NAGY ZOLTÁN ANDRÁS

A KIBER-HÁBORÚ ÚJ DIMENZIÓ – A VESZÉLYEZTETETT ÁLLAMBIZTONSÁG

(Stuxnet, DuQu, Flame – A Police malware)

Az Internet, amelyet a katonai kutatás hívott életre[375], alapvetően a kommunikáció célját szolgálta, ám a gyors technikai fejlődés eredményeként számtalan további lehetőséggel bővült. Mind a szervezett bűnözők, mind annak egy lényegesen veszélyesebb válfaja a terroristák is élnek ugyanazok technikai lehetőségekkel, mint más felhasználók, csak éppen azokat saját nemtelen céljaikra fordítják.[376] Visszaélnek a szabadság és határok nélküliség adottságával.[377] Hamis vagy azonosíthatatlan IP-címekről kommunikálnak, kép-, szöveg vagy bármely más fájlba rejtett üzeneteket küldözgetnek, töltögetnek egymástól (pl. jelszóval védett FTP- hálózatokról), tagokat toboroznak tevékenységükhöz chat-szobákban[378] vallási-politikai propagandát folytatnak szöveges-, audio és videó elérhetőséggel, kábítószert-, hamis árukat-, termékeket forgalmaznak, illegális szerencsejáték-oldalakat üzemeltetnek, pénzt mosnak[379] tisztára alapítványokon, legális vagy illegális szerencsejáték oldalakon keresztül.[380]

A kommunikáció technikája megteremti azt a lehetőséget is, hogy a felhasználók egymás számítógépeivel közvetlen kapcsolatba lépjenek (P2P), fájlokat küldözgessenek és töltögessenek le egymástól. A letöltött fájlok tartalmukban szerzői alkotások, ezen belül pl. programok is lehetnek, amelyek a felhasználók a maguk céljára, örömére, hasznosnak tartva telepítenek számítógépükre.

Ezt az adottságot használják fel arra, hogy egyéni vagy szervezett bűnelkövetők súlyos károkozó programokat terjesztenek.

---

[375] Az Internet (Internetworking System – hálózatok hálózata rövidítés). A szovjet szputnyik 1957-es sikeres fellövését követően kitört az USA-ban az ún. „szputnyik-sokk". Ezt ellensúlyozandó, többirányú fejlesztésbe kezdtek. Ezek egyike volt az, hogy a hadserege vezetésének megbénítását megakadályozandó, több vezetési pontot alakítottak ki. Ezeket földalatti kábellel kötöttek össze. Majd egyre több katonai és civil kutatóintézet és egyetem csatlakozott a hálózatra, míg végül szétvált a katonai és civil hálózatra, amely utóbbit 1993-tól lehet szabadon használni.

[376] Organised Crime in Europe: the threat of cybercrime. Council of Europe – Octopus Programme, Strasbourg, 2005. 161-170. o.

[377] Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012. 6. szám 108-125. o.
Korinek László: Kriminológia II. Magyar Közlöny- Lap és Könyvkiadó, Budapest, 2010. 310. o.
Papp Péter: Hi-tech bűnözés napjainkban. Belügyi Szemle, 2011/11-12. 5. o.
Anamaria Cristina Cercel: Criminologie. Editura Hamangiu, 2009. 101. o.

[378] Kevin Mitnick – William L. Simon: A behatolás művészete. Perfect Kiadó. Budapest, 2006. 27-58. o. Kevin Mitnick a legendás hacker, aki évekig vezette az cyber-crime körözési listákat, háromszor is elítéltek, írta meg tapasztalatait, történeteit két magyarországi kiadású könyvben.

[379] Gál István László: A pénzmosás és a terrorizmus finanszírozása. In: Korinek László – Kőhalmi László – Herke Csongor (szerk.): Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. PTE ÁJK, Pécs, 2004. 39. o.

[380] A témáról részletesen: Nagy Zoltán: Bűncselekmények számítógépes környezetben. Ad Librum. Budapest, 2009.

A malware – támadásokról általában

A malware kifejezés valamilyen rosszindulatú programot jelent, amely a malicious software angol szavak összetételéből származik. Összefoglaló elnevezés, amely a számítógépes munkafolyamatot, elektronikus adatot, a számítástechnikai eszközöket károsító programokat felöleli.

Néhány ismert program típusú malware:

- Napjaink újdonsága a Stuxnet (sztaksznet), DuQu (duku) – típusú malware-ek, amelyek célzott technikai – technológiai folyamatok megbénítására, azok károsítására alkalmas programok. Újdonságuk, veszélyességük okán erről részletesebben később külön szólunk.
- A számítógépvírusok és programférgek különböző károsító programok, amelyek adatállományok, programok, hardver ellen irányulnak. Hatásuk sokféle, pl. adatállományokat törölnek, programokat bénítanak meg. A Stuxnettől és DuQu-tól eltérően hatásuk általános, azaz minden számítógép, számítástechnikai rendszer esetében azonosak.
- A trójai - program egy másik programhoz kapcsolódik. Az eredeti program indításakor a felhasználó tudta és akarata nélkül aktiválódik (pl. egy letöltött játék-programmal egy zombi-programot is telepítünk gépünkre – ennek további veszélyéről lásd a (D)DoS-támadások elemzésénél visszatérünk). A trójai-programok alkalmazásának elterjedtségére utal az, hogy 2011-ben az ismert malware-ek 73%-a trójai-program volt,[381] nyilván összefüggésben a növekvő (D)DoS-támadásokkal.
- A backdoor - programok pedig a számítógép védelmi rendszerén nyitnak utat egy másik rosszindulatú program számára.
- A dialer program a telefonhoz modemen keresztül kapcsolódó számítógépeknél hatásos. A betárcsázó-program a számítógép indításakor a felhasználó tudtán kívül egy emelt-díjas számot hív akár folyamatosan. A hóvégi telefonszámla kifizetésekor szembesül a felhasználó a magas költséggel.
- A spyware-ek (kémprogram általános elnevezéssel) a felhasználó aktivitását (a számítógép-, és Internethasználatunkat is) rögzíti, jelszavainkat, más ránk vonatkozó adatot fürkész ki és továbbítja egy másik számítógép számára a hálózaton. Részben hírszerzési célokat, részben marketing-célokat szolgálnak. Ez utóbbi esetben (természetesen) nem a nagy vagy hivatalos marketing-cégek terjesztik, de a mások által gyűjtött „információkat elfogadják" (megvásárolják).
- A keylogger-programok speciális kémprogramok, ami billentyű-leütéseinket rögzítő, naplózó kémprogram. Tipikusan a begépelt szöveg kifürkészése a cél.
- Flame (fléjm) – program, napjaink újabb kémprogram fejlesztése. Tulajdonképpen egy multi-kémprogram, mindenre kíváncsi. Napjainkban az arab világban terjed.
- Egyéb kártékony programok.

[381] Forrás: http://press.pandasecurity.com/news/pandalabs-q1-report-four-out-of-five-new-malware-samples-are-trojans/ (Letöltés ideje: 2012. 05. 25.)

Néhány ismert szöveg típusú malware:

- A *spam*[382] kéretlen kereskedelemi küldeményeket jelent (hirdetések, semmire sem jó felmérések stb.). Sajnos, milliószámra terjednek számítógépes hálózatokon, foglalva az e-mailek memóriáját, használva a rendszergazdák drága munkaidejét, idegesítve felhasználókat a spam-ek törlésével.
- A *hoax-levelek* általános, gyerekes szövege, a felhasználó babonás félelmére apellál, hogy „küldd tovább xy.. példányban, mert … balszerencse ér."

Léteznek azonban további tipikus lánc-levelek a

- Magyarországi felhasználókhoz is eljutott *holland és spanyol lottónyer*eményekről értesítő levelek, amelyekben személyes adatainkra (többek között bankkártyánk adataira) kíváncsiak, mert a „nagy összegű nyeremények átvételéhez bizonyos (ügyvédi, ellenőrzési, átutalási stb.) költségeket kell előlegezni. A felhasználó könnyelműségét bankszámlája bánhatja.
- A *nigériai,* újabban *iraki levelek,* amelyekben arról értesítik a hiszékeny felhasználót, hogy a korábban a hatalmuktól megfosztott vezetők, kizártakat, kivégzetteket rehabilitálták, sőt visszakaphatják vagyonukat is, ám ennek költsége van, és ha a felhasználó megelőlegezné vagy beszállna a költségekbe, akkor azt többszörösen fogják majdan számára visszatéríteni stb. A további metódus ugyanaz, mint a holland- vagy spanyol lottó esetében (adatkérés, bankszámla kiürítés).
- A *phishing* (fising) magyarul adathalászat. Jellemző megvalósulása az, hogy a gyanútlan felhasználó kap egy e-mailt, amelyben arról értesítik, hogy például „bankja számítógéprendszerének karbantartása zajlott és kérik a felhasználót, hogy tekintse meg bankszámlájának adatait…" Az e-mailben mellékelt linkre kattintva megjelenik az eredeti banki oldalhoz megszólalásig hasonló web-oldal. A felhasználó – a szokásos módon, azonosítója, jelszava – és itt jön egy újdonság, amire nem figyel a felhasználó - telefonszámát begépeli (és ezzel elbúcsúzhat a bankszámláján levő összegtől). A hamis web-oldalról továbblépve jellemzően egy üres web-oldalra ér, amelyen azt olvashatja, hogy a (nem létező) karbantartás tovább tart, de akkorra már a bankszámlája eléréséhez szükséges valamennyi adatot a csalók rendelkezésére bocsátotta, és legvalószínűbb, hogy bankszámlája látja kárát gyanútlanságának. Az e-mailes adathalászat megjelent már más platformon is, így mobil-telefonon szóban vagy sms-ben is.[383]
- A police malware szintén napjaink újdonsága. Elöljáróban annyit veszélyességéről, hogy már 13 európai országban észlelték.[384] Erről később részletesen.
- Egyéb, szöveges típusú kártékony tartalmak.

[382] Sütő János: SPAMtelenül. SZAK Kiadó, Budapest, 2008. 3-9 o.

[383] Nagyon fontos lenne a képzés, tanítás, mert a hamis web-oldal némi tudással felismerhető pl. hiányzik az általában oldal jobb alsó sarkában levő titkosításra utaló „lakat" vagy más jelzés. A valódi banki belépést jelölő oldalak „https" (titkosított belépés portját jelöli) kezdődnek, és biztos, hogy a bank domain – nevéhez kapcsolódó al – domain – névvel azonosítható. Nélkülözhetetlen az a pénzintézeti propaganda, amely nem győzi hangsúlyozni, hogy e-mailben nem kérnek semmiféle azonosításra alkalmas adatot az ügyféltől. Sajnos, egyetlen érintett bank Internetes oldala mutatja be a valódi és a hamis web-oldal közötti különbséget.

[384] http://pcforum.hu/hirek/13949/Gyermekpornoval+zsarolja+aldozatait+egy+uj+interneten+terjedo+virus.html (Letöltés ideje: 2012. 05. 25.)

A hetvenes években csupán szakmai körökben "suttogtak" róla, de a nyolcvanas években már a szélesebb szakmai körökben tért hódított egy új fogalom, a vírusprogram.[385] A fogalom eredete az orvostudomány hasonló kategóriájából származott. Ugyanis a komputervírus szintén egy gócpontból kiindulva "fertőzi meg" az adatállományokat, programokat. A sajtóban e vírusokról pusztító hatásuk miatt "számítógépes AIDS-nek" valamint "delírium digitalis-nak" vagy hasonló hangzatos elnevezésekkel találkozhattunk.

Az első vírusok egyikét, az Elk Clonert egy 15 éves gyermek alkotta meg. Azóta a vírusok, és más malware-programok százezrei keringenek a számítógépes hálózatokon.

Amíg nem terjedt el a számítógépes hálózat, addig a malware-ek off-line feltöltése volt lehetséges. A hálózatok terjedésével ez ma már háttérbe szorult, de előfordulhat, sőt - ahogy majd látni fogjuk – a Stuxnet esetében szükségszerű volt az off-line feltöltés.

Jellemzői:

- körülményes, lassú
- fizikailag (erőszakkal, fenyegetéssel, megtévesztéssel) hozzá kell férni a célzott számítógéphez.

Technikai háttere:

- külső adathordozó útján terjeszthető,
- a malware-t (is) vivő adathordozó (pl. a különböző méretű hajlékony lemez[386]) sérülékeny (lehet), - ez kockázat,
- a malware-program önállóan vagy más (pl. kölcsönkapott, illegálisan letöltött) programmal települ, telepítik a felhasználó számítógépére.

Hatása:

- ha aktiválják a programot számítógép adatállományában, programjában okoz kárt és
- a malware a rá jellemző, ugyanazt a károsítást, hátrányt stb. okozza minden megfertőzött számítógépben.

A feltöltő:

- a célzott számítógép megfertőzését kívánja (egyenes szándékkal) vagy ebbe belenyugszik (eshetőleges szándékkal),[387] de nem kizárt
- a vétlenség vagy gondatlanság (bármely alakzata) sem kizárt (nem tud arról, hogy a kölcsönadott program tartalmaz malware-t).

A felhasználó:

- viszont vétlen vagy gondatlan számítógépe megfertőzésében.

Ezzel szemben a számítógépes hálózaton terjesztett, onnan letöltött malware-ek esetében on-line feltöltésről beszélhetünk:

Jellemzője:

- gyors és egyszerű a letöltés,

[385] A kezdetekről részletesen: Kis János – Szegedi Imre: Vírushatározó. Alaplap Könyvek 4. Cédrus Kiadó. Budapest, 1992

[386] A 3,5 inches méretű hajlékonylemez a magyar Jánosi Marcell remeke, sajnos nem Magyarországé lett a találmány dicsősége (mint annyi másban).

[387] Btk. 13. § *Szándékosan követi el a bűncselekményt, aki magatartásának következményeit kívánja, vagy e következményekbe belenyugszik.*
14. § *Gondatlanságból követi el a bűncselekményt, aki előre látja magatartásának lehetséges következményeit, de könnyelműen bízik azok elmaradásában; úgyszintén az is, aki e következmények lehetőségét azért nem látja előre, mert a tőle elvárható figyelmet vagy körültekintést elmulasztja.*

- nem szükséges a fizikai hozzáférés a számítógéphez.

Technikai háttere:

- számítógépes hálózaton keresztül pl. warez-oldalakról, P2P hálózatokról keresztül letöltésre,
- különböző web-helyekről illegálisan letöltött tömörített fájlokban, továbbá .exe (esetleg .com) alkalmazásokban, e-mailhez csatolt fájlban, vagy egyetlen e-mailes linkre kattintással,
- egy-egy kommersz, ismert vírus ellen a védekezés relatíve nem nehéz a vírusirtó programok, vagy azok frissített változata felismeri és így el lehet távolítani azokat.

Hatása:

- a mai malware programok hatása sokféle, károsító lehetőségük gyakorlatilag korlátlan képet mutat,
- a vírusra jellemző általános (ismert) károkat okoz, tehát minden számítógépen ugyanazokat a károsító hatásokat idézheti elő,
- ha a felhasználó - online módon - számítógépére tárolt fertőzött programot, szoftvert vagy egyéb fájlt telepít, akkor a malware a fertőzött számítógépről letöltők számítógépeiben is kárt okoz.
- A sértettek száma megbecsülhetetlen. Attól függ, hogy hányan töltik le a malware-programot és telepítik számítógépeikre.

A feltöltő:

- a vírus feltölthető más személy számítógépébe történő illetéktelen behatolást követően megkívánja fertőzni a célzott számítógépet (egyenes szándékkal) vagy
- a letöltő felhasználók ezreinek, milliói számítógépének fertőzésébe belenyugszik (eshetőleges szándékkal).

Letöltő:

- a számítógép felhasználója vétlenül vagy gondatlanul tölti le és terjesztheti szándékosan, gondatlanul vagy vétlenül.

Az áldozattá válás véletlenszerű. Bárki letöltheti a vírusprogramot és a letöltők egy része aktiválja (indítja a letöltött programot, kibontja a tömörített fájlt), míg mások nem teszik meg.

A Stuxnet-, DuQu - támadások

A Stuxnetet és DuQut azért kell külön kezelnünk, mert eltér az eddigi malware-ek tulajdonságaitól, és ez veszélyességüket rendkívül megnöveli. Egyfelől, míg az ún. nulladik napi támadást követően a malware-ek hatásmechanizmusa ismert lesz, így az ellenük kifejlesztett vírusirtó programok is hamarosan megjelennek – és legálisan vagy illegálisan – hozzáférhetők. Egy „macska - egér harc" folyik, ismertté válik egy általános jellemzőkkel bíró (valamennyi fertőzött számítógépen ugyanazon károkat okozó) malware, majd megjelenik ennek az ellenszere. A Stuxnet és a DuQu egyedi, célzott hatása miatt nem valószínű, hogy lesz általános ellenszere (felismerés, irtás). Másfelől, míg a kommersz malware-ek hatása ismert, addig ennek a két új malware csak egyetlen célba vett technikai - technológiai vagy más művelet megbénítására alkalmas.

Kiszámíthatatlan, hogy egy energetikai-, honvédelmi-, pénzügyi stb. rendszerben mely folyamatot vették célba és annak milyen hatása lesz, hogyan mutálódik majd a

malware, az elektronikus adatfeldolgozás- és átvitel mely pontján, mikor és ki fogja feltölteni a malware-t.

Ha megnézzük történetüket, akkor megértjük veszélyességüket. Egy igazi kémtörténetet olvashatunk, amelyhez hasonlót még az elmúlt évtizedek James - Bond-filmjei sem produkáltak. 2010. szeptember 25-én Irán beismerte, hogy natanzi atomerőműjében technikai problémák felmerültek. Az erőmű nukleáris centrifugáiban mechanikai hibák keletkeztek. Az irániak a centrifugákat kicserélték, és felfedezték azt a malware-t, annak mutálódott formáját, amely a centrifugák abnormális működését előidézte. Ma már – nem megerősített, de nem is cáfolt forrásból – tudjuk, hogy Bush és Obama elnökök utasítására amerikai és izraeli szakemberek alkották meg ezt a malware-t.[388] A cél az iráni atomprogram akadályozása, megbénítása.[389] Az akció fedőneve: „Olympic Games" (olimpiai játékok).

Mivel az atomerőművet állig felfegyverzett katonák védik, kérdésessé vált, hogy egy fegyveres, katonai akció meghozza-e a kívánt eredményt. Kockázatok sorával kellett és kell számolnia az izraeli hadvezetésnek az iráni atomerőművek megtámadásával pl. 1800 km-es távolság áthidalása, katonai veszteségek, nemzetközi közvélemény negatív viszonyulása, gondoljunk arra, hogy az Európai Unió is óvatosabb az iráni atomkísérletek megítélésében, továbbá egy azonnali, nyílt bosszú Iránt ól vagy Irán-barát terrorista csoportoktól a világ bármely pontján, bármikor izraeli, egyesült államokbeli polgárok (turisták, sportolók) ellen. Megoldandó feladat volt, hogy az atomerőmű belső informatikai hálózata off-line üzemmódban működött, működik, azaz nincs kapcsolata az Internettel. Bármilyen malware feltöltése csak a helyszínen lehetséges. Továbbá, az atomerőmű vezérlése rendkívül bonyolult feladat.

Mint, minden akció első lépése: a cél felderítése. Milyen technológiával működik, milyen hardver és szoftver erőforrásokkal rendelkezik az iráni natanzi atomerőmű. Ez egy hagyományos hírszerzői feladat. A megszerzett információk birtokában a cél eldöntetett: azoknak a centrifugákat kellett tönkretenni, amelyek gyors és folyamatos forgásuk révén az uránban levő 235 jelű hasadó izotóp részarányát növelik. (Egy atombomba elkészítéséhez 1000 centrifuga működése szükséges egy éven át.) Natanzban 8000 centrifuga működött.

Az „Olympic Games" hadművelet már ismert (vagy kikövetkeztethető) elemei:

a) A malware bejuttatását a számítógépes rendszerbe megkönnyítette a Windows akkori felhasználóbarát, kényelmi funkciója, ami a számítógéphez csatlakoztatott adattárolókat automatikusan betöltötte. [390] A feltöltés a fenti források szerint egy USB pendrive-on keresztül történt.[391]

---

[388] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all [2012.05..25.]

[389] Többféle módon kívánták az iráni atomprogramot lassítani, bénítani, pl. az Irán által rendelt alkatrészeket harmadik országban titokban „megbuherálták", sőt 2008-ban egy malware-rel is próbálkoztak. Talán ez a próbálkozás „altatta el" az irániakat, hogy kétszer nem lépnek ugyanabba a folyóba. De léptek, sőt sokkal agyafúrtabban.

[390] A külső adathordozó behelyezésével az azon levő programok „azonnal" indulnak. A Windows az adathorodzón észleli az autorun.inf fájlt, amely tartalmazza azt a következő lépést, amelyet a számítógépnek végre kell hajtania.

[391] A feltöltésnek még számos megoldása lehetett volna, pl. a kábelrendszer megcsapolása vagy akár a világban „keringtetve", a célzott személyekhez eljuttatva, akik majd adathordozóikon eljuttatják a végcélhoz. Ne feledjük, hogy a Stuxnet csak az adott környezetben, azt felismerve funkcionált, más környezetben passzív maradt.

b) A Stuxnetnek az operációs rendszerbe kellett beépülnie. A Windows alapú operációs rendszer – természetesen - „nem enged be" bármilyen programot, csak olyat, amely a Microsoft által elismert digitális aláírással rendelkezik. Ez volt a következő feladat olyan digitális aláírással ellátnia stuxnetet, ami a Windows számára elfogadható. Állítólag Tajvanon és állítólag lopással szerezték meg a Microsoft által is elismert JMicron és a Realtek cégek digitális aláírását. Mára egyébként ezeket a digitális jeleket érvénytelenítették. (Mondhatott volna-e mást a tajvani cég, mint azt, hogy lopás történt?)
c) A natanzi atomerőmű centrifuga vezérlőit egy Siemens WinCC program irányította, irányítja. Ehhez szoftverhez a villanymotort vezérlő eszközök csatlakoztak. Az ezek közötti kapcsolatot biztosító Step-7 nevű illesztőprogramba a Stuxnet „adminjogokkal" (adminisztrátori, azaz rendszergazda jogokkal) beépítette saját moduljait. A Stuxnet villanymotort és a centrifugavezérlők közötti kapcsolatba épült be. (Ma már lényegtelen, ám korántsem lényegtelen kérdés, honnan szereztek a Siemenshez „adminjogokat"?)
d) A Stuxnetet úgy kellett megírni, hogy más rendszerekben, funkciókban nem tehessen kárt, hiszen ez a főcélt veszélyeztette volna, másrészt felfedezését megkönnyítette volna. Célzottan a centrifugák működésének megzavarására alkották meg. A vírus hatása (feladata) a centrifugák rotorjai forgási sebességének lelassítása majd felgyorsítása volt. Először 86400 fordulat/perc-re gyorsította fel, amely olyan komoly rezonanciát keltett, ami tönkretette a centrifugát, majd a rotorokat lelassította, 120 fordulat/percre, amitől a centrifuga szinte leállt, aminek következtében a szétválasztott gáz ismét összekeveredett benne. Majd ismét felgyorsította, aztán ismét lelassította, és így tovább.

Mire felfedezték a vírust, addigra mutálódása révén három különböző verzió futott az atomerőmű számítógépein. 2009-2010-ben kétezer centrifugát kellett kicserélni az irániaknak. 2010 szeptemberére sikerült a vírust kiirtani az erőmű számítógépéről. Hogy mennyi késedelmet szenvedett a dúsítás? Legfeljebb bennfentesek ismerhetik a bizonytalan választ. Az hogy, folytatódott-e, folytatódik-e kiberháború az iráni atomlétesítmények nem tudjuk, nem tudhatjuk. A konferencia előtti napokban látott napvilágot az a hír, miszerint Irán leleplezett egy kiber-támadást, amelyet az USA, Izrael és Nagy-Britannia intézett iráni létesítmények ellen. De, hogy van-e alapja vagy nincs a bejelentésnek, indok-e egy későbbi megtorló akcióhoz, azt csak az érintettek ismerhetik.[392]

Az „Olympic Games" – Stuxnet – akció értékelése:

Az akciót eredményesnek tekinthetjük. Iránt bizonyíthatóan visszavetetette – állítólagos - atombomba előállításában, viszonylag békés körülmények között. Bár a terrorista – támadások oka, revansa mindig kétséges.

A Stuxnet negatív hatása:

Érdekeség kedvéért: egy kereskedelmi forgalomban kapható K…n márkanevű mini pendrive mérete: mindössze 3,9 cm x 1,235 cm x 0,455 cm és 3 gramm. Speciális célra nyilván kisebbek is alkothatók, amelyek beépíthetők golyóstollba, karórába, kulcstartóra rögzített kabalatárgyba, emblémába, sőt akár lemezes öv csatjába stb.

[392] Forrás:
http://www.hirado.hu/Hirek/2012/06/21/21/Teheran_azt_allitja_hogy_sulyos_informatikai_tamadast_leplezett.aspx (Letöltés ideje: 2012. 05. 25.)

Az első és legveszélyesebb az, hogy ismertté válásával „közkinccsé vált”. Elemei kikerültek a „szabadpiacra”. Ismertté váltak más a Stuxnethez hasonlító mechanizmusokat tartalmazó malware-ek.

A DuQu programot egyébként a Budapesti Műszaki és Gazdaságtudományi Egyetem CrySyS Adat- és Rendszerbiztonsági Laboratóriumának kiváló csapata fedezte fel és publikálta először az Interneten.[393]

Ma is – nyilván – sok szakértő, intézet vizsgálja szerte a Világban, hogy a vajon Stuxnetnek a DuQunak ugyanazok voltak-e a készítői? Erre a megállapításra következtetni(ne) lehet a program közös elemeiből, logikai vázából, továbbá, hogy melyik malware készült el előbb, és azt, hol készítették.

Hipotetikus továbbá az, hogy a DuQu 2008-as első Irán elleni támadáskor alkalmazott malware kísérleti példányának továbbfejlesztett változata-e vagy sem?

1) Feltétlen figyelmet érdemel az, hogy a Stuxnet és DuQu programok példái annak, hogy célzott technikai-technológiai folyamatok, más műveletek megbénítására, megzavarására alkalmasak (ez véleményem szerint nemzetbiztonsági kockázat). Gyakorlatilag olyan, mintegy precíziós bomba vagy rakéta, csak a cybert-térben, a cyber-térből.
2) Új harcmodort jelentek ezek a malware-ek. Még inkább felértékelődik a cyber-tér kockázata, a számítástechnika szerepe a nemzetbiztonságban.
3) Magasan képzett, ezzel arányosan finanszírozott szakértői csoport munkáját feltételezi.
4) Az off-line támadás lehetősége felveti egyfelől az elhárítás, másfelől az adott helyen a számítógéppel dolgozók megbízhatóságának felelősségét.
5) Pusztító, óriási károkat okozó hatás kiváltható hagyományos fegyverek bevetése nélkül.
6) Végső soron akár a célzott állam politikai - gazdasági mozgásának a befolyásolására is alkalmasak a támadások.

Zömmel ugyanezen jellemzők mondhatók el az ún. (D)DoS-támadások értékelésénél is.

(D)DoS- és botnet-támadások

A (D)DoS – támadás a számítógép helyes, funkciójának megfelelő működésének megzavarását, megbénítását jelenti. Az elnevezés a támadás angol megfelelőjének rövidítéséből ered: Denial of Service, (rövidítve: DoS). Ha ez az elektronikus-támadás történhet több forrásból, több számítógépről indul, akkor használatos a Distributed Denial of Service (rövidítve: DDoS) elnevezés. Olyan támadások összefoglaló elnevezése ez, amelyek az elektronikus adatfeldolgozó- és átviteli hálózat valamely erőforrását igénybe veszik, lefoglalják abból a célból, hogy az az erőforrás funkciója ellátásra ne legyen képes. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák – tehát - a szolgáltatás igénybevételére.

A „terheléses támadás” technikai alapja – leegyszerűsítve. Amikor felhasználó (az ún. kliens) az Internethez kapcsolódik, akkor az ún. hozzáférést biztosító szolgáltató szerveréhez kapcsolódik, amellyel adatcsomagokat váltanak egymással. Ebben megtörténik

[393] Forrás: http://www.crysys.hu/skywiper/skywiper.pdf (Letöltés ideje: 2012. 05. 25.)

az mindkettőjük azonosítása (ügyfél személye, jogosultsága, a keresett web-oldal azonosítása, a szerver azonosítása stb.), majd ez a szerver a keresett web-oldal szerverére irányítja a felhasználót (közben az IP-cím nevéből számsor lesz, majd ismét név).

A támadás esetében a célzott szerverre – egyszerre – ezer-, vagy tízezer számra érkeznek adatcsomagok, amelyekre a szervernek – időrendi sorrendben – válaszolni kell(ene).

A (D)DoS – támadás során a támadó egy általa „verbuvált" hálózat számítógépek adatcsomagjaival elárasztja a célzott szervert akkora forgalommal, hogy az képtelen lesz az adatcsomagok fogadására, azoknak válaszolására, ezzel akár a számítógépes rendszer „lefagyását" is eredményezhetik.

A „verbuvált" hálózatot elnevezése: botnet, amely a „robotnetwork" szavak összevonásából ered. A számítógépek robotoknak foghatók fel, mert előre programozott, tömegesen ismételt feladatokat hajtanak végre, és mivel ezek a (robot)számítógépek számítógépes hálózatra vannak rákapcsolva, innen származik a network (hálózat) kifejezés. Azt a számítógépet, amely vezérli a botnet-akciókat hívjuk controllernek. A robotgépeket pedig zombiknak. Megjegyzem, hogy bármely felhasználó (bármelyikünk) számítógépe válhat „zombigéppé" (bármikor). Sajnos, számítógépeink a számítógépes hálózatra történt csatlakozással ki van téve sokféle malware, köztük zombikódok „begyűjtésének" veszélyének.

A zombikódok ugyanúgy jutnak el az óvatlan felhasználó számítógépeire, mint bármely más fertőzések. Azaz az IRC-n keresztüli-, továbbá P2P-kapcsolatban fájlcserével, de (illegálisan letöltött) tömörített programok .exe vagy .com fájljaiban, keygenerátor-programokban, patchekben, nem ritkán e-mailek csatolt fájljaiban, de akár más módon is stb. A zombikódok a hálózati kapcsolatok kialakításakor egy távoli szerverre (pl. egy IRC-szerverre) kapcsolódnak fel, ahol a controller irányítása alatt a zombiszámítógépek a programok végrehajtását. A controller általában bérelt szerverre (bérelt tárhelyre) csatlakozik. Az egyéni felhasználó csak számítógépe erőforrásainak „gyengülésén" észlelheti, hogy zombiként használják számítógépét. Pl. a számítógép működése lelassult, lassabban tölti be a web- oldalakat, a le-, vagy feltöltési sebesség lecsökkent, az audió-, vagy videó kommunikáció (az Internetes rádió- és televízióadások, az Internetes telefon-, illetve Skype – beszélgetések „szakadoznak".

A magyarországi bot-net fertőzöttségre figyelmeztető az a 2009-es állapotokat az európai és észak-afrikai országokra kiterjedő Symantec-tanulmány,[394] amely szerint Magyarország a bot-fertőzött számítógépek számát tekintve térség 9. legfertőzöttebb országa, amely azt jelenti, hogy minden 25. bot-fertőzött számítógép hazánkban „működik". Nem vigasztaló számunkra az, hogy Németország, Nagy-Britannia, Oroszország az első három.[395]

A botnet-hálózatot „üzemeltető" lehet egyéni felhasználó, de valószínűbb a szervezett bűnözői-, vagy a terroristacsoportok, vagy az állam által folytatott hadviselés egyik eszköze. Ma már a számítógépes „trükkök" (pl. a hackelés, adatkikémlelés, vírus-, (D)DoS-támadások) a modern hadviselés szerves részét képezi. A 2007. májusi orosz – észt hackerháborúban, (D)DoS-támadások stb. idején. Egyes – meg nem erősített (soha nem lesz megerősítve) források szerint az egyik orosz minisztérium IP-címéről is érkezett támadás.[396]

[394] Forrás: http://infovilag.hu/hir-17557-symantec_jelentes_kiberbunozesrol_magyar.html (Letöltés ideje: 2012. 05. 25.)
[395] Ugyanígy figyelmeztető jel, hogy adathalászra használt hazai oldalak számában is 9-ek voltunk 2009-ben.
[396] Forrás: http://itcafe.hu/hir/orosz-eszt_haboru_a_kiberterben.html (Letöltés ideje: 2012. 05. 25.]

„Amatőrségre" vallott volna, ha valóban kormányzati törekvést mutatott volna a cyber-háború. Ma már az IP-címek proxy mögé rejthetők, hamisíthatók (például földrajzilag azonosíthatatlannak mutatkoznak).

Már több esete is ismert annak, hogy orosz hackerek 24 órás üzemeltetésű fogadási oldalakat zsaroltak meg, nem fizetés esetére (D)DoS-támadás végrehajtásával.[397]

Figyelmeztető jel továbbá, hogy 2012. első negyedévében a pénzügyi szektor elleni (D)DoS-támadások megháromszorozódtak.398 A Prolexic biztonságtechnikai cég közleménye szerint az észlelt támadások 70%-a Kínából jött, ott is két nagy szolgáltató rendszerét használták erre a célra. A támadások mennyiségi növekedése mellett fokozott veszélye az, hogy újabb platformokat (MAC OS X, és már mobiltelefonokat) „vontak be" a támadók, azaz még szélesebb körből meríthetnek klienseket a támadáshoz. Egy átlagos támadás ideje viszont csökkent 34 óráról 28,5-re, vélhetően a mobiltelefonon történő internetezés rövidebb ideje miatt.

A Stuxnet, DuQu és (D)DoS – támadások jogi értékelése:

a) Nemzetközi jogi problémákat is felvet.

Hiszen ezek a támadások más államok felségterületein zajlanak, illetőleg más államok felségterületein fejtik ki károsító hatásukat, ott okoznak kárt. Tehát sérül az államok szuverenitása. Kérdés, hogyan tekintsük erre a problémára?

Értékelhetjük úgy, hogy ez nem más, mint más állam területén végrehajtott szabotázs – cselekmény, amely a hidegháborús korszakban elő-előfordult, a két állam politikai viszonyában gyakorlatilag következmények nélkül maradt.

Vagy értékelhetjük akként, hogy ez már casus belli, indok a háborúra.[399] Az adott ország dönt ebben a kérdésben, a döntése meghozatalakor a politikai – diplomáciai – katonai erőtér a meghatározó.

A Stuxnet, DuQu – (D)DoS-támadások természetesen nemcsak az állambiztonságra veszélyesek. Mivel ismertté váltak ezek – ha nem is a maguk teljességében? – alkalmasak más célok végrehajtására is, így például a gazdasági konkurens számítástechnikai rendszerének (gyártási, értékesítési, pénzügyi folyamatainak) megbénítására.[400] Természetesen jelentős tőkeerő szükséges az ilyen célú malware-ek elkészítésére, műveleti feltételeinek kifürkészésére, alkalmazására, még ha bér-programírókkal, bér-hackerekkel dolgoztatnak is.

Mivel világunk gazdasági folyamataiban a tőkekoncentráció a jellemző, az állva maradó multinacionális vállalatok egymás elleni harcának egyik nemtelen eszköze lehet.

---

[397] Forrás: http://www.crime-research.org/news/29.07.2004/526/ (Letöltés ideje: 2012. 05. 25.] http://www.technewsworld.com/story/8063.html (Letöltés ideje: 2012. 05. 25.)

[398] Forás: http://www.banktech.com/risk-management/232900065 [2012. 05. 25.] és http://www.computerworlduk.com/news/security/3350609/ddos-attacks-on-financial-services-firms-triple-since-last-year/ (Letöltés ideje: 2012. 05. 25.)

[399] Ennek kétélűségére két magyarországi példa: a mind a mai napig nem kellően tisztázott 1941. június 26-án Kassát ért bombatámadás Magyarország belépését hozta a Szovjetunió ellen vívott háborúba. Ugyanakkor az 1991. október 27-éb Barcsra hullott bombák ellenére sem lépett be Magyarország a horvát-szerb háborúba.

[400] Kevin Mitnick – William L. Simon: A megtévesztés művészete. Budapest, Perfect Kiadó 2002. 229-248.o.

Visszatérve a jog területére, a támadást szenvedő állam joghatósága kiterjed az elfogott elkövetőkre.[401]

b) A büntetőjogi felelősség kérdése – elvileg – egyszerűbb.

A kárt okozó malware alkalmazása esetén a feltöltő személyek, valamint a (D)DoS – támadást végrehajtók, mint elkövetők cselekményeik a büntető törvénykönyv rendelkezései szerint minősülnek: A minősítési lehetőségek:

„300.§ (3) bekezdés
b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza, és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.
(4) A (3) bekezdésben meghatározott bűncselekmény büntetése
a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,
b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,
c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz."

Ha a malware-rel vagy (D)DoS-támadással célzott üzem a Btk. értelmező rendelkezése szerint közérdekű üzemnek minősül,[402] akkor a Btk. 260.§-ban szabályozott „Közérdekű üzem működésének megzavarása" tényállása hívandó fel.

„(1) Aki közérdekű üzem működését berendezésének, vezetékének megrongálásával vagy más módon jelentős mértékben megzavarja, bűntettet követ el, és öt évig terjedő szabadságvesztéssel büntetendő….
(3) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekményt különösen nagy vagyoni hátrányt okozva követik el.
(4) A büntetés öt évtől tizenöt évig terjedő szabadságvesztés, ha a bűncselekményt különösen jelentős vagyoni hátrányt okozva követik el."

A kár számításába a számítástechnikai rendszerben kezelt adatok és programok okozott tényleges a rendszer újratelepítése is beleszámítandó. A jövőre hatályba lépő új Büntető törvénykönyv (2012. C. törvény) szerint a szabályozás életszerűbb lesz:

„423. § (1) Aki
… b) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
c) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

---

[401] Ligeti Katalin: Büntetőjogi és bűnügyi együttműködés az Európai Unióban. KJK-Kerszöv Kiadó. Budapest, 2004. 41-56. o.

[402] *„közmű, a közforgalmú tömegközlekedési üzem, a távközlési üzem, valamint a hadianyagot, energiát vagy üzemi felhasználásra szánt alapanyagot termelő üzem"* (Btk. 260.§ (7) bekezdés.
A kárértékek a hatályos törvény szerint:
„a) kisebb, ha ötvenezer forintot meghalad, de kétszázezer forintot nem halad meg,
b) nagyobb, ha kétszázezer forintot meghalad, de kétmillió forintot nem halad meg,
c) jelentős, ha kétmillió forintot meghalad, de ötvenmillió forintot nem halad meg,
d) különösen nagy, ha ötvenmillió forintot meghalad, de ötszázmillió forintot nem halad meg.
e) különösen jelentős, ha ötszázmillió forintot meghalad."

(2) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha az (1) bekezdés b)-c) pontjában meghatározott bűncselekmény jelentős számú információs rendszert érint.
(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el."

c) Természetesen a polgárjogi kárfelelősség is érvényesíthető.

Kissé cinikusan, ám reálisan, egyéni elkövetővel szemben mértéke miatt irracionális, államok egymás közötti kárfelelősségének érvényesítése – e körben – utópisztikus.

Végső konklúzió helyett:

A háború a cyber-térben új minőségi szakaszba lépett. Ma jelentős és szervezett szellemei és anyagi háttérrel olyan malware-ek írhatók, amelyekkel egy-egy ország kritikus infrastruktúrájának vagy más számítástechnikai rendszere befolyásolható, tönkretehető, felette az uralom megszerezhető.

Nem szükséges tehát katonai erő alkalmazása, lojális személy hatalomba segítése pl. puccs árán, hitelekkel, lejárt hitelek megvásárlása és más politikai – gazdasági – pénzügyi praktikával a támadott ország politikai irányvonalát befolyásolni, eltéríteni, hanem mindez – a támadó rövid távú érdekeinek megfelelően – gyakorlatilag kockázatmentesen elérhető a cyber-térből (is).

A mindenen átgázoló gazdasági verseny eszköztára egy újabb eszközzel bővül(het).

Itt jelentkeznek azok a nemzetbiztonsági kockázatok, amelyekre fel kell készülni, és amelyek meg kell találni a technikai - technológiai és különböző jogági „ellenszereket", reakciókat.

Az új kockázatokat, akárcsak más számítástechnikai környezetben felmerülő kockázatot, az Internet árnyoldalait meg kell ismertetni a képzési formáknak megfelelő szinten, mélységben, középiskoláktól az egyetemi oktatáson át a jogalkotók a jogalkalmazók képzéséig. Jelenleg e körben bőven lenne tennivaló.

Police malware

Végére hagytam egy ma még humorosnak tűnő új jelenség ismertetését. Az Internetes illegális pénzszerzés trükkjei kimeríthetetlenek. Az illegális szerencsejátékoktól a könnyelmű és naiv felhasználók becsapásával pénz

Számtalan káros, a felhasználók számára káros, veszélyeket rejtő, a felhasználók adatainak megszerzését célzó programot, programocskát letölthetünk, kaphatunk. Ezeket gyűjtőfogalommal malware-nek nevezzük. A malware kifejezés az angol malicious software (rosszindulatú szoftver) rövidítéséből származik. A malware kifejezés felölel tehát minden olyan programot, amelyek a felhasználók számára károsok vagy bármilyen más veszélyt rejtenek magukba. Idetartoznak:

- a számítógép vagy a hálózat működését megzavaró, befolyásoló vagy elektronikus adatot, programot törlő, hozzáférhetetlenné tevő és más vírusok, férgek (worms),
- a kéretlen kereskedelmi küldemények (spamek),
- a ransomware-k: a zsaroló szándékával küldött programok,

- kémprogramok (spyware-k), amelyek a számítógépben tárolt adatainkat, internetezési szokásainkat (pl. a látogatott oldalak) gyűjtik és küldik illegálisan a spyware-k készítőinek,
- gyökércsomagok (rootkitek), a rendszer működését láthatatlanul és illegálisan ellenőrző programok, amelyek károsan is befolyásolhatják is a rendszert.

Egy új formája tűnt fel alig több mint egy éve. Ez pedig az ún. „police malware". Több európai rendőrség és más szervezet nevével, tekintélyével éltek vissza a cinikus elkövetők: Német Szövetségi Rendőrség, GEMA (német művészeti jogok szervezete), a svájci Szövetségi Igazságügyi és Rendészeti Minisztérium, az angol fővárosi rendőrség, a spanyol és a holland rendőrség. A police malware egy egyszerű zsarolás. Lényegét, pl. egy ilyen e-mail fogalmazza meg:

„*The operating system was locked for infringement against the laws of Switzerland. Your IP address is <removed>. From this IP address, sites containing pornography, child pornography, bestiality and violence against children were browsed. Your computer also has video files with pornographic content, elements of violence and child pornography. Emails with terrorist background were also spammed. This serves to lock the computer to stop your illegal activities"…150 CHF within 24 hours over Paysafecard, or the computer's hard disk contents will supposedly be erased.*"[403]

„*Az operációs rendszer volt zároltuk a svájci jogszabályok megsértése miatt. Az Ön IP címét eltávolítottuk. Erről az IP-címről, pornográf, gyermekpornográfia, a kegyetlenséget és a gyermekekkel szembeni erőszakot is bemutató web-helyeket böngésztek. A számítógépen pornográf, erőszakos jeleneteket és gyermekpornográfiát tartalmazó videó fájlok is találhatók. Észleltük, hogy e-mailek terrorista kapcsolatra utalnak. Ezen illegális tevékenységek miatt zároltuk a számítógépét … vagy fizet 150 svájci frankot a Paysafeguard rendszeren keresztül vagy 24-án belül törölnie kell a merevlemezét.*"

Több anonim átutalást lebonyolító lehetőség van az Interneten. A levélben említett paysafeguard-on kívül az Ukash is népszerű ezen elkövetőknél.

Látható, hogy a zsarolást a hivatalos szervek nevében követik el. Az átutalást lebonyolító szervet nem érdekli, hogy ki, honnan és hová szeretne utalni, mint ahogy az sem, hogy ki, miért és honnan kapja az átutalt pénzösszeget.

Ha ez az új cselekmény-típus megjelenik – reméljük, nem kerül erre sor - a hazai kriminalisztikában, akkor ennek a büntetőjogi minősítése nem fog problémát okozni.

Az elkövetőknek a zsarolás bűncselekményének egy nagyon súlyos esetéért kell majd felelniük.

„323. § (1) Aki jogtalan haszonszerzés végett mást erőszakkal vagy fenyegetéssel arra kényszerít, hogy valamit tegyen, ne tegyen vagy eltűrjön és ezzel kárt okoz, bűntettet követ el, és egy évtől öt évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a zsarolást…..
c) hivatalos személyként e jelleg felhasználásával, avagy hivatalos megbízás vagy minőség színlelésével követik el."

[403] Forrás: http://www.securitynewsdaily.com/1333-fake-cops-hijack-computers.html (Letöltés ideje: 2012. 05. 25.)