Ransomware can attack the CPU, not just the operating system: How to prevent it?

Ransomware is a serious problem in its current state and is only going to get worse. Any security programs and measures will be rendered useless when ransomware attacks the CPU.

Ransomware is a serious problem in its current state and is only going to get worse. Any security programs and measures will be rendered useless when ransomware attacks the CPU.

Ransomware can lock your CPU

Ransomware typically locks down system files and other documents inside the operating system, rendering the PC nearly unusable. CPU ransomware, on the other hand, changes the processor's microcode, completely altering its behavior.

Only chip manufacturers like AMD or Intel can provide microcode for their respective processors. This microcode comes preloaded from the factory, and you can receive updates later to improve performance, stability, or fix any bugs. If hackers can exploit a CPU firmware bug to upload malicious microcode to your processor, the game is pretty much over.

While the chances of this happening are pretty low, it's no longer entirely theoretical. Google has demonstrated a way to inject custom microcode into AMD Zen CPUs by exploiting a bug that causes the processor to pick the number 4 every time it's asked to enter a random number.

Worse still, Christiaan Beek, senior director of threat intelligence at cybersecurity firm Rapid7, has developed a viable proof of concept, according to The Register. Fortunately, he hasn't released it, but now that the idea is public, it won't be long before hackers figure it out, too. In Beek's words:

If hackers were researching this threat a few years ago, chances are some of them got smart enough at some point and started creating this.

It's possible that hackers were working on CPU or firmware ransomware. UEFI bootkits that allow hackers to bypass Secure Boot and inject malware into a system's firmware already exist and are openly sold on hacker forums on the dark web . Beek also points to quotes from leaked chats revealed in the 2022 Conti ransomware leak, suggesting that hackers may have been working on ideas for installing ransomware inside a computer's UEFI firmware.

Can you protect yourself?

While antivirus programs can detect ransomware infections early and block the processes from running, CPU ransomware is out of their reach. If the CPU is infected with ransomware, the malware will load before the operating system, bypassing all traditional security measures in place and gaining complete access to every component of the system.

The good news is that you don't need to worry right now, as Beek hasn't seen any samples of the malware working in the wild. It's unlikely that hackers will be able to create a working exploit for at least a few years. Even if a working exploit is discovered, you can be sure that CPU manufacturers will quickly patch the issue and release firmware updates. On top of that, CPU vulnerabilities of this scale are pretty rare to begin with.

Better security is one of the reasons why you should update your PC's BIOS. With the emergence of CPU ransomware, an updated BIOS and CPU drivers are more important than ever. Just keep your software up to date, don't click on random emails and links, and check before running programs downloaded from the Internet, especially if you don't trust the website or sender.

You finished reading the article "**Ransomware can attack the CPU, not just the operating system: How to prevent it?**" 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