InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Storm Worm Erupts Into Worst Virus Attack In 2 Years

Storm worm authors are blasting the Internet with two types of attacks, and both are aimed at building up their botnet.

By Sharon Gaudin, InformationWeek
July 24, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=201200849

The Storm worm authors are waging a multi-pronged attack and generating the largest virus attack some researchers say they've seen in two years.

"We are basically in the midst of an incredibly large attack," said Adam Swidler, a senior manager with security company Postini. "It's the most sustained attack that we've seen. There's been nine to 10 days straight days of attack at this level."

Swidler said in an interview with *InformationWeek* that the attack started a little more than a week ago, and Postini since then has recorded 200 million spam e-mails luring users to malicious Web sites. Before this attack, an average day sees about 1 million virus-laden e-mails, according to Postini. Last Thursday, however, the company tracked 42 million Storm-related messages in that day alone. As of Tuesday afternoon, Postini researchers were predicting they would see that day between 4 million and 6 million virus e-mails -- 99% of them associated with the Storm worm.

While the number of spam e-mails has dropped significantly, it's still far above normal levels, so Swidler isn't ready to say the attack is over.

The viruses are not embedded in the e-mails or in attachments. The e-mails, many of them otherwise empty, contain a link to a compromised Web site where machines are infected with a generic downloader. This helps pull the computers into the malware authors' growing botnet, while also leaving them open for further infection at a later date.

"This is designed to add computers to the botnet," said Swidler. "That's first and foremost their goal."

But the Storm worm authors aren't contenting themselves with this one attack vector.

Paul Henry, VP of technologies with Secure Computing, said in an interview that the electronic greeting card spam scam that the Storm worm authors launched early in July is stronger than ever. He noted that a friend of his has a company with 100 users and they're being hit with about 300 e-card spams every day.

"Back in December, we saw a huge spike in e-card spams because of the holiday," he added. "We are at the levels we were seeing back in December right now Most security professionals thought it would show up for Independence Day and then fade immediately, but it's been escalating for the last few weeks. It's definitely a pain point."

Again, the e-card spam message, which install rootkits in the infected computers, are working to build a botnet. Henry could not say if it's the same botnet as the other messages are building.

"I have seen thousands of these e-mails since Independence Day. It's got to be working for them or they wouldn't keep doing it," said Henry.

Just a few weeks ago, the Storm worm authors began trying to trick users with fraudulent e-mails warning unsuspecting

users about virus or spyware infections. Users around the world were receiving spam messages claiming that viruses or spyware had been detected on the users' systems. It was another attempt to lure users to malicious sites where their computers could be infected.