

Antivirus Technology

CSH6 Chapter 41 "Antivirus Technology" Chey Cobb & Allysa Myers

Copyright © 2015 M. E. Kabay. All rights reserved.



Topics

>AV Terminology >AV Issues History of Viral Changes Antivirus Basics Scanning Methodologies Content Filtering > Deployment Policies & Strategies



AV Terminology

1 virus, 2 viruses – don't use "viri" or "virii" 8 > AV = antivirus; AVP = antivirus product > AVPD = AVP developer Prevalence statistics □ In the wild – THOUSANDS (3405 in Nov 2014) ✓ Joe Wells' WildList → http://www.wildlist.org □*In the zoo* – > 1M for Windows ICSA Labs Anti-Virus Product Developers (AVPD) Consortium * Coordinates scientific work of AVPDs http://tinyurl.com/3yhfcsn

* <u>http://www.icsalabs.com/technology-program/anti-virus</u>

AV Issues



- New viruses appear frequently
 - Out-of-date scanners cannot stop new viruses or variants
 - □Although *heuristic* scanners help a lot
- AV products often misconfigured
 - Don't scan right file types

Some are not enabled for auto-update – critically important!

- Resistance to AV
 - □Upper management don't like them

□Constant demands for upgrades, costs of subscriptions

□Paradox of success: *if it works, no evidence of need*



History of Viral Changes (1)

Early viruses were not much of a problem
 Simple code, functions
 Spread via floppy disks – slow
 Very few in existence
 Fewer in the wild

Early AV products often focused on specific viruses



Became impossible to maintain systems

Moved to signature-based and heuristic scanning (see later)

History of Viral Changes (2)



- ~1995 MS-Office introduced Visual Basic Script (VBS)
 - Allowed sophisticated macro programming
 - Auto-execution was vigorously opposed by security experts (including MK)
 - Potentially converted office documents into programs...
 - ✓ ...and that's what happened
- Majority of today's viruses are VB macros
 - Easy to spread through infected documents and Web sites
- Instant messaging (IM) & peer-to-peer (P2P) networks also 6 exploited to spread malware Copyright © 2015 M. E. Kabay. All rights reserved.

Antivirus Basics

Introduction □Virus detection inexact □Still see false positives (Virus!!! – but not) □& false negatives (A-OK – but not) □CPU & I/O load can become noticeable > Topics **Early Days of AV Scanners** □Validity of Scanners □Scanner Internals **AV Engines & DBs**



SCANNERS

horrifying



Early Days of AV Scanners

- AV makers disagreed on how to name viruses
- No central facility for counting unique viruses
- AV vendors used wildly different virus-counts in their advertising
- Users confused / frustrated by conflicting information
- Charlatans marketed ineffective products
- None of early scanners could catch all known viruses



Validity of Scanners

NCSA* started AVPD Consortium 1991 **Established testing criteria** □ Created the zoo – AVPs shared viruses Raised standards for required detection levels every quarter Dr Richard Ford established testing standards AVPs disagreed on strategies Look only for new viruses? Look for all known viruses? Joe Wells founded WildList in 1993 □ Cooperative effort to list & name all known viruses Distinguish between those found on user systems & those found only in laboratories

*NCSA = National Computer Security Association
 M. E. Kabay was Director of Education from 1991 to 1999
 NCSA ⇒ ICSA ⇒ TruSecure ⇒ CyberTrust ⇒ Verizon Business Security

Scanner Internals

- Fundamental problem was that Windows and Mac OS lacked security kernel
 - Every process runs as if it has root privilege
 - **AVPs compensate for this design decision**
- Functions include
 - Specific detection looking for infections by known viruses
 - Generic detection looking for variants of known viruses
 - Heuristics finding unknown viruses by spotting suspicious behavior or code/file structures
 - Intrusion prevention monitoring knownsuspicious systems changes and behaviors to prevent unknown infections

AV Engines & DBs



- Engine is the expert system that looks for malicious software
- Signature database (DB) includes
 Fingerprints of known viruses
 Rules for heuristic scanners
 - Code sequences characteristic of specific viruses
- Must update both signatures and engines
 - Used to recommend monthly, then weekly updates
 - Now (2009) essential to allow at least daily updates – or hourly or minute-by-minute



- Enable automatic updates update whenever necessary by communicating with servers
- □Software looks for change in checksum indicates change

Updating: "LiveUpdate"







Scanning Methodologies

When to scan?

- □Ideally, on every file open ("on access scan")
- □Continuous monitoring of new files
- May be performance issues on old systems but not today
- Functions of scanning (see next slides)

 - **□Generic Detection**
 - **Heuristics**
 - Intrusion Detection & Prevention



"Hey, stop scanning my cards!"

Specific Detection

NORWICH UNIVERSITY

- > Look for characteristic signature strings
 - Most scanners use selective screening
 - ✓ Look for virus code in general areas of programs
 - ✓ Saves time but risks false negatives

Power of the test

- □The higher the success rate in spotting viruses (the lower the false-negative rate),
- The higher the frequency of false positives (falsely claiming that uninfected files are viruses)
- Generally offer disinfection routines

 - □Quarantine
 - **Delete**



Generic Detection



- Many malware authors & distributors are trying to make money
 - □Therefore use open-source code
 - Malware widely distributed and updated by criminals
- Therefore modern AVPs scan for common properties
 - □Widely-known viruses, Trojans...
 - In early days of file-infectors, concern about potential damage of cleaning infected programs
 - But today's malware typically installs discrete files and registry entries
 - ✓ Easier to fix without danger

Heuristics

NORWICH UNIVERSITY

- Rule-based expert systems
- Static heuristic scanners
 - Identify most likely places where viruses reside
 - □Look for known styles of viral code
 - Examines programmatic logic of suspect regions
 - Assign probabilistic score based on many clues from structure
- Dynamic heuristic scanners
 - □Similar methods to spot potential problem-code
 - **Emulate execution of the code**
 - ✓ Virtual environment = sandbox
 - ✓ Identify harmful actions
 - □Remove virus
- Widespread distribution & use of heuristic scanners have led to rapid discovery of new viruses

Heuristic from Greek ຖευρισκειν – to find





Example: NAV





symantec.

Norton SystemWorks 2005

NAV Auto-Protect

😣 Norton AntiVirus Options

System

Auto-Protect

Script Blocking

Manual Scan.

Internet

Email

Internet Worm

Protection

Instant Messenger

LiveUpdate



Threat Categories Miscellaneous

Auto-Protect

How to stay protected

- Enable Auto-Protect (recommended)
- Start Auto-Protect when Windows starts up (recommended)
- Show the Auto-Protect icon in the tray

How to respond when a virus is found

- Automatically repair the infected file (recommended).
- 🧧 Try to repair then quarantine if unsuccessful
- Deny access to the infected file.

Whic

- Θ. ed).
- \odot

Default All

h file types to scan for viruses		
C <u>o</u> mprehensive file scan	ning (recommende	
Sca <u>n</u> files using SmartSc	an <u>C</u> ustomize	
Scan <u>w</u> ithin compressed	files	
ок	Cancel	

NORWICH PRSITY

X

More Info.

NAV Heuristics

😣 Norton AntiVirus Options

System

▶ Auto-Protect

Script Blocking

🔻 Manual Scan

Bloodhound

Exclusions

Internet

▶ Email

Internet Worm Protection

Instant Messenger

LiveUpdate

Other

Threat Categories
 Miscellaneous

Bloodhound M

How to protect against new and unknown viruses

- Enable Bloodhound heuristics (recommended)
 - Highest level of protection
 - Default level of protection (recommended)
 - Lowest level of protection

NORWICH

X

More Info.

NAV E-mail Options

😣 Norton AntiVirus Options

System

Auto-Protect

Script Blocking

Manual Scan

Internet

🔻 Email

Advanced
Internet Worm Protection
Instant Messenger
LiveUpdate

Other

Threat Categories
 Miscellaneous

Email Scanning

What to scan

- 🗸 Scan incoming <u>E</u>mail (recommended)
- 🗸 Scan outgoing Email (recommended)

How to respond when a virus is found

- Automatically repair the infected file (recommended)
- 🗧 Ask <u>m</u>e what to do
- Repair then quarantine if unsuccessful
- Repair then silently guarantine if unsuccessful
- Repair then silently delete if unsuccessful

How to increase protection

🔽 Enable <u>W</u>orm Blocking (recommended)

OK

🔽 Alert when scanning email attachments

Cancel

Default All



×

More Info

NAV Anti-Worm Measures

23



NAV LiveUpdate Settings



More Info.

😣 Norton AntiVirus Options

System

Auto-Protect

Script Blocking

Manual Scan

Internet

Email
 Advanced
 Internet Worm
 Protection
 Instant Messenger
 LiveUpdate

Other

Threat Categories
 Miscellaneous

Automatic LiveUpdate

How to stay updated

Enable automatic LiveUpdate (recommended)

How to keep your virus protection updated

Apply virus protection updates (recommended)

- Apply updates without interrupting me (recommended)
- 👝 Notify me when updates are available

How to keep Norton AntiVirus updated

🔽 Notify me of Norton AntiVirus <u>p</u>rogram updates (recommended)

How to stay protected

Launch QuickScan immediately after virus protection updates are installed (recommended)

Default All

NAV Alert Settings

😣 Norton AntiVirus Options

System

Auto-Protect

Script Blocking

Manual Scan

Internet

r Email	
Advanced	
Internet Worm Protection	
Instant Messenger	
LiveUpdate	



Threat Categories
 Miscellaneous

Miscellaneous

What to do when repairing files

Create backup file in Quarantine before attempting a repair

Cancel

How to keep Microsoft Office documents protected

🔽 Enable <u>O</u>ffice Plug-in

What to do when virus protection is out of date

🔽 Alert me if my virus protection is out of date

How to control access to option settings

<u>Enable password protection for options</u>



Page Defaults

X

More Info.

How to protect my product

Enable protection for my Symantec product

OK.

Default All

Immune Systems

- Ideal: spot infection, fix infection, heal system
 - Use network access to additional resources as required
 - > Monitor behavior of connected workstations

cel

- Send suspect files to central server
- Install suspect code on testbenches
- Analyze virus, generate signature
 Send out to all connected computers (push vs)
 - pull)
 - Don't bother people unless necessary

Intrusion Detection & Prevention



- 1st line of defense: spot incoming virus
 - Particularly effective by scanning incoming e-mail
 - Also helpful to scan outgoing e-mail
- But some polymorphic viruses encrypt their code – defeat scanners
- Some AVPs use CRCs to spot changes in programs
 All changed programs will have a CRC different from that recorded originally
 Investigate changed programs further
- Special emphasis on spotting abnormal behavior

Content Filtering



- Early years "no viruses from documents"
 - □Then macro viruses became prevalent
- "No viruses from e-mail"
 - □Then e-mail enabled worms appeared
- "No viruses from unopened e-mail"
 - So viruses written that activate when preview pane shows content
- HTML code being used for harmful purposes
- Content filtering scans for suspect code and attachments – prevents receipt by users

How Content Filters Work



- Scan all incoming data on specific ports
 - Compare traffic using rules and strings
 Can forbid all or types of attachments
- Interact with AVPs
 - Send suspect files to AVP
- But all of this requires stated policies



Efficiency and Efficacy



- Operations run on mail server can see performance issues
- Scanning all incoming & outgoing e-mail raises privacy issues if policies not established to remove expectation of privacy
- May have to limit size of e-mail attachments
- Problems with quarantine may pile up false positive e-mail, frustrate users & administrators
- Need to establish response procedures for e-mail abuse
 - Consider not only technical issues
 Also include legal & HR departments



AV Deployment

- Desktop systems
 - Must prevent users from disabling scanners
 - ✓Use reasonable fullsystem scan freq
 - Schedule off-hours only
 - Definitely require scan-on-open



✓ Include removable devices (flash drives, DVDs, CDs)

□Can set passwords on configuration of AVP

- Must maintain up-to-date coverage of ALL connected systems in network
- □Push updates from server to desktops
- Servers focus on downloads, high traffic

Policies & Strategies

- Detail user responsibilities
- End-user AV awareness important
- Specify specific tasks for different roles
- Monitor compliance
 - Ensure upper management compliance / support
- Incident Response Team and emergency plan
- Analyze every virus infection

Requires report from every infected workstation

Identify holes in current procedures & policies

□Keep records – spot trends, trouble spots







Now go and study

Copyright © 2015 M. E. Kabay. All rights reserved.