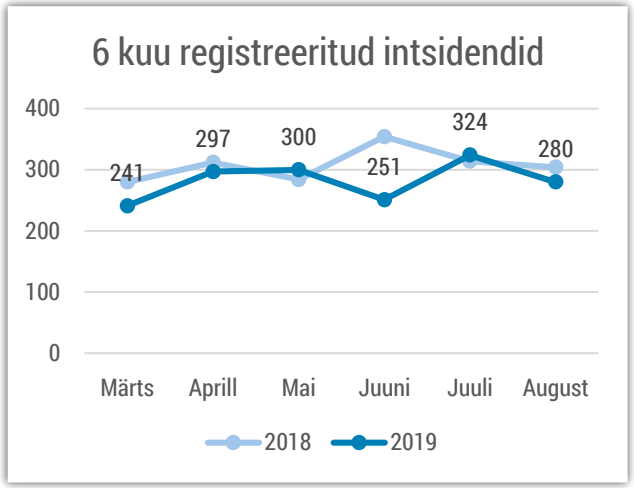
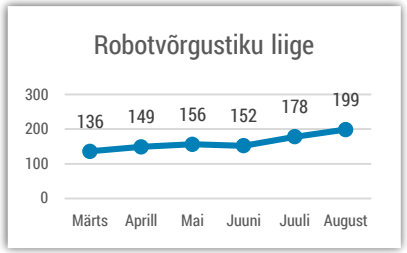
Olukord küberruumis – august 2019

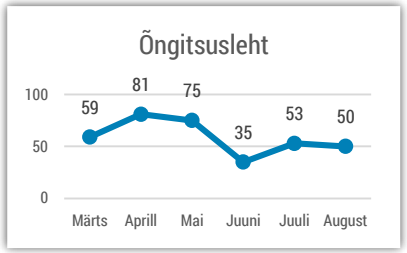
- Augustis registreerisime 280 intsidenti, mis oli samal tasemel võrreldes mullusega.
- Augustis jätkusid õngitsuskampaaniad, kus kurjategija püüab meelitada inimesi sisestama oma Smart-ID PIN2 koodi, et temalt raha varastada.
- CERT-EE on hakanud välja saatma senisest enam teavitusi haavatavustest Eesti küberruumis.
- Maailma suured tehnoloogiaettevõtted tunnistasid, et on lubanud alltöövõtjatel kuulata kasutajate loata nende omavahelisi vestlusi.



Intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtedega seotud intsidentide hulk jäi augustis umbes samale tasemele kui juulis.

Olukord Eesti küberruumis

Augustis jätkusid õngitsuskampaaniad, kus püüti Eestis tegutsevate pankade sümboolikat ära kasutades varastada ohvrite pangakontodelt raha nii, et ohver ise sisestab ülekande kinnitamiseks oma Mobiil-ID või Smart-ID PIN 2 koodi. Nendest rünnakutest kirjutasime ka oma juulikuu ülevaates ning neid on kajastatud ka meedias. Oleme järjepidevalt teavitanud avalikkust taolistest õngitsussõnumitest ja -lehtedest nii pea, kui meieni info jõuab.

Augusti lõpus tabas Tallinna linnavalitsuse töötajaid õngitsuskirjade kampaania kontoandmete kättesaamise eesmärgil, mille õnge läks kõigepealt üks töötaja, kelle kontot ära kasutades saadeti veel välja tuhandeid õngitsuskirju. Paari päeva jooksul avastati kümmekond kompromiteeritud kontot.

Niiviisi kompromiteeritud kontode puhul on esimeseks silmapaistvaks mõjuks see, et kompromiteeritud konto alt saadetakse välja uusi õngitsuskirju. Samas ei saa kuidagi välistada võimalust, et õngitsuskirjade taga olnud isikud said selle käigus juurdepääsu meilikontode tervele sisule. Oleme varem näinud taoliste lekkinud postkastide kaudu meilivestluste kaaperdamist, mille käigus üritati veel tükk aega hiljem välja petta lepingupartneritelt suuri rahasummasid.

Augustis nägime taas edukaid lunavararünnakuid Eesti ettevõtetele. Lunavarast teatasid meile ettevõtted, kes tegelevad näiteks mööbli, rõivaste ja toiduainete maaletoomise ja jaemüügiga, samuti metalliteenustega. Mitmel korral said rünnakud alguse arvutite kaugtöölauaprotokolli (*Remote Desktop Protocol* ehk RDP) teadaolevate nõrkuste ärakasutamisest.

Maailmas juba pikemalt levinud palgaandmete petuskeem jõudis augustis ka eesti keeles Eesti asutusteni: näiliselt palgatöötajalt personalijuhi või raamatupidaja aadressile saadetud kiri, mis palub edaspidi palgaraha kanda tavapärasest erinevale pangakontole. Meile pole ühestki edukast pettusest märku antud.

Tegevused küberturvalisuse parandamisel Eestis

Alates suvest oleme hakanud Eesti telekommunikatsiooniettevõtetele ja oma võrke haldavatele asutustele välja saatma automatiseeritud teateid kuritarvituste ja erinevate haavatavate seadmete/seadistuse kohta nende võrkudes. Tegemist on ülemaailmselt kogutud andmete põhjal töödeldud infoga, mis on oluline justnimelt võrkude omanikele.

Hetkel ei kogu CERT-EE andmeid haavatavuste kohta ise, vaid vahendab kolmandalt osapoolelt saadud infot nakatunud seadmetest ja haavatavustest otse võrkude haldajatele. Pikemas plaanis soovime infoallikaid laiendada ning seejärel hinnata, kas midagi olulist on jäänud kahe silma vahele ja kas peaksime CERT-EE poolt ka ise haavatavustest ja nakatumistest rohkem infot koguma hakkama.

21. augustil allkirjastas peadirektor Margus Noormaa memorandumi India Elektroonika ja Infotehnoloogiaministeeriumiga. Koostööleppe kohaselt hakkame India küberintsidentide lahendamise üksusega regulaarselt infot vahetama, üksteist nõustama ja abistama ning vajadusel eksperte vahetama. Rahvaarvu poolest suuruselt teises riigis maailmas on rohkem internetikasutajaid kui kogu Euroopas elanikke, mistõttu aitab taoliste otsekontaktide loomine kiiremini lahendada võimalikke ühiseid probleeme.

Augusti algul said valmis koolitusmaterjalideks mõeldud näidisvideod küberrünnakutest, mida võib kasutada küberhügieeni koolitustel näitlikustamaks seda, et küberintsidendid ei tähenda alati suuri ja mahukaid rünnakuid, vaid ka palju argisemaid teemasid. Kalastamist, andmeleket, teenustõkestusrünnakuid, näotustamist ja lunavararünnakut kirjeldavad videod on eestikeelsete ja venekeelsetena leitavad Youtube'ist.

Rahvusvaheline keskkond

Juulis ja augustis tunnistasid suured mitmed suured tehnoloogiafirmad, et on lubanud allhankefirmadel kuulata klientide privaatseid vestlusi. Google ja Apple ütlesid, et peatasid sellised töömeetodid. Hiljem kinnitas ka Facebook, et on kasutanud alltöövõtjaid, kes kuulaks ja paneks kirja kasutajate vestluseid nende teadmata ning on tegevuse samuti peatanud. Ka Microsoft nentis, et nemadki lasevad kuulata tõlketeenuste parendamise nimel kasutajate Skype'i vestlusi.

Ameerika Ühendriigid lükkasid taaskord edasi piiranguid Hiina tehnoloogiafirma Huawei toodete kasutamisele USA ettevõtete poolt, kuid lisasid keelunimekirja veel 46 Huaweiga seotud ettevõtet. Piirangute edasilükkamist on põhjendatud sellega, et USA ettevõtetel – sealhulgas maapiirkondades telekommunikatsiooniteenust pakkuvatel ettevõtetel – läheb arvatavast rohkem aega vaja oma tehnoloogiliste lahenduste ümbertegemiseks. Kuna keeld võib tähendada, et Huawei ei saa enam kasutada USA ettevõtte Google poolt välja töötatud Androidi operatsioonisüsteemi, teatas Hiina firma oma operatsioonisüsteemi HarmonyOS lansseerimisest.

Google'i tehnoloogid kirjeldasid augustis detailselt juba varem avastatud Apple'i telefonide kompromiteerimiseks mõeldud rünnakuid. **Mitu raportit hindab nende rünnakute sihtmärgiks olevat Hiina uiguuride vähemust** ning nende välismaal elavaid hõimukaaslasi.

Androidi veebipoes avastati 34 äppi, mis olid nakatatud Clicker Trojan pahavaraga ning mida olid kasutajad endale alla laadinud enam kui 100 miljonit korda. Pahavara tegutses telefonides taustal ning teenis raha taustal reklaamide avamisega. **Pahavara leiti veel ühel populaarsel Androidi rakendusel**, mis võis kasutajatelt raha välja petta. Ka sellel äpil oli enam kui 100 miljonit allalaadimist Google Play Store rakenduses.

Microsofti uurijad nägid, et kurikuulus Vene häkkerite grupp APT28 (tuntud ka Fancy Bear ja Strontium nime all) on hakanud otsima ligipääsu oma sihtmärkidele läbi IoT-seadmete (VOIP telefonid, printerid jne).

Prantsusmaa politsei küberüksus suutis üle võtta ja neutraliseerida umbes 850 000 seadmest koosneva robotvõrgustiku, mida kasutati näiteks lunavara laiali saatmiseks, andmete varguseks ja Monero krüptovaluuta kaevandamiseks.

Oleme Eestis ka mullu näinud suurt hulka *sextortion*-tüüpi väljapressimiskirju, mis ilma tõendusmaterjalita väitis, et on ohvrit veebikaamerast jälginud ajal, kui ta külastas pornograafilisi saite. **Prantsuskeelset maailma sihiti tänavu reaalse pahavarakampaania lainega**, mis nakatudes hakkaski salvestama ohvri veebikaamerat ajal, kui külastati taolisi lehekülgi, et salvestisi päriselt väljapressimises ära kasutada.