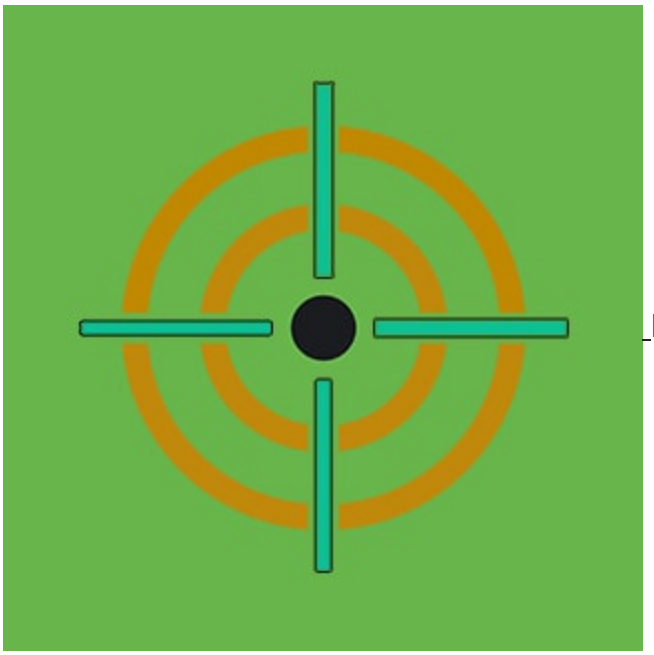
Cloud Federated Credential Abuse & Cobalt Strike: Threat Research February 2021

splunk.com/en_us/blog/security/cloud-federated-credential-abuse-cobalt-strike-threat-research-feb-2021.html

March 9, 2021

SECURITY



By Splunk Threat Research Team March 09, 2021

This month, the Splunk Threat Research team developed a total of seven analytic stories addressing different types of threats and more than a dozen of new detections to help our customers detect and fight against these threats.

In this blog post, we'll walk you through two analytic stories and a few detection searches that we want to highlight from the February 2021 releases. Watch the video below to learn more about why Splunk's Rod Soto, Principal Security Research Engineer, and Michael Haag, Senior Threat Researcher, think it is important to share their knowledge on emerging threats such as Cloud Federated Credential Abuse and Cobalt Strike.

Cloud Federated Credential Abuse

The Cloud Federated Credential Abuse analytic story addresses the recently notorious campaigns featuring tactics, techniques and procedures (TTPs) that target the extraction of credentials in cloud federated environments. These environments are composed by federation-enabling technologies such as Active Directory Federation Services, and these federations can be from inside the perimeter or between cloud vendors.

Federations are based in the flow of trusted credentials. These trusted credentials allow the seamless interaction of entities from perimeter to cloud or from cloud to cloud. Current federation credential frameworks such as OAuth2 and SAML are the most popular in use between federated environments. In this research blog we delve into how these credentials operate and how these attacks work within the perimeter and between cloud environments.

The scenarios addressed in this new analytic story (release v3.15) are the Golden SAML attack and Pass The Cookie. Specially the Golden SAML scenario, which is reported to be one of the attack techniques involved during the SolarWinds campaign. We are including detection and hunting searches for endpoint and cloud vendors such as AWS and Azure.

We decided to approach the federation attacks from two different fronts:

- **Perimeter:** The servers and endpoints where we find the elements to craft forge requests, including items such as SAML assertions or session cookies, private keys and certificates.
- **Cloud provider:** The providers of federation services where the extracted credentials are reused.

Perimeter-Focused Detection Searches

Name	Technique ID	Tactic(s)	Note

Certutil exe certificate extraction	T1552.004	Credential access	New detection
Registry keys used for privilege escalation	T1546.012	Privilege escalation, persistence	
Detect Mimikatz using loaded images	T1003.001	Credential access	
Detect Mimikatz via PowerShell and event code 4703	T1003.001	Credential access	

New Cloud-Focused Hunting and Detection Searches

Name	Technique ID	Tactic(s)	Provider
AWS SAML access by provider user and principal	T1078	Defense evasion, persistence, privilege escalation, initial access	AWS
AWS SAML update identity provider	T1078	Defense evasion, persistence, privilege escalation, initial access	AWS
O365 Excessive SSO logon errors	T1556	Credential access, defense evasion	Azure
O365 added service principal	T1136.003	Persistence	Azure
O365 new federated domain added	T1136.003	Persistence	Azure

Detecting Cobalt Strike

Cobalt Strike is threat emulation software that Red Teams, penetration testers and threat actors all use. More recently, adversaries have used cracked or leaked versions to perform post exploitation within the target's environment. In December 2020 we got a rare glimpse into FireEye's Red Team tools after an actor gained unauthorized access. As a defender,

we may not always have access to a tool like Cobalt Strike, so we need to research it to better understand how we may generate our content. With Cobalt Strike comes the ability to deploy what are called Malleable C2 profiles. Each profile is a customization to how the beacon payload will blend in with the network and endpoint. It may be as short or detailed as the operator needs. If unable to customize, there are many profiles freely available.

Functions within the Malleable C2 profile are: spawnto_x86 and **spawnto_x64**. **Spawnto_** is a process that Cobalt Strike opens to inject shellcode into. The default **spawnto_ process** is rundll32.exe.

Top five publicly available spawnto values identified in Malleable C2 profiles:

spawnto	count
rundll32.exe	401
gpupdate.exe	16
svchost.exe	8
mstsc.exe	6
WerFault.exe	3

In generating content related to Cobalt Strike, consider the following:

1. Is it normal for **spawnto_ value** to have no command line arguments? No command line arguments and a network connection?
2. What is the default, or normal, process lineage for **spawnto_ value**?
3. Does the **spawnto_ value** normally make network connections?

Content is currently in active development and much more is to come. We want to help organizations of all sizes begin to advance their detection capabilities against Cobalt Strike and more.

Name	Technique ID	Tactic	Note

Rundll32 with no command line arguments	T1218.011	Defense evasion	New detection
Suspicious rundll32 startw	T1218.011	Defense evasion	New detection
Suspicious MSBuild path/rename	T1127.001	Defense evasion	New detection
Suspicious Microsoft.Workflow.Compiler rename/usage	T1127	Defense evasion	New detection
Detect Regsvr32 Application Control Bypass	T1218.010	Defense evasion	New detection

Why Should You Care?

Some of these attack vectors are new and evolving and they seem to emulate past lateral movement techniques such as pass the hash or pass the ticket. Many vendors do not consider these attack vectors as vulnerabilities but rather an abuse of features. These types of attacks are bound to become more popular as enterprises continue to implement cloud services.

Cobalt Strike is the baseline adversary tool we defenders need to ensure we have coverage for moving forward in 2021. With the increasing usage of leaked versions of Cobalt Strike, content needs to be created to detect and ultimately prevent the capabilities it provides. In addition, defenders need to understand what malicious looks like and how to respond to activity related to methodologies using Cobalt Strike.

For a full list of security content, check out the release notes on Splunk Docs:

- 3.15.0
- 3.14.0

Learn more

You can find the latest content about security analytic stories on GitHub and in Splunkbase. Splunk Security Essentials also has all these detections now available via push update.

Feedback

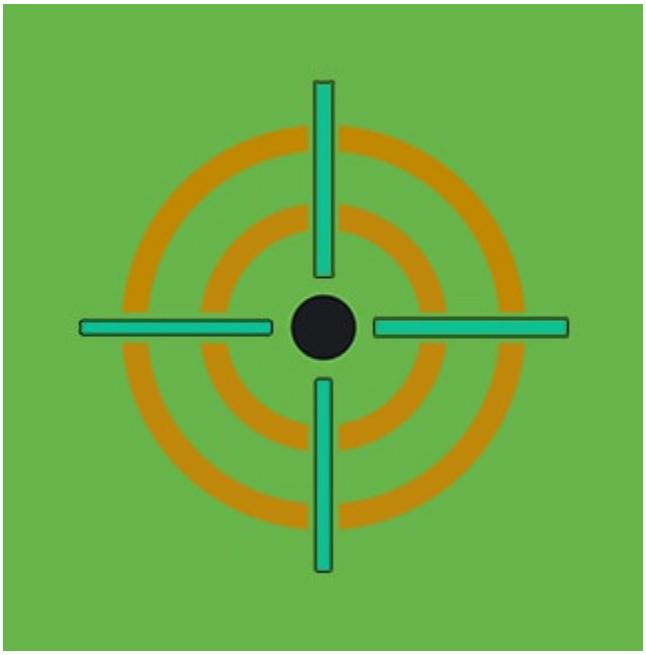
Any feedback or requests? Feel free to put in an Issue on Github and we'll follow up. Alternatively, join us on the Slack channel #security-research. Follow these instructions If you need an invitation to our Splunk user groups on Slack.

About the Splunk Threat Research Team

The Splunk Threat Research team is devoted to understanding actor behavior and researching known threats to build detections that the entire Splunk community can benefit from. The Splunk Threat Research team does this by building and open-sourcing tools that analyze threats and actors like the Splunk Attack Range and using these tools to create attack data sets. From these data sets, new detections are built and shared with the Splunk community under Splunk Security Content. These detections are then consumed by various Splunk products like Enterprise Security, Splunk Security Essentials and Mission Control to help customers quickly and effectively find known threats.

Contributors

We would like to thank Rod Soto, Michael Haag, Patrick Bareiss and Bhavin Patel for their contributions to this post, as well as all of the community contributors who provided feedback and helped generate new security content.



Posted by

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the Attack Data repository.

Our goal is to provide security teams with research they can leverage in their day to day operations and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more Splunk Security Content.

TAGS
Show All Tags

Show Less Tags

Join the Discussion