# Detecting botnets that can easily bypass Windows Defender and steal crypto wallet data

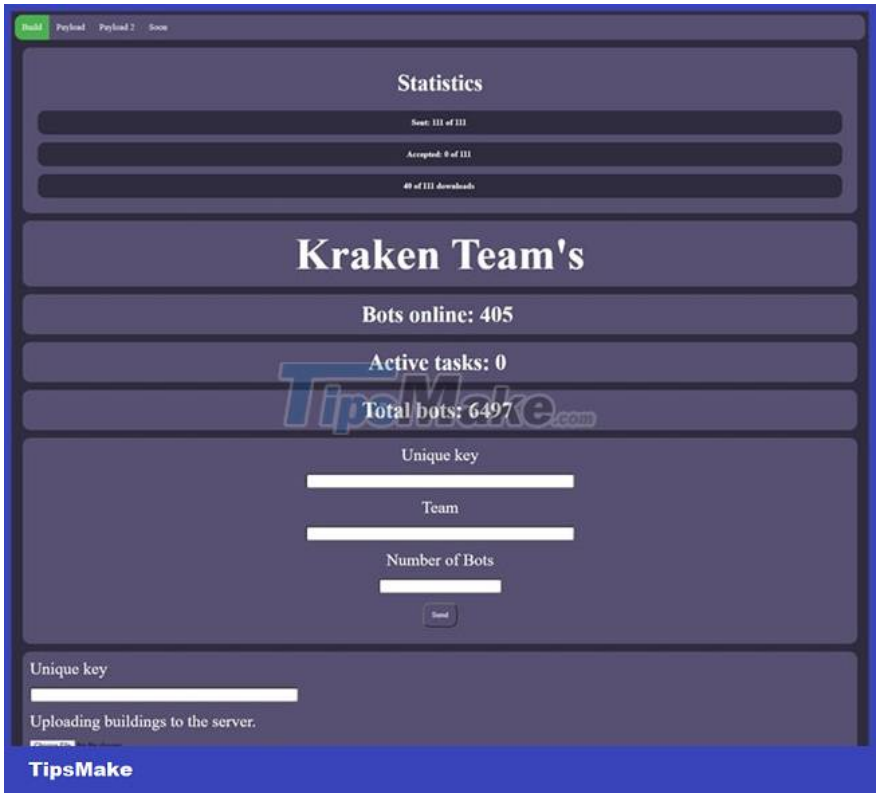
The sharp increase in the value of cryptocurrency transactions in the past few years has led to the trend of global online systems being attacked by botnets that steal virtual currency.

Any poorly secured system can easily fall victim to a malicious botnet.

Microsoft recently had to rush to release an update related to Window Defender, which removed the ability to access excluded folders and files without administrator rights. In other words, users will now be forced to own admin rights to see the list of excluded folders and files in Window Defender.

This is a notable change because threat actors often try to abuse this type of information to deploy malicious payloads inside excluded directories, with the ultimate goal of circumventing the rules. Windows Defender malware scanner.

However, this Microsoft method may not work against a new botnet called Kraken, which was recently discovered by the ZeroFox security team. The reason is that this botnet simply turns itself into the exclusion data, instead of trying to find the excluded folders and files to distribute the payload like many other botnets do. This is obviously a relatively simple but smart and effective 'trick' to bypass Window Defender's malware scanning.




The mechanism of action of the botnet is basically explained by ZeroFox as follows:

> During Kraken's installation, it will try to switch itself to %AppData%Microsoft.
>
> [.]
>
> To hide from Window Defender, Kraken runs the following two commands:
>
> powershell -Command Add-MpPreference -ExclusionPath %APPDATA%Microsoft
>
> attrib +S +H %APPDATA%Microsoft

ZeroFox notes that Kraken is primarily a data-stealing malware, similar to the recently discovered fake Windows 11 lookalike website. Experts also added that Kraken's most dangerous ability at the moment is to steal information related to users' cryptocurrency wallets.

> The most dangerous additional feature of the botnet is the ability to steal different crypto wallets from the following places:
>
> 1. %AppData%Zcash

2. %AppData%Armory
3. %AppData%bytecoin
4. %AppData%Electrumwallets
5. %AppData%Ethereumkeystore
6. %AppData%Exodusexodus.wallet
7. %AppData%GuardaLocal Storageleveldb
8. %AppData%atomicLocal Storageleveldb
9. %AppData%com.liberty.jaxxIndexedDBfile__0.indexeddb.leveldb

You can find more details on how the Kraken botnet works in ZeroFox's blog post HERE.