Bevezetés a botnetek világába

SZENTGYÖRGYI ATTILA, SZABÓ GÉZA
Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék
{szgyi, szabog}@tmit.bme.hu
BENCSÁTH BOLDIZSÁR
Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék
boldi@crysys.hit.bme.hu

Kulcsszavak: robothálózat, botnet, detektálás, darknet, honeypot

A botnet (robot network) nem más, mint számítógépek támadó által vezérelt serege. A gépek nem a támadó tulajdonát képezik, hanem többnyire rosszindulatú kóddal fertőzött otthoni számítógépek. A botnetek napjaink egyik legelterjedtebb és legveszélyesebb károkozói. Sok évvel megjelenésük után is az átlagfelhasználó keveset tud róluk, a működésükről és a védekezési módszereikről, pedig pont az ő gépeiket használja fel leggyakrabban a támadó a saját céljaira. Cikkünk célja, hogy közelebb hozzuk az olvasót ehhez a technikához: összefoglaljuk a botnetek működési elvét, kommunikációjuk és működésük lehetséges módozatait.

1. Bevezetés

Az utóbbi időkben az egyik legismertebb hálózati alkalmazásként emlegetik a robotok hálózatait, a botneteket. Sajnos ez a népszerűség nem a nagyszámú boldog felhasználó visszajelzésének köszönhető, hanem a botnetek által okozott károknak. Egyre-másra jelennek meg híradások arról, hogy egy-egy botnet-támadás milyen károkat okozott különböző szolgáltatóknak és cégeknek.

Az ilyen támadó hálózatok nemcsak a cégeket, megtámadott rendszereket, hanem az átlagembereket is megkárosítják, hiszen számítógépeik erőforrásait károkozására használják fel, miközben akár megszerezhetik a megtámadott gép gazdájának személyes adatait is, vagy akár kéretlen reklámleveleket is küldhetnek nekik. Mint látható, sok egymással összefüggő internetes támadást lehet kapcsolatba hozni a botnetek létezésével. A cikk célja, hogy összefoglalja a botnetekkel kapcsolatos információkat, hogy hatékonyan lehessen fellépni a károkozók ellen.

2. Mi a botnet?

A botnet szó a „roBOT NETwork" angol kifejezésből származik. Az első robotnak nevezett programok az Internet úgynevezett IRC (Internet Relay Chat), internetes beszélgetési szolgáltatásához kapcsolódóan jöttek létre, és olyan feladatokat láttak el, mint üzenetek átadása, üdvözlés, bizonyos jogosultságok biztosítása stb. Ezeket a távirányítható, illetve programozott robotokat kezdték el röviden „bot" néven említeni. Később jelentek meg a rosszindulatú céllal létrehozott „botok", sokszor továbbra is az IRC hálózaton át koordinált szoftverek, amelyek összehangolt támadásokat tudtak indítani.

A „botok" előre programozott feladatot hajtanak végre, például kéretlen reklámleveleket (spam) generálnak és továbbítanak, vírusokat terjesztenek vagy DoS (Denial-of-Service – szolgáltatásmegtagadásos) támadásokat visznek véghez [8]. A botnet kifejezésben a „network" fogalom azért jelent meg, mert ezek a robotok hálózatba vannak szervezve: az egyes robotok vagy egymással, vagy kevés számú (tipikusan 1-2) vezérlővel (controller) állnak kapcsolatban. Magukat az értelem nélküli robotokat zombiknak, a hálózatot pedig zombi hadseregnek is hívják. A botnetek fontosságát számos kutató felismerte már, és több publikáció is született már a tárgykörben, így hasznos lehet a további irodalmak áttanulmányozása is [2,3,6,7].

3. Botnetek keletkezése

A botnetek az életük során hasonló funkcionális lépéseken mennek keresztül, ezeket életciklusoknak nevezhetjük. Ha értjük a botnetek életciklusát, akkor nagyobb eséllyel vesszük azokat észre, és jobban lehet reagálni a veszélyre.

Egy botnet létrejöttéhez szükség van olyan számítógépekre (áldozatokra), amelyek az adott robot kódját futtatják, ez az első lépés a botnet létrehozásában. A támadók általában úgy jutnak ilyen gépekhez, hogy valamilyen módszert kihasználva terjeszteni próbálják a zombi kódját, hasonlóan más rosszindulatú kódokhoz. Amint megfelelő mennyiségű számítógépen fut a rosszindulatú kód, a támadó elkezdheti az így kialakult hálózat koordinációját, vezérlését.

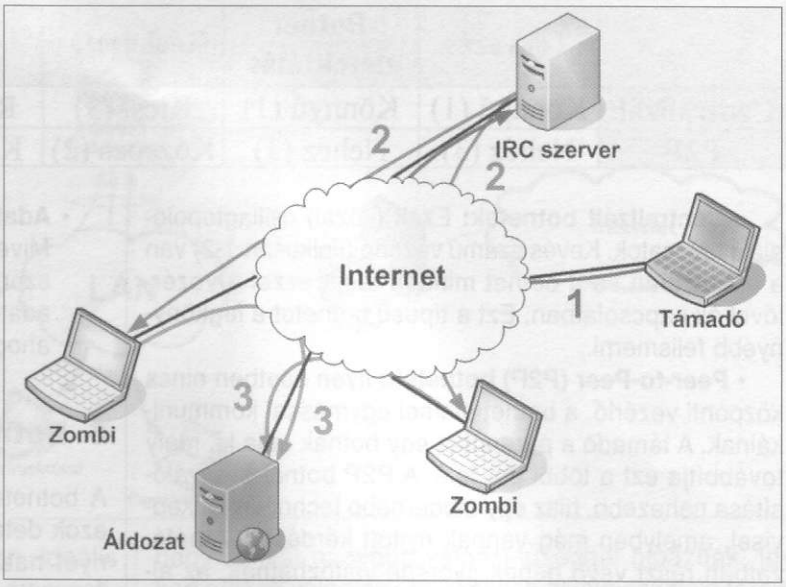
A vezérléshez speciális módszereket használhatnak fel, hogy a vezérlő kiléte titokban maradhasson, ám a botnet mégis koordinált módon működjön, megfelelően végezze a támadásokat. A botgazda parancsára a hálózat támadni kezd, hasonló módon a támadás – legyen az spam küldése vagy egy DoS támadás – rövid időn belül le is állítható.

A működő botnet egy dinamikus közeg: egyes elemeit, a felhasználók gépeit „megjavítják", így letörlésre kerül a rosszindulatú kód és a botnetből ezek a gépek

kiesnek. Új gépek is beléphetnek ugyanakkor a hálózatba. A hálózat, annak mérete és elemei így folyamatos változásban vannak.

A botnetek megszűnésére kevés példát láttunk, kevés tény ismert. Gyakori, hogy a botnet gazdája mégis lelepleződik, jogi eljárás indul ellene, ilyenkor a botnet elérkezhet megszűnéséhez. Több dolog is történhet egy botnet megszűnése közelében. A tulajdonos átadhatja vezérlését egy másik gazdának, aki sajátjaként kezelheti a hálózatot, vagy akár beolvaszthatja saját hálózatába. Az is elképzelhető azonban, hogy a botnet gazdátlanná válik, senki sem irányítja és gondozza, így egy ideig működik, majd a vezérlési rendszer szétesik. Kevés tapasztalat van azonban ezekről a folyamatokról.

A botnethez szükséges rosszindulatú kód terjesztésére az egyik leggyakoribb módszer az e-maileken keresztül terjedés. A közismert „vírusos e-mail" jellegű terjedés mellett azonban néhány egzotikusabb módszert is felhasználnak a botnetek létrehozására, mint például a gépeken más rosszindulatú kód által hagyott kiskapuk megkeresését, vagy a nyers erő támadást jelszavak kitalálására.



1. ábra
Egy zombihálózat felépítése és a támadás folyamata

3.1. A trójaiak által hagyott kiskapuk

A botnetek egy része még speciálisabb módszert is felhasznál: más kártékony kódok után hagyott kiskapukat keres az Interneten. A botnet kliensek maguk is ebbe a kategóriába sorolhatók, hisz lehetővé teszik a távoli gép vezérlését, azonban ezen túlmenően is számos ilyen kártékony kód létezik, és egy részüknél a távvezérlés könnyen átvehető, mert az adott rosszindulatú kód például nem tartalmaz hitelesítést, bárki vezérelheti a kódot és így átveheti a gép irányítását.

3.2. Jelszó kitalálása és „nyers erő"-támadások

A botnet létrehozásához olyan egyszerű támadásokat is fel lehet használni, mint a jelszavak kitalálása, próbálgatása.

Példaként az RBot (és más bot-családok is) a jelszótalálgatás több fajtáját is használják. Az RBot terjedését manuálisan indították távirányítással. Az RBot a 139-es és 445-ös portokra próbál csatlakozni véletlenül kiválasztott célpontokról, egy kiválasztott név és jelszó segítségével. Ezeket a portokat a Windows rendszer használja a fájlmegosztás és más hálózati szolgáltatások során. Ha sikerül a csatlakozás, akkor megpróbálja kitalálni a megfelelő felhasználói nevet és jelszót. Ha sikertelen a csatlakozási kísérlet, vagy semelyik tesztelendő név és jelszó párosra nem reagál a célgép, akkor a bot feladja a célgép támadását és másik potenciális áldozatot keres. A botnak egy beépített listája van a tipikus felhasználói nevekről, amelyekkel csatlakozni próbál.

Több behatolás detektáló rendszer is képes a nagyszámú bejelentkezési kísérlet alapján a fertőzött gépeket azonosítani és kiszűrni. A belépési kísérleteket a megtámadott gép eseménynaplója is tartalmazhatja.

3.3. Botnet-kliensek gyülekezése

Gyülekezéskor a botnet-kliens a botnetet irányító központtal veszi fel valamilyen módon a kapcsolatot.

A legegyszerűbb botnetek az Internet egy speciális szolgáltatását, a szöveges beszélgetést biztosító IRC rendszert használják. Amikor egy újabb botnet-elem, zombi csatlakozik a rendszerhez, az hozzákapcsolódik az előre beprogramozott IRC szerverek egyikére, és ott fellép a megadott csatornára. Ez a csatorna egy elszigetelt beszélgetési terület, amely kiválóan alkalmas arra, hogy elszigetelt módon, a botokat vezérlő személy parancsokat küldjön mindazon botoknak, amelyek csatlakoztak a rendszerhez. A támadó ezt követően az IRC csatornán kiadott parancsokkal tudja utasítani a zombi hadseregét. Ez a folyamat látható az *1. ábrán.*

Először a támadó csatlakozik az IRC szerverhez és kiadja a támadás parancsot (1). A parancs így eljut az IRC szerveren levő parancsokat figyelő zombi gépekhez (2). A parancsot értelmezve a zombik koordináltan támadást indítanak (3).

A botnetek belső rendszere kifinomult biztonsági elemeket is tartalmazhat: az irányításhoz jelszó alapú azonosítást és rejtjelezett kommunikációt is használhatnak. Az új botnet-kliens frissítéseket is letölthet. Ezek a frissítések sebezhetőségi információkat, új irányítóközpont címeket, vagy akár újabb funkciókat is tartalmazhatnak.

A botnetkliens-program, illetve a támadó azt is figyelemmel kísérheti, hogy esetleg a fertőzött gépen más támadó is elhelyezett-e rosszindulatú kódot. Amennyiben igen, úgy speciális eljárásokkal eltávolíthatja, vagy deaktiválhatja mások programjait. Hasonlóan járhat el az antivírus-programok és más védelmi szoftverek esetében.

4. Botnet-típusok

A botneteket hálózati technikájuk szerint két fő csoportra oszthatjuk:

	Tervezés	Botnet detektálás	Késleltetés	Túlélés	Vezérlő detektálás
Centralizált	Könnyű (1)	Könnyű (1)	Kicsi (3)	Rossz (1)	Könnyű (1)
P2P	Nehéz (3)	Nehéz (3)	Közepes (2)	Kiváló (3)	Nehéz (3)

1. táblázat Botnet-típusok tulajdonságai

• **Centralizált botnetek:** Ezek (közel) csillagtopológiájú hálózatok. Kevés számú vezérlő (tipikusan 1-2) van a hálózatban és a botnet minden tagja ezzel a vezérlővel áll kapcsolatban. Ezt a típusú botnetet a legkönnyebb felismerni.

• **Peer-to-Peer (P2P) botnetek:** Ilyen esetben nincs központi vezérlő, a botnet elemei egymással kommunikálnak. A támadó a parancsot egy botnak adja ki, mely továbbítja ezt a többi bot felé. A P2P botnet megvalósítása nehezebb, hisz egy modernebb technológiát képvisel, amelyben még vannak nyitott kérdések. A hálózatban részt vevő gépek gyorsan változhatnak, az alkalmazott P2P eljárásnak tehát igen hatékonynak kell lennie. A másik oldalról nézve, ilyen esetben a támadás koordináló vezérlő azonosítása nehezebb, így a támadó védettebb helyzetben lehet.

Az *1. táblázat* foglalja össze, hogy az egyes botnetek milyen tulajdonságokkal rendelkeznek.

Számos különböző botnet-kliens és így számos különböző botnet létezik. Tevékenységükben és felépítésükben vannak különbségek, de ezek jelenleg tartalmi lényegükben csak kisebb mértékben térnek el. Az egyes botnetekről, kliensekről internetes adatbázisokból, levelezési listákból és speciális publikációkból lehet több információt szerezni (lásd pl. [7])

5. A botnetek tevékenysége

A botnetek számos különböző tevékenységet látnak és láthatnak el, ezek közül a főbb tevékenységek a következők:

• **Új botok beszervezése.**
A botnet méretének növelése érdekében újabb célpontokat szervezhet be a hálózatba.

• **Szolgáltatás-megtagadásos támadás.**
Hatalmas erőforrásait felhasználva felemésztheti a célpontok erőforrásait, megbénítva azokat.

• **Levélszemét terjesztése.**
Gépek tízezrei segítségével kéretlen reklámlevelek millióinak, sőt, százmillióinak kiküldésére van lehetőség, ami jelentős bevételi forrást jelenthet. A botnetek többek között a kéretlen reklámleveleknek köszönhetik térnyerésüket, mert ezen keresztül váltak igazán pénztermelő lehetőséggé.

• **Illegális tartalom tárolása.**
A botnet, mint egy zombihadsereg egy gyakorlatilag végtelen tárolókapacitással rendelkező háttértárat jelent a támadók számára, hogy illegális tartalmakat (lopott mozifilmeket, lemásolt játékokat, drága szoftvereket) tároljanak. A fájlokat a gép felhasználójától elrejtett helyeken is tárolhatják.

• **Adatgyűjtés.**
Mivel a botkliensek gépek ezrein futnak, könnyűszerrel megszerezhetik a gépeken futó szenzitív adatokat, neveket, jelszavakat, e-mail címeket stb., ahogy azt más spyware programok is megtehetik.

6. Botnetek felismerése

A botnetek működését megértve lehetőségünk nyílik azok detektálására is. A botnetek az elosztottság előnyét használják ki, hogy detektálásuk nehézkes legyen. Egy túlságosan elosztott rendszer azonban nem elég hatékony, így a botnet tulajdonosoknak is kompromisszumot kell kötni a detektálhatóság és a használhatóság terén. Ez a tulajdonság adja meg a lehetőséget a botnetek detektálására.

Botnetek detektálása két fő módszerrel történhet:

– *Felhasználók szintjén*, amikor a felhasználók gépére telepített kódot próbáljuk meg vírusirtó programok vagy behatolásfelismerő rendszerek (IDS, Intrusion Detection System) segítségével megtalálni.

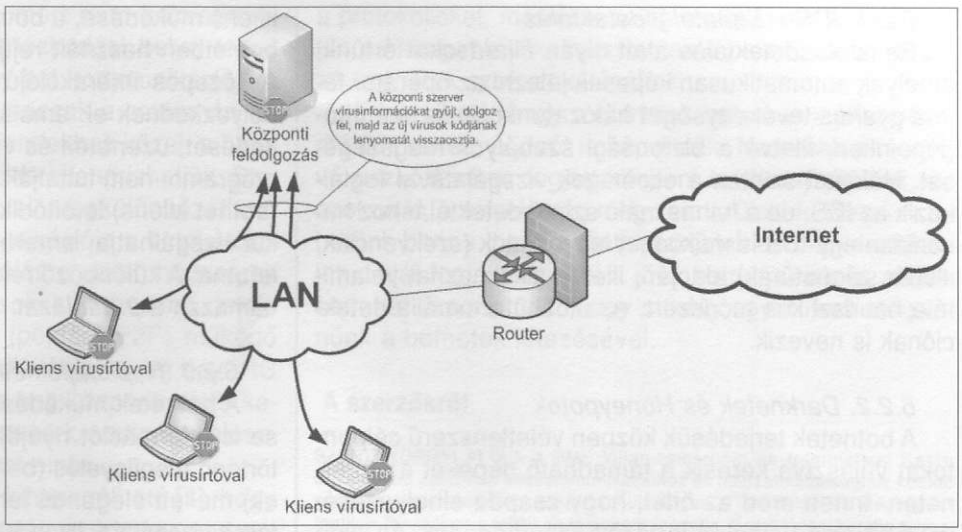
– *Hálózat szintjén*, amikor a teljes (al)hálózat forgalmát vizsgálva próbáljuk a botnetek forgalmát és tevékenységeit detektálni.

6.1. Detektálás felhasználó szinten

Alapvetően a botnetek két szinten detektálhatók. A legkézenfekvőbb megoldás a *felhasználói szintű felismerés.* Ekkor a végfelhasználónál telepített vírusirtó (illetve komplex védelmi) szoftverek segítségével észlelhetők a számítógépre telepített botnetek. A megoldás akkor lenne igazán sikeres, ha minden felhasználó rendszeresen használna vírusirtót, hiszen így garantálni lehetne a védelmet az ismert botnetek terjedése, fenntartása ellen. A felhasználói szintű védekezés azonban nem mindig lehet sikeres: sok esetben a felhasználók jelentős részénél a rosszindulatú kód hosszú időn át futásképes marad és a botnetek mérete csak csökken, de csökkent méretben is igen nagy kapacitással rendelkeznek.

Az egyéni felhasználók mellett a vállalatoknak is nagy figyelmet kell fordítaniuk számítógépeik karbantartására. Szinte mindegyik védelmi szoftver rendelkezik központosított menedzsmenttel *(2. ábra)*, jelentés és naplózás funkcióval. A központi felismerést segítheti az antivírus szoftver naplófájljainak központilag történő gyűjtése is.

Egy lokális fertőzés esetében így több gépen is sikerülhet azonosítani a veszélyforrást, mielőtt az nagyobb károkat okozhatna akár a saját hálózatunkban, akár mások hálózatában.



2. ábra
Központosított vírusfelismerés és feldolgozás

Az antivírus szoftverek mindazonáltal komplexebb feladatokat is elláthatnak, ha valamilyen egyéb hálózatbiztonsági szoftverrel – például tűzfallal – is képesek együttműködni. A gyanús viselkedési minta származhat abból a következtetésből, hogy egy program portokat nyit a felhasználó számítógépén, vagy gyanús, például nagy mennyiségű forgalmat generál bizonyos portokon. Ideális esetben a felhasználóknak maguknak kellene megszabni, hogy milyen általuk futtatott szoftverek használhatják az internetkapcsolatot, azonban ez a felhasználóktól nem várható el, pedig a védelmi szoftverek már ma is képesek lennének ilyen kifinomult ellenőrzések megvalósítására is.

Az antivírus rendszerek alapvetően két módon próbálják meg felismerni a kártékony programokat. A legegyszerűbb módszer, hogy a már ismert kártevő kódját felhasználva abból egy lenyomatot (úgynevezett szekvenciát) készítenek, ezt tárolják, majd a víruskeresés során a fájlokban ezeket a lenyomatokat keresik. Természetesen a különböző vírusirtó programok más és más algoritmusokat használnak, így ugyanarról a víruskódról más és más lenyomatot tárolnak. A megoldás előnye, hogy gyors és megbízható, hátránya viszont, hogy csak ismert kártevők vagy azok ismert variánsainak felismerésére használható.

A másik módszer a kártékony kódok keresésénél a *heurisztikus eljárás,* amelynek lényege, hogy akkor próbálja meg detektálni a vírusokat és más rosszindulatú kódokat, amikor azok lenyomata még nem létezik az adatbázisban. A kártevők megjelenése, a lenyomat elkészítése és a frissítés között eltelt idő alatt a kártevők szabadon garázdálkodhatnak, ezt illusztrálja a *3. ábra.*

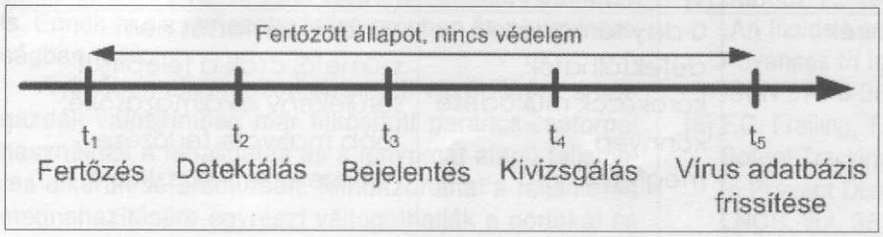
Ennek kivédésére jelentek meg a heurisztikát használó módszerek, amelyek kódokra és eseményekre alkalmazott szabályok pontozása alapján számítanak ki egy értéket, majd ennek függvényében döntik el, hogy az adott program kártevőnek minősül-e vagy sem. A heurisztikus eljárások előnye, hogy olyan kártékony kódokat is képesek felismerni, amelyeknek a lenyomata még nem szerepel az adatbázisban. Hátránya viszont, hogy sokkal nagyobb valószínűséggel hibáznak, így kártevőnek vélhetnek ártalmatlan alkalmazást és fordítva. Ez utóbbi tulajdonság miatt manapság inkább a lenyomat alapú eljárások használata a megszokott.

A felhasználói szintű védekezés hasznos a botok felderítésében, a korai felismerésben és segíthet a bothadseregek visszaszorításában, azonban önmagában nem nyújt megfelelő védelmet a heterogén felhasználói környezet miatt a bothálózatok ellen. Az is látható, hogy ez az alacsony szintű védelem önmagában nem alkalmas a botgazdák felderítésére és felelősségre vonására, továbbá a támadók lépéselőnye miatt a védelmi szoftverek előtt járva mindig használhatnak olyan módszereket, amelyekre a védelmi szoftverek még nem készültek fel.

6.2. Botnetek detektálására ismert módszerek hálózati szinten

A botnetek felderítésének egy másik módszere a *hálózati szintű felismerés.* Ebben az esetben egy egész (al)hálózat forgalmát vizsgálva, például lehallgatással történik a botnetek keresése és blokkolása. A megoldás előnye, hogy a rendszer a felhasználóktól és a botok kódjától is teljesen független, így az ismert forgalmi mintával rendelkező botok könnyen kiszűrhetőek, valamint a forgalomból bizonyos esetekben következtetni lehet a támadó kilétére is. Ennek következtében a felelősségrevonás is nagyobb eséllyel történhet meg, mint a felhasználói szintű védelem esetében.

A hálózati szintű felismerés több részre osztható a módszer függvényében. A leggyakrabban használt eljárások a csapdagépek és csapdahálózatok (honeypotok és honeynetek) és a behatolásdetektálás (IDS, Intrusion Detection System).



3. ábra
Lenyomat alapú felismerés folyamata a fertőzéstől az adatbázis frissítésig

6.2.1. IDS – Behatolásdetektálás

Behatolásdetektálás alatt olyan eljárásokat értünk, amelyek automatikusan képesek jelezni az operátor felé a gyanús tevékenységet hálózatunkban és számítógépeinken, illetve a biztonsági szabályok megszegését. Hálózati szinten a csomagok vizsgálatával foglalkozik az IDS, de a felhasználó szintű detektáláshoz hasonlóan egy IDS is működhet lenyomatok (szekvenciák, illetve szignatúrák) alapján, illetve alkalmazhat valamiféle heurisztikus módszert, ez utóbbit anomália-detekciónak is nevezik.

6.2.2. Darknetek és Honeypotok

A botnetek terjedésük közben véletlenszerű célpontokat választva keresik a támadható gépeket az Interneten. Innen ered az ötlet, hogy csapda elhelyezésével megismerhetőek a fertőzött számítógépek. Az ilyen csapdákat (angolul *honeypot,* bővebben lásd [3,4]) helyezhetjük a szokásos internetes környezetbe, de felhasználhatunk olyan IP tartományokat is, amelyek ugyan le vannak foglalva és az útvonalválasztás is működik hozzájuk, de nincsenek használatban. Az ilyen nem használt internetes címtartományokat nevezik *darknetnek.* A honeypotok gyűjtött adatainak integrálása, közös kezelése is megoldható, ezt általában honeynetnek hívjuk.

A csapdagépeket interakciós szintjük szerint kategorizálhatjuk, többnyire alacsony, közepes és magas interakciójú csapdákról beszélhetünk. Alacsony interakciós szinten a csapda szinte semmit nem enged a támadónak, elfogadja a támadást jelentő adatcsomagokat (legyen az e-mail, vagy valamilyen hiba kihasználása), de a támadónak nem enged további lehetőségeket. A másik véglet esetén, a magas interakciójú honeypot a támadás sikeres lezajlását is végrehajtja, lehetőséget biztosít a támadónak a rosszindulatú kód telepítésére és futtatására. Az alacsony interakciójú csapdák így többnyire listaszerű adatgyűjtésre szolgálhatnak fertőzött gépekről, míg a magas interakciójú csapdák segítségével pontosan megismerhető egy-egy botnet kliens működése, a botnethálózat vezérlése, de akár a botnetben használt rejtjelezés kulcsai is rögzíthetőek. A közepes interakciójú csapdák pedig a kettő között helyezkednek el: emulálják a támadható program működését, üzeneteit és válaszait, de valójában az adott programot nem futtatják. Az emuláció során a káros kód (botnet kliens) letöltődik, de a csapdát felállító fél anélkül vizsgálhatja, ismerheti meg azt, hogy az valójában lefutna. A különböző rendszerek összehasonlítását tartalmazza a *2. táblázat.*

6.2.3. Naplófájlok és hálózati forgalom analízise

A botnetek működésére a hálózati forgalom analízise is információt nyújthat. A folyamatos, céleszközzel történő megfigyelés (behatolásdetektáló eszközök, IDS-ek) mellett elegendő lehet azonban csak egyes naplófájlok vizsgálata. Ilyen lehet a kapcsolók (switchek), vagy az útvonalválasztók (routerek) naplójának vizsgálata. Ezekben a naplófájlokban a modern hálózati berendezések esetén konkrét hálózati forgalominformációk mellett már támadásokról szóló riasztásokról is információkat szerezhetünk.

Külön érdemes megemlíteni a Cisco által kifejlesztett Netflow [5] megoldást. Ez egy tárolási formátum és egyszerre egy vizsgálati módszer is. A hálózati berendezéseinken részletes információk menthetők el a hálózati forgalom egyes kapcsolatairól. Ez történhet teljeskörűen vagy részben, mintavételezéssel. A mentett adatok elemzésére modern eszközök állnak rendelkezésre, ezekkel is felfedezhetőek feltört számítógépek, bot klienseket futtató védett gépek.

6.2.4. Egyéb megoldások

A fent említett megoldásokon kívül számos cikk foglalkozik botnetek felismerésével. Ezek még kísérleti fázisban lévő megoldások, ezért az elérhető szoftverek ezeket a módszereket általában nem alkalmazzák.

Az egyik alapvető ötlet az IRC szervereken működő botok parancs-csatornáinak figyelése. Az IRC azért is

2. táblázat Honeypot-alapú támadásfelismerés típusai, működési elvük, és tulajdonságaik

	Működési elve	Előnye	Hátránya
Alacsony interakciójú honeypot	Teljes alhálózatot emulál, de szemben a darknettel, válaszol is a kérésekre	A teljes alhálózat modellezhető	Kártevők konkrét azonosítása nem megoldott, főként megfigyelésre alkalmas
Közepes interakciójú honeypot	Alkalmazási réteg virtualizációja: alkalmazások szimulálása	Káros kód nem települ, de könnyen elkapható	Károkozó hálózati forgalma nem vizsgálható
Magas interakciójú honeypot	Konkrét rendszerek megvalósítása	0-day támadások detektálhatók, károkozók működése könnyen megfigyelhető	Minden támadás nem szűrhető, csak a telepített sérülékeny alkalmazásoké, több malware fertőzése nehezen szétválasztható

előnyös a botgazda számára, mert nem közvetlenül kommunikál a botokkal, így tartózkodási helye rejtve marad még akkor is, ha néhány bot kommunikációjára fény derül. Az IRC forgalmat nemcsak a csatornán folyó beszélgetéssel, hanem a kliensekhez közel, a hálózati kommunikáció vizsgálatával is ellenőrizhetjük. Statisztikai módszerek segítségével megkülönbözethető lehet a valós személyek kommunikációja a botokétól.

Az IRC alapú botnet-detektálásra adott módszerek viszonylag széles körűek. Ám sokkal nehezebb detektálni az elosztott rendszerben (például P2P) működő botneteket. A nehézséget az adja, hogy amíg egy IRC alapú botnet detektálása során egy központi elem keresésére van lehetőség (IRC szerver), addig egy elosztott rendszer esetében ilyen host nincs.

A P2P botok detektálásakor kihasználható [1], hogy a botok egymáshoz csatlakoznak, ezért egy portnak vagy port-tartománynak folyamatosan nyitottnak kell lennie, hogy a többi bot forgalmát fogadni tudja. Ezeket a portokat keresve, esetleg a portok forgalmát monitorozva lehetőség nyílhat a botok megfigyelésére. A módszer hátránya, hogy a porthoz nem köthető teljes bizonyossággal botnet-forgalom, így sok téves riasztás is keletkezhet. További megoldás lehet a sikertelen kapcsolódások figyelése, hiszen a botok megpróbálnak kapcsolódni a megadott címlistához, ám ez gyakran sikertelen. Ezen kívül, ha több host is próbál fix IP-címhez csatlakozni, és az nem érhető el, akkor az szintén gyanús viselkedésre utalhat.

A fent említett megoldásokon túlmenően egyre újabb és újabb megoldások látnak napvilágot a botnetek felderítésére, azonban a botok is fejlődnek: kommunikációjuknak elrejtése és új botnet variánsok megjelenése megnehezíti a fertőzött forgalom és a káros kódok detektálását.

7. Összefoglalás és jövőkép

Cikkünkben ismertettük a botnetek fogalmát, működését, hatásait és a felismerés lehetőségeit. Láthattuk, hogy a botnetek a mindennapjaink részévé váltak, hiszen számítógépeinket fertőzve elosztottan visznek végbe támadásokat, illetve küldenek kéretlen reklámleveleket a botgazda utasítására. A botnetek fejlődése mindemellett a mai napig folytatódik. A régebben nagy port kavart, több százezres, sőt a legnagyobbnak becsült hálózatok esetében több milliós zombi hálózatok helyett manapság inkább már a kisebb hálózatokat preferálják a botgazdák, hiszen ezek detektálásának a valószínűsége jóval kisebb. A központosított megoldások helyett pedig előtérbe kerülnek a peer-to-peer alapokon működő botnetek is. Ennek oka a nehezebb felismerésben és a rugalmasságban rejlik.

A jövőben alkalmazott botnetek vezérlésére a botgazdák valószínűleg már titkosított parancs-csatornát használnak a lehallgatás és a lenyomat alapú felismerés elkerülése érdekében. Mindazonáltal a felismerés megnehezítésére egyrészt váltogathatják a portokat és a protokollokat, másrészt pedig a statisztikai keresés ellen paddinget is alkalmazhatnak a parancsokat hordozó üzenetek szofisztikálásához.

Elmondható, hogy a botnetek nemcsak a jelent és a múltat, hanem a jövőt is képviselik. Nemcsak a meglévő eszközeinken fogják kifejteni tevékenységüket, de azokon is, amelyek még meg sem születtek. Biztosak lehetünk benne, hogy okostelefonjaink és más eszközeink célját fogják képezni a jövő botnetjeinek és abban sem kételkedhetünk, hogy sokáig együtt kell még élnünk a botnetek létezésével.

A szerzőkről

SZENTGYÖRGYI ATTILA a BME Villamosmérnöki és Informatikai Karán diplomázott 2006-ban telekommunikációhoz és hálózatbiztonsághoz kötődő szakirányokon. Jelenlegi doktori tanulmányait a Távközlési és Médiainformatikai Tanszéken a HSNLab tagjaként folytatja. Érdeklődési körébe tartoznak a vezetéknélküli hálózatok biztonsági kérdései, az ad hoc és peer-to-peer hálózatok biztonsága, a behatolásdetekció és -megelőzés, különösképp a botnetek vizsgálata és az azonosító alapú kriptográfiai eljárások alkalmazhatósága.

SZABÓ GÉZA Kecskeméten született 1982-ben. Egyetemi diplomáját a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerezte 2006-ban. Munkája során internetes forgalom felismeréssel és modellezéssel foglalkozik. Az Ericsson Magyarországnál dolgozik kutatóként és PhD hallgató a Távközlési és Médiainformatikai Tanszék Nagysebességű Hálózatok Laboratóriumában a BME-n.

Irodalom

[1] Schoof, R., Koning, R.,
„Detecting peer-to-peer botnets",
University of Amsterdam, 2007.
http://staff.science.uva.nl/~delaat/sne-2006-2007/p17/report.pdf

[2] C. Schiller, J. Binkley, G. Evron, C. Willems, T. Bradley, D. Harley, M. Cross,
Botnets: The Killer Web App. Syngress, 2007.
ISBN 1597491357

[3] N. Provos, T. Holz,
Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison-Wesley Prof., 2007.
ISBN 0321336321

[4] Wicherski, G.,
„Medium Interaction Honeypots", 2006.
http://www.pixel-house.net/midinthp.pdf

[5] Cisco Systems,
Introduction to Cisco IOS NetFlow, 2007.
http://www.cisco.com

[6] Strayer, W. T., Walsh, R., Livadas, C. Lapsley, D.,
„Detecting Botnets with Tight Command and Control",
31st IEEE Conference on Local Computer Networks (LCN'06), 2006.

[7] Barford, P., Yegneswaran, V.,
„An Inside Look at Botnets",
Advances In Information Security, Springer, 2007.
ISBN 978-0-387-32720-4

[8] F.C. Freiling, T. Holtz, G. Wicherski,
Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks,
LNCS, Vol. 3679, 2005.