

GhostMiner Weaponizes WMI, Kills Other Mining Payloads

blog.trendmicro.com/trendlabs-security-intelligence/fileless-cryptocurrency-miner-ghostminer-weaponizes-wmi-objects-kills-other-cryptocurrency-mining-payloads/

September 19, 2019



Cybercriminals continue to use cryptocurrency-mining malware to abuse computing resources for profit. As early as [2017](#), we have also observed how they have applied fileless techniques to make detection and monitoring more difficult.

On August 2, we observed a fileless cryptocurrency-mining malware, dubbed GhostMiner, that weaponizes Windows management instrumentation (WMI) objects for its fileless persistence, payload mechanisms, and AV-evasion capabilities. This GhostMiner variant was also observed to modify infected host files that are heavily used by [MyKings](#), [PowerGhost](#), [PCASTLE](#), and [BULEHERO](#), among others.

This malware was observed mining Monero cryptocurrency, however, the arrival details of this variant has not been identified as of writing. An earlier [documented](#) sighting of GhostMiner was noted to have used multiple vulnerabilities in MSSQL, phpMyAdmin, and Oracle's WebLogic to look for and attack susceptible servers.

GhostMiner Details

GhostMiner uses [WMI Event Subscriptions](#) to install persistence in an infected machine as well as execute arbitrary code.

```
Event Filter \\.\ROOT\subscription: __EventFilter.Name="PowerShell Event Log Filter" EventNamespace : root\cimv2 Query : SELECT * FROM __InstanceModificationEvent WITHIN 3600 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System' QueryLanguage : WQL
```

FilterToConsumerBinding

```
\\.\ROOT\subscription: __FilterToConsumerBinding.Consumer="CommandLineEventConsumer.Name=PowerShell Event Log Consumer",Filter="__EventFilter.Name=PowerShell Event Log Filter" Consumer : CommandLineEventConsumer.Name="PowerShell Event Log Consumer" Filter : __EventFilter.Name="PowerShell Event Log Filter"
```

Event Consumer

```
\\.\ROOT\subscription: CommandLineEventConsumer.Name="PowerShell Event Log Consumer" CommandLineTemplate : C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe -NoP -NonI -EP ByPass -W Hidden -E <Base-64 encoded script>
```

GhostMiner will also install a WMI class named **"PowerShell_Command"** at the root\Default namespace. This WMI class contains the entries **Command** and **CCBot** that contains base-64 encoded functions.

When the **EventConsumer** is triggered, it will read entries from **Command** and **CCBot** from the installed WMI **"PowerShell_Command"** object.

The **Command** script, when executed, will do the following:

| Functions | Task |
|-----------------|--|
| WMI_KillFake | Terminates processes and deletes corresponding files based on a list of conditions |
| WMI_KillService | Terminates services based on a set of conditions |
| WMI_Scanner | Terminates processes of known cryptominers in the process memory |
| WMI_CheckFile | Verifies the integrity of the file it drops |

Table 1. List of functions the Command script performs once executed

Aside from the abovementioned functions, the Command script also has a **WMI_Killer** function, which terminates running processes, and deletes scheduled tasks and services that are associated with cryptocurrency-mining malware families such as:

1. MyKings
2. PowerGhost
3. PCASTLE
4. BULEHERO
5. Other generic MALXMR variants used by malware families, including BlackSquid

 Figure 1. List of service names that WMI_Killer terminates and deletes

Figure 1. List of service names that WMI_Killer terminates and deletes

 Figure 2. List of scheduled tasks that WMI_Killer deletes

Figure 2. List of scheduled tasks that WMI_Killer deletes

 Figure 3. List of cryptocurrency-mining-related processes that the the WMI_Killer terminate

Figure 3. List of cryptocurrency-mining-related processes that the the WMI_Killer terminates

WMI_Killer also terminates TCP traffic that uses a list of cryptocurrency-mining malware's commonly used ports

 Figure 4. List of ports that the WMI_Killer monitor

Figure 4. List of ports that the WMI_Killer monitors

Another Command script function, the **WMI_CheckHosts**, is able to modify the host files of the infected machine and modifies entries that are related to malicious malware such as BULEHERO..



Figure 5. WMI_CheckHosts function that modifies the infected machine's hosts files based on the mapped entries that are related to its competition

Meanwhile, the **CCBOT** entry uses two IP addresses, namely 118[.]24[.]63[.]208 and 103[.]105[.]59[.]68, as C&C servers. It uses Base-64 to encode the send command and ROT-13, a letter substitution cipher that changes the 13th letter after it, to decode the received command.

We observed that the backdoor communication is only enabled between 12AM to 5AM. It uses an invoke-expression (IEX) when the C&C server receives a response. Otherwise, it will continuously try to connect to the abovementioned IP addresses every 30 seconds using the **"/Update/CC/CC.php"** URI path.

Aside from **Command** and **CCBot**, The "PowerShell_Command" class also contains the following objects:

Miner : <Base-64 encoded binary code>

Ver : <Version Number> (The current version is v2.13.0)

mPid : <Process ID of the running cryptocurrency-miner>

nPid : <Process ID of the installer>

The miner is a 64-bit payload that is dropped when **Command** is decoded and executed. However, before it gets dropped, GhostMiner determines the free disk space on the root drive. If the free space is less than 1 GB, it will drop a 10 MB-sized payload. Otherwise, it will drop a 100 MB-sized payload. GhostMiner will then append 2,130 bytes of random value. The file will then be saved as **C:\Windows\Temp\lsass.exe**.

The malware will then execute the following commands as part of the miner's execution routine:

```
Takeown.exe /f C:\Windows\Temp
```

```
iCACLS.exe C:\Windows\Temp /Reset /T /C
```

```
iCACLS.exe C:\Windows\Temp /Grant Everyone:F /T /C
```

```
iCACLS.exe C:\Windows\Temp\lsass.exe /E /G Everyone:F /C
```

```
NetSH Firewall Add AllowedProgram C:\Windows\Temp\lsass.exe "Windows Update"
```

```
Start-Process -FilePath C:\Windows\Temp\lsass.exe -WindowStyle Hidden -PassThru
```

As of writing time, the XMR wallet associated with this campaign only has 50.278384965000 XMR (US\$3,868.02) in total paid value.

Trend Micro Deep Discovery Inspector protects customers from threats that may lead to C&C connection and data exfiltration via this DDI rule:

4219: GHOSTMINER - HTTP (Request)

Indicators of Compromise (IoCs)

| SHA-256 | Trend Micro Predictive Machine Learning Detection | Trend Micro Pattern I |
|--|---|-----------------------|
| 13a4751b83e53abdf0fb6d5876d6cc9dfbd33e343038dae6951de755d93c8284 | Troj.Win32.TRX.XXPE50FFF031 | Coinminer.Win64.MAL |
| 558914713cf3174c8b489aef12a1a7871ad886bc9483fd7b0790383702bfd75d | | |
| 7cec25bdb7c3cb2778168e9b02e0fdd608a6c94cb69feba7b4ee647aef0588b1 | | |
| 8ffa7f991637e28fa5b4ae7f5522fe5fee622307bed87d1d478c48fa0696dc5a | | |
| a0e0e5d0ff95e3193ed0999234588e3327ea8d759316a0d1175c5084daf5b083 | Coinminer.Win64.MALXMR.TIAOODC | |
| aa16c957a85ecedaac9f629082913dfdaefe95b8b8191d7cb3e8c02da2963452 | Coinminer.Win64.MALXMR.TIAOODBZ | |

Cyber Threats

We observed a fileless cryptocurrency-mining malware, dubbed GhostMiner, that weaponizes Windows management instrumentation (WMI) objects for its fileless persistence, payload mechanisms, and AV-evasion capabilities.

By: Carl Maverick Pascual September 19, 2019 Read time: (words)

Content added to Folio