Kibertámadási trendek és ajánlott védekezési eljárások kritikus infrastruktúráknál

Busa Attila József
MH KIMK, Képzési- és Gyakorlattámogató Osztály,
Kiber Képzési Alosztály
kibervédelmi tanácsos

BRU Infosec Kft.
alapító tag, ügyvezető

Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
1.éves doktorandusz hallgató

2023. 11. 22.

Vázlat

- Kritikus infrastruktúra elemnek tekinthető-e a az ellátási lánc?
- SolarWinds
- Industroyer
- Industroyer2 vs. DataWiper
- Összefoglalás

Az ellátási lánc lehet-e kritikus infrastruktúra

Az ellátási lánc közvetlenül nem jelenik meg a kritikus infrastruktúrák felsorolásánál, ha szigorúan értelmezzük a 2012. évi CLXVI. törvényt. Azonban mindenhol megjelenhet, mint kritikus infrastruktúrát kiszolgáló rendszerelem, hiszen a rendelkezésre állás kiemelkedően fontos ezeknél a szervezeteknél, mivel számos gazdasági, társadalmi és egyéb terület működését meghatározó elemeket foglal magában.

Az ellátási lánc a termelőktől a fogyasztókig terjedő hálózatot jelent, amely a nyersanyagok beszerzésétől a gyártáson, az elosztáson és a kiszállításon keresztül a végfelhasználókig terjedő folyamatokat foglalja magában.

Az ellátási lánc kritikus jelentőségű a gazdasági stabilitás és a társadalmi működés szempontjából

Az ellátási lánc ellen irányuló támadások felerősödése

Az ellátási lánc elleni támadás a szervezetek és beszállítóik közötti kapcsolatot veszi célba. Egy támadás akkor tekinthető ellátási lánc komponenssel rendelkezőnek, ha legalább két támadás kombinációjából áll. Ahhoz, hogy egy támadás ellátási láncot érintő támadásnak minősüljön, a szállítónak és a vevőnek egyaránt célpontnak kell lennie. A SolarWinds volt az egyik első ilyen jellegű támadás, amely megmutatta az ellátási láncot érintő támadások potenciális hatását.

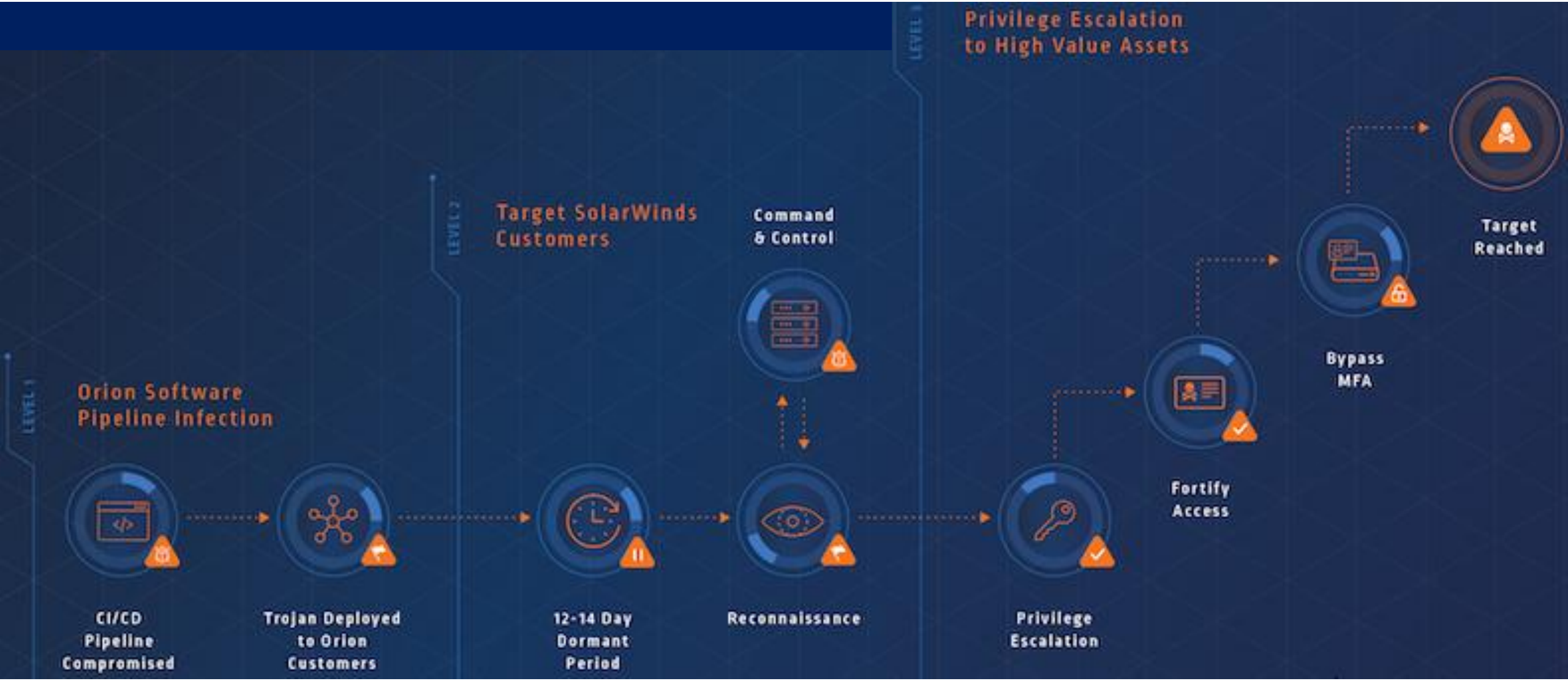
SOLARWINDS

SolarWinds

SolarWinds Orion Platform ellen irányult támadás, amely egy sikeres kiberbiztonsági incidens volt, és 2020 decemberében vált ismertté. Ezt a támadást ismertté vált "SolarWinds-hack" vagy "Sunburst" néven ismerik.

1. A támadók a SolarWinds Orion Platformba bejutva manipulálták az egyik szoftverfrissítést, amelyet a SolarWinds ügyfelek automatikus frissítési rendszere használt.
2. Az ártalmas szoftver egy backdoor-t nyitott meg a rendszereken, amelyen keresztül a támadók további tevékenységeket folytathattak a célpontokban.
3. A támadók további lépéseket tettek a célpontokban, és információkat gyűjtöttek, illetve hozzáférést szereztek a célcsoportok hálózati rendszereihez.

SolarWinds támadási lánc



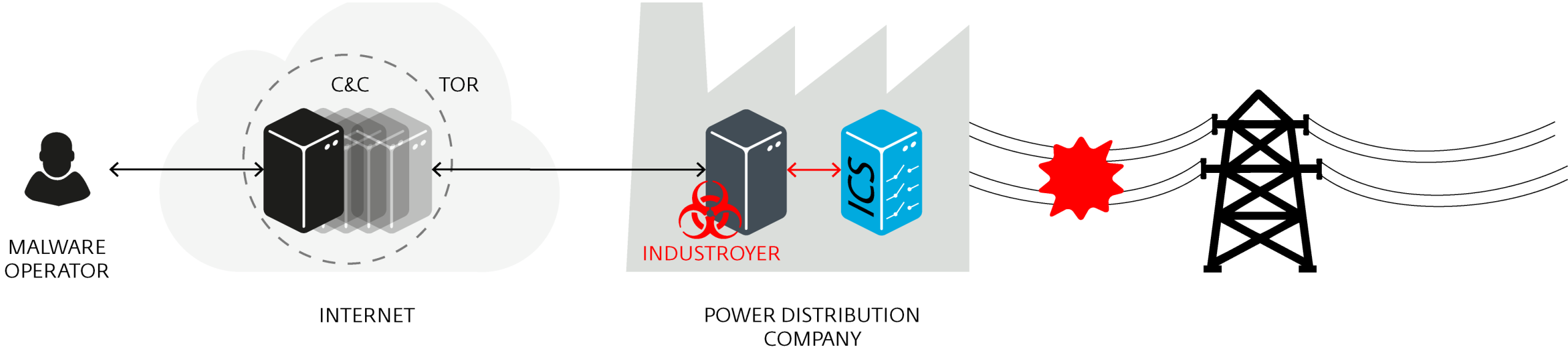
Konklúzió

- Az újonnan megjelenő szoftverfrissítések vizsgálata elengedhetetlen a szervezet biztonságos működése szempontjából (sandbox).
- Erős autentikáció és jogosultságkezelés.
- Network Monitoring és Threat Detection. Belső és külső határvédelmi rendszer fontossága (SIEM, NGFW, TOC/SOC).
- „Üzemeltetési szemlélet” csökkentése.
- Kiberbiztonsági tudatosság és képzés.

Industroyer

- Célpont: 2016, ukrán energiahálózat

Képes közvetlenül irányítani az elektromos alállomások kapcsolóit és megszakítóit. Ezek a kapcsolók és megszakítók az analóg kapcsolók digitális megfelelői. Így a potenciális hatás az áramelosztás egyszerű kikapcsolásától kezdve a tényleges meghibásodásokon át a berendezések súlyosabb károsodásáig terjedhet.

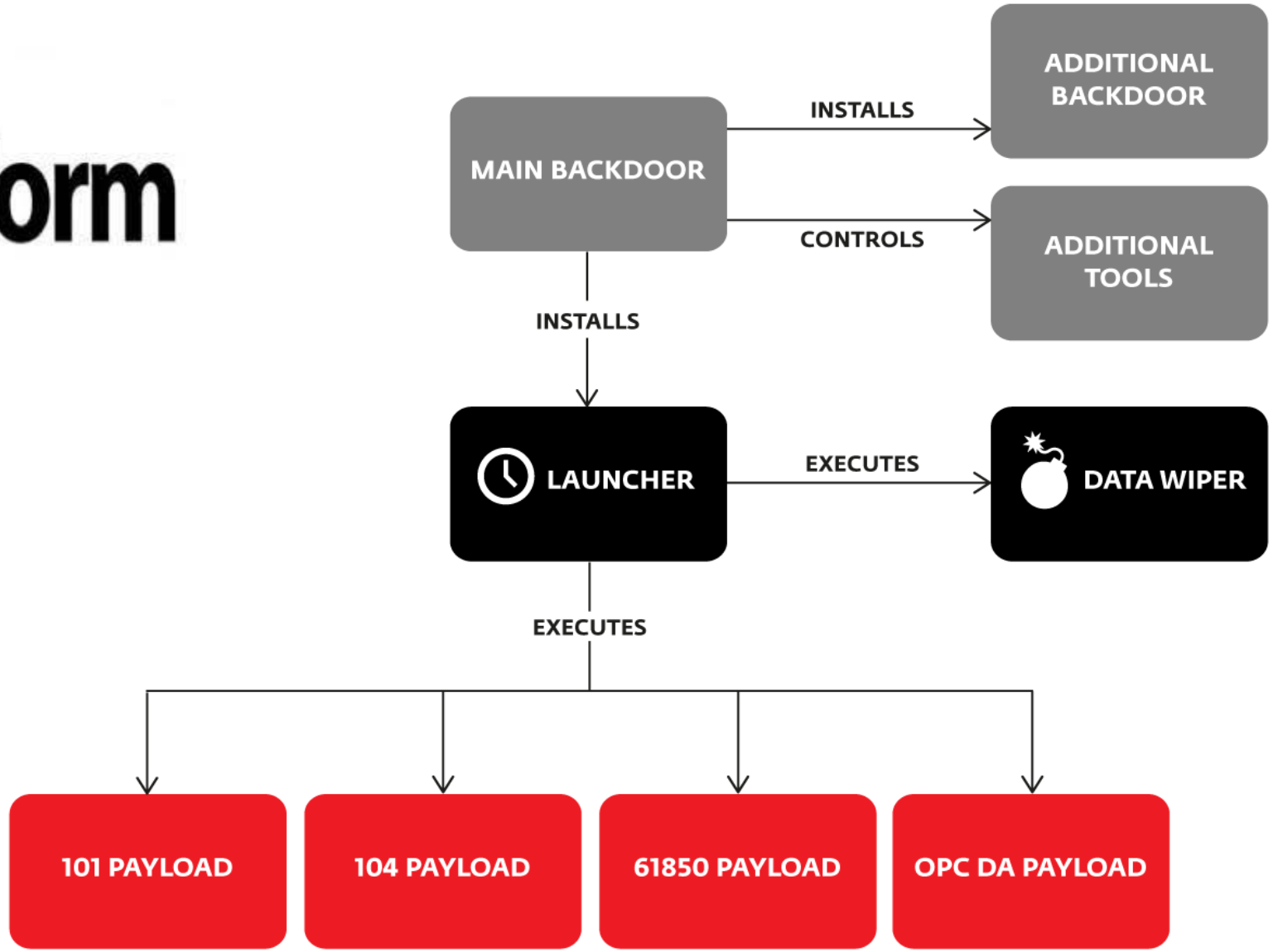


Industroyer technikai háttere

- Helyi proxyval hitelesíti magát a belső hálózaton keresztül a backdoor telepítése előtt.
- A hitelesítés után HTTP-csatornát nyit a külső a C2 szerver felé. A későbbi kommunikáció ezt követően a belső proxyn zajlik.
- Létrehoz egy fertőzött fájlt a helyi rendszeren (melyen keresztül életben tartja a kapcsolatot), amely egy futó szerviz szolgáltatáshoz kapcsolódik.
- A megfertőzött szolgáltatás folyamatosan nyitva tartja a backdoor-t, úgy, hogy előre meghatározott időközönként újranyitja a kapcsolatot a támadó szerver felé, így a rosszindulatú program továbbra is fut az újraindítások után is.

Industroyer támadási mechanizmusa

SandWorm



Konklúzió

Az Industroyer rendkívül testreszabható malware.

Az általános kommunikációs protokollok némelyikét használja.

Az elemzett kódsorok egyes összetevőit úgy tervezték, hogy specifikus, ipari környezetben használatos hardvereket célozzanak meg, ezért figyelmeztető jelként kell szolgálnia a kritikus rendszerek biztonságáért felelős személyek számára világszerte.

Kiegészítő védelmi intézkedések

- **Hálózati szegmentálás:** Az ipari irányító rendszerek és hálózatok szegmentálása, vagyis elkülönítése, segíthet minimalizálni a támadó terjedését, ha az egyik területet érinti.
- **Biztonsági mentés és visszaállítási terv:** Rendszeres biztonsági mentéseket kell készíteni a kritikus rendszerekről, és visszaállítási terveket kell kidolgozni. Ez lehetővé teszi a gyors helyreállítást és a működési szünet minimalizálását, ha egy támadás vagy károsítás történik.

Industroyer 2

Célpont: az ukrán energetikai vállalat.

Támadás időpontja: A beavatkozást 2022.04.08-ra tervezték, de a jelek arra utalnak, hogy a támadást legalább két héttel előtte előkészítették.

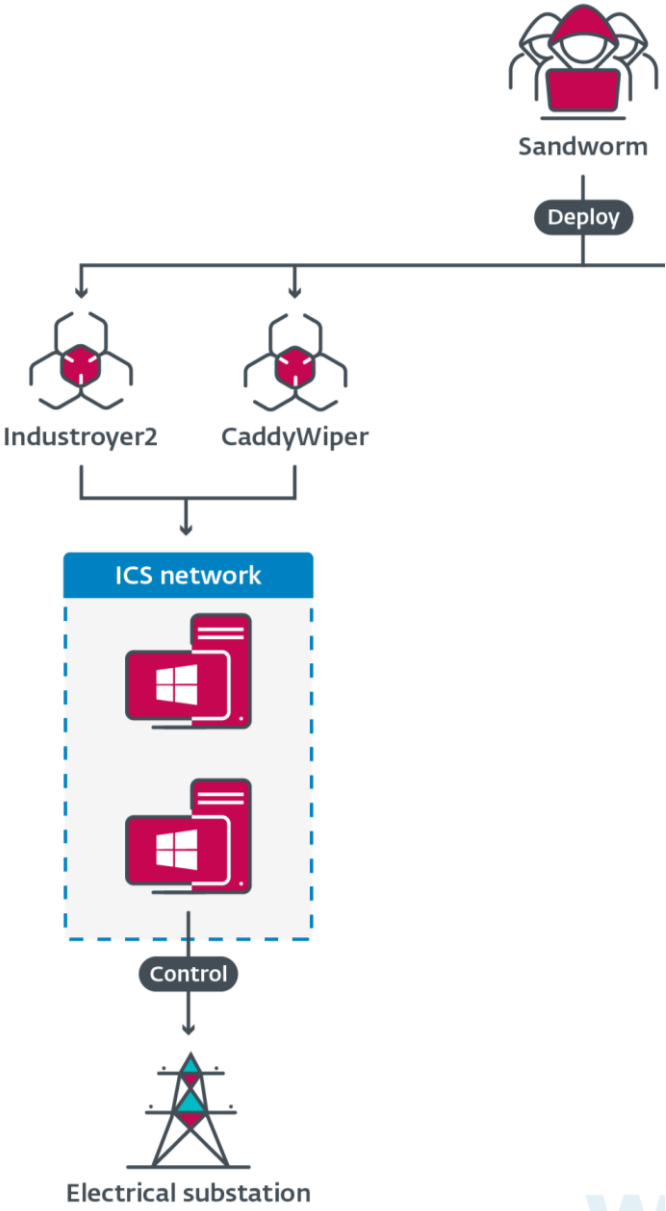
A támadásban ICS-képes rosszindulatú szoftvereket és Windows, Linux és Solaris operációs rendszerekhez alkalmazható lemeztörlőket használtak. Nagy valószínűséggel a támadók az Industroyer rosszindulatú szoftver új verzióját használták, amelyet 2016-ban az ukrajnai áramkimaradáshoz használtak.

Industroyer 2

Az Industroyer2 mellett a Sandworm több pusztító kártevő családot is használt, köztük a CaddyWiper-t.

A CaddyWiper-t először 2022.03.14-én fedezték fel, amikor egy ukrán bank ellen használták.

A CaddyWiper egy változatát 2022.04.08 14:58-án ismét felhasználták a korábban említett ukrán energiaszolgáltató ellen.



Industroyer 2

- Az Industroyer2-t egyetlen Windows futtatható fájlként telepítették, amelynek neve 108_100.exe, és egy ütemezett feladat segítségével 2022.04.08-án 16:10:00 UTC-kor futtatta le. A PE időbélyege szerint 2022.03.23-án állították össze, ami arra utal, hogy a támadók több mint két hétig tervezték a támadást.
- Az Industroyer2 nagymértékben konfigurálható. Részletes konfigurációt tartalmaz a testében, amely a rosszindulatú programok műveleteit vezérli. Ez eltér az Industroyer-től, amely a konfigurációt egy különálló .INI fájlban tárolja.
- A rosszindulatú szoftver megszüntet egy legitim folyamatot, amelyet a szokásos napi műveletek során használnak. Ráadásul átnevezi ezt az alkalmazást úgy, hogy a fájlnévhez .MZ-t ad hozzá. Ezt azért teszi, hogy megakadályozza a valódi folyamat automatikus újraindulását. Ez a komponens képes bizonyos ICS-rendszereket vezérelni az áramellátás leállítása érdekében.

Industroyer 2

- A CaddyWiper egy loader segítségével a Hex-Rays IDA Pro szoftver egyik legális komponensének, konkrétan a távoli IDA debugger szerver win32_remote.exe fájljának javított változatának álcázták.
- A patch-elt bináris kód egy fájlból tölti be a titkosított shellcode-ot, amely a CaddyWiper kissé módosított változata. Ez törli a meghajtó partícióinak kiterjesztett információit: a Master boot record (MBR) vagy a GUID Partition Table (GPT). Ezáltal a gép indíthatatlanná válik.
- A megtámadott energiavállalat hálózatán további, Linux és Solaris rendszert futtató, pusztító hatású kártevőket is találtak. A támadásnak két fő összetevője van: egy féreg és egy wiper.

Konklúzió

A jövőben várható, hogy a kritikus infrastruktúrákat célzó kibertámadások elszaporodnak. A törlőautomatizmussal kiegészített új Industroyer jellegű támadásokra nagy eséllyel számíthatunk a jövőben is.

A védekezés módja (az eddig említetteken felül) talán az lehet, hogy a nyilvánosságra került támadókódokat át kell elemezni és hozzájuk kell igazítani a védelmi rendszerek biztonsági szabályait.

Idővel nagy eséllyel a mesterséges intelligencia is sikeresen besegíthet majd az ilyen típusú támadások időben történő megállításához.

Összefoglalás

A technológiai fejlődés és a digitalizáció folyamatosan növekszik. Az ipari irányító rendszerek, az energiaellátás, a víz- és hulladékkezelés, a közlekedés és más kritikus infrastruktúrák szorosan kapcsolódnak a digitális technológiákhoz. Ezáltal a kritikus infrastruktúrák egyre sebezhetőbbek lesznek a kibertámadásokkal és a kibertérben jelentkező fenyegetésekkel szemben.

A kiberfenyegetések egyre kifinomultabbá válnak, és azok, akik támadásokat indítanak, egyre növekvő erőforrásokkal és szaktudással rendelkeznek. Ezért nagyon fontos, hogy a védelem oldaláról is tisztában legyünk az aktuális támadási trendekkel a sikeres védekezésre való felkészülés érdekében.

Kérdések?

Források

- CyberArk Blog Team: The Anatomy of the SolarWinds Attack Chain https://www.cyberark.com/resources/blog/the-anatomy-of-the-solarwinds-attack-chain (letöltve: 2023.11.18.)
- Industroyer: Biggest threat to industrial control systems since Stuxnet https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (letöltve: 2023.11.18.)
- MalPedia for win.industroyer https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer (letöltve: 2023.11.18.)
- How Kaspersky Industrial CyberSecurity deals with an APT based on Industroyer malware https://www.kaspersky.com/enterprise-security/mitre/industroyer (letöltve: 2023.11.18.)
- WIN32/INDUSTROYER A new threat for industrial control systems https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf (letöltve: 2023.11.18.)
- CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf (letöltve: 2023.11.18.)
- ENISA Threat Landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (letöltve: 2023.11.18.)
- Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (letöltve: 2023.11.18.)
- Kiberbűnözők célpontja lett az energiaszektor https://greendex.hu/kiberbunozok-celpontja-lett-az-energiaszektor/ (letöltve: 2023.11.18.)
- Kibertámadás is okozhatta a pakisztáni áramszünetet https://nki.gov.hu/it-biztonsag/hirek/kibertamadas-is-okozhatta-a-pakisztani-aramszunetet/ (letöltve: 2023.11.18.)
- WeLiveSecurity by ESET: Industroyer2 Industroyer reloaded https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (letöltve: 2023.11.18.)

Köszönöm a figyelmet!