

The Trojan couple increases spam spread rates

The total amount of spam e-mail spread in the first three quarters of the year increased sharply. The reason is that two Trojans download maliciously, using a form of PC attack and then use them to spread huge amounts of e-mail.

The total amount of spam e-mail spread in the first three quarters of the year increased sharply. The reason is that two Trojans download maliciously, using a form of PC attack and then use them to spread huge amounts of e-mail.

On Friday last week, research firm MessageLabs announced that a dangerous pair of Trojans made the rate of spam spread increase. They use sophisticated technology now that security companies can't catch up.

According to a UK security provider, the rate of spam increased dramatically to 72.9% in October compared to 64.4% in the previous month. The main reason is because two dangerous Trojans attacked PCs and used them to spread huge amounts of mail.



"WareZov Trojan is the most dangerous Trojan we have seen in recent times. Every time an attack is made, it downloads the program or the next component, changes a few bytes of source code and makes it a new version. This makes the antivirus system difficult to detect and identify," said Paul Wood, an analyst at MessageLabs.

Although not finding the final convincing evidence, MessageLabs researchers think that by automatically

changing its own source code, WarezoV (with the " *Stration* " kernel) expanded the attack window. "If anti-virus companies take 5 to 6 hours to create a symbol, the Trojan is much more extensive with new identities."

SpamThru, another source of malicious code in October, is a malicious source of malicious code for computers. SpamThru also has another name given by security companies as "spam cannon". It uses different unified mail templates to spread spam out of the network. That allows each time to run, spam takes control to take out millions of messages and still save the blacklist.

SpamThru's flexible " *command-and-control* " operation model also makes it difficult for Internet service providers (ISPs), researchers and accrediting agencies to control or lock their activity. SpamThru relies on P2P (peer-to-peer) communication between bots and the brain that controls their hackers. " *Every bot knows about other bots on the same network. If a bot loses command and control channels, it can query alternate channels from other bots. This really increases the elasticity of botnets.* ".

Together, these two Trojans combine to create a huge amount of spam in October. Research firm MessageLabs has tested and obtained nearly a million copies of WarezoV's variants within a 24-hour period at the end of the month.

" *Certainly, the rate of spam distribution will continue to increase until the end of this year .*" Even MessageLabs's Wood researcher warns that fourth quarter is the history of spammers. " *This is the highest increase rate ever. I think it will be just a little bit more and this number will be 100% .*"

In the last month's report, MessageLabs also noted that while the total amount of phishing e-mail is declining, the percentage of phishing-related malicious messages still increases.

India is the country most heavily attacked by e-mail. According to the study, in October, in India, there is a mail containing malware for every 16 mail. There is plenty of evidence to suggest that almost a double the percentage of malware-containing mails is spam. The amount of spam in October increased by more than 20.5% compared to the previous month's 49.3%.

You can download the October report of MessageLabs (PDF file type) [here](#).

You finished reading the article "**The Trojan couple increases spam spread rates**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.