Secure Computing in the Internet Age

Danbury Area Computer Society

April 13, 2005

Jeffrey A. Setaro
jasetaro@mags.net

Topics

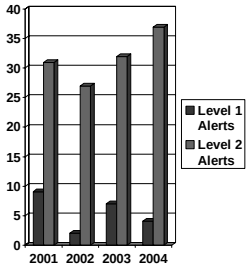
- Threats
- Solutions
- Tools

The Challenge...

- PCs have become a commodity
- Users no longer care how it works... They just want to use it.
- We have to change the plug it in and go mind set.
- PCs require regular maintenance.

2004 in Review

- 41 major virus outbreaks.
- Six virus families were in a league of their own: Bagle, Mydoom, Netsky, Sasser, Korgo & Sober.
- Massive increase in Phishing scams.
- Virus writers and spammers working together.
- 2004 was the best year ever in actually catching virus writers and other cyber criminals.



Arrests

Month	Country	What
May	Germany	Sasser & Netsky author arrested.
May	Germany	Agobot variant authors arrested.
May	Canada	Randex variant authors arrested.
May	Taiwan	Peep backdoor author arrested.
June	Finland	VBS/Lasku author arrested.
June	Hungary	Magold author arrested.
July	Spain	Cabrotor backdoor author arrested.
July	Russia	Three DDoS hackers arrested.
August	United States	Blaster.B author confesses.
November	Russia	Member of 29A virus groups sentenced.

Virus Writers and Spammers Working Together

- Collection of e-mail addresses
- Setting up e-mail servers
- Setting up web servers for offending material
- Attacks against anti-spam services

What can we expect in 2005?

- Fewer mass mailing worms.
- More Trojan Horse programs designed to install “bots”.
- Increased Phishing scams.
- Increased targeting of wireless devices.
- Continued attacks against web servers.
- More “proof of concept” malware targeting the MacOS.
- Decrease in Macro and Script based malware.

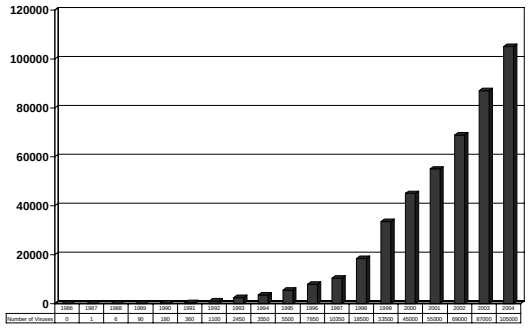
Threats

- Viruses
- Trojan Horse Programs
- Worms
- Spyware
- Rootkits
- Phishing
- Pharming
- Hoaxes

Viruses

- A computer virus is a self-replicating program containing code that explicitly copies itself and that can "infect" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus.

Number of Viruses 1986-2004



Things That Aren't Viruses

- Bugs
- Corrupted programs/files
- False alarms
- Hardware conflicts/problems
- Joke programs
- Software conflicts

Trojan Horses

- A program that does something undocumented that the programmer intended, but that some users would not approve of if they knew about it.
  - Backdoors, “Bots” and/or RATs
  - Key Loggers
  - AOL Password Stealers

Worms

- A computer WORM is a self-contained program (or set of programs), that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections).
  - W32/Blaster
  - W32/Sasser
  - W32/Witty

The Facts About Malware

- Computer viruses, Trojan horse programs and worms are computer programs. In order for one of them to do damage, some type of programmatic code has to be run.

The Malware Myth

- Computer viruses, Trojan horse programs and worms are not a security problem, they are a code integrity problem.

Spyware

- Software that collects and sends information about your Web surfing habits to a third party.
- Often installed in combination with "free" software or as a Drive-by-Download.

Spyware

- The term “spyware” become a generic catch-all for several categories of privacy and/or security risks.
  - System Monitors
  - Trojan Horse Programs
  - Adware
  - Tracking Cookies

Adware – Defenses

- Keep Internet Explorer Patched.
- Tighten Internet Explorer’s Security Settings.
- Use SpywareBlaster
  - www.javacoolsoftware.com
- Use an alternative Web browser.
  - Firefox
    - www.mozilla.org
  - Opera
    - www.opera.com

Rootkits

- The term rootkit comes from the UNIX world.
- Rootkits for the UNIX operating system were typically used to elevate the privileges of a user to the root level.

Rootkits

- Rootkits for Windows work in a different way.
- Typically used to hide malicious software from anti-virus or anti-spyware scanners.
- Not malicious by themselves but are used for malicious purposes by viruses, worms, backdoors and spyware.
- A virus combined with a rootkit produces what was known as full stealth viruses in the MS-DOS environment.

Phishing

- Is a scam to steal valuable personal information such as credit card numbers, bank account numbers, social security numbers and user IDs & passwords.

Phishing – How It Works

- Typically an official-looking e-mail is sent to potential victims pretending to be from their ISP, retail store, bank, etc., and that due to internal accounting errors or some other pretext, certain information must be updated to continue the service.
- A link in the e-mail message directs the user to an official looking Web page that asks for personal and financial information.

Pharming

- Also know as DNS Hijacking or DNS Poisoning.
- An illegal change to a DNS record that redirects the URL of a known trusted site to a different site.

Pharming – How It Works

- You type http://www.amazon.com into your web browser.
- Your computer queries a DNS server for the IP address of www.amazon.com
- The DNS server responds with 207.171.175.29
- Your computer connects to the web server @ 207.171.175.29

Pharming

- The bogus Web site might offer similar and/or competing products for sale, or it may be a vehicle to publicly smear the reputation of a legitimate Web site.
- Can also be used to steal valuable personal information such as credit card numbers, bank account numbers, social security numbers and user IDs & passwords.

Pharming

- Unlike phishing schemes that use e-mail to entice users to go to a phony site, phraming is more natural.
  1. Users are going to a site on their own.
  2. Aren't suspicious because the pages look familiar.

Hoaxes

- Do not read e-mail messages with the subject . . . . It will destroy your hard drive.
  - Good Times
  - Join the Crew
- There is a new undetectable virus named xyz.exe… Delete it from your hard drive.
  - Jdbmgr.exe virus warning
  - Sulfnbk.exe virus warning
- Resources
  - http://www.vmyths.com/
  - http://www.ciac.org/

How to Spot a Hoax

- The virus always is disastrous - "wipes your hard drive" or similar.
- "Authorities" are quoted in a quasi news release style - often IBM, Microsoft, AOL, or FBI
- There is a "technical" description of how the virus works and/or spreads.
- They ask you to pass it on to everyone, "in your address book", "that you know" or similar.

The "Zombie" Problem

- Current estimates put the number compromised systems in the millions.
- Roughly 150,000 new zombies are identified each day.
- These systems are used to:
  - Relay spam.
  - Host rouge content.
  - Conduct DDoS attacks.
- Much of the unwanted zombie activity is now coming from outside of the U.S.

Solutions

- Anti-Virus Software
- Personal Firewalls
- Broadband Router & Firewall Appliances
- Safe Hex

Understanding Anti-virus Software

- Anti-virus software is a perishable commodity that has to be updated on a regular basis in order to remain effective.
- Both the program and definition files have to be updated to keep pace with current threats.

Understanding Anti-virus Software

"Anti-virus software is by its very nature reactionary and can only "protect" against what it already knows. Relying on anti-virus software to protect you from viruses is a little like hiring Willie Sutton to guard a bank. . . it looks good on the surface but in reality all it does is offer a false sense of security.

That's not to say you shouldn't use anti-virus software. Anti-virus software should be a part of your overall defense strategy, but it should not be a replacement for the zealous practice of Safe Hex."

Understanding Anti-virus Software

- Scanners
- Change Detectors

Scanners

- Positively identify known viruses
  - On Access
    - Provides real-time memory resident detection and disinfection.
  - On Demand
    - Provides on command detection and disinfection of viruses.

Change Detectors

- Some things shouldn't change
- Record information about the program files on your computer.
- Requires users to make the final decision.

Understanding Personal Firewalls

- A personal firewall is a network security application that filters communications between your PC and the Internet.
- Application Monitoring
- Traffic Monitoring

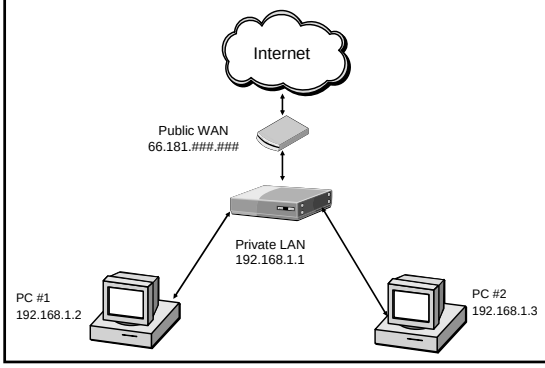
Broadband Firewall/Routers

- A firewall is a network security device positioned between your internal, trusted network and the Internet.
- A router is a device that forwards data packets from your local area network to the Internet.
  - NAT - Network Address Translation
  - SPI - Stateful Packet Inspection

A Quick & Dirty Guide to NAT

- IP addresses in these blocks are reserved for use on internal networks and are not Internet routeable.
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255

A Quick & Dirty Guide to NAT



Stateful Packet Inspection

- Tracks the transaction to ensure that inbound packets were requested by the user.
- Generally can examine multiple layers of the protocol stack, including the data, if required, so blocking can be made at any layer or depth.

Safe Hex - The Basics

- Keep your system patched
  - Use the Windows and Office Update sites
- Install and use anti-virus software
- Install and use a personal firewall
- Install and use anti-spyware software
- Make backups of important files and folders
- Use strong passwords
  - xCz7_R2ds
  - Eagle+743-doG
- Use care when downloading and installing programs

Safe Hex *(continued)*

- Disable file and printer sharing in your computer, particularly when accessing the Internet using cable modems, digital subscriber lines (DSL), or other high-speed connections.
- Use care when reading e-mail with attachments
  - Never, ever:
    - Open e-mail attachments from someone you don't know
    - Open e-mail attachments forwarded to you even if they're from someone you know
    - Open unsolicited or unexpected e-mail attachments until you've confirmed the sender actually meant to send them

Safe Hex *(continued)*

- Do not select the option on web browsers for storing or retaining user name and password.
- Do not disclose personal, financial, or credit card information to little-known or suspect web sites.
- Delete spam and chain e-mail's; do not forward these and do not use the unsubscribe feature.
- Log off the online session and turn off your computer when it is not in use.

Safe Hex *(continued)*

- Do not use a computer or a device that cannot be fully trusted.
- Do not use public or Internet café computers to access online financial services accounts or perform financial transactions.
- Ensure your browser supports strong encryption (at least 128-bit). Most browsers now provide this by default.
- Install and use a file encryption program and access controls.
- Broadband users: install and use a hardware firewall/router.

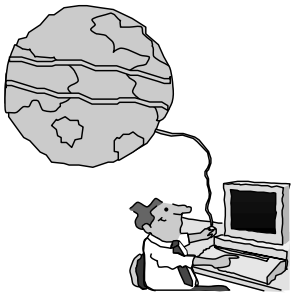
What If Disaster Strikes?

- Don't panic
- Disconnect from the network
- Walk away

What Should You Do?

- Unfortunately there isn't an easy answer.
- Check the web sites of anti-virus developers for:
  - Alerts or warnings about new viruses
  - New definition or signature updates
  - Manual removal instructions
  - Specialized removal tools
- E-mail samples of the suspect files to your anti-virus software provider for analysis.

Tools & Resources



Must Have Tools

For Windows 9x Users

- Clean write-protected startup diskette or CD-ROM.
- DOS versions of your anti-virus software on diskette or CD-ROM.
- Current backups.
- Disaster recovery plan.
- F-Prot for DOS.
  - www.f-prot.com

Must Have Tools

For Windows 2000/XP Users

- ERD Commander or PE Builder (Bart PE).
  - www.winternals.com
  - www.nu2.nu
- Current backups.
- Disaster recovery plan.

Anti-Virus Software

- F-Prot Anti-Virus
  - www.f-prot.com
- F-Secure Anti-Virus 2005 or Internet Security 2005
  - www.f-secure.com
- Kaspersky AntiVirus
  - www.kaspersky.com
- Nod32 Anti-Virus System
  - www.nod32.com
- Norman Virus Control
  - www.norman.com

Anti-Spyware Software

- Ad-aware
  - www.lavasoft.com
- eTrust Pest Patrol
  - home.ca.com
- Microsoft Anti-Spyware (beta)
  - www.microsoft.com/spyware
- SpyBot Search & Destroy
  - www.safer-networking.org
- Spy Sweeper
  - www.webroot.com

Personal Firewalls

- F-Secure Internet Security 2005
  - www.f-secure.com
- Kerio Personal Firewall
  - www.kerio.com
- Outpost Firewall
  - www.agnitum.com
- Sygate Personal Firewall
  - soho.sygate.com
- ZoneAlarm
  - www.zonelabs.com

Anti-Trojan Software

- BOClean
  - www.nsclean.com
- Tauscan
  - www.agnitum.com
- The Cleaner 4.1 Professional
  - www.moosoft.com
- TDS-3
  - www.diamondcs.com.au
- TrojanHunter
  - www.misec.net

Broadband Routers

- Linksys EtherFast Router BEFSX41
- Netgear ProSafe Router FR114P
- SonicWALL TZ 150
- SMC Barricade Plus Router SMC7004VBR
- WatchGuard Firebox SOHO 6
- ZyXel ZyWall 2

Additional Resources

- alt.comp.virus Anti-Virus pages
  - www.claymania.com/nav-map.html
- CERT Coordination Center
  - www.cert.org
- Internet Security Alliance
  - www.isalliance.org
- Internet Storm Center
  - isc.sans.org
- Microsoft Security and Privacy
  - www.microsoft.com/security
- United States Computer Emergency Readiness Team
  - www.us-cert.gov

Port Scanning Services

- PC Flank
  - www.pcflank.com
- SecuritySpace.com
  - www.securityspace.com
- Sygate Online Services
  - scan.sygate.com

10 Immutable Laws of Security

1) If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
2) If a bad guy can alter the operating system on your computer, it's not your computer anymore
3) If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
4) If you allow a bad guy to upload programs to your website, it's not your website any more
5) Weak passwords trump strong security
6) A computer is only as secure as the administrator is trustworthy
7) Encrypted data is only as secure as the decryption key
8) An out of date virus scanner is only marginally better than no virus scanner at all
9) Absolute anonymity isn't practical, in real life or on the Web
10) Technology is not a panacea

Final Thought

- Security is a process not a destination.