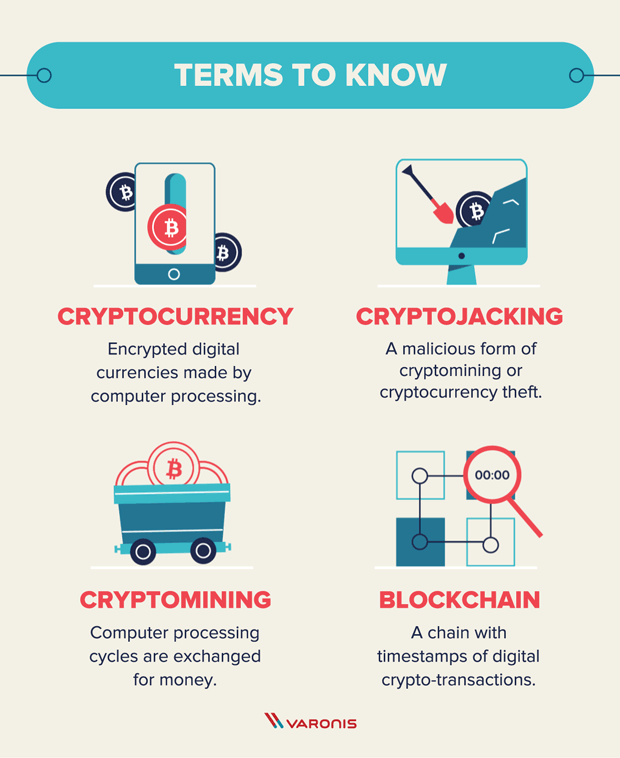
***CPU Hijackers***- *Crypto mining Malware and Cryptojackers*

*CPU hijackers, also known as cryptojacking scripts, are malicious code that secretly mines cryptocurrency on your computer without your consent.*

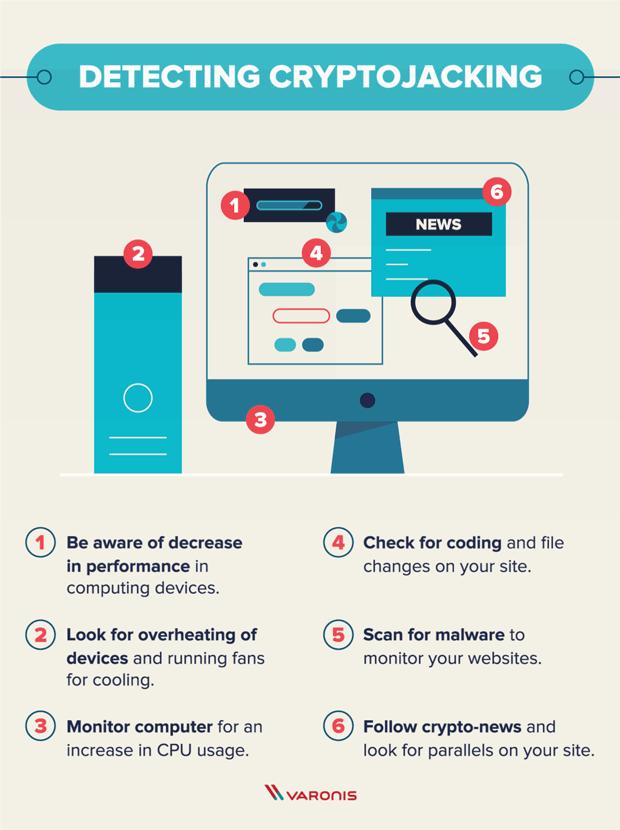
**

*These scripts can infect your computer through various ways, including:*

* *Visiting malicious websites: Clicking on malicious links or visiting websites that have been compromised with cryptojacking scripts can infect your computer.*
* *Opening infected attachments: Opening email attachments from unknown senders or clicking on suspicious links in emails can introduce cryptojacking scripts onto your system.*
* *Falling victim to malvertising: Malvertising involves injecting malicious code into legitimate advertising networks, which then delivers cryptojacking scripts to users' browsers.*
* *Installing pirated software: Downloading and installing pirated software from untrusted sources can often come bundled with cryptojacking scripts.*

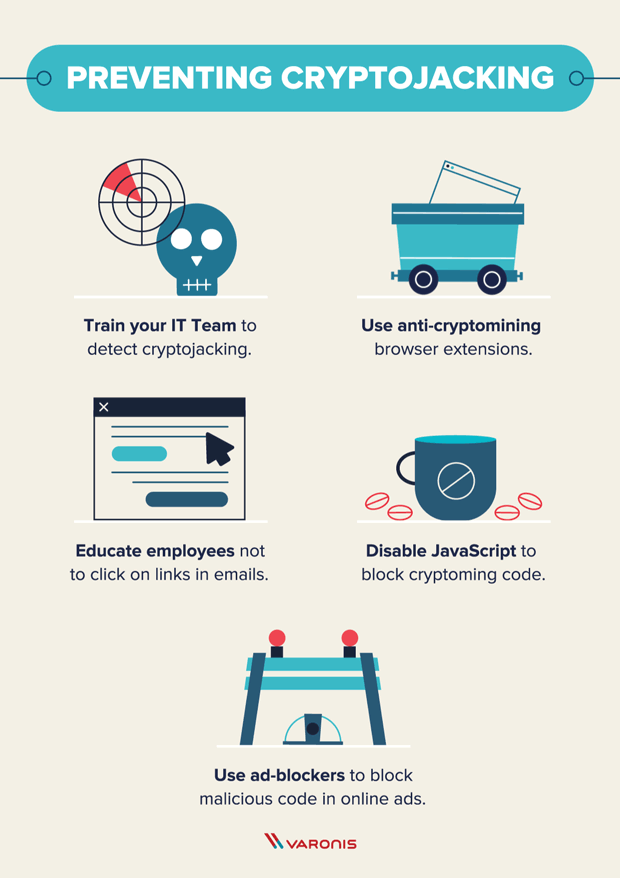
*Once a cryptojacking script has infiltrated your computer, it can silently run in the background, utilizing your CPU resources to mine cryptocurrency for the attacker's benefit. This can significantly slow down your computer's performance, increase power consumption, and potentially damage your hardware over time.*

***Detection:***

******

* *Slow computer performance: If your computer is noticeably slower than usual, it could be a sign that a cryptojacking script is consuming your CPU resources.*
* *Increased fan noise: As your CPU works harder to mine cryptocurrency, it will generate more heat, causing the fan to run more frequently and loudly.*
* *Unexpected spikes in CPU usage: Monitoring your CPU usage in the Task Manager can reveal if there are any suspicious spikes in activity, which could indicate cryptojacking.*
* *Unfamiliar processes running: Checking your running processes in the Task Manager may reveal unfamiliar or suspicious processes consuming significant CPU resources.*

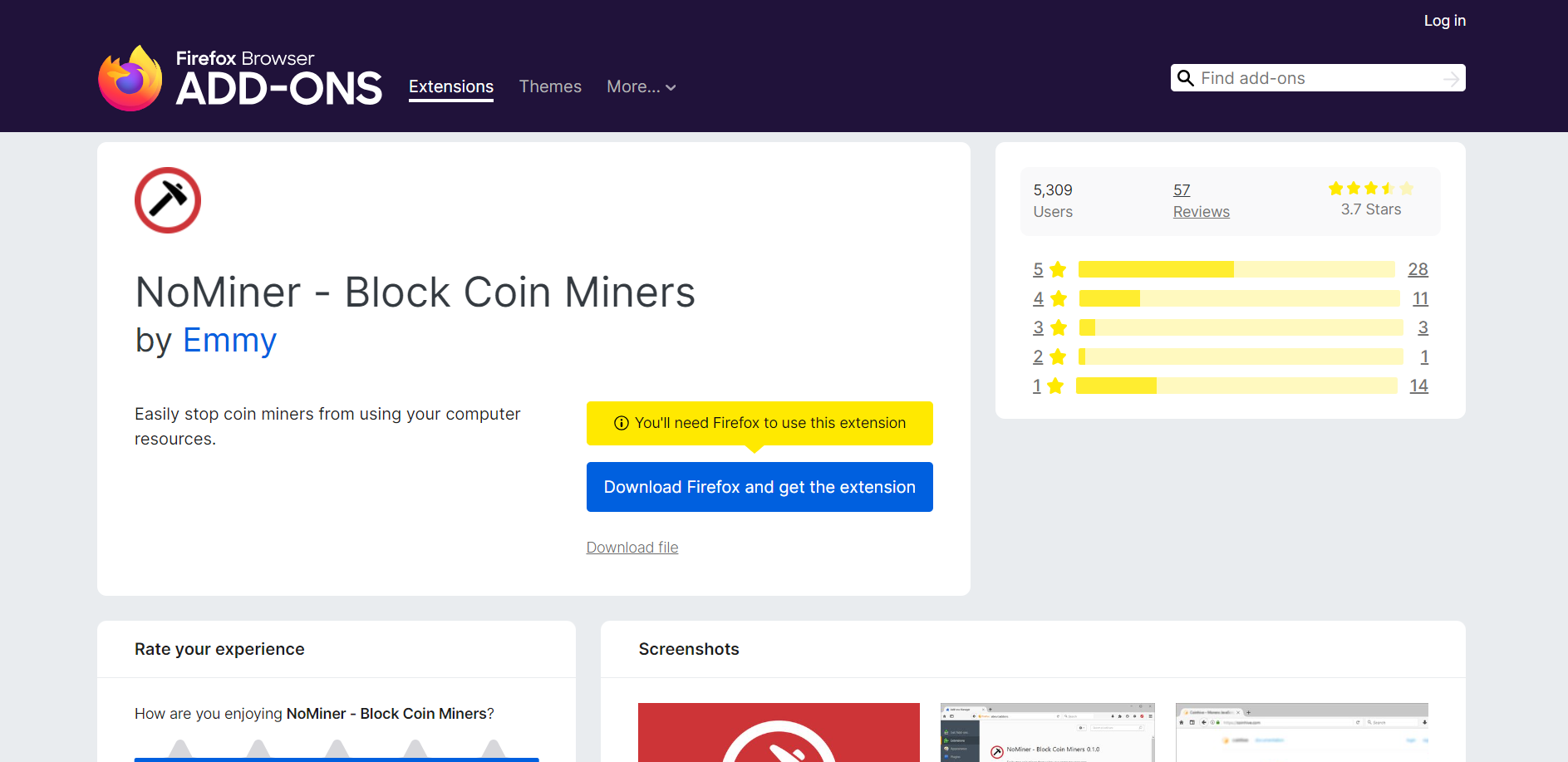
***Prevention:***

**

* *Install ad-blocking software: Ad-blocking extensions can help prevent malvertising from delivering cryptojacking scripts to your browser.*
* *Avoid pirated software: Only download software from trusted sources and official websites to avoid the risk of bundled cryptojacking scripts.*
* *Keep your software updated: Regularly update your operating system, web browser, and other software to ensure you have the latest security patches installed.*
* *Enable browser security settings: Enable enhanced protection settings in your web browser to block malicious scripts and websites.*
* *Install antivirus software: Use a reputable antivirus or anti-malware program to scan your computer regularly for potential threats, including cryptojacking scripts.*
* *Practice safe browsing habits: Avoid clicking on suspicious links, visiting untrusted websites, or opening attachments from unknown senders.*

Crypto mining malware has been a prevalent threat in the cybersecurity landscape. It is essential for individuals and organizations to remain vigilant and take steps to protect their systems from such malicious software.

*You can use extensions on browsers*

**