HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Gyebrovszki Tamás
gyebrovszki.tamas@nbsz.gov.hu

FOLYAMATOS FENYEGETÉS A KIBERTÉRBEN

Absztrakt

A cikk a kibertérben folyamatosan fennálló fejlett fenyegetésekkel (Advanced Persistent Threat továbbiakban APT) foglalkozik. A számítógépes káros kódok történetének ismertetését követően néhány ismert APT támadást sorolok fel, majd definiálom az APT fogalmát. Végezetül kitekintést adok az APT-k elleni fellépés lehetőségeiről.

This article deals with Advanced Persistent Threat in Cyber Space. It summarizes the history of malicious softwares and some known as APT attack. The article gives a definition of APT. Finally it brings solutions on the field of countermeasure.

Kulcsszavak: *APT, kibertér, rosszindulatú kódok ~ APT, cyberspace, malware*

BEVEZETÉS

Neumann János (1903-1957) matematikus nevéhez kötődik a napjainkban használt számítógép architektúra alapötlete, a tárolt programú számítógépé. A német Konrad Zuse (1901-1995) által tervezett első számítógép, a Z1 [1], programozható volt ugyan, de a programot lyukszalagon tárolta és annak programfutás közbeni változtatására nem volt lehetőség. Az 1938-ban elkészült gépről sajnos csak néhány fénykép maradt fenn. A Neumann elv alapján épült első számítógép az EDVAC (Electronic Discrete Variable Automatic Calculator) volt [2].

1. ábra. Neumann János
http://njszt.hu/sites/default/files/imagecache/belyegkep/miujsag/john-neumann.jpg

Ez a gép az adatokat és a programot is a közös memóriában tárolta. Ez ragyogó ötlet, azonban olyan problémát is okozott, amely a mai napig növekvő mértékű kárt okoz. Norbert Wiener (1894-1964) amerikai matematikus, akit a kibernetika megteremtőjének tartanak [3], az önmagát reprodukáló kód gondolatát is megalkotta. Neumann Wiener gondolatát tovább vitte. Az önmagát reprodukáló géppel foglalkozó tanulmányában leírta, hogy: „Ha valamely rendszer képes önmagát reprodukálni, akkor szükségképpen tartalmaznia kell négy komponenst: egy realizáló alrendszert (amely adott leírásokat meg tud valósítani), az egész rendszer leírását (röviden kódját), egy a kódot megőrizni, lemásolni és továbbadni képes kódátadó alrendszert, végül pedig egy az önreprodukció folyamatát vezérlő alrendszert. Ilyen alrendszerek birtokában a rendszer alkalmas arra, hogy önmagát újraalkossa.” [4], [5]

A számítógépes kártevő programok kifejlődése a Neumann-elv következtében vált lehetővé. A processzor regiszterei, a számítógép műveleti tára felülírható, a futó programjaink jól működő kódrészletei felett az irányítás átvétele lehetséges, egyfajta módosulás történik, mást is fog végezni a program, nemcsak amire programoztuk. Hasonló módon, mint ahogy a biológiában a vírusfertőzés megtörténik. A fő probléma a kibertérben azonban az, hogy ellentétben az élőlényekkel, nincs az immunrendszerrel ekvivalens fejlett önvédelmi mechanizmus, csupán védekezési módszerek léteznek. A kiberbiztonság egyre bonyolultabb eljárásokat, eszközöket és több erőforrást igényel. Mit kellene tennünk?

A SZÁMÍTÓGÉPES KÁRTEVŐ PROGRAMOK TÖRTÉNETE

Neumann bár már 1948-ban publikált és előadást is tartott az önreprodukálás gépi megvalósításáról, elméleti munkássága ezen a téren csak halálát követően, 1966-ban került kiadásra [5]. Szintén ebben az évben Robert Morris olyan játékkörnyezet megalkotását kezdeményezte, melyek egymással „harcolva" felülírva megsemmisítik a másikat. A „harci programok" első példánya a Darwin nevet kapta, ebből alakult ki a Core War [13].

2. ábra. H. R. Giger: Virus Moribundus Ante Ops Systematicae

Az elméleti alapvetés, miszerint hogyan kell önmagát reprodukáló szerkezetet tervezni és készíteni, alapvetően egy matematikai probléma megoldása, amely majdnem harminc évvel megelőzte a korát, hiszen csak 1971-ben készült olyan kód (Creeper), amely ebbe a kategóriába tartozik, az első számítógépes vírusnak tartott kód [7]. Az önmagát reprodukáló gép azonban csak jóval később, a 3D nyomtatás segítségével jöhetett létre [6].

A számítógépes vírusok széleskörű elterjedése a nyolcvanas évekre tehető. Eleinte nem a rosszindulatú szándék vezérelte a programok íróit, de kevés idő kellett ahhoz, hogy kimondottan ártó szándékkal készüljenek vírusok.

A számítógépes vírus fogalma elvont, megfoghatatlan, nehéz elképzelni. A körülöttük tapasztalható titokzatosság számos művészt ihletett meg, pl. Hansruedi Giger 2000-ben készült szobra a 2. ábrán látható. A szobor megjeleníti a megjeleníthetetlent.

Annak érdekében, hogy jobban értsük a kártékony kódok jelenlegi fejlettségét szükséges azok fejlődését áttekinteni. Ennek érdekében az alábbiakban röviden összefoglalom a kártevő programok fejlődéstörténetét évtizedenkénti szakaszokra bontva [8], [13], [14].

Hetvenes évek – az ókor

A hetvenes években csupán néhány kísérleti példány jelent meg, amelyek nagygépes környezetben működtek. Az első önreprodukáló Creeper programot Bob Thomas írta 1971-ben a BBN Technologies-nél. A DEC PDP-10-en, TENEX operációs rendszeren futó vírust tartják az elsőnek. A vírus az ARPANET-en keresztül saját másolatait helyezte el a távoli gépeken, kárt nem okozott, csupán egy üzenetet jelenített meg.

Az 1974-ben készült Rabbit a fork bomb (nyulak) első ismert példája, amely a folyamatok sorozatos duplikálódása útján a támadott gép erőforrásait felemésztve az szolgáltatás kiesését, rendszerösszeomlást okoz.

John Walker UNIVAC gépre, assembly nyelven írt Prevade és Animal vírusa 1975-ben készült. Ez az első trójai program, kárt ugyan nem okozott, mert csupán minden elérhető

könyvtárba egy-egy másolatát helyezte el. Az Animal kérdésekkel traktálta a felhasználót és ezalatt a Prevade elvégezte a másolásokat.

Nyolcvanas évek – a középkor

A mikroszámítógépeket elsőként támadó vírus az Elk Cloner volt. Az Apple II számítógépen futó programot Richard Skentra írta 1982-ben. A vírus a rendszerindításhoz használt floppylemezen a boot szektorban helyezkedett el. Ez tekinthető az első széleskörűen elterjedt vírusnak.

Frederick Cohen, amerikai informatikus 1983-ban definiálta a számítógépes vírust. Eszerint: egy program, amely képes más programok megfertőzésére oly módon, hogy saját másolatával módosítja azokat.

1986-ban a Brain bootvírus megjelenésével kezdetét vette a Microsoft operációs rendszereket fertőző kártékony szoftverek töretlen fejlődése. A vírust két pakisztáni programozó készítette.

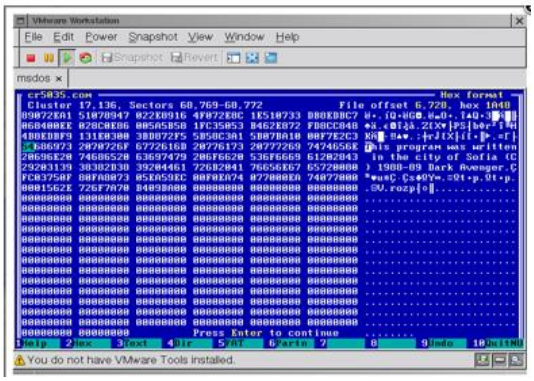
1987-ben jelent meg a Vienna, Lehigh, boot szektor vírusok: Yale, Stoned, Ping Pong. Az első önmagát rejtjelző fájlvírus a Cascade is ebben az évben jelent meg. 1987-ben készült a Jerusalem vírus, mely már 1988. május 13-án (péntek) és ezt követően péntekenként, ha az 13. napja az adott hónapnak, tönkretette az *.exe állományokat.

A Christmas Tree Exec az első levelező rendszer segítségével okozott tömeges rendszerleállást. A nem túl igényesre sikerült karaktergrafikát (3. ábra) tartalmazó üzenet lánclevélként terjedt tovább, elárasztva a postafiókokat, túlterhelést okozott a levelező kiszolgáló szervereknek, valamint jelentősen növelte a hálózati forgalmat.

3. ábra. Christmas Tree EXEC üzenet tartalma
http://securitywatch.pcmag.com/security/291931-malware-for-christmas

Az évtized utolsó éveiben egyre több és több vírus jelent meg. 1988-ban a CyberAIDS és számos változata jelent meg Apple ProDOS rendszerre. Megjelent az első Macintosh vírus a MacMag. A Score Macintosh vírus pedig komoly károkat is okozott. Az első internetes féregprogram is 1988-ban jelent meg a Robert Tappan Morris által írt Morris. A Morris DEC VAX és Sun gépeken BSD UNIX környezetben futott.

1989-ben jelent meg a Ghostball, mely többféle fertőzési módon terjedt. Egyaránt fertőzött *.exe, *com programokat és boot szektorokat is. Érzékeny felhasználói adatokat keresett és továbbított a fertőzött gépről.



4. ábra. A bolgár Dark Avangerben megtalálható szöveg
http://www.eset.hu/tamogatas/viruslabor/virusleirasok/dark_avenger-1800-c

Szintén 1989-ben készült el az első polimorf vírus, a Dark Avenger (4. ábra). Erre az évtizedre a gyors bővülés és a típusok megjelenése volt a jellemző.

Megjelentek a víruskereső módszerek és az első termékek. Az első antivírus szoftverfejlesztő céget, a német G DATA Software-t 1985-ben alapították. A számítógépes kártékony kódokkal, vírusokkal kapcsolatos fogalmak, definíciók is ebben az időszakban alakultak ki.

Kilencvenes évek – az újkor

A nyolcvanas évek tapasztalataiból származó tudást foglalta doktori értekezéssé Szegedi Imre, az Első magyar víruskönyv szerzője. Az akkor még minősített értekezés forráskód szintű elemzéseket is tartalmazott (pl. Jerusalem, Vienna, Dark Avanger).

A nyolcvanas évek végén megjelenő, mintázatalapú vírusvédelmi szoftverek kikerülésére a kilencvenes évek legelején már új módszereket kezdtek el alkalmazni a kártékony kódot fejlesztők. Ilyenek például a polimorf és a rejtjelzést alkalmazó vírusok. A DOS, majd a Windows operációs rendszereket támadó vírusok ebben az évtizedben nagyfokú fejlődésen mentek át. 1991-ben jelent meg az évtized legismertebb vírusa a Michelangelo, mely a Stoned variánsok közé tartozik. A bootszektor vírus masszív károkozása miatt vált ismertté. Michelangelo születésnapján a fertőzött gép összes adatát véletlen karakterekkel írta felül. Egyes becslések szerint tízezer esetben okozott adatvesztést.

A bootszektort fertőző Leandro and Kelly a legsikeresebben fertőző vírusok közé tartozik. A szlovák eredetű Onehalf polimorf vírus 1994-ben jelent meg. A romboló jellegű vírus minden rendszerindításkor két cilindert lekódol a merevlemez első partícióján, ha a merevlemez felével végzett, akkor jelzi azt üzenetével (5. ábra).

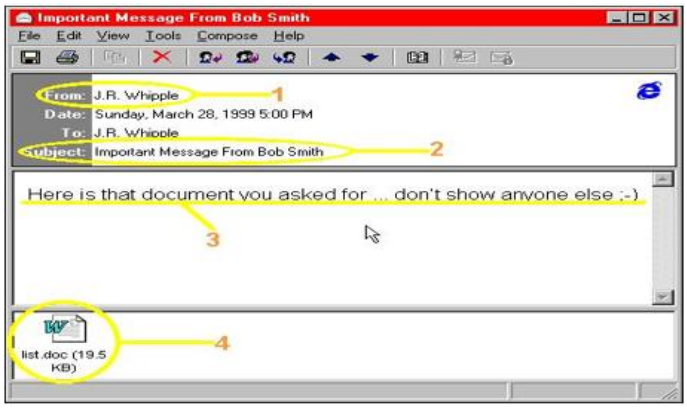
5. ábra. Már a merevlemez felét lekódolta a Onehalf
www.malware.wikia.com

A Concept az első makróvírus, 1995-ben jelent meg. A Microsoft Word programon keresztül terjedt. A Boza az első Windows 95 platformon futó vírus.

Az 1996-ban megjelent Ply kifinomult polimorf vírus, csak *.exe programokat fertőzött, azonban arra vigyázott, hogy az akkortájt ismert antivírus szoftvereket ne fertőzze meg.

A CIH vírus 1998-ban jelent meg. A fertőzési módszere lehetővé tette, hogy elrejtőzzön az antivírus szoftverek elől, mert a fertőzött fájlok méretét nem változtatta meg, azok állományaiba, az üres helyekre másolta be magát. A flash BIOS-t támadta, így okozva 250 millió dolláros kárt. A linken megtekinthető, milyen élmény lehetett elszenvedni a fertőzést (http://www.youtube.com/watch?v=RrnWFAx5vJg).

Ugyanabban az évben kezdődött a Moonlight Maze kibertámadás, amelyet az első APT támadásnak tartanak [15]. 1999-ben négy kártevőt érdemes említeni: a HAPPY99 férget, amelyik az első emailben terjedő vírus volt.



6. ábra. A Melissa fertőzött üzenete
http://www.jrwhipple.com/melissa.html

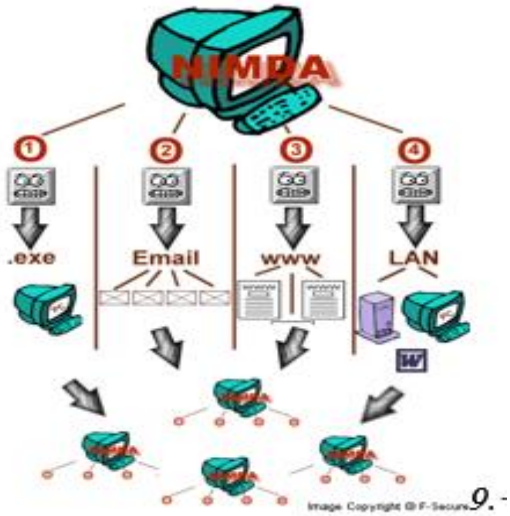
A Melissa makróvírust, mely Microsoft Word dokumentumfertőzéssel több mint 1 milliárd dollár kárt okozott. Az ExploreZip féreg hasonlóan agresszív pusztítást végzett: forráskód, valamint dokumentumfájlokat semmisített meg, míg a javascriptben megírt Kak az Outlook Express bizonyos sérülékenységét kihasználva emailekhez hozzáfűzve terjedt.

Kétezres évek – a legújabb kor

A kártékony szoftverek száma megtöbbszöröződött ebben az évtizedben. Emellett az állami szereplők (hírszerzés, elhárítás, fegyveres erők) felismerték, hogy számukra is kiaknázható eszköz jutott a birtokukba a globális kibertérben. A nem publikált sérülékenységek kihasználása útján hátsó kapuk nyithatók a rendszerekben. Több ország indította ebben az évtizedben a kiberműveleti képességeinek fejlesztését.

2000-ben az ILOVEYOU email féreg járványszerűen terjedt el világszerte. A Visual Basic Scriptben írt csatolmány (7. ábra) megnyitásával a script a Microsoft Outlook címlistája szereplő összes címzettnek továbbította a férget.

7. ábra. Az ILOVEYOU email féreg és Virtual Basic Script csatolmánya
http://2.bp.blogspot.com/-vD4Ub6pgfOM/UAP8yUfPzJI/AAAAAAAAAAc/L9obqByJDnQ/s1600/Iloveyou-virus-ver,J-1-99181-3.jpg



8. ábra. A Nimda terjedési módozatai
www.f-secure.com

Ugyanebben az évben megjelent az első gyermekeket célzó vírus a Pikachu. A futtatható állományt tartalmazó féreg, a pikachupokemon.exe csatolmány módosította az autoexec.bat állományt, melyben elhelyezett parancsok a windows és a windows\system könyvtárak törlését indította el a következő rendszerinduláskor.

2001-ben jelent meg az Anna Kournikova féreg. Hasonlóan működött az ILOVEYOU-hoz. Visual Basic Worm Generator-ral készítették. A Sadmind féreg a Sun Solaris és Windows NT/2000 operációs rendszerekben sérülékenységeket kihasználva volt képes bejutni a számítógépbe. A Deplhiben írt Sircam féreg emailen és közös hálózati meghajtókon keresztül terjedt. Károkozására példa, hogy pl. a teljes C:\ meghajtó tartalmát törölte, vagy épp teleírta a lemezt. Még 2001-ben jelent meg a CodeRed féreg, melynek egyik érdekessége az volt, hogy ha a támadott rendszer kínai nyelvre volt állítva, a féreg agresszívebben terjedt.

A Nimda vírus rendkívül gyors terjedését többféle terjedési mechanizmusa tette lehetővé (8. ábra). Kihasználta a CodeRed által létrehozott hátsó kapukat, emaileken-, fertőzött weblapokon, nyitott hálózati hozzáféréseken keresztül terjedt. 2001 végén és 2002-ben terjedt el a Klez. Az emailben fertőző féreg a Microsoft Windows, Explorer és Outlook sérülékenységeit kihasználva világszerte gyorsan elterjedt. 2003-ban a Simile metamorf vírus jelent meg. A mintegy 14000 soros assembly kódú malware kimondottan komplex, összezavart (obfuszkált) kódolást tartalmazott.

9. ábra. A Beast felülete
http://en.wikipedia.org/wiki/File:Beast_RAT_client.jpg

A Beast trójai program megjelenése is erre az évre tehető. A Remote Adminstration Tool (RAT) névvel is illetett program Windows 95 és XP operációs rendszereket fertőzött. A sikeres fertőzést követően a teljes irányítást képes volt átvenni a támadott gép felett, annak ellenére, hogy a gépet esetleg tűzfal védte. Ezt a reverse connection kapcsolódási módszerrel érte el. Széleskörű tevékenységei közé tartozott a webkamera bekapcsolása és a tárolt jelszavak megszerzése is (9. ábra).

2003-ban a Slammer féreg 30 perc alatt szinte az egész Interneten végigsöpört. A mindössze 376 bájtos malware a Microsoft SQL Server 2000 sérülékenységét kihasználva terjedt hihetetlen sebességgel. Még egy érdekesség jellemezte a Slammert és a CodeRedet is: ezek az első példányok az olyan káros kódokból, amelyek a megtámadott gép háttértárolóján nem hagytak nyomot, mert közvetlenül az operatív memóriában voltak csak megtalálhatók. Az antivírus szoftverek 2000 után kezdtek a memória átvizsgálásába, kártékony kódokat keresve. Szintén 2003-ban fedezték fel a Graybird trójait is, amelyik távoli parancsok futtatását tette lehetővé. Hasonlóképpen a török ProRAT trójai mely véletlenszerűen nyitott portokon keresztül kommunikált a támadóval. A Blaster féreg a DCOM RPC[1] puffertúlcsordulásos sérülékenységét kihasználva terjedt el és véletlenszerű IP címek felé szétküldve magát és SYN elárasztással támadta meg a windowsupdate.com-ot.

A Blasterhez hasonlóan terjedő Welchia (Nachi) féreg jóindulatú, a Blaster által is kihasznált sérülékenységet javító csomagokat töltött le és kiírtotta a Blastert. Ezután önmagával is végzett. A szintén ekkor megjelent Sobig, Swen és a Sober férgek email alapú támadásokat végeztek különféle módszerekkel, míg az Agobot féreg a botnetek alapfunkcióit[2] képes volt megvalósítani.

A Bagle féreg 2004-ben jelent meg. A tömeges levélszétküldési funkciója saját terjesztésére szolgált. A leveleket a már megfertőzött gépek (Bagle botnet ~ 150000-230000) küldték ki. Hasonló volt a MyDoom féreg, a csatolmányokban érkezett a fertőzés. Ez a féreg a leggyorsabban terjedő jelzőt kapta. A több változattal is rendelkező Netsky féreg emailbe csatolt, futtatható állományban érkezett, saját másolatait a helyi és a hálózaton elérhető könyvtárakba helyezte el. A Witty féreg új fejezetet nyitott a támadásokban. Az azonnali üzenetküldés sérülékenységét kihasználva, mintegy 12000 számítógépet fertőzött, meg csupán 45 perc alatt. A rosszindulatú kártevő a fájlrendszer lassú rombolásával okozott kárt. A Sasser féreg sérülékeny hálózati portot kihasználva terjedt. Sok rendszert le kellett állítani világszerte a féreg miatt.

10. ábra. A Caribe féreg Symbian operációs rendszeren
https://www.securelist.com/en/descriptions/old60663

1 A Distributed Computing Environment/Remote Procedure Call a Microsoft elosztott rendszerek szoftverkomponenseinek kommunikációs technológiája

2 Ez általában: a fertőzött gépen lévő „bot” frissítése, eltávolítása, parancsok és programok futtatása, portszkennelés, DDoS támadásban részvétel.

A Caribe féreg az első mobiltelefon operációs rendszert fertőző kártevő. A bluetooth-on keresztül terjedő féreg nem okozott kárt (10. ábra). A Nuclear RAT trójai program szerver és kliens gépeket is fertőzött. A fertőzött gép/rendszer felett átvette az uralmat. Még mindig 2004 terméke a Vundo trójai. A malware emailben, vagy fertőzött webhelyről fertőzött. Az alapvetően a hirdetések megjelenítésére készített malware, sokkal „több funkcióval" rendelkezett. A Bifrost trójai program távoli kódfuttatást tett lehetővé, míg, a Perlben írt Sanity az első webféreg a rendkívül gyors terjedéséről híresült el. A Google keresőszolgáltatását kihasználva a honlaprongáló 3 óra alatt mintegy 40000 honlapot fertőzött meg.

11. ábra. A Sanity féreg ezt az üzenetet jelentette meg a fertőzött honlapokon
http://www.securelist.com/en/blog?topic=199380270

A 2005-ben Farid Essebar[3] által megírt Zotob többek között pénzintézetek rendszereit fertőzte meg. A Zlob trójai program kódeknek[4], vagy kémprogram eltávolító programnak álcázva terjedt el. A Bandook Remote Administrator Tool a Beast-hez hasonlóan hátsó kaput nyitott a fertőzött számítógépen és rendszergazdai jogosultsággal érte el az erőforrásokat. Ebben az évben jelent meg az első MMS-ben terjedő féreg, a Commwarrior. A mobiltelefonos Symbian operációs rendszeren futó program bluetooth-on is terjedt. A javascriptben írt Samy a Myspace személyes oldalait fertőzte XSS[5] technikával. Szintén 2005 terméke lehet a Stuxnet [14]. A jelenleg az első bevetett kiberfegyvernek tartott APT kártevő roppant kifinomult eszközöket alkalmazott.

2006-ban jelent meg az első Mac OS X malware, mely csak a helyi hálózaton terjedt. A Blackworm (Nyxem) féreg fertőzött email csatolmányokon és nyílt hálózati erőforrásokon keresztül terjedt. A féreg a felhasználói fájlok felülírásával fejtette ki romboló hatását. A hacktivista üzeneteket megjelenítő Brontok vírus számos kellemetlen tevékenysége mellett egyszerű DOS[6] támadásokat is végrehajtott. Stration féreg fontos információnak tűnő email csatolmányban érkezett, a rendszervédelmi modulokat lekapcsolva terjedt tovább.

A Storm trójai 2007-ben söpört végig a világon. Az akár 50 millió fertőzött gépet tartalmazó Storm botnet fertőzött emailen keresztül terjedt. A botnet egyes gépei részt vettek az automatizált támadásokban, mint pl. spam-ek küldése, weblap támadása, felhasználói adatok gyűjtése. Ugyanebben az évben a Zeus trójai terjedése indult meg. Az adathalász és letöltések útján fertőző malware nagy botnetet létesített és felhasználók banki adatainak megszerzését végezte, billentyűleütések megfigyelésével.

A 2008-as Mocmex féreg digitális képkeretben érkezett. Önvédelmi modulja többek között kikapcsolta a vírusvédelmi szoftvereket, a tűzfalat, így nehezen lehetett észlelni. Cserélhető adathordozón terjedt. A Torpig trójait is 2008-ban észlelték, hasonló önvédelmi mechanizmusokkal rendelkezett. A felhasználók érzékeny adatait gyűjtő malware-t az addig ismertek legkifinomultabb bűnöző programjának titulálták. A Rustock.C változatot megelőzte a híre, a felfedezhetetlen rootkit[7] utáni hajsza majd egy évig tartott, mire 2008-ban felfedezték. A rejtve terjedő, polimorf malware, drivernek álcázva magát, hatékony önvédelmi modullal

3 Habár a marokkói-orosz állampolgárt letartóztatták, a malware további változatai jelentek meg
4 Kódoló-dekódoló szoftver
5 Cross site scripting: webes alkalmazások sérülékenységi típusa
6 Denial of Service: Szolgáltatás megtagadás
7 Adminisztrátori jogokat szerző, általában rosszindulatú célból használt szoftver

rendelkezett. A harmadik legnagyobb botnetet üzemeltető Rustock eredeti fertőzést bejuttató állományát (dropper) nem sikerült megtalálni. A Bohmini.A a távoli elérést biztosító trójai programok közé tartozik. A Facebook igénybevételével, hirdetéseket közlő hálózat segítségével terjedt el. A célpont gépen futó helyi folyamatokba injektálta a fertőző kódot, mellyel, egy távoli vezérlőszerverrel tartott kapcsolatot. A Koobface is 2008-ban jelent meg. A féreg célpontjai a Facebook, Skype és Yahoo Messenger, Twitter, Google Mail, stb. felhasználók és a bejelentkezési jelszavak megszerzése volt a fő célja. A fertőzés Facebook segítségével történt. A mai napig aktív Conficker vírus is 2008 „terméke". A világszerte elterjedt féreg a számítógépek millióit fertőzte meg az operációs rendszer hibáját kombinálva a szótáralapú jelszópróbálgatás módszerével. A legkiterjedtebb botnetet a Conficker valósította meg. A fennálló fertőzések a kiadott szoftverfrissítések mellőzése és a vírus fejlődése miatt maradt fenn.

2009-ben az email csatolmányban érkező Dozer miután a biztonsági modulokat leállította, DDoS támadásokat végzett az Egyesült Államok és Dél-Korea irányában. A Daprosy féreg a helyi hálózaton, USB meghajtókon, és spamekben terjedt. A főként a billentyűzet leütéseket kifürkésző malware-t a kétezres évek legveszélyesebbek fenyegetései közé sorolják. A kétezres évek második felében olyan kártevő változatok, módszerek (távoli elérés, kifinomult fertőzési vektorok, vírusvédelem kikapcsolása, stb.) jelentek meg, amelyek egyre hatékonyabban rejtették el tevékenységüket. Megjelentek a célzott támadásra alkalmas módszerek, amelyek vonzók lettek a különféle országok állami szereplőinek. Az első kiberfegyver is megjelent, a Stuxnet. Bizonyára több olyan eset is van, amelyek nem kaptak nyilvánosságot.

Kétezer-tízes évek – az APT kor

A kétezer-tízes évek tovább bonyolították a kibertérben folyó védelmi tevékenységet. Amellett, hogy a kiberbűnözés kimondottan megerősödött[8], az állami szereplők is alaposan kivették a részüket a támadásokban. A következő országokról jelentek meg kiberképességeiről információk a tömegmédiában konkrét példák nélkül: Egyesült Államok, Egyesült Királyság, Orosz Föderáció, Észak-Korea, Irán, Kínai Népköztársaság, Szíria, Franciaország.

12. ábra. Az NSA globális APT képessége
https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/

8 Az NSA becslése szerint 250 Mrd USD a kiberbűnözés által okozott kár világszerte (forrás: http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion)

Megnevezés	Támadás észlelése	Valószínűsített támadó	Támadott	Tevékenység
Moonlight Maze	1998	Oroszország	USA Pentagon, NASA stb.	Több tízezer dokumentumot szereztek meg
Titan Rain	2003	Kína	USA	Nem
Stuxnet	2005	USA-Izrael	Irán + kb. 10 ország	Irán urándúsító kapacitásának visszafogása
US Congressmen	2006	?	USA	Kínai disszidensekről szóló iratok megszerzése
Shady RAT	2006	Kína	USA, Kanada, Ensz + 3 ország,	Dokumentumok megszerzése
NIPRNET, SIPRNET támadás	2008	Oroszország	USA	Dokumentumok megszerzése
Red October	2008	Oroszország	Több ország külügyminisztériuma	Adatszerzés
GhostNet	2009	Kína	103 ország	Adatszerzés
Operation Aurora	2009	Kína	USA	Forráskódok elérése, módosítása
Night Dragon	2009	Kína	Energia szektorbeli cégek világszerte	Adatszerzés
Ke3chang	2010	Kína	Több ország külügyminisztériuma	Adatszerzés
Duqu	2011	N.A.	Irán + több ország ipari számítógépe	Adatszerzés
Icefog	2011	N.A.	Dél-Korea, Japán, Kína + 12 ország	Adatszerzés
Teamspy	2012	N.A.	Több ország külügyminisztériuma	Adatszerzés
Flame	2012	USA	Közel Kelet országai	Adatszerzés
Miniduke	2013	Ukrajna	Több ország	Adatszerzés
Kimsuky	2013	Észak Korea	Dél-Korea, Kína	Adatszerzés
Careto	2013	Spanyol nyelvű	31 ország	Adatszerzés
Dragonfly	2013	?	Ipari rendszerek világszerte	Szabotázs, adatszerzés
Snake/Uroburos	2014	Oroszország	Kb. 50 ország	Adatszerzés

1. táblázat. Áttekintő táblázat [15]

Az elmúlt néhány évben egyre több APT besorolású kampány került a nyilvánosságra (1. táblázat). A vélhetően spanyol Careto 31 országot érintett, több platformon is (okostelefonon) működik, szisztematikusan gyűjtötte a szenzitív adatokat, pl. a titkosítási kulcsokat. A Snake/Uroburos valószínűleg orosz kémszoftver. A Ke3Chang vélhetően kínai kémszoftver. Az amerikai NSA 2004 óta fejleszti kiberműveleti hacker képességeit. A Turbine (lásd 13. ábra) fedőnevű intelligens rendszere lehetővé teszi a számítógépes hálózatok támadását százezres nagyságrendben [11]. Az Egyesült Királyság elsőként ismerte el [12], hogy fejleszti mindenoldalú katonai kiberképességeit, mely csapásmérő erőt is tartalmaz.

Az ismertté vált esetek némelyike nagy publicitást kapott, míg másokról kevés információ került napvilágra. Az APT szerű támadások megjelenése óta folyamatosan bővültek, finomodtak a módszerek. A sérülékenységek kihasználásának két válfaját alkalmazzák már a kezdetektől: az ismert illetve a még nem ismerteket. A támadások célzott jellege miatt nagy különbségeket láthatunk az egyes APT-k között. A célpont rendszereibe való behatolás módszere eleinte a fizikai hozzáférés volt. Elsősorban hordozható média közvetlen csatlakozása és a fertőzés kivitelezése dominált azokban az esetekben, ahol erre lehetőség adódott. A közvetlen támadásokban az internetes kapcsolattal rendelkező erőforrások nyitott portjainak letapogatása távoli bejelentkezési kísérletek útján történő bejutás is elterjedt módszer. A

támadások egy részében a célpontra szabott becsapós emailek küldése volt a legelterjedtebb az elmúlt években. Az email káros kódot tartalmazó weblapra mutat, az áldozat a linkre kattintva fertőződik, vagy a csatolmányban küldenek a részükre olyan futtatható állományt, ami dokumentumnak „látszik”. A csatolmány „megnyitása” általában egy hamis tartalmú dokumentum megjelenítésén túl elvégzi a rendszer fertőzését, vagy csupán egy fertőzést okozó káros kód fut le.

Legújabban az úgynevezett watering hole támadások kerültek az előtérbe. Az elmúlt években egyre nagyobb számban láthatunk az eddigieknél kifinomultabb módszereket. A támadás első lépcsőjeként olyan legális (kihasználható sérülékenységet tartalmazó) weblapokat változtat meg a támadó, amelyet a célpontjai látogatnak. A változtatás lényege olyan iframe keret elhelyezése, mely rejtett átirányítást tartalmaz. Az átirányítás egy olyan domainre mutat, amit a támadó hozott létre, vagy fertőzött meg és menedzsel. Az átirányított áldozatról adatgyűjtést (fingerprinting) végez a támadó és ha az áldozat értékes és kihasználható sérülékenységet tartalmazó szoftvere van, akkor további átirányítás történik a már káros kódot tartalmazó domainre. Ekkor történik meg a tényleges fertőzés, míg a támadás első két fázisát víruskeresőkkel lehetetlen megtalálni, ugyanis az átirányítások, a telepített pluginek feltérképezése legális műveleteknek számítanak. A fertőzés további lépcsőket is tartalmazhat, például a kezdeti távoli elérést biztosító eszközt lehet frissíteni.

NÉHÁNY APT KAMPÁNY ISMERTETÉSE

Dragonfly [17]

A Dragonfly jelenleg az energiaszektorban működő vállalati rendszereket támadja. A támadó eszközei a Backdoor.Oldrea és a Trojan.Karagany-t. A célpontok között energiaszolgáltató, csővezeték üzemeltető, energiaipari vezérlőrendszer berendezésgyártók is voltak. Az áldozatok Spanyolországban, az USA-ban, Franciaországban, Olaszországban, Németországban, Törökországban, Lengyelországban, Romániában, Görögországban és Szerbiában voltak a legnagyobb számban. A Dragonfly APT támadói technikailag jól képzettek, és stratégiai gondolkodásra képesek. A csoport minden esetben kisebb, kevésbé védett beszállító támadásával jut a célpont közelébe.

A Symantec szakértői a támadás három lépcsőjét írták le. Az elsőben adathalász emailben malware-t tartalmazó csatolmányt küldenek a célpontnak. A másodikban a levelek címzettjeit exploit-okat tartalmazó weboldalakra vezetik. A harmadikban közvetlenül az ipari vezérlőrendszereket előállítót támadják meg, így a malware-eket még a gyárban, eladás előtt elhelyezik a szoftverekben. Ez esetben a fertőzést maga a cég végzi el a telepítésekor. A feltételezett támadó székhelye valószínűleg Kelet-Európa. A Dragonfly hasonló motivációval rendelkezik mint a Stuxnet, de adatszerzést is végez.

Uroburos[18]

A különösen kifimomult APT támadást a G DATA németországi cég hozta nyilvánosságra és a káros kódban szereplő sztring alapján kapta a nevét (lásd a kódrészlet alább).

```
80 FA FF FF D4 CB B9 09 80 FA FF FF 54 C6 B9 09  ............T...

80 FA FF FF 00 00 00 00 55 72 30 62 55 72 28 29  ........Ur0bUr()

73 47 6F 54 79 4F 75 23 00 00 00 00 00 00 00 00  sGoTyOu#........
```

Az APT tevékenységt 2011-ig vezették vissza, így a felfedezés előtt már 3 éve aktív volt. A G-Data szakemberei szerint úgy gondolják, hogy hírszerző ügynökséggel hozható összefüggésbe a támadás, vélhetően több még fel nem fedezett változat is lehet. Az Uroburos egy rootkit, amely két fájlból, egy driver-ből és egy rejtjelzett virtuális fájlrendszerből tevődik

össze. A támadó átveszi az uralmat a megfertőzött számítógép felett, bármilyen programkódot futtathat a gépen, és önvédelmi moduljának segítségével képes rejteni tevékenységét. Az Uroburos adatokat szerez és a hálózati forgalom elfogására is képes. Több víruskutató szerint kapcsolat lehet az Uroburos és egy korábbi APT támadás között, amelyet korábban az amerikai kormányzati szervek ellen használtak. Alább egy példa látható a támadó tevékenységének hálózatból vett mintázatára (a http biztonsági okokból cserélve hxxp-re).

„http GET hxxp://eu-sciffi.99k.org/B/3/6530475040”

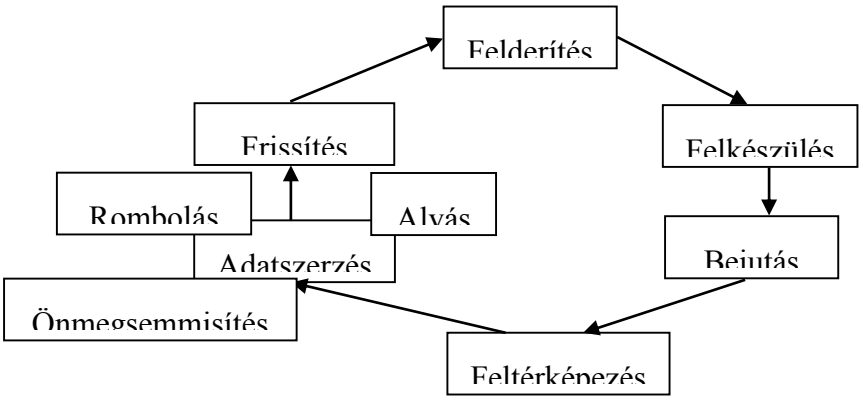
AZ APT TÁMADÁSOK ELLENI VÉDEKEZÉS LEHETŐSÉGEI

Ebben a részben vázlatosan összefoglalom a védekezés lehetőségeit. Elsőként definiálom az APT-t, majd az APT támadás ciklusát mutatom be, végül számba veszem a védekezés módozatait.

Az Advanced Persistent Threat (APT) – Folyamatosan Fennálló Fejlett Fenyegetés (4F) definíciója

Informatikai rendszerekbe észrevétlenül, célzott módon, adatszerzés és/vagy rombolás céljából bejuttatott különleges képességű folyamatok, melyek külső kapcsolat segítségével, távolról kiadott vezérlőparancsok végrehajtásával folyamatosan működve fejtik ki jogszerűtlen tevékenységüket (saját definíció).

Az APT életciklusa, funkciói



13. ábra. Az APT támadás alapsémája, funkciók

Az APT kifejezés 2005 körül jelent meg, annak érdekében, hogy a figyelmet ráirányítsa erre a jelenségre. Nem új típusú kártevő kódcsaládról volt szó akkoriban sem, hiszen az APT első része felfogható egy trójai programnak, a bejuttatott távoli elérést biztosító szoftver pedig egy Remote Access Tool-nak a vezérléstől függően bármilyen tevékenységet végezhet. Az, hogy mégis külön kategóriába kell sorolni az APT támadásokat azért van, mert az első támadások felfedezése idején precedens nélküli volt az ily mértékben körültekintő óvatossággal megtervezett és kivitelezett támadás és információszerzés. Az APT általában nem feltétlenül alkalmaz újabb technológiákat, hanem több fokozatban, egymásra épülő, gondosan kivitelezett lépések megtételével éri el a célját. Az első fokozatban az áldozat rendszerének gyenge pontjainak felderítése, feltérképezése a cél. Ezt követően kerül kidolgozásra a célzott támadás terve, mely meghatározza a rendszerbe bejutás módszerét, egy, vagy több kihasználható sérülékenység útján, majd létrehozásra kerül a támadó infrastruktúra, a vezérlőszerverek, a

támadási vektor végrehajtásának minden eleme. Ezek magukba foglalják szoftverelemek kifejlesztését, domain nevek regisztrációját, hardver elemek biztosítását, a célzott támadáshoz szükséges dokumentumok, emailek stb. elkészítését. A támadás kezdeti szakasza a rendszerbe való bejutást célozza. Még mindig a legelterjedtebb módszer az áldozat rendszerébe való bejutásra a megtévesztő email küldése, vagy egy fertőzött pendrive csatlakoztatása a célpont rendszeréhez.

Email támadási vektor esetén az email tárgya és a feladó email címe úgy kerül megválasztásra, hogy az felkeltse a felhasználó érdeklődését és így a levél nagy valószínűséggel megnyitásra, elolvasásra kerül. A levél tartalma gondosan megtervezett megtévesztés. A károkozó töltetét több formában tartalmazhatja. A levél törzse közvetlenül tartalmazhat károkozó kódot bejuttató hivatkozást, amely egy internetkapcsolattal rendelkező gépre a hivatkozás megnyitását követően letöltődhet. Másik lehetőség az email csatolmány. A különlegesen elkészített csatolmány szintén a megtévesztést szolgálja, valójában a fertőzést előidéző futtatható kódok kerülnek végrehajtásra a csatolmány megnyitását követően. A fertőzés kezdeti lépését követően a rendszerbe bejutott modul kapcsolatot létesít az APT támadás egyik vezérlőszerverével. A szerverről további modul(ok) kerülhetnek letöltésre, majd megindul a gép és a környezetének feltérképezése. A roppant kifinomult technikákat alkalmazó APT lopakodva, folyamatosan figyelheti a hálózaton elérhető szolgáltatásokat, dokumentumokat, kulcsokat, jelszavakat gyűjthet, de akár rombolást is végrehajthat. Általában önvédelmi és önmegsemmisítő modullal is rendelkezik, mely megnehezíti a hatásmechanizmusuk, céljuk, eredetük, tevékenységük felfedését.

Nagy valószínűséggel olyan állami szereplők állhatnak az APT kampányok mögött, mint pl. az ellenérdekelt hírszerző szolgálatok, fegyveres erők.

VÉDEKEZÉSI MÓDSZEREK

Az APT támadásokat legjobb megelőzni. A prevenciót a komplex biztonsági rendszer lehetőségeinek kihasználása segíti elő. Egy jól megtervezett és kivitelezett kiberbiztonsági rendszer is lehet hatástalan, ha a funkcióit nem használják.

Az információ biztonságot több szabványban (ISO 27000 szabványcsalád, ISO 15408, COBIT), valamint a 77/2013. NFM rendeletben megtalálható módon szükséges egyenszilárd módon biztosítani. A védelem adminisztratív, fizikai, humán és technikai aspektusairól a védelmet igénylőnek kell dönteni, az erőforrásokat kiválasztani. A döntés nem egyszerű, alapja a kockázatelemzés. Az alapvetően adminisztratív intézkedések betartása a biztonsági tudatosságon alapul, a szabályok figyelmen kívül hagyása a védelem képességeinek leromlásával jár. Ennek érdekében a felhasználók, üzemeltetők és a vezetők rendszeres biztonsági tudatossági képzése az alap. Szükséges kidolgozni az informatikai biztonsági szabályzatokat, ellenőrizni azok végrehajtását. Ennek keretében a jogosultságkezelés helyes menedzselése, a fizikai hozzáférés korlátozása mellett a megfelelő autentikációs rendszer alkalmazása is nagyon fontos. Szintén fontos a helyes jelszókezelési házirend bevezetése, mely megnehezíti a fiókok jogosulatlan elérését. A felhasználói tevékenység biztonságosabbá tétele, az erős jelszavak alkalmazása, azok gyakori megváltoztatása, bármilyen meglepő is a legolcsóbb, de egyben az egyik legfontosabb eleme a prevenciónak. Fontos a pendrive használat szabályozása, valamint a magántulajdonban lévő eszközök használatának menedzselése, vagy tiltása (BYOD)[9].

Nagyon lényeges a biztonság szempontjából, hogy a szoftverfrissítések lehető leghamarabb megtörténjenek. Az ismertté vált sérülékenységek kihasználhatósága ezáltal kiküszöbölhető. Nagyobb a veszély a 0-napi sérülékenységekkel kapcsolatban, ugyanis ezeket vagy még nem

9 Bring Your Own Device: Csatlakozz a sajátoddal lehetőség

ismerjük, vagy nincsen rendelkezésre álló szoftverjavítás. Ez utóbbi esetben korlátozni kell a sérülékeny szoftver használatát. Ha viszont nem ismeretes a sérülékenység, akkor az nem ismert mértékű kockázatot jelent. A prevenció technikai lehetőségei az ismert mintázatokra vonatkozóan széleskörűen rendelkezésre áll. Nem ez a helyzet az APT támadásokra.

Amennyiben egy APT támadásról partnereinktől tájékoztatást kapunk, akkor azok technikai adatait (vonatkozó IP címek, domain nevek, stb.) a határvédelmi rendszerekben felhasználhatjuk, ennek hiányában azonban nehézségbe ütközünk, mert ismeretlen mintázatú támadásra a behatolásjelző rendszerek, antivírus alkalmazások haszontalanok. A prevenció korlátai itt jelentkeznek. Az APT támadások többnyire áldozatspecifikusak, így technikai adatok korlátozottan állnak rendelkezésre. Ismeret hiányában szükségünk lenne más módszerekre is.

Az APT-k elleni védekezésben jelenleg már több termék van a piacon bár azok árfekvése meglehetősen magas. A Cisco, TrendMicro, Sourcefire és a FireEye rendelkeznek már ilyen megoldással. A védelem lehetséges eszközei ezek mellett az alábbiak.

Az ismert támadásokban elfogott káros kódok pl. hash azonosítóinak vagy hálózati forgalmi mintázatoknak keresésén alapuló módszernek a célzott támadásokban nem elégséges a használata, azonban a védelem még jelenleg is fontos eleme. Idő- és erőforrásigénye egyre nagyobb.

A hálózaton folyó forgalom valósidejű figyelésének számos előnye van. Ezek közül például a behatolásjelző/behatolásvédelmi (IDS/IPS) rendszerek az ismertté vált támadások ellen hatékonyak. A csomagszintű vizsgálat is szóba jön, mint védekezési módszer.

A hálózati anomáliák, vagyis a szokásostól eltérő forgalmi adatok vizsgálata is célravezető lehet egyes ismeretlen támadásokban.

A naplóállományok gyűjtése és elemzése nagyon fontos a támadások felismerésében. A DNS kérések naplózása és elemzése úgyszintén lehetséges.

A fekete- és fehérlisták alkalmazása a tiltandó és az engedélyezendő kapcsolódásokra megoldást jelent, de rendszeres karbantartásigénye merevvé teszi ezt a megoldást.

A futtatható állományok ellenőrzése emulált környezetben képes lehet a káros viselkedés felismerésére. Ilyen például a Cuckoo Sandbox. A káros kódot tartalmazó csatolt fájlok bejuttatása ellen a csomagszintű vizsgálatok jelenthetnek megoldást. A virtuális környezetet kialakító sandboxing technika szimulált környezetben „szabadjára engedi” a vizsgált gyanús objektumokat, viselkedésvizsgálatot végezve. Ez korszerű megközelítés bár egyes támadások védekeznek a sandbox technika ellen és nem árulják el magukat, amennyiben észlelik a sandbox-ban futást.

A különféle csapdák alkalmazása is megoldást kínál az ismeretlen támadások felismerésében. Ennél a megoldásnál például egy áldozati gépet helyezünk el a hálózaton, amelynek szándékosan gyenge védelmi megoldásai vannak. A megfertőződést pedig figyelemmel kísérjük és a támadás adatait felhasználjuk a védelemben.

Lehetőség van továbbá a viselkedési anomáliák vizsgálatára. Az ilyen jellegű termékek a megnövekedett CPU terhelés, szokatlan mennyiségű és idejű aktivitás, nem ismert folyamatok futása, folyamatváltások számának növekedése, új rendszerprogram-szálak megjelenése, egyéb események észlelése útján adhatnak riasztást.

A felsorolt módszerek hatékony alkalmazásához jól képzett szakszemélyzet szükséges. Összességében a megelőzés során a gyanús emailek, a rendszeranomáliák kivizsgálása, az ismert fájltípusokba beágyazott futtatható kódok keresése, valamint a gyanús külső hálózati kapcsolódások vizsgálata áll az eszköztárunkban rendelkezésre, azonban a csomagszintű szűrés és vizsgálatok a sandboxing technika megoldások is ígéretes hatékonysággal segítik az APT támadások elleni fellépést.

Figyelembe véve, hogy az APT támadások fő célpontjai világszerte kormányzati intézmények, tudományos intézetek, illetve kritikus infrastruktúrák üzemeltetői, szükséges

ezen a téren a védelem erősítése és megfelelő kiberbiztonsági menedzsment kialakítása, a képzett szakemberek rendelkezésre állása.

ÖSSZEFOGLALÁS

A kártékony kódok 43 éves történelmük során a számítástechnikával párhuzamosan fejlődtek. A Neumann elvű számítógép architektúra sajnos sikertörténet a számítógépes vírusok számára is.

A kilencvenes években indult meg a víruskeresők és vírusírók ma sem lankadó küzdelme a vírusirtás és a vírusok elrejtőzése területén. Napjainkban már nem elég a víruskereső programok használata, hanem több, egymást kiegészítő módszer kell a hatékonyabb védelem kialakítására.

A kiberbűnözés térnyerése és az APT támadások megjelenése a kétezres éveket jellemezte. A védelem szereplői új módszereket kénytelenek alkalmazni, egyre növekvő költséggel. A folyamatos fenyegetések a kibertérben, a kifinomult APT támadások elleni védelem jelenleg ismert módszerei nem örökérvényű megoldások. Elsősorban az egymásra épülő, rutinfeladatok fegyelmezett végrehajtása, úgymint például a biztonságtudatos eszközhasználat, a szabályok betartása, a különféle viselkedésalapú vizsgálatok, a naplóállományok elemzése növeli a rendszereink védettségét. A kifinomultabb módszerek, mint a csomagszintű vizsgálat, vagy a sandboxing, esetleg a csapdarendszerek alkalmazása tovább javíthatja a védettséget.

Az adminisztratív-, fizikai-, logikai védelmi elemeket az információs rendszerek védelme érdekében a kockázatokkal arányosan kell kialakítani a jogszabályoknak megfelelően.

Nem hagyhatjuk figyelmen kívül a felhasználók és a vezetők felelősségét sem. A legkiválóbban megtervezett rendszer sem hatékony, ha nincs érvényesítve valamely eleme. A támadók a leggyengébb ponton fognak támadni, ugyanis folyamatosan keresik a támadási pontokat.

A védelem továbbfejlesztésének lehetősége az APT támadások teljes körű megértése, a védelem adaptivitása és a reagálási sebesség növelése, proaktív mellett a kiberképességek módszertanának további kutatásában rejlik.

Felhasznált irodalom:

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

[2] http://ttk.pte.hu/ami/phare/tortenet/EDVAC.html (letöltve: 2014.03.16.)

[3] http://www.livinginternet.com/i/ii_wiener.htm (letöltve: 2014.03.16.)

[4] Bakacsi Géza, Csákány Béla: Egy szegedi néptanító emlékezete Ponticulus Hungaricus XIV. évfolyam 7—8. szám 2010. július—augusztus http://members.iif.hu/visontay/ponticulus/rovatok/limes/gaspar_dezso_elete.html (letöltve: 2014.03.16.)

[5] Neumann János: Az önmagát reprodukáló automata elmélete (Theory of Self-Reproducing Automata) 1966 University of Illinois Press Urbana and London http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf (letöltve: 2014.03.16.)

[6] http://www.mernokbazis.hu/cikkek/egy-gep-ami-onmagat-masolja (letöltve: 2014.03.16.)

[7] Bevezetés az élet játékaiba http://www.szak.hu/konyvek_htm/sample_chapters/artofvirus/chap1.pdf (letöltve: 2014.03.16.)

[8] Timeline of computer viruses and worms http://virus.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses (letöltve: 2014.03.23.)

[9] Pintér Róbert: A vírusok és azok fajtái http://artefaktum.hu/oktatashoz/internet05tav/06_biztonsag/virus_Hardwer_OC_attekintes.doc (letöltve: 2014.03.23.)

[10] Szegedi Imre: Személyi számítógépes vírusok elterjedésének veszélyei és az ellenük való védelem a Magyar Honvédségben Első magyar víruskönyv Egyetemi doktori értekezés Budapest, 1990 http://uni-nke.hu/downloads/konyvtar/digitgy/doktori/egyetemi/Szegedi_Imre.pdf (letöltve: 2014.03.23.)

[11] Ryan Gallagher, Glenn Greenwald: How the NSA Plans to Infect 'Millions' of Computers with Malware, 2014.03.12. The Intercept https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ (letöltve: 2014.03.23.)

[12] James Blitz: UK becomes first to admit offensive cyber attack capability Politics & Policy, 2013. 09.29. http://www.ft.com/intl/cms/s/0/9ac6ede6-28fd-11e3-ab62-00144feab7de.html#axzz2wra94jkt (letöltve: 2014.03.23.)

[13] Szőr Péter: A vírusvédelem története Szak Kiadó 2010.

[14] Gyebrovszki Tamás: Stuxnet - mint az első alkalmazott kiberfegyver - a Tallinni Kézikönyv szabályrendszere szempontjából Hadmérnök, 2014/1 164.-174. oldal

[15] Advanced Persistent Threats: A Decade in Review 2011. http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf (letöltve: 2014.04.12)

[16] http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf (letöltve: 2014.04.13.)

[17] http://www.cert-hungary.hu/node/259 (letöltve 2014.07.23.)

[18] http://www.cert-hungary.hu/node/237 (letöltve 2014.07.23.)