jamk

2022 Ukraine Electric Power Attack

Case study

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Case Study
Hyökkäykset ja puolustusmenetelmät sekä suojaaminen, TTC6040-3009
Palautuspäivä
Tieto- ja viestintätekniikan insinööri tutkinto

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Taulukot

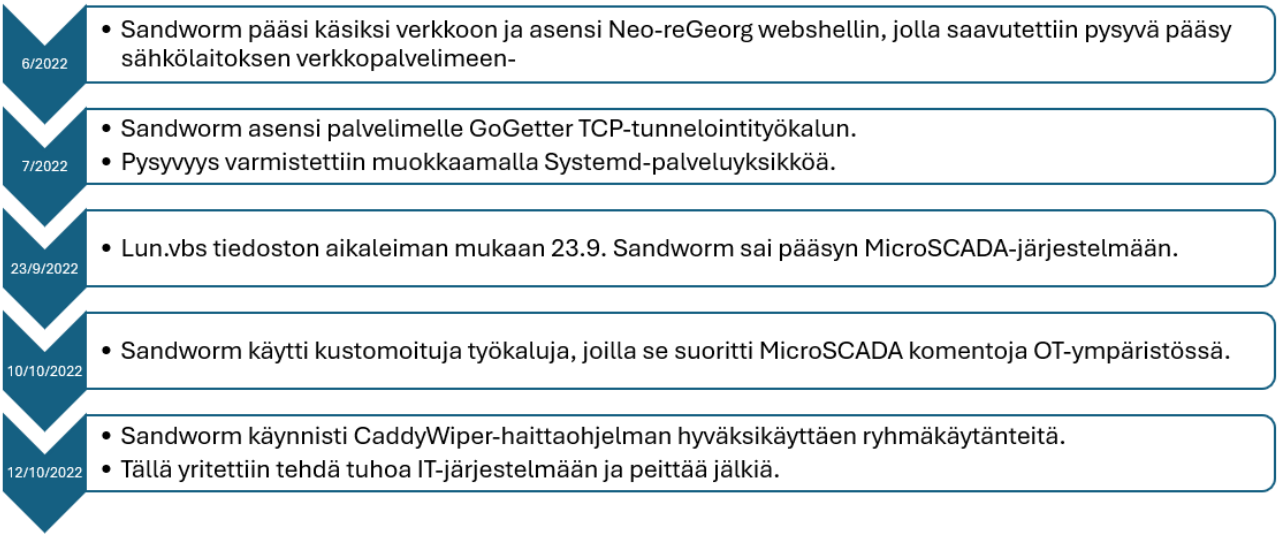
1 Johdanto

Tämä tapaustutkimus keskittyy Ukrainaan kohdistettuun kyberhyökkäykseen, joka tunnetaan nimellä 2022 Ukraine Electric Power Attack. Hyökkäyksen suoritti Sandworm- niminen hyökkääjäryhmä, joka sabotoi Ukrainan sähkönjakelua ja sähköverkkoa. Sandworm toimii Venäjän armeijan alaisena. Kyseinen ryhmä on suorittanut samanlaisia hyökkäyksiä Ukrainaa kohtaan vuosina 2015 ja 2016 sekä vaikuttanut muun muassa Ranskan vuoden 2017 presidentin vaaleihin. (2022 Ukraine Electric Power Attack. 2024.)

Tässä tapaustutkimuksessa on tarkoituksena perehtyä hyökkäyksessä käytettyihin taktiikoihin, tekniikoihin ja käytänteisiin (TTP), hyökkääjään, hyökkäyksen aikajanaan, hyökkäyksen paljastumiseen ja suojautumiskeinoihin.

2 Hyökkäys

Ukrainan sähkönjakeluun kohdistuva kyberhyökkäys alkoi kesäkuussa 2022 tai mahdollisesti jo ennen sitä. Tietoon ei ole saatu hyökkäyksen tarkkaa päivämäärää, sitä miten hyökkääjä pääsi sisään IT-järjestelmään tai kuinka ryhmä suoritti tiedustelua kohteen ympäristöstä. Hyökkäys saavutti huippunsa saman vuoden lokakuussa, kun hyökkääjäryhmä onnistui vaikuttamaan Ukrainan sähkönjakeluun. Hyökkäyksen yhteydessä hyökkääjä sai pyyhittyä laajasti omia jälkiään, jonka vuoksi osa saaduista tiedoista on puutteellisia. (Black, D., Brubaker, N., Lunden, K., McLellan, T., Proska, K., Sistrunk, C., Wilson, J., Wolfram., Zafra, D., 2023.)



Kuvio 1. Aikajana

2.1 Tiedustelu

Kohteeseen suoritetun tiedustelun toteutustapaa ei ole voitu varmentaa luotettavasti. Aiempien tapausten perusteella voitaisiin olettaa, että ryhmä on käyttänyt verkkojen haisteluun esimerkiksi

intercepter-NG työkalua. Ryhmä on aiemmin käyttänyt tiedusteluun taktiikoita kuten haavoittuvuusskannaukset sekä identiteettien, henkilöiden ja palvelin ominaisuuksien kalastelu. (Black ym. 2023; Sandworm Team. 2024.)

2.2 Aseistaminen

Hyökkäyksessä käytettiin Living Off The Land (LOTL) menetelmiä, jossa hyödynnetään mahdollisimman paljon järjestelmistä jo löytyviä työkaluja, kuten PowerShell ja WMI, sekä järjestelmästä jo löytyviä komentokieliä kuten python.

Sandworm hyödynsi myös muutamaa ulkopuolista ohjelmaa hyökkäyksessään:

1. Neo-REGEORG, joka mahdollistaa etäkomentojen suorittamisen kohteessa.
2. GOGETTER, Golang-ohjelmointikielellä kirjoitettu ohjelma, joka mahdollistaa viestinnän salaamisen ja suojaa hyökkääjää havaitsemiselta.
3. CADDYWIPER, disk wiper -haittaohjelma, jolla peitetään jälkiä ja tuhotaan tiedostoja järjestelmässä hyökkäyksen jälkeen.
4. TANKTRAP, disk wiper -haittaohjelma, joka keskittyy enemmän järjestelmän täydelliseen tuhoamiseen.

2.3 Toimittaminen

Tapaa, jolla Sandworm sai toimitettua haitalliset ohjelmistot sähkölaitoksen ympäristöön ei ole voitu todentaa, mutta voimme tutkia hyökkääjän aiemmin käyttämiä tekniikoita ja luoda kuva Toimittamis- vaiheesta.

Aiemmin hyökkääjä on käyttänyt usein spear phising -hyökkäyksiä, joissa yhreille lähetetään kohdennettuja sähköposti viestejä, jotka sisältävät haitallisia liitteitä tai linkkejä. Esimerkiksi 2015 ukrainan sähköverkkoon kohdistetussa hyökkäyksessä ryhmä levitti taktiikalla BlackEnergy-haittaohjelmaa. (Sandworm Team.)

Toinen todennäköinen taktiikka on Exploiting Public-facing applications, jossa hyödynnetään julkisesti näkyvien verkkosovellusten haavoittuvuuksia. Näihin haavoittuvuuksiin pääsee käsiksi helposti internetin kautta ja pystytään tätä kautta luomaan kompromissi järjestelmään. (Sandworm Team.)

2.4 Hyväksikäyttö

Hyökkääjä sai pääsyn operatiiviseen ympäristöön suorittamalla komentoja MicroSCADA järjestelmässä. Kyseinen MicroSCADA versio oli end-of-life (EOL) tilassa, joka tarkoittaa sitä, että kyseinen versio ei ole enää valmistajan tai version tarjoajien tukema. Sandworm pääsi käsiksi hypervisoriin, joka isännöi SCADA ympäristöä ja ajoi ISO kuvana nimeltään a.iso virtuaalisena Cd-levynä. Kyseinen ISO tiedosto sisälsi ainakin tiedostot lun.vbs sekä n.bat. (Black ym. 2023.)

2.5 Asentaminen

Sandworm asensi verkkoon yhteydessä olevalle palvelimelle Neo-REGEORG webshell haittaohjelman, jonka avulla he saavuttivat pysyvyyttä ja pystyivät kiertämään palomuureja ja muita rajoituksia. Noin kuukausi ensimmäisen pääsyn jälkeen Sandworm asensi GOGETTER-ohjelman. Se toimi tunnelina ja ohjasi viestintää palvelimeen, johon on yhdistetty ipv4-osoite 190.2.145.24. (Black ym. 2023.

2.6 Komentaminen ja kontrollointi

Sandworm aktivoi GOGETTER ohjelman, jonka avulla avattiin TLS yhteys palvelimelle. Sandworm hyödynsi Systemd palveluyksikköä, jolla se mahdollisti toiminnan jatkuvuuden, vaikka kohteen järjestelmä sammutettaisiin välissä. Tämä mahdollisti sen, että järjestelmän uudelleenkäynnistämisen yhteydessä myös GOGETTER-ohjelma käynnistyi uudelleen ja Sandworm säilytti pääsynsä järjestelmään ja mahdollisti hyökkäyksen jatkuvuuden. (Black ym. 2023.)

```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeoutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Kuvio 2. Systemd konfiguraatio. (Black ym. 2023.)

2.7 Toiminta kohteessa

Hyökkääjä otti käyttöön CADDYWIPER ja TANKTRAP- haittaohjelmat sen jälkeen, kun se oli varmistanut pääsynsä järjestelmään ja pystyi hallitsemaan sitä. Haittaohjelmien tarkoituksena oli tuhota tietoja ja lamauttaa Ukrainan sähköverkon toiminta. CADDYWIPER korruptoi ja tuhosi tiedostoja sekä peitti hyökkääjän jälkiä, kun taas TANKTRAP:n tarkoituksena oli tuhota kriittisiä tiedostoja sähköverkon lamauttamiseksi. Hyökkäyksellä onnistuttiin vaikuttamaan sähköasemien hallintaa ja siten sähkönjakeluun, joka johti laajamittaisiin sähkökatkoihin. (Black ym. 2023.)

3 Hyökkäyksen havaitseminen ja vastatoimenpiteet

Ukrainaan kohdistettua 2022 Ukraine Electric Power Attack hyökkäystä ei havaittu, joka johti sen onnistumiseen kaikessa hiljaisuudessa. Kyberhyökkäyksiltä on kuitenkin mahdollista puolustautua panostamalla niiden ennaltaehkäisyyn, havaitsemiseen ja tarvittaviin vastatoimenpiteisiin.

3.1 Havaitseminen

Hyökkäysten havaitsemiseksi olisi kriittistä suorittaa laajaa operatiivisen verkon monitorointia tunnettujen uhkien tunnusmerkkien huomaamiseksi, esimerkiksi tunnetut epäilyttävät ip osoitteet ja tiedostot. On myös suositeltavaa suorittaa ennalta ehkäisevää uhkien metsästystä, jonka ansiosta voidaan tunnistaa haitallisia taktiikoita, tekniikoita ja käytänteitä ympäristöstä. Näin saadaan mahdollisuus pysäyttää hyökkäys ennen merkittävää vahinkoa. (Dragos, Inc. 2023.)

Tässä kyseisessä hyökkäyksessä uhkien metsästyksen ja monitoroinnin avulla olisi voitu havaita esimerkiksi seuraavia merkkejä hyökkäyksestä:

- Odottamattomia tiedoston siirtoja yritys verkosta tai ulkopuoliselta palvelimelta operatiiviseen verkkoon, erityisesti ISO tiedoston siirto SCADA järjestelmään.
- Odottamattomien skriptien suorittaminen sekä siirto SCADA palvelimella
- Odottamattomien komentojen suorittaminen SCADA palvelimilta etäpääte laitteille

3.2 Vastatoimenpiteet

Sandwormin toteuttaman hyökkäyksen vaikutuksia olisi voitu pienentää tai estää varautumalla hyökkäykseen etukäteen. Hyökkäyksen kohteella oli käytössään vanhentunut MicroSCADA-järjestelmä, eikä siihen ollut saatavilla enää viimeisimpiä turvallisuuspäivityksiä. Turvallisuuden kannalta on tärkeää pitää järjestelmät päivitettynä ja ajan tasalla, että hyökkääjät eivät voi niin helposti hyödyntää tunnettuja järjestelmän heikkouksia. Taulukossa 1 on käsiteltynä joitain hyökkäyksessä käytettyjä tekniikoita ja niiden vastatoimenpiteitä.

Taulukko 1. Hyökkäyksessä käytetyt tekniikat ja vastatoimenpiteet. (2022 Ukraine Electric Power Attack.)

Käytetty tekniikka	Ehdotettu vastatoimenpide
Komentojen ja skriptien tulkitsija: PowerShell	Sovellusten hallinnan käyttäminen siellä, missä se on tarpeen. PowerShellin rajoitettua tilaa (Constrained Language Mode) voidaan käyttää rajoittamaan pääsyä arkaluonteisiin tai muuten vaarallisiin kielen elementteihin, kuten niihin, joita käytetään mielivaltaisten Windows-API-kutsujen tai tiedostojen suorittamiseen.
Järjestelmän prosessien luonti ja muokkaus: Systemd palveluyksikkö	Ohjelmien asennusten rajoittaminen vain luotettuihin tietovarastoihin ja orpojen ohjelmistopakettien varominen.
Datan tuhoaminen	Monitasoisten varmuuskopiointien tekeminen ja säännöllinen testaaminen.
Protokollien tunnelointi	Epäluotettavan tai haitallisen verkkoliikenteen estäminen verkkoliikenteen suodattamissääntöjen määrittelyn avulla.

Skriptaukset	Järjestelmän toimintojen, kuten käyttäjätileihin, palveluihin, järjestelmäkutsuihin, rekisteriin ja verkkoyhteyksiin pääsyn rajoittaminen sovellusten eristämisellä ja hiekkalaatikoiden (sandbox) käytöllä.

4 Pohdinta

Sandwormin hyökkäys Ukrainan sähköverkkoon oli mielenkiintoinen hyökkäys tutustua. Aihetta tukiessa oli mielenkiintoista päästä tutustumaan erilaisiin hyökkäystekniikoihin ja kuinka niitä sovellettiin. Hyökkäyksen tutkiminen oli hyvä ensikosketus erilaisiin suojaus- ja hyökkäysprotokolliin.

Hyökkäys olisi mahdollisesti ollut estettävissä, jos järjestelmät olisivat olleet ajan tasalla, eikä niissä olisi käytetty versioita, joille ei ole enää saatavilla valmistajan tukea. Tämä korostaa hienosti sitä, miten yksinkertaisilla asioilla on mahdollista estää suuria vahinkoja.

Tapauksesta näkee myös sen, miten onnistuneen hyökkäyksen ja jälkien peittelyn seurauksena tapausta on vaikea selvittää jälkikäteen. Sandworm sai peitettyä jälkiään sen verran hyvin, että tutkijoilla ei ole vieläkään tiedossa, miten järjestelmään on alun perin päästy sisälle.

Tehtävän aikana pääsimme hyödyntämään jo opittuja tiedonhakutaitoja ja kehittämään niitä. Tehtävä oli myös hyvä kertaus JAMK:n ohjeen mukaiseen raportointiin.

Lähteet

2022 Ukraine Electric Power Attack. Mitre ATT&CK. 2024. Viitattu 4.9.2024. https://attack.mitre.org/campaigns/C0034/

Dragos, Inc. 2023. ELECTRUM Targeted Ukrainian Electric Entity using Custom Tools and CaddyWiper malware, October 2022. Viitattu 4.9.2024. https://www.dragos.com/blog/new-details-electrum-ukraine-electric-sector-compromise-2022/

Vasquez, C., Vicens, A. 2023. Russian hackers disrupted Ukrainian electrical grid last year. Cyberscoop 9.11.2023. Viitattu 9.9.2024. https://cyberscoop.com/sandworm-russia-ukraine-grid/

Black, D., Brubaker, N., Lunden, K., McLellan, T., Proska, K., Sistrunk, C., Wilson, J., Wolfram., Zafra, D., 2023. Sandworm Disrupts Power in Ukraine Using a Novel Attack against Operational Technology. Google Cloud. Viitattu 9.9.2024. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

Sandworm Team. Mitre ATT&CK. 2024. Viitattu 4.9.2024. https://attack.mitre.org/groups/G0034/