VENEMAA KÜBERLUURE OHUSTAB EESTI JA KOGU LÄÄNE JULGEOLEKUT

Venemaa eriteenistused kasutavad aktiivselt küberruumi teabe kogumiseks, korraldades selleks küberluureoperatsioone.

Küberluure on osa Venemaa eriteenistuste tavapärasest tööst, mistõttu ei pruugi nende tegevus olla alati reaktsioon geopoliitilisele sündmusele.

Tänu Venemaa eriteenistuste küberluure edukale tegevusele on Kremlil tõenäoliselt hea arusaam Lääne plaanidest ja haavatavusest.

Võrreldes teiste riikide tegevusega kujutab Venemaa küberluure endast suurt ohtu, kuna Venemaa eriteenistustel (VET-il) on küberoperatsioonide sooritamise pikaajaline kogemus, nad otsivad pidevalt uusi nutikaid viise infosüsteemidesse sissemurdmiseks, pahavara arendamiseks, oma tegevuse varjamiseks (kuigi rakendatakse ka edukalt töötavaid võtteid, mida on varem kasutatud), panustavad ressurssi küberründe võimekusse ning on suutelised operatiivselt oma vigadest õppima, muutma oma ründevõtteid, vahetama välja paljastatud ründetaristut jmt.

NÄITEID 2021. AASTAL AVALIKUSTATUD VENE ERITEENISTUSTE KÜBEROPERATSIOONIDEST

- Aastail 2019–2021 Venemaa välisluureteenistuse (*Služba vnešnei razvedki RF*; SVR) küberluureoperatsioon. SVR sai USA ettevõtte SolarWinds kaudu ligipääsuvõimaluse kümnete tuhandete sihtmärkide infosüsteemidesse. Ründes kasutati teisigi teenuseid. Peamiselt varastati andmeid USA-st. Täpne mõju senini teadmata.[1]
- Aastail 2017–2020 Venemaa sõjaväeluure (*Glavnoe (razvedõvatelnoje) upravlenie Generalnogo štaba Vooružjonnõh Sil RF*; GRU) küberoperatsioon Prantsusmaal.[2]
- Aastail 2017–2021 Venemaa mõjutustegevus Euroopas.[3]
- Aastail 2019–2021 GRU ulatuslik küberluureoperatsioon. Püüti ära arvata tuhandete sihtmärkide kasutajaparoole Microsofti teenustes. Sihtmärke oli nii avalikus kui ka erasektoris.[4]
- 2021. aastal Venemaa Föderaalse Julgeolekuteenistuse (*Federalnaja služba bezopasnosti RF*; FSB) küberluureoperatsioonid Ukrainas.[5]
- 2021. aastal SVR-i korduvad õngitsuskampaaniad Läänes.[6]

1 http://cisa.gov/uscert/ncas/alerts/aa21-116a
2 http://cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-005
3 http://consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes
4 http://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
5 http://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy
6 http://cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf

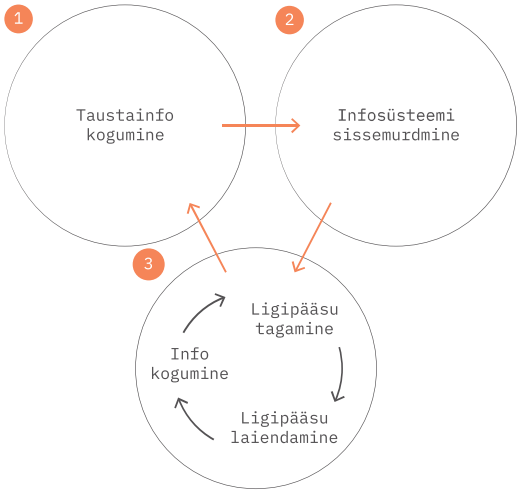
Teisalt ei suuda VET-i sihtmärgid endiselt oma küberturvalisust piisavalt tagada ning tegelevad sellega pigem pärast oluliste tagajärgedega küberoperatsiooni. Seniste küberoperatsioonide põhjal võib öelda, et sihtmärgid ei mõista vajadust järjepidevalt oma küberturvalisust hoida ning selleks ressursse eraldada.

VET-i tegevuse tõttu on Kremlil tõenäoliselt hea ülevaade Lääne arusaamadest, olukorra tõlgendustest ja muredest, ning otsustajad saavad VET-ilt viiteid, kuhu ja millist survet avaldada, selleks et oma välispoliitilisi eesmärke saavutada.

VENE ERITEENISTUSTE KÜBERLUUREOPERATSIOONIDE ETAPID

Järgnev kirjeldus Vene eriteenistuste küberluureoperatsioonide etappidest näitab lihtsustatult VET-i kübervõimet ning ei pruugi olla omane kõigile VET-i küberründe võimega keskustele.

Vene eriteenistuste küberluureoperatsioonide etapid



1. **Taustainfo kogumine**

   Sihtmärgi enda ja tema kasutatud seadmete ja infosüsteemide kohta taustainfo kogumine. Kogutu põhjal otsustavad Vene eriteenistused, kuidas sihtmärki rünnata.

2. **Sissemurdmine**

   Vene eriteenistuste tüüpilisimad viisid sihtmärgi infosüsteemi sissemurdmisel on:

   - õngitsuskirjade saatmine[1]
   - kaevurünne[2]
   - turvanõrkuse ärakasutamine
   - pahavaraga nakatatud irdmeedia[3] vmt kasutamine

3. **Ligipääsu laiendamine ja tagamine ning teabe kogumine**

   Kui Vene eriteenistused on arvutivõrku edukalt sisse murdnud[4], siis püüavad nad kaardistada teisi seadmeid arvutivõrgus. Eesmärk on saada kõige kõrgemates õigustes ligipääs kogu arvutivõrgule. Kui see on saavutatud, siis on peaaegu võimatu Vene eriteenistusi oma arvutivõrgust välja tõrjuda.

   Paralleelselt ligipääsu laiendamisega püüavad Vene eriteenistused paigaldada sihtmärgi arvutivõrku n-ö tagauksi, juhuks kui esialgne sisenemiskoht peaks mingil põhjusel ära kaduma. Kui tagavarasissepääsud peaksid kaduma, siis alustatakse uut küberluureoperatsiooni.

   Kolmanda paralleelprotsessina koguvad Vene eriteenistused varjatult sihtmärgi infosüsteemist infot, mis on küberluureoperatsiooni põhieesmärk.

   Selleks, et arvutivõrku sisse murdnud Vene eriteenistustest lahti saada, tuleb arvutivõrk sageli uuesti üles ehitada.

1 Vaata ründe kirjeldust 2019. aasta Välisluureameti aastaraamatust
2 Vaata ründe kirjeldust 2020. aasta Välisluureameti aastaraamatust
3 Irdmeedia alla kuuluvad näiteks USB-pulgad, välised kõvakettad jne
4 Meilikontosse sisse murdes käituvad VET-id sarnaselt – püüavad kindlustada oma ligipääsu ning koguvad infot (lisaks meilidele ka kasutajate andmeid). Kui meilikonto ise huvi ei ole paku, siis kasutavad VET-id seda järgmiste sihtmärkide ründamisel, nt edastades õngitsuskirju selle meilikonto kontaktisikutele

Oluline on meeles pidada, et suur luureväärtus on peale riigisaladuse ka asutusesiseseks kasutamiseks mõeldud infol, mis ei ole samaväärse tugevusega kaitstud kui riigisaladus. Piisavas koguses asutusesiseseks kasutamiseks mõeldud info valdamine võib kokkuvõttes olla sama palju väärt kui ligipääs riigisaladusele.

Venemaale väärtuslikku infot sisaldavad ka nt asutusesiseseks kasutamiseks mõeldud memod, kust võib saada infot riigiasutuste koostöö, seisukohtade kujundamise, olukorra tõlgenduste jpm kohta.

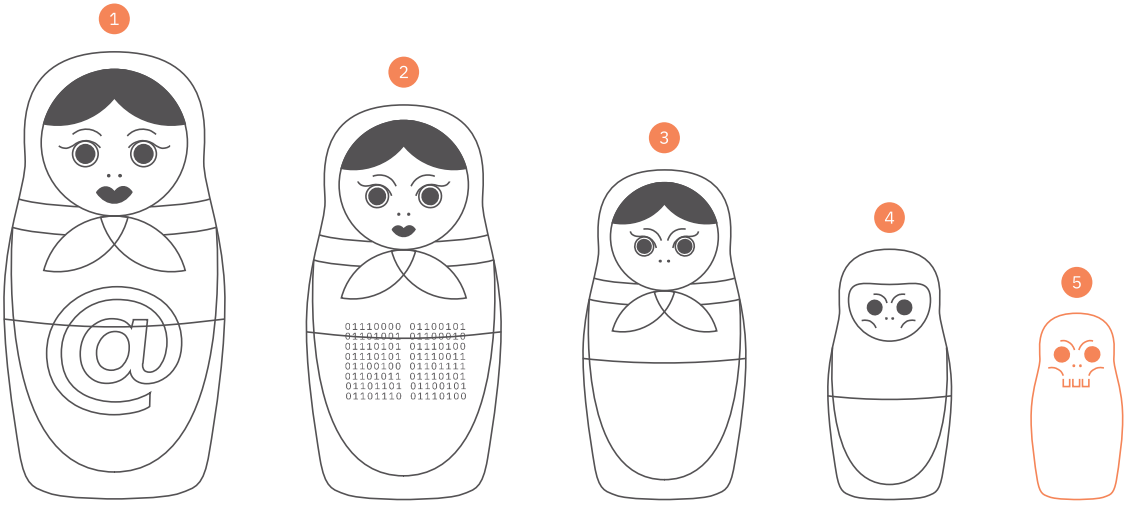
Küberluureoperatsioon on valdavas osas automatiseeritud protsesside jada. Manuaalselt kontrollitakse näiteks seda, kas ründe ohvriks langenud isiku seadmetes asuv info ja isik ise on huvipakkuvad. Kui nad huvi ei paku, siis kustutab VET pahavara infosüsteemist ära või kasutab seda teiste sihtmärkide ründamiseks. Enamasti püüab VET mitmesuguste võtetega oma tegevust varjata – nt kasutatakse ründamisel ja info kogumisel kolmandate osapoolte seadmeid, pahavara jaotatakse väiksemateks osadeks, mis laetakse sihtmärgi infosüsteemidesse eri asukohtadest jm.

MIS JUHTUB PÄRAST SISSEMURDMIST?

Venemaa eriteenistused kasutavad küberoperatsioonides palju eri pahavarasid. Kõrval asuval joonisel kirjeldame üht operatsiooni, mida nägime endise riigiteenistuja isiklikuks kasutamiseks mõeldud arvutis. Sissemurdmine toimus tõenäoliselt siis, kui teenistuja oli avanud manuse õngitsuskirja juures. Manuses asus vaid esialgne osa pahavarast. Teised osad laeti arvutisse eri kohtadest internetis. Pahavara osade saabumist võib vaadelda kui matrjoškat. Iga nukku avades käivituvad seal asuvad failid, mis toovad kohale uue osa pahavarast ning täidab talle mõeldud eriülesande. Kui kogu pahavara on arvutisse paigaldatud, siis jätkub korrapärane info liigutamine VET-i kontrollitud serverisse.

Välisluureameti hinnangul Venemaa eriteenistused jätkavad lähi- ja kaugemas tulevikus küberluureoperatsioone nii Eesti kui ka teiste lääneriikide suunal. See on sissetöötatud ja tõhus viis info kogumiseks. Seega Venemaalt lähtuv küberoht jääb püsima, kuid seda on võimalik vähendada, rakendades küberturvalisust tagavaid meetmeid.

Vene eriteenistuste küberluureoperatsioonide etapid



1. **Õngitsuskiri**

   Õngitsuskirja manusele klikates paigaldub sihtmärgi arvutisse vaid üks osa pahavarast, teised osad laetakse alla eri kohtadest internetis.

   Selles etapis kontrollib pahavara küberturvalisuse programmi olemasolu, ning olles selle tuvastanud, lõpetab kohe küberründe.

   VET-i ülesanne on vältida küberteadlikke inimesi, kes võivad kergesti nurjata kogu küberoperatsiooni.

2. **Peibutusdokument**

   Seejärel näidatakse sihtmärgile peibutusdokumenti, et tema valvsust uinutada ning kinnitada, et kõik on korras.

3. **Loob unikaalse ID**

   Saanud ligipääsu arvutile, luuakse selle kohta unikaalne ID, mille järgi on võimalik sihtmärki eristada-tuvastada. Samuti hakkab pahavara edastama arvutis olevat infot ründajale ning seadistab arvutisätted selliselt, et arvuti taaskäivitamisel käivitub ka pahavara.

   VET-i ülesanne on eristada nakatunud seadmeid ning kindlustada ligipääs.

4. **Nakatab irdmeedia**

   Pahavara otsib arvutiga ühendatud irdmeediaseadmeid ja arvutivõrgus asuvaid võrgukettaid, paigaldab neile pahavara ja püüab sealt infot varastada.

   Pahavara osade edasine laadimine on küberründeti erinev.

5. **Varastab andmed**

   Kui pahavara on end täielikult paigaldanud sihtmärgi seadmetesse, siis on VET-il võimalik liigutada korrapäraselt sihtmärgi arvutist infot enda kontrollitud serverisse, ning VET-il on kindlustatud tagavaraligipääsud.