

Harmaalla alueella toimiminen avointen lähteiden tiedustelussa (OSINT) – Pyhittääkö tarkoitus keinot organisaation suojaamisessa?

Kalle Vesanterä

Kansalaisten henkilökohtaisia terveystietoja käsittelevän organisaation tietojärjestelmiin kohdistuu yön aikana tietomurto. Tietomurron jälkeen käytännössä kaikki kriittiset järjestelmät ovat lukittuina ja hyökkääjä vaatii lunnaita näiden järjestelmien avaamiseksi. Aikaa maksun suorittamiseen on enää 20 tuntia. Hyökkäyksessä käytettiin hyväksi nollapäivähaavoittuvuutta, eli hyökkäyksen mahdollistavaa vikaa osassa tietojärjestelmää, joka ei ollut ennalta tiedossa. Samankaltaisia hyökkäyksiä on kuluneen viikon aikana tapahtunut ympäri maailmaa. Analyysien, tutkimusten ja pimeän verkon seurannan pohjalta todetaan, että uudelle haittaohjelmamarkkinapaikalle on ilmestynyt viikko sitten huutokauppa. Kyseisessä huutokaupassa myytiin tähän järjestelmään soveltuvaa haittaohjelmaa käyttöohjeineen. Lähtöhinta ensimmäiselle huudolle on 10 000 dollaria. Hinta voi kuulostaa alhaiselle, mutta satojen muiden haittaohjelmapakettien seassa kokonaisuus alkaa olla jo huomattavan arvokas.

Pimeän verkon seurannassa on siis jo aiemmin todettu, että kyseiseen järjestelmän osaan on myynnissä jonkinlainen tapa hyödyntää haavoittuvuutta. Tarkempaa tietoa tästä ei kuitenkaan voi saada, ilman että osallistuu huutokauppaan ja ostaa pääsyn sen takana olevaan tietoon. Tapauksesta tekee erityisen ongelmallisen se, että myyjä on suhteellisen tuore mutta tunnistettu toimija, joka on yhdistetty Venäjällä toimiviin tiedustelupalveluihin. Tiedon ostaminen siis todennäköisesti rahoittaisi niin kyberrikollisten, kuin vihamielisen valtion toimintaa.

Toisaalta, omat tietoturvalliset järjestelmämme eivät ole enää uhattuina vaan aktiivisesti vaarannettuina. Hyökkääjä vaatii nyt 100 000 dollarin arvosta Bitcoineja maksettuna heidän hallinnoimalleen kryptotilille. Muuten järjestelmät pysyvät salattuna ja kansalaisten terveystiedot joutuvat mahdollisesti myyntiin, elleivät ne jo ole siellä.

Tämän kaltainen skenaario voi kuulostaa Robert Ludlumin haamukirjoittajan uusimmasta kirjasta repäistyltä tarinalta. Tai ehkä aamupalapöydässä iltapäivälehdestä luettavalta uutiselta. Vastaavat hyökkäykset ovat kuitenkin varsin yleisiä. Ympäri maailmaa tietojärjestelmien ylläpitäjät, kyberturvallisuuden ammattilaiset ja konsultit sekä eri organisaatioiden johtohenkilöt joutuvat jatkuvasti painimaan niiden parissa. Uhka- ja vaarantumisindikaattoritietokantoja päivittäviltä tahoilta todennäköisesti kysytään, miksi tästä haavoittuvuudesta ei ollut tarkempaa ennakkotietoa? Indikaattoritietoja kuitenkin oli jo saatu seuraamalla eri lähteistä koostettua tiedonpalasia.

Avoimista lähteistä suoritettavalla tiedustelulla (OSINT) on mahdollista koostaa valtavia määriä informaatiota useista eri lähteistä eheäksi kokonaisuudeksi. Tämän kokonaisuuden pohjalta voidaan tukea niin johtohenkilöiden strategista päätöksentekoa, kuin löytää teknisiä indikaattoritietoja erilaisista tapahtumista, haavoittuvuuksista ja uhkakuvista. Näiden avulla voidaan ottaa käyttöön suojausmekanismeja, jotka estävät hyökkäysten mahdollistamisen. Näitä tietoja voidaan koostaa arkipäiväisten lähteiden, kuten uutisten ja sosiaalisen median ohella myös niin sanotun pimeän verkon lähteistä. Ongelmaksi muodostuu kuitenkin *crime as a service* toiminta, jota verkko- ja kyberrikollisuudessa on harjoitettu jo pitkään.

Jos me tai joku muu suotuisa taho olisi ostanut tiedot itselleen ja jakanut nämä turvallisuusyhteisön kanssa, ei tämä hyökkäysalto olisi välttämättä päässyt tapahtumaan. Kriittiset järjestelmät eivät

olisi nyt lukittuina, meiltä ei vaadittaisi lunnaita, eikä kansalaisten tiedot olisi päätyneet valtiollisen kyberuhkatoimijan käsiin. Tämä raha olisi kuitenkin mennyt rikollisten taskuun ja mahdollistanut näiden toiminnan kasvattamisen ja kehittämisen edelleen. Kuten tässä skenaariossa, tämän tyyppiset toimijat ovat usein yhdistettävissä johonkin valtiolliseen toimijaan, elleivät jopa suoraan ole sellaisia. Lunnasrahat maksamalla voimme ehkä selvitä hyökkäyksestä ennen aikarajan umpeutumista, mutta nyt maksaisimme moninkertaisesti alkuperäiseen hintaan verrattuna. Toki niin saattaisimme maksaa muutenkin?