



Trojan attack targets top executives

By Liam Tung

http://www.news.com/Trojan-attack-targets-top-executives/2100-7349_3-6209930.html

Story last modified Tue Sep 25 08:35:10 PDT 2007

Top-level employees of publicly listed companies are being targeted by cybercriminals using malware-infected RTF documents disguised as recruitment letters.

Security company MessageLabs reported that 1,100 e-mails containing malware-infected RTF (rich text file) attachments were recorded over a 16-hour period this month. Four separate waves appeared between September 13 and 14, the company said.

"All (the e-mails) were going after (top-level) management. The e-mails included the company name in the subject field, purporting to be a recruitment company. What it had in the attachment is an executable RTF file," a MessageLabs representative said.

[Similar e-mails were noticed in June](#), the representative said.

The e-mail, which contains no body text, includes a .scr screen-saver dummy file within an executable RTF file, the representative said. When recipients attempt to open the file, a message is displayed stating: "Microsoft has encountered an error and had to close." The recipient is then advised: "To view this, double click on the message."

Once activated, the RTF file starts a chain of downloads that establish a secure connection between the attacker's server and the infected computer.

The top-level nature of the targets clearly indicates that the attackers are after information, the MessageLabs representative said, but the greater concern is the social-engineering technique used to spread the Trojan-harboring e-mail.

"The way that this works has the potential to be so effective. You are getting that top-down approach--if they forward that e-mail on internally, that e-mail is coming from a trusted source," he said.

Now on News.com

[Carmakers in drive to Tokyo auto show](#) [Former techie defines success with education](#) [When the PC becomes a parenting problem](#)
[Extra: How soon can I get teleported?](#)

The representative added that all the [e-mails were addressed to a single person](#), which helped diminish their conspicuousness.

F-Secure security expert Patrik Runald recently said that the perfect attack would be a zero-day attack using a rootkit-cloaked Trojan sent to an H.R. manager who, due to company policy, would be compelled to open the document.

"These are scary cases because it's really hard to protect yourself against," Runald said. "We have to run Office, and we have to allow Word, RTF, PowerPoint and Excel files through. It shows that signature-based antivirus is not enough; you need more technology than that."

Runald said there is little that organizations can do to protect against these threat types besides educating users of the risks, because banning the receipt of common file types is impractical.

Heuristic or behavioral-based monitoring is proving to be more effective at blocking these attacks since the behavior of the file remains the same despite different signatures being used, Runald said.

Liam Tung of [ZDNet Australia](#) reported from Sydney.

[Copyright](#) ©1995-2007 CNET Networks, Inc. All rights reserved.