Bevezetés

Az elmúlt fél évben fokozatosan a legkifinomultabb számítógépes vírusnak, jelentős biztonságpolitikai eseménynek, sőt korszakhatárnak bizonyult a Stuxnet nevű kártevő. Felfedezését követően heteken belül kiderült, hogy főleg ázsiai ipari alkalmazásokra irányul. A visszafejtő munka haladásával már egyre több jel mutatta, hogy Irán nukleáris infrastruktúrája ellen hozták létre. 2010 végére már majdnem egyértelmű lett, hogy urándúsítók gázcentrifugáinak tönkretételére és a dúsítás hatékonyságának lerontására készítették. Ilyen összetett, folyamatszabályzó rendszerekbe álcázva behatoló vírust eddig még soha nem vetettek be. Ezért egészen biztos, hogy nem egy-két hacker[1], hanem hatalmas állami ráfordítás hozta létre. Eleinte csak a víruskutatók, idővel már a számítógépes hadviselés szakértői is megnyilvánultak az ügy kapcsán, de a történetre hamar rátalált a (bulvár)média is. Sajnos sem a szakértők, sem a laikus sajtó nem nagyon tudott vagy nem is nagyon akart különbséget tenni a perzsa urándúsítók és az indítás előtt álló atomerőmű közt. Sokuknak egyszerűbb és hatásosabb volt mindent összemosni és új Csernobilt vizionálni. Ideje tehát, hogy a nukleáris oldal is hallassa hangját, ezért készült jelen cikk.

A gázcentrifugák felépítése, működése

Ismert, hogy a bányászott természetes uránban a hasadó izotóp (^{235}U) aránya mintegy 0,7%. Energetikai reaktorok üzemanyagához 3-5% körüli, a kutatóreaktorokéhoz nagyobb, újabban jellemzően 20% alatti hasadóképes hányadra van szükség. Atomfegyver készítéséhez ugyanakkor legalább 20%-ra, ideális esetben több mint 90%-ra kell dúsítani az ^{235}U izotópot.

A dúsítás egyik lehetséges módszere gázcentrifuga alkalmazása. A centrifuga mintegy 2 m magas, karcsú, álló hengeres házba zárva. Benne szinte súrlódásmentes környezetben, nagy sebességgel forog egy ugyancsak hengeres, belül üreges rotor. Az uránt gázhalmazállapotban, urán-hexafluorid (UF_6) formában vezetik be a rotorba. A gáz a rotor falától gyors forgásba jön. A centrifugális erő a nehezebb uránizotópot (^{238}U) kifelé hajtja, míg a könnyebb ^{235}U középen, a tengely mellett dúsul fel. Kis terelő lemezekkel vagy a rotor alsó, külső melegítésével emellett még lassú függőleges áramlást is hoznak lére úgy, hogy a gáz belül lefelé, kívül felfelé áramlik. Így a rotor aljára lenyúló csövön át kiszívott gázban valamivel nagyobb, felülről pedig egy másik csövön kiszívott gázban valamivel kisebb az ^{235}U aránya, mint a kiinduló összetételben.

Mivel a dúsítás mértéke egy centrifugában csekély, sok (több 100, sőt 1000) centrifugát kell csövekkel egymás után kapcsolni, azaz ún. kaszkádba rendezni. A kaszkádokban az ^{235}U aránya fokozatosan növekszik a kívánt szintre.

A korszerű centrifugák akár 10 évig is működnek jelentősebb karbantartás nélkül és viszonylag kevés energiát fogyasztanak.[ ]

A fordulatszám és sebesség érzékeltetéséhez néhány szám. Egy átlagos utcai autó motorjának alapjárati fordulatszáma 1000 fordulat/perc alatti, üzemben 2000-4000 körüli (persze egy F1 versenyautót ennek akár hatszorosára, 18000-re is felpörgetnek). Az erőművi turbinák fordulatszáma Európában zömmel 3000 fordulat/perc, ami pontosan 50 Hz frekvenciát jelent. Ennél a gázcentrifugák húsz-huszonötször gyorsabbak, 800-1200 Hz a frekvenciájuk. A rotor falának kerületi sebessége 300 m/s nagyságrendjébe esik, elérheti a hangsebességet.

A kis súrlódás a ház vákuumozásával és a rotor mágneses csapágyazásával érhető el, forgás közben érintkezés a tengelycsap és a csapágyház között gyakorlatilag nincs. A rotor anyaga az egyszerűbb modelleknél alumínium, de idővel egyre inkább acélra, sőt szénszálas

[1] a számítástechnikai rendszereket mélyen ismeri, képes lehet betörni, illetéktelenül használni

kompozitokra állnak át. Annál hatékonyabb az izotóp szeparáció, minél gyorsabban forog és minél hosszabb a rotor. A sebességnek a rotor szilárdsága, a hossznak a vibrációk különféle felharmonikusainak növekedése szab határt. A forgás közben a sajátfrekvenciák körül rezonanciajelenségek léphetnek fel. Ezeken a kritikus sebességeken a gyorsuló vagy lassuló rotort hamar át kell juttatni, illetve a csapágyak lengéscsillapításának beállításával a rendszert el kell hangolni.

Összegzés

Langner bogján 2010 utolsó napjaiban az alábbi évzáró bejegyzést tette [ ]:

1. Minden kétséget kizáróan a Stuxnetet arra fejlesztették ki, hogy a centrifugák fizikai sérülését okozva késleltesse az iráni urándúsítási programot.
2. A támadást nem robbanásszerűen, hanem lassan, fokozatosan kivitelezték. Lehet arra számítani, hogy az ISIS jelentésben említett 984 centrifugán túl továbbiakat is megrongált a Stuxnet. Erre a kb. február végére esedékes következő NAÜ ellenőrzés adhat egyértelmű választ.
3. A támadás teljes elemzése lehetséges anélkül is, hogy a natanzi vezérlőszekrények közelében lennénk. Csupán az IR-1 kaszkád szervezését és működtetését kell jól érteni, valamint a műszerezés néhány alapvető adatát kell ismerni.
4. Egy ilyen nagy horderejű támadás mögött feszülő hatalmas erőket elég könnyű érzékelni. A Stuxnet kártevő kifejlesztéséhez extrém mennyiségű hírszerzési adat kellett a dúsító mű elrendezéséről, teljesen meg kellett érteni az IR-1 működését (amihez feltehetően rendelkezésre állt egy üzemképes tesztelő rendszer is), valamint a Siemens érintett termékeiről rengeteg bennfentes tudásra volt szükség. Mindez igen kevés szervezetre szűkíti le a világon azt a kört, amely a feladat megoldására vállalkozhatott.
5. A Stuxnet interneten már elérhető támadó kódja kiváló alap, elrugaszkodási pont a kiberháborús fegyverek új generációjának kifejlesztéséhez. Abból kell kiindulnunk, hogy olyan jelentős államok, mint Kína és Oroszország számítógépes hadviselési képességük bármilyen szándékkal történő létrehozásához már javában elemzik az utolsó bitekig bezáróan a kódot, koncepciókat és eszközöket hoznak létre jövőbeli hasonló támadásokhoz. De ezen fegyverek célpontjai nagy valószínűséggel már nem csak a Közel-Keletre fognak lokalizálódni.

Kiegészítő megjegyzésem az utolsó ponthoz: a nukleáris létesítmények, mint a kritikus infrastruktúra elemei szinte biztosan a célkeresztben maradnak. Ez új feladatokat jelent számunkra is.

Irodalom

Az összes fájlletöltés 2011-01-23-án történt.

[1] Institute for Science and International Security (ISIS)
- What is a Gas Centrifuge? 2003
- D. Albright, A. Stricker: Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target? NuclearIran News, 2010-11-17, jav. 12-20

http://www.exportcontrols.org/centrifuges.html http://www.isisnucleariran.org/news/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-are-iranian/

[2] Iráni hírügynökségek cikkei
- AEOI Chief Unveils New Details on West's Cyber Attack on N Sites. Teheran, FarsNews, 2010-11-23
- Envoys of IAEA members in Natanz to visit uranium enrichment site. Tehran, IRNA, 2011-01-16,
- Iran dismisses reports on Stuxnet effect on nuclear facilities. Tehran, ISNA, 2011-01-17

http://english.farsnews.com/newstext.php?nn=8909021485

http://www.irna.ir/ENNewsShow.aspx?NID=30190522
http://isna.ir/Isna/NewsView.aspx?ID=News-1697213&Lang=E

[3] AtomInfo.Ru cikkek
- Иран переконфигурировал 10 каскадов на 174 центрифуги. 2010-11-29
- Основные данные из доклада МАГАТЭ по ядерной программе Ирана. 2010-11-29
- Stuxnet и Иран: загадка модуля A26. 2010-12-28

http://atominfo.ru/news3/c0942.htm
http://atominfo.ru/news3/c0945.htm
http://atominfo.ru/news4/d0249.htm

[4] Dajkó P. írásai az ITcafében
- Biztonsági kamu: a Stuxnet mint kiberháborús eszköz. 2010-10-05
- Újabb bizonyíték, hogy a Stuxnet vírus célja szabotázs volt. 2010-11-16
- A Stuxnet következménye - milliárdos fejlesztések a hadseregeknél. 2010-11-28

http://itcafe.hu/hir/stuxnet_iran_kamu.html
http://itcafe.hu/hir/stuxnet_siemens_virus.html
http://itcafe.hu/hir/kiberhaboru_nagy-britannia_stuxnet_richards.html

[5] A New York Times cikke és egyik magyar ismertetője
- W.J. Broad, J. Markoff, D. E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. NYT, 2011-01-15
- Amerikai segítséggel fejleszthette Izrael az iráni atomerőművet támadó vírust. HVG, 2011-01-21

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
http://hvg.hu/Tudomany/20110121_stuxnet_iran_amerika_izrael

[6] Vírus Híradó cikkek
- Újra magas fordulatszámon pörög a Stuxnet-ügy. 2010-11-16
- Angol hidegvérrel szemlélik a Stuxnetet. 2011-01-18
- Tevegel a Stuxnet. Bizottság tervezte az atom-kártevőt. 2011-01-21

http://www.virushirado.hu/hirek_tart.php?id=1751&print=1
http://www.virushirado.hu/hirek_tart.php?id=1783&print=1
http://www.virushirado.hu/hirek_tart.php?id=1785&print=1

[7] Ralph Langner hamburgi vírusbiztonsági szakértő anyagai
http://www.langner.com/en/blog/

[8] A Zrínyi Miklós Nemzetvédelmi Egyetem anyagai
- Berzsenyi D., Szentgáli G.: Stuxnet - a virtuális háború hajnala. 2010-10-07
- Kovács L., Sipos M.: Stuxnet, és ami mögötte van. ZMNE, 2010-11-24

http://www.biztonsagpolitika.hu/?id=16&aid=932
http://robothadviseles.hu/pres/KovacsL_SiposM.pdf

[9] Wikipedia szócikkek
http://en.wikipedia.org/wiki/Nuclear_facilities_in_Iran
http://en.wikipedia.org/wiki/Stuxnet
http://ru.wikipedia.org/wiki/Stuxnet

[10] Orosz hacker szakfolyóirat cikkei
- Шпионский ярлык: история трояна Stuxnet. 2010-11-18
- New York Times: за червем Stuxnet стоят разведки США и Израиля, 2011-01-18
- Stuxnet полон ошибок и некачественного кода, 2011-01-20

http://www.xakep.ru/post/53950/default.asp
http://www.xakep.ru/post/54552/default.asp
http://www.xakep.ru/post/54578/default.asp

[11] Vezető víruscégek részletes és folyamatosan mélyülő elemzései
- N. Falliere, L.O Murchu, E. Chien: W32.Stuxnet Dossier v1.3, Symantec, 2010-11-12
- Matrosov, E. Rodionov,D. Harley, J. Malcho: Stuxnet Under the Microscope, Rev 1.31, eset, 2010-12-16

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf