Detecting a Chrome extension infected with malicious code, stealing the password and the user's e-wallet key

ZDNet, MEGA.nz reports - Chrome's data sharing extension has been infected with malicious code. This malicious code has the ability to collect information about visitors' websites, account names, passwords and other data.

ZDNet, MEGA.nz reports - Chrome's data sharing extension has been infected with malicious code. This malicious code has the ability to collect information about visitors' websites, account names, passwords and other data.

This malicious code was found in the updated version released today, MEGA.nz 3.39.4. If you install this extension, users will be able to steal the passwords of Google, Amazon, Microsoft, GitHub accounts, even the e-wallet for storing Bitcoin or other crypto-currency to help hackers Stealing user properties. After collecting, all data will be sent to a host in Ukraine.

If you have been using this MEGA.nz extension, please delete or disable it immediately. Then go to the menu section -> More Tools -> Extensions to check again for sure.

Neither Google nor MEGA.nz currently have any feedback on this issue.

See more:

1. Warning of new malware appear like Wannacry, capable of deleting Vietnamese percussion on computer
2. Many cheap Android smartphones are 'promotional' codes for users
3. 7 kinds of ransomware you didn't expect

You finished reading the article "**Detecting a Chrome extension infected with malicious code, stealing the password and the user's e-wallet key**" 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