



# Trendid ja tähelepanekud küberruumis

III kvartal 2022

## 1. Ummistusrünnete hulk kasvas ning sihti ka meediakanaleid

### OLUKORD

See on teine järjestikune kvartaliülevaade, milles me ei saa üle ega ümber Eesti ettevõtete ja asutuste vastu suunatud teenusetõkestusrünnetest (DDoS). Kui tavapärase tase on kümnekond märkimisväärset ummistusrünnet kuus, siis augustis registreerisime neid 65 ja septembris 31.

Suurim rünnakuline algas 16. ja lõppes 19. augustil. Nende nelja päeva jooksul rünnati 27 sihtmärki, mitut neist korduvalt. Ründajate tavapärastele „lemmikutele“ valitsus.ee, president.ee, eesti.ee, politsei.ee, id.ee, lisandusid sel korral finants- ja transpordiettevõtted. Rünnete mahud olid kohati suured: näiteks pandi id.ee vastu suunatud ummistusrünnakute tipphetkel teele enam kui 80 000 pahatahtlikku päringut sekundis.

Kaitsemeetmed, mis päätsid meid halvima aprillikuise DDoS-laine ajal, tegid seda ka augustis. Enamikul rünnakutel polnud mõju, kuid mõnel juhul tekitasid need siiski probleeme. 16. augustil pol-

nud rohkem kui tunni jooksul kättesaadav Maksu- ja Tolliameti veebileht emta.ee ning 17. augustil nägime lühiajalisi katkestusi SK ID Solutionsi teenustes, millest sõltuvad ID-kaadi, mobiil-ID ja Smart-ID toimimine.

Järgmine pahatahtlike päringute „laviin“ püüdis Eesti küberruumi ummistada 26. augustil, mil rünnati kümnet sihtmärki. Uute sihtmärkidena püüdsid ründajad sel korral maha võtta ka Eesti meediaportaale. Mõneks ajaks see neil ka õnnestus – 26. augusti hommikul olid rivist väljas Õhtulehe, Postimehe ja Ekspress Grupi veebiväljaanded.

September oli augustiga võrreldes rahulikum, kuid keskmisega kõrvutades siiski kordades aktiivsem ummistusrünnete kuu. Lisaks mainitud sihtmärkidele tõi õppeasat algus mõned rünnakud koolide vastu.

Tallinnas toimunud küberõppusega Locked Shields, siis augusti keskpaiga DDoS-kampaania algas samal päeval, mil Narvas teistsaldati punamonumente. Võimalike ajendite ritta võib lisada augustis kehtestatud sissesõidupiirangu Schengeni viisaga Venemaa kodanikele ja Eesti jätkuva toetuse Ukrainale. Olulist ega pikaajalist kahju ei õnnestunud ründajatel meie e-teenustele siiski tekitada.

Pole põhjust arvata, et olukord Eesti küberruumis lähikuudel rahuneb või et ummistusrünnete hulk oluliselt väheneks. See seab kõrgemad nõudmised nii RIA-le kui ka teistele e-teenuste osutajatele. Kui soovid infot, kuidas end teenusetõkestusrünnete eest kaitsta, loe vastavat [juhendit](#) või kirjuta [cert@cert.ee](mailto:cert@cert.ee).

### RIA HINNANG

Kui aprillis Eesti vastu suunatud ummistusrünnete laine oli tõenäoliselt seotud

## 2. Petukirjad politsei nimelt

### OLUKORD

Möödunud kvartalis saime väga palju teavitusi inimestelt, kes olid saanud ootamatu e-kirja politsei nimelt, koos manusega. Kirja teemareal oli sageli „Konvokatsioon nr ....“ ning kirjas informeeriti saajat menetluse alustamisest seksuaalkuritegude toimepanemise, lapsporno omamise ja muu taolise eest. Vahel oli kiri vormistatud kohtukutsena. Kirja saajal paluti 48h jooksul saata oma põhjendused kirjas olevale e-posti aadressile. Inimesele kinnitati, et politseil on ülevaade tema arvutis toimuvast ning kirjale mitte reageerimisel järgneb „viivitamatu vahistamine“ ning toimepandud tegude avalikustamine. Ainuüksi augustis saime ligi sadakond teavitust selliste kirjade kohta.

### RIA HINNANG

Tegemist on järjekordse variatsiooniga petukirjadest, mille eesmärk on andmepüük ja inimestelt raha välja petmine. Üldiselt toimib see nii,

et kui inimene kirjas toodud meilile kirjutab, saab ta edasised juhised, kuidas kohtumenetluse vältimiseks on võimalik maksta „trahv“ ja süüdistusest vabaneda, võidakse küsida ka inimeste isikuandmeid. Kirjad olid eestikeelsed ja ametliku ilme lisamiseks oli kasutatud korrakaitseorganite võltsitud logosid, samuti oli kasutatud Eesti õigussüsteemiga päriselt seotud või seotud olnud inimeste nimesid. Samasuguse ülesehitusega kirju levib ka teistes riikides, nt Prantsusmaal ja Leedus; tegemist on rahvusvahelise skeemiga, mida kurjategijad üritavad tõlkeprogrammide ja muu tehnoloogia abil kohalike oludega sobitada.

Nii nagu petukirjades sageli, püüti inimesi hirmutada ja sundida kiirelt tegutsema (kirjale vastama). Lisaks veidrale ja ebaloomilisele sisule on kirjades aga muidki pettusele viitavaid tunnuseid: ebaloomulik keelekasutus, ametiasutuste ebakorrektsed nimed, ebausutav meiliaadress, millele tuleb vastata jne.

Ootamatute kirjade puhul, mis näivad millegi poolest kahtlased, soovime:

- Kui pead võimalikuks, et tegemist on siiski ehtsa kirjaga, helista saatjale (nt asutuse infotelefonile) ja küsi üle.
- Ära ava manuseid ja ära vasta kirjale. Vastates kinnitad muuhulgas oma e-posti kehtivust ja võid ka tulevikus petukirju saada.
- Ära kliki kirjas olevatel linkidel – suure tõenäosusega on nende taga (ametiasutusi matkivad) õngitsuslehed, mille kaudu küsitakse sinu isikuandmeid.
- Kustuta kiri oma postkastist.

### 3. Kolm Eestis levivat pahavara

#### OLUKORD

Pahavarasid liigub internetis palju – üks funktsionaalsem kui teine. Räägime kolmest Eestis levinud pahavarast, mis on nende peamine eesmärk ja kuidas neid levitatakse.

**Formbook** – see pahavara suudab salvestada nakatunud süsteemis kasutaja klahvivajutusi, teha kuvatõmmiseid või varastada salvestatud kasutajatunnuseid veebilehitsejatest. Seda jagatakse ohvritele peamiselt pahaloomuliste e-kirjade manuses. Kui manus avada ja pahavara käivitada, seostab see enda pahaloomulise koodi mingi operatsioonisüsteemi protsessiga. Formbooki on kasutatud maailmas erinevate tööstussektori sihtmärkide vastu – nt kaitse- või kosmose-tööstuse sihtmärkide peal, samuti sel aastal Ukraina sõjas erinevate Ukraina organisatsioonide vastu. RIA täheldas, et lõppenud kvartalis jagati seda näiteks kirjadega, mille pealkiri sisaldas sõna “arve” koos hulga erinevate numbritega. Kaaskiri ütles, et kirja saajale on saadetud tellimuse arve. Manusesse oli lisatud Formbooki sisaldav Exceli fail.

**Lokibot** – Nagu Formbooki, kasutatakse Lokiboti-nimelist pahavara andmete varastamiseks nakatunud süsteemidest. See suudab varastada nii kasutajatunnu-

seid veebilehitsejatest, meiliklientidest kui ka teistest populaarsematest tarkvaradest. Tavaliselt üritatakse nakatada seadmeid, mis kasutavad Windowsi või Androidi operatsioonisüsteeme. Eesti inimestele on Lokiboti pahavara üritatud sokutada näiteks e-kirjadega, mille teemareal on „Hinnapäring” ning mis tulevad näiliselt Eesti ülikoolide töötajatelt. Manuses on tavaliselt arhiveeritud fail (nt .rar või .zip), mille sees on omakorda pahaloomuline EXE fail.

**Agent Tesla** – see on üks enim jagatud pahavarasid maailmas ja erinevaid näidiseid näeme ka Eestis. Seda levitatakse samuti e-kirjade teel ja see on võimeline enda tõelisi eesmärke suhteliselt edukalt varjama. Kui pahavara on käivitunud, otsib see esmalt süsteemist veebilehitsejaid, kust oleks võimalik erinevaid kasutajatunnuseid varastada. Samuti suudab see pahavara salvestada klahvivajutusi või teha kuvatõmmiseid. Eestis levitatakse AgentTesla pahavara tavaliselt ingliskeelsete kirjadega, mille pealkirjast leiab viiteid väljamõeldud tellimusele või arvele (nt purchase order või proforma invoice). Manusteks on kasutatud erinevaid failitüüpe, nt Wordi, Exceli või Powerpointi faile.

#### RIA HINNANG

Kuigi need pahavarad ilmusid aastaid tagasi, kasutavad küberkurjategijad erinevaid versioone tänini. Ka Eesti küberruumis liigub neid palju ja on päevi, kus pahavara püüab levida eriti intensiivselt. Näiteks ühel septembri päeval üritati Agent Tesla pahavaraga pahaloomulisi kirju saata ligi tuhandele erinevale meiliaadressile. Ehkki suure osa neist peavad kinni viirusetõrjeprogrammid ja meilifiltrid, on sellise massi puhul tõenäoline, et osa kirju ikka adressaadini jõuab ja osa manuseid ka avatakse. Kuidas end pahavarade eest kaitsta:

- Ära ava kahtlaseid kirju või linke, mis tulevad tundmatutelt saatjalt. Kui kahtled kirja eesmärkides, soovitage saata selle originaalkujul ülekontrollimiseks CERT-EE meiliaadressile [cert@cert.ee](mailto:cert@cert.ee).
- Veendu, et operatsioonisüsteemis oleks toimiv viirusetõrjetarkvara.
- Kasuta CERT-EE Encrypted DNSi rakendus. See blokeerib meile teadaolevat pahavara ja õngitsusi ning filtreerib kasutaja eest pahatahtlikke linke. Täpselt saab rakenduse kohta lugeda [siit](#).
- Tutvu ka RIA blogis sel suvel avaldatud [juhendiga](#), kuidas pahaloomulisi kirju ära tunda.

### Eurooplaste nutividinad on tulevikus turvalisemad

#### OLUKORD

Igal sekundil saab maailmas mõni asutus või ettevõtte pihta küberrünnakuga. Eeskätt just ummistusrünnete puhul – veebilehe või teenuse üle ujutamine päringutega, et see muutuks töövõimetuks – kasutatakse sageli ära tavaliste inimeste igapäevaseid nutiseadmeid. Nii võib näiteks inimese enda teadmata tema arvuti, telefon, nutikas külmkapp, ruuter või muu võrku ühendatud seade osaleda küberrünnaku tegemises. Selleks on häkker mingil ajahetkel leidnud võimaluse vidinat pahavaraga nakatada, et selle jõudu võimsamate rünnete tegemiseks ära kasutada. Enamasti pääsevad pahalased nendele seadmete ligi, kui need on uuendamata tarkvaraga või hooletult arendatud.

Just selle probleemi lahendamiseks tegi Euroopa Komisjon ettepaneku uueks regulatsiooniks, mis sai nimeks küberkerksuse õigusakt (ingl k Cyber Resilience Act). Uue ettepaneku järgi peaksid kõik nii ELis toodetud kui ka siin müüidavad di-

gitooted – tarkvara ja riistvara – vastama teatud kõrgetele küberturvalisuse nõuetele. See hõlmaks pea kõiki digitooteid, sh arvuteid, nutitelefone, nutikellasid, laste mänguasju jpm.

Näiteks näeb ettepanek ette security-by-design printsiibi rakendamist, mis tähendab, et juba toote arendamisel tuleb järgida teatud küberturvalisuse nõudeid. Samuti on ettepanekus välja toodud security-by-default kontseptsioon, mille puhul peaks turul müügis olev toode juba vaikimisi olema kõige turvalisemate sätetega (nt automaatsed uuendused). Lisaks peaks tootja andma kasutajale kaasa juhised, kuidas toodet küberturvaliselt kasutada.

#### RIA HINNANG

Inimeste igapäevaseks kasutatavate nutiseadmete hulk järjest kasvab ja nende küberturvalisus vajab ka meie hinnangul senisest rangemat regulatsiooni. CERT-EE automaatseire tuvastab iga päev üle 100 pahavaraga nakatunud seadme Eesti küberruumis, mis võivad teha palju pahan-

dust omaniku teadmata. Seetõttu tervitame Komisjoni ettepanekut probleemiga tegeleda ehk muuta inimeste nutividinad ja kogu küberruum turvalisemaks.

Vastu võtmise korral saab taolise õigusakti mõju olema suur ja teedrajav. Lisaks digitoodete tootjatele, maaletoojatele ja turustajatele lisanduvad ettepaneku järgi kohustused ka turujärelevalve ja küberturvalisusega tegelevatele riigiasutustele. Muuhulgas tekiks võimalus digitoode – näiteks mõni mobiiltelefoni mudel – turult üldse tagasi kutsuda, kui see küberturvalisuse nõuetele ei vasta.

Õigusakti jõustumiseni on veel omajagu aega, praegu on Komisjon teinud alles ettepaneku sel teemal läbirääkimiste alustamiseks. Nüüd hakkavadki liikmesriigid kokku leppima regulatsiooni ulatuse, sisu ja detailide osas. Eesti üldiselt toetab ambitsioonikat lähenemist küberturvalisusele, ent peame ettepaneku mõjusid veel analüüsima ja seisma hea selle eest, et soovitud tulemus ka praktikas tõhusalt välja kukuks.

#### LÄHEB HÄSTI: ↗

Raadio 4 eetris läbi lõppenud suve väldanud küberturvalisuse saatesari „Введи пароль” („Sisesta parool”) osutus üle ootuste populaarseks. 13-osalise saatesarja iga episoodi kuulas otse-eetris ca 43 000 inimest, saadete järelkuulamise võimalust kasutas enam kui 1500 inimest.

Saatesarja kaudu teavitati kuulajaid ohtudest ja murekohtadest küberruumis ning isiklikust vastutusest küberintsendentide ennetamisel ja tagajärgedega tegelemisel. Saatesari on järelkuulata [ivaatlik.ee/venekeelsel-lehel](http://ivaatlik.ee/venekeelsel-lehel).

#### SAAKS PAREMINI: ⚠

Tänavu oleme registreerinud kokku 17 lunavararünnet: keskmiselt kaks korda kuus saab mõni asutus või ettevõtte lunavaraga pihta. Eelmises kvartalis nägime juhtumit, kus üks ja sama ettevõtte sai lunavararündega pihta juba teist korda paari kuu jooksul. Ehkki andmed õnnestus mõlemal korral varukoopiast taastada, takistas rünnak mitme tunni jooksul ettevõtte tavapärasest tööd. Enamus lunavararünnakuid sooritatakse endiselt kaugtöölaua protokoll (RDP) kaudu, mistõttu soovitate lugeda RIA [ohuhinnangut](#), kus anname nõu RDP-ühenduse turvamiseks. Ühtlasi tuleb meelde, et elementaarne küberhügieen on oluline ka siis, kui tagavarakoopiad on olemas.

**Kokkuvõtte lõi RIA küberturvalisuse teenistus, et selgitada küberohtude trende 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.**