Anti-Virus In the Wild

Eric Johansen
ejohanse@us.ibm.com

October 2005
What is this about?

- Honeypots
- Anti-virus
- Internet
Components of this Presentation

- Anti-virus Honeynet
  - Framework provided
    - System
    - Network
    - Capture
    - Analysis
Components of this Presentation

- Anti-virus Technologies
  - Pattern-based detection
  - Packers
  - AV Shoot-out
- New Technologies
  - Network-based protection
  - Application-based detection
Anti-virus Honeynet

- Network to contain the “prey”
  - Strict firewall rules
  - Incoming traffic – TCP ports 135, 137, 138, 139, 445, and 1025 – “authentic” Windows systems exposed to the Internet
Anti-virus Honeynet

- Network to contain the “prey” (continued)
  - Outgoing traffic –
    - Blocking commonly used exploit ports:
      - Windows file sharing
      - SMTP (SPAM)
    - Allow most other traffic
      - IRC, other communications to allow bot to register
    - Drop packets
      - Denying packets looks more suspicious
      - Dropping makes it appear that the host is down
Anti-virus Honeynet (continued)

- QoS – Quality of Service – network traffic priority filter
- Comprehensive network traffic logging
  - Intrusion detection
  - Basic packet logging
Anti-virus Honeynet (continued)

Anti-Virus In the Wild | Eric Johansen – ejohanse@us.ibm.com
© 2005 IBM Corporation
Analysis

- Working with live, infected systems
  - Precautions:
    - Mounting read-only ISO of Windows XP installation CD
    - Tools and data-collection script in “hidden” folder
      - Multiple tools for each data type, i.e. network connections, registry, etc. – allows for data correlation
    - “Known-good” Windows XP cmd.exe on CD
Anti-virus Honeypot Systems

- Emulate “real-world” PCs

- Average end-user desktop
  - Windows XP with SP1 installed
  - Default configuration
  - Logged in with Administrator-level privileges
  - Behind on patches and service packs

- Average end-user network
  - Poorly implemented firewall rules
  - No intrusion prevention devices
  - No bandwidth-limiting features (i.e. QoS)
Anti-virus Honeypot Systems

- 13 systems
- Cloned off of the base image
- Generic system names (XPWK01-XPWK13)
- “DHCP-like” and “default-like” IP address scheme (192.168.0.101-113)
- Systems boot automatically into Administrator-level privileged account – “User”
Anti-virus Honeypot Systems (continued)

- **Software**
  - AFICK (yet another file integrity checker)
    - MD5SUM of all files on system.
  - WinRAR
    - Compressing samples
    - Quick analysis of RAR SFX “dropper” files
  - mIRC
    - Quick connections to “botnet” IRC servers to “poke around”
  - FTP Voyager
    - GUI-based secure FTP client for transferring samples to my file server.
  - Red Cliff Web Historian
    - Quick peek at IE history logs – valuable for “blended attacks” which feature adware/spyware.
  - Anti-virus software
Roles for these honeypots

- Capture malware in a realistic environment
  - Aid in educating support staff on basic malware analysis
- Testing
  - Aid in deciding which vendor to choose.
- Early-warning system
  - Deploy systems running a stripped down version of your corporate image
    - Internet
    - Intranet
- Many more…
Anti-virus Shootout

- Example of one way to utilize these honeypots -

- Packers
  - Tools utilized to “repackage” PE (portable executable) files to mask and compress them.

Anti-virus Shootout

- Packers (continued)
  - Original (no modification)
  - Zip Self-Extracting Archive (SFX)
  - RAR SFX
  - ASPack 2.12
  - ASProtect 1.23 RC4 build 08.07
  - exe32pack 1.42
  - EXECryptor 2.0
  - ExeStealth 3.04
  - FSG 2.0
  - MEW11 SE 1.2
  - MoleBox 2.3.3
Anti-virus Shootout

- Packers (continued)
  - Morphine 2.7
  - Packman 0.0.0.1
  - PECompact2 2.55
  - PE-PACK 1.0
  - Petite 2.3
  - UPX 1.25W
  - WWPack32 1.20
  - yoda's Crypter 1.3
  - yoda's Protector 1.0b
  - (Win)UPack 0.27 beta
Anti-virus Shootout

- Anti-virus Software Utilized
  - Symantec AntiVirus Corporate Edition 10.0.0.359 with engine 103.0.2.7
    [6/5/2005 rev. 37 definitions]
  - Trend Micro PC-cillin Internet Security 2005 with engine 7.510.1002 [2.669.00
    (06/06/05) definitions]
  - McAfee VirusScan Professional 2005 (9.0) with engine 4.4.00 [4.0.4506
    (06/03/05) definitions]
  - Sophos Anti-Virus 5.0.3 [3.94 definitions]
  - Kaspersky Anti-Virus Personal Pro 5.0.14 [06/06/05 10:42:31 AM definitions]
Anti-virus Shootout

- Anti-virus Software Utilized (continued)
  - eset NOD32 Antivirus System 2.12.3 [1.1130 (20050606) definitions]
  - CA eTrust EZ Antivirus 6.2.1.1 with engine 11.5.0.0 [9185 (Jun 6 2005) definitions]
  - Norman Virus Control 5.80 with engine 5.82.01 [2005/06/04 definitions]
  - BitDefender 8 Standard with engine 7.01620 [6/6/2005 (174896 detections) definitions]
  - Panda Titanium Antivirus 2005 (4.02.00) [06-06-2005 (96172 detections) definitions]
Anti-virus Shootout

- Anti-virus Software Utilized (continued)
  - AVG Anti-Virus 7.0 Professional (7.0.323) [267.6.4 (6/6/2005) definitions]
  - Dr.Web Scanner for Windows 95-XP v4.32b [2005-06-07 (76686 detections) definitions]
  - Hauri ViRobot Expert 4.0 with engine 2005-06-05.00 [2005-06-05.00 definitions]
Anti-virus Shootout

- **Testing Mechanism**
  - Files securely downloaded to the system in large password-protected zip bundle
  - All samples uncompressed to test realtime.
  - Realtime is then turned off, all samples are uncompressed, then a manual scan is initiated.

- Results follow…
Anti-virus Shootout

- Realtime Scanning Detection Rate Top 5
  1. 81% Kaspersky
  2. 57% BitDefender and Sophos (tie)
  3. 52% Trend Micro
  4. 43% McAfee and Dr.Web (tie)
  5. 24% Symantec and AVG (tie)
Anti-virus Shootout

- Manual Scanning Detection Rate Top 5
  1. 90% Kaspersky
  2. 76% BitDefender
  3. 71% Norman
  4. 67% McAfee
  5. 57% Trend Micro and Sophos (tie)
Anti-virus Shootout

- Conclusions?
  - Even “old” viruses such as Nimda.A pose a threat when repacked
  
  - Packer support within AV packages is lacking.
  
  - Additional protection is needed beyond classic pattern-based
    - Network protection
    - Buffer overflow protection
Anti-Virus Blooper Reel

- Actual infections from my honeypot systems
- Names of products will not be mentioned to protect the innocent (but the images should be telling).
Anti-Virus Blooper Reel

Virus Alert

File:
c:\windows\system32\winlpp32.exe

Infected with:
Backdoor.Agobot.KM

BitDefender Action:
BitDefender has blocked this virus?your computer has NOT been infected.
Anti-Virus Blooper Reel
Anti-Virus Blooper Reel

While opening file: C:\csrsss.exe
Virus identified Worm/Agobot.38.K

Select an item to format its description.

Capacity: 1.99 GB
- Used: 1.22 GB
- Free: 782 MB

arcl_dr.exe
arcsetup.exe
AUTOEXEC.BAT
AVG7DB_F.DAT
boot.ini
CONFIG.SYS
csrsss.exe
Anti-Virus Blooper Reel

An unexpected error occurred in Norman Virus Control.

- Module: cdaw.exe
- Location: C:\Virus\virus.exe
- Time stamp: Jan 12 2005
- Error code: 00130000
- Error text: NAPERC_TIMEOUT

Please make note of the information above before contacting support.

© 2005 IBM Corporation
Anti-Virus Blooper Reel

Real-time Scan
Trend Micro PC-cillin Internet Security has detected a virus, spyware application, or other Internet threat, and performed the action specified.

Infected file: C:\WINDOWS\system32\msmgr.exe
Virus name: WORM_RAOTT.Gen
User name: User
Scan action result: The Quarantine action was unsuccessful. Manually delete the file if you are sure that it is not needed.

Note: If Search for and clean Trojans is enabled and is executed after scanning, you can click Next to view final scan result information.
Anti-Virus Blooper Reel
Questions?

Eric Johansen
ejohanse@us.ibm.com

http://www.malwareblog.com/