Hardware-based threat defense against increasingly complex cryptojackers

microsoft.com/security/blog/2022/08/18/hardware-based-threat-defense-against-increasingly-complex-cryptojackers

August 18, 2022

Even with the dip in the value of cryptocurrencies in the past few months, cryptojackers – trojanized coin miners that attackers distribute to use compromised devices' computing power for their objectives – continue to be widespread. In the past several months, Microsoft Defender Antivirus detected cryptojackers on hundreds of thousands of devices every month. These threats also continue to evolve: recent cryptojackers have become stealthier, leveraging living-off-the-land binaries (LOLBins) to evade detection.

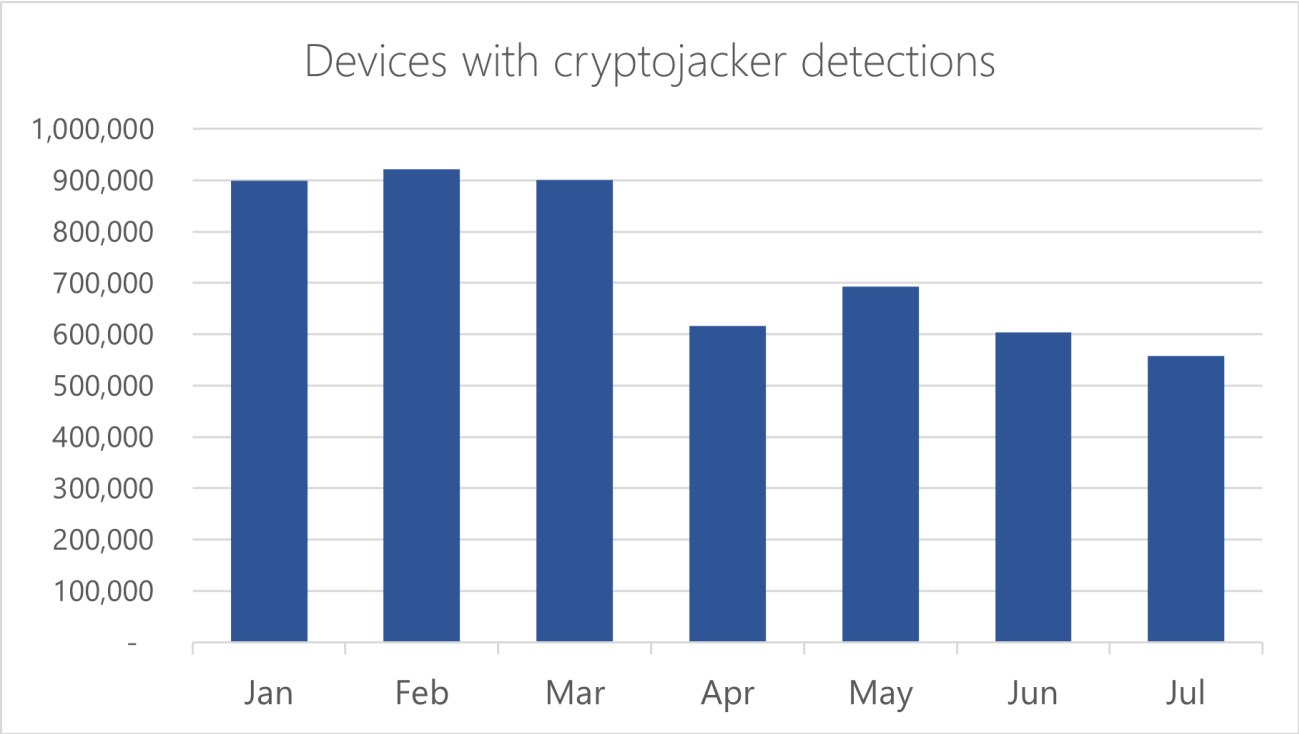

Figure 1. Chart showing number of devices on which Microsoft Defender Antivirus detected cryptojackers from January to July 2022.

To provide advanced protection against these increasingly complex and evasive threats, Microsoft Defender Antivirus uses various sensors and detection technologies, including its integration with Intel® Threat Detection Technology (TDT), which applies machine learning to low-level CPU telemetry to detect threats even when the malware is obfuscated and can evade security tools.

Using this silicon-based threat detection, Defender analyzes signals from the CPU performance monitoring unit (PMU) to detect malware code execution "fingerprint" at run time and gain unique insights into malware at their final execution point, the CPU. The combined actions of monitoring at the hardware level, analyzing patterns of CPU usage, and using threat intelligence and machine learning at the software level enable the technology to defend against cryptojacking effectively.

In this blog post, we share details from our monitoring and observation of cryptojackers and how the integration of Intel TDT and Microsoft Defender Antivirus detects and blocks this complex threat.

Looking at the current cryptojacker landscape

There are many ways to force a device to mine cryptocurrency without a user's knowledge or consent. The three most common approaches used by cryptojackers are the following:

- **Executable:** These are typically potentially unwanted applications (PUAs) or malicious executable files placed on the devices and designed to use system resources to mine cryptocurrencies.
- **Browser-based:** These miners are typically in the form of JavaScript (or similar technology) and perform their function in a web browser, consuming resources for as long as the browser remains open on the website where they are hosted. These miners are commonly injected into legitimate websites without the owner's knowledge or consent. In other cases, the miners are intentionally included in attacker-owned or less reputable websites that users might visit.
- **Fileless**: These cryptojackers perform mining in a device's memory and achieve persistence by misusing legitimate tools and LOLBins.

The executable and browser-based approaches involve malicious code that's present in either the filesystem or website that can be relatively easily detected and blocked. The fileless approach, on the other hand, misuses local system binaries or preinstalled tools to mine using the device's memory. This approach allows attackers to achieve their goals without relying on specific code or files. Moreover, the fileless approach enables cryptojackers to be delivered silently and evade detection. These make the fileless approach more attractive to attackers.

While newer cryptojackers use the fileless approach, its engagement of the hardware, which it relies on for its mining algorithm, becomes one of the ways to detect cryptojacking activities.

Misuse of LOLBins in recent cryptojacking campaigns

Through its various sensors and advanced detection methodologies, including its integration with Intel TDT, Microsoft Defender Antivirus sees cryptojackers that take advantage of legitimate system binaries on more than 200,000 devices daily.

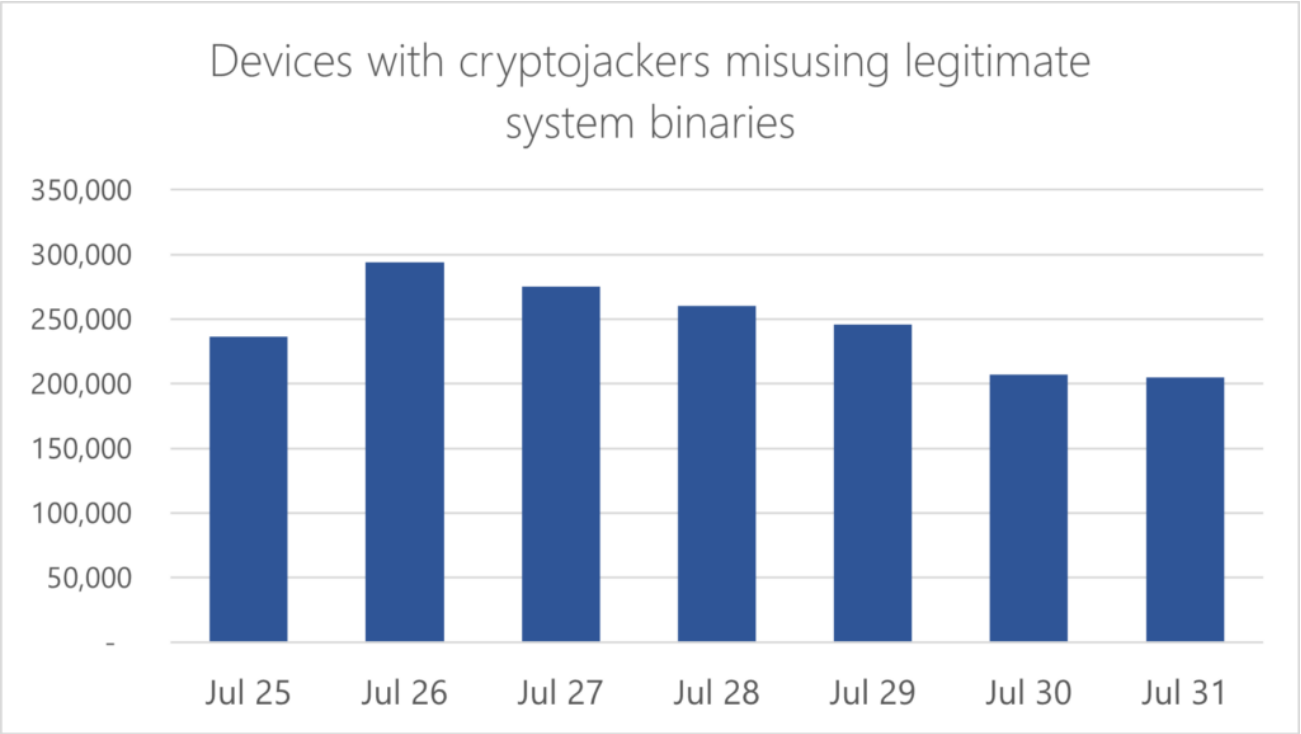

Figure 2. Chart showing the number of devices targeted by cryptojackers that misuse legitimate system binaries observed July 25-31, 2022.

Attackers heavily favor the misuse of *notepad.exe* among several legitimate system tools in observed campaigns.

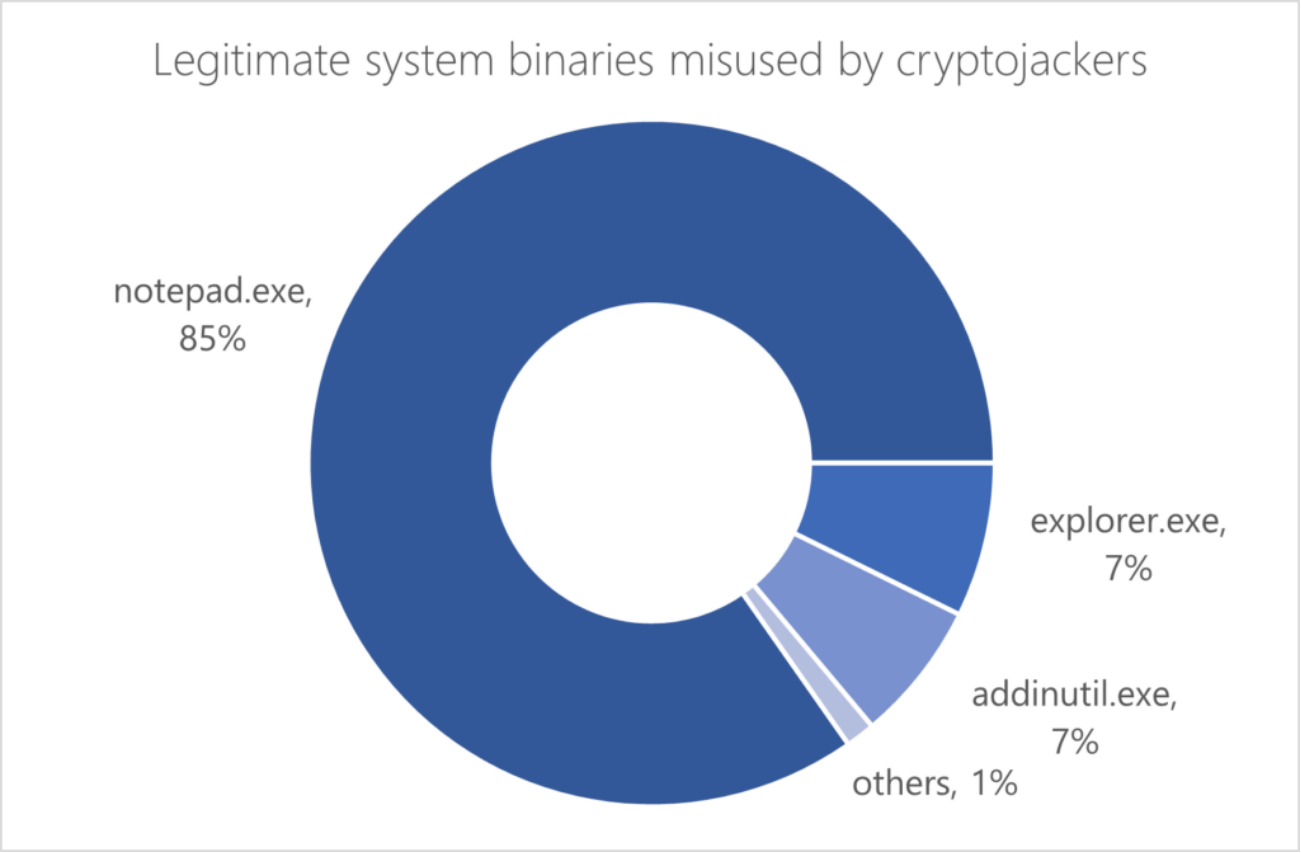

Figure 3. The chart shows that notepad.exe is the most abused tool based on the cryptojacking attacks observed from July 25-31, 2022.

We analyzed an interesting cryptojacking campaign abusing *notepad.exe* and several other binaries to carry out its routines. This campaign used an updated version of the cryptojacker known as Mehcrypt. This new version packs all of its routines into one script and connects to a command-and-control (C2) server in the latter part of its attack chain, a significant update from the old version, which ran a script to access its C2 and download additional components that then perform malicious actions.

The threat arrives as an archive file containing *autoit.exe* and a heavily obfuscated, randomly named .au3 script. Opening the archive file launches *autoit.exe,* whichdecodes the .au3 script in memory. Once running, the script further decodes several layers of obfuscation and loads additional decoded scripts in memory.

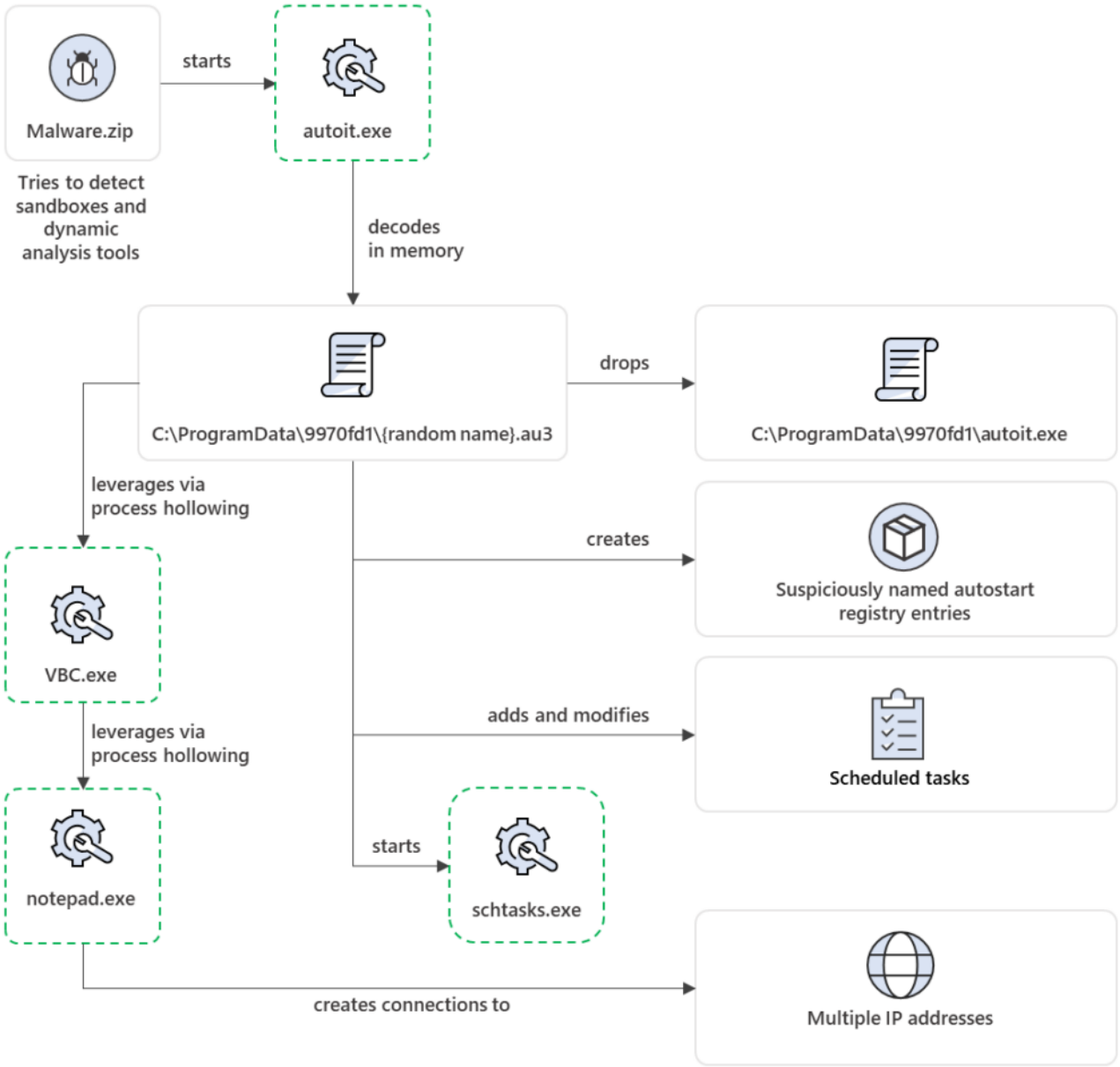

Figure 4. Infection chain of a new variant of Mehcrypt leveraging several binaries to launch its malicious routines.

The script then copies itself and *autoit.exe* in a randomly named folder in *C:\ProgramData*. The script creates a scheduled task to delete the original files and adds autostart registry entries to run the script every time the device starts.

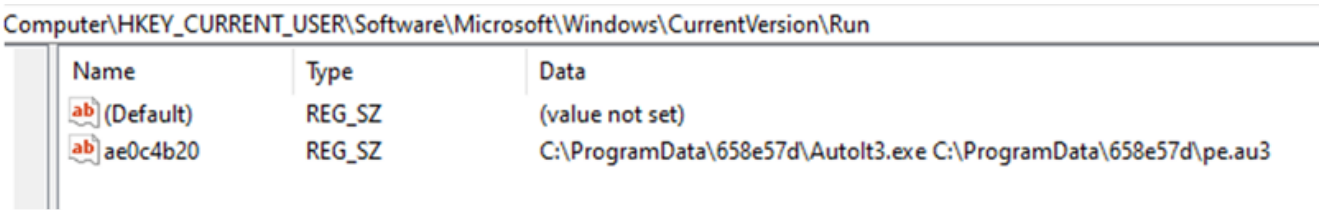

Figure 5. The malware creates an autostart registry entry to maintain persistence.

After adding persistence mechanisms, the script then loads malicious code into *VBC.exe* via process hollowing and connects to a C2 server to listen for commands. Based on the C2 response, the script loads its cryptojacking code into *notepad.exe*, likewise via process hollowing.

At this point, as the threat starts its cryptojacking operation via malicious code injected into *notepad.exe*, a huge jump in CPU usage can be observed:

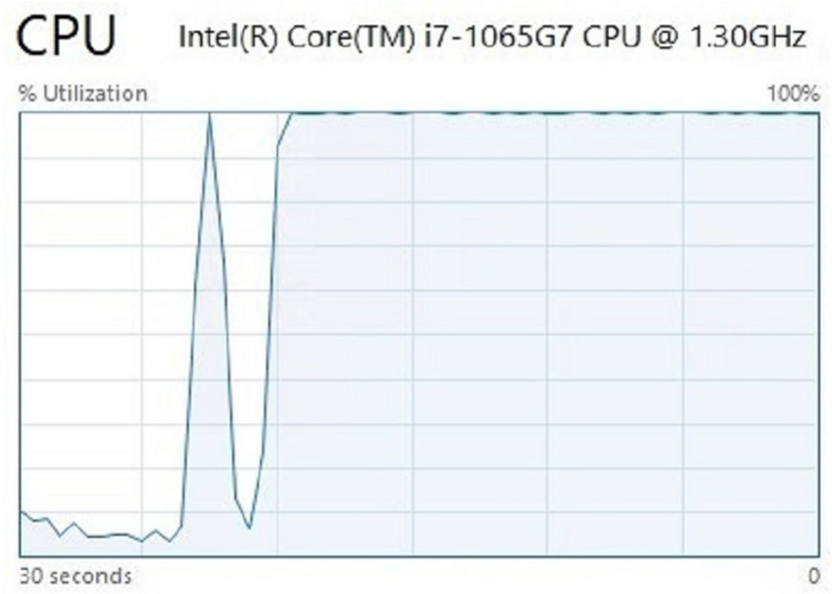

Figure 6. CPU usage shows a significant spike and continued maximum utilization as malicious activities are carried out.

This high CPU usage anomaly is analyzed in real-time by both Intel TDT and Microsoft Defender Antivirus. Based on Intel TDT's machine learning-based correlation of CPU telemetry and other suspicious activities like process injection into system binaries, Microsoft Defender Antivirus blocks the process execution (Behavior:Win32/CoinMiner.CN!tdt), and Microsoft Defender for Endpoint raises an alert.

Advanced threat detection technology helps stop cryptojacking activities

To detect evasive cryptojackers, Microsoft Defender Antivirus and Intel TDT work together to monitor and correlate hardware and software threat data. Intel TDT leverages signals from the CPU, analyzing these signals to detect patterns modeled after cryptojacking activity using machine learning. Microsoft Defender Antivirus then uses these signals and applies its threat intelligence and machine learning techniques to identify and block the action at the software level.

Intel TDT has added several performance improvements and optimizations, such as offloading the machine learning inference to Intel's integrated graphics processing unit (GPU) to enable continuous monitoring. This capability is available on Intel Core™ processors and Intel vPro® branded platforms from the 6th generation onwards. By design, Microsoft Defender Antivirus leverages these offloading capabilities where applicable.

In addition to industry partnerships, Microsoft's consistent monitoring of the threat landscape powers the threat intelligence that feeds into products like Microsoft Defender Antivirus and Microsoft Defender for Endpoint, where knowledge is translated to customer protection in real-time.

Suriyaraj Natarajan, Andrea Lelli, Amitrajit Banerjee
Microsoft 365 Defender Research Team