





With the new HP BladeSystem c-Class, powered by the Dual-Core Intel® Xeon® Processor, you can finally set IT free.

Find out how. >>

Dual-core. Do more.

'Storm' Worm Touches Down on IM

February 15, 2007

By Brian Prince

The Storm worm that wreaked havoc in January has opened up a new front in its war against users— instant messaging.

The Trojan virus that was responsible for countless spam e-mails sent around the globe has spawned a new variant that is using AOL Instant Messenger, Google Talk and Yahoo Messenger to proliferate. The worm attacks by detecting when someone is chatting and sending out a message with a link to the first stage of malware on a site. If the user clicks the link, the first stage will execute.

ADVERTISEMENT



Enable and protect your business with VeriSign intelligent infrastructure.

Learn more at the Ziff Davis Intelligent Infrastructure Zone. >>

"The botnet handlers will periodically inject new commands into this peer-to-peer network, and one of the first things they do is tell the infected machines to download several executables," explained Jose Nazario, software and security engineer for Arbor Networks, based in Lexington, Mass.

RELATED LINKS

- ['Storm' Worm Continues Surge Around Globe](#)
- [Research: IM Malware Attacks on the Rise](#)
- [Phishers Attack MySpace with QuickTime Exploit Worm](#)
- [The End of the Worm Era](#)

"These include updated binaries as well as several other components used for DDoS [distributed denial

of service], spam, and additional spreading capabilities, and a rootkit to hide the malware's presence," he continued. "The operators are constantly moving the machines to new network configurations to defeat firewalls and filters."

[Click here](#) to read about research showing that IM malware attacks are on the rise.

The worm presents itself during an ongoing chat as an innocuous message such as, "Is it about you?"

"It is definitely smarter than the average bear," said David Cole, director of Security Response at Symantec, in Cupertino, Calif. "It's really quite convincing."

The worm was nicknamed Storm last month because it spread via e-mail with subject lines referring to major storms in Europe.

In addition, the worm also targets anti-spam Web sites, and even servers supporting rival malware with denial-of-service attacks, Nazario said. While it is not common for malware to attack one another, it has happened in the past, he said. The battle between Storm and Warezov—a mass-mailing worm that sends itself as e-mail attachments to addresses found on infected computers—is more external than malware-on-malware battles have been in the past, he said.

[For advice on how to secure your network and applications, as well as the latest security news, visit Ziff Davis Internet's Security IT Hub.](#)

"Instead of targeting the same infected boxes, the authors are choosing to DDoS each other's base of operations," Nazario said. "They have also targeted high-impact DDoS events against anti-spam and anti-criminal efforts, such as Spamhaus. These two malware networks are built specifically for spam, it seems, and so anti-spam efforts go a long way to hurting their spam delivery efforts."

Malware attacks using IM have been on the rise for the past few years. A research report by security software maker Akonix Systems, in San Diego, unearthed some 406 new IM-borne threats in 2006, compared with 347 attacks tracked by the company in 2005. Officials at the company predicted the number would increase in 2007 as well.

Nazario said the number of worms that are IM-specific appears to have leveled off; in their place however are multivector worms that know how to use instant messaging systems to propagate.

PC users can protect themselves from malware targeting IM systems in a number of ways. First, Nazario said, they should configure their IM clients to ignore messages from people not on their buddy lists. Secondly, they should practice the same kind of security there that they do for e-mail—treat unsolicited messages with suspicion.

"Sometimes asking someone to resend the link is enough to see that it was a machine sending the message and not a person," he said. "All of this goes a long way towards defeating the simplest attack of all, the social engineering attack."

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

[Copyright \(c\) 2007 Ziff Davis Media Inc. All Rights Reserved.](#)