HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

Illési Zsolt
Proteus Consulting Kft.
illesi.zsolt@proteus.hu

BOTNETEK KIALAKULÁSA, HASZNÁLATUK, TRENDJEIK

Absztrakt

Az internet fejlődésével, az információ- és a kommunikációs technológiák konvergenciájával új bűncselekmények jelentek meg. Ezen technikák egyike a „botnet", melynek hatására egyre több számítógép van kitéve a zombi gépek támadásának, illetve a zombivá válás fenyegetésének.
Jelen munka összefoglalja a botnetek fejlődését, azonosítja a lényeges ismérveit, elemzi a botnetek architektúráját és a főbb támadási módokat. A botnetek fejlődésnek elemzésekor a szerző előrevetíti azokat az irányokat, amelyek a botnetek struktúrájára, illetve az a támadási módszerekre jellemzők lehetnek a jövőben.

Expansion of the internet, the convergence of information and communication technology get new criminal techniques surfaced. One of these is botnet, which made unavoidable that more and more networked computers are under the attack or suffers from the attacks of zombie computers.
This paper summarises the evolution of botnets, identifies its main criteria, and analyses the architecture and main attack methods. In the trend analysis of botnet evolution, taking into consideration both attack methods and botnet architecture, the author highlights some possible directions of future enhancements.

***Kulcsszavak**: internet, rosszindulatú szoftver, zombi, botnet ~ internet, malware, zombie, botnet*

Bevezetés

Az internet térhódítása megállíthatatlan. A múlt század utolsó évtizedében viharos gyorsasággal terjedtek el a számítógépek és fejlődött a globális hálózat is. Ma már az élet minden területén ott vannak a számítógépek, az internethasználat természetes és nélkülözhetetlen.

Az informatika és a kommunikáció konvergenciájával a papír alapú irodák lassan eltűnnek, a nyilvántartások adatbázisokba, adattárházakba kerülnek, amelyeket már csak

számítógéppel lehet keresni, megtekinteni. Az ipari rendszerek irányítása is egyre inkább automatizált lesz, a termeléstervezés, a folyamatirányítás és az adminisztráció terhei és aprólékos részletei is a gépekre hárulnak. A gazdaság többi szereplője is számítógépfüggővé válik, nincs bank, repülésirányítás, de számvitel, sőt lassan levelezés sem számítógépek, hálózatok és internet kapcsolat nélkül. A kor követelményeihez igazodva az államigazgatás is, az állampolgár-barát állam az ügyfélkapukon keresztül egyre több szolgáltatást biztosít az interneten keresztül, és az államigazgatás feladatai közül is egyre többet számítógépesítenek.

E trend elől a katonai szervezetek sem tudnak kitérni. Az információs képességek fejlődésével a korszerű számítástechnikai megoldások, kommunikációs technikák is jelen vannak a korszerű haditechnikai megoldásokban. A tudás alapú hadsereg (Knowledge Based Army) a legkorszerűbb digitális technológiát használja felderítésre, kommunikációra, információs műveletekre, az adatok feldolgozására, a vezetési-döntési feladatok hatékonyságának növelésére, a harctevékenység támogatására.

A számítógépek egyre inkább felgyorsítják az ügyintézést, a folyamatirányítást, egyszerűbbé és kényelmesebbé teszik a mindennapokat. A technológiai fejlődéssel együtt azonban a bűnözés is fejlődött. A hagyományos bűnözés mellett megjelent a kiberbűnözés, a kiberterrorizmus is. Az új típusú bűnözés természetesen sajátos bűnelkövetési módszerekkel is rendelkezik, megjelentek a programozott és az információtechnológiához kapcsolódó egyéb fenyegetések, amelyeket a biztonsággal, információ biztonsággal vagy információs terrorizmussal foglalkozó szakembereknek is meg kell ismerniük, hogy felkészülhessenek az ellenük való védekezésre.

Dolgozatomban ezek közül az új technikák közül szeretnék egyet – a botneteket – bemutatni, feltárva a sajátosságait, ismertetve a felhasználásának módját és a fejlődésének lehetséges trendjeit.

Botnetek fogalma, kialakulása

A botnet szó a robot és a hálózat (network) szavakból keletkezett informatikai zsargon, az együttműködő szoftver robotok számítógép hálózaton keresztül összekapcsolódó és együttműködő csoportját jelenti. Az ilyen szoftver robot hálózatok tudományos, mérnöki vagy például üzleti célokra is létre lehet hozni, és ezek főleg az elosztott, párhuzamos vagy többszálas számítások terén alkalmazhatók hatékonyan. A legitim felhasználás mellett a botnetek szolgálhatják az internetes alvilágot abban, hogy illegálisan pénzt vagy adatokat szerezzenek. A továbbiakban ezekkel, a bűnözők által működtetett botnetekkel foglalkozom.

A kiberbűnözők által menedzselt botneteket olyan internetes kapcsolattal rendelkező szoftver robotok, ún. zombi számítógépek alkotják, amelyeket a gépen futó valamely program sebezhetőségét kihasználva távolról megfertőznek, vagyis amelyekre valamilyen távoli menedzselésre is alkalmas rosszindulatú programot telepítenek a felhasználó tudta és akarata nélkül. Zombivá bármilyen internetre kötött programozható, memóriával és processzorral rendelkező eszköz válhat, tekintet nélkül arra, hogy milyen módon kapcsolódik az internetre vagy, hogy milyen technológiát képvisel, így PC-k, notebookok, PDA-k, mobiltelefonok is megfertőzhetők.

A botneteket az ún. pásztor (herder, botherder) irányítja, rendszerint valamilyen közbeiktatott számítógépen keresztül (Command and Control, vagy C&C szerver). [1] [2]

A botnetek kialakításának első lépése egy olyan program megírása, amely lehetővé teszi a sebezhető számítógépek megfertőzését és az azok feletti kontrol megszerzését. Ezek a programok rendszerint úgy vannak megírva, hogy sikeres fertőzés után további célpontokat keressenek (és fertőzzenek meg), illetve felvegyék a kapcsolatot a C&C szerverrel (és szolgálatra jelentkezzenek), vagy megnyissanak egy portot, amelyen keresztül lehetővé teszik,

hogy a pásztorok egy célzott portszkennelés során felismerhessék őket és átvehessék az uralmat. Ezeket a programokat a fejlesztőik egyre gyakrabban automatizált módon mutálják, vagyis úgy módosítják a program felépítését, kódját, hogy az ne érintse a programok funkcionalitását, azonban megnehezítse a víruskeresők számára a felismerést.

A botnet kliens természetesen a saját működést nem csak a víruskeresők elől, hanem a számítógép jogosult felhasználója elől különböző technikák alkalmazásával is eltünteti. Az álcázás során elrejtheti a futtatásához szükséges könyvtárakat, fájlokat, processzeket, vagy valamely jogosult program nevében futva ártalmatlannak tünteti fel magát.

A botnetek kialakítására és működtetésére a legtöbb esetben az Internet Relay Chat (IRC: RFC 1459 és RFC 2812) kliens-szerver alapú csevegő protokollt használják, de a botnetek fejlődésével egyéb protokollokat (pl. HTTP) vagy egyenrangú kapcsolatot biztosító (peer to peer vagy p2p) technológiára épülő megoldásokat is alkalmaznak már. Ezek a nem IRC alapú botnet kliensek általában megnyitnak egy portot, amelyen keresztül megszólíthatók és menedzselhetők.

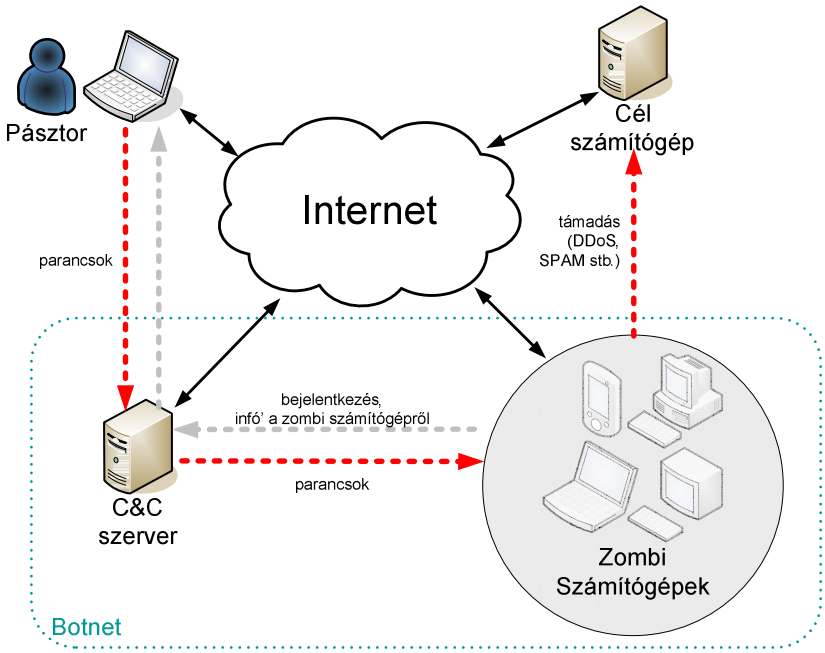
A megfertőzött gép általában nem marad passzív a megfertőzést követően, hanem a környezetében lévő számítógépeiket pásztázza, hogy van-e közöttük olyan, amelyet megfertőzhetne. Ennek az aktivitásnak a következményeként egyes becslések szerint az interneten lévő számítógépek akár fele is zombi számítógép lehet.

A pásztor feladata a fertőző kór megírása és szabadon eresztése után már „csak” annyi, hogy megtalálja és vezérelje a zombikat. A pásztorok azonban nem csak a számítógép felhasználókkal küzdenek a gép kontrolljáért, de egymás közt is rivalizálnak, hogy a mások által megfertőzött gépeket hogyan tudnák saját uralmuk alá hajtani. A több zombi ugyanis jelentősebb támadási potenciált, több adatot és nagyobb erőforrásparkot jelent.

A kontrollált gépekkel a pásztor rendszerint az IRC alapú C&C szerveren keresztül kommunikál, azonban arra is lehetőség van, hogy valamely zombi szervert a pásztor C&C szerverré nevezzen ki, és azon a gépen keresztül kommunikáljon a „nyájjal”.

A pásztor a zombi számítógépekről közvetlenül is letöltheti az azokon tárolt adatokat, illetve utasíthatja azokat valamilyen célpont megtámadására. A zombi-szerver, valamint a szerver-pásztor csatornát a protokollba ágyazott titkosítás védheti, így az egyszerű hálózati betörésfigyelő rendszerekbe épített mintafelismerő rutinok sem képesek minden esetben azonosítani a nemkívánatos kommunikációt.

A botnet sémáját és a működésének vázlatát a következő ábra mutatja be:



1. ábra – A botnetek működési sémája [szerk.: Illési Zsolt]

Az első botnetek az IRC hálózatok kialakulását követően jöttek létre. Az IRC kényelmi szolgáltatásainak bővülésével lehetővé vált a szerverek és a kliensek egyes feladatainak automatizálása. A szkriptekkel[1] automatizált kényelmi szolgáltatásokat nyújtó IRC kliensek voltak a botnetek előfutárai. A hackerek természetesen már korán felismerték az automatizmusokban rejlő lehetőségeket és felderítették a rendszerben rejlő sebezhetőségeket. A korai támadások egyszerűek voltak, és csak néhány parancs eredeti, a rendszer mély ismeretéről tanulságot tevő utasítás alkalmazásából állt.

A technológia elterjedésével nőtt a kliensek száma, de ezzel együtt nőtt a renitens felhasználók és a visszaélések száma és a támadások bonyolultsága. A támadók először gyerekes csínyként az IRC szerver, egyes felhasználók egymás gépei, illetve IRC kliensei felett vették át az uralmat és tevékenykedtek a nevükben, majd megjelentek a „keményebb játékosok", akik már rosszindulatúan vagy nyereségvágyból használták fel a tudásukat és okoztak kárt.

Az IRC operátorok természetesen ott voltak a „tűzvonalban" és a támadások szaporodásával ők is kivették a szerepüket: a rosszindulatú felhasználókat és a szerver szabályait megszegőket kitiltották a szerverről. A kizárt felhasználók természetesen visszavágtak: az első DoS (Denial of Service, azaz szolgáltatás-megtagadás) és DDoS (Distributed Denial of Service, azaz megosztott szolgáltatás-megtagadás) támadásokat az IRC szerverekkel szemben indították.

[1] A szkriptek (makrók, parancs, batch stb.) valamely programhoz kapcsolódó magas szintű programnyelven megírt parancsállományok, amelyek lehetővé teszik az alkalmazáshoz kapcsolódó funkciók automatizált, paraméterezett végrehajtását, adatstruktúrák manipulálását. A szkriptelésre példa a DOS/Windows rendszerekben alkalmazott batch, a Linux környezetben a shell programozás, de ilyen például az MS Office esetében a VBA (illetve a VBA makrók), Open Office környezetben a Python makrók.

Az IRC protokoll nyitott jellege egyébként is vonzotta a problémás elemeket és a rosszindulatú kódokat. Megindult az IRC sebezhetőségét és gyenge pontjait kihasználó eljárások és kódok fejlesztése, illetve a kliens gépek meghódításáért folytatott verseny.

A korai internet protokollok strukturális sebezhetősége egyébként is kedvezett a visszaéléseknek, például a spam elterjedésének oka is javarészt az SMTP gyengeségében keresendő.

Az IRC funkcionalitásának bővülése, az ezt használó felhasználók számának növekedése, illetve a megfertőzött számítógépek számának növekedése felkeltette az alvilág figyelmét is, elkezdték felfedezni az ebben rejlő lehetőségeket.

A botnetek kialakításának és felhasználásának az alvilág figyelme új fejeztet nyitott, ami az internet közössége számára több megfertőzött gépet, több problémát, a bűnözők számra komoly profitot jelent.

Botnetek főbb felhasználási területei

Jelenleg a „csata" az operátorok, biztonsági szakemberek és a botneteket kialakító, felhasználó kiberbűnözők között még nem dőlt el. Az IRC folyamatos finomítása és a protokoll ismert sebezhetőségeinek kiküszöbölése az ismert támadási vektorok számát csökkenti ugyan, de a vírus, féreg és trójai programfejlesztők bevonása, a támadási módszerek finomodása újabb kiskapukat nyit meg a bűnözői körök előtt. [1]

A zombi számítógépeket a bűnözők többféleképp is felhasználhatják. A megfertőzött gépen lévő adatokat közvetlenül elérhetik, vagy a tömegben rejlő lehetőségeket felhasználva megtámadhatnak további meg nem fertőzött célszámítógépet. Ezeket a támadásokat a következőképp lehet csoportosítani:

- adat lopás;
- csalás;
- szolgáltatás megbénítás vagy blokkolás;
- rosszindulatú kód továbbítása.

2. ábra – Támadások botnetekel és zombi számítógépekkel [szerk.: Illési Zsolt]

Az adatlopás során elsősorban a zombi gépeken tárolt bankkártya adatokhoz, hitelesítési adatokhoz (felhasználónév, jelszó), személyes adatokhoz, üzleti titkokhoz férhet hozzá a támadó. Mivel a pásztor a felhasználó gépe felett teljesen átveszi az uralmat, a megszerzett adatokat letöltheti a saját vagy más számítógépére, módosíthatja, vagy törölheti azokat.

Egyes bot klienseknek külön az adatlopásra kifejlesztett rutinjaik vannak, amelyek szisztematikusan kutatnak a megfertőzött gépen dokumentumok, képek videók, bankkártya adatok, felhasználói azonosítókat és jelszavakat tartalmazó rendszerfájlok, vagy egyéb érzékeny adatok után.

A támadónak lehetősége van arra is, hogy a jogosult felhasználót megszemélyesítve jelenjen meg az internet közössége előtt és a felhasználók nevében kövessenek el csalást.

A jellemző elkövetési módot az internetes zsargon a clickfraudnak nevezi. A támadás alapja a kattintás alapú hirdetés (pay per click), vagyis egy olyan internetes üzleti modell, amelyben egy weblap tulajdonos és egy marketing cég megállapodnak abban, hogy a hirdető vagy marketinges cég a weblapok felületén megjelenő hirdetésekre történő kattintások alapján fizet a weblap tulajdonosnak (pl. Google AdSense) valamilyen előre megállapított összeget.

A csalás során a zombi gépek, valós IP cím, esetleg valós felhasználói adatok felhasználásával, szimulálják a felhasználói magatartást és a hirdetésekre kattintásokat. A kattintások számának növelésével a reklámstatisztikák használhatatlanná válnak, megzavarják a viselkedés-alapú hirdetések értékelését, így rontva egy-egy marketing kampány hatásfokát, továbbá a jelentősen megnövelt kattintások eredményeként többletköltséget is okoznak a hirdetőnek. A kattintási statisztikák szabálytalanságai aláássák a bizalmat is a szerződő felek között, és ennek eredményeként a hirdetési felületeket bérbeadók elveszthetik a beszerzési forrásaikat. [1]

A zombi számítógépek felhasználhatók szervergépek szolgáltatásának megbénítására úgy, hogy legitimnek látszó kérésekkel árasztják el a célszámítógépet, amely így nem lesz képes a valódi felhasználók igényeinek kielégítésére, és jelentősen megnő a válaszideje vagy megbénul (szolgáltatás megbénítás: DoS vagy Denial of Services). A zombik számának növelésével a támadások számát radikálisan növelni lehet ezáltal a célszámítógép szolgáltatásait sokkal nagyobb valószínűséggel lehet leállítani, illetve jelentősen meg lehet növelni a leállás időtartamát (DDoS). [1]

A támadók célja lehet valamely vetélytárs informatikai szolgáltatásainak (webhely, fájlmegosztás, internetes alkalmazás vagy e-szolgáltatás) tartós megbénítása. Esetenként a támadók „védelmi pénzeket” szednek olyan vállalkozásoktól, amelyeknek üzleti-kritikus alkalmazásai elsődlegesen az interneten keresztül érhetők el (pl. internetes fogadás). A támadó ilyen esetben demonstrálja, hogy képes megakasztani a kritikus alkalmazások működését, a megtámadott pedig ezt követően vagy üzleti modellt vált, vagy megpróbálja a sávszélesség, a szerverek kapacitásának növelésével védeni magát, vagy beadja a derekát és kifizeti a zsarolónak a váltságdíjat.

A támadó célszámítógép megbénítása nélkül, a kritikus adatfájlok titkosításával is ellehetetlenítheti a jogszerű használatot, illetve zsarolhatja a felhasználót, hogy váltságdíj vagy valamilyen fizetős szolgáltatás fejében (például gyógyszerkészítmény vásárlása legalább 50 USD értékben valamelyik orosz webáruházban) tegye újra lehetővé a kódolt adat hasznosíthatóságát. [3]

A zombi számítógépek felhasználhatók arra, hogy aktívan bővítsék a botnet „klienseinek” körét, és a hálózati kapcsolaton keresztül az ismert sebezhetőségeket kihasználva további számítógépeket keressenek és fertőzzenek meg (vírus, trójai programok stb. távoli telepítésével).

A zombik egyik legismertebb adattovábbítási funkciója a kéretlen levelek (spam) küldése. A kéretlen levelek „kék pirulákkal”, szépészeti beavatkozásokkal, legális és illegális termékekkel és szolgáltatásokkal bombázzák az internet közösségét. A statisztikák szerint a spam felel a legális internet forgalom jelentős részéért, komoly fejtörést és többletterhet róva az internet szolgáltatókra, levélszerver üzemeltetőkre és a levelezést folytató felhasználókra, hogy hogyan kezeljék a megnövekedtet adatforgalmat, illetve hogyan szűrjék ki a kéretlen levelek áradatából azokat a leveleket, amelyeket legitim céllal legitim felhasználók küldenek a címzettnek.

A botnetek jelenlegi adatforgalmának kisebbik része a felhasználói magatartások nyomon követése. A zombi gépek közvetlenül vagy közvetve személyes információkat

gyűjtenek (spyware), amelyek hozzájárulnak a spam kampányok címlistáinak kialakításához és finomhangolásához.

Botnet trendek

A botnetek fejlődése nem állt meg. A támadók felismerték a védetlen felhasználói gépekben rejlő lehetőségeket. A pásztorok már nem csak maguknak gyűjtik a zombi gépeket, hanem megindult a botnetek kereskedelme is. Egyre nagyobb létszámú és egyre jobban szervezett botneteket lehet venni vagy bérelni spam küldésre, adatgyűjtésre, vagy a konkurencia működésének megzavarására. [4] [5] A kereskedelmi lehetőségek hatására a támadók köre kibővült, nem kell informatikai szakértőnek lenni, hogy egy botnet tulajdonosaként azt támadási célra felhasználja valaki. Több botnet egyidejű birtoklásával, pedig egymástól függetlenül, de egy időben vagy egy esemény bekövetkeztekor is elindíthatók a támadások, ezzel is növelve a támadás hatékonyságát és eredményességét.

Az eddig fegyverrel, bombával „dolgozó” terrorszervezetek:

- a zombi gépekből nyert adatok adatbányászati módszerekkel történő feldolgozásával a támadásaik előkészítéséhez nyerhetnek többletinformációt;
- a letöltött hitelesítési adatokat közvetlenül felhasználva a jogosult felhasználót megszemélyesítve, annak jogaival visszaélve tevékenykedhetnek informatikai rendszerekben;
- szolgáltatás megbénítással a kritikus infrastruktúrát vezérlő számítógépeket, informatikai rendszereket állíthatnak le;
- kéretlen levélszemétben széles körben reklámozhatják a céljaikat, toborozhatnak tagokat, gyűjthetnek pénzt és erőforrásokat.

A technológia fejlődésével várhatóan a támadó egyre inkább a névtelenség homályába fog süllyedni, például újabb és újabb C&C szerverek bevonásával az irányítási hierarchia szintek bővítésével, a kommunikációs csatornák következetes és hatékony titkosításával. A csatorna titkosítására használhatnak szabványos protokollokat (SSH), anonim kommunikációs csatornákat (onion routing), egyedi fejlesztésű kriptográfiai megoldásokat vagy ezek valamilyen kombinációját. Ezek alkalmazásával nem csak a támadó személyét egyre nehezebb felderíteni, hanem a botnetekhez tartozó zombikat és a botnet egyedei közötti kommunikációt is. A jövőben az IRC alapú vezérlés mellett egyre nagyobb szerephez jutnak az egyenrangú kliensekből álló botnetek, amelyben bármely gép rendelkezik a C&C szerver képességeivel, és a pásztor véletlenszerűen alakíthatja ki a feladathoz legjobban illeszkedő irányítási struktúrát.

A kliensek intelligenciájának növelésével a jövő botnetjei képesek lesznek elkerülni a felderítést, a csatornatitkosítás mellett, például a botnet kliens program polimorfikus kódolásával, a csatornák/portok szélesebb körének kihasználásával. Az intelligens botnet kliensek képesek lesznek az operátorok és a biztonsági szakemberek által állított csapdák (honeypot, kliens kód visszafejtés, beépülés) észlelésére és kijátszására. [6] [7]

A botnetek önvédelmi funkcióit a fejlesztők kiegészítik a „megelőző csapás” képességgel, így például a botnetek a felderítést érzékelve:

- viszont felderítést (sebezhetőségi vizsgálatot) és a feltárt gyenge pontok ellen célzott, vagy
- DDoS

támadást intéznek az ellen a számítógép ellen, ahonnan a felderítés indult.

A botnetek egy másik várható fejlődési iránya az elosztott párhuzamos számítások végzése. A hackerek már jelenleg is komoly eredményeket értek el a kriptográfiai kódok megfejtésének időproblémájának tárhely problémává konvertálásával kapcsolatban[2] [8] [9], illetve egyes csoportok már kísérleteznek a zombi gépekből kialakítható szuperszámítógépekkel [10]. Az elosztott párhuzamos számítások célja a kriptográfiai támadások mellett lehet például a begyűjtött adatok adatbányászati elemzés hatékonyságának növelése.

A bűnözők mellett a katonai szervezetek is felfigyeltek a botnetekben rejlő lehetőségekre. A honi informatikai infrastuktúra szerepének növekedése és külföldi hadseregek (pl. Kína) online jelenlétének megerősödése és az ebből adódó fenyegetés miatt az USA katonai vezetői egyre többet és egyre komolyabban foglalkoznak saját katonai célú botnet hálózat kifejlesztésével és működtetésével. A defenzív stratégiai megoldások mellett a „digitális szőnyegbombázás", az ellenséges országok, szervezetek internetes infrastruktúrájának megbénítása jelentős tényező lehet a modern stratégák eszköztárában. [11]

Összefoglalás

Az internet térhódításával az informatika és a kommunikációs technikák-technológiák konvergenciájával elkerülhetetlen, hogy egyre több és több számítógép legyen kitéve a botnetek hatásainak. A hálózatba kötött gépeket vagy a zombivá válás, vagy a zombik támadása fenyegeti.

Dolgozatomban összefoglaltam a botnetek lényeges ismérveit, a rendszereztem lényeges támadási módszereket. A trendek elemzésénél kiemeltem azokat a fejlődési irányokat, amelyek a véleményem szerint a jövőben meghatározói lesznek ennek a támadási módszernek.

A botnetek fenyegetése ellen csak a jogalkotók, a gyártók, az internet szolgáltatók és a felhasználók együttesen tudnak hatékonyan fellépni.

A jogalkotóknak olyan normákat kell alkotniuk, amelyek megteremtik a támadók felderítésének és felelősségre vonásának kereteit, meghatározzák a gyártóktól, az internet szolgáltatóktól, az egyedi és szervezeti felhasználóktól, a szervezetvezetőktől elvárható gondosság szintjét. A jogalkotónak a követelmények támasztása mellett a rendvédelmi, igazságszolgáltatási, honvédelmi és egyéb államigazgatási szervek feladati ellátásához szükséges tárgyi, jogi és anyagi feltételekről is gondoskodnia kell. A botnetek elleni hatékony fellépéshez egy ország erőfeszítései nem elegendőek. A hazai jog mellett nemzetközi fellépésre is szükség van a határokon átívelő problémák megelőzésére, felderítésére és hatékony kezelésére.

A gyártóknak a jelenleginél hatékonyabb és hibatűrőbb biztonsági protokollokat és funkciókat kell beépíteniük a termékeikbe. Amennyiben a gyártók felelősség tehetők a biztonsági szempontból alkalmatlan termékek (egyedi vagy dobozos szoftver, hardverbe ágyazott program), úgy várhatóan több biztonságos termék jelenne meg a piacon. A biztonságosabb termék nem csak a felhasználónak jelent magasabb garanciát arra, hogy a rendszer az elvárásai szerint fog működni, de a termék környezetében működő társfelhasználóknak is kevésbé kéne tartaniuk egy hibás termék miatti fenyegetéstől.

Az adatbiztonsági, adatvédelmi és titokvédelmi törvények mellett néhány speciális szervezet (hírközlési szolgáltatók, pénzügyi szervezetek) számára a jogalkotó már most is

[2] Az ingyenes 400 MB-os szivárvány tábla segítségével 99%-os valószínűséggel törhetők fel az akár 14 karakter hosszú, betűket és számokat tartalmazó jelszavak, a 9GB-s pénzért beszerezhető változat, pedig már külön kezeli a kis és nagybetűket, valamint a speciális karaktereket is.

meghatároz olyan speciális feladatokat, amelyeket az informatikai rendszer védelmében meg kell tenniük. Azonban az informatikai szolgáltató (pl. szakértői-tanácsadó tevékenységet vagy kiszervezett informatikai üzemeltetést végző) szervezetek felelősségét, az ilyen szervezetektől elvárható személyi és tárgyi feltételeket is a jelenleginél részletesebben, például az építészek sajátos szakmai követelményeihez és jogosultságaihoz hasonlóan, kellene meghatározni ahhoz, hogy az internetes fenyegetettség szintje csökkenjen.

Az internet szolgáltatóknak a jelenleginél hatékonyabban kellene kontrollálniuk az általuk kezelt alhálózatba –be és kiáramló adatot a legális felhasználók tevékenységének tiszteletben tartása mellett.

Az egyéni felhasználóknak is el kell sajátítaniuk a biztonságtudatos számítógép és internet használat alapjait. Ebben az oktatás, az új fenyegetéseket és az elhárításukat tudatosító kampányok és a biztonságot is érdemben tárgyaló – és nem utolsó sorban érthető – dokumentáció nyújthat segítséget.

Irodalomjegyzék

[1] Wikipedia: Internet bot, Zombie computer, Dosnet; Wikipedia, h.n., http://en.wikipedia.org

[2] Sándor Munk: Software robots (softbots), their characteristics, and military applications, ZMNE, h.n., 2001. http://www.zmne.hu/tanszekek/ehc/konferencia/april2001/munk.html

[3] David Emm: Focus on trojans – holding data to ransom, Network Security Volume 2006, Issue 6, June 2006, p 4-7

[4] Robert Lemos: Bot herder pleads guilty to 'zombie' sales, Security Focus, h.n., 2006. http://www.securityfocus.com/news/11370

[5] kdawson: US Bot Herder Admits Infecting 250K Machines, Slashdot, h.n., 2007. http://it.slashdot.org/article.pl?sid=07/11/10/2054234&from=rss

[6] Elia Florio and Mircea Ciubotariu: Peerbot: Catch me if you can, Symantec Security Response, Ireland, 2007. www.symantec.com/avcenter/reference/peerbot.catch.me.if.you.can.pdf

[7] John Canavan: The Evolution of Malicious IRC Bots, Symantec Security Response, h.n., 2005. www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf

[8] Index: Percek alatt fejti meg jelszavainkat az új hackerszerszám, Index, h.n., 2007. http://index.hu/tech/szoftver/passwd110907/

[9] http://ophcrack.sourceforge.net/

[10] Kristóf Csaba: A botnetek verik a szuperszámítógépeket, Computerworld, h.n., 2007, http://www.computerworld.hu/botnetek-verik-szuperszamitogepeket.html

[11] COL. CHARLES W. WILLIAMSON III: Carpet bombing in cyberspace, Why America needs a military botnet, 2008/05, http://www.armedforcesjournal.com/2008/05/3375884