



Storm worm deluges February malware chart

Posted by Rene Millman at 12:32PM, Thursday 1st March 2007

Only phishing emails detected more than worm.



The Storm worm has thundered to the top of malware charts in February, according to findings from security appliance vendor Fortinet.

The worm, also known as Tibs, accounted for per cent of all malware detected in the month. Only phishing emails were more prevalent than worm.

According to Guillaume Lovet, threat response team leader at **Fortinet** less than 36 different variants of the Storm Worm were seen active this month.

"The overwhelming presence of the Storm worm is not without consequence, as it is being leveraged to generate and relay massive amounts of spam," said Lovet.

"However, the battle against spam is not lost. A purely factual analysis the situation tends to prove that in the final race to arms against content analysis filters, spammers are losing ground."

The company found that on 8 February, one variant of the Storm worm accounted 60 per cent of all Tibs-related detections.

Lovet said that one very observable consequence of the worm was an increase in the volume of spam emails that has been occurring since the end of 2006.

The Storm worm, alongside another worm named "Stration", were purely meant to create large-sized botnets, more or less centralised. Stration's net consists in syndicated smaller traditional IRC botnets while Tibs implement a peer-to-peer botnet.

"Reducing the number of infected machines would effectively tackle the spam problem, at least, in the proportions it has taken today," said Lovet. "The problem is the number of infected machines, on the contrary, is growing everyday. The reasons for that are multi-fold, but the consequence is that we are left trying to cope with massive amounts of spam."

Lovet added that content analysis is not the only means to block spam.

"Analysing the envelope rather than the content of the letters is a strategy frequently implemented in anti-spam filtering systems," he said. "For instance, it may consist in comparing the incoming IP address to real block lists or reputation systems."

He said that although such approaches are often purely reactive, leaving windows of opportunity opened for rogue IP addresses to send out spam, but it could also help reduce the amount of bulk mails reaching end users boxes.

Submit to: [Digg](#) | [Slashdot](#) | [Del.icio.us](#)

[Rene Millman's blog](#)

[Email this Article](#)

Related News

[Online crime more profitable than drugs](#)
[New Storm worm variant targets blogs, forum websites](#)
[Network slowdown prompts PlusNet refunds](#)
[Storm worm causes weekend of trouble](#)