

CNN TARGETED BY RINBOT

Turner Broadcasting System, owner of CNN, was allegedly hit by a Rinbot worm last week, according to reports.

The Rinbot worm spreads using known vulnerabilities in Windows software, as well as a flaw in Symantec's antivirus software that the vendor has now patched.

"Only CNN can know what really happened inside its organisation," Graham Cluley, senior technology consultant at Sophos, told vnunet.com.

"We do know that Delbot, also known as Rinbot, exploits a vulnerability in Symantec's security software, and it is possible that this was a factor in the media company being infected," he added.

Cluley stressed that firms need to be vigilant in updating their security software.

"Even though Symantec issued a fix for the flaw in its software last year, some companies experience difficulties keeping up-to-date on patches and rolling them out across all of the computers on their network," Cluley added, according to the report.

EX MCAFEE LAWYER ON OPTIONS CHARGE

McAfee's former lawyer Kent Roberts has been indicted on charges he backdated stock options for financial gain.

Roberts, fired nine months ago after a probe into backdating of stock options, was charged last week with devising a scheme to defraud by granting himself and others options while hiding their true nature and value from board members and others, including the US Securities and Exchange Commission (SEC).

The seven-count indictment alleges that the former general counsel caused the company's then-controller to change the grant date on his options to a date when their exercise price was lower than the market price, thus securing gains.

Roberts is charged with two counts of mail fraud, one count of wire fraud, three counts of making false SEC filings and one court of falsifying books. If convicted, Roberts faces a maximum penalty of 20 years in prison and a US\$250,000 fine.

McAfee is one of more than 170 US companies currently under investigation for their stock options practices.

SYMANTEC BOOSTS PARTNER SUPPORT

Aimed at improving its relations with partners, Symantec has launched a three-pronged global strategy focusing on assessment, support and investment.

The three initiatives, launched last month, include a technical specialist and assessments programme, a unified technical support programme, and a three-fold investment in partner infrastructure.

Symantec said the goal of these initiatives was to help make it easier for partners to engage with Symantec as well as be more successful in servicing their customers.

A key part of the strategy is the technical specialist programme, which enables partners to validate their technical skills and product knowledge online. Symantec said the scheme was designed to help "differentiate partner services and ensure partner credibility".

"Our partners now have round the clock access to the latest information on Symantec's products and new releases. This is important as Symantec's stable of software has grown considerably through acquisition and innovation," said Katie Spurgeon, Middle East channel and alliances manager at Symantec.



Spurgeon said partners had access to round the clock technical support for its products.

Partners can access the scheme through Symantec's online portal PartnerNet. Another change made by Symantec is that it has shifted its partner portal to a more robust platform.

The vendor has also unified its technical support for resellers to give them support access 24x7.

FEEDBACK

STORM STRIKES MONTHLY MALWARE RANKINGS

The Storm Worm dominated malware ratings last month, accounting for around half of malicious software tracked, according to the latest figures from security firms.

The worm, which hit the headlines last month after showing up in numerous e-mails disguised as a message about recent storms in Europe, was February's top ranked threat by security software firm Sophos, accounting for 50.3% of all malware tracked.

The Storm Worm, also known as the W32/Tibs.gen threat, scored highly in security systems vendor Fortinet's February rankings as well, coming in fourth with 3.91% of all e-mail threat detections.

According to Guillaume Lovet, Europe, Middle East and Africa (EMEA) threat response team leader for Fortinet, 36 different variants of the Storm Worm were seen active during the month, although one variant accounted for nearly 60% of related detections.

"The overwhelming presence of the

Storm Worm is not without consequence as it is being leveraged to generate and relay massive amounts of spam," Lovet said.

The Storm Worm was kept out of the top three spots in Fortinet's rankings by three phishing threats, with the HTML/BankFraud.E!phish scoring the highest number of detections during the month.

● Sophos said the Storm Worm made up 50.3% of all tracked malware
● Fortinet put the Storm Worm fourth in its monthly threat report, accounting for 3.91% of detections