Millions of Macs have been updated and can still be hacked via the EFI firmware

But even if you tried to update all the software for your device, it is still possible that your computer is outdated and vulnerable.

'Keep the latest operating system and software updates' is one of the most popular and important advice that security experts still offer to avoid network attacks.

But even if you tried to update all the software for your device, it is still possible that your computer is outdated and vulnerable.

Researchers from technology company Duo Labs analyzed more than 73,000 Macs and found that many Apple Mac computers either failed to install the firmware patches on the EFI or didn't receive any updates. both.

Apple uses Intel's Extensible Firmware Interface (EFI) on Mac computers, works at a lower level than the OS and virtual machine on the computer - and controls the boot process. EFI runs before macOS boot and has higher permissions. If hacked, hackers can use EFI malware to control everything without being detected.

What's worse is that besides ignoring EFI updates on some devices, Apple doesn't warn users when the update process fails, causing millions of Mac users to be attacked.

Duo said that on average 4.2% of the 73,324 Macs used in the enterprise run the EFI firmware they should not run, based on the hardware, the OS version and the EFI version released for that OS.

Even though you tried to update it all, it doesn't mean you're safe

You will be surprised to know that 43% of iMac models (21.5 " at the end of 2015) are analyzed running old, unsafe firmware and at least 16 Mac models have never been updated to the RFI firmware when Mac OS X was released. 10.10 and 10.12.6.

'Even if you are running the latest version of macOS and installing the latest patch is released, our data shows that there is still the firmware EFI firmware you are running is not the latest version', Duo said.

Duo found that 47 models running macOS versions 10.12, 10.11 and 10.10 did not receive EFI firmware updates with patches for Thunderstrike vulnerabilities 1, 31 models did not receive the patch updates Thunderstrike bug 2. Initial Thunderstrike attacks used by NSA, also included in the WikiLeaks Vault 7 data leak and also mentioned the attack based on the old firmware.

Details about Macs can be found in the report of Duo Labs here *https://duo.com/assets/ebooks/Duo-Labs-The-Apple-of-Your-EFI.pdf*

According to Duo Labs, their research focuses on the Mac ecosystem because, to a certain extent, Apple has a unique position in controlling the entire ecological environment, but can also be attacked. 'We think that the main problem we have found affects all companies that use the EFI firmware, not just Apple.'

Mac users can also check if they have used the latest version of EFI with the open source EFIgy tool. *https://github.com/duo-labs/EFIgy*