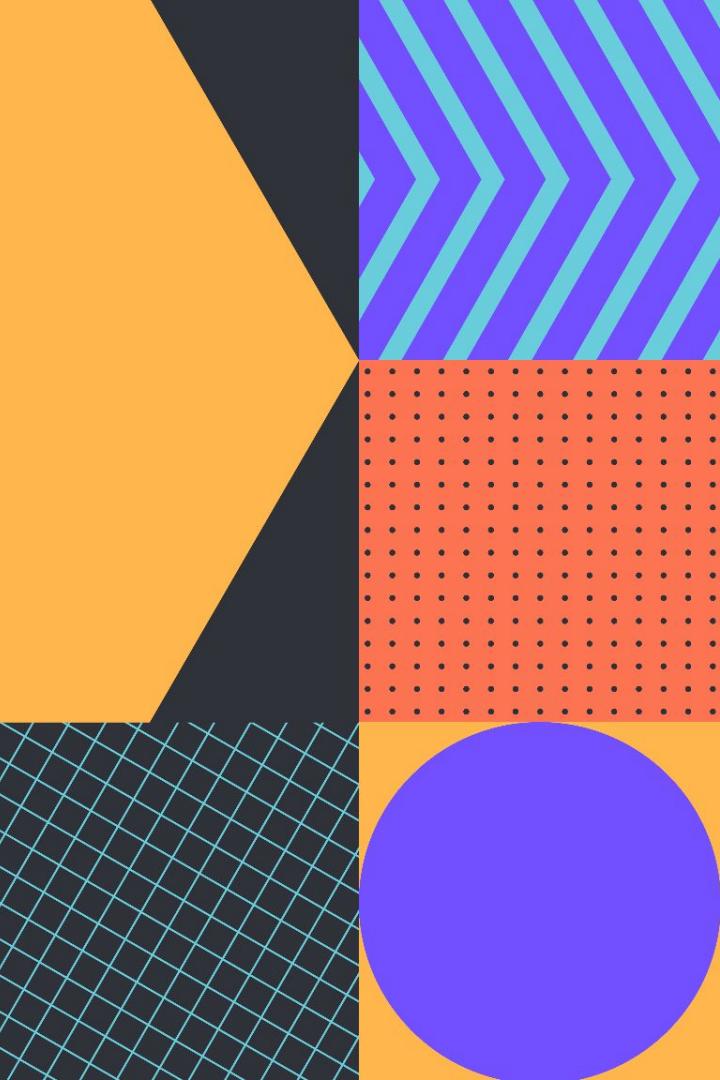




Understanding the new SaaS cyber kill chain

Luke Jennings



- Red teaming + offensive security research
- EDR design + threat hunting research
- Identity and SaaS security research



- 1 Brief history**
- 2 SaaS adoption**
- 3 Traditional attacks**
- 4 New cyber kill chain**
- 5 Interesting new techniques**
- 6 Chaining it all together**



Brief History

Era	Techniques of the day	Response
2000s Traditional perimeter hacking	Port scanners, vuln scanners, buffer overflows, web app attacks, WiFi hacking, client/server backdoors	Firewalls, DMZs, patch management, secure coding, WPA, penetration testing
2010s Endpoint is the new perimeter	Phishing, office macros, file format bugs, browser exploits, memory resident implants, C2 frameworks	Endpoint hardening, EDR, SIEMS, red teaming, threat hunting
2020s Cloud identities are the new perimeter?	???	???



What drives shifts in attacks?



Improved security controls

- Firewalls
- VPNs
- Patch management
- Secure coding
- EDR/XDR



Technological shifts

- Complex web applications
- WiFi
- Remote working
- SaaS-native organizations

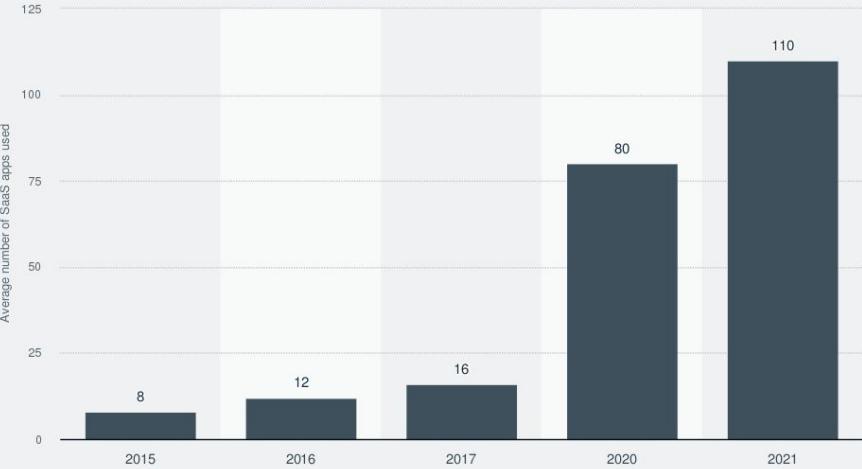


SaaS adoption

- SaaS - any business app you don't host yourself
- SaaS use is rising rapidly
- Many startups are now SaaS-first
- Enterprises are migrating
- New attacks require new responses

80% of workers admit to using SaaS applications at work without getting approval from IT.

Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2021

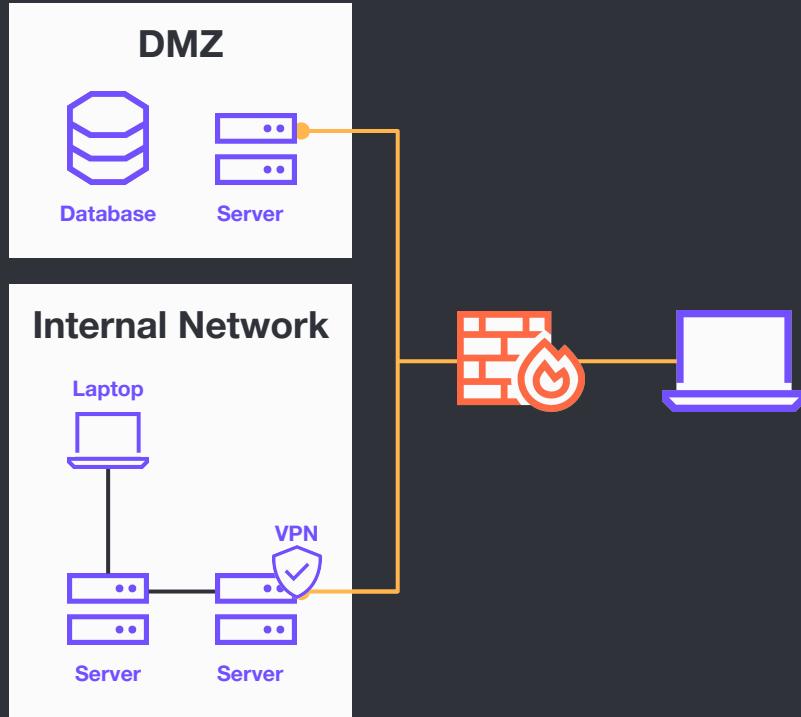


Source
BelterCloud
© Statista 2022

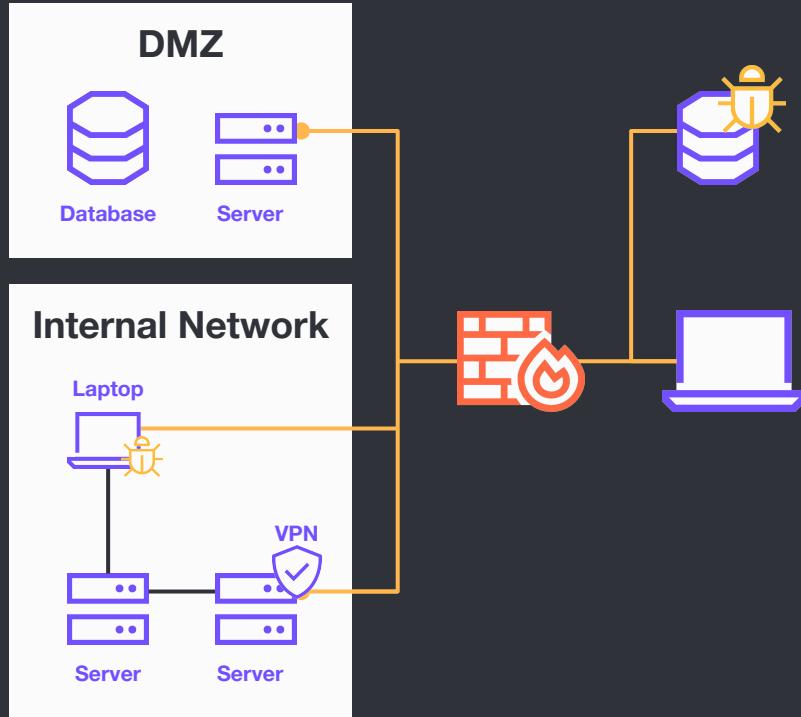
Additional Information:
Worldwide; 2015 to 2021; 523 respondents; IT and security professionals



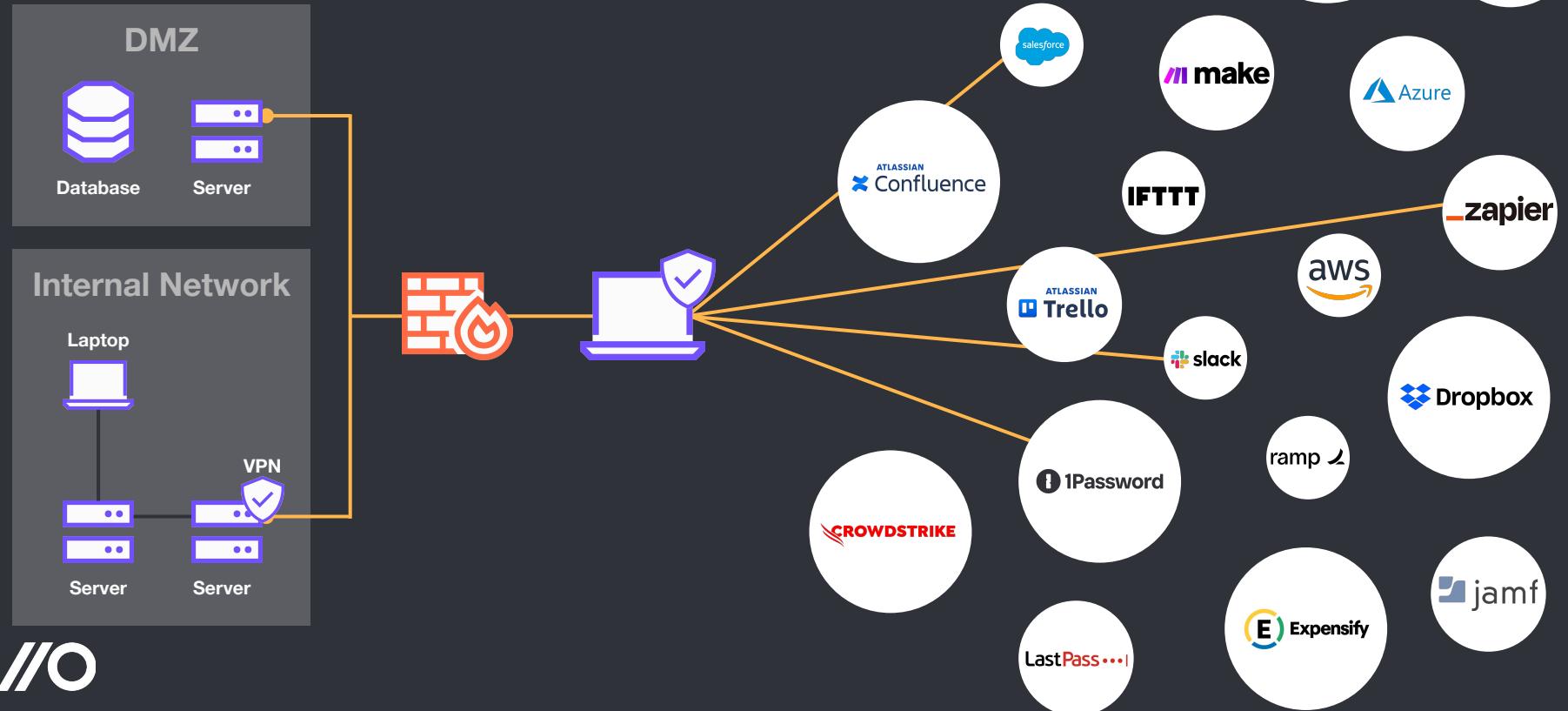
Infrastructure comparison



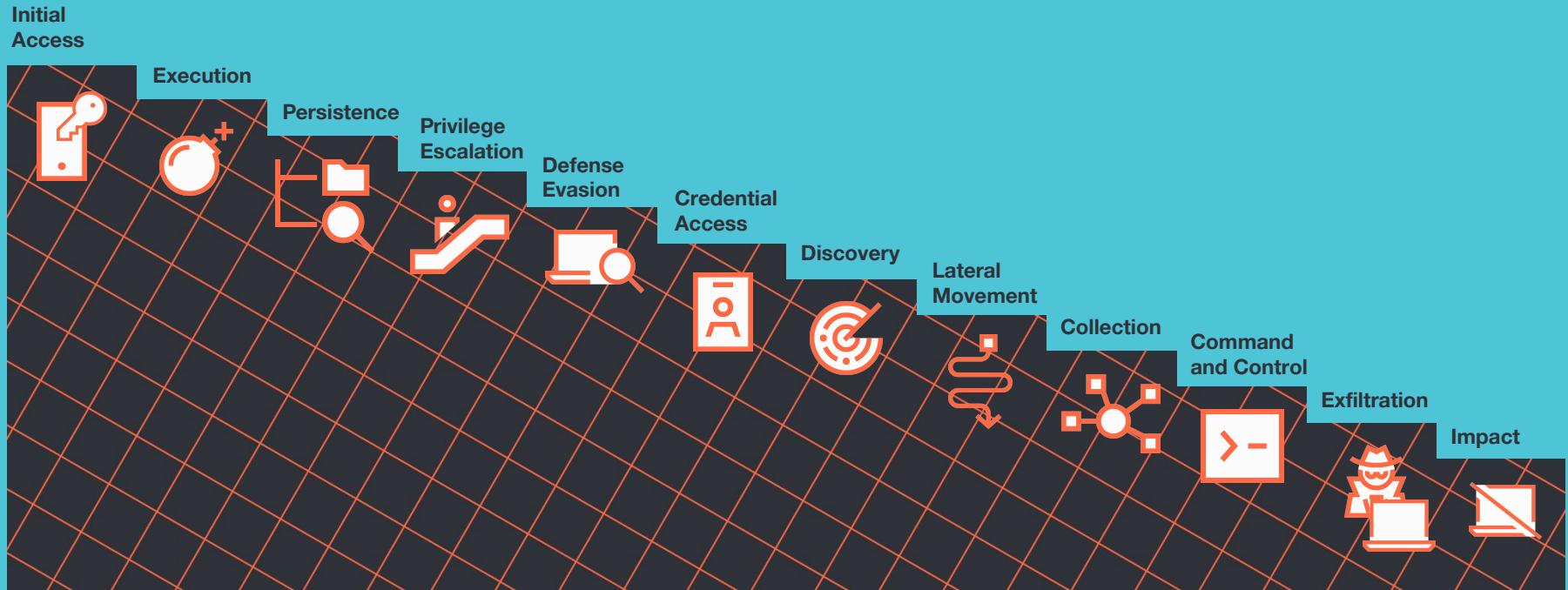
Infrastructure comparison



Infrastructure comparison



What do the kill chain phases look like now?



Recon

Traditional

- Port scanning
- Service enumeration

SaaS-native

- SaaS discovery
- Cloud identity enumeration
- SSO enumeration



Recon: SAML enumeration

Request URL:	https://api.ramp.com/v1/public/users/sso-provider?domain=test.com
Request Method:	GET
Status Code:	● 404
Remote Address:	104.18.23.203:443
Referrer Policy:	strict-origin-when-cross-origin

▼ General

Request URL:	https://api.ramp.com/v1/public/users/sso-provider?domain=webflow.com
Request Method:	GET
Status Code:	● 200
Remote Address:	104.18.22.203:443
Referrer Policy:	strict-origin-when-cross-origin

```
▼ {provider_id: "saml.okta_15464ac3-801f-4448-bb89-4fb56ccb421a"}  
  provider_id: "saml.okta_15464ac3-801f-4448-bb89-4fb56ccb421a"
```

Sign In With SSO

Enter your email address to continue.

Email Address
test@test.com

The email address you submitted is not configured to use SSO.

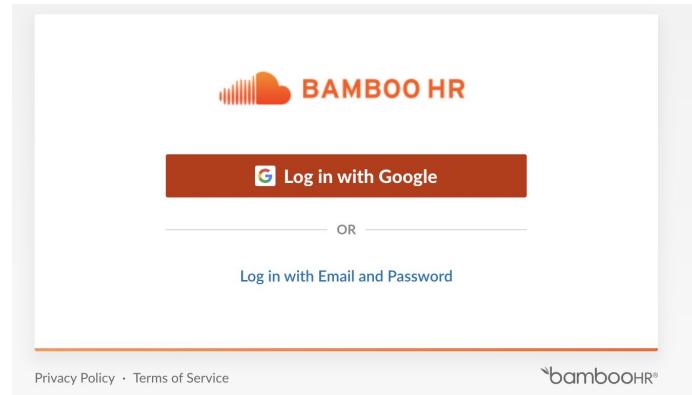
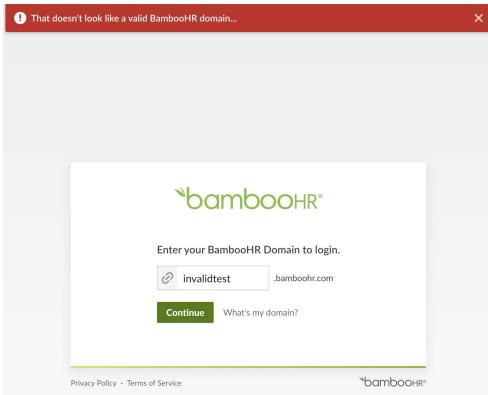
Continue

[Take me back](#)



Recon: Slug tenant enumeration

```
% curl -XGET "https://app.bamboohr.com/ajax/domain.php?test=invalidcustomer"  
{"taken":false}%  
% curl -XGET "https://app.bamboohr.com/ajax/domain.php?test=soundcloud"  
{"taken":true}%
```



Initial Access

Traditional

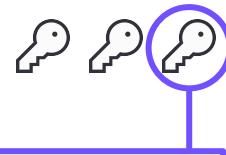
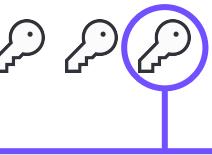
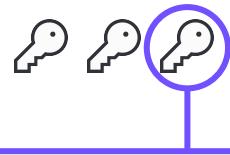
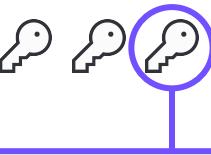
- Phishing
- Office macros
- Endpoint compromise

SaaS-native

- Credential stuffing
- (Consent + IM + AITM) phishing
- Cloud identity compromise



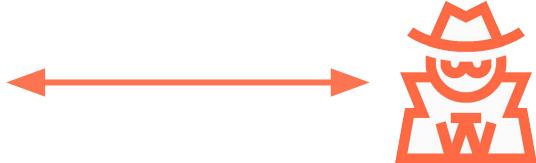
Initial access: Credential stuffing



Entirely
automated

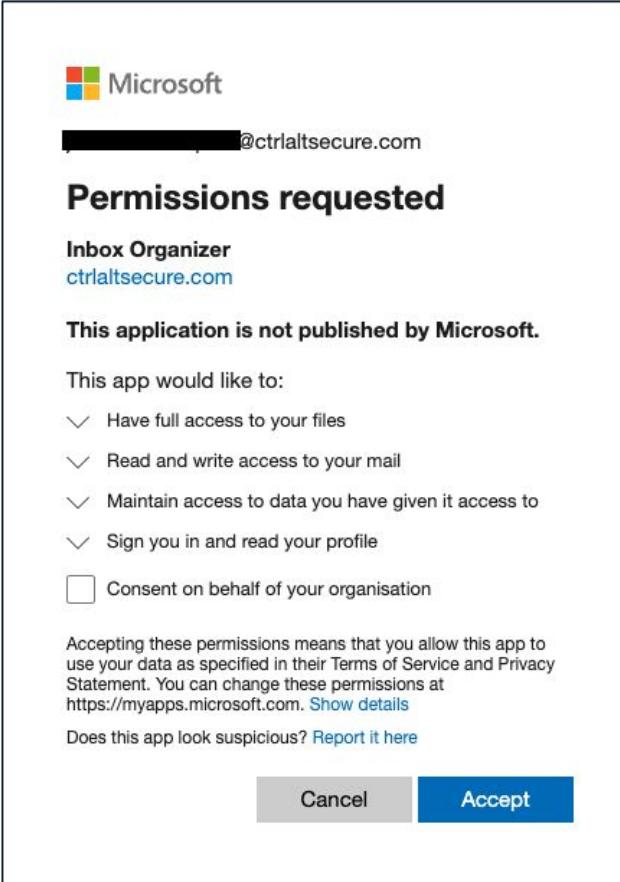
Gather credentials:

- Public breach
- Phishing
- Purchased / stolen
- Guessed



Initial access: Consent phishing

- Uses legitimate URLs
 - Grants permanent access
 - MFA provides no extra protection



Initial access: IM phishing + spoofing



A screenshot of a mobile Slack application. On the left, a dark vertical sidebar displays a context menu with options: Direct messages, Mentions & reactions, Drafts & sent, Canvases, Slack Connect (which is highlighted in orange), Files, and More. To the right, a light-colored card titled 'New invitations' shows a notification: 'You were invited to direct message with: Jeff Bezos from Amazon'. It includes a small purple profile icon with a white letter 'A', a timestamp 'Today at 19:27', and two buttons: 'Ignore' and 'Accept'.

A screenshot of a Slack channel. At the top, it asks 'Has anyone seen this?'. Below is a post from the account [pushsecurity.com](#) with the subject 'Half of account compromise attacks included malicious mail rules'. The post text states: 'Attackers routinely use mail rules to hide their attacks, exfiltrate sensitive data, and to get persistent access to victim accounts. (1 MB) ▾'. Below the text is a photograph of three people standing in front of a wall with large posters that read 'Push', 'Security', and 'Forward'. To the right of the post is a sidebar showing a profile picture of Mark Zuckerberg with the text 'Mark Zuckerberg (you) ● CEO' and a timestamp '12:06 PM local time'. There is also a 'Set a status' button.

A screenshot of a Slack channel. On the left, a message from the account [zuck](#) at 11:58 AM says 'Hey there!'. Below the messages is a text input field with placeholder text 'Jot something down' and a toolbar with various text and emoji icons.

Initial access: Poisoned tenants

- Attacker sets up a tenant
- Social engineer users to use it
- Legitimate email invites are common



Luke invited you to join "Ctrlaltsecure" [Inbox](#) [x](#)

 **Nuclino** <contact@nuclino.com> [Unsubscribe](#)
to me ▾

14:54 (0 minutes ago) [☆](#) [↶](#) [☰](#)



Luke invited you to join "Ctrlaltsecure"

Luke Jennings invited you to join team "Ctrlaltsecure" on Nuclino. Join now to bring all your knowledge, docs, and projects together and make Nuclino your team's collective brain!

[JOIN NOW](#)

[!\[\]\(67438e63ecafcf7b534ce8cebfb9cba1_img.jpg\)](#) [!\[\]\(52ba8aa9450cc0402b35b109f9fde7e9_img.jpg\)](#) [!\[\]\(65bad109385619f30aa905a0c02f9a90_img.jpg\)](#)

[Reply](#) [Forward](#)

Initial access: SAMLjacking

- Use SAML maliciously
- Redirect a legitimate SaaS login to a malicious URL

ⓘ Data for your SSO provider

Copy and paste the following data to the settings of your SSO provider during setup:

ACS URL

<https://api.nuclino.com/api/sso/2c2777fe-46ca-4ae0-8ab2-a1323c398190/acs>

COPY

Copy and paste this to the settings of your SSO provider.

Entity ID

<https://api.nuclino.com/api/sso/2c2777fe-46ca-4ae0-8ab2-a1323c398190/metadata>

COPY

Copy and paste this to the settings of your SSO provider.

ⓘ Data supplied by your SSO provider

Copy the data supplied by your SSO provider from their settings and paste it here:

SSO URL

The SAML 2.0 Endpoint URL supplied by your SSO provider.



Initial access: SAMLjacking

- Use SAML maliciously
- Redirect a legitimate SaaS login to a malicious URL



Log in to team

Log in to team Ctrlaltsecure123.

[LOG IN WITH SINGLE SIGN-ON \(SSO\)](#)

Don't have access to this team yet?
Contact the team administrator for an invitation.

[Log in without single sign-on \(SSO\)](#)

my-evil-saml-server.com

Log in to team

Log in to team Ctrlaltsecure123.

[LOG IN WITH SINGLE SIGN-ON \(SSO\)](#)

Don't have access to this team yet?
Contact the team administrator for an invitation.

[Log in without single sign-on \(SSO\)](#)

Google Sign in Use your Google Account

Email or phone

Forgot email?

Not your computer? Use Guest mode to sign in privately.
[Learn more](#)

Create account [Next](#)

English (United States) ▾ Help Privacy Terms

Attack chain

Poisoned tenant +
SAMLjacking



Create an account

Or log in with your social media account.

Persistence

Traditional

- Endpoint persistence
- Run keys
- Scheduled Tasks
- Services

SaaS-native

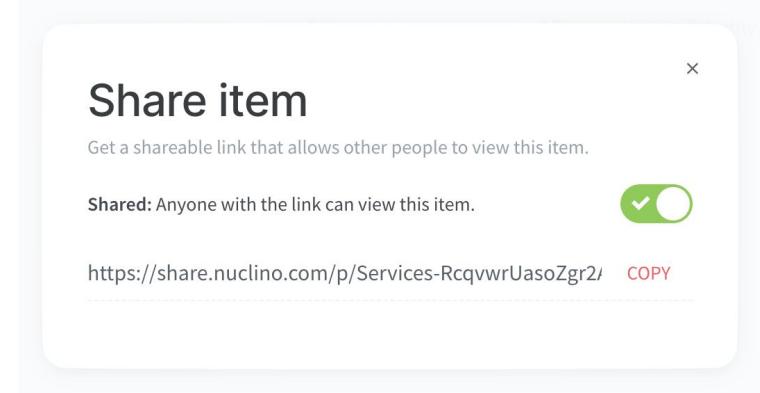
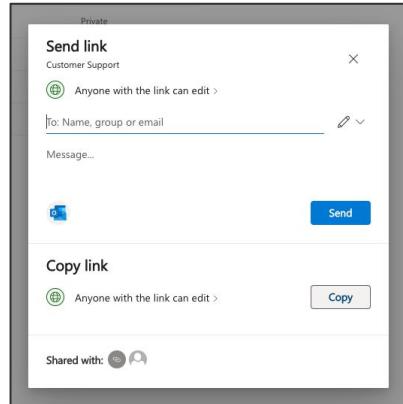
- SaaS persistence
- OAuth access
- API keys
- Link sharing
- Ghost logins
- Inbound federation



Persistence: Link sharing



Name	Modified	Modified By	File size	Sharing
Customer Support	About an hour ago	Luke Jennings	3 items	Shared
Design Documents	About an hour ago	Luke Jennings	0 items	Private
Finance	About an hour ago	Luke Jennings	0 items	Private
Git Repos	About an hour ago	Luke Jennings	0 items	Private
HR	About an hour ago	Luke Jennings	0 items	Private
Legal	About an hour ago	Luke Jennings	0 items	Private
Sales and Marketing	About an hour ago	Luke Jennings	0 items	Private
Document.docx	October 12	Guest Contributor	10.3 KB	Shared



Persistence: API keys

Settings > API Tokens

API tokens can be used to interact with the [Shortcut REST API](#). Note that when you generate a new token, the value will only be displayed once, so be sure to write it down.

 Token **backdoor :)** generated.

This is the only time this token value will be displayed:

64 [REDACTED] 42

Name	Last Used
backdoor :)	Never

Token Name

Generate Token



Persistence: Ghost logins

The screenshot shows the 'Settings > Security' page. The 'Password' tab is selected. A message box states: 'You haven't set a password yet. Setting a password will apply to all Workspaces that you are a member of.' Below this is a 'Set Password' input field with a redacted password and a 'Set Password' button.

Linked accounts

You can use these to quickly log into your IFTTT account. [Learn more](#)



Apple is not linked

[Link your account](#)



Facebook is not linked

[Link your account](#)



Google is linked

[Unlink](#)

The screenshot shows the 'Secondary Logins' page. It lists two entries:

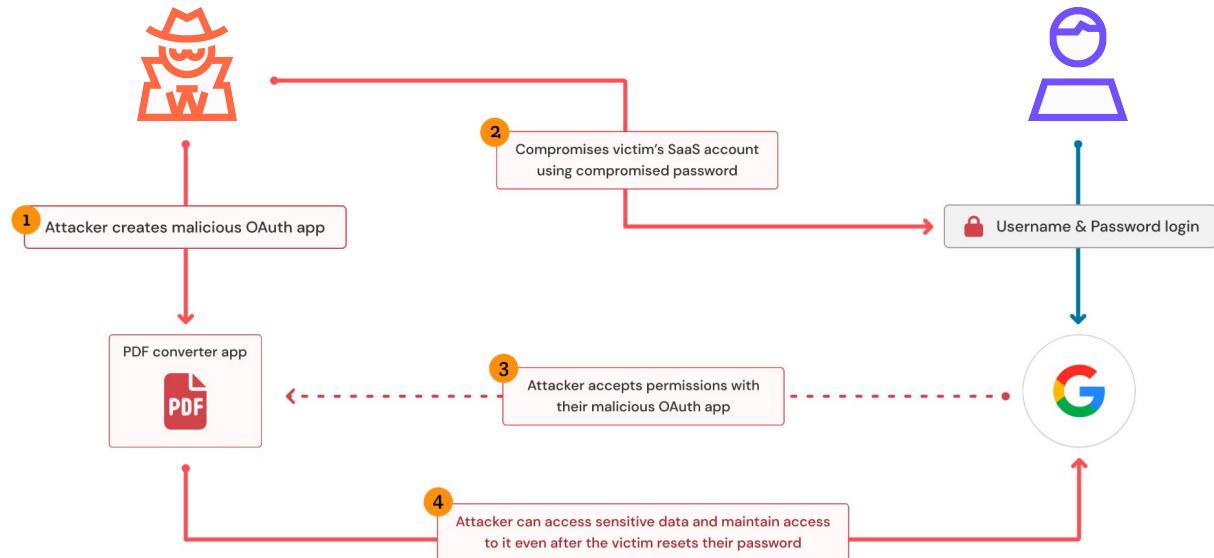
ACCESS	LOGIN	TYPE
expensify.com	luke.jennings@ctrlaltsecure.com	primary
expensify.com	lukejennings1000@gmail.com	secondary

At the bottom right are buttons for 'Make Primary' and 'Remove'.



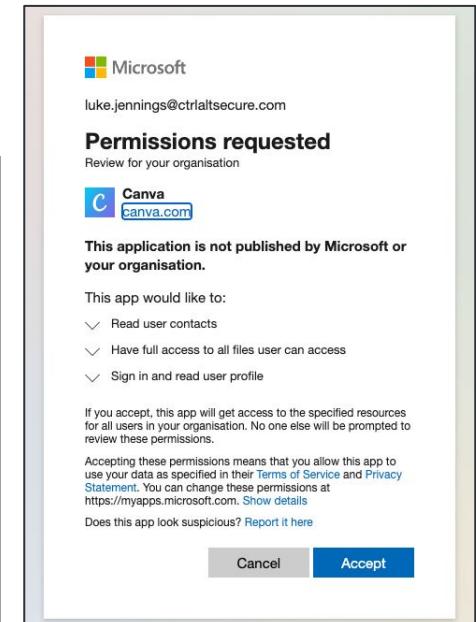
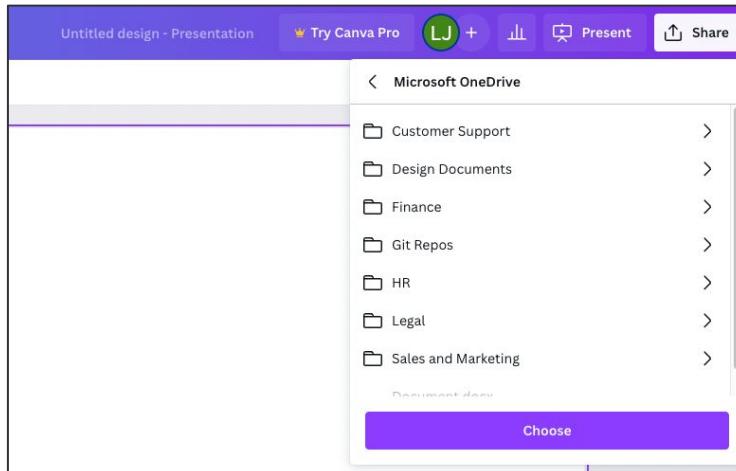
Persistence: OAuth integrations

- Custom OAuth apps
- Legit SaaS apps
- Impersonate client-side apps



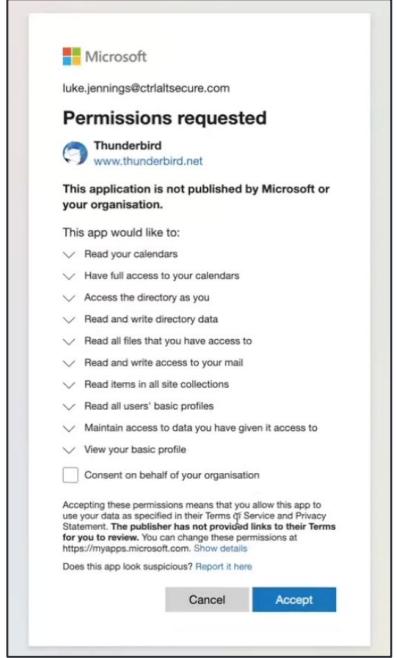
Persistence: OAuth integrations

- Custom OAuth apps
- Legit SaaS apps
- Impersonate client-side apps



Persistence: OAuth integrations

- Custom OAuth apps
- Legit SaaS apps
- Impersonate client-side apps



```
73 * For the moment these details are hard-coded, since dynamic client
74 * registration is not yet supported. Don't copy these values for your
75 * own application - register one for yourself! This code (and possibly even the
76 * registration itself) will disappear when this is switched to dynamic
77 * client registration.
78 */
79 var kIssuers = new Map([
80   [
81     "accounts.google.com",
82     {
83       clientId:
84         "406964657835-aq8lmia8j95dhlia2vharmfk3t1hgqj.apps.googleusercontent.com",
85       clientSecret: "kSmqreRr0qBWJgbf5Y-PjSU",
86       authorizationEndpoint: "https://accounts.google.com/o/oauth2/auth",
87       tokenEndpoint: "https://www.googleapis.com/oauth2/v3/token",
88     },
89   ],
90 ]);
```

```
127.0.0.1 -- [21/Nov/2022 12:25:23] "GET /graphcall HTTP/1.1" 200 -
[*] Using token for 08162f7c-0fd2-4200-a84a-f25a4db0b584 (Thunderbird)
[*] Scopes available - Calendars.Read Calendars.ReadWrite Directory.AccessAsUser.All Directory.ReadWrite.All Files.Read.All
IMAP.AccessAsUser.All Mail.ReadWrite openid POP.AccessAsUser.All profile Sites.Read.All SMTP.Send User.ReadBasic.All email
[*] Enumerating OneDrive root folder
[*] Calling https://graph.microsoft.com/v1.0/me/drive/root/children
(Folder) Customer Support
(Folder) Design Documents
(Folder) Finance
(Folder) Git Repos
(Folder) HR
(Folder) Legal
(Folder) Sales and Marketing
(File) Document.docx
127.0.0.1 -- [21/Nov/2022 12:25:23] "GET /graphcall HTTP/1.1" 200 -
```



Execution

Traditional

- Native code
- Memory-resident implants
- Offensive powershell

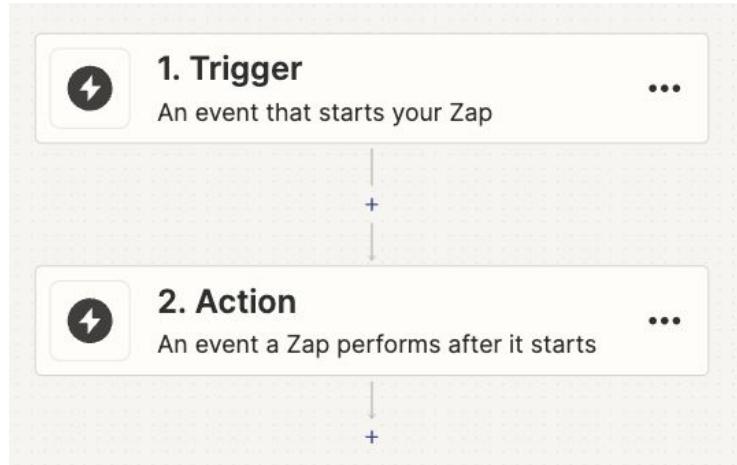
SaaS-native

- Automation workflows
- No-code/low-code
- OAuth tokens/
API access



Execution: Shadow workflows

- The most “code-execution-like” technique
- The offensive powershell of SaaS
- Scattered Spider/OctoTempest seen using FiveTran



A screenshot of the Zapier "Change trigger" screen. At the top, it says "Change trigger" and "A trigger is an event that starts your Zap". Below is a search bar with the placeholder "Search...". A grid of trigger options is shown, including Google Calendar, Google Contacts, Google Docs, Google Drive, Gmail, Google Sheets, Google Slides, Microsoft Outlook, OneDrive, and Email by Zapier. Below the grid, it says "...and over 5,000+ more". To the right, there are sections for "Built-in tools" (Tables, Schedule, Webhook), each with a brief description and a "Learn more" button.

Defense evasion: Evil twin integrations

- Integrate an app that's already in use
- Avoid detection of:
 - New OAuth integrations
 - New user consents

Core Directory	ApplicationManagement	Consent to application	Success	Zapier To Do
Core Directory	UserManagement	Add app role assignment g...	Success	Zapier To Do, luke.jennings...
Core Directory	ApplicationManagement	Add delegated permission ...	Success	Microsoft Graph, 8d2f8b13...



Attack chain

Shadow workflows +
evil twin integration



Requirement	Initial Answer	Execution	Performance	Module Specialization	Delivery Options	Customer Answer
OAuth 2.0 support	Custom protocol	Standard interface	Very fast	User monitoring	API keys	Protocol monitoring
Robustness	Protocol analysis	Custom library	OAuth tokens	OAuth monitoring	Custom tokens	API token management
Integration	Standard protocols	Open API	Fast	Multiple protocols	Cloud integration	
Modular architecture	Microservices	Open API monitoring	Fast fail	Multiple protocols	Cloud integration	
JSON web token support	Protocol analysis	Microservices	Fast fail	Multiple protocols	Cloud integration	
Universal interface	Customized API	REST API	Fast fail	OAuth monitoring	Cloud integration	
API monitoring	Protocol analysis	Protocol analysis	Fast fail	Protocol analysis	Cloud integration	
Config persistence	Cloud storage	Cloud storage	Fast fail	Cloud storage	Cloud integration	
API grouping	Protocol analysis	Cloud storage	Fast fail	Cloud storage	Cloud integration	
API versioning	Protocol analysis	Protocol analysis	Fast fail	Protocol analysis	Cloud integration	
API security	Protocol analysis	Protocol analysis	Fast fail	Protocol analysis	Cloud integration	

Lateral movement

Traditional

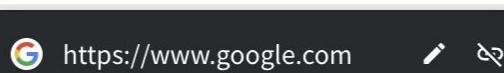
- Endpoint/Server #1 → Endpoint/Server #2
- Credential dumping
- Remote service creation
- Software deployment tools

SaaS-native

- SaaS app #1 → SaaS app #2
- Link backdooring
- Account recovery
- Abusing existing integrations



Lateral movement: Link backdooring



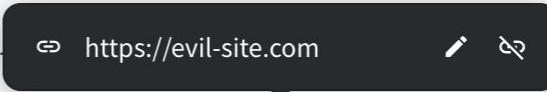
Links can be embedded with text like [this](#).

Or you can fake the link itself <https://www.google.com>

And you can be sneakier and abuse the limited link preview size to fake a link to
<https://internal-sharepoint-server.legitcompany.com/>



Lateral movement: Link backdooring

Links can be embedded with  ↗ <https://evil-site.com>

Or you can fake the link itself <https://www.google.com>

And you can be sneakier and abuse the limited link preview size to fake a link to <https://internal-sharepoint-server.legitcompany.com/>



Lateral movement: Link backdooring

<https://internal-sharepoint-server.legitcompany.com.myevildomain.com/>

Links can be embedded with text like this.

Or you can fake the link itself <https://www.google.com>

 <https://internal-sharepoint-server.legitcompany.com.myevildomain.com/>  

And you can be sneaky and abuse the limited link preview size to fake a link to
<https://internal-sharepoint-server.legitcompany.com/>



Lateral movement: Account recovery

New password

Confirm password

Reset password

Log in to Canva

Welcome back! Enter this code within the next 10 minutes to log in:

388271

This email's meant for your eyes only! If someone's asked you to share this email or code with them, or if you think you received this by mistake, [please report it](#).

 Made for you with ❤️ from Canva
Canva®, 110 Kippax St, NSW 2010, Australia

IFTTT <mail@ifttt.com>
to luke-low-priv2 ▾

Hi lukelowpriv2,

We received a request to reset your IFTTT account password.

To reset your password, click the link below. If you did not make the request, please ignore this email.

Reset your password



Lateral movement: Abuse existing integrations



Apps

Search apps + Add connection

App	Connections	Zaps	Action
Gmail	1	1	>
Google Drive	1	1	>
Microsoft Outlook	1	1	>
OneDrive	1	1	>

Untitled design - Presentation 🎉 Try Canva Pro LJ + ⌂ Present ⌂ Share

Microsoft OneDrive

- Customer Support >
- Design Documents >
- Finance >
- Git Repos >
- HR >
- Legal >
- Sales and Marketing >

Document.docx

Choose

<https://github.com/pushsecurity/saas-attacks>

Introducing the SaaS attack matrix

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration
SAML enumeration	Consent phishing	Shadow workflows	API keys	Link backdooring	API keys	Password scraping	Email discovery	Link backdooring	Takeout services
Subdomain tenant discover	Poisoned tenants	OAuth tokens	OAuth tokens	Abuse existing OAuth integrations	OAuth tokens	API secret theft	App user directory lookup	Abuse existing OAuth integrations	Webhooks
Slug tenant enumeration	SAML jacking	Client-side app spoofing	Evil twin integrations	Malicious mail rules	Evil twin integrations		OAuth token enumeration	API secret theft	Shadow workflows
DNS reconnaissance	Account ambushing		Malicious mail rules		Malicious mail rules			Passwordless logins	
Username enumeration	Credential stuffing		Link sharing		Link sharing			Account recovery	
	App spraying		System integrations		System integrations			In-app phishing	
	Email phishing		Ghost logins		Ghost logins			IM user spoofing	
	IM phishing		Client-side app spoofing		Client-side app spoofing			Automation workflow sharing	
	IM user spoofing								
	nOAuth								
	MFA fatigue								



Introducing the SaaS attack matrix

Ghost logins

ID: SAT1017

Tactics

- Persistence
- Defense Evasion

Summary

A common SaaS app feature allows logins to the same account using multiple methods simultaneously – for example, a standard password-based authentication (local to the SaaS app) and an SSO mechanism, such as an OIDC social login or SAML login.

If an adversary gains access to a SaaS account temporarily, they can configure an alternative authentication method to maintain access to the account, alongside the legitimate user. If the user uses a social login to access the account, an adversary may be able to configure a separate username/password login to access the account or even (though much less commonly) connect a second social account that the adversary controls.

This allows the adversary to maintain persistent access to the user account even in the event of password changes or MFA changes.

This attack will go unnoticed if the victim organization relies on SSO logs for auditing access to SaaS applications. The attack bypasses SSO as the login remains local to the SaaS app or, in the case of an OIDC SSO login, the adversary's own social account.

Examples

- [Shortcut](#)
- [Expensify](#)

References

- [MITRE ATT&CK - Use Alternate Authentication Material](#)

Inbound federation

ID: SAT1041

Tactics

- Persistence
- Lateral Movement

Summary

Inbound federation allows users to login to a target identity provider by authenticating with a source identity provider. This is often used in scenarios that involve multiple large divisions that form part of a larger parent, such as with conglomerates or during mergers and acquisitions.

An adversary who has gained administrative control of an application, such as a core identity provider, can use this to both maintain persistent access as well as effectively laterally move to other user accounts by authenticating against an identity provider they control and having those accounts mapped automatically to existing accounts on the target identity provider.

This shares similarities with [ghost logins](#), but affects all users of an application instead of being tied specifically to one user account.

Examples

- [Okta](#)

References

- [Okta Cross-Tenant Impersonation](#)



Introducing the SaaS attack matrix

Original research SaaS attack methods

Oktajacking

In this article, we'll show you how to use Okta to do keylogging for you, without needing to have your own malicious domain hosting your malicious SAML server.

Luke Dec 6, 2023

[Read more →](#)

Identity security Original research

Abusing Okta's SWA authentication

We'll cover the implications of using Okta's SWA authentication method. Learn what security teams need to know in an account breach and IR scenario.

Abusing Okta's SWA authentication

Luke Nov 30, 2023

[Read more →](#)

Original research SaaS attack methods

Slack Attack: A phisher's guide to initial access

In this article, we'll demonstrate how IM apps, specifically Slack, are an increasingly attractive target for a range of phishing & social engineering attacks.

Luke Oct 24, 2023

[Read more →](#)

Original research SaaS attack methods

Slack Attack: A phisher's guide to persistence and lateral movement

In this post, we're going to demonstrate how to phish via Slack to gain persistence and move laterally.

Luke Oct 24, 2023

[Read more →](#)

Original research SaaS attack methods

Phishing Microsoft Teams for initial access

In this article, we will cover a number of spoofing and phishing strategies that can be employed by external attackers to target an organization using Teams.

Luke Jan 23, 2024

[Read more →](#)

OAuth SaaS attack methods

SAMLjacking a poisoned tenant

In this article, we're going to demo combining two of our favorite new SaaS attack techniques to make a simple, but effective attack chain.

SAMLjacking a poisoned tenant

Luke Aug 17, 2023

[Read more →](#)

OAuth SaaS attack methods

The shadow workflow's evil twin: A nearly invisible attack chain

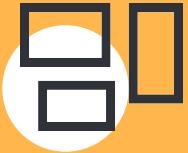
In this article, we're going to demonstrate how combining two of our favorite new SaaS attack techniques makes a simple, but very stealthy persistence approach.

Luke Sep 11, 2023

[Read more →](#)



Key Takeaways



The world is already hybrid SaaS and increasingly SaaS-native



There are many SaaS-orientated attack techniques that do not require endpoint compromises



Even in a traditional endpoint compromise scenario, SaaS opens up a whole new world of persistence



If you're a red/blue teamer, the SaaS attacks matrix can help you

Key Takeaways

- This space is evolving rapidly
- “Real” threat actors are now moving in this space
- Scattered Spider/OctoTempest
- Midnight Blizzard/APT29





Thank you.

For more information, check out

<https://pushsecurity.com>

<https://github.com/pushsecurity/saas-attacks>

