HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kovács László
kovacs.laszlo@zmne.hu

Sipos Marianna
sipos.marianna@zmne.hu

A STUXNET ÉS AMI MÖGÖTTE VAN:
TÉNYEK ÉS A CYBERHÁBORÚ HAJNALA[1]

Absztrakt

A Stuxnet nevű féreg hatalmas riadalmat okozott 2010 nyarán illetve kora őszén. A riadalom oka elsősorban az volt, hogy ez volt az első olyan rosszindulatú program, amely ipari létesítmények vezérlő szoftvereit támadta meg. Jelen írás nagyon röviden bemutatja magát a Stuxnet-et, és elemzi azokat a várható hatásokat, amelyek az információbiztonságban e féreg után felmerülhetnek. Az írás következő részében (a Hadmérnök következő számában) a komplex információbiztonság és a kormányzat lehetséges szerepe a védelemben kerül bemutatásra.

A worm called Stuxnet caused great alarm in summer and the early autumn of 2010. The main reason of the panic was that it was the first malicious program, which challenged the software to control industrial plants. This paper briefly describes itself the Stuxnet, and analyze the potential effects that may arise after this worm on the field of information security. The next part of this paper (planned in the next issue) will focus on the complex information security and the role of government on this field.

Kulcsszavak: *Stuxnet, zero-day, információbiztonság, cyberhadviselés, ipar, PLC, folyamatirányítás, SCADA ~ Stuxnet, zero-day, information security, cyberwar, industry, PLC, process controll, SCADA*

[1] Jelen publikáció a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

BEVEZETŐ

2010 őszén rendkívül aggasztó hírről adtak tájékoztatást a világsajtó különböző orgánumai. Egy olyan rosszindulatú program gyors terjedéséről érkeztek beszámolók, amelyek nem az egyszerű otthoni felhasználókat vette célba, hanem az elvileg jól őrzött és komoly, nagy biztonsági rendszerekkel rendelkező ipari létesítményeket.

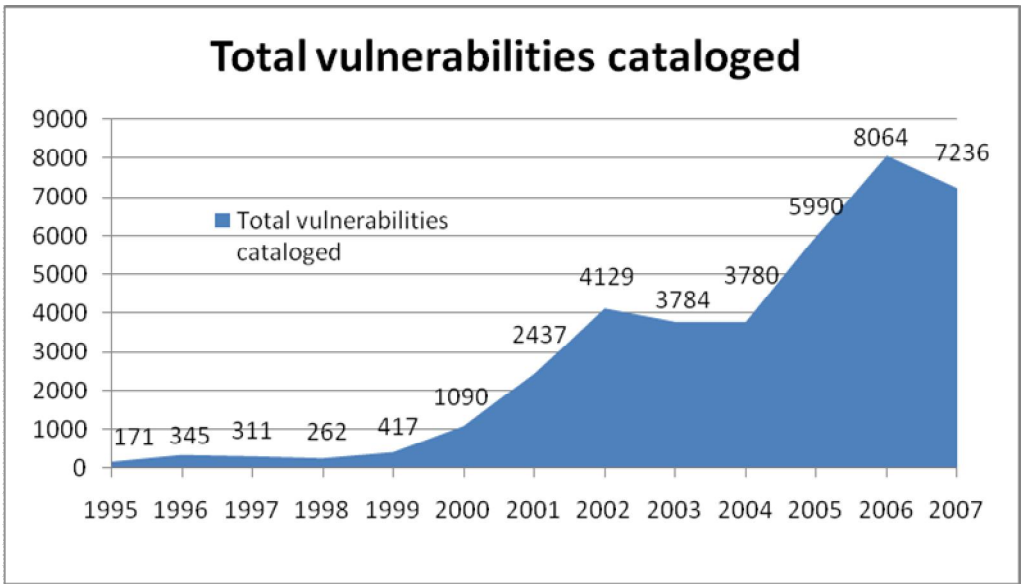
A Stuxnet névre keresztelt féreggel kapcsolatosan nagyon sok találgatás látott napvilágot. E találgatások oka elsősorban e program újdonságában keresendő. A rosszindulatú programok több évtizedes történetében ez az első olyan szoftver, amely nagy tömegben ipari létesítmények vezérlő szoftverei működését támadta.

A találgatások politikai felhangoktól sem voltak mentesek, hiszen a féreg előfordulási gyakorisága és észlelése Iránban volt a legmagasabb. Ez rögtön szemet szúrt a különböző médiumoknak, és rögtön hírül is adták: a féreg célpontja az iráni atomlétesítmények, konkrétan azok működésének leállítása. Ezeket a találgatásokat az informatikai biztonsági cégek elemzései még részben alá is támasztották, hiszen nagyon gyorsan kiderült valóban olyan ipari vezérlő szoftverek ellen készült a Stuxnet, amelyeket Irán is használ pl. a bushehri atomerőműben, vagy a natanzi centrifugáinál.

Jelen írás röviden felvázolja a Stuxnet működését és összetevőit, majd elemzi annak hatásait a különböző szoftverkörnyezetekben. Az elemzés utánajár azoknak a kérdéseknek, amelyek a Stuxnet hatása mögé engednek bepillantást.

A STUXNET

Az elmúlt évtizedekben az informatikai támadások – és ezzel együtt a rosszindulatú szoftverek száma – komoly mértékben nőtt. Természetesen a támadások az addig még nem ismert, vagy nem megfelelően kezelt sérülékenységek ellen irányulnak, illetve ezeket használják ki. [1] Az 1. ábra a CERT Statistics által katalogizált sérülékenységeket mutatja a 1995-től 2007-ig.



1. ábra. A CERT Statistics által katalogizált sérülékenységek 1995-2007-ig [2]

2010 júniusában a VirusBlokAda[2] cég fedezte fel azt a férget, amely a Stuxnet nevet kapta.

Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. Egészen pontosan a féreg a Siemens SIMATIC WinCC HMI WIMATIC Step7 által felügyelt ipari rendszereket célozta meg. [3] A dolog érdekessége, hogy ezek a szoftverek Windows operációs rendszeren futnak, tehát a Stuxnet Windows szervereken terjedt.

Ha a szerveren nem futott a fenti vezérlők valamelyike, akkor a féreg felvette a kapcsolatot az egyik központi szerverrel, elküldte neki a gép adatait, de ezen kívül ezt a gépet csak továbbterjedésre használta. Ha megtalálta a fenti ipari vezérlő szoftverek valamelyikét, akkor a WinCC adatbázis szoftverhez kapcsolódott annak kódjába előre definiált (hardcoded) default jelszóval.

A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. Elsősorban PLC[3] szoftvereket támadott, bár a múltidő használata nem teljesen helyes, hiszen a 2010 őszi események után ma is kapunk híreket a Stuxnetről, illetve annak alkalmazásáról. A WinCC/Step 7 szoftver volt mindezek közül az elsődleges, amelyet a Stuxnet megcélzott. Ez a szoftver adatkábelen keresztül kapcsolódik a PLC-hez és eléri a memória tartalmat, képes folyamatokat újrakonfigurálni, programokat feltölteni és a végrehajtás során rendelkezik bizonyos nyomkövetési funkciókkal is. Ha a PLC már programozásra került, akkor lekapcsolható róla, és a PLC már önmagában is képes a működésre. A Stuxnet e szoftver segítségével juttatta be kódblokkjait a PLC-be, majd ezeket el is rejtette.

A cél a működés szabotázsa volt, valamint az, hogy hosszú ideig lehetőleg ne fedezzék fel. Ez fél-, egyes források szerint egy évig sikerült is, miközben az eredeti Stuxnet-et továbbfejlesztették. Különböző források szerint a 2009. júniusi megjelenés tűnik a legvalószínűbbnek, ugyanakkor a Kaspersky 2009. júliusi, míg a Symantec 2010. januárról beszél. [3] [4]

A közvéleményt foglalkoztató kérdések mellett számos szakmai kérdés is felmerült. Mi az, amiben a Stuxnet féreg túlmutat az eddigi támadásokon? Miért foglalkozik vele ilyen szinten a média? Miben különleges a Stuxnet támadása az eddigi incidensekhez képest? Jelentheti ez a hadviselés egy új ágának megszületését?

A 2. ábra a nemzetközi sajtó féreggel kapcsolatos megnyilvánulásait mutatja, hiszen a világ különböző országainak közismert, hitelesnek elfogadott újságai, hírforrásai kiemelten foglalkoztak a témával.

A szakmai elemzőket – legyenek azok biztonságpolitikával, vagy akár informatikával, illetve információbiztonsággal foglalkozók – szintén felvillanyozta a Stuxnet megjelenése.

Az egyik hazai biztonságpolitikai portálon Berzsenyi Dániel és Szentgáli Gergely elemzésükben a következőket mondják: „A 2010-es év és a Stuxnet felbukkanása új mérföldkővé válhat a virtuális világ hackerek dominálta szegmensének történelmében.” [3]

---

[2] A VirusBlokAda céget 1997-ben alapították Fehéroroszországban. Alapvető tevékenységi köre a víruskereső szoftverek gyártása, illetve az ehhez kapcsolódó szoftverelemző és értékelő munka. Honlapjuk szerint a Vba32 nevű terméküket sikeresen alkalmazzák a Belarusz Köztársaság Nemzeti Bankjában, illetve számos fehérorosz szervezetnél és vállalkozásnál. A Stuxnet felfedezése meghozta a világhírt is a cégnek. [16]

[3] A PLC - Programmable Logic Controller, azaz programozható logikai vezérlő. PLC-ket nagy számban az ipari szabályozástechnikában, a különböző villamos, illetve az ilyen módon működtetett folyamatok irányításában használják. Ezeket az ipari folyamatokat – pl. szerszámgépek, vagy gyártósorok vezérlése – a PLC-ket megelőzően logikai hálózattal, vagy relés rendszerekkel oldották meg. Ezek egyik igen komoly hátránya az volt, hogy sok alkatrészből álltak, hibakeresésük bonyolult, valamint fejlesztési igény esetén módosításuk nehézkes volt. A PLC-k szabványosított be- és kimenettel rendelkeznek. Kompakt felépítésük, valamint az említett szabványosítás lehetővé teszi az egyszerű szabályozási rendszer megépítését, valamint az üzembiztos működést, és a program módosításával a szabályozás későbbi megváltoztatását is.

A Symantec informatikai biztonsági elemzője, O Murchu jelentette ki: „Soha nem láttunk ilyet eddig”, és ehhez a kijelentéshez csatlakozott a Kaspersky is, hiszen az ő elemzéseikben és rosszindulatú szoftverek elleni munkájukban sem találkoztak még ehhez hasonlóval. [4]

2. ábra. Stuxnet a médiában.

A 4 zero day exploit és más módszerek

A Stuxnet nem úgy működik, mint egy szokásos kártékony program. Nem lop személyes adatokat, nem használja a hitelkártyák információit, nem nyúl a bankszámlákhoz, nem teszi tönkre a fertőzött gépek szoftvereit és hardverjét. Nem fenyeget a DoS támadással, mint egy bűnszervezet, váltságdíjat követelve. A Stuxnet magára a szabotázsra készült, titokban terjedve. [5]

A Stuxnet felfedezői és első elemzői megdöbbenve tapasztalták: a féreg négy, eddig még fel nem fedezett biztonsági hiányosságot, azaz sebezhetőséget használ ki. „4 zero-day-t használ, ez valóban, igazi őrület” állítja O Murchu. [4] „Hihetetlen, a Stuxnet 4 zero-day sérülékenységet használ ki, ami példa nélkül álló” áll a Symantec biztonsági jelentésében. [6]

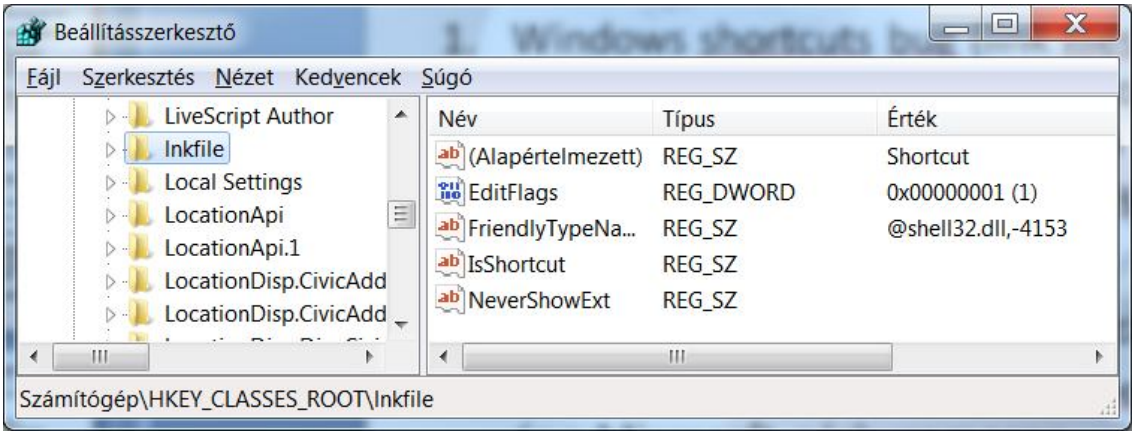
A Zero-day bug, azaz a nulladik napi támadás javítatlan (unpatched) biztonsági rést jelent. A kifejezést azokra a számítógépes biztonsági fenyegetésekre (hibákra) használják a szakemberek, amelyek egy adott számítógépes alkalmazás még felfedezetlen, nem publikált sebezhetőségét jelentik. Egy rosszindulatú program jellemzően egy zero-day bug-ot használ ki, hisz egy újonnan felfedezett sérülékenység önmagában is jelentős érték, mivel rendkívül bonyolult a felfedezése. Természetesen a szoftvergyártók igyekeznek biztonsági rések nélkül létrehozni programjaikat és a felfedezett sérülékenységet minél előbb egy javító csomaggal megszüntetni. Általában egyetlen zero-day bug is komoly veszélyt jelent, hisz a megtámadott alkalmazás készítőjének nincs tudomása e sérülékenységről, vagy még nem sikerült javítást készíteni hozzá, tehát még nincs védelem ellene.

A Stuxnetben a következő 4 zero-day bug-ot fedezték fel:

1. Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) CVE-2010-2568: [7]

Ez egy Windows shortcuts bug, melyet szokás link fájlnak is nevezni, mert a fájlok kiterjesztése .lnk, és a megjelenített ikonhoz csatolja, linkeli az alkalmazást, vagy a mappát. Használható helyi fájlok vagy URL-ek gyors eléréséhez. Mindkét esetben egy meggörbült nyíl ikon látható a hivatkozás ikonjának bal alsó sarkában, és nem szerepel a kiterjesztés a név mögött. Ez a kiterjesztés rejtve marad a Windows Explorer felhasználói számára, még akkor is, ha az ismert fájlok kiterjesztésének elrejtése opciót kivesszük a megjelenítésből, mivel elrejtését, amint azt a 3. ábrán láthatjuk, a registryben a HKEY_CLASSES_ROOT\lnkfile mappa NeverShowExt tulajdonsága vezérli. Az IsShortcut tulajdonság váltja ki a bal alsó sarokban a görbült nyíl ikon megjelenítését. Ezt a technikát használja ki a féreg az USB-ről a számítógépre való feljutáshoz.

2. Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073): [8]
   Nyomtató puffer szolgáltatás távoli kód végrehajtással. Ennek segítségével másolta át magát a fertőzött gépről egy másikra. Ez a sérülékenység teszi lehetővé, hogy egy fájlt írhassunk a még tiszta kapcsolódó gép %System% könyvtárába.
3. Windows Win32k.sys Local Privilege Escalation vulnerability (MS10-073): [15]
   EoP (elevation of privilege) bug, vagy local privilege escalation vulnerability, magasabb hozzáférési szint engedélyezés. A sérülékenység a Windows Kernel-Mode meghajtóinál engedélyezheti a magasabb hozzáférést.
4. Egy további EoP bug: [4]

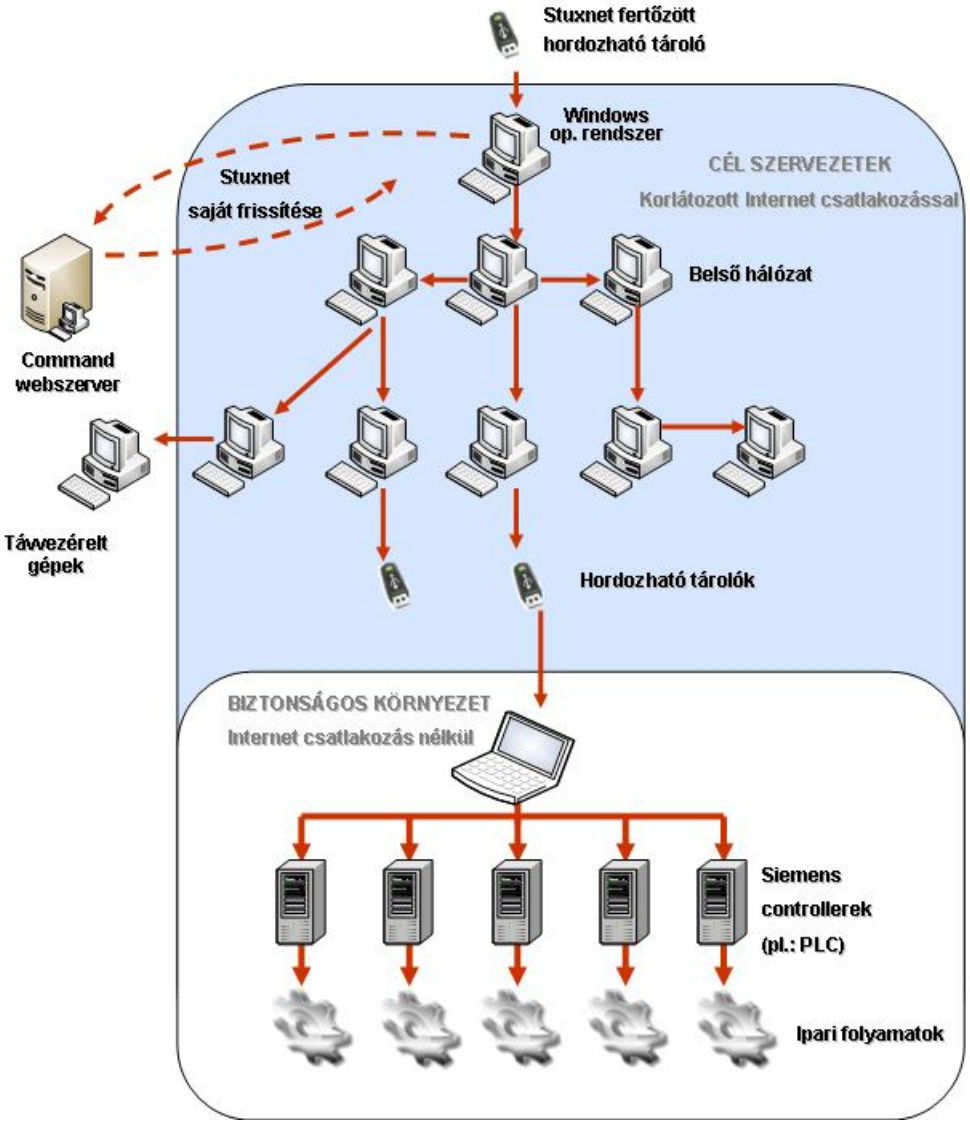


3. ábra. Link fájlok beállításai a registryben.

Ezen kívül a Stuxnet használta még a Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874) sérülékenységet, melyet az a notorious Conficker féreg is használt, amely 2008-2009 fordulóján gépek millióit fertőzte meg. A Panda Security a Global ThreatWatch oldalán narancsjelzésűre minősítette, amely azt jelenti, hogy figyelemre méltó veszélyt jelent. [9] [10] [11]

Ugyanakkor érdemes megjegyezni, hogy ezt a sérülékenységet már 2008.október 23-án az MS08-067 „an emergency pach" frissítésében javította a Microsoft. [12]

Mindezeken túl a féreg kihasznált egy eddig – szintén – felderítetlen sérülékenységet a Siemens felügyelő szoftverben. Mindezeken túl legalább két lopott digitális aláírással rendelkezett, így legitimnek tűnt.



4. ábra. A Stuxnet terjedése a belső hálózaton [17]

A Stuxnet működése

A féreg másolatot készített saját magáról és létrehozta az .lnk fájlokat is, amelyek erre a másolatra mutatnak. Amikor egy alkalmazás, amely ikonokat tud megjeleníteni, pl. a Windows Explorer böngészi a meghajtót, a link fájl futtatja a férget. Ezzel a módszerrel USB-n keresztül terjed, tehát fertőzött USB-vel a zárt hálózatra is feltelepül. Mint tudjuk a zárt hálózatok szoftvereinek karbantartását többnyire USB-k segítségével oldják meg.

Az USB-t használó rosszindulatú szoftverek leggyakrabban az AutoRun funkciót felhasználva jutnak a számítógépre. Természetesen javasolt ennek a funkciónak a kikapcsolása védett rendszerek esetén, ennek ellenére a Stuxnet így is terjedhetett. [14]

Kikapcsolt AutoRun esetén a link fájlok futtatási funkciójában felfedezett 1. zero-day bugot kihasználva jutott fel az USB meghajtóról a számítógépre. A hálózaton a 2. zero-day bug segítségével terjedt tovább.

A fertőzött USB a következő fájlokat tartalmazta:

- Négy darab .lnk fájlt:
  - Copy of Shortcut to.lnk;
  - Copy of Copy of Shortcut to.lnk;

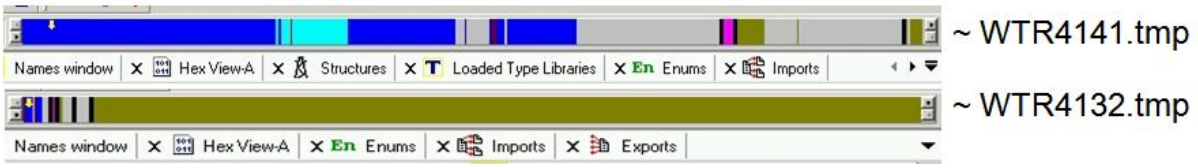
    - Copy of Copy of Copy of Shortcut to.lnk;
    - Copy of Copy of Copy of Copy of Shortcut to.lnk;
- valamint a következő valójában dll fájlokat:
    - ~WTR4141.tmp (~25Kb);
    - ~WTR4132.tmp (~500Kb).

Ezen fájlok nevei rögzítettek a kódban (hardcoded). Amikor egy ikonokat megjeleníteni tudó alkalmazás futni kezd, a féreg .lnk fájljai az ikonok megjelenítése helyett a ~WTR4141.tmp kódját hajtják végre ezzel átadva a vezérlést a féregnek.

A kisebb .dll feladata a nagyobb betöltése, de előtte még elrejti saját magát úgy, hogy a kernel32.dll és az ntdll.dll fájlkezelő függvényeiben beállítja, hogy az '.lnk'-ra végződő és a '~WTR'-el kezdődő valamint '.tmp'-re végződő fájlokat ne mutassa meg. Tehát minden ilyen fájlt elrejt. [13] Emiatt rögzítettek (hardcoded) a fájlnevek.

Ezután a kisebb .dll betölti a nagyobb .dll-t a memóriába, de nem a LoadLibrary API felhasználásával, ahogyan a szokott módon a .dll-ek betöltődnek, hiszen normál esetben a LoadLibrary kivételt dobna, mivel nem találná meg a betöltendő fájlokat, amiket a Stuxnet már elrejtett. Az Ntdll.dll figyeli a LoadLibrary-t és speciális fájlnév hívásakor átveszi az irányítást. [14]

Az 5. ábrán láthatjuk a két dll fájl szerkezetét. Az első, kisebb méretű fájl kis fehér nyíllal jelzett kék területe a kód, itt ez a nagyobb méretű, míg a második .dll-ben a khaki színű adatszegmens a nagy terület, hisz ez tartalmazza a kódolt valódi férget. A 2. dll kisméretű kódszegmense szinte csak a kicsomagolás kódját tartalmazza.



5. ábra. A dll fájlok szerkezete, kék a kódszegmens, khaki az adatszegmens.

A ~WTR4132.tmp a betöltés után átveszi a vezérlést és kicsomagolja a memóriába a valódi támadást végző dll fájlt.

A féreg az operációs rendszer típusának és verziójának ellenőrzése után megnyitott egy rejtett ablakot, az ablak osztályának neve: 'AFX64c313'. Ez az ablak arra várt, hogy egy USB drivert tegyenek a gépbe. Mielőtt megfertőzte volna az új USB-t, leellenőrizte, hogy az aktuális dátum még ne legyen 2012. június 24. A fertőzés nem lehetett 21 napnál régebbi; a meghajtón legalább 5 MB szabad helynek kellett lennie; valamint a meghajtón legalább 3 fájlnak már fent kellett lennie …

A Stuxnet ha internet elérést talált, külső szerverekhez kapcsolódott. A fertőzés elején ezek a szerverek a www.mypremierfutbol.com Malaysiai és a www.todaysfutbol.com Dániai szerverek voltak, de időközben változtak. A féreg külső szerverekhez kapcsolódva frissíteni is tudta magát, és peer-to-peer frissülésre is képes volt. Peer-to-peer frissülésnek ebben az esetben azt a folyamatot hívjuk, amikor két vírus találkozásakor a frissebb él tovább.

A Stuxnet terjedése során ellenőrizte a gépre telepített vírusellenőrző programokat és a gépen található vírusirtó szoftvertől függően választotta ki, mely engedéllyel rendelkező futó folyamatba injektálja be magát, ráadásul további, már futó folyamatba is át tudta magát injektálni. [13]

Amint a féreg aktívvá vált a gépen, első feladata saját fájljainak elrejtése volt. Bizonyos feltételek esetén, ha már fertőzött volt az adott USB meghajtó, akkor letörölte a féreg saját magát. Ugyanez igaz volt abban az esetben is, ha az USB meghajtó már további 3 gépet is

megfertőzött, azaz a Stuxnet ebben az esetben is letörölte magát. Az utóbbi két technikával jelentősen csökkentette a felfedezésének esélyét. [14]

A Stuxnet, amint azt korábban említettük 2012. június 24 után nem fertőz tovább. [14]

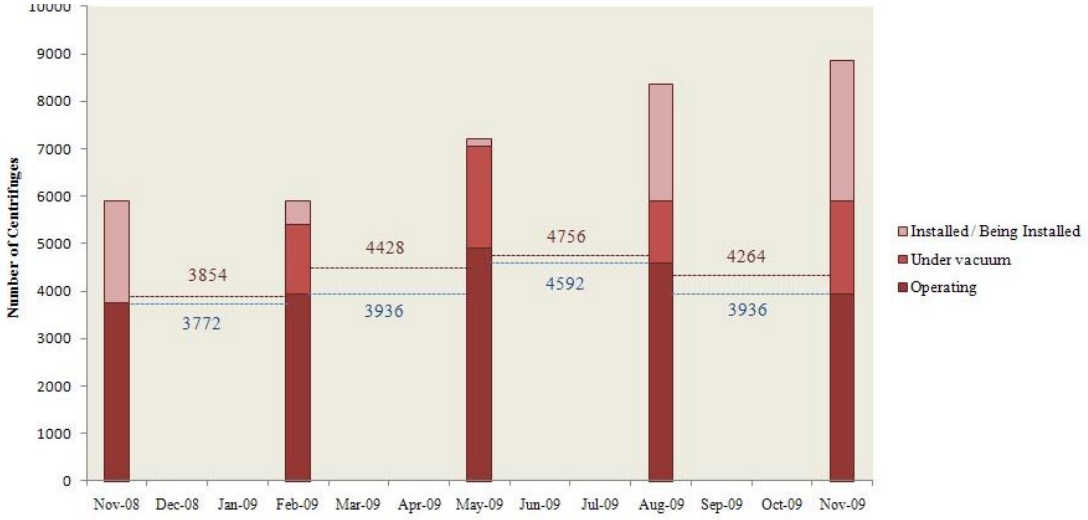
AMI A STUXNET MÖGÖTT VAN

Jelen írás is számos olyan kérdésnek adott hangot, amely a Stuxnet valódi céljait vagy akár létrehozóit érintette, mindazokon túl, hogy nagy vonalakban ismertette a féreg felépítését és működését.

Bruce Schneier információbiztonsági guru szerint a Stuxnetet létrehozni meglehetősen drága munka volt. Becslések szerint 8-10 nagyon jól képzett programozó, minimum hat hónapos munkája van benne. Ezen kívül ott van még a tesztelés kérdése is, amely csak egy jól felépített laborban történhetett, hiszen ez elengedhetetlen lehetett a féreg útjára bocsátása előtt. A zero-day exploitok kérdése is érdekes, hiszen ezek közül egy is komoly értéket képvisel. Akárki is írta a Stuxnetet – mondja Schneier –, egy csomó pénzt volt hajlandó költeni rá. [18]

2011 januárjában a New York Times (NYT) adott elsőként hivatalosan hírt arról, hogy a Stuxnet mögött Izrael áll, hiszen mindezidáig a féreg forrásáról csak feltételezések és találgatások léteztek. A NYT cikke összhangban áll Schneier előbb idézett véleményével, hiszen a cikk szakértőkre hivatkozva szintén megemlíti, hogy a férget olyan ipari létesítményben kellett tesztelni, mint a későbbi célpontok. Ez a létesítmény pedig nem más, mint az izraeli Negev sivatagban lévő Dimona komplexum, amely köztudottan az izraeli nukleáris kutatás központja. Itt tesztelték és próbálták ki az urándúsítás elengedhetetlen kellékein, az izotópcentrifugákon, illetve ezek irányító szoftverein a Stuxnetet. A cikk kitér arra is, hogy Hillary Clinton és a nemrég nyugdíjba vonult Moszad vezető, Meir Dagan egymástól függetlenül, de nagyjából azonos időben kijelentették: remélik az események az iráni atomprogramot akár több évvel is visszavetik. Ez természetesen arra is következtetni enged, hogy az akció nemcsak Izrael magánakciója volt, hanem az USA is hathatósan közreműködött. [19]

Ezzel összefüggésben érdekes összehasonlító adatsor jelent meg a Federation of American Scientists egyik oldalán. E szerint a működő iráni centrifugák száma jelentősen visszaesett 2009 novemberére. (6. ábra) [20] [21] [22]



6. ábra. Az iráni izotópcentrifugák számának alakulása a Stuxnet terjedése idején. [20]

Az események során a média hatalmas érdeklődése szinte nyilvánvaló volt, hiszen a Stuxnet, pontosabban annak veszélyessége miatt rendkívül sok egyéb kérdés is felmerült.

Gyakran elhangzott a kérdés: most kezdődött az információs háború kora? Erre a kérdésre azonban nem egyértelmű a válasz. A cyberhadviselés első és igen komoly – akár az olyan nemzetközi politikai vagy katonai szervezetet, mint a NATO-t is komolyan érintő – eseménye a 2007-es észtországi konfliktus volt. Már akkor számos olyan kérdés vetődött fel, amelyekre azóta sem igen kaptunk választ.

Ezekre a kérdésekre keresi a választ jelen írás következő része, amely többek között a komplex információbiztonság szerepét, valamint az állam ezen a téren megvalósítandó feladatait tervezi elemezni.

2011. február elején, az immár 47-ik alkalommal megrendezésre kerülő Munich Security Conference különös aktualitást ad ezeknek a kérdéseknek. A konferencián, amelyen államfői, illetve külügyminiszteri szinten képviselteti magát sok vezető hatalom (pl. az USA, Nagy-Britannia, Oroszország, Németország), első ízben kerül sor nagyhatalmak részéről annak tisztázására, hogy hol kezdődik a háború a cybertérben. Ezen kívül a program kitér arra is, hogy meg kell teremteni a cybertérben is a genfi, illetve a hágai egyezményekhez hasonlóan a cyberhadviselés szabályait. [23]

(*Folytatjuk ...*)

IRODALMI HIVATKOZÁSOK

[1] A. Householder, K. Houle, C. Dougherty: Computer Attack Trends Challenge Internet Security. Computer magazine, IEEE Computer Society (2002 April) pp. 5-7. http://csdl2.computer.org/comp/mags/co/2002/04/r4s05.pdf

[2] CERT Statistics. http://www.cert.org/stats/#vuls

[3] Berzsenyi D, Szentgáli G.: STUXNET: a virtuális háború hajnala. http://www.biztonsagpolitika.hu/?id=16&aid=932&title=STUXNET:_a_virtu%C3%A1lis_h%C3%A1bor%C3%BA_hajnala (2010. október 7)

[4] G. Keizer: Is Stuxnet the ’best’ malware ever? http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_?

[5] B. Schneier: *Schneier on Security, Stuxnet*, http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[6] W32.Stuxnet, Symantec Security Response, http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=2

[7] Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (bugtraq ID 41732), (CVE-2010-2568) Security Focus, http://www.securityfocus.com/bid/41732, Published: Jul 15 2010, Updated: Aug 11 2010, Detected: VirusBlokAda.

[8] Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073). Security Focus, http://www.securityfocus.com/bid/43073, Published: Sep 14 2010, Updated: Sep 27 2010, Detected: Microsoft.

[9] Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874), Security Focus, http://www.securityfocus.com/bid/31874, Published: Okt 22 2008, Updated: Feb 9 2009, Detected: Microsoft

[10] G. Keizer: 'Huge increase' in worm attacks plagues unpatched Windows PCs, Computerword, http://www.computerworld.com/, Computerword Inctitute, (2009. January 12.) http://www.computerworld.com/s/article/9125737/_Huge_increase_in_worm_attacks_plagues_unpatched_Windows_PCs

[11] Global ThreatWatch, http://www.pandasecurity.com/homeusers/security-info/gtw/ Panda Security Press, http://press.pandasecurity.com/

[12] Microsoft Security Bulletin MS08-067 – Critical Vulnerability in Server Service Could Allow Remote Code Execution (958644), TechNet, http://www.microsoft.com/technet Microsoft Corporation http://www.microsoft.com (2008. October 23.) http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

[13] N. Falliere, L. O Morchu, E. Chien: Win32.Stuxnet Dossier, Symantec Security Response, Symantec AntiVirus Research Center, (Nov. 2010) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[14] L. O Murchu: W32.Stuxnet Installation Details, Symantec blogs, http://www.symantec.com/connect/blogs/w32stuxnet-installation-details

[15] Microsoft Security Bulletin MS10-073 – Important, Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957), (2010, October 12.) http://www.microsoft.com/technet/security/bulletin/ms10-073.mspx

[16] http://www.anti-virus.by/en/index.shtml

[17] http://www.nytimes.com/ imagepages/2011/01/16/world/16stuxnet_g.html?ref=middleeast

[18] Schneier on Security. A blog covering security and security technology. Stuxnet. http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[19] W. J. Broad, J. Markoff, D. E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. In: New York Times, 2011. január 15. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2&sq=stuxnet&st=cse

[20] http://www.fas.org/blog/ssp/wp-content/uploads/NumberCentrifuges1.jpg

[21] Kim Zettes: Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage. In: Wired, 2010.november 15. http://www.wired.com/threatlevel/2010/11/stuxnet-clues/

[22] Mit buherál a Stuxnet? http://buhera.blog.hu/2010/11/14/mit_buheral_a_stuxnet

[23] Munich Security Conference (Münchener Sicherheitskonferenz) http://www.securityconference.de/