HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Gyebrovszki Tamás
gyebrovszki.tamas@nbsz.gov.hu

STUXNET - MINT AZ ELSŐ ALKALMAZOTT KIBERFEGYVER - A TALLINNI KÉZIKÖNYV SZABÁLYRENDSZERE SZEMPONTJÁBÓL

Absztrakt

A cikk meghatározza, hogy a Tallinni Kézikönyvben lefektetett szabályok alapján hogyan válaszolhat egy állam egy olyan kibertámadásra, amilyet a Stuxnet féreg valósított meg Iránban. Választ keres továbbá arra a kérdésre, hogyan kell alkalmazni a kiberhadviselés szabályait a hagyományos hadviselés függvényében. Végül sürgeti a kiberműveleteket szabályozó jogi keretrendszer kidolgozását.

This article defines a response should be done to a cyber attack such as worm called Stuxnet performed in Iran based on rules defined in Tallinn Manual. It searches an answer how to apply rules of cyberwarfare in comparison with traditional warfare. It points up a need for establishing legal framework regarding to cyber operations.

Kulcsszavak: *Stuxnet, kiberfegyver, kiberkonfliktus, kritikus infrastruktúra. Stuxnet, cyber weapon, cyber conflict, critical infrastructure.*

BEVEZETÉS

A tömeges számítások elvégzése a tudomány számos területén okozott fejfájást, így a számítógép feltalálása nagy ugrást jelentett. Konrad Zuse német feltaláló a világon elsőként létesített programvezérelt számítógépet 1938-ban [1]. A számítógépet később már információ feldolgozásra, tervezési feladatokra is felhasználták, példa erre a Budapesten található Erzsébet-híd újjáépítése, amikor a híd statikai számításait az MTA Kibernetikai Kutatócsoport végezte a Magyarországon első, az M3 megnevezésű 1959-ben átadott számítógép segítségével [2]. Viszonylag rövid idő alatt megjelentek számítógépek a távközlés, az irányítástechnika, gyártásirányítás, kereskedelem és még számos területen. Napjainkra kevés olyan feladat létezik, ahol nem alkalmazható számítógép.

Korunk számítógépe magában hordozza a globális összekapcsolhatóságban rejlő páratlan lehetőséget és persze az ezzel járó veszélyeket is. Az egyre kisebb méretű és egyre nagyobb képességű eszközök általi fejlődési lehetőséget csak elcsépelt jelzőkkel illethetjük, mint forradalmi, vagy ugrásszerű. Csak a távközlés területén egyetlen példa, hogy akár kerékpározás közben is megkapjuk elektronikus leveleinket a világ bármely részéről, ami az információhoz jutásunkat, gazdasági lehetőségeinket segítheti elő. A kibertér azonban nemcsak előnyös tulajdonságokkal segíti életünket, hanem sajnos potenciális veszélyforrás is egyben.

Ahogy az alkalmazások egyszerűsítik azokat a feladatokat, amelyekkel korábban sok időt töltöttünk, egyre több olyan van, melyekben nem kellene megbíznunk, sőt óvakodnunk kellene használatba vételüktől. Jó példa ezekre az olyan mobilalkalmazások, amelyek egyre népszerűbbek, azonban gyanús tevékenységeket, vagy egyenesen rosszindulatú funkciókat is végeznek. Az elmúlt egy évben sokszorosára emelkedett a mobiltelefonokra fejlesztett malware-k száma [3]. Az okostelefonok elterjedtek és a használói között kormányfők, állami intézmények vezetői, védett személyek is szép számmal vannak. E személyek célpontok, elsősorban kémkedési célzattal gyűjtenek adatokat róluk, a hagyományosnak mondható eszközökkel [4] illetve a mobil malware-k útján, vagy akár piaci termékek is találhatók [6] személyek követésére, ellenőrzésére. A kritikus infrastruktúrák kitettsége is okot ad a fejfájásra, ugyanis ezek az ipari vezérlőrendszerek (ICS) sok esetben elavultak és sérülékenyek [12].

A kritikus infrastruktúrát üzemeltető intézményeket fenyegető kibertámadások már emberáldozattal is járhatnak, ami indokolta, hogy az elmúlt években komoly hangsúlyt kapott a védelmi képességek erősítése, a rendszerek védelme.

Az informatika fejlődése a társadalom fejlődését erősíti, olyan módon, hogy egy államnak és annak szereplőinek minőségileg magasabb színvonalú életet kínál, magasabb hatékonysággal gazdálkodik, termel, szolgáltat. Az információs társadalom elsősorban nem azt jelenti, hogy az állampolgárok többsége rendelkezik Internet hozzáférési lehetőséggel, hanem azt, hogy az állam, a kormányhivatalok, az önkormányzatok és a közigazgatás egyéb szereplői, gazdaság szereplői olyan saját belső (többnyire összekapcsolt) informatikai rendszereket alkalmaznak, amelyeknek központi szerepe van a termelésben, a gazdaságban és általában a társadalomban.

Kulcskérdés értékelnünk, hogy mekkora a kár, ha a fent említett kritikus infrastruktúrákat, információs társadalmat éri kibertámadás, hogyan védekezzünk a támadások ellen, amikor az információ szabad áramlása és hozzáférhetősége társadalmi érték? Hogyan kell védekezni, csökkenteni a kárt, milyen eszközöket vethetünk be, melyek a jogi keretek [7]? Az Irán urándúsító kapacitását támadó Stuxnet malware a Tallinn Kézikönyv szerint hogyan sorolható be és mi lehetne a jogos válaszintézkedés?

Cikkemben többek között ezekre a kérdésekre adok választ a Tallinni Kézikönyv felhasználásával.

„TALLINN KÉZIKÖNYV A KIBERHADVISELÉS NEMZETKÖZI JOGI SZABÁLYAIRÓL” [5]

Tallinn a 2007-ben elszenvedett kibertámadás, Észtország fővárosa. A NATO Cooperative Cyber Defence Centre of Excellence-t (NATO Kibervédelmi Kiválósági Központot, továbbiakban CCDCOE) 2008. május 14-én létesítették Tallinnban, célja a védelmi képességek erősítése. A CCDCOE megalapításától kezdve a NATO vezetőinek ad technikai és jogi tanácsokat a kiberhadviseléssel kapcsolatos ügyekben. A szponzorok között van Hazánk, Észtország, Lettország, Litvánia, Németország, Olaszország, Lengyelország, Szlovákia, Spanyolország, Hollandia és az Egyesült Államok.

A 2013-ban a Cambridge University Press által kiadott könyv a „Tallinn Manual on the International Law Applicable to Cyber Warfare” címet viseli (továbbiakban Kézikönyv). A Kézikönyv szerzőit és közreműködőit a CCDCOE hívta meg neves egyetemekről, intézményekből független nemzetközi jogászszakértők, technikai szakértők, a szerkesztőbizottság, és a megfigyelők voltak, összesen 46 fő. A három évig tartó munka célja az új típusú hadviselés, a kiberhadviselés terén alkalmazható jogi és katonai lépések vizsgálata volt mind a jus ad bellum mind a jus in bello vonatkozásában. A fő hangsúlyt azonban a békeidőben végzett ellenséges kibertevékenységek elleni jogi lehetőségek vizsgálatára fordították. A munka eredménye lett a 302 oldalas Kézikönyv. A projekt során szorosan együttműködtek a tallinni CCDCOE kutatóintézettel. A projekt igazgatója Michael N. Schmitt professzor volt aki a US Haditengerészeti Főiskola Nemzetközi jogi tanszékének vezetője, koordinátora Dr. Eneken Tikk vezető szakértő volt. Dr. Tikk, a 2007-es kibertámadás elemzésével és dokumentálásával foglalkozott, ezt követően számos országgal, nemzetközi szervezettel működött együtt a kiberbiztonság stratégia területén. Bár a Kézikönyv nem hivatalos dokumentum, nem tükrözi sem a CCDCOE, sem a szponzor államok, sem pedig a NATO nézőpontját, a maga nemében egyedülálló értékkel bír, nincs ilyen átfogó jellegű, a kiberbiztonság területén alkalmazható jogi lépésekről, elvekről szóló könyv. Véleményem az, hogy az egyes országok felhasználhatják a nemzeti jogszabályalkotásukban.

A Kézikönyv 2 részből áll, a részeken belül fejezetek vannak, ezeket pedig szekciók tagolják tovább. Az egyes szekciókon belül találhatóak meg a szabályok. Minden szabályt pontokba foglalt kommentár, magyarázatok és példák támasztják alá. Az első rész a „Nemzetközi kiberbiztonsági jog”, a második a „Kiberhadijog” címet viseli.

Maga a Kézikönyv 95 szabályt tartalmaz. A szövegek nem kötelező érvényű ajánlást, hivatalos álláspontot tükröznek, hanem többféle szempont bemutatásával a jogalkotás további lépéseiben ad zsinórmértéket. A szerzők véleménye szerint az állam vagy felelősségre vonja az agresszort, vagy „arányos ellenintézkedésekkel” válaszolhat.

Az első fejezet az állam és a kibertér viszonyát határozza meg. A kibertámadásokat „fegyveres támadásnak” lehet minősíteni, így jogos az önvédelem a megtámadott állam részéről, beleértve a hagyományos fegyverek alkalmazását is. Ugyanakkor nem tekinthető fegyveres támadásnak a kiberkémkedés, a számítógépes lopás, a honlapok elleni támadások, amennyiben a károk nem állami méretűek. Az agresszor állam viseli a felelősséget, akkor is, ha más országokból való közvetítők útján végzi a támadást. A kézikönyv összeállítói szerint a kibertámadásokat a vegyi, a biológiai és a radiológiai fegyverek alkalmazásához kell hasonlítani.

A szuverenitás keretében az állam hatalma kiterjed a fennhatósága alatt álló területen, a kibertér és a kibertevékenység ellenőrzésére is. Jogosult szabályokat alkotni azon személyek vonatkozásában, akik a fennhatósága alatt álló területen kibertevékenységet folytatnak, valamint magáról az ellenőrzése alatt álló kibertér infrastruktúrájáról is. A nemzetközi légtérben és vizeken, valamint a világűrben – a légügyi és a tengeri hajózási joghoz hasonlóan – az adott

járműben vagy objektumban folytatott kibertevékenységre a tulajdonos állam szabályai vonatkoznak, és az azok elleni kibertámadás az adott állam elleni támadásnak minősül. Az államok felelősséggel tartoznak, ha területükről az ellenőrzésük alatt álló szervezetek más országok ellen kibertámadást hajtanak végre. Az azonban, hogy a kibertámadást egy adott országból indították, még nem bizonyítja az érintett ország felelősségét. Fennáll ugyanis annak a lehetősége is, hogy más államok használták az adott ország kiberterét a támadás elkövetésére. A kibertérben megtámadott államnak joga van arányos ellenlépéseket tenni.

A kiberművelet akkor minősül erő alkalmazásának, amikor hatása összemérhető egy hagyományos fegyveres támadással. Az erő alkalmazásának tisztázása érdekében a szerzők meghatározták az erővel való fenyegetés fogalmát. Megállapították, hogy olyan kibertámadás esetén, amelynek hatása felér egy fegyveres támadásával, az államnak joga van az önvédelemhez, de ennek során figyelembe kell vennie a szükségesség és az arányosság elvét. Egy adott állam jogosult a kibertámadás ellen fellépni, ha az már bekövetkezett vagy fenyegető közelségben van a bekövetkezése. Az államoknak joguk van az önvédelmet több országgal közösen kollektív védelem keretében biztosítani. Az önvédelemnek összhangban kell lennie az ENSZ Alapokmányának 51. cikkelyével, amely szerint a támadás tényéről azonnal tájékoztatni kell az ENSZ Biztonsági Tanácsát. A nemzetközi szervezetek kiberhadviselésben történő szerepvállalását az ENSZ Biztonsági Tanácsa esetében, illetve a regionális szervezetek vonatkozásában áttekintették és megállapították, hogy a kibertámadások során a nemzetközi szervezeteknek is joguk van a fellépésre.

A Kézikönyv második fejezete a kiberkonfliktusokkal foglalkozik, az állam joga az önvédelemre, arányos ellenlépés megtételére és a nemzetközi szervezetek beavatkozásának lehetőségét.

A harmadik fejezet pedig áttekinti a fegyveres konfliktusok jogszabályi hátterét és azok alkalmazhatóságát a kiberhadviselésre. Fontos megállapítás, hogy a kibertámadásokra is az általános hadviselésre érvényes szabályok vonatkoznak. Ezt követően a kiberhadviselés földrajzi kiterjedésének kérdésével foglalkoztak, majd megszabták a nemzetközi és az államon belüli fegyveres kiberkonfliktusok kereteit.

Az alapvető probléma itt jelentkezik, hiszen a támadó kilétének meghatározása nem triviális, a hadviselő felek azonosítása a hagyományos hadviselésben biztosított, a kibertérben ez nincs így, a *Támadó meghatározása komoly nehézségekbe ütközik.*

A negyedik fejezet magát a kiberkonfliktust tekinti át, ennek keretében foglalkozik a támadások szereplőivel, a támadásokkal, a hadviselés módszereivel, az óv- és ellenintézkedésekkel, az árulással, a kémkedéssel. Megállapították, hogy nincs arra vonatkozó szabály, ki vehet részt a kiberkonfliktusokban. Amennyiben a fegyveres erők tagjai a nemzetközi jog alapján elveszítik katonastátusukat, akkor elfogásuk esetén nem tekinthetők hadifogolynak. A konfliktusban érintett lakosság azon tagja, aki részt vesz a műveletekben, elveszíti a civilekre vonatkozó védettségét. A kiberműveletekben részt vevő felbérelt zsoldosok nem tekinthetők harcoló félnek, így hadifogolystátuszt sem kaphatnak.

Védekező és támadó kiberhadműveletről a következőket mondják: Akkor minősül egy művelet a kibertérben elkövetett támadásnak, ha hatására személyek sérülnek vagy halnak meg, illetve vagyontárgyak rongálódnak vagy semmisülnek meg. A támadások célszemélyei lehetnek a fegyveres testületek és szervezetek tagjai. A nemzetközi jog a kibertérben is tiltja a terrorizmust és annak eszközeit. A hadviselés eszközei és módszerei kapcsán ügyelni kell arra, hogy nem szabad felesleges sérülést és szükségtelen szenvedést okozni ellenfélnek. A kiberműveletekre is vonatkozik az arányosság elve, amelynek alapján a megtámadott fél nem okozhat sokkal nagyobb veszteséget a támadónak, mint amennyit elszenvedett. A kiberműveletekben a szemben álló feleknek figyelembe kell venni a polgári személyek

védelmét, valamint ügyelni kell a támadási módszerek megválasztására, a célok kiválasztására, a támadás előtti figyelmeztetésre, illetve a megtámadott fél védelmi kötelezettségére.

A kiberhadviselésben az árulás, a megtévesztés és a kémkedés kérdéskörét vizsgálva megállapították, hogy hasonló jogok vonatkoznak ezekre a tevékenységekre, mint a hagyományos hadviselés során.

A Tallinni Kézikönyv szerzői az ötödik fejezetben a védett személyek és objektumok meghatározásával és védelmével foglalkoznak. Védettséget élveznek az egészségügyi, a vallási, az ENSZ-hez tartozó személyek, eszközök és objektumok, valamint a gyermekek, az őrizetben lévő személyek, az újságírók, a polgári lakosság, a veszélyes létesítmények, a diplomáciai testületek és a kulturális javak.

A hatodik fejezet a megszállással kapcsolatos nemzetközi jogi kérdéseket dolgozza fel. A kiberművelet során elfoglalt területen a védendő személyek jogaira figyelemmel kell lenni, valamint olyan mértékben biztosítani kell a kibertérhez való hozzáférést, amely a védett személyek biztonságához szükségesek. A megszálló hatalom jogosult intézkedéseket és általános szabályokat foganatosítani a megszállt területen, valamint integrálhatja a megszállt területeken lévő számítógépes hálózatokat saját rendszereibe. Ennek keretén belül joga van a hálózatok lefoglalására.

Az utolsó, hetedik fejezet a semleges államokkal foglalkozik. A hadviselő feleknek tilos a semleges államok informatikai rendszereit megtámadni, illetve a kibertámadásokhoz a semleges államok területét vagy számítógépes hálózatait felhasználni.

A STUXNET [7, 8, 10, 11, 13, 14, 15]

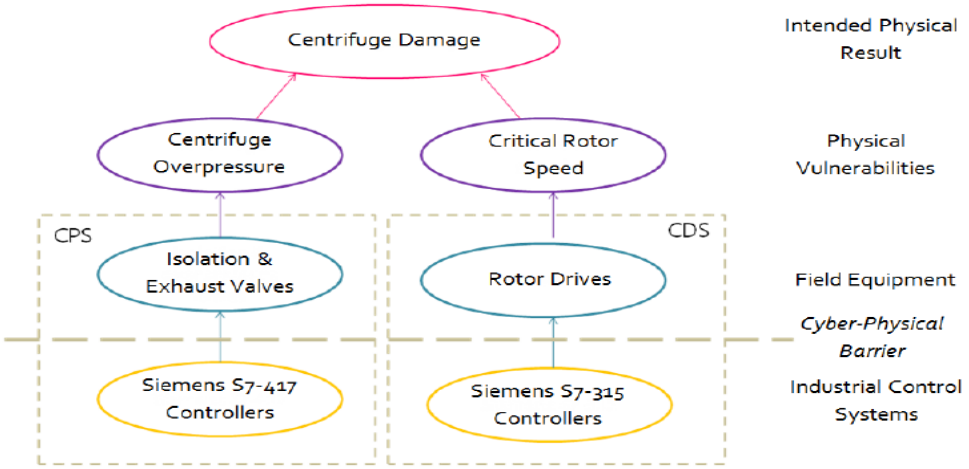
A Stuxnet egy olyan káros szoftver, amelyet célzottan ipari vezérlőrendszerek megfertőzésére, manipulálására és rombolására fejlesztettek ki. Ezt tekinthetjük az első ismertté vált kiberfegyvernek. Bevetésére az „Operation Olympic Games" fedőnevű, titkos művelet keretében történt, amelynek célja Irán atomprogramjának lassítása volt, meghibásodások előidézése útján. A kifinomultabb, első változatot elsőként 2007. november 15-én töltötte fel egy ismeretlen személy a Virustotal-ra, majd egy virulensebb változata elszabadult és elkezdte a terjedést.

Irán atomprogramja az ötvenes években kezdődött. A 79-es forradalmat követően azonban az megrekedt. Első atomerőművét 2011 szeptemberében adták át Bushehr-ben. Egyik urándúsító üzemét Natanz-tól mintegy 32 km-re észak-északnyugati irányban találhatjuk meg a 7. főközlekedési út és a 665-ös út kereszteződésénél (Ész 33º43'24,43" Kh 51º43'37,55"). A kivitelezés során a telep nagy része a föld alá került, nyilván az esetleges légitámadások elleni védekezés jegyében. Az üzem létezését csak 2003-ban ismerték el az irániak. 2009-re 5000 IR-1 centrifuga működött az üzemben. Bár Irán folyamatosan állítja, hogy atomprogramja békés célú, az ENSZ-BT 2006-tól kezdődően 8 határozatot hozott Irán ellen, a dúsítási tevékenység felfüggesztése tárgyában. A P5+1 országok és Irán külügyminisztereinek 2013 novemberében Genfben folytatott tárgyalása eredményeként Irán 6 hónapra visszafogja atomprogramját és átfogó vizsgálatot tesz lehetővé nukleáris létesítményeiben a Nemzetközi Atomenergia Ügynökségnek.

A Stuxnet az elemzések szerint a Siemens Simatic S7 PLC családjába tartozó S7-300 (315) és S7-400 (417) eszközök működésébe avatkozott be olyan feltételek mellett, amiből kiderül, hogy azt valóban az Iránban működtetett urándúsító üzem gyártási folyamatának lassítására fejlesztették ki.

1. ábra. A Siemens Simatic S7 termékcsalád
(http://www.plcdev.com/book/export/html/373)

Erre mutatnak az adatok, ugyanis Irán egy elavult technológiát alkalmazott, olyan speciális peremfeltételekkel, amit sehol nem alkalmaztak. A pakisztáni *Abdul Qadeer Khan* által megszerzett urándúsító centrifugák technológiai leírásai váltak a pakisztáni atomfegyver előállításának alapjává. Ezek alapján kidolgozott P-1 jelű centrifugák eljutottak Iránba is. A megbízhatatlannak jellemzett iráni változat az IR-1 nevet kapta és mintegy 8000 állt rendelkezésre Natanzban 2009-ben. A gyártási technológia részletes ismertetése helyett azt emelném ki, hogy a technológiai ismeretbéli hiányokat saját megoldásokkal egészítették ki az iráni mérnökök, ezzel azt egyedülálló technikai jellemzőkkel ruházva fel. Ez utóbbi a bizonyíték a támadás céljára. Megjegyzendő, hogy bár a Stuxnet szinte minden Windows platformot képes volt megfertőzni, azonban csak az iráni Natanzban fejtette ki a hatását. A Stuxnet féreg fizikai kárt képes okozni az iráni urándúsító berendezésekben. A károkozás az UF_6 molekulákat feldolgozó centrifugarendszer szelepeinek vezérlését zavarta meg a kalibrációs adatok megváltoztatásával, majd későbbi verziója a centrifugák sebességének vezérlését vette át, az urándúsítási folyamat akadályozása céljából. Mindkettő megoldás egyaránt rongálta a centrifugákat. Az alábbi ábrán látható, hogy a kétféle változat hogyan fejtette ki a hatását.



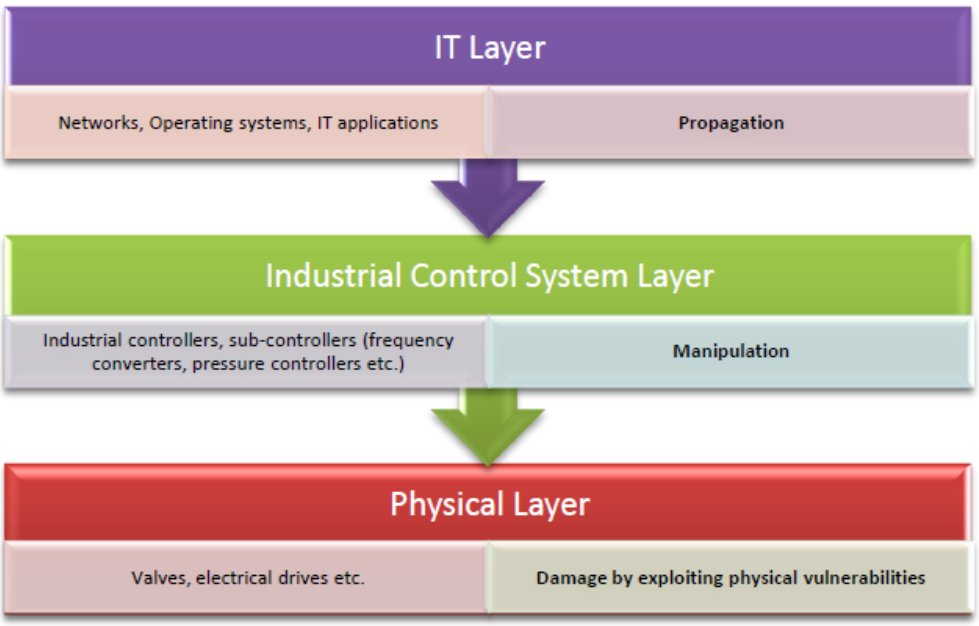
2. ábra. A két fő Stuxnet változat hatásmechanizmusa[1]

1CPS: Cascade Protection System, iráni fejlesztés, a túlnyomás elkerülésére. CDS: Centrifuge Drive System, a centrifuga motorvezérlő rendszere.

Az első kifinomultabb változat (Stuxnet 0.500) többek között lopott digitális tanúsítványokat alkalmazott, adatot gyűjtött a fertőzött rendszer üzemi paramétereiről, rögzítette a normál üzem adatait majd azokat játszotta vissza a kezelők megnyugtatása érdekében, miközben az urándúsító centrifugák nyomása a kritikus tartományba emelkedhetett. A malware hét szakaszból álló ciklusában négy szolgál rombolásra, három előkészítésre és a normál üzemre visszaállásra.

A második, némiképp agresszívabb változat (Stuxnet 1.x) szintén alkalmazott ellopott digitális tanúsítványokat, a rotorok sebességét változtatta meg az üzemi tartományon kívülre, így a centrifugák korai meghibásodását idézte elő. A káros tevékenységében öt szakaszt váltogat különböző időtartammal pl. 1410 Hz-re gyorsítja a centrifugákat, majd „rátapos a fékre" és 2 Hz-re csökkenti a sebességet. Ez a mechanikus megterhelés rövidtávon károsítja a centrifugákat, de a lassú szakasz az addig szétválasztott molekulák összekeveredését is eredményezi, így a gyártás hatásfoka ezáltal is degradálódik. Az egyes romboló szakaszok után a vezérlés visszaáll névleges frekvenciára. A cél a centrifuga fokozatos, észrevétlen tönkretétele és a dúsítási folyamat megzavarása. Ez utóbbi kockázatosabb formája a támadásnak, könnyebben lelepleződhet a Stuxnet, ugyanis a sebesség változtatása nem része a gyártási folyamatnak, a centrifugák zajának változását vélhetően füllel is lehet észlelni.

A fertőzés és a hatás kiváltása az alábbi ábrán látható módon 3 rétegen keresztül valósulhatott csak meg. Az 1. réteg az IT réteg, amelyen keresztül a folyamatba a káros kód bejuttatása megtörtént (windows, wincc). A 2. réteg a folyamatirányító rendszer és alrendszerei, amelyek a beavatkozásért felelősek. A Stuxnet ebben a rétegben módosította a működést. A 3. réteg maga gyártási folyamat fizikai környezete, azok a folyamatirányító rendszer által vezérelhető elemek, amelyek befolyásolása a szabályozási láncba való beavatkozást jelenti.



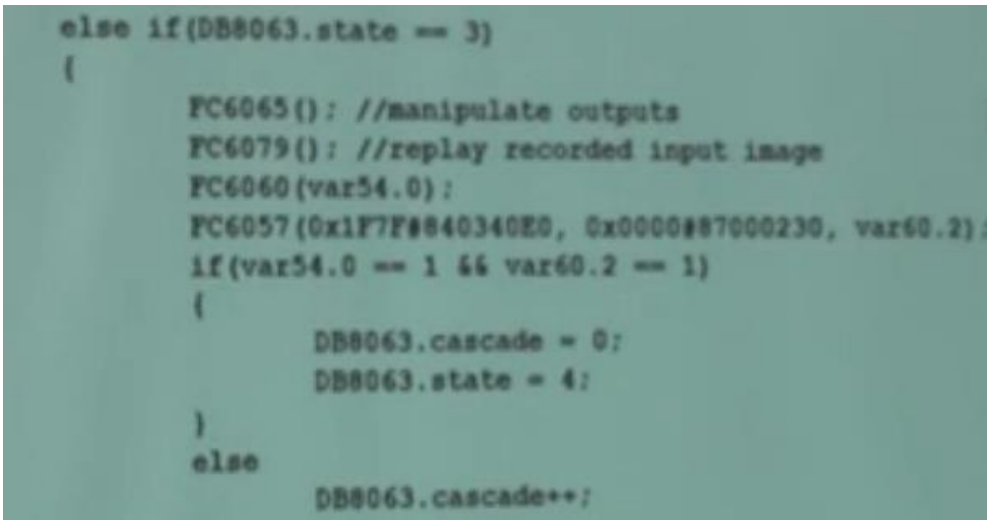
3. ábra. A Stuxnet hatásmechanizmusa

Érdemes a támadást vizsgálni az időtartományban is. A legelső változat (symantec: Stuxnet 0.500) 2005. november 3. – 2009. július 4. között, míg az azt követő (symantec: Stuxnet 1.001, Stuxnet 1.100, Stuxnet 1.101) 2009. június 22. – 2012. június 24. között működött. Ez azt jelenti, hogy a Stuxnet többlépcsős fejlődésen ment keresztül.

A vezérlőszerverekről annyit lehetett megtudni, hogy az első változat 4 vezérlőszerverrel működött négy ország területén (Egyesült Államok, Franciaország, Kanada, Thaiföld). Ezek a szerverek a fertőzés kezdeti szakaszában, még az IT rétegben voltak képesek kommunikálni a

fertőzött géppel. Magát a fertőzést egy izolált rendszerbe kellett bejuttatni, amit egy közbenső adathordozó fertőzésével valósítottak meg. Egy vélhetően szerződéses mérnöknek aki a fertőzött Step 7 projekt fájlokhoz (.s7p vagy .zip) hozzáfért és jogosult volt az izolált rendszerhez hozzáférni lehetett az összekötőkapocs a pendrive-jával.

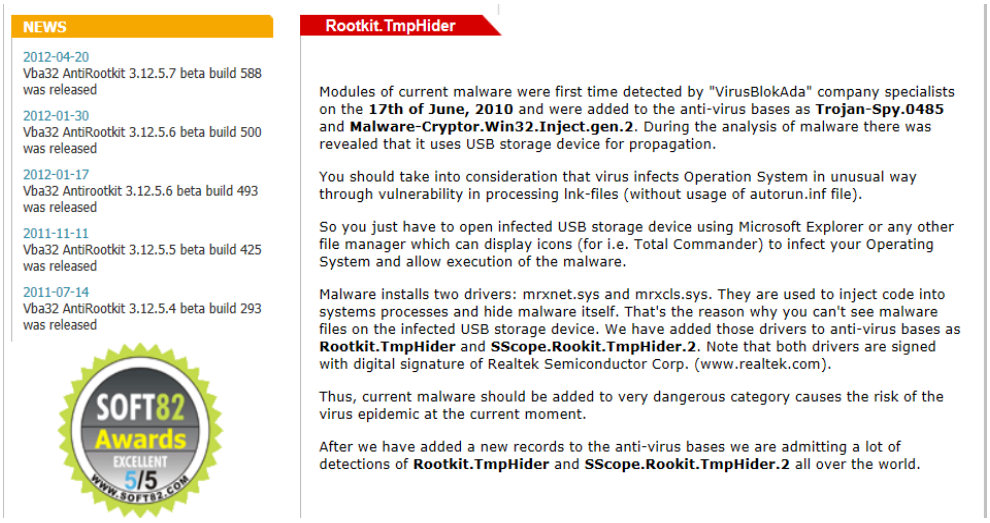
A Stuxnet kivizsgálásáról a legrészletesebb beszámolót a Symantec tette közzé. Konkrét fertőzéssel kapcsolatos adat, kód, (mélyelemzést Langner tett közzé, de nem ismert milyen forrásból jutott hozzá) nem állt a rendelkezésemre a cikk írása során, de annyi bizonyos, hogy a Stuxnet 2010-ig, tehát évekig gyakorlatilag zavartalanul működhetett. Az alábbi ábra Langner elemzéséből származik, a pszeudokód-részlet a többek között a korábban rögzített adatok visszajátszását mutatja.



4. ábra. Stuxnet visszafejtett és kommentezett kódrészlete
(Langner prezentáció)

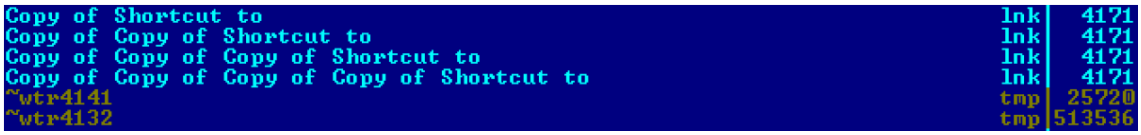
Az összesen 4 -féle változat többféle fertőzési vektorral rendelkezik, de az összes változatban közös, hogy Siemens Step 7 projekt fájlokat fertőz, USB- keresztül érkezik a fertőzés (bár itt háromféle változat létezett).

2010. június 17-én a fehérorosz VirusBlokAda antivírus szakértője Sergey Ulasen azonosította a Stuxnet 1.1000 változatát, akkor még más néven. Az első publikáció az alábbi ábrán látható.



5. ábra. Az első azonosítás
http://anti-virus.by/en/tempo.shtml

Az alábbi ábrán látható a CVE-2010-2568 sérülékenység kihasználásával fertőző pendrive tartalmának listája Far Manager-el. A két fertőzést tartalmazó fájl a VirusBlokAda munkatársaitól két elnevezést kapott, a Trojan-Spy.0485 és a Malware-Cryptor.Win32.Inject.gen.2. A tmp kiterjesztésű fájlok futtatható kódot tartalmaznak. A pendrive tartalmának explorerrel történő listázása elegendő volt a fertőzésre.



6. ábra. A Stuxnet 1.100 fertőzött pendrive tartalma

A kritikus infrastruktúra elemek kitettsége nem változott jelentősen az elmúlt években sem. A Stuxnet csak az első az azóta ismertté vált többi között, így ennek tükrében nagyobb hangsúlyt kell fektetni a kibervédelemre.

A STUXNET A TALLINI KÉZIKÖNYV TÜKRÉBEN

A támadó az Egyesült Államok és valószínűleg Izrael [8]. A *Támadó pontos kilétét meg kell állapítani* annak érdekében, hogy az arányos ellenlépés megtehető lehessen. Ez sok esetben komoly nehézségekbe ütközik. A jelenlegi meghatározáshoz az segített hozzá, hogy Cartwright nyugalmazott tábornok kiszivárogtatta [8]. A Stuxnet vezérlő és kommunikációs szervereinek vizsgálata (4 ország területén) nem tette volna lehetővé a támadó kilétének megállapítását.

A Kézikönyv alapszabálya szerint tehát *arányos ellenintézkedés* szóba jöhet.

A Stuxnet féreg véleményem szerint kritikus infrastruktúra támadását hajtotta végre. A célpont a Natanz (Irán) közelében található üzem, melyben mintegy több ezer centrifugát alkalmaztak urándúsításra. Figyelembe véve, hogy a UF_6 (urán-hexafluorid) erősen mérgező, agresszív anyag, emellett radioaktív is, ezért egy üzemi baleset előidézése személyi sérüléssel, esetleg emberi áldozatokkal járhat, ezért a *fegyveres támadás besorolás megfontolandó*.

Nem tudjuk jelenleg eldönteni, hogy összemérhető-e egy fegyveres támadással a Stuxnet, mert nem tudjuk, hogy valójában okozott-e üzemi balesetet, vagy „csak” meghibásodás történt, ami javítható volt. Amennyiben történt rombolás, áldozatok voltak, akkor azt erő alkalmazásának kell tekinteni, ugyanis a hatása felért a fegyveres támadás hatásával.

ÖSSZEGZÉS, KÖVETKEZTETÉS

A Tallinni Kézikönyv tisztázza a kiberhírszerzés, kiberhadviselés, nemzetközi jogi alapjait. Az elkészült munka alapja lehet Magyarország védelmi-, nemzeti biztonsági-, kiberbiztonsági stratégiáinak megújításának, a magyar jogalkotás kihasználhatja a Kézikönyv által összefoglaltakat annak érdekében, hogy a kiberműveletek jogi hátterét megteremtse, kiberhadviselés terén a nemzetközi hadijogi hátteret a későbbiekben átemelhesse.

A Tallinni Kézikönyv nem ad segítséget a kibertérben a területi hatály (földrajzi terület) fogalmára. A nemzetközi jog alapján minden ország felelős a területéről egy másik ország érdekeltsége ellen állami, vagy nem állami szereplő által indított támadásért. Kérdéses azonban, hogy felelőssé tehető-e egy ország azért, ha egy, a területén működő kliens gépről juttatnak be károkozó számítógépes vírust egy másik ország létfontosságú elektronikus információs rendszerébe. Ezen túlmenően a kiberhadviselésben nem tisztázott az állami és a nem állami szereplők helyzete sem, mert a kézikönyv is leegyszerűsíti a kérdést az állam területe feletti felelősségére.

A Stuxnet féreg támadás álláspontom szerint sérti a megtámadott szuverenitását (rules 1.4.), ezért arra a Kézikönyv szerint arányos ellenintézkedést (rules 13. 14.) tehet, de javasolt az

ENSZ BT összehívása. Mindazonáltal az ENSZ szankciókkal sújtott Irán ezt nyilván nem alkalmazhatta.

Fontos lenne a magyar jogalkotásnak a kiberműveletek jogi hátterét megteremteni, melynek első lépéseként a téma széleskörű konzultációja szükséges. Elsősorban meg kell határozni a Magyar Honvédség a kiberműveleti tevékenységének alapelveit [9], de ugyanilyen sürgető a többi, kiberműveletek terén illetékes területet meghatározni, valamint az alapelveket lefektetni. További kutatást igényel a kibertámadó azonosítási módszereinek kutatása és fejlesztése. Nem utolsósorban szükséges a kibertámadó-képességek kialakítása az új jogi keretek mentén.

Kiemelést érdemel, hogy a kibervédelmi képességek megerősítése még ennél is sürgetőbb, különös tekintettel az új törvényi keretek közötti lehetőségekre. Az elkövetkező évek számos kiberbiztonsági feladata között a kibervédelmi együttműködésekben rejlő szinergiák kiaknázása lehet a megoldás a hatékonyabb és kevésbé kitett kibervédelmi menedzsment kialakítására.

Felhasznált irodalom

[1] Konrad Zuse Internet Archive (letöltve: 2013.07.07.) http://zuse.zib.de/

[2] Lőcs Gyula: fejezetek az informatika történetéből *http://web.itf.njszt.hu/wp-content/uploads/2012/11/Locs_inftort11-15.pdf* (letöltve: 2013.07.07.)

[3] Dara Kerr: Mobile malware grows by 614 percent in last year http://news.cnet.com/8301-1009_3-57591042-83/mobile-malware-grows-by-614-percent-in-last-year/ (letöltve: 2013.07.07.)

[4] Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger, James Ball: GCHQ intercepted foreign politicians' communications at G20 summits http://www.guardian.co.uk/uk/2013/jun/16/gchq-intercepted-communications-g20-summits (letöltve: 2013.07.15.)

[5] The Tallinn Manual *http://www.ccdcoe.org/249.html* (letöltve: 2013. 06. 12.)

[6] mSpy honlap http://www.mspy.com/features.html?gclid=CMfIzPbcnLgCFcyR3god4ycAHA (letöltve: 2013.07.07.)

[7] W32.Stuxnet Dossier http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (letöltve:2013.07.15.)

[8] David E. Sanger: Obama Order Sped Up Wave of Cyberattacks Against Iran The New York Times 2012.06.01. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1& (letöltve:2013.07.15.)

[9] Kassai Károly: Kiberveszély és a Magyar Honvédség. http://hadmernok.hu/2012_4_kassai.pdf (letöltve:2013.07.15.)

[10] Ralph Langner: Egy XXI. század kibernetikai fegyvere - a Stuxnet megfejtése http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (letöltve:2013.07.15.)

[11] Ralph Langner: To-kill-a-centrifuge.pdf
http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
(Letöltve:2013.12.21.)

[12] ENISA: Can we learn from SCADA security incidents?
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents/at_download/fullReport (Letöltve:2013.12.30.)

[13] Ralph Langner: Stuxnet deep dive (prezentáció)
http://www.digitalbond.com/blog/2012/01/31/langners-stuxnet-deep-dive-s4-video/
(Letöltve:2013.12.30.)

[14] Cserháti András: A STUXNET VÍRUS ÉS AZ IRÁNI ATOMPROGRAM
Fizikai Szemle 2011/5. 150.o.
http://wwwold.kfki.hu/fszemle/fsz1105/cserhati1105.html (Letöltve:2013.12.30.)

[15] Oleg Kupreev, Sergey Ulasen: Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.gen.2 Review
http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf (Letöltve:2013.12.30.)