jamk

Mitre ATT&CK

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Kyberuhkatieto TTC6030-3011
1.12.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Taulukot

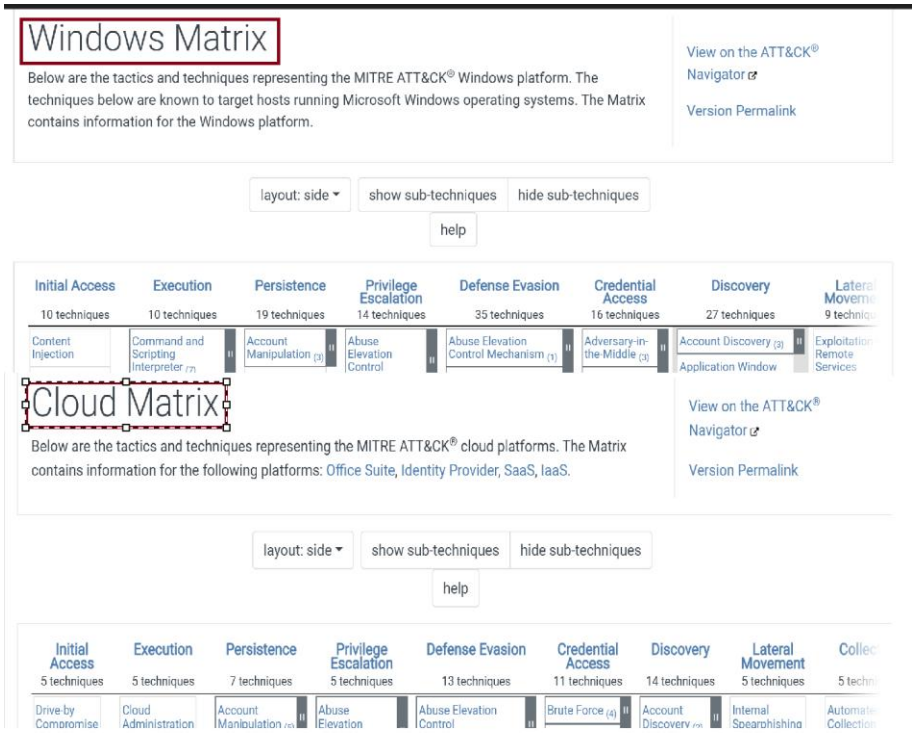
1 Johdanto

Tämän harjoitustyön tarkoituksena on perehtyä MITRE ATT&CK-viitekehykseen, joka on laajasti käytetty tietoturvauhka-analyysi työkalu. ATT&CK tarjoaa kattavan ja systemaattisen kuvan erilaisista uhkista, haavoittuvuuksista ja hyökkäystekniikoista eri ympäristöissä. Viitekehyksen avulla pystymme ymmärtämään kyberhyökkäysten toimintatapoja ja kehittämään tehokkaampia suojaustoimia.

2 Pilvipalveluiden haavoittuvuudet

Pilvipalveluiden haavoittuvuuksien huomioiminen on organisaatiolle tärkeää, varsinkin kun pilvipalvelut ovat nykyään osa jokaisen yrityksen IT-ratkaisuja. MITRE ATT&CK-viitekehys tarjoaa laajasti tietoa näiden haavoittuvuuksien kartoittamiseksi.

Aloitetaan hieman tutkimalla pilvipalveluiden ja Windows-järjestelmän haavoittuvuuksien eroja. Kun katsomme haavoittuvuuksien määrää, huomaamme heti, että pilvipalveluiden haavoittuvuuksia on paljon vähemmän. (Kuvio 1).



Kuvio 1. Vertailu Windows ja pilvipalveluiden haavoittuvuuksien välillä

Eroavuus määrissä johtuu suurimmaksi osaksi pilvipalveluiden hyökkäyspinta-alan pienuudesta verrattuna käyttöjärjestelmään. Pilvipalvelut koostuvat pääasiassa palvelinpuolen ympäristöistä, joissa ei ole suoraa pääsyä käyttöjärjestelmään. Tämän vuoksi hyökkäysmahdollisuuksia on vähemmän.

Vaikka pilvipalveluihin kohdistuvia hyökkäysmenetelmiä on vähemmän, niin aiheutuneen vahingon laajuus on suurempi. Käyttöjärjestelmään kohdistuvat hyökkäykset vaikuttavat usein vain paikalliseen laitteeseen tai verkkoon, kun taas pilvipalveluihin kohdistuva hyökkäys kohdistuu koko pilvipalvelimeen. Pilvipalveluiden haavoittuvuuksien korjaaminen voi olla myös haastavampaa ja vaatii konfiguraation muutoksia.

Windowsin ja pilvipalveluiden eroa kuvaa myös tiettyjen MITRE taktiikoiden määrä, kun niitä vertaa toisiinsa. Esimerkiksi Persistence taktiikassa on Windows käyttöjärjestelmän matriisissa (Windows Matrix) 19 tekniikkaa, kun pilvessä (Cloud Matrix) niitä on vain 7. Windows matriisissa useat tekniikat järjestelmässä pysymiseen liittyvät käyttöjärjestelmän käynnistyksen yhteydessä tapahtuvaan haittaohjelman käynnistymiseen skriptin avulla (Boot or Logon Initialization Scripts - T1037) tai käyttöjärjestelmän alla tapahtuvan kovalevyn manipuloinnin Bootkitin-haittaohjelman (Pre-OS Boot: Bootkit - T1542) avulla. Pilvipalveluissa näitä tekniikoita ei ole, koska niissä hyökkääjä ei samalla tavalla pääse käsiksi käyttöjärjestelmään ja sen alimpiin tasoihin. Pysyvyys taktiikat pilvessä liittyvät käyttäjätietojen manipulointiin, jotta voidaan kirjautua uudestaan palvelimelle. Yksi selkeä ero Windowsissa ja pilvipalveluissa on myös se, että Windows laitteita on ollut niin pitkään markkinoilla verrattuna pilvipalvelualustoihin, joita on alettu käyttää myöhemmin enemmän. Myös sen vuoksi, MITRE ATTACK- taktiikoita on enemmän Windows käyttöjärjestelmiä kohtaan. (Windows Matrix. Cloud Matrix. 2024)

3 Stuxnet

Tutkitaan seuraavaksi MITRE ATT&CK-viitekehyksen avulla Stuxnet haittaohjelmaa. Stuxnet on erittäin tunnettu, sillä se on ensimmäinen julkisesti raportoitu haittaohjelma, jonka kohteena on tuotannon hallinta laitteistot. Haittaohjelman tavoitteena oli vaikuttaa Iranin ydinohjelmaan ja sen uskotaan olleen osa Yhdysvaltojen ja Israelin yhteistä projektia nimeltä Operation Olympic Games. (Langner, R. 2013)

Kyseinen haittaohjelma on melko laaja ja monimutkainen, se käyttää hyväkseen useita eri tekniikoita, kuten nollapäivä haavoittuvuuksia, Windows rootkittiä sekä erilaisia verkon saastuttamistapoja. Sen pääkohteena on kuitenkin Siemensin SCADA laitteistot, erityisesti juuri Iranin ydinohjelmassa käytetty järjestelmä. Aiheuttaakseen vahinkoa teollisuusjärjestelmille Stuxnet muun muassa pystyi ohjelmoimaan PLC:t (Programmable Logic Controller) uudelleen ja muokkaamaan taajuusmuuttajien asetuksia. (MITRE Stuxnet. 2024.)

Stuxnetin hienostuneisuutta kuvaa se, että se ei vain pystynyt löytämään tietyn tyyppistä laitetta, jonka haittaohjelman luojat tiesivät olevan Iranin ydinvoimalaitoksella, vaan myös löydettyään sen, muuttamaan laitteen asetuksia, tehden fyysistä vaurioita laitteisiin voimalassa. Haittaohjelman tarkka kohdennus tiettyihin laitteisiin kertoo sen edistyksellisyydestä.

3.1 Miten vaasalainen yritys liittyy?

Vaasa-lähtöinen Vacon Oyj, nykyisin osa Danforssia, liittyy Stuxnet-haittaohjelmaan sen valmistamien taajuusmuuttajien kautta. Valcon valmistamat laitteet olivat yksi kahdesta laitetyypistä, joihin Stuxnet kohdistui. Stuxnet etsi ohjelmoitavista logiikkaohjaimista (PLC) Vacon NX-sarjan taajuusmuuttajia, jotka ohjelma tunnisti 9500h-tunnisteella. Ohjelma etsi tämän tunnisteen laitetta, koska niitä käytettiin Iranin ydinvoimalan sentrifugien (linko) pyörimisen taajuuden hallinnassa. Kun Stuxnet löysi laitetyypin, se pystyi manipuloimaan sentrifugien toimintaa. (Vacon. 2024)

4 Mobiili uhat

Mobiililaitteet ovat nykyään osa jokaisen elämää ja ne kulkevat meidän mukanamme läpi päivän, mukaan lukien työpaikalle. Ne sisältävät usein paljon tietoa, harmillisen usein myös tärkeää tietoa, kuten salasanoja.

Tutustutaan seuraavaksi MITRE ATT&CK:stä mobiililaitteen lukitusnäytön ohitukseen hyödynnettäviä menetelmiä ja kuinka torjua niitä.

MITRE ATT&CK on tunnistanut seuraavat ohitustekniikat:

- Brute-Force-hyökkäykset

- Salasanan arvaaminen
- Salasanan kurkkiminen
- Biometrisen tunnistuksen ohittaminen
- Haavoittuvuuksien hyödyntäminen

Hyökkääjä voi ohittaa biometrisen tunnistautumisen, kuten sormenjälki- ja kasvojentunnistus, käyttämällä väärennettyä biometriikkaa. Hyökkääjä siis esiintyy käyttäjänä tavallaan. Android ja iOS osittain estävät tämän pyytämällä käyttäjältä lukituskoodin biometrisen tunnistuksen sijaan/lisäksi, laitteen uudelleenkäynnistyksen ja tietyn määritellyn ajan välein. Monitasoinen tunnistautuminen tuo laitteelle lisäsuojaa ja auttavat varmistamaan käyttäjän olevan mobiililaitteen omistaja. (MITRE Lockscreen Bypass. 2024.)

Hyökkääjä voi saada haltuunsa lukitusnäytön PIN-koodin/salasanan, joko testaamalla sitä satunnaisilla yrityksillä, Brute-forcella tai katsomalla, kun puhelimen omistaja näppäilee sen (Shoulder Surfing). Näitä torjutaan mobiililaitteissa asteittain pitenevillä aikaviiveillä tarpeeksi monen epäonnistuneen kirjautumisyrityksen jälkeen. Laite voi myös tyhjentää kaikki tiedot, kun on niin paljon epäonnistuneita kirjautumisyrityksiä, että laitteen voidaan kuvitella olevan väärissä käsissä. (MITRE Lockscreen Bypass. 2024.)

Haavoittuvuuksia voidaan hyväksikäyttää, jotta lukitusnäyttö saadaan avattua. Mobiililaitteista voi löytyä haavoittuvuuksia, joiden avulla hyökkääjä pääsee ohittamaan lukitusnäytön ilman pääsykoodeja. Laitevalmistajat ja käyttöjärjestelmän hallinnoijat paikkaavat ongelmat, kun ne tulevat esille. (MITRE Lockscreen Bypass. 2024.)

Lisäksi on mainittu kaksi haittaohjelmaa:

- **BRATA:** Haittaohjelma voi pyytää käyttäjää avaamaan laitteen lukituksen tai jopa avata sen etänä.
- **Escobar:** Haittaohelma voi pyytää DISABLE_KEYGUARD luvat ottaakseen lukitus salasanan pois käytöstä.

Näiden torjumiseksi Mitren suosittelemia keinoja ovat:

- Salasanan monimutkaisuuden vähimmäisvaatimukset
- Laitteen tietojen tyhjentäminen, kun väärä salasana syötetään liian monesti
- Biometrisen tunnistautumisen käytöstä poisto
- Käyttöjärjestelmien turvallisuuspäivitykset

5 Toimitusketjun vaarantuminen (Supply Chain Compromise)

Toimitusketjun vaarantuminen on tekniikka, joka hyödyntää muita yrityksiä ja heidän tuotteitaan saadakseen vaikutettua kohde yritykseen.

Tämä voi tarkoittaa käytännössä esimerkiksi:

- **laitteistokomponenttien manipulointia toimitusketjun aikana**
- **Ohjelmistojen muokkaamista**
- **Riippuvuuksien hyväksikäyttöä**
- **Palveluntarjoajiin kohdistettuja hyökkäyksiä**

Toimitusketjun vaarantuminen (Supply Chain Compromise) on hyökkäystekniikka, jossa hyökkääjä manipuloi tuotteita ja ohjelmistoja ennen kuin ne päätyvät asiakkaalle. Muokatun tuotteen avulla hyökkääjä pyrkii saamaan pääsyn asiakkaan järjestelmään. Toimitusketjun vaarantuminen voi tapahtua monessa vaiheessa toimitusketjua, kuten kehitystyökalujen manipuloinnissa, tuotteiden itsensä manipuloinnissa, tai ne voivat tulla, vaikka ohjelmistopäivitysten mukana. Ne voivat tulla esimerkiksi troijalaisina tärkeiden päivitysten tai ohjelmistojen mukana, vaikka ne olisivat peräisin luotetulta sivustolta. (MITRE Supply Chain Compromise. 2024.)

Toimitusketjun vaarantuminen voi kohdistua valvontajärjestelmiin (IT- ja OT-verkoissa), näissä hyökkäys voi johtaa pääsyyn IT-ympäristön lisäksi operatiiviselle puolelle (OT). Näin hyökkääjä voi päästä esimerkiksi PLC- laitteisiin kiinni ja hallitsemaan niiden toimintoja. Myös globaali toimitusketju voidaan vaarantaa tuomalla sinne väärennettyjä laitteita, jotka tuovat mukanaan turvallisuus- ja toiminnallisuusriskejä. Kyberuhkatoimijat tekaisevat sertifikaatteja ja merkitsevät tuotteet niin, että ne pääsevät laaduntarkastuksista läpi ja jakeluun, kuin ne olisivat oikeanlaisia laitteita, vaikka ne eivät täytä tarvittavia standardeja. (MITRE Supply Chain Compromise. 2024.)

Nämä kaikki tarkoittavat käytännössä sitä, että hyökkäys ei kohdistu suoraan kohde yritykseen, vaan päästään hyökkäämään kohteeseen toisen yrityksen tuotteiden tai palvelujen välityksellä.

6 Industroyer haittaohjelma

Industroyer on edistynyt haittaohjelma, joka on suunniteltu vaikuttamaan kohteen tuotannonohjausjärjestelmiin (ICS, Industrial Control Systems). Kyseistä haittaohjelmaa käytettiin esimerkiksi Ukrainan sähkönjakeluverkkoon kohdennetussa hyökkäyksessä vuonna 2016. Haittaohjelmaan on vahvasti yhdistetty APT ryhmä Sandworm Team, joka on liitetty Venäjän sotilastiedustelupalveluun. (MITRE Industroyer. 2021)

Ohjelma kykenee manipuloimaan sähköverkon kytkimiä ja katkaisijoita, joka voi johtaa sähkökatkoksiin. Sen avulla pystytään myös estämään järjestelmien hallinnointi.
Haittaohjelma sisältää myös pyyhkimiskomponentteja (wiper), jotka pyyhkivät järjestelmän tietoja ja tehtyjä muutoksia, tehden palauttamisesta ja iskun tutkimisesta haasteellista. (MITRE Industroyer. 2021)

Brute Force I/O on yksi Industroyerin hyödyntämistä taktiikoista, jonka avulla ohjelma pyrkii aiheuttamaan teollisuusprosessin häiriöitä. Ohjelman IEC 104 moduuli myös hyödyntää tätä Brute Force I/O taktiikkaa. Moduulissa on 3 tilaa, range, shift ja sequence. (MITRE Industroyer. 2021)

7 Cellebrite & Grayshift

Cellebrite ja Grayshift ovat yrityksiä, jotka keskittyvät tiedonkeruuseen mobiililaitteista. Ne tarjoavat palveluita esimerkiksi valtiollisille toimijoille ja lainvalvontaviranomaisille.

Selvitetään miten nämä yritykset liittyvät mobiililaite-haavoittuvuuksiin käyttäen hyödyksi MITRE ATT&CK-viitekehystä.

Viitekehyksestä etsimällä, yritykset on mainittu tekniikan kehittäminen siirrettävän median kautta (Replication Through Removable Media) alla. Yritysten työkalut voivat avata pääsykoodin ainakin joihinkin iOS laitteisiin käyttäen USB laitteita.

7.1 Cellebrite & Grayshift työkalut

GrayKey on Grayshiftin kehittämä työkalu, jolla voidaan purkaa salaus ja kerätä tietoja mobiililaitteista (iPhone-laitteet, jotkin Adndroid-laitteet). Se murtaa Brute-force-hyökkäyksellä laitteen lukituksen, jotta päästään laitteen tiedostoihin ja metatietoihin. GrayKey-työkalua pääosin käyttävät lainvalvontaviranomaiset mobiililaitteiden forensiikkatutkimuksissa. (Grayshift. 2024.)

Celebrite UFED (Universal Forensic Extraction Device) on tiedonkeruulaite, jota myös käytetään mobiililaitteiden tietoihin pääsyyn. Sillä voidaan kerätä dataa useiden eri laitevalmistajien mobiililaitteista. UFED:ia käytetään myös forensiikkatutkimuksissa viranomaisten puolesta. MITRE ATTACK- viitekehyksestä ei löytynyt tietoa paljoakaan näistä organisaatioista tai niiden työkaluista. Vain Replication Through Removable Media- kohdassa mainittiin nämä toimijat, ja tunnetuimmat

työkalut liittyen näihin yrityksiin ovat juuri fyysisiä laitteita, jotka kytketään suoraan uhrilaitteeseen. (Cellebrite UFED. 2024.)

Lähteet

Cellebrite UFED. Wikipedia artikkeli. 2024. Viitattu 20.11.2024. https://en.wikipedia.org/wiki/Cellebrite_UFED.

Grayshift. Wikipedia artikkeli. 2024. Viitattu 20.11.2024. https://en.wikipedia.org/wiki/Grayshift.

Stuxnet. MITRE ATT&CK artikkeli. 2024. Viitattu 22.11.2024. https://attack.mitre.org/software/S0603/.

Supply Chain Compromise. MITRE ATT&CK artikkeli. 18.4.2020. Viitattu 2.12.2024. https://attack.mitre.org/techniques/T1195/.

Industroyer. MITRE ATT&CK artikkeli. 4.1.2021. Viitattu 2.12.2024. https://attack.mitre.org/software/S0604/.

Vacon. Wikipedia artikkeli. 2024. Viitattu 20.11.2024. https://en.wikipedia.org/wiki/Vacon.

Langner, R. To Kill a Centrifuge. 11.2013. Viitattu 2.12.2024. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Liitteet

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko