How Falcon Complete Stopped a SolarWinds Serv-U Exploit Campaign

crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/

Alex Clinton - Tasha Robinson October 21, 2021

This blog describes how the CrowdStrike Falcon Complete™ team quickly responded to a recent campaign involving the SolarWinds Serv-U product exploitation. SolarWinds issued a public notice of the vulnerability in July 2021 along with releasing a hotfix to mitigate the exploit. The National Vulnerability Database has more details, found here: CVE-2021-35211.

The Falcon Complete team identified active implants at multiple customers and neutralized the threat by performing network containment of the affected systems, preventing any further lateral movement or follow-on activity. Investigation revealed that the threat actor attempted to deploy additional tooling, which likely indicated preparation for ransomware. One of the unique artifacts about this campaign is the multi-stage Component Object Model (COM) persistence mechanism used, allowing an attacker to execute arbitrary code on behalf of a trusted process. Although machine-based detections are highly effective at uncovering intrusion activity, today's sophisticated adversaries can fly under the radar by abusing trusted processes to gain access to an environment, underscoring the need for human expertise in tracking and neutralizing threats.

The events outlined in this blog have been attributed to the GRACEFUL SPIDER adversary group by CrowdStrike Intelligence. GRACEFUL SPIDER is suspected to be operating out of Eastern Europe and Russia. They have typically been seen targeting companies in a variety of sectors across the world. The common monetization techniques are requiring ransom payments through cryptocurrency, extorting stolen data if the ransom is not paid, engaging in monetary theft through wire fraud from victim accounts, and likely selling payment card data via criminal marketplaces.

The Initial Detection

Early in the adversary's post-exploitation activity, a CrowdStrike Falcon® detection was triggered on an MFT server for execution of a reverse shell with a parent process of WINLOGON.EXE. Analysis of the SYSINFO.EXE binary indicated that TinyMet, which is an open-source Meterpreter-based reverse shell, was used to provide the attackers with access to the target host. In addition, network telemetry from both of these processes indicated they were attempting to communicate with suspicious IPs.

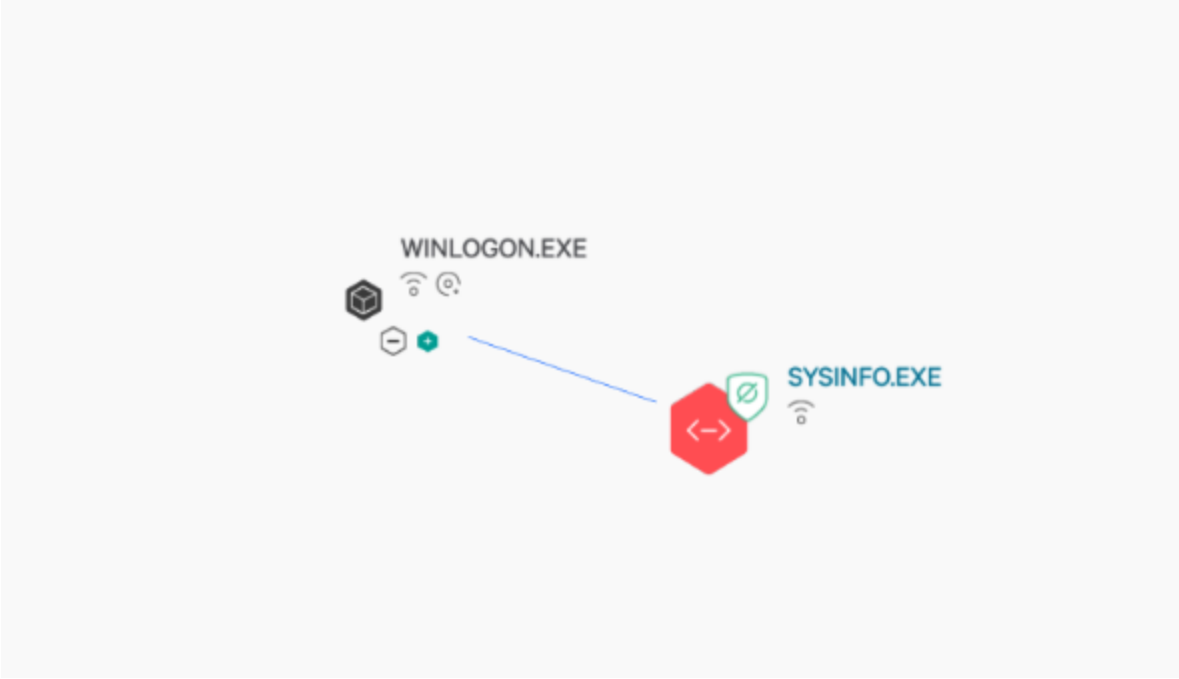

Figure 1. TinyMet shell execution

Soon after, another detection was triggered for encoded PowerShell execution with a parent process of SVCHOST.EXE. Decoding this PowerShell confirmed that it was malicious as it used randomly named variables and attempted to execute content pulled from a registry key, both of which would be highly abnormal for a legitimate script.

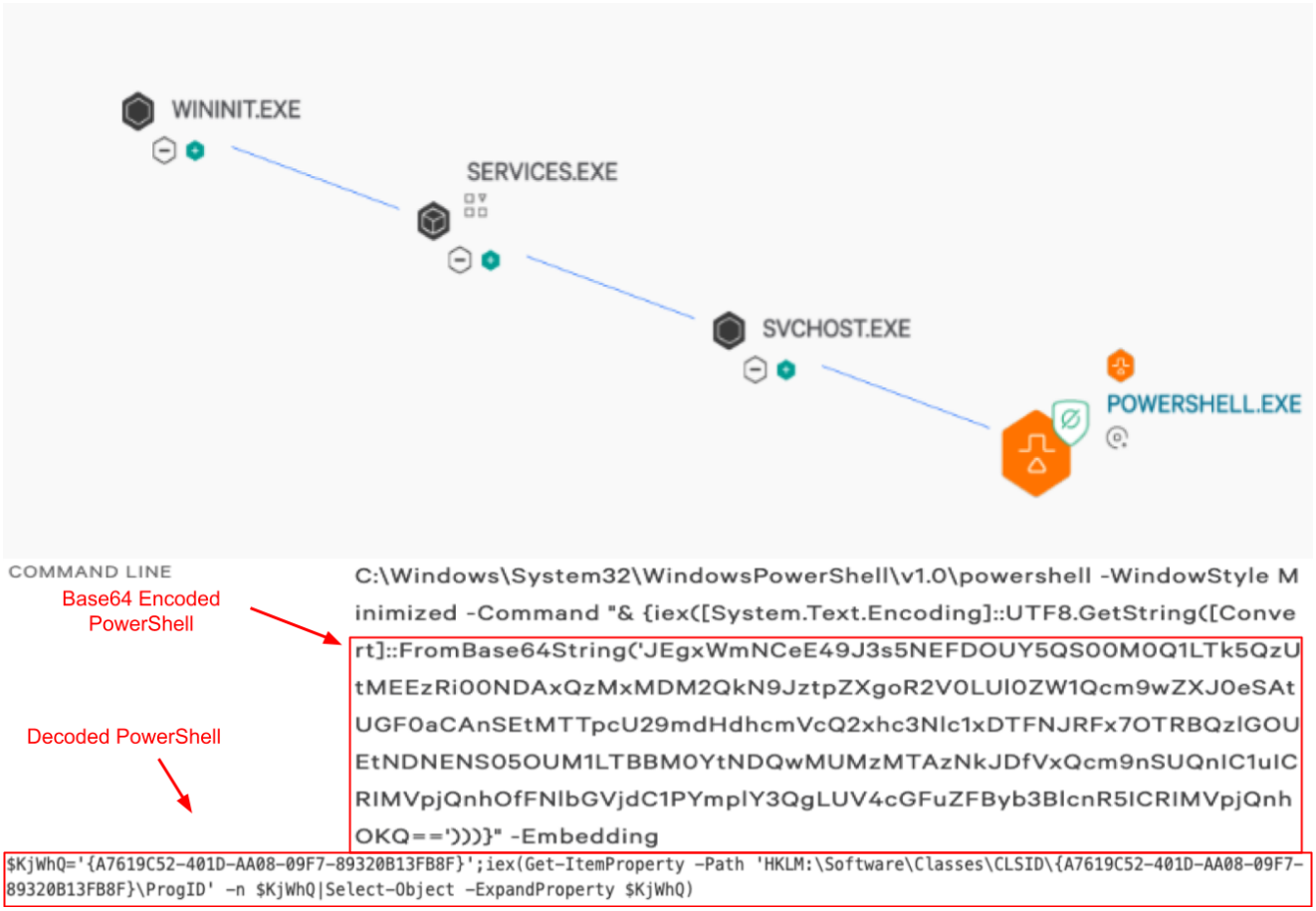

Figure 2. Encoded PowerShell execution

Both of these actions were prevented by Falcon, but the active connections to suspicious infrastructure and execution of a malicious PowerShell script, without an obvious source for either, indicated there was an unresolved threat on the device. The host was immediately network-contained and isolated to prevent further actions on the objective, while Falcon Complete continued its investigation to ascertain the source of the threat.

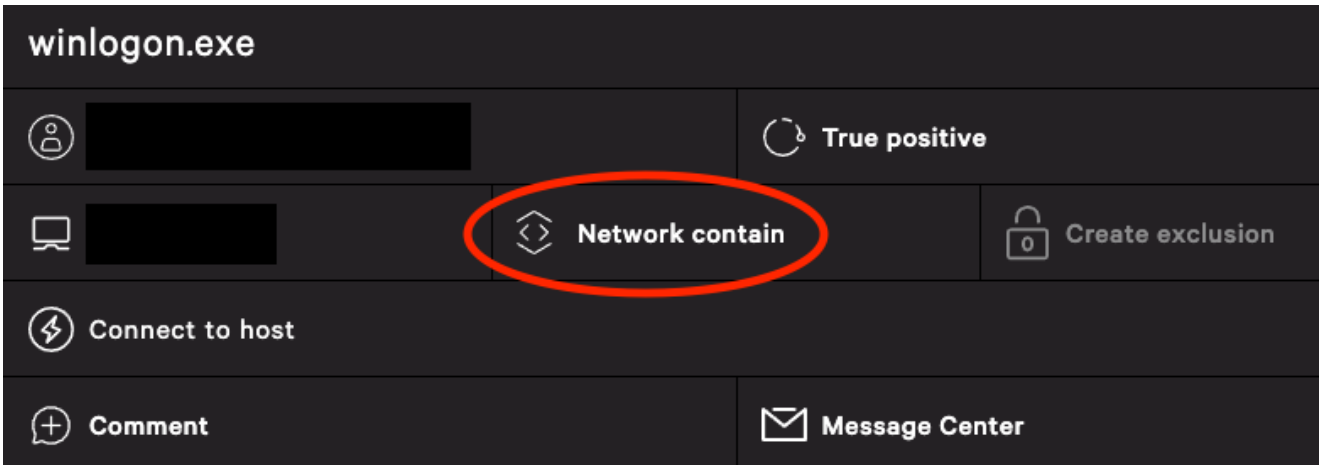

Figure 3. Network Containment

The malicious activity being executed by legitimate Windows processes as well as the SYSTEM user account indicated that the host may have been compromised by a public-facing exploit and not another attack vector such as a user-level phish. In addition, as a portion of the suspicious activity was originating from legitimate WINLOGON.EXE processes, there was a high likelihood of process injection.

From here, the Falcon Complete team pivoted the investigation into endpoint activity monitoring (EAM) data to gain further context and determine the origin of the activity.

Investigation with Endpoint Detection and Response Data

Once Falcon Complete reviewed the detection information at hand and confirmed that the activity noted was malicious, the next step was to identify the full scope of the threat. This is where Falcon Complete's knowledge and skill set come into play.

Let's take a step back and outline what occurred.

Finding the Foothold

In order to prevent further malicious activity, the Falcon Complete team needs to identify how the threat actor managed to gain a foothold on the host.

Based on the data reviewed thus far, the team suspected that the adversary may have gained access to this host through exploitation of a public-facing service. By viewing the running processes on the device, Falcon Complete was able to see that it hosted a SolarWinds Serv-U FTP server. Searching through various sources for the hash of the associated process provided the version number of the software.

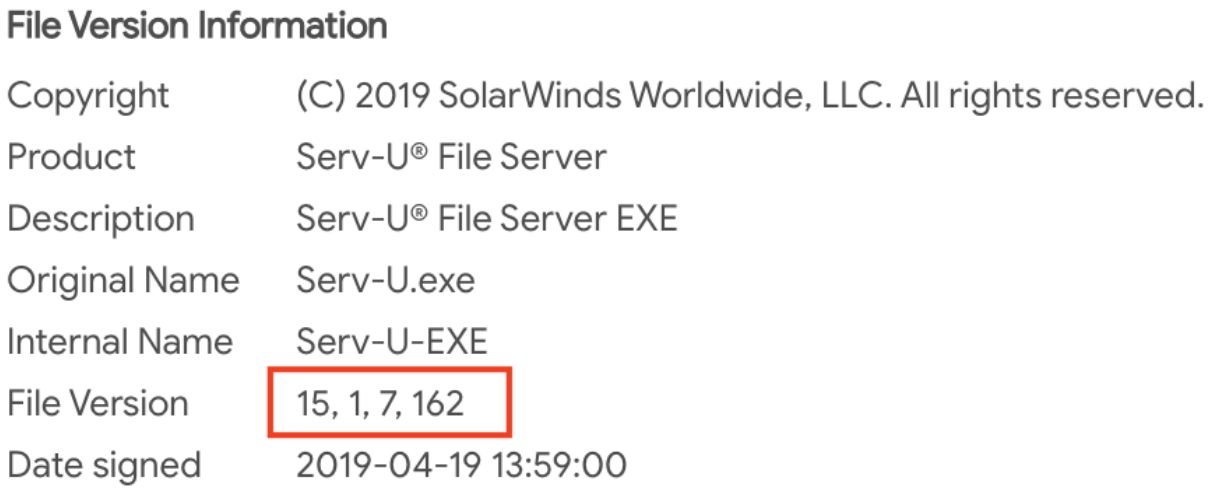

Figure 4. SolarWinds Serv-U Version Information

A quick search for this version confirmed that there are multiple known exploits including CVE-2021-35211, for which a CISA advisory had recently been released.

Our starting point in this investigation was the malicious usage of the legitimate WINLOGON.EXE process. This process is often used by threat actors hoping to achieve further stealth via process injection. The following EAM search was used to identify process injection attempts on the host.

```
(event_simpleName=*Reflective* OR DetectName=*Reflective* AND
ReflectiveDllName!=NULL) OR (event_simpleName=*Inject* OR event_simpleName=*inject*)
| table _time aid event_simpleName ComputerName InjectorImageFileName
InjecteeImageFileName  Reflective* Injected* CallStackModuleNames SourceThreadModule
TargetThreadModule ParentProcessId_decimal TargetProcessId_decimal
ContextProcessId_decimal
```

event_simpleName	ComputerName	InjectorImageFileName	InjecteeImageFileName
ProcessInjection	[redacted]	\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\System32\winlogon.exe
InjectedThread			
InjectedThread			
ProcessInjection		\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\explorer.exe
InjectedThread			
ProcessInjection		\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\explorer.exe
InjectedThread			
ProcessInjection		\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\System32\winlogon.exe
ProcessInjection		\Device\HarddiskVolume1\Program Files\RhinoSoft\Serv-U\Serv-U.exe	\Device\HarddiskVolume1\Windows\System32\lsass.exe

Figure 5. Process injection chain (Click to enlarge)

Based on the information in Figure 5, we are able to see that Serv-U.exe was the initial source of the injection into lsass.exe, followed by lsass.exe injection into winlogon.exe. Lsass.exe was also used to perform injection into explorer.exe. This injection chain confirmed that Serv-U was the source of the infection. In addition, utilizing Falcon's Process Timeline dashboard, the IP performing the initial exploitation could be identified.

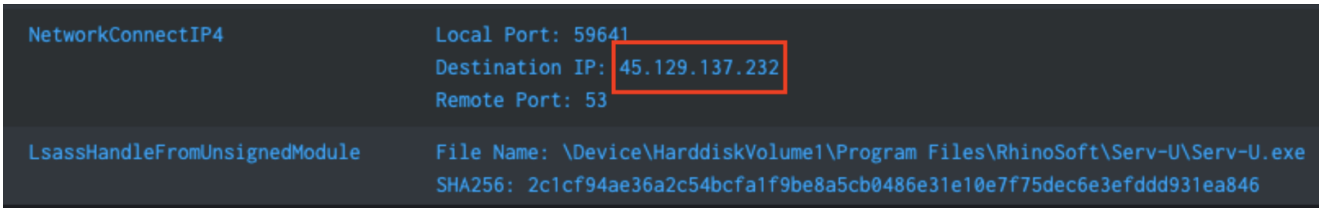

Figure 6. Falcon Process Timeline: Serv-U

Finally, by reviewing the Process Timeline for each of the injected processes during the relevant times, we are able to see that the adversary attempted to deploy additional tooling including the previously identified TinyMet shell, a Cobalt Strike beacon (which was prevented by Falcon), and a copy of AdFind. Tools like TinyMet and Cobalt Strike are often used by eCrime groups, including GRACEFUL SPIDER, to sell or transition access to an environment. These remote access tools (RATs) along with AdFind (generally used for enumeration of the environment) will often indicate the initial steps taken by a threat actor before the deployment of ransomware. The increase in ransomware broker networks highlights the necessity for quick action when detections are triggered on a host.

Persistence

When any compromise is identified, Falcon Complete will always ensure the host and the customer environment is brought to a clean state before resolution of the incident. The next stage was to identify any mechanisms the threat actor had used to keep their foothold on the host. Although a variety of persistence mechanisms was reviewed, an investigation of scheduled tasks on the host quickly revealed a multi-stage execution chain utilizing COM registry objects.

Although the source of the infection was identified, the host still had multiple detections triggered for Base64-encoded PowerShell execution unrelated to WinLogon. This indicated that the threat actor had likely established a persistence mechanism on the host, potentially using a scheduled task due to the frequency of incoming detections.

A search for recently registered scheduled tasks on the host revealed a single task that pointed to a COM object within the Windows registry.

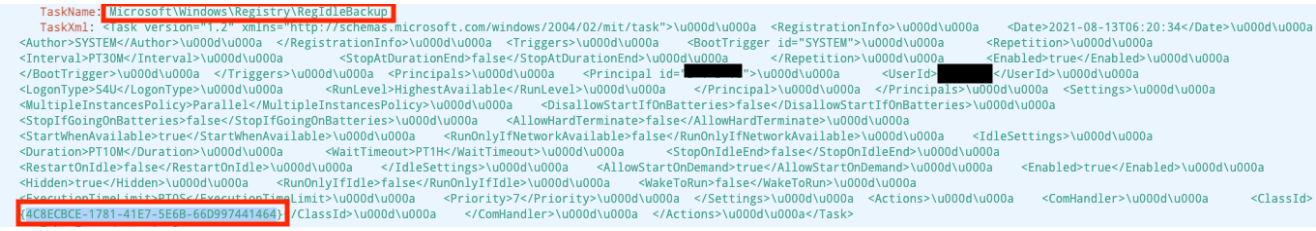

Figure 7. Scheduled task registration (Click to enlarge)

This scheduled task is a known default scheduled task that appears on many Windows hosts, making it an easy target for the threat actor to target and point it to their malicious COM object. COM objects within the Windows registry are effective locations to hide malware, as they will allow for some forms of auto-execution without being in an obvious location. This feature is used legitimately by a variety of software on Windows, but in this case it was hijacked for malicious code execution.

At this point, Falcon Complete was able to pivot to Falcon Real Time Response (RTR) on the host for further analysis. RTR provides analysts with a shell on the host to quickly validate and complement data found within EAM. In addition, once investigation is complete, RTR can be used to perform remediation of malicious artifacts on the host. A review of this COM object using RTR identified a TreatAs key pointing to a second COM object registry key.

```
C:\> reg query 'HKLM:\Software\Classes\CLSID\{4C8ECBCE-1781-41E7-5E6B-66D997441464}\'
Subkeys of HKLM:\Software\Classes\CLSID\{4C8ECBCE-1781-41E7-5E6B-66D997441464}\ :

SubKeyName SubKeyCount ValueCount
---------- ----------- ----------
TreatAs              0          1



C:\> reg query 'HKLM:\Software\Classes\CLSID\{4C8ECBCE-1781-41E7-5E6B-66D997441464}\TreatAs'
Properties of (HKLM:\Software\Classes\CLSID\{4C8ECBCE-1781-41E7-5E6B-66D997441464}\TreatAs) :

Property                                                                          Type Value
--------                                                                          ---- -----
(default)                                                                        String {2BF05F19-8356-2699-CABC-18BE40D06A03}

C:\>
```

Figure 8. Malicious COM object (Click to enlarge)

A review of the second registry key revealed the Base64-encoded PowerShell that had been attempting to execute, as shown in Figure 2. Decoding this revealed a PowerShell command to pull the contents of a third COM-based registry key and execute it.

The script found within the third key was encoded and lightly obfuscated with unused code. When decoded and deobfuscated, we were able to confirm that the script would clear the host's EventLog, but its primary function was to load a DLL into memory, which was located within a fourth registry key.

```
13    Get-EventLog -LogName *|ForEach{Clear-EventLog $_.Log};
8     $aul1=Get-ItemProperty -Path 'HKLM:\Software\Classes\CLSID\{2BF05F19-8356-2699-CABC-18BE40D06A03}\VersionIndependentProgID' -n $HhIKu0|s
9     $bd31Xw3H=[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((UdEV1a 'VirtualAllocEx'),(aYIvGc4 @([IntPtr],[IntPtr]
```

Figure 9. Malicious PowerShell snippet

Analysis of the DLL by the CrowdStrike Intelligence team confirmed that it located the payload at a fifth and final registry key calculated using the hostname and drive serial number. The malware loaded from this location was a RAT unique to GRACEFUL SPIDER called FlawedGrace.

This persistence chain was relatively stealthy, as it kept the malicious content largely in memory, except for additional tooling deployed.

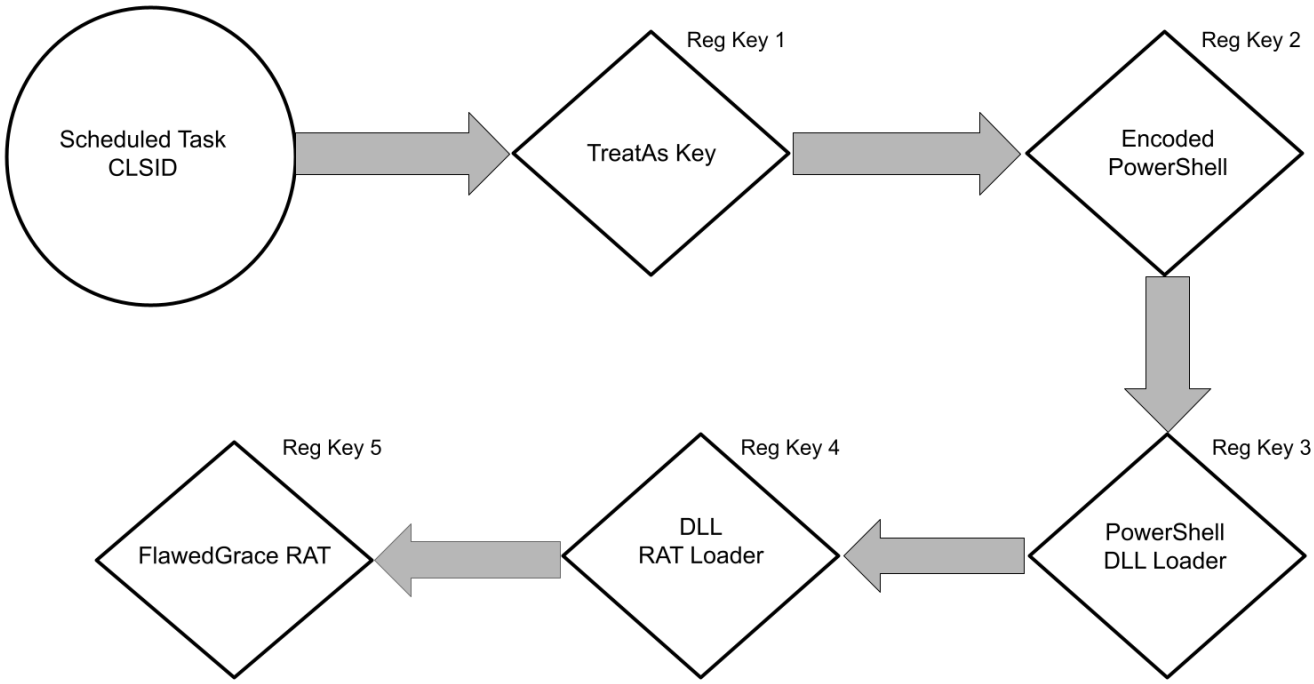

Figure 10. Persistence chain

Analysis of this persistence mechanism by the Falcon Complete team, as well as partnership with the CrowdStrike Falcon OverWatch™ and CrowdStrike Intelligence teams, allowed for quick attribution of this incident to GRACEFUL SPIDER, as well as identification of malicious artifacts at affected customers.

The Remediation

Once triage and investigation reached a conclusion, the Falcon Complete team remediated the host of any malicious artifacts associated with this incident. This includes all persistence mechanisms, which in this case were the elusive COM registry objects:

```
HKLM\Software\Classes\CLSID\(unique ID_1)\TreatAs
HKLM\Software\Classes\CLSID\(unique ID_2)\LocalServer
HKLM\Software\Classes\CLSID\(unique ID_2)\ProgID
HKLM\Software\Classes\CLSID\(unique ID_2)\VersionIndependentProgID
```

The additional tooling identified in EAM (TinyMet shell and AdFind) was ultimately blocked and then quarantined by the Falcon sensor. They were not found on disk and did not require any additional action to remediate. As part of the investigation, the team identified multiple injected processes on the host. In order to completely clean the system and prevent reinfection, these processes were terminated, including the original source, Serv-U.exe.

Along with Falcon Complete's remediation summary, the affected customers were provided with all indicators of compromise and a list of all available patches applicable to the system to prevent any further exploitation in the future. Falcon Complete recommended blocking the

associated IPs at the perimeter, resetting passwords for all user accounts on the affected systems (due to the compromise of LSASS), and applying all available patches as soon as possible. The customers promptly performed these actions in order to prevent the possibility of data exfiltration and ransomware deployment.

Associated C2 Activity

```
46.161.40[.]87 - Injected WinLogon
179.60.150[.]26 - TinyMetShell C2
179.60.150[.]32 - Cobalt Strike C2
45.129.137[.]232 - remote IP contacted by exploited Serv-U.exe process
```

Conclusion

Falcon Complete identified an active campaign on public-facing Serv-U MFT servers, contained the activity and prevented the attacker from completing their actions on objectives. The team leveraged EAM, the Falcon Process Timeline dashboard, Falcon RTR, and some open-source intelligence (OSINT) to quickly shut down this attempted breach in real time.

In addition to removing the associated artifacts, Falcon Complete identified the vulnerable application being exploited early on and was able to quickly provide all affected customers with the critical, time-sensitive information they needed to patch their vulnerable public-facing MFT servers, secure their business from further attacks and check other servers for vulnerabilities.

In rare cases where the hosts were not patched in a timely fashion, GRACEFUL SPIDER has been known to return for further attempts to deliver Cobalt Strike beacons. These attempts were quickly blocked by the Falcon agent. Campaigns such as these illustrate the persistence and stealth tactics that can be employed by an adversary like GRACEFUL SPIDER to gain and keep a foothold in target organizations. Fortunately, Falcon provides the telemetry and tools to quickly identify, investigate and remediate attacks that remain largely in memory, such as this one.

The Falcon Complete team works closely with the Falcon OverWatch and CrowdStrike Intelligence teams, applying vast skill sets to enable organizations to investigate and identify threat groups quickly — and fueling our mission to stop breaches.

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.*
- *Read about adversaries tracked by CrowdStrike in 2020 in the 2021 CrowdStrike Global Threat Report.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™.*