Microsoft warns of an increasing trend of attacks targeting firmware and worrying public indifference

This is indeed a worrying 'lethargy', especially given the recent increase in the number of attacks targeting system software.

The Security Signals periodic security report for the first quarter of 2021 shows an alarming statistic that up to 80% of businesses surveyed have faced at least one related attack. firmware on its systems over the past two years. However, less than a third of businesses' security spending budgets are dedicated to the software protection aspect.

This is indeed a worrying 'lethargy', especially given the recent increase in the number of attacks targeting system software.

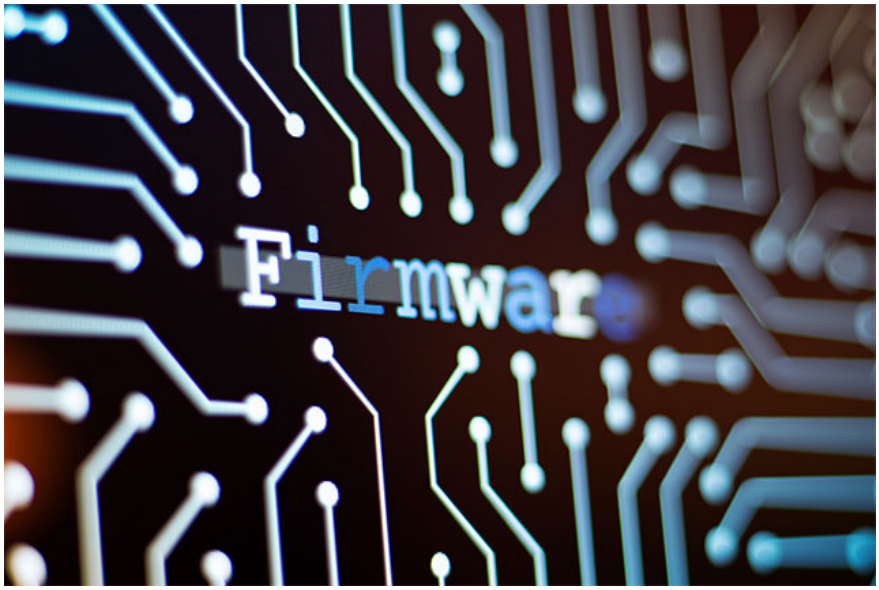
Essentially, firmware attacks are difficult to deal with and have huge consequences. This can be clearly seen in prominent cases that have been recorded. Such as the case of the infamous hacker group APT28 (also known as Fancy Bear). Several members of this group were arrested in 2018, after running an offensive campaign using the rootkit Unified Extensible Firmware Interface (UEFI) to target Windows computers, shocking the world.

There have also been attacks targeting hardware drivers, including RobbinHood, Uburos, Derusbi, Sauron and GrayFish, as well as ThunderSpy (targeting Thunderbolt ports) - all of which cause heavy damage. .

In response, last year, Microsoft launched a series of "Secured-Core" Windows 10 PCs to combat malware that spoofed code in the motherboard booted PC. The Redmond company has also released a UEFI scan tool in Microsoft Defender ATP to scan inside the firmware file system for the presence of malware.

These efforts are commendable, but just the effort from Microsoft is not enough. Many (if not the majority) of businesses do not take firmware attacks on their systems seriously enough.

' *Vulnerabilities in firmware are often harder to track and control. Software vulnerabilities are also exacerbated by lack of awareness and initiative* .



However, businesses also have their own difficulties. Firmware firmware, for example, is often located 'deep below' the operating system, and is a storage place for authentication information and encryption keys in memory. This is an area most anti-virus software solutions cannot reach. At the same time, it is also a weakness that hackers have recognized and focused on exploiting.

The question is whether security teams pay enough attention to potential threats. Microsoft says this interest is not enough, at least for now. The Security Signals survey results show that 36% of businesses have invested in hardware-based memory encryption and 46% are buying hardware-based kernel protections.

Notably, Microsoft also found that enterprise security teams are focusing primarily on security models in the "protection and detection" style, while only 39% of the time the security teams spend. is intended for the prevention and early prevention of threats.

According to Microsoft, the lack of active defense investment on firmware-level attack vectors is a prime example of this outdated security paradigm.

Most of the 1,000 enterprise security management experts interviewed (82%) said they did not have the resources to deal with firmware attack prevention issues, as they were too busy with bug fixes, hardware upgrades and minimization of internal and external vulnerabilities.

You finished reading the article "**Microsoft warns of an increasing trend of attacks targeting firmware and worrying public indifference**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com