NHS Information Authority

Virus Incident Management at the Gateway

David Harley, NHS Information Authority

use the NHS number

NHS Information Authority

whoami

- David Harley
- NHS Threat Assessment Centre Manager
- Anti-Virus/Email Abuse Specialist
- Independent AV Researcher/Author
- Long-standing member of AVIEN, Team Antivirus and various other affiliations.

AVIEN

use the NHS number

NHS Information Authority

What *is* malware management?

- Proactive
- Reactive

use the NHS number

NHS Information Authority

Policy, Standards & Guidelines

- Conformance with legislation: data protection, computer misuse etc.
- Formulation/implementation of internal standards
- Internal policy development
- Conformance with external standards and certification: ISO17799 etc.

use the NHS number

NHS Information Authority

A.6.3 *Responding to security incidents and malfunctions*

- *Control objective:* To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.
- *Controls*
- **A.6.3.1** *Reporting security incidents*
- Security incidents shall be reported through appropriate management channels as quickly as possible.
- **A.6.3.2** *Reporting security weaknesses*
- Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.
- **A.6.3.3** *Reporting software malfunctions*
- Procedures shall be established for reporting software malfunctions.
- **A.6.3.4** *Learning from incidents*
- Mechanisms shall be put in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.
- **A.6.3.5** *Disciplinary process* The violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process.

use the NHS number

NHS Information Authority

Education, Training and Information Dissemination

- Education and Training/Self-Education
- Threat Information Gathering
- Helpdesk/IS/Management/Staff Training
- Information channels/dissemination of information
- On/offline publications
- Online services (Intranet web pages, mailing lists)

use the NHS number

Multi-Layered Systems/Network Administration

- Level 1: desktop protection, including remote users and home users whose home systems may interface at some point with their work systems.
- Level 2: workgroup/LAN server protection, including file and print servers, application servers, database, email and Intranet servers.
- Level 3: Internet/Extranet Protection, including perimeter devices, mail gateways, proxy servers, VPN hosts and other choke points

Development Areas

- Product evaluation
- Configuration and functional testing
- Performance and compatibility testing
- Installation/rollout/update testing and execution
- Incident management testing
- Meeting threats the market doesn't yet address

Incident Handling

- Incident logging/Reporting
- Confirming existence of malware, if necessary by submission of samples
- Disinfection/disinfestation
- Dealing with direct damage
- Advising sources of infection
- Secondary Infection and damage
- Secondary damage (including psychosocial issues)
- Post-infection/disinfection remediation/uprating
- Dealing with false alarms
- Hoax management
- Regular Reports/Analysis
- Re-evaluation

What do you really want to do with malware at the perimeter?

- Incoming:
  - clean if cleanable, block if not
  - verify and warn the source if possible
  - log and learn from the incident (monitor effectiveness, analyse trends)
- Outgoing:
  - As above, but include cleanup of an internal source and feed back into improving security posture

What happens in real life?

Incoming

- Viruses are blocked
- Disinfectables may be disinfected
- The apparent source is warned
- The intended recipient is warned
- An aggregated report is published in due course

Real Life Revisited

Outgoing

- Mail is blocked, possibly bounced. (Hopefully)
- Sender is notified. Whether there's a follow-up from the Gods of IT depends on service and configuration.
- Recipient may be warned.
- Report in due course.

Building the Extension

- .bas, .bat, .chm, .cmd, .com, .cpl
- .crt, .eml, .exe, .hlp, .hta, .inf, .ins
- .isp, .js, .jse, .lnk, .mdb, .mde, .msc
- .msi, .msp, .mst, .pcd, .pif, .reg
- .scr, .sct, .shs, .url, .vbs, .vbe
- .wsf, .wsh, .wsc

Caveats

- Malware may evade generic controls that aren't aware of specific vulnerabilities
- Filename extension vs. true file type
- Poorly thought-out rules for comparing extension and file type
- Unscannable objects: zips/archives, encrypted files

Very High Risk

- File types almost never exchanged legitimately by email and used by mass mailers: e.g. .PIF, .LNK, .BAT, .SHS.
- Filenames with double extensions, especially where one type is a non-executable and the last one isn't e.g. myfile.txt.pif
- File types that don't match the filename extension, and the file type is more dangerous than the filename suggests

Essential Blockings

- .BAT .COM .SHS
- .LNK .SCR .CHM
- .HLP .CPL .PIF
- .SHB .DLL

High Risk

- File types heavily used by mass mailers, but are also exchanged legitimately, e.g. .EXE, .SCR(?), .VBS(?)

Medium Risk

- File types not frequently used by mass mailers, but could carry executable/malicious code.

Medium-Low Risk

- Executable files of types not currently associated with virus action, or only with extinct viruses, or zoo viruses (esp. proof-of-concept viruses that exist only “to show it’s possible”)

Low Risk

- Non-executables.

Uncategorisable

- Files whose executability/infective status is unknown/can’t be determined.
- Files of unknown file type.
- Encrypted files
- Archives that can’t be unpacked (fully or at all) for scanning.

Tripod model of security

- The number of file types that could be exploited by a virus runs into hundreds, and the final choice has to be made by the end site. Blocking all of them, or all the options on one of the common lists, at any rate, is easy, but not secure.
- Privacy and Integrity, fine. Aren’t we also supposed to maintain Availability?

Generic Filtering & Managed Services

- One size doesn’t fit all

“For every locked front door, there’s a back door...”

- End sites must allow for the passage of legitimate traffic using normally proscribed file types where necessary.

Causing an Incident

- "...any event **which** is not part of the standard operation of a service and **which** causes, or may cause, an interruption to, or a reduction in, the quality of that service." (CCTA)

BS7799

- Timely reporting of security incidents
- Reporting of actual or possible security weaknesses and threats to systems and services
- Reporting of software malfunctions
- Quantification and monitoring of type, volume and cost trends of incidents and malfunctions
- Implementation of a process for dealing with the violation of security policies and procedures.

Security Incident

- A security incident is defined as "any breach or potential breach of information/data security …Incidents may be internal, external or both..."

What constitutes a virus/malware incident?

- "Any case where a program reports a potential virus or Trojan symptom…In such a case, it's perfectly legitimate to run an up-to-date and reputable anti-virus package under controlled conditions.….In fact, it's legitimate to scan for viruses even where there are no perceived virus indicators whatsoever."

Reports and notifications: frequent assumptions

- The approach already implemented is optimal and does not customer review or monitoring.
- Incidents are fully managed automatically.
- The point of information gathering is, therefore, to prove to the customer that everything works as it should. Reports of incidents managed need only be retrospective, aggregated data to take to the Board.
- There is no need to identify sources of infection. Notifying the sender is enough, and the sender is always the person in the From: or Reply-To field.

What's the Ideal?

- Clean and forward what you can, and deny entry to what you can't clean.
- Manage all incidents
  - Notify and assist infectees inside the organisation
  - Notify external infectees and suggest sources of assistance
- This assumes you can identify the real source

Taste and Discrimination

- Discriminate against spoofers in terms of notification.
  - Turn off alerts for massmailers
  - Turn off alerts altogether
  - Modify alerts to acknowledge that the alert may be misdirected

Some Scenarios (1)

- No infection detected: pass it on.
- No specific virus infected, but contains suspicious object. Discard, quarantine, or pass on with warnings to sender and recipient. (Some services send the warning in a separate message which may or may not arrive before the infected message!) Contentious...
- Disinfectable virus detected. Clean and pass on, or discard, or pass on with warnings. Clearly, first option is best incident management.
- Non-disinfectable virus detected. Delete infectable object and pass on message, or pass on a standard advisory message, or pass on undeleted with warnings, or discard with no warning.

[More detail]

- No known malware detected in message. No attachment. Mail passed on. Transaction not logged.
- No known malware is detected in message/attachment. Attachment file type/file name extension turns out to be proscribed. Mail discarded, quarantined, or passed on but flagged as suspicious? Sender notified? Recipient notified? Transaction logged automatically? What level of detail? Transaction checked manually by servicing organisation? Customer notified to allow any necessary incident handling?
- Known malware is detected in message. Classified as infected but contains legitimate message content. Mail discarded, quarantined, or passed on but flagged as infected. Sender notified? Recipient notified? Transaction logged automatically? What level of detail? Transaction checked manually by servicing organisation? Customer notified for incident handling?

Scenarios and questions to ask your service/software supplier

- Known malware is detected in message. Contains no legitimate content. Mail discarded, quarantined, or passed on but flagged as infected. Sender notified? Recipient notified? Transaction logged automatically? What level of detail? Transaction checked manually by servicing organisation? Customer notified?
- Message content suggests known virus. Attachment is infected. Mail discarded, quarantined, or passed on but flagged as infected? Passed on but attachment deleted? Sender notified? Recipient notified? Transaction logged automatically? What level of detail? Transaction checked manually by servicing organisation? Customer notified?

Blah, blah...

- Actually or possibly infective. Origin is internal to the organization. Any change in process?
- Actually or possibly infective. Origin is external to the organization. Any change in process?
- File encrypted: no meaningful scan possible. What action? Notification?
- Message digitally signed. Notification? Will it unhinge the signature?
- Virus is identified as spoofing virus. Any change in process? (Try to identify real sender? Notify apparent sender with caveat?)

Massmailers and spoofers

Anti-spoofing

- Many products don't modify alerts according to the virus.

Actions

- Quarantine
- Pass Through/Back Uncleaned with notification
- Discard

Why tell the sender?

- If it's one of your users, it's your job to fix 'em
- If not:
  - it's socially responsible to offer info
  - Addresses the global problem over the long haul
  - But you have to be right about who is the sender!

Why tell the recipient?

- (apart from saying, "Look, this wonderful product is saving you from viruses")

Incident management

- How does a service handle infection?
- Does it detect malware and take no action (alert only), delete everything, or clean what can be cleaned?
- If a virus is processed, there's an infected machine somewhere. Is the apparent owner of the machine notified? What if the virus spoofs? Does the service distinguish between spoofing and non-spoofing viruses and notify accordingly? If not, does it at least modify its standard notification message to take spoofing into account? Can notification text be configured or specified by the customer?

Questions to resolve

- Does the recipient need to know about an infected message? Does the need to know vary according to the virus (spoofing/non-spoofing)? Is it possible to turn off notification to the recipient if the infected message is discarded anyway? Does the product offer a choice? If the service provider also provides messaging services and charges on a message volume basis, do they allow for exemption from charges arising from the generation of multiple alerts? Can they notify the customer as well or instead by diverting recipient notifications to an IT administrative account to allow the customer to monitor virus activity and intervene if appropriate?
- What does the client organisation regard as a responsible modus operandi for dealing with an incident, and does it match the view of the service management supplier? Is it enough to block incoming malware, or only to inform the *apparent* sender of a spoofing virus? Does the software discriminate between spoofing and non-spoofing viruses? Does the wrapper/rules engine have the same level of discrimination as the AV engine?

The Difference Engine

- Do you differentiate between senders within the organisation and external senders? Can notifications be regulated by domain?
- Do you scan at the email gateway inbound and outbound? (Do you assume that all malware is inbound?)

Logs and Reports

- What logs are kept? Does the *customer* have access to full logs, or partial logs, or none?
- How regular are reports? How detailed?

Keep it zipped

- Do you scan archives? Do you scan nested archives? What archive formats does the service scan? How does it treat archives it can't scan?

Cryptic Comments

- How do they handle encrypted archive files (.ZIP etc.) and other encrypted files? (Scan and clear, scan and flag, scan and discard or quarantine?)
- How do they handle encrypted messages?
- How do they handle signed messages?
- Do they recognise organisation-specific EDI transaction sets?

Configurability

- What degree of configurability does the service have? Does it match the configurability of the AV engine?
- What handling choices are you offered? Block/discard? Quarantine? Pass through flagged?

Maintenance and testing

- What do they do manually to maintain the efficiency of the service?
- Do they routinely follow up alerts, or only when a problem is flagged?
- Do they boost the volume of alerts with aggressive EICAR testing?

Traffic Cop

- Do they include any form of traffic analysis to flag massmailer activity and other potential abuse?

Hoax Virus, Hoax Solution

From: Administrator [mailto:Administrator@xxxxx]
Sent: Thursday, September 18, 2003 11:41 AM
Subject: Virus Hoax

You have sent an Email that contains a Virus Hoax.
Please refer to http://vil.nai.com/VIL/hoaxes.asp for further information.
This message was sent by xxxx Email scanning software.
Administrator

The End

- david.harley@nhsia.nhs.uk
- david.harley@nhs.net
- macvirus@dircon.co.uk