How Falcon OverWatch Detected SILENT CHOLLIMA's Custom Tooling

crowdstrike.com/blog/how-falcon-overwatch-detected-silent-chollima-custom-tooling/

Falcon OverWatch Team

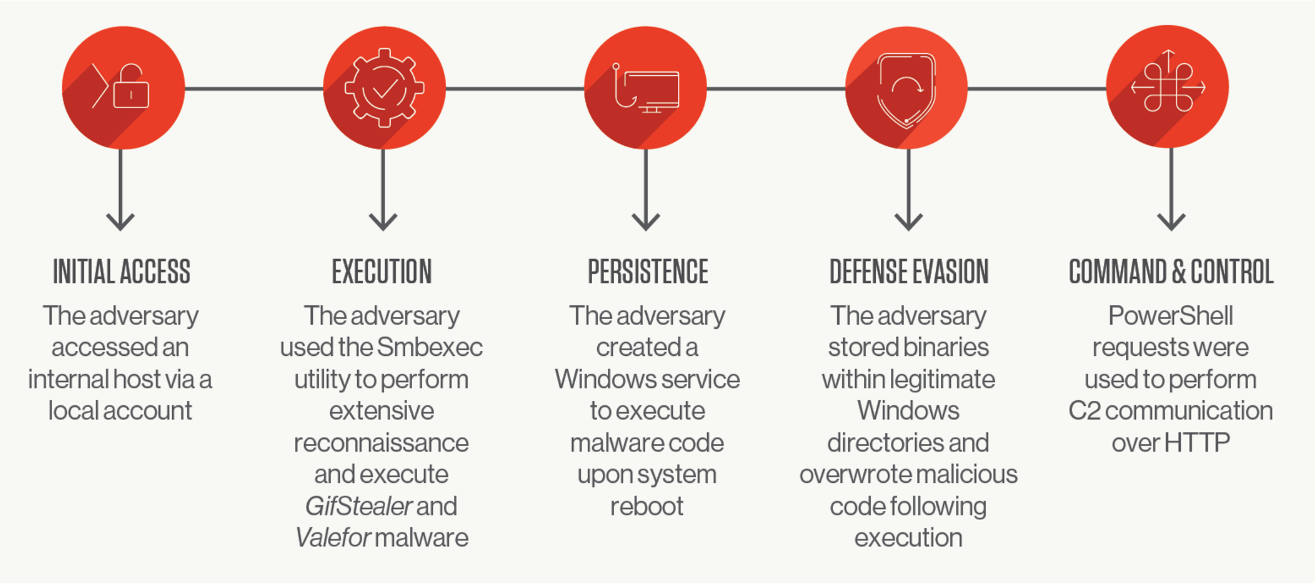
November 29, 2021

CrowdStrike Falcon OverWatch™ recently released its annual threat hunting report, detailing the interactive intrusion activity observed by hunters over the course of the past year. The tactics, techniques and procedures (TTPs) an adversary uses serve as key indicators to threat hunters of who might be behind an intrusion. OverWatch threat hunters uncovered an intrusion against a pharmaceuticals organization that bore all of the hallmarks of one of the Democratic People's Republic of Korea (DPRK) threat actor group: SILENT CHOLLIMA. For further detail, download the CrowdStrike 2021 Threat Hunting Report today.

Threat Hunters Uncover SILENT CHOLLIMA's Custom Tooling

OverWatch threat hunters detected a burst of suspicious reconnaissance activity in which the threat actor used the Smbexec tool under a Windows service account. Originally designed as a penetration testing tool, Smbexec enables covert execution by creating a Windows service that is then used to redirect a command shell operation to a remote location over Server

Message Block (SMB) protocol. This approach is valuable to threat actors, as they can perform command execution under a semi-interactive shell and run commands remotely, ultimately making the activity less likely to trigger automated detections.



INITIAL ACCESS

The adversary accessed an internal host via a local account

EXECUTION

The adversary used the Smbexec utility to perform extensive reconnaissance and execute *GifStealer* and *Valefor* malware

PERSISTENCE

The adversary created a Windows service to execute malware code upon system reboot

DEFENSE EVASION

The adversary stored binaries within legitimate Windows directories and overwrote malicious code following execution

COMMAND & CONTROL

PowerShell requests were used to perform C2 communication over HTTP

As OverWatch continued to investigate the reconnaissance activity, the threat actor used Smbexec to remotely copy low-prevalence executables to disk and execute them. The threat hunters quickly called on CrowdStrike Intelligence, who together were able to quickly determine the files were an updated variant of Export Control — a malware dropper unique to SILENT CHOLLIMA.

SILENT CHOLLIMA then proceeded to load two further custom tools. The first was an information stealer, named GifStealer, which runs a variety of host and network reconnaissance commands and archives the output within individual compressed files. The second was Valefor, a remote access tool (RAT) that uses Windows API functions and utilities to enable file transfer and data collection capabilities.

OverWatch Contains Adversary Activity

Throughout the investigation, OverWatch threat hunters alerted the victim organization to the malicious activity occurring in the environment. As the situation developed, OverWatch continued to alert the organization, eventually informing them of the emerging attribution of this activity to SILENT CHOLLIMA.

Because this activity originated from a host without the CrowdStrike Falcon® sensor, OverWatch next worked with the organization to expand the rollout of the Falcon sensor so the full scope of threat actor activity could be assessed. Increasing the organization's coverage and visibility into the intrusion, threat hunters identified six additional compromised hosts. Through further collaboration with the organization, OverWatch was able to relay their findings in a timely manner, empowering the organization to contain and remove SILENT CHOLLIMA from their network.

OverWatch discovered a service creation event that was configured to execute the Export Control loader every time the system reboots, allowing the threat actor to maintain persistence if they temporarily lose connection.

```
sc create [REDACTED] type= own type= interact start= auto error=ignore binpath= "cmd
/K start C:\Windows\Resources\[REDACTED].exe"
```

The threat actor was also mindful to evade detection by storing their Export Control droppers and archived reconnaissance data within legitimate local directories. By doing this, threat actors attempt to masquerade the files as benign activity. The threat actor continued its evasion techniques, removing traces of the collected GifStealer archives by deleting them and overwriting the GifStealer binary itself using the string below. This technique is another hallmark of SILENT CHOLLIMA activity.

```
"C:\Windows\system32\cmd.exe" /c ping -n 3 127.0.0.1 >NUL & echo EEEE >
"C:\Windows\Temp\[REDACTED]"
```

Conclusions and Recommendations

The OverWatch team exposed multiple signs of malicious tradecraft in the early stages of this intrusion, which proved to be vital to the victim organization’s ability to successfully contain the campaign and remove the threat actor from its networks. In this instance, OverWatch worked with the organization to rapidly expand Falcon sensor coverage. Though the Falcon sensor can be deployed and operational in just seconds, OverWatch strongly recommends that defenders roll out endpoint protection consistently and comprehensively across their environment from the start to ensure maximum coverage and visibility for threat hunters. OverWatch routinely sees security blind spots become a safe haven from which adversaries can launch their intrusions. The Falcon sensor was built with scalability in mind, allowing an organization to reach a strong security posture by protecting all enterprise endpoints in mere moments.

The expertise of OverWatch’s human threat hunters was pivotal in this instance, as it was the threat hunters ability to leverage their expertise that allowed them to discern the SMB activity was indeed malicious.

For defenders concerned about this type of activity, OverWatch recommends monitoring:

- Service account activity, limiting access where possible
- Service creation events within Windows event logs to hunt for malicious SMB commands

- Remote users connecting to administrator shares, as well as other commands and tools that can be used to connect to network shares

Ultimately, threat hunting is a full time job. Defenders should also consider hiring a professional managed threat hunting service, like OverWatch, to secure their networks 24/7/365.

Additional Resources

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