EvilQuest / ThiefQuest ransomware for macOS shows the importance of using independently tested Mac antivirus software

EvilQuest / ThiefQuest ransomware is now blocked by Avast; AVG; Avira; Bitdefender, CrowdStrike; FireEye; Kaspersky; Trend Micro - tested by AV-Comparatives

EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

INNSBRUCK, TYROL, AUSTRIA, July 8, 2020 /EINPresswire.com/ -- First Appearance of EvilQuest / ThiefQuest

On 29th June, K7 security researcher Dinesh Devadoss @dineshdina04 tweeted about the discovery of a new macOS ransomware program (https://twitter.com/dineshdina04/status/1277668001538433025?lang=en).

Known as EvilQuest / ThiefQuest, not to be confused with the game of the same name, it appears at first glance to be a fairly standard ransomware program that encrypts user files and demands payment in return for a decryption key. However, it transpires that it's especially nasty.

Although the ransom note provides a BitCoin address for payment, there is no apparent means for victims to contact the attackers or prove that they have paid.

What does it do?

Worse still, EvilQuest / ThiefQuest has some other nasty tricks in its box. It installs a keylogger, to record the victim's every keystroke, and connects the targeted system to a command and control centre, enabling the attackers to run further commands. Finally, it will attempt to exfiltrate specific files relating to cryptocurrency wallets, in an attempt to steal more money.

EvilQuest's authors seem to have made an effort to prevent malware researchers analysing the

program. It appears that it may not run on virtual machines – frequently used for malware analysis – or if specific Mac antivirus programs are installed on the system (https://www.macworld.co.uk/news/mac-software/mac-ransomware-evilquest-thiefquest-3791288/).

EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

Good News / Bad News

The good news about EvilQuest is that it's pretty difficult to get infected. As a standalone installer, it will now be blocked by the built-in security mechanisms in macOS, assuming these have access to Apple's cloud services. It appears that infections have only occurred when users have downloaded compromised installers for cracked versions of legitimate applications, such as Little Snitch and Mixed in Key8, via torrenting services. Even then, it will infect the Mac only if the security warnings from macOS are blindly clicked through.

Shall I pay the ransom?

Paying ransomware authors to decrypt your files is always a lottery at the best of times, but in most cases, it seems more or less certain that the encrypted data is lost forever, even if you do pay up.

> Do a backup, don't pay the ransom! The best option is to run a backup frequently. Make sure, that the backup medium gets disconnected from your computer afterwards, to avoid encryption of the backup!"
>
> *Peter Stelzhammer, co-founder, AV-Comparatives*

What can I do?

Do a backup, don't pay the ransom! The best option is to run a backup frequently. But you have to make sure that you disconnect the backup medium from your computer afterwards, as otherwise the backup will be encrypted by the ransomware too!

Use Antivirus Software for macOS

For Mac users who take their chances by running software from potentially risky sources, the importance of running effective, independently tested and certified antivirus software for macOS becomes apparent.

You can rely on independent comparative tests but not on online comparatives tools, eg.

VirusTotal. It is by no means a guarantee of protection. Whilst these online scanners have their uses, they rely exclusively on command-line scanners to check uploaded files for malware, which does not simulate real-world. Additionally, some Mac malware may not be detected on VT unless they have the correct file extension.

A full antivirus program running on the local system has a whole host of other protection mechanisms, such as URL blockers, reputation services and behaviour blockers, which greatly increase the chances of protecting the system against infection. Such security software can also perform dynamic analysis of a program as it is executed, thus getting around obfuscation techniques (such as proprietary packing methods) that cannot be detected in a simple scan of the inactive installer.

Where to find a reliable macOS antivirus software test?

The test methodology employed by AV-Comparatives in their Mac Malware Test allows tested programs to use a variety of protection mechanisms, including cloud-based services, to protect the system before, during or after execution of malicious programs. Large numbers of verified malware samples also ensure the statistical relevance of the results.

EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

Logo AV-Comparatives


EvilQuest / ThiefQuest macOS Security Review by AV-Comparatives

As well as Mac malware, the test additionally checks protection against Mac PUA – an increasing nuisance – and detection of Windows malware samples. The latter ensures that macOS users do not accidentally pass on malicious programs to friends, family or

colleagues who use the Windows operating system. A false-positives test additionally checks that the tested Mac antivirus programs do not plague users with false alarms on legitimate software.

Programs tested and certified this year are, in alphabetical order:

Avast Security for Mac; AVG Internet Security for Mac; Avira Antivirus Pro for Mac; Bitdefender Antivirus for Mac; CrowdStrike Falcon Prevent for Mac (enterprise product); FireEye Endpoint Security for Mac (enterprise product); Kaspersky Internet Security for Mac; Trend Micro Antivirus for Mac. The report includes a user-interface review, so that readers get a picture of what each program is like to use in everyday situations.

Like all AV-Comparatives' public reports, the 2020 Mac Security Test and Review is made available to everyone free of charge. It can be downloaded here: https://www.av-comparatives.org/tests/mac-security-test-review-2020/

Peter Stelzhammer
AV-Comparatives
+43 720 115542
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
