computing

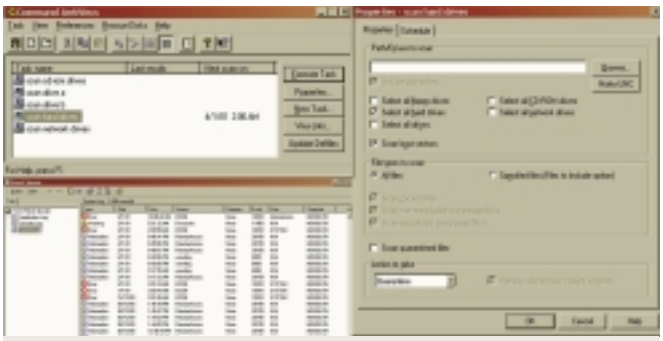
Review: Command AntiVirus performed well last time we tested it. So we threw the lethal MTX virus/worm combination at it

Chris Green

WE FIRST looked at Command's anti-virus (AV) package just over a year ago, and were impressed by its ability to protect against both known and unknown viruses. The latest version, which offers support for Windows 2000, has just been released.

Command AntiVirus (CAV) is based around a simple task-based interface, allowing users or administrators to schedule virus checking events in a very similar style to setting a diary entry in a program such as Microsoft Outlook.

Updates to the all-important definition (Def) database file can either be deployed centrally or activated from within the program with a single button click. This will cause CAV to connect to the Command web site and pull.



Command AntiVirus makes good use of simplified user interfaces

- Command AntiVirus now covers Windows, Dos, NetWare, OS/2, Lotus Notes, Microsoft Exchange and Windows 2000
- In our tests, it was the only application to stop our test strain of the MTX virus/worm combination

www.command.co.uk
www.vnunet.com/Products/83786

This can be administered using either the remote administration console, or controlled directly from the desktop.

Beyond this, CAV generally sits in the task tray minding its own business and monitoring the data activity on the host machine, while maintaining detailed, if a little confusing, activity and error logs.

Heuristic scanning

Any AV package with a totally up-to-date Def file will do a perfectly reliable job. The real test is how well it can cope with the viruses that are not already identified and logged in the Def file.

The process for doing this is known as heuristic scanning, whereby the AV application identifies the characteristics of a potential virus, worm, or dodgy script purely by its behaviour in active memory or by the actions it performs on your computer. This is supposedly one of CAV's strongest points, thanks to its HoloCheck heuristic scanning technology.

For our test we used a particularly nasty virus – MTX.9244. MTX is both virus and worm combined. It blocks Internet access to the web sites of many leading AV software providers, preventing the user from downloading an updated Def file that will identify it. It will even open a backdoor into a system.

Testing in the wild

For our test we set up five identical machines – all basic AMD K6-2 500Mhz computers on an isolated network. Along with CAV, we also tested Norton Anti-Virus, McAffee VirusScan, Sophos, and Dr Solomon's Anti-Virus. All five AV applications were set up with the most recent revision of their Def file that did *not* include reference to the strain of MTX we were using.

The virus was introduced as an email attachment to all five machines, via Microsoft Outlook Express. On executing the attachment, two files named IE_PACK.EXE and MTX_.EXE are dropped into the Windows system directory and executed. This is where we expected all five AV applications to race into action ...except three of them didn't.

Dr Solomon, McAffee and Sophos all failed to spot anything at all. Command successfully intercepted and isolated the virus and the worm element, though it did not know what exactly it had caught. Norton also identified that something was attempting to execute a virus-like action, though it failed to stop the worm part of MTX from executing, causing disruption to that machine's Internet connection.

On the back of our experiences with it, Command AntiVirus remains one of the best AV tools of recent years. It continues to strike a good balance between its database and heuristic scanning abilities, yet retains a simple interface and maintenance structure that can be administered remotely if necessary.

chris_green@vnu.co.uk

Verdict:

Performance

In day-to-day use, CAV performed well. It was transparent to the user once configured and made no significant impact on the operating performance of the client machines we used. Detection of a selection of common viruses and worms was swift and precise

Usability

Most parts of CAV are extremely intuitive, with the core virus scanning tasks resembling Outlook diary reminders. The Event Viewer still needs some work, as data is badly presented and difficult to navigate

Value for money

With a per-seat price of about £15 with a year's full technical support, Command Anti Virus is a low-cost, but by no means underpowered, application

