Crime On The Internet
Dealing With Spyware, Botnets
And Other Cyber Attacks

David Aucsmith
Senior Director
Institute for Advanced Technology in Governments
Microsoft Corporation
awk@microsoft.com
On The Front Line

Our Products
- 80% of world’s critical infrastructures
- Determined, resourceful, global adversaries

Our Resources
- Attacked > 4,000 times a day
- At least one DDoS a day
- Logged attacks from every country

Our Business
- Subject to Phishing, Bots, Root-kits, …
Short History of "Hacking"
Short History of “Hacking”

- Mainframes
- Emanations
- Insiders
- Tempest
- TCSEC, Common Criteria
- 80s
Short History of “Hacking”

80s
Mainframes
- TCSEC, Common Criteria
- Insiders
- Tempest

90s
Networks
- Eavesdropping
  - DES, AES, IPSec
- Network Protocols
  - Sync flood, DNS spoofing
- Network Stacks
  - “Ping of death”

Emanations
- Tempest
Short History of “Hacking”

- **Mainframes**
  - **80s**: Emanations
    - Tempest
  - **90s**: Insiders
    - TCSEC, Common Criteria
  - **00s**: Networks
    - Operating System Services
      - Buffer overruns, XSS
      - Web spoofs, worms
    - Application Services
      - SQL injection, SQL Slammer
      - Media players
    - Network Protocols
      - Sync flood, DNS spoofing
    - Network Stacks
      - “Ping of death”
  
- **Networks**
  - **90s**
  
- **Eavesdropping**
  - DES, AES, IPSec

- **Services**
  - **80s**
  
- **Application Services**
  - **00s**
    - Buffer overruns, XSS
    - Web spoofs, worms
  
- **Operating System Services**
  - **90s**
    - SQL injection, SQL Slammer
    - Media players
  
- **Network Protocols**
  - Sync flood, DNS spoofing
  
- **Network Stacks**
  - “Ping of death”
Vulnerability Timeline

- Undiscovered
- Experimentation
- Correction
- Packaging
- Customer Testing / Deployment

Steps:
- Early Disclosure
- Responsible Disclosure
- Actual Vulnerability To Attack
- Module Gap

Events:
- Software Ship
- Vulnerability Discovered
- Vulnerability Disclosed
- Component Fixed
- Customer Fix Available
- Fix Deployed
Vulnerability Timeline

- Undiscovered Vulnerability
- Discovered
- Correction
- Component Fixed
- Packaging
- Customer Testing / Deployment
- Fix Deployed
- Customer Fix Available
- Early Disclosure
- Responsible Disclosure
- Vulnerability Disclosed
- Vulnerability Discovered
- Software Ship
- Actual Vulnerability To Attack
- Module Gap
- Experimentation
- Undiscovered

Rarely discovered
Vulnerability Timeline

Why does this gap exist?

Actual Vulnerability To Attack

Module Gap

Early Disclosure
Responsible Disclosure

Undiscovered Experimentation Correction Packaging

Software Ship Vulnerability Discovered Vulnerability Disclosed Component Fixed Customer Fix Available Fix Deployed

Customer Testing / Deployment
• Days From Patch To Exploit
  - Have decreased so that patching is not a defense in large organizations
  - Average 6 days for patch to be reverse engineered to identify vulnerability

Source: Microsoft
Blaster shows the complex interplay between security researchers, software companies, and hackers.
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM.

Time before shutdown: 00:00:53

Message: Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly.
Investigation

- Analysis of code led us to t33kid.com
  - FBI/USSS watched and gathered intelligence
- Real-time Subpoena
  - ISP Cari.net in San Diego (issued by on call AUSA)
- Virtual host led to Texas
- Owner of site in Texas
  - Had criminal record
  - Was potential suspect
- T33kid.com leased space from Texas owner
- Investigative work led us to Jeffrey Lee Parson
  - Seven computers seized
Investigation

p2p.teekid.c
my little p2p worm spreads via kaza and mesh, downloads a file from web. No biggie.
Download | # of downloads 720

webdl.c
webdownload example in c
Download | # of downloads

p2p.duoload.vb
Dudoad made be teekid and b0b, modified a tiny bit from the c distro.
Download | # of downloads

http://www.t33kid.com/ - mailto:root@t33kid.com
“Less than 24 hours after Microsoft released its Security Bulletins for August, exploit code was made publicly available for the vulnerabilities addressed in Microsoft Security Bulletin MS05-038 and MS05-041. The postings, titled ‘Microsoft Internet Explorer COM Objects Instantiation Exploit (MS05-038)’ and ‘Microsoft Windows Remote Desktop Protocol DoS Exploit (MS05-041),’ were published by the French security firm FrSIRT. A second piece of code was published on August 11th for MS05-038.’

“Three pieces of exploit code targeting the Windows Plug and Play issue (MS05-039) have been made publicly available. These are listed as the ‘Microsoft Windows Plug and Play Remote Buffer Overflow Exploit (MS05-039),’ ‘Microsoft Windows 2000 Plug and Play Universal Remote Exploit (MS05-039),’ and ‘Microsoft Windows 2000 Plug and Play Universal Remote Exploit #2 (MS05-039)’ on the FrSIRT Web site. One of which has also been included as an exploit module in the Metasploit Framework.”

“ Authorities in Morocco and Turkey have arrested two people believed to be responsible for unleashing a computer worm that infected networks at U.S. companies and government agencies earlier this month, the FBI said Friday.

…

Microsoft played a role in locating the suspects, the FBI said.”

http://www.msnbc.msn.com/id/9086742/
Answers “Where are the greatest risks?”
Exploits written in 2005 for 6 popular Operating Systems
- Win32
- Linux (4 distributions)

2005 Vulns and Exploits (YTD)

<table>
<thead>
<tr>
<th></th>
<th>Vulns</th>
<th>Exploitable</th>
<th>Trivial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>344</td>
<td>96</td>
<td>61</td>
</tr>
</tbody>
</table>

Exploits written 2005 YTD - all platforms

Thru May 31, 2005
Exploit Statistics - 2005 (YTD)

Network service

- squid 25%
- ethereal 21%
- tcpdump 13%
- tcpip 13%
- dnsmasq 8%
- telnet 4%
- pppx 4%
- kdenet 4%
- msmq 4%
- ftp 4%

Thru May 31, 2005
Understanding the Landscape

- National Interest
- Personal Gain
- Personal Fame
- Curiosity
Understanding the Landscape

- National Interest
- Personal Gain
- Personal Fame
- Curiosity

Script-Kiddy | Hobbyist Hacker | Expert | Specialist

Vandal
Understanding the Landscape

- National Interest
- Personal Gain
- Personal Fame
- Curiosity

- Script-Kiddy
- Hobbyist Hacker
- Expert
- Specialist

Vandal Trespasser
Understanding the Landscape

National Interest

Personal Gain

Personal Fame

Curiosity

Script-Kiddy

Hobbyist Hacker

Expert

Specialist

Vandal

Trespasser

Author
Understanding the Landscape

National Interest

Personal Gain

Personal Fame

Curiosity

Script-Kiddy

Hobbyist Hacker

Thief

Trespasser

Author

Expert

Specialist
Understanding the Landscape

National Interest

Personal Gain

Personal Fame

Curiosity

Script-Kiddy

Hobbyist Hacker

Expert

Specialist

Vandal

Thief

Trespasser

Author

Spy
Understanding the Landscape

National Interest

Personal Gain

Personal Fame

Curiosity

Tools created by experts now used by less skilled attackers and criminals

Script-Kiddy

Hobbyist Hacker

Expert

Specialist

Vandal

Thief

Trespasser

Author

Spy
Understanding the Landscape

National Interest
Personal Gain
Personal Fame
Curiosity

Script-Kiddy
Hobbyist Hacker
Expert
Specialist

Tools created by experts now used by less skilled attackers and criminals
Understanding the Landscape

Tools created by experts now used by less skilled attackers and criminals
Legacy

- 16-bit 100 MHz processor
- 10 GByte disk
- 20 MByte ram
- CD drive
- 13” VGA monitor

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

32-bit 2.5 GHz processor
250 GByte disk
3 GByte ram
DVD R/W drive
21” digital monitor


1990 2005
Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

Windows XP SP2
ICF
USB
UPnP
Windows Update

32-bit 2.5 GHz processor
250 GByte disk
3 GByte ram
DVD R/W drive
21” digital monitor

Legacy

Windows 95
FAT FS
IPX and NetBIOS
Open networking

16-bit 100 MHz processor
10 GByte disk
20 MByte ram
CD drive
13” VGA monitor

Legacy creates security issues


Windows XP SP2
ICF
USB
UPnP
Windows Update

32-bit 2.5 GHz processor
250 GByte disk
3 GByte ram
DVD R/W drive
21” digital monitor

1990 2005
The security kernel of Windows NT was written:
- Before there was a World Wide Web
- Before TCP/IP was the default communications protocol
Keeping It In Perspective

- The security kernel of Windows NT was written:
  - Before there was a World Wide Web
  - Before TCP/IP was the default communications protocol

- The security kernel of Windows Server 2003 was written:
  - Before buffer overflow tool kits were available
  - Before Web Services were widely deployed
Honey Pot Projects

- Six computers attached to Internet
- Different versions of Windows, Linux and Mac OS
Honey Pot Projects

- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks
Honey Pot Projects

- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks
- No up-to-date, patched operating systems succumbed to a single attack
Six computers attached to Internet
- Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks
- No up-to-date, patched operating systems succumbed to a single attack
- All down rev systems were compromised
  - Windows XP with no patches
  - Infested in 18 minutes by Blaster and Sasser
  - Within an hour it became a "bot"

Source: StillSecure, see http://www.denverpost.com/Stories/0,1413,36~33~2735094,00.html
Insiders and Outsiders
Trusted Insider

- Compromise of security by trusted party
- Traditional domain of TCSEC and Common Criteria

Compromise of design or implementation

Compromise during distribution

Compromise by user

Compromise by admin
Un-trusted Outsider

- Traditional “hacker”
  - Asynchronous network attack via vulnerability
  - User self-betrayal

Fool user into self-betrayal

Attacker

Exploit vulnerability
Malware
- Spam, phishing, worms, bots, …

Asymmetric
- Attacker need only find one victim
- Defender needs to protect all

Force multiplier
- Write once, attack all

Harvest
- Harvest the “interesting” successes
Mass unsolicited email

For commerce

Direct mail advertisement

For Web traffic

Artificially generated Web traffic

Phishing

For fraud

Harassment

Credential theft

Identity theft
“Our first program pays you $0.50 for every validated free-trial registrant your website sends to [bleep]. Commissions are quick and easy because we pay you when people sign up for our three-day free-trial. Since [bleep] doesn't require a credit card number or outside verification service to use the free trial, generating revenue is a snap.

The second program we offer is our pay per sign-up plan. This program allows you to earn a percentage on every converted (paying) member who joins [bleep]. You could make up to 60% of each membership fee from people you direct to join the site.

Lastly, [bleep] offers a two tier program in addition to our other plans. If you successfully refer another webmaster to our site and they open an affiliate account, you begin earning money from their traffic as well! The second tier pays $0.02 per free-trial registrant or up to 3% of their sign-ups.”
“Our first program pays you $0.50 for every validated free-trial registrant your website sends to [bleep]. Commissions are quick and easy because we pay you when people sign up for our three-day free-trial. Since [bleep] doesn’t require a credit card number or outside verification service to use the free trial, generating revenue is a snap.

The second program we offer is our pay per sign-up plan. This program allows you to earn a percentage on every converted (paying) member who joins [bleep]. You could make up to 60% of each membership fee from people you direct to join the site.

Lastly, [bleep] offers a two tier program in addition to our other plans. If you successfully refer another webmaster to our site and they open an affiliate account, you begin earning money from their traffic as well! The second tier pays $0.02 per free-trial registrant or up to 3% of their sign-ups.”

Key Points

• $0.50 for every validated free-trial registrant
• 60% of each membership fee
Do the Math

- SoBig spammed over 100 million inboxes
Do the Math

- SoBig spammed over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people
Do the Math

- SoBig spammed over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people
- If 1% of people who went to site signed up for 3-days free trial
  - = (100,000 people) x ($0.50) = $50,000
Do the Math

- SoBig spammed over 100 million inboxes
- If 10% read the mail and clicked the link
  - = 10 million people
- If 1% of people who went to site signed up for 3-days free trial
  - = (100,000 people) x ($0.50) = $50,000
- If 1% of free trials sign up for 1 year
  - = (1,000 people) x ($144/yr) = $144,000/yr
California Man Charged with Botnet Offenses

November 3, 2005

Botnets are big business ... U.S. case against an alleged computer hacker, who authorities believe netted $60,000 in cash and a BMW from a personal army of zombie computers.

Federal authorities arrested a 20-year-old California man Thursday and charged him with running a network of 400,000 compromised computers called a "botnet," including computers used by the U.S. government for national defense.

Ancheta was a member of affiliate networks used by unnamed "advertising service companies," who paid him around $60,000 to install their advertising software on the machines he controlled, the statement alleges.

Ancheta allegedly distributed software for Gammacash, of Quebec, and LoudCash, part of CDT of Montreal, which was purchased by 180 Solutions Inc. in April.
Phishing

- Faking
  - An e-mail that seems to be from a legitimate source

- Spoofing
  - A Web site that appears to be “official”

- Phishing
  - Luring users to provide sensitive data

---

From: joe@Citizensbank.com [mailto:joe@Citizensbank.com]
To: [Redacted]
Subject: Citizensbank.com account holder

![Image of phishing email]

---

Dear Citizensbank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:

https://www.citizensbankonline.com/online/login/verification-process-1.html

AFTER SUBMITTING, PLEASE DO NOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citizens Bank Business Development, this process cannot be externally requested through Customer Support.

Sincerely,
Citizensbank.com
Business Department
Phishing

- **Faking**
  - An e-mail that seems to be from a legitimate source

- **Spoofing**
  - A Web site that appears to be “official”

- **Phishing**
  - Luring users to provide sensitive data
Deceptive Address
Source code reveals actual mail from address as "href=mailto://accmanager@msn-network.com"
Impersonal Message

Be wary if a company with which you regularly do business fails to address you by name.
Alarmist Message
Criminals try their best to create a sense of urgency so you'll respond without thinking. Also, look for misspellings, grammatical errors, and typos—such as “...an access to MSN services for your account...”
Deceptive Link
Source code reveals that the actual address linked to is
"href=http://www.online-msnupdate.com/?sess=qCKWmHUBPPZwT8n4GEMNn70wHDEG140IHKG5tAGiG0INeov&amp;cid=bettevost@msn.com"

The difference between these two URLs could be a sign that the message is fake. (However, even if the URLs are the same, don’t let down your guard, because the pop-up could be a trick, too.)
Know the Company

eBay generally does not send out emails to customers containing login links. Look carefully at the status bar for all links and URLs—the URL in the status bar for the login link is not eBay.com.
Differences between links or URLs in an email and the status bar should make you suspicious. If you receive an email like this one, open a new browser window, type in the URL yourself and login into your account to see if there are any real account problems.
Phishing
MSN Billing Phishing Case
1. MS filed John Doe lawsuit in WA
1 MS filed John Doe lawsuit in WA

2 Issued subpoenas to web hosts in CA
1 MS filed John Doe lawsuit in WA

2 Issued subpoenas to web hosts in CA

3 Subpoenas identified ISP in Austria
1. MS filed John Doe lawsuit in WA

2. Issued subpoenas to web hosts in CA

3. Subpoenas identified ISP in Austria

4. Austrian ISP identified IP address registered to Qwest in the US
1. MS filed John Doe lawsuit in WA

2. Issued subpoenas to web hosts in CA

3. Subpoenas identified ISP in Austria

4. Austrian ISP identified IP address registered to Qwest in the US

5. Subpoena to Qwest and investigations identified Jayson Harris in Iowa, US

6. Referred to FBI and obtained $3 million Default Judgment
Most people are spoofed
- Over 60% have visited a fake or spoofed site

People are tricked
- Over 15% admit to having provided personal data

Target for spoofing attacks
- Banks, credit card companies, Web retailers, online auctions (E-bay) and mortgage companies.

Economic loss
- 1.2 million U.S. adults have lost money
- The total dollar impact: $929 million

Source: TRUSTe & Gartner
Spyware

- Software that:
  - Collects personal information from you
  - Without your knowledge or permission
Spyware

Software that:
- Collects personal information from you
- Without your knowledge or permission

Privacy
- 15 percent of enterprise PCs have a keylogger
  Source: Webroot's SpyAudit
- Number of keyloggers jumped three-fold in 12 months
  Source: Sophos
Spyware

- **Software that:**
  - Collects personal information from you
  - Without your knowledge or permission

- **Privacy**
  - 15 percent of enterprise PCs have a keylogger
    
    - Source: Webroot's SpyAudit
  - Number of keyloggers jumped three-fold in 12 months
    
    - Source: Sophos

- **Reliability**
  - Microsoft Watson
    - ~50% of crashes caused by spyware
Spyware

- **Software that:**
  - Collects personal information from you
  - Without your knowledge or permission

- **Privacy**
  - 15 percent of enterprise PCs have a keylogger
    - Source: Webroot’s SpyAudit
  - Number of keyloggers jumped three-fold in 12 months
    - Source: Sophos

- **Reliability**
  - Microsoft Watson
    - ~50% of crashes caused by spyware

- **Support Costs**
  - Dell, HP, IBM: Spyware causes ~30% of calls
  - Estimated support costs at $2.5m+ / year
Dubbed "Trojangate," the incident resulted in nearly 20 arrests, with some reports indicating that there were hundreds -- perhaps thousands -- of documents stolen from multiple Israeli firms. About 100 servers containing stolen data have been seized and are being investigated.”  

-- BBC
Spyware as Espionage

Israel Spyware

“Dubbed "Trojangate," the incident resulted in nearly 20 arrests, with some reports indicating that there were hundreds -- perhaps thousands -- of documents stolen from multiple Israeli firms. About 100 servers containing stolen data have been seized and are being investigated.”  

“In 2004, MessageLabs came upon a Trojan horse created for the purpose of attacking a type of software used in airplane design.” 

BBC

AP
Spyware as Espionage

Israel Spyware

“In 2004, MessageLabs came upon a Trojan horse created for the purpose of attacking a type of software used in airplane design.” *AP*

“Dubbed "Trojangate," the incident resulted in nearly 20 arrests, with some reports indicating that there were hundreds -- perhaps thousands -- of documents stolen from multiple Israeli firms. About 100 servers containing stolen data have been seized and are being investigated.” *BBC*

“Someone placed surveillance software on sheriff's office computers, apparently enabling unauthorized access to sensitive information about prisoner movements, confidential homeland security updates and private personnel files.” *AP*
UK police foil massive bank theft

Police in London say they have foiled one of the biggest attempted bank thefts in Britain. The plan was to steal £220m ($423m) from the London offices of the Japanese bank Sumitomo Mitsui. Computer experts are believed to have tried to transfer the money electronically after hacking into the bank’s systems. A man has been arrested by police in Israel after the plot was uncovered by the National Hi-Tech Crime Unit. Unit members worked closely with Israeli police...
Combating Spyware Threats

Microsoft Windows AntiSpyware

Helps protect Windows users from spyware and other potentially unwanted software

Detect and remove spyware
- 17 million downloads, 23 million spyware packages cleaned
- Scheduled scans help maintain PC security and privacy

Improve Internet browsing safety
- Continuous protection guards 50+ ways spyware gets on a PC
- Intelligent alerts handle spyware based on your preferences

Stop the latest threats
- Global SpyNet™ community helps identify new spyware
- Automatic signature downloads keep you up-to-date
### Feb. 2005 OCA Snapshot

<table>
<thead>
<tr>
<th>Driver</th>
<th>Characteristic</th>
<th>Instance count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delprot.sys</td>
<td>Deletion protection for iSearch adware/spyware.</td>
<td>81870</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.03%</td>
</tr>
<tr>
<td>“LoadMeDude” TROJ_LODMEDUD_A</td>
<td>Randomly named driver that hides processes, registry, files.</td>
<td>25496</td>
</tr>
<tr>
<td></td>
<td>Auto-update capability.</td>
<td>0.32%</td>
</tr>
<tr>
<td></td>
<td>Bundled with Comedy Central adware/spyware.</td>
<td></td>
</tr>
<tr>
<td>winik.sys</td>
<td>Protects CommonName adware/spyware.</td>
<td>13583</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.17%</td>
</tr>
<tr>
<td>iesprt.sys TROJ_BANKER.W</td>
<td>Steals banking passwords.</td>
<td>2386</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.03%</td>
</tr>
<tr>
<td>Hxdefdrv.sys “Hacker Defender”</td>
<td>Public domain source rootkit. Resource hiding and backdoor capability.</td>
<td>1323</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.02%</td>
</tr>
</tbody>
</table>
Bots

- Bot Ecosystem
  - Bots
  - Botnets
  - Control channels
  - Herders
Bots

- Bot Ecosystem
  - Bots
  - Botnets
  - Control channels
  - Herders

- It began in mass with MyDoom.A
  - Eight days after MyDoom.A hit the Internet
  - Scanned for the back door left by the worm
  - Installed Trojan horse called Mitglieder
  - Then used those systems as their spam engines
  - Millions of computers across the Internet were now for sale to the underground spam community
<table>
<thead>
<tr>
<th>Age (days)</th>
<th>Name</th>
<th>Server</th>
<th>MaxSize</th>
</tr>
</thead>
<tbody>
<tr>
<td>02.00</td>
<td>nubela.net</td>
<td>dns.nubela.net</td>
<td>10725</td>
</tr>
<tr>
<td>10.94</td>
<td>winnt.bigmoney.biz (randex)</td>
<td>winnt.bigmoney.biz</td>
<td>2393</td>
</tr>
<tr>
<td>09.66</td>
<td>PS 7835 - y.eliteirc.co.uk</td>
<td>y.eliteirc.co.uk</td>
<td>2061</td>
</tr>
<tr>
<td>09.13</td>
<td>y.stefanjagger.co.uk (#y)</td>
<td>y.stefanjagger.co.uk</td>
<td>1832</td>
</tr>
<tr>
<td>03.10</td>
<td>ganjahaze.com</td>
<td>ganjahaze.com</td>
<td>1507</td>
</tr>
<tr>
<td>01.04</td>
<td>PS 8049 - 1.j00g0t0wn3d.net</td>
<td>1.j00g0t0wn3d.net</td>
<td>3689</td>
</tr>
<tr>
<td>10.93</td>
<td>pub.isonert.net</td>
<td>pub.isonert.net</td>
<td>537</td>
</tr>
<tr>
<td>08.07</td>
<td>irc.brokenirc.net</td>
<td>irc.brokenirc.net</td>
<td>649</td>
</tr>
<tr>
<td>01.02</td>
<td>PS 8048 - grabit.zapto.org</td>
<td>grabit.zapto.org</td>
<td>62</td>
</tr>
<tr>
<td>10.34</td>
<td>dark.naksha.net</td>
<td>dark.naksha.net</td>
<td>UNK</td>
</tr>
<tr>
<td>08.96</td>
<td>PS 7865 - lsd.25u.com</td>
<td>lsd.25u.com</td>
<td>UNK</td>
</tr>
<tr>
<td>UNK</td>
<td>PS ? - 69.64.38.221</td>
<td>69.64.38.221</td>
<td>UNK</td>
</tr>
<tr>
<td>Server</td>
<td>Name</td>
<td>Age (days)</td>
<td>MaxSize</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>dns.nubela.net</td>
<td>nubela.net</td>
<td>02.00</td>
<td>10725</td>
</tr>
<tr>
<td>winnt.bigmoney.biz</td>
<td>randex</td>
<td>10.94</td>
<td>2393</td>
</tr>
<tr>
<td>y.eliteirc.co.uk</td>
<td>y.eliteirc.co.uk</td>
<td>09.66</td>
<td>2061</td>
</tr>
<tr>
<td>y.stefanjagger.co.uk</td>
<td>(#Y)</td>
<td>09.13</td>
<td>1832</td>
</tr>
<tr>
<td>ganjahaze.com</td>
<td>ganjahaze.com</td>
<td>03.10</td>
<td>1507</td>
</tr>
<tr>
<td>PS 8049 - 1.j00g0r0wn3d.net</td>
<td>ganjahaze.com</td>
<td>01.04</td>
<td>3689</td>
</tr>
<tr>
<td>pub.isonert.net</td>
<td>pub.isonert.net</td>
<td>10.93</td>
<td>537</td>
</tr>
<tr>
<td>irc.brokenirc.net</td>
<td>grabit.zapto.org</td>
<td>08.07</td>
<td>649</td>
</tr>
<tr>
<td>dark.naksha.net</td>
<td>dark.naksha.net</td>
<td>01.02</td>
<td>62</td>
</tr>
<tr>
<td>PS 7365 - lsd.25u.com</td>
<td></td>
<td>10.34</td>
<td>UNK</td>
</tr>
<tr>
<td>PS 7365 - lsd.25u.com</td>
<td></td>
<td>08.96</td>
<td>UNK</td>
</tr>
<tr>
<td>PS 7365 - lsd.25u.com</td>
<td></td>
<td></td>
<td>UNK</td>
</tr>
</tbody>
</table>
As of 12 August 2005:
Tracking 3523 bot-nets of which 700 are active
Average size is 80,000 computers

<table>
<thead>
<tr>
<th>Age (days)</th>
<th>Name</th>
<th>Server</th>
<th>MaxSize</th>
</tr>
</thead>
<tbody>
<tr>
<td>02.00</td>
<td>nubela.net</td>
<td>dns.nubela.net</td>
<td>10725</td>
</tr>
<tr>
<td>10.94</td>
<td>winnt.bigmoney.biz (randex)</td>
<td>winnt.bigmoney.biz</td>
<td>2393</td>
</tr>
<tr>
<td>09.66</td>
<td>PS 7835 - y.eliteirc.co.uk</td>
<td>y.eliteirc.co.uk</td>
<td>2061</td>
</tr>
<tr>
<td>09.13</td>
<td>y.stefanjagger.co.uk (#y)</td>
<td>y.stefanjagger.co.uk</td>
<td>1832</td>
</tr>
<tr>
<td>03.10</td>
<td>ganjahaze.com</td>
<td>ganjahaze.com</td>
<td>1507</td>
</tr>
<tr>
<td>01.04</td>
<td>PS 8049 - 1.j00g0t0wn3d.net</td>
<td>1.j00g0t0wn3d.net</td>
<td>3689</td>
</tr>
<tr>
<td>10.93</td>
<td>pub.isonert.net</td>
<td>pub.isonert.net</td>
<td>537</td>
</tr>
<tr>
<td>08.07</td>
<td>irc.brokenirc.net</td>
<td>irc.brokenirc.net</td>
<td>649</td>
</tr>
<tr>
<td>01.02</td>
<td>PS 8048 - grabit.zapto.org</td>
<td>grabit.zapto.org</td>
<td>62</td>
</tr>
<tr>
<td>10.34</td>
<td>dark.naksha.net</td>
<td>dark.naksha.net</td>
<td>UNK</td>
</tr>
<tr>
<td>08.96</td>
<td>PS 7865 - lsd.25u.com</td>
<td>lsd.25u.com</td>
<td>UNK</td>
</tr>
<tr>
<td>UNK</td>
<td>PS ? - 69.64.38.221</td>
<td>69.64.38.221</td>
<td>UNK</td>
</tr>
</tbody>
</table>
Botnet with 10,000 Machines Shut Down

Sept 8, 2004

“A huge IRC "botnet" controlling more than 10,000 machines has been shut down by the security staff of Norwegian provider Telenor, according to the Internet Storm Center. The discovery confirms beliefs about the growth of botnets, which were cited in the recent distributed denial of service (DDoS) attack upon Akamai and DoubleClick that sparked broader web site outages. [...]”

In The News

Botnet with 10,000 Machines Shut Down
Sept 8, 2004
“A huge IRC "botnet" controlling more than 10,000 machines has been shut down by the security staff of Norwegian provider Telenor, according to the Internet Storm Center. The discovery confirms beliefs about the growth of botnets, which were cited in the recent distributed denial of service (DDoS) attack upon Akamai and DoubleClick that sparked broader web site outages. [...]”

FBI busts alleged DDoS Mafia
Aug 26, 2004
“A Massachusetts businessman allegedly paid members of the computer underground to launch organized, crippling distributed denial of service (DDoS) attacks against three of his competitors [...]”
Payloads

- Keystroke loggers for stealing CC, PII
- SYN or application flooding code
  - Used for DDoS
  - DDoS has been used many times
  - Including public attacks against Microsoft.com
- Spam relays – 70-80% of all spam
  Source SpecialHam.com, Spamforum.biz
- Piracy
- Future features
### Botnet Damage Potential

#### 10,000-member botnet

<table>
<thead>
<tr>
<th>Attack</th>
<th>Requests/bot</th>
<th>Botnet Total</th>
<th>Resource exhausted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth flood (uplink)</td>
<td>186 kbps</td>
<td>1.86 Gbps</td>
<td>T1, T3, OC-3, OC-12</td>
</tr>
<tr>
<td>Bandwidth flood (downlink)</td>
<td>450 Kbps</td>
<td>4.5 Gbps</td>
<td>T1, T3, OC-3, OC-12, OC-48 (2.488Gbps)</td>
</tr>
<tr>
<td>Syn flood</td>
<td>450 SYN/seg</td>
<td>4.5M SYN/seg</td>
<td>4 Dedicated Cisco Guard (@$90k) OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20 tuned servers</td>
</tr>
<tr>
<td>Static http get (cached)</td>
<td>93/seg</td>
<td>929,000 seg</td>
<td>15 servers</td>
</tr>
<tr>
<td>Dynamic http get</td>
<td>93/seg</td>
<td>929,000 seg</td>
<td>310 servers</td>
</tr>
<tr>
<td>SSL handshake</td>
<td>10/seg</td>
<td>100,000 sec</td>
<td>167 servers</td>
</tr>
</tbody>
</table>
## Botnet Damage Potential

### 10,000-member botnet

<table>
<thead>
<tr>
<th>Attack</th>
<th>Requests/bot</th>
<th>Botnet Total</th>
<th>Resource exhausted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth flood (uplink)</td>
<td>186 kbps</td>
<td>1.86 Gbps</td>
<td>T1, T3, OC-3, OC-12</td>
</tr>
<tr>
<td>Bandwidth flood (downlink)</td>
<td>450 kbps</td>
<td>4.5 Gbps</td>
<td>T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) 50% of Taiwan/US backbone</td>
</tr>
<tr>
<td>Syn flood</td>
<td>450 SYNs/sec</td>
<td>4.5M SYN/sec</td>
<td>4 Dedicated Cisco Guard (@$90k) OR 20 tuned servers</td>
</tr>
<tr>
<td>Static http get (cached)</td>
<td>93/sec</td>
<td>929,000/sec</td>
<td>15 servers</td>
</tr>
<tr>
<td>Dynamic http get</td>
<td>93/sec</td>
<td>929,000/sec</td>
<td>310 servers</td>
</tr>
<tr>
<td>SSL handshake</td>
<td>10/sec</td>
<td>100,000/sec</td>
<td>167 servers</td>
</tr>
</tbody>
</table>

>$350.00/weekly - $1,000/monthly (USD)
>**Type of service:** Exclusive (One slot only)
>**Always Online:** 5,000 - 6,000
>**Updated every:** 10 minutes

>$220.00/weekly - $800.00/monthly (USD)
>**Type of service:** Shared (4 slots)
>**Always Online:** 9,000 - 10,000
>**Updated every:** 5 minutes
Malicious Software Removal

Complements traditional Antivirus technologies by providing one tool that removes prevalent viruses and worms from a PC

- Updated monthly to remove prevalent malware
- Targeted at consumers without antivirus
- Enterprise deployable as part of a defense-in-depth strategy
- Available through:
  - Windows Update
  - Auto Update
  - Online interface
  - MS Download Center
Cleaner Statistics (as of 27 July 2005)

<table>
<thead>
<tr>
<th>Release</th>
<th>Days Live</th>
<th>Executions</th>
<th>Disfections</th>
<th>Value</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>28</td>
<td>124,613,632</td>
<td>239,197</td>
<td>0.1920%</td>
<td></td>
</tr>
<tr>
<td>February</td>
<td>28</td>
<td>118,209,670</td>
<td>351,135</td>
<td>0.2970%</td>
<td></td>
</tr>
<tr>
<td>March</td>
<td>35</td>
<td>145,502,003</td>
<td>443,661</td>
<td>0.3049%</td>
<td></td>
</tr>
<tr>
<td>April</td>
<td>28</td>
<td>125,150,400</td>
<td>590,714</td>
<td>0.4720%</td>
<td></td>
</tr>
<tr>
<td>May</td>
<td>35</td>
<td>164,283,730</td>
<td>1,154,345</td>
<td>0.7027%</td>
<td></td>
</tr>
<tr>
<td>June</td>
<td>28</td>
<td>162,763,946</td>
<td>642,955</td>
<td>0.3950%</td>
<td></td>
</tr>
<tr>
<td>July</td>
<td>18</td>
<td>156,379,734</td>
<td>627,414</td>
<td>0.4090%</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>200</td>
<td>1,001,824,331</td>
<td>4,093,531</td>
<td>0.4106%</td>
<td></td>
</tr>
</tbody>
</table>

Source: Microsoft
The Economics of Crime

- Increase the value of an enterprise by damaging a competing enterprise
- Manipulate the value of a futures contract
- Divert delivery of value, to someone to whom it was not intended
- Make a coercive threat credible
- Stop by direct intervention an activity perceived as destroying value
- Reduce an opponent’s defensive or destructive capabilities

Source: Scott Borg, an economist at Dartmouth
The Fundamental Problem
The Fundamental Problem

Intended Behavior
The Fundamental Problem

Intended Behavior

Actual Behavior
The Fundamental Problem

Intended Behavior

Actual Behavior

Traditional Bugs
The Fundamental Problem

Intended Behavior

Actual Behavior

Most Security Bugs

Traditional Bugs
Threat Modeling Process

- Create model of app (DFD, UML etc)
- Categorize threats with STRIDE
- Build threat tree
- Rank threats with DREAD
- Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Elevation of Privilege
- Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability
1.2.1 Parse Request
1.2.1 Parse Request

Threat (Goal)

STRIDE

Threat (Goal)

STRIDE

Threat (Goal)

KEY

Threat
Sub threat
Condition
1.2.1 Parse Request

STRIDE
Threat (Goal)

STRIDE
Threat (Goal)

Threat
Threat
Threat

Condition
Subthreat

Condition
Condition

DREAD

DREAD

KEY

Threat
Sub threat
Condition
The underlying DLL (NTDLL.DLL) not vulnerable

Code made more conservative during Security Push
The underlying DLL (NTDLL.DLL) not vulnerable

Even if it was vulnerable

Code made more conservative during Security Push

IIS 6.0 not running by default on Windows Server 2003
The underlying DLL (NTDLL.DLL) not vulnerable

Even if it was vulnerable

Even if it was running

Code made more conservative during Security Push

IIS 6.0 not running by default on Windows Server 2003

IIS 6.0 doesn’t have WebDAV enabled by default
<table>
<thead>
<tr>
<th>The underlying DLL (NTDLL.DLL) not vulnerable</th>
<th>Code made more conservative during Security Push</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Even if it was vulnerable</em></td>
<td><em>IIS 6.0 not running by default on Windows Server 2003</em></td>
</tr>
<tr>
<td><em>Even if it was running</em></td>
<td><em>IIS 6.0 doesn’t have WebDAV enabled by default</em></td>
</tr>
<tr>
<td><em>Even if it did have WebDAV enabled</em></td>
<td><em>Maximum URL length in IIS 6.0 is 16kb by default (&gt;64kb needed)</em></td>
</tr>
<tr>
<td>Scenario</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The underlying DLL (NTDLL.DLL) not vulnerable</td>
<td>Code made more conservative during Security Push</td>
</tr>
<tr>
<td>Even if it was vulnerable</td>
<td>IIS 6.0 not running by default on Windows Server 2003</td>
</tr>
<tr>
<td>Even if it was running</td>
<td>IIS 6.0 doesn’t have WebDAV enabled by default</td>
</tr>
<tr>
<td>Even if it did have WebDAV enabled</td>
<td>Maximum URL length in IIS 6.0 is 16kb by default (&gt;64kb needed)</td>
</tr>
<tr>
<td>Even if the buffer was large enough</td>
<td>Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)</td>
</tr>
</tbody>
</table>
The underlying DLL (NTDLL.DLL) not vulnerable

Even if it was vulnerable

Even if it was running

Even if it did have WebDAV enabled

Even if the buffer was large enough

Even if it there was an exploitable buffer overrun

Code made more conservative during Security Push

IIS 6.0 not running by default on Windows Server 2003

IIS 6.0 doesn’t have WebDAV enabled by default

Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)

Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)

Would have occurred in w3wp.exe which is now running as ‘network service’
As of June 2, 2005

Focus Yields Results

Days After Product Release

Important = Critical bulletins issued after product release

Windows 2000 Server

Windows Server 2003

Bulletins 614 Days
After Product Release

Bulletins 564 Days
After Product Release

Microsoft Exchange Server 2000

Microsoft Exchange Server 2003

Released 11/29/2000

Released 09/28/2003

Released 05/31/2001

Released 11/17/2003

Released 05/31/2001

Released 11/17/2003

As of June 2, 2005