c|net NEWS.COM http://www.news.com/

Top executives face personalized e-mail attacks

By Tom Espiner
http://news.com.com/Top+executives+face+personalized+e-mail+attacks/2100-7349_3-6194497.html

Story last modified Mon Jul 02 06:37:46 PDT 2007

Online miscreants have targeted 500 key business executives in what is believed to be the first mass-targeted malicious-software attack, according to security vendor MessageLabs.

Targeted attacks aim to bypass security measures by individually addressing e-mails, which often contain zero-day exploits.

On June 26, MessageLabs intercepted more than 500 individual e-mail attacks targeted at individuals in senior management positions in a variety of organizations around the world. Normally, MessageLabs sees approximately 10 targeted attacks per 200 million e-mails per day, according to Mark Sunner, MessageLabs' chief security analyst.

The malicious e-mails contain the name and job title of the victim in the subject line. The vertical sector most targeted was banking and finance, with chief investment officers being targeted in 30 percent of the attacks, according to Sunner. However, other verticals were also targeted. Eleven percent of the intended victims were chief executive officers, while 6 percent were chief finance officers.

Now on News.com
Pay-for-blogging site raises questions E3 gets down to business Rivals respond to Microsoft's CRM plans Extra: 12 IT skills that employers can't say no to

Sunner said the executives being targeted were perhaps "not that tech-savvy." In the attacks, an executable file was embedded in a Microsoft Word document. If the victim opened the document and clicked on a link, the file would have run a data-stealing Trojan horse that relied on creating buffer overflow conditions in Office documents.

MessageLabs said it did not know who had perpetrated the attack. "It's a certainty that some executives were compromised," Sunner said.

The intended victims' spouses and relatives were also targeted by name, in attempt to infect other computers related to the victim. The intent was to indirectly gain access to confidential correspondence and intellectual property relating to the target, MessageLabs said.

Sunner said he suspected that the hackers harvested the information using search and social-networking sites.

"Someone somewhere has really done their homework," Sunner said.

Tom Espiner of ZDNet UK reported from London.