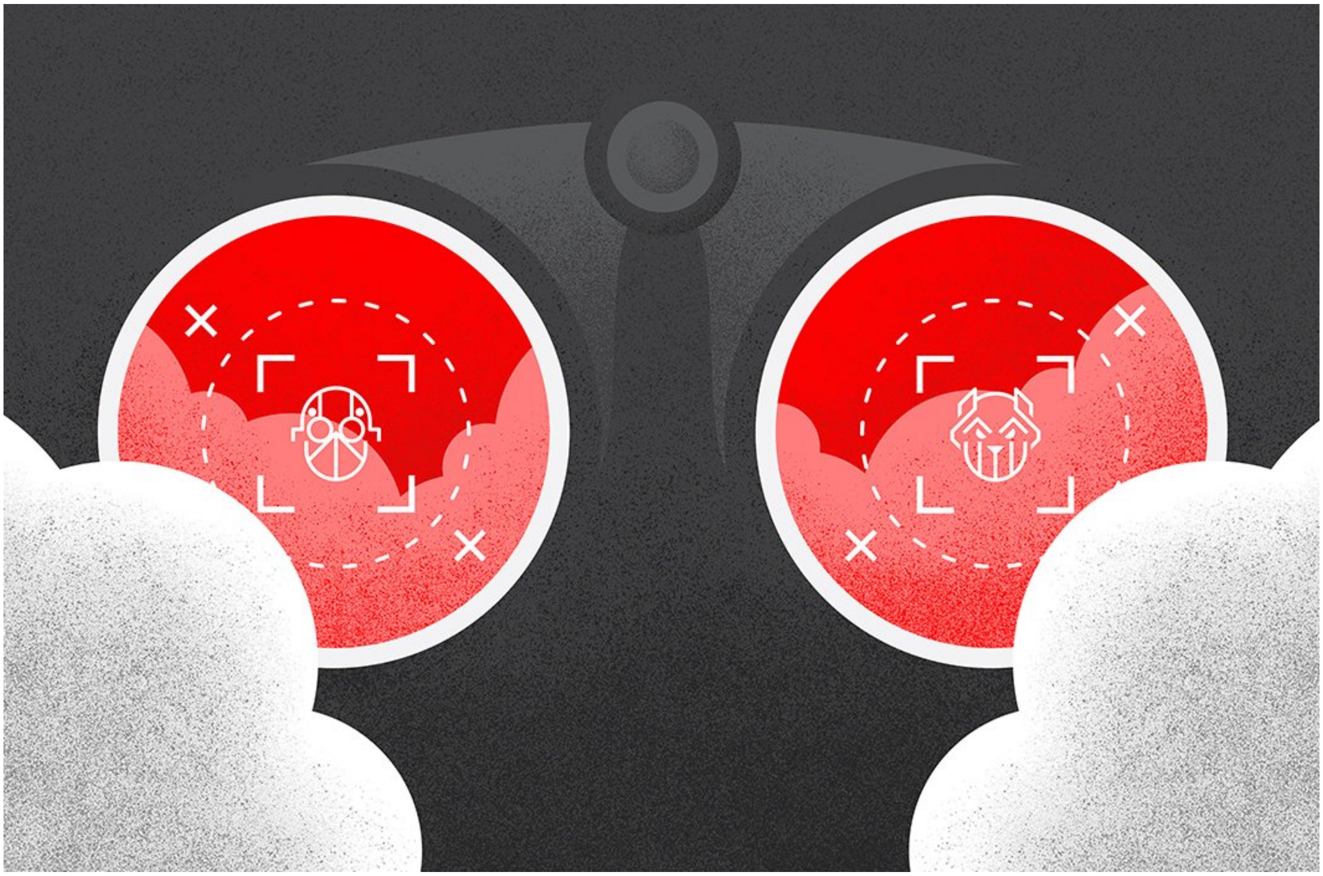
Falcon OverWatch Contributes to BlackCat Protection

crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/

Falcon OverWatch Team

March 23, 2022



In an effort to stay ahead of improvements in automated detections and preventions, adversary groups continually look to new tactics, techniques and procedures (TTPs), and new tooling to progress their mission objectives. One group — known as BlackCat/ALPHV — has taken the sophisticated approach of developing their tooling from the ground up, using newer, more secure languages like Rust and highly customized configuration options per victim.

While these techniques and tools may be sophisticated, the CrowdStrike Falcon® platform in combination with Falcon OverWatch™ proactive human-driven hunting proved effective in blocking and unraveling this novel threat. OverWatch gave the victim organization context-rich notifications about the emerging threat to their environment, providing essential information for this organization to secure themselves against a novel eCrime threat. OverWatch is continually hunting to unearth evolving TTPs used by big game hunting (BGH) ransomware adversaries and other highly impactful intrusions as highlighted in this recent unsuccessful ransomware attack.

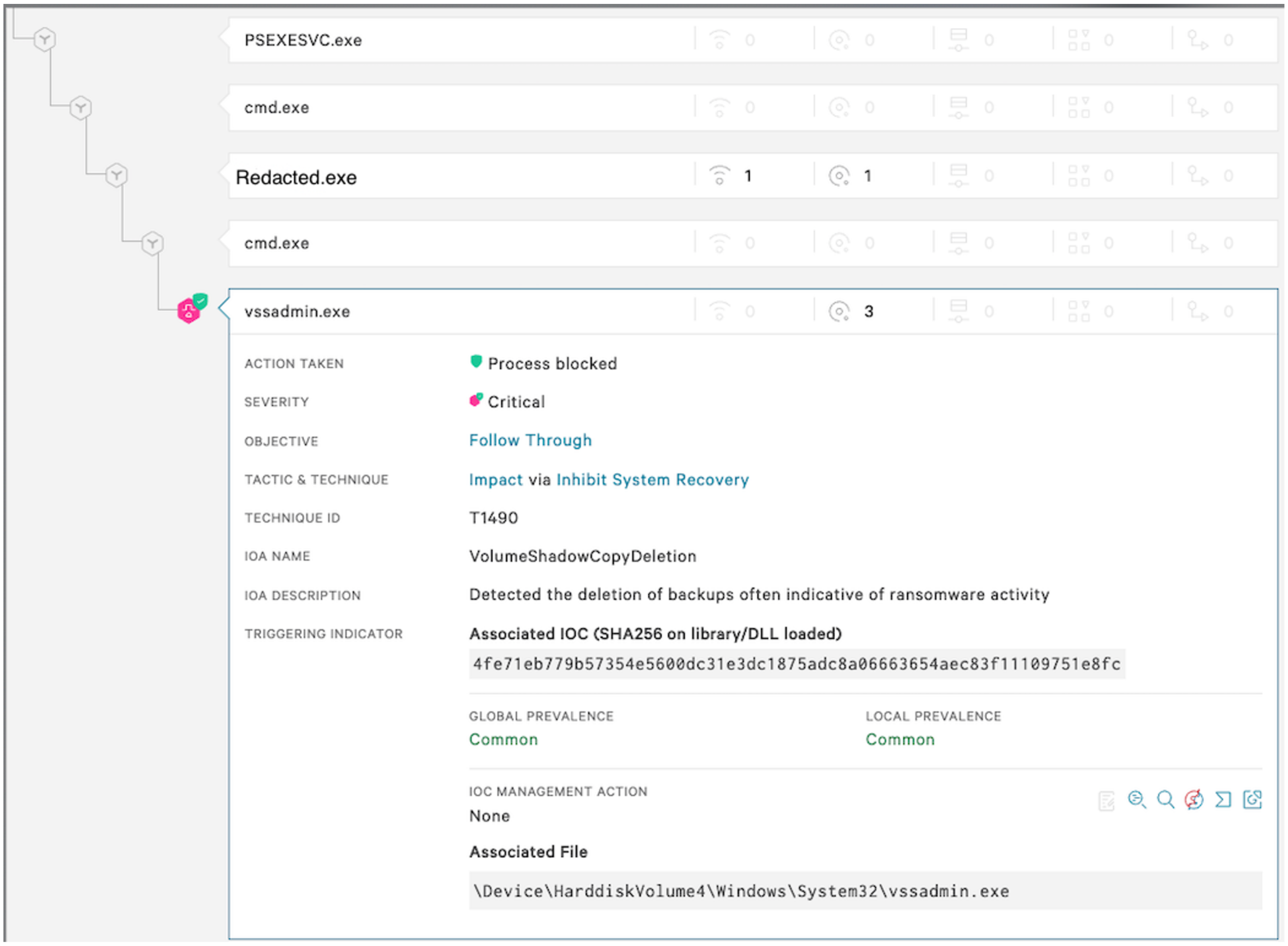
In late 2021, CrowdStrike Intelligence first became aware of BlackCat/ALPHV advertising to affiliates on underground forums. The group advertised a newly developed Rust-based ransomware-as-a-service (RaaS) offering, along with an enticing affiliate program that allows affiliates to retain a relatively generous 80% to 90% compared to the more typical 30% to 60%, depending on the RaaS and how successful it is.

By the end of January 2022, within weeks of launching, BlackCat/ALPHV had already gained notoriety for its expertise and aggressive approach to extorting victims. Extortion techniques used by BlackCat/ALPHV and affiliates include naming victims on a dedicated leak site (DLS), threatening to leak data on the DLS, encrypting data through ransomware, and finally implementing distributed denial of service (DDoS) attacks.

Good for Victim When BlackCat Crosses OverWatch’s Path

This blog details an unsuccessful BlackCat ransomware attack on an organization in the technology sector. OverWatch worked as a seamless extension of the Falcon platform to trace and track the adversary’s movements, providing critical context to the victim organization to facilitate comprehensive remediation.

Despite the adversary’s use of the novel BlackCat tooling, the Falcon sensor effectively blocked the attack, both preventing the deletion of volume shadow copies and the execution of the ransomware tool itself. Just as adversaries continuously evolve their approaches, the CrowdStrike Falcon® platform is continuously honed to detect and prevent emerging malicious activity. The Falcon platform takes a layered approach to detecting and preventing ransomware by using behavior-based indicators of attack (IOAs) and advanced machine learning (ML). Its detection capabilities are also informed by OverWatch’s front-line insights into novel threats.



PSEXESVC.exe 0 0 0 0 0

cmd.exe 0 0 0 0 0

Redacted.exe 1 1 0 0 0

cmd.exe 0 0 0 0 0

vssadmin.exe 0 3 0 0 0

ACTION TAKEN: Process blocked

SEVERITY: Critical

OBJECTIVE: Follow Through

TACTIC & TECHNIQUE: Impact via Inhibit System Recovery

TECHNIQUE ID: T1490

IOA NAME: VolumeShadowCopyDeletion

IOA DESCRIPTION: Detected the deletion of backups often indicative of ransomware activity

TRIGGERING INDICATOR: **Associated IOC (SHA256 on library/DLL loaded)**

```
4fe71eb779b57354e5600dc31e3dc1875adc8a06663654aec83f11109751e8fc
```

GLOBAL PREVALENCE: Common

LOCAL PREVALENCE: Common

IOC MANAGEMENT ACTION: None

Associated File

```
\Device\HarddiskVolume4\Windows\System32\vssadmin.exe
```

Figure 1. Falcon sensor detects and blocks critical severity attempt to delete volume shadow copies (Click to enlarge)

The Falcon platform’s detection and automated prevention of malicious activity sparked a rapid retrospective hunt to understand the threat to the victim’s environment, which revealed that the intrusion had stemmed from an unmanaged host. OverWatch is adept at finding adversary discovery activity or attempts to establish a persistent foothold in a victim’s environment. However, in this particular intrusion, the adversary gained initial access on a host that did not have the Falcon sensor installed, meaning that there was no visibility of this pre-ransomware activity for OverWatch. Despite this, OverWatch was still able to effectively track the adversary and provide the victim organization with a rapid context-rich notification about the activity underway in its environment before serious damage was done.

Upon investigation, OverWatch quickly uncovered the adversary’s use of “sender2” — identified as a file exfiltration tool (also known as Exmatter) — that was executed remotely with PsExec from an unmanaged host.

The sample sender2 executable crawls the computer for files with a list of file extensions and is configured to send them to a remote server via the SFTP or WebDAV protocols. In the activity observed by OverWatch, the tool was set to evade detection in the following ways:

- It executes using the parameter `-nownd`, causing the tool's window to be hidden during execution.
- At the completion of its execution, it launches a PowerShell command to forcibly stop the sender2 process and delete the executable.

Self-deletion powershell.exe command:

```
powershell.exe -WindowStyle Hidden -C $path = '\\[REDACTED]\123\sender.exe';Get-
Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr =
new-object byte[] 830483531;Set-Content -Path $path -Value $arr;Remove-Item -Path
$path;
```

Further analysis of the tool also revealed that the sample had a build time of approximately one hour before it was deployed, indicating that the adversary likely compiled the executable specifically for this intrusion.

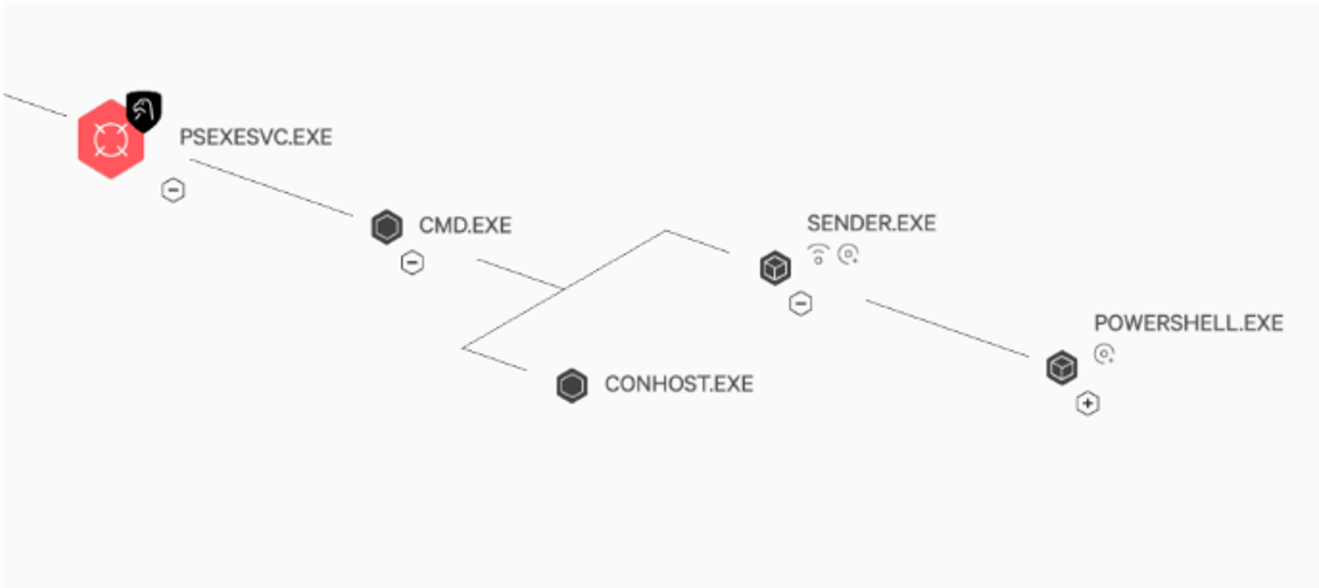


Figure 2. OverWatch detects malicious file exfiltration tool "sender2," executed under PsExecSvc.exe (Click to enlarge)

After the attempted data exfiltration, the adversary moved to deploy the BlackCat ransomware. The ransomware executable file was masquerading under the name of a legitimate third-party managed service security provider (MSSP). The ransomware was executed remotely under PsExec, from a network shared folder named `123` and was launched as a child process of Microsoft's File Explorer tool in another attempt to evade detection.

The ransomware executable included a required command line argument `--access-token=[access_token]`. This unique token is used to create the access key that is written into and appended to the `.onion` link of the ransomware `readme` file. This provides a unique link per victim to their negotiating Tor payment site.

Another distinctive characteristic of the BlackCat ransomware is its worming functionality with its ability to self-propagate within infected networks, observed in the following ways.

The ransomware:

- Acquires the system Address Resolution Protocol (ARP) table.
- Scans the network over NetBIOS TCP port 137. This service provides a legacy name service for name registration and resolution.
- Sets the maximum number of suggested network connections for client requests that can be maintained for each client of the server in the Windows registry.
- Modifies symbolic link evaluation of the host with Fsutil to support the encryption of symbolically linked files that redirect to a different file or directory, including connected network shares.

OverWatch also identified that the adversary had used the customer’s Microsoft Group Policy Object (GPO) settings to author scheduled tasks on Microsoft Windows domain joined hosts. The scheduled tasks were registered for sender2 and the ransomware. However, the files were not successfully executed using this method.

Scheduled Task for “sender2”:

```
TaskAuthor: [REDACTED]
TaskExecArguments: -nownd
TaskExecCommand:  "cmd" /c \\[REDACTED]\\123\sender.exe
TaskName: test2
```

Scheduled Task for the Ransomware:

```
TaskAuthor: [REDACTED]
TaskExecArguments: --access-token
TaskExecCommand: "cmd" /c \\[REDACTED]\\123\[REDACTED].exe --access-token [REDACTED]
TaskName: test123
```

While the attack stemmed from a host that did not have the Falcon sensor installed, OverWatch was able to use the cloud telemetry emitted from endpoints that did have Falcon sensor coverage to uncover the scope of this intrusion. OverWatch used the available telemetry to identify the source of the machine spreading the infection and was also able to identify and quickly notify the victim about the attack, which included:

- When the activity began
- The compromised user account used to conduct the malicious activity
- The unmanaged host used in the attack vectors, including relevant network indicators
- The ransomware strain and the configured file rename extension
- Files, hashes and indicators on impacted hosts
- Guidance to prevent further activity and assist with the initial response

Human-Driven Threat Hunting Seamlessly Augments Automated Detection and Prevention

This intrusion is a clear illustration of how OverWatch’s human threat hunting augments automated security controls to pinpoint and rapidly communicate malicious activities at the earliest possible stage.

The Falcon sensor played a crucial role in containing this attack. The Falcon sensor successfully detected and blocked attempts to delete volume shadow copies and deploy ransomware. These preventions gave the victim organization time to take the correct action stemming from OverWatch’s findings and evict the adversary from their network.

OverWatch’s immediate investigation uncovered crucial details about the scope of the adversary’s activity, even when dealing with unmanaged endpoints. This information was crucial to the victim organization, enabling their response efforts to eradicate the adversary from their environment.

It is essential for defenders to recognize that, although OverWatch was ultimately able to track this intrusion as it traversed the victim’s network, full visibility would have enabled much quicker identification of this activity and potentially could have prevented the adversary from gaining initial access. OverWatch strongly recommends that full endpoint protection — including next-generation antivirus (NGAV) and endpoint detection and response (EDR) — is deployed across all endpoints to ensure complete visibility. While it is impossible to anticipate where an adversary will gain access, it is likely that they will look for blind spots in order to operate undetected within your environment.

TABLE 1. Ransomware Execution

```
"cmd" /c \\[REDACTED]\\123\[REDACTED].exe --access-token <redacted>
```

NOTE: Ransomware binary execution under PSEXECSVC.exe

```
"C:\Windows\system32\cmd.exe" /c "wmic csproduct get UUID"
```

NOTE: Acquire the System Management BIOS UUID, likely to gather information.

```
"C:\Windows\system32\cmd.exe" /c "fsutil behavior set SymlinkEvaluation R2L:1"
```

NOTE: Enable remote-to-local symlink evaluation

```
"C:\Windows\system32\cmd.exe" /c "fsutil behavior set SymlinkEvaluation R2R:1"
```

NOTE: Enable remote-to-remote symlink evaluation

```
"C:\Windows\system32\cmd.exe" /c "iisreset.exe /stop"
```

NOTE: Stop all IIS-related processes

```
"C:\Windows\system32\cmd.exe" /c "reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
/v MaxMpxCt /d 65535 /t REG_DWORD /f"
```

NOTE: Set the maximum suggested outstanding network connections

```
"C:\Windows\explorer.exe" --child --access-token [REDACTED]
```

NOTE: Run the ransomware executable as a child process

```
"C:\Windows\system32\cmd.exe" /c "arp -a"
```

NOTE: Acquire system ARP table

```
"C:\Windows\system32\cmd.exe" /c "vssadmin.exe Delete Shadows /all /quiet"
```

NOTE: Delete file shadow copies

TABLE 2. sender2 File Exfiltrator Execution

The file exfiltrator tool, sender2, will crawl the computer for files with the following extensions:

```
.doc, .docx, .xls, .xlsx, .xlsm, .pdf, .msg, .ppt, .pptx, .sda, .sdm,
.sdw, .csv, .zip, .json, .config, .ts, .cs, .sqlite, .aspx, .pst, .rdp,
.accdb, .catpart, .catproduct, .catdrawing, .3ds, .dwt, .dxf
```

It also has a few exceptions configured; it will not crawl any of the following directories:

```
C:\Documents and Settings
C:\PerfLogs
C:\Program Files\Windows Defender Advanced Threat Protection
C:\Program Files\WindowsApps
C:\ProgramData\Application Data
C:\ProgramData\Desktop
C:\ProgramData\Documents
C:\ProgramData\Microsoft
C:\ProgramData\Packages
C:\ProgramData\Start Menu
C:\ProgramData\Templates
C:\ProgramData\WindowsHolographicDevices
C:\Recovery
C:\System Volume Information
C:\Users\All Users
C:\Users\Default
C:\Users\Public\Documents
C:\Windows
```

System Volume Information

And it will also skip every path that contains one of the following strings:

```
OneDriveMedTile
locale-
SmallLogo
VisualElements
adobe_sign
Adobe Sign
core_icons
```

Additional Resources

- *Read the 2021 Threat Hunting Report blog or download the report now.*
- *Learn more about Falcon OverWatch's proactive managed threat hunting.*
- *Discover the power of tailored threat hunting OverWatch Elite provides customers in this blog post.*
- *Watch how Falcon OverWatch proactively hunts for threats in your environment.*
- *Read more about how part-time threat hunting is simply not enough in this blog post.*
- *Learn more about the CrowdStrike Falcon® platform.*