Who Owns Your Network?

A Discussion of Bot Networks

Norman Elton - Matt Keel
College of William & Mary

The more one learns...

...the more paranoid one becomes.

© 2005 – College of William & Mary. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
Intro

- Obligatory introductions
- About our campus and network
- Our involvement in bot research
- What we hope to accomplish today
What’s a Bot?

- A piece of software that connects back to a centralized control channel.
- Allows unauthorized control of many machines from a single point.
- Typically lies dormant, waiting for commands from its controller.
- The single greatest threat facing humanity.
Bot Lifecycle

1 Initial infection and payload
Bot Lifecycle

2 Command and Control Server

Infection Source → C&C
Bot Lifecycle

3 Download additional payload

Infection Source ➔ C&C ➔ Additional Payload
Bot Lifecycle

4 Spread to additional machines
Initial Infection Vectors

- Unpatched operating systems with remotely exploitable vulnerabilities
  - LSASS, RPC-DCOM, etc.
- Weak/non-existent administrator passwords
- Malicious websites exploiting vulnerable browsers
- Social engineering exploiting vulnerable users
Social Engineering

- **The Goal** – Convince the user to download and execute an evil payload
- The payload changes often, avoiding anti-virus software
- The payload is typically transparent – the user notices nothing
  - “I clicked, but nothing happened!”
- Can be very creative
Methods of Social Engineering

- Embed payload inside popular downloads on peer-to-peer networks
- Send e-mail to all the contacts in an infected PCs address book, referring them to a link
- Send IM to all friends on buddy list
- Change a user’s instant messenger profile or away message. This method is particularly prevalent on campus networks.
Methods of Social Engineering

Pre-Infection
Methods of Social Engineering

Post-Infection
Types of Initial Payload

- EXE
- SCR
- PIF
- GIF/JPEG when the display engines are found vulnerable
Payload delivery

- Typically regular HTTP requests to a compromised web host
- Occasionally FTP, TFTP, DCC, CSend
- Perhaps P2P
Command and Control

- Allows control of many hosts from one centralized system
- Typically IRC (Internet Relay Chat)
- Credible reports of Yahoo Messenger
- Honeynet paper references encrypted chat channel called Waste. This is too scary to contemplate.
Command and Control - IRC

evil.example.com
192.168.64.23
10.1.100.4
172.18.3.42
Command and Control - IRC

evil.example.com
192.168.64.23
172.18.3.42
Command and Control - IRC

- Once online, bots await commands from botmaster.
- Attacker typically authenticates identity to the bots using a password. example: `.login 1aml33t`
- Once authenticate, botmaster has control over all bots in the channel.
- Issues commands in channel, all bots react and respond as programmed.
Typical C&C Abilities

- Download and run additional payload, exploit new vulnerabilities
- Transfer files to/from infected host
- Spread infection to the local network, often bypassing firewall and IDS
- Perform massively coordinated portscans, often for reconnaissance for future attacks
- Perform distributed denial-of-service (DDoS) attacks
Typical C&C Abilities

- Open spam relay
- Open SOCKS proxy
- Log keystrokes
- Monitor HTTP traffic for cookies in order to steal web sessions
- Harvest bank account information, often PayPal
- Install spyware or other pop-up software
Motivations for Botting

- Entertainment
- Pride
- Revenge against another botnet
  - Botnet theft is not uncommon
- Jumpstart a worm outbreak
- Money
Motivations for Botting - $$

- Spam relay
- Corporate blackmail/extortion
- Rent-a-network
- PayPal
  - Drain an account
  - Used for exchanging money with others
  - ATM cards allow for spending
Motivations for Botting - $$$

- Spyware
  - Often paid on a per-installation basis, usually around $.15
  - Paid more as users view/click advertisements
  - Forced install on tens of thousands of machines
  - Can be used as a tracking mechanism
Detecting Infected Machines

- NIDS Signatures
  - IRC Joins
  - PIF/SCR downloads
  - Common bot commands (aim.goaway, .advscan)
  - Backdoor or shell commands
  - Make sure signatures are not restricted to common ports

- DNS logs
  - Queries for known bad host names or domains
Detecting Infected Machines

- Flow logs
  - Port scanning
  - Inbound IRC connections
  - Connections to known C&C IP addresses and port numbers
Researching an Infection

- **First goal** - Find the C&C DNS name
- Download the payload to a safe machine
  - `wget` or `curl` the file from the compromised website
- Submit the file to VirusTotal and Norman Antivirus Sandbox.
  - [www.virustotal.com](http://www.virustotal.com)
  - [sandbox.norman.no](http://sandbox.norman.no)
- **Run** `strings` **against the file**
  - Not useful if payload is encrypted/compressed
  - Can yield names of related files, compile-time information, etc.
This is a report processed by VirusTotal on 04/01/2005 at 16:53:21 (CET) after scanning the file "pz.x" file.

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Version</th>
<th>Update</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntiVir</td>
<td>6.30.0.7</td>
<td>04.01.2005</td>
<td>TR/Spy.KStaff</td>
</tr>
<tr>
<td>AVG</td>
<td>718</td>
<td>04.01.2005</td>
<td>LowZones.A</td>
</tr>
<tr>
<td>BitDefender</td>
<td>7.0</td>
<td>03.31.2005</td>
<td>HTML.MediaTickets.A</td>
</tr>
<tr>
<td>ClamAV</td>
<td>devel-20050307</td>
<td>04.01.2005</td>
<td>no virus found</td>
</tr>
<tr>
<td>DrWeb</td>
<td>4.32b</td>
<td>04.01.2005</td>
<td>Trojan.DownLoader.1843</td>
</tr>
<tr>
<td>eTrust-Iris</td>
<td>7.1.194.0</td>
<td>04.01.2005</td>
<td>Win32.Secdrop.BE! Trojan</td>
</tr>
<tr>
<td>eTrust-Vet</td>
<td>11.7.0.0</td>
<td>04.01.2005</td>
<td>Win32.Secdrop.BE</td>
</tr>
<tr>
<td>Fortinet</td>
<td>2.51</td>
<td>03.31.2005</td>
<td>no virus found</td>
</tr>
<tr>
<td>F-Prot</td>
<td>3.16a</td>
<td>03.31.2005</td>
<td>virus dropper</td>
</tr>
<tr>
<td>Ikarus</td>
<td>2.32</td>
<td>04.01.2005</td>
<td>no virus found</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>4.0.2.24</td>
<td>04.01.2005</td>
<td>Trojan-Clicker.JS.Linker.j</td>
</tr>
<tr>
<td>McAfee</td>
<td>4459</td>
<td>03.31.2005</td>
<td>Downloader-QG</td>
</tr>
<tr>
<td>NOD32v2</td>
<td>1.1042</td>
<td>03.31.2005</td>
<td>Win32/Advare.MediaTickets</td>
</tr>
<tr>
<td>Norman</td>
<td>5.70.10</td>
<td>03.31.2005</td>
<td>no virus found</td>
</tr>
<tr>
<td>Panda</td>
<td>8.02.00</td>
<td>03.31.2005</td>
<td>Adware/MediaTickets</td>
</tr>
<tr>
<td>Sybari</td>
<td>7.5.1314</td>
<td>04.01.2005</td>
<td>Trojan.WinREG.LowZones.a</td>
</tr>
<tr>
<td>Symantec</td>
<td>8.0</td>
<td>04.01.2005</td>
<td>Trojan.LowZones</td>
</tr>
</tbody>
</table>

VirusTotal is a free service offered by Hispacell Sistemas. There are no guarantees about the availability and continuity of this service. Although the detection rate afforded by the use of multiple antivirus engines is far superior to that offered by just one product, these results DO NOT guarantee the harmlessness of a file. Currently, there is not any solution that offers a 100% effectiveness rate for detecting viruses and malware.
Click on a samples "Date" to display its Sandbox analysis.

Report created: 01.04.2005 16:37:47

Automatic Sandbox analysis of W32/MEWpacked.gen
[ General information ]
* **Locates window "NULL [class mlRC]" on desktop.
* File length: 81254 bytes.

[ Changes to filesystem ]
* Creates file C:\WINDOWS\SYSTEM\xagwx.exe.
* Deletes file 1.

[ Changes to registry ]
* Creates value "Windows update"="xagwx.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
* Creates value "Windows update"="xagwx.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices".
* Creates key "HKCU\Software\Microsoft\OLE".
* Sets value "Windows update"="xagwx.exe" in key "HKCU\Software\Microsoft\OLE".

[ Network services ]
* Looks for an Internet connection.
* Connects to "bott.haxnet.se" on port 15000 (TCP).
* Connects to IRC Server.

[ Security issues ]
* Possible backdoor functionality [Authenticate] port 113.

[ Process/window information ]
* Creates a mutex biach.
* Will automatically restart after boot (I'll be back...).
Strings

=OleInitialize
SHGetMalloc
SetMenu
Rar!
&$t
x.bat
k.html
/1T>X
X2s)
staff.html
pck+
trofkz.REG
'}^+<
cQ{e`
$dSR&
Other Research Methods

- Run the payload in a monitored lab environment
  - Often, payload will often not function inside VMware/VirtualPC
- Blink an infected user’s network port and monitor DNS requests as the bot reconnects to the C&C
- Use a disassembler to examine binary
  - Requires lots of time and knowledge
Containing an Outbreak

- Quarantine the infected hosts
  - VLAN
  - Disable network jack
  - NetReg

- Block access to the payload.
  - Use ACLs to deny traffic to the payload host
  - Utilize Packeteer to redirect all web requests for the payload file name.

- Poison DNS resolution of payload server
  - Relies on internal DNS server
Containing via Packeteer

class new /Inbound UserEducation nодеfault inside
  host: any TCP
service: Client outside host: any service: HTTP
  "Web:url:/*bestfriends.scr"
class rule add /Inbound/UserEducation inside
  host: any TCP service: Client
outside host: any service: HTTP
  "Web:url:/*newpics.scr"
policy apply never /Inbound/UserEducation
policy admit /Inbound/UserEducation squeeze nontcp
policy admit /Inbound/UserEducation refuse nonweb
policy admit /Inbound/UserEducation refuse web

Questions to packeteer-edu@lists.stanford.edu
Containing via DNS Poisoning

DNS Config
zone "example.com." {
  type master;
  file "example.com.db";
  allow-update { none; ];
};

example.com.db
example.com. IN SOA ns1.YOUR.edu.
dns.example.com. (<dns options>);
example.com. IN NS ns1.YOUR.edu.
example.com. IN NS ns2.YOUR.edu. ;
*.example.com. IN A 127.0.0.1
Cleaning Infected Machines

- Hahaha
- Best practice – Format and reinstall
  - Guaranteed to clean infection
  - User education
  - Be sure the newly installed OS is protected
- Ensure user changes all passwords that were used from the machine
- Be aware that antivirus software can’t be trusted to certify a machine as “clean”
Cleaning. No, really.

- Use the results from the Norman AntiVirus Sandbox as a starting point
- Use RegMon, FileMon, RootKitRevealer and others from SysInternals
- Remember that the bot may have downloaded additional payload beyond the original
- When the PC is reconnected, monitor traffic for suspicious connections
Additional Research

- Add the newly found bot DNS name to your DNS watch list.
  - DNSWatch - aharp.ittns.northwestern.edu/software
- Watch flow logs for connections to the C&C IPs.
- Scan your network for any ports opened by the bot
  - These are reported from the Norman AntiVirus Sandbox
  - NMap – www.insecure.org
- Use www.awayhunter.com to find other websites hosting the payload
  - The data on the site is usually a couple of weeks old but can still be useful
AWAY MESSAGE SEARCH RESULTS:

2/20/2005 @ 6pm (Views: 3)  
WTF LOOK http://www.kimpearson.net/bestfriends.scr ?!?!?! ... read more
by: sydnashious

2/4/2005 @ 7pm (Views: 0)  
WTF LOOK http://www.valleyviewgolfcommunity.com/bestfriends.scr ?!?!?! ... read more
by: xx1cairo21xx

2/2/2005 @ 8pm (Views: 0)  
WTF LOOK http://www.hodginsauctioneers.com/bestfriends.scr !??!!!?! ... read more
by: macgillivray11

2/2/2005 @ 6am (Views: 0)  
WTF LOOK http://www.hodginsauctioneers.com/bestfriends.scr !??!!!?! ... read more
by: enjoimenow

1/25/2005 @ 7pm (Views: 0)  
OMG LOOK http://www.emalia.net/bestfriends.scr ?!!!??! ... read more
by: medda407

1/22/2005 @ 3pm (Views: 1)  
OMG LOOK http://www.hyperion-wines.co.nz/bestfriends.scr ?!!!??! ... read more
by: oxdarkblissxo
Additional Research

- Attempt a zone transfer for the domain containing the command and control record.
  - `dig @SOA -t AXFR domain.name`
  - Often blocked, but can yield several additional DNS records being used for command and control
Zone Transfer

; <<<>> DiG 2.1 <<<>> @dns.exandedns.com example.com. axfr; (1 server found)

... 

example.com. 3600 NS dns1.exandedns.com
example.com. 3600 NS dns2.exandedns.com

aolx.example.com. 3600 A 192.168.0.2
bckup.example.com. 3600 A 192.168.0.3
bckup3.example.com. 3600 A 192.168.0.4
rofkgj.example.com. 3600 A 192.168.0.5
roxz.example.com. 3600 A 192.168.0.6
surf.example.com. 3600 A 192.168.0.7

example.com. 3600 SOA dns.exandedns.com ( ... ); minimum (1 hour)
Removing the Payload

- Use **whois** to get contact info for the site hosting the payload
- Check the website for contact info
- Be polite and include log files in email
- Many larger sites have dedicated abuse departments and e-mail addresses
- Be ready to explain why the file being hosted is bad. Remind them that A/V software will likely not detect it
Removing the Payload

- Check to see if the file returns
  - The entire server could be compromised
- The bot master will have more compromised sites ready to host the file. Be ready for it to move.
Shutting Down C&C

- Use `whois` to get contact information for remote IP address
- Explain that they are running an IRC server that is coordinating a bot network
Removing the DNS Records

- Takes time, but can disable an entire botnet.
- Contact the company hosting the DNS records. This information can be found using `dig` and `whois`.
- They are typically more apprehensive than web hosts. Have logs ready.
- Some botnets use two DNS providers. Work with both providers simultaneously.
- Coordinate with others.
Coordinating With Others

- University Security Operations Group
  - www.dshield.org/mailman/listinfo/unisog
- Internet Storm Center
  - isc.sans.org
- Research and Education Network ISAC
  - www.ren-isac.net
- Incidents Mailing List
  - www.securityfocus.com/archives
- Windows-HiEd
  - www.windows-hied.org
Working with Law Enforcement

- Get permission from university
- Save *all* log files
- Fully document your investigation
  - If you call another company (hosting, DNS, etc), record time, phone number, and contact person
- Be ready to estimate damages
  - Include lost bandwidth, cleaning costs, hours spent in research, lost productivity. $5000 seems to be the magic number for federal prosecution.
- Coordinate with your campus police
  - They usually will give you a contact in the FBI
Impending Doom

- Encrypted C&C communication
  - Waste
  - Challenging for IDS
- Payload deployment over P2P
  - Hard to block
Caveats

- Get permission before logging
  - DNS queries
  - IRC traffic
  - Flow records

- Connecting to a C&C and impersonating a bot is a sure fire way to get DDoSed.

- Trying to hijack a bot network and issue an uninstall command seems like a good idea at first, but could cause damage, and is likely illegal.
Credits/References

- John Kristoff – *Botnets*
  - www.nanog.org/mtg-0410/kristoff.html
- HoneyNet Project – *Know Your Enemy*
  - www.honeynet.org/papers/bots
- Penny Jones – *Battle of the Bots*
  - asia.cnet.com/enterprise/infrastructure
Q&A

Norman Elton
norm@wm.edu

Matt Keel
matt@wm.edu

Presentation will be available on www.educause.edu