Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

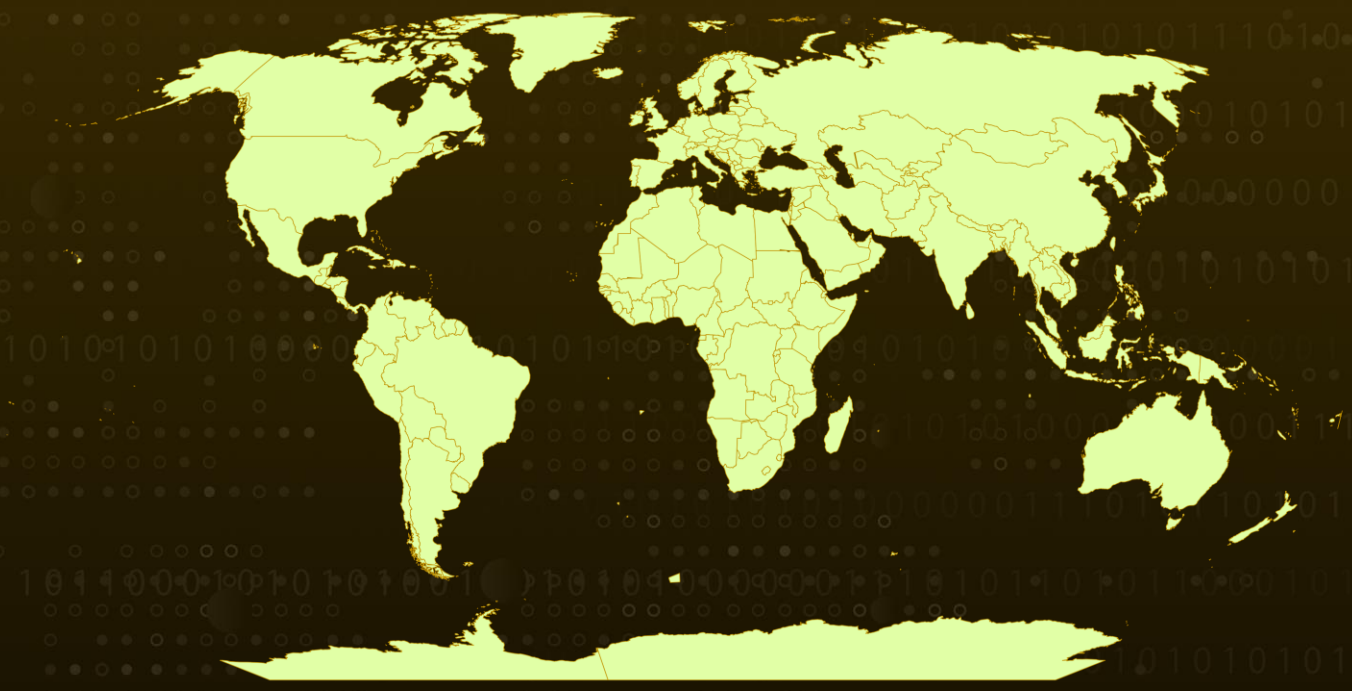
Unveiling the Minas Miner's Deceptive Tactics

Date of Publication	Admiralty Code	TA Number
May 18, 2023	A1	TA2023235

Summary

First seen: June 2022
Malware: Minas
Attack Region: Worldwide
Attack: Minas is a multi-stage cryptocurrency miner with a concealed presence. It evades detection through encryption, randomization, and persistence techniques, showcasing determined network compromise.

Attack Regions



Attack Details

#1 Minas is a multi-stage cryptocurrency miner infection that utilizes a standard implementation to conceal its presence. This infection follows a chain of events where an encoded PowerShell script, likely generated via Group Policy Objects (GPO), acts as a running task. The main objective of this PowerShell script is to initiate the malware installation process.

#2 To accomplish this, the script retrieves an encrypted payload from a remote server and subsequently decrypts it using a custom XOR encryption algorithm. The decrypted payload takes the form of a .NET binary (DLL) which is then executed by the PowerShell process.

#3 The Minas miner employs a standard implementation to effectively conceal its presence. It achieves a high level of detection evasion through encryption, random name generation, and the utilization of hijacking and injection techniques. Additionally, it possesses the capability to persist on the infected system by employing various persistence techniques.

#4 The method by which the initial PowerShell command is executed remains unknown, which is particularly alarming as it suggests that the attackers have successfully compromised the network. This signifies their determination to install Minas miners, indicating the extent of their efforts.

Recommendations

- Continuously Monitor Networks for Malicious Activity: Implement robust network monitoring tools and practices to detect suspicious or malicious activity signs. Stay updated with the latest indicators of compromise (IOCs) by regularly updating security tools and threat intelligence feeds.
- An Antivirus (AV) Solution with Behavior-Based Detection: When selecting an AV solution, opting for one that doesn't solely depend on signature detection is advisable. Instead, prioritize an AV solution that incorporates behavior analysis of processes. This approach allows for more comprehensive and effective detection of threats like the Minas Miner, which employs deceptive tactics to evade traditional signature-based detection methods.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**T1127** Trusted Developer Utilities Proxy Execution	**T1140** Deobfuscate/Decode Files or Information	**T1055** Process Injection
T1057 Process Discovery	**T1106** Native API	**T1574** Hijack Execution Flow	**T1083** File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	08da41489b4b68565dc77bb9acb1ecb4 06fe9ab0b17f659486e3c3ace43f0e3a f38a1b6b132afa55ab48b4b7a8986181 63e0cd6475214c697c5fc115d40327b4

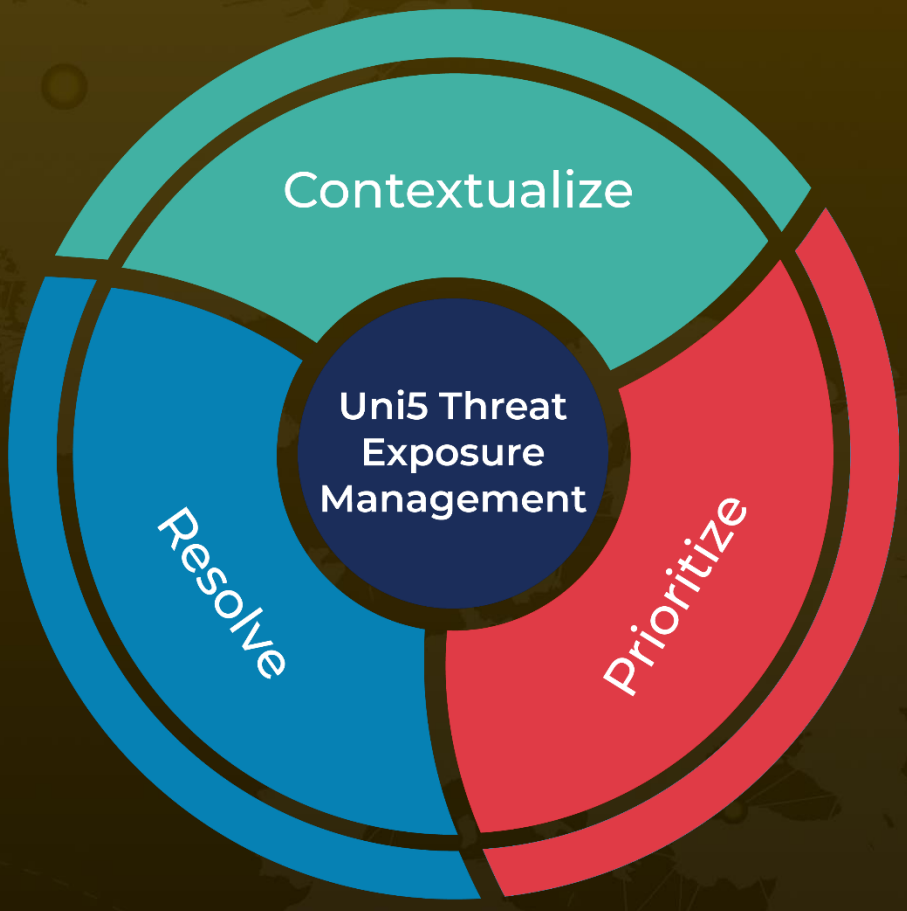
References

https://securelist.com/minas-miner-on-the-way-to-complexity/109692/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 18, 2023 • 5:55 AM

More at www.hivepro.com