saas-attacks/techniques/evil_twin_integrations/description.md at main · pushsecurity/saas-attacks

By jukelennings

Archived: 2026-04-05 16:06:48 UTC

Latest commit

Evil twin integrations

ID: SAT1016

Tactics

- Persistence
- Defense Evasion

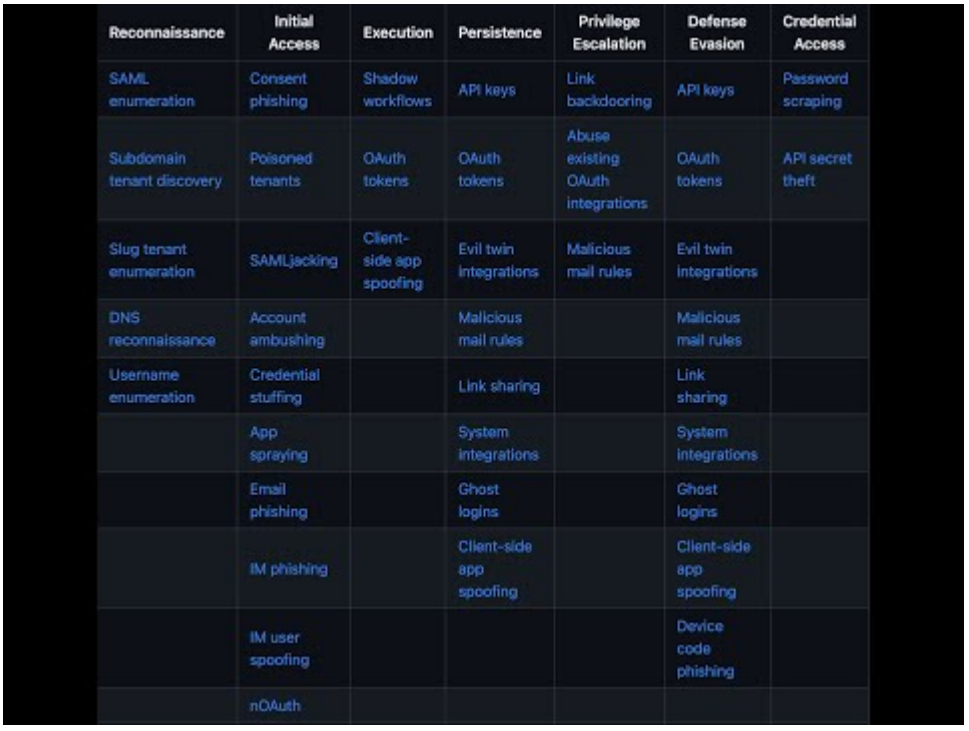
Summary

OAuth apps provide a mechanism for maintaining long-term persistent access to compromised accounts that resist normal recovery actions, such as password resets. However, an in-depth investigation may lead to the discovery of OAuth integrations created by the adversary. Once these malicious integrations are deleted, the adversary would lose their persistence mechanism as soon as the access token expires (within hours or minutes).

Instead, the attacker could enumerate existing OAuth integrations the user has already granted/installed, find one that exposes useful scopes and functionality, and create a second instance or twin of that integration. These twin integrations look identical to the original integration as SaaS apps don’t display the details of the account on the other side of the integration, and are therefore unlikely to be discovered and deleted.

This attack relies on the victim having already installed or created an OAuth integration that would be useful to the attacker. Existing integrations with workflow automation / no-code automation platforms are typically the most useful, but other apps that access (and expose) sensitive data like email are common in marketing, sales and customer support tools.

A demo video of an attack chain combining shadow workflows with an evil twin integration is given below:



Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
SAML enumeration	Consent phishing	Shadow workflows	API keys	Link backdooring	API keys	Password scraping
Subdomain tenant discovery	Poisoned tenants	OAuth tokens	OAuth tokens	Abuse existing OAuth integrations	OAuth tokens	API secret theft
Slug tenant enumeration	SAMLjacking	Client-side app spoofing	Evil twin integrations	Malicious mail rules	Evil twin integrations	
DNS reconnaissance	Account ambushing		Malicious mail rules		Malicious mail rules	
Username enumeration	Credential stuffing		Link sharing		Link sharing	
	App spraying		System integrations		System integrations	
	Email phishing		Ghost logins		Ghost logins	
	IM phishing		Client-side app spoofing		Client-side app spoofing	
	IM user spoofing				Device code phishing	
	nOAuth					

Examples

- Hubspot

References

- Maintaining persistant access in a SaaS-first world - Technical blog post
- The shadow workflow's evil twin - Technical blog post

Source: https://github.com/pushsecurity/saas-attacks/blob/main/techniques/evil_twin_integrations/description.md