*Brányi Bence**

Szemelvények a kiberhadviselés jelenéből III. rész

Az informatika uralta haderők sebezhetőségének érzékeltetése öt példán keresztül

Iráni nukleáris létesítmények megtámadása (Stuxnet)

Technikai szempontból a modern Izrael állam megalapítására (a Földközi-tenger keleti partján) igen kedvezőtlen földrajzi környezetben került sor – egy elsivatagosodott, csekély természeti erőforrásokkal rendelkező vidéken. A palesztinok által is maguknak követelt területen a fő problémát az jelenti, hogy Izrael egyetlen jelentős szövetségese az Amerikai Egyesült Államok. A környező arab országok, köztük Szaúd-Arábia, Egyiptom és Irán a zsidó állam elpusztítását annak létrejötte óta tervezik; Izrael ezért megalapítása óta számos háborút vívott a fennmaradásáért. Ezek közé tartozott az 1947–49-es függetlenségi háború, az 1956-os szuezi válság, az 1967-es hatnapos háború, az 1973-as jom kippuri háború és a 2008–2009-es gázai háború.

Izrael a jelentős külföldi (zsidó közösségek általi) adományoknak és a nagy mennyiségű amerikai hadianyagnak köszönhetően eddig minden háborúból győztesen került ki, de a hagyományos hadviselés mellett, már a hidegháborúban megjelent egy új típusú fenyegetés Irán nukleáris programja képében. Izrael korábban büntetlenül támadhatta a környező országokat, ha viszont Irán nukleáris fegyverekhez jutna, a zsidó állam valószínűleg nem merne megkockáztatni egy támadást (a minimális távolság miatt az atomtöltetek célba juttatására szolgáló interkontinentális ballisztikus rakétákra ebben az esetben nincs szükség).

Irán nukleáris programja már 1957-ben elindult, majd 1967-ben az amerikaiak 5,545 kg dúsított uránt és 0,112 kg plutóniumot adtak át egy kísérleti reaktor beindításához. A munkálatok lassan haladtak, és amikor 1979-ben az iszlamista erők megdöntötték az Amerika-barát sah hatalmát, az ország nemzetközi embargó alá került, amelynek részeként a busheri atomerőművet építő Siemens AG is kivonult.

Irán ennek ellenére folytatta a nukleáris programot, külföldi államok, köztük Niger, majd a Szovjetunió és Kína segítségére támaszkodva. Izraeli politikusok az iráni nukleáris programot az országot fenyegető legnagyobb veszélyként kezelték, és mindent megtettek annak lassítására. Amerikai nyomásra Kína visszavonta ajánlatát egy urándúsító létesítmény felépítésére és időlegesen sikerült Iránt tárgyalóasztalhoz ültetni, lehetővé téve az IAEA (Nemzetközi Atomenergia-ügynökség) munkatársainak, hogy megvizsgálják az iráni létesítményeket.

A sorozatos időhúzást megelégelve, Irán 2004-ben feltörte a Natanz városában található, leállított urándúsító egység lepecsételt bejáratait, és újraindította a centrifugákat. Irán (bár folyamatosan hangoztatta, hogy nukleáris programja békés célokat szolgál) elsődleges célja nyilvánvalóan a nukleáris fegyverekhez szükséges tisztaságú hasadóanyag létrehozása.

Izrael számára katasztrofális eredménnyel járna, ha bármelyik ellenséges arab ország atomfegyverre tenne szert, ezért mindent megtett ennek megakadályozása érdekében. 1981-ben az izraeli légierő elpusztította Irak (francia segítséggel épített), kifejezetten polgári célú atomerőművét (Operation Opera), 2007-ben a légierő csapást mért Szíria feltételezett nukleáris létesítményére (Operation Orchard), 2010 és 2011 között pedig legkevesebb 5 iráni atomtudóst gyilkoltak meg az izraeli Moszad ügynökei.

Az irániak azonban tanultak a támadásokból. Megerősítették a tudósok védelmét, a zsidó ügynököket elfogták, nukleáris létesítményeiket pedig városok közelébe, a föld alá telepítették és erős légvédelemmel látták el, gyakorlatilag lehetetlenné téve egy hatásos (civil áldozatok nélküli) támadást. Mindezek ellenére, 2010-ben a Stuxnet nevű számítógépes program megsemmisítette az urándúsításhoz kulcsfontosságú natanzi egység urán-centrifugáinak kb. 20%-át.

A Stuxnet nevű számítógépes férget (a számítógépes vírushoz hasonló, de önállóan is működő programot) valószínűleg amerikai segítséggel az izraeli 8200-as egység, az izraeli hírszerző ügynökség (Haman) egyik alegysége hozta létre, tesztelésére egyes információk szerint az izraeli Dimona városában elkülönített környezetet építettek ki. Ehhez nyilvánvalóan titkosszolgálati segítséget használtak, mert minden fontosabb információ birtokában voltak; többek között részletesen ismerték az egyedi centrifugát és gyártóit, a finn Vacon és az iráni Fararo Payo cégeket, valamint a centrifugák Simatic vezérlőrendszerét is.

10. ábra. Az izraeli 8200-as egység katonái munka közben

* ORCID: 0000-0001-6025-1547

DOI: 10.23713/HT.53.1.04

11. ábra. Mahmud Ahmadinezsád iráni elnök látogatása a natanzi urándúsítóban. A hivatalos elnöki fotó egyes információk szerint segíthette a támadókat, mert a kép alsó részén látható az erőmű centrifugáit irányító rendszer elosztása (a működő centrifugák zöld, a nem működők szürke pontként)

A féreg már rövid idővel elkészültét követően megkezdte a fertőzést. Az internet nélküli, fizikailag leválasztott iráni létesítménybe fertőzött USB-tárolón (pendrive-on) keresztül jutott be. A Stuxnet a világ valószínűleg addigi legszofisztikáltabb férge, amelyet kifejezetten egy rendkívül szűk célpont támadására fejlesztettek ki. Működése három jól elkülöníthető lépésből állt. Először a Windows operációs rendszer több hibáját, köztük a .LNK sebezhetőségét (CVE-2010-2568) kihasználva jutott be, majd további kiskapukon keresztül terjedt tovább. A Stuxnet kb. 100 000 számítógépet fertőzött meg, ezek közel felét Iránban.

Amennyiben a vírus sikeresen bejutott egy számítógépbe, megkezdődött a második szint, a célpont azonosítása. A Stuxnet a Siemens ipari felügyeleti szoftverére (Simatic WinCC-re) utaló jeleket keresett (a korábbi változatban az S7-417-es, később S7-315-ös PLC-t). Amennyiben talált ilyet, folytatta a kutatást a PLC (speciális programnyelvet használó célszámítógép) rendszerében, egyedi, kifejezetten az IR-1-es (Iran 1) urándúsító-centrifugákra jellemző programsorokat keresve. Amennyiben a második keresés is sikeres volt, módosította a programot (a PLC-k a Stuxnet támadása előtt minimális védelemmel rendelkeztek, mivel a vírusok szinte kizárólag egyéni felhasználókat és céges, illetve állami adatbankokat vettek célba).

A PLC feladata ebben az esetben a centrifugák sebességének szabályozása volt, amibe a féreg kétféleképpen avatkozott be: a dokumentált adatokat átírta, ezért a kezelőknek nem tűnt fel a változás, másrészt időről időre módosította a centrifugák sebességét.

A Stuxnet három fő sorozatban készült első változatát 2009 júniusára datálták, de később kiderült, hogy már 2007-ben bevetették. 2010-es lebukásában az is szerepet játszott, hogy (valószínűleg a döntéshozók türelmetlensége miatt) a pusztítás felgyorsítása érdekében módosították a programot. A frissített verzió hibájából azonban a féreg – tévedésből – egy mérnök laptopját is megfertőzte, majd miután a férfi otthonában rácsatlakozott az internetre, ezen keresztül a Stuxnet tovább terjedt (Irán mellett indonéziai, indiai, azerbajdzsáni, pakisztáni, sőt, amerikai számítógépeken is megjelent, lehetővé téve az azonosítását).

A Stuxnet 2009-es, 0.5-ös változata a következőképpen működött: 30 napig a centrifuga kifogástalanul üzemelt, majd a program lezárta a kiengedő szelepeket, ezért a beérkező gáz (urán-hexafluorid) nyomása növekedni kezdett. Ezt követen a féreg várt két órát, vagy ameddig a nyomás a megengedett érték ötszörösére nőtt. Ekkora nyomásnál a gáz lecsapódott, és rátapadt a centrifugalapátokra, amelyek ettől megbillentek és nekicsapódtak a centrifuga falának, kisebb sérüléseket okozva, hosszabb távon kárt téve a centrifugában és tönkretéve a dúsítási folyamatot. Végül a program módosította a naplózási adatokat, elfedve a tevékenységét, majd a folyamat újraindult.

2010-ben megjelent egy újabb változat, amelyben a centrifugákat a program 15 percre a másodpercenként 1064 fordulatú üzemi sebességről 1410-re gyorsította, majd visszalassult és 27 napon keresztül hiba nélkül üzemelt. Ezt követően 50 percen keresztül lényegesen lassabban, másodpercenként 600 fordulattal üzemelt, mielőtt újraindult volna a folyamat. A szűk sebességtartományban, állandó sebességre tervezett alumínium turbinalapátok az erős fékezés és gyorsítás hatására kitágultak és deformálódtak, szó szerint széthajtva a turbinákat, amelyek élettartama drasztikusan lecsökkent. Nem sokkal később a hajtóművek leégtek.

A támadás eredményeit a nagyközönség máig nem ismerhette meg, de néhány közvetett információ elérhető. 2009-ben Iránban egy komoly nukleáris baleset következett be, aminek hatására az iráni atomenergiáért felelős szervezet vezetője lemondott, a natanzi urándúsító komplexum pedig leállt.

Az IAEA egyik akkori vezetője, Olli Heinonen szerint a támadás után, a 2009 novemberéig telepített kb. 8700 centrifugából 2009–2010 során egy-kétezret le kellett cserélni. A legnagyobb veszteség maga a leállítás volt: az iráni atomprogram 1-2 évvel távolabb került céljától, mivel a natanzi létesítmény gépparkjának fokozatos cseréje és a hálózatnak a Stuxnet-től való megtisztítása óriási munkát igényelt. (A Stuxnet felfedezését követően tovább folytatódtak az iráni nukleáris tudósok elleni támadások).

A Stuxnettel kapcsolatban hivatalosan sem Izrael, sem az Amerikai Egyesült Államok nem ismerte el érintettségét, de érdemes megjegyezni, hogy a féreg a támadásokról rendszeresen jelentéseket küldött egy-egy maláj és dán szerverre (mypremierfutbol.com, todaysfutbom.com). A megszerzett információ sorsa ismeretlen. A Stuxnet féreg határozott célja az urándúsító környezetkímélő módon történő tönkretétele volt, azonban az ehhez hasonló, fejlett vírusokkal rendkívüli károkat lehet okozni egy üzemelő nukleáris létesítményben.

A Stuxnet után 2011-ben a Budapesti Műszaki Egyetem Híradástechnikai Tanszékén található CrySyS Adat- és Rendszerbiztonság Laboratórium fedezte fel az eltérő feladatkörű, de rendkívül hasonló felépítésű Duqu kártevőt. Ezt követően 2012-ben a hasonló Flame kártevőt, illetve a 2017 decemberében észlelt Triton-t szintén összekapcsolták a Stuxnet-tel.

Drónelfogás (Irán)

A kiberhadviselés célja általában pénz- vagy információszerzés, az ilyen technikával végrehajtott fizikai támadás ritka (a Stuxnet a kivételek egyike), azonban mára realitássá vált a közvetlen harctéri támadás is (pl.: helymeghatározó- vagy barát-ellenség felismerő-rendszerek adatainak módosítása révén). A legveszélyeztetettebb célpontok a pilóta nélküli (elsősorban légi) járművek, röviden drónok. Ezek jelenleg használt modelljei a légi fölény kivívására még nem alkalmasak, azonban egyre több ország használja őket irreguláris csapatok (szervezett bűnözői csoportok, lázadók, terroristák) elleni harcra (lásd MQ–1-es „Predator” és MQ–9-es „Reaper”), illetve megfigyelésre (RQ–4-es „Global Hawk”).

Az ezek leváltására tervezett következő generációs drónok egyike a felderítő feladatkörű Lockheed Martin

12. ábra. A zsákmányolt RQ–170-es drón egy iráni tornateremben kiállítva

RQ–170-es „Sentinel”, egy lopakodó-karakterisztikájú, csupaszárny-kialakítású típus, amelyet valószínűleg 2007-ben vetettek be először Afganisztánban, azóta pedig Irak és Pakisztán felett is alkalmazták. Az amerikai légierő (USAF) és a Központi Hírszerző Ügynökség (CIA) által üzemeltetett RQ–170-est közel teljes titoktartás övezi, a jármű képességeiről nincs elérhető (megerősített) információ, ezért az egész világot meglepetésként érte, amikor 2011. december 4-én az iráni hadsereg működőképes állapotban zsákmányolt egy RQ–170-est, majd erről négy nappal később videófelvételt tett közzé.

A támadásról a következők ismertek. Az amerikaiak a drónt kémkedésre szánták; a jármű képességei a pilótás U–2-esét valószínűleg nem érik el, ugyanakkor lopakodó kialakítása lehetővé teszi számára az erős légvédelmű területek feletti működést. A típust 2009-ben Dél-Koreában tesztelték – a RQ–170-est az amerikaiak által ellenségnek tekintett országok, köztük Észak-Korea, Irán és Pakisztán feletti kémkedésre szánták. Hivatalosan a drónt a Közel-Keleten terrorista-sejtek felderítésére használták. A radarokkal és légvédelemmel gyakorlatilag nem rendelkező félkatonai csoportok ellen szükségtelennek tűnik a különleges típus használata és a rendkívüli titoktartás.

Az iráni incidenst követő napon, december 5-én amerikai katonai források (nem hivatalosan) elismerték egy RQ–170-es elvesztését, de a fedőtörténet szerint a gépet a Nemzetközi Biztonsági Közreműködő Erő (ISAF) üzemeltette. Ez nyilvánvalóan hazugság volt – további egy nappal később egy neve elhallgatását kérő amerikai tiszt azt állította, hogy a drónt a CIA iráni nukleáris létesítmények megfigyelésére használta, amikor elvesztették vele a kapcsolatot.

A felvételek bizonysága szerint a pilóta nélküli repülő gyakorlatilag épen került iráni kézbe, ezért valószínűleg vagy szoftverhiba miatt kényszerleszállást hajtott végre, vagy (az iráni állítás és egyes amerikai feltételezések szerint) az irániak kibertámadásának áldozatává vált.

Az egyik lehetséges magyarázat szerint a drónt egy (orosz) Kvant 1L222-es „Avtobaza” önjáró radarrendszerrel támadták, amely blokkolta mind a pilóta nélküli repülőgépet irányító földi állomás, mind az önálló repüléshez szükséges GPS jelét, majd egy adóállomás a globális helyzetmeghatározó rendszerhez hasonló jelet közvetített.[8]

A jelet a drón valódi (műholdas) GPS-jelként érzékelte, majd ezt használva visszatért és leszállt az általa védett amerikai előretolt bázisnak vélt, valójában iráni területen (egyes feltételezések szerint a gép földet éréskor három darabra szakadt, de ez az elfogás tényét nem befolyásolja).

Az incidens kapcsán számos kérdés merült fel, például amennyiben az irániak zavarták a GPS-jelet, az RQ–170-es drón miért (pl.: esetleg a szoftver hibás tervezése miatt) nem tért át a lényegesen pontatlanabb, de éppen ilyen helyzetre megtartott, független tehetetlenségi navigációs rendszer (INS) használatára, amikor a fejletlenebb MQ–1-es és MQ–9-es is az INS-t részesíti előnyben a GPS-szel szemben.

Az Amerikai Egyesült Államok kérvényezte a drón visszaszolgáltatását, amit az irániak megtagadtak. Bejelentették, hogy lemásolják az RQ–170-est, amit 2016-ban Saegheh néven mutattak be, de ezen típus vizsgálata már nem tartozik szorosan a témához.[9] A hasonló támadások száma az autonóm drónok további terjedésével valószínűleg nőni fog, és a helyzetet súlyosbítja, hogy az eltérített, pilóta nélküli drónok akár fegyvereket is szállíthatnak.

Tanulság

Ahogy látható, az utóbbi években a kiberhadviselés sosem látott mértékűvé vált. Gyakorlatilag az élet minden területén megjelent, egyaránt támadva állami intézményeket és cégeket, katonai beszállítókat és egészségügyi, valamint energetikai létesítményeket.

A Magyar Honvédség számára – korlátozott erőforrásai miatt – egy kifejezetten kibertámadásra tervezett ütőképes egység létrehozása nem reális és nem is lenne értelme, azonban a nagyon is valós fenyegetettség, a civil és kato-

nai adatok védelme, az esetleges támadások elhárítása a jelen és a közeljövő egyik legnagyobb kihívása. A fizikailag leválasztott belső hálózatok kora régen lejárt, és ahogy a példa is mutatja, nem is életképes. A hálózati alapú rendszerek hatékony védelme, ha nem is a leglátványosabb, de mindenképpen kiemelt feladat, amelyre az egyszerű felhasználótól a kormányig mindenkinek érdemes lehetőségéhez mérten költenie.

Források

Akhgar, Babak – Brewster, Ben (szerk.): Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Springer, 2016. DOI: 10.1007/978-3-319-38930-1;

Zetter, Kim: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Broadway Books, 2015;

Chawki, Mohamed et al.: Cybercrime, Digital Forensics and Jurisdiction. Springer, 2015. DOI: 10.1007/978-3-319-15150-2;

Bernik, Igor: Cybercrime and Cyber Warfare. Wiley-ISTE, 2014. DOI: 10.1002/9781118898604;

Kshetri, Nir: Cybercrime and Cybersecurity in the Global South. New York: Palgrave Macmillan, 2013. DOI: 10.1057/9781137021946

Gragido, Will et al: Blackhatonomics: An Inside Look at the Economics of Cybercrime. Syngress, 2012. DOI: 10.1016/c2011-0-05155-4;

Gragido, Will; Pirc, John: Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011. DOI: 10.1016/c2010-0-64928-5;

McQuade III, Samuel C. (szerk.): Encyclopedia of Cybercrime. Greenwood, 2008;

Interjú Anders Fogh-gal. PC World, 2018.01.15 https://pcworld.hu/pcwpro/meltdown-spectre-serulekenyseg-testkozelbol-interju-242545.html [2018.10.01.];

Lara Seligman: Final Software Load Plagues F-35 Test Jets. Aviation Week Network, 2016 07.11. http://aviationweek.com/defense/final-software-load-plagues-f-35-test-jets [2018.10.01.];

Sam Kim: How North Korea Built An Army of Hackers: Q&A. Bloomber Technology, 2017.10.17. https://www.bloomberg.com/news/articles/2017-10-17/how-north-korea-built-an-army-of-cyber-warriors-quicktake-q-a [2018.10.01.];

David E. Sanger, David D. Kirkpatrick, Nicole Perlroth: The World Once Laughed at North Korean Cyberpower. No More. New York Times, 2017.10.15. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html [2018.10.01.];

Paul Mozur, Choe Sang-Hun: North Korea's Rising Ambition Seen in Bid to Breach Global Banks. New York Times, 2017.03.25. https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html [2018.10.01.];

Janene Pieters: Russian servers linked to DDoS attack on Netherlands financial network. nltimes.nl, 2018.01.29. https://nltimes.nl/2018/01/29/russian-servers-linked-ddos-attack-netherlands-financial-network-report [2018.10.01.];

zerocool: DoS, és DDoS támadások (túlterheléses támadások). Ethical hecker tutorials, 2013.12.06. http://backtracktut.blogspot.hu/2013/12/dos-es-ddos-tamadasok-tulterheleses.html [2018.10.01.];

Dömös Zsuzsanna: Mit kellene megbocsátani Edward Snowdennek? Origo, 2016.09.15. http://www.origo.hu/techbazis/20160915-edward-snowden-nsa-lehallgatasi-botrany-kembotrany.html [2018.10.01.];

Bolcsó Dániel: Csatát vesztett az NSA, de a totális megfigyelésnek nincs vége. Index.hu, 2015.12.11. https://index.hu/tech/2015/12/11/nsa_freedom_act_megfigyeles_snowden/ [2018.10.01.];

NSA monitored calls of 35 world leaders after US official handed over contacts. The Guardian, 2013.10.24. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls [2018.10.01.];

Exclusive: NSA pays £100m in secret funding for GCHQ. The Guardian, 2013.08.01. https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [2018.10.01.];

NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 2013.06.06. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [2018.10.01.];

NSA collects millions of e-mail address books globally. The Washington Post, 2013.10.14. https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?utm_term=.c720a62d5abf [2018.10.01.];

Beismerték Merkel lehallgatását. Index.hu, 2013.10.30. https://index.hu/tech/2013/10/30/az_nsa_a_google-t_es_a_yahoo-t_is_figyelte/ [2018.04.16.];

Paul Mueller, Babak Yadegar: The Stuxnet Worm https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf [2018.10.01.];

Jim Finkle: Researchers say Stuxnet was deployed against Iran in 2007. Reuters, 2013.02.06 https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226 [2018.10.01.];

David Shepardson: Tesla driver in fatal ‚Autopilot' crash got numerous warnings. Reuters, 2017.06.19 https://www.reuters.com/article/us-tesla-crash/tesla-driver-in-fatal-autopilot-crash-got-numerous-warnings-u-s-government-idUSKBN19A2XC [2018.10.01.];

Loveday Morris, Ruth Eglash: The drone shot down by Israel was an Iranian copy of a U.S. craft, Israel says. The Washington Post, 2018.02.11 https://www.washingtonpost.com/world/israel-confirms-downed-jet-was-hit-by-syrian-antiaircraft-fire/2018/02/11/bd42a0b2-0f13-11e8-8ea1-c1d91fcec3fe_story.html?utm_term=.b9c1d24ea8ec [2018.10.01.].

Jegyzetek

8 Ez az angolul „GPS spoofing attack"-nak nevezett megoldás nem túlzottan bonyolult, 2013-ban a Texasi Egyetem mérnökhallgatói sikeresen eltérítették a White Rose jachtot, amely Monacóból indulva egészen Rodosz szigetéig hajózott, követve az ál-jeladó információit.

9 Érdekességként azonban megemlíthető, hogy 2018. február elején egy izraeli AH–64-es harci helikopter megsemmisített egy, a légterébe belépő, az RQ–170-eshez kísértetiesen hasonlító iráni drónt (valószínűleg a Saegheh egy példányát), majd 8 db izraeli F–16-os légicsapást mért több, Szíriában található iráni célpontra, köztük a drón irányító-központjára. A támadásban (több évtized után először) az izraeli légierő elvesztette egyik repülőgépét.

(Illusztrációk a szerző gyűjteményéből.)