A Stuxnet sztori

Na, ez a bejegyzés most hosszú lesz. Ráadásul, sok esetben a tényeket nélkülözve, találgatásokat is beleépítek ebbe a bejegyzésbe, ami – így talán – egy kerek történetté áll össze. Tények ugyanis nincsenek, hivatalosan ennek az akciónak sem végrehajtója, sem áldozata sincs.

Csak egy kósza vírus, ami bár szanaszét fertőzte a világ hálózatait, alapvetően semmit nem csinált, csak terjedt. Ha esetleg valaki rendelkezik a teljes történettel, kérem jelentkezzen, hogy korrigálhassam a bejegyzést.

Azaz.. ne, mégse; tartsa csak meg magának.

Izrael

Izrael léte a környező országok számára mindig is szálka volt, azaz annál azért több. Többször próbálták már lerohanni, megsemmisíteni; sikertelenül. Az izraeliek is árgus szemekkel vizslatják a szomszédaikat, és amikor **Irán atomfegyver-fejlesztési program**ba kezdett, komoly fenyegetésként élték meg. A nyílt odacsapás szinte azonnali háborúval fenyeget mind a mai napig a térségben, így inkább titkosszolgálati akciókkal próbálták – és vélhetően próbálják – elszabotálni és ellehetetleníteni az efféle törekvéseket.

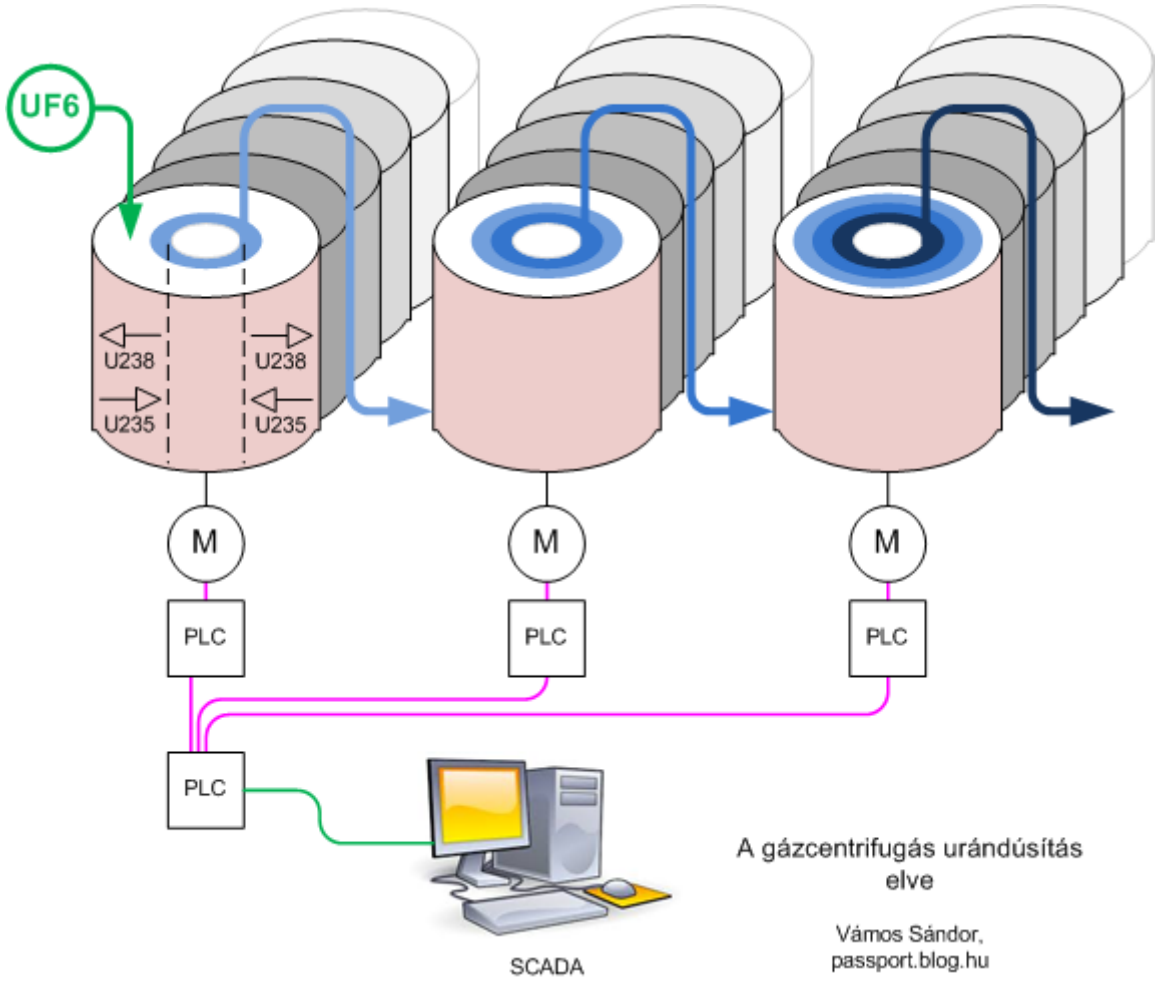
Az első, valóban sikeres cyber-támadást is szinte biztos, hogy ők hajtották végre egy iráni urándúsító üzemmel szemben. Emlékeztetőül; nem ez volt vélhetően az első cyber-attack, például már itt a blogon is írtam már a Trans-Szibéria vezeték 1983-as robbanásáról.

Az urándúsítás

Az atombombák építéséhez szükséges uránt dúsítással lehet létrehozni. Az uránnak a természetben a 234-es, 235-ös és 238-as tömegszámú izotópjai fordulnak elő, de ezek közül csak egy, az ún. **235U** használható a bombához.

Ez meglehetősen ritka a természetes környezetben, az uránérc eleve csak 0,7%-nyi 235U izotópot tartalmaz. Ezt atomfegyverek esetén ideális esetben 90%-ra kell dúsítani.

Ez tényleg valami olyasmi, mint hogy egy nagy zsák mákban keresünk egy kiskanálnyi olyan mákot, melynek a tömege egy nagyon kicsit eltér a többitől. A dúsításnak többféle módszere létezik, de a legelterjedtebb a gázcentrifugázás.



Az szobahőmérsékleten szilárd uránt melegítve és adalékolva gáz halmazállapotú vegyületté (urán-hexafluoriddá, **UF6**) alakítják át, s a két izotópot többnyire gázcentrifugákkal, több lépcsőben választják szét.

A centrifugák nagy fordulatszámon (kerületi sebességük a 600 m/s-ot is elérheti) a nagyobb tömegű U238-at a palást felé „préselik”, míg a könnyebb U235-ös lépésről lépésre nagyobb koncentrációban a tengelyhez közel lesz kinyerhető. Ehhez természetesen rendkívül precíz hűtés és nagyon stabil fordulatszám szükséges, ugyanis a fordulatszám változásával (lesz még ennek szerepe a későbbiekben) a rétegződés felkeveredik, mint a sunshine koktél, ha megforgatjuk a poharat vagy egy kiskanállal összekavarjuk azt.

A centrifugák vezérléséről speciális kontrollerek – nevezzük ezeket **PLC**-knek – gondoskodnak. Ezek veszik át a kezelőktől a **SCADA** nevű PC-ken keresztül a parancsokat és továbbítják oda a működési paramétereiket.

A technológia alapvetően nem boszorkányosan bonyolult, de rendkívül sok centrifugát és vezérlőegységet igényel, no meg mind az urán, mind a HF6 meglehetősen mérgező. A lenti fotó **Mahmoud Ahmadinejad** 2008-as látogatásakor készült. Kétoldalt a centrifugák hosszú sora látható.

Natanz

Natanz városa körülbelül 225 kilométerre, délkeletre található Teherántól, oázisai híresek az itt termelt körtéről, mellyel egész Iránt innen látják el. Az iráni kormányzat 2001-ben ide telepítette az urándúsító üzemét.

A mindösszesen 100.000 m² alapterületű csarnokokat légvédelmi okokból 8 méterrel a föld alá telepítették, majd a későbbiekben – az izraeli haditechnika fejlődésével szinkronban – még több földet hordtak rá.

2009-ben a berendezés 8000 centrifugájából 5000 működött, és egy újabb telep létesítésébe fogtak Qom közelében. A pakisztáni P–1-es centrifuga iráni változatának a kódneve az IR–1, és ennek a továbbfejlesztett változatai rendre IR–2, IR–3,.. névre hallgatnak.

Egy centrifugában viszonylag kis mértékű dúsítás érhető el, ezért ezeket úgynevezett kaszkádokba szervezik. A kaszkádokban a dúsított HF6 egyik irányban való áramoltatásával szemben a csökkentett 235U koncentrációjú HF6 a másik irányban mozog. A kaszkádok párhozamos kötésekkel is rendelkeznek. Feltételezések szerint ebben az üzemben a centrifugákat 164 elemű, 15 fokozatú kaszkádokba szervezték.

Az üzem létezését nem is nagyon titkolták a külvilág elől, bőséges információt szolgáltatva az izraeliek számára, akik egy rendkívül összetett szabotázsakció végrehajtása mellett voksoltak az üzem ellen, és egy addig ismeretlen **három fokozatú vírus** fejlesztésébe kezdtek, mely feladatot az izraeli hadsereg high tech különítményére, a **Unit8200**-ra bíztak.

„Myrtus” projekt

A tökéletes végrehajtás érdekében egy tesztberendezést is felépítettek Dimonában. Az urándúsító centrifugák technikai adatait azoknak a gyártóitól, a finn **Vacon**-tól és az iráni **Fararo Paya**-tól szerezték meg. Ez az *„adatszerzés”* még a szakértőket is meglepte, hiszen a Fararo Paya-t olyan szinten próbálták elrejteni az iráni hatóságok, hogy az **IAEA** (*International Atomic Energy Agency: Nemzetközi Atomenergia-ügynökség*) se tudott róla.

A fejlesztésbe rendkívül sok energiát és időt öltek, erre utal a kártevő komplexitása és fejlett hatásmechanizmusa, így szinte kizárt a magányos hacker teóriája, aki otthon, hobbiból fejlesztette volna a kódot. Itt egy komoly szakértőkből álló csoportnak kellett állnia a háttérben, a fertőzés jól irányzott volta, és az, hogy a kártevő elérte a célját, profi kivitelezőket és bőséges finanszírozást feltételez.

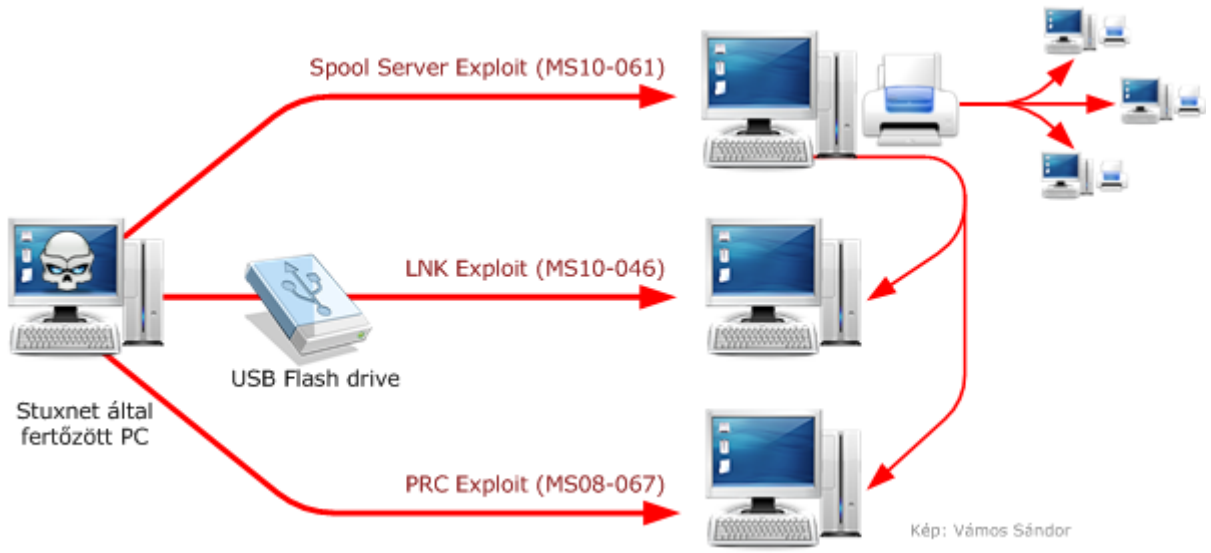
A fejlesztés a „**Myrtus**” projekt keretein belül történt, erre utal a beforgatott kód path-je: **myrtus**\src\objfre_w2k_x86\i386\guava.pdb

A *„Myrtus”* lehet egy hivatkozás a bibliai Eszterre, aki megmentette a perzsáktól az ókori zsidó államot, de lehet akár a *„My_RTU”* (remote terminal unit – távoli elérésű terminál) is.

A fejlesztéshez kiindulásként valószínűleg, egy korábbi kártevő, a **Conficker** kódját használták. A féreg tevékenységéről egy maláj és egy dán szerverre folyamatosan jelentéseket küldött (www.mypremierfutbol.com, www.todaysfutbom.com), majd a natanzi támadás után ezeket a szervereket lekapcsolták üzemeltetőik.

Első fokozat

A vírus alapvetően egy (nem publikált) Windows hibát (0-day Windows exploit) kihasználva pen-drive-ról tud fertőzni, majd a fertőzést követően – további operációs rendszerhibákat kihasználva – a hálózatokon terjedni.



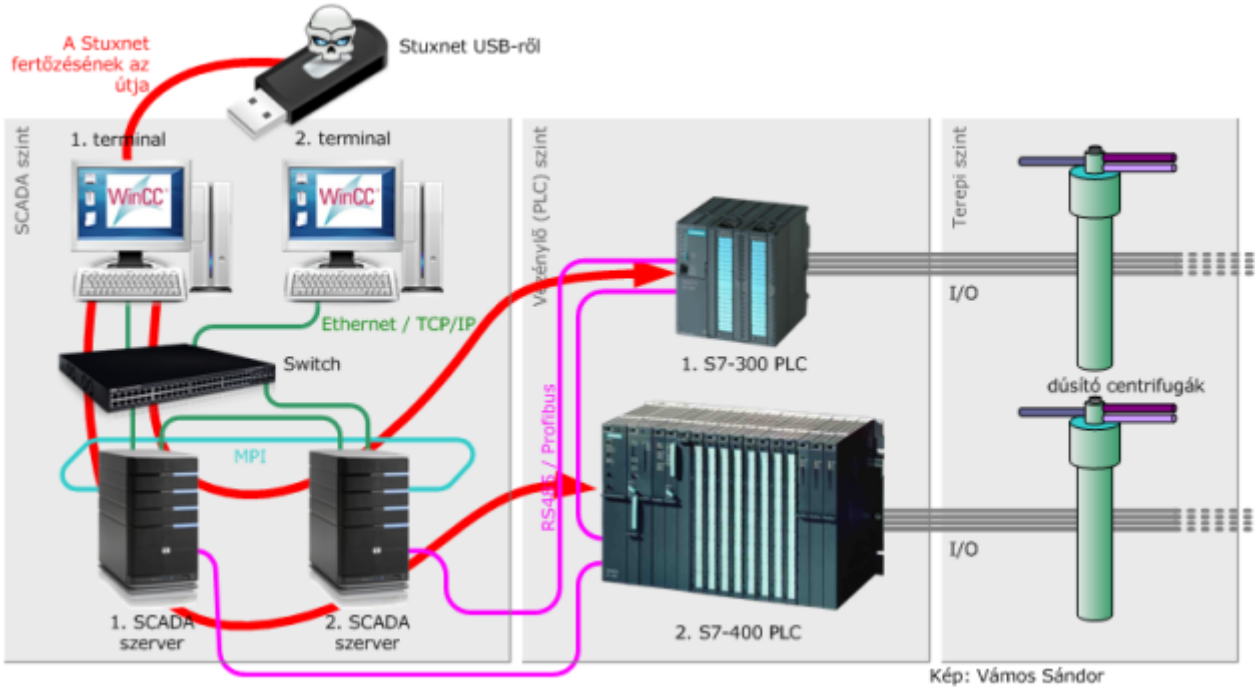
Ez a fokozat olyan jól sikerült, hogy a vírus gyakorlatilag letámadta a világot, és bár közvetlen kárt nem okozott, azért nagyon jelentős pánikot generált. A kártevő 2010 júniusában *„bukott le”* a

fehérorosz „**VirusBlokAda**” cég által Iránban, a Bushehr erőmű egyik gépén, és azóta bebizonyosodott, hogy több, mint 100.000 számítógépet fertőzött meg, a Simatic **WinCC** SCADA-kat SIMATIC] WinCC] SCADA] keresve.

Csak Iránban 45.000 felügyeleti számítógép és szerver tartalmazta a vírust.

Második fokozat

A vírus a fertőzést követően a WinCC jelenlétét kezdte keresni a gépen. Ez egy Siemens SCADA rendszer, melyen keresztül technológiák felügyeletét lehet megvalósítani.



Kép: Vámos Sándor

Leegyszerűsítve, ezek előtt a gépek előtt ülnek az operátorok, és unott fejjel bambulják a monitorjaikon megjelenített ábrákat, hogy éppen mi történik a rendszeren, illetve adott esetben pár kattintással itt tudnak beavatkozni a technológia működésébe. Ha a vírus rábukkant a WinCC-re, az azon keresztül elérhető PLC-ken megnézte, hogy megtalálható e ott pár speciális, csak a dúsítócentrifugákhoz köthető program. Ha igen, felülírta ezeket.

Harmadik fokozat

A vírus a PLC program módosításával a centrifugák sebességszabályozásába kétféle módon avatkozott be:

Egyrészt

A kártevő a natanzi urándúsító létesítményben kb. ezer IR–1 típusú urándúsító centrifugát égetett le. Ezeknek a berendezéseknek a hajtómotorja 1007 cps-nél (cycles per second, másodpercenkénti fordulatszám) is már tönkremegy, a Stuxnet viszont rövidebb fázisokra észrevétlenül 1064 cps-es

tempót diktált nekik, ezzel széthajtva őket.

Másrészt

A centrifugák fordulatszámát időnként szakaszosan manipulálta, először lecsökkentette azt, majd *„túlhúzta”*. Ezzel olyan hatást váltott ki, mint amikor vasárnap egy botmixerrel nekiugrok a szombati húslevesnek és jól összeturmixolom. (Ínyenceknek: sajtot is keverek hozzá és pirított szikkadt kenyér kockákkal tálalom ezt *„sajtleves”* fedőnévvel, a kölykeim imádják. Gasztroblog bejegyzés vége).

A módszerrel az urán rétegződését klasszul felkeverte a vírus, és mivel ezt észrevétlenül tette, az üzem fenntartói a program hibájára gyanakodhattak éveken keresztül – ha úgy vesszük, jogosan. Szinte biztos, hogy volt pár keresetlen szavakban bővelkedő beszélgetésük a centifugát gyártó és programozó cégekkel.

Harmadrészt

A program a SCADA felé meghamisított fordulatszám-adatokat küldött, így a visszamenőleges adatelemzések sem tárhatták fel, hogy mi történik a *„mélyben”*, a PLC-k szintjén. A kezelők meg unottan bámulhatták a monitorjaikat tovább.

Eredmény

AZ első körben még az iráni hatóságok számára sem volt világos, hogy a vírus a **Bushehr Nukleáris Erőmű**vet, vagy a nantanzi urándúsító üzemet támadja-e. Ugyanis mindkét létesítményben rohamosan elterjedt a vírus, és lefertőzte a vezérlőrendszert. Az erőműben ugyanakkor – azon kívül persze, hogy egy vírustámadás érte el a belső SCADA rendszert, ami már önmagában is felettébb kínos – más fennakadást nem okozott a Stuxnet felbukkanása. Terjedt, de nem csinált semmit. Ott nem.

2010. november 16-án Irán leállította az urándúsítóit, miután a centrifugák legalább 20%-a megsemmisült a Stuxnet tevékenysége nyomán, azaz a kártevő elérte a célját. Egyes kutatók megkérdőjelezik, hogy az elért siker megérte-e a befektetett hatalmas összegeket, ugyanakkor a támadás új fejezetet nyitott a cyber-hadviselés történelmében.

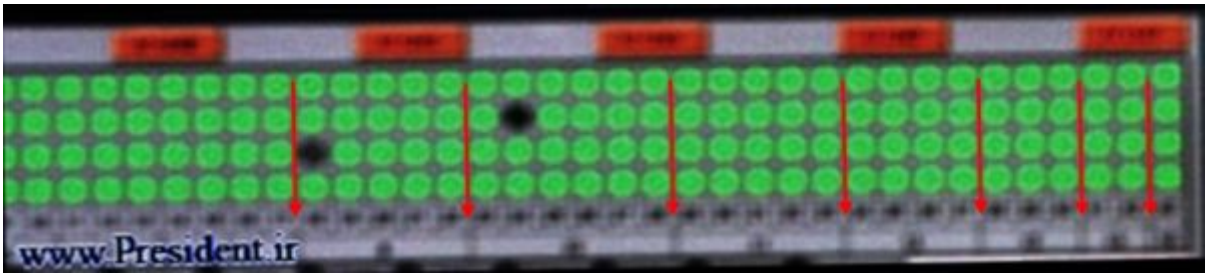
A telep vezetőjét leváltották, és vele együtt több alkalmazott is nyomtalanul eltűnt az okokat firtató *„vizsgálatokat”* követően. Persze, ez nem csoda egy olyan helyen, ahol a rossz teljesítés esetén alkalmazható következmények körét kiegészítették a munkaszerződésben pár tétellel, úgymint kínzás, kényszermunka vagy éppen kivégzés.

Bizonyítás

Sokáig rejtély maradt, hogy a vírus melyik létesítmény szabotálására íródott, miután kiderült, hogy felépítése olyan speciális, hogy csak egy célzott támadásra volt alkalmas. Persze a *„gyanúsítottak”* között már akkor is ott volt a natanz-i berendezés, de az iráni kormányzat nem sietett a nyomozók segítségére egy beismerő nyilatkozattal – mind a mai napig. Ebben az esetben is egy sajtófotó

segített leleplezni a rejtélyt, ez:

Jellegzetes fotó a nagyfőnökről, Mahmoud Ahmadinejad iráni államfőről, amint látszólag rendkívül elmélyül az egyre gyűrűző technológiai problémák tengerében, van olyan ikonikus, mint a *„Kim-Jong-Un a vazelingyárban”*, vagy a *„Rákosi elvtárs a búzában (hugyozik)”*. Ennyi. Vagy mégsem? Most jön az a rész, mint az NCIS-ben, a *„nagyítsál csak rá a képre egy kicsit!”*:



A fenti képen a zöld pontok a működő centrifugákat jelölik, ezek összesen 4, 8, 12, 16, 20, 24, 20 egységet tesznek ki, és vajon hol található meg ez a tagolás? Nos, valóban, a Stuxnet kódjában.

A két fekete pont két kihullott centrifugát jelölhet – nagyon valósínű, hogy ezeket a vírus intézte el. Egyébként is különös dolog a sajtófotó, ahol az elnök, vagy akármelyik fejes tetszeleg, és mutatja önnön nélkülözhetetlenségét a látványos berendezések háttere előtt.

A szakértőknek ezek a fotók jelentik az aranybányát, gyakorlatilag a teljes (egyébként titkos) technológiai rendszert fel tudják térképezni az elejtett részletek alapján; érdemes megnézni a források között feltüntetett **Langner jelentés**t. Sok kérdést vetettek fel például az alábbi képeken látható amerikai gyártmányú, meglehetősen speciális **MKS Baratron** nyomásszenzorok, hogy ugyan már, vajon hogyan kerülhettek tömegével az embargó sújtotta Iránba:

Egy régi barátom, mielőtt leadta volna az egyik nagy erőmű villamos áramút-terveit, mind a 15 dossziét, az egyikben elrejtett egy cetlit: *„ha valaki olvassa ezt a lapot, hívjon fel ezen a számon, és meghívom egy sörre!”*. 6 év múlva csörgött a telefonja. Márminthogy ezügyben.

Sajnos ezt, így nem tudom a műfaji korlátok okán eljátszani, de aki eddig elért az olvasással és van Facebook hozzáférése, kérem, dobjon egy kommentet, vagy akár csak egy akármilyen emoji-t ide, a bejegyzés alá!

Köszönöm.

Ajánló

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

- A Davis-Besse atomerőmű esete a vírussal 2025/07/20 08:26
- A Stuxnet sztori 2025/07/20 08:26
- A Supermicro történet 2025/07/20 08:26
- A Trans-Szibéria gázvezeték 1983-as robbanása 2025/07/20 08:26
- A Világ valódi csodái 2025/07/20 08:26
- Krétával és palatáblával a zsarolóvírus ellen 2025/07/20 08:26
- Xiongmai sztori 2025/07/20 08:26

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, 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 blog helyekhez köthető bejegyzései a google.maps térképen is megtalálhatók: A világ valódi csodái. A mostanában a blogon megjelent írások a főoldalon jelennek meg.

2025/07/20 08:26

Források

Wikipedia: Urán
Wikipedia: Stuxnet
ob121.blog.hu: A Stuxnet és hatásai (első rész)
ob121.blog.hu: A Stuxnet és hatásai (második rész)
Cserháti András: A Stuxnet vírus és az iráni atomprogram
Langner jelentés: To Kill a Centrifuge

tech, történelem, vírus, atombomba, érdekes történet, 2017, cyberwar, Izrael, Irán, Teherán, Qom, Natanz, urándúsító, Stuxnet, Urán, UF6, Simatic, U235, U238, PLC, Mahmoud Ahmadinejad, centrifuga, IAEA, Vacon, Myrtus, Windows, Bushehr, WinCC, SCADA, Langner, MKS Baratron, hacker, Bushehr Nukleáris Erőmű

Bejegyzésmegtekintések száma: 405