CERT

Botnets as a Vehicle for Online Crime

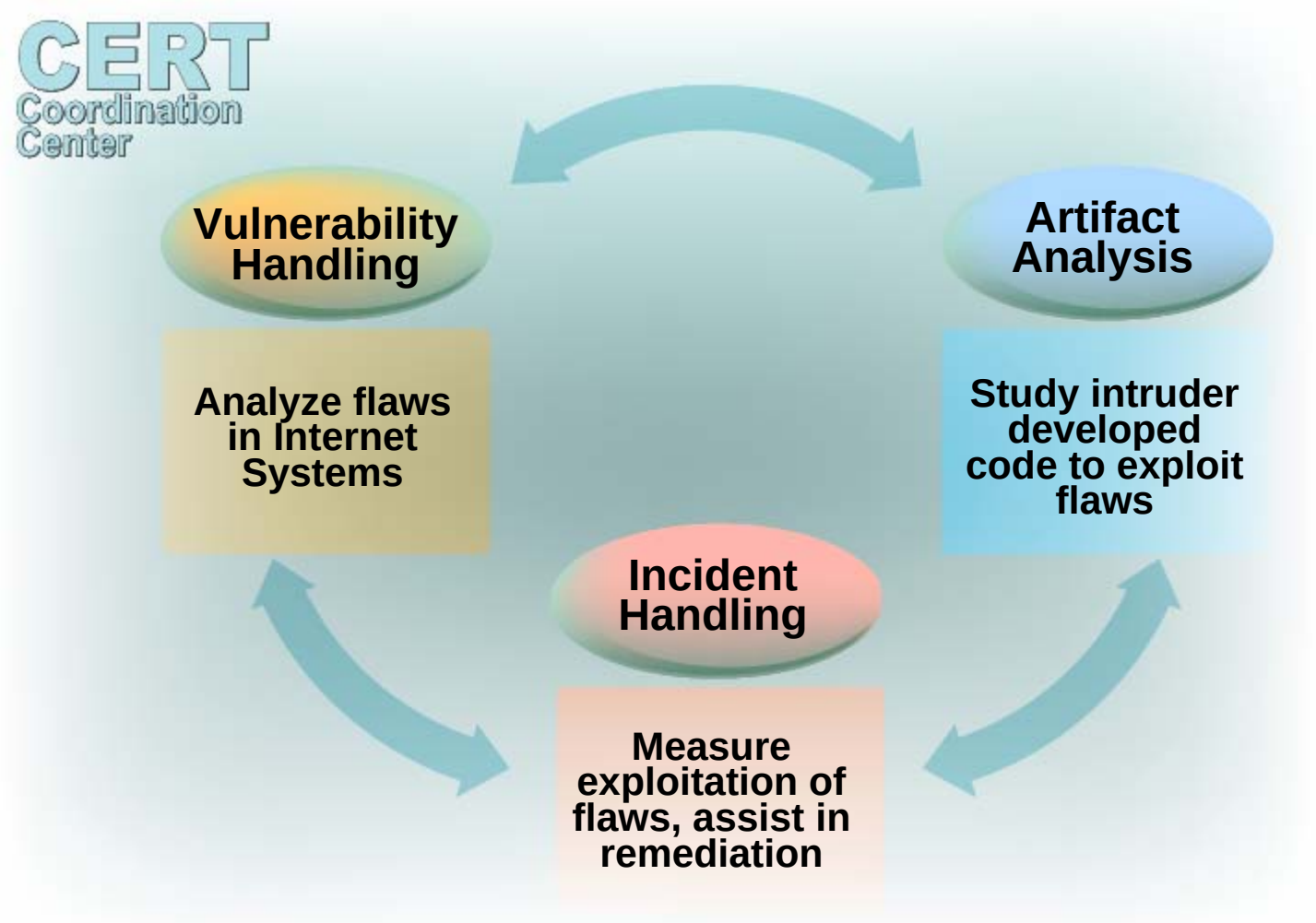
Aaron Hackworth
Nicholas Ianelli

Software Engineering Institute

Agenda

- Overview of CERT®/CC
- How botnets are built
- What capabilities botnets possess
- How botnets are operated
- How botnets are maintained and defended
- Tracking Botnets and Bot Herders

CERT®/CC Teams



What You Need To Understand

- It is about the underground economy
  - Information Theft
  - Extortion
- It is about the money
- Malware and malicious techniques evolve as quickly as necessary to maintain or create new revenue streams
- The Underground Motto…
  ”Just enough is good enough”

CERT

How Botnets are Built

Building from scratch

- Vulnerability exploitation
  - Scan
  - Exploit

- Social Engineering
  - Collecting a target list
    - Web Client Attacks
    - Email Attacks
    - Instant Messaging Attacks

Hijacking, Purchasing, Trading

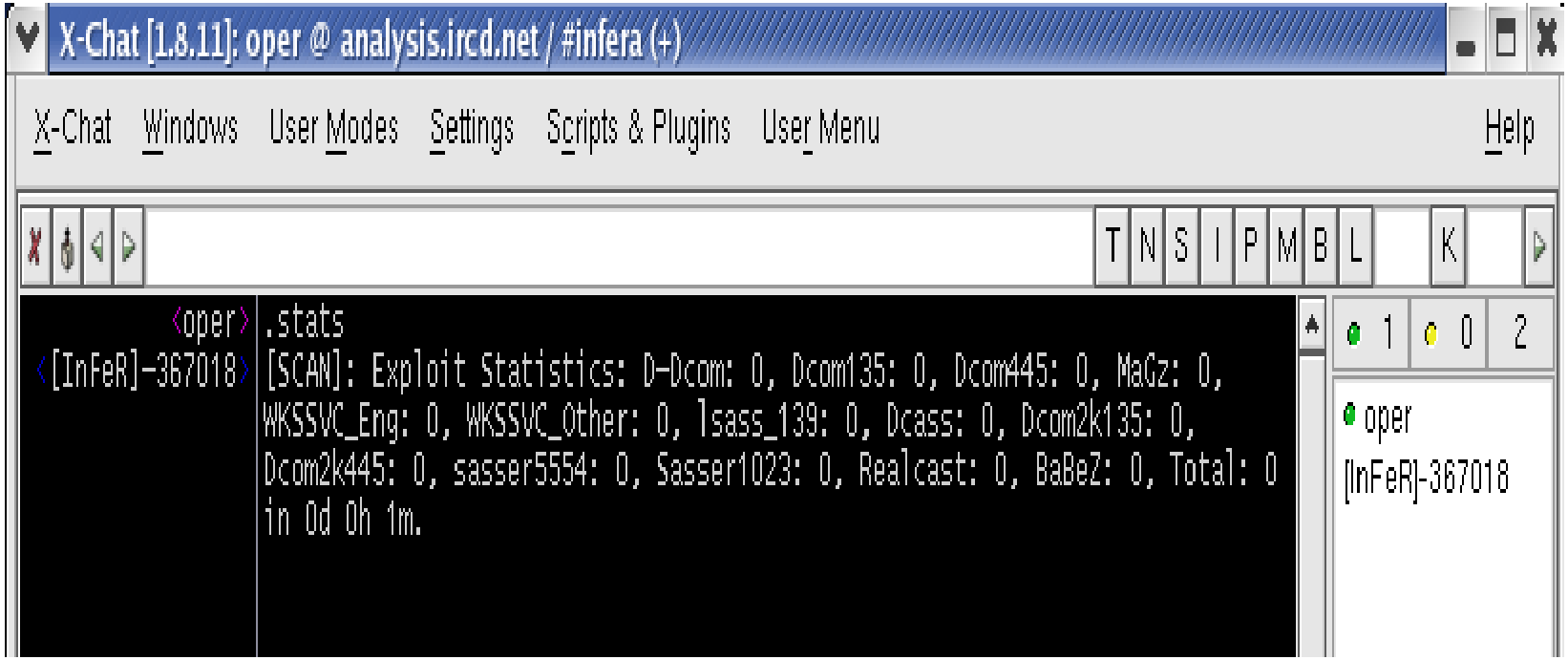
- Hijacking
  - Many botnets include packet sniffers
- Underground economy
  - Purchase
  - Trade

CERT

Botnet Capabilities

Botnet capabilities

- Scanning/Autorooting

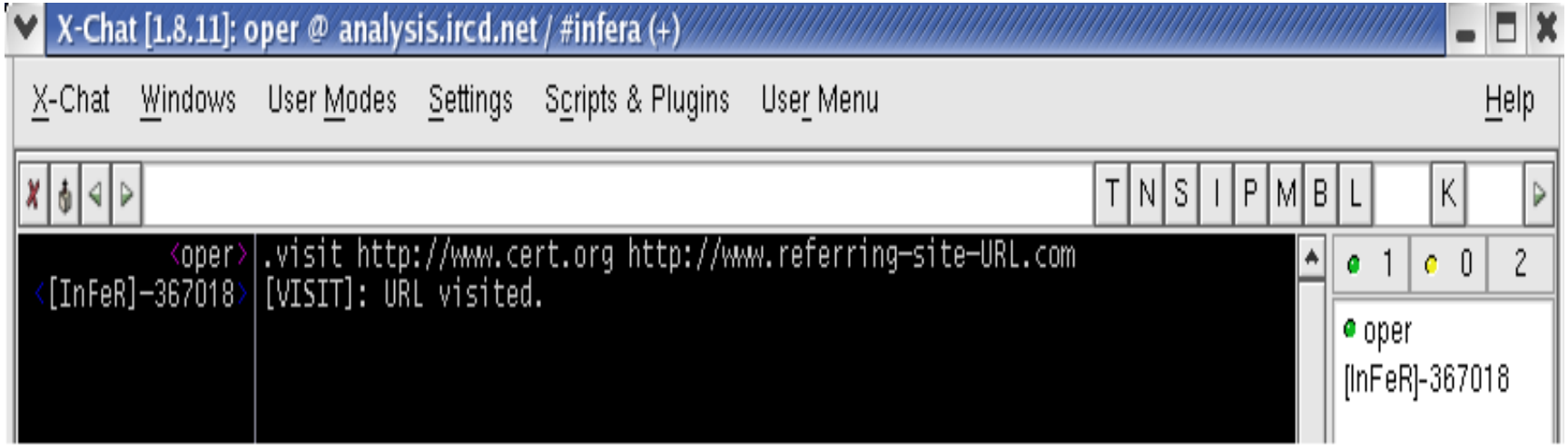


Botnet capabilities (2)

- DDoS
  - Extortion
- Download and Installation
  - Malicious Executables
  - Spyware/Adware

Botnet Capabilities (3)

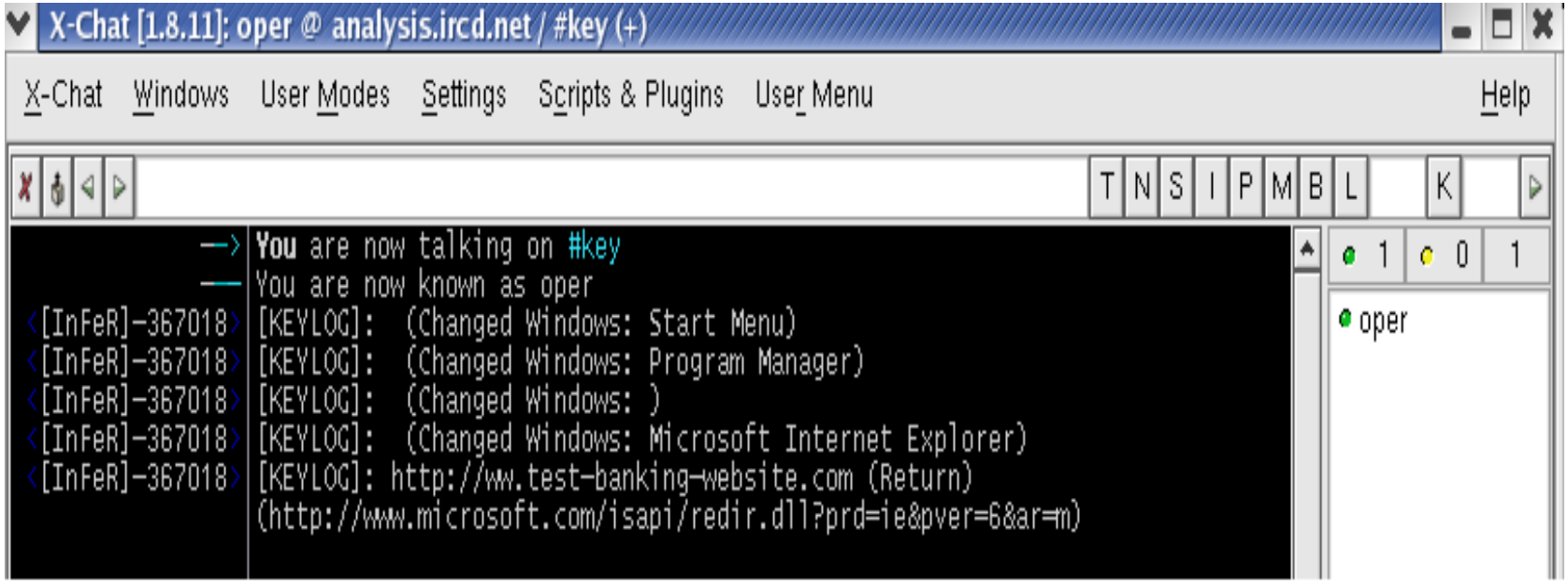
- Click Fraud
  - Generate revenue with ads and affiliates



Botnet capabilities (4)

Spyware Features – Keyloggers and Screenshots

- Key logging/screen captures
  - Credit card information
  - Authentication credentials
  - Personal information useful for identify theft



Botnet capabilities (5)

Spyware Features – Data Theft

- Searching and Stealing Data
  - File system
  - Registry
  - Copying clipboard content
- Searching for ICQ buddy file location and enumerating the contents
- Searching for the Windows Address Book file and enumerating its contents

Botnet capabilities (6)

Spyware Features – Email and Contact Theft

- Searches files and registry for known formats or pattern matching

- Some commonly searched file extensions include:
  - .asp
  - .dhtm
  - .doc
  - .htm
  - .html
  - .xml
  - .js
  - .msg
  - .php
  - .rtf
  - .txt
  - .vcf
  - .wab
  - .xhtm

Botnet capabilities (7)

Spyware Features

- Windows Protected Storage
  - Outlook passwords
  - Passwords for websites
  - MSN Explorer passwords
  - Internet Explorer AutoComplete passwords
  - Internet Explorer AutoComplete field

Botnet capabilities (8)

Packet Capture

- bool IsSuspiciousBot(const char *szBuf) – looks for keywords related to bot activity.
  - ":.login“
  - ":!Login“
  - ":.secure
- bool IsSuspiciousFTP(const char *szBuf)
  - looks for FTP credentials triggered by keywords such as USER and PASS.
- bool IsSuspiciousHTTP(const char *szBuf)
  - attempts to gather HTTP based authentication credentials and other valuable data
    - "paypal“
    - "paypal.com“
    - "Set-Cookie: "
- bool IsSuspiciousVULN(const char *szBuf)
  - looks for keywords that indicate vulnerable server versions
    - "OpenSSL/0.9.6“
    - "Serv-U FTP Server“
    - "OpenSSH_2"

Botnet capabilities (9)

Server Class Services

- Phishing sites
- Web pages where infected systems can log their infection status
- Malware download sites
- Spyware data drop off sites
- Bot command and control sites

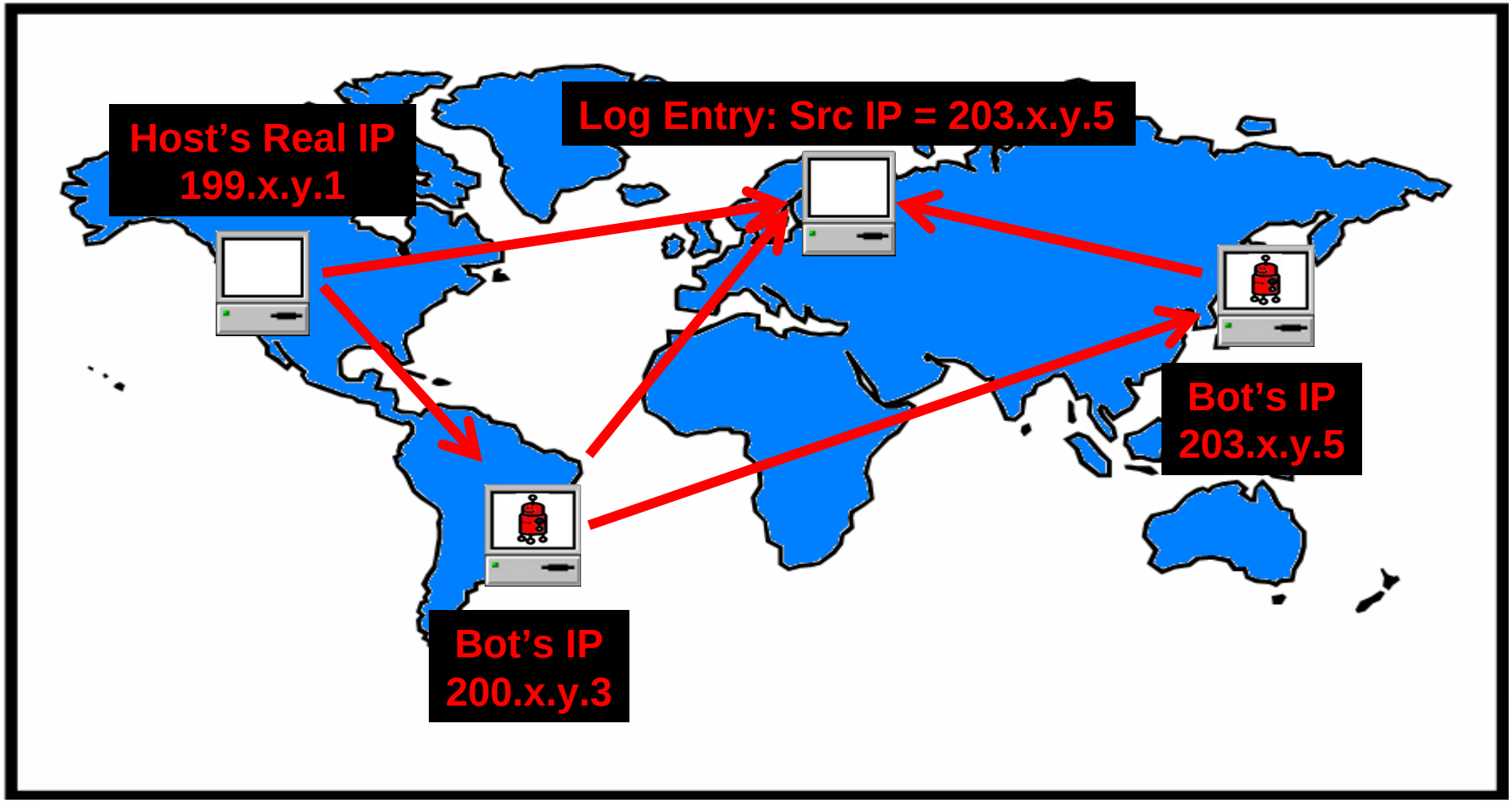
Botnet capabilities (10)

Proxies

- Gateway and proxy functionality
  - Generic port redirection
  - HTTP proxy
  - Socks proxy
  - IRC bounce
- Common Uses of Proxies
  - Relaying Spam
  - Hiding Attacker Identity
  - TCP Relay to Hide Infrastructure
    - Hide C&C Servers
    - Hide Phishing Websites

Botnet capabilities (11)

Proxy Network Flow



CERT

Botnet Operation Management and Defense

Software Engineering Institute

How botnets are operated

: 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)

IRC Topic for Botnet Command and Control

2 Channel Operators
52 compromised hosts currently connected to this botnet

Randomely generated username

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

/who information on a particular user

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

2 ops, 52 total

FRA|69031
FRA|93381
KOR|18185
NOR|68153
NOR|86753
NOR|96233
POL|74747
RUS|10552
RUS|16220
RUS|21312
RUS|31707
RUS|39839
RUS|40129
RUS|57765
RUS|62579
RUS|63892
RUS|90332
SWE|11601
TWN|23399

USA|08884

Direct client-to-client
CTCP
Oper
Mode
Ignore
Kick/Ban
Info
External
Open Dialog Window

USA|35687

Quazie #num3

How botnets are operated (2)

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http:/[redacted]/script/socks/

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

IP Address of compromised host

Socks Proxy port compromised host is listening on

Is the compromised host connected: 1 = True 0 = False

Randomely generated Machine ID

List

IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION
Copy IP [redacted]179.202	58197	Copy ID IKIHIEFBPRGGAAKHCUUPFUQSJIVZYUH	United States	San Jose	CA	1
Copy IP [redacted].20.196	34104	Copy ID MBPLJVYVBSGXEPIVRMAXPDVHERDJAAI	United States	Herndon	VA	1
Copy IP [redacted].0.34	22474	Copy ID GVPWSDZNABSEYKAEIZRVCMZMJKLXDPR	United Kingdom	Nottingham		1
Copy IP [redacted].162.161	59694	Copy ID GSCIYTQWUSZVUPKRSFKIHUNQHVKBVZC				1
Copy IP [redacted].0.34	27750	Copy ID OIXTGWOELLBRVOBFDLJIZJVNDRZITRD	United Kingdom	Nottingham		1
Copy IP [redacted].15.22	47130	Copy ID BOJQMWWOZNHGDHQWXFXXSIYRKCGIALO	Canada	Toronto		1
Copy IP [redacted]240.3	11902	Copy ID CFJEEWVUENSLXGRWKGODTHFSQAYPZQL	Ireland	Dublin		1
Copy IP [redacted]160.7	15591	Copy ID DHTLNBHISTVKGHKVQEVEGTCPTYUANEC	United Kingdom	Baguley		1
Copy IP [redacted]94.220	55939	Copy ID TDJKLONNUHWYLXZVPJBSKSLUCYPKTNO	United Kingdom	Ipswich		1
Copy IP [redacted]118.252	51371	Copy ID KLRNWCVGVFRNYNFMNKFNCWQDUTCMBHO	United States	Atlanta	GA	1
Copy IP [redacted]135.241	49127	Copy ID SGJPQPEWOVJZLATCTKROAIDBQZGBBPM	United Kingdom	Ipswich		0
Copy IP [redacted]109.92	22065	Copy ID ENZGHVOKCWNCPKEERFOEBQWNRDKGEPN	Canada	Calgary		1

Total: 44

Physical location of compromised host, with image of their national flag

Total number of bots being controlled by this C&C

Send socks list on email: Submit

Generate socks list for spam from current online socks: Submit

Mark socks ID as USED: Submit

Done

How botnets are operated (3)

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http:/[redacted]socks/bot/cmd.htm

Go

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:	

UPLOAD HOSTS FILE:

Submit ID:

Done

CERT

How botnets are operated (4)

- Peer-to-Peer
  - Phatbot
    - WASTE Protocol
  - Instant Messaging Networks
  - Sinit (Update)
  - Nugache

- DNS
  - Kaminsky
  - Used by everyone

Botnet Maintenance and Defense

- DNS
- Modifying the Command Language
- Disabling security applications and updates
- Authentication

Botnet Maintenance and Defense (2)

- SSL
- Binary obfuscation
- Customized IRCds

Botnet Maintenance and Defense (3)

Obfuscation:

- Techniques that do not require key material to return clear text data
  - Can be understood through code analysis
  - Examples Include XOR, ROT13, BASE64 …
- Techniques that require key material that is present to return clear text data
  - Symmetric key cryptography
- Techniques that require key material that is not present to return clear text data
  - Public key cryptography or symmetric key cryptography where the key is somehow not present in the malware

Botnet Maintenance and Defense (4)

Malware starts a thread that executes an infinite loop similar to the ProcessKill function shown below:

```
const char *ProcessnamesToKill[18] = { "msblast.exe", "tftpd.exe", "penis32.exe",      // W32.Blaster.Worm variants
                                       "index.exe", "root32.exe", "teekids.exe",
                                       "mspatch.exe", "mslaugh.exe", "enbiei.exe",
                                       "worm.exe", "lolx.exe", "dcomx.exe",            // Backdoor.IRC.Cirebot
                                       "rpc.exe", "rpctest.exe“,
                                       "scvhost.exe", "bot.exe",                       // common trojan filenames
                                        NULL};
```

Pseudo Code to represent ProcessKill

```
{
Infinite_loop {
    for each process in running process {
        if process in ProcessnamesToKill array {
            terminate the process
            delete the file associated with the process
        }
    }
    pause for 1.5 seconds
} // restart loop (infinite_loop)
```

Botnet Maintenance and Defense (5)

- Rootkit and Anti-Analysis Techniques

```
hFile = CreateFile( "\\\.\NTICE",
                    GENERIC_READ | GENERIC_WRITE,
                    FILE_SHARE_READ | FILE_SHARE_WRITE,
                    NULL,
                    OPEN_EXISTING,
                    FILE_ATTRIBUTE_NORMAL,
                    NULL);

if( hFile != INVALID_HANDLE_VALUE )
 {
   CloseHandle(hFile);
   return TRUE;
 }

return FALSE;
```

Attempt to open a handle to SoftICE driver

If successful, return TRUE to indicate SoftICE is running

Tracking botnets and bot herders

- Analysis of malware
  - Run Time
  - Reverse Engineering
- Analysis of network traffic
  - Router / IDS / Firewall logs
  - Packet captures
  - Work with ISPs
- Follow the money trail
  - Watch the physical world
  - Tracking payments related to affiliate ID
    - ID can be recovered via malware analysis
    - Affiliate ID can be hidden by layers of loaders

Questions or comments

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA
Hotline: +1 412 268 7090

CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989
Web: http://www.cert.org/
Email: cert@cert.org