RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] Oktoober 2020

Kaugtöö riskid seoses pahavara levikuga

Pandeemiast tulenevalt on kaugtöö muutunud väga paljude töötajate ja ettevõtete jaoks igapäevaelu osaks ja see trend ilmselt jätkub ka edaspidi. Ehkki kaugtöö lahenduste turvalisemaks muutmise vajadustest on palju kirjutatud nii Eestis kui mujal, soovime juhtida tähelepanu ühele kaasnevale riskile: **kaugtöö puhul võib olla oluliselt raskem tuvastada tööjaama nakatumist pahavaraga ja sellele õigel ajal jaole saada**. Kaugtööd võimaldavad seadistused ja turvareeglid tuleks seetõttu üle vaadata ja vajadusel rangemaks muuta.

Emotet pahavaralainest tulenevad ohud

Käesoleval sügisel on Eestis ja ka mujal maailmas väga laialt levimas Emotet troojalane, millega nakatumine toimub enamasti e-postiga kaasas olevate pahaloomuliste manuste avamise, harvemini linkide klikkimise teel. Taolisi Emoteti sisaldavad meile liigub Eesti küberruumis iga nädal tuhandeid. Tõhusamad viirusetõrjeprogrammid ja õigesti seadistatud meilifiltrid ja tulemüürid aitavad seda ohtu vähendada, ent ka pahavara on võimeline oma tunnuseid ja levimisviisi kiiresti muutma ning on käesoleva laine ajal seda ka mitmeid kordi teinud (vt ka RIA kvartaliülevaade). Ehkki nakatumisest ei pruugi kasutajale olla esialgu ühtegi nähtavat märki, on ettevõtte või asutuse IT-spetsialistidel seda siiski võimalik tuvastada ebaloomuliku liikluse ja autoriseerimata andmevahetuse tõttu. Emotetiga nakatumisel loob seade ühenduse kurjategijate kontrolli all oleva juhtserveriga ning hakkab täitma sealt saabuvaid käsklusi, milleks esimeses etapis on üldjuhul andmete, näiteks postkasti sisu edastamine juhtserverile.

Kaugtöö tõttu on paljud asutused ja ettevõtted olukorras, kus kasutajate seadmed on töötajatel kodus, ühendatud kodusesse wifi võrku. Ehkki ametialane suhtlus (töömeilid) liigub VPNi kaudu, kasutab sama seade muude lehtede sirvimiseks või näiteks erameili lugemiseks otse kodust internetti. Endiselt leidub ka tööandjaid, kes ei nõua töömeili kasutamiseks üldse VPN-i. VPN-i väline liiklus asutuse seadmes aga ei ole kuidagi tööandjale nähtav ega kontrollitav, vastav info on koduse internetiteenuse pakkujal, kes seda aga mõistagi sellisel tasandil ei jälgi.

Seega võib juhtuda, et tööandja seadme nakatumine ja andmete kadu toimub märkamatult ja ka tagantjärele on pea võimatu aru saada, kuidas nakatumine toimus ja kas ja millised andmed on lekkinud. Eestis aset leidnud rohkem kui saja Emotetiga nakatumise hulgas on mitmeid juhtumeid, kus intsidendi mõju ja tekkinud kahju hindamine on keeruline või võimatu, kuna seadet kasutatakse ka mujal kui asutuse sisevõrgus. Kuna Emoteti ja ka paljude teiste pahavaradega nakatumine **tähendab enamasti ka andmeleket,** millega kaasneb andmekaitse inspektsiooni teavitamiskohustus ja halvemal juhul trahvid ning usaldusekadu, on kahjude hindamine ja piiritlemine samas hädavajalik.

Soovitused infoturbejuhtidele

[1] 1 1 KüTS'i paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

1. Olukorrapildi tagamiseks:

1.1. Muuda tööseadmete kaudu toimuv internetiliiklus võimalikult kontrollitavaks. Kaalu kogu liikluse suunamist läbi VPN-i või siis võrgulogide keskset kogumist ja säilitamist.

1.2. Pööra praegu iseäranis suurt tähelepanu väljuva võrguliikluse anomaaliatele. Analüüsi väljuva liikluse logisid (http Proxy, DNS logid) tuvastamaks, kas seade on asunud suhtlema võõra juhtserveriga. Emotetiga seostatud juhtserverite tuvastamiseks on abi allolevast veebilehest:

https://feodotracker.abuse.ch/browse/

2. Nakatumise vältimiseks:

2.1. Veendu, et lõppkasutajate seadmetes on aktiivne ja uuendatud viirusetõrjeprogramm

2.2. Vaata üle veebi- ja meilifiltrite seadistused. Soovitavalt blokeeri MS Office'i makrosid sisaldavad failid ning suuna .zip failid täiendavaks kontrolliks võimaliku pahavara suhtes

2.3. Diferentseeri (ja minimeeri) kasutajaõigusi rollipõhiselt, vajadusel loo ühele kasutajale erinevad kontod erinevate õigustega

2.4. Hoia kasutajad aktuaalsete ohtudega kursis ja soovita jälgida CERT-EE postitusi Twitteris – sinna jõuavad hoiatused hetkel liikvel olevate pahavarade kohta kõige kiiremini

2.5. Kui kasutad MS Defender viirusetõrjeprogrammi, kaalu selle pilvepõhise kaitse (cloud-delivered protection) aktiveerimist. CERT-EE analüüsis Emoteti ühe praegu laialt leviva variatsiooni näitel ja tuvastas, et Emotetil õnnestus MS Defender viirusetõrjeprogrammist mööda hiilida, ent seda vaid juhul, kui *cloud-delivered protection* oli välja lülitatud. Defenderi seadistusvõimaluste ja pilvepõhise kaitse kohta saab lugeda siit:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/enable-cloud-protection-microsoft-defender-antivirus

3. Kui on põhjust kahtlustada, et seade võib olla nakatunud:

3.1. Isoleeri seade võrgust niipea kui võimalik

3.2. Kontrolli esimesel võimalusel üle ka teised seadmed, mis võivad olla nakatunud

Emoteti tuvastamisel võib olla abi Jaapani CERT-i avalikuks kasutamiseks mõeldud tööriistast:

https://github.com/JPCERTCC/EmoCheck/releases

3.3. Muuda ära kasutajatunnused ja paroolid (eriti local admin ja domain admin)

3.4. Nakatunud konto omanik peaks alternatiivkanali kaudu teavitama oma kontakte, et temalt tulnud meilid, eriti manustega, võivad sisaldada pahavara

3.5. Teavita https://raport.cert.ee/ kaudu või cert@cert.ee

Lisalugemiseks – PaloAlto Unit 46 blogipostitus, mis selgitab konkreetse näite najal lahti, kuidas Emotet levib varastatud meilivestluste abil:

https://unit42.paloaltonetworks.com/emotet-thread-hijacking/