

2021 Cryptojacking Trends + Investigation Recommendations

crowdstrike.com/blog/2021-cryptojacking-trends-and-investigation-recommendations/

Falcon OverWatch Team

October 27, 2021



Throughout 2021, the CrowdStrike Falcon OverWatch™ team has observed the volume of cryptojacking intrusions more than quadruple compared to 2020. ECrime adversaries are using cryptojacking as a means of monetizing an intrusion, in addition to ransom demands and data extortion — and they’re going to greater lengths to employ stealthy techniques to optimize the performance of their tooling and make system changes to avoid discovery.

Cryptojacking involves the unauthorized use of a system’s resources to mine cryptocurrency, one of any number of digital currencies. This can be done via the installation of malware or by injecting malicious code into a webpage. Cryptojacking can impact the performance of systems and consume excess energy, and crucially, it indicates a more significant issue with the integrity of an organization’s security.

There will always be sophisticated attackers with the resources and motivation to bypass or exploit technology-based defenses, and threat actors are increasingly leveraging valid accounts and native tooling to avoid detection. This blog unpacks the interesting hands-on

cryptojacking tradecraft that OverWatch threat hunters uncovered in the first half of 2021 and provides recommendations for identifying cryptojacking tradecraft within your environment.

OverWatch tracks interactive intrusion activity against the MITRE ATT&CK® Enterprise Matrix, and cryptojacking tradecraft is categorized under the [Resource Hijacking \(T1496\)](#) technique, part of the “Impact” tactic group.

Why eCrime Adversaries Are Using Cryptojackers

ECrime adversaries are, by definition, primarily motivated by financial gain. Cryptojacking is yet another tool in their arsenal to anonymously extract payment following a compromise. Cryptocurrency prices have spiked to unprecedented heights in recent months, and eCrime adversaries, looking to profit from these inflated prices, have responded by incorporating cryptojacking into their toolset. In this climate, it is likely that the number of cryptojacking victims is high, but because this activity does not involve data theft, there is often no requirement for victims to disclose attacks and risk reputational damage.



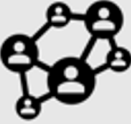











Another likely motivation behind the adoption of cryptojacking activity is the fact that it can be relatively straightforward to execute. These applications generally do not require elevated permissions and can be installed by standard accounts. Many commodity cryptojackers also have browser extension tooling, so installation can be very quick and easy. OverWatch often finds adversaries attempting to take advantage of limited software controls to install cryptojacking applications, and threat hunters are critical for unearthing activity where adversaries are operating under valid accounts to configure cryptojackers.

In addition, most mining applications have a minimal code base, and due to the simplicity of the disk operations required, adversaries can quickly write cryptojacking code to disk that can blend in with legitimate scripts. Cryptojacking applications are mostly platform-agnostic, so adversaries can reuse code against multiple operating systems. Finally, adversaries can subvert network-based defenses by blending their requests into everyday telemetry and leveraging encryption or obfuscation to hide the payload data. CrowdStrike [Falcon Prevent™](#) next-generation antivirus (NGAV) has the ability to detect and prevent up to 99% of known and unknown threats, but human defenders will always be necessary when up against human attackers. Depending on the adversary’s level of sophistication and access, they may opt for cryptojacking rather than ransomware objectives after gaining hands-on-keyboard access. Continuous threat hunting operations will augment your ability to identify tradecraft that bypasses traditional controls and the techniques designed to subvert technology.

What’s Changing in 2021

OverWatch is seeing cryptojacking activity in 2021 that far outpaces 2020 and has uncovered hands-on cryptojacking activity in 14 industry verticals. The vast array of targeted verticals indicates that no organization is safe from eCrime adversaries looking to profit from

cryptojacking attacks, and the rapid increase in this type of tradecraft suggests that these intrusions are increasingly opportunistic.

						
Academic	Automotive	Conglomerate	Engineering	Financial	Food & Beverage	Government
						
Manufacturing	Maritime	Media	Pharmaceutical	Retail	Technology	Telecommunications

The hands-on cryptojacking activity that OverWatch uncovers shares similarities with other eCrime activity, where actors are leveraging valid accounts and native tooling to avoid detection. This was certainly the case in a recent intrusion by an unknown eCrime group that performed extensive discovery using WMIC to enumerate the host's system and hardware information. The adversary operated under a PostgreSQL service after remotely compromising the vulnerable server. They proceeded to use a highly obfuscated Base64 PowerShell command to acquire a low-prevalence cryptojacker to disk. The following graphic shows the process tree associated with this activity. Investigation revealed that along with acquiring the cryptojacker, the adversary leveraged native tooling for reconnaissance. At every step of this intrusion, the adversary attempted to evade defenses, from subtly acquiring the binary to performing enumeration using native tools.

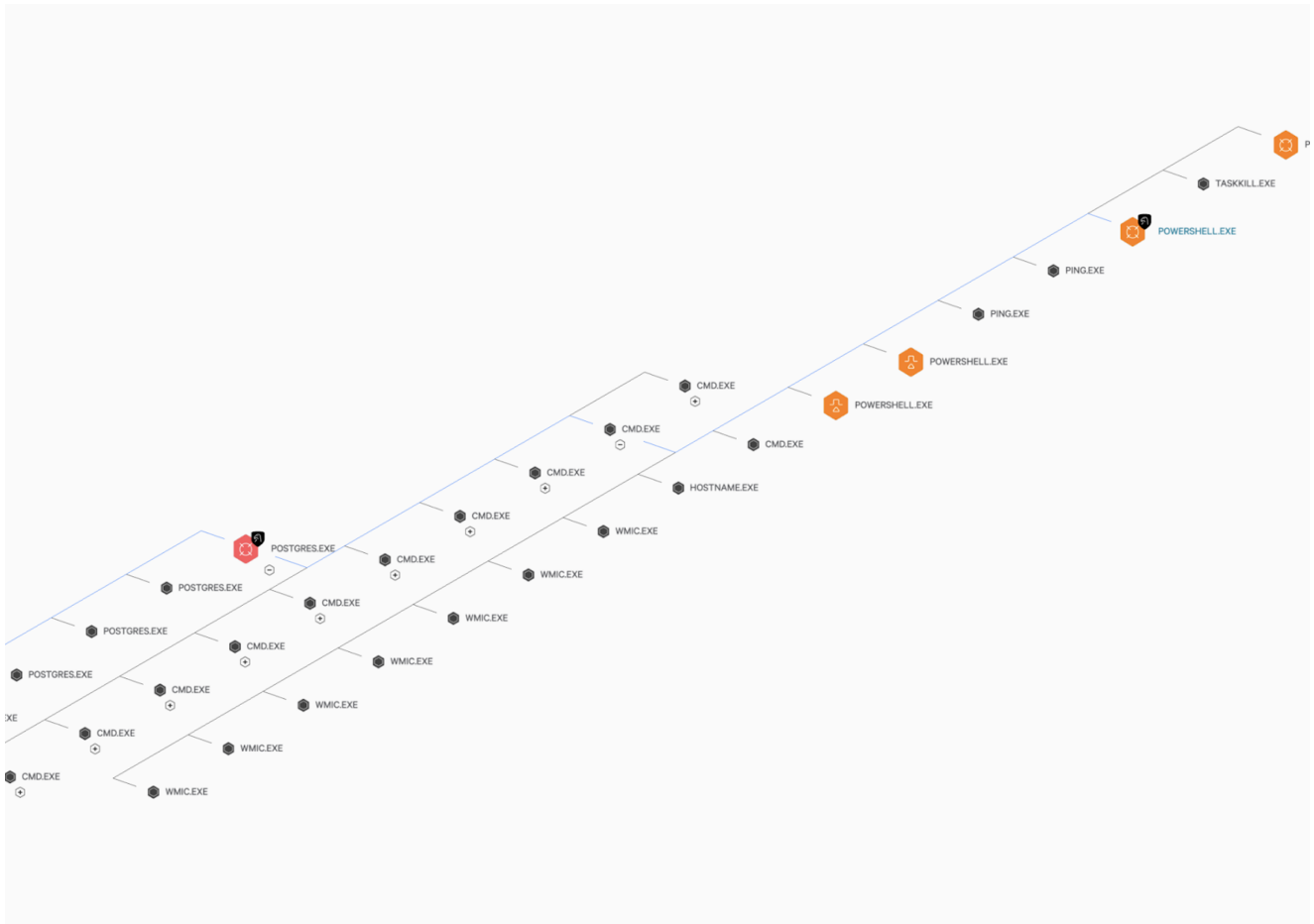


Figure 1: Ecrime adversary operating under a PostgreSQL session, performing host reconnaissance using native tooling, and acquiring a custom cryptojacker to disk using obfuscated PowerShell commands. (Click to enlarge)

An interesting development in the cryptojacking activity that OverWatch has observed is the adversaries' efforts to modify victim hosts to ensure that cryptojacking applications operate under the radar. In one such eCrime intrusion, the adversary gained access via RDP password spraying and wrote a Kryptex Monero cryptojacker to disk. The adversary then set scheduled tasks to routinely execute the binary for persistence purposes. In an attempt to run the cryptojacker covertly and bypass defenses, they made firewall changes to allow only outbound Kryptex traffic and deny any unnecessary inbound Kryptex server connections.

The adversary proceeded to invoke multiple registry changes, shown in the commands below. The first command modifies the default value of the `TdrDelay` key from 2 seconds to 20 seconds. This key handles GPU preempt requests — it is likely that the adversary made this change to force their cryptojacker to run “low and slow” and therefore be less likely to trigger any detections for high GPU usage.

```
C:\Windows\system32\cmd.exe /d /s /c "reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers /v TdrDelay /t
REG_DWORD /d 0x14 /f"
```

Similarly, the adversary also changed another GPU registry key named `TdrDdiDelay`, increasing the value from 5 to 10 seconds. This key controls the rate at which threads leave the GPU driver, and this delay allows their cryptojacking threads to execute at a much slower rate.

```
C:\Windows\system32\cmd.exe /d /s /c "reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers /v TdrDdiDelay /t
REG_DWORD /d 0xa /f"
```

OverWatch has also observed similar tradecraft amongst Linux systems. The following two command lines were observed in separate intrusions where eCrime adversaries invoked system changes likely intended to improve the performance of custom cryptojackers. This is a timely reminder that adversaries do not discriminate and will actively target hosts regardless of the installed operating system.

The first command is a native utility, HugePages, which was used to increase from 4KB to 128KB the memory pages supported by the operating system. This memory efficiency change was likely to allow their cryptojacker to run without causing potential resource exhaustion issues.

```
sysctl vm.nr_hugepages=128
```

The second intrusion featured the adversary using the native utility MSR in an effort to improve the performance of a custom cryptojacker by enabling prefetch writes. These Linux intrusions were both preceded by a brief period of reconnaissance to collect details on the system. This reconnaissance also took advantage of “living off the land,” using tooling already installed natively on the system to blend into everyday telemetry.

```
sh -c /sbin/modprobe msr allow_writes=on > /dev/null 2>&1
```

Threat Hunting as a Tool to Unearth Cryptojacking Tradecraft

Threat hunters are incredibly well placed to proactively search for early signs of cryptojacking activity, understand the context of the activity and determine how widespread the intrusion is. Outlined below are several recommendations for defenders looking to proactively investigate this activity.

- As shown above, the registry can be modified to alter mining requests, and it is therefore recommended to look for any anomalous registry changes to GPU or CPU keys. In addition, any fluctuations in GPU/CPU temperature that cannot be accounted for or that take place out of hours should be reviewed, along with inspecting any sustained utilization on hosts that differ from the baseline or expected volume.

- Cryptojacking applications will often attempt to stop a range of commodity cryptojacking process names to eliminate competition from any other mining application that may be currently installed. OverWatch recommends looking for this activity, which may also be associated with an unsigned binary, a rogue browser extension, or a file stored within a suspicious location.
- Adversaries may manually write cryptojacking code to disk, so it can also be useful to look for signs of file compilation events. This may also be found around the same time as associated events, such as new scheduled tasks being set for persistence purposes or native tools being used to timestamp the file in an attempt to make the malware appear legitimate.
- OverWatch further recommends investigating network connections to known mining network pools and any connections to suspicious domains such as Pastebin or Github, where commodity cryptojacking tools can be easily acquired and can masquerade as a legitimate code base.
- In addition to these investigations, it is also essential to consider the basics, as adversaries will always exploit low-hanging fruit. IT hygiene is critical, such as establishing an unauthorized software policy and ensuring rapid patching of systems following any legitimate vendor updates. It is also important to understand your environment and its critical assets, ensure full endpoint detection and response (EDR) coverage across all hosts to support visibility, and maintain strong content filtering protections across installed security technologies.

For more information on cryptojacking, see our [Cybersecurity 101 page](#).

Additional Resources

- *[Read about the latest trends in threat hunting and more in the 2021 Threat Hunting Report or simply download the report now.](#)*
- *[Learn more about Falcon OverWatch proactive managed threat hunting.](#)*
- *[Watch this video](#) to see how Falcon OverWatch proactively hunts for threats in your environment.*
- *[Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.](#)*
- *[Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.](#)*