

HOME COMPUTER SECURITY

A Workshop by the Seattle Office of Information Security

Whatever problems you may be having with computer security,
I can assure you that mine are far greater.

- With apologies to Albert Einstein



THIS IS PART OF A SERIES

- Infosec 101: Web and e-mail self defense techniques
- Infosec 102: Home computer security
- Infosec 103: Home network security



HOW THIS PRESENTATION WILL GO

- Introductions to the OIS
- Vocabulary
- Examples and scary stuff
- Web and e-mail self-defense
- Break
- Computer controls
 - Anti-Virus
 - Patching
 - Firewalls
 - Browser configuration



TODAY YOU WILL LEARN

- A bit about what we do at the City
- The Who, What, Why and How of Attacks Against
 - Your Computer
 - Your Money
 - Your Privacy
- Controls to implement on your home computers
- How to fight back



OFFICE OF INFORMATION SECURITY

- Cross-department function
- Citywide IT governance
- Policies, standards, procedures
- Network security
- Desktop security
- Awareness and outreach
- Security monitoring
- Incident response



WHAT INFORMATION DOES LOCAL GOVERNMENT PROTECT?

- H/R Records
- Constituent Data
- Business License Information
- Justice Information
- Cardholder Data
- Critical Infrastructure
- Brand Value

Add Public Disclosure, E-Discovery, Shake Well



WHY ARE WE DOING THIS?

- The more we all know about computing hygiene at home, the safer we'll all be
- It's part of the mission of the Office of Information Security
- We really don't want anyone losing their bank accounts



USEFUL TERMS

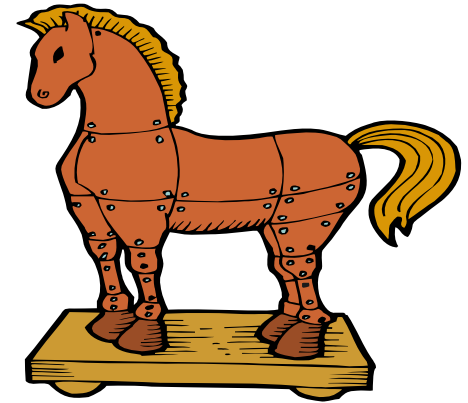
- Threat: something that could go wrong
- Vulnerability: susceptibility to attack
- Exploit: leveraging a vulnerability to realize threat (noun and verb)
- Impact: consequence of the threat
- Risk: product of threat probability and impact
- Zero-day exploit: one for which no fix exists



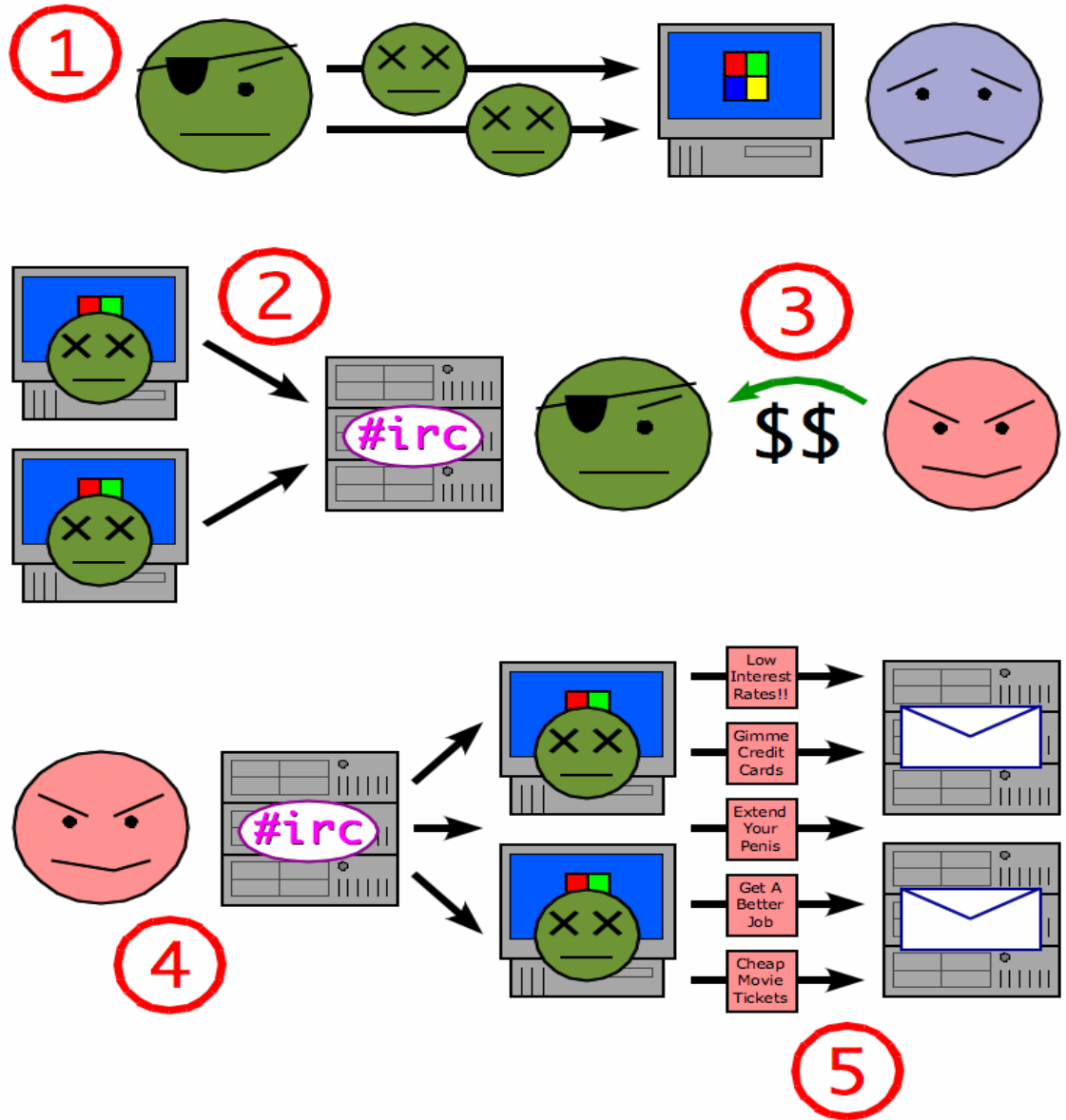


A FEW MORE

- Adware: generates advertising messages
- Spyware: tracks online activity
- Malware: general term
- Trojan: program that lies in wait on your computer
- Rootkit: method of hiding malware
- Botnet: collection of compromised computers under central command and control



The Cartoon Botnet



VULNERABILITY EXAMPLE

US-CERT Current Activity

Adobe Flash Player Vulnerability

Original release date: May 27, 2008 at 6:44 pm

Last revised: May 27, 2008 at 6:44 pm

US-CERT is aware of public reports of a vulnerability in Adobe Flash Player. **By convincing a user to open a specially crafted Flash file, a remote, unauthenticated attacker may be able to execute arbitrary code.**

Public reports indicate that **this vulnerability is being actively exploited.** To help mitigate the risks, US-CERT encourages users to implement best security practices as described in the Securing Your Web Browser document.

US-CERT will provide additional information as it becomes available.



THREAT EXAMPLE

US-CERT Current Activity

United States Tax Court Spear-Phishing Attack

Original release date: May 15, 2008 at 3:15 pm

Last revised: May 15, 2008 at 3:15 pm

US-CERT is aware of public reports of a spear-phishing attack circulating via email messages that claim to be petitions from the US Tax Court. These messages appear to be legitimate because they may contain very specific information about the message recipient. The message requests that the user follow a link to download additional information about the petition, but **if a user clicks on this link, malicious code may be installed on the system.**



POTENTIAL IMPACTS

- Nuisance – SPAM, Adware, slow computer
- Cost: Computer Cleaning Software, Technician Time, New Disk (or Computer!)
- Disclosure of financial or other passwords
- Loss of privacy; threat to safety



WHAT'S THE MOTIVE?

- “Willie Sutton used to say he robbed banks because that’s where the money is. The same applies today to crooks and the Internet.”

Keith Lordeau
FBI, Special Agent



Willie Sutton



ORGANIZED CYBERCRIME

- This is a BUSINESS
 - Profit maximization
 - Low Risk
 - Global market access
- Home base in weak states
 - Safe haven for international ops
 - Added protection from law enforcement: “jurisdictional arbitrage”
- The Internet is anonymous



THE PROBLEM IS HERE TO STAY

- Cybercrime is worth \$105 billion/year
- More lucrative than the drug trade
- Well-resourced, professional developers
- “Industry” groups, coding contests
- A zero-day exploit is worth \$100K

“If you rob a 7-11 you’ll get much harsher punishment than if you steal millions online.”

- David DeWalt, CEO McAfee



TODAY'S LANDSCAPE

- Email threats decline while malicious web content grows
- More trojans, fewer “viruses”
- Malware types differ according to location
 - >30% of all malware is now written in China, most of it taking the form of Trojans used for gaining a backdoor into users' computers.



LACK OF IT JOBS DRIVING IT PROS TO MALWARE

Malware writers earn more than legitimate technology jobs in some parts of the world.

In China, 43 per cent of IT graduates are unemployed, and hacker "training" web sites are creating a pool of effective malware authors and paying them like a legitimate business.



Source: Computing Magazine, 2-26-08

EXAMPLES



E-MAIL ATTACKS

- You have received a card from an admirer!
- Yassar Arafat's Wife: Nigerian 419 scams
- Become an EBay Powerseller!
- Your card was used in Bulgaria
- Saddam Hussein Found Alive!
- Check out this video of the lunar eclipse!



HOSTILE WEBSITES

- Can exploit vulnerabilities on your computer just by visiting
- Usually deploy adware and spyware
- Golf site, gambling site – it doesn't matter
- Russian (and other) kits available to equip websites with deployment functionality: \$999.00
- 285,000,000 clicks to compromised sites every month
- Newer payloads are keystroke loggers



DRIVE-BY DOWNLOAD

Song Lyrics Domain - Discover the songs you love... - Internet Explorer

File Edit View Favorites Tools Help

← Back → Stop Home Search Favorites Media

Address <http://www.lyricsdomain.com/>

LyricsDomain Discover the songs you love...

Tell a Friend! Browse: [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Y] [Z] [#]

Song Lyrics Domain - Welcome!

Everyday we hear so don't want to miss a site: helping you dis

Site News

March 14, 2004

NORAH JONES LYRI
Thing", "Don't Miss `Harder The Fall)", "Midnight And Dayligh", "I Will Stand", "Stea", "Lonely, Needin' Lov Good", "Everywhere", "Feel That Way Agair Goes Down", "The W I Think About Leavir

Security Warning

Do you want to install and run "**Software Plugin**" signed on 3/14/04 9:30 PM and distributed by:

[Software Plugin Ltd.](#)

Publisher authenticity verified by Thawte Server CA

Caution: Software Plugin Ltd. asserts that this content is safe. You should only install/view this content if you trust Software Plugin Ltd. to make that assertion.

Always trust content from Software Plugin Ltd.

Yes No More Info

Link to more information

Link to digital certificate

Help for digital certificates

WHAT MAKES THESE ATTACKS WORK?

- Bad decisions on the part of the user
- Vulnerable computers
- Readily-available exploits



[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILW0RM

[remote]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-02-26	Move Networks Quantum Streaming Player Control BOF Exploit	593	R	D X	Elazar
2008-02-25	Rising Antivirus Online Scanner Insecure Method Flaw Exploit	992	R	D X	John Smith
2008-02-19	Durgame GLWorld 2.x hgs_startNotify() ActiveX Buffer Overflow Exploit	3392	R	D	luoluo
2008-02-18	Thecus N5200Pro NAS Server Control Panel RFI Vulnerability	2949	R	D	Crackers_Child
2008-02-14	Philips VDIP841 (Firmware <= 1.0.4.800) Multiple Vulnerabilities	3532	R	D	ikki
2008-02-13	IBM Domino Web Access Upload Module SEH Overwrite Exploit	3360	R	D X	Elazar

[local]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-02-21	X.Org xorg-x11-xfs <= 1.0.2-3.1 Local Race Condition Exploit	2596	R	D	vl4dZ
2008-02-18	DESlock+ <= 3.2.6 DLMFDISK.sys local kernel ring0 SYSTEM Exploit	1735	R	D	mu-b
2008-02-18	DESlock+ <= 3.2.6 local kernel ring0 link list zero SYSTEM Exploit	1055	R	D	mu-b
2008-02-18	DESlock+ <= 3.2.6 (list) Local Kernel Memory Leak PoC	912	R	D	mu-b
2008-02-13	Microsoft Office .WPS File Stack Overflow Exploit (MS08-011)	9484	R	D	chujwanwdupe
2008-02-09	Linux Kernel 2.6.23 - 2.6.24 vmsplce Local Root Exploit	31199	R	D	qaaz

[web apps]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-02-26	Nukedit 4.9.x Remote Create Admin Exploit	130	R	D	r3dm0v3
2008-02-25	DBHcms <= 1.1.4 Remote File Inclusion exploit	1184	R	D	Iron
2008-02-25	MiniNuke 2.1 (members.asp uid) Remote SQL Injection Vulnerability	901	R	D	S@BUN
2008-02-25	PHP-Nuke Module Kose_Yazilari (artid) SQL Injection Vulnerability	1484	R	D	xcorpitx
2008-02-25	PORAR WEBBOARD (question.asp) Remote SQL Injection Vulnerability	1140	R	D	xcorpitx
2008-02-24	php Download Manager <= 1.1 Local File Inclusion Vulnerability	1831	R	D	BeyazKurt

[dos / poc]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-02-26	Apple Mac OS X xnu <= 1228.3.13 ipv6-ipcomp Remote kernel DoS PoC	705	R	D	mu-b
2008-02-25	MyServer 0.8.11 (204 No Content) error Remote Denial of Service Exploit	998	R	D	shinnai
2008-02-19	X.Org xorg-server <= 1.1.1-48.13 Probe for Files Exploit PoC	2115	R	D	vl4dZ
2008-02-18	Apple iPhoto 4.0.3 DPAP Server Denial of Service Exploit	1263	R	D	David Wharton
2008-02-18	DESlock+ <= 3.2.6 DLMFENC.sys Local Kernel ring0 link list zero PoC	841	R	D	mu-b
2008-02-14	Rosoft Media Player 4.1.8 M3U File Remote Buffer Overflow PoC	1204	R	D	securfrog

[shellcode]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2007-06-27	win32 Tiny Download and Exec Shellcode 192 bytes	44052	R	D	czy
2007-06-14	win32 download and execute 124 bytes	27944	R	D	Weiss
2007-05-31	win32 IsDebuggerPresent ShellCode (NT/XP) 39 bytes	15120	R	D	ex-pb
2007-04-02	linux/x86 raw-socket ICMP/checksum shell 235 byte	18929	R	D	mu-b

LET'S TAKE A BREAK

Have a stretch...
back in 10 minutes



LAYERED CONTROLS

- Awareness and good decisions
- Manage your passwords
- Anti-virus/anti-spyware software
- Patches and updates
- “Personal” firewall
- Secure browser configuration
- Consider encryption (advanced)
- Make backups!



BE AWARE

- Learn to recognize attacks
- Know what's happening today
 - www.us-cert.gov
 - www.secunia.com
 - www.securitytracker.com
 - www.theregister.com



BE SUSPICIOUS

- Be very cautious about unexpected email, especially if it has an attachment
- Don't follow links that you aren't sure about – or surf dangerous sites
- Don't open executable attachments (.exe, .com, .scr) or any attachment you weren't expecting (even if it's from a friend)



BE ALERT

- Know the types of activities to avoid
- Check for the lock symbol if you are disclosing confidential information
- Know what your kids are doing online – make rules
- Watch for symptoms
 - Computer slow to start or shut down
 - Applications lock up



PASSWORD MANAGEMENT: FINANCIAL SITES

- Use *at least* 8 characters
- Think of a “Pass Phrase”
- Use mix of numbers, letters (upper and lower case) and non-alphanumeric characters: \$ # @ ! * &

Example: The pass phrase, “I hate to be late” would look like: lh82BL8!



PASSWORD MANAGEMENT: OCCASIONAL SHOPPING SITES

- On First Login, Set up a Password So Complex You Will Never Remember
- Each Time You Return, Have Your Password E-Mailed To You
- On Login, Change it to Something You Will Never Remember



PASSWORD MANAGEMENT: E-MAIL SITES

- Lower Risk than Financial or Shopping
- Substitute 2-3 Numbers for Letters
Inserted Into a Word: N0v3mb3r
- Change Routinely



TECHNICAL CONTROLS

- Keeping your computer patched
- Anti-virus and anti-spyware programs
- Use a firewall
- Browser configuration
- Make backups
- Consider the use of encryption

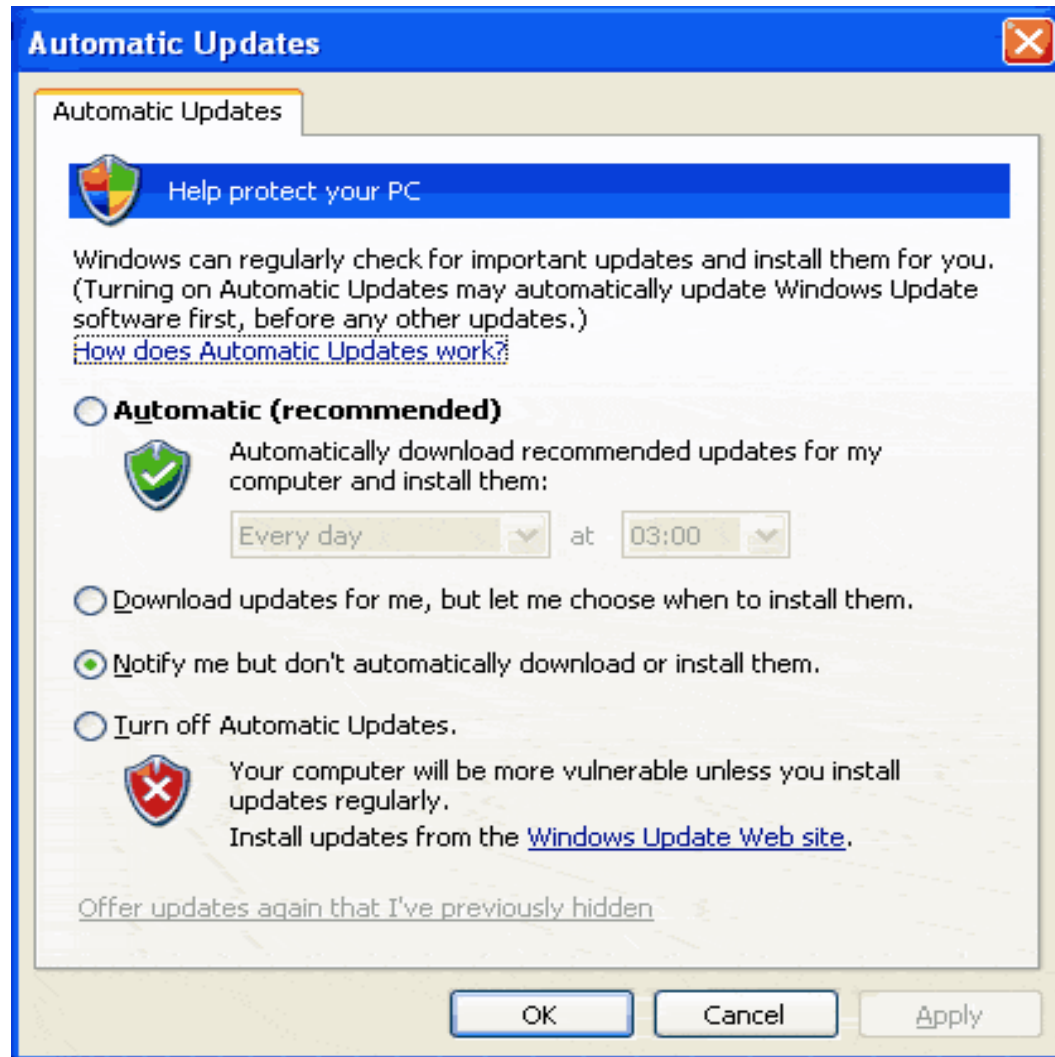


PATCHING

- Updating vulnerable applications and operating system components
- Use a tool to see what needs to be patched (secunia.com has a good free one)
- Make sure “Automatic Updates” is turned on!



AUTOMATIC UPDATES

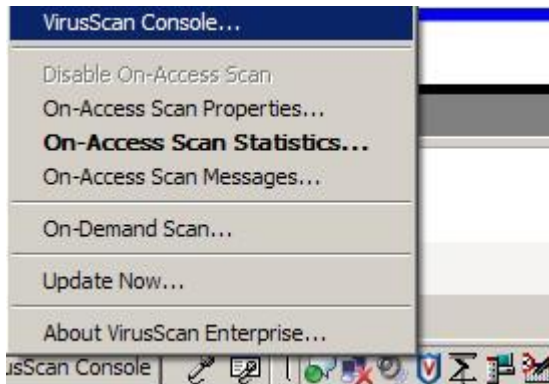


ANTI-VIRUS AND ANTI-SPYWARE

- Subscription-based service
- Use on-access AND weekly sweeps
- Use “signatures” to detect attempts at exploiting vulnerabilities
 - McAfee
 - Norton/Symantec
 - Webroot Spysweeper
 - AVG



VERIFYING ANTI-VIRUS



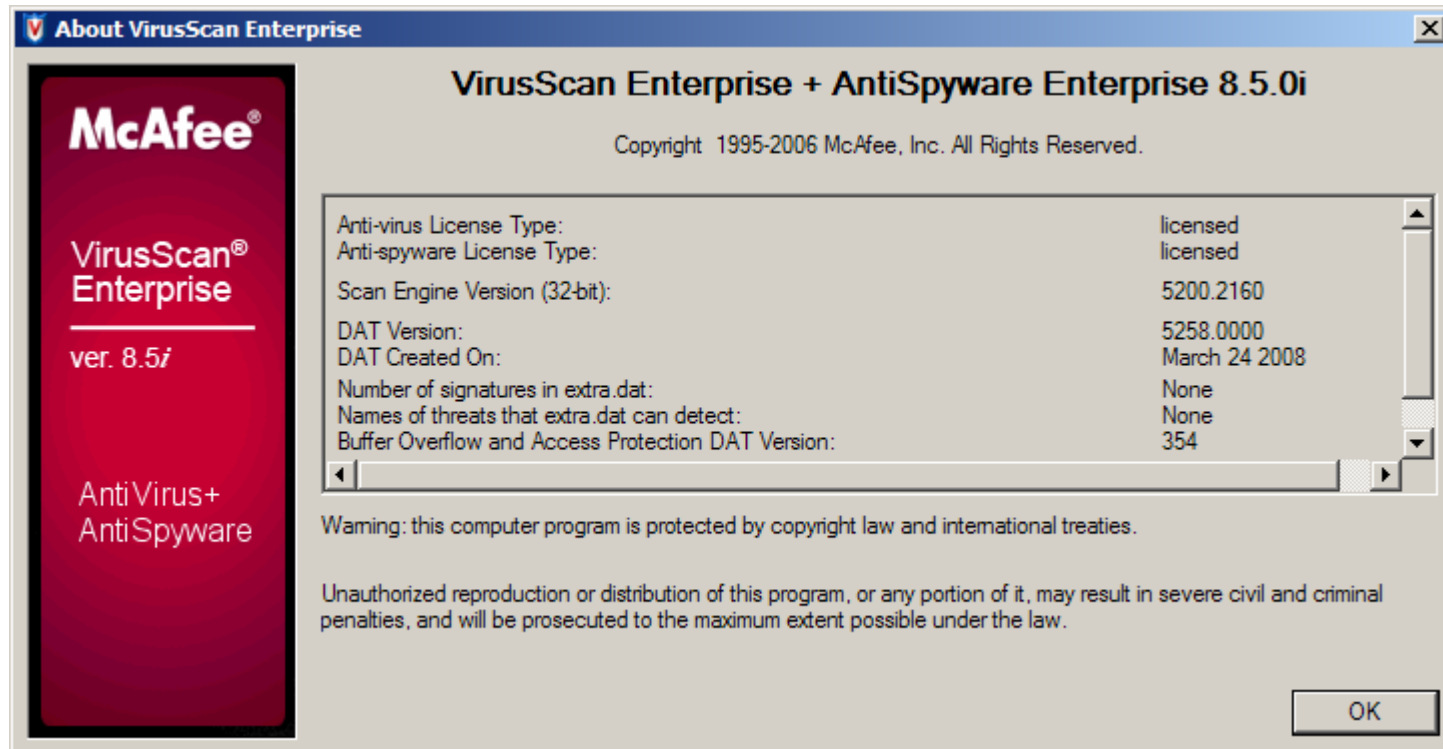
The VirusScan Console application window is shown with the Help menu open. The Help menu items are: Help Topics, McAfee AVERT Labs Threat Library, Submit a Sample, Technical Support, Repair Installation..., and **About VirusScan Enterprise**.

Task	Enabled	Last Result	Last Run
Access Protection			
Buffer Overflow Protection			
On-Delivery E-mail Scanner			
Unwanted Programs Protection			
On-Access Scanner	Enabled		
Quarantine Manager Policy			
Full Scan			
Targeted Scan			
(managed) Daily process scan		Nothing found	Monday, March 24, 2008
(managed) Weekly Full Scan 8.5		Nothing found	Wednesday, March 26, 2008
AutoUpdate			
(managed) Periodic Client Update			

Displays program information including the version, license, and copyright information.



VERIFYING ANTI-VIRUS

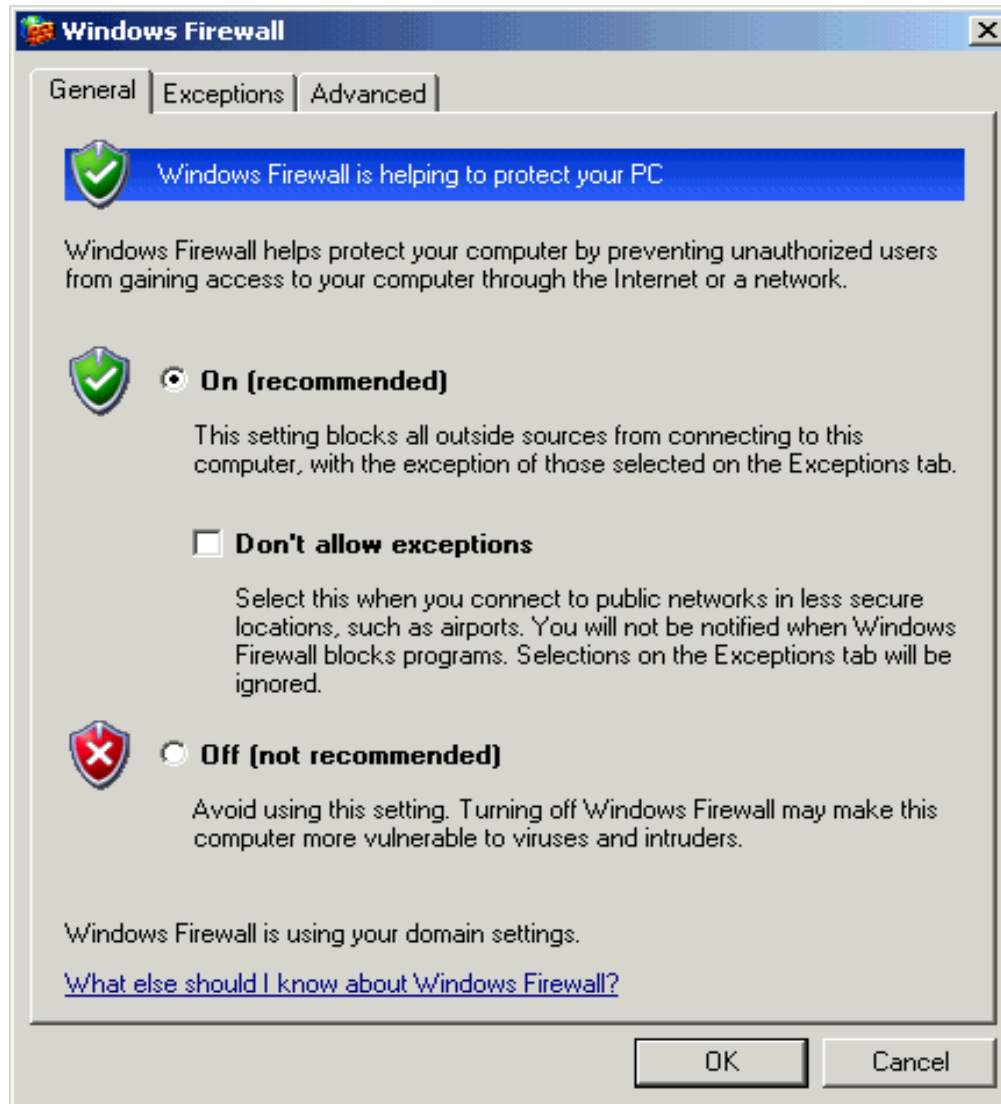


PERSONAL FIREWALL

- One comes with XP/Vista
- Will block attempts to send packets to your computer
- Others
 - Norton Internet Security/Norton 360
 - Zonealarm Internet Security Suite
 - Kaspersky Internet Security

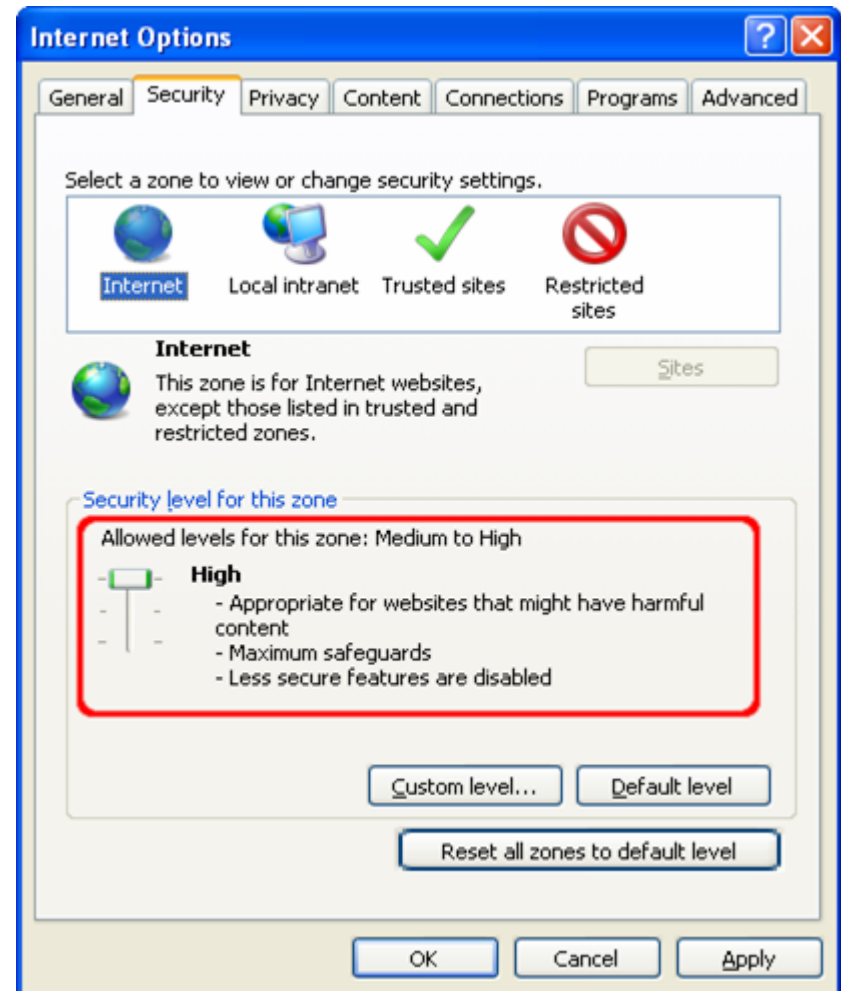


MICROSOFT FIREWALL



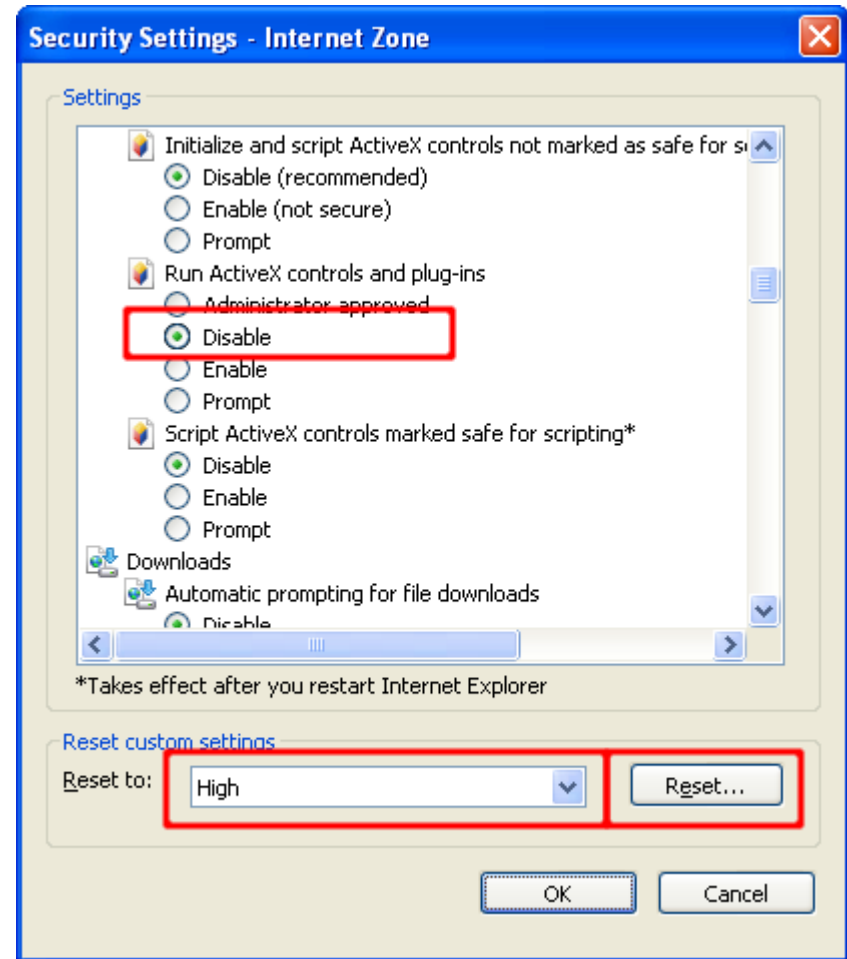
BROWSER CONFIGURATION: SECURITY

Set up Internet
security zone and
use custom settings



BROWSER CONFIGURATION: SECURITY

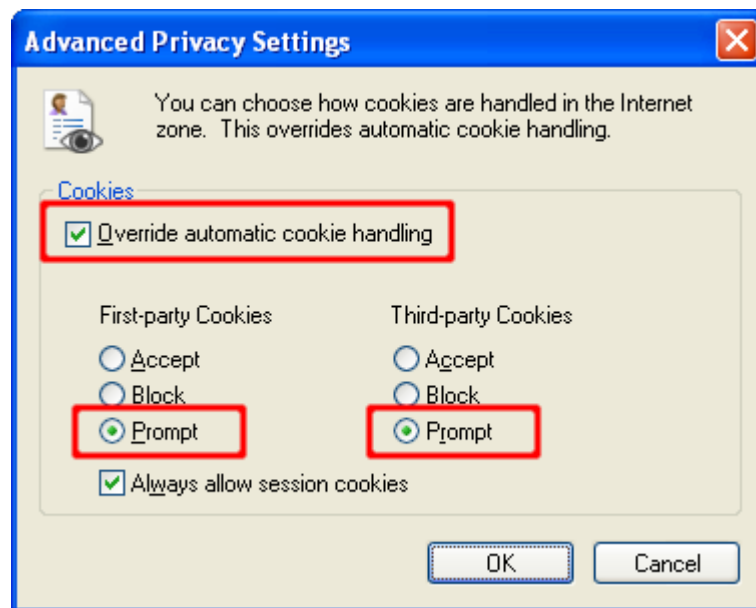
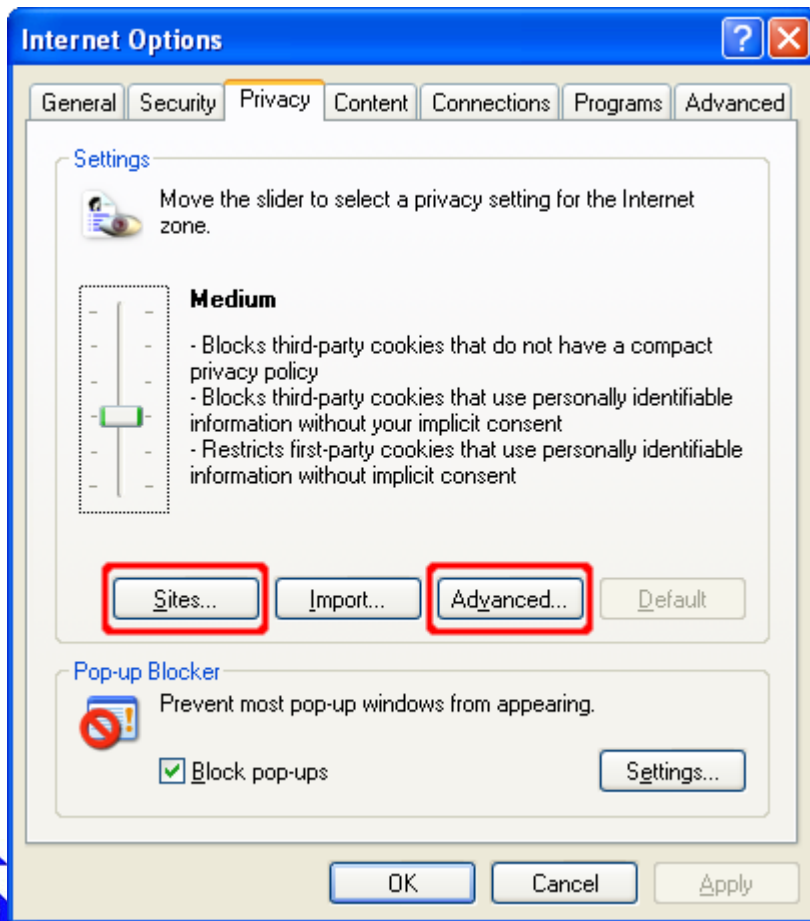
Set to **prompt** for
Active-X controls





BROWSER CONFIGURATION: PRIVACY

Privacy settings are all about cookies.



USING TWO BROWSERS

- One for routine surfing – expect it to be attacked
- Another for financial transactions
 - Mozilla, Opera, etc.
 - Be fastidious about keeping it updated
- A “clean” computer in the house is even better



BACKUPS

- Critical questions to ask:
 - What files?
 - How often?
 - What media?
 - Store where?
 - How long?



BACKUPS - SUGGESTIONS

- Make copies of important information on CD or DVD (external drives work well)
- Backup frequency depends on how often the information changes
- Put a reminder on your calendar
- Home: store in a safe if you have one
- If it's your business, invest in backup software and store off-site



IF YOU THINK YOU'VE BEEN HACKED

- Disconnect from all networks
- Back up important files
- Spysweeper and A/V will find many trojans, keystroke loggers, etc.
- Special applications to find rootkits
 - PCTools (.com)
 - RootkitRevealer



IF YOU THINK YOU'VE BEEN HACKED

- If you have a sample, upload it to [virustotal.com](https://www.virustotal.com)
- Scan backup files before restoring
- **CHANGE ALL PASSWORDS!**



LET'S SUMMARIZE

- Organized crime is rampant on the Internet, and will not go away
- In order to avoid being a victim:
 - Know they're out there, and be wary
 - Keep your computer and applications patched, or updated
 - Use a set of layered technical controls



MORE INFORMATION

Threat and vulnerability information

- www.theregister.com/security
- www.secunia.com
- www.cnet.com

Mailing Lists

- www.seattle.gov/informationsecurity
- www.us-cert.gov



FURTHER READING

US-CERT Computer Virus Resources http://www.us-cert.gov/other_sources/viruses.html

Before You Connect a New Computer to the Internet

http://www.us-cert.gov/reading_room/before_you_plug_in.html

Home Network Security http://www.us-cert.gov/reading_room/home-network-security/

Home Computer Security http://www.us-cert.gov/reading_room/HomeComputerSecurity/

Understanding Firewalls <http://www.us-cert.gov/cas/tips/ST04-004.html>

Good Security Habits <http://www.us-cert.gov/cas/tips/ST04-003.html>

Continuing Threats to Home Users <http://www.us-cert.gov/cas/alerts/SA04-079A.html>

Windows Update <http://windowsupdate.microsoft.com/>

Protect Your PC <http://www.microsoft.com/security/protect/default.asp>

Increase Your Browsing and E-Mail Safety

<http://www.microsoft.com/security/incident/settings.msp>



STILL MORE INFORMATION

Anti-Virus and Spyware Vendors

- www.webroot.com
- www.mcafee.com
- www.symantec.com
- www.kaspersky.com
- www.trendmicro.com



IF ALL WENT WELL, WE HAVE TIME FOR QUESTIONS

***City of Seattle
Office of Information Security
ois@seattle.gov***

