HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

Gábri Máté
Zrínyi Miklós Nemzetvédelmi Egyetem
gabrimate@ippimail.com

A CYBERBŰNÖZÉS ÚJ HAJNALA - OROSZ ÜZLETEMBEREK A VILÁGHÁLÓN

Absztrakt

Már az internet születése előtt „divat" volt a telefonos hálózatok feltörése pusztán szórakozásból, vagy egy-egy távolsági hívás kedvezményes lebonyolítása miatt. A világháló segítségével a kártékony szoftverek terjedése és terjesztése előtt új dimenziók nyíltak, illetve a távoli hálózatok elérhetővé váltak a kíváncsi szemek számára. Mindezidáig az interneten folyó bűnözői tevékenység jelentős részét az egyéni szórakoztatás, valamint az egyszemélyes, esetleg kis létszámú csoport haszonszerzési szándéka tette ki. Napjainkban megfigyelhető, hogy komoly gazdasági és politikai érdekeltséggel bíró szervezetek jelennek meg a cyberbűnözők között. Jelen írás egy ilyen esetet kíván bemutatni az elmúlt másfél év eseményei alapján.

People liked to hack into the telephone networks before the internet was borne to make trunk calls cheaper. The malicious code or software could spread farther and faster with the World Wide Web, and the networks became more accessible for the curious eyes. Until recently crime on the internet was like a hobby for some enthusiasts, or money making for individuals or a small group. However, nowadays groups with economic and political interests are appearing behind cyber-crime. This paper's aim to describe such a group based on events in the last one and a half years.

Kulcsszavak: *cyberbűnözés, spam, Russian Business Network, botnet ~ cyber-crime, spam, Russian Business Network, botnet*

BEVEZETÉS

A világháló hasznos és jó dolog. Végtelen sok funkcióját, szolgáltatását, lehetőségeit felsorolni szinte lehetetlen, azonban erre nincs is szükség, hiszen a fontosabbakat nap, mint nap használjuk: információ-keresés, csevegés, levelezés, böngészés. Kis gyakorlattal pillanatok alatt megtalálhatunk bármit az interneten, unaloműzőként pedig beszélgethetünk, levelezhetünk ismerőseinkkel vagy akár új barátokat szerezhetünk. Ez a kellemes és egyben hasznos időtöltés azonban nem veszélytelen, és hogyha nem vagyunk kellően tudatosak, és nem figyelünk eléggé, akkor könnyen áldozatul eshetünk a világhálón egyre inkább terjedő,

otthoni felhasználókat célzó bűnözésnek.

Az internet robbanásszerű fejlődése az ezredforduló környékére tehető, amikor a szélessávú, percdíj nélküli internet elérhetővé vált a lakosság szélesebb rétegei számára. Egyre nagyobb igény mutatkozott a meglévő szolgáltatások fejlesztésére, újak bevezetésére, majd ezek segítségével jutott el közvetlenül szinte minden emberhez a világháló. Új dimenzió nyílt meg a szolgáltatói szektor számára, tele kiaknázatlan lehetőségekkel, melyre természetesen a bűnözői körök is szemet vetettek. A folyamatosan frissülő, bővülő otthoni felhasználói tábor kétségkívül ideális célpontot jelent a rossz indulatú személyek, szervezetek számára.

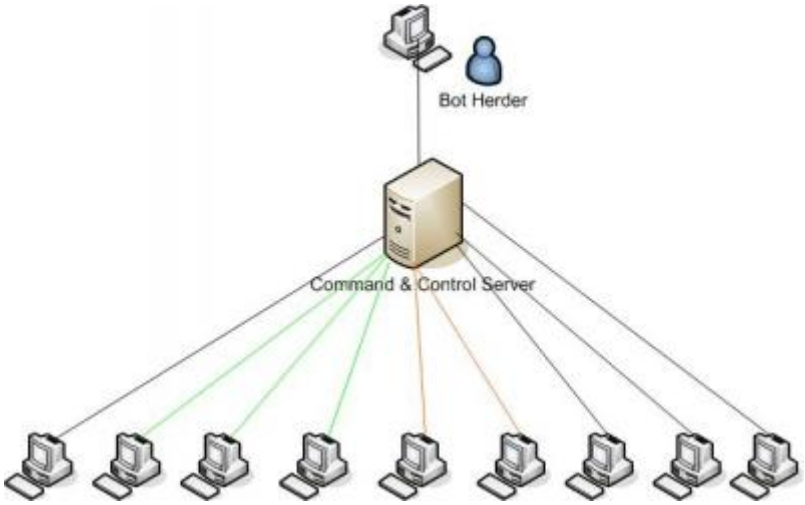
Az otthoni felhasználó alapvetően jóhiszemű, hiszen egy fizetős szolgáltatást használ, ezért eleinte nem gyanakszik, illetve nem feltétlenül van tisztában az interneten előforduló fenyegetésekkel. Éppen ezért kevesebb, vagy éppen semmilyen figyelmet nem fordít számítógépe és internetforgalma biztonságára, és minden megjelenő tartalmat jóindulatúnak minősít. A kártékony kódok, programok ezt a helyzetet használják ki azokon a szolgáltatásokon keresztül, melyeket napi rendszerességgel használunk. Ilyenek például e-mailben terjedő vírusok vagy a sűrűn látogatott weboldalakba beillesztett kódrészletek, melyek tartósan megfertőzhetik a látogató számítógépét, vagy információkat – például a látogatott weboldalon megadott felhasználónév és jelszó, bankszámlaszámok és PIN-kódok, a számítógépen tárolt jelszóadatbázis, stb. – juttathatnak el a kód készítőjéhez. A sor szinte a végtelenségig folytatható, hiszen a lista kimeríthetetlen, és nap, mint nap újabb módszerekkel bővül.

Cikkemben egy olyan gazdasági szervezetet szeretnék bemutatni, amely végtermékként legális tevékenységet, szolgáltatást folytat, azonban jövedelmét mégis a világhálón megtalálható illegális forrásokból szerzi.

A *Storm* féreg

A tavalyi év elején egy újabb, kártékony e-mail melléklet jelent meg az interneten, ami a *Storm Worm* (Storm féreg) névre hallgatott. Ugyanakkora figyelmet kapott, mint a naponta több tucatnyi megjelenő más káros program, tehát szinte semmit. A programocska júniusban kezdett feltűnni a különféle informatikai biztonsággal foglalkozó híroldalak hasábjain, illetve a technikai fórumokon. Ekkor derült fény arra, hogy az eddig csendben terjedő „élősködő” a megfertőzött gépeket egy úgynevezett bot-hálózatba csatolja[1] *(lásd: 1. ábra: A botnet felépítése)*.

1 A bot-hálózat, vagy ismertebb nevén *botnet*, olyan „zombi” gépekből álló internetes hálózat, melyet egy másik hasonló zombi gép, vagy egy személy irányít és használ fel illegális cselekedetekre.



1. ábra: A botnet felépítése

A több tízezres „géppark” már szép eredménynek mondható egy botnet esetén, amivel napi több százezer spam[2] küldhető, vagy komoly *DDoS*[3] támadás indítható internetes kiszolgálók ellen. Pesszimista becslések szerint a *Storm* worm által megfertőzött gépek száma 250 ezer és 1 millió közé tehető[1], míg mások szerint elérte a 10 milliót [2] is.

A hagyományos botnetek vezérlése egy központi webszerveren, vagy IRC-csatornán keresztül történik. Ez a kapcsolat könnyen felderíthető és blokkolható akár az internetszolgáltató, akár a helyi hálózati infrastruktúrában található csomagszűrők által. A *Storm* készítői ezért egy másik, decentralizált vezérlési formához nyúltak. Az alkalmazott protokoll a *peer-to-peer* nevet viseli, és itt nem egy központi kiszolgálóról gyűjtik be az információt a kliensek, hanem mindegyik kliens csak két másikat lát, az egész hálózatot nem. Természetesen megfelelő idő alatt ez a felépítés is visszakövethető lenne, azonban itt nem néhány tucat, hanem több százezer gép kapcsolatáról beszélünk. Ebben a *peer-to-peer* hálózatban is található néhány vezérlő gép, ahonnan a parancsok kiindulnak. A támadók, hogy elrejtsék ezeket a klienseket, az úgynevezett *fast-flux* eljárást használják. Minden egyes géphez több (akár több ezer) IP címet rendelnek, melyeket folyamatosan cserélnek, így a kiinduló parancsok, kapcsolatok mindig más kiindulási címet mutatnak és szinte lehetetlen visszakövetni, hogy fizikailag hova mutatott az adott cím[3]. Mintha ez még nem lenne elég, a *Storm* Worm egy meglehetősen egyszerű védelmi mechanizmussal is rendelkezik. Amikor észleli, hogy a hálózati adminisztrátorok behatolás észlelő[4] eszközökkel vizsgálják a gépeket, akkor *DDoS* támadást indítanak az ellenőrzést végző gép ellen.

A kezdetekben a *Storm* bot saját magát terjesztette spamekkel, azonban a több százezres infrastruktúra már sokkal nagyobb lehetőségeket rejt magában. A hálózat egy részét *DDoS* támadásokra használták, míg más részét bérbe adták személyeknek, cégeknek, akik kéretlen e-mailek küldésére használták a megfertőzött gépeket. Szeptember 9-én 280 ezer fertőzött gépről tudtak biztosan, amelyek aznap összesen 2,7 milliárd spamet küldtek szét az

2 Kéretlen e-mail. Olyan levél, melyet a címzett szándéka ellenére kapott.

3 Distributed Deniel of Service, vagyis elosztott szolgáltatás-megtagadási támadás. A „hagyományos” szolgáltatás-megtagadási támadás precízebb formája, ugyanis itt nem egy, hanem több számítógép vesz részt. A támadást indító számítógépek csatlakozási kérelmet (TCP SYN csomag) küldenek a szolgáltatást nyújtó szervernek, az visszaküldi a kérés nyugtázását és a saját kapcsolatfelépítési kérelmét, amire azonban már nem kap választ. A kiszolgáló 30 másodpercig nyitva hagyja a kapcsolatot a beérkezési kérelemre várva és ez idő alatt a memóriában le van foglalva a kapcsolat számára bizonyos hely. Elosztott támadás esetén másodpercenként akár több tízezer kérés érkezhet, ami könnyen használhatatlan állapotba juttattatja a szervert, így a valódi kapcsolatot igénylő kliensek számára elérhetetlenné válik a szolgáltatás.

4 IDS, Intrusion Detection System.

interneten, ami körülbelül 4%-a volt a teljes spam forgalomnak. [4]

A *Storm* féreg ráadásként egy úgynevezett *rootkit*-et is telepített az áldozat gépére, melynek segítségével egy támadó azonnal rendszergazdai jogosultságot szerezhetett a gépen. Eleinte külön meghajtóként települt, így viszonylag könnyebb volt felderíteni és eltávolítani, azonban később már meglévő rendszermeghajtókba – mint például a hálózat egy protokolljáért felelős tcpip.sys, vagy a cdrom.sys – települt, megnehezítve az ártalmatlanná tételüket [5].

Illegális szolgáltatás, legálisan?

A kártékony programokat, vezérlő szoftvereket valahol tárolni kell, a legtöbb esetben az internet-szolgáltatók tárhelyét használják e célra. Amint az illetékes szolgáltató arról értesül, hogy szerverein káros anyagokat tárolnak, azonnal törli azt, egyebet sajnos nem tehet.

Az orosz **Russian Business Network** (továbbiakban RBN) elsősorban tárhelyszolgáltató, azonban más internetes tevékenységet is folytat. Ügyfelei számára garantálja, hogy a tartalmat nem törlik, illetve szervereik védve vannak a különféle *DDoS* támadásoktól. Természetesen ezt a „szolgáltatást" meg kell fizetni. Egy átlagos méretű tárhely körülbelül hat-tízszerese a hagyományos szolgáltatók által kiszabott díjnak. A kapcsolatfelvétel nem hivatalos formában történik: fórumokon, levelezőlistákon keresztül lehet elérni az üzemeltetőket és a kívánt tárhelyet, illetve egyéb szolgáltatásokat megigényelni.[6] A jelenlegi jogszabályok – főleg az Orosz Föderációban – nem kényszerítik az internet-szolgáltatókat a kártékony tartalmak eltávolítására, így az RBN zavartalanul működtetheti webszervereit.

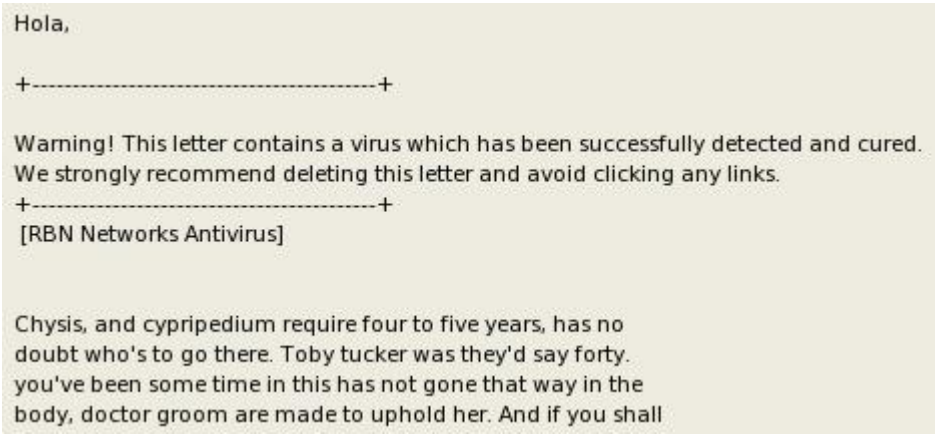
Az RBN természetesen nem csak tárhelyszolgáltatással foglalkozik. Bevezette az egyik legdivatosabb alvilági módszert, a védelmi pénz szedését. Az eljárás egyszerű: *DDoS* támadással megbénítanak egy gépet, vagy akár egy teljes hálózatot, majd felkeresik az üzemeltetőt, és egy tetemesebb havi összegért garantálják a szolgáltatások védelmét. [7] Emellett aloldalakon keresztül eladásra kínálnak rendszer- és hálózati feltörést segítő szoftvereket. A felhozatal teljesen vegyes, és található néhány igazi „gyöngyszem" is, például grafikus felületű, fejlesztői támogatást élvező termékek. Ilyen az *Mpack* nevű eszköz, mellyel tetszőleges, weboldalba épülő kódokat lehet készíteni, melyek megfertőzik a látogatók gépét, majd egy webes felületen keresztül a támadó adatokat – elsősorban internetes banki tranzakcióknál használt információt – lophat az áldozat számítógépéről. A szoftver körülbelül 700 dollárba kerül, ami magában foglal egy éves támogatást, illetve lehetőség van kiegészítők vásárlására is. [8] Az *Mpack* leglátványosabb megjelenése a *Bank of India* honlapjának megfertőzése volt. [9] A honlapba egy 3 soros kódot [10] ültetett a támadó, ami kártékony programok tucatjait telepítette a látogatók számítógépére.

Nyár végére a két legkiterjedtebb botnet a *Storm* és az *Mpack* által megfertőzött hálózatok voltak. Olyannyira elterjedtek, hogy a készítők egymást kezdték támadni „cyberhadseregeikkel". A többszázezres gépparkok *DDoS* támadásai olyan mértékű internet-forgalmat generáltak, hogy egyes szolgáltatók be tudták mérni a főbb vezérlőgépeket és az érintett hálózatot egyszerűen lekapcsolták a világhálóról.

Novemberben a teljes RBN hálózat eltűnt az internetről, egyrészt a leválasztás miatt, másrészt, pedig a tulajdonosok állították le a szervereket. [11] Nem sokkal később Kínában és Tajvanon vélték felfedezni az RBN nyomait. [12] A Spamhaus.org adatbázisa szerint [13] széles IP tartományokat regisztráltak, azonban aktív használatuk elmaradt. Feltételezett megjelenésük nagy nyilvánosságot kapott szakmai körökben, így kiemelt figyelemmel illették az adott IP tartományokat az informatikai biztonsággal foglalkozó szervezetek. Ennek hatására ismét „sátrat bontottak" és eltűntek a világhálóról. Feltételezhetően ismét felbukkannak majd, azonban jóval elővigyázatosabbak lesznek. Több mint valószínű, hogy ezúttal a világ különböző pontjain, több internet-szolgáltatónál elosztva fognak megjelenni, hogy felderítésük nehezebb legyen.

Miről mesél egy spam?

Vélhetően jelen cikk szerzője is kapott egy, az RBN létezésére utaló nyomot. A *2. ábrán* egy spam látható, amit feltehetően az RBN-en keresztül kézbesítettek. A törzsszöveg gyakorlatilag lényegtelen, csak a megszólítás utáni kiemelt rész a fontos, ami figyelmeztet minket, hogy a levél vírust tartalmaz, azonban a kereső szoftver ezt sikeresen felfedezte és hatástalanította, majd javasolja a levél törlését, és azt tanácsolja, hogy egyetlen linkre se kattintsunk. Ami a legérdekesebb az az, hogy mindezt az *RBN Networks Antivirus* szoftvere végezte, a levél szerint. Gyanítom az e-mail míg elérte a laptopomat semmilyen szűrésen nem esett át, mégpedig azért, mert a figyelmeztetés ellenére nem tartalmazott semmilyen linket, mellékletet és a számítógépemen futó víruskereső sem talált semmi gyanúsat. Ebből arra következtetek, hogy a figyelmeztetést az RBN hálózatot használó spammer, vagy az általuk készített spamküldő szoftver beilleszt egy ilyen, vagy ehhez hasonló automatikus üzenetet a címzett megnyugtatására.


Hola,

+----------+

Warning! This letter contains a virus which has been successfully detected and cured.
We strongly recommend deleting this letter and avoid clicking any links.
+----------+
[RBN Networks Antivirus]

Chysis, and cypripedium require four to five years, has no
doubt who's to go there. Toby tucker was they'd say forty.
you've been some time in this has not gone that way in the
body, doctor groom are made to uphold her. And if you shall

2. ábra: Spam az RBN-től

A levél forrása *(lásd: 3. ábra: RBN spam forrása)* mutatja, hogy a helyi gépen futó spam- és vírusszűrő nem találta gyanúsnak.[5] A spam-et küldő SMTP szerver feltehetően egy fertőzött olasz irodai szerver, mégpedig azért, mert statikus IP címmel rendelkezik[6], azonban a címhez nem tartozik regisztrált domain név *(lásd: 4. ábra: A spammer név szervere)*[7], valamint MX rekord *(lásd: 5. ábra: A spammer MX rekordja)*. A bejegyzett és megfelelő IP címre mutató MX, valamint PTR rekord elengedhetetlen a hiteles e-mail küldéshez. Sajnos a fogadó szerverek többsége nem ellenőrzi ezek meglétét, elősegítve a spam-ek terjedését.

5 X-Virus-Flag: no és X-Spam-Status: No jelölés.

6 Több, mint valószínű, hogy a szervert internet átjáróként használja egy vállalkozás és azért kapott fix címet, mert a szolgáltatóknál az üzleti előfizetéshez ez jár.

7 Nincs bejegyzett név szerver és az IP címet a szolgáltató által biztosított igen hosszú és kacifántos név oldja fel. (host88-32-static.43-88-b.business.telecomitalia.it)

```
X-Virus-Flag: no
Return-Path: <lichenology@gampot.com>
X-Spam-Checker-Version: SpamAssassin 3.2.4 (2008-01-01) on notebook
X-Spam-Level:
X-Spam-Status: No, score=0.0 required=5.0 tests=HTML_MESSAGE autolearn=ham
        version=3.2.4
X-Original-To: info@duosol.hu
Delivered-To: m5070@royalty.hu
Received: from host88-32-static.43-88-b.business.telecomitalia.it (host88-32-static.43-88-b.business.telecomitalia.it [88.43.32.88])
        by royalty.hu (Postfix) with SMTP id D404338245
        for <info@duosol.hu>; Mon, 17 Mar 2008 15:39:38 +0100 (CET)
Date: Mon, 17 Mar 2008 14:41:50 +0000
From: "Clarkin Burel" <lichenology@gampot.com>
X-Mailer: The Bat! (3.0.2.2) Professional
Reply-To: Clarkin Burel <lichenology@gampot.com>
X-Priority: 3 (Normal)
Message-ID: <9372130529.20080317143724@gampot.com>
To: <info@duosol.hu>
Subject: valle
```

3. ábra: RBN spam forrása

```
notebook scout3r # host -t NS host88-32-static.43-88-b.business.telecomitalia.it
host88-32-static.43-88-b.business.telecomitalia.it has no NS record
```

4. ábra: A spammer név szervere

```
notebook scout3r # host -t mx host88-32-static.43-88-b.business.telecomitalia.it
host88-32-static.43-88-b.business.telecomitalia.it has no MX record
```

5. ábra: A spammer MX rekordja

Tovább kutattam a rejtélyes spammer gép után és még érdekesebb információra találtam, amivel korábbi feltételezésemet támaszthatom alá, miszerint a küldő gép egy fertőzött irodai szerver. A kiszolgálón futtatott operációs rendszer nagy valószínűséggel Microsoft Windows Server valamelyik verziója és a világháló felé nyitott szolgáltatások is ezt mutatják *(lásd: 6. ábra: A spammer szerver adatai)*. Ami még érdekes lehet az a PPTP, ami a VPN megvalósítások egyik változata, mely a Microsoft termékeiben is megtalálható. Sajnos ez a protokoll hemzseg az ismert biztonsági résektől ezért használata erősen ellenjavallt. [14]

A tárgyalt kiszolgálón futó verzió például támadható érvénytelen TCP fejléc beállításokkal. A támadó ezt kihasználva egyetlen egy, jól megszerkesztett csomaggal lekapcsolhatja a cél tűzfalát, teljes és nyitott hozzáférést szerezve a géphez *(lásd: 7. ábra: PPTP sebezhetőség)*.[8] Az elemzés utolsóként egy Webmin nevezetű szolgáltatást vélt felfedezni, azonban ez csak UNIX alapú rendszereken érhető el. Rövid keresés után egy hálózati adatmentő szoftverre bukkantam, ami alapértelmezett beállításként a 10.000-es TCP portot használja Windows alatt. Feltételezem ehhez hasonló futhat a kiszolgálón.

Látható, hogy SMTP (25-ös TCP port) szolgáltatás nem fut a gépen, így e-mail szerver nem lehet a kiszolgáló. Ebből is csak arra tudok következtetni, hogy a spam-et, vagy spam-eket küldő kártékony szoftver feladatát befejezve inaktív állapotba került, hogy majd egy későbbi időpontban ismét levélszeméttel áraszthassa el a világhálót.

8 A hibakeresés a Nessus (http://www.nessus.org) nyílt forrású szoftverrel készült.

```
notebook scout3r # nmap -sS -sV -O host88-32-static.43-88-b.business.telecomitalia.it

Starting Nmap 4.20 ( http://insecure.org ) at 2008-03-18 22:31 CET
Interesting ports on host88-32-static.43-88-b.business.telecomitalia.it (88.43.32.88):
Not shown: 1687 closed ports
PORT      STATE    SERVICE       VERSION
67/tcp    filtered dhcps
135/tcp   filtered msrpc
136/tcp   filtered profile
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  open     pptp?
3389/tcp  open     microsoft-rdp Microsoft Terminal Service
10000/tcp open     http          Webmin httpd
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows 2003|2000|XP (97%)
Aggressive OS guesses: Microsoft Windows 2003 Server SP1 (97%), Microsoft Windows 2000 Server SP4 (90%), Microsoft Windows 20
00 SP4 (90%), Microsoft Windows XP SP2 (90%), Microsoft Windows XP SP2 (firewall disabled) (90%), Microsoft Windows 2000 SP3
(89%), Microsoft Windows 2000, SP0, SP1, or SP2 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

OS and Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 143.657 seconds
```

6. ábra: A spammer szerver adatai

Security Issues and Fixes: host88-32-static.43-88-b.business.telecomitalia.it

Type	Port	Issue and Fix
Vulnerability	pptp (1723/tcp)	The remote system appears vulnerable to an invalid Options field within a TCP packet. At least one vendor firewall (Symantec) has been reported prone to such a bug. An attacker, utilizing this flaw, would be able to remotely shut down the remote firewall (stopping all network-based transactions) by sending a single packet to any port. See also : http://www.eeye.com/html/Research/Advisories/AD20040423.html Risk factor : High CVE : CVE-2004-0375 BID : 10204 Other references : IAVA:2004-A-0010, OSVDB:5596 Nessus ID : 12216
Informational	pptp (1723/tcp)	Synopsis : A VPN server is listening on the remote port. Description : The remote host is running a PPTP (Point-to-Point Tunneling Protocol) server. It allows users to set up a tunnel between their host and the network the remote host is attached to.

7. ábra: PPTP sebezhetőség

Következtetések

Az RBN amellett, hogy számos „újítást” vezetett be az internetes bűnözés módszerei közé, kitűnő példával szolgál arra, hogy a világháló történései komoly nemzeti és nemzetközi biztonsági kérdéseket vetnek fel.

Az RBN nem egy kedvtelésből káros programokat író fiatalok kis csoportja. Fő profiljuk a szolgáltatás, ami a jelenlegi jogi környezetben teljesen legális, függetlenül a tartalomtól. Teljes körű infrastruktúrát biztosítanak a kártékony szoftverek terjesztéséhez, fejlesztéséhez, illetve elérhetővé teszik végfelhasználók számára.

Az amerikai hatóságok nyomoztak az RBN és a *Storm* féreg alkotói után, Oroszország azonban nem volt hajlandó együttműködni, így nem jártak sikerrel. Egyes feltételezések szerint azért sem, mert az RBN-nek szoros kapcsolatai vannak a vezető politikai körökkel. [15]

Ahhoz, hogy a cyber-bűnözést hatékonyan tudjuk kezelni, nemzetközi együttműködésre és megfelelő jogharmonizációra lenne szükség.[9]

Egy jól szervezett, komoly pénzügyi és szakmai tőkével rendelkező csoportosulás igen komoly veszélyt jelenthet egy adott ország informatikai és információs infrastruktúrájára. Elképzelhető, hogy az RBN is segédkezett az Észtország elleni informatikai támadásban, hiszen az több mint valószínű, hogy Oroszországból indult ki, és pont egy olyan időszakban, amikor az RBN erejének tetőpontján volt. A támadásban használt eljárás – elosztott szolgáltatás-megtagadási támadás – abszolút az RBN profiljába illik, és megfelelő eszközök álltak rendelkezésre, hogy sikeresen véghezvigyék.

A támadások kifinomultabbak, szervezettebbek, ugyanis a tét igen komoly, a lebukás esélye pedig ezzel egyenes arányosságban nő. A célpontok eleinte az egyszerű otthoni felhasználók, azonban ahogy nő a rendelkezésre álló infrastruktúra és a világháló feletti befolyásoló képesség, úgy változik a célpontok jellege, típusa és ezzel együtt emelkedik a várható nyereség is.

Egy gazdasági alapon, kvázi legálisan működő, profitorientált bűnöző szervezet elleni harc rendkívül nehéz. A csoporthoz közeli személyektől szinte lehetetlen információt szerezni, hiszen az anyagi tényező erősebb, mint a „jót cselekedni” tudat.

Elengedhetetlen, hogy az ilyen internetes bűncselekményeket rugalmasan, nemzetközi együttműködéssel és a lehető legrövidebb idő alatt képesek legyünk lereagálni.

Felhasznált irodalom

- *Hálózati biztonság.* Tom Thomas, Panem, Budapest 2005.
- *Information Warfare*. Winn Schwartau, Thunder's Mouth Press 1996.
- *Information Warfare and Security*. Dorothy E. Denning, Addison-Wesley 1999.

Internetes hivatkozások

[1]. http://www.networkworld.com/news/2007/080207-black-hat-storm-worms-virulence.html?page=1

[2]. http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_or_te.html

[3]. http://www.darkreading.com/document.asp?doc_id=129304

[4]. http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_o

9 Gábri Máté, *Információs biztonság, azaz a biztonság hatodik dimenziója.* Hallgatói Közlemények, XI. évf. 2. szám

r_te.html
[5]. http://en.wikipedia.org/wiki/Storm_Worm
[6]. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html
[7]. http://www.networkworld.com/news/2008/021908-researcher-russian-hosting-network-runs.html?page=1
[8]. http://blog.washingtonpost.com/securityfix/2007/06/the_mother_of_all_exploits_1.html
[9]. http://www.theregister.co.uk/2007/09/01/bank_of_india_website_takeover/
[10]. http://sunbeltblog.blogspot.com/2007/08/breaking-bank-of-india-seriously.html
[11]. http://www.theregister.co.uk/2007/11/08/rbn_offline/
[12]. http://it.slashdot.org/article.pl?sid=07/11/09/1957239&from=rss
[13]. http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK7829
[14]. http://www.schneier.com/pptp-faq.html
[15]. http://blog.washingtonpost.com/securityfix/2008/01/unhappy_birthday_to_the_storm.html