

McAfee Anti Virus

The background features a green-tinted technical illustration of a virus particle. The virus has a central core with a logo resembling the letter 'E' inside a square. It is surrounded by a complex, multi-layered structure. The entire scene is set against a dark green background with a grid pattern and several concentric circles and lines, suggesting a technical or scientific environment.

A Technical Overview

Matthew Cook

<http://escarpment.net/>

Introduction



- The past
- A project overview
- What is available now
- Dealing with incidents
- The need to patch
- Problems
- Futures

The Past

- Loughborough University has used the McAfee Anti Virus product for many years
- NAI Network Associates
- Dr Solomon's Anti Virus tool kit
- Anti Virus requirements have changed

A Project Overview

- A specific 'Virus Software Review' project
- Provision of Anti Virus Software
- Standardisation of version and builds
- Improving distribution
- Improving documentation
- Review of Virex for Macintosh

Moving on...

- McAfee Virus Scan 4.5.1, 7.0 and 8.0i
- Distribution via CDRROM or managed services
- DAT updates from a shared Linux FTP server
- Limited reporting
- Good documentation
- DAT revisions on the web site

What is available now?

- McAfee Virus Scan Enterprise 8.0i
- Standard build for desktop and server OS
- Standard to be used by all managed services
- Package created from step-by-step instructions
- Single exe file
- Support for Microsoft Windows 2000 and XP
- NO support for 9x, ME or NT 4.0

Who is it available to?

- Everyone!
- Every machine owned by Loughborough University
- Every member of staff
- Every student
- Individual use at home covered for the duration of time as a member of staff or as a student.
- Considerable investment!

New Features

- Buffer Overflow protection
- Unwanted Programs
- Port Ranges
- Access Protection

Why make it available to all?

- Time has changed
- Attack vectors for Virus infection has moved
- 16% of all attempted Virus infection on the Staff Desktop service is via USB pen/removable media
- The stand-alone disc scanner is not enough
- Remote working (off campus access)

Documentation

- Technical step-by-step setup available to all
- Revised Anti Virus web pages
 - All information revised
 - 18 point FAQ
 - Anti Virus Download (via Intranet)
 - Advice and Guidance
 - Virus Information Database and hoaxes links

DAT File Notification

- McAfee moved from once a week updates
- Checking revisions on web site
- Remote users
- Mail list dat-update
- Notifications each day of DAT file update and version number of current DAT

DAT File Repository

- Moved to dedicated Linux server with fault tolerance/redundancy
- Mirror of McAfee FTP site starts at 4am
- Current DAT replaced at 6am
- Status of FTP daemon checked every 15mins
- All happens in parallel on both servers
- Managed Services now use ePO

Dealing with Incidents

- WMF exploit (zero day)
- 27th December 2005
- Technically all machines from Win 3.1 – XP affected
- Windows patch not available for several weeks
- Most staff away from campus
- Many staff follow Internet best practice

Dealing with Incidents...

- By the 28th news has started to spread
- No DAT file coverage until 01/01/2006
- eTrust-Vet 12.4.1.0 01.01.2006 Win32/Worfo
- McAfee 4664 01.01.2006 Exploit-WMF
- Symantec 8.0 01.01.2006 Backdoor.Trojan

Dealing with Incidents...

- By the 3rd January:
 - Message to IT-Information
 - Checked DAT files on all servers
 - Additional update at 9.30am on managed services
 - Seen 484 requests for exploit
 - Seen five attempted local infections out of 2231 machines managed in ePO
 - Upgraded the DAT files on 386 managed

Dealing with Incidents...

- By the 4th January:
 - Emails containing WMF exploit seen on campus
 - Helpdesk staff contacted all recipients
 - Very few (single figures) infections
- By the 5th January:
 - Microsoft patch released
 - Managed services started testing

Dealing with Incidents...

- By the 6th January:
 - Staff Desktop service completed testing and released internally to Computing Services
- By the 9th January:
 - Patch released to Staff Desktop service
- By the 10th January:
 - Patch released to PC Labs service

Dealing with Incidents...

- No major outbreak of infected machines
- Limited Anti Virus protection through heuristics at zero-day
- Full Anti Virus protection within five days
- Additional DAT updates forced
- Release of patch to all managed services in five days

The need to patch

- McAfee Virus Scan has a number of patch levels
- 'About VSE' "Patch Versions:
- Patch 10 current on campus
- Patch 11 has issues with DFS (hotfix)
- Patch 12 due imminently
- However VSE 8.5 is also due imminently

Problems

- McAfee Virus Scan product is very good
- Support is more of an issue
- Two main outstanding issues
 - Scanning of compressed or image files
 - ePO interaction
 - telnet 127.0.0.1 8081

Futures

- Protection Software Review Dec 06
- Including all Malware (Virus, Worm, Trojan, Adware and Spyware).
- Increasing risks on Macintosh platforms
- 42 known OS X Malware items (not counting Viruses)
- Apple's move to Intel based hardware



Questions

<http://escarpment.net/>