās šāda tipa uzbrukumos. *Mirai* robotu tīkls tika izveidots, pateicoties lielam skaitam nedroši konfigurētu IoT iekārtu, kurās uzbrucēji izmantoja sen zināmas ievainojamības un noklusējuma paroles.

  Eksperti uzskata, ka nākotnes DDoS uzbrukumi varētu sasniegt 10 Tb/s, kas ir pietiekami, lai spētu padarīt internetu nepieejamu kādā no valstīm.

Sociālie tīkli

- Tika reģistrēts ziņojums no kāda sociālā tīkla lietotāja, kurš saņēmis draudu vēstuli, ka tiks publicētas privātas fotogrāfijas, ja netiks samaksāta izpirkuma maksa. Izpirkums ticis samaksāts, bet bilžu publiskošanu tas nav kavējis, papildus pieprasot vēl naudu, lai to pārtrauktu. Cietušajam CERT.LV ieteica vērsties policijā.
- 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.
- Oktobra sākumā vairāki *Facebook* lietotāji no Latvijas kļuva par kaitīgās programmas *Slinky* upuri. Tā masveidā izplatījās, lietotājiem neapdomīgi instalējot aplikāciju, kas uzdeva sevi par profila statistikas attēlošanas rīku. Kaitīgā programma veica dažāda satura ierakstus lietotāju vārdā un nākotnē varētu tikt izmantota arī ļaunatūras izplatīšanai.
- Kāds lietotājs, atsaucoties uz *Facebook* pamanītu reklāmu, samaksāja vairāk kā 100 EUR viltotā e-veikalā www.canadagoosemallhut.com. Veikals no kredītkartes noņēma ne tikai summu par nepiegādāto preci, bet arī vairāk kā 15EUR dažādas papildu „komisijas" maksas. Krāpnieciskā vietne tika slēgta. Apkrāptajam pircējam CERT.LV ieteica sazināties ar savas kredītkartes izdevējbanku, lai risinātu naudas atgūšanas jautājumus.
- Kādas tīmekļa vietnes uzturētāji savā *Facebook* kontā saņēma vēstuli, kurā pieprasīti 400 USD un draudēts dzēst viņu mājas lapu, ja nauda netiks samaksāta. Uzbrucējs, nesaņemot prasīto summu, lapu tiešām izdzēsa. Lapa tika atjaunota no rezerves kopijām un uzlabota to uzturošā servera drošība. Dati par šo izspiešanas mēģinājumu nodoti policijai.

3. Sadarbības un komunikācijas pasākumi

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

27. aprīlī CERT.LV pārstāvis piedalījās Digitālās drošības alianses 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.

4. oktobrī CERT.LV pārstāvis piedalījās Digitālās drošības alianses rīkotajā preses konferencē, ar kuru tika uzsākta kampaņa "Mirklis pirms klik", kas tika vērsta uz uzņēmējiem ar mērķi veicināt darbinieku izglītošanu par digitālās drošības jautājumiem.

26. oktobrī Eiropas Kiberdrošības mēneša ietvaros CERT.LV organizēja "Mediju brokastis", kurās mediju pārstāvji tika informēti par Kiberdrošības mēneša norisi un IT drošības aktualitātēm Latvijā.

Gada laikā stabili pieaug sekotāju skaits populārajās sociālo tīklu platformās *Twitter* un *Facebook*.
Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1615.
CERT.LV *Facebook* profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 473.

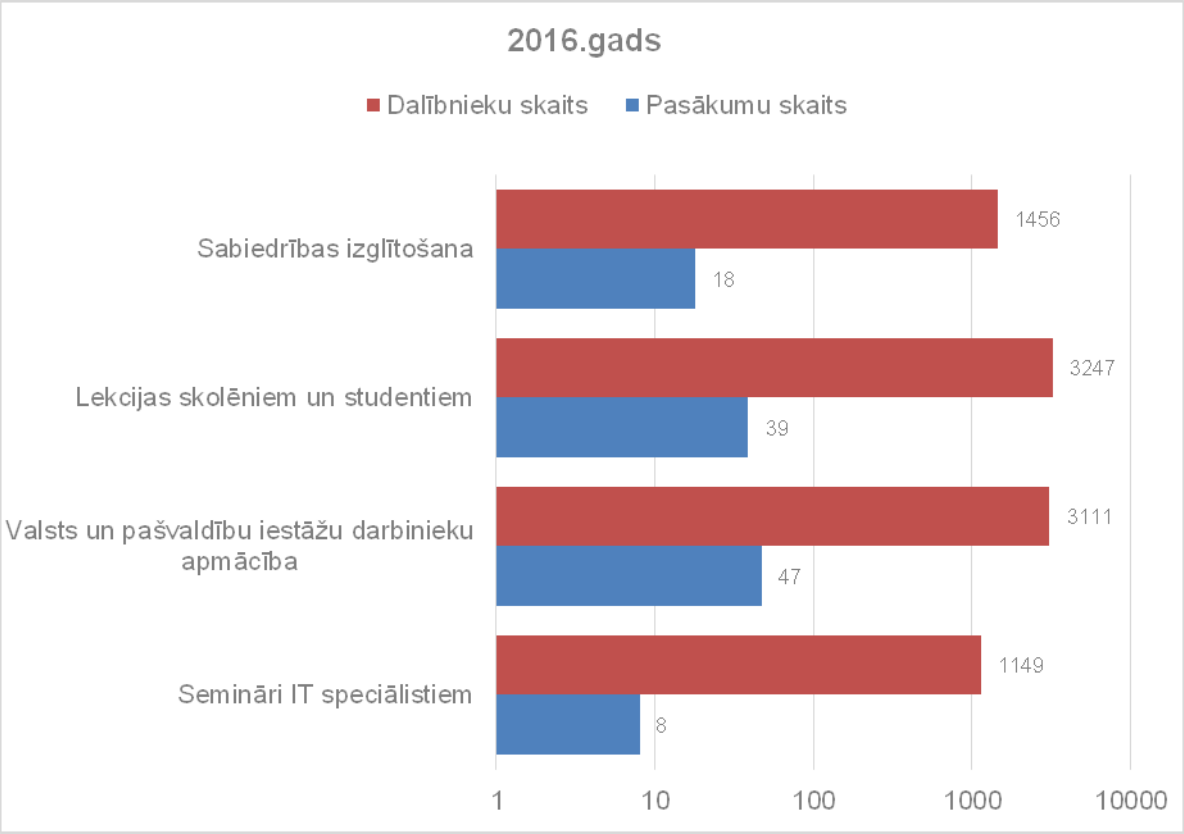
Pārskata periodā CERT.LV sadarbībā ar Latvijas Alternatīvo finanšu pakalpojumu asociāciju izveidoja interaktīvu digitālo testu "Cik grūts medījums Tu esi krāpniekiem?". Tajā ikviens varēja novērtēt savu prasmju un zināšanu līmeni par personīgo datu drošību, kā arī iegūt noderīgus ieteikumus.

CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. Kopā CERT.LV lapai bijuši 60,837 unikāli apmeklējumi jeb sesijas.

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

4. Izglītojošie pasākumi

2016. gadā CERT.LV turpināja rīkot izglītojošus pasākumus par drošības jautājumiem IT drošības speciālistiem, valsts un pašvaldību iestāžu darbiniekiem, studentiem, skolēniem un citiem interesentiem. Pārskata periodā CERT.LV piedalījās 112 pasākumos un izglītoja 8963 klausītājus.



4.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2016. gadā.

Gada lielākais pasākums bija ikgadējā IT drošības konference „Kiberšahs 2016", kas notika 6. oktobrī Rīgas Latviešu biedrības namā. Konferenci klātienē apmeklēja gandrīz 600, bet pieteicās vairāk nekā 700 dalībnieki, savukārt tiešsaistē tai bija 2000 unikālu skatījumu.

Nozīmīgākās tēmas bija izspiedējvīrusu draudi, mobilo iekārtu drošība, tīkla drošība, privātums digitālajā vidē, personas datu aizsardzības aspekti un kvantu datoru ietekmi uz kiberdrošību.

Konference tika organizēta sadarbībā ar *ISACA Latvijas nodaļu*. Pasākumu atbalstīja *SIA DEAC* un *SIA Latvijas Mobilais Telefons*.

CERT.LV organizētie pasākumi IT drošības speciālistiem

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.

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.

07.septembrī CERT.LV uzsāka lekciju kursu IT drošības speciālistiem “Kibernoziedznieku vēsture”. Lekcijas tika ierakstītas un videomateriāls pieejams tīmekļa vietnē esidross.lv.

8. decembrī CERT.LV sadarbībā ar Aizsardzības ministriju organizēja kiberdrošības mācības "Kiberdzirnas 2016", kurās piedalījās valsts un pašvaldību iestāžu vadītāji un par informācijas tehnoloģiju drošību atbildīgie darbinieki no 23 institūcijām. Mācību mērķis bija veicināt institūciju vadītāju izpratni par kiberdrošības incidentiem, to iespējamām sekām, kā arī nepieciešamo rīcību kiberdrošības incidentu novēršanai.

13. decembrī CERT.LV organizēja semināru IT drošības speciālistiem “Esi drošs”. Seminārs tika veltīts atvērto datu drošībai, elektroniskās identifikācijas uzraudzības komitejai, aizdomīgu darbību identifikācijai informācijas sistēmās un atbildīgai ievainojamību atklāšanai.

CERT.LV prezentācijas par IT drošību

10. un 11. martā CERT.LV pārstāvji sniedza prezentācijas par IT drošību *VARAM* rīkotajā seminārā “e-Iespējas pašvaldībās”. Seminārs notika E-prasmju nedēļas ietvaros.

27. oktobrī CERT.LV pārstāvji uzstājās ar prezentācijām "IoT security driven by hacker & cybercrime community" un "Responsible disclosure process – Latvian approach" konferencē “DSS ITSEC 2016”.

Sabiedrības izglītošana

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 bija neliels CERT.LV pētījums par IoT iekārtām Latvijas internetā.

9. martā E-prasmju nedēļas ietvaros un 19. oktobrī Eiropas Kiberdrošības mēneša 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. Datorologa akciju 2016. gadā apmeklēja 109 interesenti. Kā Datorologi akcijā iesaistījās arī IT drošības eksperti no *SIA Latnet Serviss/Stream Networks* un *SIA Lattelecom*. *SIA Lattelecom* ir saņēmuši arī kvalitātes zīmi “Atbildīgs interneta pakalpojumu sniedzējs”.

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

24. novembrī CERT.LV pārstāvis piedalījās videomateriāla filmēšanā “*Amigo* iniciatīvas laimīgām ģimenēm" video cikla "Kā būt par vecāku 21.gadsimtā?" ietvaros, stāstot par drošu informācijas un komunikāciju tehnoloģiju lietošanu.

5. Sadarbība ar valsts iestādēm

CERT.LV 2016. gadā piedalījās dažādu darba grupu darbā, likumprojektu izstrādē un sniedza konsultācijas IT drošības jautājumos dažādām valsts iestādēm.

Sadarbība ar Aizsardzības ministriju

Regulāri notika tikšanās ar ministrijas Valsts sekretāru un komunikācija ar Nacionālās kiberdrošības politikas koordinācijas nodaļu.
CERT.LV turpināja darboties Aizsardzības ministrijas darba grupā par atbildīgas ievainojamību atklāšanas politikas ieviešanu.

Citi sadarbības partneri

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

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

Tika sniegtas konsultācijas valsts un pašvaldību iestādēm par MK noteikumu nr. 442 ieviešanu.

Pārskata periodā tika veiktas drošības pārbaudes 119 valsts un pašvaldību tīmekļa vietnēs. Būtiskas ievainojamības tika atklātas 20 valsts un pašvaldību resursos. CERT.LV informēja par ievainojamībām vietņu uzturētājus un koordinēja ievainojamību novēršanu.

6. Starptautiskā sadarbība

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

Augustā tika parakstīti sadarbības līgumi ar starptautiskiem IT drošības veicināšanas projektiem *CyberGreen* un STOP.THINK.CONNECT.

Sadarbība ar CERT kopienu

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

Maijā CERT.LV Rīgā organizēja 48. *TF-CSIRT* sanāksmi, kurā piedalījās gandrīz 100 pārstāvji no dažādām Eiropas CERTu komandām.

No 19. līdz 22. septembrim Cīrihē notika *TF-CSIRT* sanāksme, kurā CERT.LV vadītāja Baiba Kaškina atkārtoti tika ievēlēta par *TF-CSIRT* grupas priekšsēdētāju. Šajā sanāksmē tika arī oficiāli paziņots par CERT.LV sertifikāciju *Trusted Introducer* servisā un izsniegts apliecinājums. CERT.LV sertificēta no 2016. gada 1. septembra uz trīs gadiem.

Sadarbība ar ENISA

Daudzveidīga sadarbība notika ar Eiropas Tīkla un informācijas drošības aģentūru, piemēram, rīkojot seminārus un mācību kursus

10. maijā Rīgā notika CERT.LV un *ENISA* organizētais NIS direktīvas *CSIRT* tīkla veidošanas otrā neformālā sanāksme, kuras laikā norisinājās diskusijas darba grupās par *CSIRT* tīkla darbības principiem. Sanāksmē piedalījās vairāk nekā 50 pārstāvji no gandrīz visām ES dalībvalstīm.

10. maijā CERT.LV organizēja un piedalījās arī *ENISA* sanāksmē "Incident handling and taxonomies" Rīgā.

No 10. līdz 11. maijam CERT.LV organizēja un piedalījās "ENISA's 11th annual workshop - CSIRTs in Europe" Rīgā.

3. jūnijā CERT.LV piedalījās *ENISA* mācībās par Eiropas līmeņa krīžu novēršanas standarta procedūru īstenošanu.

No 13. līdz 14. oktobrim notika *ENISA* organizētājās kiberdrošības mācībās ”Cyber Europe 2016”. Latvijas pusē tās koordinēja CERT.LV. Mācību norise vērtējama kā veiksmīga, iespējami uzlabojumi sadarbībā starp valsts un privāto sektoru.

Sadarbība ar NATO CCDCoE

CERT.LV pārstāvji sadarbojās ar *NATO Cooperative Cyber Defence Centre of Exelence*.
Nozīmīgākais pasākums bija starptautiskās kiberdrošības mācības “Locked Shields 2016”, kuras notika no 18. līdz 23. aprīlim. Šajās mācībās CERT.LV pārstāvji piedalījās 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.

No 1. līdz 4. jūnijam CERT.LV pārstāvji piedalījās *CCDCoE* organizētajā *CyCON* konferencē Tallinā, Igaunijā.

Tāpat tika papildinātas zināšanas un prasmes *NATO CCDCoE* rīkotajos mācību kursos par IT drošības tēmām.

Starptautiskie pasākumi

2016. gadā CERT.LV pārstāvji piedalījās starptautiska līmeņa pasākumos, lai veicinātu sadarbību un apgūtu jaunas zināšanas un prasmes.

Nozīmīgākie pasākumi:

- *Microsoft Digital Crimes Consortium* konferencē Vīnē;
- *GFCE* (*Global Forum of Cyber Expertise*) rīkotā *RDP* (*Responsible Disclosure Policy*) darba grupas sēde Budapeštā;
- “BlackHat” konference Singapūrā;
- "8th Baltic Cyber Security Coordination Meeting" Tallinā;
- Nīderlandes CERT konference “One conference” un NIS direktīvas CSIRT tīkla pirmā neoficiālajā veidošanas sanāksmē Hāgā;
- CERT-EE simpozijs Tallinā, kur vingrinājumā “Iegūsti karogu” (Capture the Flag) CERT.LV

pārstāvis izcīnīja pirmo vietu;
- "The Networking Conference 2017" (agrāk TERENAs konference) programkomitejas darbi un sanāksmes Amsterdamā;
- IT drošības ekspertu sanāksme "4GH" Nīderlandē;
- "ITU-ENISA Regional Cybersecurity Forum" Sofijā.

Starptautiskās kiberdrošības mācības

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

No 13. līdz 14. oktobrim notika *ENISA* organizētājās kiberdrošības mācībās "Cyber Europe 2016". Latvijas pusē tās koordinēja CERT.LV. Mācību norise vērtējama kā veiksmīga, iespējami uzlabojumi sadarbībā starp valsts un privāto sektoru.

No 28. novembra līdz 3. decembrim CERT.LV sadarbībā ar *MilCERT* un *Kiberaizsardzības vienību* piedalījās *NATO* kiberdrošības mācībās "Cyber Coalition 2016".

Plašāka informācija par CERT.LV uzdevumu izpildi pieejama CERT.LV mājaslapā:
https://cert.lv/lv/2017/02/cert-lv-darbibas-parskats-par-2016-gada-4-ceturksni

Atskaiti sagatavoja:
CERT.LV Sabiedrisko attiecību projektu vadītāja Līga Besere, tālrunis 67085888,
e-pasts liga.besere@cert.lv

2017. gada 21. februārī