GHOSTENGINE Malware Exploits Vulnerable Drivers to Terminate EDR Agents

Date: 24th May 2024 | Severity: High

Summary

Discovered REF4578, an intrusion set that uses vulnerable drivers to disable established security solutions (EDRs) for crypto mining and deploys a malicious payload known as GHOSTENGINE.

GHOSTENGINE oversees locating and running the machine's modules. To download files from a configured domain, it mostly uses HTTP, with a backup IP in case the domain is unavailable. It also uses FTP as a backup protocol that includes embedded credentials.

This campaign required an unusual level of complexity to ensure the XMRIG miner would be installed and persistent.

Attack Vectors

This file downloads and runs a PowerShell script that manages the intrusion's whole execution flow when it is executed.

According to analysis, this program executes a hardcoded PowerShell command line to obtain an obfuscated script called get.png. This script is then used to download more tools, modules, and configurations from the attacker C2.

The PowerShell script attempts to disable Windows Defender, enable remote services, and clean the Windows event log channels to establish persistence, get.png creates the OneDriveCloudSync,DefaultBrowserUpdate, and OneDriveCloudBackup scheduled tasks as SYSTEM.

GHOSTENGINE installs several modules that can check for software updates, build with security tools, and construct a backdoor.

The main function of the smartscreen.exe module is to end any running EDR agent processes before downloading and setting up a cryptocurrency miner.

The goal of the REF4578 intrusion set was to gain access to an environment and deploy a persistent Monero crypto miner, XMRig.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Hash Value	• a179c4093d05a3e1ee73f6ff07f994aa • bd877072c51ee58ec7aaf091bff0b80c • 0c0195c48b6b8582fa6f6373032118da • 2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753 • 18957d83337a7f6a879d739be02b173e • 125982676af23e93fa58b31ef1bdb93725cb91c3 • 11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5 • 5d6b9e80e12bfc595d4d26f6afb099b3cb471dd4 • 41fce204948df6af1fe2f3f6dec02086678eab3b • d25340ae8e92a6d29f599fef426a2bc1b5217299 • 7c242a08ee2dfd5da8a4c6bc86231985e2c26c7b9931ad0b3ea4723e49ceb1c1 • aac7f8e174ba66d62620bd07613bac1947f996bb96b9627b42910a1db3d3e22b • 6f3e913c93887a58e64da5070d96dc34d3265f456034446be89167584a0b347e • 786591953336594473d171e269c3617d7449876993b508daa9b96eedc12ea1ca • cc4384510576131c126db3caca027c5d159d032d33ef90ef30db0daa2a0c4104 • 2b33df9aff7cb99a782b252e8eb65ca49874a112986a1c49cd9971210597a8ae • 35eb368c14ad25e3b1c58579ebaeae71bdd8ef7f9ccecfc00474aa066b32a03f • 4b5229b3250c8c08b98cb710d6c056144271de099a57ae09f5d2097fc41bd4f1 • 3b2724f3350cb5f017db361bd7aae49a8dbc6faa7506de6a4b8992ef3fd9d7ab • 3ced0552b9ecf3dfecd14cbcc3a0d246b10595d5048d7f0d4690e26ecccc1150
Domains	• Download[.]yrnvtklot.com • Online[.]yrnvtklot.com • ftp[.]yrnvtklot.com
IPs	• 111[.]90.158.40 • 93[.]95.225.137

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes and block IPs.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://cybersecuritynews.com/ghostengine-malware-terminates-edr-agents/
- https://www.broadcom.com/20240522-ghostengine-malware-terminates-edr-agents-and- deploys-coin-miner