

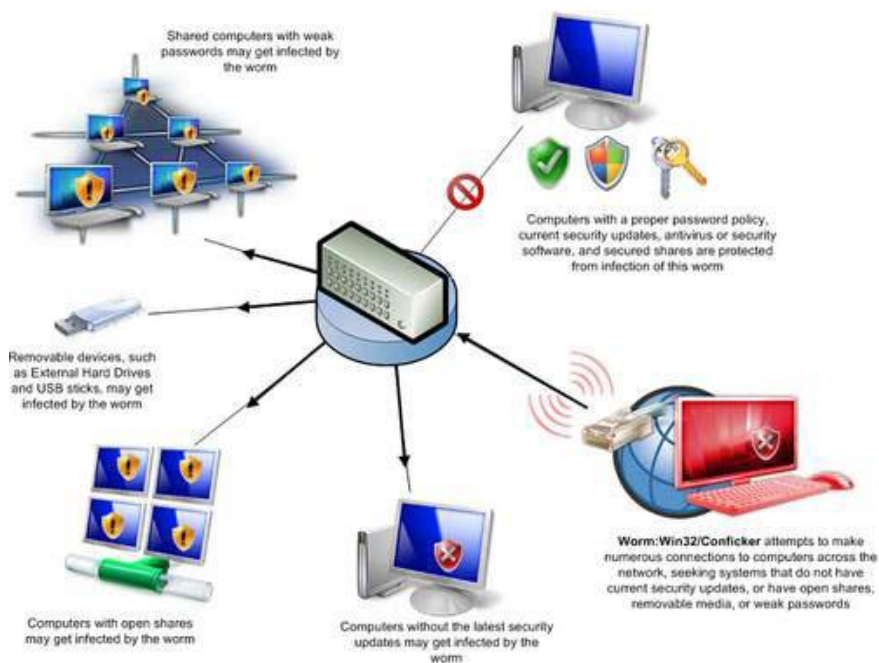
Release the free tool to kill ZBot malware

Security vendor BitDefender has just released a free tool to detect malware Zbotsau 14 hours detected. This is a malicious code that fears a reputation, focusing primarily on user information on financial websites

Security vendor BitDefender has just released a free tool to detect malware Zbotsau 14 hours detected. This is a malicious code that ruins the reputation, concentrating mainly on user information on financial websites, through online banking transactions that have just appeared a new dangerous variant.

Distributed primarily in the form of spam and its malicious websites, mostly in the form of a common legitimate application, Zbot has the old version to monitor the system and steal those Other user credentials. The latest variants of this malicious code also have the ability to collect the addresses of web pages visited by users as well as information provided by users open online and retrieve screen shots.

However, just 14 hours after the latest variants of this malicious code were called 'face names', BitDefender provided a free anti-malware tool ZBot.



The path of the ZBot malicious code.

Catalin Cosoi, BitDefender's online threat research manager, said: ' Besides the information and instructional role of helping global computer users to deal with computer threats, BitDefender also developed. ZBot removal tool. This tool will check user computers to detect and eliminate ZBot quickly '. Users can download this free tool

from the ' **Removal Tools section** ' section of the website www.malwarecity.com.

' When ZBot is one of the fastest-growing malicious codes in the world, we recommend that you regularly visit Malwarecity.com malware removal tool to update the tool. this. The computers using BitDefender's security software are certainly protected against this malicious code thanks to its multi-layer security technology and cloud computing application , "Cosoi said.

To ensure that your computer is always protected, users should consider installing and using malware protection products on their computers. Downloading and testing BitDefender security products within 30 days for free at the ' **download and try** ' section of www.malwarecity.com can be a good choice.

ZBot's destructive schedule

A massive spam campaign implicated the message sent from the US Centers for Disease Control (CDC), asking recipients to receive H1N1 vaccines that made the security headache painful. leads users to a website that looks very trustworthy. Here, the victims were asked to create a personal file so that they could receive the vaccine. Users are also urged to download the vaccine database from a link available in the mail.

However, when clicking on the link, the real thing "getting into the machine" and reinstalling is a new variant of the Trojan called Zbot. Named by several security firms, Zeus, the most powerful god of ancient Greek mythology, the malware specializes in attacking Windows computers to serve dark intentions, such as distributing mail. garbage, denial of service attacks.

When impersonation messages began arriving in mailboxes, many security firms said their filters had to clash with huge spam streams, averaging 18,000 CDC spams per minute, or about 1.1 million. fake mail every hour. The fake CDC website also has a backup attack plan, in case the recipient is careful enough not to click on the link. On the site is the presence of IFRAME, a very small, invisible element containing malicious code, specializing in drilling into Adobe Software and Flash vulnerabilities.

Zbot Trojan is particularly active in collecting the computers that have been defeated and set up botnets. Two Britons were arrested by police and accused of using Zbot to steal account holders' names and online banking passwords. More dangerous, hackers can edit this trojan into a set of tools to sell on the black market.

You finished reading the article "**Release the free tool to kill ZBot malware**" 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.