Watch out, the Kraken botnet can easily bypass Defender and steal your crypto

By Alexandru Poloboc

Published: 2022-02-21 · Archived: 2026-04-05 21:07:35 UTC

As most of you may already know, the Redmond-based tech company recently made an important update to the Window Defender Exclusions permission list.

Now, due to the change implemented by Microsoft, it is no longer possible to view the excluded folders and files without administrator rights.

As you can imagine, this is a significant change as cybercriminals often use this information to deliver malicious payloads inside such excluded directories in order to bypass Defender scans.

But, even so, safety is a relative term and whenever we think that we are safe, there are always going to be insidious third parties ready to breach our security.

Beware of the new Kraken botnet

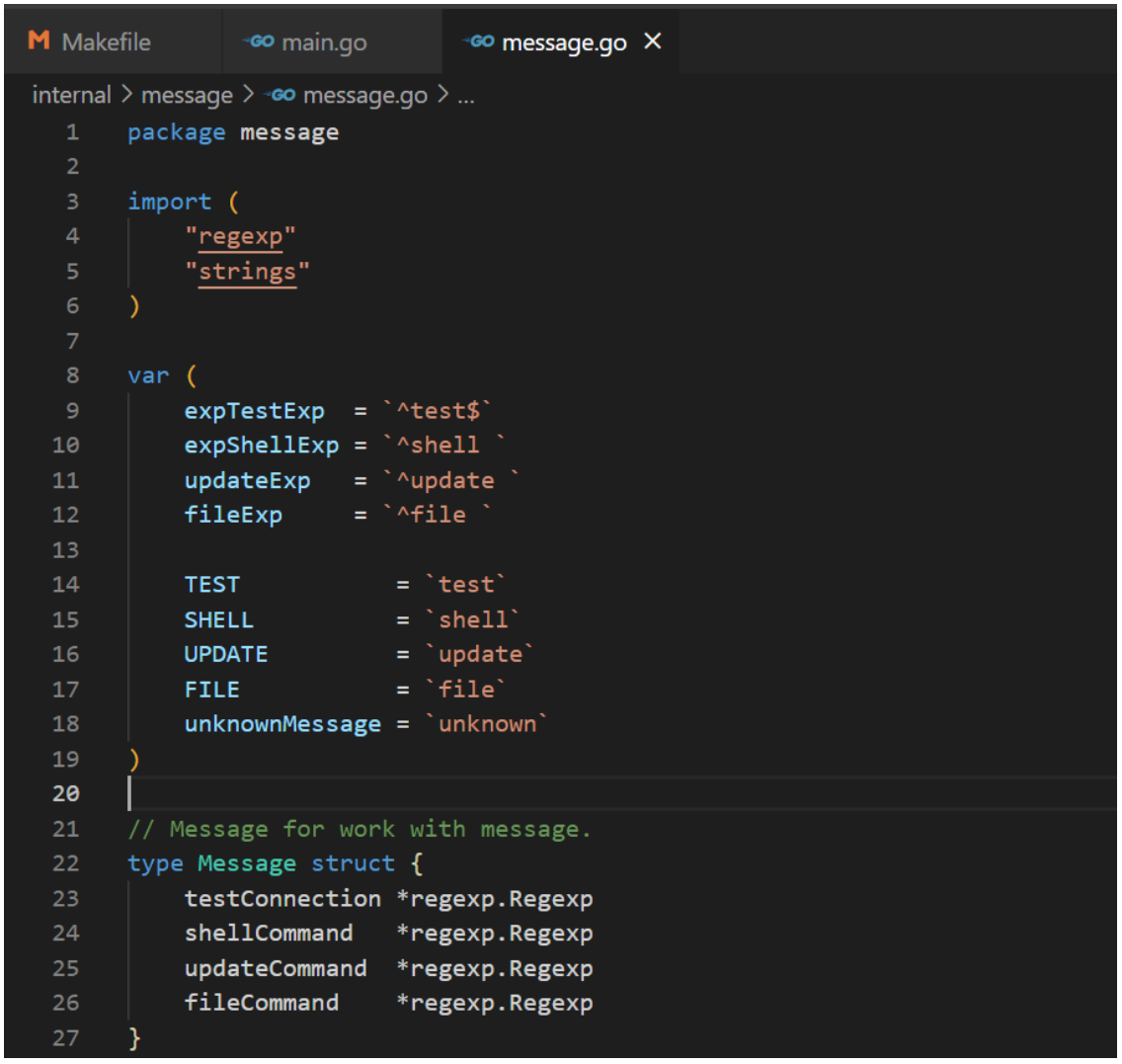
Even with all the safety measures taken by Microsoft, a new botnet called Kraken, which was recently discovered by ZeroFox, will still infect your PC.

Kraken adds itself as an exclusion instead of trying to look for excluded places to deliver the payload, which is a relatively simple and effective way to bypass Windows Defender scan.

The team stumbled upon this dangerous botnet back in October 2021, when nobody was aware of its existence, or the harm it could do.

Though still under active development, Kraken already features the ability to download and execute secondary payloads, run shell commands, and take screenshots of the victim’s system.

It currently makes use of SmokeLoade in order to spread, quickly gaining hundreds of bots each time a new command and control server is deployed.



The security team that made the discovery also noted that Kraken is mainly a stealer malware, similar to the recently discovered Windows 11 lookalike website.

Kraken's capabilities now include the ability to steal information related to users' cryptocurrency wallets, reminiscent of the recent fake KMSPico Windows activator malware.

The botnet's feature set is simplistic for such software. Although not present in earlier builds, the bot is capable of collecting information about the infected host and sending it back to the command and control (C2) server during registration.

The information collected seems to vary from build to build, though ZeroFox has observed the following being collected:

- Hostname
- Username
- Build ID (TEST_BUILD_ + the timestamp of the first run)
- CPU details
- GPU details
- Operating system and version

If you want to find out more about this malicious botnet and how you can better protect yourself against attacks, make sure you read the full ZeroFox diagnostic.

Also, be sure to also stay on top of any sort of attacks that might come via Teams. It pays to always stay one step ahead of hackers.

Have you ever found yourself being a victim of such a cyber attack? Share your experience with us in the comments section below.

Alexandru Poloboc Shield

Tech Journalist

With an overpowering desire to always get to the bottom of things and uncover the truth, Alex spent most of his time working as a news reporter, anchor, as well as TV and radio entertainment show host. A certified gadget freak, he always feels the need to surround himself with next-generation electronics. When he is not working, he splits his free time between making music, gaming, playing football, basketball and taking his dogs on adventures.

Source: https://windowsreport.com/kraken-botnet/