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 3. ceturksnis (01.07.2015. – 30.09.2015.)

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

Pārskata periodā interneta lietotājiem masveidā tika izsūtīti e-pasti it kā Paypal tiešsaistes maksājumu sistēmas vārdā, ziņojot par konta bloķēšanu. Lai apstiprinātu savu identitāti, 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. Uzbrukumi Paypal lietotāju kontiem dažādos veidos turpinājās visu periodu.

IT drošības pasauli atkārtoti pāršalca ziņa par drošības trūkumiem attālinātas serveru vadības protokolam IPMI (Intelligent Platform Management Interface).
Uz kopējā fona Latvijā šādu servisu skaits ir salīdzinoši neliels, tomēr sekmīga uzbrukuma gadījumā var rasties būtiski zaudējumi, jo iespējams kompromitēt serveri, kas, iespējams, uztur virkni dažādu resursu.

Pārskata periodā vērienīgākais drošības incidents bija uzbrukums Ministru kabineta mājas lapai www.mk.gov.lv. 2015.gada 14.jūlijā pl. 12:00, sākoties Ministru kabineta sēdei, sākās arī intensīvs, 14 stundu ilgs uzbrukums, kura mērķis bija iespējamo mājas lapas ievainojamību meklēšana un izmantošana. Uzbrukums tika sekmīgi atvairīts.

Jūlijā CERT.LV uzsāka publicēt iknedēļas ziņas par notikušajiem IT drošības incidentiem. Ziņas raisa sabiedrības un mediju uzmanību, jo atspoguļo kiberdrošības aktualitātes Latvijā un pasaulē.

No 4. līdz 6. augustam CERT.LV sadarbībā ar ENISA rīkoja semināru "Pierādījumu vākšana un artefakti digitālajā vidē". Seminārā piedalījās 34 dalībnieki, kuri trīs dienu laikā iepazinās ar mobilo iekārtu incidentu veidiem un to risināšanu, pierādījumu vākšanu un artefaktu analīzi digitālajā vidē.

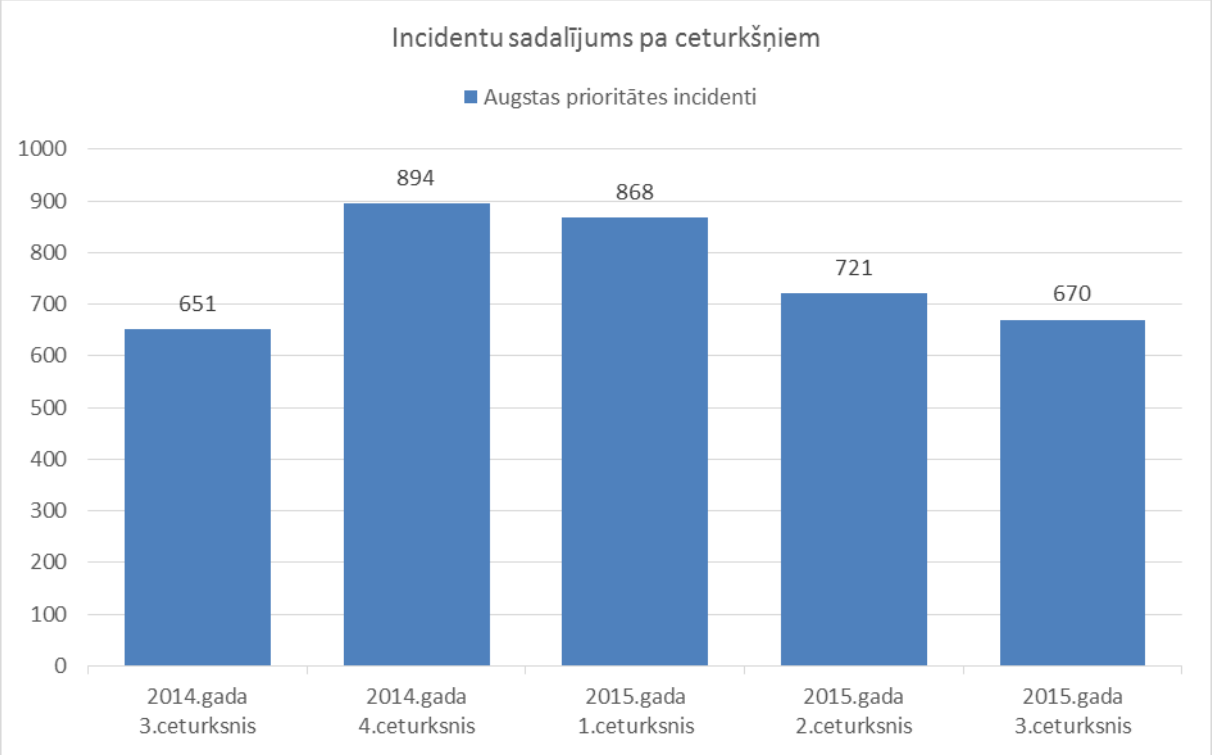
2015. gada 3. ceturksnī CERT.LV reģistrēja un apstrādāja 670 augstas prioritātes incidentus un 126 993 zemas prioritātes incidentus.

Pārskata periodā CERT.LV pārstāvji piedalījās 15 pasākumos, apmācot 755 cilvēkus, ievietoja 33 jaunas ziņas vietnē www.cert.lv, piedalījās 3 radio pārraidēs un 7 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

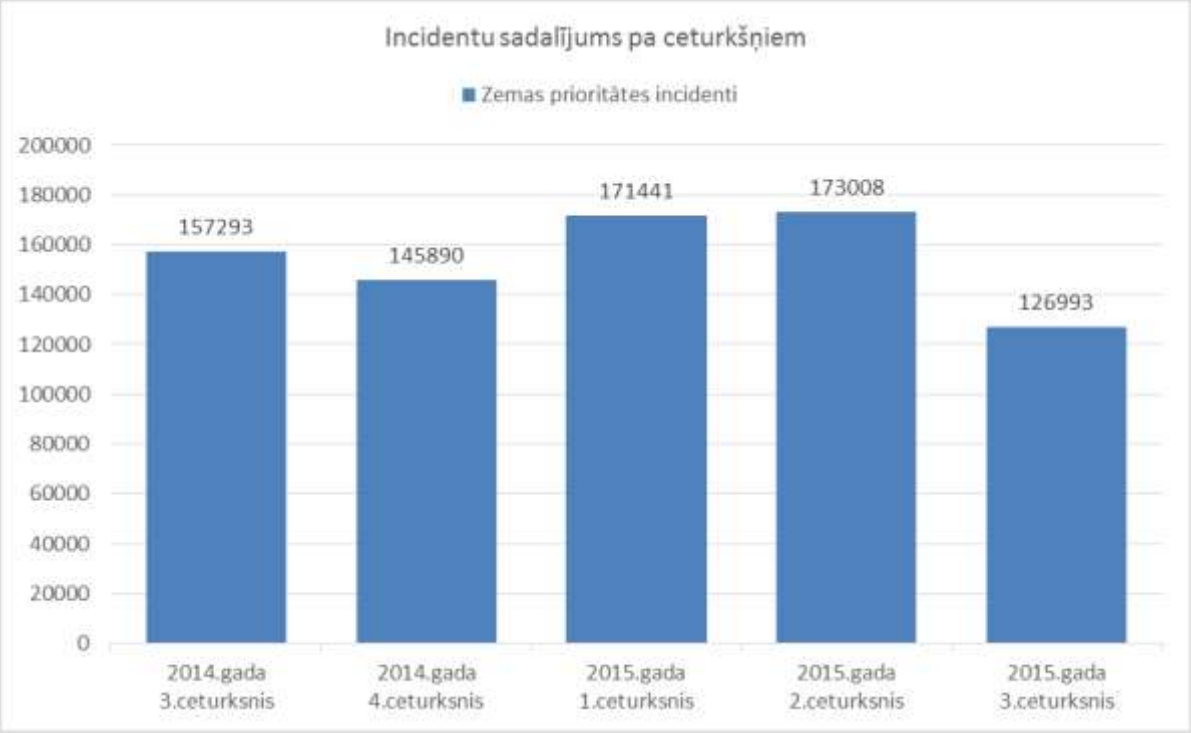
CERT.LV ik mēnesi apkopo informāciju par notikušajiem incidentiem, iedalot incidentus augstas prioritātes (visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas vai ko ir 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 3. ceturksnī CERT.LV apstrādāja 670 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāts 721 augstas prioritātes incidents, bet 2014. gada 3. ceturksnī 651 augstas prioritātes incidents.



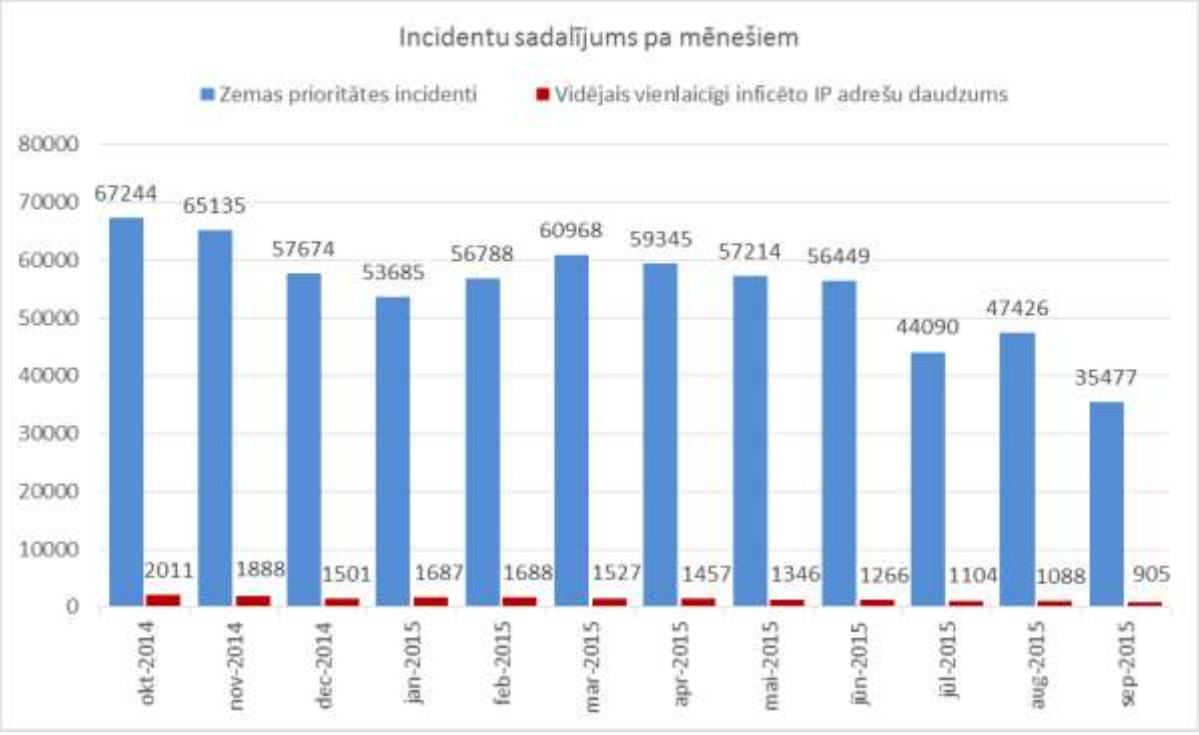
1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2014. un 2015. gadā.

Reģistrēto incidentu skaitā saglabājas kritums, arī gada griezumā augstas prioritātes incidentu skaits ir līdzīgs pagājušajā gadā apstrādāto incidentu skaitam. Nekādas jaunas un tieši uz Latviju mērķētas uzbrukumu kampaņas arī šajā periodā netika novērotas.



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

2015.gada 3.ceturksnī CERT.LV reģistrēja 126 993 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 173 008 zemas prioritātes incidenti, bet 2014. gada 3. ceturksnī – 157 293 incidenti. Zemas prioritātes incidentu skaits, pretēji iepriekšējam ceturksnim ir piedzīvojis krasu samazinājumu, kas saistīts ar ārzemju sadarbības partneru piegādātās informācijas izmaiņām.

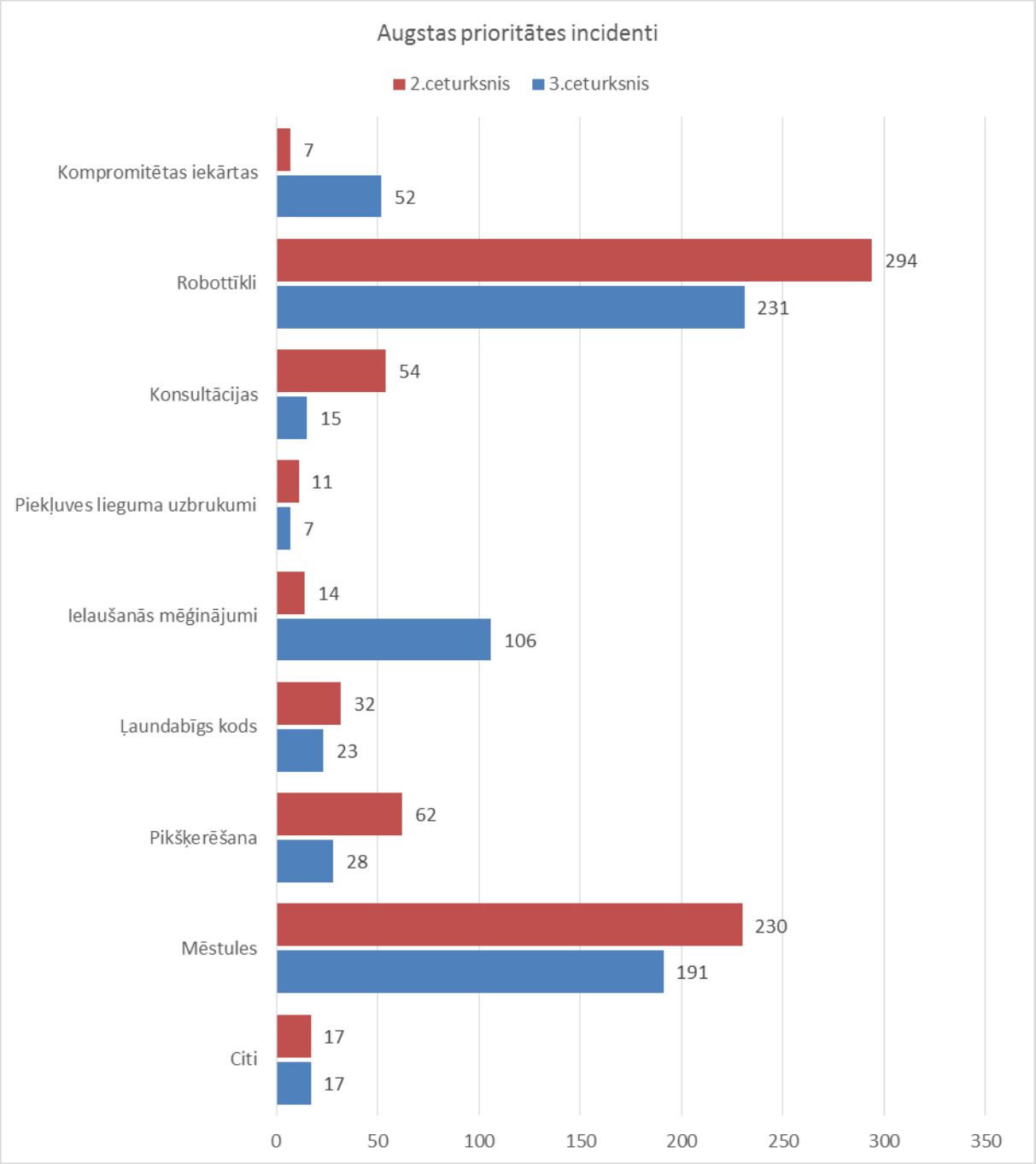


3.attēls – Reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu skaits 2014. un 2015. gadā.

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". Atbildīgo IPS kopskaits saglabājās bez izmaiņām – 13.

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

Pārskata periodā CERT.LV reģistrēja un apstrādāja 670 augstas prioritātes incidentu.

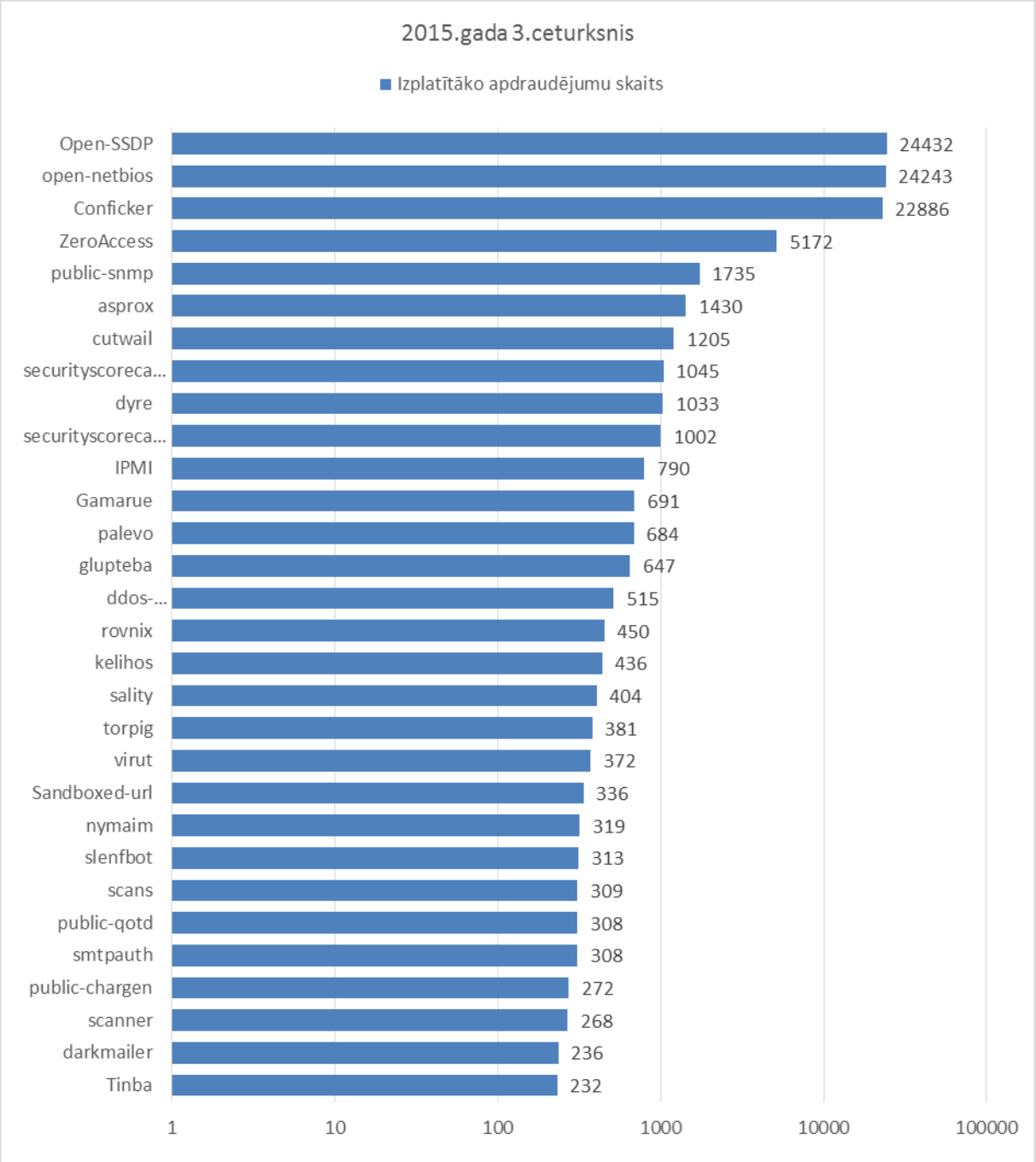


4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2015. gada 2. un 3. ceturksnī.

Analizējot 3. ceturkšņa augstas prioritātes incidentu statistiku, jāsecina, ka pikšķerēšanas uzbrukumi kļūst arvien mazāk izplatīti. Īpaši pikšķerēšana samazinās pret internetbanku lietotājiem, jo uzbrucēji dod priekšroku mēģinājumiem inficēt gala lietotāja datorus un

mobilās ierīces. Jāsecina, ka uzbrucēji pielāgojas internetbanku drošības uzlabojumiem un arī lietotāju spējai atpazīt pikšķerēšanu.

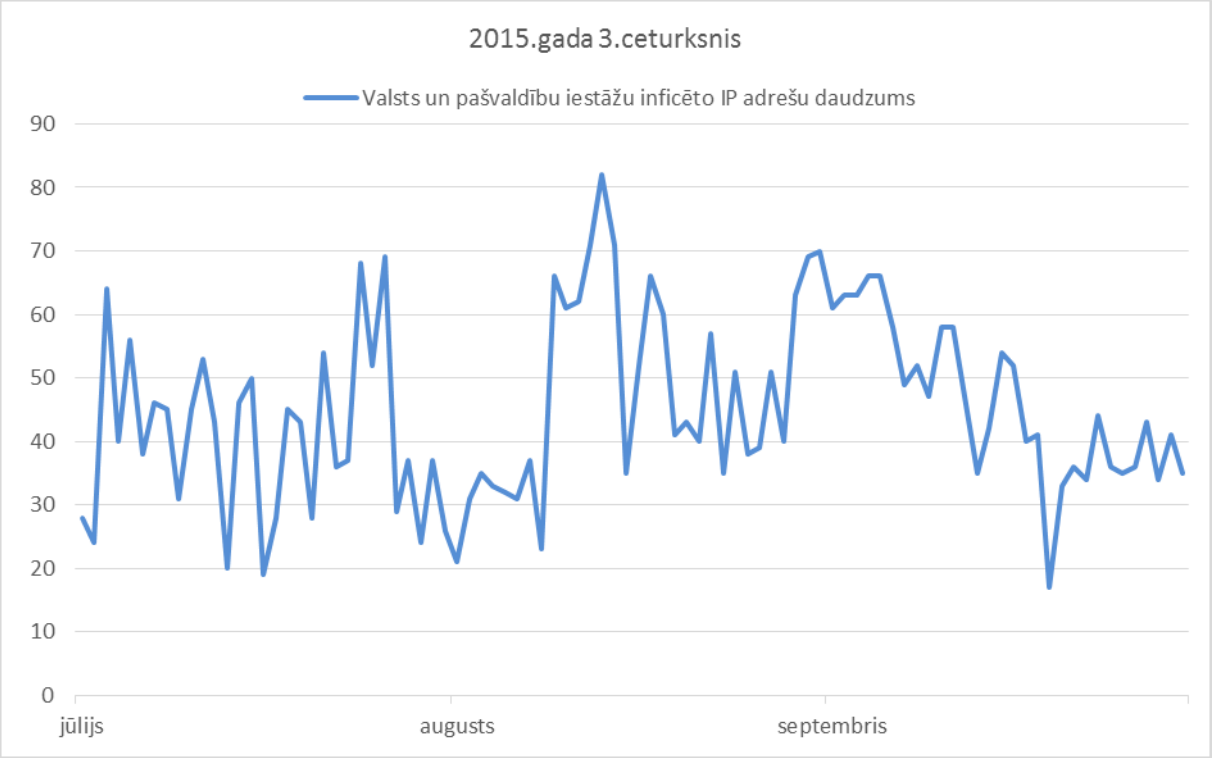
Pārskata periodā CERT.LV reģistrēja 126 993 zemas prioritātes incidentus.



5.attēls - CERT.LV reģistrētie zemas prioritātes incidenti no 2015. gada 1.jūlija līdz 30.septembrim pa apdraudējumu veidiem.

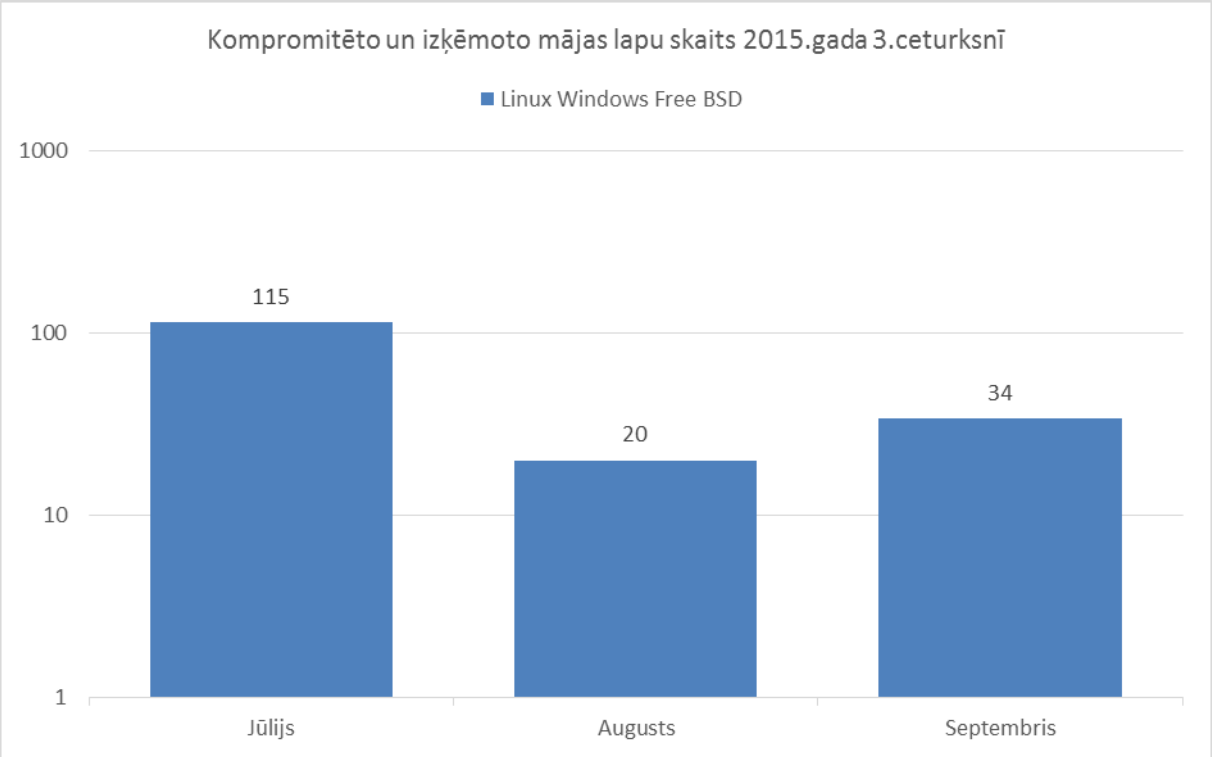
CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā inficētas.

Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm.



6.attēls – Iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2015.gada 3.ceturksnī.

CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus.



7.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2015. gada 3. ceturksnī.

Pēc CERT.LV novērojumiem, Latvijā aptuveni 50% no kompromitētām tīmekļa vietnēm tiek

kompromitētas atkārtoti, kas norāda uz resursu turētāju un/vai administratoru paviršo attieksmi pret drošības ielāpu ieviešanu. Lielā daļā gadījumu kompromitētā lapa tiek atjaunota no rezerves kopijām ar tām pašām vecajām ievainojamībām. Ir tikai laika jautājums (no dažām dienām līdz nedēļai), kad uzbrucējs atkal izmanto tos pašus "vārtus", pa kuriem ienācis iepriekš.

Pārskata periodā notika virkne dažādu uzbrukuma kampaņu, kas bija mērķētas gan uz valsts un pašvaldību iestādēm, gan uzņēmumiem, gan internetbanku lietotājiem.

Zemāk uzskaitīti svarīgākie pārskata periodā risinātie incidenti un to novēršana.

Jūlijā:

- 01.07. CERT.LV palīdzēja izvērtēt e-pastos reklamētu lapu www.careerjournalonline.com, kas ir daļa no finanšu piramīdas tipa krāpniecības shēmas. Turpmākajos mēnešos šī un līdzīgas lapas e-pastos tiek reklamētas regulāri, CERT.LV konsultēja vairākas personas.
- 02.07. Izmantojot viltotus rēķinus, tika mēģināts izkrāpt naudu no juridiskām personām. CERT.LV izskaidroja situāciju potenciālajiem upuriem, kas vērsās pēc palīdzības.
- 11.07. CERT.LV saņēma ziņojumu par kāda portāla lapas kopiju, kas izveidota piekļuves datu izkrāpšanai. Lapas uzturētāji tika brīdināti, lapa tika slēgta.
- 14.07. Pret MK mājaslapu www.mk.gov.lv notika DDoS uzbrukums. Izveidotā aizsardzības sistēma to veiksmīgi bloķēja. Ministru kabineta mājas lapas aizsardzībai izmanto LVRTC un Valsts kancelejas aizsardzības risinājumus.
- 20.07. CERT.LV izmeklēja mērķētu uzbrukumu kāda programmēšanas uzņēmuma darbiniekam. Uzbrukumu kāds mēģināja realizēt, pa pastu nosūtot vīrusu saturošu USB zibatmiņu uz darbinieka mājas adresi. Kā piegādātais vīruss tika izvēlēts novecojušais VIRUT, kas ir atpazīstams lielākajā daļā antivīrusu ražotāju. CERT.LV regulāri apstrādā datus par VIRUT datorvīrusa upuriem Latvijā. 2015. gada jūlijā Latvijā ir 145 IP adreses, kas inficētas ar šo vīrusu. Uz kopējā fona tas ir neliels skaitlis.
- 23.07. CERT.LV identificēja 62 uzlauztas tīmekļa vietnes, kas inficēja apmeklētāju datorus, izmantojot *Angler exploit kit* rīkus. Mazāk kā puse šo resursu ir .lv domēnu zonā, taču visi ir uzturēti uz Latvijas IP adresēm. Resursu turētāji tika informēti un uzsāka darbu pie tīmekļa vietņu labošanas vai slēgšanas. Lielākā daļa uzlauzto vietņu uzturētas uz novecojušas Worpdpress vai Joomla satura vadības sistēmas.
- Nedrošas tīmekļa vietnes izmantotas pikšķerēšanas uzbrukumu veikšanai pret Brazīlijas banku klientiem. Latvijas domēnu zonā [.lv] esošas tīmekļa vietnes bija iesaistītas Brazīlijas bankas CAIXA klientu datu izkrāpšanā, uzturot pikšķerēšanas resursus. Visas iesaistītās tīmekļa vietnes bija kompromitētas. Ar iesaistīto resursu turētājiem CERT.LV ir sazinājies, incidenti ir novērsti, taču datus analīzei nav izdevies iegūt, jo uzturētāji tos nebija saglabājuši.
- Kāds iepazīšanās portāls pārsūtīja apmeklētājus uz Policijas vīrusa web versiju saturošu vietni. Kā noskaidrojās, portāls lietoja ārvalstu baneru apmaiņas sistēmas, pār kurām

viņiem nebija nekādas kontroles. Uzbrucējiem, kompromitējot šo baneru sistēmu, izdevās piegādāt kaitīgu kodu visām tīmekļa vietnēm, kas lietoja ievainojamo baneru sistēmu.

- 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.

Augustā:

- 06.08. CERT.LV atmaskoja vērienīgu *typosquat* domēnu infrastruktūru. Daļa no tās bija uzturēta, lai iegūtu ar Latvijas prezidentūru ES padomē saistīto informāciju. Izmeklēšanas tehniskā informācija tika nodota tiesībsargājošām iestādēm.
- 07.08. CERT.LV identificēja vairākas zagtu kredītkaršu informācijas tirdzniecības vietnes .lv domēnu zonā. Incidenta tehniskā informācija tika nodota Valsts policijai. Iesaistītie domēni jau ir bijuši iesaistīti šādās aktivitātēs iepriekš.
- 12.08. CERT.LV panāca pikšķerēšanas tīmekļa vietņu slēgšanu, kas uzturētas Latvijā, lai veiktu uzbrukumus pret Paypal maksājumu sistēmas klientiem.
- 16.08. .lv zonā reģistrēts domēns icloud.lv tika izmantots Apple piekļuves datu izkrāpšanai. Pēc brīdinājuma uzturētājam, lapa tika slēgta.
- 18.08. Izmantojot datorvīrusa nozagtu e-pasta piekļuves informāciju, vairāku pašvaldību lietotājiem masveidā tika izsūtītas mēstules ar saitēm uz finanšu piramīdas tipa krāpniecības lapām. Pēc CERT.LV rīcībā esošas informācijas, mēstules tika izsūtītas inficēta datora e-pasta programmas saglabātās adrešu grāmatas kontaktpersonām. Darbinieki reaģēja profesionāli, uz saitēm neviens neklikšķināja un par incidentu tika informēts CERT.LV. Incidenta ietekme netika novērota.
- 18.08. CERT.LV veica Microsoft Word dokumentā iekļauta makrovīrusa analīzi, kas tika piesūtīts kādam uzņēmumam.
- 27.08. Kādas pašvaldības mājaslapā tika ievietoti kaitīgi Iframe, iemesls - novecojis CMS. Pēc brīdinājuma CMS tika salabots.
- Latvijas akadēmiskajā tīklā esošs serveris piedalās masveida mēstuļu izsūtīšanā. Konstatēts, ka serveris ir uzlauzts un tiek izmantots masveida mēstuļu izsūtīšanai. Uzbrukuma vektors ir bijis ievainojama tīmekļa vietne, caur kuru uzbrucējs ir spējis izvietot kaitīgo kodu. Tīmekļa vietne tika bloķēta līdz turētājs novērsīs drošības trūkumus.
- Notika uzbrukums kādas pašvaldības e-pasta serverim un lietotāju kontiem. Uzbrukuma metodes bija paroļu piemeklēšanas mēģinājumi. Neviens sekmīgs, nesankcionētas pieslēgšanās gadījums netika konstatēts.
- CERT.LV saņēma ziņas par uzbrukuma kampaņu, kurā tika izsūtīti kaitīgu kodu saturoši Microsoft Word dokumenti. Datori tika inficēti ar Zeus saimes trojāni. Kaitīgie dokumenti tika izsūtīti masveidā, taču, lai sekmīgi inficētu upura datoru, lietotājam

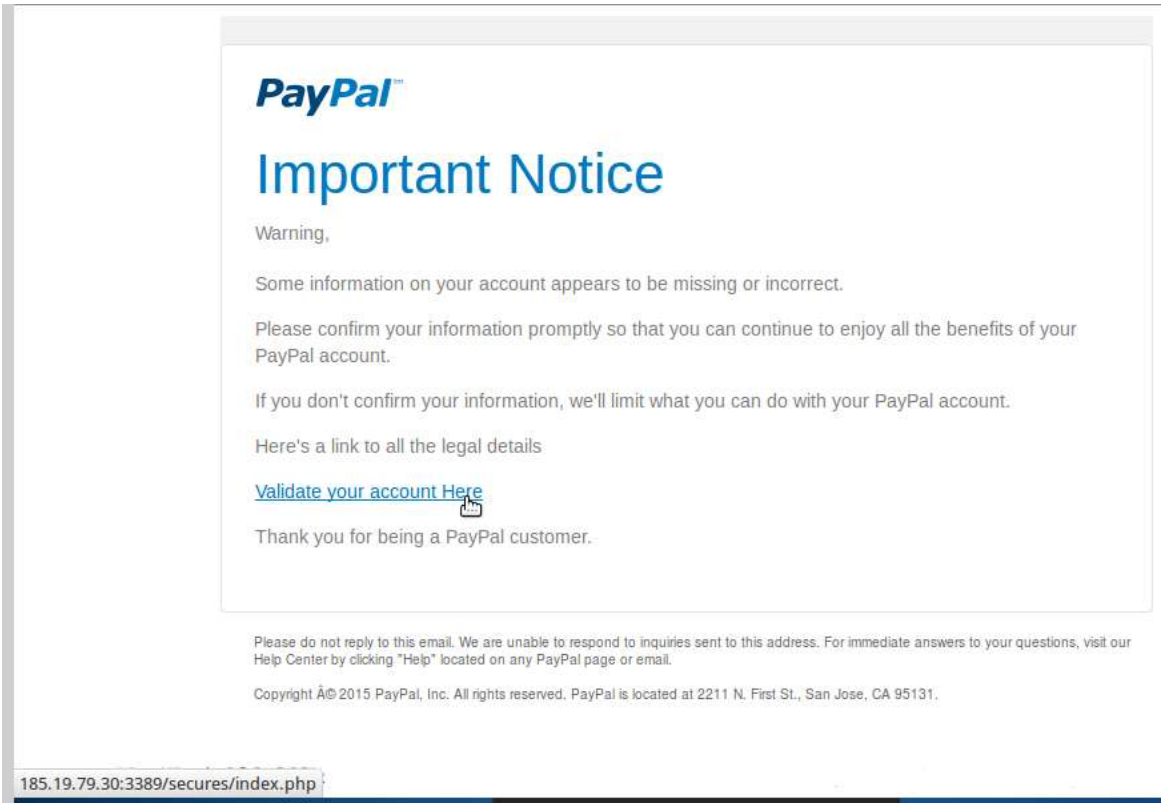
jāpiekrīt izpildīt aktīvo dokumenta komponenti (*macro*). Šobrīd zināms pielikuma faila nosaukums: item_list.doc. Incidenta risināšana turpinās.

- Notikuši vairāki DDoS uzbrukumi tīmekļa vietnēm Latvijā. Uzbrucējs visdrīzāk bija viens un tas pats. Vairāku tīmekļa vietņu turētāji informēja CERT.LV par DDoS incidentiem. Noskaidrots, ka tika pielietots HTTP DDoS un visus gadījumus vieno pazīme "undefined" URI laukā. CERT.LV sniedza norādījumus cietušajiem uzbrukuma ietekmes mazināšanai un sazinājās ar pakalpojumu sniedzējiem. Noskaidrots, ka uzbrukumā piedalās kompromitēti koplietošanas tīmekļa serveri.
- Kāda uzņēmuma darbinieki e-pastā saņēma inficētus MS Word dokumentus, kas aprīkoti ar jaunākajiem *exploit* kodiem. Uzņēmuma tehniskais departaments savlaicīgi atpazina apdraudējumu. CERT.LV turpina incidenta izmeklēšanu.
- Kāda interneta vietne tika izmantota uzbrukumā, mēģinot piegādāt kaitīgu kodu vietnes apmeklētājiem. Veicot incidenta analīzi, konstatēts, ka vietne tika uzturēta uz novecojušas Joomla 1.5 versijas. Nenoskaidroti uzbrucēji izmantoja publiski zināmu ievainojamību, lai izvietotu vietnē kaitīgu kodu, kas mēģina inficēt vietnes apmeklētāju datorus.
- Latvijas interneta lietotāji saņēma elektroniskās vēstules ar Bladabindi vīrusu pielikumā. Uzbrukuma kampaņa bija starptautiska un nebija mērķēta uz Latvijas interneta lietotājiem. Bladabindi vīruss ir informācijas zagšanas rīks, kas nodrošina arī papildu funkcionalitātes pievienošanu uzbrucējam, lejupielādējot tās uz upura datora. Uzbrucējam ir pilna kontrole pār upura datoru. CERT.LV rīcībā nav informācijas par sekmīgi inficētām iekārtām šīs kampaņas ietvaros, taču Latvijā ir vairāki tūkstoši ar šo vīrusu inficētu iekārtu. Bladabindi tiek izplatīts ar masvieda e-pasta satrpniecību, kas satur pielikumus ar nosaukumiem: "My Picture.SCR", "my pictures.zip", "specification.zip", u.c. nosaukumiem.

Septembrī:

- 03.09. No kādas pašvaldības datortīkla tika izsūtītas mēstules, vainīgais dators identificēts un iztīrīts.
- 09.09. Ar viltus rēķiniem tika izplatīts šifrēšanas izspiedējvīruss, CERT.LV konsultēja vienu no upuriem, kas zaudējis savus datus.
- 10.09. CERT.LV apturēja Latvijā uzturēta Android OS ļaunatūras kontrolcentru. Kaitīgā programmatūra pārsvarā tika mērķēta pret Spānijas banku klientu Android viedierīcēm.
- 14.09. CERT.LV konsultēja kādu vidusskolu par droša bezvadu tīkla izveidi.
- 18.09. Pret kādas pašvaldības mājaslapu tika veikts DDoS uzbrukums, lapas uzturētāji to veiksmīgi novērsa.
- Tika kompromitēta kāda pašvaldības tīmekļa vietne. Uzbrucēji nesankcionēti izvietoja savu saturu, kurā tiek ziņots, ka par uzbrukumu atbildību uzņemas Turku hakeri, slavinot Islāmu.
- Kādas pašvaldības atsevišķu lietotāju e-pasta konti tika kompromitēti un tika izmantoti mēstuļu sūtīšanai ar mērķi realizēt tālākus uzbrukumus.

- 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 veic autentifikācijas mēģinājumu, tad lietotājvārds un parole nonāca uzbrucēju rīcībā.



- Masveidā tika izplatīti e-pasta paziņojumi ar it kā datoru drošības sistēmas paziņojumiem, kas aicina atvērt pielikumu. Pielikumā ir .ZIP arhīvs, kas satur .EXE izpildāmo failu. Ja e-pasta saņēmējs atver pielikumu, tad ar Upatre Trojan starpniecību tika veikts mēģinājums inficēt datoru, lejupielādējot citus kaitīgus failus no IP adresēm Čehijā, ASV un Nigērijā. Šiem soļiem izpildoties sekmīgi, dators tiek inficēts ar Dyre Trojan, kas ir Zeus saimei līdzīgs banku datu zagšanas trojāns. Incidenta analīzes brīdī kaitīgos failus spēja atpazīt mazāk kā 10 no 56 populārākajām antivīrusu programmām. Zināms, ka šīs kampaņas ietvaros atsevišķas Latvijā strādājošas bankas bija uzbrucēju interešu sarakstā.

- Tīmekļa vietnes izplata datorvīrusus ar *Neutrino exploit kit* starpniecību, kā arī piedalās pikšķerēšanas uzbrukumu kampaņās. Visas uzbrukumos iesaistītās tīmekļa vietnes tika uzlauztas, jo tika uzturētas uz novecojušām Wordpress un Joomla satura vadības sistēmu versijām. Uzbrucēji, neizmainot vietnes oriģinālo saturu, ievietoja neredzamo instrukciju <iframe>, kura interneta pārlūku instruē apmeklēt uzbrucēju sagatavoto resursu, kā rezultātā inficē apmeklētāja datoru ar mērķi iegūt autentifikācijas operāciju detaļas un internetbanku transakciju datus. Pikšķerēšanas kampaņas, kas uzturētas uz Latvijā esošām tīmekļa vietnēm, lielākajā daļā gadījumu ir paredzētas ārvalstu

maksājumu sistēmu lietotāju datu izkrāpšanai. Divu nedēļu laikā tika aizvērtas piecas šādas vietnes.

- CERT.LV redzeslokā nonāca krāpnieciskiem mērķiem radīta tīmekļa vietne www.icloud.lv. Tā apzināti izveidota, lai izkrāptu Apple lietotāju datus. Tīmekļa vietne šobrīd ir aizvērta.
- 3. ceturksnī IT drošības pasauli atkārtoti pāršalca ziņa par drošības trūkumiem attālinātas serveru vadības protokolam IPMI (Intelligent Platform Management Interface).
  Uz kopējā fona Latvijā šādu servisu skaits ir salīdzinoši neliels, tomēr sekmīgs uzbrukums šādam serverim var radīt būtiskus zaudējumus, jo iespējams kompromitēt serveri, kas, iespējams, uztur virkni resursu. Pat ja speciāli IPMI interfeisam veltītais tīkla interfeiss nav pieslēgts datortīklam, noklusētajā konfigurācijā pie servera pārstartēšanas IPMI vadības modulis pieprasīs *broadcast* ziņojumā DHCP konfigurāciju caur standarta tīkla interfeisu (kurš nav IPMI). Ja *broadcast* domēnā atradīsies kāds DHCP serveris, tad konfigurācija tiks iedota un IPMI interfeiss saņems IP adresi un kļūs pieejams internetā ar nedrošu, noklusēto konfigurāciju.

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

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

Pārskata periodā CERT.LV pārstāvji sniedza komentārus radio un televīzijā, kā arī informēja ziņu portālus par jaunākajām aktualitātēm. Informācija par CERT.LV pasākumiem, aktuālākajiem drošības apdraudējumiem un citas ziņas tika ievietotas CERT.LV mājas lapā un CERT.LV sociālo tīklu kontos.

1) Intervijas un ziņas radio:

- 10.07. CERT.LV pārstāvis piedalījās LR4 raidījumā Jūsu tiesības: Datora un datu aizsardzība - eksperta padomi.
- 24.07. CERT pārstāvis piedalījās LR4 raidījumā "День за днем", par kiberuzbrukumu pret valsts iestāžu mājaslapām novēršanas pieredzi.
- 03.08. CERT pārstāvis piedalījās LR1 raidījumā "Krustpunkti" par troļļiem un hibrīdkaru.

2) Sižeti televīzijā, tiešraides:

- 16.07. Tika sniegta intervija LTV7 ziņām par MK lapas kompromitēšanu.
- 12.08. Tika sniegta intervija LTV1 Panorāmai par mobilo iekārtu drošību.
- 19.08. CERT.LV pārstāvis sniedza interviju TV3 raidījumā "Bez tabu" par mobilo iekārtu drošību.
- 28.08. Tika sniegta intervija LNT raidījumā 900 sekundes par vispārējo kiberdrošības situāciju Latvijā.
- 09.09. CERT.LV pārstāvis piedalījās Lattelecom TV 360 raidījumā „Ideju domnīca”. par hakeriem.
- 10.09. CERT.LV pārstāvis sniedza telefonintervijuLTV1 rīta panorāmā par draudiem maksājumu sistēmām.
- 23.09. CERT.LV pārstāvis sniedza komentāru TV3 raidījumam "Bez Tabu" par vecāku kontroles iespējām uz planšetēm un mobilajiem tālruņiem.

3) Ziņas portālos:

- 15.07. Visticamāk, no Krievijas noticis 14 stundu ilgs uzbrukums MK mājaslapai - TVNET.LV
- 15.07. CERT: сайт Кабинета министров ЛР подвергся атаке со стороны России - rus.delfi.lv
- 15.07. "CERT.lv": visticamāk, no Krievijas noticis 14 stundu uzbrukums MK mājaslapai - BNS
- 15.07. No Krievijas, iespējams, noticis uzbrukums Ministru kabineta mājaslapai -ir.lv
- 15.07. No Krievijas veikts nesekmīgs kiberuzbrukums Latvijas Ministru kabineta mājaslapa - delfi.lv
- 15.07. No Krievijas veikts 14 stundu ilgs un nesekmīgs kiberuzbrukums Latvijas MK mājaslapai - kasjauns.lv
- 15.07. No resursiem Krievijā uzbrukts Valsts kancelejas mājaslapai - diena.lv
- 15.07. Noticis uzbrukums Ministru kabineta mājas lapai - db.lv

- 16.07. CERT.LV pārstāvis sniedza interviju LTV7 krievu ziņēm par MK mājas lapas uzlaušanu un hakeru foruma likvidāciju.
- 16.07. CERT.LV pārstāvis sniedza interviju TV3 zinām par MK mājas lapas uzlaušanu un hakeru foruma likvidāciju.
- 16.07. "CERT.lv": kiberuzbrukuma MK vietnei organizētāji savas darbības nav slēpuši - la.lv, apollo.lv.
- 30.07. intervija žurnālā "Ir" ar B. Kaškinu - par uzbrukumu MK lapai un aktivitātēm kibertelpā.
- 03.08. Otrajā ceturksnī Cert.lv reģistrējis 721 augstas prioritātes drošības incidentu - tvnet.lv
- 12.08. Trīs Latvijas interneta forumos tirgoti zagtu kredītkaršu dati - delfi.lv, tvnet.lv
- 17.08. Sekmīgi atvairīts kiberuzbrukums kādam Latvijas ziņu portālam - apollo.lv, tvnet.lv
- 25.08. Pret Apple kontu lietotājiem vērsta kiberuzbrukumu kampana - tvnet.lv

4) CERT.LV tīmekļa vietnes:

Pārskata periodā vietnē https://www.cert.lv publicētas 26 ziņas.

Pārskata periodā populārākā sadaļa bija par jaunākajiem vīrusiem, kas kopumā apskatīta 10 144 reizes. Nākamā populārākā sadaļa bija ziņa par iespēju pieteikties konferencei „Kiberšahs. Stratēģija un taktika virtuālajā vidē" ar 2777 apmeklējumiem un lapas sadaļa "Jaunumi" ar 1 920 apmeklējumiem.

Kopā CERT.LV mājaslapai bijuši 15291 skatījumi, kurus veido 9637 unikāli lapu skatījumi no 106 valstīm. Arī šajā periodā lielākā daļa – 84 % apmeklējumu bija no Latvijas.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 11370 lapu skatījumi, no tiem 9129 unikāli lapu skatījumi.

Portālā esidross.lv publicētie raksti:

- Izaicini savu drošības sajūtu
- Divu pakāpju verifikācija
- Kā neatdot ļaundariem savas paroles
- Rezerves kopijas un sistēmu atjaunošana
- Datorlietotājiem pieejama OUCH! ziņu lapa

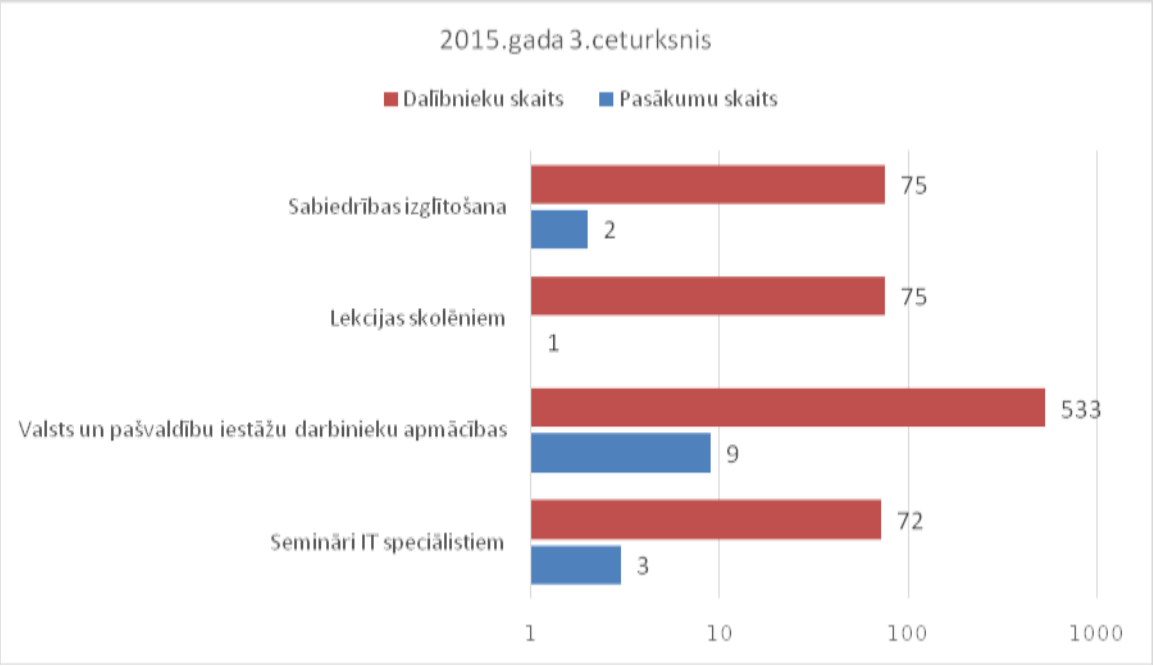
4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

30.07. CERT.LV organizēja semināru "Moderno operētājsistēmu ekspluatācijas pamati", kas bija paredzēts IT drošības speciālistiem ar priekšzināšanām, piedāvājot iespēju veikt praktiskus uzdevumus par semināra tēmām. Seminārā piedalījās 12 dalībnieki.

04.- 06.08. CERT.LV sadarbībā ar ENISA rīkoja semināru "Pierādījumu vākšana un artefakti digitālajā vidē". Semināra dalībnieki iepazinās ar mobilo iekārtu incidentu veidiem un to risināšanu, pierādījumu vākšanu digitālajā vidē un digitālās ekspertīzes pamatprincipiem, kā arī uzzināja par artefaktu analīzi digitālajā vidē. Semināru apmeklēja 34 dalībnieki no valsts un pašvaldību iestādēm.

Visu periodu notika gatavošanās CERT.LV un ISACA Latvijas nodaļas organizētajai IT drošības konferencei „Kiberšahs. Stratēģija un taktika virtuālajā vidē".

Pārskata periodā CERT.LV par IT drošību izglītoja 755 cilvēkus, iesaistoties 15 izglītojošos pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2015.gada 3.ceturksnī

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

28.07. tika apstiprināti MK noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".
Noteikumi nosaka valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģiju (IKT) minimālās drošības prasības un kārtību, kādā tiek nodrošināta valsts un pašvaldību institūciju IKT sistēmu atbilstība šīm prasībām.

Augustā CERT.LV atbalstīja Kiberaizsardzības vienību, nodrošinot IT drošības izaicinājumu tiešsaistes platformu, kurā dalībnieki var risināt dažādas sarežģītības tehniskus uzdevumus, gūstot par to punktus un sacenšoties savā starpā.

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

- 09.07., 13.08. un 10.09. notika DEG sanāksmes.
- 15.07. Notika tikšanās ar J. Sārtu.
- 11.09. Notika tikšanās ar J. Garisonu.
- Pārskata periodā notika vairākas sadarbības tikšanās un vizītes iestādēs par sadarbību ar valsts iestādēm par Agrās brīdināšanas sistēmu.

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.

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 2015. gada 2. ceturksni - ir saņemtas atbildes no 63 ESK. Līdz 30. septembrim 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.

Augustā tika parakstīts saprašanās memorands starp CERT.LV un CERT.GOV.GE no Gruzijas. Memoranda mērķis ir veicināt sadarbību un informācijas apmaiņu abu CERT vienību starpā.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 03.07. CERT.LV pārstāvji piedalījās Kaspersky rīkotajā seminārā Tallinā, Igaunijā.
- 31.08.- 04.09. CERT.LV pārstāvji piedalījās CERT-RO organizētajos kursos Bukarestē, Rumānijā.
- 22.09. Notika sadarbības tikšanās ar NCSC-NL Hāgā, Nīderlandē.
- 23.09. CERT.LV pārstāvis piedalījās "visitors programme" of Cyber emergency preparedness and response exercise - Cyber HEDHOG2015, Tallinā, Igaunijā.
- 24-25.09. CERT.LV pārstāvji piedalījās TF-CSIRT un Trusted Introducer sanāksmēs Tallinā, Igaunijā. CERT.LV vadītāja vadīja sanāksmes, CERT.LV vadītāja vietnieks sniedza prezentāciju.
- 25.09. Notika sadarbības tikšanās ar CERT.EE Tallinā, Igaunijā.
- 23-24.09. CERT.LV pārstāvis piedalījās "ENISA Trainers Workshop" Tallinā, Igaunijā.
- 29-30.09. CERT.LV pārstāvis piedalījās CERT-EU konferencē Briselē, Beļģijā.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 14.07. Notika telekonference ar Deliotte, sadarbība "Invitation to be interviewed for the study “Update of Impact Assessment and Roadmap”" ietvaros.
- 16.07. CERT.LV pārstāvji piedalījās NATO Strategic Communications Centre of Excellence prezentācijā par pētījumu “Internet trolling as a hybrid warfare tool: the case of Latvia”.
- 28.07. Notika sadarbības tikšanās ar SIA Stikpoint.
- 19.08. Notika intervija ar Igaunijas doktorantūras studentu.
- 20.08. CERT.LV pārstāvis piedalījās Net Safe konsultatīvās padomes sēdē.
- 20.08. CERT.LV pārstāvis piedalījās Kiberjaunsardzes sanāksmē.
- 03.09. CERT.LV pārstāvis piedalījās Kiberjaunsardzes sanāksmē.

9. 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 01.07.2015. līdz 30.09.2015. ir saņēmusi un izvērtējusi 88 ziņojumus. No tiem 37 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 5 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 4 ziņojumos konstatēta personas goda un cieņas aizskaršana un 1 ziņojums par naida kurināšanu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 7 ziņojumi, 21 ziņojumu saturs nav bijis pretlikumīgs, 13 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 14 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 20 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.

Pārskata periodā sadarbojoties ar Valsts policiju un interneta servisa piegādātājiem ir izdevies dzēst visus bērnu seksuālās izmantošanas materiālus, kas tika uzturēti Latvijā un par kuriem tika saņemti ziņojumi. Vidēji nelegālā satura dzēšanai bija nepieciešamas 10 dienas.

2015. gada 15. oktobrī

Sagatavotājs – Svetlana Amberga
Tālrunis: 67085888
E-pasts: svetlana.amberga@cert.lv