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.

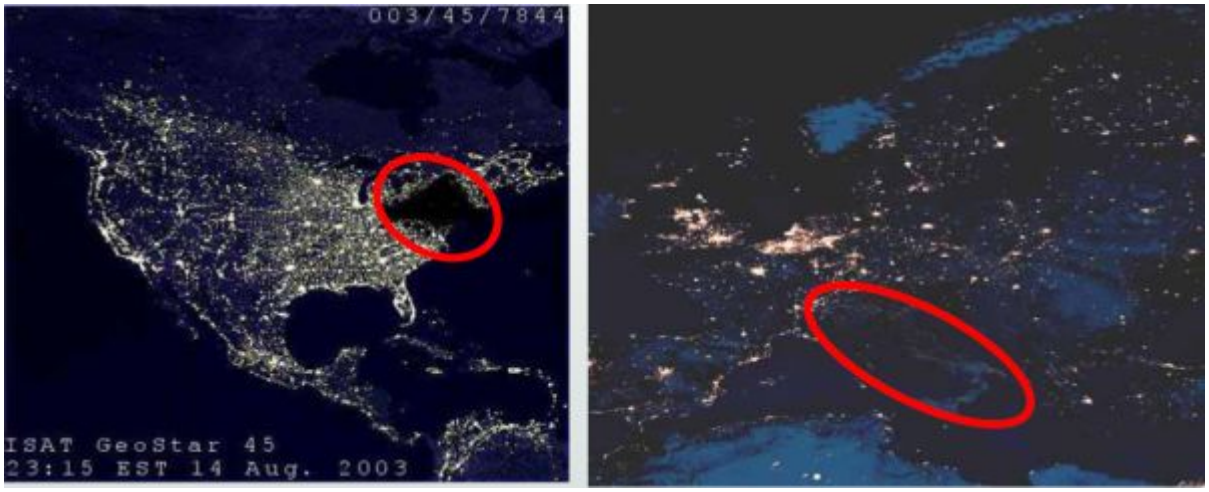
Rossz belegondolni annak a lehetőségébe, hogy a Slammer helyett valami Stuxnet-szerűség támadta volna meg a David-Besse-t. Az pedig Fukushima óta tudjuk, hogy a leállított (persze, a fukushima-i egy kényszerleállás volt, itt pedig egy tervezett technológiai leállás történt) atomerőmű még okozhat nagyon 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.

Ajánló

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

• A Davis-Besse atomerőmű esete a vírussal	2020/08/15 12:11	Vámos Sándor
• A Stuxnet sztori	2021/05/08 19:33	
• A Supermicro történet	2020/06/15 17:11	
• A Trans-Szibéria gázvezeték 1983-as robbanása	2020/06/15 17:11	
• A világ valódi csodái	2021/04/18 01:17	Vámos Sándor
• Krétával és palatáblával a zsarolóvírus ellen	2020/06/15 17:11	
• Xiongmai sztori	2020/06/15 17:11	

szerző: Vámos Sándor

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

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

Eddigi bejegyzések a bolyongó.hu-n

Az összes bejegyzés ABC-be rendezett indexe itt található.

A bejegyzések időrendben:

Bejegyzések: 175..151
Bejegyzések: 150..126
Bejegyzések: 125..101
Bejegyzések: 100..076
Bejegyzések: 075..051
Bejegyzések: 050..026
Bejegyzések: 025..001

A passport.blog tag-jei itt találhatók felhő fomában. A tag-ek a bejegyzésben felbukkanó kifejezések és szavak. Ezekkel több bejegyzés is összeköthető.

2022/04/05 20:27

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