



**Research Report:**  
Which Tools Rule for Security Compliance  
Orchestration: Policy Management or  
Risk Assessment?



## Spam Spreads Storm Trojan Across Internet

August 22, 2007

By Brian Prince

The Storm worm continues to sweep through the Internet, this time via a new series of spam e-mails that use login account confirmation details as bait to get recipients to visit malicious Web sites.

ADVERTISEMENT

The TRACE ([Marshal Threat Research and Content Engineering](#)) team reported the spam e-mails appear to come from a legitimate organization and offer recipients temporary login confirmation details for a Web site. The spam uses text such as "for security purposes, please login and change the temporary Login ID and Password" and includes a link to an IP address that is actually a Web site infected with the Storm Trojan.

### RELATED LINKS

['Storm' Worm Continues Surge Around Globe](#)  
['Storm' Worm Touches Down on IM](#)  
[Don't Talk to Strangers on Yahoo Messenger Webcam](#)  
[Facebook Leaks Its Own Code](#)  
[Biggest Pump-and-Dump Scam Ever Spikes Spam 445%](#)

"We have noticed overnight a strong up-tick in the volume of confirmation spam from 18 percent of all spam yesterday to 35 percent," said Bradley Anstis, director of product management at United Kingdom-based Marshal, in an interview with eWEEK. "This suggests to us that many people are getting caught by it. This is not surprising since the malicious code itself seems to be morphing every 30 minutes or so, making it very difficult to detect with AV scanners...The Storm Trojan has been in circulation now since early this year and is quickly becoming one of the worst offenders of all time!"

**Click here to read more about the Storm worm.**

The Storm worm first touched down on the Web in January. Also known as Zhelatin and Nuwar, the Trojan spread through massive waves of e-mail with subject lines referencing a major storm in Europe and other current events. In the ensuing months, the group behind the malware used a variety of different kinds of spam ploys, including malicious e-cards, to propagate the worm.

Earlier this month, Atlanta-based security firm SecureWorks reported the number of hosts launching the attack via e-mail had jumped from 2,815 in the beginning of the year through the end of May to a total of 1.7 million in June and July.

Finnish security company F-Secure warned about the latest twist involving the Storm worm Trojan.

"A few times over the last week we've posted on how the e-mails used by the Zhelatin/Storm gang have changed, so we weren't too surprised to see them change once again," a F-Secure researcher wrote on the company's security [blog](#). "This time though, they look very different as they talk about 'you' having signed up for different services such as MP3 World or Internet Dating."

Anstis noted the new "confirmation spam" outbreak has been launched by the same group that launched the Hot Pictures spam campaign earlier in the week. Though in the past, spam campaigns such as the greeting card campaign would last for weeks at a time, spammers are now modifying or launching new spam campaigns almost daily, he said.

"They are trying to stay one or two steps ahead of the security companies. It typically takes a lot longer for a security company to react to a new threat than it takes for them to release," he said. "In this case, the Storm Trojan in all its guises is getting a lot of press, e-card spam, PDF spam, etc., so users are quite well versed. They have to try new techniques so that they can continue infecting PCs and expanding their Botnets. With the malicious code they are using to infect people morphing so often and also other clever techniques like refusing to launch in virtual sessions, it is making it ever harder to track and detect."

Anstis advised anyone who receives a message like this from a person they do not know, or have not heard from for a long time, to delete it without opening it.

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.](#)