semperis

SILVER SAML THREAT: HOW TO AVOID BEING A VICTIM

Eric Woodruff of Semperis on Improving Certificate Management Practices

iSMG
INFORMATION SECURITY
MEDIA GROUP

Semperis researcher **Eric Woodruff** and **Tomer Nahum** discovered Silver SAML – a new technique used to launch attacks from an identity provider against applications configured to use it for authentication. How does it differ from Golden SAML, and how can enterprises respond to the threat? Woodruff shares insight.

In this interview with Information Security Media Group, Woodruff discussed:

- The evolution from Golden SAML to Silver SAML;
- Challenges brought by externally generated certificates;
- How to avoid being a victim of Silver SAML attacks.

Eric Woodruff

Woodruff focuses on ITDR and cloud identity resilience. He is a Microsoft MVP for security, recognized for his expertise in the Microsoft identity ecosystem. Throughout his 23-year career in information technology, Woodruff has held a diverse range of roles, including technical manager in the public sector, senior premier field engineer at Microsoft, and security and identity architect in the Microsoft partner ecosystem.

"With Silver SAML, our focus is business-critical applications. A lot of enterprises have things like Workday, Salesforce, AWS, Google Workspace and Cloud all configured to authenticate against Entra. An attacker could use something like Silver SAML to move into those."

FROM GOLDEN SAML TO SILVER SAML

TOM FIELD: How are the Silver SAML attacks different from what we know as Golden SAML?

ERIC WOODRUFF: Golden SAML and Silver SAML are really the same in that they're SAML forging attacks. When you authenticate, the core piece of material is a SAML response, and both attacks are essentially forging that. The difference is the target that you're going after.

FIELD: Can Silver SAML attacks access business-critical applications? And if so, what could an attacker potentially do?

WOODRUFF: In a lot of the Golden SAML attacks, the target was usually moving off of ADFS, which was Microsoft's Active Directory Federation Services, into something like Azure AD, which is now known as Entra ID. With Silver SAML, our focus is business-critical applications. If you're a big Microsoft shop and you're using Entra ID, a lot of enterprises have things like Workday, Salesforce, AWS, Google Workspace and Cloud all configured to authenticate against Entra. An attacker could use something like Silver SAML to move into those. What they can do in there is up to what user they are impersonating.

EXTERNALLY GENERATED CERTIFICATES

FIELD: What are identity providers doing wrong, and why is using externally generated certificates a problem?

WOODRUFF: It's not that identity providers are doing anything wrong; it's more like a business behavioral problem. Before working at Semperis, I was consulting with and working with organizations during my time at Microsoft, and I saw that people were not handling certificates securely. It's not just an SAML problem. People don't understand the gravity of how they treat this material.

CERTIFICATE MANAGEMENT CHALLENGES

FIELD: Why can't we apply our broader certificate management directives and policies to leveraging certificates for SAML signing?

WOODRUFF: Comparing different certificate management practices is like comparing apples to oranges. Many organizations that want to use externally generated certificates have a model that we might use where we have a one-to-many relationship, where we have lots of clients that have certificates provided to them or web services where you have a certificate on your web server. Then you need to create a trust relationship between all your clients and that web server. So we're talking SSL or TLS.

With SAML, the trust model is different because it's one-to-one. Let's say we acquire Salesforce. When we're configuring SAML, I as the administrator or working with the business unit that owns Salesforce in our org, configure the SAML trust relationship between Salesforce and Entra ID. As the admin, I'm the trust anchor. If that certificate is compromised from an authentication perspective, there's nothing that certificate revocation brings us.

If we go to a web server model, if the certificate for a web server is compromised, we use certificate revocation to tell all the clients, "Don't trust this certificate anymore." But with SAML, if that certificate is compromised, we have to rotate it and go through another manual process, in most instances. So there's no benefit to certificate revocation because that would break auth, and it's likely that if we know we're compromised, our IT pros are going to be in there rotating that certificate anyway. The problem is a lack of understanding that revocation doesn't really bring anything to the table in these instances.

PREVENTING SILVER SAML ATTACKS

FIELD: What should defenders do to avoid being a victim of Silver SAML attacks?

WOODRUFF: A lot of orgs, whether their security folks or their IT pros are managing and using SAML, need to prioritize learning how SAML functions. A lot of organizations have hundreds and hundreds of applications integrated with SAML, and you run into scenarios where the attackers understand how the authentication mechanism works better than the defenders do. I know that time, resources and money all weigh into why we don't do this. But if people really understood the fundamentals of SAML and configuring

"With Silver SAML, our focus is business-critical applications. A lot of enterprises have things like Workday, Salesforce, AWS, Google Workspace and Cloud all configured to authenticate against Entra. An attacker could use something like Silver SAML to move into those."

it and the management and why they're doing what they're doing, they would see that the easiest practice to protect yourself from a Silver SAML attack is to not use externally generated certificates.

In the realm of Entra and Entra ID, if we use a Microsoft-generated certificate, it's still strong. It doesn't have any negative qualities to it. But the private key material, which is what an attacker would need, cannot be exported out of Entra. So it's a very simple protection that you can do by just not using externally generated certificates. Whenever I say this, people push back and say, "But what if you want alternatives?" There are other things that you can do with signing of SAML requests that can also protect you against SAML forging attacks. Our blog details what you can do to protect yourselves.

THE SEMPERIS APPROACH

FIELD: What is Semperis doing to help its customers prepare for and respond to the Silver SAML threat?

WOODRUFF: Both our free product, Purple Knight, and our Directory Services Protector product contain indicators of exposure. They look for security misconfigurations that range from warnings to critical issues about things you're doing within Active Directory, or in this case Entra ID, that are opening the door for attackers. We've written an indicator that is helping organizations look for Silver SAML. It's a bit of a challenge because some of the auditing things that would allow us to be really precise in trying to detect this don't exist in Entra ID. But we're trying to work with Microsoft to change how they audit things to make it more robust so that we can have precision in detecting if orgs set themselves up for potential compromise.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io