Mitre att&ck

Juuso Leppänen, TTV22S3

Opiskelutehtävä
Kyberuhkatieto ja data-analytiikka TC6030-3011, Heikki Järvinen
8.12.2024
Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Taulukot

1 Kuvaotsikkoluettelon hakusanoja ei löytynyt.**Johdanto**

Mitre ATT&CK -viitekehys tarjoaa tietoa kyberuhkien tunnistamisesta ja torjunnasta eri ympäristöissä, kuten Windows-järjestelmissä, pilvipalveluissa, mobiilialustoilla ja teollisuusohjausjärjestelmissä (ICS). Tämä raportti tarkastelee pilvipalveluiden ja Windows-järjestelmien haavoittuvuuksia, analysoi haittaohjelmia kuten Stuxnet ja Industroyer, sekä käsittelee mobiilialustojen uhkia ja niitä hyödyntäviä yrityksiä, kuten Cellebrite ja Grayshift.

2 Pilvipalveluiden ja windows laitteiden haavoittuvuudet matriisissa

Pilvipalveluissa on vähemmän kohteita Mitre ATT&CK -matriisissa kuin Windows-järjestelmissä, koska pilvipalvelut ovat yleensä standardoituja ja keskitetysti hallittuja ympäristöjä. Ne tarjoavat parempaa suojausta, kuten tiukkoja roolipohjaisia käyttöoikeusjärjestelmiä (esim. IAM) ja tehokkaita turvallisuusratkaisuja. Lisäksi pilvipalveluiden käyttäjät noudattavat usein tarkempia turvallisuusohjeita. (MITRE n.d.-a.)

Windows-järjestelmät taas voivat olla heterogeenisiä ja paikallisesti hallittuja, mikä lisää haavoittuvuuksien määrää. Windows-haavoittuvuudet liittyvät usein käyttöjärjestelmävirheisiin, ohjelmistopäivityksiin ja puutteelliseen suojaamiseen. Pilvipalveluissa riskit painottuvat sen sijaan konfiguraatiovirheisiin, käyttöoikeusongelmiin ja tietojen suojaamiseen pilven monikäyttäjäympäristössä. (MITRE n.d.-b.)

3 Stuxnet

3.1 Vaasalainen yritys liittyen Stuxnetiin

Vaasan yritys, joka liittyy Stuxnetiin, on Vacon. Vacon valmisti taajuusmuuttajia, jotka olivat Stuxnetin kohteena. Taajuusmuuttajat olivat avainroolissa teollisuusprosessien ohjauksessa, ja Stuxnet hyökkäsi niihin häiritäkseen prosessien toimintaa. (Linnake 2010)

3.2 Mitä Stuxnet tekee?

Stuxnet on monimutkainen haittaohjelma, joka on suunniteltu sabotoimaan teollisuuden ohjausjärjestelmiä, erityisesti uraanin rikastukseen käytettyjä sentrifugeja. Se hyödyntää useita zero-day-haavoittuvuuksia ja asentaa Windows-juuripaketin, joka piilottaa sen toiminnot. Stuxnet manipuloi taajuusmuuttajia muuttamalla niiden toimintanopeutta, mikä johtaa koneiden fyysiseen vaurioitumiseen ilman, että operaattorit huomaavat ongelmaa heti. (MITRE n.d.-c.)

3.3 Kuka Stuxnetin takana voisi olla?

Stuxnetin uskotaan olevan valtiollisten toimijoiden, kuten Yhdysvaltojen ja Israelin, kehittämä. Haittaohjelma liittyy erityisesti Iranin Natanzin ydinlaitoksen rikastusprosessin sabotoimiseen, osana operaatio Olympic Games -nimellä tunnettua kyberhyökkäyskampanjaa. (Fruhlinger 2022).

4 Mobile-osion lukitusnäytön ohitustekniikat

MITRE ATT&CK® -kehyksessä on kolme pääasiallista mobiililaitteiden lukitusnäytön ohitustekniikkaa. Biometrinen huijaus (Biometric Spoofing), jossa hyökkääjä huijaa laitteiden biometristä tunnistusta, voidaan estää vaatimalla salasanaa laitteen käynnistyksen tai tietyn ajan kuluttua. Lukitusnäytön avauskoodin ohitus (Unlock Code Bypass) estetään käyttämällä aikakatkaisuprosesseja ja tietojen pyyhkimistä epäonnistuneiden yritysten jälkeen. Haavoittuvuuksien hyödyntäminen (Vulnerability Exploit) voidaan estää säännöllisillä ohjelmistopäivityksillä.
Torjuntakeinoihin kuuluvat monivaiheinen tunnistus, aikakatkaisuprosessit ja säännölliset päivitykset, jotka yhdessä parantavat mobiililaitteiden turvallisuutta. (MITRE n.d.-d.)

5 Supply Chain Compromise (ICS)

Supply Chain Compromise tarkoittaa, että hyökkääjä manipuloi tuotteen tai ohjelmiston toimitusketjua saadakseen pääsyn kohdeympäristöön. Tavoitteena on saastuttaa tuotteet ennen niiden päätymistä loppukäyttäjälle, mikä voi johtaa tietojen tai järjestelmien vaarantamiseen. Hyökkäykset voivat tapahtua missä tahansa toimitusketjun vaiheessa, kuten kehitystyökaluissa, ohjelmistoissa tai jakelukanavissa. Esimerkiksi väärennetyt laitteet voivat aiheuttaa turvallisuusriskejä, ja troijalaiset voivat päästä järjestelmiin luotettavista lähteistä ladattujen ohjelmistojen kautta. (MITRE n.d.-e.)

6 Industroyer

Industroyer on haittaohjelma, joka on suunniteltu häiritsemään teollisuusohjausjärjestelmiä (ICS), erityisesti sähköasemien komponenteissa. Sitä käytettiin hyökkäyksissä Ukrainan sähköverkkoon joulukuussa 2016. Industroyer hyödyntää ICS-järjestelmien heikkouksia ja voi manipuloida I/O-portteja, esimerkiksi brute force -hyökkäyksillä, saadakseen hallinnan järjestelmiin ja aiheuttaakseen häiriöitä sähköverkon toimintaan (MITRE n.d.-f.)

7 Cellebrite ja Grayshift

Yritykset ja mobiililaitteiden haavoittuvuudet: Cellebrite ja Grayshift valmistavat laitteita ja ohjelmistoja, joita käytetään mobiililaitteiden tietojen purkuun ja analysointiin, usein lainvalvontakäytössä.
Haavoittuvuudet: Ne hyödyntävät mobiililaitteiden ohjelmistojen haavoittuvuuksia, kuten lukitusnäytön ohituksia, päästäkseen käsiksi tietoihin. (MITRE n.d.-g.)

8 Pohdinta

Kyberturvallisuus on monivaiheinen prosessi, joka vaatii jatkuvaa valppautta ja sopeutumista uusiin uhkiin. Mitre ATT&CK -viitekehys tarjoaa arvokasta tietoa eri ympäristöjen, kuten pilvipalveluiden, Windows-järjestelmien ja teollisuusohjausjärjestelmien haavoittuvuuksien tunnistamiseen. Haittaohjelmat kuten Stuxnet ja Industroyer osoittavat, kuinka vakavia seurauksia kyberhyökkäykset voivat aiheuttaa kriittisessä infrastruktuurissa. Mobiililaitteiden suojaus ja toimitusketjun kompromissien ehkäisy korostuvat myös, sillä haavoittuvuudet voivat olla vaikeasti havaittavissa. Turvallisuus edellyttää monivaiheisia suojakeinoja, säännöllisiä päivityksiä ja valppautta.

Lähteet

MITRE. (n.d. -a). Enterprise Matrix: Cloud. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/matrices/enterprise/cloud/

MITRE. (n.d. -b). Enterprise Matrix: Windows. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/matrices/enterprise/windows/

MITRE. (n.d.-c). Stuxnet, Software S0603. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/software/S0603/

Linnake, T. 2010. "*Stuxnet avasi koko teollisuuden silmät*". Ilta-Sanomat 25.11.2010. Päivitetty 25.11.2010. Viitattu 7.12.2024. https://www.is.fi/digitoday/tietoturva/art-2000001693533.html

Fruhlinger, J. 2022. ”Stuxnet explained: The first known cyberweapon”. csoonline 31.8.2022. Viitattu 7.12.2024. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

MITRE. (n.d.-d). Lockscreen Bypass, Technique T1461 - Mobile. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/techniques/T1461/

MITRE. (n.d.-e). Supply Chain Compromise, Technique T0862 - ICS. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/techniques/T0862/

MITRE. (n.d.-f). Industroyer, Software S0604. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/software/S0604/

MITRE. (n.d.-g). Replication Through Removable Media, Technique T1458 - Mobile. MITRE ATT&CK. Viitattu 7.12.2024. https://attack.mitre.org/techniques/T1458/

Liitteet

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko