

Ransomware 'Your Windows has been banned' extorting users with a face value of 50 USD Bitcoin

Recently, the new version of ransomware 'Your Windows has been banned' has been reported by many websites and warned that all computers and infected users should remember that this is a scam.

Recently, the new version of ransomware '**Your Windows has been banned**' has been reported by many websites and warned that all computers and infected users should remember that this is a scam.

'Your Windows has been banned' is a ransomware infection discovered by Microsoft security experts at the end of 2016. Basically, this ransomware will block the victim's computer screen and it's simply infection and pretend to encrypt files on the infected computer.

The infection displays the message on the "blue screen of death" and asks the victim to pay \$ 50 Bitcoin to unlock the screen and retrieve the files on the infected computer. This type of ransomware message is displayed on the lock screen and usually appears when the user starts the computer.

1. With the NMR's 15 free Ransomware decoding tools, you won't need to ransom the file anymore
2. Summary of effective Anti-Ransomware software



This new version of ransomware "Your Windows has been banned" displays 2 options for users:

1. Buy a new Windows key for \$ 50 (buy a new Windows key for \$ 50).
2. Xoá all d? li?u và t?o b?n ng??i dùng b? l?i (Delete all data and your computer will be unusable).

In this case, you should use a virus removal tool to scan for malware, and contact customer support directly for assistance.

It is known that this ransomware is not too dangerous. However, no one wants to be troubled by any kind of ransomware. Hopefully this virus will soon be prevented.

You finished reading the article "**Ransomware 'Your Windows has been banned' extorting users with a face value of 50 USD Bitcoin**" 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.
