OBSIDIAN

SOLUTION BRIEF

Combat SaaS Token Compromise with Obsidian

Stolen session tokens grant adversaries direct, persistent access to your SaaS environment. Detect and mitigate these attacks with Obsidian.

Understanding session token compromise

In order to streamline the user experience and avoid authentication fatigue, SaaS applications generate session tokens for user access. Identity providers (IdPs) are often used to manage digital identities and further streamline access with SSO and MFA. IdPs also have their own session tokens that provide access to every connected SaaS application.

SaaS session tokens undoubtedly offer user convenience, but long-lasting authentication is also attractive to attackers. Bad actors are foregoing simple credential theft to target session tokens which enables them to bypass MFA and establish discreet, longer-term persistence in the SaaS environment. Vendor compromise, malware, and man-in-the-middle attacks are the most prevalent techniques for obtaining these tokens.

> With a valid identity provider token, an adversary can potentially maintain weeks of uninterrupted access to your SaaS applications while evading detection by most traditional security solutions.

Vendor Compromise

If your SaaS application vendor is compromised, it is possible for the adversary to pivot into your environment. The adversary can access your data by creating their own credentials or authenticated sessions into your environment. This activity would show as authenticated sessions from “valid” accounts because all of the compromise activity is occurring on SaaS vendor systems.

Malware

There are a variety of avenues that attackers can exploit to trick users into unknowingly installing malware on their devices. Once a user authenticates an endpoint with cookie-stealing malware installed, their token is captured and relayed to the attacker. From there, the adversary can reuse this token to bypass MFA, authenticate to the IdP, and pivot to connected SaaS applications.

Adversary-in-the-middle

In an adversary-in-the-middle attack, adversaries phish users with authentication infrastructure that they control. This often involves a fake login page that closely resembles the real experience. The attacker relays traffic—including the MFA challenge—between the end user and identity provider, capturing the session token granted to the user. Because the authentication experience appears legitimate, the user rarely suspects a thing.

Case Study: Okta HAR Breach

On October 20, 2023, Okta disclosed their support case management systems were accessed by an unauthorized actor via stolen credentials of a valid Okta account. This bad actor accessed customer support cases where the customer had uploaded HTTP archive (HAR) files to help troubleshoot issues within the Okta environment. These HAR files contained detailed web traffic, including cookies and session tokens for customer application environments.

Okta and its customers identified adversarial activity being performed within customer environments as a result of this access. The adversary was able to gain access to multiple customer environments using the stolen session tokens.

The following organizations have disclosed adversarial activity related to this Okta incident:

- 1Password: The adversary was able to modify their IdP configurations and attempted to identify administrative users to possibly perform an impersonation attack to gain super admin access to the environment.

- BeyondTrust: The adversary was able to authenticate via Okta API and create a new backdoor account within the customer's environment.
- Cloudflare: The adversary was able to compromise two Cloudflare employee accounts within their Okta platform.

Okta has not confirmed when the initial access to their support case management systems occurred. However, 1Password has confirmed their observed activity occurred September 29, 2023—almost a full month prior to Okta's disclosure. Without the proper visibility and detection strategy for stolen SaaS session tokens, the adversary had ample time to further their compromise and increase their impact on the affected businesses.

Obsidian Security is the industry's most advanced threat detection solution designed for SaaS. From account takeovers and insider threats to third-party supply chain compromises, Obsidian makes it possible to identify, investigate, and mitigate threats early in order to prevent the exfiltration of your sensitive data.

Case Study: Azure AD and Microsoft 365 compromises from stolen Microsoft authentication keys

On June 16, 2023, Microsoft was notified by a customer of unauthorized access to their email systems. After an investigation, Microsoft identified a system support file ("crash dump") in an unsecured location containing the consumer signing key. This signing key is used to create valid session tokens for Azure AD.

The threat actor successfully compromised a Microsoft engineer's corporate account and accessed the crash dump containing the consumer signing key. It is unclear from the disclosure exactly when the threat actor compromised the signing key due to log retention, but Microsoft stated it was sometime "after April 2023." The threat actor used this key to forge Azure AD keys, gaining access to customer environments. This access was used to exfiltrate email via the OWA API.

On July 11, 2023, Microsoft disclosed details of an incident that allowed a threat actor to steal a Microsoft signing key and forge session tokens to access customer email systems via OWA and Outlook.com. From the time of the initial compromise to the disclosure, the threat actor would have had three to four months of persistent access to their target's environment.

Minimizing Dwell Time

With the heightened speed and sophistication of adversaries, reducing the dwell time of a compromise is crucial to protecting your business's sensitive data. On average, attackers have reduced the time until impact to less than 5 days, fully deploying ransomware within hours.

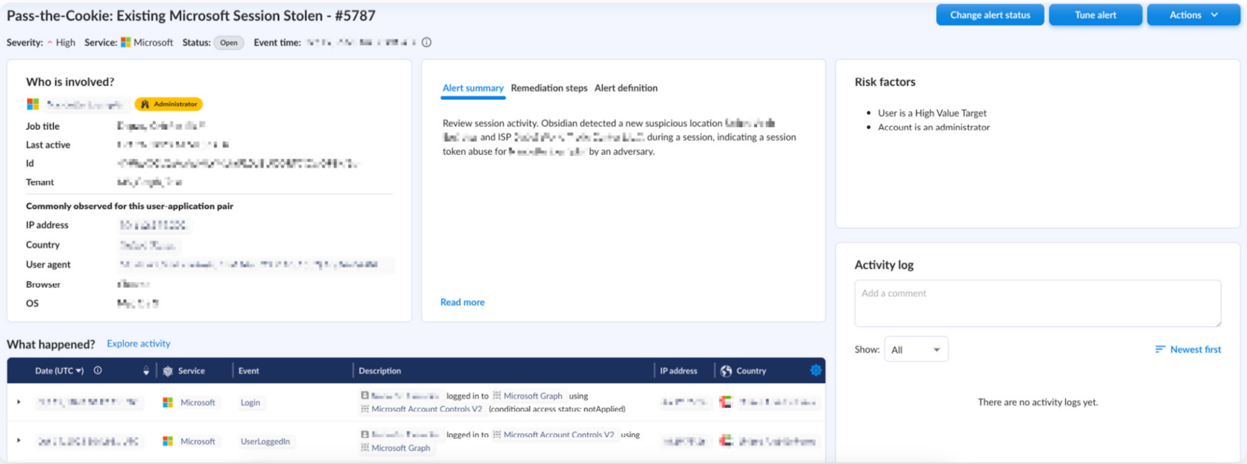
In the Okta and Microsoft case studies above, we see the dwell time for the threat actor was measured in months from initial access to public disclosure. Fortunately for Okta and Microsoft, customers were able to detect the downstream compromises and alert the vendor's security teams to remediate the incident.

When companies are not able to onboard SaaS logs to their detection platforms, they are forced to place 100% trust in these vendors. Obsidian Security brings visibility and detection capabilities to your security operation within minutes.

Detect Session Token Compromise with Obsidian

Obsidian Security is the industry's most advanced threat detection solution designed for SaaS. From account takeovers and insider threats to third-party supply chain compromises, Obsidian makes it possible to identify, investigate, and mitigate threats prior to the exfiltration of your sensitive data.

Research shows that the average cost of a data breach is currently $4.45 million (IBM). Ensuring visibility and detection capabilities within your SaaS environment is key in reducing this exposure and the corresponding costs of security events.



Pass-the-Cookie: Existing Microsoft Session Stolen - #5787

Severity: High Service: Microsoft Status: Open Event time: [redacted]

Who is involved?

[redacted] Administrator

Job title	[redacted]
Last active	[redacted]
Id	[redacted]
Tenant	[redacted]

Commonly observed for this user-application pair

IP address	[redacted]
Country	[redacted]
User agent	[redacted]
Browser	[redacted]
OS	[redacted]

Review session activity. Obsidian detected a new suspicious location [redacted] and ISP [redacted] during a session, indicating a session token abuse for [redacted] by an adversary.

Risk factors

- User is a High Value Target
- Account is an administrator

Activity log

Show: All

There are no activity logs yet.

What happened?

Date (UTC)	Service	Event	Description	IP address	Country
[redacted]	Microsoft	Login	[redacted] logged in to Microsoft Graph using Microsoft Account Controls V2 (conditional access status: notApplied)	[redacted]	[redacted]
[redacted]	Microsoft	UserLoggedIn	[redacted] logged in to Microsoft Account Controls V2 using Microsoft Graph	[redacted]	[redacted]

With advanced detection models and a deep understanding of user behaviors and risk factors, Obsidian accurately identifies session token theft to isolate threat activity in as little as one hour. Because the platform continuously examines user and client connections to identity providers and applications, Obsidian is the first and only SaaS security solution capable of detecting session token reuse by a bad attacker. Early and accurate identification of this threat enables your security team to investigate and eradicate attacker persistence quickly and completely, reducing damaging dwell time from weeks to minutes.

Reducing the Impact of Token Compromise with Posture Management

Token compromises can be devastating depending on the access, privileges, and configurations available to the adversary. If an adversary compromises a session that has administrative access to all of your applications for 30 days, it would be much more costly to remediate than if the session only had access to a single application, with a specific scope, for a limited time. Ensuring a secure configuration for your SaaS applications can reduce the impact by limiting the scope of a compromise and isolating the adversary into a limited portion and time frame of your environment.

Securing and maintaining a hardened SaaS security posture is critical in reducing the blast radius of a token compromise. This presents a challenge for security because the average enterprise has hundreds of SaaS apps being leveraged across its workforce, each with its own intricacies and complex configuration management systems.

Obsidian Security is the only SaaS security platform that gives your team a clear understanding of the gaps putting your applications at risk—and the power to address them. Providing the visibility and control over configurations and privilege that you need to minimize risk and reduce the impact of potential threats.