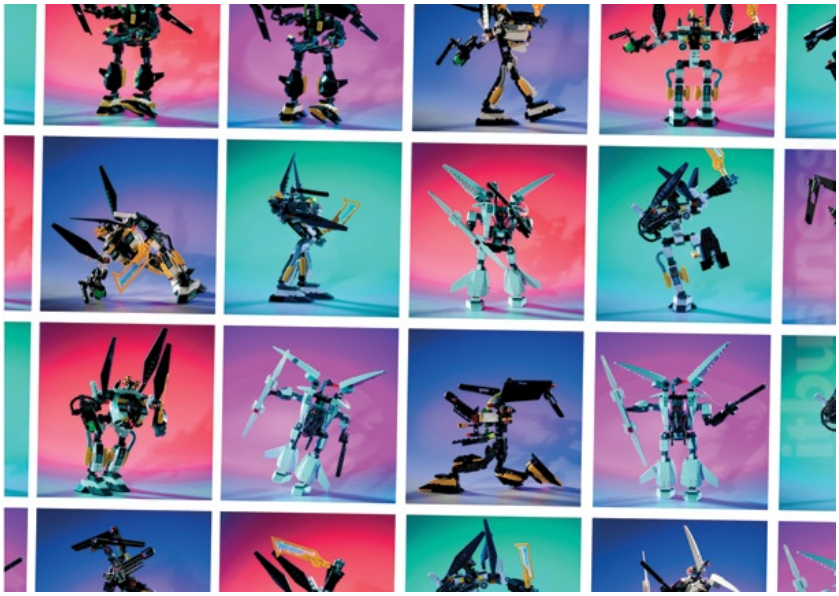
Megint lőnek, ropogtatnak
Kiss Gábor, 2010. 03. 01. hétfő



*Ideje leszámolnunk a magányos hacker illúziójával, hálózatunkon bűnszövetkezetek és hadseregek vívják harcukat, legtöbbször észrevétlenül.*

Percekig sorolhatnánk a film- és könyvcímeket, ahol a gonosz behatolók adatokat lopnak, rendszereket bénítanak meg, vagy akár gazdaságokat döntenek romba. Az ilyen támadások tényét és jelentőségét ma már valódi veszélyként kezelik bárhol a világon, a védekezés azonban nem mindenhol magától értetődő. A támadások sokféle céllal történnek a rendszer megbénításától az adatlopáson át a fizikai megsemmisítésig. Az elhárítás egyik legnehezebb kérdése jelenleg nem technikai, hanem elvi vagy, mondhatjuk, politikai. Kinek a feladata – és milyen eszközökkel – a támadások kiszűrése, elhárítása és az esetleges válaszlépések megtétele? Más eszközeik és jogaik vannak a magáncégeknek, a rendvédelmi szerveknek, a hadseregeknek és a titkosszolgálatoknak. Egyáltalán, mi számít még „szimpla” ipari kémkedésnek, és hol kezdődik a háború?



Az internetes hadviselés és kémkedés többször is a közvélemény elé került az elmúlt években, legutóbb a Google elleni Kínából kiinduló támadás hozta felszínre a témát. Egyes vélemények szerint a támadás mögött a kínai állam sejthető, de természetesen ezekre a vádakra nem találtak bizonyítékot. Elég valószínűtlen, hogy bárki bármikor rá tudja bizonyítani egy államra, hogy a támadások mögött nem civilek, hanem állami akarat áll.

**Árnyékboksz**

Ez a lenyomozhatatlanság és bizonytalanság az internetes hadviselés egyik legnagyobb rákfenéje *Szabó László,* a Kürt Zrt. informatikai biztonsági szakértője szerint. A számítógép- és internethasználat elterjedésével szinte bárki játszva indíthat támadásokat, szervezhet hálózatokat megfertőzött gépekből, vagy próbálhat behatolni mások számítógépére. Nincs szükség nagy befektetésre, különleges hardverre ahhoz, hogy valakiből hacker legyen. A megszerzett tudás felhasználásának módja természetesen már az egyénen múlik, rengeteg programozó foglalkozik hivatásszerűen vagy hobbiból biztonsági rendszerek tesztelésével, amibe a feltörésük is beletartozik. A védekező szempontjából azonban sokkal nehezebb a helyzet, az egyre kifinomultabb támadások egyre nagyobb ráfordításokat követelnek meg a védekező féltől. Nem elég a megfelelő vírusirtókat és tűzfalakat beszerezni. Szabó László véleménye megegyezik a legtöbb it-biztonsági szakemberével: ezekben a rendszerekben a leggyengébb láncszem az ember. Hiába az erős gép, a jó szoftver, ha a felhasználó önként, figyelmetlenségből trójait vagy keyloggert telepít a gépére. Egy meggondolatlan döntés, egy kis ingyenes játék, film, esetleg pornó, és gépünk máris fegyverré vált.

A Google elleni támadás egyik tanulsága is ez volt, hiába lehet azonosítani a gépeket, amelyek részt vettek a támadásban, semmi esély arra, hogy az értelmi szerzőket megtalálja bármilyen hatóság. Kína egyébként is homályos folt az ilyen esetekben, hiszen az állami szabályozás miatt csak olyan gépet lehet vásárolni, amelyen előre telepített cenzúraszoftver van. Az ebben található biztonsági résen keresztül bárki könnyedén használhatja a gépeket spamküldésre, túlterheléses támadásra vagy káros kód terjesztésére. Ha feltételezzük, hogy a biztonsági rés szándékosan maradt a programban, és azt a kínai állambiztonság használja, akkor Kínának elég jelentős erőforrások állnak rendelkezésére egy hálózati háborúhoz. Az ilyenfajta hadviselés egyik legnagyobb előnye a támadó – és legnagyobb hátránya a védekező – szempontjából, hogy a felelősség megállapítása gyakorlatilag lehetetlen. Szabó László elmondása szerint a nemzetközi szabályozás és a törvényi háttér hiánya rendkívül megnehezíti az ilyen esetek felderítését. Nem lehet egyértelműen eldönteni, hogy egy államon belül kinek a feladata a védelem, és milyen



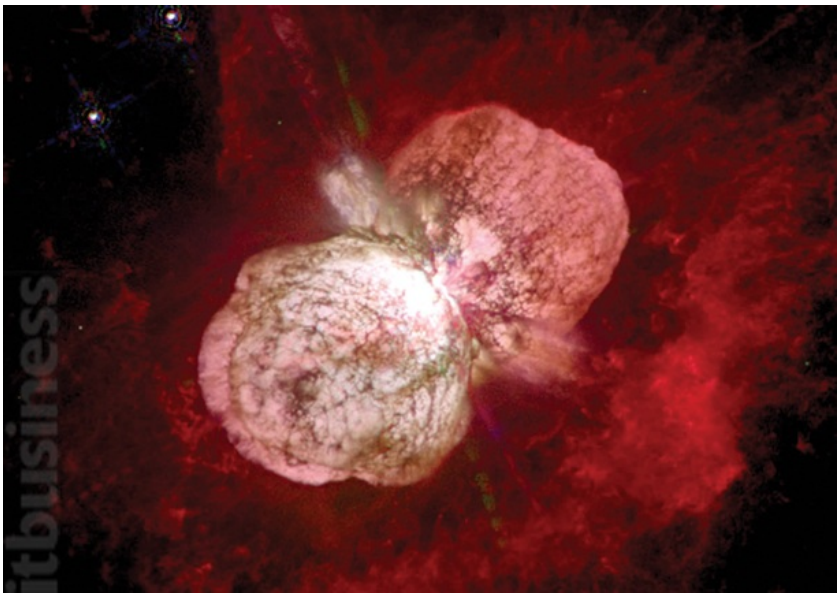

Szabó László, Kürt

eszközökkel élhet jogos érdekeinek védelmében. A nemzetközi szabályozás is hiányos, hiszen ami az egyik államban bűncselekménynek minősül, az máshol akár hazafias tett is lehet.

A védekezés sem feltétlenül egy hadsereggel kezdődik az államon belül, hiszen, mint a példának felhozott esetben, a támadás nem egy államot ért, hanem egy magáncéget. Mi tartozik bele az állam által megvédendő körbe, kinek kell megvédenie a magáncégeket és milyen szinten? Ezekre a kérdésekre jelenleg hazánkban még nincsenek egyértelmű válaszok. A legjobb intézkedés ezekben az esetekben még mindig a védekezés, Szabó László szerint a támadásokat csupán kivédeni lehet, a tisztázatlan szabályozás miatt más lehetőségük sem az államoknak, sem a magánszektornak nincsen. Kívánatos lenne, ha minden számítógépes rendszert üzemeltető számára előírnának egy kötelező védekezési szintet, illetve oktatásokat tartanának a felhasználóknak. A jelenlegi szabályozás elég tágan értelmezi a védekezést, így a legtöbben az olcsóbb, kevésbé kielégítő megoldásokat választják, a Kürt szakembere szerint még sokan nem ismerték fel a dolog jelentőségét. A mostani helyzetben a legcélszerűbb és szinte az egyetlen lehetőség a védekezésre való berendezkedés, a rendszerek folyamatos tesztelése és a hibák javítása. Szerencsére hazánkban többen is foglalkoznak etikus hackeléssel, konferenciákat is szerveznek a témában, amelyeken már a szakképzett munkaerőre vadászó cégek és állami szervezetek is megjelentek.

**Fegyverkezési verseny**

Bár nyíltan eddig csupán az Egyesült Államok ismerte el, hogy megkezdte cyberhadseregének építését, sejthető, hogy a többi katonai és gazdasági nagyhatalom sem ül tétlenül. Kérdés, hogy az így felállított szervezetek mikor fognak kilépni a védekező, megelőző, nyomozó szerepből, és formálódnak komoly katonai csapásmérő egységekké.



A 2007-es észt–orosz konfliktus is mutatta, hogy milyen komoly károkat lehet okozni egy jól irányzott támadással, ebben az esetben a teljes észt banki rendszert sikerült megbénítani. *Csizmazia István,* az Antivírus blog szerzője és a Sicontact Kft. vírusvédelmi szakértője szerint a 2007-es esemény jól mutatta, hogy mekkora a függés az informatikai rendszerektől. Szerinte az állam feladata a fontos közszolgáltatások védelmének ellátása, hiszen nemzeti érdek, hogy egy banki vagy telekommunikációs rendszer ne legyen egyszerűen támadható vagy adott esetben elpusztítható. A kínai támadásokra kitérve a szakértő szerint nem kell azonnal a kínai kormányzatra mutogatni, ha éppen onnan érkezik támadás. Tisztában kell lennünk a ténnyel, hogy a legtöbb aktív internetező Kínában él, ezért nyilvánvalóan ott lehet fertőzött gépekből a legnagyobb zombihálózatokat létrehozni. Segíti még a bűnszövetkezetek munkáját az is, hogy a kínai doménregisztráció szokatlanul engedékeny, pillanatok alatt lehet hamis adatokkal saját doménhez jutni. Nem meglepő, hogy a kínai gépekről indított támadások mögött sokszor egészen más országok szervezetei állnak.

**Még mindig: haszonszerzés**

Azt is érdemes megjegyezni, hogy az internetes adatlopások és támadások mögött még mindig a haszonszerzés a fő mozgatórugó. A cyberhadseregek létező dolgok, de funkciójuk jelenleg sokkal inkább a védekezés és a biztonsági rendszerek tesztelése, mint a csapásmérés. A fegyverkezés tényét, vagy a fegyverek létezését egyik állam sem ismeri el, ez természetesen államtitoknak minősül. Az pedig, hogy a védekezésre szánt eszközöket mennyire lehet felhasználni támadásban, ismét egy másik kérdéskör. Egyes, elvileg védekezésre kifejlesztetett fegyverek például alkalmasak az ellenség elektronikus eszközeinek elpusztítására.


Csizmazia István, Sicontact

Csizmazia István szerint jelenleg Kína legnagyobb hátránya a nyugati országokkal szemben a saját fejlesztés hiánya. Jelenleg a lépéselőny az innovatív, fejlődésre képes országoknál van. Szintén 2007-ben történt, hogy német és angol minisztériumokban kínai eredetű behatolásra és kémkedésre utaló nyomokat találtak. A kémkedés tényét, illetve annak állami voltát soha senki sem tudta rábizonyítani az országra, mindazonáltal Kínát már többször figyelmeztették, hogy az általa alkalmazott vagy publikált tudományos eredmények vagy fejlesztések idegen eredetűek voltak. A fejlesztések titokban tartása természetesen minden cég és állam érdeke és kötelessége. A szakértő szerint a fontos közszolgáltatások védelmét ugyanúgy az államnak kell megszerveznie, mint ahogyan az egyes polgárok védelmét is. A magánembernek ugyanis lényegesen kevesebb eszköze és jogosultsága van az önvédelemre. Természetesen itt is elvárható, hogy az egyén megtegyen mindent a saját védelmének érdekében – mint ahogy a lakását is mindenki bezárja, a számítógépére is hasonló figyelmet kell fordítania. A magyar helyzet ebből a szempontból elkeserítő: sok helyen még vállalati szinten sem hajlandóak komolyabb védelmi rendszerekre pénzt áldozni. Hiányzik továbbá a vezető rétegből az a fajta tudatosság, ami segítené a szakemberek munkáját, sajnos nagyon sok helyen hiányoznak a különböző szintű védelmi rendszerek, és hiányos az oktatás is.

A veszély pedig nagyon is valós, a vírusírás és trójaikészítés ma már nem követel meg akkora programozói tudást, mint eddig. Kis kitartással bárki találhat olyan honlapot, ahonnan megfelelő minták tölthetők le egy program elkészítéséhez, de pénzért akár komplett támadócsomag is vásárolható, illetve a bűnözők magas haszonnal bérbe is adják fertőzött botnet-hálózatukat.

Magyarország felkészültségi helyzetét elégtelennek tartja *Krasznay Csaba,* a Zrínyi Miklós Nemzetvédelmi Egyetem doktorandusza. Véleménye szerint a magyar szakma felkészült és megfelelően kvalifikált egy megfelelő védelmi rendszer kidolgozására és üzemeltetésére, de jelenleg ennek még csak a kezdeményeit lehet látni. Biztató, hogy több hackeléssel kapcsolatos konferenciát is tartanak, és ezeken már a kormányzati szervek is részt vesznek, valamint a magánszektor is érdeklődik a programozók munkája iránt. Magyarországon 2010 januárjától létezik a Nemzeti Hálózatbiztonsági Központ, amely a közigazgatási és a kritikus információs infrastruktúrát jelentő hálózatok biztonságáért felel. Ez azonban közalapítványi formában működik, ezért nem helyettesítheti a rendvédelmi hatóságokat, illetve a hadsereget. A rendőrség nyomozati jogkörrel rendelkezik, nem feladata az elhárítás, reagálása ezért nem elég gyors, és technikai feltételei sem adottak, ami egy internetes támadás esetében végzetes hiba. A honvédségen belül, amelynek feladata az országszintű támadások elhárítása, szintén csupán kutatások folynak a témában, illetve a Zrínyi Miklós Nemzetvédelmi Egyetemen már folyik a jövő védelmi szakembereinek képzése.

**Tények és számok**

Egyes források szerint az Egyesült Államok jelenleg 10 milliárd dollárt költ évente cyberhadseregére.

A 2007-es támadás után az észt Hansabank kára saját számításai szerint 1 millió dollár volt.

Egyetlen személyt találtak bizonyíthatóan felelősnek az észt–orosz cyberháború után. A férfi 870 dollárnak megfelelő büntetést kapott.

Az eddigi legnagyobb kémkedési és adatlopási ügy szintén Kínából indult. A Ghostnet hálózat üzemeltetői többek között a Lockheed Martin és a NASA gépeibe is behatoltak.

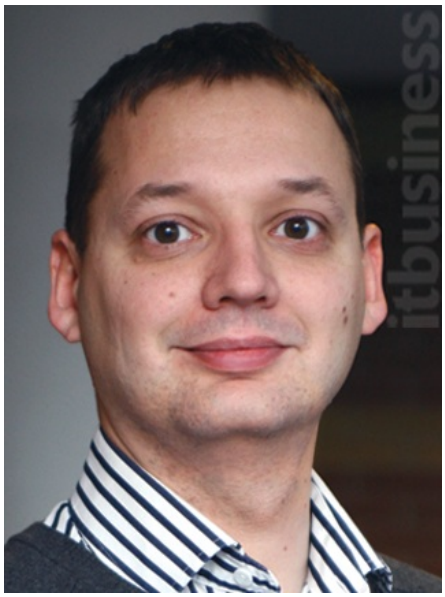
A Google szervereit a gyanú szerint kínai egyetemisták törték fel, korábban a Northrop Grumman cég szervereinek feltörésével is a védekezés Krasznay Csaba szerint nem egyértelműen katonai, illetve állami feladat, mert a hálózati csatározásoknál összemosódik a magán- és állami szektor. A Google-nak otthont adó állam is csak akkor értesült a támadás tényéről, amikor a vállalat tájékoztatta. Szoros együttműködésre van tehát szükség a magáncégek és az állam között a támadások felismerésére és elhárítására, különösen akkor, ha a magáncég egy stratégiai fontosságú szolgáltató. A másik probléma a jogi háttér tisztázatlansága, adott esetben egy Kína területén szolgáltatásokat nyújtó vállalat ellen irányult a támadás, és vélhetően olyan személyek ellen nyomoztak, akik a helyi törvények szerint bűncselekményt követtek el. Ami nyugati szemmel a magánszféra és a szólásszabadság súlyos megsértése, az a kínai törvények szerint akár legális cselekmény is lehet. A szakértő szerint az országoknak meg kell tanulniuk együtt élni az ilyen fenyegetéssel, és a terrorfenyegetések mintájára fel kell készülniük egy esetleges támadásra.

Jiaotong egyetem diákjait gyanúsították.

**Cyberhadseregek pedig léteznek**

Sürgősen szükség lenne egy olyan hatóságra, amelyik rendelkezik a megfelelő jogosítványokkal a beavatkozásra, valamint a megfelelő szakértői gárdára, amelyik képes a gyors és hatékony fellépésre. Mivel a jelenlegi civilizációs norma szerint a fejlett országok nem támadják meg egymást, mindenki csak a védekezésre rendezkedik be, az internetes hadviselésnek nincsenek kialakult szabályai. Az utóbbi évek történései, például a 2008-as orosz–grúz konfliktus azonban megmutatta, hogy a reguláris hadseregek mellett az államok hajlandóak bevetni internetes harcban járatos szakembereiket is. Az események bebizonyították, hogy cyberhadseregek léteznek akkor is, ha nem beszélnek róluk, hiszen az akciók jóval többnek látszottak hazafias hackerek egyszerű magánháborújánál.

*Krasznay Csaba* szerint hazánkban éppen szemléletváltás zajlik a hálózati biztonság ügyében; a 223/2009-es kormányrendelet rendezi a kritikus információs infrastruktúrák védelmének számos kérdését, például kötelezővé teszi az elektromos szolgáltatók számára a rendszeres penetrációvizsgálatot, amit etikus hackerek végeznek. Az utóbbi évek Hacktivity konferenciái – amelyeknek korábban aktív szervezője volt – megmutatták, hogy az ipari szektor komolyan érdeklődik az etikus hackerek, a hackelés iránt, elindult a párbeszéd a szakma és a kritikus szolgáltatásokat nyújtó szervezetek között.



*Krasznay Csaba, Zrínyi Miklós Nemzetvédelmi Egyetem*

Úgy tűnik, Magyarországon a döntéshozók is tisztában vannak a veszélyekkel, egy komoly védekező rendszer felállítása és üzemeltetése azonban rendkívül költséges, ezért a szakmára vár a feladat, hogy kényszerítse a politikai döntést.

**Defenzívából offenzívába**

A jelenlegi gyakorlat szerint a NATO üzemeltet Tallinn mellett egy kifejezetten informatikai támadások kivédésére szakosodott szakértői csoportot, amelynek feladata a megfelelő stratégiák kidolgozása egy esetleges katonai jellegű internetes támadás esetére. Krasznay Csaba elmondta: szükség esetén bármely tagállam kérhet segítséget a NATO-tól, ám a korábban már említett jogi tisztázatlanság miatt nem lehet egyértelműen eldönteni, hogy mi az a támadás, amelynek esetén a tagországok jogosultak segítséget kérni. A támadások természetét, jellegét és célját nehéz megállapítani, és lassú nyomozási folyamattal lehet csupán felgöngyölíteni. Egyelőre nem lehet tudni, hogy mikor országszintű egy támadás, mi számít nyílt háborúnak, és mi a terrorizmus, hol ér véget az önvédelem, és mikor lehet külső segítséget kérni.

Úgy tűnik, hogy az elkövetkező években a hálózati harc defenzívából offenzívába fordulhat, a megfelelő forrásokkal rendelkező államok az egyre gyakoribb és agresszívabb támadásokra már felelni fognak. Ehhez nagy szükség lesz egy valódi és mindenki által elismert szabályrendszer felállítására, hogy a válaszlépések egyértelműek és hatásosak lehessenek. Az internetes harc jellegéből adódóan leginkább a terrorizmusra hasonlít, katonái arctalan hátország nélküli partizánok, akik egy állam hallgatólagos beleegyezésével esetleg támogatásával vagy éppen tudtán kívül harcolnak. Amíg nem születik egységes globális szabályozás, nem lehet megállapítani, hogy ki a katona, ki a terrorista, és ki a nyereségre vadászó bűnöző. Addig csak egy dolog biztos: ha figyelmetlenek vagyunk, számítógépeink bármikor fegyverré válhatnak egy összecsapásban.