Case study raportoidusta hyökkäyksestä

Kiristyshaittaohjelmahyökkäys Costa Rican hallitukseen

Elmeri Söderholm, AA3979

Harjoitustyö
Hyökkäykset ja puolustusmenetelmät sekä suojaaminen, Jarmo Nevala
Palautuspäivä
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Tämä harjoitustyö on Hyökkäys ja puolustusmenetelmät sekä suojaaminen -kurssin ensimmäinen harjoitustyö. Käyn läpi tässä tiedonhakutehtävässä tämän vuoden huhtikuussa alkanutta monivaiheista kiristyshaittaohjelmahyökkäystä Costa Rican hallitukseen. Hyökkäys oli poikkeuksellinen ja hyvin merkittävä hallitustason kyberhyökkäys. Käyn dokumentissa läpi, kuka oli vastuussa hyökkäyksestä, kuka oli hyökkäyksen kohde, hyökkäystavat sekä malli hyökkääjän toimenpiteistä, aikajana hyökkäyksestä, miten hyökkäys havaittiin, sekä vastatoimenpiteet. (Harjoitustyö 1. ohjeet. 2022).

2 Conti, kiristyshaittaohjelma Venäjältä

Conti on venäläisen hakkeriryhmän luoma, erittäin vahingoittava kiristyshaittaohjelma, joka purkaa tietoa hyvin nopealla tahdilla ja leviää eri järjestelmiin. Ohjelman alkuperästä ei tiedetä paljoa, mutta on spekuloitu, että sen on luonut venäläinen hakkeriryhmä nimeltä Wizard Spider. Tätä ryhmää on seurattu vuodesta 2020 asti ja Yhdysvaltojen hallitus tarjoaa palkkiota tietoa vastaan. Ei ole varmaa onko kyseinen ryhmä Costa Rican hallituksen hyökkäyksen takana, joten monissa lähteissä puhutaan vain ”Conti hakkeriryhmästä”. (Tudor D. 2022).

3 Hyökkäys

3.1 Kohde

Hyökkäyksen kohteena oli Costa Rican hallitus, johon iskettiin erittäin suurella voimalla. Hakkeriryhmä iski ensimmäisenä valtiovarainministeriön järjestelmiin ja jo viikon päästä, hyökkäys oli murtanut kaksi avainjärjestelmää. Nämä olivat digitaalinen veropalvelu sekä tullivalvonnanIT-järjestelmät. Nämä murrot vuotivat useita terabittejä dataa sekä vaikuttivat satoihin valtiovarainministeriön palvelimiin. Murto vaikutti myös laajasti yksityissektoriin. Koska tullivalvontaa häirittiin, tuonnin ja viennin liiketoiminta koki häirintää ja häviöt vaihtelivat 38 miljoonasta päivässä, jopa 125 miljoonaan dollariin yli 48 tunnin aikana. Hyökkäys vaikutti siis suuresti Costa Rican kaupankäyntiin.

Valtiovarainministeriön lisäksi hyökkäyksiä tehtiin myös tämän jälkeen enemmän, joista jotkut hyökkäykset onnistuivat, jotkut eivät. Kohteiksi joutui monia eri hallituksen organisaatioita päivittäin. Esimerkiksi virkavalta ja työ- ja sosiaaliministeriö joutuivat hyökkäyksien kohteeksi ja myös Costa Rican sosiaaliturvarahasto saatiin murrettua. Murto sosiaaliturvarahastoon vaikutti terveydenhuollon järjestelmiin merkittävästi. Potilaat alkoivat tekemään valituksia viivästyksistä ja tulostimet alkoivat tulostamaan mitä sattui. Terveydenhuoltoon tuli myös monia muita häiriöitä, jotka vaikeuttivat palvelun käyttöä. (O'Connor P. 2022), (Burgess M. 2022).

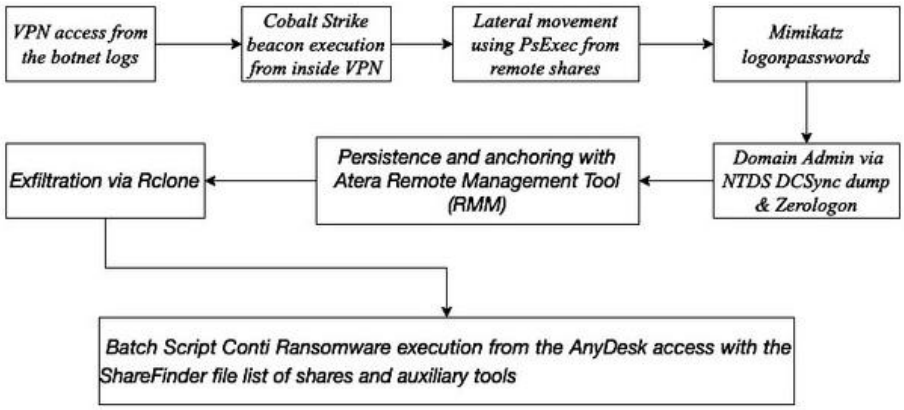
3.2 Hyökkäystapa sekä hyökkääjän toimenpiteet

Hyökkäys oli monivaiheinen sekä laaja kokonaisuus hyökkääjän näkökulmasta. Hyökkäys alkoi 11. huhtikuuta 2022 tiedustelutoiminnalla sen jälkeen, kun hyökkääjä sai ensimmäisen kerran pääsyn Costa Rican hallituksen verkkoon. 15. huhtikuuta hallituksen verkossa suodatettiin 672 gigabittiä dataa ja tänä aikana kiristyshaittaohjelma suoritettiin.

Sisääntulopiste verkkoon oli valtiovarainministeriön järjestelmässä johon jäsen, joka kuului ryhmään ”MemberX”, sai pääsyn VPN yhteyden avulla vuodettujen tunnistetietojen avulla. Tunnistetiedot oli saatu malwaren avulla, joka oli asennettu hallituksen verkkoon kuuluvaan tietokoneeseen. Kun hyökkääjällä oli nyt pääsy verkkoon, alkoi erilaisten Cobalt Strike beaconeiden eli eräänlaisten penetraatioagenttien leviäminen verkossa. Näillä beaconeilla on erilaisia toimintoja, jota hyökkääjä käytti hyväksi hyökkäyksessä. (Ilascu I. 2022) (Cobalt Strike. N.d)

Tämän jälkeen agentin avulla alkoi erilaisten domain käyttäjäsuhteiden listaaminen sekä tiedostojen skannaaminen. Kun näitä saatiin listattua, alkoi tiedon siirtäminen backdoor toiminnon avulla ulos paikalliselle koneelle. Conti teki paljon muita exploitation toimintoja saadakseen järjestelmänvalvojatietoja, sekä muita kirjautumistietoja verkosta. Conti teki myös puolustustoimenpiteitä Atera Remote Management Toolin avulla siltä varalta, että beaconit huomataan. (Ilascu I. 2022).

Tarkemmat työkalut ja vaiheet löytyvät diagrammista (ks. kuvio 1.)



Kuvio 1. Kill chain malli hyökkäyksestä

4 Hyökkäyksen aikajana, havainnot sekä vastatoimenpiteet

Hyökkäys Costa Rican hallitukseen alkoi tiedustelulla 11. huhtikuuta 2022. Tämä kesti neljän päivän ajan, jonka jälkeen 15. huhtikuuta alkoi ensimmäisen kiristyshaittaohjelman runnaaminen järjestelmiin. 18. päivä ensimmäiset murrot oli tehty valtiovarainministeriöön sekä useisiin eri organisaatioihin hallituksen sisällä. Espanja, Yhdysvallat ja useat yksityisyritykset auttoivat Costa Rican hallitusta puolustamaan hyökkäyksestä. Siitä huolimatta ensimmäinen hyökkäys kesti yli kuukauden, joka vaikutti muun muassa kaupankäyntiin ja valtio teki tänä aikana merkittävää häviötä. Toukokuun alussa Costa Ricassa oli vaalit meneillään, jonka takia presidentti vaihtui kesken hyökkäyksen. Tämä varmasti vaikutti hyökkäyksen pitkittyneisyyteen ja hallituksen toimintaan myös. Uusi presidentti julisti kansallisen hätätilan 8. toukokuuta kiristyshaittaohjelmahyökkäyksien takia ja kutsui hyökkääjiä ”kyberterroristeiksi” Tämä oli ensimmäinen kerta kun missään maassa on julistettu hätätila kiristyshaittaohjelman vuoksi. (Burgess M. 2022)

Hallituksen heikosta kyberpuolustuksesta ei annettu virallista lausuntoa, mutta Costa Rican kyberturvallisuusyrityksen White Jaguarsin toimitusjohtaja Mario Robles sanoi, että järjestelmät ovat vanhentuneita ja joillain osastoilla ei edes ole työntekijää kyberturvallisuuspuolella. Hän lisäsi myös, että tämä on iso ongelma latinalaisamerikkalaisissa valtioissa. (Burgess M. 2022)

Toinen hyökkäys tapahtui 31. toukokuuta, jolloin kohteeksi joutui sosiaaliturvarahasto. Hyökkäys joka suurilta osin koski terveydenhuoltoa, kesti kesäkuun loppuun asti. Hallitus oli vastahakoinen maksamaan kaikkia lunnaita, jonka takia hyökkäykset venyivät pitkälle kesäkuuhun. Tällöin Costa Rica maksoi joitakin lunnaita, jotta palveluita saatiin palautettua. Lopulta Contin johto lopetti toimintansa, jonka jälkeen hyökkäykset loppuivat kesäkuun lopussa. (Ilascu I. 2022)

5 Pohdinta

Harjoitustyön tekeminen oli erittäin kiinnostavaa ja mielestäni valitsin myös hyvän aiheen tähän tehtävään. Työtä oli suhteellisen helppo tehdä, sillä tietoa löytyi helposti netistä ja useassa lähteessä oli käyty hyvin perinpohjaisesti läpi tapauksen kulkua. Lähteissä oli myös vaihtelevaisuuksia, joissain kerrottiin yleisemmin tapahtuman kulusta ja hyökkäyksen vaikutuksista valtioon, kun taas toisissa kerrottiin tarkemmin hyökkäyksen toimenpiteistä teknilliseltä kannalta ja kerrottiin hyvin mitä työkaluja oli käytetty.

Oli myös mielenkiintoista lukea, millä tavalla Costa Rica vastasi tähän hyökkäykseen. Mielestäni oli yllättävää saada selville, miten suuri vaikutus kyberhyökkäyksellä voi olla valtioon. Aikaisemmin oli mainittukin heikosta kyberpuolustuksesta latinalaisamerikkalaisissa valtioissa. Hyökkäys oli tehty myös Costa Rican vaalien aikaan, mikä saattoi olla sattumaa sillä Ukrainan sota oli juuri alkanut eikä Venäjä voinut oikein tehdä tällöin enää hyökkäyksiä esimerkiksi Yhdysvaltoihin, koska kaikki yhteydet Venäjään oli katkaistu eikä lunnaiden siirto olisi ollut mahdollista.

Koska tietoa löytyi paljon, opinkin myös paljon uusia asioita. En ollut esimerkiksi vielä tietoinen näistä beaconeista, joita käytetään hyökkäyksissä. Oli paljon muitakin termejä ja työkaluja, joiden ymmärtäminen olisi vaatinut syvempää osaamista, mutta mielestäni ymmärsin hyökkäyksen päävaiheet ja sen vaikutukset.

Kaiken kaikkiaan, aiheeni tähän työhön oli mielenkiintoinen ja myös herätys siihen, miten suuri vaikutus onnistuneella kyberhyökkäyksellä voi olla kokonaiseen valtioon.

Lähteet

Burgess M. 12.6.2022. Viitattu 29.10.2022. https://www.wired.com/story/costa-rica-ransomware-conti/

Cobalt Strike. N.d. Viitattu 29.10.2022. https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike

Harjoitustyö 1. ohjeet. 15.9.2022. Viitattu 29.10.2022. https://moodle.jamk.fi/pluginfile.php/806100/mod_resource/content/0/TTC6040-Harjoitusty%C3%B6_01.pdf

Ilascu I. How Conti ransomware hacked and encrypted the Costa Rican government. 21.7.2022. Viitattu 29.10.2022. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/

O'Connor P. The biggest cyber attacks of 2022. 26.9.2022. Viitattu 29.10.2022. https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/

Tudor D. All about Conti Ransomware. 1.6.2022. Viitattu 29.10.2022. https://heimdalsecurity.com/blog/what-is-conti-ransomware/