Lühijuhend lunavarajuhtude ennetamiseks ja lahendamiseks

Sisukord

Ülevaade

Krüpteeriv lunavara on üha suuremaks ohuks kõikidele internetikasutajatele, sealhulgas isegi väidetavalt turvaliste korporatiivvõrkude kasutajatele. Ründajad nakatavad süsteemi pahavaraga, mille eesmärgiks on kasutaja lokaalses masinas kõikide failide krüpteerimine. Pärast failide krüpteerimist (ja väga tihti kasutatakse krüpteerimiseks arenenud krüpteerimisviise), üritavad ründajad kasutajalt failidele ligipääsu taastamise eest raha nõuda. Sellised ründed võivad olla väga edukad, eriti korporatiivvõrkudes, kus failiserverid on laialdaselt kasutusel (NAS ja CIFS serverid).

2017. aasta mais avastati uus oht (WannaCry lunavara). WannaCry lunavara kasutab arvutite vahel levimiseks ära varasemalt teadaolevat Eternalblue eksploiti (mida kasutati NSA operatsioonides ning mis “Shadow brokers” lekkes avalikuks tuli). See rünne kasutab ära haavatavust SMBv1 protokollis. Turvalisuse huvides soovitame paigata kõik süsteemid ja/või keelata SMBv1. Teise võimaliku turvameetmena on võimalik vastavate portide filtreerimine. Microsoft on väljastanud ka probleeme lahendavad turvapaigad. praeguseks ka juba mittetoetatud operatsioonisüsteemidele (Windows XP/2003).

Soovitused

Isegi kui Sa ei ole praeguse kampaania ajal ega kunagi varem lunavarарünde ohvriks langenud, tuleks Sul siiski mõelda, milliseid ennetavaid meetmeid rakendada saaksid, et ka tulevikus nakatumist vältida või nakatumise korral minimaalseid kahjusid kanda.

WannaCry lunavaraga nakatumist ennetavad meetmed

- Paika kõik MS17-010 poolt mõjutatud süsteemid. Turvapaigad väljastati ka mitte-toetatud süsteemidele.
- Keela kõikjal SMBv1 kasutamine.
- (Tagasiulatuvalt enne 12. maid) Pane kõik e-mailid, mille manuse sisus on aktiivne kood karantiini (faililaiendite loetelu on toodud edasises tekstis).

- Kontrolli kõiki sissetulevaid käivitatavaid faile veebi/proxy kaudu.
- Kontrolli tagastatud sülearvutid enne nende ettevõtte võrku ühendamist.
- Teavita töötajaid, eriti eemalviibivaid, ohust ning tuleta neile meelde, et tundmatutele linkidele ei tohi vajutada ega tundmatuid manuseid avada.
- Kontrolli varunduse seiskorda ning terviklust.
- Juhul kui lõppseadme kaitse on aktiveeritud, piira ligipääsu teistele portidele.

Ennetavad meetmed

- Parim kaitse krüpteeriva lunavara vastu on **töökindel varundus**. Olles võimeline tagavarakoopiast probleemideta varundama, nurjub ründaja peamine eesmärk.
- Varukoopiad peavad asuma *offline*-režiimis (sõltumata võrgu või süsteemi ühendusvõimest). Kuna krüpteeriv lunavara püüab krüpteerida kohalikke faile nii kohalikul kettal ja välistel andmekandjatel kui ka võrguketastel, peab varukoopia asuma eraldi, et tagavarakoopia omakorda võrguketta krüpteerimise korral ei nakatuks.
- Tagavarakoopiast taastamise periood tuleks üle vaadata. Ärge unustage, et krüpteeriv lunavara võib taustal toimida mitu päeva enne kui see ükskord avastatakse. Mida pikema aja taha tagavarakoopia tegemise periood jääb, seda suurem on eduka taastamise tõenäosus.
- Pidage meeles, et ka tagavaraserverid on haavatavad ning on samamoodi ründajate sihtmärgiks.
- Luba failiserveritesse auditilogimine tuvastamaks ka võimalikud nakatunud failid, mis omakorda võrgukettal asuvad failid krüpteerida võivad.
- Võta kasutusele monitooringuskriptid tuvastamaks süsteemid, mis muudavad lühikese aja jooksul suure hulga faile. Sellist monitooringut saab kasutada tuvastamaks pro-aktiivselt faile krüpteeriv süsteem.
- Krüpteeriva lunavaraga nakatumine toimub kõige sagedamini:
  - E-kirja manuses sisalduva kaudu pahatahtliku koodi käivitumisel.
  - E-kirjaga saadetud linkide kaudu pahatahtliku sisuga dokumentidele.
  - Haavatavate veebilehitsejate või tarkvarakomponentide ärakasutamisel.
- Vaadake üle oma meililüüsi ja veebilüüsi turvapoliitikad ning kindlustage, et logimine on sisse lülitatud (see aitab ka tuvastada nakatunud kasutajad).
- Meililüüs ja veebilüüs peaksid blokeerima või panema karantiini kõik dokumendid, mis sisaldavad käivitatavaid faile, konteineriformaate ja faile, mis võivad potentsiaalselt sisaldada aktiivsisuga faile. Näiteks tuleks blokeerida või panna karantiini alltoodud faililaiendid:
  - **Konteineriformaadid:** .zip, .rar, .ace, .gz, .tar, .7z, .z, .bz2, .xz, .iso
  - **Potentsiaalselt aktiivsisu sisaldavad failid:** .pdf, .doc, .rtf, .ppt, .xls, .odt
  - **Rakendused:** .exe, .pif, .application, .gadget, .msi, .msp, .com, .scr, .hta, .cpl, .msc, .jar
  - **Skriptid:** .bat, .cmd, .vb, .vbs, .vbe, .js, .jse, .ws, .wsf, .wsc, .wsh, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .msh, .msh1, .msh2, .mshxml, .msh1xml, .msh2xml
  - **Otseteed:** .scf, .lnk, .inf
  - **Muud:** .reg, .dll
  - **Office makrofailid:** .docm, .dotm, .xlsm, .xltm, .xlam, .pptm, .potm, .ppam, .ppsm, .sldm
  - **wirecode poolt keelatud failid:** .asf, .asx, .au, .htm, .html, .mht, .vbs, .wax, .wm, .wma, .wmd, .wmv, .wmx, .wmz, .wvx
- Kindlusta, et uuenduspoliitikat rakendatakse ka veebilehitsejatele, sealhulgas laienditele ja pistikprogrammidele.
- Vaata üle oma “Too ise oma seade” (BYOD) poliitika, vähendamaks nakatunud seadete arvu, mis ettevõtte masinaid nakatada võivad.

Krüpteeriva lunavarajuhtumi lahendamine

- Juhtumi tuvastamise korral eemalda koheselt nakatunud seade võrgust (ära unusta juhtmevaba võrku).
- Juhul kui Sa tahad ise sooritada esmase pahavaraanalüüsi, peab enne kettahõivet läbi viima mäluhõive (juhul kui süsteemi välja ei lülitatud ning kest on ligipääsetav).
- Mõnedel harvadel juhtudel on võimalik mõnede failide taastamine (näiteks Windowsi varjukoopiad, tõmmiste või nõrka krüpteerimist kasutanud lunavara puhul). Sellise meetodi peale ei tohi lootma jääda ning tuleb rakendada ülalkirjeldatud ennetavaid meetmeid.
- Nakatumise korral soovitab CERT-EE operatsioonisüsteemi tagavarakoopiast taastada või teha puhas install, vältimaks taasnakatumist. Enne tagavarakoopiast taastamist tuleb tagavarakoopia puhul veenduda, et tagavarakoopia pole samuti pahavaraga nakatunud.
- Ära võta ründajaga ühendust ning ära maksa nõutud lunaraha! Lunaraha makstes toetad Sa kurjategijate äri!
- Võimalusel jäta alles tegelik nakatunud seade, mille saad dekrüptori väljatulekul taas kasutusele võtta.