Detecting new malware on WinRAR can infiltrate computers and steal data

Researchers have discovered a new type of malicious code that could take advantage of the security bug on WinRAR decompression software to hijack and hijack computers to steal data.

Researchers have discovered a new type of malicious code that could take advantage of the security bug on WinRAR decompression software to hijack and hijack computers to steal data.

This malicious code is in .RAR format and spreads through emails with attractive titles. Specifically, in order to lure users to download the compressed files attached to the email, the crook will send the email with the title related to the hot news on the network today. If the user has not updated WinRAR to the latest version and downloaded this malicious code, the hacker will take advantage of the security flaw in WinRAR software to copy the malicious code to the machine to hijack, steal data, data encryption .

If you haven't updated the WinRAR software to the latest version, please quickly update it to limit the attack. In addition, you should also be respectful when downloading attachments and should not click suspicious links in emails.

Link download the latest version of WinRAR https://www.rarlab.com/download.htm.

In case it is necessary to download attachments in mail, please visit the website below to check for malware before opening.

https://www.virustotal.com/

For documents in email, to be safe you should open with Google Docs or online document editing applications.

You finished reading the article "**Detecting new malware on WinRAR can infiltrate computers and steal data**" 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.

© 2019 TipsMake.com