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

DDOS TÁMADÁSOK VESZÉLYEI ÉS AZ ELLENÜK VALÓ VÉDEKEZÉS

Absztrakt

Az információs technológiák térnyerése miatt a társadalom sokkal nagyobb mértékben támaszkodik az informatikai rendszerekre és az ezeket összekötő hálózatokra. Az informatikai világhálózat kialakulásával a számítógépes bűnözők és a terroristák is új fegyverhez jutottak, céljaik elérésére egyre gyakrabban használják is az Internetet. Emellett az országok is kiemelt figyelmet szentelnek a virtuális térben alkalmazható harc módszereinek. Érdekes módon a technológiai fejlettség nagyobb veszélyt jelent, mivel a fejlett – és így bonyolultabb – információs infrastruktúra több támadható pontot is jelent. Új támadási formák jöttek létre, amelyek ellen nehéz védekezni, a támadások bekövetkeztekor szinte lehetetlen az elkövetőket azonosítani. Cikkemben egy ilyen speciális támadási módszer, a szolgáltatás megtagadást okozó túlterheléses támadás fajtáit rendszereztem, igyekezve bemutatni a lehetséges védelmek módozatait is.

Owing to the advances of information technology our society gets to lean on the information systems and communication networks increasingly. By the development of global communication network the cyber criminals and terrorists have got a new weapon, and for their aims they get to use the Internet more and more. Besides, the countries are also paying attention to the methods of war aplicable in virtual space. Interestingly, the advanced technological state is fraught with more danger, as the advenced – and more complicated – information infrastructure is more vulnerable. There are new forms of attack has been created which are hard to defend against, and when these occure it is almost impossible to identify the perpetrators. In my article I have systematized the types of these special attacking methods which cause denial of service by overloading, and I have tried to perform the possible methods of defence.

Kulcsszavak: *információs terrorizmus, cyber támadások, túlterheléses támadások, Distributed Denial of Service*

Bevezetés

A számítógépes bűnözés gyakorlatilag egyidős a számítógépekkel, de az igazán nagy lökést a gépek kommunikációs hálózatba kötése jelentette. A globális hálózatok megjelenésével az informatikai rendszerek sebezhetősége is megnövekedett, immár egy ilyen rendszer megtámadásához nem szükséges a célpontot fizikailag is megközelíteni, elegendő biztonságos távolságból, a hálózat lehetőségeit kihasználva elindítani az akciót. Ráadásul az igénybe vehető szolgáltatások száma és komplexitása is egyre gyarapszik, ami a kiszolgálókon futó alkalmazásokban előforduló hibák számát növeli. Egy hibásan megírt alkalmazás potenciális veszélyforrás, a hiányosságokat kihasználva átvehető a kiszolgáló ellenőrzése vagy egyszerűen működésképtelenné tehető a teljes informatikai rendszer.

Az informatikai rendszerek feletti ellenőrzés átvétele nem egyszerű feladat, jelentős szakértelmet, előkészítést igényel, ráadásul a siker sem biztosított. Egy gondos rendszergazda számára rendelkezésre állnak biztonságtechnikai módszerek, amelyekkel kivédheti az ilyen típusú próbálkozásokat, az emberi hibák (a rendszert karbantartó személyek gondatlansága, elővigyázatlansága) kihasználásához pedig közvetlen kontaktus szükséges, ami veszélyekkel járhat. Egy számítógépes rendszert nem is mindig szükséges uralni ahhoz, hogy kárt okozzon a támadó, az esetek nagy részében elegendő, ha működésképtelenné teszi azt. A működésképtelenné tétel egy számítógépes hálózaton keresztül elérhető rendszer esetében már akkor is megvalósul, ha a rendszer nem képes a felhasználók számára a kívánt szolgáltatást nyújtani.

Lehetséges célpontok

A számítógépes bűnözők elsődleges célpontjai azok a rendszerek, amelyek megtámadásával anyagi hasznot remélhetnek. Ha a támadások célja nem a haszonszerzés, akkor a lehetséges célpontok száma megsokasodik. A vallási, politikai, ideológiai ok, mint motiváció megjelenésével veszélybe kerülhetnek az állami infrastruktúrák és a gazdaság szereplőinek informatikai rendszerei. Előbbiek az állam elnyomó szerepének, utóbbiak pedig a kizsákmányolás jelképeként kerülhetnek be a támadók célkeresztjébe. Különösen kényes célpontok a fegyveres erők, rend-, és katasztrófavédelmi szervezetek rendszerei, amelyek általában erősen védettek, így sikeres működésképtelenné tételük komoly eredménynek számít. A sikeres támadások sajtóvisszhangja jelentős, így az elkövetők kellő publicitást szerezhetnek céljaik ismertetéséhez, támogatók szerzéséhez.
Természetesen az informatikai infrastruktúrák jelenlegi szintje nem azonos a világ államaiban; paradox módon a fejlettebb társadalmak jóval sérülékenyebbek, mint a fejletlenebbek. A tehetősebb országokban nagyobb elterjedtségnek örvendenek a számítógépes rendszerek, a hétköznapi tevékenységek során nagyobb mértékben támaszkodnak rájuk. A fejletlenebb, szegényebb országokban nincs olyan infrastruktúra, amelyet ilyen módon támadni lehetne, viszont ezekből az államokból is lehetőség van támadásokat indítani.
Természetesen egy informatikai támadás veszélyessége jelenleg még nem mérhető össze egy hagyományos fegyverekkel végrehajtott támadás veszélyességével, azonban nem szabad lebecsülni a veszélyeket. Sok szakértő szerint túlmisztifikált a cyber támadások veszélyessége ("There are many ways terrorists can kill you--computers aren't one of them." [1]), azonban nem szabad elfeledkezni a gazdasági hatásokról sem. A gyorsan változó gazdasági környezetben a pénzintézetek néhány napos leállása is beláthatatlan következményekkel járhat, emberek milliói rohanhatják meg a bankfiókokat, a pénzüket féltve. Magyarországon is volt már példa a kialakult pánik miatt veszélybe került pénzintézetre: 1997 februárjában a Postabank ügyfelei között elterjedt, a bank csődjéről szóló hírek hatására néhány óra alatt mintegy 70 milliárd forintot, a pénzintézet forrásainak egyhatodát vették ki az ügyfelek. A fegyveres erők is egyre nagyobb mértékben támaszkodnak az információs hálózatokra, az ilyen hálózatok működésképtelenné tétele veszélyeztetheti a rendfenntartási feladatokat, amely egy más jellegű katasztrófahelyzettel kombinálva komoly veszteségeket, akár emberéletben mérhetőket is okozhat. A kritikus infrastruktúrák (energia, távközlés és kommunikációs technológiák, pénzügy, egészségügy, élelmiszer, víz, közlekedés, biztonság[4], kormányzás, illetve termelőipar [2]) is kiemelt célpontok lehetnek, egy ilyen rendszer erőszakos leállítása jelentős kockázatokat hordoz magában. A következő fejezetben olvasható néhány, erre a célra alkalmas támadási technika összefoglalója.

Szolgáltatás megtagadás

Az informatikai rendszerek kapacitása természetesen nem végtelen. Egy rendszer méretezése során figyelembe veszik a várható terhelést, így alakítják ki az eszközparkot, amely képes a csúcsidőszakban beérkező forgalmat kiszolgálni. Ha a rendszert ennél a tervezett maximális forgalomnál nagyobb terhelés éri, akkor a rendszer lelassul, szélsőséges esetben pedig akár működésképtelenné is válik. Felhasználói szemszögből működésképtelennek tekinthető egy rendszer, ha válaszideje meghaladja a felhasználó tűréshatárának maximumát, így nem is szükséges teljesen működésképtelenné tenni azt. A túlterhelést okozó támadási módszereket összefoglaló néven Denial of Service (DoS) néven emlegetik, amit magyarul szolgáltatás megtagadásra fordítanak. Az elnevezés arra utal, hogy a célpont a támadás következtében megtagadja a szolgáltatás nyújtását, azonban talán szerencsésebb a „túlterheléses támadás" kifejezés.
Egy ilyen támadás sikeres kivitelezéséhez a támadó:

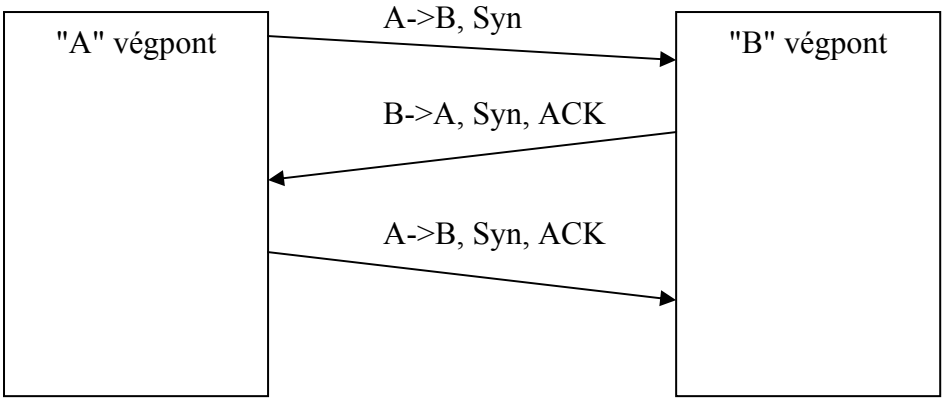
- a célpontnál nagyobb erőforrásokkal rendelkezik, vagy
- a célpont valamely hibáját használja ki.

A támadás irányulhat a célpont hálózati kapcsolatának, vagy pedig a célpont rendszerben működő valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére. Ennek megfelelően szokás a támadásokat hálózati vagy alkalmazási rétegben végrehajtott típusokra osztani, az OSI modell két rétegére utalva. A hagyományos DoS támadások során az elkövetők a célpontot egyetlen pontból támadják, általában egy „feltört", megfelelő adottságokkal rendelkező hálózati végpontot (hálózatra kötött számítógépet) használva fegyverül. A támadó célja a célpont erőforrásainak lefoglalása. A DoS támadásokról részletesen a CERT [1]weboldalán olvasható [3].

Hálózati rétegben végrehajtott DoS támadás: TCP SYN Attack

Az IP hálózatok – így az Internet is - legnépszerűbb szolgáltatásai (SMTP, HTTP, FTP) TCP (Transmission Control Protocol) kapcsolatot használnak. Az IP (Internet Protocol) egy összeköttetés-mentes, csomagkapcsolt hálózati protokoll, amely azt jelenti, hogy a két fél között az adatok kisebb, tipikusan néhány 100 byte méretű csomagokban közlekednek; minden csomag továbbítása a hálózatban működő útválasztók segítségével, a csomag fejlécében elhelyezett forrás- és célcímek alapján történik. Nincs átviteli csatorna lefoglalás, minden csomag továbbítása egyedileg történik, így a csatorna sávszélességén osztozik az összes áthaladó csomag. Két, egymást követő csomag továbbítása nem feltétlenül ugyanazon az útvonalon történik, a hálózatban el is tűnhetnek csomagok. Mindezek ellenére a TCP segítségével virtuális összeköttetés alakítható ki a két fél között, a TCP-t használó alkalmazások úgy képesek kommunikálni egymással, hogy nem kell foglalkozniuk a továbbítás során bekövetkező hibák kezelésével. Ezt a virtuális kapcsolatot egy úgynevezett „háromutas" kézfogás hozza létre, ami során a két fél megállapodik a kapcsolat paramétereitől. [4]
Normál esetben ez a következő módon történik:

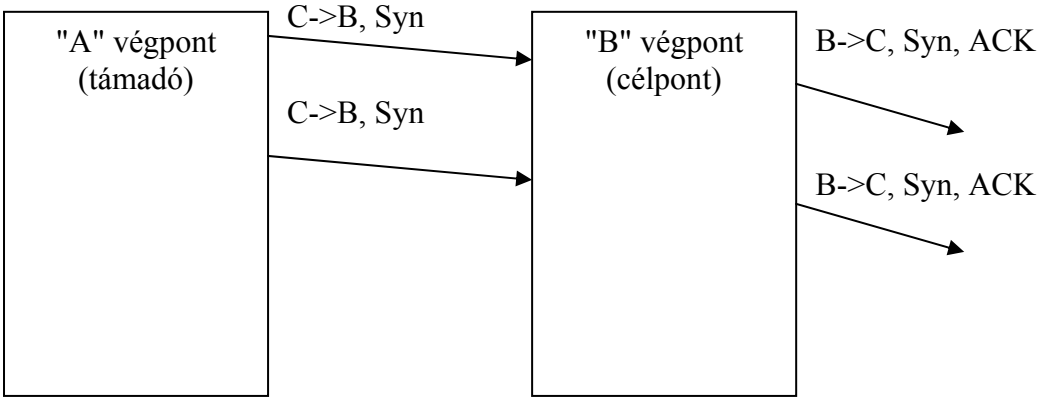
[1] CERT: Computer Emergency Response Team. Számítógépes biztonsági rések, hibák, veszélyek felderítésével, megfigyelésével foglalkozó szervezet. Székhelye az Egyesült Államok Carnegie Mellon Egyetemén található. A tudomásukra jutott veszélyeket publikálják, riasztásokat adnak ki.



1. ábra: TCP kapcsolat létrehozása

- A kliens Syn csomagot küld.
- A szerver Syn + ACK csomaggal nyugtáz.
- A kliens Syn + ACK csomaggal nyugtáz. A kapcsolat ettől a ponttól működőképes, a csatorna kiépült.

A támadás menete:



2. ábra: TCP Syn flood

A támadó a célpont számára egy hamisított forráscímmel Syn csomagot küld. A célpont ennek hatására előkészíti a létrehozandó kapcsolatot, meghatározza az általa használni kívánt kezdősorszámot, és tárolja a paramétereket. Ezután Syn + ACK nyugtázó csomagot küld a feladónak a hamisított forráscímre. A célpont erre az üzenetére természetesen nem kap választ, ezért néhányszor (általában még háromszor) újraküldi azt, minden alkalommal kivárva az előírás szerinti időt. Ha az utolsó próbálkozásra sem kap választ, akkor felszabadítja a kapcsolat tárolására szolgáló memóriát. [5]

A „félkész” kapcsolatok paramétereinek tárolására szolgáló memória mérete véges, ezért ha a támadó nagy mennyiségű Syn csomaggal árasztja el a célpontot, akkor hamarosan megtelik ez a tárterület, így nem lesz képes új TCP kapcsolatot létrehozni, ami a felhasználók szempontjából a szolgáltatás működésképtelenségét jelenti.

A védekezés módszerei már rendelkezésre állnak, a „félkész” kapcsolatok tárolására szolgáló memória megnövelése illetve a Syn Cookie nevű eljárás képében. A memóriaméret megnövelése természetesen csak növeli a védekezőképességet, igazi megoldást a Syn cookie

használata biztosít. Bár a támadási módszer és a védekezés is régóta ismert, a 2007 májusi észt DoS támadások során is sikerrel alkalmazták az elkövetők. [6]

Alkalmazási rétegben végrehajtott DoS támadás: email flooding.

A támadó a célpont SMTP[2] szerver számára nagy mennyiségű – esetleg speciálisan a célpont hiányosságaihoz méretezett - elektronikus levelet küld. Ha a célpont a beérkező elektronikus levelek számára kisméretű tárolókapacitással rendelkezik, akkor lehetséges a célpont háttértárának megtöltése, amely a további levelek fogadását, szélsőséges esetben akár a teljes operációs rendszer működését is lehetetlenné teszi. Mivel napjainkban egyre több kéretlen levél érkezik, ezért a levelezőszervereken gyakran működnek spam[3] illetve vírusszűrő alkalmazások. Egy ilyen szűrő is megtámadható, speciális levelekkel (igen nagyméretű tömörített állományok csatolása) a szerver erőforrásai lefoglalhatók.
A hatásos védekezés első lépése a támadás tényének felismerése, ezt követően a támadó végpontjának címe meghatározható, majd a hálózati rétegben kitiltható.

Alkalmazási rétegben végrehajtott DoS támadás: Webszerver támadása

Egy HTTP[4] kiszolgáló általában maximalizálja az egy időben működő példányainak (processz vagy szál) számát, pont a túlzott igénybevétel megakadályozására. Ha a támadó egyidejűleg sok ilyen példányt hozat létre a webszerverrel (egy időben sok letöltést indít el kis sebességű hálózaton), akkor igénybe veszi az összes rendelkezésre álló processzt, így a többi felhasználó nem képes a kiszolgálóhoz csatlakozni.
Egy ilyen támadást kivitelezni normál DoS (1 támadó végpont-1 célpont) módszerrel csak helytelenül konfigurált kiszolgáló ellen lehetséges.

Distributed Denial of Service: elosztott szolgáltatás megtagadásos támadási módszerek

A DoS támadási módszerek kiterjesztése, a támadó akcióját egy időben több végpontról indítja. Ehhez természetesen ellenőrzést kell szereznie a támadásra szolgáló számítógépek felett, amelyekre egy távvezérlést biztosító programot telepítenek számítógépes trójai programok vagy speciális weboldalak segítségével. Ezek a programok látszólag semmilyen aktivitást nem mutatnak, viszont a támadó bármikor képes őket aktivizálni. Az ilyen – zombinak nevezett – számítógépek hálózatba szervezhetők, amelyekkel veszélyes támadások indíthatók.
Ugyanúgy, mint a hagyományos DoS támadásokat, a DDoS akciókat is lehetséges a hálózati rétegben vagy az alkalmazási rétegben kivitelezni.

Hálózati rétegben kivitelezett ICMP flooding

Az ICMP (Internet Control Message Protocol) az IP fontos segédprotokollja. Segítségével tudatják az útválasztók egymással a csomagok továbbítása során bekövetkező hibákat, eseményeket, emellett diagnosztikai célokat is szolgál. Egy hálózati végpont a leggyorsabban úgy győződhet meg egy másik végpont működőképességéről (vagy az odáig vezető hálózati

---

[2] SMTP: Simple Mail Transfer Protocol. Az elektronikus levelet küldő kliens, és a levél célba juttatását végző szerver közti kommunikációt meghatározó eljárás. Leírása az RFC 821-ben található.
[3] Spam: a kéretlen – elsősorban reklám – levelekre alkalmazott kifejezés, eredetileg egy húskészítmény neve. Az elnevezést a Monty Python társulat egyik tévés jelenetére vezetik vissza, amelyben az eladó leginkább csak spam-et kívánt a vendégekre tukmálni. http://www.youtube.com/watch?v=BIWk5bGno58
[4] HTTP: Hypertext Transfer Protocol. A weboldalak lekérésére, a kliens és a szerver között használatos kommunikációt meghatározó protokoll.Az RFC 2616 írja le.

út működőképességéről), hogy küld számára egy „Echo Request” ICMP üzenetet. A másik végpont, ha megkapta a kérést, egy „Echo Reply” üzenettel válaszol. Ez az üzenetváltás játszódik le a legtöbb operációs rendszer alatt elérhető „ping” parancs hatására. Ezek a csomagok rövidek (tipikusan 74 byte méretűek), így normál alkalmazás mellett nem terhelik jelentősen sem a hálózatot, sem pedig a végpontok számítási kapacitását. Lehetséges azonban az „Echo Request” üzeneteket nagyobb méretben is küldeni, Windows XP használatakor a –l, Linux alatt pedig a –s kapcsolók használatával. A támadás kivitelezése során a támadó – esetleg ilyen módon megnövelt méretű - „Echo Request” csomagokat küld a célpont számára egyszerre nagyszámú végpontot használva. A támadó végpontok számától és a rendelkezésükre álló sávszélességtől függően a célpont sávszélessége túlterhelhető, így az álatala nyújtott szolgáltatások annyira lelassulnak, hogy a normál, üzemszerű működés lehetetlenné válik.
A védekezés nehéz, főként azért mert a támadó végpontok a hálózaton szétszórva találhatók. Csomagszűréssel a hálózati forgalomból kiszűrhetők az ICMP üzenetek, de ez sok kényelmetlenséggel is jár. Egyrészt a szűrés számítási teljesítményt vesz igénybe a hálózati eszközökben, másrészt az ICMP üzenetek eredeti funkciója – a hálózati problémák felderítése, a diagnosztika – nem lesz elérhető.

Alkalmazási rétegben kivitelezett HTTP támadás

A HTTP (Hypertext Transfer Protocol) a weboldalak eléréshez használt internetes protokoll, talán a legszélesebb körben használt internetes technológia. [7] A működése kliens-szerver modellt követ, tranzakció alapú. A kliens a lekérni kívánt weboldal – vagy egyéb elérhető objektum – azonosítóját (URL: Unified Resource Locator) elküldi a szervernek, a szerver pedig a válaszüzenetében továbbítja a kért objektumot. A kérés általában sokkal rövidebb, mint a válasz, vagyis a legtöbb webes szolgáltatás aszimmetrikus működésű. Manapság egyre több webes szolgáltatás dinamikusan, a kérés kiszolgálása során valamilyen adatbázist felhasználva állítja elő a kért oldalt, ezáltal extra szolgáltatásokat biztosítva a felhasználók számára. Ilyen extra szolgáltatás lehet a tartalomban végzett szabadszöveges keresés, amelynek kiszolgálása során sok, nehezen optimalizálható lekérdezést kell végrehajtani az adatbázisban tárolt adatokon. Ha a támadó képes ilyen, sok erőforrást igénylő kérést előállítani és azt nagyszámú végpontról egy időben elküldeni a kiszolgáló számára, akkor jelentős terhelést okoz a kiszolgáló adatbázis kezelőjének. Szélsőséges esetben ez akár a kiszolgáló leállásához is vezethet. A helyzetet súlyosbítja, hogy egy HTTP kérés mérete néhány 100 byte, így nagyon rövid idő alatt sok is elküldhető belőle, míg a válasz összeállítása nagy teljesítményű számítógépek használata mellett is több időt vesz igénybe.
A szolgáltatások általában aszimmetrikus működésűek (a kérést elküldeni egyszerűbb, mint a választ előállítani), így könnyű lefoglalni az erőforrásokat (hálózati sávszélesség, számítási kapacitás).
A támadás akár egy egyszerű HTML oldal betöltésével is kezdeményezhető, amelyet egy időben nagyszámú végponton elindítva komoly terhelést lehet okozni. Ilyen támadásra alkalmas lehet az alábbi kód:

```
<html>
<head>
<title>DOS</title>
<script type="text/javascript">
function Tolt()
{
      sSearch = "";
      for (i=0; i<7; i++)
            sSearch+=String.fromCharCode(65+Math.floor(Math.random()*27));
      sSearch="http://www.aldozat.valahol/kereso?keresd="+sSearch;
```

```
      document.getElementById("dframe").src=sSearch;
      var tt = setTimeout("Tolt()",1000);
}
</script>
</head>
<body onload="Tolt()">
<iframe id="dframe" src="about:blank" width="600" height="600"></iframe>
</body>
```

Egy ehhez hasonló (természetesen jóval kifinomultabb módszert használó) támadás ellen csaknem lehetetlen védekezni, roppant nehéz a rosszindulatú forgalmat megkülönböztetni a normál, üzemszerű forgalomtól. Ha sikerült a támadás módszerét azonosítani, az adott támadás ellen már lehetséges egyedileg védekezni. Drága megoldást jelent az elosztott architektúra (cache szerverek, fürtözés), az ilyenek használatával a hálózatban elosztott támadó végpontok nem képesek egy célpontra összpontosítani a támadást.

Reflektív DDoS támadások

A DDoS támadási módszerek továbbfejlesztését jelentik az ilyen támadások, amelyeknek során más, „ártatlan” végpontokat használnak fel támadóként (vagy inkább fegyverként). Ezeket a végpontokat nem szükséges uralni, elegendő az Internet sajátosságait megfelelő módon kihasználni. A reflektív támadás során a támadó gondosan megválasztott adatforgalom segítségével készteti a támadásban részt vevő ártatlan végpontokat, hogy a célpont számára kárt okozó adatforgalmat generáljanak, ezért a tényleges támadó kiszűrése szinte lehetetlen.
A DDoS támadásokhoz hasonlóan, a hálózati és az alkalmazási rétegben egyaránt kivitelezhető.

Hálózati rétegben kivitelezett reflektív DDoS támadás: TCP Syn+ACK Attack.

A támadás nagyon hasonló a TCP Syn Flood támadáshoz, azonban ebben az esetben nem a célpont számára küldik a kapcsolat felvételi kérést, hanem egy ártatlan cégpontnak. Természetesen a csomag forrás IP címe hamisított, és a célpont IP címét tartalmazza. A Syn csomagra válaszul keletkezik egy Syn+ACK csomag, amelyet a célpont kap meg. A módszernek két nagy előnye van:

- a célpont számára érkező csomag egy semleges helyről érkezik, így a csomagszűrők nagy valószínűséggel átengedik;
- az ártatlan végpont nem csak egy Syn+ACK csomagot küld. Mivel a célponttól nem érkezik meg a háromutas kézfogás utolsó csomagja, így még legalább háromszor újraküldi azt, tehát a támadó egyetlen csomagjának hatására a célpont négy csomagot kap. [5]

Hatásosan védekezni ilyen támadások ellen csak az internet-szolgáltatók bevonásával lehet, mivel a káros csomagokat még a célpont hálózatának határain kívül kell elfogni. A legtöbb hálózati rétegben végrehajtott DoS támadás alkalmazza a forrás IP címek hamisítását, ezért az internet-szolgáltatók feladata a saját hálózatuk határain működő útválasztók helyes konfigurálása, amely meggátolja a saját hálózatukból más hálózatok felé tartó olyan csomagok szűrése, amelyek forrás IP címe nem a saját hálózati címtartományába tartozik. Ezt

[5] Egy valós, ilyen módszert használó támadás leírása a következő címen olvasható: http://www.grc.com/dos/drdos.htm

az RFC 2827[6] részletezi. [8] Ez a módszer azonban sajnos nem véd a szabálynak megfelelő, de mégis hamisított forráscímű csomagok ellen.

Hálózati rétegben kivitelezett reflektív DDoS támadás: „Smurf" attack

Minden IP hálózatnak létezik egy broadcast (szórási) címe, amelyre üzenetet küldve a hálózat összes végpontja megszólítható. Ha a hálózat rendszergazdája az útválasztót úgy állítja be, hogy ez a cím külső hálózatok irányából is elérhető, akkor egy kívülről érkező, a hálózat broadcast címére szóló csomagra a hálózat minden tagja válaszol. A „Smurf attack" során a támadó keres ilyen hibásan konfigurált, nagy sávszélességű, sok végpontot tartalmazó hálózatokat.
A célpont címét hamisítva feladóként, a hálózat broadcast címére elkezd Echo request üzeneteket küldeni, amire a hálózat összes végpontja válaszol, Echo reply üzeneteket küldve a célpont címére. A támadási módszerről a CERT weboldalán olvasható részletes leírás. [9]
A támadási módszernek ma már inkább történelmi jelentősége van, az újonnan forgalomba kerülő hálózati útválasztók már gyárilag úgy konfiguráltak, hogy ne tegyék lehetővé az ilyen jellegű módszereket.

Alkalmazás rétegben kivitelezett reflektív email támadás

Az elektronikus leveleket továbbító SMTP (Simple Mail Transfer Protocol) egy egyszerű, párbeszédes módszert alkalmaz a levelek kézbesítésére, melyet az alábbi üzenetváltás mutat be:

```
HELO tamado
250 Hello 3e44bd93.adsl.enternet.hu [62.68.189.147], pleased to meet you
MAIL FROM: bill.gates@microsoft.com
250 2.1.0 bill.gates@microsoft.com... Sender ok
RCPT TO: george.w.bush@whitehouse.gov
550 5.7.1 george.w.bush@whitehouse.gov... Relaying denied
RCPT TO: bill.clinton@kewl.hu
550 5.1.1 bill.clinton@kewl.hu... User unknown
```

A vastagított sorokban olvasható üzeneteket a kliens küldi, a levél címzettjét az „RCPT TO:" után adja meg a küldő. A címzett megadása után a szerver döntési helyzetbe kerül:

- azonnal ellenőrizze, hogy a címzett létezik-e vagy
- átvegye a levelet, elhelyezze egy feldolgozási sorba, majd később ellenőrizze, hogy a levél kézbesíthető-e.

Az első lehetőség meglehetősen erőforrás igényes, hiszen a beérkező levél esetén, a szerver aktuális terheltségétől függetlenül azonnal el kell végezni az ellenőrzést. A második lehetőség a levél beérkezésekor kevesebb erőforrást igényel, viszont később, a várakozó sor feldolgozásakor a szabványnak megfelelően értesíteni kell a feladót arról, hogy levele kézbesíthetetlen.
A hagyományos email DDoS támadások ellen már léteznek hatásos technikák (Reverse DNS figyelés, feketelisták), azonban a reflexió elvét kihasználva megtámadható egy jól védett szerver is. Az ilyen támadás a második módon beállított levelezőszervereket használja a célpont megtámadására, hamisított feladói email címmel küld leveleket (ezt a „MAIL

[6] Az IP cím két részből tevődik össze: a hálózat azonosítójából és a hálózaton belül kiosztott végpont címből. Az IP címek hamisításakor a feladó saját azonosítója helyett egy tetszőlegesen választott másik címet illeszt a csomagba, így a későbbiekben nemhogy a feladó, de még a feladó hálózata sem azonosítható. Mivel a feladó mindenképpen a saját hálózatából küldi a hamis csomagokat, a hálózat útválasztóján (routeren) keresztülhalad. Az RFC 2827 előírja, hogy az ilyen útválasztók külső hálózatba csak a saját hálózatuk címtartományába tartozó feladójú csomagokat továbbíthatják. Ezáltal a támadó csak saját hálózatán belüli végpontcímet képes hamisítani.

FROM:” után kell megadni) a szervernek, a szerveren nem létező email címre. A szerver ezeket átveszi, majd az értesítést a célpont számára küldi el, jelentős terhelést okozva. [10]
Ha egy ilyen támadásra botneteket és nagyszámú reflexiós szervert használnak, a védekezés meglehetősen nehézzé válik. A levelező szerverek helyes és gondos konfigurálása mindenképpen csökkenti az ilyen akciók bekövetkezésének esélyeit. Az elektronikus levelezés gyengeségeit jól mutatja a rengeteg kéretlen levél is, amivel mindenki naponta szembesül.

Nagyobb nyilvánosságot kapott DDoS támadások

Elosztott támadások egyre gyakrabban következnek be, ami az informatikai infrastruktúra fejlődése mellett az új típusú fenyegetések megjelenésének köszönhető. Napjaink egyik legnagyobb problémáját a félelmetes ütemben növekvő botnetek jelentik, amelyekre már egész iparág épül. A botnetekben működő, távolról irányítható számítógépek képesek akár kéretlen reklámlevelek küldésére (ami jelenleg a számítógépes bűnözők számára a fő bevételi forrás), akár pedig bármi más feladat végrehajtására, amire megrendelés érkezik. A számítógépes világnak szembe kell néznie a több millió végpontból álló, egyszerre cselekedni képes hálózatok problémájával. Bár ezeket jelenleg inkább a kereskedelmi megrendelések mozgatják, azonban csak idő kérdése, mikor vetik be őket terroristák, céljaik elérése érdekében. A kereskedelmi célpontok támadása mellett előfordultak már politikai indíttatású cyber támadások is, amelyek a DDoS technikát alkalmazták.

DNS infrastruktúra elleni támadások

A DNS (Domain Name System) egyike az Internet egyik alapvető szolgáltatásának, ezek a szerverek fordítják le az emberi felhasználók által jobban kezelhető domain neveket a számítógépes hálózatokban használt IP címekre. A DNS infrastruktúra leállása néhány órán (tipikusan legfeljebb 24 órán) belül gyakorlatilag működésképtelenné tenné az Internetet. Ennek megfelelően a rendszer kellően hibatűrő, 13 fizikailag is elosztott végpontot (root szerverek) tartalmaz, amelyek közül 7 egyenként is elosztott rendszer. A DNS teljes leállításához egy időben kellene az összes root szervert leállítani, ami nem egyszerű feladat, ezért az informatikai támadásokra specializálódott szakértők számára komoly kihívást jelent. Ennek ellenére napjainkig összesen két jelentősebb támadást regisztráltak már, amelyek képesek voltak kisebb fennakadásokat okozni. Az első ilyen támadás 2002. október 22-én történt, és egy óra lefolyású volt. A 13 root szerver közül 9 leállt, ám a maradék 4 képes volt átvenni a kiesőktől a feladatokat, így komoly fennakadást nem okozott. A második támadás 2007. február 6-án történt, és hosszabb ideig, mintegy öt óra hosszat tartott. A hosszabb támadási időtartam ellenére egyetlen root szerver sem állt le, viszont kettő közülük nagyon komoly terhelést kapott. A támadást egy botnet hajtotta végre, amely IP címtartománya az ázsiai régiókhoz kapcsolható. Feltételezések szerint a támadást egy dél-koreai csapat hajtotta végre.

Dán weboldalak elleni DoS támadások

2006-ban néhány dán újságban az iszlám prófétáját, Mohamedet gúnyoló karikatúrák jelentek meg. A Dániában tevékenykedő iszlám vallási vezetők hathatós segítségével az eset nagy nyilvánosságot kapott a muzulmán vallású országokban. Mivel az iszlám tiltja a próféta bármilyen képi ábrázolását, a tiszteletlen karikatúrákat hatalmas felzúdulás fogadta. A helyzetet súlyosbította a dán politikusok és a dán közvélemény jelentős részének álláspontja, akik a sajtó- és véleménynyilvánítás szabadságának korlátozásának tekintették volna a képek betiltását. Az így kialakult helyzetnek köszönhetően aztán elkezdődtek a dán weboldalak elleni támadások, amelyek egy része az oldalak feltörésére, elcsúfítására – deface – irányult,

más részük pedig túlterheléses támadás volt. A feltört oldalakon iszlám csoportok helyeztek el üzeneteket, amelyekben szent háborút hirdettek a vallásgyalázók ellen.

Orosz-észt konfliktus

2007. április 27-én a helyi orosz kisebbség tiltakozása ellenére a tallini szovjet második világháborús emlékművet lebontották és áthelyezték. Hamarosan utcai zavargások törtek ki, Oroszország tiltakozott az eset miatt. Az emlékmű áthelyezését követően hamarosan megindultak a DDoS támadások. Az észt szakértők szerint sok ezek közül közvetlenül visszavezethető volt orosz kormányzati számítógépekre. A megtámadott célpontok közül néhány:

www.pol.ee
www.fin.ee
www.riigikogu.ee
www.riik.ee
www.peaminister.ee
www.valitsus.ee
www.envir.ee
www.sm.ee
www.agri.ee [6].

A támadások közel két hétig tartottak, váltakozó intenzitással.
A konfliktus felvet jó néhány jogi problémát is:

- Ha egy szuverén állam informatikai infrastruktúráját egy másik állam megtámadja, a megtámadott milyen lépéseket tehet?
- Mekkora károkozás bekövetkeztekor élhet a megtámadott ország a katonai válaszcsapás lehetőségével?
- Mi a támadás megítélése, és mik az ellenlépések egy olyan esetben, amikor a támadó egy harmadik – semleges – ország infrastruktúráját használja a támadás végrehajtásához?
- Mi történik, ha a megtámadott rosszul méri fel a helyzetet, és nem a tényleges támadó ellen teszi meg az általa szükségesnek vélt ellenlépéseket?

Összegzés

A közeljövőben elkövetett DDoS támadások száma valószínűleg csak növekedni fog. Egyre több ember használja az Internetet, így a potenciális áldozatok száma is növekszik. A számítógépes bűnözés mellett egyéb csoportok is felfigyeltek az ilyen támadások után megnövekvő médiafigyelemre, és igyekeznek saját céljaikra kihasználni ezeket. Új tényezőként megjelentek a támadások kivitelezéséhez infrastruktúrát (botneteket) biztosító "vállalkozók" is, akik bérbe adják az általuk uralt számítógépeket kéretlen levelek küldésére vagy DoS támadások végrehajtására. A kéretlen levelek küldésében részt vevő botnetek mérete döbbenetes mértékben megnőtt, az ilyen hálózatok bármikor felhasználhatók a világ bármely informatikai infrastruktúrája elleni támadásokra. Az informatikai hálózatok ellen elkövetett támadásokra gyorsan kell reagálni, azonban a lehetséges ellentevékenységek köre meglehetősen szűk, ráadásul állami, katonai szereplők esetén rengeteg konfliktuslehetőséget hordoz. A támadások visszaszorítása érdekében megfontolandó a megelőző tevékenység erősítése, amelynek ki kell terjednie a felhasználók oktatására, illetve a kialakult botnetek felderítésére és hatástalanítására is.

Irodalomjegyzék

[1] Joshua Green: The Myth of Cyberterrorism
http://www.washingtonmonthly.com/features/2001/0211.green.html

[2] Précsényi Zoltán - Solymosi József: ÚTON AZ EURÓPAI KRITIKUS INFRASTRUKTÚRÁK AZONOSÍTÁSA ÉS HATÉKONY VÉDELME FELÉ
http://www.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html

[3] CERT® Coordination Center: Denial of Service Attacks
http://www.cert.org/tech_tips/denial_of_service.html

[4] RFC793: Transmission Control Protocol
http://tools.ietf.org/html/rfc793

[5] Tom Thomas: Hálózati biztonság. Panem Könyvkiadó, 2005.

[6] Jose Nazario: Estonian DDoS Attacks - A summary to date
http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

[7] RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
http://www.ietf.org/rfc/rfc2616.txt

[8] RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Spoofing
http://www.ietf.org/rfc/rfc2827.txt

[9] Smurf IP Denial-of-Service Attacks
http://www.cert.org/advisories/CA-1998-01.html

[10] Will Knight: Email attack could kill servers
http://www.newscientist.com/article.ns?id=dn4858

Az internetes források 2007. december 17-én elérhetők voltak.