HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Berki Gábor
berkigabor@t-online.hu

A KIBERTÉRI KONFLIKTUSOK VÁLTOZÁSAI

Absztrakt

Az utóbbi néhány évben egyre több hírt hallunk számítógép-hálózati támadásokról. A célpontok között szerepelnek nemzetközi nagyvállalatok, kormányzati szervek, pénzügyi vállalatok és kritikus infrastruktúrák is. A támadók bevallott céljai nagyon különbözőek, a kíváncsiságtól, az anyagi haszonszerzésen át a politikai, vallási célok eléréséig. Ha azonban összességében tekintünk ezekre az eseményekre, megláthatjuk azokat a tendenciákat, amelyek világunkat fenyegetik, ha nem teszünk megfelelő lépéseket a védekezésre.

In recent years there have been growing reports of attacks on computer network. Targets include international corporations, government agencies, financial firms and critical infrastucture. The attackers' declared goals range from simple cuoriousity through to financial gain and political and religious aims. Unless adequate protective measures are put in place, such developments will continue to threaten today's world.

Kulcsszavak: *kiberhadviselés, hackerek, rosszindulatú programok, információbiztonság, folyamatirányítás ~ cyberwar, hackers, malewares, information security, process controll*

BEVEZETÉS

Az Internet elterjedésével egyszerűbbé vált az élet, a hivatalos ügyintézésektől kezdve, a banki átutalásokon át a webes vásárlások lebonyolításáig. Ám a számítógép-hálózatokkal átszőtt világunk sosem volt olyan sebezhető, mint napjainkban. Ez a sebezhetőség a bonyolult technikai, infokommunikációs rendszerektől való függésnek, illetve az egymással összekapcsolódó létfontosságú infrastruktúráknak köszönhető. A telekommunikációs hálózatok, energiaszállítási útvonalak, vízutánpótlási rendszerek, szállítási hálózatok, banki és pénzügyi szolgáltatások, állami szolgáltatások és vészhelyzeti szolgáltatások működésképtelenné tételének lehetősége komoly fenyegetést jelent. [1] Az ártó szándékú támadók kihasználva a sebezhetőségeket, a saját céljaik – legyen az ideológiai, vallási vagy pénzszerzési - elérése érdekében korlátozni, bénítani igyekeznek az információs társadalom részegységeinek működését. A nagy sajtóvisszhangot kiváltó támadások azonban csak a jéghegy csúcsát jelentik, véleményem szerint a háttérben igen intenzív felderítő munkát végeznek bizonyos csoportok, országok, hogy a jövőben esetleg kialakuló konfliktusok során előnyös pozícióból tudják támadni az ellenfél informatikai, folyamatirányító rendszereit, kritikus infrastruktúráit. Az alábbiakban – a nagyobb kibertámadások mellett - az erre utaló tevékenységeket is bemutatom. A közelmúltban nagy visszhangot kiváltó Stuxnet és a magyar CrySyS labor által felfedezett Duqu, Flamer és egyéb, a közelmúltban detektált vírusok bemutatásával rávilágítok a célzott informatikai támadások lehetőségeire. Az Anonymous hackercsoport kampányszerű támadásaiban is megpróbálok logikus rendszert találni.

AZ ELSŐ INFORMATIKAI TÁMADÁSOK

Habár a szakirodalom szerint a legelső dokumentált kibertámadást 1997-ben egy sri lanka-i terrorszervezet, a tamil tigrisek követték el, úgy gondolom, nem mehetünk el szó nélkül az 1982-es szibériai gázvezeték-robbanás mellett sem. Thomas C. Reed, az amerikai Nemzetbiztonsági Hivatal egykori munkatársa 2004-ben megjelent könyvében[1] leírja, hogy a robbanás nem a véletlen műve volt, hanem a szovjetek elleni gazdasági hadviselés része. A Szovjetunió megpróbált embargós nyugati technológiához jutni, az Egyesült Államok viszont meg akarta akadályozni, hogy a szovjetek valutabevételhez jussanak a nyersanyagszállításokból. [2]

Egy, a KGB-be beépült ügynök juttatta el a CIA-hoz azt a listát, amelyen a szovjetek által beszerezni kívánt technológia szerepelt. Ezen találták azt a bizonyos szoftvert, amelyet a nyersanyagvezetékek irányítási rendszereihez használtak volna. Egy kanadai vállalaton keresztül a CIA adta el a szovjeteknek a szoftvert, amelybe azonban olyan hibákat építettek, hogy néhány hónapos kifogástalan működés után összezavarta a szállítási folyamatokat. Ezt a vezeték irányítószelepeinek precízen megtervezett fals működtetésével érték el. Ennek eredménye volt az eddigi legnagyobb, nem nukleáris eredetű robbanás, amely a szovjet gazdaságot is megrázta 1982 nyarán.

Ez az emberéletet nem követelő, de hatalmas kárt okozó robbanás indította el a hidegháború utolsó felvonását - állítja a könyv szerzője. Mert noha a szovjetek rájöttek, hogy manipulált technológiát vettek, innentől kezdve nem bízhattak meg egyetlen beszállítójukban sem.[3]

Ez az akció előrevetítette a számítógép vezérelte rendszerek sebezhetőségét is.

1999-ben szerb hackerek – a NATO szerbiai bombázásaira válaszul - támadták meg a szövetség szervereit és néhányat DDoS2 módszerrel tettek átmenetileg elérhetetlenné, valamint feltörtek néhány weboldalt és propaganda üzeneteket helyeztek el rajtuk.

---

[1] At the Abyss: An Insider's History of the Cold War New York 2004. ISBN 0-89141-821-0

[2] Distributed Denial of Service – elosztott szolgáltatás-megtagadással járó támadás

A 2000-es évek elején kezdődtek azok a támadások, amelyek célja nem a károkozás vagy a figyelemfelkeltés, hanem az amerikai ipari és katonai infrastruktúra feltérképezése volt. A támadásokat orosz illetve kínai számítógépekre vezették vissza, de ezen országok vezetői hevesen tagadták, hogy kormányaiknak bármi közük is lenne hozzájuk. A leghíresebb támadássorozat a Titan Rain fedőnevet kapta és egyértelműen Kínához volt kapcsolható.[4] A legkülönbözőbb célpontok támadása során a védelmi rendszerek hatékonyságát és működését tesztelték. Természetesen nem tudható, hogy ezek a támadások milyen eredménnyel jártak, de nem járunk messze a valóságtól, ha azt feltételezzük, hogy a támadók igen pontos információkkal rendelkeznek ezen rendszerekről és egy komolyabb konfliktusban nagyszerűen ki tudnák használni a feltérképezett hibákat és komoly csapást tudnának mérni célpontjaikra.

Az első kibertámadás, amelyet egy ország ellen indítottak, 2007-ben következett be. Az igen fejlett informatikai kultúrával rendelkező Észtországban 2007. április 27-én zavargások törtek ki a tallinni szovjet hősi emlékmű eltávolítása miatt. Az első túlterheléses támadások jelei néhány nappal az első tüntetések után jelentkeztek a parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit az orosz hatóságok természetesen tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt. Az ország online adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott. Egyes szakértők szerint a kibertámadás sokkal súlyosabb gazdasági károkat okozott Észtországnak, mint amit azok a kereskedelmi szankciók okoztak volna, amikkel Oroszország a krízis első heteiben fenyegetőzött.

Bár kezdetben NATO-szakértők is részt vettek a támadások felderítésében, azok jellegéből adódóan a támadók azonosítása szinte lehetetlen volt. Számos támadót lehetett ugyan azonosítani orosz területen, de annak egyértelmű igazolása, hogy kormányzati szerverek voltak, sikertelennek bizonyult. Általánosan elterjedt nézet szerint orosz hazafias érzelmű hackerek olyan botnet hálózatot hoztak létre, amelybe orosz gépeken kívül számos más ország területén lévő számítógépeket is beszerveztek a tudtuk nélkül (zombi gépek), és ezeken keresztül hajtották végre a támadásokat.[2]

A 2008 augusztusában kitört orosz-grúz háborúnak is volt kiber aspektusa. Mint az köztudott, a hosszú évek óta tartó grúz-oszét és a grúz-abház konfliktust a grúz elnök 2008. augusztus 8-án katonai úton próbálta megoldani az említett területek megtámadásával. Rosszul mérte fel azonban az erőviszonyokat, amikor nem számolt azzal, hogy Oroszország nem fogja szó nélkül hagyni a támadást, már csak azért sem, mivel csapatai ENSZ felhatalmazással békefenntartó missziót teljesítettek Dél-Oszétiában. Az orosz csapatok erőteljes válaszcsapásokat mértek a grúz erőkre és öt napig tartó heves harcok után a grúzok kénytelenek voltak fegyverszünetet kérni.[5]

A fegyveres konfliktussal egy időben megindult Grúzia ellen egy kiber hadjárat is. Az internet-forgalmat ellenőrzése alá vonta Oroszország - vagy legalábbis valakik Oroszországból, állította a grúz kormány, amely valóságos kiber-emigrációba kényszerült, és a hadi jelentések mellett sorra jelentette meg a virtuális támadásokról szóló közleményeit.3

A leglátványosabb hacker-akciók ugyanis az ország kormányzati weboldalai ellen indultak, amelyeket kívülről megbénítottak, illetve a tartalmukat kicserélték4. Az orosz földről érkezett

[3] http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html
[4] Ezt nevezi az internetes szaknyelv defacementnek

hackerek Mihail Szakasvili elnök portréjával vandálkodtak. Az államfő képére Hitler-bajuszt rajzoltak, és egy sor olyan képet tettek ki róla az oldalra, ahol a náci diktátor pózaiban ábrázolták, vagy a történelem nagy gonosztevői közé kopírozták be az arcmását.

A megtámadott oldalak között volt az elnök saját weblapja mellett a grúz külügy- és hadügyminisztérium is. Szakasvili elnök erre válaszul a hazája ügyét nyíltan támogató Lengyelország vezetőjétől kért és kapott segítséget: az államfő, illetve stábja Lech Kaczynski hivatalos, angol nyelvű oldalán is lehetőséget kapott arra, hogy tájékoztatást adjon a háborús eseményekről. Még ezt a hivatalos, nagyban gesztusértékű lépést megelőzően a honlap nélkül maradt grúz külügyminisztérium blogot indított a Google által birtokolt Blogspot blogszolgáltatónál.

Mindezekkel egy időben megindultak az ország lejáratását célzó, dezinformációs céllal indított weboldalak is - a hiteles forrásokat a konfliktusról percről percre-bontásban beszámoló blog a linkek között listázta. A kaukázusi országban a .ru végződésű webcímek is elérhetetlenné váltak, amelyeket egyes források szerint maga a grúz kormányzat tilttatott le, hogy útját állja az orosz propagandának, és a Tbilisziben lévő orosz nagykövetség munkatársai szerint a mobil- és vezetékes telefonszolgáltatásban is fennakadások voltak a túlterhelés miatt (igaz, ennek inkább a katonai offenzívához lehetett köze). [6]

Véleményem szerint a grúz kormány erősen eltúlozta az ellene indított kiber támadásokat, hisz korántsem rendelkezett olyan infrastruktúrával, mint például Észtország, így a támadásoknak sem volt olyan hatása, nem bénult meg a bankrendszer, illetve a kormányzat. Az interneten keresztül zajló nagyszabású támadások akkor különösen hatékonyak, ha egy olyan ország ellen irányulnak, amely erőteljesen támaszkodik információs technológiára és annak infrastruktúrájára. Grúzia esetében ez nem mondható el: az interneten keresztül a támadók nem tudtak nagyobb károkat okozni, mint az ország földjére lépő orosz katonák. Hétköznapi ésszel érthetetlen, hogy a kormány miért foglalkozott olyan erőteljesen a kiber-támadásokkal, miközben városait, infrastruktúráját lőtte és bombázta az orosz hadsereg.

Mind az orosz-észt, mind az orosz-grúz konfliktus vonatkozásában elmondhatjuk, az orosz hivatalos szervek kategorikusan tagadták, hogy közük lenne a támadásokhoz. A konfliktusok lezárulta utáni elemzések csupán azt tudták kimutatni, hogy orosz nacionalista érzések vezérelték a támadókat, ám az orosz állam közreműködését nem sikerült bebizonyítani.

A ROSSZINDULATÚ PROGRAMOK ÚJ GENERÁCIÓJA

Az első vírusokat még a 70-es években készítették, a világ legelső ismert vírusa a Creeper volt amely a Tenex operációs rendszert használó számítógépek hálózatán terjedt. A Creeper kiirtására hozták létre a Reaper nevű programot, ez az első ismert vírusirtó.[7] A "számítógépes vírus" kifejezést először a neves elméleti víruskutató Fred Cohen használta 1983-ban egy tudományos munkában. Az első kifejezetten PC-re írt vírus 1986 januárjában tűnt fel. A floppy lemezen terjedő Brain nem okozott semmi kárt, de ezzel elindult az a folyamat ami, még napjainkban is mérgezi az informatika világát.

A vírusokkal, férgekkel és egyéb rosszindulatú programokkal folytatott több évtizedes harc azonban új, jelentős mérföldkőhöz érkezett 2010 júniusában, amikor a fehérorosz VirusBlokAda cég felfedezett egy új férget, amelyet Stuxnetnek neveztek el.

Az új féreg Microsoft operációs rendszereken terjed és kizárólag ipari folyamatirányító rendszerek ellen lett kifejlesztve. A Stuxnet kivételes mivoltát és specializáltságát erősíti az a tény is, hogy az említett ipari felügyeleti, vezérlő és adatgyűjtő rendszereket egyetlen cég a *német Siemens gyártja (SIMATIC WinCC HMI és WIMATIC STEP 7)* és alapvetően a nehézipari szektorban, illetve az energiatermelés és szállítás területén használják, azaz

fenyegetést alapvetően csak olyan létesítményekre jelent, melyek egy része kritikus infrastruktúrának minősül.[8]

A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. Elsősorban PLC[5] szoftvereket támadja. A WinCC/Step 7 szoftver volt mindezek közül az elsődleges, amelyet a Stuxnet megcélzott. Ez a szoftver adatkábelen keresztül kapcsolódik a PLC-hez és eléri a memória tartalmat, képes folyamatokat újrakonfigurálni, programokat feltölteni és a végrehajtás során rendelkezik bizonyos nyomkövetési funkciókkal is. Ha a PLC már programozásra került, akkor lekapcsolható róla, és a PLC már önmagában is képes a működésre. A Stuxnet e szoftver segítségével juttatta be kódblokkjait a PLC-be, majd ezeket el is rejtette. [10]

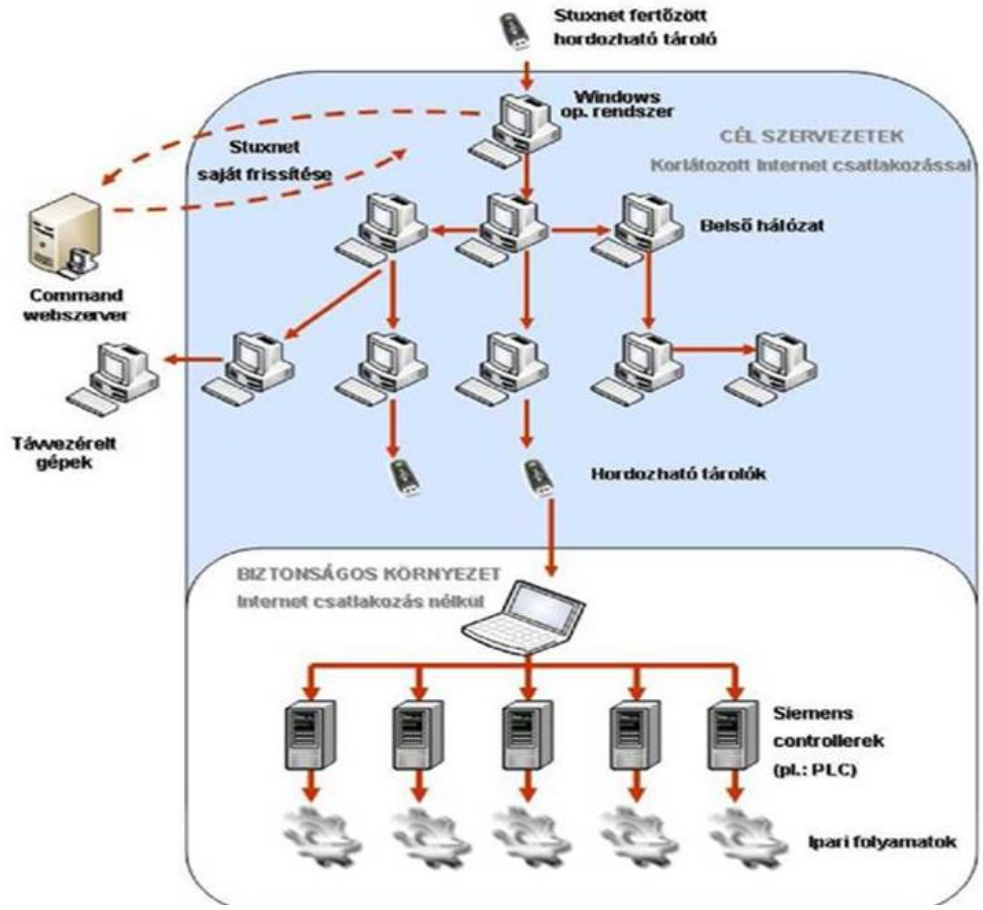
A Stuxnet a PLC-ken bizonyos konkrét ipari eszközök, nevezetesen nagy sebességű motorok frekvencia átalakítói után kutat és csak akkor lép akcióba, ha a finn Vacon és az iráni Fararo Paya készülékeire talál, valamint a felügyelt eszköz 807 és 1210 Hz között működik. Ilyen frekvencia átalakítók és motorok szinte kizárólag az iráni urándúsítókban használatosak.[10]

A vírus egyértelmű célja az urándúsító centrifugák észrevétlen tönkretétele és a dúsítási folyamat megzavarása volt. Ezt a célt sikeresen el is érte, hisz legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban és mértékadó vélekedések szerint legalább két évvel vetette vissza az iráni atomprogramot.

A támadó kód megírásának profizmusára utal, hogy egyszerre négy zero-day[6] fenyegetést is kihasznált a terjedéséhez és két lopott digitális aláírással is tudta igazolni legitimitását. Terjedését az alábbi ábra mutatja be.

[5] A PLC - Programmable Logic Controller, azaz programozható logikai vezérlő. PLC-ket nagy számban az ipari szabályozástechnikában, a különböző villamos, illetve az ilyen módon működtetett folyamatok irányításában használják.

[6] A *zero-day/zero-hour,* vagyis *nulladik napi támadás* kifejezést azokra a számítógépes biztonsági fenyegetésekre használják a szakemberek, amelyek egy adott számítógépes alkalmazás még felfedezetlen, nem publikált sebezhetőségét használják ki. A támadó a sebezhetőség felfedezését követően úgynevezett *zero-day exploit*ot készít, amely az a tényleges számítógépes kód, ami képes a sérülékenység kiaknázására. Azonban a sérülékenységek nehéz és bonyolult detektálhatósága miatt a kártékony programok készítői számára jelentős értéket képvisel egy újonnan felfedezett sérülékenység, ezért egy program általában csak egy sérülékenység kihasználására épül. Ezen támadások idején a megtámadott alkalmazás fejlesztőjének még többnyire nincs tudomása a sérülékenységről, vagy még nem tudott javítást készíteni hozzá.



1. ábra. A Stuxnet terjedése a belső hálózaton [9]

Származásáról nincsenek pontos adatok, de mindenki rögtön az Egyesült Államokra és Izraelre gondolt, mint olyan országokra, amelyeknek érdekében és módjában is állhatott az iráni atomprogram elleni akció. Ralph Langner hamburgi vírusbiztonsági szakértő blogjában mélyrehatóan foglalkozott a Stuxnettel és a 2010. december 31-i bejegyzésében az alábbiakat írta:

„Egy ilyen nagy horderejű támadás mögött feszülő hatalmas erőket elég könnyű érzékelni. A Stuxnet kártevő kifejlesztéséhez extrém mennyiségű hírszerzési adat kellett a dúsító mű elrendezéséről teljesen meg kellett érteni az IR-1[7] működését (amihez feltehetően rendelkezésre állt egy üzemképes tesztelő rendszer is), valamint a Siemens érintett termékeiről rengeteg bennfentes tudásra volt szükség. Mindez igen kevés szervezetre szűkíti le a világon azt a kört, amely a feladat megoldására vállalkozhatott.”[11]

Egy amerikai IT biztonsági szakértő azonban arra is rámutatott, hogy Oroszországnak is fűződhettek érdekei az iráni centrifugák elleni támadáshoz.[12]

Politikai szempontból nem tűnik logikai bakugrásnak, ha az iráni atomprogramba amúgy besegítő orosz tudósok révén Moszkva lassítani próbálja a teheráni eredményeket – amíg a program eredménytelen, az áttételes támogatás nem okoz az eddigieknél is súlyosabb problémát az orosz-amerikai diplomáciai kapcsolatokban, ráadásul a közreműködés során szerzett belső információk lehetővé teszik a Stuxnethez hasonlóan célirányos eszköz kifejlesztését.

Nem szabad elfelejteni azt sem, hogy a terrorfenyegetéssel nemcsak a nyugati világnak kell számolnia. Moszkva és Washington erőfeszítéseinek köszönhetően mára a két szuperhatalom készleteiből csak nagyon nehezen kerülhet atomfegyver készítésére alkalmas

[7] A pakisztáni P-1 urándúsító centrifuga iráni változatának a külvilág által adott neve

alapanyag szélsőséges csoportok kezére, azonban Irán egy sikeres atomprogrammal a lehetséges források közé emelkedhet, márpedig a csecsen felkelők, és szélsőséges iszlám csoportok az orosz nemzetbiztonságra is veszélyt jelentenek.

A cikk írója egyúttal arra is emlékeztet, hogy szimpla gazdasági érdekek is állhatnak az iráni atomlétesítmények elleni támadás mögött – amíg szükség van az orosz szakértelemre, a megrendelések is folyamatosan érkeznek majd. A szakértő szerint áttételesen az is ezt a forgatókönyvet igazolja, hogy a rosszindulatú kód visszafejtése közben kizárólag olyan nyomokat és utalásokat találtak, amik amerikai és izraeli fejlesztőket sejtetnek. Ráadásul orosz szempontból meglehetősen kényelmes volt, hogy még a végzetes atomkatasztrófa előtt egy fehérorosz cég felfedezte a Stuxnetet, ezzel időt adva az iráni mérnököknek a védekezésre.[12]

Minden esetre a Stuxnet elkészítéséhez szükséges tudás Oroszországban is rendelkezésre állt.

Még nem is sikerült teljesen megfejteni a Stuxnet minden részletét, amikor 2011 szeptemberében egy újabb rosszindulatú program vált ismertté. Felfedezése a Budapesti Műszaki Egyetem Híradástechnikai Tanszékén működő CrySyS Adat- és Rendszerbiztonság labor munkatársaihoz fűződik. A magyar szakemberek Duqu-nak nevezték el az új kártevőt, amely nagyon sok hasonlóságot mutat a Stuxnettel. Az elemzések szerint valószínűsíthető, hogy a Duqu készítői hozzáfértek a Stuxnet forráskódjához. Az nem tisztázódott, hogy a két program közül melyik volt előbb, vagy csupán egy közös tőről származó, azonban függetlenül fejlesztett kártevőkről van-e szó. Persze lehetséges az is, hogy a Duqu készítői csupán visszafejtették a Stuxnet kódját és egy ahhoz nagyon hasonlót írtak, hogy ezzel a gyanút másfelé tereljék. Még nem sikerült pontosan kideríteni, hogy mi is lehet az új kártevő feladata, de hála a gyors felismerésnek, már elkészült rá a védelem. Az eddig elfogott példányok feladata a megfigyelés volt, a központtól a kártevő letöltötte a megfelelő adatgyűjtő alkalmazást, majd az adatokat visszaküldte. A felfedezett esetekben az adatgyűjtés a számítógépen futó folyamatok listájára, képernyőmentésekre, hálózati felderítésre és billentyűzetfigyelésre terjedt ki.[13]

2012. májusában a budapesti CrySyS labor és vele egy időben a Kaspersky Lab felfedezett egy újabb rosszindulatú kódot, amelyet a magyarok sKyWipernek, a Kaspersky Flamernek nevezett el. Szintén felfedezhető volt a hasonlatosság a Stuxnet kódjával. Ez a malware is modul rendszerű, nagyon kifinomult eszköz, mely a moduloknak köszönhetően tevékenységét rendkívül széles skálán képes kifejteni. Néhány figyelemre méltó káros tevékenység:

- hálózat figyelés, hálózat felderítés, sérülékeny jelszavak gyűjtése
- a fertőzött rendszerek lemezeit átvizsgálja meghatározott programok és egyéb tartalmak után kutatva
- képernyőmentéseket készít, amikor bizonyos folyamatok vagy ablakok aktívak
- a számítógéphez csatlakoztatott mikrofonnal fel tudja venni a környezetben elhangzott zajokat
- a mentett adatokat az irányító szerverekre menti
- tíznél több C&C[8] szervert azonosítottak
- SSH és HTTPS protokollok segítségével kapcsolódik a C&C szerverekhez
- megkerüli a széles körben használt víruskeresőket és egyéb biztonsági szoftvereket
- Windows XP, Vista és Windows 7 operációs rendszereket támad
- képes nagyméretű helyi hálózatokat megfertőzni [14]

[8] Command & Control – olyan szerver, amely irányítja a kártevő tevékenységét

A CrySys Lab jelentésében kiemeli, hogy ez az eddig talált legkifinomultabb kártevő és kifejlesztése nagyon jelentős anyagi és szellemi ráfordítást igényelt, ami állami részvételre utalhat.[15]

2012 augusztusában egy újabb rosszindulatú szoftver tűnt fel. A Gauss névre keresztelt vírus elsősorban banki és egyéb hozzáférési adatokat gyűjt a fertőzött rendszerből, majd továbbítja azokat a Command and Control (C&C) szerverek felé. Egy biztonsági cég szerint a Gauss jelenleg elsősorban Libanonban, Izraelben és a Palesztin területeken aktív, de az Egyesült Államokból is jelentettek fertőzést. A káros szoftver elemzése során a szakemberek számos hasonlóságot fedeztek fel a Gauss és a Duqu, a Flame valamint a Stuxnet férgek között. A moduljait beilleszti különböző böngészőkbe, hogy lehallgassa a felhasználó munkamenetét, valamint, hogy onnan ellopja a tárolt jelszavakat, sütiket valamint a böngésző előzményeket. A jelentések szerint a hordozható adattárolókat fertőző információgyűjtő modul tartalmaz egy titkosított ”payload”-ot is, amely funkciója egyelőre ismeretlen. [16]

2013 januárjában a Kaspersky jelentette be, hogy leleplezett egy nagyarányú online kémkedési akciót. A vírusirtó cég által Vörös októbernek nevezett kártékony kód már 2007 óta volt aktív, főképp Kelet-Európában, a volt szovjet tagköztársaságokban, illetve Kelet-Ázsiában, de találtak fertőzött gépeket szerte a világon kormányszervezetekben, nagykövetségeken, kutatóközpontokban is. A vírus fő célja titkos dokumentumok megszerzése volt, de ezen kívül információkat gyűjtött a megfertőzött hálózatokról is. Ez a vírus is, akárcsak az előzőekben ismertetett kártevők, igen kifinomult és több, eddig ismeretlen metódust alkalmaz működése során. A terjedéséhez viszont régi, bevált módszereket, adathalász emaileket, fertőzött weboldalakat, a Word- és Excel sérülékenységeket használ. A program moduláris felépítésű, több mint ezer modult fejtettek vissza eddig. Az egyik érdekes modul például a fertőzött számítógépre csatlakoztatott okostelefonokról, illetve a gépre dugott pendrive-okról le tudja menteni az érdekesnek tűnő tartalmat, még a törölt fájlokat is vissza tudja állítani ezekről. A forráskód, illetve az ahhoz fűzött megjegyzések orosz programozók munkájára engednek következtetni. Persze az is elképzelhető, hogy ez csak az álcázás része, és az orosz, illetve programozói szlengben elterjedt kifejezésekkel csak félrevezetésből szórták meg az angol nyelvű megjegyzéseket a programsorok mellett.[17]

2013 februárjában a CrySys Lab és a Kaspersky közösen azonosított egy újabb kártevőt, amely 23 ország 59 célpontját támadta, főleg a diplomáciai körökben. A Miniduke-nak elnevezett program az Adobe Reader azóta már javított sérülékenységét használta ki, a kódot egy fertőzött pdf dokumentummal juttatták a kiszemelt számítógépre. Az egyik ilyen anyag például Ukrajna NATO csatlakozásának terveiről szól. A fertőzés után a vezérlőszerverekkel történő kommunikációra a Twittert használja a program. A szakemberek szerint a Miniduke egyedülálló alkotás. Még nem tudni, milyen adatokat sikerült a támadóknak megszerezniük.[18]

A fentebb említett kártevők megjelenése is mutatja, hogy a vírusok és különböző rosszindulatú programok készítői már nem kamaszok, vagy sértett informatikusok, akik a szobájuk mélyén gyártják ezeket a kódokat, mint régen. Ezen kódok írói komoly anyagi és szellemi háttérrel rendelkező fejlesztők, akik a szervezett bűnözés megbízásából dolgoznak vagy állami támogatással a jövő háborúinak fegyvereit készítik.

AZ ANONYMOUS CSOPORT

Az elmúlt időszakban szinte naponta lehetett olvasni az Anonymous csoport támadásairól. Ez a laza szerveződésű internetes közösség vélt, vagy valós sérelmek megtorlásául vagy egyszerűen valamely ügyet felkarolva indít támadásokat internetes tartalmak, cégek, kormányzatok ellen.

2. ábra. Az Anonymous logója
(forrás: http://en.wikipedia.org/wiki/Anonymous_(group) letöltve: 2011. december 02.)

Az Anonymous logója egy fej nélküli, babérkoszorúba foglalt öltönyös figura, tagjai pedig, ha utcára mennek vagy képet tesznek ki magukról a netre, akkor a *V, mint vérbosszú* című filmből ismert mosolygó Guy Fawkes maszkot viselik, amelyet annak főhőse hordott.

A közösség a 2003-ban alakult 4chan nevű képmegosztó oldal felhasználóiból verbuválódott. A kezdetben a japán képregények rajongóinak szóló oldal hamar nagy népszerűségre tett szert, tartalmában és stílusában azonban az internet sötét oldalához tartozik. A beszélgetések úgy általában a tizen-huszonéves internet, online pornó és videojáték-mániás amerikai fiatalok szellemi színvonalán zajlik, akik ebből ítélve az oldal törzsközönségét alkotják. Az obszcén tartalmairól és féktelen szabadosságáról ismert fórum, vagyis képes üzenő fala már kevesebb látogató számára érdekes és vállalható, de így is az internet egyik legnagyobb hatású oldala. Jellemző, hogy felhasználói a kortárs online popkultúra rengeteg fontos elemét termelték, termelik ki és dolgozzák fel újra folyamatosan. A 4chan mindezek ellenére, vagy talán épp ezért, az online tömegkultúra egyik termékeny alkotóműhelyévé vált, amelynek látogatói saját elvetemült humoruk és a Photoshop segítségével rengeteg internetes mémet, vagyis egy adott témára épülő, továbbküldés útján terjedő, folyamatosan remixelt műalkotást dobnak be a köztudatba. A 4chanról származnak például a lolmacskák, vagyis az internetes szlengben feliratozott vicces macskás képek. [19]

Ebből a közegből származik az Anonymus, melynek fontos eszköze a weboldalakat automatikus lekérdezésekkel megbénító túlterheléses támadás, amire magasztos hangnemben megfogalmazott webes szórólapjain toborozza a résztvevőket, rendszerint nem csak a 4chanon, hanem más csevegő szobákban és fórumokon is. A szaknyelven dosolásnak nevezett támadásokban való részvételhez nem is kell más, csak pár ingyenesen letölthető szoftver, amelyek beszerzéséhez, használatához a felhasználók rendszerint már a szórólapokon megkapják a szükséges instrukciókat. 2007-ben először így bénították meg a rasszista kijelentéseiről elhíresült amerikai rádiós, Hal Turner műsorát, noha a 4chanon mindennapos dolog a niggerezés vagy más népek, országok alpári stílusú pocskondiázása. A következő nagy támadás, amely hellyel-közzel a mai napig tart, a szcientológiai egyház ellen indult

2008-ban. Tiltakozásul az egyház által véleményük szerint elkövetett csalások, illegális tevékenységek, személyes szabadságok korlátozása miatt, kiterjedt támadásba kezdtek ellenük. [20] A szolgáltatásmegtagadásos támadásokon kívül nyilvánosságra hoztak több száz iratot és dokumentumot, amelyeket számítógépes betörések útján szereztek.

Saját meghatározásuk alapján tiltakoznak és fellépnek minden olyan jelenség ellen, amely a szólásszabadságot és az Internet szabadságát veszélyeztetik.

Ebbe belefért a Sony ellen indított támadás is, mely során több millió felhasználó adatait, köztük bankkártya számait lopták el és tették nyilvánossá azért, mert a Sony perbe fogta azt a hackert, aki feltörte a PlayStation védelmét.

A legnagyobb port felvert támadássorozatuk a Wikileaks támogatását megakadályozó amerikai intézkedések miatt következett be. Mint az ismeretes, 2010-ben a Wikileaks több ezer titkos amerikai diplomáciai és katonai iratot jelentetett meg az Interneten a szólásszabadság jegyében. Ez komoly diplomáciai feszültséget és még komolyabb biztonsági problémákat okozott, elsősorban az amerikai hadsereg műveleti területein. Az amerikai kormány komoly politikai nyomást fejtett ki az oldal ellehetetlenítésére, többek között a finanszírozásával kapcsolatban. A PayPal, a Visa vagy a MasterCard e nyomás hatására nem engedélyezte a Wikileaks számláira történő utalásokat. Ennek hatására hirdette meg az Anonymous a fenti pénzintézetek elleni támadássorozatát, amelyben sikerült is kisebb fennakadásokat okozni.

Létezik az Anonymous csoportnak magyar szárnya is, Facebook oldaluk is van, ahol a hitvallásukat is közzétették:

Anonymous vagyunk. Egy eszme vagyunk. A pénzügyi és politikai zsarnokság ellen küzdünk itthon és globális szinten, Egy emberibb világot akarunk, ahol nem a profit, a hatalom, az erőszak számít, hanem az igazság, a szabadság, az egyenlőség. Változást szeretnénk elérni: a tudás, az információ nyílt áramlását, a cenzúra eltörlését, a szűk, kapzsi elit uralmának a végét és a 99% valódi hatalmát. Közvetlen demokráciát, igazi beleszólást akarunk. A jelenlegi rendszer igazságtalan, embertelen és végpusztulás felé sodorja a civilizációt. Nincsenek vezetőink, nincsenek rendszabályaink, nincsenek bombáink, Sokan vagyunk, napról-napra egyre többen vagyunk. Légiót alkotunk. Nem felejtünk, nem bocsájtunk meg. Számolj velünk és számíts ránk! Csatlakozz hozzánk és legyél részese egy győztes forradalomnak![21]

Magyarországi tevékenységük weboldalak feltörésével kezdődött, 2012. március 4-én feltörték az Alkotmánybíróság honlapját és átírták az Alaptörvény szövegét, április 8-án a Nemzeti Rehabilitációs és Szociális Hivatal következett. Augusztus 28-án túlterheléses támadást intéztek a Közgép Zrt. honlapja ellen, amelyet sikerült is egy rövid időre megbénítani. Ennek az ügynek a kapcsán a rendőrség őrizetbe vett öt személyt, akik el is ismerték azt, hogy részt vettek a támadásban. Ellenük számítástechnikai rendszer és adatok elleni bűncselekmény megalapozott gyanúja miatt indítottak eljárást.[22]

A magyar Anonymous saját csoportjának méretét 50-60 aktív főre tesz, akik állandóan akcióra készek, valamint további 150-200 fő elkötelezett követőre.

Hosszan sorolhatnánk a csoport által elkövetett támadásokat, a világ szerzői jogvédő hivatalaitól az arab tavasz támogatásán át a világméretű pedofilhálózat feltöréséig.

Céljaik néhány esetben támogathatók ugyan, de a módszereik veszélyesek és egyértelműen törvénytelenek. Nincsenek nevesített vezetőik, szervezetük decentralizált és tagjaik a világ minden részén megtalálhatók. Az, hogy milyen célpontot támadnak sikeresen, attól is függ, hogy mennyi támogatót tudnak megnyerni maguknak.

Ha a dolgok mögé nézünk, az a víziónk támadhat, hogy ha valaki a megfelelő időben, megfelelő módon tudná befolyásolni ez a világméretű közösséget, akkor nagyon komoly károkozásra lehetne képes, legyen az akár terrorista, akár egy ország.

KÖVETKEZTETÉSEK

Cikkemben be kívántam mutatni, hogy az elmúlt néhány évben milyen fejlődésen ment keresztül az informatikai támadások metodikája.

Mint azt a fenti példák mutatják, az számítógép-hálózatok elleni támadások egyre jobban beépülnek a hagyományos konfliktusok eszköztárába. Az, hogy a konfliktusokban részt vevő felek még nem ismerik el a felelősségüket a kibertámadásokban, az annak köszönhető, hogy nem akarják az ilyen irányú képességeiket a világ elé tárni. Mindenki számára nyilvánvaló, hogy például Oroszország rendelkezik azokkal a képességekkel, amelyekkel az észtországi vagy a grúziai támadásokat kivitelezhették, azonban a „hazafias hacker-csoport" teória remek fedőtörténet az események magyarázatára. Kínában, ahol nagy súlyt fektetnek a hadsereg számítógép-hálózati műveleti képességének fejlesztésére, szintén az országban működő hacker csoportok tevékenységével magyarázzák az amerikai és európai kormányzati, katonai célpontok elleni kínai szerverekről érkező támadásokat. Nehéz azonban elképzelni, hogy a több ezer kiképzett katonai hacker csak gyakorlatozik a laktanyákban, miközben néhány fekete kalapos támadó ilyen kiemelt fontosságú célpontokat támad. Tisztában kell lennünk azzal, hogy a világ számos hadseregében lázasan készülnek a kiberhadviselésre és nem csak a védekezésre, hanem a támadásra is.

A rosszindulatú programok készítésében is megfigyelhető az ilyen irányú fejlődés. A fent bemutatott programok kifejlesztése már olyan infrastruktúrát és magasan képzett programozók összmunkáját feltételezi, amely mögött kormányzatokat kell sejtenünk. Felvethető még a szervezett bűnözés tevékenysége is, azonban számukra a pénzszerzés a fő motívum, vélhetően nem keveredtének olyan ingoványos talajra, mint a katonai titkok fürkészése, főleg nem az Egyesült Államok kárára. Az utóbbi idők történései azt látszanak bizonyítani, hogy a hírszerzés egyre jobban kiterjed a kibertérre, mindenki igyekszik kifürkészni a riválisországok kritikus informatikai infrastruktúráját, megismerni a számítógépeken őrzött katonai, diplomáciai, pénzügyi, ipari titkait. A Stuxnet-tel pedig már a kiberfegyver is elkészült, amellyel fizikai károk is okozhatók. Úgy vélem, nem nehéz a jövőt sem megjósolni. Egyre kifinomultabb rosszindulatú szoftverek fognak születni és ezek egy jelentős részét csak akkor fogja megismerni a világ, amikor már egy éles, háborús helyzetben használták őket. Nincs kétségem afelől, hogy számos ország rendelkezik már ilyen fegyverrel és egy adott helyzetben használni is fogják őket.

Néhány évvel ezelőtt egy konferencián az egyik előadó azt mondta, hogy a kiberháború nem fog kitörni, hanem már folyik. Az elmúlt idők eseményeit nézve ez bizony nagy igazság. Az igazi kérdés az, hogy az egyes országok mennyire tudják majd megvédeni magukat az interneten keresztül érkező támadásokkal szemben.

Nem szabad félvállról venni a különböző hacktivista csoportokat sem, amelyek bizonyos célok mellé felsorakozva nagyon komoly erőt jelenthetnek. Ha például az Anonymous tagjait sikerülne meggyőzni érvekkel vagy akár megtévesztéssel egy kibertámadás támogatására valamely kormányzatnak vagy érdekcsoportnak, komoly segítséget jelentenének a sikerhez. Természetesen ez fordítva is igaz lehet, ha a célpont ország tudná segítségül hívni őket, jelentősen javíthatna az esélyein.

Ezek ellen a fenyegetések ellen ki kell építeni a megfelelő védelmi rendszereket minden olyan országnak, amely fejlett információtechnológiával rendelkezik, így hazánknak is. Az ilyen védelem kiépítésénél számításba kell venni a köz és magánszféra erőforrásait is. A kritikus infrastruktúrák védelme mellett azonban létre kellene hozni egy ütőképes, jól felkészült egységet is, amely sikerrel tudna számítógép-hálózati műveleteket bonyolítani, legyen szó védekezésről vagy megelőző csapásról. A nemzetközi példákat alapul véve ezt a szervezetet a Magyar Honvédség kötelékében lenne célszerű kialakítani. Ezáltal hadseregünk egy újabb, akár a NATO számára felajánlható képességgel is gyarapodhatna.

Felhasznált irodalom

[1] A hálózati társadalom sérülékenysége
http://www.nato.int/docu/review/2002/issue2/hungarian/features2.html
(letöltve: 2012. október 12.)

[2] Haig Zsolt – Kovács László: Fenyegetések a cybertérből, Nemzet és biztonság. I. évfolyam, 5. szám. Budapest, 2008. május, pp.: 61-69 ISSN 1789-5286

[3] Steve Kettmann: Soviets Burned By CIA Hackers?
http://www.wired.com/culture/lifestyle/news/2004/03/62806
(letöltve: 2012. október 12.)

[4] Kovács László: Információs hadviselés kínai módra, Nemzet és biztonság II. évfolyam 7. szám. Budapest 2009. szeptember pp.: 35-44, ISSN 1789-5286

[5] Németh József, Hajzer Tamás: Az orosz-grúz háború néhány jellemző vonása
http://www.biztonsagpolitika.hu/?id=16&aid=709&title=Az_orosz-grúz_háború_néhány_jellemző_vonása, (letöltve: 2012. október 12)

[6] Az Interneten kis zajlik az orosz-grúz összecsapás
http://www.origo.hu/techbazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html (letöltve: 2012. október 12.)

[7] Jeremy Norman: The First Computer Virus
http://www.historyofinformation.com/expanded.php?id=2860
(letöltve: 2013. január 25.)

[8] Berzsenyi Dániel, Szentgáli Gergely: STUXNET: a virtuális háború hajnala
http://www.biztonsagpolitika.hu/index.php?id=16&aid=932
(letöltve: 2012. október 12.)

[9] Kovács László, Sipos Mariann: A stuxnet és ami mögötte van
Hadmérnök V. évfolyam 4. szám Budapest, 2010. december pp.:163-172,
ISSN 1788-1919

[10] Cserháti András: A Stuxnet vírus és az iráni atomprogram, Nukleon IV. évfolyam 1. szám Budapest 2011 március p.:85, ISSN 1789-9613

[11] Ralph Langner hamburgi vírusbiztonsági szakértő blogja,
http://www.langner.com/en/blog/page/5/

[12] Panayotis A. Yannakogeorgos: Was Russia Behind Stuxnet?
http://the-diplomat.com/2011/12/10/was-russia-behind-stuxnet/?all=true
(letöltve: 2012. október 12.)

[13] Symantec Security Response: W32.Duqu The precursor to the next Stuxnet
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdff (letöltve: 2012. október 22.)

[14] Flamer/sKyWIper – egy újabb veszélyes kiberfegyver bukkant fel,
http://tech.cert-hungary.hu/tech-blog/120529/flamerskywiper-egy-ujabb-veszelyes-kiberfegyver-bukkant-fef (letöltve: 2012. október 22.)

[15] sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks
http://www.crysys.hu/skywiper/skywiper.pdf (letöltve: 2012. október 22.)

[16] Újabb taggal bővült a Stuxnet család
http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad (letöltve: 2012. október 22.)

[17] „Red October" Diplomatic Cyber Attack Investigation
http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (letöltve: 2013. január 20.)

[18] The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor,
https://www.securelist.com/en/blog/208194129%20The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_Micro_Backdoor (letöltve: 2013. február 28.)

[19] Vámosi Gergő: A kretének háborúja zajlott az Interneten,
http://www.origo.hu/techbazis/20101117-a-4chan-a-tumblr-ellen-a-kretenek-haboruja-zajlott-az.html (letöltve: 2012. október 22.)

[20] Anonymous vs. scientology,
https://whyweprotest.net/anonymous-scientology/ (letöltve: 2012. október 22.)

[21] Az Anonymous Operation Hungary adatlapja a Facebook-on,
https://www.facebook.com/OpHunAnon/info (letöltve: 2012. október 22.)

[22] Dajkó Pál: Elfogták a Közgépet megtámadó Anonymous-szimpatizánsokat,
http://itcafe.hu/hir/orfk_anonymous_kozgep.html (letöltve: 2012. október 22.)