

Asia Pacific Network Information Centre
APNIC

APRICOT/APNIC 27

**APNIC Training
Team Cymru**

Introduction to Botnets and Forensics

Manila, Philippines

24 February, 2009


Asia Pacific Network Information Centre
APNIC

Presenter:
Cecil Goldstein,
APNIC Training Manager
cecil@apnic.net

Material developed and kindly
made available by Team Cymru

Ryan Connolly
ryan@cymru.com

Marcel van den Berg
marcel@cymru.com



Team Cymru

BOTNET BASICS

Introduction to Evolved Malware

3

Botnets 101
Agenda

Agenda

- Introduction
- What is a Botnet?
- What are Botnets used for?
- How are Botnets created?
- How are Botnets controlled?
- Can Botnets be stopped?

Team Cymru, ©2008

Botnets 101
Introduction

Introduction

- Purpose of this presentation
 - Provide an introduction to the world of Botnets
 - Explore their capabilities
 - Illustrate their increasing sophistication
 - Describe current countermeasures
- Foundational in content
 - Assumes a basic understanding of malware
 - But no prior knowledge of Botnets themselves

Team Cymru, ©2008

What's a Botnet?

Team Cymru, ©2008

Botnets 101
What is a Botnet?

Terminology

- Bot
- Botnet
- Drone
- Bot Herder (controller)
- Command & Control

Team Cymru, ©2008

7

Botnets 101
What is a Botnet?

What is a Bot?

- To understand Botnets, lets first look at “bots”
 - Shorthand for “software robots”
 - A piece of automated (robotic like) software that runs silently on the host and waits for commands from its control infrastructure
 - Allows a 3rd party to direct the affected machine (drone) to execute malicious tasks
 - Can act singularly or in concert with hundreds (or thousands) of other peer bots in a “grid computing” like fashion

Team Cymru, ©2008

8

Botnets 101
What is a Botnet?

What is a Botnet?

- A controlled collection of “drones”
 - All running semi-homogeneous bot software
 - Centrally controlled by a third party
 - Machine’s true owner is typically unaware
- Intent: leverage collective resources
 - Sum of the whole is greater than the parts ...
 - Hundreds, thousands, or even millions of machines acting with single purpose can rival the computing power of some of the worlds fastest supercomputers!

Team Cymru, ©2008

9

Botnets 101
What is a Botnet?

Are Botnets a threat?

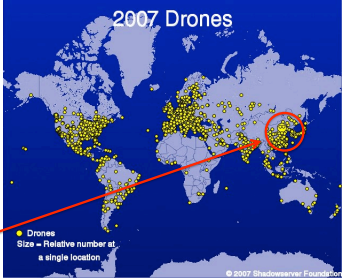
- Considered to be the primary security threat on the Internet today
 - “Botnets: The New Threat Landscape” (Cisco, 2007)
- Because of their growing size
 - Botnet computing power is bought/sold/traded like a commodity
 - Often used for large scale Internet attacks
 - Use is increasingly focused on financial gain (fraud) not just digital vandalism (spam, denial of service)
- Botnets are highly dynamic
 - Making them hard to detect, locate, and shut down
 - They adapt quickly to new detection controls

Team Cymru, ©2008 10

Botnets 101
What is a Botnet?

Where are these Botnets?

- Largest percentage in western countries and Asia
- Growing into South America and India
- Highest concentration in China



Team Cymru, ©2008 11

“What are Botnets used for?”

Team Cymru, ©2008 12

Botnets 101
What are Botnets used for?

Motivations of Botnet creators

- In the past ...
 - Curiosity, wondering what was possible
 - Underground research or non-malicious “hacking”
 - Resource sharing between peers (grid computing)
 - Exploring alternative methods of Internet communication
- More recently ...
 - Increased capacity to execute digital vandalism
 - Information gathering for financial fraud and monetary gain

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Motivations of Botnet creators

- In the past ...
 - Curiosity, wondering what was possible
 - Underground research or non-malicious “hacking”
 - Resource sharing between peers (grid computing)
 - Exploring alternative methods of Internet communication
- As of late ...
 - **Increased capacity** to execute digital vandalism
 - **Information gathering** for financial fraud and monetary gain

We'll explore these two in greater detail

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Motivation: increasing capacity

- Attackers want “capacity” ... defined as
 - **Bandwidth** or Internet throughput
 - **Resources** such as hard drive space, processing power, and other machine capabilities
- The goal
 - To infect as many systems as possible with bots
 - Thus, increasing the collective size of the Botnet
 - Thus, increasing the power associated with control of such resources

Team Cymru, ©2008

Botnets 101
What are Botnets used for?


Motivation: information gathering

- Attackers also want “information” ... defined as
 - Usernames & passwords (for the local machine)
 - Usernames & passwords (for websites, etc)
 - E-mail contents & contacts
 - Financial information & trade secrets
 - Network traffic on your subnet, etc ...
- The goal
 - Extract **your** personal information
 - Which they can use, trade, or sell
 - Which can be input for more complex attacks
 - Which can be used for extortion or other crimes
 - Thereby, increasing **their** financial gain

Team Cymru, ©2008 16

Botnets 101
What are Botnets used for?

Botnet capabilities

- Botnets are flexible and have many uses
- Some of the most popular
 - Distributed Denial of Service (DDoS) attacks
 - System exploitation
 - Hosting services
 - Internet click fraud
 - Proxies
 - Spyware
- We will examine each of these individually 

Team Cymru, ©2008 17

Botnets 101
What are Botnets used for?

DDoS


- Network-based digital vandalism attack
- The goal
 - Overwhelm the target with network packets to slow or stop its ability to process legitimate requests
 - Leverage thousands (millions?) of drones for maximum impact
- Often a specific website is the target, however, upstream routers and switches fail as well

Team Cymru, ©2008 18

Botnets 101
What are Botnets used for?

DDoS attacks

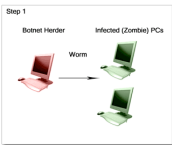
- Ping / UDP floods
 - Large volume of ICMP ECHO or UDP packets sent to a single host or limited set of destinations
 - Bandwidth is consumed, service slows or stops responding to legitimate requests
- TCP flood
 - Large volume of half-open TCP handshake requests
 - “State table” maintained in memory of the responding device is crammed full of bogus TCP sessions
 - Resource eventually crashes or slows to a crawl

 Team Cymru, ©2008 19

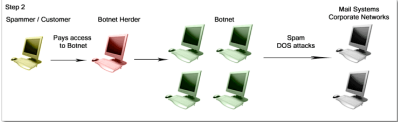
Botnets 101
What are Botnets used for?


DDoS attacks

Step 1



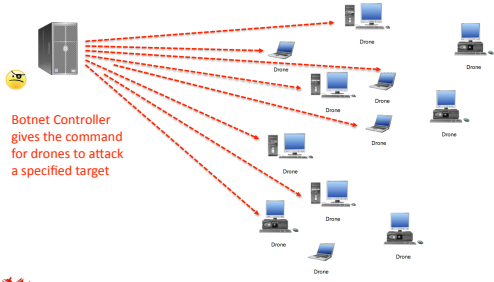
Step 2




 Team Cymru, ©2008 20

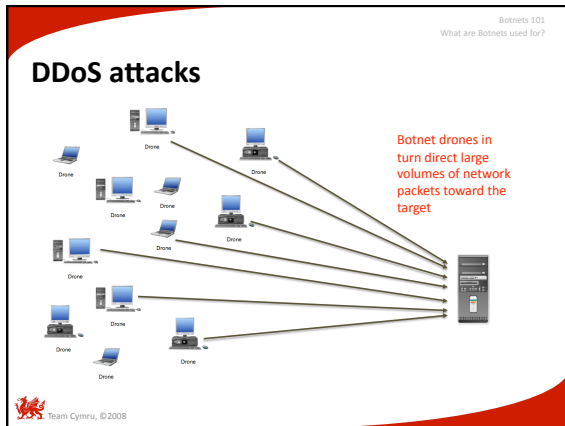
Botnets 101
What are Botnets used for?

DDoS attacks



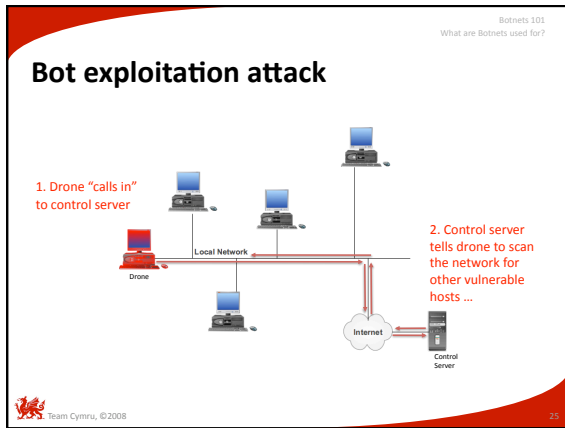
Botnet Controller gives the command for drones to attack a specified target

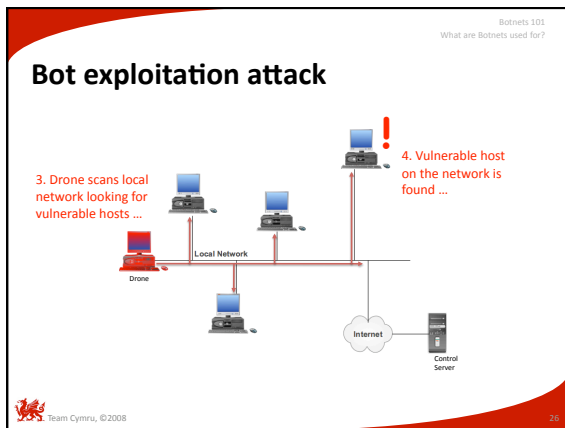
 Team Cymru, ©2008 21

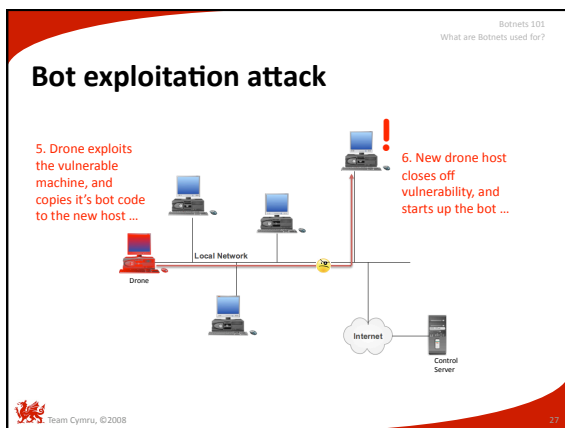


- Botnets 101
What are Botnets used for?
- ### DDoS extortion
- Attackers threaten DDoS if demands are not met
 - Starts with a sample demonstration attack
 - Followed by a statement of demands (usually \$)
 - If paid, attackers go away
 - If not, resources are brought down
 - Slippery slope
 - Once you pay, chances are high that attackers will return with further demands ...
- Team Cymru, ©2008
- The slide features a red header and footer with the text 'Botnets 101 What are Botnets used for?' and 'Team Cymru, ©2008'. The main content is a bulleted list describing DDoS extortion, including a sample demonstration attack, demands for payment, and the slippery slope of further demands.

- Botnets 101
What are Botnets used for?
- ### Exploitation
- Bots include the ability to "hack" other machines
 - Scan the network with built in sniffing tools
 - Look for open TCP ports / vulnerable services
 - Exploit unsecured or un-patched machines
 - Replicate the bot code to the new machines
 - Modular design
 - Bots are created to be modular and flexible
 - Built in "hacking tools" are updated by the controller when new ones become available
- Team Cymru, ©2008
- The slide features a red header and footer with the text 'Botnets 101 What are Botnets used for?' and 'Team Cymru, ©2008'. The main content is a bulleted list describing bot exploitation and modular design, including scanning for vulnerabilities and updating tools.







Botnets 101
What are Botnets used for?

Bot exploitation attack

7. New drone calls in to the control server to announce its existence ...

8. Control server adds the new bot to the Botnet.

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Hosting services

- Bots are capable of turning their drone host into:
 - HTTP web servers
 - To host phishing sites
 - To host web pages infected with bot code
 - FTP file servers
 - To host pirated software or music
 - To store malware for others to use
 - IRC chat servers
 - So that Botnet owners can communicate
 - For command & control of Botnets themselves

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Hosting services

- SMTP mail servers
 - For distributing spam
- As of January 2008
 - 80% of all spam originated from Botnets
 - 8% of all spam originated from the **Storm Botnet**
 - Based on the Storm worm created in 2007
 - Estimated to have over 1 million drones
 - http://en.wikipedia.org/wiki/Storm_botnet

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Botnet spam lifecycle*

1. Spammer sends request (and money) to Botnet controller
2. Botnet controller generates spam details
3. Spam commands is sent to the Botnet
4. Drones awaken and execute given command to spam
5. Spam forwarded to other high-throughput SMTP servers
6. Spam is sent to e-mail inboxes
7. Users open spam, click on links, and compromised information is sent back to originator

*From Wikipedia

Team Cymru, ©2008 31

Botnets 101
What are Botnets used for?

Click fraud

- Online advertisers pay affiliates for generating clicks on their Internet ads
 - Known as Pay Per Click advertising (PPC)
 - Google's AdWords/AdSense & Yahoo! Search Marketing
 - When a click occurs, a small amount of money is deposited into the affiliate's bank account
- But, what if ...
 - Ad clicking could be simulated
 - Ad clicking could be manipulated by a collection of thousands of machines
- Botnets are an ideal medium

Team Cymru, ©2008 32

Botnets 101
What are Botnets used for?

Click fraud

- Illegal
 - Felony offense in the US, UK, and other countries
- Example: Clickbot.A
 - Bot code designed for click fraud
 - Appears as an Internet Explorer plugin
 - Discovered by SANS in 2006
 - 100,000+ machines infected today

Team Cymru, ©2008 33

Botnets 101
What are Botnets used for?

Click fraud

THI

Robot is set up to click for Advertiser

Advertiser pays Google for clicks. Google shares that revenue with the page site that generated clicks.

Team Cymru, ©2008

34

Botnets 101
What are Botnets used for?

Proxy servers

- Network traffic can be “bounced” or proxied through intermediary hosts
 - Has both legitimate and illegitimate uses
- In the case of Botnets
 - Redirecting network traffic through drones avoids detection and attribution
 - Routing IP-based services through several drones in several countries makes tracing nearly impossible

Team Cymru, ©2008

35

Botnets 101
What are Botnets used for?

Proxy server types

- HTTP / HTTPS
 - Redirects web traffic to hide origin IP address
- SOCKS
 - Redirects other TCP & UDP based services
 - E.g. IMAP, POP3, instant messaging, SMTP for spam
- IRC
 - Hides source IP when joining IRC chat rooms
 - Often used to hide Botnet command & control traffic
- Generic traffic redirection
 - Anonymizing other services
 - Very popular and developed use of Botnets

Team Cymru, ©2008

36

Botnets 101
What are Botnets used for?

Proxy server types

Free software exists which leverages numerous "proxy hosts" across the Internet. Many of these have been compromised by Botnets

Proxy IP	Port	Proxy Name	Ext.	Last Check	Response
206.171.134.229	80	cache1.era01.sco.net	NET	03/07/0...	00:03:120
207.136.80...	80	proxyhard.idirect.com	COM	03/07/0...	00:01:101
207.34.202.2	3128	cache1.cc.intellog.com	COM	03/07/0...	00:02:530
208.20.42.6	80	cache1.toronto.intellog.com	COM	03/07/0...	00:02:470
209.20.42.6	3128	cache1.toronto.intellog.com	COM	03/07/0...	00:01:850
209.103.145.3	80	fastnet142003.voyager.net	NET	03/07/0...	00:01:850
216.56.42.3	80	www.casabland12.vie.us	US	03/07/0...	00:03:100
209.228.51.9	80	rfcache1.int.net	NET	03/02/0...	00:01:870
208.133.208.1	80	208.133.208.1		03/02/0...	00:01:270
204.26.177.33	80	204.26.177.33		03/02/0...	00:01:260
202.226.51.9	8080	HL_Cache1.int.net	NET	03/02/0...	00:00:000
212.206.65.3	8080	www.quatenet.fr	FR	02/03/0...	00:00:000

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Spyware

- Bots can spy on your computer activity through the use of
 - Keystroke loggers
 - Network packet captures
 - Screen shot captures
 - Host pilfering & data theft
- Typically, data is extracted & uploaded offsite
 - Data upload sites are called "drops"

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Spyware

- Keystroke loggers can capture
 - Credit card information
 - Passwords
 - E-mail, IM, and other communications
 - Personal data (identity theft)
- Network packet sniffers
 - Trigger logging based on keywords
 - E.g. "paypal.com" or "yourbank.com"
 - Also used to see if competing Botnets are within proximity

Team Cymru, ©2008

Botnets 101
What are Botnets used for?

Spyware

- Screen shot captures
 - Works like a keystroke logger
 - Grabs a picture of the entire screen
 - Have been known to enable webcams & microphones too!
- Host pilfering & data theft
 - Search the Windows registry for valuable data
 - Search Windows Protected Storage for credentials
 - Grab IM contacts
 - Grab E-mail contacts (for spam lists)
 - Grab documents with known file extensions (e.g. doc, xls, txt)

Team Cymru, ©2008 40

Botnets 101
What are Botnets used for?

Spyware

• New Spyware created

• Spyware inserted into a pop-up ad

• Spyware reports browsing habits back to the marketing company

• Spyware tracks internet browsing habits

• Spyware is downloaded to computer

• Person clicks on the pop-up ad

Click on the money to win money!

... could also be other information of value

Team Cymru, ©2008 41

“How are Botnets created?”

Team Cymru, ©2008 42

Botnets 101
How are Botnets created?

Build a Botnet

- Used to be an elite skill
 - Creating a decent bot was hard enough
 - Creating a full-functioning, resilient, and effective Botnet was a serious undertaking
- More recently, it's become "point and click"
 - Software / tools have matured
 - Wealth of information available for newcomers
 - Some IRC chat channels even offer training
- Botnet community willing to share
 - Exploitation frameworks
 - Tools, techniques, and traps

Team Cymru, ©2008

Botnets 101
How are Botnets created?

Build a Botnet

- Finding vulnerable hosts is easier than in the past
- Internet-wide IP netblocks have been documented
 - Which netblocks are unallocated
 - Which netblocks have vulnerable systems
 - Which netblocks are heavily monitored
 - Which netblocks are allocated to what organization
- Educational address space is targeted
 - Poor security, large amount of storage, fast connections
- Military & government targeted for different reasons
 - Bragging rights, access to sensitive information

Team Cymru, ©2008

Botnets 101
How are Botnets created?

Build a Botnet

- Attacking hosts is also becoming easier
 - Vulnerability exploitation is a maturing process
 - Social engineering is highly successful
 - Phishing & e-mail attacks still work in 2008
 - Instant messaging attacks are on the rise

Team Cymru, ©2008

Botnets 101
How are Botnets created?

Buy a Botnet

- Underground cyber-crime commodity
- Can be bought or sold
 - Custom Botnets can be created for the right price
- Can be traded
 - For physical goods such as jewelry or computer gear
 - For Batches of credit card information
 - For Shell accounts on remote servers
 - For other Botnets!

Team Cymru, ©2008 46

Botnets 101
How are Botnets created?

Steal a Botnet

- If you don't want to build/buy it, steal it
 - Referred to as "hijacking" or "jacking"
 - Essentially, talking over drones of another Botnet
- Bots assimilate each other
 - Sniff network traffic for command & control conversations between drones and their server
 - Usually unencrypted, but not always
 - Data in the network traffic provides most of what is needed to "convert" a drone to your Botnet
 - Bots can be automated to do this, requiring little effort!

Team Cymru, ©2008 47

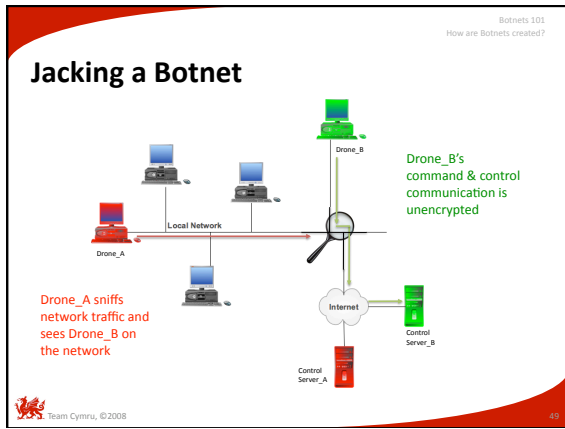
Botnets 101
How are Botnets created?

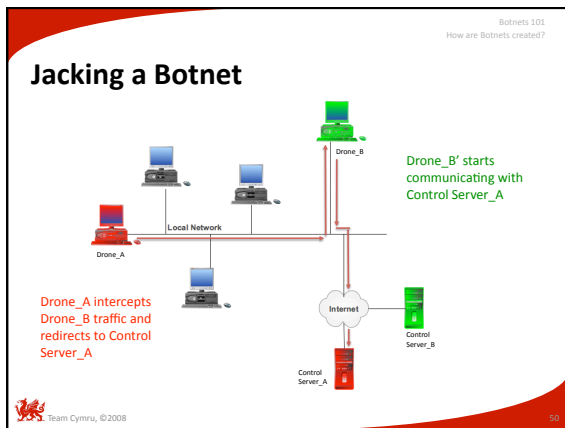
Jacking a Botnet

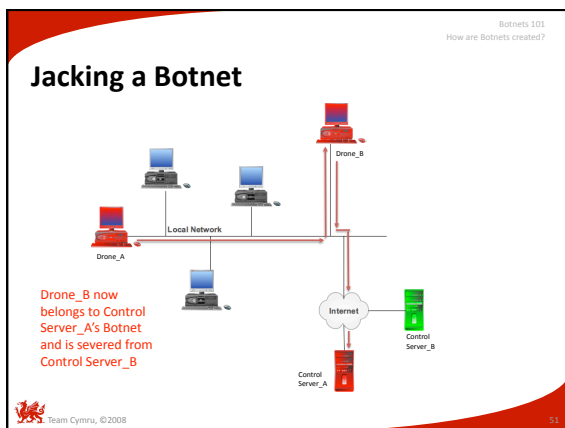
Drone_A is connected to Control Server_A

Drone_B is connected to Control Server_B

Team Cymru, ©2008 48







Botnets 101
How are Botnets created?

In sum, three scenarios

- “I have technical skills, and no money”
 - Learn to build your own Botnet
- “I have money, and no technical skills”
 - You can buy or trade for a Botnet
- “I have neither”
 - You can steal a Botnet

Team Cymru, ©2008

“How are Botnets controlled?”

Team Cymru, ©2008

Botnets 101
How are Botnets controlled?

Command & control

- Managing a Botnet can be complicated
 - Geographically dispersed drones
 - Must negotiate firewalls, switches, intrusion detection, and numerous other network controls
 - Need a seemingly benign way to “give orders” and receive results
 - Botnet controller (herder) needs to maintain anonymity
- Certain network protocols are ideally suited
 - Old standbys: IRC, HTTP
 - Up and coming: P2P, DNS

Team Cymru, ©2008

Botnets 101
How are Botnets controlled?

Command & control

- Managing a Botnet can be complicated
 - Geographically dispersed drones
 - Must negotiate firewalls, switches, intrusion detection, and numerous other network controls
 - Need a seemingly benign way to “give orders” and receive results
 - Botnet controller (herder) needs to maintain anonymity
- Certain network protocols are ideally suited
 - Old standbys: IRC, HTTP
 - Up and coming: P2P, DNS

← We'll explore these in greater detail

Team Cymru, ©2008 55

Botnets 101
How are Botnets controlled?

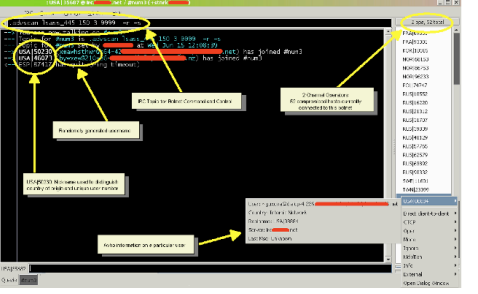
IRC command & control

- Oldest, most common
- Uses public IRC servers
 - But, private IRC servers are also prevalent
- Typical scenario
 - Drones are connected to the controller as IRC chat participants waiting for commands
 - Controller issues commands by inserting specially formatted text into the conversation
 - Drones see the command, and execute instructions on their local host
 - Results are returned to the chat session

Team Cymru, ©2008 56

Botnets 101
How are Botnets controlled?

IRC command & control



Team Cymru, ©2008 57

Botnets 101
How are Botnets controlled?

HTTP command & control

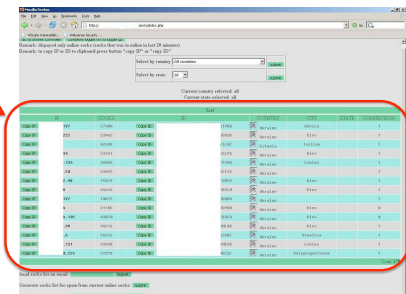
- Looks even more benign
 - Blends in with other web traffic noise on the Internet
- Typical scenario
 - Drones use HTTP to connect to a remote web server
 - A PHP script is accessed on the web server, including self identifying information (I am here)
 - Controller views and tracks the Botnet via a web interface
 - Commands are embedded in a webpage which is queried by the drones on a set time interval
 - Results are returned by accessing the PHP scripts and including results information

Team Cymru, ©2008 58

Botnets 101
How are Botnets controlled?

HTTP command & control

List of active bots and their locations, etc

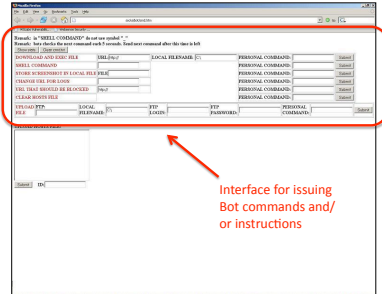


IP	OS	CPU	MEM	...
192.168.1.1	Windows	100%	100%	...
192.168.1.2	Windows	100%	100%	...
192.168.1.3	Windows	100%	100%	...
192.168.1.4	Windows	100%	100%	...
192.168.1.5	Windows	100%	100%	...
192.168.1.6	Windows	100%	100%	...
192.168.1.7	Windows	100%	100%	...
192.168.1.8	Windows	100%	100%	...
192.168.1.9	Windows	100%	100%	...
192.168.1.10	Windows	100%	100%	...

Team Cymru, ©2008 59

Botnets 101
How are Botnets controlled?

HTTP command & control



Interface for issuing Bot commands and/or instructions

Team Cymru, ©2008 60

Botnets 101
How are Botnets controlled?

DNS command & control

- Somewhat newer than IRC or HTTP
- Nearly invisible to observers
 - Looks like generic DNS resolution traffic
 - DNS (TCP/UDP 53) allowed in and out of nearly all networks
- Typical scenario
 - Drones uses DNS to attempt to resolve a domain name
 - The hostname being resolved is crafted with special information
 - E.g. bot-3987645-us.netmanager.somedomain.com
 - Controller tracks the bots via DNS queries
 - Commands are embedded in the DNS resolution responses
 - Results are returned by resolving additional DNS queries and passing along specially crafted hostnames

Team Cymru, ©2008 61

Botnets 101
How are Botnets controlled?

P2P command & control

- Growing in popularity
- Being heavily researched by universities in the US
- Relies on a web of peer controllers vs. a single server
 - If the controller is shutdown, the Botnet survives


Team Cymru, ©2008 62

“Can Botnets be stopped?”

Team Cymru, ©2008 63

Botnets 101
Can Botnets be Stopped?

Stopping Botnets

- Very difficult to outright stop a Botnet
 - Designed to be resilient to discovery & termination
 - Modular, flexible, and constantly changing
 - Network connections cross international borders
- Better question: can we **understand** Botnets?
 - Before they can be stopped, they have to be understood
 - Once understood, we can build defenses (offenses?)
 - Time, patience, and diligence are required
 - Fortunately, the tools are getting better ... 

Team Cymru, ©2008 64

Botnets 101
Can Botnets be Stopped?

Understanding Botnets

- Observation as a tool
 - Often called “runtime analysis”
 - Let the bot run in an isolated environment (sandbox)
 - Observe bot behavior and actions
 - Watch attempts to connect to controller
 - View traffic & look for IP address or domain name of the control server, IRC channel, website, et al
- Common tools for research
 - Honeypots

Team Cymru, ©2008 65

Botnets 101
Can Botnets be Stopped?

Understanding Botnets

- Decomposition as a tool
 - Often called “reverse engineering”
 - Time consuming but more thorough
 - Requires advanced programming language knowledge
 - Reveals similar information, but also hidden functions, passwords, & and other details not immediately apparent with observation
- Common tools for research
 - Sandboxes, disassemblers, debuggers

Team Cymru, ©2008 66

Botnets 101
Can Botnets be Stopped?

How do we proceed?

- First, we need to capture a bot
 - Using a honeypot
- Second, we need to analyze it
 - Using a sandbox

Team Cymru, ©2008 67

Botnets 101
Can Botnets be Stopped?


Bot capture with honeypots

- We need to create a monitored and controlled environment that looks enticing
- For this we can use a **“honeypot”**
 - A computer that appears to be part of a network but which is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource that would be of value to attackers
- One honeypot ideally suited for Botnet analysis
 - Nepenthes

Team Cymru, ©2008 68

Botnets 101
Can Botnets be Stopped?

Nepenthes



- Originated in 2005
- Runs on Linux/UNIX variants
 - Can be run in VMware on Windows if desired
- Free, open-source, honeypot technology designed to intercept and capture malware
- Ideally designed for Botnet and bot analysis
- Offers passive analysis by emulating known Windows vulnerabilities and downloads malware trying to exploit these vulnerabilities
- Can be obtained from Sourceforge at: <http://nepenthes.mwcollect.org>

Team Cymru, ©2008 69

Botnets 101
Can Botnets be Stopped?

How Nepenthes works

Some rudimentary setup is initially required.
Once configured, listening services can be viewed

```
#lsaf -l
nepenthes 25917  nepenthes 6u IPv4 162588  TCP *:smtp (LISTEN)
nepenthes 25917  nepenthes 7u IPv4 162589  TCP *:pop3 (LISTEN)
nepenthes 25917  nepenthes 8u IPv4 162590  TCP *:imap2 (LISTEN)
nepenthes 25917  nepenthes 9u IPv4 162591  TCP *:imap3 (LISTEN)
nepenthes 25917  nepenthes 10u IPv4 162592  TCP *:smtpp (LISTEN)
...
```

70

Botnets 101
Can Botnets be Stopped?

How Nepenthes works

As malware (bots) attempt to compromise the honeypot, their actions are tracked

```
[ Network services ]
* Looks for an Internet connection.
* Connects to xxx.example.net on port 7654 (TCP).
* Sends data stream (24 bytes) to remote address xxx.example.net, port 6667.
* Connects to IRC Server.
* IRC: Uses nickname Bot-UQ-298746yt.
* IRC: Uses username Borria45.
* IRC: Joins channel #8kyn3t_world with password D0wntlm3.
* IRC: Sets the usermode for user Borria45 to ...
```

71

Botnets 101
Can Botnets be Stopped?

How Nepenthes works

Individual binaries are tracked and hashed along with their point of origination

```
# ls /var/lib/nepenthes/binaries/
01a7b93e758ac9bb04c24c739b090db0 54776589d56462d5d4d789038b4c4db
99b5a36286e33b8b4011785d038576db 055690bcb9135a2086290130ae8627dc
54b27c050763667c2b476a1312bb49ea ...

# tail -1 /var/log/nepenthes/logged_submissions
[2006-07-05T20:37:52]
ftp://ftp.password0k.portal.info:21/host.exe eb6f41b9b17158fa1b765a5cb3f36a0
ftp://account1.bellonite.com:21/W32code.exe 54b27c050763667c2b476a1312bb49ea
...
```

72

Botnets 101
Can Botnets be Stopped?

Bot analysis with sandboxes


- We have captured several bots and chunks of binary code ... what now?
- Analysis can be done with a “sandbox”
 - Virtual environment where programs may execute in safe surroundings without interfering with the real processes, program files and network environment.
- We will examine two sandbox tools
 - Norman SandBox
 - CWSandbox

Team Cymru, ©2008 73

Botnets 101
Can Botnets be Stopped?

Norman SandBox

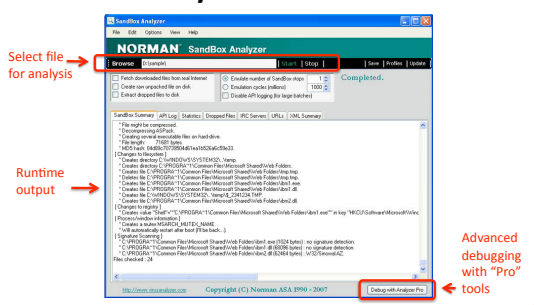
- Built by Norman ASA
 - Headquartered in Norway
- Experts in malware analysis & sandbox technology
- Features a line of products that can be used online, or locally (Windows-based tools)
- Focused on observation analysis, but “Pro” versions of the tool will also do advanced decomposition
- Offers detailed output showing exactly what bot does when executed, and evaluates malicious activity
- Commercially available at <http://www.norman.com/microsites/nsic/en-us>



Team Cymru, ©2008 74

Botnets 101
Can Botnets be Stopped?

SandBox Analyzer screenshot



Team Cymru, ©2008 75

Botnets 101
Can Botnets be Stopped?

Norman SandBox output logfile

```

D:\VRUS\MYTEST_EX_... \WS2\Backdoor
----- Sandbox output -----
[ General Information ]
**IMPORTANT PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.ND.
REMEMBER TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)!*.
* Display message box (kernel): sample, to smol.
* Display message box (kernel): KERNL32, to smol.
* File length: 58368 bytes.
* MD5 hash: 664862411748364e4ab3729bc53b.

[ Changes for registry ]
* Deletes file C:\WINDOWS\SYSTEM32\smrn12.asa
* Creates file C:\WINDOWS\SYSTEM32\smrn12.asa

[ Changes for registry ]
* Creates key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce".
* Sets value "smrn12"="C:\WINDOWS\SYSTEM32\smrn12.asa /v:" to key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce".

[ Changes to system settings ]
* Creates WindowsHook monitoring keyboard activity

[ Connections ]
* Connects to "100.222.8.130" on port 6667 (IRC).
* Connects to IRC server.
* IRC: Uses nickname CurrentUser(PFRK219).
* IRC: Uses username SEVERIND.
* IRC: Joins channel #54R4K_00T.

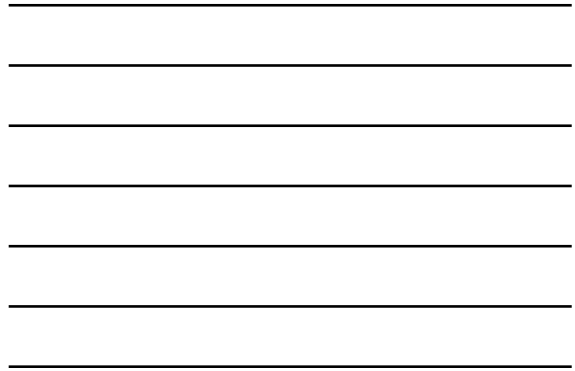
[ Processes and services ]
* Creates a mutex Z2M0909Y.
* Creates a mutex S\VFIC.
  
```

Bot modifies system files

Bot injects keyboard sniffer

Bot joins IRC channel

Team Cymru, ©2008 76



Botnets 101
Can Botnets be Stopped?

CWSandbox

- Built by SunBelt Software USA
 - Headquartered in Tampa Bay, Florida
- Leading provider of security software
- Features a FREE online malware analysis tool in their developer & research portal
- Can be directly fed from Nepenthes honeypot
- Offers autonomous analysis of large volumes of malware samples in a short period of time
- Submit malware directly at:

<http://research.sunbelt-software.com/Submit.aspx>

Team Cymru, ©2008 77



Botnets 101
Can Botnets be Stopped?

CWSandbox screenshot

Submit file, and return e-mail address (for results)

Team Cymru, ©2008 78



Botnets 101
Can Botnets be Stopped?

Code attribution

- Sometimes a software package's source code will indicate its author
- Usually difficult with bots
 - Modified regularly
 - Easy to forge information
 - Some are co-developed between geographically dispersed individuals

Team Cymru, ©2008 79

Asia Pacific Network Information Centre

Thank You Questions?

ryan@cymru.com
marcel@cymru.com
cecil@apnic.net

Manila, Philippines
24 February, 2009