Infokommunikáció 2025

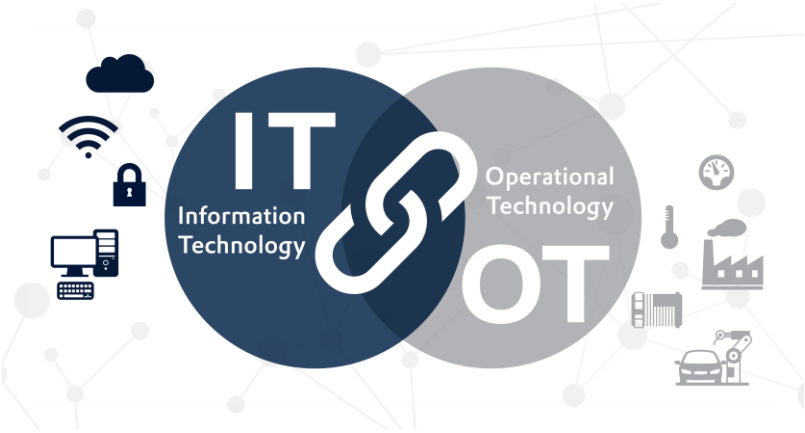
KRITIKUS INFRASTRUKTÚRÁK A DIGITÁLIS HARCMEZŐN

Busa Attila József
MH KIMK, Képzési Osztály
osztályvezető
BRU Infosec Kft.
ügyvezető
Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
3. éves doktorandusz hallgató

VÁZLAT

- InfoSec vs. ITSec vs. OTSec
- Mik lehetnek kritikus infrastruktúrák?
- Miért sérülékenyebbek az OT területek?
- Van-e megoldás?
- Mit hoz a jövő?

INFOSEC VS. ITSEC VS. OTSEC



Information Security

„Információ Biztonság”

Magának az információnak (digitális vagy kézzel fogható) a védelme.

Bizalmasság (**C**onfidentiality), sértetlenség (**I**ntegrity), rendelkezésre állás (**A**vailablity) elve.

Information Technology Security

„Informatikai Rendszerek Biztonsága”

security

Igyekeznek a CIA mindhárom alapelvét betartani.

Operational Technology Security

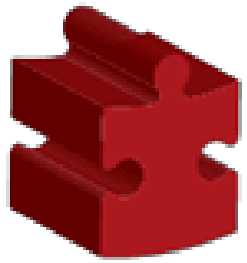
„Ipari vezérlőrendszerek Biztonsága”

safety

Alapvetően az állandó rendelkezésre állás a fő kritérium ezeknél a rendszereknél.

MIK LEHETNEK KRITIKUS INFRASTRUKTÚRÁK?

Kritikus Infrastruktúra



LÉTFONTOSSÁGÚ RENDSZER, AMELY ELENGEDHETETLEN A LÉTFONTOSSÁGÚ TÁRSADALMI VAGY GAZDASÁGI FOLYAMATOKHOZ.

Energia

Ivóvízellátás

Banki szolgáltatások

Élelmiszeripar és mezőgazdaság

Közbiztonság védelem

Digitális infrastruktúra

Közlekedés

Pénzügyi Piaci Infrastruktúrák

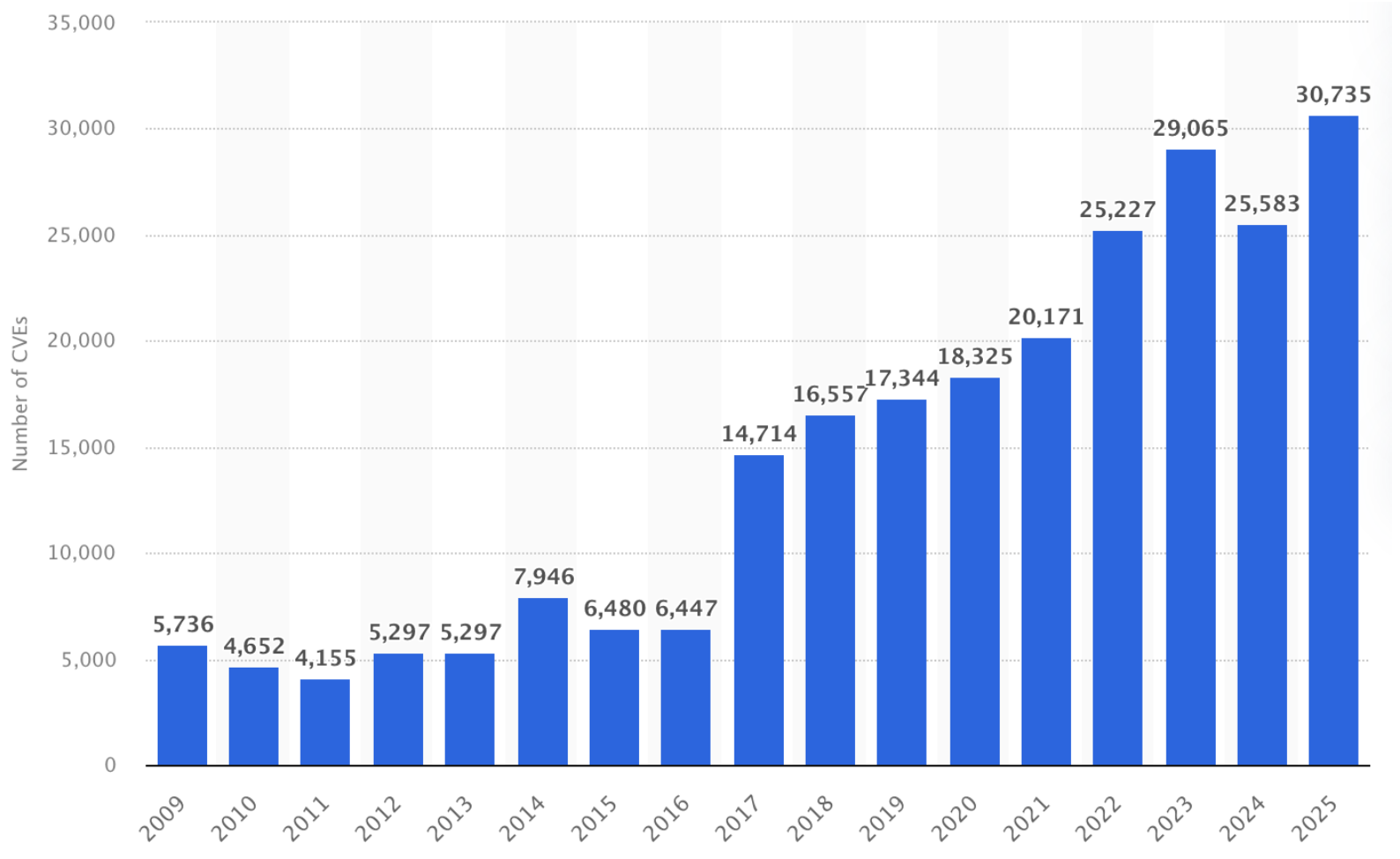
Egészségügyi ellátó létesítmények

Ezeket vezérlik az ipari vezérlőrendszerek!

MIÉRT SÉRÜLÉKENYEBBEK AZ OT TERÜLETEK?

- Sok OT-rendszer évtizedekig működik frissítés nélkül, így gyakran futnak rajtuk támogatás nélküli régi operációs rendszerek (pl. Windows XP, Windows 7).
- A szétválasztás az IT és OT rendszerek között megszűnt, egyre gyakoribb az összekapcsolódás, ami lehetővé teszi, hogy az IT rendszer kompromittálása után a támadó az OT hálózatra is beléphessen. (Hogyan kapcsolódhat ide az IoT Sec?)
- Az ipari hálózati protokollok (pl. Modbus, ION, DCS, SCADA) gyakran autentikáció és titkosítás nélkül működnek, így lehallgatható vagy manipulálható az adatforgalom.
- Az esetleges leállások magas kockázatot jelentenek.
- Gyenge, vagy alapértelmezett jelszavak használata, elavult belépési protokollok alkalmazása szintén kockázatot jelent az ipari környezetek számára.
- Helytelen felsővezetői gondolkodás?

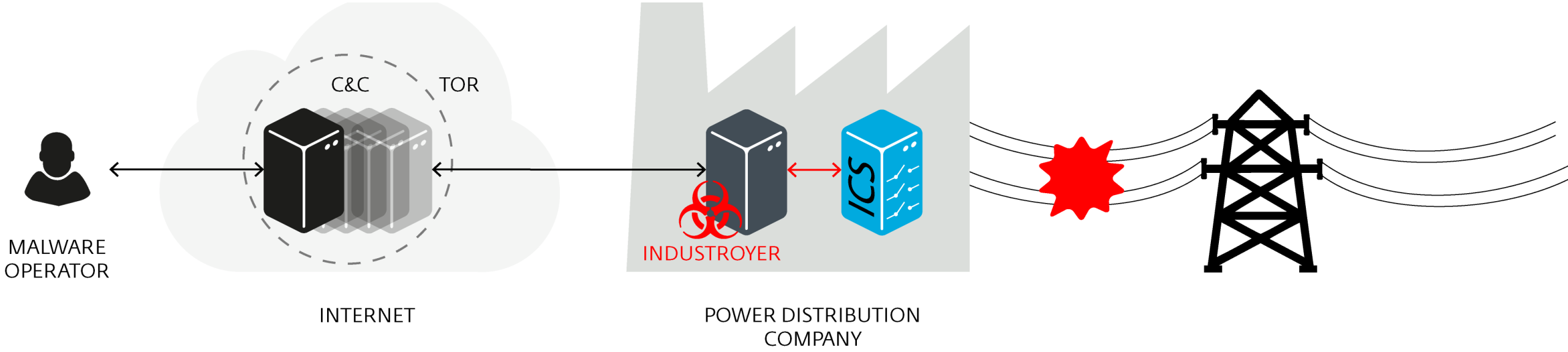
AZ ELMÚLT NÉHÁNY ÉV „FELFEDEZETT” SÉRÜLÉKENYSÉGEINEK STATISZTIKÁJA.



INDUSTROYER

- <u>Célpont:</u> 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.

JAVASOLT 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.

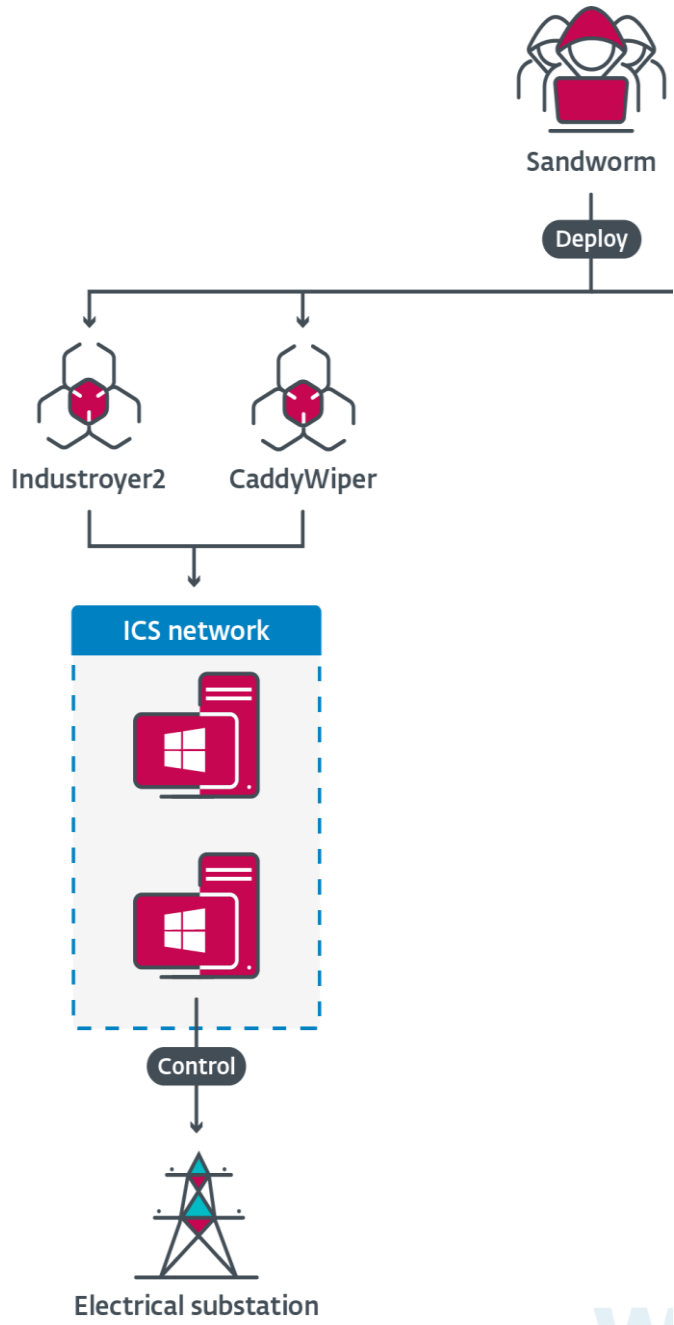
A támadásban ICS-képes rosszindulatú szoftvereket és Windows, Linux és Solaris operációs rendszerekhez alkalmazható lemeztörlőket használtak. Nagy valószínűséggel a támadók az Industroyer rosszindulatú szoftver új verzióját használták, amelyet 2016-ban az ukrajnai áramkimaradáshoz használtak.

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 ismét felhasználták a korábban említett ukrán energiaszolgáltató ellen.



MIT HOZ A JÖVŐ?

- 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. Ezért nagyon fontos, hogy a védelem oldaláról is tisztában legyünk az aktuális támadási trendekkel a sikeres védekezésre való felkészülés érdekében.

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: 2025.10.23.)
- 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: 2025.10.23.)
- MalPedia for win.industroyer https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer (letöltve: 2025.10.23.)
- How Kaspersky Industrial CyberSecurity deals with an APT based on Industroyer malware https://www.kaspersky.com/enterprise-security/mitre/industroyer (letöltve: 2025.10.23.)
- WIN32/INDUSTROYER A new threat for industrial control systems https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf (letöltve: 2025.10.23.)
- CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf (letöltve: 2025.10.23.)
- ENISA Threat Landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (letöltve: 2025.10.23.)
- Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (letöltve: 2025.10.23.)
- Kiberbűnözők célpontja lett az energiaszektor https://greendex.hu/kiberbunozok-celpontja-lett-az-energiaszektor/ (letöltve: 2025.10.23.)
- Kibertámadás is okozhatta a pakisztáni áramszünetet https://nki.gov.hu/it-biztonsag/hirek/kibertamadas-is-okozhatta-a-pakisztani-aramszunetet/ (letöltve: 2025.10.23.)
- WeLiveSecurity by ESET: Industroyer2 Industroyer reloaded https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (letöltve: 2025.10.23.)

Köszönöm a figyelmet!