A Davis-Besse atomerőmű esete a vírussal

A Cyberwar kifejezéssel jellemzően az olyan számítógépes támadásokat szokás illetni, ahol a támadás célirányos és a végrehajtás egyik eszköze a számítógépes hálózat, adott esetben az internet.

Ebben a történetben célirányos támadásról (szerencsére) nem beszélhetünk, de jól illusztrálja a modern technológiai rendszerek - ebben az esetben egy atomerőmű - sérülékenységét.

A történetet kezdjük a résztvevők bemutatásával:

Davis-Besse atomerőmű, Ohio

Az erőművet (Davis Besse Nuclear Power Station) az ohio-i Erie-tó partján, nem messze Oak Harbor-tól kezdték meg építeni 1971-ben. Hat évvel az első kapavágás után 925 MW teljesítményű reaktora üzembe állt, és csatolták a hálózatra.

Davis-Besse atomerőmű, Ohio

2002-ben a reaktortartályból bórsav szivárgott el, emiatt a berendezést két évre, 2004-ig leállították, és ez idő alatt javították és felújították. A berendezés felügyeleti rendszere ez idő alatt is üzemben maradt.

SQL Slammer

Az SQL Slammer egy olyan számítógépes féreg, ami a Microsoft SQL Server 2000 egy, még befoltozatlan hibáját kihasználva puffer túlcsordulást okozott a betámadott adatbázisokban.

Habár a Microsoft 2002-ben kiadott egy javítócsomagot, nagyon sok gépen ez nem került telepítésre. A Slammer **2003 január 25.-én** indult hódító útjára, és az első fél órában 75.000 számítógépet sikerült megfertőznie.

A két szereplő találkozása

Az erőmű belső rendszere természetesen tűzfallal volt védve, azonban legalább egy csatlakozási pont megkerülte a tűzfalat, itt a féreg akadálytalanul jutott be a berendezésbe.

A fent említett javítócsomag az erőmű informatikusainak elkerülte a figyelmét, így a féreg a belső felügyeleti rendszert futtató Microsoft munkaállomásokat megtámadta.

A felhasználók **2003 január 25.-én**, 9:00 órakor a hálózat drasztikus lassulására figyeltek fel. 16:50-kor az un. Safety Parameter Display System (**SPD**) állt le. Az SPD felügyeli az erőműben a legfontosabb biztonsági mutatókat (hűtőrendszer, mag hőmérséklet-érzékelők, külső sugárzás érzékelők).

17:13-kor egy másik, igaz, kevésbé kritikus monitoring (SCADA) rendszer, a „Plant Process Computer” is kifagyott a féreg tevékenysége nyomán. Mindkét rendszer többszörös redundanciákkal és mentésekkel is rendelkezett, a lefagyás a közvetlen irányítástechnikára nem volt hatással, de az operátorok által a technológiai beavatkozás lehetősége az összeomlás idejére megszűnt.

Az SPD rendszer helyreállítása majdnem 5, **az erőmű működésének normalizálása és teljes visszaállítása 6 órát vett igénybe**.

A felügyeleti rendszer kiesése a berendezés és a reaktor működését szerencsére jelentősen nem befolyásolhatta, mivel az karbantartás és átépítés alatt állt.

A féreg (Slammer) tevékenysége nem az erőmű ellen irányult, az pusztán beleesett a kártevő szórásába.

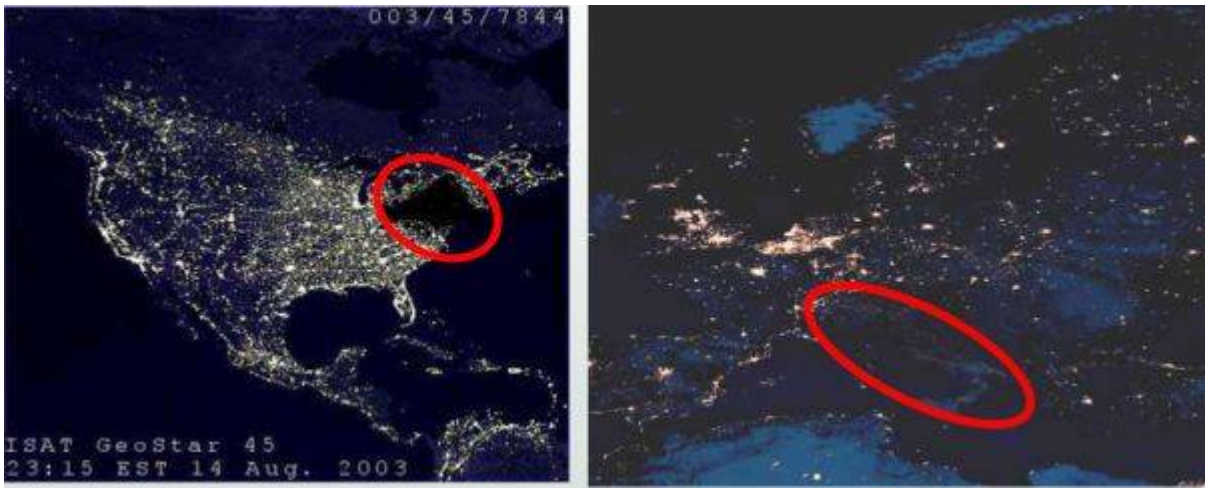
Rossz belegondolni annak a lehetőségébe, hogy a Slammer helyett valami Stuxnet-szerűség támadta volna meg a David-Besse-t. Az pedig Fukushima óta tudjuk, hogy a leállított (persze, a fukushima-i egy kényszerleállás volt, itt pedig egy tervezett technológiai leállás történt) atomerőmű még okozhat nagyon kellemetlen meglepetéseket, főleg, ha a hűtőrendszere kontroll és/vagy áram nélkül marad.

A Slammer támadás további találgatásokra is lehetőséget adott, ugyanis 2003-ban a villamos hálózati kiesések (blackout-ok) száma nagyon megemelkedett a további évekhez képest.

Hálózati kiesések 2003-ban:

- augusztus 14.: villamos hálózati kiesés az USA-ban, 50 millió ember maradt áram nélkül
- augusztus 28.: villamos hálózati kiesés Londonban
- szeptember 23.: villamos hálózati kiesés Dániában és Svédországban, 3 millió ember maradt áram nélkül

- szeptember 28.: villamos hálózati kiesés Olaszországban, 57 millió ember maradt áram nélkül
- október 5.: hálózati kiesés Athénban. A görög főváros több kerülete órákra áram nélkül maradt
- október 6.: hálózati kiesés Csehországban, Nyugat-Csehország egy fél órára áram nélkül maradt.



A villamos hálózati kiesések hatása az USA és Olaszország hálózatára

Persze a fenti hálózati kiesés hullám lehet akár a véletlen műve is, de amíg az atomerőművekben bekövetkező eseményekre szigorú jelentési előírások vonatkoznak, ez a hálózatüzemeltetőkre nem feltétlenül igaz.

Great bugs

Egy számomra *„kedves”* és közelálló témát szeretnék egy blogsorozat formájában körbejárni, ami ezzel a bon mot-tal foglalható össze:

A program utasításaid és nem szándékaid szerint működik.

„Programs do what you tell them to do, not what you want them to do.”

Mivel a munkám egy jelentős része az ipari (PLC) szoftverfejlesztésről szól, ezért jól ismerem belülről a témát, én (illetve ugye a programom) is produkált már meglehetősen hajmeresztő hibákat; mondjuk a fél hamburgi kikötő áramtalanítása egy mozdulattal (meg egy benézett földeléskábellel).

A sorozat várható és már megírt bejegyzései:

- Therac-25: A hibaüzenet, amit senki nem értett
- Patriot rakéta: Hogyan ölt meg 28 embert egy tizedesvessző?
- Ariane-5: A 370 millió dolláros „copy-paste”.
- Boeing 737 MAX / MCAS: Amikor a pénzügyesek helyettesítik a mérnököket
- A B-2 Spirit és a pára: Miért nem bírja az esőt a világ legdrágább gépe?
- Mars Climate Orbiter: Akkor most mérföld vagy kilométer?
- Deepwater Horizon 2010: Amikor a „téves riasztások” igazzá válnak
- Intelsat-708: Tech-transzfer és katasztrófa
- A Davis-Besse atomerőmű esete a vírussal
- A Trans-Szibéria gázvezeték 1983-as robbanása - Az első igazán káros trójai kód
- A Stuxnet sztori - Mindössze egy berendezésre írt vírus

2026/05/05 20:02

Ajánló

Hasonló jellegű bejegyzéseket a **cyberwar** tag alatt talál:

- A Davis-Besse atomerőmű esete a vírussal 2026/06/26 22:42
- A Stuxnet sztori 2026/06/26 22:43
- A Supermicro történet 2026/06/26 22:43
- A Trans-Szibéria gázvezeték 1983-as robbanása 2026/06/26 22:43
- A Világ valódi csodái 2026/06/26 22:45
- Krétával és palatáblával a zsarolóvírus ellen 2026/06/26 22:45
- Xiongmai sztori 2026/06/26 22:46

Kedves olvasóm! Ha már idáig eljutottál az olvasásban, talán joggal feltételezhetem, hogy nem volt teljesen érdektelen számodra ez a bejegyzés. Jaj, le ne ixelj még; nem pénzt akarok tarhálni.

Pusztán annyit kérek, hogy ha van olyan ismerősöd, akivel jót tudnál vitatkozni az itt leírtakról, vagy csak simán megosztanád vele, kérlek, ne késlekedj!

Továbbra is keresek megjelenési lehetőséget az írásaim számára. Ha esetleg van ötleted, oszd meg velem! Elérhetőségeim az Impresszumban találhatók.

A passport.blog jelenlegi egyetlen megjelenési lehetősége a Facebook. Ha értesülni szeretnél az új bejegyzésekről, kövesd a Bolyongó Facebook oldalt.

Ha szeretnéd a bejegyzést kinyomtatni, vagy önálló formában menteni, ennek a legegyszerűbb módja a PDF formába konvertálás. Ezt a jobb oldali, fentről negyedik (Adobe) ikonnal teheted meg.

Eddigi bejegyzések a bolyongó.hu-n

Az összes bejegyzés ABC-be rendezett indexe itt található. A blog helyekhez köthető bejegyzései a google.maps térképen is megtalálhatók: A világ valódi csodái. A mostanában a blogon megjelent írások a főoldalon jelennek meg.

2026/05/28 18:05

Források

Kernkraftwerk Davis Besse
Wikipedia: Wikipedia: SQL Slammer
security focus: Slammer worm crashed Ohio nuke plant network

tech, történelem, vírus, atomerőmű, érdekes történet, 2003, cyberwar, USA, Ohio, Oak Harbor, vírus, Davis-Besse, villamos hálózat, blackout, SQL, SQL Slammer, tűzfal, SPD, SCADA