Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2015

2015. gada 1. ceturksnis (01.01.2015. – 31.03.2015.)

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

Janvāris sākās ar Latvijas prezidentūras Eiropas Savienības Padomē aktivitātēm. Tā kā kiberdrošība ir viena no Prezidentūras dienaskārtības tēmām, mediju pārstāvji izrādīja pastiprinātu interesi par kibertelpā notiekošo, mēģinot sasaistīt dažādus ārpolitikas notikumus ar kiberdraudu iespējām. CERT.LV reģistrētie drošības incidenti pārskata periodā, saistībā ar Prezidentūras aktivitātēm, uzrādīja vairākus apjomīgus DDoS uzbrukumus, kas tika vērsti pret valsts iestādēm.
Prezidentūras ietvaros CERT.LV pārstāvji iesaistījās dažādos ar kiberdrošības tēmām saistītos pasākumos, sniedzot prezentācijas un piedaloties diskusijās.

Pārskata periodā vērienīgākais drošības incidents bija „CTB Locker" vīrusa izsūtīšanas kampaņa. Uzbrukumu mērķis bija inficēt datorus ar vīrusu, kurš sašifrē datorā esošos failus, prasot izpirkuma maksu. Vīruss tika izsūtīts vairākās kampaņās ar mēstuļu palīdzību. CERT.LV aicināja interneta lietotājus rūpīgi izvērtēt e-pasta saturu un to pielikumus, lai nekļūtu par krāpnieku upuriem.

No 5.-6.martam CERT.LV un Zemessardzes Kiberaizsardzības vienība organizēja tehniskās mācības „Marta migla" ar mērķi pārbaudīt dalībnieku prasmes IT infrastruktūras aizsardzībā, IT drošības uzbrukumu atklāšanā un novēršanā. Mācībās piedalījās 59 dalībnieki.

No 23. līdz 27. martam Eiropā norisinājās „E-prasmju nedēļa". CERT.LV iesaistījās kampaņas pasākumos. 25.martā iedzīvotājiem bija iespēja veikt bezmaksas datora pārbaudi ikgadējās „Datorologa akcijas" ietvaros. 27. martā CERT.LV vadīja prezentāciju par IT drošību pašvaldību iestāžu darbiniekiem Ogrē.

2015.gada 1.ceturksnī CERT.LV reģistrēja un apstrādāja 868 augstas prioritātes incidentus un 171 441 zemas prioritātes incidentu.

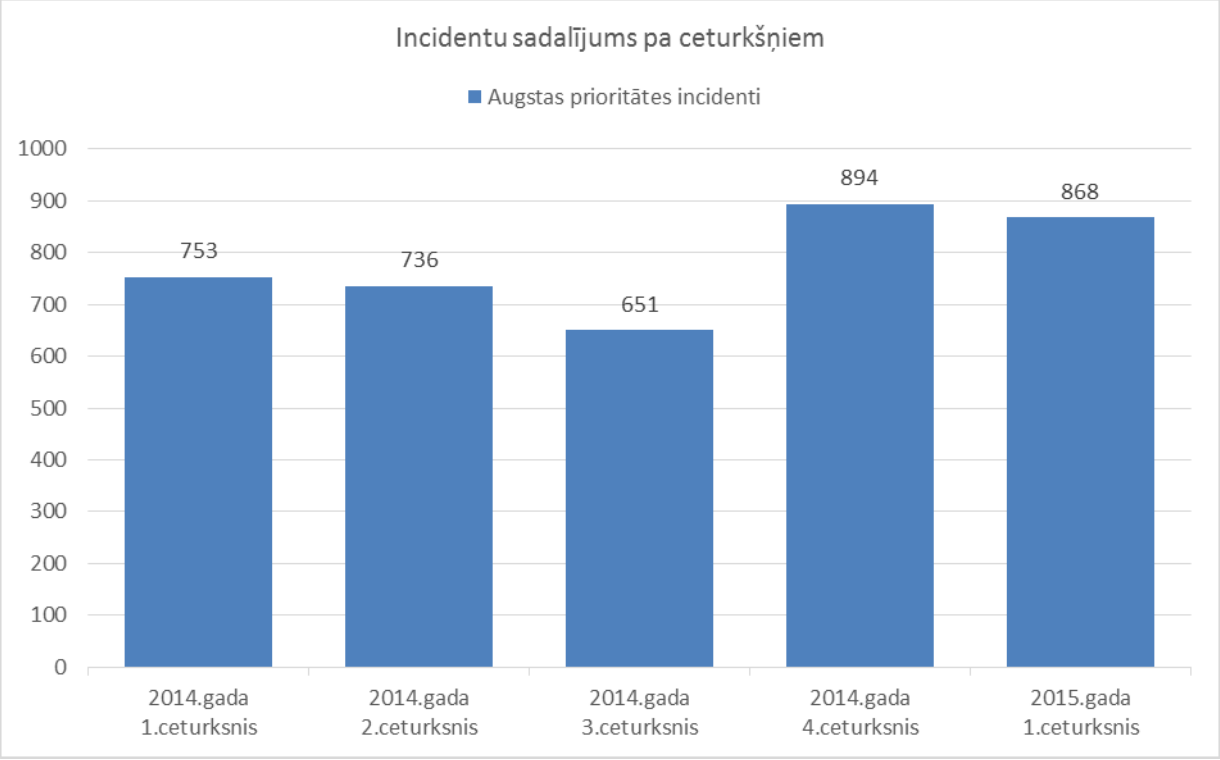
Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās „CTB Locker" vīrusa masveida izsūtīšanas kampaņas.

Kopā pārskata periodā CERT.LV piedalījās 28 pasākumos, apmācot 1933 cilvēkus, ievietoja 26 jaunas ziņas portālā www.cert.lv, piedalījās 5 radio pārraidēs un 9 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

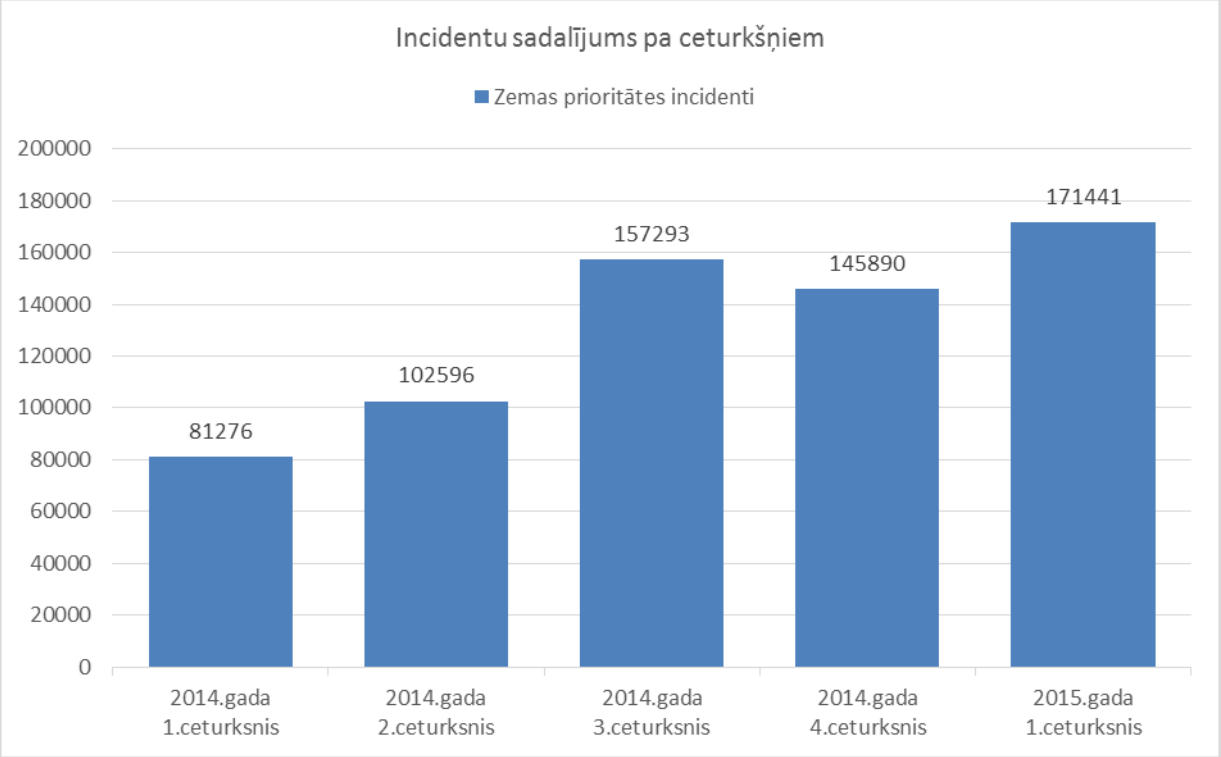
CERT.LV ik mēnesi apkopo informāciju par notikušajiem incidentiem, iedalot incidentus augstas prioritātes (visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas vai ko ir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

2015.gada 1.ceturksnī CERT.LV apstrādāja 868 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 894 augstas prioritātes incidenti, bet 2014.gada 1.ceturksnī 753 augstas prioritātes incidenti.

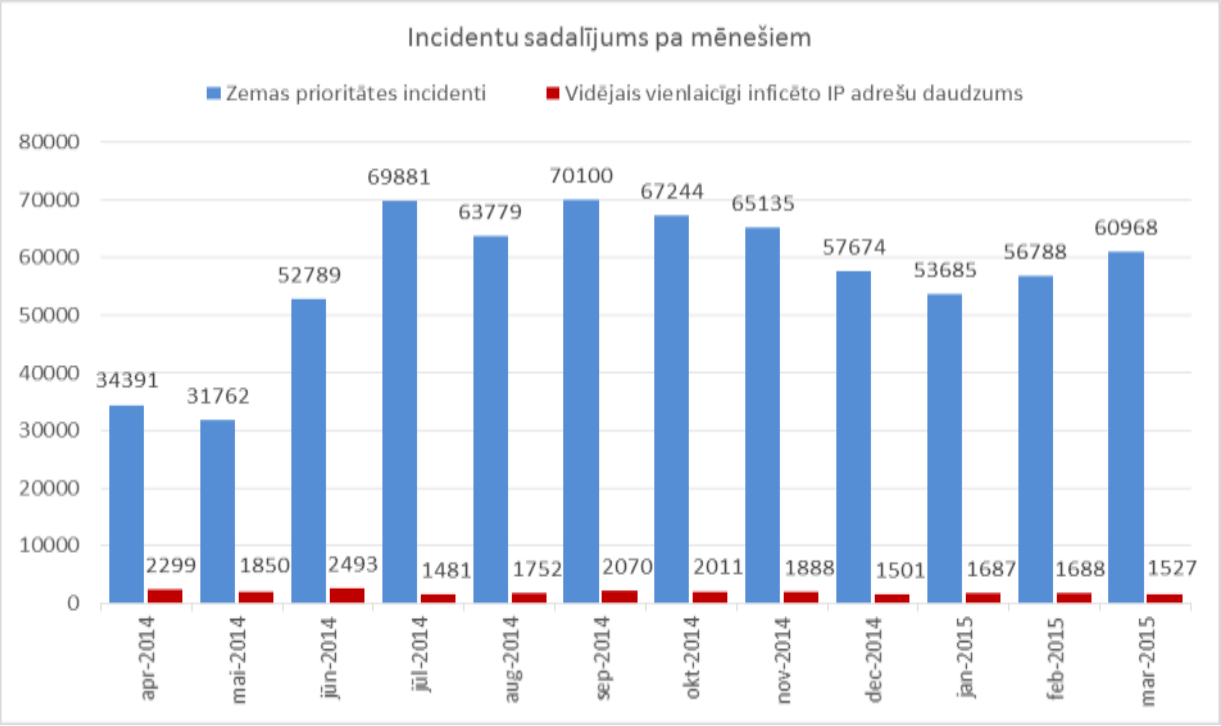


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2014. un 2015. gadā.

2015.gada 1.ceturksnī CERT.LV reģistrēja 171 441 zemas prioritātes incidentu. Iepriekšējā ceturksnī tika reģistrēti 145 890 zemas prioritātes incidenti, bet 2014.gada 1.ceturksnī – 81276 zemas prioritātes incidenti.



2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2014. un 2015.gadā.



3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem.

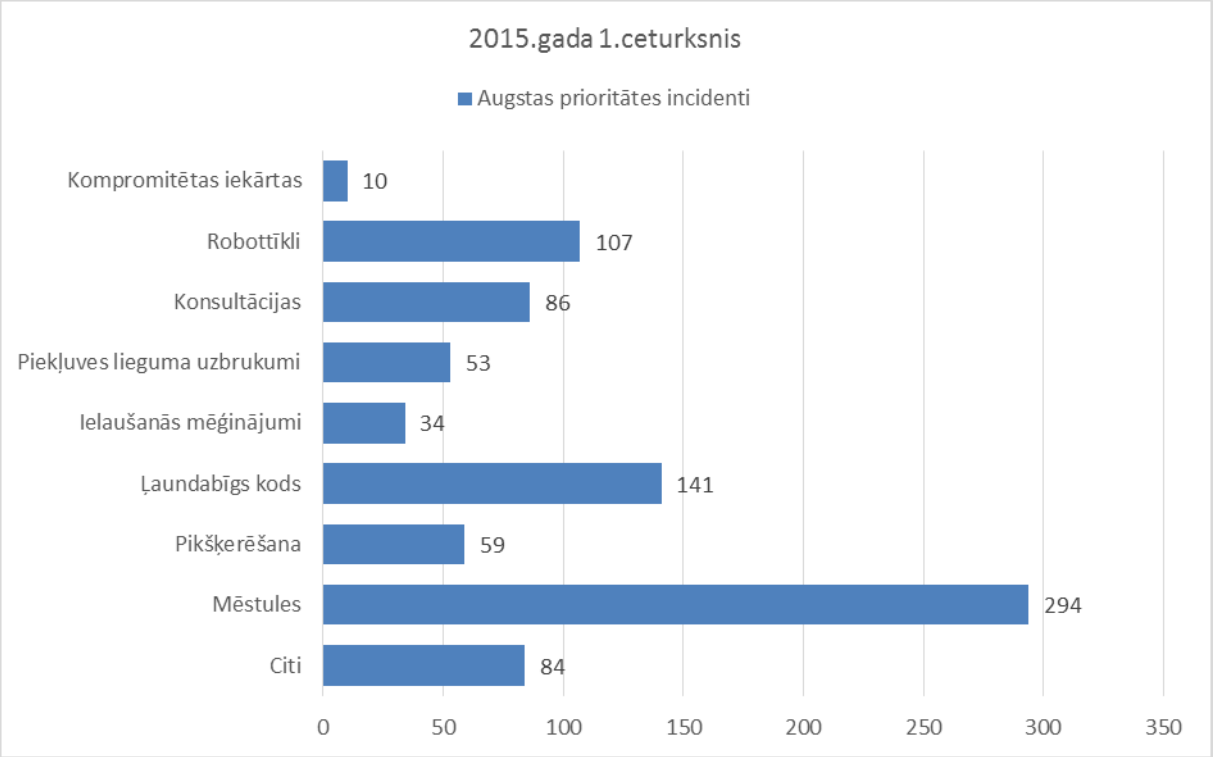
Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Janvārī šis skaits bija 1687, februārī – 1688, savukārt martā – 1527 inficētas IP adreses.

Lai samazinātu kopējo inficēto 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". Pārskata perioda beigās atbildīgo IPS kopskaits saglabājās bez izmaiņām – 13.

Turpinot sadarbību iniciatīvas ietvaros, CERT.LV organizētajā „Datorologa akcijā" 23.martā piedalījās pārstāvji no SIA „Lattelecom" un SIA „Stream Networks".
Uzņēmumu pārstāvji līdzās CERT.LV IT drošības speciālistiem konsultēja iedzīvotājus par datora drošas izmantošanas principiem, pārbaudīja inficētos datorus, izmantojot pretvīrusu programmatūru, un veica citus pasākumus, lai novērstu problēmas, ar kurām lietotāji bija saskārušies.

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

Pārskata periodā CERT.LV reģistrēja un apstrādāja 868 augstas prioritātes incidentus.



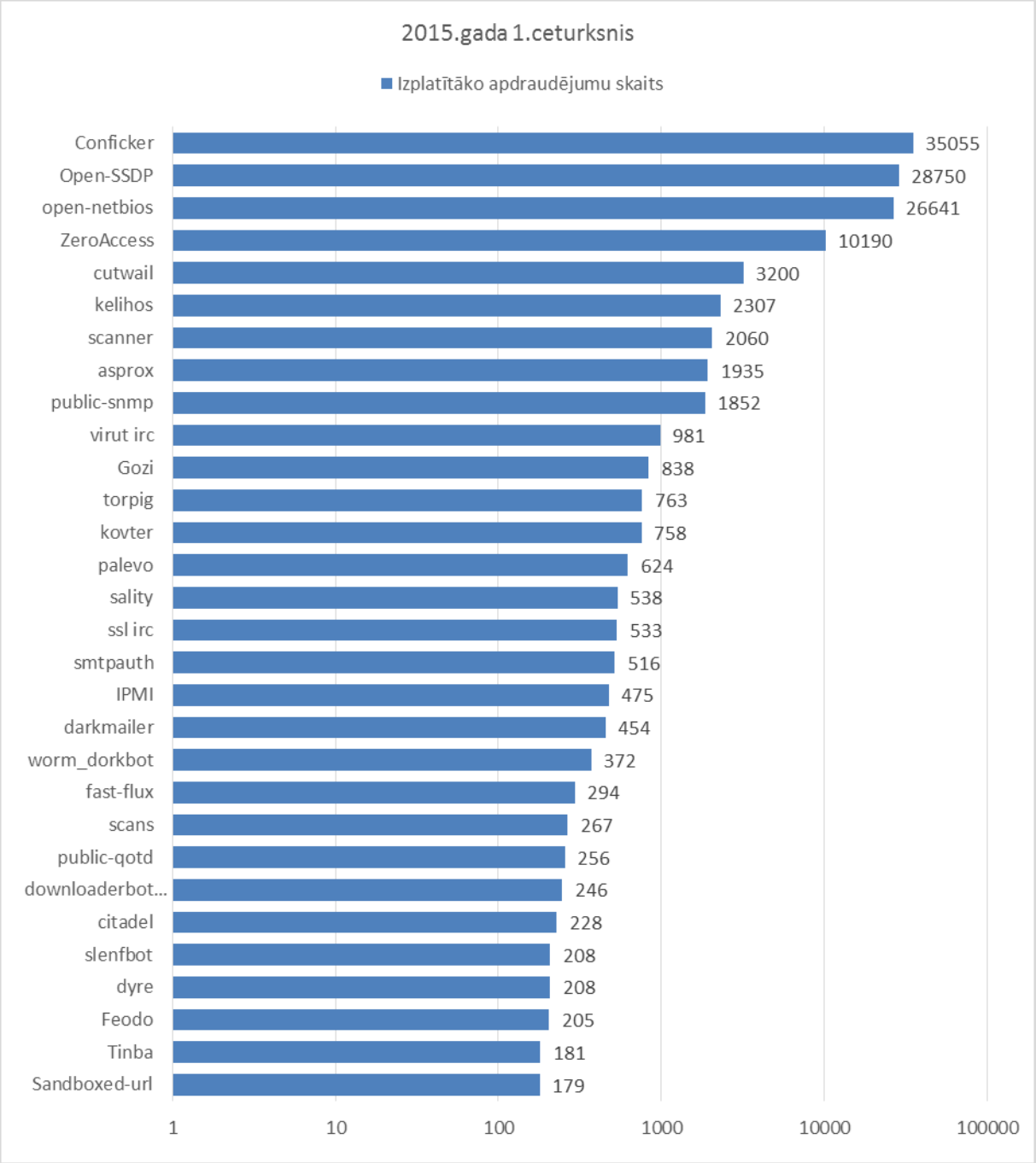
4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2015.gada 1.ceturksnī.

Mēstuļu skaits, salīdzinot ar iepriekšējo periodu, ir saglabājies nemainīgi augstā līmenī (iepriekšējā ceturksnī tika reģistrēti 284 ar mēstulēm saistīti incidenti).

Liels incidentu pieaugums vērojams kategorijā „ļaundabīgs kods" (iepriekšējā ceturksnī reģistrēti 57 incidenti). Tas saistīts ar vērienīgajām „CTB Locker" vīrusa izplatīšanas aktivitātēm.

Pieaudzis arī piekļuves lieguma jeb DDoS uzbrukumu skaits (iepriekšējā ceturksnī reģistrēti 25 incidenti), iespējams, saistībā ar Prezidentūras aktivitātēm.

Pārskata periodā CERT.LV reģistrēja 171 441 zemas prioritātes incidentu. Izplatītāko apdraudējumu veidi joprojām ir nedroši konfigurētas tīkla iekārtas un inficēti datori ar neatjauninātu programmatūru.



5.attēls - CERT.LV reģistrētie zemas prioritātes incidenti no 2015.gada 1.janvāra līdz 31.martam pa apdraudējumu veidiem.

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.

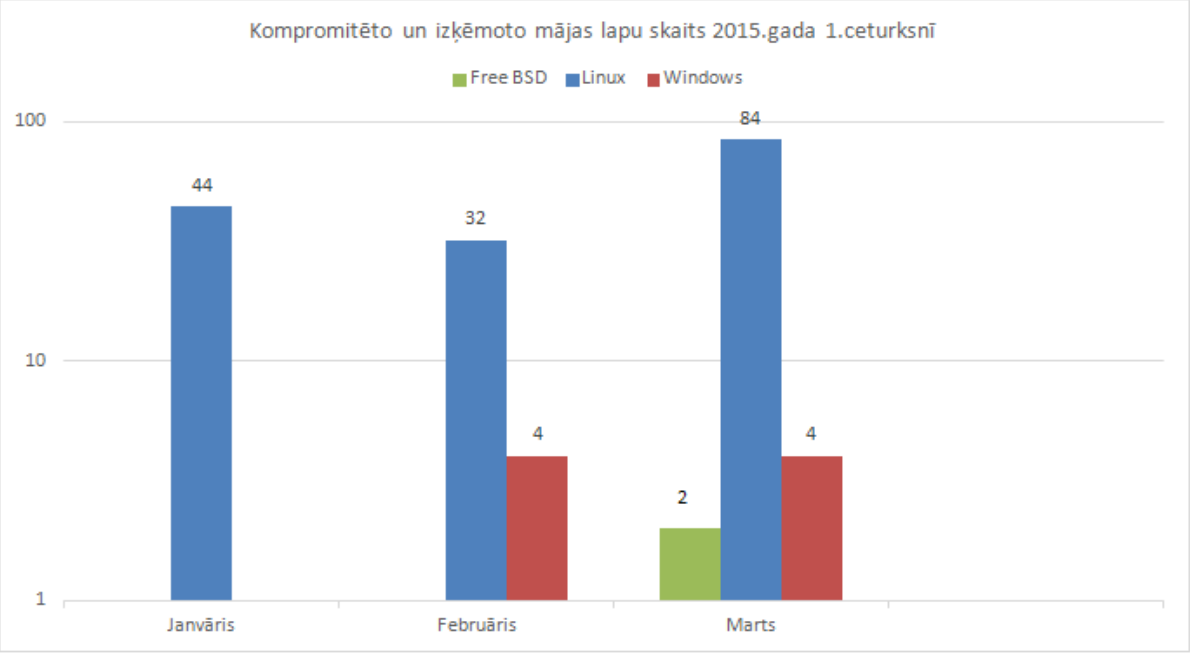
Neskatoties uz CERT.LV aktivitātēm, Latvijā joprojām ir salīdzinoši lieli „Conficker" vīrusa infekcijas rādītāji - vairāk kā 35000 inficētu IP adrešu, turklāt reāli skarto iekārtu skaits varētu būt pat lielāks. Statistika liecina, ka lielākā daļa ar šo vīrusu inficētie datori lieto novecojušu Microsoft Windows XP operētājsistēmu, turklāt netiek lietota arī pretvīrusu programmatūra. Satraucoši tas ir tādēļ, ka, kaut arī šis vīruss uzskatāms par novecojušu (zināms jau no 2008.g) un nu jau ir salīdzinoši nekaitīgs, kā arī no tā var diezgan vienkārši atbrīvoties, inficēto datoru īpašnieki nepūlas to darīt, padarot savu datoru par vīrusu perēkli un apdraudējumu citiem datorlietotājiem. Statistika – trīsdesmit pieci tūkstoši – norāda lietotāju daudzumu, kas izturas bezatbildīgi pret savu un līdzcilvēku drošību internetā.

Nākamais rādītājs, kas liecina, ka sabiedrības uzmanība vairāk jāpievērš savas drošības apzināšanai IT vidē, ir lielais nedroši konfigurēto ierīču skaits, kas statistikā atzīmēts kā open-ssdp un open-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

Latvijā joprojām ir daudz kompromitētu tīmekļa serveru, kurus izmanto ļaunatūras izplatīšanai. Tāpat joprojām pastāv liels skaits mājaslapu, kuras tiek kompromitētas atkārtoti, kas nozīmē, ka drošības uzturētāji nepievērš pietiekamu uzmanību atjauninājumu instalēšanai satura vadības sistēmās.

CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus. Šādu gadījumu skaits:



6.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2015.gada 1.ceturksnī.

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

Janvārī notika apjomīgi „CTB Locker" datorvīrusa izplatīšanas uzbrukumi. Kampaņai bija ļoti labs tehniskās sagatavotības līmenis – ticamas e-pasta adreses, ticami teksti. Lai uzbrukumu realizētu sekmīgāk, tika iegūtas arī reālas grāmatvežu e-pasta adreses, uz kurām mērķtiecīgi tika nosūtīti vīrusu saturoši e-pasti. No uzbrukumiem cieta gan privātpersonas, gan uzņēmēji, gan valsts un pašvaldību iestādes.

Pret vairākām valsts iestādēm tika vērsti apjomīgi DDoS uzbrukumi. Viens no tiem tika vērsts pret tieslietu sektoru. CERT.LV sadarbībā ar interneta pakalpojumu sniedzēju veica incidentu tehnisko analīzi un ietekmes mazināšanas pasākumus.

Svarīgākie pārskata periodā risinātie incidenti un to novēršana:

- 05.01. Tika identificētas infekcijas kādas ministrijas tīklā. Atbildīgās personas tika informētas, veica situācijas apzināšanu un risināšanu.
- 05.01. Parādījās pirmie vīrusa „CTB Locker" izplatīšanas gadījumi Latvijā. CERT.LV saņēma informāciju par izspiedējvīrusa upuri kādas pašvaldības datortīklā. Rezultātā notika datu zudums vienā datorā.
- 07.01. Latvijā tika identificēts ZeuS robotu tīkla kontrolserveris. Tas bija izveidots uz uzlauzta tīmekļa servera, kas uzturēja kādu novecojušu Wordpres tīmekļa vietni. CERT.LV atklāja, ka upuru skaits, kuru kontrolē serveris, ir 32, taču neviens no tiem neatradās Latvijā. Tika informētas attiecīgo valstu CERT vienības. Robotu tīkla kontrolcentrs sadarbībā ar Valsts policiju tika likvidēts.
- 07.01. Tika identificēta kaitīgu kodu saturoša mājas lapa .lv domēnu zonā. Identificētais resurss bija kompromitēts un tika izmantots ļaunatūras izplatīšanai. CERT.LV sazinājās ar resursa turētāju un sniedza konsultāciju situācijas risināšanai.
- 07.01. Atsākās mēstuļu izplatīšana Gmail kontu piekļuves datu izkrāpšanai. Krāpnieciskā forma tika izvietota uzlauztās lapās ar Wordpress CMS. Tika brīdināti serveru īpašnieki.
- 07.01. Izmantojot viltotu portāla tvnet.lv lapu, notika mēģinājums izkrāpt kredītkaršu lietotāju datus. Pikšķerēšanas lapa tika slēgta.
- 08.01. Pēc atkārtota drošības audita CERT.LV atklāja vairākas joprojām nesalabotas ievainojamības kādas valsts iestādes mājaslapā. Izstrādātājs atklātos trūkumus novērsa dažu dienu laikā.
- 08.01. Latvijā esošā serverī tika izvietots ZeuS saimes botneta komand un kontroles centrs. CERT.LV brīdināja lapas īpašniekus, serveris tika salabots. Tika uzsākta incidenta datu analīze.
- 12.01. Kompānijas DHL vārdā tika mēģināts izkrāpt kredītkaršu datus, izmantojot domēnu dhllv.lv. Domēns tika slēgts, jo reģistrēts, izmantojot nepatiesus īpašnieka datus.

- 19.01. Masveidā tika izplatītas e-pasta vēstules, kas noformētas kā automatizēta faksa sūtījumi. Pielikumi bija inficēti ar „CTB Locker" datorvīrusu.
- 20.01. Ar lielu vērienu Latvijā un citās ES valstīs sāka izplatīt „CTB Locker" vīrusu. Noziedzīgie grupējumi kampaņu izvērsa vairākos piegājienos. Izplatība notika galvenokārt caur e-pasta vēstulēm, kas noformētas pareizā latviešu valodā, izliekoties par parādu piedzinējiem vai valsts iestādēm. Pielikumā bija arhīvs, kurš saturēja izpildāmo failu ar paplašinājumu .scr vai .exe. Atverot pielikumu un izpildot kaitīgo programmu, datorā esošie faili tika šifrēti un upurim tika pieprasīta samaksa 2 bitcoin (~ 600 EUR) par sašifrēto datu atgūšanu. Atgūt sašifrētos datus no inficētas mašīnas nemaksājot ir ļoti sarežģīti, vai pat neiespējami.

  Vīrusa ekrānšāviņš:

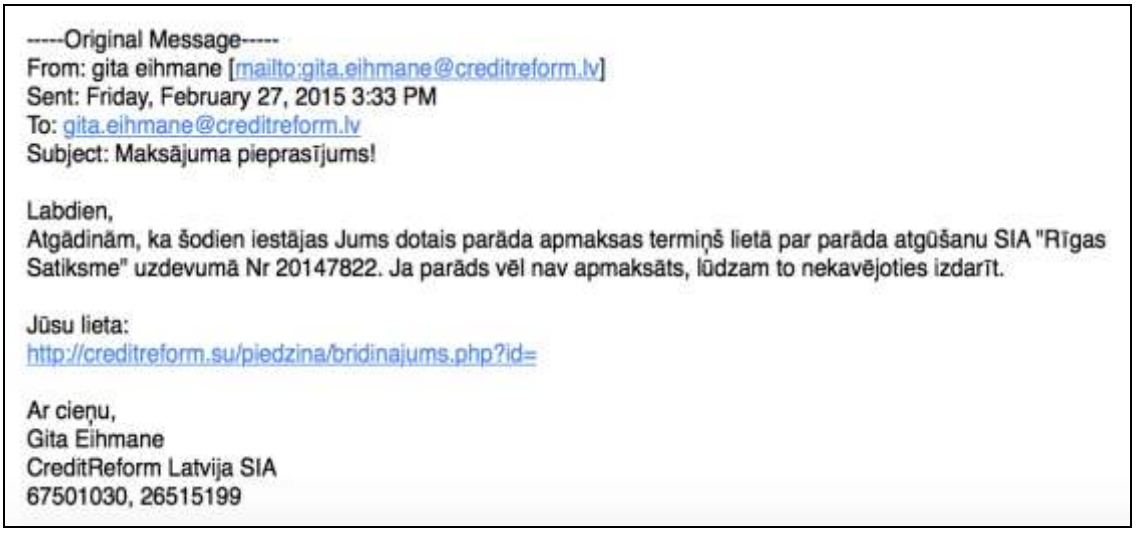
Incidenta risināšanas ietvaros CERT.LV veica vairāku kontrolcentru bloķēšanu, tika ieviesti mēstuļu atpazīšanas mehānismi un notika aktīva informācijas apmaiņa ar sadarbības partneriem Eiropā. Vairākas valsts iestādes būtiski cieta no vīrusa radītajām sekām, zaudējot datus. CERT.LV norādīja uz nepilnībām, kas šīm iestādēm jānovērš, lai situācija neatkārtotos un apdraudējuma ietekme būtu mazināta. Līdzīgas „CTB Locker" datorvīrusa izplatīšanas kampaņas notika visā pasaulē.

- 26.01. CERT.LV veica kāda ZeuS kontrolcentra analīzi, rezultāti tika nodoti Valsts Policijai.
- 27.01. Masveidā tika izsūtīti e-pasti, noformēti kā viltus rēķini, kas saturēja saites uz „CTB Locker" datorvīrusu.
- 27.01. Atklājās, ka „CTB Locker" izspiedējvīrusa izplatīšanā piedalās Latvijā zināmas programmatūras izstrādes kompānijas serveris. Konstatēts, ka attiecīgais serveris ticis

kompromitēts un uzbrucēji to izmantoja vīrusa izplatīšanai, izsūtot mēstules. Uzbrukuma vektors serverim bija novecojusi satura vadības sistēmas versija. Kompānija veica profilakses darbus, lai novērstu radīto kaitējumu un turpmāk nepieļautu šādas situācijas.

- 27.01. Pret tieslietu sektoru tika vērsts apjomīgs DDoS uzbrukums, kura ietekmē tika būtiski traucēta sektora institūciju un tīmekļa vietņu darbība. CERT.LV veica incidenta tehnisko analīzi, kuras rezultātā izdevās noskaidrot arī patieso uzbrukuma avotu neskatoties uz to, ka tas tika slēpts ar tehnoloģiskām metodēm.
- 27.01. Tika publiski izziņota kritiska ievainojamība LINUX glibc / eglibc bibliotēkā. Šī ievainojamība ietekmēja lielāko daļu Linux sistēmu, taču bija salīdzinoši vienkārši labojama, ieviešot atjauninājumus. CERT.LV aicināja uzstādīt ielāpus apdraudētajām sistēmām.
- 02.02. CERT.LV veica incidenta izmeklēšanas analīzes datu apkopojumu par uzbrukumu kādas valsts iestādes tīmekļa vietnei janvāra sākumā. Uzbrukums īslaicīgi radīja traucējumus tīmekļa vietnes darbībā, liedzot tai pieeju. Iestādei tika sniegtas rekomendācijas vietnes slodzes noturības uzlabošanai.
- 03.02. Atkārtoti tika izsūtīti e-pasti, kas noformēti kā viltus rēķini ar saiti uz „CTB Locker" datorvīrusu, vēstuļu teksts bija mainīts.
- 04.02. Latvijas akadēmiskais tīkls un kāds datu centrs piedzīvoja apjomīgu DDoS uzbrukumu, kurā bija iesaistīti vairāki tūkstoši uzbrūkošo serveru. Uzbrukums tika vērsts pret vienu IP adresi. Uzbrukuma ietekmi izdevās mazināt 20 minūšu laikā.
- 05.02. Tika konsultēti servera uzturētāji par drošības uzlabošanu CMS Wordpress lapām.
- 05.02. Pret kādu datu centru tika vērsts DDoS uzbrukums, izmantojot .ru domēnus ar palielinātu DNS pakešu teksta lauku. Domēnus uzbrucēji bija izveidojuši un specifiski konfigurējuši tieši uzbrukuma mērķiem. Sadarbībā ar domēnu reģistriem tika panākta domēnu bloķēšana.
- 10.02. Vairākas Nīderlandes valsts iestādes piedzīvoja DDoS uzbrukumu, kas būtiski traucēja arī vairāku iestāžu tīmekļa vietņu darbību. CERT.LV iniciēja informācijas apmaiņas procesu ar Nīderlandes CERT vienību, lai skaidrotu uzbrukuma metodes un apjomus.
- 12.02. Masveidīgi tika izsūtīti e-pasti, noformēti kā parādu piedziņas firmas paziņojumi, kas saturēja saites uz „CTB Locker" datorvīrusu.

Vēstules paraugs:



-----Original Message-----
From: gita eihmane [mailto:gita.eihmane@creditreform.lv]
Sent: Friday, February 27, 2015 3:33 PM
To: gita.eihmane@creditreform.lv
Subject: Maksājuma pieprasījums!

Labdien,
Atgādinām, ka šodien iestājas Jums dotais parāda apmaksas termiņš lietā par parāda atgūšanu SIA "Rīgas Satiksme" uzdevumā Nr 20147822. Ja parāds vēl nav apmaksāts, lūdzam to nekavējoties izdarīt.

Jūsu lieta:
http://creditreform.su/piedzina/bridinajums.php?id=

Ar cieņu,
Gita Eihmane
CreditReform Latvija SIA
67501030, 26515199

- 20.02. Tika atkārtoti izsūtīti e-pasti, noformēti kā parādu piedziņas firmas paziņojumi, kas saturēja saites uz „CTB Locker" datorvīrusu.
- 23.02. CERT.LV rīcībā nonāca informācija par iespējamu ievainojamību kādā ar izglītības sistēmu saistītā portālā. Resursa turētājam tika izskaidrota situācija, trūkumi tika novērsti.
- 09.03. Kādas iestādes datoros tika konstatētas datorvīrusu aktivitātes. Tika konstatēts apjomīgs incidents, kas ietvēra kompromitētas darbstacijas un vienu serveri. Tika uzsākta izmeklēšana.
- 11.03. CERT.LV sniedza konsultācijas par kādas ļaunatūras aktivitātēm Latvijā, kas tajā brīdī tika izmeklēta.
- 13.03. CERT.LV sniedza konsultācijas saistībā ar Latvijas prezidentūru Eiropas Savienības Padomē par tīmekļa serveru konfigurācijas optimizāciju un korektu DDoS aizsardzības risinājuma ieviešanu un korektu DDoS aizsardzības risinājuma ieviešanu.
- 16.03. Izmantojot novecojušu OpenCart versiju, notika ielaušanās kādā internetveikalā. CERT.LV sniedza konsultāciju, kā problēmu risināt.
- 20.03. CERT.LV veica incidenta pārbaudi, kura ietvaros radās aizdomas, ka nesankcionēti iegūts saraksts ar e-pasta adresēm, uz kurām vēlāk uzbrucēji izsūtīja „CTB Locker" vīrusu. Vienā no „CTB Locker" uzbrukuma kampaņām ~80% saņēmēju izrādījās grāmatveži vai cilvēki, kas saistīti ar grāmatvedību.

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 5. un 8.punktā.

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

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.

Pārskata periodā vispopulārākā mājas lapas sadaļa bija par jaunākajiem vīrusiem, kas kopumā apskatīta 13 351 reizes. Nākamās populārākās sadaļas bija ziņas par vīrusu „CTB Locker" - ziņa *„Izplatās bīstams datorvīruss "CTB Locker""* ar 9 474 apmeklējumiem un ziņa *„Ar mēstuļu palīdzību izplata izspiedējvīrusu „CTB Locker""* ar 6 227 apmeklējumiem.

Kopā CERT.LV mājaslapai bijuši 34 609 skatījumi, kurus veido 25 213 unikāli lapu skatījumi no 99 valstīm. Arī šajā periodā lielākā daļa – 92,06% apmeklējumu bija no Latvijas.

Pārskata periodā CERT.LV tīmekļa vietnē tika publicētas 26 ziņas, sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicētas CERT.LV prezentācijas, mediju ziņas un CERT.LV publiskais darbības pārskats par 2014.gada 4. ceturksni.

CERT.LV Twitter kontā https://twitter.com/certlv tika publicētas 40 ziņas par dažādiem jaunumiem. Pārskata perioda beigās konta sekotāju skaits sasniedza 1191. Kopumā 801 reizi @certlv ziņas tikušas „retvītotas" jeb pārpublicētas. Augstais pārpublicēto ziņu skaits skaidrojams ar to, ka ļoti aktīvi tika retvītota informācija par „CTB Locker" datorvīrusu, arī citi twitter lietotāji, piemēram, SIA „Lattelecom" un Aizsardzības ministrija ievietoja brīdinājumus par vīrusu, atsaucoties uz CERT.LV.

Gadījumos, kad CERT.LV saņem informāciju, par to, ka izsūtīts liels skaits ar inficētām mēstulēm, sociālie mediji ir efektīvs veids, kā ātri brīdināt datorlietotājus. Arī ziņu portāli bieži publicē informāciju uzreiz pēc CERT.LV ziņu parādīšanās sociālajos tīklos, tādējādi paātrinot komunikāciju.

CERT.LV profilā sociālajā tīklā Facebook http://www.facebook.com/certlv pārskata periodā publicētas 32 ziņas. Sociālajā tīklā Google+ https://www.google.com/+CertLv publicētas 32 ziņas un CERT.LV draugiem.lv lapā http://www.draugiem.lv/certlv publicētas 40 ziņas.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata periodā portālam bija 18 348 lapu skatījumi no tiem 14 483 unikāli lapu skatījumi.

Pārskata periodā CERT.LV pārstāvji sniedza komentārus radio un televīzijā, kā arī informēja ziņu portālus par jaunākajām aktualitātēm. Sīkāka informācija:

1) Intervijas un ziņas radio:
   - 13.01. Tika sniegta intervija Latvijas Radio 1 raidījumā "Zināmais nezināmajā" par kiberdraudiem un drošības sistēmu pilnveidošanu.

- 15.01. Tika sniegta intervija Latvijas Radio 4 raidījumā „Jūsu tiesības" par IT drošības problēmām.
- 21.01.Tika sniegta telefonintervija 1.Biznesa radio par „CTB Locker" izplatību.
- 03.02. Tika sniegta telefonintervija 1.Biznesa radio par CERT.LV darbību, incidentu veidiem un kiberdrošību.
- 10.03. Tika sniegta intervija Latvijas radio 4 ziņām par kiberdrošības situāciju Latvijā un kiberdrošību Prezidentūras kontekstā.

2) Sižeti televīzijā, tiešraides:

- 06.01. Tika sniegta intervija LNT raidījumā „900 sekundes" par kiberdrošību.
- 28.01. Tika sniegta telefonintervija LTV1 ziņām par „CTB Locker".
- 28.01. Tika sniegta telefonintervija LTV1 raidījumam „Rīta panorāma" par „CTB Locker".
- 30.01. Tika sniegta intervija LTV7 ziņām par „CTB Locker".
- 04.02. Tika sniegta intervija RĪGA TV 24 raidījumā „Tīkla vīzija" par kiberdrošību.
- 18.02. Tika sniegta intervija LTV 1 raidījumā „Panorāma" par „CTB Locker".
- 20.02. Tika sniegta intervija LTV 1 raidījumam „Rīta panorāma" par kiberdrošību.
- 10.03. Tika sniegta intervija LNT raidījumā „900 sekundes" par kiberdrošības situāciju Latvijā.

3) Ziņas portālos:

- 20.01. Izplatās bīstams datorvīruss „CTB Locker" - raksts lvportals.lv
- 20.01. Izplatās bīstams un nepatīkams datorvīruss - raksts tvnet.lv
- 20.01. Brīdina par bīstama izspiedējvīrusa izplatīšanos - raksts apollo.lv
- 27.01. Bīstams datorvīruss mēstulēs par it kā nesamaksātu rēķinu - raksts diena.lv
- 27.01. Brīdina par mēstulēm ar tēmu „Neapmaksāts rēķins", kas izplata vīrusu - raksts tvnet.lv
- 27.01. Brīdina par bīstama kibervīrusa izplatību e-pastā - raksts kasjauns.lv
- 27.01. Bīstamais datorvīruss e-pastos slēpjas zem tēmas „Neapmaksāts rēķins!" - raksts lsm.lv
- 27.01. Brīdinājums visiem iedzīvotājiem: viena kustība var radīt lielus zaudējumus - raksts apollo.lv
- 27.01. Mēstules ar tēmu "Neapmaksāts rēķins" izplata vīrusu - raksts la.lv
- 27.01. Neveriet vaļā mēstules ar tēmu „Neapmaksāts rēķins!" - raksts db.lv
- 27.01. Brīdinājums neatvērt mēstulēs ar nosaukumu "Neapmaksāts rēķins" u.c. - raksts nozare.lv
- 28.01. Aicina uzmanīties – izsūta jaunu inficētu mēstuļu porciju - raksts delfi.lv
- 05.02. Bīstamais izspiedējvīruss turpina izplatīties; ir pieci svaigākās versijas upuri - raksts apollo.lv
- 06.02. Eksperti iesaka nemaksāt hakeriem par failu atkodēšanu - raksts lsm.lv
- 25.02. Aizvadītajā gadā reģistrēti 3034 augstas prioritātes kiberuzbrukumu incidenti - tvnet.lv
- 25.02. Aizvadītajā gadā reģistrēti 3034 kiberuzbrukumu incidenti - delfi.lv
- 26.02. Arvien biežāk apzog, izmantojot virtuālajā vidē atrodamos personas datus - raksts la.lv

- 10.03. Saistībā ar prezidentūru un Ukrainas notikumiem pret Latviju vērsti vairāki kiberuzbrukumi – raksts delfi.lv
- 20.03. Eksperti: Digitālā drošība ir viena no svarīgākajām biznesa prioritātēm - tvnet.lv
- 23.03. E-prasmju nedēļā speciālisti bez maksas pārbaudīs datoru un Android ierīču „veselību" - raksts diena.lv
- 24.03. Trešdien bez maksas varēs pārbaudīt datoru pie CERT.LV speciālista - diena.lv

4) Sadarbības un komunikācijas pasākumi:

- Janvārī „SIA DPA" sadarbībā ar CERT.LV veica aptauju valsts iestādēs par autentifikācijas līdzekļu lietojumu. Aptauja tika veikta ar mērķi pievērst Latvijas organizāciju un uzņēmumu pārstāvju uzmanību lietotāju identitātes aizsardzībai.
- Pārskata periodā CERT.LV sniedza informatīvo atbalstu AS „Swedbank" digitālās drošības izstādes "7 zelta likumi tavu datu drošībai internetā" izveidē. Paralēli izstādei „Swedbank" rīkoja semināru ciklu "7 zelta likumi tavu datu drošībai internetā", kuru vadīja Swedbank drošības eksperti. 23. februārī CERT.LV vadītāja uzstājās ar prezentāciju par IT drošību Swedbank digitālās drošības izstādes atklāšanas pasākumā.
- Martā CERT.LV sniedza komentārus „DNB Latvijas barometra" pētījumam par krāpšanas veidiem internetā.

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

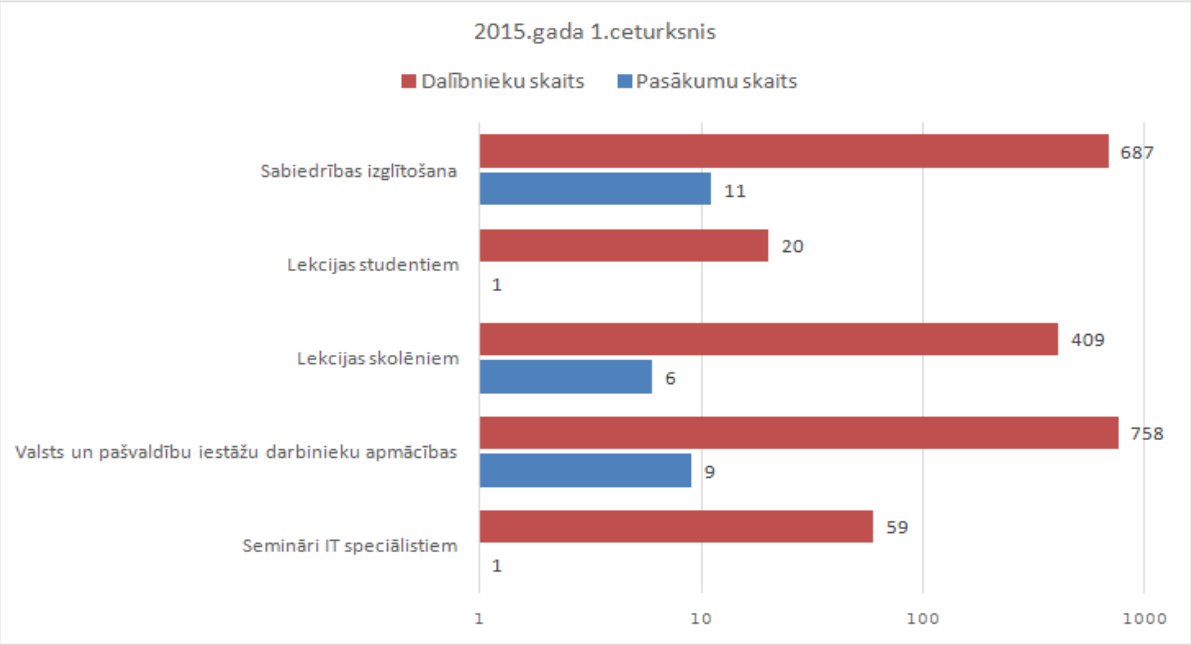
2015.gada sākumā CERT.LV uzsāka valsts un pašvaldību iestāžu darbinieku aptauju. Aptaujas mērķis ir noskaidrot darbinieku drošības paradumus, lietojot internetu, un veikt izplatītāko risku analīzi. Aptaujas rezultāti tiks apkopoti 2015.gada otrajā pusē.

No 5.-6.martam CERT.LV un Zemessardzes Kiberaizsardzības vienība organizēja tehniskās mācības „Marta migla", izmantojot uzkrāto pieredzi no iepriekšējām mācībām un citiem pasākumiem. Mācību mērķis bija pārbaudīt dalībnieku prasmes IT infrastruktūras aizsardzībā, IT drošības uzbrukumu atklāšanā un novēršanā. Mācības sniedza iespēju apmainīties ar pieredzi un iepazīties ar nozarē strādājošiem kolēģiem, strādājot komandā pie kopīga mērķa sasniegšanas. Mācībās piedalījās 59 dalībnieki.

No 2015.gada 23.marta līdz 27.martam CERT.LV iesaistījās "E-prasmju nedēļas 2015" aktivitātēs. 25.martā CERT.LV organizēja ikgadējo „Datorologa akciju", kuras ietvaros iedzīvotājiem bija iespēja veikt bezmaksas datora pārbaudi. Akciju apmeklēja 38 dalībnieki.
27.martā CERT.LV pārstāvis uzstājās ar prezentāciju seminārā „E-iespējas pašvaldībās" un stāstīja par IT drošības jēdzienu un teoriju, par informācijas drošības aspektiem un privātās informācijas aizsardzību ikdienā, kā arī par IT drošības aktualitātēm, izmantojot praktiskus piemērus. Semināru bija iespējams vērot video tiešraidē.

Uzsākts darbs pie IT drošības konferences "Kiberšahs. Stratēģija un taktika virtuālajā vidē" sagatavošanas. Konference norisināsies 2015.gada 1.oktobrī Latvijas Nacionālās bibliotēkas telpās. CERT.LV ir izsūtījis uzaicinājumu pieteikt referātus konferencei, pieteikumu iesniegšanas termiņš – 31.maijs.

Pārskata periodā CERT.LV par IT drošību izglītoja 1933 cilvēkus, iesaistoties 28 izglītojošos pasākumos.



7.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2015.gada 1.ceturksnī

CERT.LV pasākumi pārskata periodā:

1) ***Semināri IT speciālistiem:***

- 04.- 05.03.CERT.LV rīkoja IT drošības tehniskās mācības „Marta Migla".

2) ***Valsts un pašvaldību iestāžu darbinieku apmācības:***

- 30.01. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Realitāte virtuālajā vidē 2015" Veselības ministrijā.
- 13.02. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Rundāles pašvaldībā.
- 17.02. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Centrālajā finanšu un līgumu aģentūrā.
- 19.02. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību skolotāju seminārā Priekuļos.
- 17.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību LU Matemātikas un informātikas institūta darbiniekiem.
- 24.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Realitāte virtuālajā vidē 2015 Dobeles pašvaldībā.
- 27.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Indivīds interneta vidē" Ogres pašvaldībā E-prasmju nedēļas ietvaros.
- 31.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Realitāte virtuālajā vidē 2015" Talsu bibliotēkā.
- 31.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Realitāte virtuālajā vidē 2015" Talsu pašvaldībā.

3) ***Lekcijas skolēniem:***

- 29.01. CERT.LV pārstāvji uzstājās ar prezentāciju par IT drošību „Prasme pasargāt sevi digitālajā laikmetā – 2" Rīgas 3.ģimnāzijā.
- 11.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Prasme pasargāt sevi digitālajā laikmetā – 3" Ulbroklas vidusskolā, VARAM rīkotajā pasākumā saistībā ar „E-prasmju nedēļas" aktivitātēm.
- 12.03. CERT.LV pārstāvis uzstājās ar divām prezentācijām par IT drošību „Prasme pasargāt sevi digitālajā laikmetā – 2" un „Prasme pasargāt sevi digitālajā laikmetā – 3" Limbažu 3.vidusskolā.
- 31.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „.Prasme pasargāt sevi digitālajā laikmetā – 1" Vandzenes pamatskolā.
- 31.03. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību „Prasme pasargāt sevi digitālajā laikmetā – 2" Talsu vidusskolā.

4) ***Lekcijas studentiem:***

- 24.03. CERT.LV pārstāvis novadīja vieslekciju RTU Telekomunikāciju Institūta studentiem par aktuālajiem apdraudējumiem IT drošības jomā.

5) Sabiedrības izglītošana:

- 13.01. CERT.LV pārstāvis uzstājās ar prezentāciju Kredītinformācijas apmaiņas atbalsta asociācijas konferencē "Kā notiks kredītinformācijas apmaiņa Latvijā?".
- 18.02. CERT.LV pārstāvis uzstājās ar prezentāciju Latvijas atvērto tehnoloģiju asociācijas konferencē „Atvērtā Eiropa: atvērtie dati atvērtai sabiedrībai".
- 18.02. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Ventspils bibliotēkā.
- 20.02. CERT.LV pārstāvis piedalījās VARAM un LIKTA organizētajā sanāksmē par „E-prasmju nedēļas" pasākumiem un uzstājās ar prezentāciju „Prasme pasargāt sevi digitālajā laikmetā – 3".
- 23.02. CERT.LV pārstāvis uzstājās ar prezentāciju Swedbank digitālās drošības izstādes un semināru cikla atklāšanā "Zelta likumi tavu datu drošībai internetā".
- 12.03. CERT.LV pārstāvis uzstājas ar prezentāciju par IT drošību Swedbank privātpersonu finanšu institūta rīkotajā konkursā "Jaunais finanšu eksperts 2015", kā arī piedalījās konkursa noslēguma posma debašu vērtēšanā.
- 13.03. CERT.LV pārstāvis piedalījās konferences "e-Skills for Jobs 2015" paneļdiskusijā „The Impact of ICT on Employment".
- 18.03. CERT.LV pārstāvis sniedza prezentāciju "Kiberdrošības situācija Latvijā - statistika un tendences" biznesa tehnoloģiju platformas BiSMART meistarklasē "Drošība - modes lieta vai biznesa vitālais jautājums?"
- 20.03. CERT.LV pārstāvis uzstājās ar prezentāciju Kaspersky Lab organizētā pasākumā.
- 23.03. CERT.LV organizēja „Datorologa akciju" „E-prasmju nedēļas" ietvaros.
- 26.03. CERT.LV pārstāvis piedalījās ar prezentāciju konferencē, „Cybercrime – Strategic", kas notika Latvijas prezidentūras ES Padomē ietvaros.

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

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta atskaites 2.punktā. Zemāk uzskaitītas citas sadarbības tikšanās un konsultācijas.

- 08.01. CERT.LV vadītāja piedalījās ES Prezidentūras atklāšanas pasākumā un Digitālās prioritātes preses konferencē Latvijas Nacionālajā bibliotēkā.
- 08.01. CERT.LV pārstāvis piedalījās „Digital Europe" delegācijas vizītē Latvijā, kas notika Aizsardzības ministrijā.
- 08.01., 12.02. un 12.03. Notika DEG sanāksmes.
- 13.01. Aizsardzības ministrijā notika ENISA mācību plānošanas sanāksme.
- 06.02. Notika sadarbības tikšanās ar Valsts policijas Ekspertīžu centru.
- 10.02. Notika tikšanās Aizsardzības ministrijā par kiberjaunsardzes veidošanu.
- 11.02. Notika sadarbības tikšanās ar LVRTC par ES struktūrfondu projektiem.
- 17.02. Notika sadarbības tikšanās ar LVRTC un VARAM par ES struktūrfondu projektiem.
- Pārskata periodā CERT.LV piedalījās Aizsardzības ministrijas darba grupā par MK noteikumu izstrādi "Noteikumi par kārtību, kādā valsts un pašvaldības institūcijas nodrošina informācijas un komunikāciju tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām".
- 05.03. CERT.LV pārstāvji piedalījās sanāksmē Aizsardzības ministrijā par kompetentās un atbildīgas iestādes veidošanu.
- 12.03. Notika tikšanās ar Kases aparātu tirgotāju un servisa dienestu asociācijas pārstāvjiem.

6. 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 2015.gada 31.martam CERT.LV ir apkopojis informāciju par 1380 kontaktpersonām, kuras ir atbildīgas par IT 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.

Saistībā ar rīcības plāniem nav izmaiņu attiecībā pret 2014.gada 4.ceturksni - ir saņemtas atbildes no 63 ESK. Līdz 31.martam saņemti 58 ESK rīcības plāni, kā arī 5 ESK rakstiski apliecinājuši, ka neuztur publisko elektronisko sakaru tīklu, no kuriem 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).

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

Pārskata periodā notika aktīva sadarbība ar citu valstu IT drošības incidentu novēršanas vienībām, gan lūdzot palīdzību un informāciju par incidentiem, kas notiek Latvijā, gan palīdzot ar citās valstīs notikušu incidentu risināšanu, gan arī kopīgi uzlabojot incidentu risināšanas metodoloģiju, rīkus un procedūras.

24.02.- 26.02. CERT.LV piedalījās Eiropas Tīkla un informācijas drošības aģentūras (ENISA) kiberdrošības mācību "CYBER EUROPE 2014" trešajā - stratēģiskajā fāzē. Mācības noritēja divās daļās. Pirmajā notika dalībvalstu prezentācijas par atsevišķiem praktiskiem piemēriem, kā arī ENISA un Eiropas Komisijas pārstāvju prezentācija par labo praksi. Otrajā daļā notika liela mēroga Eiropas kiberkrīzes scenārija apspriešana diskusijas formā. Mācībās piedalījās pārstāvji no CERT.LV un Aizsardzības ministrijas.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 26.- 28.01. CERT.LV pārstāvji piedalījās TF-CSIRT un FIRST tehniskajā seminārā, kas notika Las Palmas, Gran Canaria, Spānijā. Sanāksmi vadīja CERT.LV vadītāja.
- 17.02.- 19.02. CERT.LV pārstāvis piedalījās UK Trade & Investment Nordic Baltic ICT grupas organizētajā pasākumā UKTI Nordic Baltic kiberdrošības konferencē Londonā, Lielbritānijā.
- 24.02.-26.02. Dalība Eiropas Tīkla un informācijas drošības aģentūras (ENISA) kiberdrošības mācību "Cyber Europe 2014" trešajā - stratēģiskajā fāzē Briselē, Beļģijā.
- 27.02. CERT.LV pārstāvis tikās ar Igaunijas aizsardzības ministrijas pārstāvjiem par projekta „Cyber Hygiene" ieviešanas iespējām Latvijā. Tikšanās notika Tallinā, Igaunijā.
- 06.03. Notika tikšanās ar Lietuvas valdības CERT pārstāvjiem.
- 11.-12.03. CERT.LV pārstāvji piedalījās NATO CCD CoE organizēto mācību „Locked Shields 2015" testa pasākumā Tallinā, Igaunijā.
- 16.03. CERT.LV pārstāvis piedalījās sanāksmē Hamburgā, Vācijā, kur notika tikšanās ar Trusted Introducer servisa nodrošinātājiem un GEANT asociācijas pārstāvjiem.
- 24.03.-28.03. CERT.LV pārstāvis piedalījās NATO Cooperative Cyber Defence Centre of Exelence IT drošības aizsardzības uzraudzības kursos Tallinā, Igaunijā.
- 25.-26.03. CERT.LV pārstāvis piedalījās Aizsardzības ministrijas un Vācijas Federālās aizsardzības ministrijas organizētajā konferencē „Conference on Cyber Defence in Europe" Latvijas prezidentūras ES padomē ietvaros Berlīnē, Vācijā.

Sadarbība konkrētu incidentu gadījumos aprakstīta šī pārskata 2.punktā.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 09.01. Notika tikšanās ar VARAM un LIKTA par „E-prasmju nedēļas" organizēšanu.
- 12.01. Notika tikšanās ar SIA DPA par sadarbību pētījuma ietvaros.
- 23.01. Notika tikšanās ar Swedbank par sadarbību IT drošības semināra organizēšanā.
- 04.02. Notika sadarbības tikšanās ar Microsoft Latvia.
- 04.02. Notika sadarbības tikšanās ar SIA Opticom.
- 09.02. Notika sadarbības tikšanās ar IBM.
- 24.02. Notika tikšanās par 2015.gada IT drošības konferences organizēšanu.

9. Aģentūras papildu pasākumu veikšana.

Atskaite par elektronisko ziņojumu līniju (turpmāk – ZL) par nelegālu interneta saturu nodrošināšana laika posmā no 2015.gada 1.janvāra līdz 31.martam.

Latvijas interneta asociācijas Net-Safe Latvia drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2015. līdz 31.03.2015. ir saņēmusi un izvērtējusi 288 ziņojumus. No tiem 171 ziņojumā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 8 ziņojumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 3 gadījumos konstatēti vardarbību atainojoši materiāli, 10 ziņojumos konstatēta personas goda un cieņas aizskaršana. Naida kurināšana noteikta 3 ziņojumos, 18 ziņojumi saņemti par finanšu krāpniecības mēģinājumiem internetā, 69 ziņojumu saturs nav bijis pretlikumīgs, no kuriem 23 gadījumos ziņotājiem tika sniegti ieteikumi problēmsituāciju risināšanai.

Valsts policijai nosūtīti 104 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 71 ziņojums par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites. 3 ziņojumi par naida kurinošu saturu ir nosūtīti ZL sadarbības partnerim Latvijas cilvēktiesību centram izvērtēšanai un turpmāko darbību veikšanai.

Pārskata periodā, sadarbojoties ar Valsts policiju un interneta servisa piegādātājiem, izdevies dzēst visus bērnu seksuālās izmantošanas materiālus, kas tika uzturēti Latvijā un par kuriem tika saņemti ziņojumi. Vidēji nelegālā satura dzēšanai bija nepieciešamas septiņas dienas.

2015.gada 12.maijā

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