HADMÉRNÖK

III. Évfolyam 4. szám - 2008. december

Előházi János
ZMNE Katonai Műszaki Doktori Iskola
elohazi.janos@gmail.com

AZ INTERNET, MINT KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA TÁMADHATÓSÁGA

Absztrakt

A cikk megpróbálja összegezni, milyen helyet is foglal el az Internet, mint infrastruktúra Magyarországon. Elemzi milyen fontossággal bír, és milyen módon is használjuk szolgáltatásait az országban. Az Internet technológia alapjait ismerve, az olvasó jobban megértheti, miként is végzik el a támadók a műveleteiket, és mik azok az értékek, melyeket védenünk kell; egy Internetre kapcsolt rendszernek milyen biztonsági aspektusoknak kell megfelelnie; és milyen lehetséges támadási módszerek állnak ma rendelkezésre; milyen forrásokból kerülhetnek a rendszerbe nem kívánt kártékony programok, és milyen mértékben veszélyeztetik egyes fajtájuk az elektronikus értékeinket. A cikk felsorolja a rendelkezésre álló védekezési módszereket, ahogy az egyes felhasználók és szervezetek megvédhetik adataikat az Internetről érkező támadásokkal szemben.

In this article I try to summarise, the place of the Internet as an infrastructure in Hungary, its importance, and the ways it is used in the country. Knowing the basics of Internet technology, the reader gets a better understanding how attackers are performing their operations in this area, and what are the values, that need protection; how an Internet facing system has to set up its security guidelines, and what sort of possible attacking methodologies are available and common today; what are the sources of malicious programmes, what is their scope of destruction. The article also outlines the possible defensive methods how individuals and organisations can protect their electric values against attacks from the Internet.

Kulcsszavak: *információs társadalom, internetes biztonság, kártékony programok ~ information society, Internet security, malicious softwares*

Bevezetés

Az információs társadalom politikai és gazdasági működésének középpontjában az információ előállítása, elosztása, terjesztése, használata és kezelése áll. A megfelelő hatékonyság és sebesség elérése érdekében az információ-technológia vívmányainak széles körű alkalmazása a jellemző.[1] Így amellett, hogy az információs-társadalom működési formája a ma ismert leghatékonyabb, rettentő módon függ a felhasznált technikai eszközöktől. Az információ feldolgozás minden pontján kiemelt szerepet kap a digitális technológia. Az információ tárolását nagy tárolókapacitású számítógépes szerverfarmok oldják meg, az információ előállítását nagy részben számítógépes programok valósítják meg, az információhoz való hozzájutást és annak kezelését szintén számítógépekkel végezzük, az információk elosztásában és terjesztésében pedig a számítógépes hálózatok játszanak szerepet.

Az információ kezelés végpontjai (az előállítás és a kezelés) megvalósítható hálózati kapcsolatok nélkül, un. offline módon is. Vegyünk például egy űrlap kitöltését, egy fénykép elkészítését vagy egy dokumentum megírását. Ezek a műveletek nem igényelnek hálózati kapcsolatokat. Az információ kezelése is megvalósítható hasonló módon, vegyünk például egy elektronikus könyv elolvasását, vagy a digitális fényképek szerkesztését. Az információ feldolgozásának legkritikusabb pontja az információ elosztása és terjesztése. Ezt leggyorsabban számítógépes hálózatok segítségével tehetjük meg. A modern háztartások és munkahelyek elengedhetetlen infrastruktúrája a (szélessávú) hálózati kapcsolat. A mindenki számára elérhető hálózati infrastruktúra pedig az Internet.

Az Internetet használjuk, hogyha a munkánk elvégzéséhez szükségünk van plusz információra (pl.: internetes keresőprogramok használata), ha az előállított információt továbbítani szeretnénk (pl.: e-mail formájában). Az Internet univerzitásának köszönhetően ma már segítségével nézünk videó filmeket (pl.: youtube), tartjuk a kapcsolatot ismerőseinkkel (pl.: chat programok), intézzük adminisztrációs ügyeinket (pl.: elektronikus kormányzat, vagy internetes banki alkalmazások), szórakozunk (pl.: online játékok használata). De az Internetet vesszük igénybe akkor is, ha olyan „hagyományos” szolgáltatásokat veszünk igénybe, mint a telefonálás (pl.: VoIP[1], vagy UMTS [2]mobil hálózatok), tévé adások megtekintése (pl.: IP TV vagy Joost), vagy ha bankkártyánkat felhasználva fizetünk a megvásárolt árucikkekért. Látható, hogy az Internet az életünk minden pontján jelen van, és nap, mint nap igénybe vesszük az általa nyújtott szolgáltatásokat.

Az Internet egyben kritikus információs infrastruktúrának is minősül. Működése alapvető fontosságú az információs társadalom léte szempontjából. Ezért az Internet biztonságának szavatolása a kritikus információs infrastruktúra védelem egyik sarkalatos pontja.

Az Internet technológiai alapjai

Az Internet technológia megszületése 1978-ra tehető. A kor számos egymással inkompatibilis hálózati megoldásai egy olyan magas szintű protokollt kívántak meg, ami tetszőleges hardverarchitektúrán működik, elfedve a hálózatot használó alkalmazások elől annak technikai sajátosságait, és egységes felületet biztosít a magasabb rétegek felé. Ez a hálózati protokoll az Internet protokoll (IP). Az IP egy állapotnélküli, úgynevezett csomagkapcsolt protokoll, melynek az adatátvitel mellett a fő funkciója az útvonalválasztás heterogén fizikai rendszerek felett. A végpontokon és a köztes csomópontokon (routerek) egyaránt implementált. Az útvonalválasztás az IP csomag fejlécében meghatározott paraméterek, vagy fix útvonal leírás alapján történik a köztes csomópontok fix útvonalválasztó tábláinak felhasználásával. A csomag küldője meghatározhatja, hogy a csomag sértetlensége, vagy

[1] Voice Over IP – IP alapú hangátvitel
[2] Universal Mobile Telecommunications System, a 3G mobil hálózatok technológiája

gyors átvitele a fontosabb számára. Az elsőt adatátvitelnél, a másodikat valósidejű alkalmazások (VoIP, video on demand) esetében alkalmazzák. A köztes csomópontok ezen információk alapján illetve statisztikai adataik felhasználásával el tudják dönteni, merre küldjék tovább a csomagot. Példa lehet az útvonalválasztás befolyásolására, amikor a küldő rendelkezik olyan információval, mely hálózati szegmenseken nem szeretné keresztülküldeni csomagját (pl.: afganisztáni szervereken keresztül), és e hálózati szegmenseket az IP csomag fejlécében feltünteti.

Az IP protokoll számos biztonsági problémával küzd:

- az egyes csomagok tartalmát az átvitel során bárki módosíthatja, mivel azok nem védettek (nem titkosítottak, nincsenek aláírva);
- tetszőleges IP csomag létrehozható tetszőleges forrás IP címet megadva, mivel az IP címek nincsenek azonosítva;
- az IP csomagok adattartalma titkosítható, a fejléce viszont nem kódolt, ezért az abban tárolt információ szabadon hozzáférhető, lehetővé téve a támadó félnek, hogy forgalomanalízis segítségével következtetéseket vonjon le;
- a köztes csomópontok közötti routing-táblák aktualizálása hitelesítés nélkül zajlik le, ami lehetővé teszi az egyes routerek tárolt információinak összezavarását, ezáltal létrehozhatók hurkok és elszigetelt partíciók, átirányítható minden forgalom a támadó hálózatára, hogy ott szabadon azt megfigyelje, vagy módosítsa, ill. túlterhelt csomópontok hozhatóak létre (DoS[3] támadás). [2]

A fenti bekezdésekből látható, hogy ma már az informatikai biztonság legalapvetőbb feltételeinek sem felel meg a 30 éves protokoll. Ennek főképp történelmi okai vannak. Egyrészt a technológia megszületésekor a hálózatok mai szintű elterjedése nem volt jellemző, ezért a mérnökök nem is gondoltak magas védettség alkalmazására. Másrészt az Egyesült Államokban a titkosítási algoritmusok exportja tilos volt, azok külföldre juttatása börtönbüntetést vont maga után. Mivel a hálózatok országhatárokon átíveltek, ezért a titkosítási technológia nemzetközi szinten való alkalmazását a törvénykezés nem tette lehetővé. Bár később születtek megoldások, melyek az IP szintjén kezelték a biztonságot (IPSec), de mivel alkalmazásuk nem volt kötelező, nem terjedtek el általános hálózatokon. Ezen okok miatt, a mai napig magasabb szinten, az alkalmazásokban kell megoldani az adatok biztonságát.

Az Internet biztonsági kritériumai

A számítógépes rendszerek rendkívül összetettek. Ugyanaz az infrastruktúra számos alkalmazást szolgál ki, pl.: fájlmegosztás, nyomtatószerver, levelezés, alkalmazás-szerverek kommunikációja, VoIP kommunikáció, videokonferenciák közvetítése. Lehetetlennek tűnő feladat minden alkalmazás szemszögéből megvizsgálni az infrastruktúra biztonságát, ám a gyakorlat öt tényezőt talált, melyek mentén egy informatikai rendszer biztonsága mérhető.

- Azonosítás: mind a kiszolgáló mind a kliens azonosítását értjük alatta. Az azonosítás történhet valamilyen közös titok alapján (belépési név/jelszó páros) – ez az azonosítási forma ma már nem nyújt megfelelő védelmet. Ha nem körültekintően választjuk meg a jelszót, az a mai nagy teljesítményű számítógépekkel, és a létező szótáradatbázisok segítségével viszonylag könnyen kitalálható. Az azonosítás történhet valamilyen birtok és a hozzá tartozó jelszó párosával. Ilyen a gyakorlatban a digitális aláírást tartalmazó smart-card és a hozzá tartozó PIN kód. A kártya ellopásával a támadók nem férhetnek hozzá a rendszerhez, amíg a hozzá tartozó kód nem kerül a birtokukba. A legmagasabb szintű azonosítás a biometriai azonosítás, ami a felhasználóra

[3] Denial of Service – Túlterheléses támadás online rendszerek ellen

egyedileg jellemző tulajdonságot alkalmazó authentikációs folyamat: ujjlenyomat, írisz minta, fül alakja, hang.

- Integritás: az üzenet sértetlenségét és megmásíthatatlanságát biztosító eljárásokat értjük alatta, melyek védik az átviendő adatokat az átvitel során. A gyakorlatban az átvitt adatból nyernek mintát, valamilyen egyirányú függvénnyel (hash függvény: az adatból bármikor előállítható a lenyomat, de a generált mintából nem állítható elő maga az adat), és ezt a mintát írják alá digitálisan. A vevő ugyanúgy legenerálja a mintát a fogadott adat alapján, amit összevethet a küldő által átküldött, aláírt mintával. Ha a kettő megegyezik, az átvitel során nagy valószínűséggel nem módosult az adat.
- Letagadhatatlanság: a tranzakció végrehajtásának bizonyíthatóságát szolgálja minden résztvevő számára. Főleg banki és e-business alkalmazásokban jelentős.
- Bizalmasság: a címzetteken kívül más ne férhessen az adatokhoz. Valamilyen szabványos szimmetrikus vagy aszimmetrikus kulcsú titkosítási eljárás segítségével az átviendő adatot titkosítják (DES[4], AES[5], Rijndael[6], RC4[7], RSA[8]). A szimmetrikus eljárás során ugyanaz a kulcs a titkosító és a dekódoló függvény kulcsa, amíg aszimmetrikus titkosítás során a két kulcs különböző, és egymásból nem kiszámítható. Míg az első esetben meg kell oldani, hogy a vevő fél is megkapja a kulcsot, a második esetben a kódoló kulcs nyilvános, a dekódoló kulcs csak a fogadó által ismert. Az aszimmetrikus eljárás elég költséges művelet, ezért a gyakorlatban aszimmetrikus kódolással titkosítják a szimmetrikus kódoló kulcsot, és így juttatják el a fogadó fél számára. Magának az adatnak a titkosítása a kevesebb számítást igénylő szimmetrikus kulcsú titkosítással történik.
- Rendelkezésre állás: a legegyszerűbb támadás során a cél a szolgáltató megbénítása, így az képtelen válaszolni a hozzá érkező valós kérésekre. Ezek az úgynevezett denial of service támadások, melyek kivédésére számos technika létezik.[2]

A fertőzések forrásai

Az Internet amellett, hogy az élet számos területén meggyorsítja az ügyintézést és az információhoz való hozzájutást, egyben számos veszélyforrást is jelent. Egy számítógép vírus- és tűzfalvédelem hiányában számos (automatikus) támadásnak van kitéve, melyek eredményeképpen perceken belül több tucat különböző kártékony kód kerülhet a gépre. Ezek nagy része a felhasználó aktív közreműködése nélkül, az operációs rendszer hiányosságait kihasználva, automatikusan feltepül. A gép felhasználója a telepítési procedúrából semmit sem érzékel, csupán a fertőzés eredményét veheti észre. Ez állhat abból, hogy a számítógép teljesítménye rohamosan csökken, vagy gyanús működést produkál. Az egyik ilyen fertőzés például az un. távoli eljáráshívási protokoll hiányosságait kihasználva a számítógép folyamatos újraindítását okozza [3]. Ez a fertőzés az adott számítógép használatát korlátozza, illetve más sebezhető gépek fertőzését végzi el.

Az ilyen típusú fertőzést automatikus szkriptek okozzák, melyek véletlenszerűen kiválasztanak egy IP címet a hálózaton, és az ehhez az IP címhez tartozó gépet fertőzik meg, így a felhasználónak nem „kell” aktívan közreműködnie. Léteznek azonban olyan kártékony kódok is, melynek telepítéséhez a felhasználó aktív közreműködése szükséges. Kihasználva a felhasználó hiányos ismereteit a kártékony kódot valamilyen Internetes interakció során juttatják fel a támadók a célszemély számítógépére. A kód általában egy weboldalon kerül

[4] Data Encryption Standard – szimmetrikus kulcsú blokk-titkosítási eljárás
[5] Advanced Encryption Standard – szimmetrikus kulcsú blokk-titkosítási eljárás
[6] Az AES algoritmus másik elnevezése
[7] Szimmetrikus kulcsú folyamkodolási eljárás
[8] Aszimmetrikus (nyilvános) kulcsú titkosítási eljárás

elhelyezésre, melynek betöltődése során a kártékony program automatikusan felkerül a weboldalt látogató számítógépére. A nehezebb feladat, hogy a felhasználót a kártékony weboldalra irányítsák. Erre számos módszer létezik. A legkézenfekvőbb megoldás az internetes kéretlen levelek alkalmazása. Ezek az un. spam e-mailek. A spam e-mailek tartalma általában valamilyen termék vagy szolgáltatás eladása a bolti ártól jóval olcsóbban, az e-mail szövege pedig tartalmaz egy linket a kártékony oldalra. Az ilyen e-mailek tartalmazhatnak pornográf típusú hirdetéseket, melyekben internetes videókamerák vagy videó-chatszobák internetes címei találhatóak, de számos egyéb, az érdeklődést felkeltő tartalom szerepelhet spam üzenetekben. Elterjedt módszer közismert, gyakran látogatott oldalak címéhez hasonló című oldalak létrehozása is, melyekre a felhasználók az eredeti cím mellégépelésével jutnak. Az e-mailekben eljuttatott címek sokszor un. spoofing üzenetek elküldésével is eljuttathatók a célszemélyhez. A spoofing e-mailek olyan weboldalakra irányítják a felhasználót, melyek hasonlítanak az eredeti szolgáltató oldalaira, de a céljuk a felhasználók titkos, személyes adatainak a megszerzése, de emelett tartalmazhatnak kártékony kódokat is. Ilyen spoofing üzenetek lehetnek hamis eBay üzenetek, vagy a tavalyi év során kifejezetten magyar piacra szánt internetes banki portálokra irányító üzenetek is.

A felhasználó e-mail címére sokféleképpen tehetnek szert a támadók. Egyrészt a fertőzött gépeken szereplő levelezőrendszer címjegyzékét felhasználva, vagy internetes oldalakat átfésülve publikált e-mail címek után kutatva gyűjthetőek be ezek az információk.
Az ilyen módszerekkel települt kártékony kódok sokféle feladatot látnak el. Egyrészt továbbíthatnak szenzitív adatokat a felhasználó akcióiról (milyen weboldalakat látogatott meg, felhasználói nevek és jelszavak ellopása), felhasználhatják a felhasználó gépét a kártékony kódra irányító e-mailek elküldésére (a felhasználó címjegyzékében szereplő e-mail címek felhasználásával), de legtöbbjük lehetővé teszi, hogy a támadó a fertőzött gépet tetszőleges célra alkalmazhassa a felhasználójának tudta nélkül. Az ilyen típusú kóddal fertőzött számítógépeket nevezzük zombi gépeknek. Az elnevezés abból ered, hogy a felhasználó tudta nélkül, egy harmadik személy akaratát is végrehajtják ezek a számítógépek. [4]

Kártékony kódok fajtái

A számítástechnikai biztonsággal kapcsolatos szakzsargon botnet-nek nevezi az olyan számítógépekből álló hálózatot, melyeken olyan program került telepítésre, ami lehetővé teszi egy kívülálló számára, hogy az adott eszközt tetszőlegesen felhasználhassa saját céljai eléréséhez. Az ilyen zombi számítógépek így részt vehetnek a felhasználójuk tudta nélkül internetes támadásokban. [5] [6]
A támadó céljait megvalósító kártékony programok három csoportba sorolhatóak:

- férgek,
- trójai programok és
- backdoor programok.

A férgek önmagukat sokszorosítani képes programok, melyek a fertőzött számítógép hálózati kapcsolatait kihasználva más eszközök megfertőzésére törekszenek anélkül, hogy bármiféle felhasználói interakciót igényelnének ennek a műveletnek a végrehajtására. A vírusokkal ellentétben nem szükséges, hogy más programokhoz kapcsolódjanak. A férgek általában a gazda számítógép erőforrásait nem károsítják, csupán az általa használt hálózat átviteli képességeit rontják, mivel a forgalom nagy része a féreg replikációs folyamataiból származik. A férgek általában az operációs rendszer gyenge pontjait használják ki. Az operációs rendszer naprakészen tartásával, rendszeres frissítések letöltésével megakadályozható, hogy a számítógépen települt férgek további kárt tegyenek más rendszerekben [7].

A trójai programok nevüket a trójai faló története kapcsán kapták, mert működési elvük nagyban hasonlít a klasszikus történetben szereplő trójai faló céljához. A trójai programok rendelkeznek egy elsődleges és egy másodlagos funkcióval. Az elsődleges funkció az, amit a számítógép felhasználója érzékel, és ez számára lehet bármilyen hasznos feladat megoldása. A háttérben azonban a trójai programok vírusokhoz hasonló műveleteket is elvégeznek, melyekről a felhasználó egyáltalán nem szerez tudomást. A másodlagos funkciók lehetnek kártékonyak is az adott eszközre nézve, de az esetek nagy többségében olyan interfészt szolgáltatnak tetszőleges kívülálló fél számára, mely felhasználásával az adott gép erőforrásait képes felhasználni. A trójai programok nem sorolhatóak a vírus kategóriájába, mert önmaguk sokszorosítására nem képesek, vagy nem is szerepel az alkotóik céljai között, de működésük a felhasználó és számítógép nagyfokú kiszolgáltatottságához vezetnek. A trójai programok rejtett szolgáltatásai általában a következők:

- külső hozzáférés biztosítása a rendszer erőforrásaihoz,
- adatkárosítás,
- letöltések végrehajtása,
- trójai szerver (HTTP, FTP, IRC, e-mail stb. szerverek futtatása),
- biztonsági programok kiiktatása és
- DoS támadásokban való részvétel.

A fertőzés általában úgy kerül a rendszerbe, hogy a felhasználó (megfelelő biztonsági programok üzemeltetésének hiányában) félrevezethető, és önmaga telepíti a kártékony kódot a számítógépre. A kártékony kód eljuttatható a felhasználóhoz e-mailben, ftp-n, weboldalon, tetszőleges adathordozón (CD, USB drive stb.). A trójai programok a számítógépen valamilyen rejtett formában léteznek, ezért legtöbbször a böngésző program átmeneti fájljai között találhatóak meg, vagy a lomtár területén, de kapcsolódhatnak legitim programokhoz is, mint például egy szövegszerkesztő alkalmazás. [8]

A backdoor programok egy hátsó ajtót nyitnak a fertőzött rendszeren, melynek felhasználásával a támadó a rendszer azonosítási folyamatait megkerülve képes elérni az eszköz erőforrásait anélkül, hogy jelenléte feltűnne a rendszer felhasználóinak. Az ilyen jellegű programok a többfelhasználós operációs rendszerek széles körű elterjedésével jutottak jelentős szerephez. A hátsó ajtót nyitó programok felkutatása nem egyszerű feladat, hiszen számos formában létezhetnek: lehetnek csupán egy véletlenül a programban felejtett alapértelmezett felhasználó név/jelszó páros vagy egyéb akár gépelési hiba is. Az ilyen biztonsági rések nehezen felfedezhetőek, mert sok esetben a program forráskódját kell elemezni hozzá, ami kereskedelmi programok esetén nem megoldható, hiszen a gyártó nem bocsátja rendelkezésre azt, illetve a korunkra jellemző összetett és nagyméretű alkalmazások esetén ez több millió programkód átvizsgálását jelentené.

A backdoor programoknak két nagy fajtája van a szimmetrikus és az aszimmetrikus programok. A szimmetrikus backdoor bárki által használható, aki tud a létezéséről, az aszimmetrikus backdoor-t csak az tudja használni, aki eredetileg is alkalmazni akarta, még akkor is, ha a kód teljes implementációja publikussá válik. Az aszimmetrikus backdoor programokkal foglalkozó tudományág a kriptovirológia. [9]

A zombi számítógépek hálózatából álló botnetek számos célt szolgálnak. Segítségükkel küldhető el nagy mennyiségű spam e-mail vagy végezhető el akár elosztott DoS támadás. A hálózat összetettsége miatt a támadás indítójának kiléte nehezen kideríthető. 2007-ben az amerikai FBI programot hirdetett a botnetek üzemeltetői ellen. A program során csupán az első egy évben 20 millió dollár értékű bizonyított kárról számoltak be. A károk megtérítésére nem sok esély van, viszont a felelősök szigorú büntetésével azt remélik, hogy az elrettentő hatású lesz. [10]

A végső megoldást ugyanakkor a kártékony technológia felszámolása lenne, ugyanakkor ez rendkívül nehéz feladat, mert a jelenlegi rendszerek használatával a felhasználók

felelősségteljesebb magatartását követeli meg, ami a nem megfelelő képzettség miatt, lehetetlen követelményt támaszt.

Támadási módszerek

Számos módszer létezik arra, hogy számítógépeket olyan kártékony kóddal fertőzzenek meg, melynek segítségével jogosulatlan fél is igénybe veheti erőforrásait. A támadási módszereket két nagy csoportba oszthatjuk: az egyik csoportba tartozó támadási módszerek nem igénylik a felhasználói interakciót, mert az operációs rendszer biztonsági hibáit használják ki; a másik csoportba tartozó módszerek viszont a felhasználó tudatlanságát kihasználva juttatják a kártékony kódot a rendszerbe. Mindkét módszernek megvannak az előnyei és a hátrányai. Az első csoport támadási módszereinek az előnyei:

- a támadás sikeressége nem függ a felhasználótól;
- automatizált támadási folyamat, így sokkal gyorsabban és nagyobb számú célpontot ér el.

Hátránya viszont, hogy a gyártók igyekeznek minden felfedezett biztonsági rést a legrövidebb idő alatt kijavítani, így egy ilyen módszer igazán csak nagyon rövid ideig hatékony; bár a gyakorlat azt mutatja, hogy nagy számban vannak olyan felhasználók, akik nem törődnek rendszereik folyamatos frissítésével, ezért ők továbbra is veszélyeztetettek illetve veszélyforrásnak számítanak.

A második csoportba tartozó módszerek a felhasználó aktív közreműködését igénylik, kihasználva felhasználói ismeretének hiányait vagy hiszékenységét. Az ilyen támadások legtöbbször e-mailben vagy azonnali üzenetküldő rendszereken (pl.: MSN Live, IRC) terjednek. A forgatókönyv minden esetben hasonló: a címzettet el kell irányítani egy weboldalra, amelyről a kártékony kód települ a számítógépére. Számos módszer létezik arra, hogy a felhasználó óvatosságát kijátsszák, melyek az előző fejezetben kerültek ismertetésre.

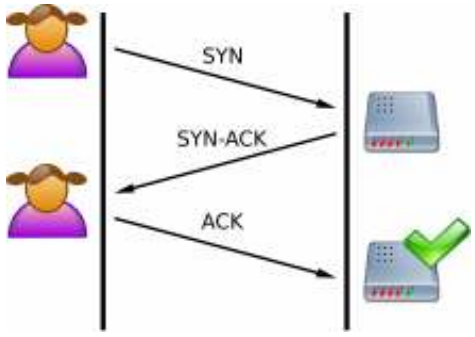
Az Internet elterjedésével szinte megszűntek a hagyományos módon, adathordózón terjedő kártékony kódok. A 80-as és 90-es években szinte csupán floppy lemezen majd később optikai hordozón esetleg USB tárolón terjedő férgek és vírusok léteztek. A manapság létező ilyen programok nagy része, nem is próbál cserélhető háttértárolókon terjeszkedni, hiszen az online világban sokkal gyorsabban és hatékonyabban végezhető el ez a munka, illetve az offline számítógépeken nem is tudják igazi céljukat elérni. A klasszikus vírusokkal ellentétben a mai társaik már nem a számítógépek használhatatlanná tételére összpontosítanak, hanem a fertőzött eszköz kapacitását és erőforrását igyekeznek kihasználni, és harmadik fél számára rendelkezésre bocsátani, hogy könnyen felhasználhatóak legyenek egy online harcban.

Sajnos minden erőfeszítés ellenére az Internet forgalmának nagy részét a mai napig a kártékony célú adatfolyam teszi ki. Mivel ez hasznos sávszélességet foglal el, az egész rendszer hatékonysága csökken. A szélessávú elérések terjedésével és azáltal, hogy egyre több háztartás kapcsolódik az online világhoz a rendszer hatékonyságának növelése egyre égetőbb feladat, ezért a kártékony célú programok ellen folytatott harc egyre nagyobb jelentőségű.

Az elosztott túlterheléses támadás az egyik legelterjedtebb, és egyben legegyszerűbb támadási forma. A túlterheléses támadások célja olyan mennyiségű célzott adattal bombázni a célpontot, hogy az nem képes tovább valós feladatát ellátni mivel a rendelkezésre álló sávszélességét a túlterheléses támadás fogja le, vagy az adatok feldolgozásával próbálkozva számítási és memória kapacitása kerül túlzott mértékben felhasználásra. Bizonyos esetekben ez a módszer a célzott rendszer összeomlásához is vezethet, ezáltal a célpont hosszabb ideig nem képes kiszolgálni az igényeket anélkül, hogy a támadónak aktív támadást kellene végeznie, mivel a rendszer helyreállításához és újraindításához hosszabb idő szükséges.

A hagyományos túlterheléses támadás esetében a támadó rendszer bemérhető, hiszen csupán onnan érkezik a nagymennyiségű adatfolyam. A küldő izolálásával a támadás kivédhető. Az elosztott túlterheléses támadás esetében a túlterhelő adatfolyam nem egy, hanem akár több millió forrásból is jöhet. Az adatfolyam nagyságát az egyes forrásokra vetítve nem is biztos, hogy kiugró mennyiségről van szó, csupán a sok kicsi, sokra megy elvet követve éri el a támadó a célját. A védekezés egy ilyen támadás ellen nagyon nehéz, hiszen szinte lehetetlen felismerni a támadók kilétét és kizárni őket a rendszerből.

A túlterheléses támadásnak számos típusa létezik, ami az internet protokoll (IP) különböző gyenge pontjait igyekszik kihasználni. A legegyszerűbb mód a célpont nagyszámú TCP[9]vagy UDP[10] csomagokkal való bombázása. A TCP és UDP csomagok normális esetben az átviendő adatot tartalmazzák, ezek feldolgozása minden internetes szerver elsőrangú feladata. Ha ezekből egyszerre több érkezik, mint amivel a célpont meg tud birkózni, a támadás sikeres. Emellett léteznek olyan támadási formák, ami az IP vezérlő folyamatait támadják. Ilyen például a SYN támadás. A SYN támadás a TCP protokoll három utas protokollja, ami egy kliens és egy szerver közötti alacsony szintű kapcsolat felépítését végzi el. Normális esetben a kliens küld egy SYN üzenetet a szervernek, aki visszaküld egy SYN-ACK üzenetet a kliensnek, aki egy ACK üzenetben válaszol (ld.: 11. ábra). Ha ez a protokoll sikeresen lezajlott a szerver és a kliens azonosította a kettejük közötti adatfolyamot, és megkezdődhet a tényleges adás. Az ez ellen történő támadás azt használja ki, hogy a szerver egy ideig fenntart a kapcsolatkérő számára csatornát, amíg az ACK üzenetet nem kapja meg. A támadó nagyszámú SYN üzenetet küld a szervernek, aki SYN-ACK üzenetekkel válaszol, és megteszi a szükséges erőforrás lefoglalásokat, hogy az újonnan nyitott csatornák rendelkezésre álljanak az ACK üzenet megérkezésekor. A támadó azonban vagy nem küldi vissza az ACK üzeneteket, vagy az eredeti kérésben hamis IP címet szerepeltet, így a SYN-ACK üzenetek nem érnek sohasem célba. A támadás végén a szerver összes erőforrása le lett foglalva, és az újonnan érkező kliensek számára már nem létezik használható csatorna, és a szerver nem képes ellátni a feladatát. [15]



1. ábra TCP három utas kapcsolatfelépítés [14]

A SYN támadás mellett még létezik az IP spoofing, a smurf és a fraggle támadás. Az IP spoofing kihasználja, hogy az IP csomag fejlécében szerepel a küldő fizikai címe. A támadó nem a valós címét közli a címzettel, és annak válaszát igyekszik megbecsülni, ezáltal felépít egy kapcsolatot a kiszolgálóval úgy, hogy elrejti saját fizikai címét, vagy a támadó egyáltalán nem is törődik a válasz tartalmával. Túlterheléses támadás során a kiszolgáló úgy érzékeli, hogy a csomagok más-más gépről érkeznek, szemben a valósággal, és ez által nem képes kiszűrni a támadó személyét. [16] A smurf támadás során hamis címről küld a támadó ping üzeneteket. A ping üzenetek eredeti célja felderíteni, hogy a ping címzettje elérhető-e azáltal,

[9] Transmission Control Protocol – Átviteli protokoll IP alapú hálózatokon, amely a csomagok sorrendjét megőrzi
[10] User Datagram Protocol – Átviteli protokoll IP alapú hálózatokon, amely a csomagok sorrendjére nem fordít figyelmet

hogy válaszol-e a ping üzenetre vagy sem. A ping üzenetek broadcast címre irányításával elérhető a támadott rendszer túlterhelése. [17] A fraggle támadás annyiban különbözik a smurf támadástól, hogy nem a TCP rétegen, hanem az UDP rétegen végzi el ugyanazt a támadási mechanizmust. [18]

Az elosztott túlterheléses támadás kivitelezése a nagyszámú, kártékony kóddal fertőzött online számítógépeknek köszönhető. A legtöbb kártékony kód célja (önmaguk replikálásán túl) egy ilyen támadásban való részvétel. Erre egy példa a MyDoom nevű féreg, ami 2004-ben jelent meg, és a MS Windows operációs rendszerrel futó számítógépeket támadta meg. A MyDoom egy hátsó ajtót nyitott a számítógépen, és túlterheléses támadásban volt képes részt venni. A támadás idő- és célpontja előre meg volt adva, a fertőző kód magában foglalta ezt az információt. A támadónak tulajdonképpen semmilyen feladata nem volt a támadás kivitelezésében, minden automatizáltan történt. [12]

A Stacheldraht egy klasszikus dDOS eszköz, ami Linux és Solaris rendszerekre készült. Háromrétegű rendszer, melynek kliens rétegét használja a támadó arra, hogy irányítsa a kezelőket, melyek feltérképezik a fertőzött számítógépeket, és kiadják a megfelelő támadási utasításokat. Egy kezelő több ezer fertőzött számítógépet képes kezelni. [13] Ellentétben a MyDoom féreggel, ez a rendszer képes arra, hogy dinamikusan változtassa meg a célpontot és a támadás időpontját.

A túlterheléses támadás szinte minden esetben kártékony célú, ugyanakkor meglepő módon már többször is alkalmazták jó ügy érdekében is. Amikor olyan oldalakra bukkannak melyek a felhasználók adatait igyekeznek kicsikarni (un. spoofing oldalak), ellenük hatékonyan vethető be a túlterheléses támadás, megakadályozva így, hogy további kárt okozzanak. Erre példa az un. nigériai csalás felszámolásáért indított túlterheléses támadás. [11]

Az Internet elleni támadás hatásai

A 2007-es év második felében az online sajtó az észt-orosz kiber-konfliktusról szóló cikkel telt meg. A feltételezések szerint az észtországi internetes szervereket orosz hackerek támadták meg, elérhetetlenné téve azok szolgáltatásait. A több órás vagy napos szolgáltatás-kiesés megoldása végül az észt országon kívülről érkező internetes adatforgalom blokkolása lett. A napokig tartó támadás az egész világnak megmutatta, hogy milyen sebezhető az online világ, és mennyire tehetetlenek a szolgáltatók egy ilyen támadás kivédésében. Az ügy számos katonai vezető figyelmét is felkeltette és a NATO is magas szinten vizsgálta az ügyet,. [19] A vizsgálatok feltárták, hogy a világ különböző pontjain lévő botnetek végezték el a támadást az észt internetes infrastruktúra ellen.

Magyarország összehasonlítva az észt helyzettel messze nem rendelkezik olyan mértékű Internetes penetrációval, de a cél, hogy az állampolgárok az összes önkormányzati és egyéb hivatalos ügyet az Interneten keresztül végezhessék el a közeljövőben. A magyar bankok mindegyike rendelkezik internetes felülettel, számos önkormányzati ügy végezhető el a www.magyarorszag.hu portálon, és az állampolgárok rengeteg adathoz férhetnek hozzá, saját személyüket illetően, mint például a saját TB adataik. A vállalkozások adóügyeinek intézése ma már teljes mértékben elektronizált felületen történik. A tömegkommunikációs szolgáltatók a hírek nagy részét az Internet segítségével gyűjtik be. A telekommunikációs forgalom nagy százaléka internetes technológián alapul már a mai nap. Ezt figyelembe véve, ha hazánkat érné hasonló támadás, az számos kellemetlenséget okozna az állampolgároknak.

Egy esetleges támadás célpontjai ezek alapján az internetes szolgáltató cégek, az állami és a banki szektor szolgáltatásai. Sajnos Magyarország az elmúlt évben támadások célpontjaivá vált. Míg eleinte az adathalász oldalakat hirdető e-mailek, ha el is jutottak magyar felhasználókhoz, azok külföldi szolgáltatások ellen irányuló támadást rejtettek, nem létezett olyan verziójuk, ami magyar szolgáltatások támadását segítette elő; nemrégiben a magyar szolgáltatásokat támadó oldalak és az őket „reklámozó” e-mailek is megjelentek. A múlt

évben számos magyar bank, például a CIB, Raiffeisen, MKB, Budapest Bank és számos Takarékszövetkezet ügyfeleit környékezték meg a támadók és igyekeztek az internetes banki adataikat megszerezni. A magyar bankok nagyon gyorsan léptek, és a támadásokról és azok kivédéséről szóló figyelemfelkeltő cikkek számos magyar sajtótermékben láttak napvilágot, így a felhasználók nagyrészt időben tájékoztatva lettek. Néhány bank, hogy minimalizálja a támadásból keletkező károkat, internetes szolgáltatásait egy ideig felfüggesztette. Összességében elmondható, hogy a támadás maga nem volt elég sikeres ahhoz, hogy rendkívüli mértékű kárt okozzon. [21] [22]

Sajnos a magyar hálózaton online lévő számítógépek nagy arányban fertőzöttek kártékony kódokkal. [20] [23] Ez köszönhető annak, hogy a magyar internet-felhasználók nagy többsége nem rendelkezik elég széles körű és alapos tudással, hogy képes legyen saját számítógépe megfelelő védelméről gondoskodni. Ezt a környezetet rosszindulatú támadó csoportok kihasználhatják, és belföldről indíthatnak megfelelő erejű támadást.

A lehetséges célpontok közül a banki szolgáltatások lebénítását megvizsgálva egy hatékony támadás eredménye, amellett hogy jelentős anyagi kárt tud okozni a felhasználók adatainak ellopása révén, számos kényelmi szolgáltatást tehet elérhetetlenné. A bankok által nyújtott online szolgáltatás igen népszerű a lakosság és a vállalkozások körében. Összességében elmondható, hogy az online tranzakciók aránya meghaladja az 50%-ot Magyarországon. A banki online szolgáltatások kiesésével ez a gazdasági ágazat komoly károkat szenvedne.

Az online kormányzati szolgáltatások ismertek a lakosság körében. Egy 2006-os felmérés szerint a lakosság több mint fele tud róla, ügyeiket ugyanakkor mindössze 2-3% intézi online. Az elmúlt két évben ez a szám valószínűleg növekedett. [25] Azóta számos törekvés lépett életbe, ami a hagyományos papír alapú adminisztrációt igyekszik háttérbe szorítani, és az olcsóbb online ügyintézést előtérbe helyezni. Ennek eredményeképpen a vállalkozások adminisztrációját ma már szinte teljes körűen csak az Interneten lehet elvégezni. Az online kormányzati szolgáltatások blokkolása ezért igen érzékenyen érinti az adminisztrációt.

Az ország online szolgáltatásaira a legnagyobb csapást az mérheti, ha az internetes szolgáltatók rendszereit megbénító sikeres támadás történik. Ez esetben a felhasználók nem tudnának kapcsolódni szolgáltatójukhoz, és nem érnének el egyetlen online szolgáltatást sem. Ez alapvetően számos kényelmi szolgáltatástól vágná el az ország lakosságát. Az elmúlt években azt mutatták a trendek, hogy számos hagyományos szolgáltatás is az Internetre tevődött át. Ilyen szolgáltatási körök a telefon és kábeltévé. A magyarországi Internet-elérés megbénításával ezen szolgáltatások is veszélybe kerülnének, így a hagyományos tájékoztatás lehetősége sem lenne meg, egy sikeres támadás esetén. A vállalkozások és háztartások egyre nagyobb százalékban bonyolítják vezetékes telefonforgalmukat IP alapú rendszereken, mivel ezek havi- és percdíja sokkal kedvezőbb a hagyományos telefon árainál. Azok számára, akik rendszeresen telefonálnak külföldre, ez az alternatíva még kedvezőbb lehetőséget biztosít. Az IP alapú telefon forgalom alapvetően ugyanazon hálózaton forgalmaz, mint a magyarországi Internet többi szolgáltatása. Az internetes kábeltévé egyelőre nem elterjedt olyan arányban, hogy a szolgáltatás kiesése jelentős problémát okozna.

Alapvetően elmondható, hogy egy sikeres támadás életünket számos ponton nehezítené meg. A modern szolgáltatások nagy része az Internetet használja, melyekhez a felhasználók hozzászoktak, és hiányuk érzékenyen érintené őket, mivel egy körülbelül tíz évvel ezelőtti állapotra lennének kénytelenek újra átállni. A kényelmetlenségek nagy valószínűséggel elégedetlenséget váltanának ki a lakosságban, és a támadás sikerességének a ténye pedig sokkoló pszichikai hatást eredményezne. Az Internetet ugyanis nem csak szórakozásra és kapcsolattartásra használjuk manapság, hanem rajta bonyolódnak fontos üzleti folyamatok is, mint például a banki ügyek intézése.

Védekezés a támadások ellen

Az irányított zombi számítógépek elleni harc nagy jelentőségű. Az Internet forgalmának nagyobb százalékát teszi ki az általuk generált forgalom, mint a hasznos adatáramlás, így a rendszer hatékonysága messze nem kielégítő. Kártékony tevékenységük fontos szolgáltatásokat veszélyeztetnek, és pénzügyi vagy akár komolyabb károkat okoznak.

A védekezés a felhasználók oktatásával, az operációs rendszerek hibáinak javításával, a rendszerfrissítések letöltésének egyszerűsítésével és a kártékony kódokat detektáló biztonsági programokkal lehetséges. Mivel a felhasználók oktatása nehéz feladat, csupán rájuk támaszkodva a kártékony programok terjedése nem állítható meg, ezért pár éve paradigmaváltás figyelhető meg az operációs rendszerek gyártóinál illetve bizonyos szolgáltatóknál. Az operációs rendszerek frissítése egyre egyszerűbb feladat, hozzá nem értő felhasználók számára is könnyen véghezvihető illetve sok esetben automatizált. Alapértelmezett beállítás lett az operációs rendszerekben a frissítések megjelenésének rendszeres figyelése és azok automatikus telepítése.

A kártékony programok a legtöbb esetben e-mailben érkeznek. Mivel a felhasználói oldalon nem megfelelő a védekezés, számos szolgáltató (saját rendszereit is védve) az e-mailek szerver oldali ellenőrzését vezette be biztosítva ezzel, hogy a felhasználóhoz minimális mennyiségű kártékony kód juthasson csak el. A legtöbb ingyenes e-mailt adó szolgáltató szerverein, de az Internet előfizetésekhez tartozó e-mail szervereken is megjelentek a szerver oldali víruskereső programok, melyek nem engedik, hogy a fertőzött alkalmazás a végfelhasználókhoz kerüljön.

Az újabb kártékony programok egy része az azonnali üzenetküldő rendszereken terjed, mint például az IRC, Skype vagy MSN Messenger. Ezek a programok, hogyha küldött fájlt akarunk letölteni ma már minden esetben egy figyelmeztető üzenetet jelentetnek meg a felhasználó számára, amiben felhívják a figyelmet arra, hogy a letöltött fájl kártékony programot is tartalmazhat akár, és csak akkor töltse le, ha az megbízható forrásból származik. Ezen erőfeszítések nagyon hasznosak és nagymértékben növelik a védelem hatékonyságát, de közel sem jelentenek száz százalékos megoldást, mivel a felhasználók nagy része, az ilyen felbukkanó figyelmeztető ablakokat elolvasás nélkül bezárja.

A harcot a kártékony programok ellen nagyban hátráltatja, hogy a legtöbb védelmi megoldásért fizetni kell. Pár évvel ezelőtt nagyon nehéz volt találni ingyenes vírusírtó vagy tűzfal programot. Megfigyelhető hogy ezen a téren is alapvető változások mentek végbe, mivel szinte mindegyik gyártó megjelent rendkívül olcsó egy-kétezer forintos alapszolgáltatásokat nyújtó eszközzel, vagy sok esetben teljesen ingyenes megoldással. Ezen alapverziók megfelelő állandó védelmet nyújtanak, különbség a drágább, vagy pénzbe kerülő társaiktól bizonyos kényelmi szolgáltatások hiánya legtöbb esetben. A támadásoknak legjobban kitett Microsoft operációs rendszerek esetében maga a gyártó szolgáltat megoldást ezekre a kérdésekre, hiszen havonta frissülő kártékony kód eltávolító programot bocsát a felhasználók rendelkezésére, illetve a második javítócsomagban egy egyszerű tűzfal is szerepel, ami alapértelmezésben bekapcsolva települ, és alapfokú védelmet szolgáltat a felhasználó számítógépe számára.

Ezen változásokat összegezve leszögezhető, hogy azok a felhasználók, akik minimálisan is, de fontosnak tartják saját gépük védelmét megfelelő eszközöket kapnak ahhoz, hogy megállítsák a világméretű fertőzési hullámot. További előny, hogy a számítástechnikai oktatás Magyarországon ma már az általános iskolában megjelenik, így a jövő felhasználói időben kapnak információt arról, mire kell odafigyelniük, és miképpen védhetik meg saját számítógépeiket.

Összegzés

Maga az internetes infrastruktúra törékeny. Az újabb IP protokoll elterjedése számos alapvető biztonsági problémát megoldana, de a költségek gátat szabnak a gyors terjedésnek. A magyarországi felhasználók nagy többsége nincsen tisztában az alapvető biztonsági folyamatokkal, ismeretük hiányos. A számítógéppark nagy százaléka kártékony kóddal fertőzött, ezért egy belföldről indított támadás is sikeres lehet, ezáltal a támadó blokkolása (pl.: külföldi kérések letiltása) nem jelentene megoldást. Az internetes szolgáltatások ugyanakkor bár nem létfontosságú feladatokat látnak el még egyelőre, az élet számos terén megjelentek; hiányuk sokkoló lenne a lakosságra és az üzleti életre nézve.

Szerencsére Magyarország viszonylag kis piac, ezért egy átfogó támadás nem jelentene jelentős anyagi nyereséget a támadó számára. Magyarország nem képvisel szélsőséges álláspontot semmilyen külpolitikai ügyben, ezért a nagy terrorista szervezetek célpontjaként egyelőre még nem szerepel. Amennyiben az ország szomszédaival, a nagyhatalmakkal és az arab államokkal baráti viszonyt tart fent, elkerülhető, hogy internetes és egyéb támadások célpontjává váljon.

Felhasznált irodalom

[1] http://hu.wikipedia.org/wiki/Inform%C3%A1ci%C3%B3s_t%C3%A1rsadalom
[2] Előházi János: Internetbiztonság (Robothadviselés 5 konferencia kiadvány, 2006)
[3] http://www.symantec.com/security_response/writeup.jsp?docid=2004-050116-1831-99
[4] http://en.wikipedia.org/wiki/Zombie_computer
[5] http://en.wikipedia.org/wiki/Botnet
[6] http://ironport.com/company/ironport_pr_2006-06-28.html
[7] http://en.wikipedia.org/wiki/Computer_worm
[8] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
[9] http://en.wikipedia.org/wiki/Backdoor_%28computing%29
[10] http://www.virushirado.hu/hirek_tart.php?id=1234
[11] http://en.wikipedia.org/wiki/Ddos#Distributed_attack
[12] http://en.wikipedia.org/wiki/MyDoom
[13] http://en.wikipedia.org/wiki/Stacheldraht
[14] http://en.wikipedia.org/wiki/Image:Tcp_normal.png
[15] http://en.wikipedia.org/wiki/SYN_flood
[16] http://en.wikipedia.org/wiki/IP_spoofing
[17] http://en.wikipedia.org/wiki/Smurf_attack
[18] http://en.wikipedia.org/wiki/Fraggle_attack
[19] http://www.sg.hu/cikkek/53256/amerikai_eszt_egyuttmukodes_a_kibertamadasok_ellen
[20] http://www.stop.hu/articles/article.php?id=308696
[21] http://itcafe.hu/hir/ujabb_adathalasz-tamadas_magyar_bank_ellen.html
[22] http://www.itport.hu/hir/957
[23] http://spamblog.hu/2008/03/11/kemprogrammal-fertozott-szamitogepen-sokkal-nehezebb-dolgozni/
[24] http://index.hu/gazdasag/magyar/ntbnk070920/
[25] http://www.hwsw.hu/hirek/32046/elektronikus_kormanyzati_szolgaltatasok_ugyfelkapu_apeh.html