Malware in the Enterprise

A review of SANS course 569

March 17, 2011

Michael Hill

Overview of Course

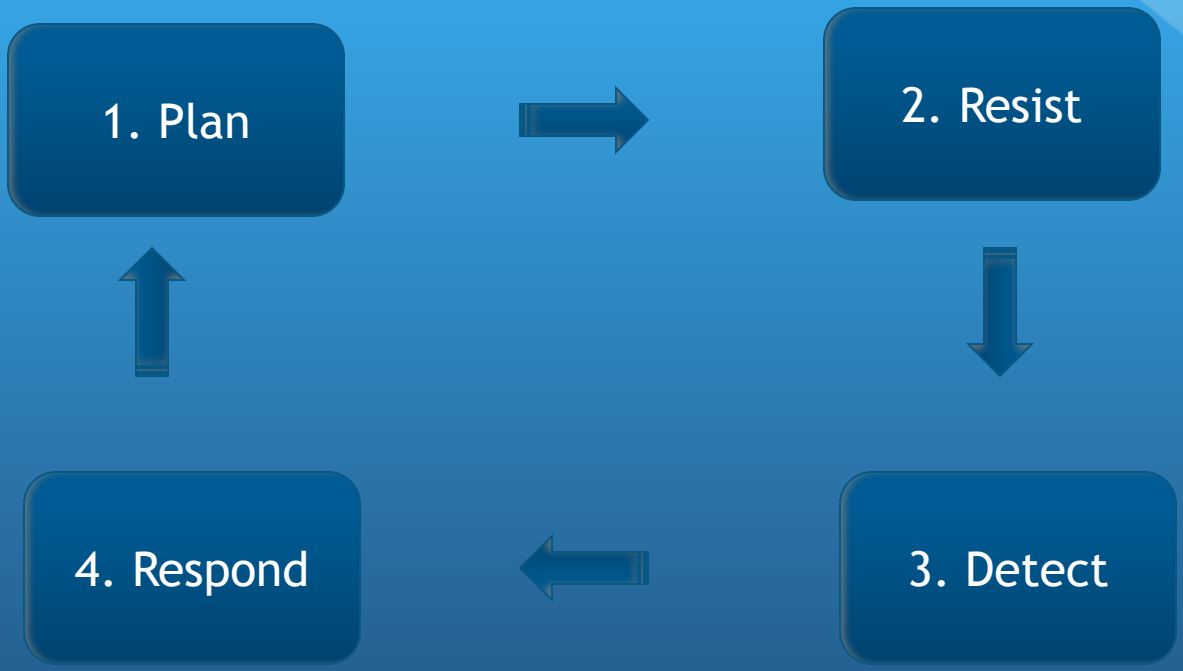
Pros

- Lots of information in books
- 2 day online course
- No travel required
- Sessions archived online for 6 months

Cons

- Lots of information in books
- Many interruptions in course
- No hands-on labs
- Fast paced (only hit topics at high level)

Incident Cycle



Day One

- Covered Detect and Respond in the Incident Cycle
  - Definition of Malware and Classifications
  - Anti-Virus
  - Humans as Malware Detectors?
  - Change Management
  - Tools to identify compromise
  - Containing and Cleaning Up Malware

Malware Definition

- According to NIST SP-800-83

  “Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications or operating system or otherwise annoying or disrupting the victim”

- SANS simplified definition:

  “Malware is code that is used to perform malicious actions.”

Forms of Malware

- Compiled binary executable
  - C, C++, Delphi, etc…
- Script that OS can execute
  - Perl, Python, VBScript, batch script, etc…
- Browser module or script
  - JavaScript, VBScript, ActiveX Object, Flash, etc…
- A file that stores data
  - Microsoft Office files, Adobe PDF documents, etc…

Malware Classifications

- Virus
- Worm
- Trojan
- Backdoor
- Rootkit
- Botnet
- Spyware
- Downloader
- Dropper

Anti-Virus

- Anti-virus tools are the most common method for fighting malware
- What should be scanned?
  - Processes, stored files, boot sectors
  - Files in transfer (email, USB key)
  - Executables and Scripts
  - Web Pages: browser scripts, ActiveX, Java applets, etc…
  - Document Files: Microsoft Office and PDF
- There is lots it does not catch
  - 55% of Zeus infected systems had up-to-date anti-virus

Humans as malware detectors?

- End users know when something doesn't feel right
  - My computer is slow.
  - It keeps rebooting.
  - There are new icons in the system tray.
- System Admins should be trained to recognize signs
  - Where to look and how
  - When to escalate and who to contact
- System Admins have discovered logic bombs in the past
  - Medco
  - Fannie May

Change Management

- Application change management makes it easier to identify “unwanted” or “malicious” changes
- Source code control software should be used to track all changes
  - Subversion, Visual SourceSafe, etc…
- Maintain separation of duties
  - Different users review code vs. checking it in

Tools to help identify compromise

- Process Explorer
  - Powerful tool for examining processes on the host
  - Replacement for built-in Task Manager
  - GUI only, but command-line tools mimic some features
- Sysinternals Autoruns
  - Comprehensive tool for identifying programs that automatically run on Windows
  - Both command-line and GUI tools
- PowerShell
  - Built-in command MS is positioning to replace command prompt

Containing Malware

- Understand scope, so you can contain infection
- Understand characteristics of the malware
- Look for characteristics across the environment
- Key malware containment options:
  - User participation – need strong communications
  - Automated tools – anti-virus, IPS, etc…
  - Disable targeted services – email, SQL, web, etc…
  - Disable network connectivity – disconnect affected systems

Malware Cleanup

- Need to decide b/w Disinfect and Restore/Rebuild
- Only disinfect if all these conditions are met:
  - Infection was non-severe
  - Able to fully remove all malware from host
  - Certain that attacker did not install additional tools
- If there is any doubt then restore/rebuild
  - Can be difficult if no backups to restore from
  - Need to make sure the files are clean
  - Catalog, backup, and examine data stored before restore
  - Sensitivity of the data will help classify severity of incident

Day Two

- Covered Plan and Resist in the Incident Cycle
  - Operating Systems
  - VDI
  - IE vs. Firefox
  - Adobe Reader
  - Microsoft Office
  - Windows Firewall

Operating Systems

- Focus of course on Microsoft Windows
  - Claims were made that Linux & Apple were less vulnerable
- Results from Microsoft SIR
  - XP + SP3 has twice infection rate of Windows 7
  - 56% of Office attacks affected programs not updated since 2003
  - 44% of browser-based exploits related to Adobe Reader
- Recommended 64 bit version of Windows 7
  - Most computers are still 32 bit
  - Hackers are less familiar (for now)
  - All kernel-mode binaries must be 64 bit and digitally signed by Microsoft

Study on Microsoft Security Bulletins

- Study conducted In March 2010 by BeyondTrust Software on Microsoft's 2009 security bulletins
- Results showed that most vulnerabilities do less harm if users are not members of the Administrators group
- % of vulnerabilities mitigated by not being an administrator
  - 100% of Office vulnerabilities reported in 2009
  - 100% of IE 8 vulnerabilities reported in 2009
  - 64% of all Microsoft vulnerabilities reported in 2009

Virtual Desktop Infrastructure (VDI)

- Technologies that allow a user's applications to run somewhere else other than on the OS of the physical workstation where the user is sitting.
- Some myths related to VDI
  - You don't need to patch VMs or install AV
  - Simply running in a VM makes software secure
  - A user's remote VM cannot access local USB ports
  - The local file system is inaccessible to VMs
  - Network traffic of VMs is safer

Internet Explorer vs. Firefox

IE

- 99% of IE settings can be configured w/ group policy
- Configure Internet Zone
  - Disable active scripting and ActiveX controls
  - Setup trusted and restricted zones
- SmartScreen Filter
- XSS Filter

Firefox

- Lower infection rate than IE
- Preference settings managed through JavaScript files
- Firefox Policies
- NoScript Add-on
  - Protect against ClickJacking and XSS

Adobe Reader

- In 2009 Adobe Reader was the most exploited application
- Surpassed Word and Excel combined!
- New versions of Reader should be pushed out as quickly as possible
- Alternatives to Adobe Reader:
  - Foxit Reader
  - Brava Reader
  - Perfect PDF Reader
  - OpenOffice

Microsoft Office

- Most exploits against Office use the pre-XML file formats with Office 2003 and earlier
- Switch to XML file formats (docx, xlsx, and pptx)
- Restrict macros and ActiveX
- Information on hardening Microsoft Office
  - Microsoft Office Security Guide
  - Microsoft Office Resource Kit

Windows Firewall

Pros

- Built-In (Free)
- Enabled by Default
- Integrated w/ IPSec
- Stateful Filtering
- Centralized Management
- W3C Extended Logging

Cons

- Only for Vista and later
- No IDS features
- No behavioral monitoring
- No centralized logging
- Complex

Windows Firewall

- Recommended that it is enabled on all systems
  - Not just for laptops and home users
- Different settings for each network category
  - Domain
  - Public
  - Private
    - Home or Work
- Order of processing for Firewall rules
  - Does not follow “First Match Wins”
  - Follows “Best Match Wins”

Questions/Discussion

Resources

- Course materials from SANS 569 Combating Malware in the Enterprise