Secure Computing in the Internet Age

Danbury Area Computer Society

April 7, 2008

Jeffrey A. Setaro
www.jasetaro.com

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.

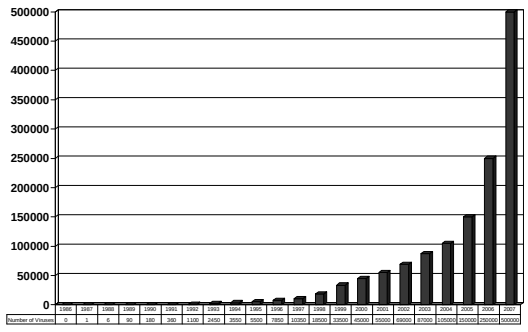
2007 in Review

- No major virus outbreaks.
- Fake video codecs targeting both Windows and the MacOS.
- Banking Trojans.
- Phishing scams.
- Virus writers and spammers working together.

2007 in Review

- Slightly more than half of malware hosting web sites (51.4%) are in China.
- Slightly less than half (48.7%) of malware is hosted on web sites running Apache.
- Slightly less than a quarter (21%) of all malware is written in China.
- Roughly a quarter of all Spam originates in the United States.
- Your chance of receiving an infected e-mail attachment dropped to 1 in 909.

Malware 1986-2007



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 2008?

- More Storm worm Variants.
- More Trojan Horse programs designed to target both Windows and the MacOS.
- Phishing scams.
- Continued targeting of wireless devices.
- Continued attacks against web servers.
- Increased targeting the MacOS.

Threats

- Viruses
- Trojan Horse Programs
- Worms
- Spyware
- Rootkits
- Phishing
- 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.

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

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

Spyware – Defenses

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

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.

Malware Myths

1. Malware relies on bugs or vulnerabilities in operating systems or applications to infect your computer.
2. Malware is not a security problem, it's a code integrity problem.
3. The MacOS and Linux are immune.

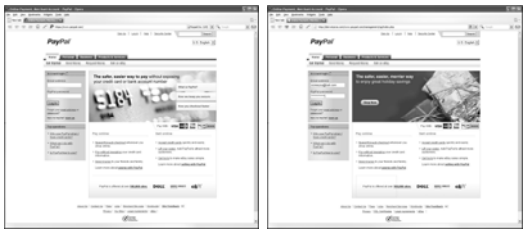
Phishing

- 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.

Phishing – How It Works



Phishing – How It Works

Phishing – How It Works

Phishing – How It Works

Phishing – How It Works

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://hoaxbusters.ciac.org/
  - http://www.snopes.com

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

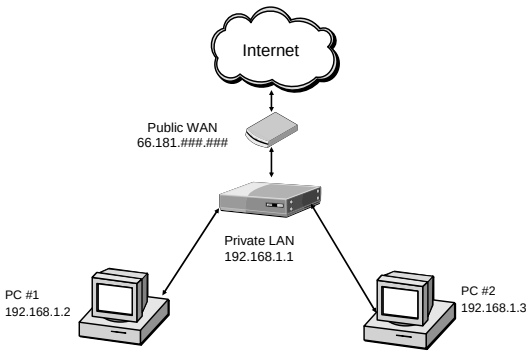
Broadband Firewall/Routers

- 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
  - Visit the Windows Update site regularly.
- 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.

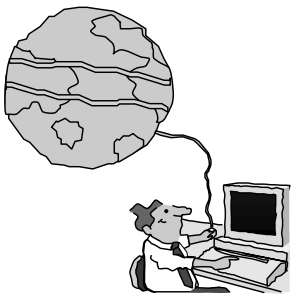
What If Disaster Strikes?

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

What Should You Do?

- Minimize the damage
- Remove the malicious code
  - Update your anti-virus software
  - Check for alerts or warnings about new viruses, manual removal instructions and/or specialized removal tools
- E-mail samples of the suspect files to your anti-virus software provider for analysis.

Tools & Resources



Must Have Tools

- PE Builder (Bart PE).
  - www.nu2.nu
- Current backups.
- Disaster recovery plan.
- Sysclean from Trend Micro

Anti-Virus Software

- F-Prot Anti-Virus
  - www.f-prot.com
- F-Secure Anti-Virus or Internet Security
  - www.f-secure.com
- Kaspersky AntiVirus or Internet Security
  - www.kaspersky.com
- Nod32 Anti-Virus or Smart Security
  - www.eset.com

Anti-Spyware Software

- Ad-Aware 2007
  - www.lavasoft.de
- CounterSpy
  - www.sunbeltsoftware.com
- SpyBot Search & Destroy
  - www.safer-networking.org
- Spy Sweeper
  - www.webroot.com
- SUPERAntiSpyware
  - www.superantispyware.com

Personal Firewalls

- F-Secure Internet Security
  - www.f-secure.com
- Kaspersky Internet Security
  - www.kaspersky.com
- Outpost Pro Firewall
  - www.agnitum.com
- Sunbelt Personal Firewall
  - www.sunbeltsoftware.com
- ZoneAlarm
  - www.zonelabs.com

Additional Resources

- alt.comp.virus Anti-Virus pages
  - www.claymania.com/nav-map.html
- 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

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.