

Botnets

An Introduction Into the World of Botnets

Tyler Hudak

KoreLogic Security

thudak@korelogic.com



What will we cover?

- ◆ What are botnets?
- ◆ History
- ◆ How do they work?
- ◆ What are they used for?
- ◆ Who cares? Why you should.
- ◆ Detection and Prevention Methods

Botnets

- ◆ “A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task.”¹
 - Typically refers to botnets used for illegal purposes.
- ◆ Controlled by one person or a group of people (aka. the botmaster)
 - Under a command and control structure (C&C)

1. <http://www.shadowserver.org>

History

- ◆ Bots originally used in multiple places as a way to automate tasks
 - IRC, IM, MUDS, online games
 - Protect a channel, carry out conversations, automated gaming tasks, etc.
- ◆ Evolved into a way to automate malicious tasks
 - Spam, Control a PC, propagate, etc.
- ◆ Botnets started with DoS/DDoS against servers
 - TFN, stacheldraht, trinoo (1999)

History

- ◆ Attackers created better ways to control bots
 - Moved from proprietary command and control mechanisms (C&C) to more publicly available ones
 - HTTP, IRC, P2P
- ◆ Bots started to become payloads for worms
 - Allowed for faster compromises, bigger botnets
 - Sobig/SDBot/Rbot/Agobot/Phatbot...
- ◆ 10,000 bots in a single botnet is not uncommon.
- ◆ Today, botnets are big business!

How do they work?

1. Botmaster infects victim with bot (worm, social engineering, etc)



Botmaster



Victim



C&C Server

How do they work?



Botmaster



Victim



C&C Server

2. Bot connects to C&C server. This could be done using HTTP, IRC or any other protocol.

How do they work?



Botmaster

3. Botmaster sends commands through C&C server to bot



C&C Server



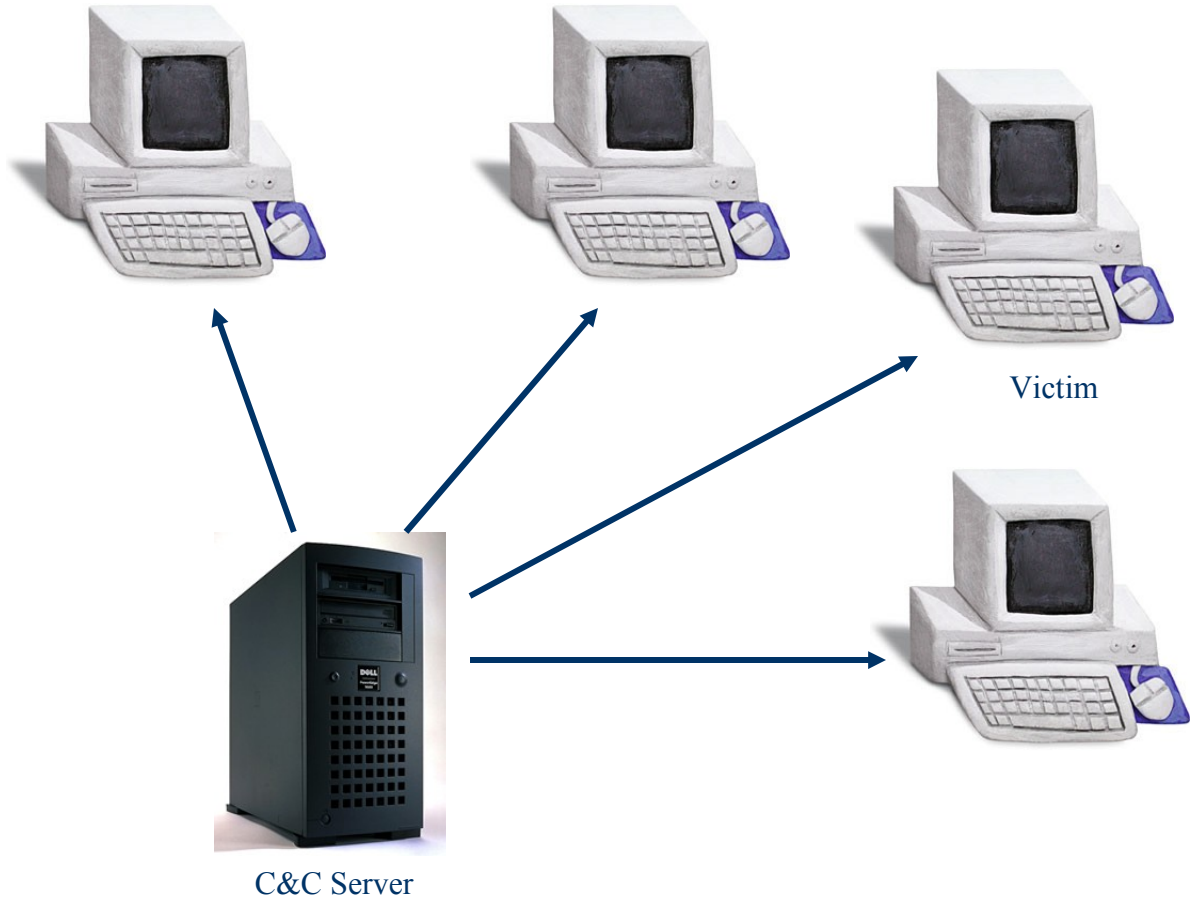
Victim

How do they work?



Botmaster

4. Repeat. Soon the botmaster has an army of bots to control from a single point



What are they used for?

- ◆ Botmasters have botnets in upwards of 400,000 bots. What do they use them for?
- ◆ Often only one thing:



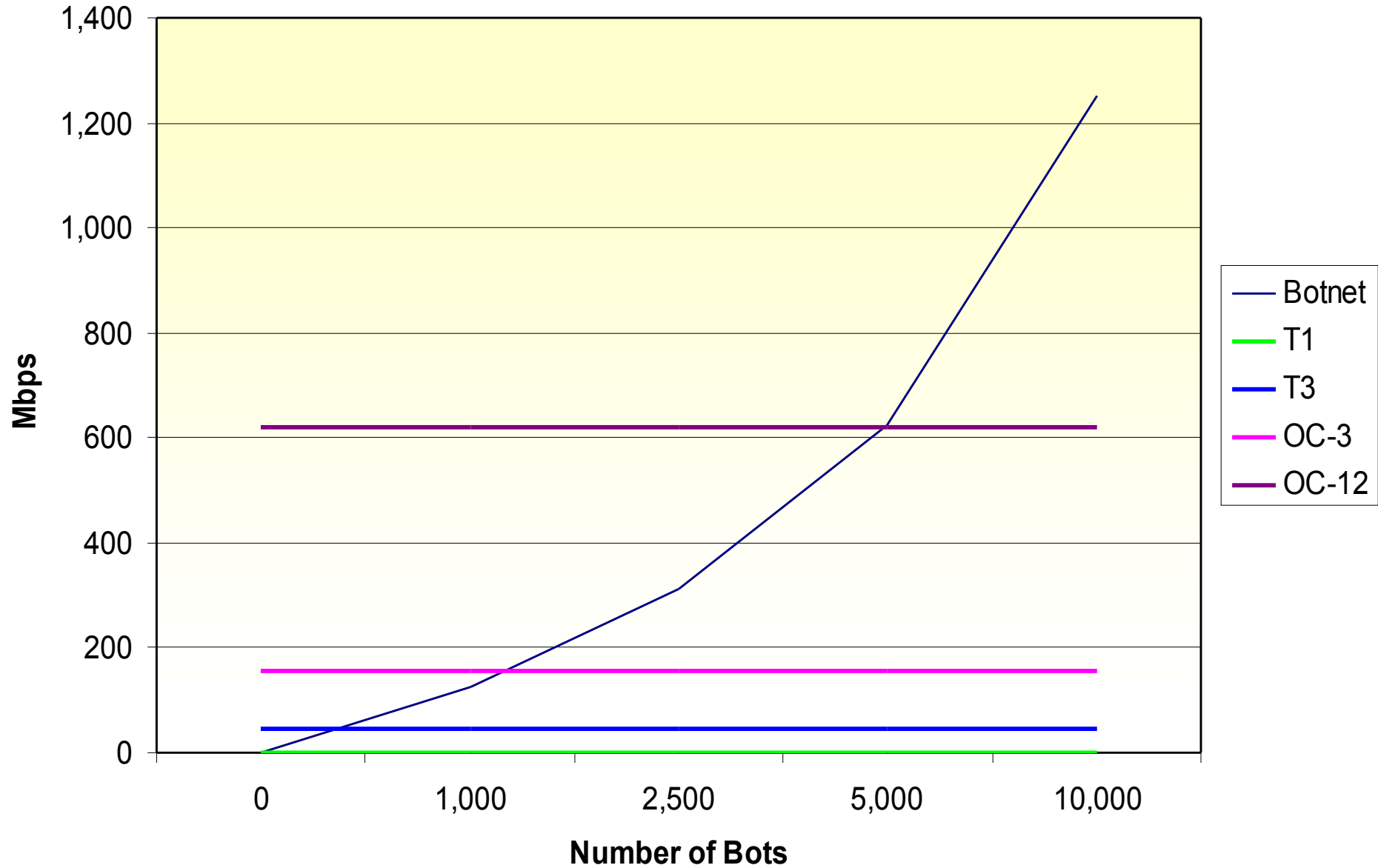
Botnet Uses

- ◆ Distributed Denial of Service (DDoS)
- ◆ Spam/Phishing
- ◆ Ad-ware
- ◆ Click Fraud
- ◆ Others...

Uses: DDoS

- ◆ DDoS has been available in bots since the beginning
- ◆ Used for extortion
 - Take down systems until they pay – threats work too!
- ◆ Example: 180Solutions – Aug 2005
 - Botmaster used bots to distribute 180Solutions ad-ware
 - 180Solutions shut botmaster's account down
 - Botmaster threatened DDoS attacks unless paid
 - When not paid, used botnet to DDoS 180Solutions

Botnet Bandwidth Consumption



DDoS Case Study: BlueSecurity

- ◆ Effective anti-spam company
 - Would fight spam with spam
- ◆ May 2006 – Russian spammer rented botnet to DDoS BlueSecurity
 - BlueSecurity would switch hosts/networks, DDoS would follow
 - Attack disrupted 5 major ISPs and DNS
- ◆ BlueSecurity shut down services



Uses: Spam / Phishing

- ◆ Many bots are able to send out spam or phishing attempts
 - Built-in functionality
 - Backdoor proxy servers
- ◆ Spam goes out from many different machines
- ◆ Gives the spammer/phisher a way to send out thousands of emails and easily beat spam defenses

Uses: Ad-ware Installation

- ◆ Ad-ware pays by the number of “installs” a person has
- ◆ Many bots download and install ad-ware when they are loaded
 - Often multiple versions of ad-ware
- ◆ Generates income from ad-ware revenues
 - Jan 2006 - Jeanson James Ancheta convicted for operating a 400,000 strong botnet used to install ad-ware.
 - Earned over \$60,000 from ad-ware.

Make Money

THESE FOLLOWING TOOLBAR PROGRAMS CAN MAKE YOU MONEY
OFF OF YOUR EXISING WEBSITE TRAFFIC.

GET PAID EVERYTIME A VISITER INSTALLS THE TOOLBAR.

Just click on the links below and signup to start making money.

1. [LoudCash](#) (formerly [SearchBarCash](#)) (Paid ME VIA-paypal)

Payout Info:

\$0.20 Per US Install

\$0.20 Per Internatonal Install

\$5.00 CPM

\$500 Bonus after 50,000 Installs

2. [MediaTicket](#) (Paid ME Via-paypal)

Payout Info:

\$0.15 Per US install

\$0.01 Per Reffered Install

3. [GammaCash](#) (Paid ME Via-check)

Payout Info:

\$0.15 per install (toolbarcash)

4. [Media-Motor](#) (Paid ME Via-paypal)

Payout Info:

\$0.15 Per US/Canada/UK install

\$0.01 International Installs

5. [Overnro](#) (Paid ME Via-paypal)

Uses: Click Fraud

- ◆ Online advertisers pay by the number of unique “clicks” on their ads
- ◆ Thousands of bots can generate thousands of unique clicks
- ◆ Botmaster “rents” out the clicks and gets a piece of the revenue
- ◆ Clickbot. A botnet found with more than 34,000 machines in it

Other Uses

- ◆ Malware installation
 - Rootkits
 - Other malware to increase the odds of keeping that machine
- ◆ Spyware - Identity Theft
 - Sniff passwords, keystroke logging
 - Grab credit card, bank account information
- ◆ Rent out the botnet!
 - Pay as little as \$100 an hour to DoS your favorite site!

Botnet Email Ad

Tired of being scammed?
Tired of servers downtime?
Tired of high latency?
Being Blocked or Blacklisted too fast?

FORGET ABOUT THAT!

Get rid of asian datacenters and choose a better Spam friendly solution with us. We have the latest development in Bulletproof Webservers that will handle your high complaint loads.

Contact us for pricing!

ICQ #:

MSN Messenger:

AIM:

yahoo:

Botnet Hosting Servers

5 Ips that changes every 10 minutes (with different ISP)

Excellent ping and uptime.

100 percent uptime guarantee. Easy Control Panel to add or delete your domains thru webinterface.

Redhat / Debian LINUX OS.

SSH Root Access.

FTP Access.

APACHE2 PHP CURL ZEND MYSQL FTP SSH.

We have Direct Sending Servers, and we also do Email Lists Mailings.

How do they spread?

- ◆ Exploiting known vulnerabilities
 - Scan other hosts for vulnerable services
 - MS-RPC DCOM, LSASS, VNC
- ◆ Social Engineering
 - Spam/Phishing
 - Website Downloads
 - Instant Messaging
 - P2P networks

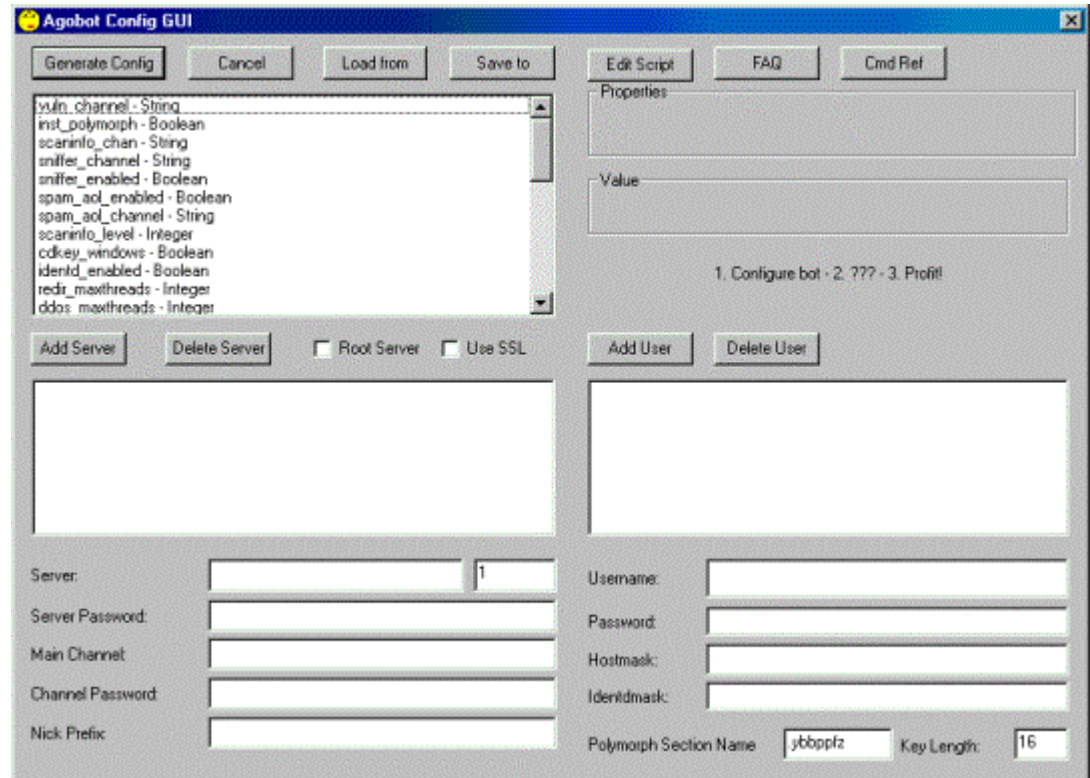


Types of Bots - Agobot

- ◆ Bots all derived from same “family”
 - Over 500 variants exist in the wild
- ◆ Well-written, GPL'd C++ code
 - Modular code – easy to add enhancements
- ◆ GUI configuration
- ◆ Both Windows and Linux versions exist
- ◆ Capabilities include DoS, multiple exploits, sniffers, virtual machine and debugger detection
- ◆ IRC or P2P-based C&C

Agobot GUI Config

- Point and Click
- Turn on/off features
- Change C&C servers
- Set passwords
- Add polymorphism



Types of Bots - SDBot

- ◆ Over 4000 variants exist
 - aka. Rbot, Rxbot, Urbot...
- ◆ GPL'd C-code
 - Modular, small
- ◆ Many patches exist which extend capabilities
 - DoS, exploit propagation, sniffers, encryption, etc.
- ◆ IRC-based C&C

Types of Bots – GT Bot

- ◆ Uses Windows IRC program mIRC
 - Bot code within mIRC scripts
 - Packaged with mIRC executable
- ◆ Bot installs mIRC and scripts
 - Hides mIRC with “HideWindow” program
- ◆ Limited functionality
 - Some scanning, DoS and exploit functionality

Types of Bots - Others

- ◆ Perl-based bots
 - Written in Perl – very small
 - Provide typical bot functionality
 - Usually seen on Linux/UNIX servers
- ◆ Q8Bots, Kaiten bots
 - Linux bots
 - Small, easy to compile
 - Typical feature set

Command and Control

- ◆ The methods and infrastructure which the botmaster uses to send instructions to his bots.
- ◆ Number of different ways to control bots
- ◆ Most common is through IRC (public or private)
 - Bots log into a specific IRC channel
 - Bots are written to accept specific commands and execute them (sometimes from specific users)

Command and Control - IRC

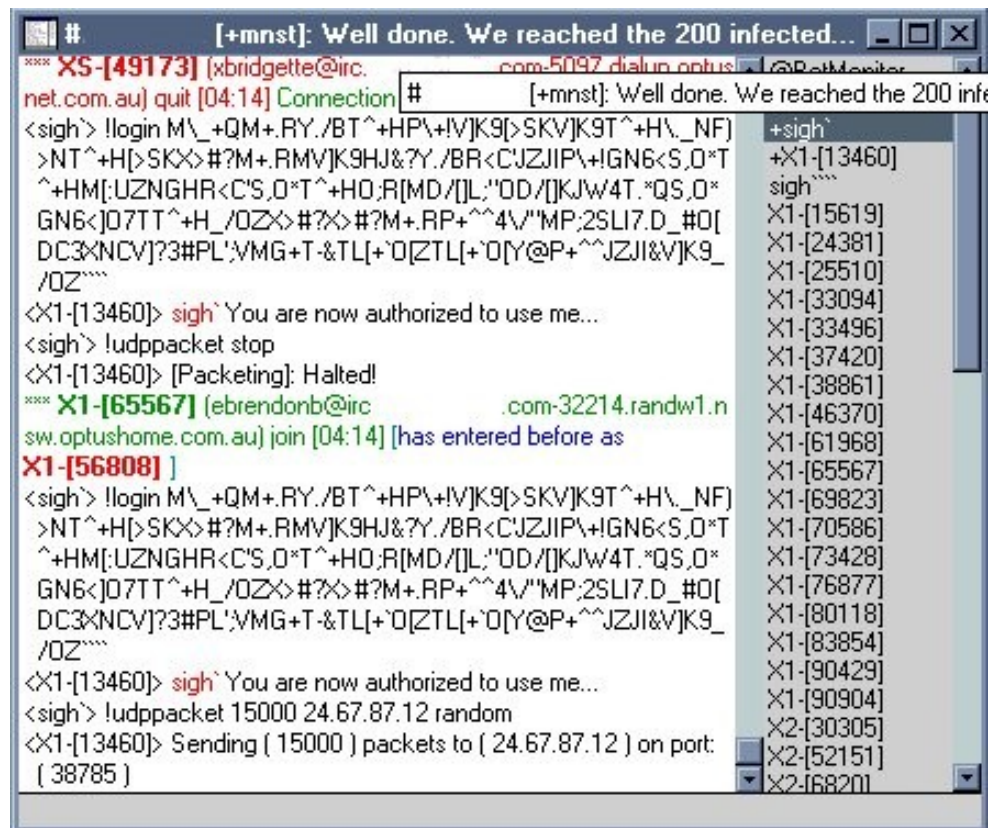
♦ Advantages

- Infrastructure already set up and maintained
- Have lots of traffic flowing to them already
- Easy to hide – difficult to detect
- Code already exists – just drag and drop!

♦ Disadvantages

- Usually unencrypted
- Easy to get into, take over or shut down

Command and Control - IRC



The screenshot shows an IRC chat window with a title bar that reads "[+mnst]: Well done. We reached the 200 infected...". The chat log contains the following text:

```
*** XS-[49173] (xbridgette@irc. com-5097.dialup.optus. ) [BotMonitor  
net.com.au] quit [04:14] Connection # [+mnst]: Well done. We reached the 200 infe  
< sigh> !login M\_^QM+.RY./BT^+HP\+IV]K9[>SKV]K9T^+H\_NF)  
>NT^+H[>SKX>#?M+.RMV]K9HJ&?Y./BR<CUZJIP\+IGN6<S,O*T  
^+HM[;UZNGHR<C'S,O*T^+HO.R[MD/[JL;"OD/[KJW4T."QS,O*  
GN6<]O7TT^+H_/OZX>#?X>#?M+.RP+^4V"MP;2SLI7.D_#O[  
DC3XNCV]?3#PL'VMG+T-&TL[+`O[ZTL[+`O[Y@P+^JZJI&V]K9_  
/OZ""  
<X1-[13460]> sigh` You are now authorized to use me...  
< sigh> !udppacket stop  
<X1-[13460]> [Packeting]: Halted!  
*** X1-[65567] (ebrendonb@irc. com-32214.randw1.n  
sw.optushome.com.au) join [04:14] [has entered before as  
X1-[56808] ]  
< sigh> !login M\_^QM+.RY./BT^+HP\+IV]K9[>SKV]K9T^+H\_NF)  
>NT^+H[>SKX>#?M+.RMV]K9HJ&?Y./BR<CUZJIP\+IGN6<S,O*T  
^+HM[;UZNGHR<C'S,O*T^+HO.R[MD/[JL;"OD/[KJW4T."QS,O*  
GN6<]O7TT^+H_/OZX>#?X>#?M+.RP+^4V"MP;2SLI7.D_#O[  
DC3XNCV]?3#PL'VMG+T-&TL[+`O[ZTL[+`O[Y@P+^JZJI&V]K9_  
/OZ""  
<X1-[13460]> sigh` You are now authorized to use me...  
< sigh> !udppacket 15000 24.67.87.12 random  
<X1-[13460]> Sending ( 15000 ) packets to ( 24.67.87.12 ) on port:  
( 38785 )
```

On the right side of the chat window, there is a list of users with their nicknames and IDs:

- +sigh`
- X1-[13460]
- sigh`
- X1-[15619]
- X1-[24381]
- X1-[25510]
- X1-[33094]
- X1-[33496]
- X1-[37420]
- X1-[38861]
- X1-[46370]
- X1-[61968]
- X1-[65567]
- X1-[69823]
- X1-[70586]
- X1-[73428]
- X1-[76877]
- X1-[80118]
- X1-[83854]
- X1-[90429]
- X1-[90904]
- X2-[30305]
- X2-[52151]
- X2-[68201]

Command and Control - IRC



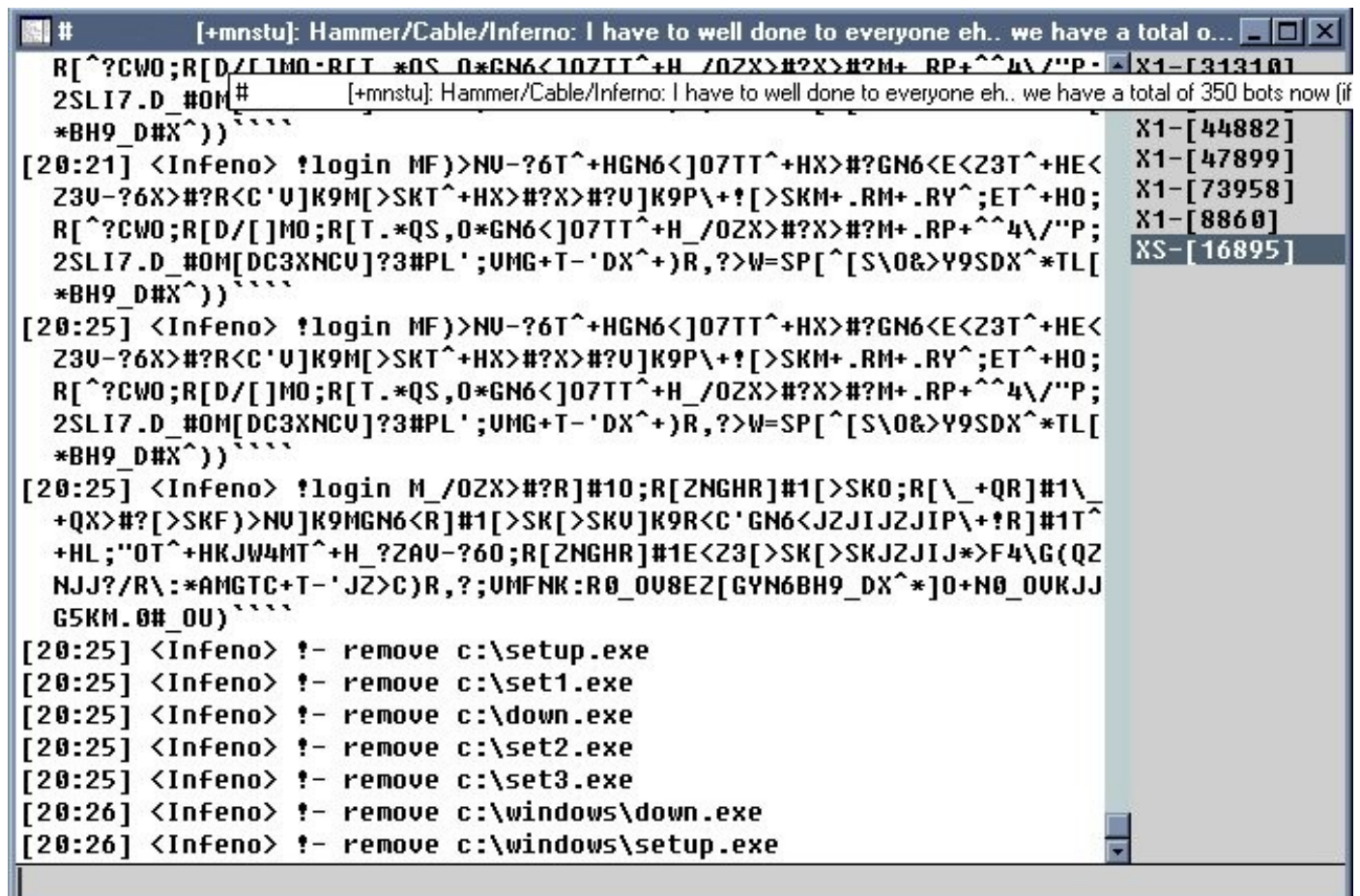
The screenshot shows an IRC chat window with a title bar that reads "[+mnst]: Well done. We reached the 200 infected...". The chat log contains the following text:

```
#
optushome.com.au) quit [04:24] # [+mnst]: Well done. We reached the 200 infected
< sigh> 64 bytes from 24.67.87.12: icmp_seq=57 ttl=112
time=363.636 ms
< sigh> 64 bytes from 24.67.87.12: icmp_seq=58 ttl=112
time=465.716 ms
< sigh> 64 bytes from 24.67.87.12: icmp_seq=59 ttl=112
time=737.483 ms
< sigh> wtf
*** X1-[73428] (~elvira@irc. .com-48114.buf.adelphia.
net) quit [04:24] Ping timeout
< sigh> !pepsi
< sigh> !login M\ _QM+.RY./BT^+HP\+IV]K9[>SKV]K9T^+H\_NF)
>NT^+H[>SKX>#?M+.RMV]K9HJ&?Y./BR<CJZJIP\+IGN6<S.O*T
^+HM[:UZNGHR<C'S.O*T^+HO.R[MD/[JL,"OD/[JKJW4T.*QS.O*
GN6<]D7TT^+H/_OZ>#?>#?M+.RP+^^4V"MP;2SLI7.D_#O[
DC3XNCV]?3#PL'VMG+T-&TL[+O[ZTL[+O[Y@P+^^JZJI&V]K9_
/OZ""
<X1-[13460]> Syntax: (!pepsi ip howmany size port, ie: !pepsi
127.0.0.1 1000 200 139)
<X1-[13460]> sigh` You are now authorized to use me...
*** XS-[84442] (uelizebetl@irc. .com-23329.ipt.aol.com
) join [04:25]
< sigh> !icmp 24.67.87.12 1000 1000
<X1-[13460]> IGMP Attack Started On < IP: 24.67.87.12 Amount:
1000 Size: 1000 >
< sigh> !login M\ _QM+.RY./BT^+HP\+IV]K9[>SKV]K9T^+H\_NF)
>NT^+H[>SKX>#?M+.RMV]K9HJ&?Y./BR<CJZJIP\+IGN6<S.O*T
```

On the right side of the chat window, there is a list of users with their nicknames and IDs:

- +Cable
- +sigh`
- +X1-[13460]
- X1-[15619]
- X1-[24148]
- X1-[24381]
- X1-[33094]
- X1-[33496]
- X1-[37758]
- X1-[38861]
- X1-[46370]
- X1-[53653]
- X1-[69823]
- X1-[70586]
- X1-[80118]
- X1-[83854]
- X1-[90904]
- X2-[30305]
- X2-[52151]
- X2-[6820]
- X2-[9793]
- XS-[12799]
- XS-[14769]
- XS-[16895]
- XS-[21283]
- XS-[21687]
- XS-[25692]
- XS-[28847]

Command and Control - IRC



```
# [+mnstu]: Hammer/Cable/Inferno: I have to well done to everyone eh.. we have a total o... X1-[31310]
2SLI7.D_#OM# [+mnstu]: Hammer/Cable/Inferno: I have to well done to everyone eh.. we have a total of 350 bots now (if
*BH9_DX^))
[20:21] <Infeno> !login MF)>NU-?6T^+HGN6<]07TT^+HX>#?GN6<E<Z3T^+HE< X1-[44882]
Z3V-?6X>#?R<C'U]K9M[>SKT^+HX>#?X>#?U]K9P\+! [>SKM+.RM+.RY^;ET^+H0; X1-[47899]
R[?CWO;R[D/[ ]MO;R[T.*QS,0*GN6<]07TT^+H_/OZX>#?X>#?M+.RP+^4\/'P; X1-[73958]
2SLI7.D_#OM[DC3XNCU]?3#PL';VMG+T-'DX^+)R,?>W=SP[^[S\O&>Y9SDX^*TL[ X1-[8860]
*BH9_DX^)) XS-[16895]
[20:25] <Infeno> !login MF)>NU-?6T^+HGN6<]07TT^+HX>#?GN6<E<Z3T^+HE<
Z3V-?6X>#?R<C'U]K9M[>SKT^+HX>#?X>#?U]K9P\+! [>SKM+.RM+.RY^;ET^+H0;
R[?CWO;R[D/[ ]MO;R[T.*QS,0*GN6<]07TT^+H_/OZX>#?X>#?M+.RP+^4\/'P;
2SLI7.D_#OM[DC3XNCU]?3#PL';VMG+T-'DX^+)R,?>W=SP[^[S\O&>Y9SDX^*TL[
*BH9_DX^))
[20:25] <Infeno> !login M_/OZX>#?R]#10;R[ZNGHR]#1[>SK0;R[\_+QR]#1\
+QX>#? [>SKF)>NU]K9MGN6<R]#1[>SK [>SKU]K9R<C'GN6<J2JIJ2JIP\+!R]#1T^
+HL;'OT^+HKJW4MT^+H_?ZAV-?60;R[ZNGHR]#1E<Z3 [>SK [>SKJ2JIJ*>F4\G(QZ
NJJ?/R\:*AMGTC+T-'JZ>C)R,?;VMFNK:R0_OU8EZ[GYN6BH9_DX^*]0+N0_OVKJJ
G5KM.0#_OU)
[20:25] <Infeno> !- remove c:\setup.exe
[20:25] <Infeno> !- remove c:\set1.exe
[20:25] <Infeno> !- remove c:\down.exe
[20:25] <Infeno> !- remove c:\set2.exe
[20:25] <Infeno> !- remove c:\set3.exe
[20:26] <Infeno> !- remove c:\windows\down.exe
[20:26] <Infeno> !- remove c:\windows\setup.exe
```

Command and Control - HTTP

- ◆ Provides simple interface for both the bots and the botmaster
- ◆ Advantages:
 - IRC not always allowed through corporate firewalls, HTTP almost always is
 - Web servers are found everywhere
 - Encryption (SSL)

Command and Control

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

sodis/bot/cmd.htm

WSLabs Vulnerabili... 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: <input type="text" value="http://"/>	LOCAL FILENAME: <input type="text" value="CA\"/>	PERSONAL COMMAND: <input type="text"/>	Submit
SHELL COMMAND	<input type="text"/>		PERSONAL COMMAND: <input type="text"/>	Submit
STORE SCREENSHOT IN LOCAL FILE	FILE: <input type="text"/>		PERSONAL COMMAND: <input type="text"/>	Submit
CHANGE URL FOR LOGS	<input type="text"/>		PERSONAL COMMAND: <input type="text"/>	Submit
URL THAT SHOULD BE BLOCKED	<input type="text" value="http://"/>		PERSONAL COMMAND: <input type="text"/>	Submit
CLEAR HOSTS FILE			PERSONAL COMMAND: <input type="text"/>	Submit

UPLOAD FILE	FTP: <input type="text"/>	LOCAL FILENAME: <input type="text" value="CA\"/>	FTP LOGIN: <input type="text"/>	FTP PASSWORD: <input type="text"/>	PERSONAL COMMAND: <input type="text"/>	Submit
-------------	---------------------------	--	---------------------------------	------------------------------------	--	--------

UPLOAD HOSTS FILE:

Submit ID:

Command and Control

- ◆ C&C interfaces starting to become more complex
- ◆ Dynamic DNS services often used
 - Service which allows changing the IP address of a hostname at will
 - Allows attackers to move their C&C servers quickly and easily

Command and Control

- ◆ More C&C interfaces emerging
- ◆ Phatbot/Nugache worm uses encrypted P2P network (WASTE)
 - Bots contact other peers, not central server
 - Much more difficult to find botmaster or shut down botnet



Technical Analysis - Dopebot

- ◆ Based on Agobot
- ◆ Written in C++ for Windows
- ◆ Source Code freely available, GPL'd
- ◆ IRC C&C
- ◆ Provides a number of typical bot features
- ◆ Can install as service or just auto-started

Technical Analysis - Dopebot

- ◆ Provides “security” in using the bot
 - Requires a password to use
 - Only specific IRC nicks may use it
 - XOR Obfuscation capabilities
- ◆ Configuration done within source code
 - + Only need to send one file to install
 - Have to recompile to make changes

Dopebot Configuration

```
//Daemon Settings
const char *ftpduser = "dopebot";
const char *ftpdpass = "dopebot";
const int ftpdport = 21;
const int tftpdport = 69;
//Install Settings
const char *filename = "svchost32.exe";
const char *regkeyname = "svchost32";
const char *servicename = "svchost32";
const bool useregistry = TRUE;
const bool useservice = FALSE;
//IRC Settings
serverlist servers[] =
{
    {"127.0.0.1", 6667},
    {"irc.dal.net", 6667},
    {NULL, 0}
};
const char *serverpassword = "dOpe";
const char *channel = "#dopebot";
const char *channelpassword = "pwn";
const bool useoschannel = FALSE;
//Security Settings
const char *botpassword = "hi";
const char *hostauth[] =
{
    "dope!",
    "\0"
};
const char *teakey = "jbeqtnab";
const int xorkey = 3;
//Sniffer Settings
```

Backdoor configuration

Installation settings

IRC C&C settings

Security settings

Obfuscation settings

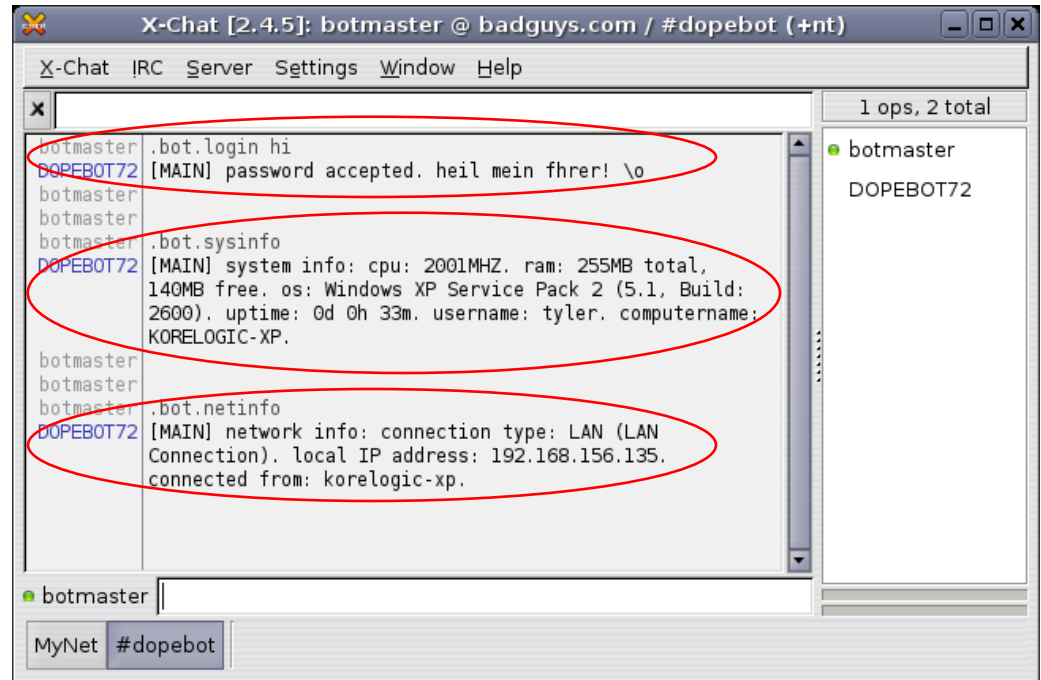
Dopebot Stealth Features

```
#define NO_FWB          //Disable Firewall Bypass Functions
#define NO_INJECTION    //Disable Library Injection Function
//-----
#define NO_SFC          //Disable SFC Disabling And Patching Functions
//-----
#define NO_9XHIDEPROC    //Disable Windows 9X Hide Process Function
#define NO_KERNELKIT     //Disable Kernel Kit Function
#define NO_REGPORT      //Disable Register Port Function
#define NO_SP2BYPASS     //Disable Windows XP SP2 Firewall Disable Function
#define NO_USERKIT      //Disable User Kit Function
..
```

- ◆ XP SP2 Firewall Bypassing
- ◆ DLL Injection
- ◆ System File Protection Disabling
- ◆ Process Hiding (Win 9X)
- ◆ User-level Rootkit
- ◆ Kernel-level Rootkit
- ◆ System Hardening
- ◆ Virtual Machine Detection

Dopebot - Bot Commands

- ◆ Bot commands given in IRC channel
- ◆ Commands are preceded by a prefix
 - “.” by default
- ◆ No spaces between prefix and command*
- ◆ Will take commands from channel topic as well



Dopebot – Exploit Propagation

- ◆ Can propagate through scanning and exploitation
 - LSASS overflow (MS04-011)
 - Optix Pro Trojan Master Password
- ◆ Internal source code makes it simple to add new exploits

```
botmaster .scan.start 192.168.156.1 lsass 0 5
DOPEBOT72 [SCAN] sequential exploitscan started on:
          192.168.156.1, exploit: lsass, delay: 0, threads 5.
```

Dopebot – Exploit Propagation

```
tyler@localhost:/var/log/snort/bak
File Edit View Terminal Tabs Help

[**] [1:2466:7] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
09/06-11:07:25.218877 192.168.156.135:1038 -> 192.168.156.2:445
TCP TTL:128 TOS:0x0 ID:132 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x9A377085 Ack: 0xBDF396AA Win: 0xF970 TcpLen: 20

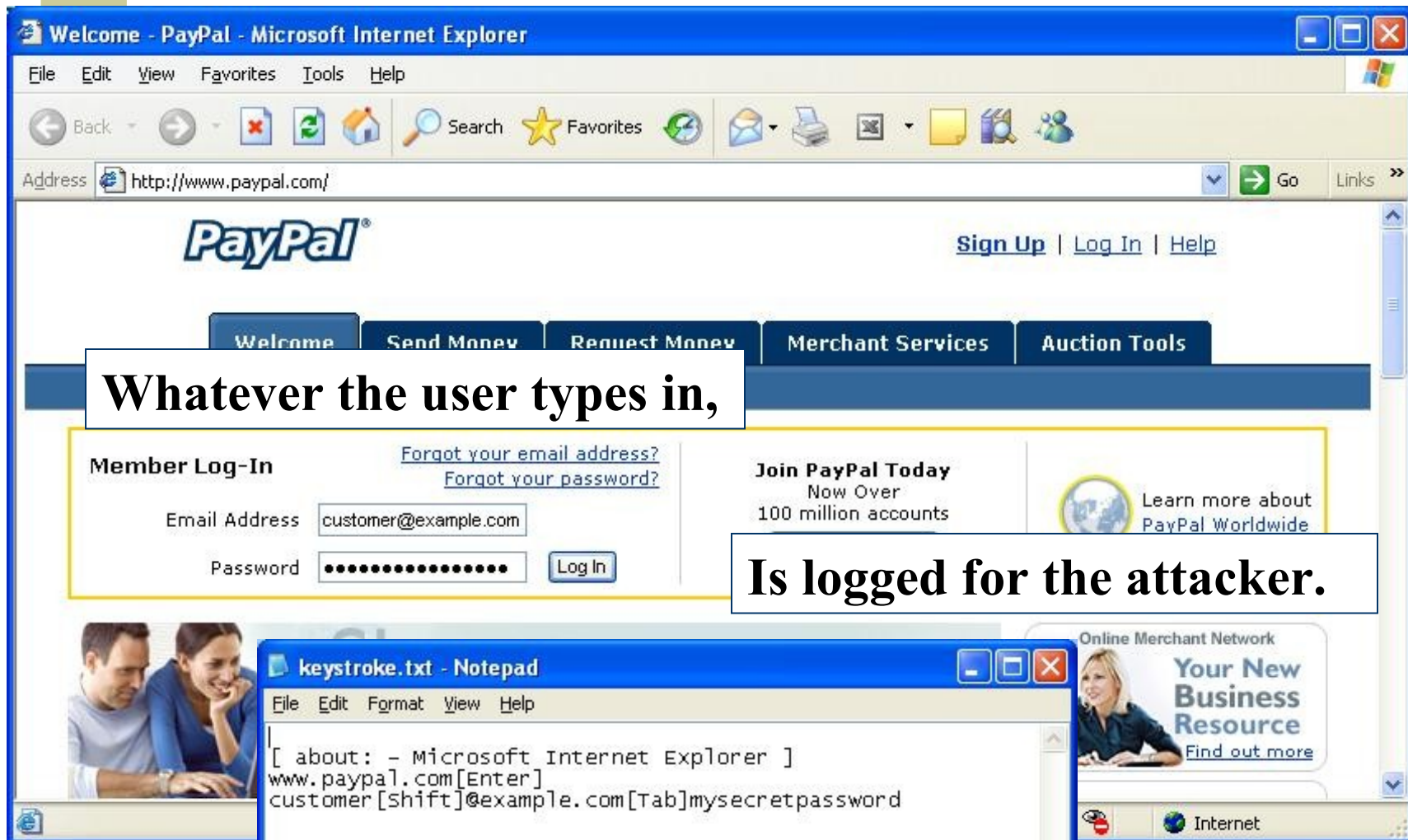
[**] [1:5219:2] NETBIOS SMB-DS lsass DsRolerUpgradeDownlevelServer unicode little
endian overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
09/06-11:07:25.232992 192.168.156.135:1038 -> 192.168.156.2:445
TCP TTL:128 TOS:0x0 ID:138 IpLen:20 DgmLen:1500 DF
***A*** Seq: 0x9A3782E9 Ack: 0xBDF397AA Win: 0xF870 TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS04-011.msp] [Xref =>
http://cgi.nessus.org/plugins/dump.php3?id=12205] [Xref => http://cve.mitre.org/cg
i-bin/cvename.cgi?name=2003-0533] [Xref => http://www.securityfocus.com/bid/10108]

localhost snort #
```

Dopebot – Keystroke Logging

- ◆ Comes with keystroke logging functionality
 - Useful for grabbing usernames, passwords, CC #, bank information, etc.
- ◆ Logs keystrokes to a hidden file on the system
- ◆ Performs logging by hooking the Windows keyboard events

```
botmaster|.keylog.start keystroke.txt
DOPEBOT72 [KEYLOG] keylog started (*WINDIR*\system32\keystroke.txt
).
```



Dopebot – Other Commands

- ◆ bot.login Login to the bot with a password
- ◆ bot.sysinfo Display bot system information
- ◆ bot.netinfo Display bot network information
- ◆ bot.info Display the bots version
- ◆ bot.raw Send the bot a raw IRC command
- ◆ bot.logout Logout of the bot
- ◆ bot.remove Remove the bot off of the compromised system

Dopebot – Other Commands

- ◆ ddos.bandwidth Flood a URL with traffic
- ◆ download.http Download a file from a URL and optionally run it
- ◆ download.update Replace the current bot with a downloaded file
- ◆ file.delete Delete a file
- ◆ file.execute Execute a file, can be hidden

Dopebot – Other Commands

- ◆ `file.open` Open a file on the remote computer
- ◆ `process.list` List currently running processes
- ◆ `process.kill` Stop a process (by name)
- ◆ `sniff.start` Start the network sniffer
- ◆ `sniff.stop` Stop the network sniffer



Detection and Response

Detection Methods

- ◆ No single method
- ◆ Use defense in depth
- ◆ Watch anti-virus/anti-spyware logs
 - Many bots are caught by anti-virus
 - Not a 100% fool-proof plan
- ◆ Monitor firewall logs for C&C traffic
 - Watch FW logs for both allowed and denied connections to common C&C services
 - IRC (TCP 6667), P2P (varies), odd ports

Detection Methods

- ◆ Use IDS to watch for:
 - IRC/P2P/Botnet activity
 - Attacks and DoS traffic coming FROM your network
- ◆ Network flow analysis
 - Watch for increase in traffic
 - Unusual traffic patterns
- ◆ Your users

IDS Example Alert

[**] [1:2001584:6] **BLEEDING-EDGE VIRUS Bot Reporting Scan/Exploit** [**]

[Classification: A Network Trojan was detected] [Priority: 1]

09/06-11:03:05.276438 **192.168.156.1:6667 -> 192.168.156.135:1036**

TCP TTL:64 TOS:0x10 ID:35834 IpLen:20 DgmLen:125 DF

AP Seq: 0x4F1A5097 Ack: 0x7A6E6985 Win: 0x25B0 TcpLen: 20

[Xref => <http://www.nitroguard.com/rxbot.html>] [Xref =>
<http://cert.uni-stuttgart.de/doc/netsec/bots.php>]

09/06-11:03:05.276438 0:50:56:C0:0:8 -> 0:C:29:27:DF:FF type:0x800 len:0x8B

192.168.156.1:6667 -> 192.168.156.135:1036 TCP TTL:64 TOS:0x10 ID:35834 IpLen:20
DgmLen:125 DF

AP Seq: 0x4F1A5097 Ack: 0x7A6E6985 Win: 0x25B0 TcpLen: 20

3A 62 6F 74 6D 61 73 74 65 72 21 7E 74 79 6C 65 :botmaster!~tyle

72 40 31 32 37 2E 30 2E 30 2E 31 20 50 52 49 56 r@127.0.0.1 PRIV

4D 53 47 20 23 64 6F 70 65 62 6F 74 20 3A 73 63 MSG **#dopebot :sc**

61 6E 2E 73 74 61 72 74 20 31 39 32 2E 31 36 38 **an.start 192.168**

2E 31 35 36 2E 30 2F 32 34 20 6C 73 61 73 73 20 **.156.1 lsass**

30 20 35 0D 0A **0 5..**

You've detected it, now what?

- ◆ Begin incident response
 - Treat it like a virus infection
- ◆ First priority is removal of malware
- ◆ If possible, determine how it got on
 - This will help prevent further infections
- ◆ Prevent it from happening again
 - Patch, user awareness, etc.

Advanced Response

- ◆ Can you get forensic information on the malware?
- ◆ Got a copy of the executable?
 - Submit it to anti-virus vendors
 - <http://www.virustotal.com>
- ◆ Command and control information?
 - Send it to the Shadowserver Foundation, ISC Handlers

DO NOT CONNECT TO THE C&C CHANNEL!

Roadmap to Botnet Prevention

- ◆ Patch, patch, patch
 - Both workstations AND servers
 - Bots were using MS06-40 exploits 2 days after patches were released
- ◆ Teach users safe computing habits
 - Safe browsing habits
 - Not running unknown files will help prevent bot infection
- ◆ Maintain up to date anti-virus signatures
 - Its not 100% effective, but important!

Why should you care?

- ◆ Bot infections can be costly
 - Cleaning up 1 infection is easy. How about 1,000?
- ◆ Better understanding = better protection
- ◆ Botmasters are organized. We need to be as well.



[RULES] -

1. do not ever tell anyone about this site and group.
2. do not ever leak any shit to any person outside of group.
3. any exe's that you compiled from this source code is for your use only.
4. exe's should be kept to yourself.
5. if you have friend who wanting to give you bots. give them your other bot like sdbot.



results of not following those rules:

- being worked for life from us.
- your sites will be reformatd.

The Future of Botnets

- ◆ Attackers are going to get better
 - Evron/Vixie argument
- ◆ More complicated botnets will appear
 - More encryption, harder to track C&C
- ◆ Flash botnets?
 - July 2006 – MySpace ad infection “a million users”
 - Only installed ad-ware, but what if it installed a bot?

Additional Resources

- ◆ Know Your Enemy: Botnets
 - <http://www.honeynet.org/papers/bots>
- ◆ Swatit Botnets Resource
 - <http://swatit.org/bots>
- ◆ Shadowserver group
 - <http://www.shadowserver.org>
- ◆ Google
 - bots, botnets, botmaster, “command and control”



Thank you!

Any questions?

thudak@korelogic.com

<http://www.korelogic.com>

<http://www.hudakville.com/infosec>