



# Criminal Computer Intrusion Unit

Erkan A. Chase  
Chief  
Criminal Computer  
Intrusion Unit





# CCIU Mission

- Provide administrative and operational support and guidance to field offices investigating criminal computer intrusions which have an impact upon the National Information Infrastructure of the United States.
- The Strategic goal of CCIU is to identify and neutralize the most significant individuals or groups
  - conducting computer intrusions
  - disseminating malicious code
  - performing other computer related crimes



# CCIU Initiatives

- Identify significant domestic and international groups developing BOT networks for the purpose of conducting criminal activity on the Internet.
- Identify disrupt significant Eastern European hacking groups targeting U.S. e-commerce sites.
- Identify significant domestic and international malicious code writers who are conducting criminal activity on the internet, in an effort to disrupt their activities and dismantle their groups.
- Identify significant domestic and international groups targeting U.S. PBX systems

# Private Branch Exchange (PBX)

- These compromises involve three different schemes:
- Scheme 1 - Hackers compromise a Voice Mail System (VMS) and change the greeting of the voice mail to say something to the effect of "Hello, yes, yes, yes", which allows for a collect call to automatically be accepted whenever the automated operator is used. Once the collect call is accepted, the hacker can then make an international call through the compromise of the private branch exchange (PBX) or make a call to another compromised PBX.

# Private Branch Exchange (PBX)

- Scheme 2 - Intruder gains unauthorized access to a VMS, usually through the use of the default password, then configures the system to automatically dial out (page out) to the Philippines when a message is left in the voice mail box. The intruder then leaves a nonsense message in the box to trigger the outdialing. The intruder creates several mailboxes, thereby allowing the system to call the programmed number every minute, causing a denial of service attack. This scheme could easily target critical numbers in the United States such as 911 systems.

# Private Branch Exchange (PBX)

- Scheme 3 - International fraudulent calls are made, which connect to a local access number at an ISP, thereby giving the caller free Internet service in which the subject could easily use to conduct computer intrusions. In these cases it would be difficult to trace the intrusion due to the difficulty in tracing these fraudulent callers.



# Intelligence Initiatives

- Collect and evaluate intelligence received from U.S. based and extra-territorial sources operated by the field.
  - CIS sources are well placed professionals in the IT industry (anti-virus and network security communities)
  - Criminal subjects now cooperating with the FBI.
- Coordinate the collection of intelligence to efficiently utilize and leverage resources available to the U.S. government.
- Disseminate intelligence in accordance with policy and procedures established by the Office of Intelligence.



# CCIU Liaison

- Anti-Virus Community

- A. McAfee, Symantec, Message Labs, Computer Assoc., Microsoft, F-Secure, Sophis, etc.....

# Identity Theft

- Over the past year approximately 32 universities reported vulnerabilities which led to network compromises.
- Example of media reports featuring Universities.



# DDoS Major Case

- Since April 2004, 28 victims of DDoS extortion across 14 divisions
- Subjects use similar email addresses, sign communications with different names, and use different IP addresses to send email
- Method typically begins with a DDoS attack followed by an email or, if the victim has a chat client on its website, the subject enters the chat and makes threat
- One email address in particular was used in DDoS extortion cases in the US, Canada, and UK
- CCIU is coordinating with RCMP and NHTCU



# Bot Major Case

- In January of 2003, an FBI investigation was centered around a group of individuals that were launching DDoS attacks against entities on the Internet.
- One individual owned and operated a web hosting provider in the basement of his house.
  - some of the clients were legitimate, including IRC servers
- Forensic analysis of the victims' logs lead the FBI to a UK subject using an IRC channel hosted by an Ohio based Web Hosting Company.
- UK subject commanded an army of 20,000 – 50,000 bots - infected with of SDbot and Agobot



# Bot Major Case

- During 2003, individuals from this group launched numerous DDoS attacks driving the entities to the Ohio based web hosting Co. for protection.
- FBIHQ coordinated with New Scotland Yard on the arrest and interview of the UK subject. UK subject implicated the owner of Web hosting provider in Columbus, Ohio.
- On February 14, 2004, "Cyber St. Valentine's Day Massacre", the FBI executed a search warrant on the Ohio based web hosting Co. Over 299 systems were seized, the largest takedown in FBI cyber history.



# Bot Major Case

- FBI determines that the Ohio based web hosting Co. administrator had hired DDoS henchmen to launch attacks against entities on the Internet.
- One of these henchman has been identified and turned into a cooperating witness targeting a 20-member malicious code development team responsible for Sasser, Agobot, phatbot, and Sdbot.
- To date, six search warrants and one arrest in Germany have been conducted.



# Bot Major Case Investigation Continued

- The Columbus individual owned and operated a web hosting provider in the basement of his house. Some of the clients were legitimate, including IRC servers.

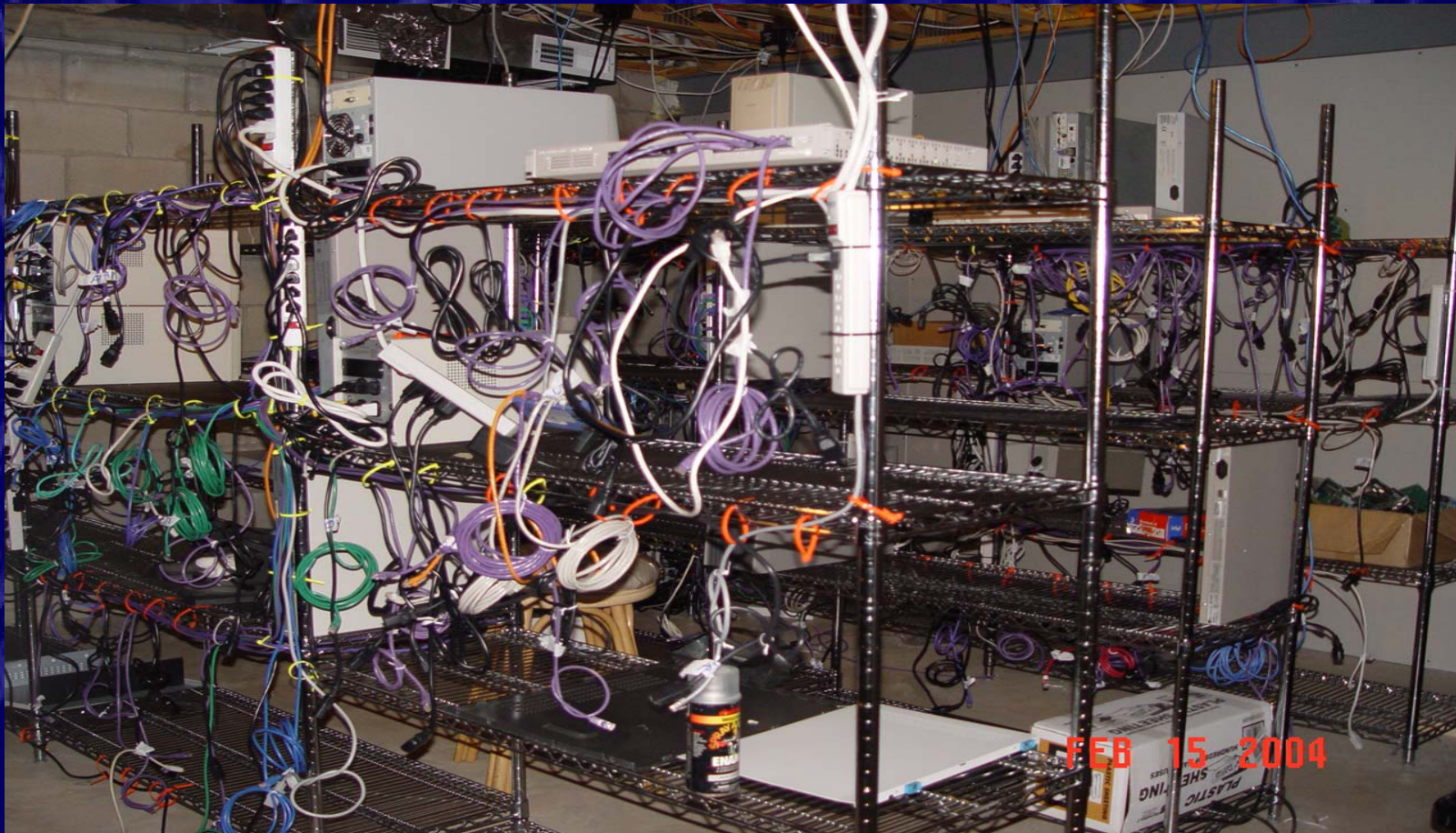


- On February 14, 2004, “Cyber St. Valentine’s Day Massacre”, the FBI executed a search warrant on Foonet. Over 299 systems were seized, the largest takedown in FBI cyber history.

Unclassified



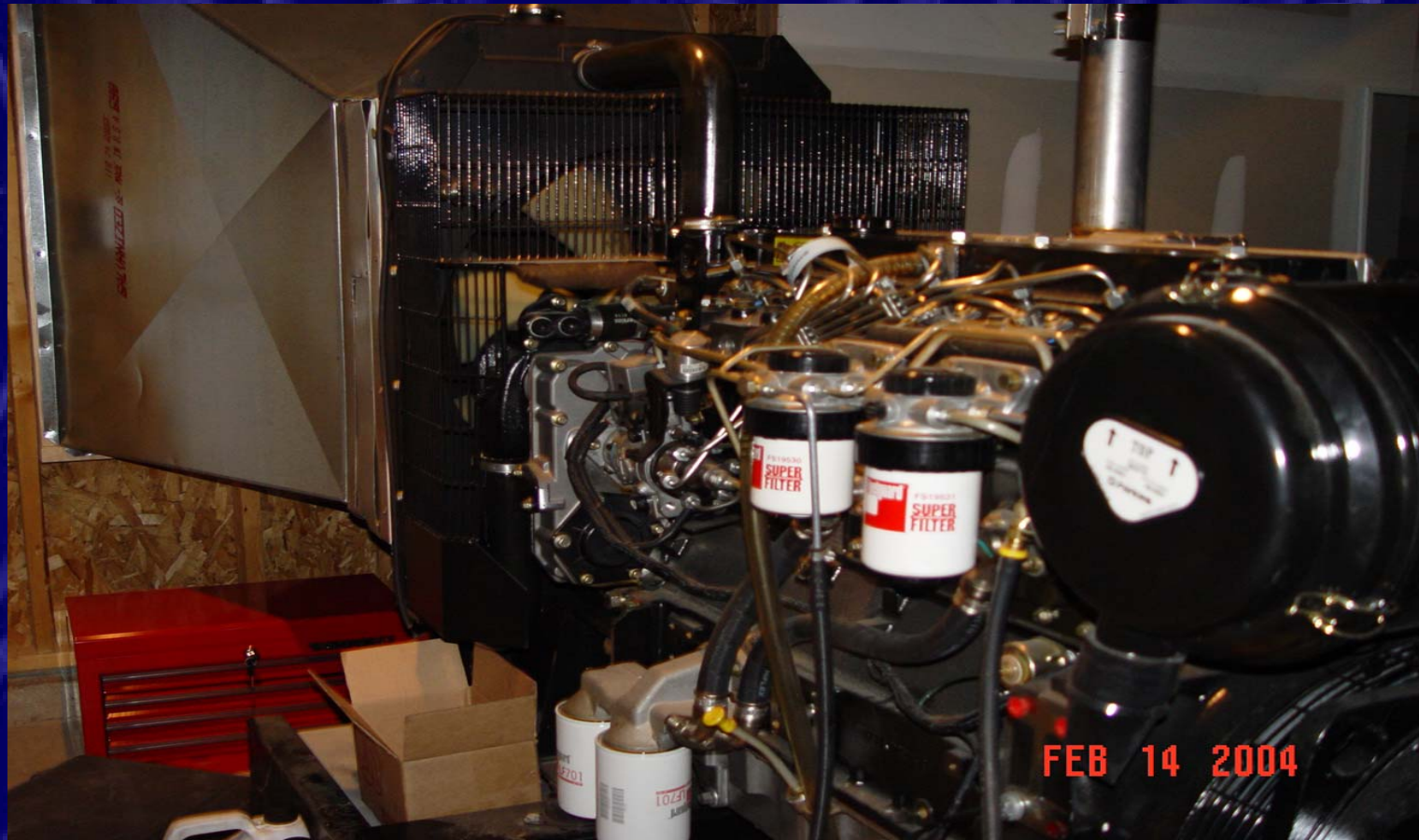
# Bot Major Case Investigation Continued



Unclassified



# Bot Major Case Investigation Continued



Unclassified



# Intrusion Major Case

- From Jan-Mar 2004 a subject identified to reside in Sweden hacks into US based National Laboratories, multiple military installations, a National Research Facility, and US based Supercomputing Centers. (IDG News Service, April 14, 2004)
- Subject claims responsibility for the intrusion. (IDG News Service, May 18, 2004)



# Intrusion Major Case

- On 20 August 2004 CCIU combined eight separate investigations, creating a Major Case.
- This case has required the cooperation of ten field offices, six Legats, 13 federal agencies and organizations working as a unified task force.
- Sweden Subject compromised 2000-4000 .edu, .gov, and .mil computers worldwide, beginning as early as November 2003. He used valid usernames and passwords sniffed from trusted relationships.
- English subject was arrested in connection with the Cisco theft and the Swedish subject was arrested in Sweden for intrusions he committed within his own country.
- To date, no known sites containing classified information have been compromised.



# Carding Major Case

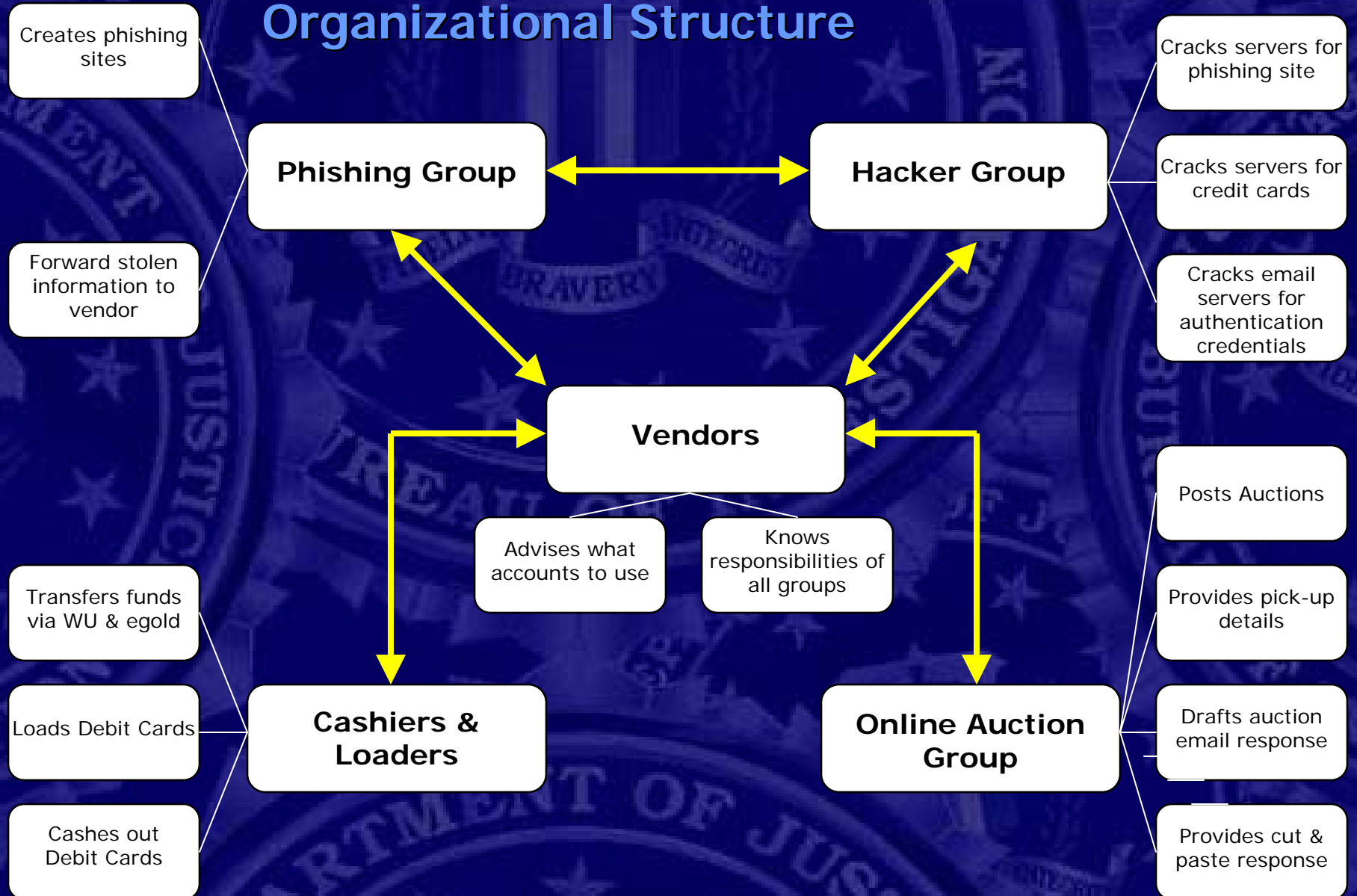
- Eastern European Subjects compromised numerous computer networks, stealing data and subsequently extorting the victim companies to ensure silence.
- 52 cases
- 28 FBI Field Offices.
- Consolidated into Major Case.
- Over 100 victim companies in 20 states.
- An estimated thirty million credit card accounts, including personal information were compromised.
- The stolen information was released whether victim company paid the subjects through online transfers or refused the extortion demands.



# Carding Major Case

- Even after stolen information was posted on the web by the subjects, roughly half of the victim companies continued to deny that their networks had been compromised.
- Subjects utilized well publicized vulnerabilities for which patches were readily available.
- Damages are conservatively estimated at 15 billion dollars.
- Two subjects lured from Russia. One subject voluntarily surrendered to US Law Enforcement. Two subjects prosecuted in Belarus.
- Established continuing relations with Cyber investigators in numerous Eastern European Countries.
- FBI targets, Romanian Criminal Enterprise

# Romanian Criminal Enterprise Organizational Structure





# Malicious Code

- Analysis Objectives
- Phases of Analysis
- Cycle of Malicious Code
- Top 20 Computer Threats by SANS Institute



# Analysis Objectives

What is the author's skill level??

What does the code do??



When was it written??

Who wrote the code??

What OSs are affected??

What is the purpose??

What is the author's maturity level??



# Phases of Analysis

- Static Analysis and Dynamic (Run-Time) analysis
- During Static analysis forensic examiner can identify if there are any obfuscations techniques being deployed such as: compression, encryption, anti-disassembly and debugging
- During Dynamic run-time analysis the forensic examiner can monitor: I/O connections, network traffic, and registry modifications.
  - Shows which files are created, copied, or accessed, and/or deleted
  - Shows active connections associated with suspected malicious code
  - Shows which registry keys are created and accessed



# Static Analysis

```

sobig-f.vxe
00 87C0: BC 6F D9 3B 6C FA 90 28 D8 18 82 F3 0F 73 0A 37 .o.;l..(.....s.7
00 87D0: 3D 4C 37 2F 43 F1 2C 23 85 9F AF EB 2C AB 3E FA =L7/C.,#.....>.
00 87E0: 32 62 94 4E 00 3A D3 2F 36 70 55 AA D7 07 9E 46 2b.N.:./6pU...F
00 87F0: 94 32 FE EA 27 34 77 A8 F2 70 B2 03 C9 53 2D 9E .2..'4w..p...S-.
00 8800: 3B 99 64 D6 BF 6F 1A B4 D0 CF 2F 7B 49 28 70 3E ;.d..o.../{I(p>
00 8810: EA B5 DE 85 6B 8F 9F F3 78 E7 E4 77 DF BE EC 7C ....k...x..w...|
00 8820: 76 3B CD C3 D0 9A D9 74 1B A3 0A 98 3C E0 DD C8 v;.....t....<...
00 8830: 36 94 50 ED D0 9B 00 E1 33 74 AF AC E3 9F 7D 26 6.P.....3t....}&
00 8840: F3 0A 18 67 12 22 EE 3B 0E 90 68 C3 1D E8 7A D6 ...g.".;..h...z.
00 8850: 29 F7 AB CD 49 3B FF 05 F4 77 F8 0A F8 22 2A D8 )...I;...w..."*
00 8860: 50 F6 DB FD 4F F6 3A 2B EA 17 80 15 E4 E3 84 45 P...O.:+.....E
00 8870: A1 09 BE 92 26 DA CD EA 59 93 DB 6D 8D 0E 9F 7E ....&...Y..m...~
00 8880: A2 CE 2B CD 25 2D A3 59 EC FC AD B8 19 54 79 C8 ..+.%-Y.....Ty.
00 8890: 33 31 0E 72 03 4C FE 02 01 4F 3B 5A 48 3F B6 41 31.r.L...O;ZH?A
00 88A0: 2D 76 DB 27 A1 00 38 D7 84 59 87 64 54 7C 6F 4C -v..'..8..Y.dT|oL
00 88B0: 2F 71 4E E8 65 87 94 36 99 FE F4 45 3A D1 C3 B7 /qN.e..6...E:...
00 88C0: 6D D2 21 3C 45 37 4E DE C8 C1 37 EE 76 FD 7C 41 m.!<E7N...7.v.|A
00 88D0: 27 9E 2B B5 D8 1C 63 30 C9 90 35 F4 DD 0E B2 05 '.+....c0..5.....
00 88E0: 69 14 57 3A 4F F3 2C 29 59 5B 47 B8 5B D2 6E E8 i.W:0.,)Y[G.[.n.
00 88F0: 15 8C 87 83 07 72 39 B7 DB 48 D2 80 9D A6 18 73 .....r9..H.....s
00 8900: AE 57 44 81 BE 7F AE 10 8C 48 8C 41 CD B7 FF C3 .WD.....H.A....
00 8910: 35 52 F4 C9 9F 8C D5 77 9E 73 C2 8A BD F8 6D 9E 5R.....w.s....m.
00 8920: 7C 42 55 F3 89 B4 98 FF 47 0B 3F 96 FE 88 AF 5E |BU.....G.?....^
00 8930: C4 6B 81 05 7B 59 5D F6 E0 C7 AF B6 54 F7 C4 66 .k...{Y}.....T..f
00 8940: 96 1D BB 5E 54 B8 1D D3 CB 47 F4 24 C7 7E B6 BD ...^T....G.$..~..
00 8950: 95 CF B1 6F 96 8B 4E 62 DE 30 0F 15 91 DD CC D3 ...o..Nb.0.....
00 8960: A4 88 74 4C DF 41 46 CF E0 FE 3E 90 82 87 25 FF ..tL.AF...>...%.
00 8970: 69 F8 5E 4C 4E F6 18 9F AA 0B 8D 38 B4 51 ED 7E i.^LN.....8.Q..~
00 8980: A5 D6 9C A0 35 87 8B EF 01 99 48 1B D5 C4 B6 0A .....5.....H.....
00 8990: DC 4A 6D 07 0B D6 85 18 1A 73 39 EC 23 B7 65 16 .Jm.....s9.#.e.
  
```

```

AUTH LOGIN.....
MAIL FROM: <%s>.
.....RCPT TO: <%s
>.....DATA
.....200.68.60.24
6...62.119.40.98
.....150.254.183.
15...132.181.12.1
3...193.79.237.1
4...131.188.3.22
2...131.188.3.22
0...193.5.216.14
.....193.67.79.20
2...133.100.11.8
.....193.204.114.
232.138.96.64.10
.....chronos.cru.
fr..212.242.86.1
86...128.233.3.10
1...142.3.100.2.
200.19.119.69...
137.92.140.80...
129.132.2.21...
See the attached
file for detail
s...Please see t
he attached file
for details...
your_document.pi
f...document_all
  
```



# The Cycle of Malicious Code

Harvesting

Harnessing

Execution

Unclassified



# Harvesting Phase

- During the months of January to April over seventy-five pieces of malicious code were released into the wild. (*Mydoom (15), Netsky(30), and Beagle(30)*)

Mass-Mailing worm that arrive as an attachment

Establishing listen threads on TCP ports

Creates a notification thread that will contact to a remote site

Enables the intruder to download and execute arbitrary files

- Forensic analysis revealed an online war of words between the authors
- Economic Damage from MyDoom, Netsky, and Beagle where estimated over 100 billion world-wide
- Vendors estimated that MyDoom was the most successfully comprising over 450K
- Targeting SCO with a DDoS masked the true intention of the author



# Harnessing Phase

- The next phase is to herd the victimized systems into a Bot-network by gaining unauthorized access left behind by the worm infections.
- A backdoor command and control software is then executed on the victimized system from the holes left behind by the worms.

Backdoor.Sdbot: Discovered on April 30, 2002; Variants 29; Latest October 14, 2004

AgoBot: Discovered on Sept. 17, 2003; Variants 52; Latest Nov. 9, 2004

- Allows the intruder to remotely control a compromised computer and perform any of the following actions:
  - **Download and execute files**
  - **Delivers system and network information to the author**
  - **Harvest email addresses**
  - **Dynamically updates the installed Trojan**
  - **Probes the compromised system with password generators**
  - **Control the IRC client on a compromised computer**
  - **Creates a random IP address and performs a DDoS attack**
  - **Acts as a proxy server to direct attacks against another machine.**

Unclassified



# Execution Phase

- The victimized boxes are herded into a Bot-network to launch DDoS attacks.
- DDoS attacks are used to extort money out of victim companies to have access to the Internet
- Bot-networks can be used as platform to launching next-generation worms and viruses.
- Bot-networks can be sold to spammers and/or novices to manipulate.
- The information that resides on the compromised system is stolen and sold to different organized groups.
  - credit card information
  - social security numbers
  - banking login ID and Passwords
  - Corporate secrets
  - Espionage
  - cookies and web cash



# Leaves Worm

- Infected host scan for sub7 hosts
- Downloaded files from websites
- Periodic checks for time
- Infected host check for updates at different websites
- Once infected, the intruder had the ability to move, copy, delete and execute files on the host system
- Amassed a bot network of 50,000 thousands infected systems. Why?





# Bugbear A B C

- Propagation via local area network shares
- Trojan Backdoor – remote command and control of victim system
- Trojan Keylogger – Logs and Exfiltrates personal information (i.e. credit cards, SSNs)
- E-mail information to multi – Dropsites
- Deletes Antivirus and security programs
- Targeted the Financial Community



**Unclassified**



# Trojan/Webber - A B C

- Propagation via email (mass- mailing) July 16, 17, and 22 2003
- Doesn't delete or modify any files
- Displays an application to be filled about Home Equity's loans
- Password stealing Trojan attempts to extract sensitive information
  - credit card information
  - social security numbers
  - banking login ID and Passwords
  - Corporate secrets
  - Espionage
  - Cookies and web cash
- Checks for internet connections, if successful, sends captured information to CGI scripts at another website or holds data for later date.
- Targeted three Financial Institutions  
Estimated losses are upwards of 4 million dollars



# Infrastructure Under Attack

- Slammer affected access to over 13,000 ATM machines and caused sever delays in airline flights. (SQL server left un-patched)
- Slammer penetrated a private network at Ohio nuclear power plant in January and disabled a data system. ( T1 Line by passed the plant firewall)
- Bugbear.B in June, wreaked havoc on targeted financial institutions by capturing private keystroke information from its victims and leaving a backdoor for future access.
- “Welchia” was blamed for fouling up Air Canada's electronic check-in system last tuesday, forcing the carrier to check in passengers manually (Un-patched vulnerabilities in the Microsoft Remote Procedure Call Interface)
- Sobig.F infected CSX Corp.'s computers so thoroughly that the 23 states on the east coast railways where shut down. The worm disrupted signaling, dispatching, as well as, other system controls. ( Human intervention)

Unclassified



# Top 20 Computer Threats unveiled

- Oct 9, 2004, SANS Institute released the Top 20 security vulnerabilities in Windows and Unix/Linux software. <http://www.sans.org/top20/>
- The vast majority of worms and other successful cyber attacks are made possible by vulnerabilities in a small number of common operating systems.
- The easy and destructive spread of worms, such as MSblaster, Slammer, Code Red and Nimba, can be traced directly to exploitation of un-patched vulnerabilities.
- 2,500 software vulnerabilities found every year many organizations need help to know which ones to tackle first.
- Hackers take the easiest and most convenient route and exploit the best-known flaws with the most effective and widely available attack tools.



# Top 20 Computer Threats

- Web Servers & Services
- Workstation Services
- Windows Remote Access Services
- Microsoft SQL Server (MSSQL)
- Windows Authentication
- Web Browsers
- File-Sharing Applications
- LSAS Exposures
- Mail Client
- Instant Messaging
- BIND Domain Name System
- Web Server
- Authentication
- Version Control Systems
- Mail Transport Service
- Simple Network Manage Protocol (SNMP)
- Open Secure Sockets Layer (SSL)
- Mis-configuration of Enterprise Service
- Databases
- Kernel



# Conclusions

- It isn't about technology; it's about crime. (Money > Ego)
- Analysis is becoming increasingly more challenging
  - Obfuscation is an 'Arms Race'
- 2,500 software vulnerabilities found every year
  - Dealing with a weak infrastructure
- We are living in the Chicago 20's all over again
  - Everything has value and will be traded
- Law Enforcement cannot do it alone.....( What can we do)



# What you can do ?

## PREVENTION

- A/V Scanners
- Stay away from unknown attachments
- Download latest patches/updates
- Intrusion Detection Systems (IDS)
- Password-Protect Drive Shares
- Rename or remove key executables
- Configure browser settings and zones
- Use firewalls

## AWARENESS

- Publications: Cybernotes/ BugTraq
- CERT/CC advisories
- Knowledge of your own network
- Crisis Action Plan
- New technologies (Wireless Networks)
- Lots and lots of reading



**Malicious Code + Low Risk =  
Great Rewards**

**UC Erkan Chase  
Cyber Division – FBIHQ  
202 -324-0303  
echase@fbi.gov**

Unclassified