Hackers Selling Undetectable Proton Malware for macOS in 40 BTC

By Waqas

Published: 2017-02-18 · Archived: 2026-04-05 23:36:55 UTC

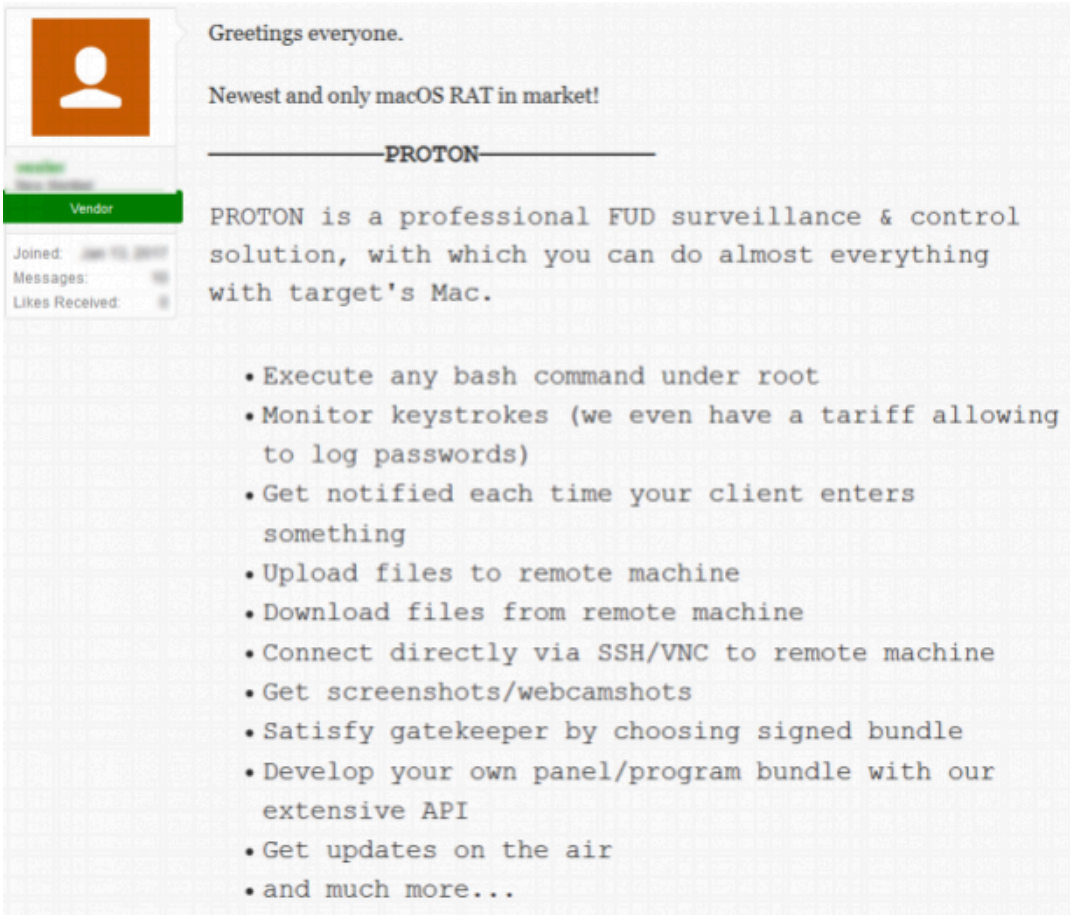
Hackers are selling a malware for Mac devices on a prominent dark web marketing claiming that it is undetectable and comes with capabilities including taking full control of macOS devices by evading anti-virus detection.

Dubbed Proton by its developers, the malware is a RAT (Remote Administration Tool) and is being sold in one of the leading closed Russian cybercrime message boards. The discovery was made by Sixgill, a cyber-intelligence company that detects cyber-attacks and sensitive data leaks originating from the Dark Web before they occur.

In their threat report, researchers at Sixgill explained that the initial price of Proton RAT was 100 BTC (USD $100,000), but lately it is being sold 40 BTC (USD $41891) with unlimited installations while a license to install on a single PC with genuine Apple certifications would set a cyber criminal back only 2 BTC.

Capabilities of Proton RAT:

Proton comes with capabilities including taking full control of a targeted device, keylogging, Observers with SMS notifications, SSH/VNC tunneling with VPS, webcam/screen surveillance, premium customer support, file uploadings, and downloads.



Listing screenshot from the dark web message board

“Proton can present a custom native window requesting information such as a credit card, driver’s license and more. The malware also boasts the capability of iCloud access, even with 2FA enabled,” notes Sixgill.

Proton RAT, a threat against MAC OS:

Sixgill’s report also highlights the threat Proton possess against Mac OS. For instance, hackers are selling this malware with genuine Apple code-signing signatures. This means there has been a lot of sophistication behind the development of Proton.

“The author of Proton RAT somehow got through the rigorous filtration process Apple places on MAC OS developers of third-party software, and obtained genuine certifications for his program. Sixgill evaluates that the malware developer has managed to falsify registration to the Apple Developer ID Program or used stolen developer credentials for the purpose,” reveals the report.

The report further goes on to explain that “gaining root privileges on MAC OS is only possible by employing a previously unpatched 0-day vulnerability, which is suspected to be in possession of the author. Proton’s users then perform the necessary action of masquerading the malicious app as a genuine one, including a custom icon and name. The victim is then tricked into downloading and installing Proton.”

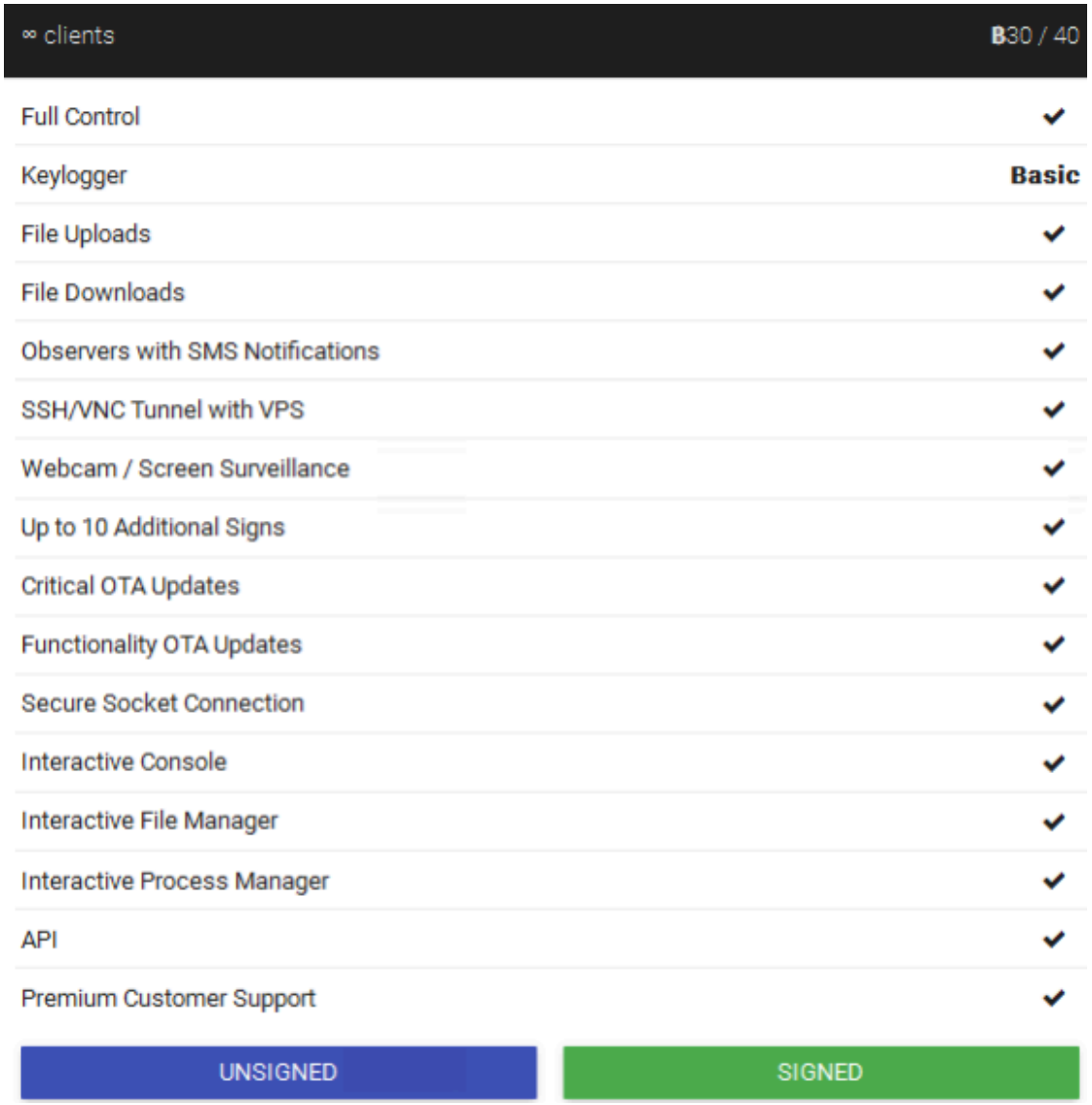
Discover more

Gaming security guides

Security software reviews

Cybersecurity courses

A full list of Proton's features can be checked below:



Screenshot from Proton's official website – Source: Sixgill

"Sixgill's Dark Web intelligence platform leads the way in early detection of cyber security threats when the damage can still be avoided", said Avi Kasztan, CEO and Co-founder of Sixgill. "Our analysts are constantly on the lookout for new and emerging threats, and we work closely with law enforcement authorities to report this activity."

The developers have also uploaded a video demonstration on YouTube explaining how Proton works and information about its installation.

Although the threat report identified that hackers are aiming at selling Proton malware to companies, families, sysadmins and parents; it is obvious that putting their listings on the dark web cybercrime message boards is an open offer for cyber criminals to take advantage of this malicious software.

Discover more

Tech news platform

Antivirus software plans

Computer Security

This is not the first time when hackers have been selling malicious software on a dark web marketplace. In the past, Stampado ransomware was also sold for just for Just $39. However, researchers, later on, discovered that Stampado was not FUD as claimed by its developers.
