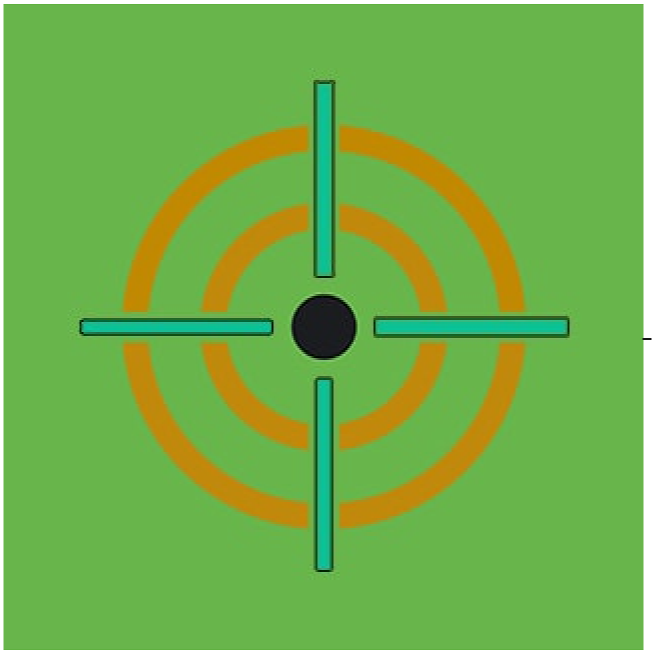
Detecting Password Spraying Attacks: Threat Research Release May 2021

splunk.com/en_us/blog/security/detecting-password-spraying-attacks-threat-research-release-may-2021.html

June 10, 2021

SECURITY



By Splunk Threat Research Team June 10, 2021

The Splunk Threat Research team recently developed a new analytic story to help security operations center (SOC) analysts detect adversaries executing password spraying attacks against Active Directory environments. In this blog, we'll walk you through this analytic story, demonstrate how we can simulate these attacks using PurpleSharp, collect and analyze the Windows event logs, and highlight a few detections from the May 2021 releases.

Watch the video below to learn more about how we can simulate and detect password spraying attacks using PurpleSharp in a lab environment built with the Splunk Attack Range.

Password spraying (T1110.003) is a technique by which adversaries leverage a single password or a small list of commonly used passwords against a large group of usernames to acquire valid account credentials. Unlike a brute force attack that targets a specific user or small group of users with a large number of passwords, password spraying follows the opposite approach and increases the chances of obtaining valid credentials while avoiding account lockouts. This allows adversaries to remain undetected if the target organization does not have the proper monitoring and detection controls in place. Penetration testers, cybercriminals as well as nation-state actors have been known to leverage this effective technique.

Password spraying can be leveraged by adversaries across different stages in a breach. It can be used to obtain initial access to an environment but can also be used to escalate privileges when access has been already achieved. In many scenarios, this technique ironically capitalizes on a common security control deployed by organizations: password rotation. As enterprise users change their passwords when they expire, some of them may pick predictable, seasonal passwords such as “Summer2021”.

Specifically, this Analytic Story is focused on detecting potential password spraying attacks against Active Directory environments in two scenarios where an attacker has obtained access to the target network:

- An adversary has obtained physical access to the network with a rogue device and can perform spraying attacks against internal hosts.
- An adversary is controlling a domain endpoint previously compromised and is leveraging it to perform spraying attacks.

In properly monitored Active Directory environments, there are several detection opportunities to identify password spraying attacks. This analytic story presents eight different detection analytics that leverage Windows event logs which can aid defenders in identifying instances where a single user, source host, or source process attempts to authenticate against a target or targets using a high and unusual number of unique users. A user, host, or process attempting to authenticate with multiple users is not common behavior for legitimate systems, and should be monitored by security teams. Possible false positive scenarios include but are not limited to vulnerability scanners, remote administration tools, multi-user systems and misconfigured systems.

Name	Technique ID	Tactic	Description
Multiple users failing to authenticate from host using kerberos	T1110.003	Credential Access	Identifies one source endpoint failing to authenticate with multiple valid users using the Kerberos protocol. This detection will only trigger on domain controllers, not on member servers or workstations.
Multiple users failing to authenticate from host using NTLM	T1110.003	Credential Access	Identifies one source endpoint failing to authenticate with multiple valid users using the NTLM protocol. This detection will only trigger on domain controllers, not on member servers or workstations.
Multiple disabled users failing to authenticate from host using Kerberos	T1110.003	Credential Access	Identifies one source endpoint failing to authenticate with multiple disabled domain users using the Kerberos protocol. This detection will only trigger on domain controllers, not on member servers or workstations.

Multiple invalid users failing to authenticate From host using Kerberos	T1110.003	Credential Access	Identifies one source endpoint failing to authenticate with multiple invalid domain users using the Kerberos protocol. This detection will only trigger on domain controllers, not on member servers or workstations.
Multiple invalid users failing to authenticate from host using NTLM	T1110.003	Credential Access	Identifies one source endpoint failing to authenticate with multiple invalid users using the NTLM protocol. This detection will only trigger on domain controllers, not on member servers or workstations.
Multiple users attempting to authenticate using explicit credentials	T1110.003	Credential Access	Identifies a source user failing to authenticate with multiple users using explicit credentials on a host. This detection will trigger on the potentially malicious host, perhaps controlled via a trojan or operated by an insider threat, from where a password spraying attack is being executed.
Multiple users failing to authenticate from process	T1110.003	Credential Access	Identifies a source process name failing to authenticate with multiple users. This detection will trigger on the potentially malicious host, perhaps controlled via a trojan or operated by an insider threat, from where a password spraying attack is being executed.
Multiple users remotely failing to authenticate from host	T1110.003	Credential Access	Identifies a source host failing to authenticate against a remote host with multiple users. This detection will trigger on the host that is the target of the password spraying attack. This could be a domain controller as well as a member server or workstation.

Why Should You Care?

Password spraying is leveraged by all sorts of offensive actors including penetration testing consultants, cyber crime actors as well as cyber espionage actors. It’s an effective technique available to adversaries to obtain valid account credentials. Unlike other password-based attacks like brute forcing, spraying accounts allows adversaries to remain undetected by avoiding account lockouts.

According to the Verizon's 2020 Data Breach Investigations Report, more than 80 percent of breaches within the "Hacking" category "involve brute force or the use of lost or stolen credentials."

Cyber defenders need to design and deploy effective monitoring capabilities that allow them to detect and respond to password spraying attacks against Active Directory as well as other authentication services.

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. In the upcoming weeks, the Splunk Threat Research team will be releasing a more detailed blog post on this analytic story. Stay tuned!

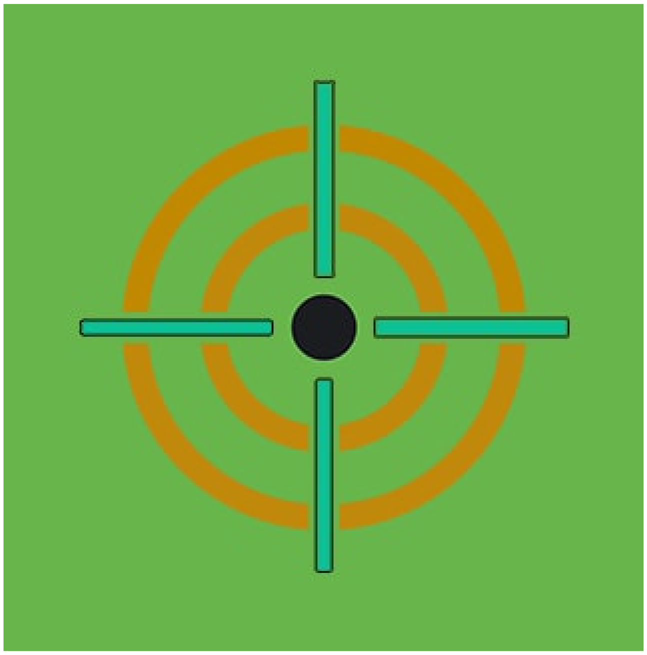
For a full list of security content, check out the release notes on Splunk Docs.

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.

Contributors

We would like to thank Mauricio Velazco for his contributions to this post and open source security tools.



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.

Join the Discussion