HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

Gyányi Sándor
Budapesti Műszaki Főiskola
gyanyi.sandor@kvk.bmf.hu

CYBER-TÁMADÁSOK ELLENI VÉDEKEZÉS ÉS A VÁLASZCSAPÁSOK LEHETŐSÉGEI

Absztrakt

A számítógépes hálózatok egyre nagyobb szerepet töltenek be a mindennapi életben, az államigazgatásban, a banki szektorban és nem utolsó sorban a fegyveres erőknél is. A térnyeréssel párhuzamosan a számítógépes támadások száma is növekszik, új bűnözői és terrorista csoportok is fokozzák jelenlétüket, egyre több állam kezdi el – bevallottan vagy titkoltan – hadseregét felkészíteni a virtuális térben folytatandó műveletek végrehajtására. A technológia fejlődését azonban nem kíséri a gondolkodásmód, a jogszabályi háttér és a nemzetközi jog ilyen irányú fejlődése, így a cyber támadások vizsgálata, a tettesek utáni kutatás során sokszor adódhatnak vitás, nehezen értelmezhető helyzetek. Igyekeztem a virtuális térben folyó és a hagyományos tevékenységek közötti hasonlóságokat bemutatni, analógiákat keresni a kétféle tevékenység között.

Nowadays computer networks are playing more and more important part in our everyday life, in the government, in monetary sector and last but not least in armed forces. Together with the extension the number of attacks is increasing. There are new groups of criminals and terrorists appearing, more and more governments start to prepare (either admittedly or in secret) their armies for carrying out operations in cyber space.
However, the development of technology is not followed by the development of thinking, of law background and of international law, so investigation of cyber attacks and searching for criminals often bring about controversial situations.
I tried my best to show the similarities between virtual and convential activities and to look for analogies between them.

***Kulcsszavak**: információs terrorizmus, cyber támadások, botnet ~ information terrorism, cyber attacks, botnet*

Bevezetés

A modern katonai műveletek során egyre nagyobb szerepet kap a harcoló egységek informatikai támogatása, az információs fölény kivívása. A tendencia az, hogy – költséghatékonysági okokból - a hadseregek a polgári életben alkalmazott informatikai technológiákat igyekeznek rendszeresíteni, természetesen a különleges követelmények figyelembe vételével. Ezek a rendszerelemek azonban széles körben használt technológiákat tartalmaznak, amiket jól ismernek a polgári élet szakemberei, így a potenciális támadók („harcosok") köre is jelentősen kibővült. Egy jövőbeli, közel azonos technikai fejlettségű hatalmak közti katonai incidens fontos helyszíne lesz a virtuális tér (Cyber-space), emiatt fontos az ilyen „hadszíntéren" folyó műveletek előzetes felmérése, a várható veszélyhelyzetek megismerése. Érdekes gondolatmenet a virtuális és a valódi harchelyzetek, eszközök párhuzamba állítása, és ebből kiindulva egy ilyen konfliktus értékelése.

Párhuzamok

A virtuális hadszíntéren lényegesen egyszerűbb bármilyen akciót elindítani, mint a valódi helyszíneken. Nem szükséges a haditechnika felvonultatása, a harcolókat itt a számítógépes hálózatok végpontjai helyettesítik. A mai nyilvános informatikai hálózatok (és itt leginkább az Internetre kell gondolni) alacsony költségek mellett jelentős adat mozgatását teszik lehetővé fizikailag egymástól nagy távolságokra levő végpontok között. Az Internetre bárki csatlakozhat, a mai technikai fejlettség mellett a szegényebb, katonailag jelentéktelenebb államok, militáns csoportok vagy akár magánszemélyek is komoly eszközparkot képesek felvonultatni. Az informatikai támadásokkal szemben ráadásul a fejlettebb infrastruktúrával rendelkező országok sokkal sebezhetőbbek, mint egy fejletlenebb hátterű ország, emellett az ilyen támadások elkövetőit azonosítani is rendkívül problémás.
A támadásokban – akár áldozatként, akár támadóként – szereplőket három nagy csoportba sorolhatjuk (természetesen a szereplők alatt az általuk birtokolt, használt infrastruktúrát kell érteni):

- önállóan tevékenykedő magánszemélyek;
- csoportok, szervezetek;
- államok.

Ha ebből összeállítjuk a lehetséges támadó-célpont kombinációkat, akkor többnyire csak kriminalisztikai szempontból érdekes változatokat kapunk. A magánszemély-magánszemély, magánszemély-szervezetek, szervezetek-magánszemély, szervezetek-szervezetek kombinációkra rengeteg ismert példát lehet felhozni, az ilyen támadások fő motivációja általában az anyagi haszonszerzés. Az igazán érdekes párosítások a következők:

- magánszemély támad államot;
- állam támad magánszemélyt;
- szervezet támad államot;
- állam támad szervezetet;
- állam támad másik államot.

A „magánszemély támad államot" kategória való világbeli analógiája a magányos merénylő lehetne, azonban egy elszigetelten működő magánszemély által sikeresen végrehajtott, a célpontnak, és csak a célpontnak komoly károkat okozó informatikai támadás nehezen kivitelezhető. Voltak komoly pusztítást végző – általában számítógépes vírusok vagy férgek

által végrehajtott – akciók, azonban ezek egyike sem állami infrastruktúrát támadott. Az első világméretű pusztítást okozó, magát az Interneten terjesztő számítógépes malware a 2000. május 4-én elszabadult „I love you” nevű féreg volt, amely az agresszív terjedésével több komoly levelező rendszert is időszakosan működésképtelenné tett. Szerzőjeként egy Onel de Guzman nevű Fülöp-szigeteki diákot azonosítottak, akit azonban a helyi törvények szerint nem lehetett elítélni, mivel a Fülöp-szigeteken a számítógépes víruskészítés nem számított bűncselekménynek [1].

Az előző kombináció ellentéte, az „állam támad magánszemélyt” nem túl valószínű forgatókönyv, bár sokan az állam túlzott érdeklődését az állampolgárok privát dolgai iránt is támadásnak tartják. Egyfelől a hatalom a pozitív szándékait hangsúlyozza, a minél több információ begyűjtésével könnyebben derítheti fel a különböző bűnözői vagy – napjainkban egyre nagyobb nyilvánosságot kapó – terrorista csoportok szándékait, terveit. Másfelől az állampolgárok félelme is érthető, mivel könnyű az orwelli „1984” világába képzelni magunkat.

A „szervezet támad államot” a legvalószínűbb, előbb-utóbb biztosan bekövetkező esemény. A különböző szélsőséges csoportok, terrorszervezetek bizonyítottan előszeretettel használják az Internetet egymás közti titkos kapcsolattartásra, propagandaanyagok terjesztésére, toborzásra. Az ilyen tevékenység különösen erős Nagy-Britanniában és a szintén jelentős iszlám közösséggel rendelkező Németországban [2]. Az említett funkciók használata mellett komoly esély van arra is, hogy a szervezési feladatok segítése mellett fegyverként is felhasználják majd az informatikai hálózatokat. Iszlám ideológiákat követő hackerek komoly mennyiségű weboldalt támadtak meg és törtek fel sikeresen, helyeztek el rajta propaganda jellegű üzeneteket. Ezek az akciók azonban általában kevésbé gondosan védett informatikai rendszereket értek, és a támadások ezen típusa ellen hatékony óvintézkedések tehetők. Az infrastrukturális feladatokat ellátó rendszereket veszélyeztető legkomolyabb módszer az elosztott túlterheléses (DDoS – Distributed Denial of Service) támadás, amely ellen hagyományos módszerekkel nehéz védekezni. A DDoS támadás során egy időben, nagyszámú internetes végpontról végzik a célpont megbénítására szolgáló adatcsomagok küldését, emiatt a támadó végpontok – vagy legalább az általuk generált adatforgalom – semlegesítése nem megoldható. Az elkövető számára az egyetlen nehézséget a szükséges mennyiségű, hálózatra kötött számítógép megszerzése jelenti. Erre automatizált megoldást kínálnak a számítógépes vírusok, férgek és trójai alkalmazások, amelyek segítségével átvehető egy fertőzött számítógép feletti uralom. A háttérben zajlanak a „fegyverkezési verseny” folyamatai, szinte elképzelhetetlen mennyiségű számítógépet vonnak uralmuk alá különböző szervezetek, amelyeket aztán hálózatba szerveznek, divatosan elnevezéssel zombie hálózatokat (botnet) alakítanak ki. Ezeket a botneteket valószínűleg bűnözői csoportok hozzák létre, legfontosabb alkalmazási területük a kéretlen elektronikus levelek küldése, azonban a megfelelő ellenszolgáltatásért cserébe az ilyen kapacitások bérelhetők is tőlük. Ez azt jelenti, hogy akár egy terrorcsoport is képes azokat felhasználni saját céljainak megvalósítására, csak a megfelelő anyagi háttérre van szükségük.

Ha egy állam egy szervezet ellen követ el informatikai támadást, akkor a logika szabályai szerint annak megelőző jellegűnek kell lennie. A támadónak kellő indokokkal, bizonyítékokkal kell rendelkeznie, a támadásnak a veszélyforrással arányosnak kell lennie, amennyiben a fegyveres konfliktusokra érvényes szabályokat próbáljuk rájuk alkalmazni. Az ellentámadás indokoltsága és különösen a módszere sok vitás pontot tartalmaz, amelyekkel érdemes behatóbban foglalkozni.

Az „állam támad másik államot” kategória túllép a civil szféra határain, hiszen ez két szuverén hatalom közti fegyveres konfliktusnak is tekinthető, amelyet nem halálos fegyverekkel vívnak. A legfrissebb ilyen esetként sokan a 2007. májusi észtországi szerverek ellen elkövetett DDoS támadást tekintik, jóllehet az orosz állam szerepe nem bizonyított az akcióban. Az észt szakemberek sok olyan végpontot azonosítottak, amelyek orosz állami hivatalokban működtek, azonban ezek a végpontok lehettek fertőzött gépek is, amelyek egy botnet tagjaként vették ki részüket a támadásból. Az államok közti cyber támadások rengeteg jogi problémát is felvetnek, amivel mindeddig keveset foglalkoztak a döntéshozók. Kína már az 1990-es évek elején kialakította saját, cyber hadviselésre szolgáló katonai infrastruktúráját. 1999-ben a Kínai Néphadsereg két ezredesének nyilatkozata szerint egy Tajvan miatti USA-Kína incidens esetén kínai hackerek képesek lennének lerombolni az USA polgári informatikai infrastruktúráját [3]. A kínaiak mellett természetesen más országok (Franciaország, Oroszország, Nagy-Britannia, Izrael) is rendelkeznek kifejezetten katonai jellegű informatikai támadások végrehajtására kiképzett állománnyal. Érdekes módon az Egyesült Államok Légiereje (USAF) csak 2007-ben hozta létre saját, Cyber Command nevű egységét, amelynek feladata a virtuális térben felvenni a harcot a potenciális támadókkal.

Lehetséges konfliktusok

A társadalom informatikai függőségének növekedésével párhuzamosan a kockázatok is növekednek. Egy jól kivitelezett támadás a társadalom kritikus informatikai infrastruktúráinak időszakos leállását vagy meghibásodását is okozhatja, amivel az állampolgárok mindennapi életét nehezíthetik meg, aláásható a pénzügyi, államigazgatási rendszerekbe vetett hitüket, szélsőséges esetben, pedig fizikai sérülést is okozhatnak. Az államoknak kötelességük polgáraikat megvédeni, ami igaz a virtuális térben kivitelezett támadások esetére is. A legnagyobb problémát az idegen államokból érkezett támadásokra adott reakciók jelentik, itt ugyanis a diplomáciai és nemzetközi jogi szabályok akadályozhatják az alkalmazható módszereket. Ha sikerül egy idegen államot egy informatikai támadás kiinduló pontjaként azonosítani (ami nem triviális feladat), akkor három különböző lehetőség jöhet szóba [8]:

- a kiinduló ország illetékeseivel felvenni a kapcsolatot, és közösen leállítani a támadást;
- a kiinduló ország illetékeseinek tudta nélkül felderíteni a támadót és megpróbálni letiltani hozzáférését (a hozzáférést biztosító szolgáltató segítségével);
- a kiinduló ország illetékeseinek tudta nélkül semlegesíteni a támadót.

Az első megoldás fő problémája az együttműködés hivatalos folyamatának hosszadalmas volta. Míg egy támadás elindításához néhány másodperc is elegendő, a hivatalos szervek kapcsolatfelvételéhez ennél lényegesen több idő szükséges. Figyelembe véve a szervereken képződő naplók mennyiségét és a szükséges rendszernaplók számát (egy támadó általában több feltört rendszer közbeiktatásával csatlakozik a tényleges akciót végző végpontokhoz, így tényleges címének felderítéséhez több végpontot is meg kell vizsgálni), a hivatalos csatornák közbeiktatásával kevés esély mutatkozik a valódi elkövető azonosítására. A második változat esetében diplomáciai gondot okozhat az, hogy bár a hírszerzést általánosságban nem tiltja a nemzetközi jog, egy külföldi ország ügynöke által elkövetett kémkedést a legtöbb ország jogrendszere szankcionálja. A harmadik eset a legveszélyesebb, egy idegen államban elkövetett, nem bejelentett akció akár háborús helyzethez is vezethet, természetesen csak elméleti síkon maradva. Mindhárom esetben még kényesebbé válhat a helyzet, ha a támadás kiindulási pontjaként azonosított országról kiderül, hogy az ottani végpont csak egy korábban

uralom alá vont (tehát szintén áldozat) végpont, amit az elkövető proxy-ként használt céljaihoz. Ha a tettes egy harmadik államból – vagy extrém esetben a célpont országból - kezdte akcióját, akkor az ellentevékenység komoly presztízsveszteséget okozhat mindegyik félnek.
Ha előfordulna az az alacsony valószínűségű eset, hogy a támadóról minden kétséget kizáróan bebizonyítható, hogy egy idegen állam megbízásából tevékenykedett, akkor az incidens akár komolyabb következményekkel is járhat. Az eddig napvilágra került esetek egyikében sem sikerült minden kétséget kizáróan felfedni az elkövető kilétét, jóllehet sejtések vannak ez ügyben. A sort 1999-ben, a Pentagon hálózata ellen elkövetett adatlopási akció nyitotta. Az események felderítésére indított "Moonlight Maze" [9] kódnevű FBI akció felderítette, hogy a támadók sikeresen bejutottak a Pentagon routereibe - hálózati útválasztóiba - és az adatforgalmat 8 másik olyan végponton vezették keresztül, amelyet könnyen lehallgathattak. A támadás szisztematikus volt, nem véletlenszerű adatokra vadásztak, a támadást elkövető végpontok közül, pedig sikerült azonosítani egy Moszkvától 30 kilométerre található internetes szervert. Az orosz érintettséget a szakértők azzal is igyekeztek bizonyítani, hogy az akciók mindig moszkvai idő szerint 8:00 és 17:00 között, tehát munkaidőben történtek. Természetesen az orosz hatóságok tagadták érintettségüket az ügyben. A következő, nagy port kavaró esetet a nyomozók által Titan Rain [10] névre keresztelt kínai hackercsoport követte el, több fontos amerikai katonai beszállító ellen. A nyomozás során kínai végpontokig sikerült a nyomokat visszakövetni, de természetesen a kínai szervek nem vállalták a felelősséget.
Ha az a helyzet állna elő, hogy egy állam egy másik kritikus infrastruktúráját megtámadta, akkor a megtámadott ellentevékenységéhez jelenleg nem állnak rendelkezésre kiforrott eljárások. A nem cyber támadások esetén az ENSZ alapokmányának [11] VII. fejezete ad útmutatást, érdemes megvizsgálni ennek alkalmazhatóságát. A 41. cikkely rendelkezik a nem fegyveres erők felhasználásával foganatosítható rendszabályokról: *"A Biztonsági Tanács határozza meg, hogy milyen fegyveres erők felhasználásával nem járó rendszabályokat kíván foganatosítani abból a célból, hogy határozatainak érvényt szerezzen és felhívhatja az Egyesült Nemzetek tagjait arra, hogy ilyen rendszabályokat alkalmazzanak. Ilyeneknek tekintendők a gazdasági kapcsolatok, a vasúti, tengeri, légi, postai, távírói, rádió és egyéb forgalom teljes vagy részleges felfüggesztése, valamint a diplomáciai kapcsolatok megszakítása."*

Az angol nyelvű változatban az "egyéb forgalom" eredetileg "other means of communication" kifejezésként szerepel, ami "a kommunikáció egyéb formája" értelmű. Vagyis, ha a Biztonsági Tanács a nem katonai jellegű beavatkozás mellett dönt, akkor a támadó fél valamennyi kommunikációs lehetőségét (beleértve az Internethez hozzáférést is) korlátozhatják. Ha ezek az intézkedések nem hoznak eredményt, akkor a 42. cikkely szerint: *"Ha a Biztonsági Tanács úgy találja, hogy a 41. cikkben említett rendszabályok elégtelenek, vagy elégteleneknek bizonyulnak, úgy légi, tengeri és szárazföldi fegyveres erők felhasználásával olyan műveleteket foganatosíthat, amelyeket a nemzetközi béke és biztonság fenntartásához, vagy helyreállításához szükségesnek ítél. Ezek a műveletek az Egyesült Nemzetek tagjainak légi, tengeri és szárazföldi hadereje által foganatosított tüntető felvonulásból, zárlatból (blokád) vagy egyéb műveletekből is állhatnak."*

Ennek értelmében az ENSZ felügyelet alatt akár fegyveres akcióvá is eszkalálódhat egy virtuális konfliktus, aminek – bár elméleti lehetőség van rá – valószínűsége napjainkban csekély. A Biztonsági Tanács tevékenységére eddigi fennállása során még a komoly fegyveres konfliktusok esetén sem a gyorsaság és az egyetértés volt a jellemző. Talán emiatt, az 51. cikkely biztosítja az államok számára az önvédelem jogát: *"A jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült Nemzetek valamelyik tagja ellen irányuló*

fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette. A tagok az önvédelem e jogának gyakorlása során foganatosított rendszabályaikat azonnal a Biztonsági Tanács tudomására tartoznak hozni és ezek a rendszabályok semmiképpen sem érintik a Biztonsági Tanácsnak a jelen Alapokmány értelmében fennálló hatáskörét és kötelességét abban a tekintetben, hogy a nemzetközi béke és biztonság fenntartása vagy helyreállítása végett az általa szükségesnek tartott intézkedéseket bármikor megtegye."

A fegyveres támadás kifejezés kiterjesztése a cyber támadásokra egy újabb érdekes problémát vet fel: mi számít fegyvernek egy támadás során? Ha olyan eszközre gondolunk, amely segítségével képes a fegyver használója emberéletben kárt okozni, akkor érdemes elgondolkodni egy olyan – filmekben előszeretettel bemutatott - számítógépes támadáson, amely segítségével egy atomerőmű vezérlését teszi tönkre a behatoló, ezzel az erőmű leállását vagy túlterhelését okozva. De példát lehetne hozni egyéb kritikus infrastruktúrára is, és bár nem túl valószínű egy tisztán informatikai eszközökkel végrehajtott ilyen jellegű támadás, de egyéb akciók támogatásaként teljesen valószerű.

A továbbiakban tekintsük át a cyber támadások során alkalmazott módszereket, illetve a megelőzés vagy az ellencsapás lehetőségeit.

Felderítés

Egy számítógépes hálózat mindig vonzza a rosszindulatú embereket, akik valamilyen motiváció miatt szeretnének bizalmas információkat szerezni, a hálózat erőforrásait uralni, erkölcsi és anyagi kárt okozni, a hálózat működését lehetetlenné tenni. A számítógépes hálózatok sikeres megtámadásához alapvető fontosságúak a célpont részletes műszaki paraméterei, amit – jó esetben – a rendszer adminisztrátorai igyekeznek titokban tartani. Ha a támadó nem ismeri a védvonalakon (tűzfalakon) belül elhelyezkedő célpontok paramétereit, nem sok esélye van célja elérésére. A szükséges információ megszerzésére több lehetőség is adódik:

- a célrendszert használók hibáit, jóindulatát kihasználva begyűjteni a hálózati sajátosságokat (egyes alrendszerek elérhetősége, bejelentkezési jogosultságok), tehát az emberi tényezőre építeni;
- fizikai hozzáférést szerezni az adott rendszerben, vagyis a rendszernek helyet biztosító épületekben hírszerzést folytatni;
- a számítógépes hálózaton keresztül speciális alkalmazások futtatásával begyűjteni a szükséges adatokat.

Az első két módszer veszélyeket hordoz magában, hiszen a támadónak meg kell jelennie a helyszínen, emberekkel kell találkoznia, ami könnyen lebukáshoz vezethet. Nehezíthetik az elkövető dolgát emellett a nyelvi nehézségek, etnikai különbözőségek is. Emiatt a harmadik, tisztán technikai megközelítés a leggyakoribb, széles körben rendelkezésre álló segédprogramok könnyítik meg az információszerzést.
Egy informatikai rendszer támadása három fő kategóriába sorolható:

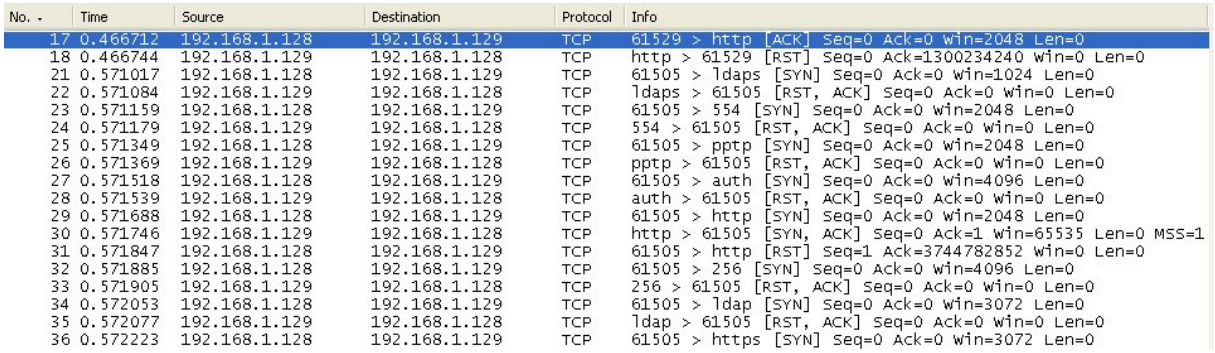
- lehallgatás;
- uralom átvétele;

- az üzemszerű működés lehetetlenné tétele.

A három módszer közül a lehallgatás megvalósítása csak speciális feltételek mellett (fizikai hozzáférés a célpont belső hálózatához, a rendszer valamelyik eleme feletti ellenőrzés megszerzése) vihető végbe. A rendszer feletti uralom megszerzése hosszadalmas, aprólékos munkát igényel, és szükséges hozzá valamilyen üzemeltetői hiba (helytelen rendszerkonfiguráció, a rendszer valamelyik elemének hibája, felhasználói gondatlanság). Az üzemszerű működés lehetetlenné tétele egy DoS vagy DDoS támadás segítségével könnyen végrehajtható, ha megvannak hozzá a szükséges eszközök. Egy rendszer sikeres megtámadásához a támadónak először fel kell mérnie a célpont sajátosságait:

- a célpont informatikai hálózatában üzemelő végpontok címeit;
- az ismert végpontok sajátosságait (operációs rendszer, szolgáltatások elérhetőségei);
- a végpontokon futó szolgáltatások esetleges hibáit;
- a rendszert használók adatait, esetleges hozzáférési jogosultságait.

Mindezt persze úgy kell elvégezni, hogy a célpontot üzemeltetők ne szerezzenek tudomást a készülő akcióról. A végpontok címeinek felmérése az Interneten viszonylag egyszerű. Az Internet hálózati protokolljaként a már nem túl fiatal IP (Internet Protocol), annak is a v4 verziója szolgál - bár létezik már egy korszerűbb, kevesebb sérthetőséggel rendelkező v6 változat is, annak elterjedése még várat magára. Az IPv4 minden hálózati végponthoz egy 32 bites azonosítót rendel, amely két részből áll össze: hálózati cím (ami a célpont hálózatát azonosítja) és végpont cím (amely a megcímzett hálózaton belül jelöli ki a végpontot). Az internetes címek kiosztása nem egyenként történik, hanem nagyobb egységekben, címtartományba szervezve. A címtartományok mindig csupa „0” értékű végpontbitekkel kezdődnek, és csupa „1” értékű végpontbitekkel érnek véget, a címtartományok egyediségének biztosítása céljából a tartományokat központilag tartják nyilván, és ugyanabba a címtartományba tartozó címeket nem osztanak ki két tulajdonosnak. Ezek a nyilvántartások bárki számára elérhetők, az európai IP címtartományokról például a http://www.ripe.net weboldalon lehet információt kérni. A keresés segítségével meghatározható az a tartomány, amelyben a célhálózat egyes elemei elhelyezkedhetnek, ezután már csak a tartományon belüli címeket kell ellenőrizni. A végpontok működőképességének ellenőrzésére egyszerűbb esetben elegendő a legtöbb operációs rendszerben „ping” névre keresztelt parancs használata, amely ICMP Echo Request üzeneteket küld a célpont számára, majd a válaszul kapott ICMP Echo Reply üzenetek beérkezését jelzi a kérést kiadó felhasználónak. Mivel az Echo Request üzenetre válaszoló végpontok könnyen elárulják a felderítést végzőnek létezésüket, ezért sok rendszergazda szűri az ilyen típusú üzeneteket. Ilyenkor tesznek jó szolgálatot a portszkennerek, amelyek speciális csomagok elküldésével és a válaszok elemzésével képesek a végponton üzemelő TCP vagy UDP módszerrel kommunikáló szolgáltatások felderítésére. A legismertebb és talán a legsokoldalúbb ilyen eszköz az „nmap” névre hallgató segédprogram, amely ingyenesen elérhető, akár forráskóddal együtt. Sokoldalú képességei nem csak a nyitott, de a külvilág irányába csomagszűrési beállításokkal lezárt szolgáltatások felderítése mellett az operációs rendszer hozzávetőleges megállapítására is alkalmasak. Az nmap népszerűsége és elterjedtsége akkora, hogy az Internetre kötött végponton néhány percenként megjelenik egy ilyen típusú felderítést végző program. Ha a szkennelés működését megvizsgáljuk, akkor látható, hogy a specifikus csomagok nem okoznak jelentős hálózati forgalmat, egyetlen port felderítése mindössze 114 byte adatforgalmat generál.



No.	Time	Source	Destination	Protocol	Info
17	0.466712	192.168.1.128	192.168.1.129	TCP	61529 > http [ACK] Seq=0 Ack=0 Win=2048 Len=0
18	0.466744	192.168.1.129	192.168.1.128	TCP	http > 61529 [RST] Seq=0 Ack=1300234240 Win=0 Len=0
21	0.571017	192.168.1.128	192.168.1.129	TCP	61505 > ldaps [SYN] Seq=0 Ack=0 Win=1024 Len=0
22	0.571084	192.168.1.129	192.168.1.128	TCP	ldaps > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
23	0.571159	192.168.1.128	192.168.1.129	TCP	61505 > 554 [SYN] Seq=0 Ack=0 Win=2048 Len=0
24	0.571179	192.168.1.129	192.168.1.128	TCP	554 > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
25	0.571349	192.168.1.128	192.168.1.129	TCP	61505 > pptp [SYN] Seq=0 Ack=0 Win=2048 Len=0
26	0.571369	192.168.1.129	192.168.1.128	TCP	pptp > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
27	0.571518	192.168.1.128	192.168.1.129	TCP	61505 > auth [SYN] Seq=0 Ack=0 Win=4096 Len=0
28	0.571539	192.168.1.129	192.168.1.128	TCP	auth > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
29	0.571688	192.168.1.128	192.168.1.129	TCP	61505 > http [SYN] Seq=0 Ack=0 Win=2048 Len=0
30	0.571746	192.168.1.129	192.168.1.128	TCP	http > 61505 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
31	0.571847	192.168.1.128	192.168.1.129	TCP	61505 > http [RST] Seq=1 Ack=3744782852 Win=0 Len=0
32	0.571885	192.168.1.128	192.168.1.129	TCP	61505 > 256 [SYN] Seq=0 Ack=0 Win=4096 Len=0
33	0.571905	192.168.1.129	192.168.1.128	TCP	256 > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
34	0.572053	192.168.1.128	192.168.1.129	TCP	61505 > ldap [SYN] Seq=0 Ack=0 Win=3072 Len=0
35	0.572077	192.168.1.129	192.168.1.128	TCP	ldap > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
36	0.572223	192.168.1.128	192.168.1.129	TCP	61505 > https [SYN] Seq=0 Ack=0 Win=3072 Len=0

1. ábra: nmap portszken csomagjai

A tapasztalt támadók ráadásul hosszabb idő alatt, kis intenzitással végzik az ilyen feladatot, emiatt a rendszeradminisztrátor számára láthatatlan lesz tényked esük. Néhány ritka kivételtől eltekintve a port letapogatás a végpont működését sem veszélyezteti, így az ilyen tevékenység nehezen minősíthető támadásnak. A célpont üzemeltetője – még ha tudomására is jut egy ilyen akció – semmilyen ellentevékenységet sem tud kifejteni (maximum olyan eljárásokat alkalmazhat, amik meghamisítják a felderítés eredményét).
Ha szolgáltatások adatait ismeri a támadó, a következő lépés a szolgáltatás verziószámának meghatározása, ennek ismeretében lehet valamilyen meglevő programozási hibát találni, aminek felhasználásával hozzáférés szerezhető. Természetesen erre is léteznek segédprogramok, azonban lényegesen egyszerűbb, „csendesebb” módon is meghatározhatók a kívánt paraméterek. A legtöbb szolgáltatást megvalósító program a kapcsolat létrejötte után egy üdvözlő szöveget küld a kliensnek (banner), és bár a lehetőség adott a szöveg eltüntetésére vagy kevesebb kényes információt tartalmazó módosítására, a legtöbb adminisztrátor nem veszi a fáradságot erre. Például egy SMTP szerver verziószámának lekérdezéséhez elegendő a célpont 25-ös TCP portjára csatlakozni egy egyszerű telnet alkalmazással:

```
telnet célpont 25

220 ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge3; Mon, 26 May 2008 20:38:11
+0200
```

A válasz árulkodó: a szerveren egy Sendmail nevű alkalmazás végzi az elektronikus levelek továbbítását vagy kézbesítését, előzékenyen még az operációs rendszer típusát (Debian Linux) is elárulja. Mivel a lekérdezés gyakorlatilag megegyezik egy levelező kliens tevékenységével, ezért itt sem beszélhetünk bűncselekményről, a nagyszámú beérkezett kapcsolat között elvesznek az ilyen típusú próbálkozások.
Ha gondatlan a rendszeradminisztrátor, akkor a felhasználói nevek könnyen meghatározhatók az elektronikus levélcímből, a támadónak ezután már csak egy megfelelő jelszót kell találnia. Ha a felhasználó saját jelszavát nem eléggé körültekintően választotta meg, akkor megint csak a reménybeli behatoló dolgát könnyítette meg.
Hasonló példákat lehetne még sorolni, az ismertetett eljárásokból viszont így is kiderül az a tény, hogy bár minden támadás a felderítéssel kezdődik, azonban ezt a folyamatot nem könnyű észrevenni. Ha mégis sikerül felfedni, akkor sincs túl sok törvényes lehetőség az elkövető korlátozására (általában még személyazonosságának felderítésére sem).

Passzív védekezés

Ha egy informatikai hálózat nem tartalmaz hibás, megtámadható elemeket, a rendszert használók kellően képzettek, vagyis minden ideális állapotban van, akkor nincs szükség védekezésre. Természetesen ez csak egy idealizált helyzet, hiszen minden rendszerben találhatók gyenge pontok, amiket egy kellően türelmes támadó képes kihasználni. Minden operációs rendszerben - akár a tűzfalakon futókban is - előfordulhatnak „0 napos sebezhetőségek" (0-day vulnerabilities), vagyis olyan programhibák, amelyeket még nem javítottak ki a rendszert fejlesztők. Az ilyen hibák ellen a leggondosabb rendszergazda is tehetetlen, mivel egy nem létező hibajavítást még ő sem tud telepíteni. A 0 napos sebezhetőségek egy támadónak kincset érnek, segítségével jelentős mennyiségű rendszert képes feltörni rövid idő alatt. Emiatt aztán az informatikai rendszerek folyamatos felügyeletet igényelnek, a támadás első jelére meg kell tenni a megfelelő ellenlépéseket. Az ellenlépések köre korlátozott, és csak akkor hajtható végre, ha a támadás ténye már bizonyított:

- a támadást - esetleg még csak a felderítést, ha a célpont ezt veszélyesnek ítéli - kezdeményező végpont elérésének korlátozása technikai eszközökkel (csomagszűrés hálózati szinten);
- a nemkívánatos tevékenységet végző végpont hálózati infrastruktúráját biztosító illetékes szervezet megkeresése és figyelmeztetése.

Mindkét megoldásban közös a probléma: a nemkívánatos végpontot megbízhatóan azonosítani, majd tevékenységét korlátozni kell. A végpont azonosítása látszatra egyszerű, mivel a rendszer naplóállományaiból kinyerhető az IP cím. Azonban az esetek döntő többségében a cím nem a tényleges támadóhoz tartozik, hanem egy proxy végpontként használt számítógéphez vagy pedig egy bárki által elérhető, névtelenül is használható hozzáférési ponthoz. A végpont tevékenységének korlátozása szintén gondokat okozhat. Példának okáért, egy üzleti tevékenységet végző weboldal a látogatói számára szolgáltatást nyújt. Ha ebből a szolgáltatásból egy személyt vagy egy csoportot kizár, akkor esetleg megszegi a saját szerződési feltételeit, ami miatt akár bíróságon is megtámadható.
A másik módszer szerint a megtámadott illetékese felveszi a támadó hálózati hozzáférését biztosító szervezettel a kapcsolatot és jelzi a támadás tényét. Az ilyen szervezet többnyire egy internet-szolgáltató, akinek erkölcsi feladata saját ügyfeleire ügyelni. Az általános gyakorlat szerint a szolgáltatók az „abuse@" kezdetű email címen fogadják az ilyen jellegű bejelentéseket. Az már egy teljesen más problémakör, hogy mekkora reakcióidővel dolgoznak (saját tapasztalataim szerint a 2 óra és a soha közötti intervallumon belül mozognak). A legtöbb esetben egy ilyen ügy véget ér azzal, hogy a szolgáltató ügyfelének gépén megtalálják a támadó által használt vírust vagy trójai alkalmazást és eltávolítják, a támadó pedig egy másik hálózatot igénybe véve rövidesen újra megjelenik a célpont hálózatának védvonalait vizsgálgatva. A nagyobb magyar internet-szolgáltatók szerződési feltételeit megvizsgálva azt tapasztalhatjuk, hogy foglalkoznak a hálózatukból kiinduló rosszindulatú akciók elkövetőinek korlátozásával. Az egyik megközelítés a T-Online ÁSZF-ben [4] található, és az ügyfél szolgáltatásának korlátozását helyezi kilátásban, ha az:
10.1.b.4 pont: „Az Előfizető a számára nyújtott szolgáltatást felhasználva jogosulatlan adatszerzésre, adatküldésre vagy más számítógépes rendszerekbe történő behatolásra tesz kísérletet illetve hajt végre…"
A UPC Magyarország ÁSZF [5] ezzel szemben nem részletezi a szankcionálandó tevékenységeket, hanem az Internet Szolgáltatók Tanácsa által kiadott hálózathasználati irányelveket fogadja el:

„A Szolgáltató elfogadja, és magára nézve kötelezőnek tekinti az Internet használata kapcsán kialakult és nemzetközileg elfogadott Hálózathasználati Elveket (AUP – „Acceptable Use Policy”), amelyek Magyarországon az Internet Szolgáltatók Tanácsa tesz közzé és vizsgál felül rendszeresen.”
A hálózathasználati irányelvek [6] megsértőivel szemben szintén a szolgáltatás korlátozását vagy a szolgáltatási szerződés felmondását helyezi kilátásba. Az ISzT irányelveiben részletesen szerepel minden tiltott tevékenység, beleértve az informatikai rendszerekbe történő behatolást és a túlterheléses (DoS) támadásokat is.
A külföldi hálózatok ügyfeleivel szemben azonban kétséges a fellépés eredményessége, egy rendszergazda gyakorlatilag a külföldi hálózat üzemeltetőire van utalva az ellenséges tevékenységet folytató ügyfelekkel szemben vívott harcában. Az ilyen esetekben lenne szükség állami felügyeletekre, akik a szolgáltatókat rákényszerítenék az együttműködésre és a hathatós segítség nyújtására.
Megállapíthatjuk, hogy bár a passzív védekezési módszerek fontos és elkerülhetetlen részei az informatikai rendszerek biztonságos üzemeltetésének, azonban hatékonyságuk nem a legmagasabb.

Aktív védekezés

Az aktív védelem két területre osztásával a katonai fogalmakkal újabb párhuzam állítható fel: ezek az ellencsapás és a megelőző csapás fogalmai. Az ellencsapás cyber megfelelője tisztán technikai szinten is kivitelezhető, nem szükséges a politikai, diplomáciai kapcsolatrendszert felhasználni hozzá. A támadó által alkalmazott módszerek a célpont számára is elérhetők, amiket a támadó azonosítása után be is vethet. Azonban a célpontra is vonatkoznak a szabályok, a támadásra hivatkozva sem alkalmazhat illegális módszereket. Egy klasszikus példa erre az eset, ami 1998-ban az Electronic Disturbance Theater (EDT) nevű radikális politikai szervezet és a Pentagon között történt [12]. Az EDT által a Pentagon webszervere ellen alkalmazott támadási módszer egy DoS támadás volt, a támadó végpontok internetes böngészőjében egy JavaScript nyelven írt alkalmazás nagy sebességgel elkezdett weboldalakat lekérni a Pentagon szerveréről. Kellően sok böngészővel és megfelelő hálózati sávszélességgel ez a módszer jelentős terhelést okoz a kiszolgálónak. Ahogy a támadás ténye kiderült, a Pentagon szakemberei azonnal ellentámadásba lendültek. A támadó kliensekre töltöttek egy Java appletet (hostileapplet), amely a böngésző képernyőjén kávéscsészéket - a Java logója - és az "ACK" üzenetet jelenítette meg akkora mennyiségben, hogy a böngésző erőforrásai elfogytak, ami a támadó számítógép lefagyását idézte elő. Az EDT fontolóra vette a Pentagon perbe fogását a „Posse Comitatus”, egy 1878-as törvény alapján, amely tiltja a katonaság bevetését a belföldi törvények betartatása során.
A megelőző csapás fogalmát a virtuális térben értelmezve a „békeidőben” végzett felderítés és a felfedett potenciális veszélyforrások megszüntetése jelenti, amire érdemes több figyelmet szentelni.
Napjainkban a legnagyobb fenyegetést a gomba módra szaporodó és egyre több végpontot tartalmazó botnetek jelentik. A botnetek felelnek a legtöbb DDoS támadásért, a kéretlen reklámlevelek küldésében pedig szinte egyeduralkodókká váltak. A klasszikus, előzetes felderítésen alapuló, a célrendszer sebezhetőségeit kihasználó betörés kivitelezése egyre nehezebb, a legtöbb operációs rendszeren már megvalósított automatikus rendszerfrissítéseknek köszönhetően. A rendszerüzemeltetők is egyre gondosabbak lesznek, az informatikai biztonság fontossága lassan bevonul a köztudatba. A hagyományos, „kézműves” jellegű támadásokat sem szabad lebecsülni, hiszen ezekkel lehet a legnagyobb erkölcsi és anyagi károkat okozni, azonban a túlterheléses támadások ellen keveset tehet az

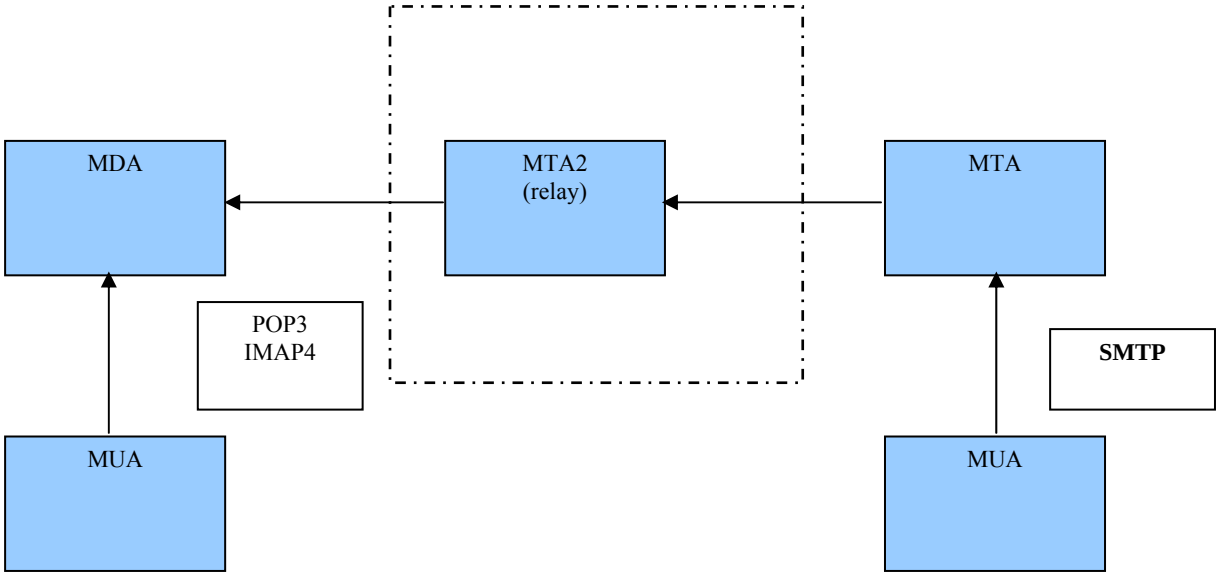
áldozat. Ha a támadás megindult, akkor már csak a kárenyhítés lehetséges, a túlterhelést okozó végpontok nagy száma miatt gyakorlatilag nem lehetséges egyedileg kitiltani az összeset. A nagyobb címtartományok kitiltása értelemszerűen korlátozza a nyújtott szolgáltatást legálisan igénybe vevők körét is.
A botnetek elleni küzdelemben fontos módszer lehet a megelőzés, a már megfertőződött végpontok – botok – felderítése és a szükséges ellenintézkedések megtétele. Egy botnet tag általában nyit a hálózat felé egy kommunikációs portot, amelyen keresztül várja az irányító számítógépektől az elvégzendő feladatot. Egyszerű feladat egy olyan alkalmazást készíteni, amely az Internetet (vagy csak a saját szűkebb környezetét) bejárva ellenőrzi az ismert botnet kliensek által megnyitott parancscsatornákat, majd ha ilyenre talál, akkor riasztást ad. Egy sikeresen elkapott és kivizsgált kliensből aztán már további információk nyerhetők a vezérlő, úgynevezett „command&control" végpontokról, így a teljes hálózat felgöngyölíthető. A gyakoribb botnet kliensek tesztelésére rendelkezésre is állnak ilyen alkalmazások, azonban a szélesebb körű, automatizált használattal szemben is lehet érveket felhozni:

- mivel ez az eljárás lényegében egy szűkített méretű portszkennelés, ezért – bár a cél nemes – az ilyen felderítést végző is az illegális tevékenység határait súrolja;
- az újgenerációs kliensek már szakítottak a hagyományos alá- és fölérendeltségi viszonyokon - a Command & Control struktúrával - és egyenrangú, Peer-to-peer hálózatként funkcionálnak (például a Storm Worm nevű [7]), emiatt az ilyen kliensek felderítése nem triviális;
- készíthetők olyan botnet kliensek, amelyek a felderítési szándékot érzékelve ellentámadást indítanak.

Egy másik, erkölcsileg sem támadható botnet kliens felfedési metódus az alábbi tényezőket használhatja ki:

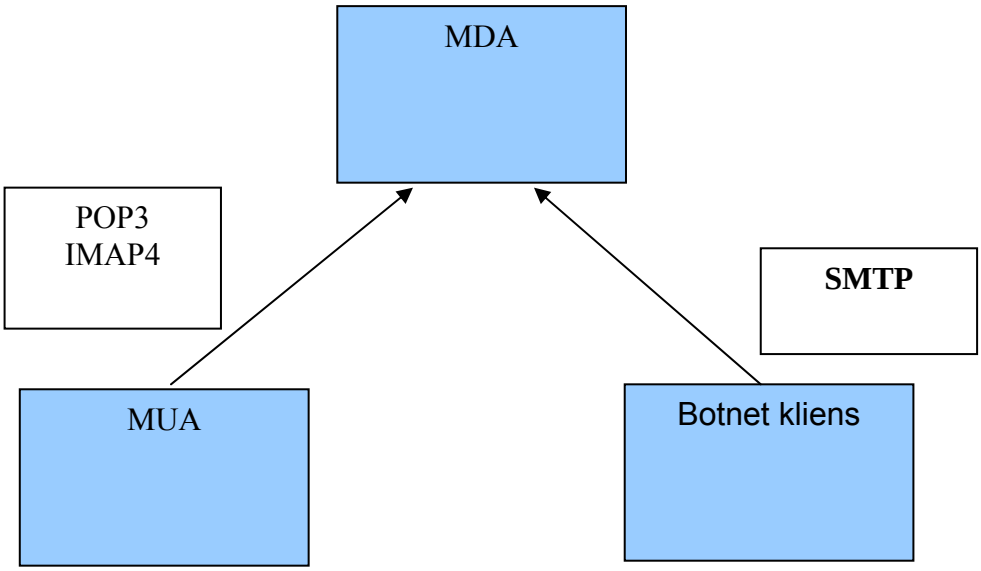
- a botnetek egyik legfontosabb feladata a kéretlen reklámlevelek (SPAM) küldése;
- a SPAM üzenetek túlnyomó többsége manapság botnet kliensektől származik;
- a SPAM a levelező szervereken viszonylag nagy megbízhatósággal szűrhető (95% feletti hatékonysággal);
- a levelező szerver a levél átvételekor ismeri a küldő végpont IP címét.

A metódus ismertetéséhez érdemes röviden áttekinteni az elektronikus levelek célba juttatásának menetét. A 2. ábra a folyamatban közreműködő elemeket mutatja be.



2. ábra: az elektronikus levelezés elemei

A levelet feladó a kliensprogram (Message User Agent – MUA) segítségével összeállítja a levelet, majd SMTP (Simple Mail Transfer Protocol) használatával elküldi a levelező szervernek (Message Transfer Agent – MTA). A levelező szerver megkeresi a címzett postafiókját kezelő másik levelezőszervert (Message Deliver Agent – MDA) és szintén SMTP használatával elküldi neki a levelet. A folyamatba közbenső szerverek is részt vehetnek (relay), ez főként nagyobb rendszerek esetén használatos. Az SMTP kezdeti verziója nem tartalmazott semmilyen hitelesítési folyamatot, ezért gyakorlatilag bárki küldhetett egy SMTP szerver számára levelet, amit az továbbított a címzett számára. Ekkor jelentek meg először a kéretlen leveleket küldők, akik könnyedén juttatták célba leveleiket az ilyen szerverek használatával. Később az SMTP szerverek a levéltovábbítási kéréseket (tehát az olyan levelek továbbküldését, amelyek címzettje nem a saját fennhatóságuk alá tartozik) már feltételekhez kötötték, például a küldőnek a szervert üzemeltető szolgáltató ügyfélkörébe kellett tartoznia, vagy egy jelszót kellett megadnia. A nem ezt a politikát követő SMTP szervereket feketelistára helyezik, ami azt jelenti, hogy a feketelistát figyelő más levelezőszerverek nem vesznek át leveleket tőlük.
Hamarosan megjelentek az olyan káros programok, amik saját SMTP továbbító mechanizmust tartalmaznak, azaz nem a szolgáltató SMTP szerverének küldik el a továbbításra a levelet, hanem közvetlenül a címzett postafiókját kezelő MDA számára.



3. ábra: közvetlen levéltovábbítás

Az első ilyen mechanizmust használó alkalmazások vírusok voltak, amelyek saját maguk terjesztésére használták a beépített SMTP motort. Napjainkban azonban már minden trójai program tartalmaz ilyen funkciót, vagyis a kéretlen levelek keresztül sem haladnak a botnet klienst futtató számítógép hálózati szolgáltatójának SMTP szerverén. Emiatt az ilyen levelek szűrése csak a címzett postafiókját kezelő szerveren (MDA) lehetséges, persze ha eltekintünk attól a valószínűtlen lehetőségtől, hogy az IP csomagok továbbítását végző útválasztók ismerjék fel a kéretlen leveleket.
Az MDA általában nem egyetlen címzett postafiókját kezeli, így komoly mennyiségű levél halad rajta keresztül. A levelek tartalmának vizsgálatára rengeteg termék áll rendelkezésre, víruskeresőktől kezdve a komolyabb szűrőprogramokig, amelyek a levelek szövegének statisztikai elemzésével öntanuló módon ismerik fel a kéretlen leveleket.
A SPAM minősítést kapott levelek feladója – pontosabban a feladó email címe – nem ismert, mivel mind a feladó neve, mind a feladó email címe hamisított. Ellenben az MDA rendelkezik egy fontos adattal: a számára a kéretlen levelet átadó végpont IP címével. A botnet kliensek hatékony felismeréséhez tehát elegendő a kéretlenként azonosított levelek küldőjének IP címét, valamint a küldés időpontját tárolni, és máris rendelkezésre áll egy lista a potenciális támadó végpontokról. Mivel a küldő gépek általában magánszemélyek otthoni gépei, ezért IP címeik nem tekinthetők állandónak. A legtöbb internet-szolgáltató ügyfelei számára nem biztosít kizárólagos használatú IP címeket, hanem rendszeres időközönként – tipikusan 24 óránként – megváltoztatja azt, ezért egy ilyen lista csak rövid ideig érvényes. A rövid érvényesség ellenére azért a végpontok azonosítására alkalmas, mivel az internet-szolgáltatók naplózzák az ügyfeleik számára kiadott címeket, így záros határidőn belül visszakereshető a fertőzött gép tulajdonosa.
A módszer hatékonyságának igazolására elvégeztem egy kísérletet. Olyan email címmel rendelkezem, amely nyilvánosan elérhető weboldalon szerepel, így már évekkel ezelőtt bekerült a SPAM küldők címlistájára. Ennek eredményeképpen napi több száz kéretlen levél érkezik a postafiókomat kezelő szerverre, amely szintén saját tulajdonú. 2008. április 25 és 2008. május 25 közti 30 napban azonosított 9904 kéretlen levelet összegyűjtöttem, majd egy egyszerű script segítségével kigyűjtöttem belőlük a küldő végpont IP címét, az eredményt pedig egy SQL táblába helyeztem. A feldolgozás eredménye az lett, hogy a 9904 kéretlen levelet 9117 különböző IP címről küldték, vagyis a legtöbb végpont nem fáradt azzal, hogy több kéretlen levelet is elküldjön. Az, hogy ez a szám ténylegesen hány fertőzött gépet és hány különböző botnetet jelent, ezzel a módszerrel persze nem lehet megállapítani. Fennáll

annak esélye, hogy ugyanaz a fertőzött gép több nap, különböző IP címekről is küldött levelet, bár ennek valószínűsége nem túl magas, figyelembe véve a SPAM küldés célpontjainak magas számát, illetve a botnetek roppant méreteit.
Látható, hogy egy viszonylag kis forgalmú levelező szerver és nem túl nagy mennyiségű levél vizsgálatával is komoly méretű, fertőzött gépekből álló hálózatokat lehet felfedni. Egy komolyabb forgalmú levelező szerver, amely naponta több százezer vagy akár millió elektronikus levelet vizsgál át, képes teljes botnetek feltérképezésére is. A folyamat automatizálásával megoldható lenne az IP címek szolgáltatók szerinti szétválogatása és a szolgáltatók illetékes szakembereinek értesítése is. Ha az internet-szolgáltatók felkészülnének – esetleg erre jogszabály kötelezné őket - az ilyen listák alapján az ügyfelek értesítésére vagy végső esetben a fertőzött ügyfél hozzáférésének korlátozására, akkor komoly pusztítást lehetne végbevinni a botnetek között, ami az Internet veszélyforrásait csökkentené.

Összegzés

Igyekeztem bemutatni a virtuális és a valóságos térben végrehajtott támadások közti árhuzamokat, rámutatni az ilyen jellegű tevékenységek elleni fellépés problémáira. A jog jelenleg még nem készült fel a tényleges támadás és az ártalmatlan felderítés közti vékony határvonal kezelésére. Az Internetet sokan használják illegális tevékenységre, amelyekkel a tisztességes felhasználók érdekeit veszélyeztetik, a „békeidőben” végzett megelőző tevékenységek pedig nem kellően szabályozottak, szervezettek. Bemutattam egy egyszerűen használható felderítési mechanizmust, amelyekkel fertőzött számítógépek fedhetők fel.

Irodalomjegyzék

[1] No 'sorry' from Love Bug author
http://www.theregister.co.uk/2005/05/11/love_bug_author/

[2] Terror Base UK

[3] Cyber catch-up
C4ISR Journal, March 2008 p: 20-21

[4] Általános szerződési feltételek a T-Online internet szolgáltatásra
http://www.t-online.hu/attached/20080411internet_aszf_20080411.pdf

[5] A UPC Magyarország Telekommunikációs Korlátolt Felelősségű Társaság
Internet-hozzáférési szolgáltatás nyújtására vonatkozó Általános Szerződési Feltételei
http://www.upc.hu/pdf/internet_ASZF_2008_0513.pdf

[6] Az ISzT által támogatott hálózathasználati irányelvek
http://www.iszt.hu/iszt/aup.html

[7] Storm Worm DDoS Attack
http://www.secureworks.com/research/threats/view.html?threat=storm-worm

[8] Gregory D. Grove, Seymour E. Goodman, Stephen J. Lukasik:
Cyber Attacks and International Laws
Survival, vol. 42, no. 3, Autumn 2000, pp.89-103

[9] Russians Seem To Be Hacking Into Pentagon
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL

[10] The Invasion of the Chinese Cyberspies
http://www.time.com/time/magazine/article/0,9171,1098961,00.html

[11] Az Egyesült Nemzetek alapokmánya
http://www.menszt.hu/layout/set/print/content/view/full/186

[12] Civil Disobedience in Cyberspace
http://home.clara.net/heureka/gaia/elec-act.htm

Az internetes források 2008. május 27-én elérhetők voltak.