A STUXNET VÍRUS ÉS AZ IRÁNI ATOMPROGRAM

Cserháti András
Paksi Atomerőmű Zrt. Kapacitásbővítési Igazgatóság

Az elmúlt háromnegyed évben – egyre inkább – 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 mind több jel mutatta, hogy Irán nukleáris infrastruktúrája ellen hozták létre. 2010 végére már egyértelmű lett, hogy urándúsítók gázcentrifugáinak tönkretételére és a dúsítás hatékonyságának lerontására készítették.

Ilyen összetett, folyamatszabályozó 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 Stuxnet vírus rendkívüli kialakítása és jellemzői

Stuxnet olyan különleges számítógépes féreg [1–6], amely MS Windows operációs rendszert futtató gépeket fertőz, és azokon terjed, de hatását végső soron ipari folyamatirányító rendszereken keresztül fejti ki. Támadja a folyamatok felügyeleti irányítását és adatgyűjtését (SCADA[2]), és nem csak kémkedik a célzott ipari rendszer után, hanem át is programozza azt. Az első olyan kártevő, amely programozható logikai vezérlők (PLC[3]) rootkitje,[4] azaz rejtett, privilegizált módon fér hozzájuk, aláaknázva rajtuk a szabványos operációs rendszer vagy más alkalmazás működését. A Stuxnet kivételes képességei ezen túl egyetlen gyártó termékeire összpontosulnak: a Siemens cég – főleg vegyipar, energiatermelés, szállítás területén használatos – eszközeire (WinCC HMI, illetve STEP7).

Egy sor vírustechnológiai különlegességet is rejt magában a kártevő. Mivel ezt 2010 őszén a vezető informatikai biztonsági cégek elég részletesen kivesézték, csak összefoglalom:

- Nagy mérete (0,5 MB) és több nyelven (C és C++) írt részletei szokatlanok.
- 3 egymás utáni rétegen keresztül juttatja célba végső támadó kódjait (Windows operációs rendszer, WinCC/Step7 ipari alkalmazás, Siemens PLC).

Windows réteg

- Szinte minden Windows verziót (~ XP-SP2, -SP3; ~ Vista-SP1, -SP2; ~ Server-2003, -2008, -2008 SP2; ~ 7; ~2008 R2) megfertőz, viszonylag gyorsan és válogatás nélkül.
- A jellemző egy helyett négy felfedezetlen, javítással nem rendelkező biztonsági rést[5] használ ki.
- USB-s tároló eszközökről települ, korai verziójában AutoRunnal, újban nélküle, ikonokat beolvasó fájlkezelők (például Windows Intéző, Total Commander) segítségével.
- Tovább fertőz internettel kapcsolatban nem álló, megosztott hálózati erőforrásokon keresztül, fájljait elrejti.
- Két hamisított digitális aláírást (a tajvani JMicron és Realtek tanúsítványai) vet be eszközmeghajtói megbízhatóságának igazolására.
- Két Stuxnet vírus találkozásakor a frissebb él tovább.

WinCC/Step7 réteg[6]

- Alapértelmezett Siemens gyári felhasználót és jelszavakat alkalmaz.
- Ha van internetkapcsolata, egy sor kódolt adatot elküld egy külső szerverre (eddig dán és maláj szervert találtak elfogott vírusokban), ahonnan vagy kódolt parancsot kap meglévő rutinja indítására, vagy letölt, installál és elindít egy frissítést.
- Adatkábeles összekötés esetén beékelődik a Windows munkaállomáson futó WinCC és a PLC közti adatforgalomba és észrevétlenül támadó kódot installál a PLC-kre.

PLC réteg

- A specializáció további lépcsőjeként a támadó kódok akkor fejtik ki hatásukat, ha két konkrét vezérlőt és azok felügyelete alatt bizonyos konkrét berendezéseket találnak.

Az írást, amely megjelent a *Nukleon* internetes folyóirat márciusi számában a szerző és a főszerkesztő engedélyével közöljük.

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

[2] Supervisory Control And Data Acquisition

[3] Programmable Logic Controller

[4] Root (minden jogosítvánnyal rendelkező) + Kit (feladatot megvalósító szoftverösszetevő), kártevőre utaló

[5] Zero day bug vagy ~ vulnerability

[6] Alapfeladatai: PLC konfigurálás (projekt felépítés, adatforrások, jelek felvétele, képek megrajzolása, objektumok, esemény- és hibanapló dinamizálása, trendek generálása) és projektfuttatás (indítás, on-line állapotba váltás, amikor látható a képeken a figyelt készülékek által küldött információk hatása) Windows munkaállomásról.

1. ábra. Simatic S7 központi egységek (forrás: www.ob121.com).

A megtámadott vezérlők és a rájuk kapcsolódó ipari eszközök

A vírus a Siemens Simatic S7 PLC sorozatának (*1. ábra*) következő típusait használja [1]:

1. S7-300 (315) közepes, általános célú vezérlő, 256 kB memóriával,

2. S7-400 (417) csúcsmodell, akár 30 MB memóriával; redundáns és hibatűrő rendszerekben is alkalmazzák, egyebek közt erőművek turbinavédelmében is.

A vírus a PLC-ken bizonyos konkrét ipari eszközök, nevezetesen nagy sebességű motorok frekvenciaátalakítói után kutat, és csak akkor lép akcióba, ha a finn Vacon és iráni Fararo Paya készülékeire talál, valamint a felügyelt eszköz 807 és 1210 Hz között működik.

Ilyen frekvenciaátalakítók és motorok szinte kizárólag az iráni urándúsítókban használatosak. A továbbiak megértéséhez tekintsük át először általában a gázcentrifugákat, majd iráni alkalmazásukat.

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 hasadó képes 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 [7–9]. A centrifuga pár méter magas, karcsú, álló hengeres ház, amelyben szinte súrlódásmentes környezetben, nagy sebességgel forog egy ugyancsak hengeres, belül üreges rotor (*2. ábra*). Az uránt gáz halmazállapotban, 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 létrehozhatnak úgy, hogy a gáz belül felfelé, kívül lefelé áramlik. Így a rotor aljára lenyúló csöveken át a szélekről kiszívott gázban valamivel kisebb, míg felső csöveken középről kiszívott gázban pedig valamivel nagyobb az ^{235}U aránya, mint a beadott összetételben [4, 7].

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 korai gázcentrifugák is húsz-huszonötször gyorsabbak, 800–1200 Hz a frekvenciájuk. A rotor falának kerületi sebessége legalább 300 m/s nagyságrendjébe esik (hangsebesség).

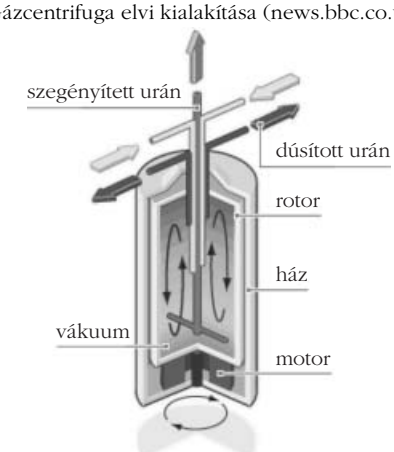
A kis súrlódás a ház vákuumozásával és a rotor mágneses csapágyazásával érhető el, forgás közben érintkezés a tengelycsap és a csapágyház között gyakorlatilag nincs. A rotor anyaga az egyszerűbb modelleknél alumínium, de idővel egyre inkább acélra, sőt szénszálas kompozitokra állnak át. Annál hatékonyabb az izotópszeparáció, 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. Eleinte a kritikus fölötti sebességre tervezett, úgynevezett szuperkritikus modelleket fejlesztettek, viszont az újabbaknak úgy optimalizálták anyagát, hosszát és csapágyait, hogy még nagyon nagy sebességen is szubkritikusak lehetnek [7–9].

Az iráni urándúsítás, a centrifugák eredete

Az irániak által használt centrifugák sajátos terjedési és fejlődési láncon keresztül kerültek az országba.

1945–1956 során német hadifogolyként 60 fős csapata élén az osztrák *Gernot Zippe* tökéletesítette a szovjet gázcentrifugákat, az egyik kifinomult típus máig az

2. ábra. Gázcentrifuga elvi kialakítása (news.bbc.co.uk nyomán).



3. ábra. Elnöki látogatás a dúsító műben, egy IR-1 kaszkád (forrás: www.president.ir).

ő nevét viseli. Miután hazakerült a hadifogságból, meglepődve realizálta: műszaki színvonaluk a nyugati világét meghaladta. Emlékezetből felidézte, majd szabadalmaztatta a megoldásokat. Amerikai csábításra egy ideig Virginiában dolgozott, de rövidesen visszatért Európába, és további fejlesztéseket végzett, új projektekben vett részt. Terveit az európai energetikai reaktorok nukleáris üzemanyagának gyártásában, az Urenco csoport hollandiai telepén is alkalmazták.

A hetvenes években az Urencónak bedolgozó egyik amszterdami K+F intézetben nagy szilárdságú anyagokat tanulmányozott a pakisztáni *Abdul Qadeer Khan* mérnök és anyagtudós. Úgy került közel a centrifugákhoz, hogy intézete ötvözeteit azok rotorjaiban is használták és a sok nyelvet jól beszélő Khant bevonták centrifugatervek fordításába. Khan a tudással hazatérve a pakisztáni atomfegyverprogram kulcsfigurája lett. Az irányításával a nyolcvanas évek elején kifejlesztett Pak-1 vagy P-1 jelű centrifugák nem csak a pakisztáni uránbombákhoz vezettek el, hanem feketepiaci hálózatán a kilencvenes évek közepén egyebek közt Iránba és Líbiába is eljutottak [4].

Natanz és Qom telepei, az újabb fejlesztések

Irán dúsító kapacitását Natanz közelében alakították ki. A natanzi telep legfontosabb elemeit igyekeztek légitámadásoktól minél jobban megvédeni. Az összesen mintegy 100 ezer m^2 területű üzemcsarnokokat eleve 8 m-rel a felszín alá rejtették, és 2,5 m vastag vasbetonfödémmel látták el. 2004-ben még tovább vastagították a betont, majd arra további 22 m magasan földtakarást hordtak. Egy kísérleti és egy teljes léptékű üzem is kiépült. Létezésüket 2003-ban ismerték el az irániak, ekkor töltöttek fel urán-hexafluoriddal egy 10, majd 164 centrifugát tartalmazó kaszkádot. 2009-ben már körülbelül 8000 centrifuga volt beépítve, és ebből már 5000 működött Natanzban. Ugyanebben az évben Irán nyilvánosságra hozta, hogy további félüzemi gázcentrifugás urándúsítót létesített Qom közelében (a hasonlóan védett utóbbi létesítményt az elemzők Fordow néven is említik).

A pakisztáni P-1 centrifuga iráni változatának a külvilág által adott neve IR-1, míg a további modernebb sorozatoké IR-2, IR-3 stb. Az IR-1 még alumínium rotoros hosszú szerkezet, szuperkritikus sebességű. Az IR-2 szénszálas rotorja már nagy szilárdságú és csak mintegy fél méteres, így 450 m/s szubkritikus kerületi sebességen üzemeltethető. A hasonlóan rövid, szintén kompozit rotoros IR-3 prototípus pedig még gyorsabb: kerületi sebessége ugyan 600 m/s, de még így is szubkritikusan forog [4, 8].

A natanzi IR-1 és IR-2 centrifugákról a legtöbb képi információt *Mahmud Ahmedinezsád* 2008. áprilisi látogatása (*3. ábra*) kapcsán hozták nyilvánosságra [10]. A több tucatnyi fotó ma is letölthető az elnöki honlapról, amatőr és profi analízisek aranybányájaként.

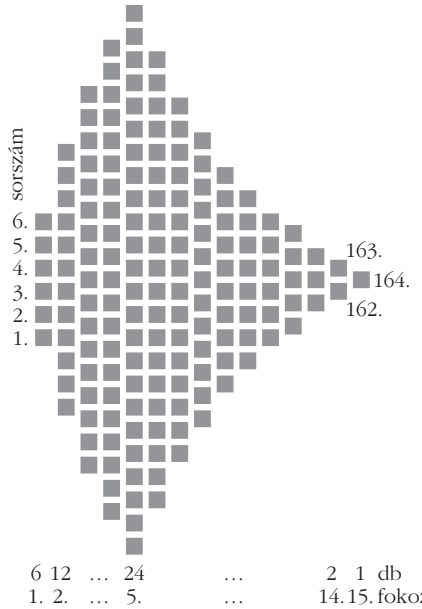
Az iráni atomfegyverkezést kutató civil tudósok, egyetemi és katonai szakértők valamint a Nemzetközi Atomenergia Ügynökség felügyelői évek óta elemzik a békés célúnak mondott dúsító kapacitások hirtelen hadicélú átállításának lehetséges forgatókönyveit.[7] Vizsgálják, hogy az ismert létesítmények, kaszkádok, centrifugatípusok mellett milyen gyors az átállás, és mennyi idő kell egy-két uránbomba anyagának elkészítéséhez. Az alap forgatókönyv a békés: természetes uránból alacsony dúsítású reaktor-üzemanyag előállítása. Továbbiak: a természetes uránból vagy a már felgyűlt alacsony dúsítású uránból magasan dúsított urán, mint bombaalapanyag. Azt is értékelik, hogy mennyire észrevehető a felügyelőknek, hírszerzésnek az átállás, és például a Natanzból Fordowba vagy esetleg más még ismeretlen létesítménybe való átszállítások [8, 9].

A centrifugák kaszkádjai, optimumok, anyaghozamok

Mivel a dúsítás mértéke egy centrifugában csekély, sokat (több százat) kell csövekkel egymás után kapcsolni, azaz kaszkádba rendezni. Az ^{235}U aránya így centrifugáról centrifugára, fokozatosan növekszik a kívánt szintre. A kapcsolat továbbá nem csak előre menő (amikor a kissé dúsított gázt a következő fokozat centrifugájába vezetik), hanem visszamenő is (a szegényített gáz visszakerül az előző fokozat centrifugájába). A kaszkád tehát egy sok oda/visszacsatolással rendelkező hálózat. Még jobban bonyolítja e hálózatot, hogy nem csak sorosan, egyesével fűzik fel a centrifugákat, hanem az egymás utáni fokozatok több párhuzamosan kötött centrifugából is állhatnak. A soros kapcsolás a dúsítás mértékét (minőség) növeli, míg a párhuzamos a kapott anyagot (mennyiség). A fokozatokon belüli centrifugaszámok alkalmas kiválasztásával javítható a kihozatal. Más az optimális kapcsolás alacsonyabb és magasabb dúsítások esetén.

Még Pakisztánban, de később Iránban is a centrifugákat 164 elemű, 15 fokozatú kaszkádokba rendezték, amit egy iráni vezető tv-nyilatkozata is megerősített. Analitikus számításokkal kimutatható, hogy eb-

[7] breakout scenario



4. ábra. A 164 elemű kaszkád ideális elrendezése (*Physics Today* cikke nyomán).

ben az esetben ideális dúsítási teljesítmény akkor érhető el, ha a *4. ábra* szerinti elrendezést követik (rendre 6, 12, 17, 21, 24, 20, 16, 13, 10, 8, 6, 5, 3, 2, 1 centrifuga tartozik egy fokozatba). A legtöbb centrifuga az ötödik fokozatban található, itt történik a kiinduló gáz bevezetése a kaszkádba [2, 8].

A 315-ös támadó kód

Jelentősen egyszerűsített leírás: lényegében öt szakaszt váltogat ciklikusan, ebből leghosszabb a kiváró (13–90 nap), a többi órás nagyságrendű. A rongáló szakasz során – miközben a kezelőknek a korábban felvett normál üzemi paramétereket mutatja – felpörgeti 1410 Hz-re, majd lelassítja 2 Hz-re a centrifugát (majdnem törésig viszi a rotort, átlépteti a kritikus fordulatszámon, illetve hagyja az addig szeparált UF_6 újbóli összekeveredését), ezután visszaáll a névleges frekvenciára [1]. A cél a centrifuga fokozatos, észrevétlen tönkretétele és a dúsítási folyamat megzavarása.

Mit fenyegethet még a Stuxnet a centrifugákon kívül?

E fontos kérdésben a mértékadó álláspontok az elmúlt év végére eléggé módosultak. Ragadjunk ki a továbbiakban *Langner* blogjából [2] néhány részletet:

2010-11-13

Míg a 315-ös támadó kódról már eléggé kiderült feladata, a 417-es támadó kód kapcsán ezt egyelőre csak találgatni lehet. Két lehetséges irány:

1. A centrifugakaszkád magasabb szintű vezérlésének megzavarása. A 315-ös PLC-k ugyanis egyedül nem képesek a centrifugák irányítására, és biztosan nem ellenőrzik az egész kaszkádot. Alighanem csak a rotorok egyedi, modulszintű vezérlésére képesek. Kell tehát lennie kiegészítő vezérlőnek, amely a szivattyúkat, szelepeket stb. vigyázza. Ez lehet a 417.

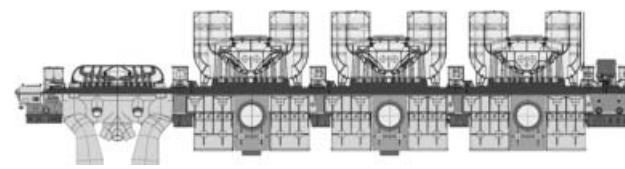
2. Az iráni nukleáris eszközpark másik fontos eszközéhez kapcsolódó kártétel.

Langner akkor nagyobb esélyt adott a második iránynak. A kézenfekvő objektumot pedig a Bushehri Atommerőműben, annak nagy turbinájában (lásd alább az apró betűs részt) vélte megtalálni, kezdettől elhárítva a reaktor és primerköri rendszerek támadására irányuló találgatásokat. Nyomozása szerint a turbina a vezérlőkön keresztül elvileg többféle módon megrongálható. Túlpörgethető teljes gőzáram mellett a generátor terhelésének hirtelen ledobásával, vagy rezgésbe vihető a kritikus fordulatszám-tartományban. Ha a turbinának a szabályozásán kívül netán a védelme is be van integrálva a 417-es PLC-be, akkor ez szinte biztosan megtehető. Még akkor is, ha a rendszer – esetleg – több azonos redundáns elemből épül fel, hiszen mindet közös módon támadja a féreg.

A bushehri turbina, gyártója és irányítástechnikája

A K-1000-60/3000-3 típusú orosz turbinát az LMZ (Leningrádszkij Metallicseszkij Zavod) gyártotta. A nagy múltú szentpétervári energetikai gépgyár 2000-ben sorolt be hat további nehézipari céggel a Szilmas (Szilovije Masini) konglomerátumba, amelynek tulajdonosai közt a Siemens is 25%-kal szerepel.

A generátoron 1014 MW villamos teljesítményt leadó, 5,88 MPa (~60 bar) nyomású gőzt nyelő és percenként 3000 fordulatú turbina – ahogy az *5. ábrá*n is látható – egy kettős kiömlésű nagynyomású és három ugyancsak kettős kiömlésű kisnyomású házból áll. Mindez egy tengelyen, több mint 40 m hosszúságú kivitelben.[8]



5. ábra. A bushehri turbina metszete (forrás: LMZ előadás, 2008).

Vélelmezhető, hogy a Siemens által résztulajdonolt LMZ turbináit nem a konkurencia vezérlőivel látják el. Több olyan dokumentum fellelhető az interneten, amely szerint a Siemens által vagy tervei alapján gyártott Simatic S7-400 (417) egységeket oroszok atomerőműben is alkalmaznak (a Kalinyini Atomerőmű 3. blokkján létesült digitális mintarendszer több eleme elterjedt más atomerőművekben, így Bushehrben is).

2010-12-27

Langner felfigyelt rá, hogy a 417-es támadó kód egy 164×6-os tömböt kezel. Ebből arra a következtetésre jutott, hogy alighanem a centrifugák védelmét ellátó rendszert bénítja le. A 417-es PLC tehát valószínűleg szelepeket és gázfúvókat vezérel. Ha például alapfunkcióként a rotor egyensúlyhiányát észlelve az urán-hexafluorid gázt gyorsan le kellene ürítenie, de

[8] A cikk szerzőjének személyes motívuma: 2009. októberben látogatást tett az üzembe helyezés kezdetén lévő bushehri atomerőműben. Perzsa kísérőivel végigmászta a konténmentet a reaktorcsarnokkal, elsétált a turbina mellett, járt a blokkvezénylőben. Akkor, másfél éve úgy becsülte, kellhet még egy év az indításhoz…

ezt nem hagyja neki a támadó kód, a bennmaradó gáz a rotorok repedéséhez vezethet, ráadásul a centrifuga törése a drága gáz kiömlésével jár.

2010-12-29

417 adatszerkezete = kaszkád struktúra = kárjelentés beszédes című bejegyzés szerint (*6. ábra*) a támadó kód hatszor hív meg egy szubrutint, amelyen belül egy 164 elemű ciklus van.

Mint láttuk, a natanzi IR-1 centrifugák 164 elemű kaszkádokba vannak rendezve. Hat kaszkád 984 centrifuga, közel 1000 gép. Éppen ennyi leállításáról és cseréjéről szóltak a hírek, a képbe beleillő időzítéssel [1]. Nyilván ugyanarra a 417-es fertőzött vezérlőre kapcsolódtak. A két támadó kód így a biztos találat érdekében két lövés, két irányból ugyanarra a célra. A turbina tehát alaptalanul keveredett gyanúba.

A 417-es támadó kód további kártétele

Az idei év elejére az is kiderült, hogy a 417-es támadó kód egy további rutinja átrendezi a kaszkádon belül a centrifugák kapcsolását. Szinte tükrözi az ideális elrendezést: a kaszkád elejére kevesebb, a végére több centrifugát tesz. A fokozaton belüli maximális szám ugyan 24 marad, de ez nem az 5. hanem a 10. fokozatban jelenik meg. Ezzel a kívülről nem látható művelettel – hiszen a kezelőnek a korábban, eredeti elrendezés során felvett normál üzemi adatokat mutatja – jelentősen lerontja a dúsítás hatásfokát [2].

Vélhető támadók, áttételesen igazolódott hatások

2011. január közepén a *New York Times* cikke független szakérőkre hivatkozva azt sugallta, hogy a vírus megrendelői az amerikai és izraeli titkosszolgálatok. Akarva vagy sem, a német Siemens is érintett lehet, mivel 2008-ban az Idaho National Laboratory szakembereivel együtt tanulmányozták a Siemens SCADA rendszerek sebezhetőségeit és ezek az adatok szivároghattak tovább a CIA, majd a Moszad kezébe. Vélelmezhető az is, hogy Izrael kapott a Khan által Líbiába exportált, majd *Moamer Kadhafi* atomfegyverről való lemondása után az USA-ba szállított P-1 centrifugákból és azokból a titkos izraeli atomtelepen, Dimonában egy működő mintarendszert épített ki a támadó kódok kipróbálásához, finomításához [11].

A hivatalos Irán máig legfeljebb kisebb zavarokat ismer el a dúsító műveiben, illetve annyit, hogy foglalkoznia kellett vírusfertőzéssel [12]. Az adatok ennél jóval többet mutatnak. A NAÜ vizsgálati anyagok szerint a Natanzban beépített centrifugák száma már 2009 novemberében majdnem 2000-rel esett vissza, és a 2009 augusztusát követő év folyamán csak a centrifugák fele, vagy még annyi sem volt feltöltve UF_6-tal [1]. Ma már egyre inkább a vírus okozta problémákhoz kötik *Gholam Reza Aghazadeh,* az iráni nukleáris

```
FC6068 is called from FC6070 six times, passing 1..6 as arg2

void FC6068(arg2, arg4)
{
      ar2 = arg2 << 3; // make pointer from offset

      for(int i=1 ; i<=164 ; i++) // for all centrifuges in the cascade
      {
            if(DB8061.[ar2] & 0x400000 == 0)
            {
                  ar1 = DB8061.[ar2] & 0x7FFF8;
                  DB8063.[arg4] = DB8063[ar1]
                        & ((1 >> DB8061.[ar2] & 0x07) +1);
            }
            arg4 += P#0.1; // next boolean
            ar2 += 4.0;    // next input address
      }
}
```

6. ábra. A visszafejtett 417-es támadó kód egy részlete (forrás: Langner blog).

csúcsszervezet vezetője 2009. júliusi – akkoriban nehezen érthető – leváltását is. Sokatmondó és ugyancsak súlyos kártételre utal az a 2010. november végi hír, hogy Natanzban az összes 54 kaszkádból 10-et már átkonfiguráltak 174 centrifugásra [13].

A Stuxnet mértékadó vélekedések szerint mintegy két évvel vetette vissza az iráni nukleáris programot, még akkor is, ha az iráni dúsítási kapacitás 2010-ben tovább növekedett. Mindezt zajos katonai csapás, bunkerrobbantó bombák, közvetlen áldozatok és súlyosabb politikai terhek nélkül érte el. Ráadásul az sem kizárt, hogy a féreg eddig fel nem fedezett, így szokványos támadás számára elérhetetlen további objektumokban is pusztított [2, 11].

Záró gondolatok

Ahogy láttuk, fokozatosan egyre több tény, adat bontakozik ki, vélekedés jelenik meg – néha váratlan fordulatokkal – a vírus kapcsán és rajzol ki egyre élesebb, összefüggő képet. A közeli jövőben sem kizártak új információk, meglepetések, de a lényeg már nemigen változik. Talán legjobb megint Langner 2010-es évet záró bejegyzését idézni [2]:

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. Arra lehet számítani, hogy az ISIS jelentésben említett 984 centrifugán túl továbbiakat is megrongált a Stuxnet. Erre a 2011. 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 ren-

geteg bennfentes tudásra volt szükség. Mindez igen kevés szervezetre szűkíti le a világon azt a kört, amely a feladat megoldására vállalkozhatott.

5. A Stuxnet interneten 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.

Kiegészítésem az 5. ponthoz: a nukleáris létesítmények, mint a kritikus infrastruktúra elemei szinte biztosan a célkeresztben maradnak. Ez új feladatokat jelent számunkra is.

Irodalom[9]

1. Vezető víruscégek részletes és folyamatosan mélyülő elemzései
   - N. Falliere, L. O. Murchu, E. Chien: W32.Stuxnet Dossier v1.3, Symantec, 2010-11-12; http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
   - Matrosov, E. Rodionov, D. Harley, J. Malcho: Stuxnet Under the Microscope, Rev 1.31, 2010-12-16; http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
2. Ralph Langner hamburgi vírusbiztonsági szakértő blogja: http://www.langner.com/en/blog
3. A Zrínyi Miklós Nemzetvédelmi Egyetem anyagai
   - Berzsenyi D., Szentgáli G.: Stuxnet – a virtuális háború hajnala. 2010-10-07; http://www.biztonsagpolitika.hu/?id=16&aid=932
   - Kovács L., Sipos M.: Stuxnet, és ami mögötte van. ZMNE, 2010-11-24; http://robothadviseles.hu/pres/KovacsL_SiposM.pdf
4. Wikipedia szócikkek
   http://en.wikipedia.org/wiki/Stuxnet; http://ru.wikipedia.org/wiki/Stuxnet; http://en.wikipedia.org/wiki/Nuclear_facilities_in_Iran, http://en.wikipedia.org/wiki/Zippe-type_centrifuge, http://en.wikipedia.org/wiki/Abdul_Qadeer_Khan
5. 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, 1783, 1785
6. Orosz hacker szakfolyóirat cikkei
   - Шпионский ярлык: история трояна Stuxnet. 2011-11-18
   - New York Times: за червем Stuxnet стоят разведки США и Израилия. 2011-01-18
   - Stuxnet полон ошибок и некачественного кода, 2011-01-20

   http://www.xakep.ru/post/53950/default.asp, 54552, 54578
7. Institute for Science and International Security (ISIS)
   - What is a Gas Centrifuge? 2003; http://www.exportcontrols.org/centrifuges.html
   - D. Albright, A. Stricker: Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target? Nuclear Iran News, 2010-11-17, jav. 12-20; http://www.isisnuclearіran.org/news/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-are-iranian/
   - D. Albright, P. Brannan, C. Walrond: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? 2010-12-22 http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf
8. Wood H. G., Glaser A., Kemp S.: The gas centrifuge and nuclear weapons proliferation. *Physics Today,* 2008. szeptember; http://www.princeton.edu/~rskemp/Kemp%20-20Gas%20Centrifuge%20and%20Nonproliferation%20-%20SPLG.pdf
9. Műszaki, tudományos és biztonságpolitikai elemzések
   - Oelrich I., Barzashka I.: Engineering Considerations for Gas Centrifuges, FAS, 2010; http://www.fas.org/programs/ssp/nukes/fuelcycle/centrifuges/engineering.html
   - Barzashka I.: Using Enrichment Capacity to Estimate Iran's Breakout Potential, FAS, 2011-01-21; http://www.fas.org/pubs/_docs/IssueBrief_Jan2011_Iran.pdf
10. Nagy felbontású centrifuga fotók Ahmadinezsád elnök natanzi látogatásáról. 2008. április
    http://www.president.ir/piri/media/main/28832.jpg … 28881.jpg
11. A New York Times cikke és magyar ismertetése
    - W.J. Broad, J. Markoff, D. E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. NYT, 2011-01-15; http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
    - Amerikai segítséggel fejleszthette Izrael az iráni atomerőművet támadó vírust. HVG, 2011-01-21; http://hvg.hu/Tudomany/20110121_stuxnet_iran_amerika_izrael
12. Iráni hírügynökségek cikkei
    - AEOI Chief Unveils New Details on West's Cyber Attack on N Sites. Teheran, FarsNews, 2010-11-23; http://english.farsnews.com/newstext.php?nn=8909021485
    - Envoys of IAEA members in Natanz to visit uranium enrichment site. Tehran, IRNA, 2011-01-16; http://www.irna.ir/ENNewsShow.aspx?NID=30190522
    - Iran dismisses reports on Stuxnet effect on nuclear facilities; http://isna.ir/Isna/NewsView.aspx?ID=News-1697213&Lang=E
    - http://isna.ir/Isna/PicView.aspx?Pic=Pic-1697213-1&Lang=ETehran, ISNA, 2011-01-17
13. 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, c0945, d0249

[9] Az összes fájlletöltés 2011-01-23-án történt