Kybersodan aika, osa II

Edellisessä kolumnissani 24.3.2022 kirjoitin kyberturvallisuuden merkityksestä nykyaikaisessa sodankäynnissä. Kirjoitukseni jälkeen sain Facebookin kautta muutamia kysymyksiä aiheesta, ja tämänkertainen kolumnini käsittelee valtiollisia uhkia ja niiden toimijoita, APT-ryhmiä (Advaneced Persistant Threat).

Valtiollisten toimijoiden suorittama kybervakoilu uhkaa kansallista turvallisuutta. Tavoitteena on hankkia kohdevaltiosta tietoa, joka kaventaa sen kansainvälistä liikkumatilaa tai vaikuttaa sen asemaan globaalissa kilpailussa.

Lyhennettä APT käytetään kuvaamaan kybervakoiluoperaatioita, joissa tunkeudutaan tietojärjestelmiin hyödyntäen erilaisia työkaluja erittäin suunnitelmallisesti. Tietojärjestelmistä etsitään ja kopioidaan tietoa sekä pyritään tekemään kaikki täysin salassa, kenenkään huomaamatta.

APT-ryhmät ovat erittäin hyvin organisoituja ja ammattitaitoisia. Ne eivät kuitenkaan ole henkilöiden muodostama ryhmä, vaan pikemminkin teknisten jälkien joukkoja.

Kunkin APT:n on nimennyt julkisen tunnistuksen tehnyt taho eli yleensä tietoturvayritys. Usealla APT:lla on monta eri nimeä, koska eri yritykset ovat tehneet nimeämisen kukin oman datansa pohjalta.

Toisiinsa liittyvät kyberoperaatiot pyritään tunnistamaan niissä käytettyjen menetelmien, ohjelmistotyökalujen ja verkkoinfrastruktuurin jättämien jälkien avulla. Vakoilun taustalla olevasta valtiosta ja myös tiedustelupalvelusta saadaan usein tietoa APT-tunnisteiden kautta.

On vahvaa näyttöä siitä, että Sandworm -niminen ryhmä on toteuttanut kyberhyökkäysten sarjan Ukrainassa. Ryhmän epäillään olevan sekä ranskalaisiin IT-alan yrityksiin että yhdysvaltalaisiin energia-alan organisaatioihin kohdistuneiden tietomurtojen takana.

Sandworm on linkitetty julkisissa lähteissä Venäjän sotilastiedusteluun (GRU) ja sitä kautta APT28-ryhmään. APT28:ksi nimetty Venäjän sotilastiedustelun GRU:n operaatio tunnetaan myös nimellä Sofacy.

Yhdysvaltojen kyberturvallisuusvirasto CISAn (Cybersecurity & Infrastructure Security Agency) mukaan ATP28 liittyy GRUn 85. pääerikoispalvelukeskuksen toimintaan. APT28 on toiminut ainakin vuodesta 2004 ja sen kohteita ovat ensisijaisesti valtion organisaatiot, matkailu- ja ravintola-alan

yhteisöt, tutkimuslaitokset ja kansalaisjärjestöt muiden kriittisen infrastruktuurin organisaatioiden lisäksi.

APT28:n kerrotaan muun muassa vaarantaneen Hillary Clintonin presidentinvaalikampanjan vuonna 2016 yrittäen puuttua Yhdysvaltain presidentinvaaleihin. APT28:n kyberhyökkäysten kehitystyö ja verkkotunnusten rekisteröinnit osoittavat myös kiinnostuksensa Natoa ja muita eurooppalaisia turvallisuusjärjestöjä kohtaan.

APT28:a tukee todennäköisesti joukko kehittäjiä, jotka luovat pitkäaikaiseen ja monipuoliseen käyttöön tarkoitettuja työkaluja. Tämä viittaa siihen, että APT28 saa suoria jatkuvia taloudellisia ja muita resursseja vakiintuneelta organisaatiolta.

APT28:n haittaohjelma-asetukset viittaavat siihen, että kehittäjät ovat tehneet suurimman osan työstään venäjänkielisessä rakennusympäristössä Venäjän aukioloaikoina. Vaikuttaakin siltä, että Venäjän hallitus on APT28:n sponsori.

Ismo Turve

Kirjoittaja on kyberturvallisuus orientoitunut heinolalainen ja Tietojenkäsittelyn lehtori Hämeen ammattikorkeakoulusta.