Secure Computing in the Internet Age

Danbury Area Computer Society
May 3, 2011

Jeffrey A. Setaro
jasetaro@yahoo.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.

2010 in Review

- No major virus outbreaks.
- Social networks targeted.
- Phishing scams.
- Politically motivated hacking and DDoS attacks.
- Malware writers and spammers working together.
- Arrests, arrests and more arrests.

2010 in Review

- Nearly 40% of malware hosting web sites are in The US.
- The US leads the world in Spam accounting for roughly 16% of all junk e-mail.
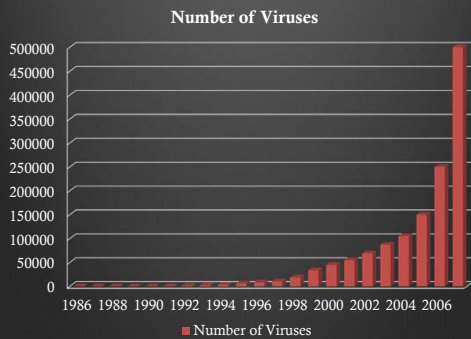- Despite a smaller overall market share IIS web servers host roughly same amount of malware as Apache servers.

Malware 1986-2007

Number of Viruses

What can we expect in the future?

- More attacks on older versions of Windows.
- Copycat attacks based on Stuxnet.
- More mobile malware targeting the Andriod platform and jailbroken iOS devices.
- Facebook spam goes global.
- Increased spear phishing attacks.

Malware 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

Threats

- Malware
- Spyware
- Ransomware
- Phishing
- Pharming
- Unsecured Wi-Fi Networks

Malware

- Malware is a generic term for several types of malicious programs including:
  - Viruses
  - Worms
  - Trojan Horse Programs
  - Rootkits
  - Spyware

Malware - 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.

Malware - 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

Malware - Trojan Horse Programs

- 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
  - Rogue Anti-Malware products

Malware - 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.

Malware - Rootkits

- Rootkits for Windows work in a different way.

- Typically used to hide malicious software from anti-malware scanners.

- Not malicious by themselves, but are used for malicious purposes by malware programs.

- A virus combined with a rootkit produces what were known as full stealth viruses in the MS-DOS environment.

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

Ransomware

- Ransomware is computer malware which holds a computer system, or the data it contains, hostage by demanding the user pay ransom for its restoration.

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 a security problem, it's not… 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
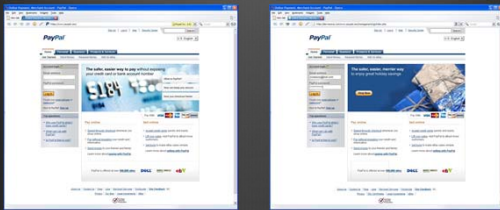

Phishing – How It Works

Phishing – How It Works

Phishing – How It Works

Fake:

Real:

Phishing – How It Works

Pharming

- Pharming is a hacker's attack aiming to redirect a website's traffic to another, bogus website.

- It works by changing the DNS entry of a legitimate web site so that it points a different IP address.

The Perils Of Unsecured Wi-Fi

- Download child pornography
- Download copyrighted movies and music via P2P
- Download Warez and abuse your bandwidth
- Send bomb hoaxes, terror or threatening emails.
- Send spam (sexual aids, pharmacy or money laundering scams)

The Perils Of Unsecured Wi-Fi
(continued)

- Infiltrate and break into internal machines
- Modify DNS settings on the router to point to a rouge server.
- Sniff Wi-Fi traffic for usernames and passwords

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 rogue content.
  - Conduct DDoS attacks.
- Much of the unwanted zombie activity is now coming from outside of the U.S.

Solutions

- Safe Hex
- Risk Mitigation Tools

Dump Internet Explorer 6

- It's time to upgrade!

- Either upgrade to IE8 or use an alternative Web browser.
  - Firefox
    - www.mozilla.com
  - Opera
    - www.opera.com

Safe Hex - The Basics

▪Keep your system patched
  ◆Use Secunia's Personal Software Inspector.
▪Install and use anti-malware software
▪Install and use a personal firewall
▪Broadband users: install and use a hardware firewall/router.
▪Make backups of important files and folders
▪Use strong passwords
  •xCz7_R2ds
  •Eagle+743-doG
  •x+rAy&0997-Mi

Safe Hex *(continued)*

▪ Use care when downloading and installing programs
▪ 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.
▪Protect your privacy by blocking third party cookies.

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.

Mobile Safe Hex

- Keep your device updated.
- Install a security application in your device.
- Watch where you click and land.
- Refrain from doing transactions on a public network.
- Install or obtain applications from trusted sources.
- Make it a habit to check each applications' data access on your device.

Risk Mitigation Tools

- Anti-Malware software
- Personal firewall software
- Encryption software
- Broadband router/firewall appliances

Anti-malware Software

- Anti-malware software is a perishable commodity that has to be updated on a regular basis in order to remain effective.
- Positively identify known viruses
  - On Access
    - Provides real-time memory resident detection and disinfection.
  - On Demand
    - Provides on command detection and disinfection of viruses.

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

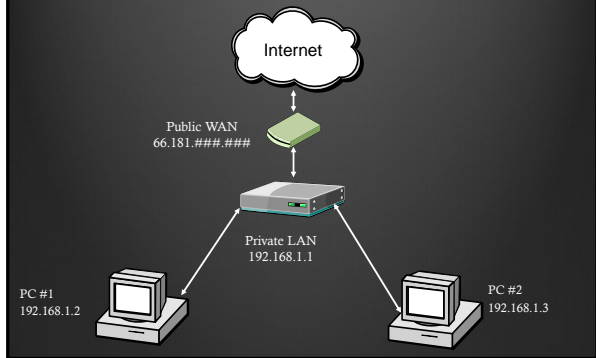## A Quick & Dirty Guide to NAT

Internet

Public WAN
66.181.###.###

Private LAN
192.168.1.1

PC #1
192.168.1.2

PC #2
192.168.1.3

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.

What If Disaster Strikes?
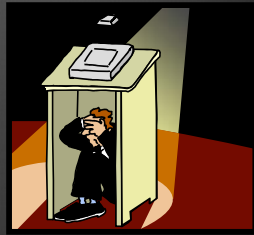
- Don't panic
- Disconnect from the network
- Walk away

Must Have Tools

- Current backups.
- Disaster recovery plan.
- F-Secure's Bootable Rescue CD
- A thumb drive with recovery tools
  - Sysclean from Trend Micro
  - SuperAntispyware Portable Edition
  - F-Secure Blacklight & EasyClean
- SpywareBlaster
  - www.javacoolsoftware.com

Additional Resources

- Looks To Good To Be True
  - www.lookstoogoodtobetrue.com/
- Snopes
  - www.snopes.com
- Internet Storm Center
  - isc.sans.org
- Microsoft Security and Privacy
  - www.microsoft.com/security
- United States Computer Emergency Readiness Team
  - www.us-cert.gov
- Internet Crime Complaint Center
  - www.ic3.gov

Final Thoughts

- Security is a process not a destination.
- Technology is not panacea.