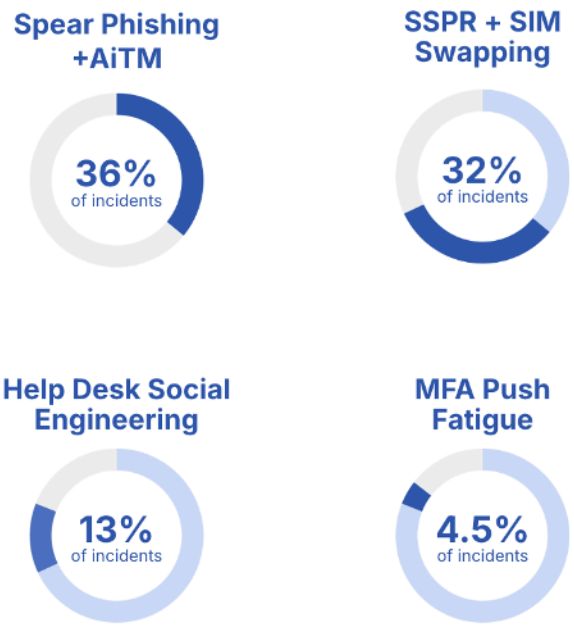
Webinar - Token Theft

SaaS and Identities - they keys to the kingdom



The adoption of Software-as-a-Service (SaaS) solutions in enterprise environments has accelerated in recent years, driven by the need for flexibility, scalability, and cost efficiency. However, this shift to the cloud has also amplified the importance of user identities. In the SaaS world, user identities are the keys to accessing sensitive corporate data and applications. Ensuring robust identity management, including strong authentication and granular access controls, is paramount to prevent unauthorized access and potential data breaches, safeguarding both the enterprise and its valuable digital assets.

Data from investigating 100's of breaches involving or originating from SaaS solutions shows that identities are more often targeted than misconfigurations within SaaS applications. Interestingly, two attack types account for the majority of the observed breaches:

- Spear Phishing combined with Adversary in The Middle (AiTM)
- Self-Service Password Reset (SSPR) + SIM Swapping tactiques

Let's examine the risks and detection possibilities for common Adversary in The Middle scenarios.

A typical phishing attempt - just log in

Let’s examine a typical phishing attack - and that includes sub-types such as spear-phishing or whaling. We will focus on a scenario which aims to gain access to a typical SaaS application by stealing credentials and session tokens, granting access to the attacker.

1) The attacker prepares the environment to lure phishing victims in and handle the resulting traffic. One example of an out-of-the-box toolkit, sometimes referred to as Adversary in The Middle / AitM toolkits, is called EvilGinx3.
2) A more or less plausible email with a call to action is sent to targeted individuals - there are plenty of ready to use templates available
3) The link contained within the phishing email directs the user to the infrastructure set up in step 1 - from a user’s perspective, the look and feel of the page is exactly as the legitimate web page she is expecting to see
4) The user enters her credentials, getting access to the expected SaaS application without any indication of malfunction/reduced functionality
5) The attacker observes the authentication traffic between the browser of the user and the actual SaaS application and is able to retrieve login credentials as well as session/authentication tokens
6) The attacker will (most likely) be able to login to the SaaS application impersonating the phishing victim and gaining access to data/admin functionality as that user.

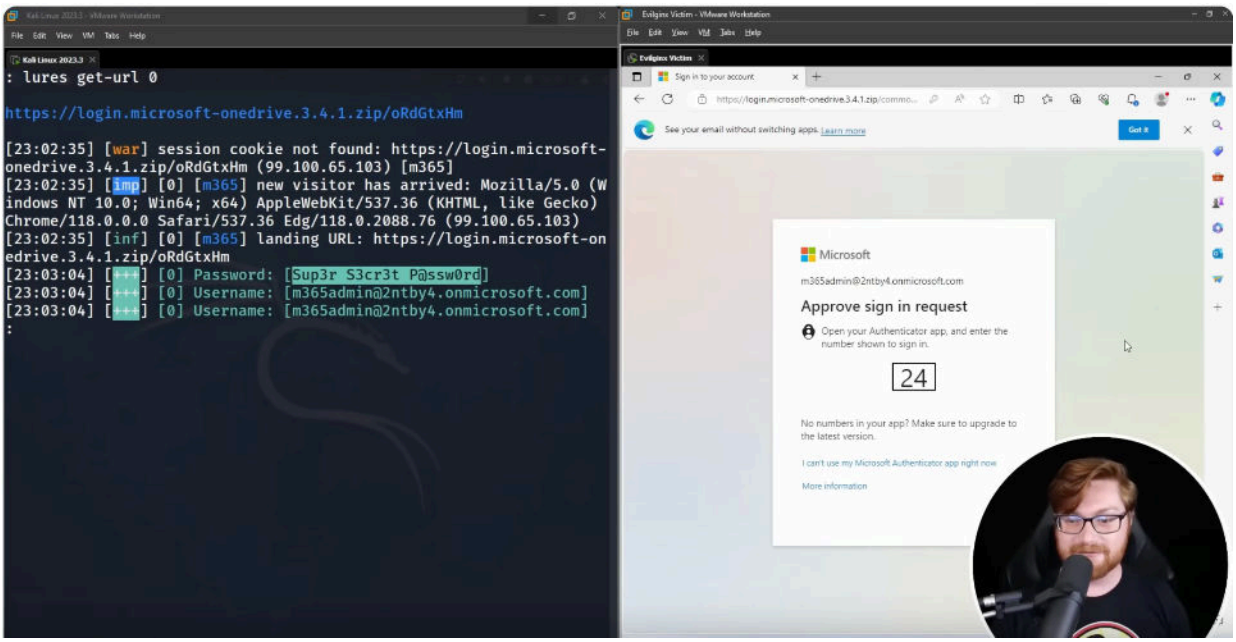
These phishing attempts have only increased in recent years and the quality of phishing emails received has steadily increased. Gone are the days when it was easy to sport an obvious phishing email by looking for grammatical errors or misspelled words.

Session token theft?

Multi-Factor Authentication (MFA) is absolutely crucial when it comes to securing SaaS access in enterprise environments. These additional factors typically do no not prevent the stealing of session tokens and the subsequent use of these tokens to access SaaS applications.

Think of session tokens as a temporary access badge after a user's identity has been identified. This token/badge has a limited lifetime before it needs to be renewed.

In the screenshot below we see a user logging in to a SaaS application, using a strong MFA mechanism. The attacker observes the entered credentials and is able to extract these session tokens. (EvilGinx shown here).



"I Stole a Microsoft 365 Account. Here's How." by John Hammond

Building an effective defense

To defend against phishing, organizations must evaluate their security controls across all layers. A key strategy is to identify choke points—critical areas that attackers cannot bypass. In SaaS environments, two natural choke points emerge:

- The SaaS application: Monitoring and logging every interaction at the application layer ensures visibility into any suspicious behavior.
- The browser: Most SaaS interactions occur through a browser, making browser security essential in preventing phishing attacks.

At Obsidian, our strategy focuses on these choke points. Our browser extension provides real-time phishing detection and administers warnings when users visit malicious sites. If an attack slips past the browser extension, our detection systems analyze SaaS activity logs to identify suspicious behaviors, stopping potential breaches before they escalate.