Warning: The number of malware designed to target the M1 chipset is increasing rapidly, making it harder to detect

The success of the MacBook M1 became a favorite technology product, and this also attracted the attention of hackers.

Apple's decision to include the company's self-developed M1 chip on a series of MacBook, iMac, and even iPad Pro models, has brought a very positive response from the market. Up to now, it can be said that this is a successful step of the US technology giant when the new chip gives MacBooks impressive performance as well as good software compatibility.

The success of the MacBook M1 became a favorite technology product, and this also attracted the attention of hackers. The transition to Apple's new chip requires app developers to build new versions of their products to ensure better performance and compatibility. On the opposite side, hackers are taking similar steps to create new strains of malware with native execution capabilities, allowing them to work more efficiently on Apple's M1 systems.

As noted by security experts as well as anti-malware solutions, more and more malware targeting the M1 chipset has been detected and disabled recently. In other words, the number of new types of malware designed to specifically target the M1 and products using this chip is growing rapidly.

In theory, devices running on the new M1 architecture should be better protected against physical access and remote exploitation by general malicious actors. However, to deal with this, malware developers have redesigned their malicious code (usually Windows malware) to be able to run more efficiently on the macOS

operating system.

According to Apple's security expert Patrick Wardle, more and more malware targeting the M1 platform has been reported, many of which are Windows-derived variants. "As attackers evolve and change the way they deploy their malware, we, as malware analysts and security researchers, need to keep a close eye on that," he said. the expert added. According to statistics, up to half of all macOS malware recorded in 2020 are customized from Windows or Linux variants.

Wardle's research found that when anti-malware systems split macOS malware binaries, one for Intel-based Mac platforms and one for M1-based platforms, the results show that malware targeting Intel platforms is generally easier to detect than variants targeting M1, with a rate of about 10%.

This led Patrick Wardle to conclude that the signatures of most current anti-virus software on macOS only work effectively on Intel processor platforms, not Apple Silicon like M1. However, the same researcher also stated that the M1 system can essentially be more effective in enhancing security at the hardware level.