Golden SAML Revisited: The Solorigate Connection

December 29, 2020

In the past few weeks, we've been witnessing one of the most elaborate supply-chain attacks unfold with a threat actor that infected SolarWinds Orion source code and used the update process to get to around 18,000 victims all around the globe. One of the most (if not the most) innovative techniques used in this attack, now known as Solorigate, is the "Golden SAML" technique. The threat actor (UNC2452) did a phenomenal job across all stages of the attack — from meticulously planting the backdoor code and making it look like yet another legitimate class, to avoiding almost every possible forensics/analysis tool you can name, and even hiding data in DNS queries and making all the traffic look as if it's part of the SolarWinds Orion communication protocol. There's no doubt the threat actor knew what they were doing and tried to do everything in the best way possible. Still, we believe that performing a Golden SAML attack is the most innovative part of the attack (as of writing this post), having it be the first-ever documentation of such an attack. We (CyberArk Labs) did describe this attack vector at the end of 2017, but this is the first time we've seen it used **in the wild**. Golden SAML is an attack vector that can serve sophisticated attackers in their post-exploitation stages allowing them to maintain persistency and gain access to different services in a convenient and stealthy manner.

In this blog post, we'll first have a quick refresh on the basics of Golden SAML. Then we'll try to illustrate why it can be so powerful in the hands of attackers and how it fits the UNC2452 threat actor's perceived modus operandi like a glove. Finally, we'll share a few mitigation tactics that can be used by defenders to mitigate this risk.

Golden SAML Recap

Golden SAML is a technique that allows attackers, once they got privileged access to the victim's network, to impersonate almost any identity in the organization and acquire any type of privilege across almost all services of the organization (this depends on what services in the organization use SAML as their authentication protocol). You may already be familiar with a similar technique called – Golden Ticket. Golden SAML introduces to a federation environment the same advantages that golden ticket offers in a Kerberos environment. It simply applies the same principle in a different environment. If you would like to get into the details of this attack vector, you can find the full details on our blog.

Why Do Attackers Want to Use Golden SAML?

In this section we'll list a few of the powerful advantages this attack vector can offer for attackers.

Flexibility – Golden SAML provides a lot of flexibility for attackers, in the sense that they can impersonate any identity they wish in the federation. It is beneficial for two main reasons:

1. Attackers capable of performing a Golden SAML attack can basically get access to every service or asset in the organization (as long as it's a part of the federation of course). This means that they are not limited to the credentials/access they were lucky enough to stumble upon – they can practically gain access to anything they want.
2. Being able to do that gives attackers more than just access. In the majority of the cases, sophisticated attackers go to great lengths in trying to hide their activity and avoid detection. Imagine you're an attacker and that you have gained the ability to perform a Golden SAML attack in your target's network, which is monitored heavily. Whatever action you choose to perform next, you can do that using the identity of a user that is "known" to take this action from time to time, thus diminishing the chances of looking like a suspicious action, and ultimately getting detected and ruining the whole operation. Simply put, you are blending malicious actions with normal, legitimate activities. The attackers behind SolarWinds did just that, we can see it in the code they've planted, the communication protocol they used, and in their usage of legitimate configuration files for the backdoor's needs. It is very likely that it was this flexibility and the ability to blend in which were the factors that "sold" UNC2452 on the idea to use the Golden SAML vector.

MFA (Multi-Factor Authentication) Bypass – The usage of this technique can potentially make the additional security layer **MFA provides completely useless**. Since users get a valid SAML token **after** they've authenticated using MFA, attackers that are using Golden SAML don't need to go through that stage at all. The attackers basically skip it altogether and go straight to forging an identity using the stolen certificate, without having to know the user's password or to have other authentication factors. This is a very substantial ability, and it shows that the sense of security MFA provides, might just be a false one in some cases.

The ability to bypass MFA depends on the specific implementation of MFA an organization might have. MFA bypass can only be applied if the integration is on the identity provider side. If the integration is on the service provider side, then multi factor authentication happens only after the SAML token has been generated, thus making Golden SAML ineffective in bypassing it. Having said that, we need to remember that times organizations often use federated service for the sake of convenience in the form of SSO, and this could have the potential of damaging the overall security of the organization, as we see in the Golden SAML case.

Difficulty to Detect – Detection of such an attack can be extremely challenging for defenders. Even though there are methods that can potentially detect such malicious behavior (which we'll elaborate on in the next section), many organizations are not aware of this type of threat and do not monitor SAML authentication (especially not in the pre-Solorigate era).

Difficulty to Remediate – If an attacker steals your password, it's relatively easy to change this password and take back control of your identity. But if an attacker steals your SAML token signing certificate, it's a whole different ballgame. First, if you'll naively try to change your passwords, the attacker can easily continue to make SAML tokens that impersonate you, without the need to know the actual password (same case as being able to bypass MFA). So, what you really need to do is to change the actual token signing certificate. Which basically means reestablishing the trust across your entire federation.

Long-Term Persistency – Let's compare this to passwords again. Passwords are being changed every set period of time (a few weeks if your organization has proper credential management), but a SAML token signing certificate is almost never changed, or. This allows attackers to potentially maintain their access for a long period of time.

Golden SAML Detection and Mitigation

- Follow best practices of your federation Identity Provider (IdP) technology. Here are, for example, the AD FS (Active Directory Federation Services by Microsoft) best practices. Some IdP support protecting your token signing certificate in a hardware security module (HSM). This should make stealing your token signing certificate a much harder task for attackers.
- Do as much as you can to protect your tier-0 assets (a federation identity provider should be included here). This includes having proper credential hygiene, deploying a privileged access management solution, an EDR, etc. This will make it very difficult for attackers to gain sufficient privileges for stealing a token signing certificate in the first place.
- Examine SAML tokens to identify suspicious ones (such as tokens with an unusually long lifetime or with unusual claims).
- Correlate logs between your Identity Provider and your Service Provider. If you see a SAML authentication in your Service Provider that doesn't correlate to a SAML token issuance by the Identity Provider – something is wrong.
- Use third-party security solutions to protect the token signing certificate from being stolen by attackers. CyberArk Endpoint Privilege Manager (EPM) has the ability to do just that.

For more information on detection and mitigation please see this document by the NSA and this advisory by Sygnia.

Conclusion

At the time of writing this post, we're still learning new things on Solorigate with every day that passes. This attack has been an important lesson for everyone in the information security field, whether you were impacted directly or not.

As for Golden SAML, we do expect to see this tactic become more commonly used for two reasons:

- With more and more services being ported to the cloud, there is a greater need to establish some level of trust between them and between on-premise services – and SAML has become the de facto authentication and authorization standard. **Attackers operating in those types of environments will have to adapt their methods to fit the new norm. For instance, instead of settling on getting the domain's KRBTGT and forging any identity within that domain, attackers can now steal the SAML token signing certificate and forge almost any identity across the entire organization.**
- Seeing Golden SAML being used in one of the most sophisticated and elaborate cyber-attacks we have seen in recent years (and we are still not aware of the full impact of it), potential future attackers will come to know this tactic and possibly use it as well in the future.

We need to find joy in the rare cases in which defenders beat attackers at their own game and anticipate attack vectors before they're being used in the wild by malicious threat actors. This timeframe between the discovery of a new attack vector and its use by attackers should be utilized by defenders to prepare their network for such an attack as best as they can – setting up monitoring rules to detect this and deploying protection mechanisms that should block it. Golden SAML is a great example of such an opportunity, and we hope that as a security community we can learn from that and do better in the future.

References

- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
- https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF
- https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps
- https://www.sygnia.co/golden-saml-advisory