Novel EDR-Killing 'GhostEngine' Malware Is Built for Stealth

darkreading.com/cyberattacks-data-breaches/novel-edr-killing-ghostengine-malware-stealth

Elizabeth Montalbano, Contributing Writer

Source: Jack Maguire via Alamy Stock Photo

A novel malware that targets vulnerable drivers to terminate and thus evade endpoint detection and response (EDR) solutions has come to light, for now used in service of an elaborate cryptomining campaign.

Researchers at Elastic Security Labs identified what they are calling an "intrusion set" dubbed "REF4578," that uses a multimodal malware called GhostEngine; it can disable EDR, they revealed in a blog post published today. The attack also demonstrates capabilities to establish persistence as well as install a previously undocumented backdoor in addition to executing a cryptominer.

"GhostEngine leverages vulnerable drivers to terminate and delete known EDR agents that would likely interfere with the deployed and well-known coin miner," Elastic researchers Salim Bitam, Samir Bousseaden, Terrance DeJesus, and Andrew Pease wrote in the post.

"This campaign involved an uncommon amount of complexity to ensure both the installation and persistence of the XMRig miner."

Meanwhile, a team at Antiy Labs also observed the attacks, calling the payload "Hidden Shovel" and characterizing it as a "mining Trojan" that delivers a two-stage approach to disabling EDR and installing a backdoor, according to a blog post.

Ultimately, the goal of the campaign as described by both sets of researchers is to take out the security barriers present in a corporate network and use it to mine cryptocurrency without administrators detecting the action. The legitimate miner XMRig leveraged by attackers is used for mining Monero.

Neither security team outlined which organizations or individuals are the targets of the campaign, nor did they identify which threat actor might be behind it.

The GhostEngine Attack Vector

As described by Elastic, REF4578's initial intrusion occurs with the execution of a PE file named Tiworker.exe that impersonates the legitimate Windows TiWorker.exe file.

"This file downloads and executes a PowerShell script that orchestrates the entire execution flow of the intrusion," the researchers wrote. This process downloads attacker tools, GhostEngine malware modules, and configurations from the attacker's command-and-control (C2) server.

GhostEngine then proceeds to download and execute its various attack modules on the machine. Its tasks also include purging the system of remnants of prior infections belonging to the same family of malware but from different campaigns, as well as attempting to disable Windows Defender and clean various Windows event log channels.

The malware also has a persistence mechanism and a process for downloading its modules on the infected system. These modules "can tamper with security tools, create a backdoor, and check for software updates," the Elastic researchers wrote.

Most interestingly, the modules include an EDR agent controller and miner module that primarily terminates any active EDR agent processes before downloading and installing a cryptominer. It's written in C++, and has redundancy built into its operation, according to Elastic. It also includes a PowerShell script that functions like a backdoor, enabling remote command execution on the system. Elastic researchers also extracted the configuration file from the XMRig miner used in the campaign, "which was tremendously valuable, as it allowed us to report on the Monero Payment ID and track the worker and pool statistics, mined cryptocurrency, transaction IDs, and withdrawals," they wrote.

Detecting GhostEngine

As attackers have been known to mount attacks that evade EDR solutions before, it's important for defenders to identify how to detect when these barriers have been breached.

In terms of the GhostEngine malware, its first objective is to incapacitate endpoint security solutions and disable specific Windows event logs — such as security and system logs, which record process creation and service registration.

As such, the researchers recommended that organizations prioritize the detection and prevention of these initial actions to detect its presence on a network, including: suspicious PowerShell execution; execution from unusual directories; elevating privileges to system integrity; and deploying vulnerable drivers and establishing associated kernel mode services.

"Once the vulnerable drivers are loaded, detection opportunities decrease significantly, and organizations must find compromised endpoints that stop transmitting logs to their SIEM," the Elastic researchers wrote.

Further, network traffic may generate and be identifiable if DNS record lookups point to known mining pool domains over well-known ports such as HTTP (80) and HTTPS (443), the researchers noted. Meanwhile, Stratum is also another popular network protocol for miners, by default, over port 4444, they said.

Detection rules and behavior prevention events associated with the campaign include the following: suspicious PowerShell downloads; service control spawned via Script Interpreter; local scheduled task creation; process execution from an unusual director; unusual parent-child relationship; clearing Windows event logs; and tampering with Microsoft Windows Defender, among others.

About the Author(s)

Elizabeth Montalbano, Contributing Writer

Elizabeth Montalbano is a freelance writer, journalist, and therapeutic writing mentor with more than 25 years of professional experience. Her areas of expertise include technology, business, and culture. Elizabeth previously lived and worked as a full-time journalist in Phoenix, San Francisco, and New York City; she currently resides in a village on the southwest coast of Portugal. In her free time, she enjoys surfing, hiking with her dogs, traveling, playing music, yoga, and cooking.

See more from Elizabeth Montalbano, Contributing Writer

Keep up with the latest cybersecurity threats, newly discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

Subscribe