Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

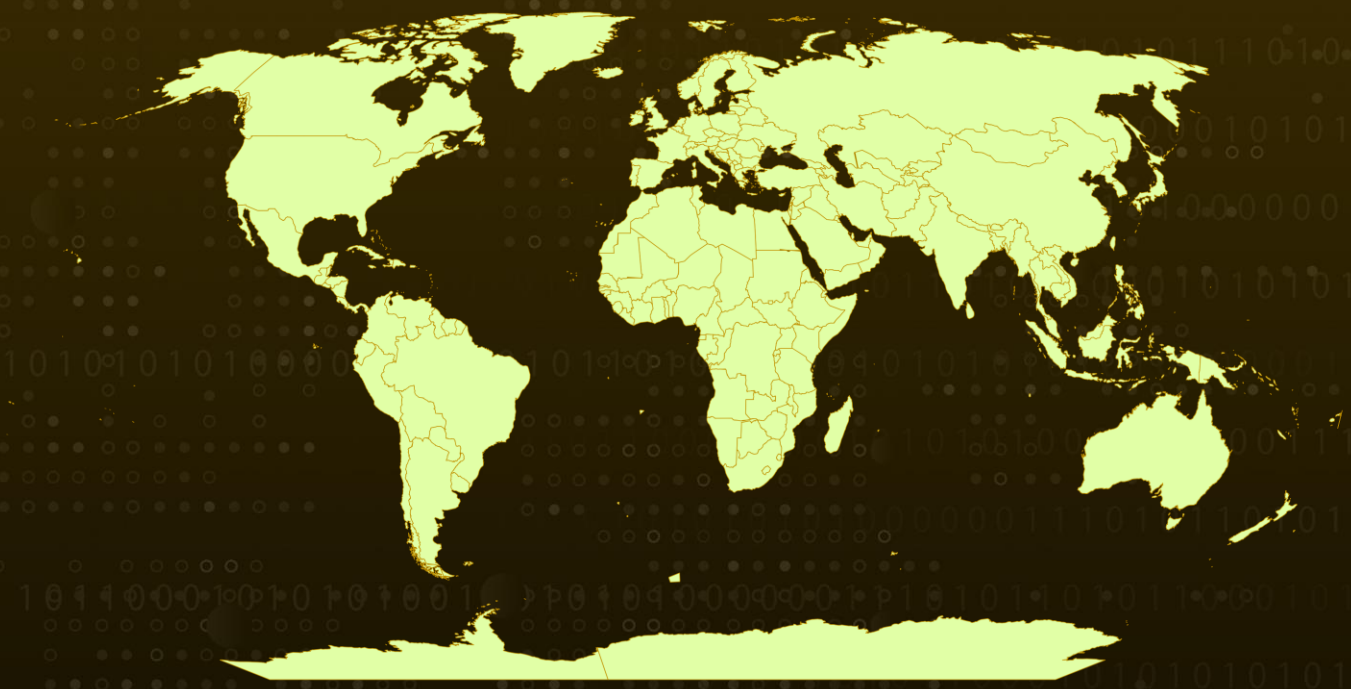
REF4578 Campaign Unleashes the Highly Modular GhostEngine Malware

Date of Publication	Admiralty Code	TA Number
May 23, 2024	A1	TA2024203

Summary

Attack Began: May 6, 2024
Attack Region: Worldwide
Malware: GhostEngine, XMRigMiner
Campaign: REF4578
Attack: A malicious crypto mining campaign, codenamed 'REF4578,' has been discovered deploying a malicious payload named GhostEngine. This payload exploits vulnerable drivers to disable security products and deploy an XMRig miner. The campaign is notable for its complexity, which ensures both the installation and persistence of the XMRig miner.

Attack Regions



Attack Details

#1 The 'REF4578' crypto mining campaign has been identified, utilizing GhostEngine as its primary payload to exploit vulnerable drivers, disable security products, and deploy an XMRig miner. This campaign demonstrates complexity in ensuring the installation and persistence of the miner. The intrusion was initiated on May 6, 2024, with a PE file disguised as a legitimate Windows file, which triggered the download and execution of a PowerShell script.

#2 GhostEngine, the core script utilized in the campaign, operates by retrieving and executing multiple modules via HTTP and FTP protocols. It conducts system cleanup by removing remnants of previous infections and malicious files from specific directories. Additionally, it clears Windows event log channels and attempts to disable Windows Defender during execution. The script further enables remote services and ensures sufficient disk space for file downloads.

#3 To ensure persistence, GhostEngine creates multiple scheduled tasks as SYSTEM. Its Update/Persistence module (oci.dll) acts as a service DLL and gets auto invoked with mstdc. Additionally, it downloads and verifies the hashes of retrieved PE files to check for and download updated binaries when necessary.

#4 Furthermore, GhostEngine other modules like the EDR agent controller and miner module (smartsscreen.exe) terminate active EDR agents and install a crypto-miner. It employs two kernel drivers, aswArPots.sys and IObitUnlockers.sys, to terminate EDR software and delete associated executables. The EDR agent termination module (kill.png) injects shellcode to terminate security agents and load PE files into memory.

#5 Finally, the PowerShell backdoor module (backup.png) enables remote command execution on the compromised system. This multifaceted approach highlights the sophistication and danger of the 'REF4578' campaign, which aims to exploit vulnerabilities, disable defenses, and profit through illicit crypto-mining activities.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1070 Indicator Removal	T1070.001 Clear Windows Event Logs	T1036 Masquerading	T1055 Process Injection
T1057 Process Discovery	T1041 Exfiltration Over C2 Channel	T1132 Data Encoding	T1496 Resource Hijacking
T1489 Service Stop			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 4b5229b3250c8c08b98cb710d6c056144271de099a57ae09f5d2097fc41bd4f1, 2b33df9aff7cb99a782b252e8eb65ca49874a112986a1c49cd9971210597a8ae, 3ced0552b9ecf3dfecd14cbcc3a0d246b10595d5048d7f0d4690e26ecccc1150, 3b2724f3350cb5f017db361bd7aae49a8dbc6faa7506de6a4b8992ef3fd9d7ab, 35eb368c14ad25e3b1c58579ebaeae71bdd8ef7f9ccecfc00474aa066b32a03f, 786591953336594473d171e269c3617d7449876993b508daa9b96eedc12ea1ca, 11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5, aac7f8e174ba66d62620bd07613bac1947f996bb96b9627b42910a1db3d3e22b, 6f3e913c93887a58e64da5070d96dc34d3265f456034446be89167584a0b347e, 7c242a08ee2dfd5da8a4c6bc86231985e2c26c7b9931ad0b3ea4723e49ceb1c1, cc4384510576131c126db3caca027c5d159d032d33ef90ef30db0daa2a0c4104
Domain	download.yrnvtklot[.]com, ftp.yrnvtklot[.]com, online.yrnvtklot[.]com
IPv4	111[.]90[.]158[.]40, 93[.]95[.]225[.]137

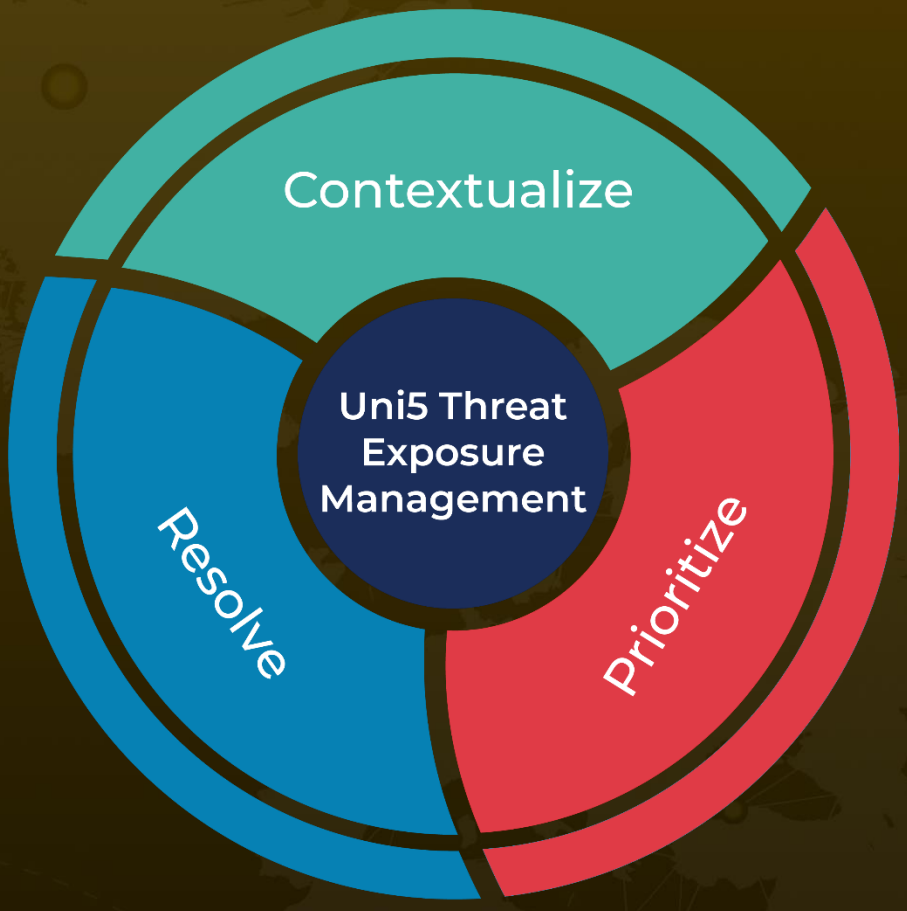
References

https://www.elastic.co/security-labs/invisible-miners-unveiling-ghostengine

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 23, 2024 • 6:30 AM

More at www.hivepro.com