OBSIDIAN

SOLUTION BRIEF

SaaS Security Across the MITRE ATT&CK Framework

Understand adversarial techniques being used against SaaS environments through the lens of the MITRE ATT&CK framework.

What is the MITRE ATT&CK Framework?

The MITRE ATT&CK framework is a curated knowledge base of adversarial tactics and techniques employed across every phase of the entire attack lifecycle. Not only does ATT&CK provide a common taxonomy for offensive and defensive cybersecurity teams, but also serves as an invaluable reference tool for organizations looking to improve their security posture and threat response capabilities.

Applying ATT&CK to SaaS Threats

Obsidian Security delivers unmatched threat detection for business-critical SaaS applications, helping security teams identify and respond to attacks with speed and precision. By applying cutting-edge machine learning models to continuous activity monitoring, Obsidian can accurately detect user account compromises, insider threats, and SaaS integration abuse.

Given our team's unique SaaS security expertise and extensive threat research, we wanted to share some knowledge around emerging adversarial techniques being used against SaaS environments within a slightly modified version of the ATT&CK framework.

It's important to note that the below matrix is focused specifically on SaaS compromises. A technique from an adjacent ATT&CK matrix, such as the Enterprise ATT&CK matrix, can be a means to execute another technique against a SaaS environment. For example, an attacker having already gained Initial Access to a machine executes malware on the endpoint to obtain Credential Access within the SaaS environment. The attacker does not achieve Initial Access to SaaS until those credentials are successfully reused.

Credential Access Capturing user account credentials and other authenticating factors.	Application Access Token Capture Brute Force Account Leaked credentials MFA Request Generation Malware: Credential Stealing Password Stuffing Password Spraying Phishing Session Token Capture
Initial Access Successfully establishing access to target SaaS applications.	Session Token Reuse Valid Account Valid Application Access Token Support Account
Persistence Implementing measures to improve and guarantee longevity of access.	Create New Account Create New Application/Integration Deregister MFA Device Mailbox Rule Creation Modify Existing Account Modify Existing Application/Integration Modify Access Policy Unfreeze User Account Modify Mailbox Folder Permissions Mail Transport Rules
Privilege Escalation Increasing permissions to expand potential scope of access.	Modify Existing Account Modify Existing Application/Integration
Defense Evasion Taking measures to evade detection by traditional security solutions.	Bypass Access Control Impair Defenses
Discovery Attempting to better understand the target environment and find valuable resources.	Enumerate Controls Enumerate Accounts/Roles/Settings Enumerate Resources Secret Scanning
Lateral Movement Using interconnections to gain access to other services, accounts, and more.	Internal Spearfishing Taint Shared Content
Impact Taking action to manipulate, destroy, or otherwise tamper with SaaS resources.	Account Access Disabled Data Deletion Data Encryption Financial Fraud
Exfiltration & Collection Stealing data from the target SaaS environment.	Data Exportation Data Synchronization Data Sharing Data Transfer Mail Synchronization Mail Forwarding