Riigi Infosüsteemi Amet

Trendid ja tähelepanekud küberruumis

Kvartaalne ülevaade, II kvartal 2020

Lunavararünnakute uus oht: andmevargus

OLUKORD

Ehkki lunavararünnakutest ei räägita enam nii palju kui 2017-2018 aastal, pole need kuskile kadunud. Viimaste kuude intsidendid kinnitavad, et ründajad on taktikat jõhkramaks muutnud: lisaks andmete krüpteerimisele need ka varastatakse ja ähvardatakse avalikustada.

Klassikalisel lunavararünnakul oli tavaliselt kolm sammu:

1. Ründaja paigaldab ohvri arvutisse või serverisse lunavara. Üha enam kasutatakse selleks turvanõrkustega kaugtöölauarakendust või murtakse sisse nõrkade või korduvkasutatud paroolide tõttu. Samuti levitatakse pahavara e-kirjaga saadetud failides.

2. Lunavara krüpteerib kas osa arvutites või serverites olevatest failidest või kõvakettad tervikuna. Pärast seda ei saa ohver enam faile avada.

3. Ründaja nõuab andmete taastamise ehk lahtikrüptimisvõtme eest lunaraha, enamasti mõnes krüptovaluutas (nagu Bitcoin).

Kuna organisatsioonid on üha enam saanud aru varundamise olulisusest ja kaitsevad oma andmeid paremini, ei maksa nad lunaraha, sest krüpteeritud andmed saab taastada ka ilma lahtikrüptimisvõtmeta. Sellest tulenevalt on lunavararünnakute läbiviijad lisanud neljanda sammu: esialgse sissetungi käigus andmed varastatakse ja ähvardatakse maksmata jätmise korral need avalikustada.

CERT-EEle on teada, et hiljuti tabas selline lunavararünne üht rahvusvahelist meditsiinisektori asutust (ei asu Eestis). Kui ohver keeldus dekrüpteerimisvõtme eest maksmast, teatasid ründajad, et avalikustavad rünnaku käigus varastatud andmed ning viisid selle ähvarduse ka ellu. Selle tulemusel lekkisid patsientide tundlikud isikuandmed, nagu nimi, sünniaeg, märkmed allergiate, testitulemuste jms kohta.

Andmevargus muudab lunavararünnaku keerukamaks ja aeglasemaks ning suurendab varase avastamise tõenäosust, kuid võimalus saada lunaraha ka varundust kasutavatelt organisatsioonidelt on sedalaadi rünnakute osakaalu kasvatanud. Prantsusmaa küberturbeagentuuri ANSSI hinnangul moodustavad andmevargust ja nende avaldamise ähvardust sisaldavad rünnakud ligi veerandi neile teadaolevatest lunavararünnakutest.

RIA HINNANG

Kõik asutused peaks lähtuma eeldusest, et lunavararünnaku korral nende seadmetes olnud andmeid mitte ainult ei krüpteerita, vaid üha kasvava trendina ka varastatakse ja avalikustatakse. Seetõttu ei piisa lunavararünnakute vastu võitlemisel andmete varundamisest.

Summad, mida kurjategijad välja pressivad, ulatuvad miljonitesse eurodesse. Tihti ajendab ohvreid maksma hirm Euroopa isikuandmete kaitse määrusega kaasnevate (GDPR) trahvide ees, kui organisatsiooni käsutuses olevad isikuandmed peaksid lekkima. Ka kurjategijad viitavad üha enam GDPRi rikkumiste trahvidele, et veenda ohvreid maksma.

RIA soovitused, kuidas end lunavararünnakute eest kaitsta, leiad SIIT. Varukoopiaid tuleks kindlasti jätkuvalt teha, kuid enam ei ole võimalik vaid niimoodi lunavararünnakute eest end kaitsta.

Eriolukorra tagajärg: uued kontod, vanad paroolid

OLUKORD

COVID-19 pandeemia takistamiseks kehtestatud eriolukorra tõttu kodutööle ja –õppele jäänud inimestel oli vaja kiirkorras mitmel platvormil uus konto luua. Harvemal juhul oli vaja kasutada vaid üksikuid uusi teenuseid, kuid mitmes kooliastmes käivate laste vanemate puhul oleme kuulnud ka kümnetest tööks ja õppimiseks vajalikest uutest kontodest.

Praktika näitab, et uute kontode salasõnade erilisuse mõtlemise peale ei pühendata piisavalt aega ning käiku lähevad juba mujal kasutusel olevad salasõnad (seda kinnitab ka Google 2019. aastal USA-s läbiviidud uuring, kust ilmneb, et 65% inimestest kasutavad sama salasõna enda mitmel või kõigil kontodel). See aga tähendab, et kui parool ühe keskkonna kaudu lekib, satuvad automaatselt ohtu ka kõik teised sama parooliga justkui kaitstud kontod.

Ulatuslikke andmelekkeid näeme aga pidevalt ning igal pool, alates lennufirmadest kuni laste virtuaalmängutubadeni välja. Tõenäoliselt sattus Briti lennufirma Easyjeti mais avalikustatud andmelekke tulemusel ohtu ka mitmete Eesti elanike isiku- ning pangateave. Olgugi, et andmete vargusi leiab aset üsna tihti, on inimeste käitumine küberruumis jätkuvalt riskialdis – üks peamistest riskidest on siinkohal salasõnade korduvkasutamine eri platvormidel.

RIA HINNANG

Rõhutame, et tugev salasõna on oluline osa küberhügieenist ning soovitame kõigil võtta hetk ning veenduda enda paroolide kaitstuses. Kui eriolukorras oli prioriteetne olukorraga kohaneda ja erinevate veebikeskkondadega harjuda, siis nüüd võiks oma edasised internetiharjumused rahulikult läbi mõelda, kontod korrastada ja nende kasutamine turvalisemaks muuta. Käepärast võiks siinkohal olla RIA soovitused turvalise kasutajakonto loomiseks. Kuivõrd paljud ettevõtted kiirendasid eriolukorra kontekstis äri veebi kolimise protsessi ning müüvad kodulehe kaudu teenuseid, siis on asjakohane ka üle vaadata meelespea teenuseosutajale.

Nii mujal maailmas kui Eestis näeme ka seda, et lekkinud salasõnu ja varastatud andeid ei realiseerita sageli kohe, vaid alles mitme kuu, vahel isegi pikema aja möödudes. Seega ei pruugi kasutajad teadlikudki olla, et nende kasutajaandmed on lekkinud ja isiklikud andmed ning kontod ohus.

Küberhügieeni mõistes on kindlasti turvalisem kasutada iga konto jaoks eraldi parooli ning kasutada olulisemates ning tundlikuma infoga keskkondades lisaks kaheastmelist autentimist. Erinevate salasõnade haldamiseks võib võtta kasutusele paroolihalduri ehk spetsiaalse tarkvara (neid on mitmeid, tuntumatest näiteks KeePass, LastPass või 1Password).

Teenusetõkestusrünnete oht püsib

OLUKORD

Aprillis ja mai alguses nägime tavapärasest rohkem teenusetõkestusründeid (DDoS) Eesti veebisaitide vastu. Neid toimus kokku kümmekond, kestvusega mõnest minutist kuni ligi ööpäevani. Pikemad rünnakud toimusid kahe finantsettevõtte vastu, mille tulemusel oli mõlema ettevõtte veebilehe kasutamine klientide jaoks häiritud terve tööpäeva vältel. Lühemaajalisi ründeid toimus transpordisektori, avalike teenuste ja elutähtsate teenuste osutajate veebilehtede vastu.

Ehkki lühiajaliste rünnete puhul suudeti teenused kiiresti taastada, põhjustas näiteks pooletunnine teenusekatkestus laialt kasutatavas e-õppekeskkonnas eriolukorra tingimustes ligi kümnele tuhandele kasutajale siiski üksjagu ebamugavust.

Ehkki erinevad teenusetõkestusründeid toimub pidevalt, pälvisid teise kvartali rünnakud meie tähelepanu kahel põhjusel. Esiteks toimus neid lühikese aja (ligikaudu nelja nädala) jooksul tavapärasest rohkem ning kuna tegemist oli ka eriolukorraga, mil inimesed kasutasid kõikvõimalikke e-teenuseid rohkem, oli mõnedel rünnakutel ka tavapärasest suurem mõju. Teiseks oli mõnede rünnete käekiri sarnane: teostati HTTP Get päringuid, ründajatel oli sama või sarnane kasutajaagent ning rünnete objektiks olid Eestis palju kasutatud ja olulised veebilehed.

RIA HINNANG

Antud juhtumite põhjal ei saa teha piisavalt järeldusi rünnete eesmärgi või ründaja kohta, küll aga näitab see, et teenusetõkestusrünnete ohtu tuleb jätkuvalt võtta väga tõsiselt. Rünnete läbiviimiseks kasutatakse tavapäraselt kas robotvõrgustikke (botnetid) või kompromiteeritud seadmete võrgustikke ning antud ründelaine puhul tuvastas CERT-EE, et mõnedel juhtudel kasutati kompromiteeritud Miktrotiki ruutereid üle maailma (sh Eestis). Kompromiteerumist saanuks ilmselt ära hoida, kui oleks õigel ajal uuendatud ruuteri tarkvara – seetõttu ei väsi me kordamast vajadust uuendada regulaarselt kõikide internetti ühendatud seadmete tarkvara.

Maailmas üldiselt näib teenusetõkestusrünnete trend käesoleval aastal olevat tõusuteel nii arvuliselt kui ka oma mõju poolest. Lisaks seni teada haavatavustele nii tarkvaras kui riistvaras leitakse pidevalt ka uusi, mille kaudu neid läbi viia. Nii näiteks jõudis maikuus avalikkuseni lisraeli teadlaste avastus haavatavusest ülemaailmses domeeninimede lahendamise teenuses (DNS), mille kaudu on potentsiaalselt võimalik suhteliselt väikse seadmete arvuga viia läbi väga suure võimendusefektiga ründeid. Täpsemalt loe RIA ohuhinnangut siit.

Vähem müra, selgem ohupilt

Kavatseme olulise muuta küberintsidentide arvu kajastamist statistikas. Alates käesoleva aasta juulist lõpetame robotvõrgustikega Avalanche ja Necurs nakatumiste kajastamise CERT-EE intsidentide loetelus. Avalanche'i robotvõrgustik peatati rahvusvahelise politseioperatsiooni tulemusel 2016. aasta detsembris (kuid nakatumised jätkusid hiljemgi), Necursi võrgustiku sai Microsoft enda kontrolli alla 2020. aasta märtsis. Seega võib hinnata, et need kaks võrgustikku enam aktiivselt küberruumi ei ohusta.

Nende kahe võrgustikuga nakatumised on 2017-2019. aastal moodustanud ca 95% kõigist meie robotvõrgustikuga nakatumiste intsidentidest ning kuna me saame ja saadame neid teavitusi välja mõnikord mitu korda ööpäevas, siis moodustavad need ca 60% kõigist intsidentidest üldse.

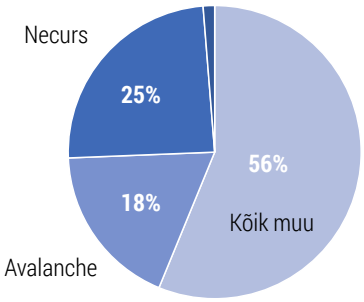
See ei tähenda, et me enam nende nakatumistega ei tegeleks. Vastupidi – CERT-EE saadab üha tihedamini ja üha rohkem teavitusi välja robotvõrgustike (ja muu pahavaraga) nakatumiste kohta. Alates 2019 suvest on CERT-EE hakanud Eesti telekommunikatsiooniettevõtetele, veebiteenuste majutajatele ja oma võrke haldavatele asutustele välja saatma automatiseeritud teateid erinevate haavatavate seadmete / seadistuste kohta nende võrkudes. Automatiseeritus tähendab seda, et meie serverid saavad masinloetava info kätte usaldusväärselt allikalt, kes on loonud endale taristu haavatavuste ja nakatumiste tuvastamiseks üle terve maailma. Meie süsteemid jagavad info automaatselt edasi Eesti internetiruumis toimetavatele võrkude omanikele. Hetkel jõuab CERT-EEni info ca 3000 nakatumise kohta ööpäevas, mis mõjutab enam kui 700 serverit ja arvutit. Mõne seadme puhul on nakatumine olnud mitme pahavaraga korraga.

Automatiseeritud lahendused

Mida rohkem taolisi allikaid me oma süsteemidesse integreerime, seda paremat pilti haavatavustest ja nakatumistest me Eesti IP-ruumi klientidele suudame pakkuda. Samas tähendab see ka teavituste tiheduse kasvu, mille ükshaaval statistikas kajastamine ei aita kaasa ohupildi selgemaks saamisele. Näiteks mai keskpaigast juuni keskpaigani oleme teada saanud ja seega ka teenusepakkujaid teavitanud 103 000-st nakatumisest. Numbreid analüüsides aga on näha, et ca 86 000 nendest olid seotud vaid kolme IP-aadressiga ja kokku teame 1701-st erinevast pahavaraga IP-aadressist. Paljud korduvad, paljud nakatumised on samuti seotud juba neutraliseeritud pahavarataristuga, seega ei anna need numbrid statistikas nii palju selgust juurde.

Avalanche' ja Necurs nakatumiste kajastumise muutus hakkab esialgu silma paistma järsu intsidentide langusena (hinnanguliselt 50 – 60%), aga muudatuse tulemusel kajastab meie intsidentide statistika tegelikku ohupilti selgemalt. Kokkuvõtteid robotvõrgustikest plaanime teha ka edaspidi, aga teistmoodi, näidates nakatumiste trende üle teatud aja ning keskendudes nende dünaamikale.

2020. aasta CERT-EE registreeritud intsidendid



2020. aastal on Necurs ja Avalanche nakatumisteated moodustanud 97% kõigist robotvõrgustike intsidentidest ja 43% üldse kõigist CERT-EE registreeritud intsidentidest.

LÄHEB HÄSTI:

Ehkki märtsi keskpaigast kuni mai keskpaigani kestnud eriolukord pani nii e-teenuste kasutajad kui teenusepakkujad suurema pinge alla ning rahvusvahelised küberkurjategijad olid virgad COVID-19 temaatikat oma huvides ära kasutama, ei toonud see kokkuvõtteks Eesti jaoks kaasa tavapärasemast rohkemaid või suurema mõjuga küberintsidente. Jäime puutumata üksikuid Euroopa riike tabanud suunatud rünnetest meditsiinisektori vastu ning ka suurt rahalist kahju põhjustanud COVID-19 teemalistest petuskeemidest.

SAAKS PAREMINI:

30. juunil lõppes Magento tarkvara tugi versioonidele 1x, mis on Eestis väga laialt kasutusel olev kodulehtede ja e-poodide platvormi tarkvara. CERT-EE hinnangul kasutab ligikaudu kolm neljast Eesti e-poest Magento tarkvara ning turvalise kauplemise jätkamiseks on vaja üle minna uuele versioonile 2x. CERT-EE saatis mais teenusepakkujatele ka vastava teavituse. Juuli alguse seisuga ei ole aga paljud seda siiski teinud, sealhulgas toidu- ja esmatarbekaupu tarnivad e-poed. See aga tähendab, et ohtu võivad sattuda klientide krediitkaardiandmed. Kuna häkkerid on Magento varasemaid turvanõrkusi mujal maailmas edukalt ekspluateerinud, on probleemile tähelepanu juhtinud ka Visa ja Mastercard.

Käesoleva kokkuvõtte koostas RIA küberturvalisuse teenistus eesmärgiga selgitada küberohtude trende võimalikult laiale auditooriumile, sealhulgas lugejatele väljaspool Eestit. Olukorda küberruumis analüüsib RIA küberturvalisuse teenistus detailsemalt igakuistes kokkuvõtetes. Tehnilisemaid soovitusi jagab CERT-EE koolitustel ja RIA kodulehekülje kaudu.