How to protect yourself from the new 'EvilQuest' ransomware on Mac

One of the latest malware threats for Mac that you should be aware of is 'EvilQuest'.

One of the latest malware threats for Mac that you should be aware of is 'EvilQuest'.

However, this ransomware has only been circulating between pirated software on Macs so far. Unless you frequently install pirated programs, you shouldn't be too worried. MalwareBytes claims that this new malware exists in fake installations of at least two applications: Little Snitch and Mixed in Key 8. MalwareBytes also found some evidence that the malware is present in Ableton Live, so the possibility of it being present in other software is very high.

Unlike the official Little Snitch and Made in Key 8 installation files (which have official logos and include a complete installation package), this ransomware uses a generic installation package icon and includes an unrelated drive image. MalwareBytes also found a highly suspicious 'patch' file within the EvilQuest installation package and discovered that it lacked the standard code (a type of digital signature in files provided from a trusted source).

Like other ransomware, EvilQuest encrypts files on your device (including hard drives and external storage) and makes them inaccessible. The only way to regain access is to pay a ransom to the hacker, usually via Bitcoin or a private money transfer service. Hackers typically give a deadline for the ransom, otherwise your files will be locked or permanently deleted. EvilQuest gives a 3-day deadline.

How to avoid EvilQuest

Ransomware is often terrifying, but it's entirely preventable. Pirated software is the primary way malware infiltrates systems, so the easiest way to avoid it is to refrain from installing pirated programs or using media files from unknown sources. This way, you both prevent malware and avoid copyright infringement.

However, it's impossible to be certain that malware won't infiltrate official software downloaded from the web. Thoroughly research software through forums or ask those who have used it to ensure its safety before downloading.

You can check the programs you intend to download beforehand. The easiest method is to use antivirus applications to find files containing malware. If it's ransomware, make sure to scan it thoroughly before it infects your Mac.

You should also back up your data in case something goes wrong due to malware or system errors.

What should you do if you get infected with ransomware?

The best way to prevent this is to keep your computer secure. However, in the worst-case scenario of a ransomware infection, as long as you have backed up your data properly, you can easily recover it without paying. Remove the malware using MalwareBytes or other malware removal software. If your software has been blocked, perform a full system reset and use your backups to recover your data.

For more information about ransomware strains:

1. How to remove MOBA ransomware from your operating system
2. Warning about Sqpc ransomware, belonging to the STOP/Djvu family.