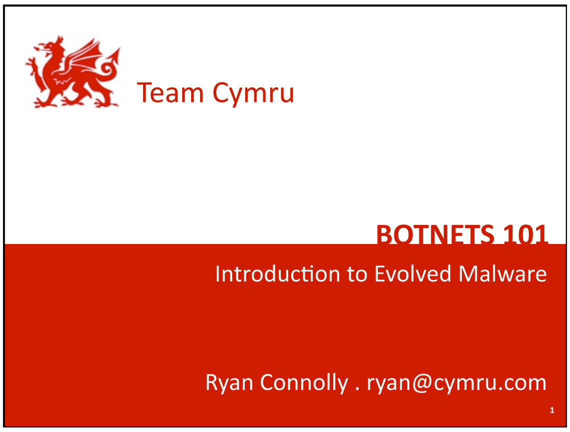


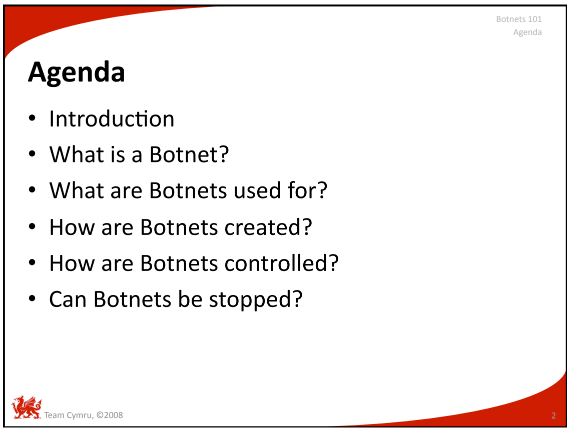
Team Cymru

BOTNETS 101

Introduction to Evolved Malware

Ryan Connolly . ryan@cymru.com

1



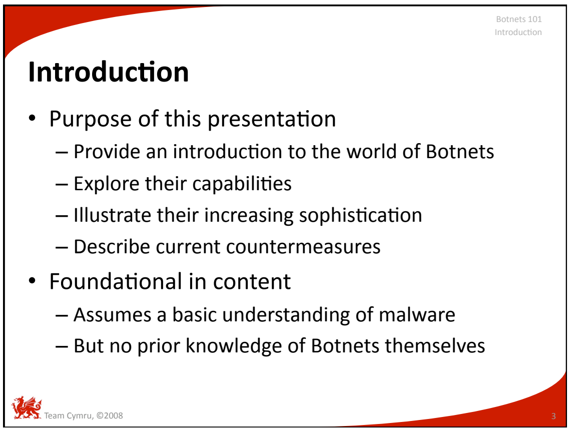
Botnets 101
Agenda

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

2



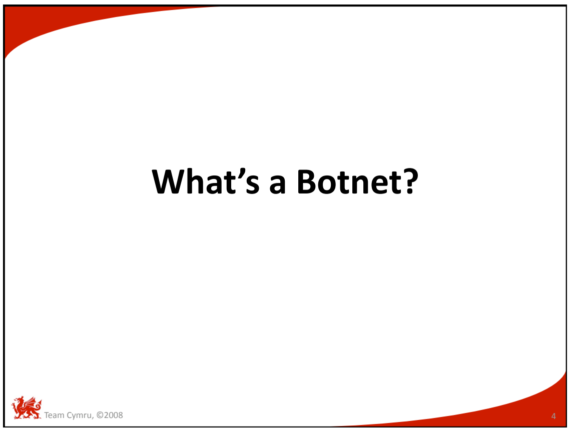
Botnets 101
Introduction

Introduction

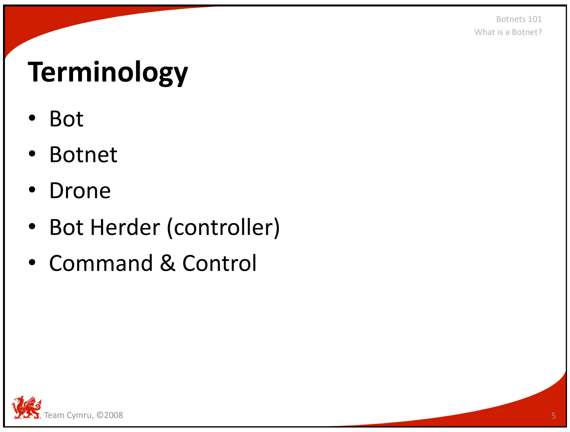
- Purpose of this presentation
  - Provide an introduction to the world of Botnets
  - Explore their capabilities
  - Illustrate their increasing sophistication
  - Describe current countermeasures
- Foundational in content
  - Assumes a basic understanding of malware
  - But no prior knowledge of Botnets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

Team Cymru, ©2008

3

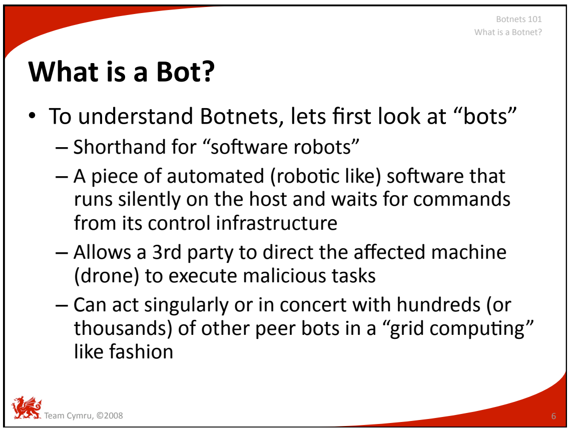


What’s a Botnet?



Terminology

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



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

What is a Botnet?

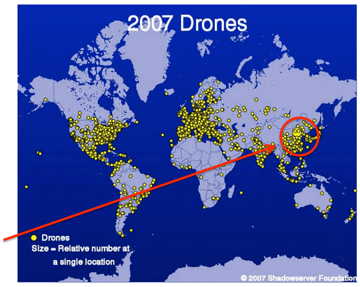
- A controlled collection of "drones"
  - All running semi-homogeneous bot software
  - Centrally controlled by a third party
  - Machine's true owner is typically unaware
- Intent: leverage collective resources
  - Sum of the whole is greater than the parts …
  - Hundreds, thousands, or even millions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

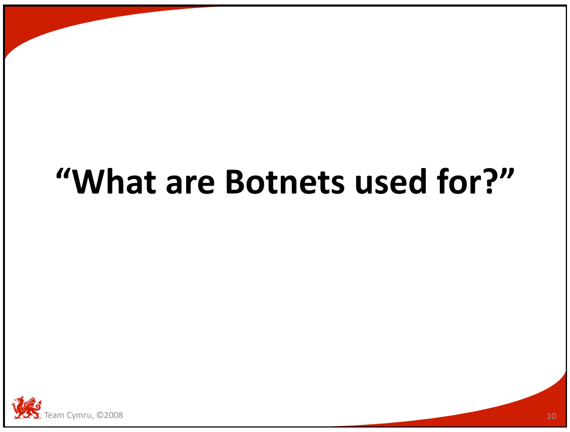
Are Botnets a threat?

- 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

Where are these Botnets?

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

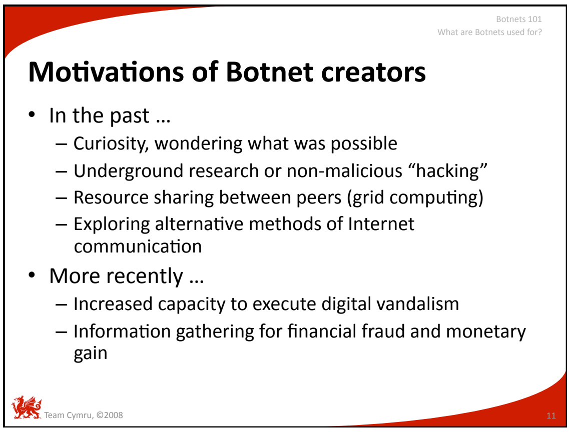

2007 Drones
● Drones
Size = Relative number at a single location
© 2007 Shadowserver Foundation



“What are Botnets used for?”

Team Cymru, ©2008

10



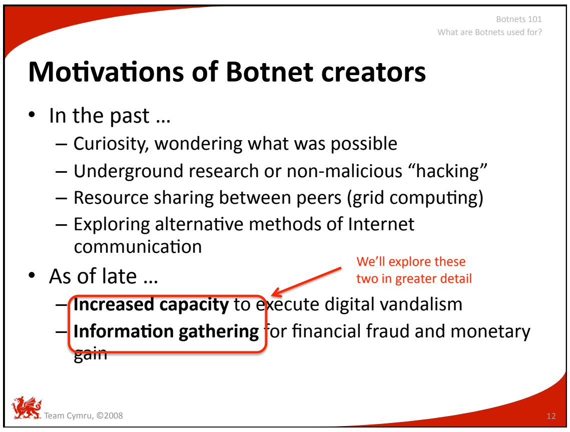
Botnets 101
What are Botnets used for?

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

11



Botnets 101
What are Botnets used for?

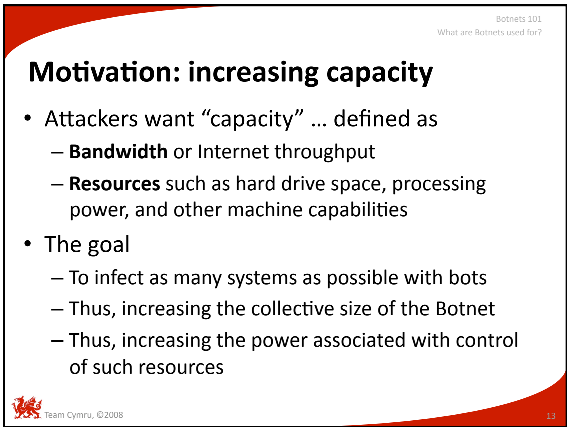
Motivations of Botnet creators

- 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

12

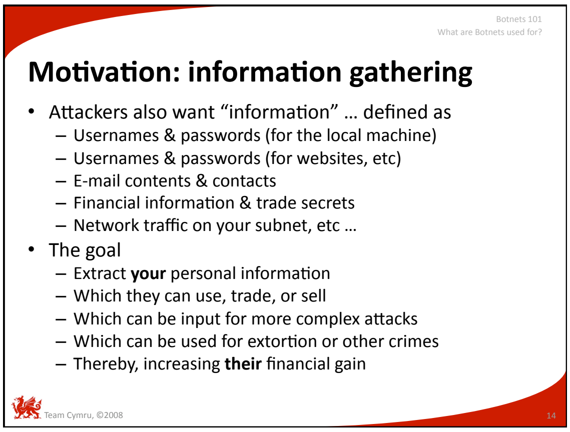


Botnets 101
What are Botnets used for?

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 13

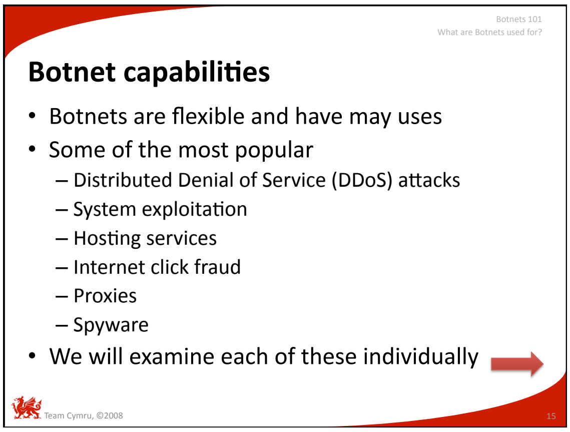


Botnets 101
What are Botnets used for?

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 14

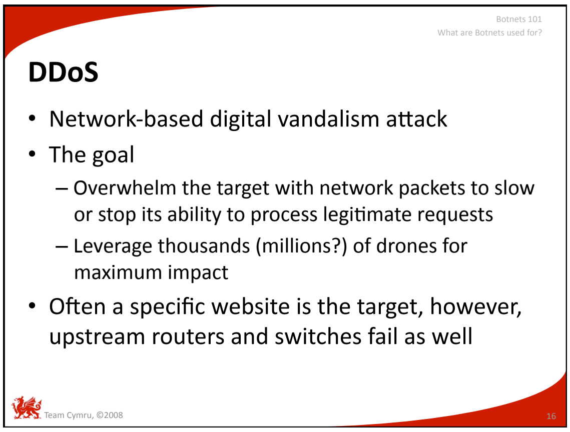


Botnets 101
What are Botnets used for?

Botnet capabilities

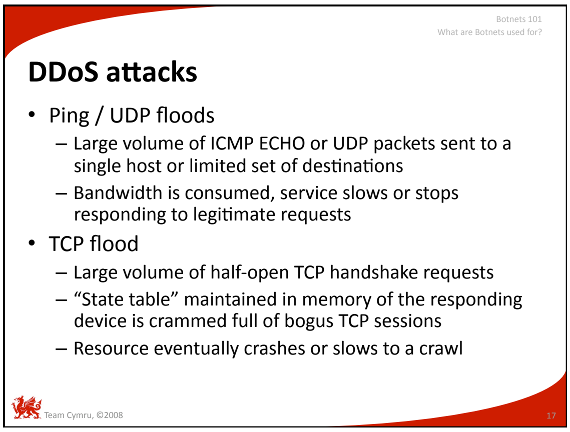
- Botnets are flexible and have may uses
- Some of the most popular
  - Distributed Denial of Service (DDoS) attacks
  - System exploitation
  - Hosting services
  - Internet click fraud
  - Proxies
  - Spyware
- We will examine each of these individually ➡

Team Cymru, ©2008 15



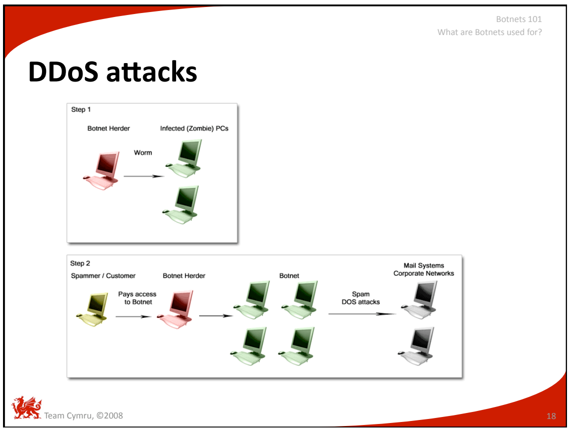
DDoS

- 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

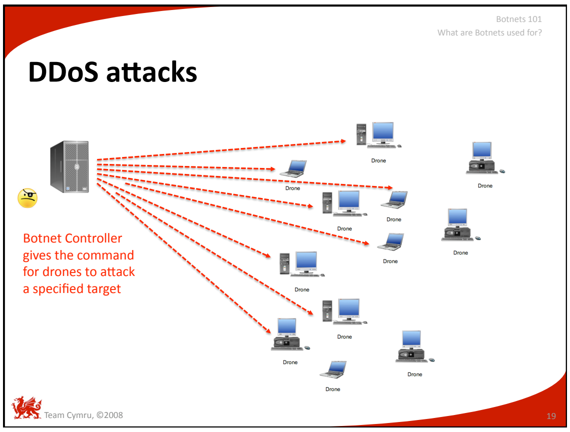


DDoS attacks

- 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



DDoS attacks



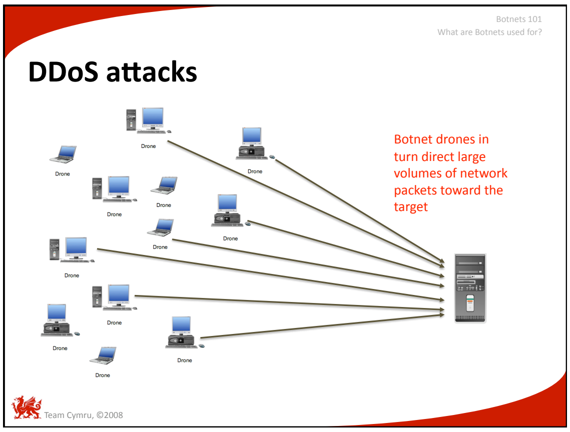
Botnets 101
What are Botnets used for?

DDoS attacks

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

Team Cymru, ©2008

19

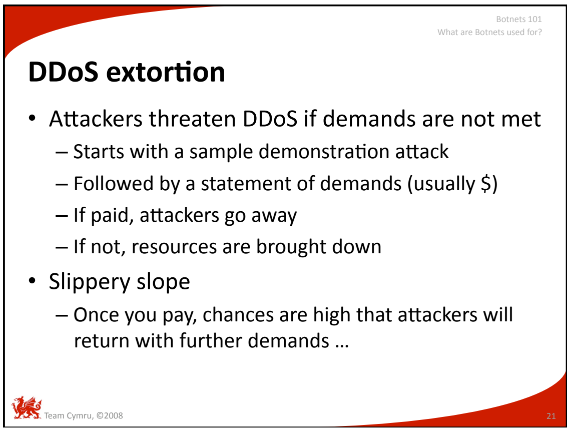


Botnets 101
What are Botnets used for?

DDoS attacks

Botnet drones in turn direct large volumes of network packets toward the target

Team Cymru, ©2008



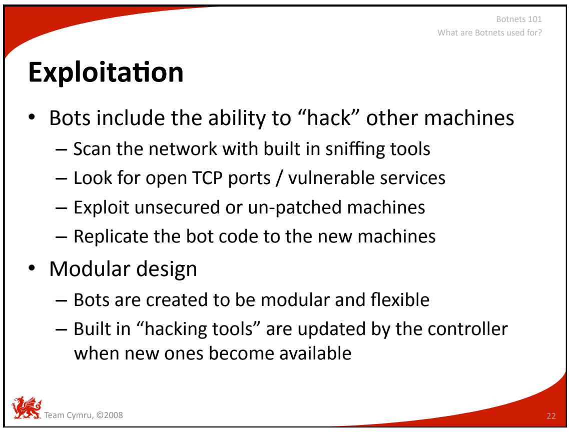
Botnets 101
What are Botnets used for?

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 …

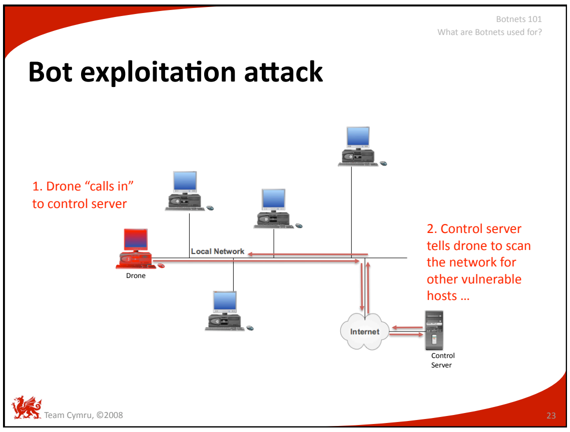
Team Cymru, ©2008

21



Exploitation

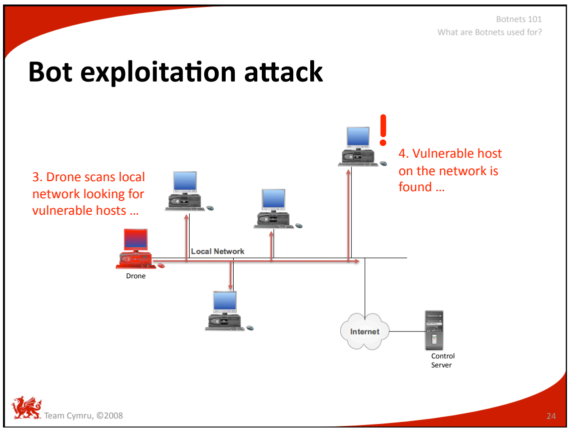
- Bots include the ability to “hack” other machines
  - Scan the network with built in sniffing tools
  - Look for open TCP ports / vulnerable services
  - Exploit unsecured or un-patched machines
  - Replicate the bot code to the new machines
- Modular design
  - Bots are created to be modular and flexible
  - Built in “hacking tools” are updated by the controller when new ones become available



Bot exploitation attack

1. Drone “calls in” to control server

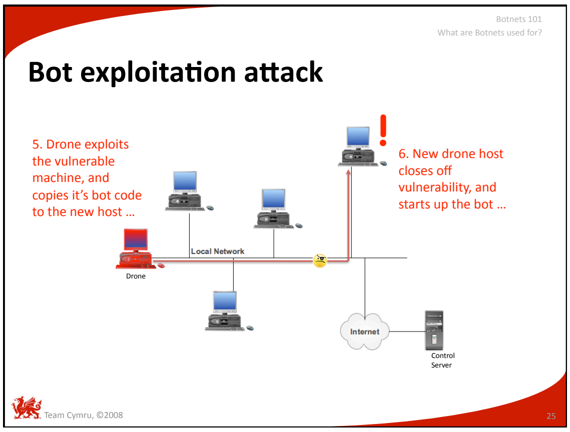
2. Control server tells drone to scan the network for other vulnerable hosts …



Bot exploitation attack

3. Drone scans local network looking for vulnerable hosts …

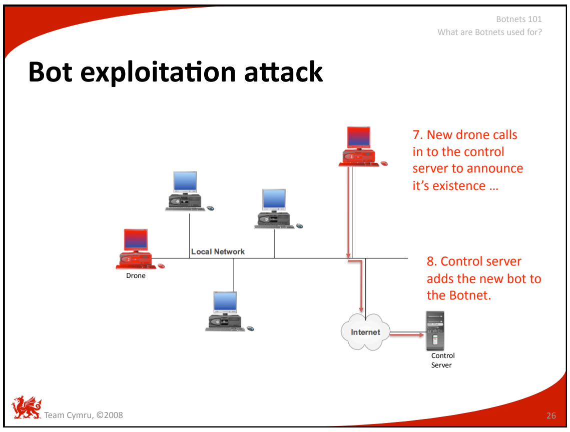
4. Vulnerable host on the network is found …



Bot exploitation attack

5. Drone exploits the vulnerable machine, and copies it's bot code to the new host …

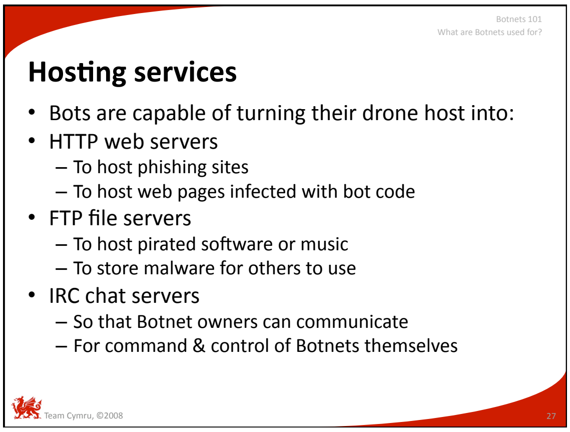
6. New drone host closes off vulnerability, and starts up the bot …



Bot exploitation attack

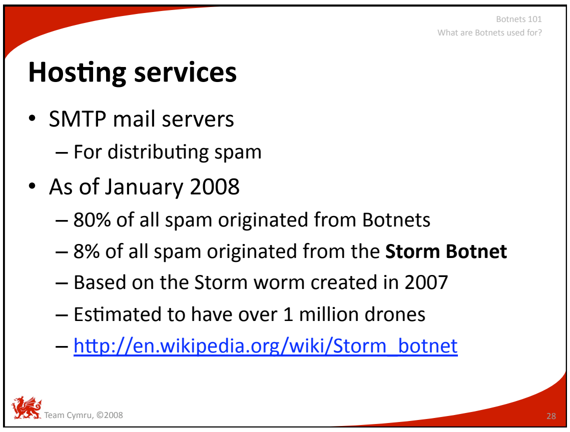
7. New drone calls in to the control server to announce it's existence …

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



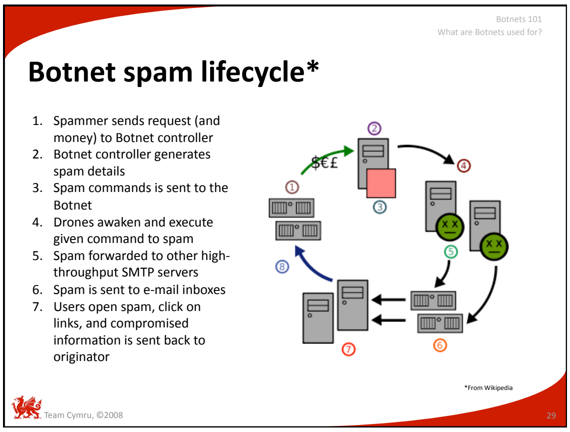
Hosting services

- 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



Hosting services

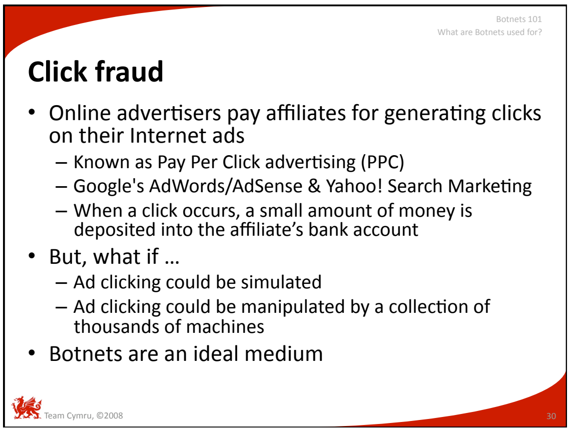
- SMTP mail servers
  - For distributing spam
- As of January 2008
  - 80% of all spam originated from Botnets
  - 8% of all spam originated from the **Storm Botnet**
  - Based on the Storm worm created in 2007
  - Estimated to have over 1 million drones
  - http://en.wikipedia.org/wiki/Storm_botnet



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



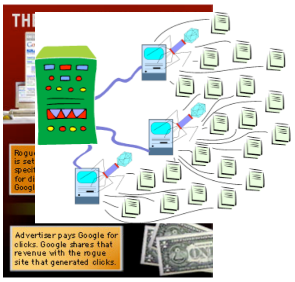
Click fraud

- 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

Click fraud

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

Click fraud


THE
Rogu
is set
specif
for di
Googl
Advertiser pays Google for clicks. Google shares that revenue with the rogue site that generated clicks.

Proxy servers

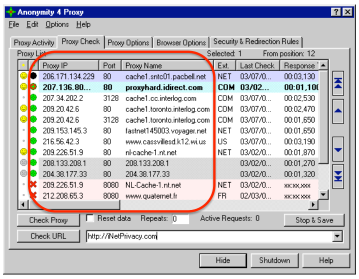
- Network traffic can be “bounced” or proxied through intermediary hosts
  - Has both legitimate and illegitimate uses
- In the case of Botnets
  - Redirecting network traffic through drones avoids detection and attribution
  - Routing IP-based services through several drones in several countries makes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

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
  - Anonomizing other services
  - Very popular and developed use of Botnets

Proxy server types

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



Proxy List Selected: 1 From position: 12

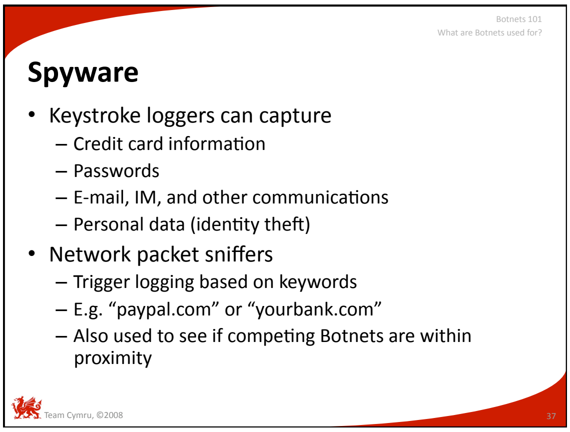
Proxy IP	Port	Proxy Name	Ext.	Last Check	Response
206.171.134.229	80	cache1.sntc01.pacbell.net	NET	03/07/0...	00:03,130
207.136.80...	**80**	**proxyhard.idirect.com**	**COM**	**03/02...**	**00:01,10(**
207.34.202.2	3128	cache1.cc.interlog.com	COM	03/07/0...	00:02,530
209.20.42.6	80	cache1.toronto.interlog.com	COM	03/07/0...	00:02,470
209.20.42.6	3128	cache1.toronto.interlog.com	COM	03/07/0...	00:01,650
209.153.145.3	80	fastnet145003.voyager.net	NET	03/07/0...	00:01,650
216.56.42.3	80	www.cassvillesd.k12.wi.us	US	03/07/0...	00:03,190
209.226.51.9	80	nl-cache-1.nt.net	NET	03/02/0...	00:01,870
208.133.208.1	80	208.133.208.1		03/02/0...	00:01,270
204.38.177.33	80	204.38.177.33		03/02/0...	00:01,320
209.226.51.9	8080	NL-Cache-1.nt.net	NET	03/02/0...	xx:xx,xxx
212.208.65.3	8080	www.quaternet.fr	FR	02/03/0...	xx:xx:xxx

☐ Reset data Repeats: 0 Active Requests: 0

http://iNetPrivacy.com

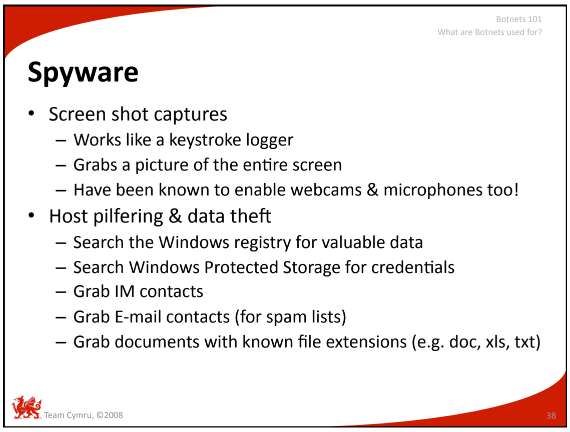
Spyware

- 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”



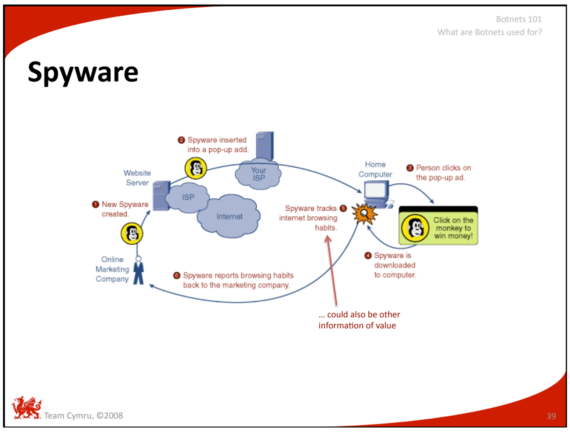
Spyware

- 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



Spyware

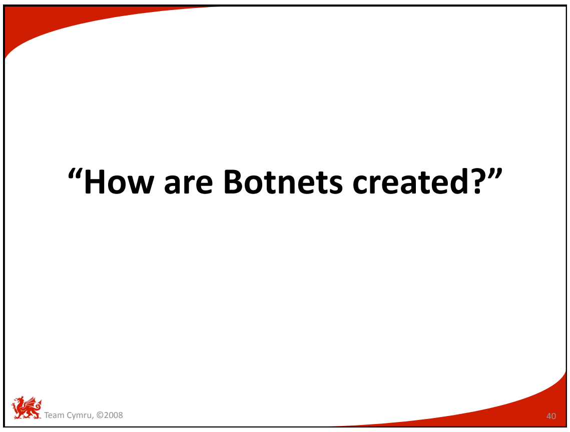
- Screen shot captures
  - Works like a keystroke logger
  - Grabs a picture of the entire screen
  - Have been known to enable webcams & microphones too!
- Host pilfering & data theft
  - Search the Windows registry for valuable data
  - Search Windows Protected Storage for credentials
  - Grab IM contacts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



Spyware

❶ New Spyware created.
❷ Spyware inserted into a pop-up add.
❸ Person clicks on the pop-up ad.
❹ Spyware is downloaded to computer.
Spyware tracks ❺ internet browsing habits.
❻ Spyware reports browsing habits back to the marketing company.
Website Server
ISP
Your ISP
Internet
Home Computer
Click on the monkey to win money!
Online Marketing Company

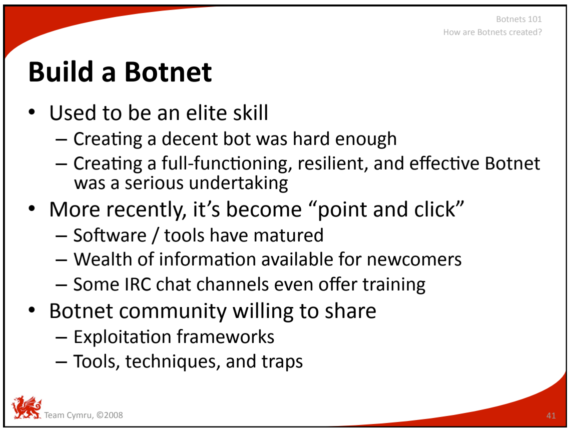
… could also be other information of value



“How are Botnets created?”

Team Cymru, ©2008

40



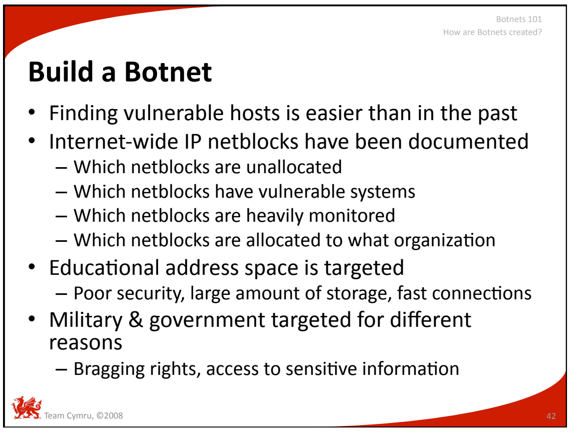
Botnets 101
How are Botnets created?

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

41



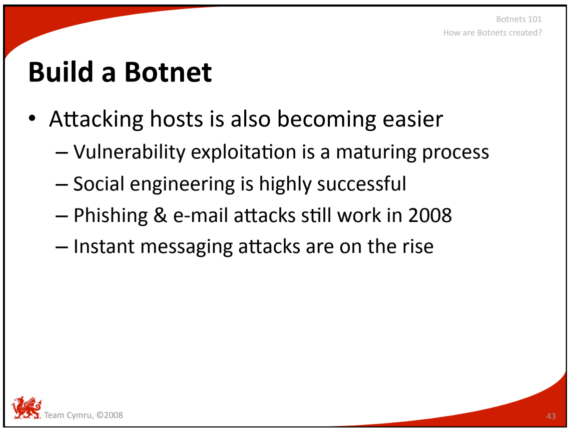
Botnets 101
How are Botnets created?

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

42



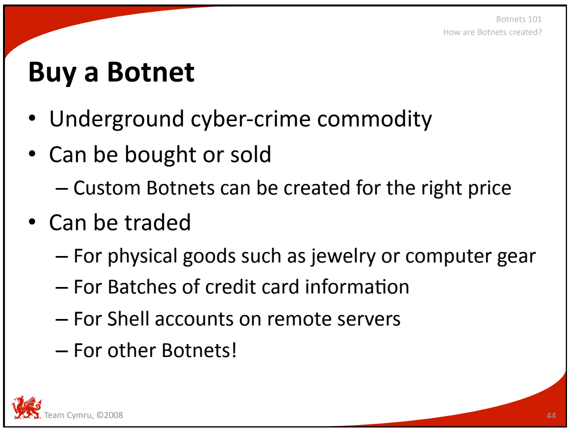
Botnets 101
How are Botnets created?

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

43



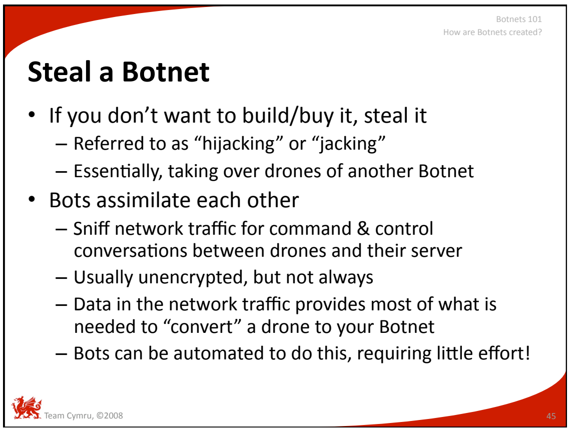
Botnets 101
How are Botnets created?

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

44



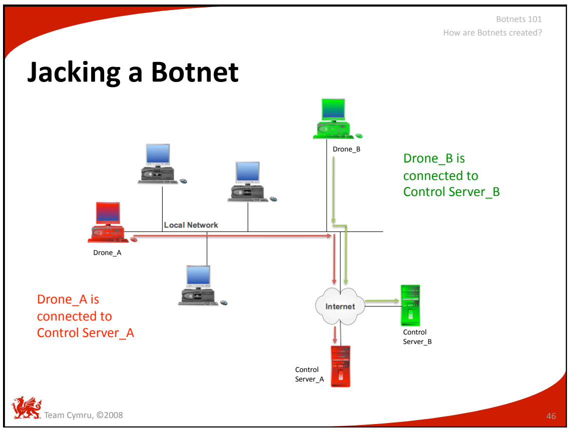
Botnets 101
How are Botnets created?

Steal a Botnet

- If you don’t want to build/buy it, steal it
  - Referred to as “hijacking” or “jacking”
  - Essentially, taking 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

45



Botnets 101
How are Botnets created?

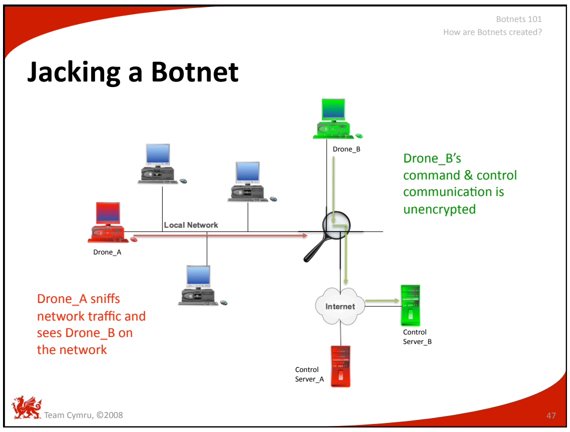
Jacking a Botnet

Drone_B is connected to Control Server_B

Drone_A is connected to Control Server_A

Team Cymru, ©2008

46



Botnets 101
How are Botnets created?

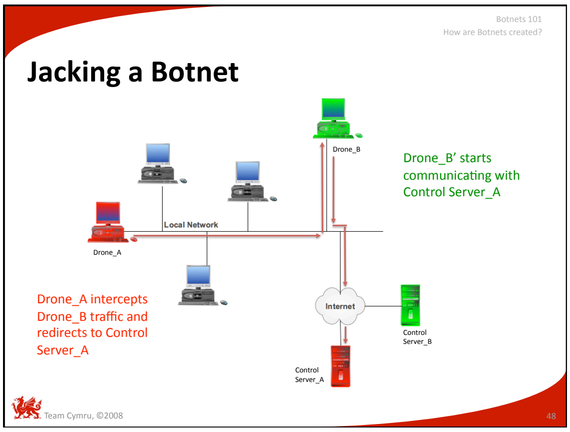
Jacking a Botnet

Drone_B's command & control communication is unencrypted

Drone_A sniffs network traffic and sees Drone_B on the network

Team Cymru, ©2008

47



Botnets 101
How are Botnets created?

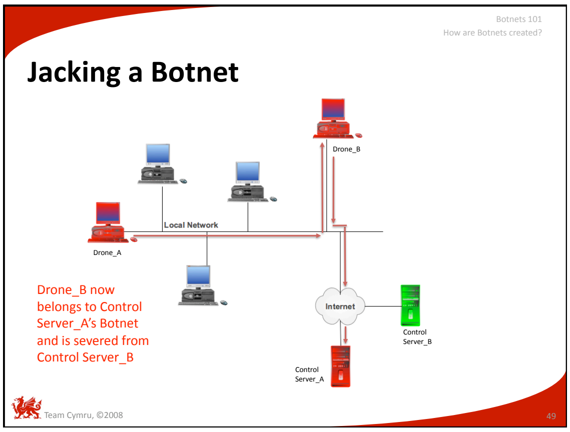
Jacking a Botnet

Drone_B' starts communicating with Control Server_A

Drone_A intercepts Drone_B traffic and redirects to Control Server_A

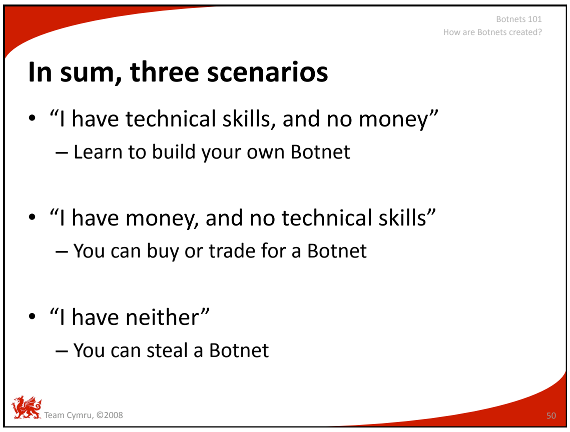
Team Cymru, ©2008

48



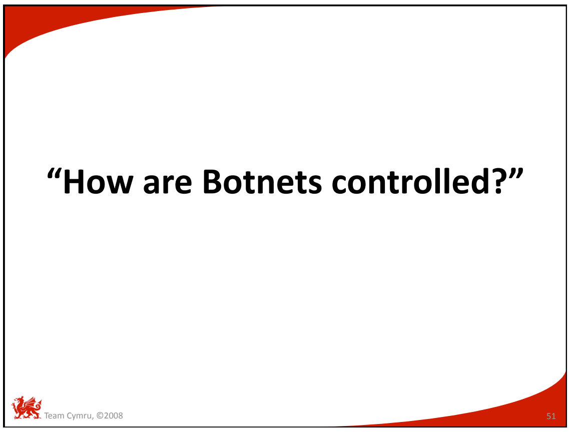
Jacking a Botnet

Drone_B now belongs to Control Server_A's Botnet and is severed from Control Server_B

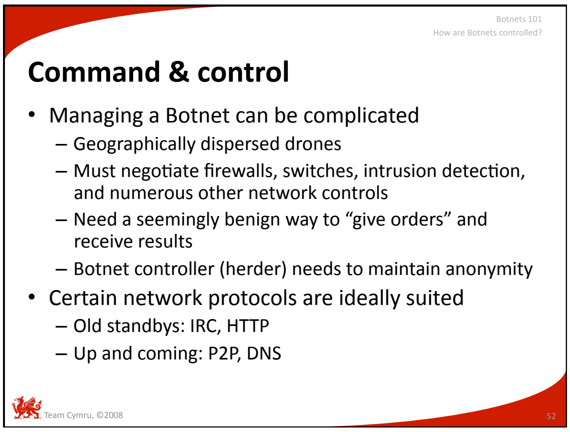


In sum, three scenarios

- "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



"How are Botnets controlled?"



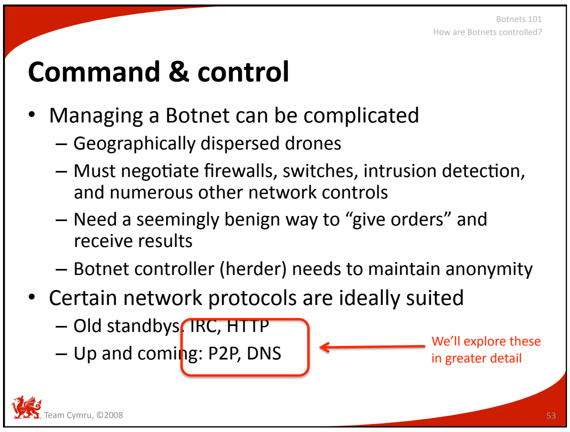
Botnets 101
How are Botnets controlled?

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

52



Botnets 101
How are Botnets controlled?

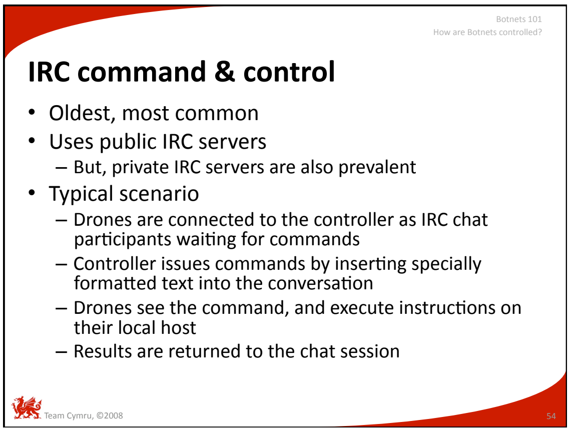
Command & control

- 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

53



Botnets 101
How are Botnets controlled?

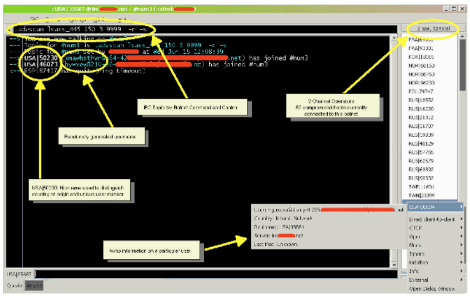
IRC command & control

- 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

54

IRC command & control



```
:USA|35687 @ irc[redacted].net / #num3 (+stnrk[redacted])
.advscan lsass_445 150 3 9999 -r -s
--> You are now talking on #num3
--- Topic for #num3 is .advscan lsass_445 150 3 9999 -r -s
--- Topic for #num3 set by [redacted] at Wed Jun 15 12:08:39
--> USA|50230 (xmawhsthwr@64-42[redacted].net) has joined #num3
--> USA|46073 (bywxew@210-86-[redacted].nz) has joined #num3
<-- ESP|87417 has quit (Ping timeout)
```

```
2 ops, 52 total
FRA|69351
FRA|93001
KOR|10005
NOR|68153
NOR|86753
NOR|96233
POL|74747
RUS|10552
RUS|16220
RUS|21312
RUS|31707
RUS|39009
RUS|40129
RUS|57755
RUS|62579
RUS|63802
RUS|90332
SWE|11601
TWN|23399
USA|08884
```

```
User: ~guacusa@dialup-4.239[redacted]net
Country: Internic Network
Realname: USA|08884
Server: irc[redacted].net
Last Msg: Unknown
```

IRC Topic for Botnet Command and Control

2 Channel Operators
52 compromised hosts currently connected to this botnet

Randomly generated username

USA|50230: Nickname used to distinguish country of origin and unique user number

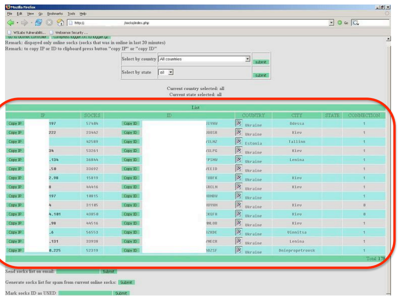
Whois information on a particular user

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

HTTP command & control

List of active bots and their locations, etc



Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http:// /socks/index.php
WSLabs Vulnerabili... Websense Security ...
Go to botnet controller
Compress logger.txt to logger.gz

Remark: dispayed only online socks (socks that was in online in last 20 minutes)
Remark: to copy IP or ID to clipboard press button "copy IP" or "copy ID"

Select by country: All countries [submit]
Select by state: all [submit]

Current country selected: all
Current state selected: all

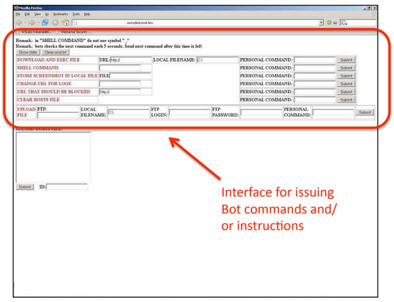
List

IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION
Copy IP [redacted]197	57404	Copy ID [redacted]JIVHW	Ukraine	Odessa		1
Copy IP [redacted]222	23442	Copy ID [redacted]JOOSR	Ukraine	Kiev		1
Copy IP [redacted]	42589	Copy ID [redacted]VILNZ	Estonia	Tallinn		1
Copy IP [redacted]34	53261	Copy ID [redacted]VXLPG	Ukraine	Kiev		1
Copy IP [redacted].134	36844	Copy ID [redacted]FPSNW	Ukraine	Lenina		1
Copy IP [redacted].58	33692	Copy ID [redacted]VEEID	Ukraine			1
Copy IP [redacted]2.98	15819	Copy ID [redacted]FUBFK	Ukraine	Kiev		1
Copy IP [redacted]8	44416	Copy ID [redacted]SRCLN	Ukraine	Kiev		1
Copy IP [redacted]197	10815	Copy ID [redacted]HONBV	Ukraine			1
Copy IP [redacted]4	31105	Copy ID [redacted]HUYHM	Ukraine	Kiev		0
Copy IP [redacted]4.101	43850	Copy ID [redacted]CKGFH	Ukraine	Kiev		0
Copy IP [redacted].98	44516	Copy ID [redacted]HNLOB	Ukraine	Kiev		1
Copy IP [redacted].6	56553	Copy ID [redacted]BZKDE	Ukraine	Vinnitsa		1
Copy IP [redacted].131	33938	Copy ID [redacted]VNECR	Ukraine	Lenina		1
Copy IP [redacted]0.225	52319	Copy ID [redacted]AOZSF	Ukraine	Dniepropetrovsk		1

Total 178

Send socks list on email: [Submit]
Generate socks list for spam from current online socks: [Submit]
Mark socks ID as USED: [Submit]

HTTP command & control


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
socks/bot/cmd.htm
Go
WSLabs Vulnerabiliti... Websense Security ...

Remark: in "SHELL COMMAND" do not use symbol "_"
Remark: bots checks the next command each 5 seconds. Send next command after this time is left

Show stats | Clear cmd.txt

DOWNLOAD AND EXEC FILE	URL: http://	LOCAL FILENAME: C:\	PERSONAL COMMAND: Submit
SHELL COMMAND			PERSONAL COMMAND: Submit
STORE SCREENSHOT IN LOCAL FILE	FILE		PERSONAL COMMAND: Submit
CHANGE URL FOR LOGS			PERSONAL COMMAND: Submit
URL THAT SHOULD BE BLOCKED	http://		PERSONAL COMMAND: Submit
CLEAR HOSTS FILE			PERSONAL COMMAND: Submit

UPLOAD FILE FTP: LOCAL FILENAME: C:\ FTP LOGIN: FTP PASSWORD: PERSONAL COMMAND: Submit

UPLOAD HOSTS FILE:

Submit ID:

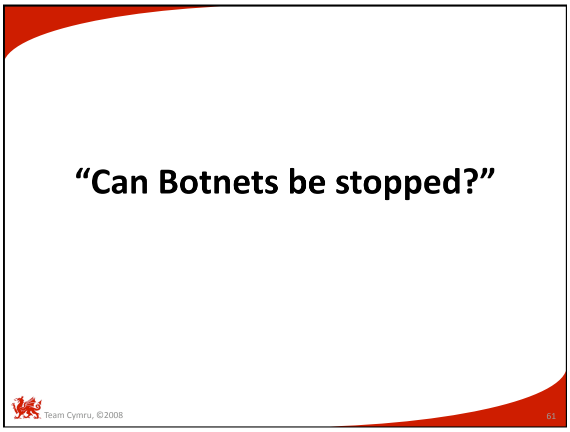
Interface for issuing Bot commands and/ or instructions

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

P2P command & control

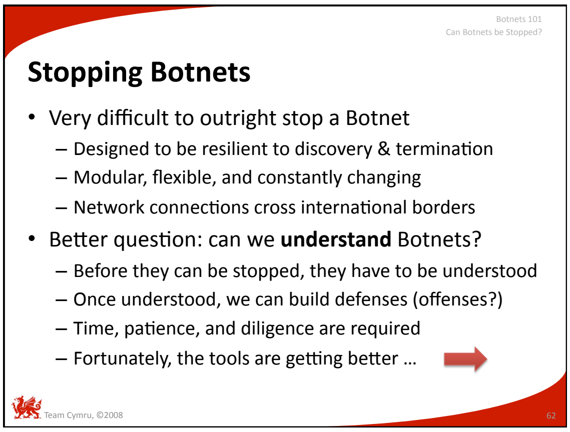
- Growing in popularity
- Being heavily researched by universities in the US
- Relies on a web of peer controllers vs. a single server
  - If the controller is shutdown, the Botnet survives



"Can Botnets be stopped?"

Team Cymru, ©2008

61



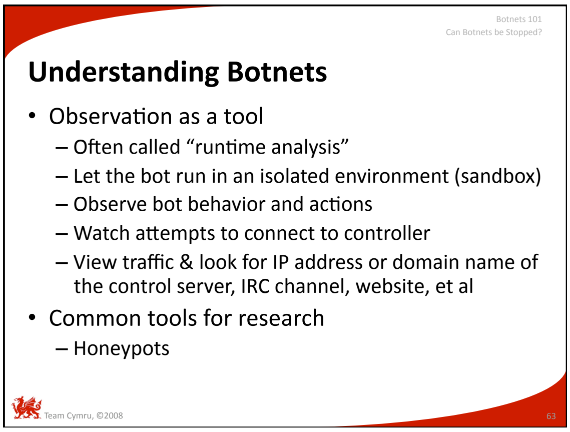
Botnets 101
Can Botnets be Stopped?

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

62



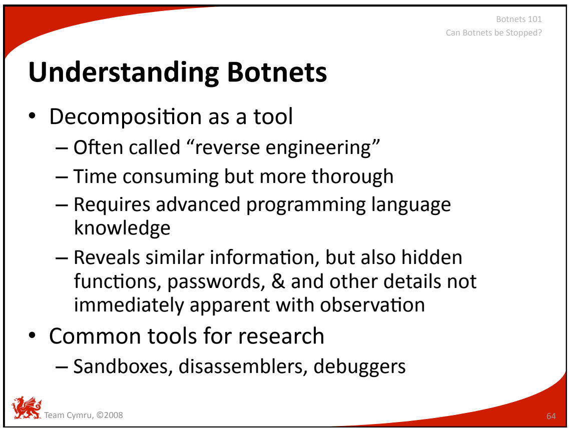
Botnets 101
Can Botnets be Stopped?

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

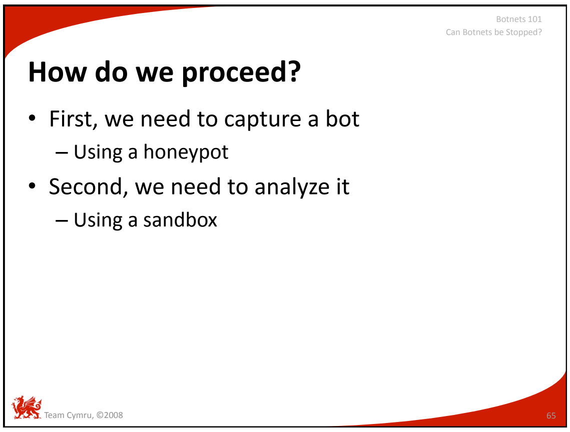
Team Cymru, ©2008

63



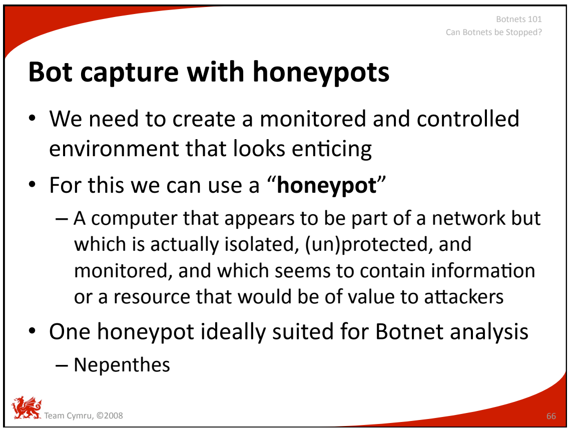
Understanding Botnets

- 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



How do we proceed?

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



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

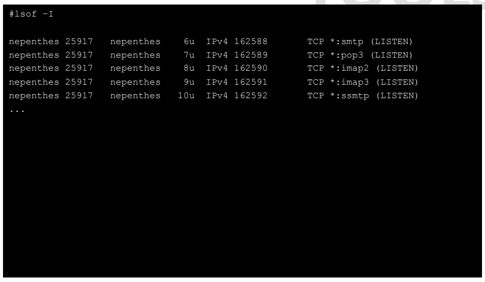
Nepenthes

- 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

How Nepenthes works

TOOLS

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



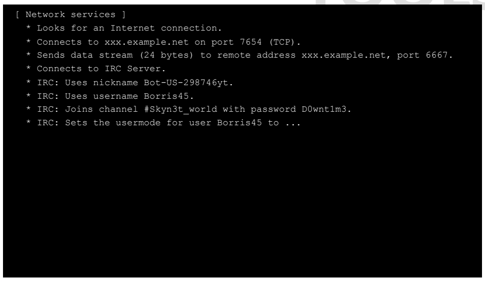
```
#lsof -I

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 *:ssmtp (LISTEN)
...
```

How Nepenthes works

TOOLS

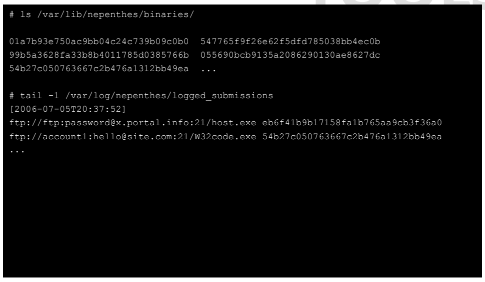
As malware (bots) attempt to compromise the honeypot, their actions are tracked



```
 [ 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-US-298746yt.
   * IRC: Uses username Borris45.
   * IRC: Joins channel #Skyn3t_world with password D0wnt1m3.
   * IRC: Sets the usermode for user Borris45 to ...
```

How Nepenthes works

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



```
# ls /var/lib/nepenthes/binaries/

01a7b93e750ac9bb04c24c739b09c0b0  547765f9f26e62f5dfd785038bb4ec0b
99b5a3628fa33b8b4011785d0385766b  055690bcb9135a2086290130ae8627dc
54b27c050763667c2b476a1312bb49ea  ...

# tail -1 /var/log/nepenthes/logged_submissions
[2006-07-05T20:37:52]
ftp://ftp:password@x.portal.info:21/host.exe eb6f41b9b17158fa1b765aa9cb3f36a0
ftp://account1:hello@site.com:21/W32code.exe 54b27c050763667c2b476a1312bb49ea
...
```

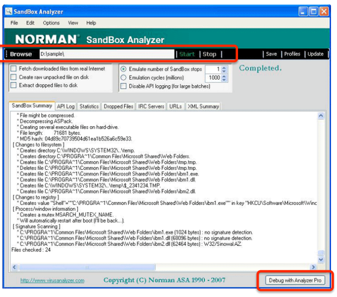
Bot analysis with sandboxes

- 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

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

SandBox Analyzer screenshot



D:\sample\

□ Fetch downloaded files from real Internet
□ Create raw unpacked file on disk
□ Extract dropped files to disk

● Emulate number of SandBox stops 1
○ Emulation cycles (millions) 1000
□ Disable API logging (for large batches)

Completed.

```
  * File might be compressed.
  * Decompressing ASPack.
  * Creating several executable files on hard-drive.
  * File length:        71681 bytes.
  * MD5 hash: 04d89c70739504d61ea1b526a6c59e33.
[ Changes to filesystem ]
  * Creates directory C:\WINDOWS\SYSTEM32\..\temp.
  * Creates directory C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders.
  * Creates file C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\tmp.tmp.
  * Deletes file C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\tmp.tmp.
  * Creates file C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm1.exe.
  * Creates file C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm1.dll.
  * Creates file C:\WINDOWS\SYSTEM32\..\temp\$_2341234.TMP.
  * Creates file C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm2.dll.
[ Changes to registry ]
  * Creates value "Shell"=""C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm1.exe"" in key "HKCU\Software\Microsoft\Winc
[ Process/window information ]
  * Creates a mutex MSARCH_MUTEX_NAME.
  * Will automatically restart after boot (I'll be back...).
[ Signature Scanning ]
  * C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm1.exe (1024 bytes) : no signature detection.
  * C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm1.dll (68096 bytes) : no signature detection.
  * C:\PROGRA~1\Common Files\Microsoft Shared\Web Folders\ibm2.dll (62464 bytes) : W32/Sinowal.AZ.
Files checked : 24
```

http://www.virusanalyzer.com Copyright (C) Norman ASA 1990 - 2007

Select file for analysis

Runtime output

Advanced debugging with "Pro" tools

Norman SandBox output logfile

```
–   D:VIRUSMYTEST.EX_ : W32/Backdoor
–   ====> Sandbox output:
–   [ General information ]
–   * **IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO -
–   REMEMBER TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)**.
–   * Display message box (sample) : sample, te amo!.
–   * Display message box (KERN32) : KERN32, te amo!.
–   * File length: 58368 bytes.
–   * MD5 hash: 60a8d2e41147f48364e1eb3729ac53fb.

–   [ Changes to filesystem ]
–   * Deletes file C:WINDOWSSYSTEM32kern32.exe.
–   * Creates file C:WINDOWSSYSTEM32kern32.exe.

–   [ Changes to registry ]
–   * Creates key "HKLMSoftwareMicrosoftWindowsCurrentVersionRunOnce".
–   * Sets value "kernel32"="C:WINDOWSSYSTEM32kern32.exe -sys" in key "HKLMSoftwareMicrosoftWindowsCurrentVersionRunOnce".

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

–   [ Network services ]
–   * Connects to "200.223.3.130" on port 6667 (TCP).
–   * Connects to IRC server.
–   * IRC: Uses nickname CurrentUser[FRK][19].
–   * IRC: Uses username SErVERINO.
–   * IRC: Joins channel #Sl4cK_r0oT.

    [ Process/window information ]
–   * Creates a mutex ZZM9H9YY.
–   * Creates a mutex SrVFrK.
```

Bot modifies system files

Bot injects keyboard sniffer

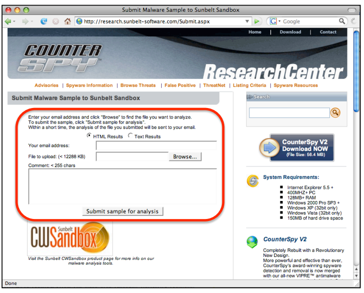
Bot joins IRC channel

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

CWSandbox screenshot

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


Submit Malware Sample to Sunbelt Sandbox
http://research.sunbelt-software.com/Submit.aspx
Google
Home | Download | Contact
COUNTER SPY
ResearchCenter
Advisories | Spyware Information | Browse Threats | False Positive | ThreatNet | Listing Criteria | Spyware Resources
Search
CounterSpy V2 Download NOW (File Size: 56.4 MB)
Browse...
Submit sample for analysis
CWSandbox Sunbelt
Done

Submit Malware Sample to Sunbelt Sandbox

Enter your email address and click "Browse" to find the file you want to analyze.
To submit the sample, click "Submit sample for analysis".
Within a short time, the analysis of the file you submitted will be sent to your email.

● HTML Results ○ Text Results

Your email address:

File to upload: (< 12288 KB)

Comment: < 255 chars

Visit the Sunbelt CWSandbox product page for more info on our malware analysis tools.

System Requirements:

- Internet Explorer 5.5 +
- 400MHZ+ PC
- 128MB+ RAM
- Windows 2000 Pro SP3 +
- Windows XP (32bit only)
- Windows Vista (32bit only)
- 150MB of hard drive space

CounterSpy V2

Completely Rebuilt with a Revolutionary New Design.
More powerful and effective than ever, CounterSpy's award-winning spyware detection and removal is now merged with our all-new VIPRE™ antimalware

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