Push

Understanding the new SaaS cyber kill chain

Luke Jennings

- Red teaming + offensive security research

- EDR design + threat hunting research

- Identity and SaaS security research

AGENDA

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

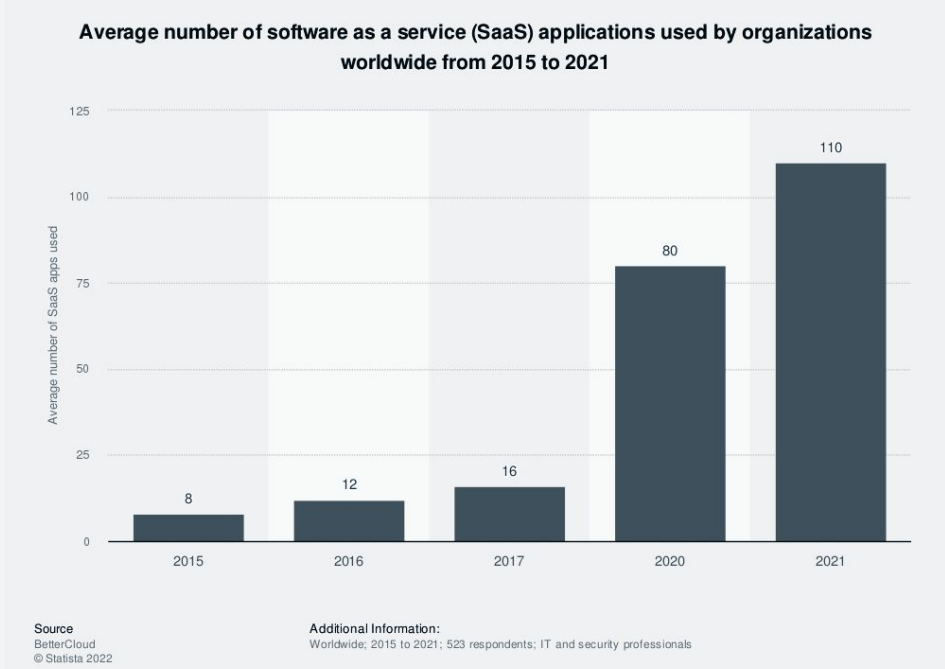
Technological shifts

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

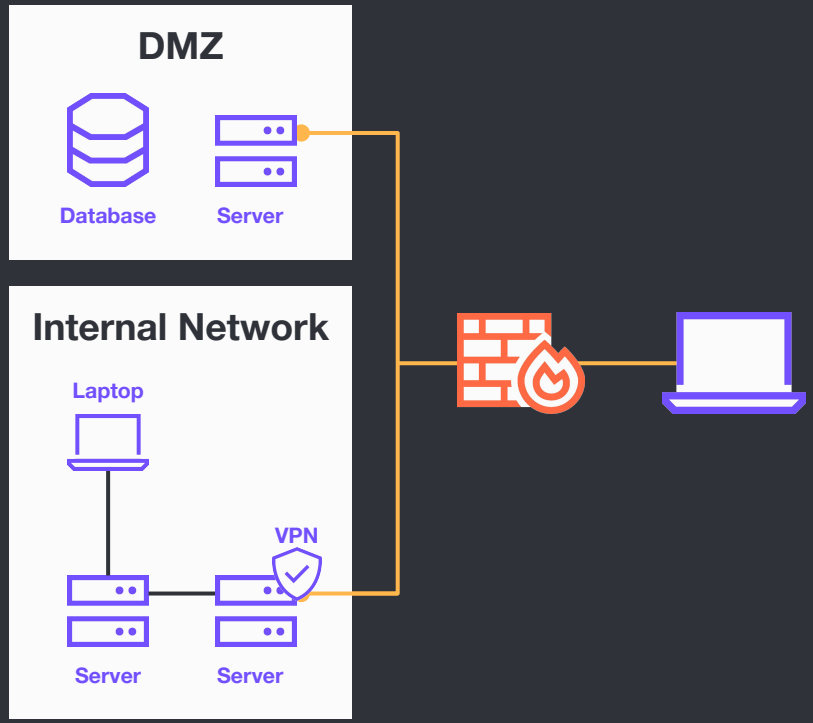
SaaS adoption

- 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

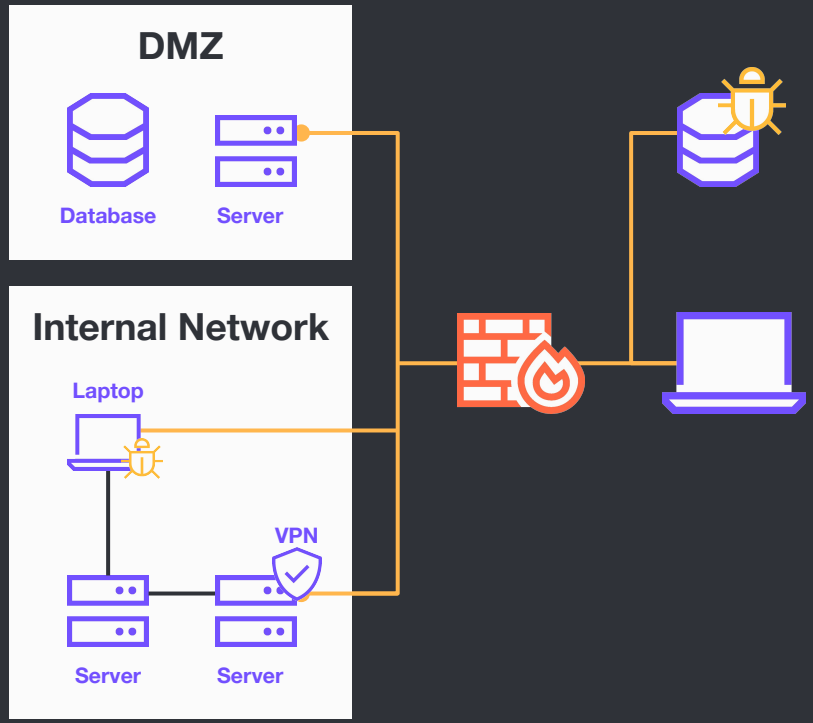
80% of workers admit to using SaaS applications at work without getting approval from IT.



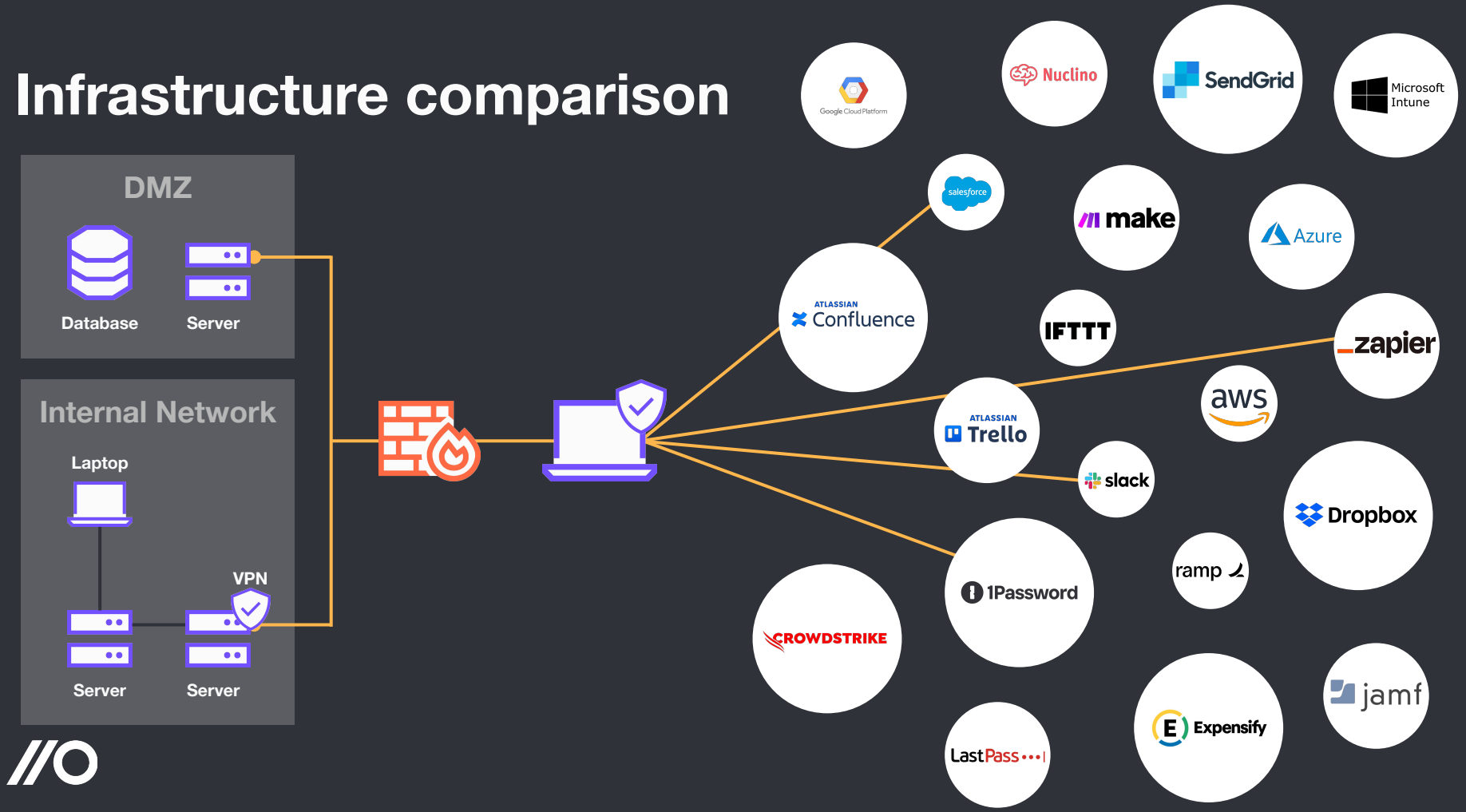
Infrastructure comparison



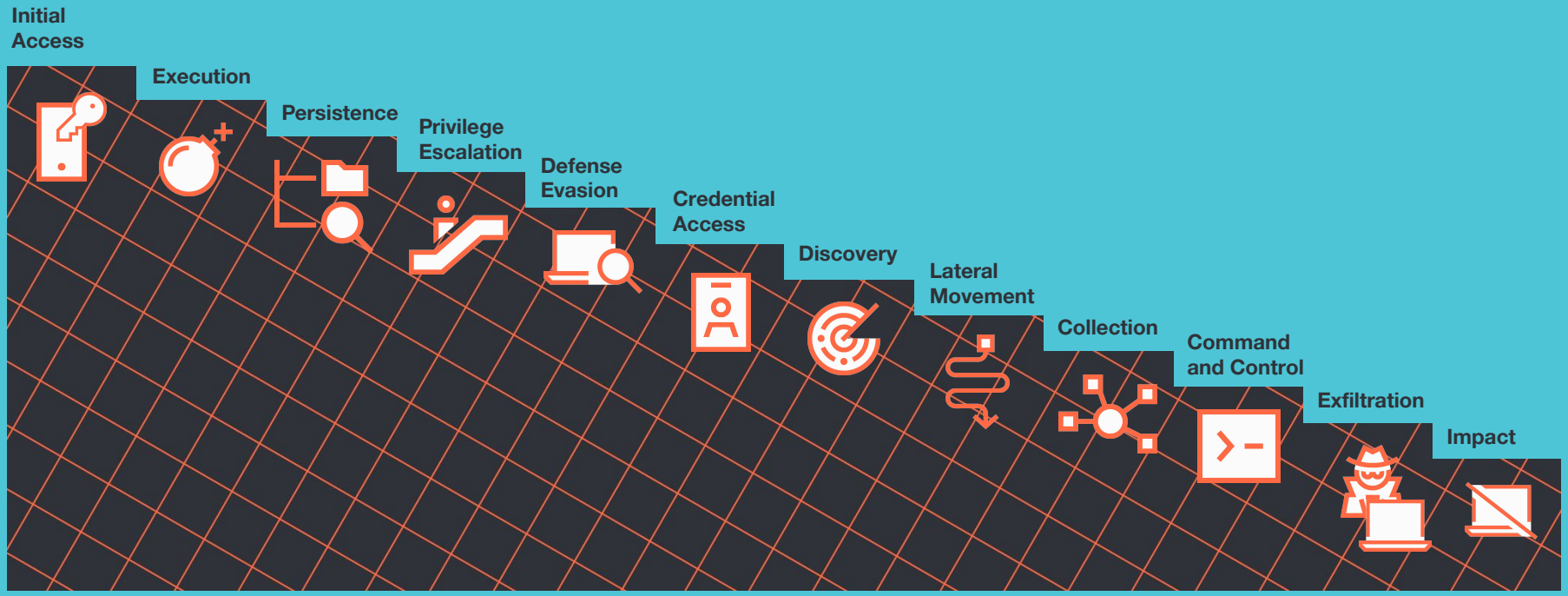
Infrastructure comparison



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

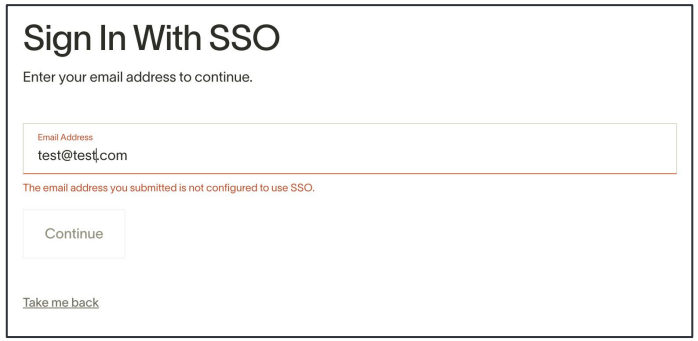
Recon: SAML enumeration

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

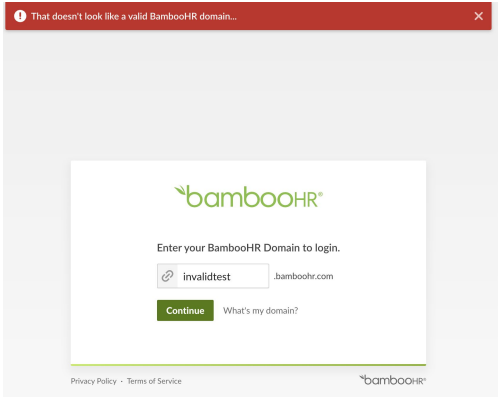
Request URL:	https://api.ramp.com/v1/public/users/sso-provider?domain=webflow.com
Request Method:	GET
Status Code:	200
Remote Address:	104.18.22.203:443
Referrer Policy:	strict-origin-when-cross-origin

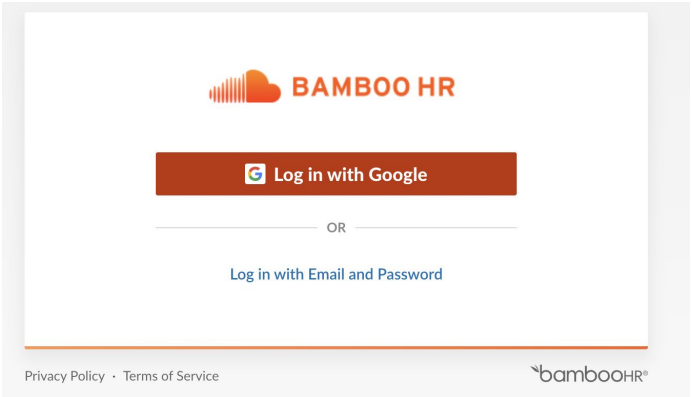
▼ {provider_id: "saml.okta_15464ac3-801f-4448-bb89-4fb56ccb421a"}
provider_id: "saml.okta_15464ac3-801f-4448-bb89-4fb56ccb421a"



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

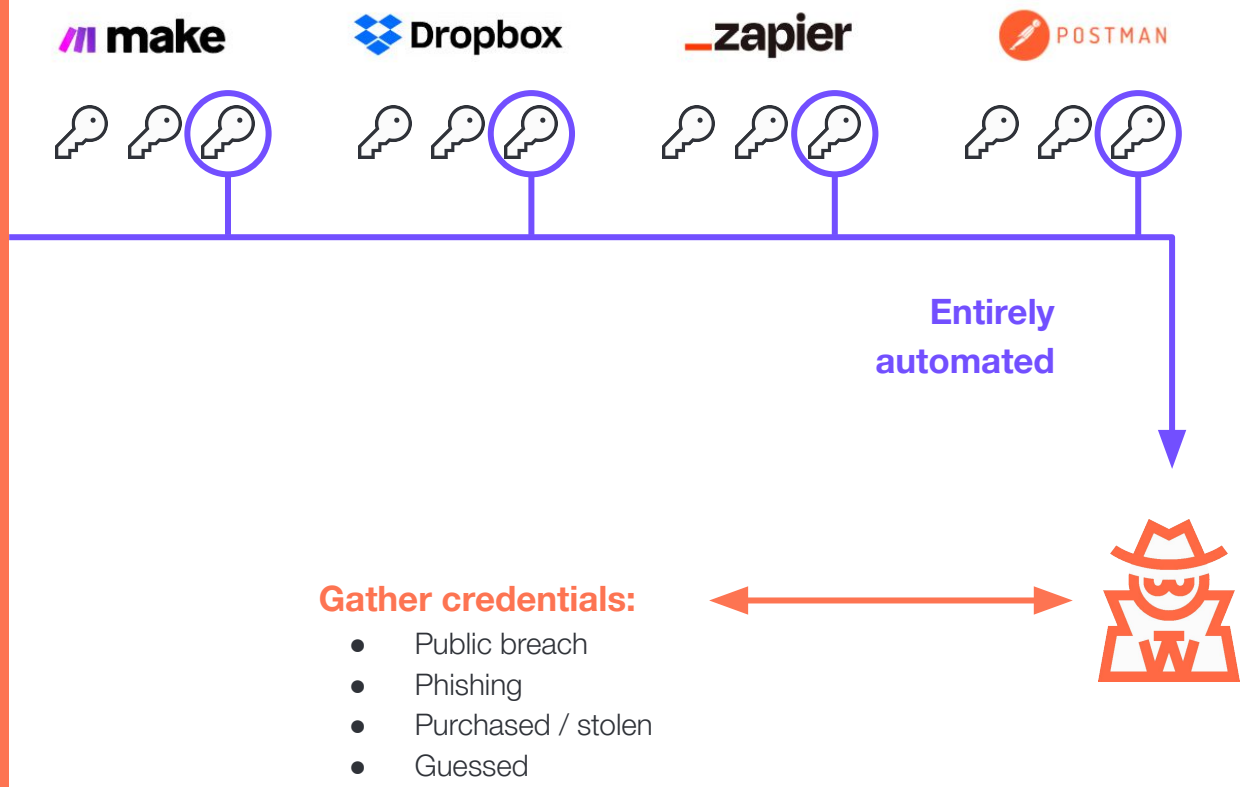
Traditional

- Phishing
- Office macros
- Endpoint compromise

SaaS-native

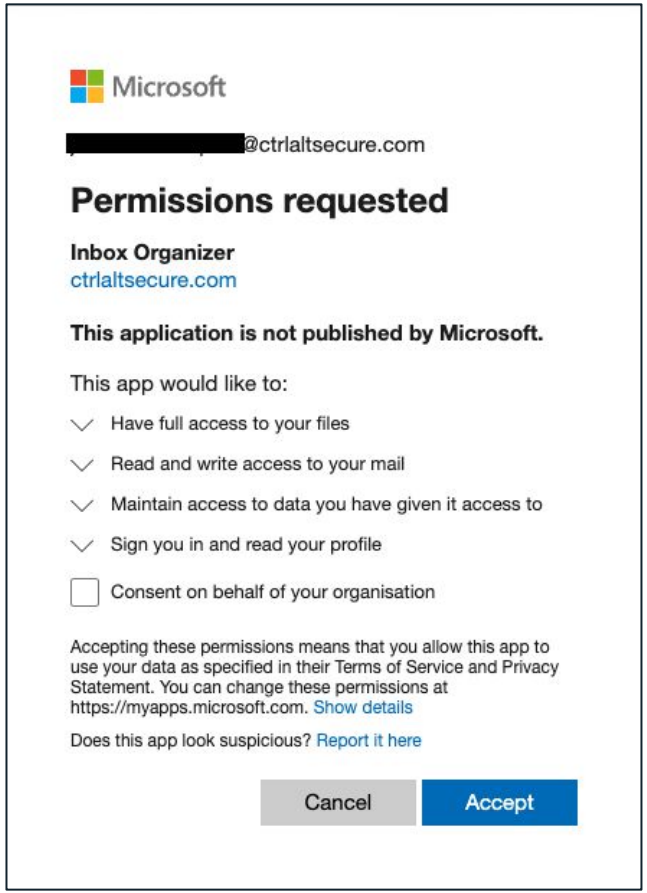
- Credential stuffing
- (Consent + IM + AITM) phishing
- Cloud identity compromise

Initial access: Credential stuffing

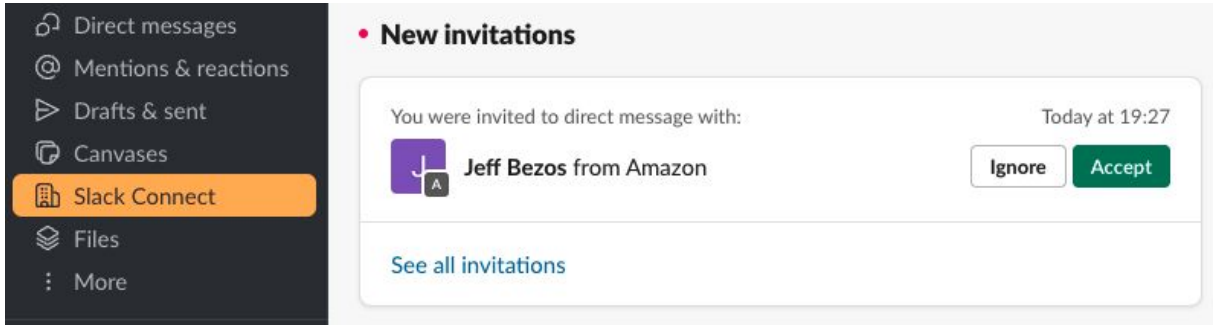


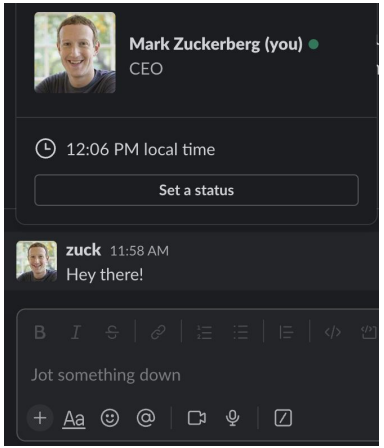
Initial access: Consent phishing

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



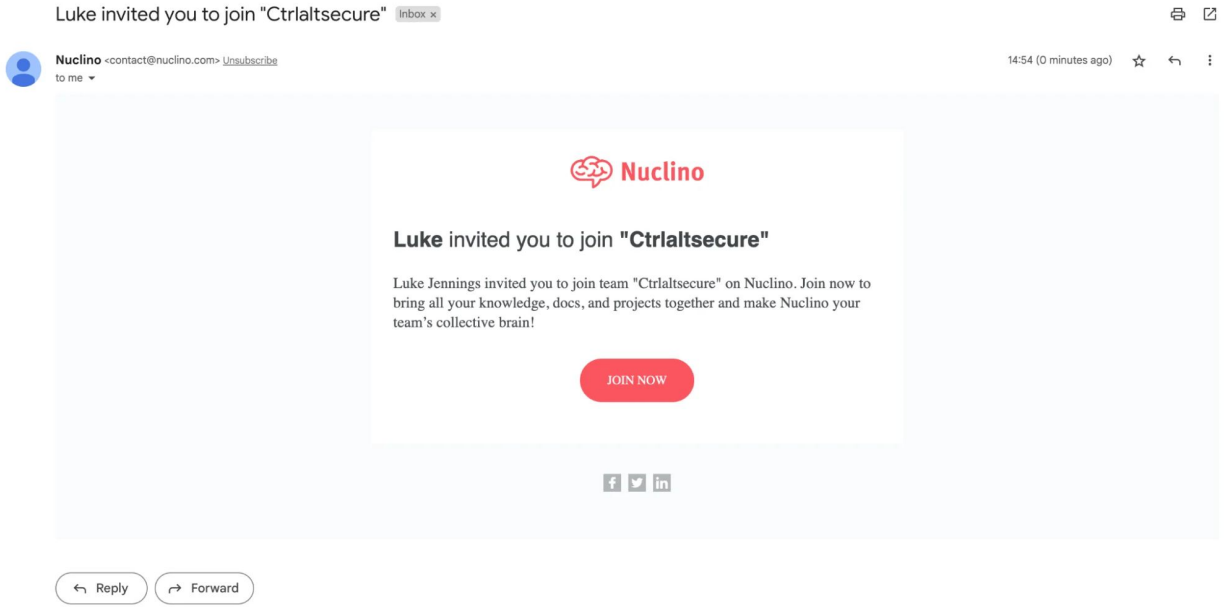
Initial access: IM phishing + spoofing





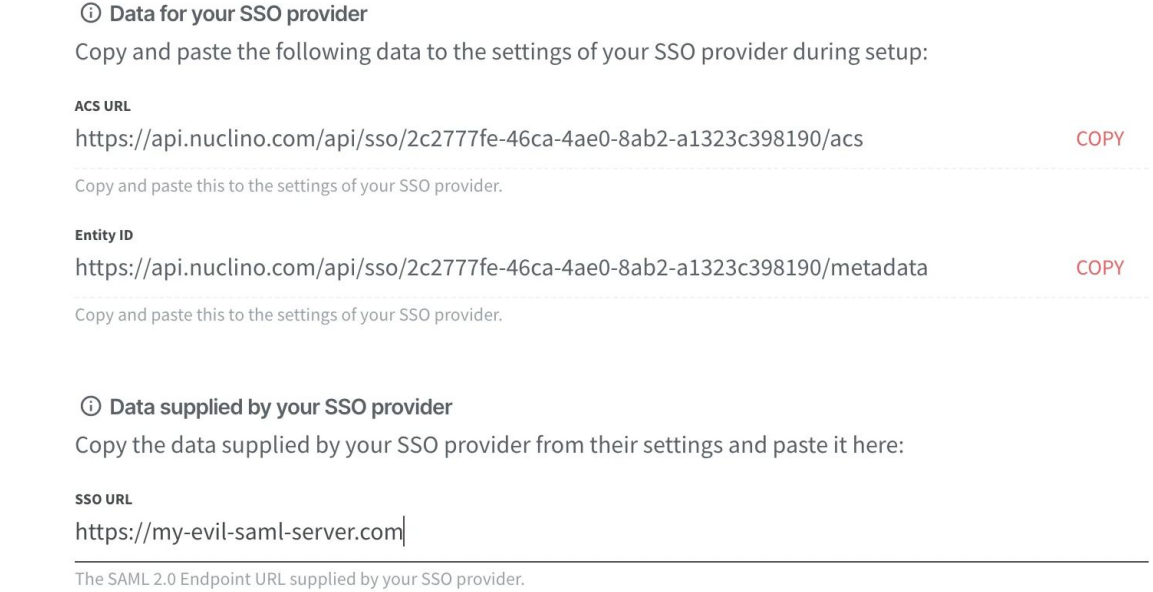
Initial access: Poisoned tenants

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



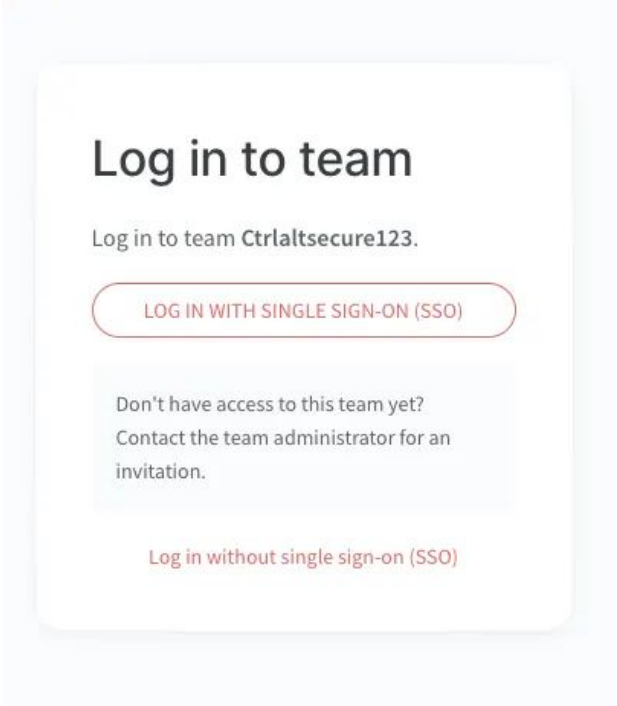
Initial access: SAMLjacking

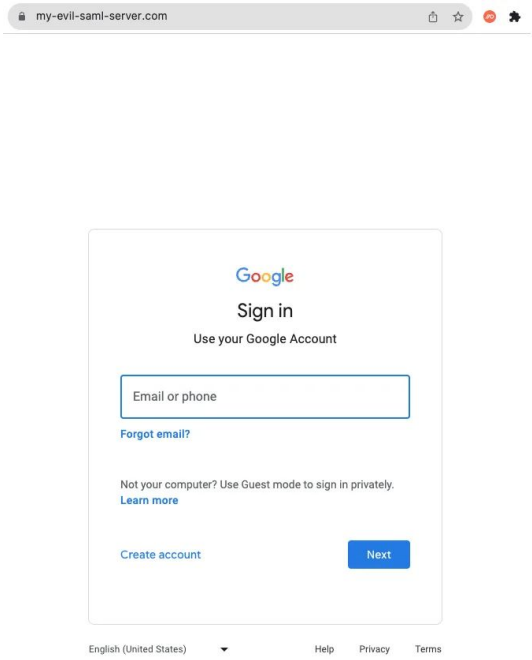
- Use SAML maliciously
- Redirect a legitimate SaaS login to a malicious URL



Initial access: SAMLjacking

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





Attack chain

Poisoned tenant + SAMLjacking


Create an account

Persistence

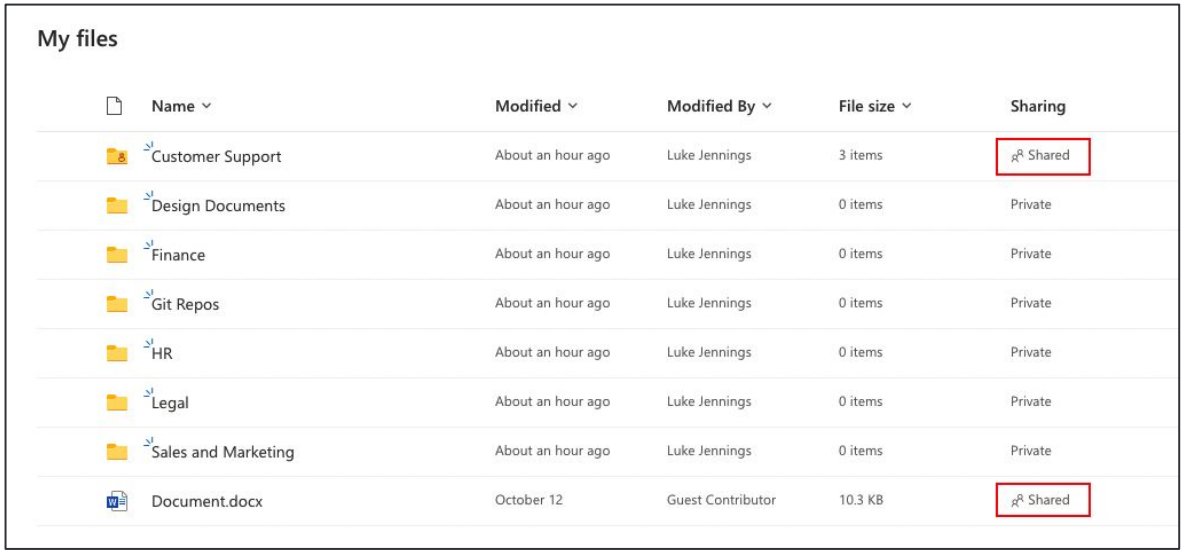
Traditional

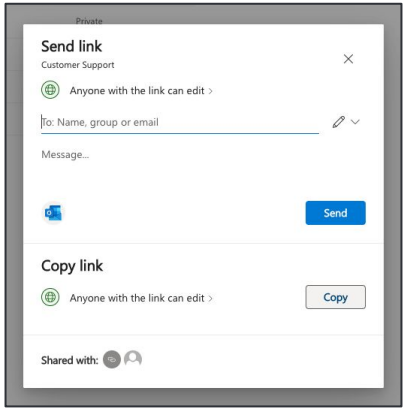
- Endpoint persistence
- Run keys
- Scheduled Tasks
- Services

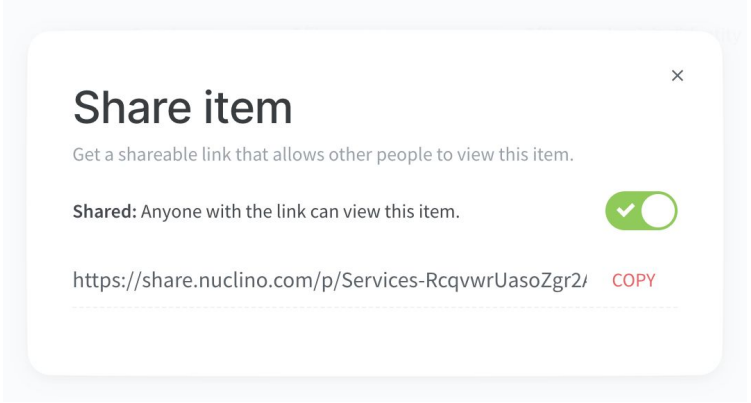
SaaS-native

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

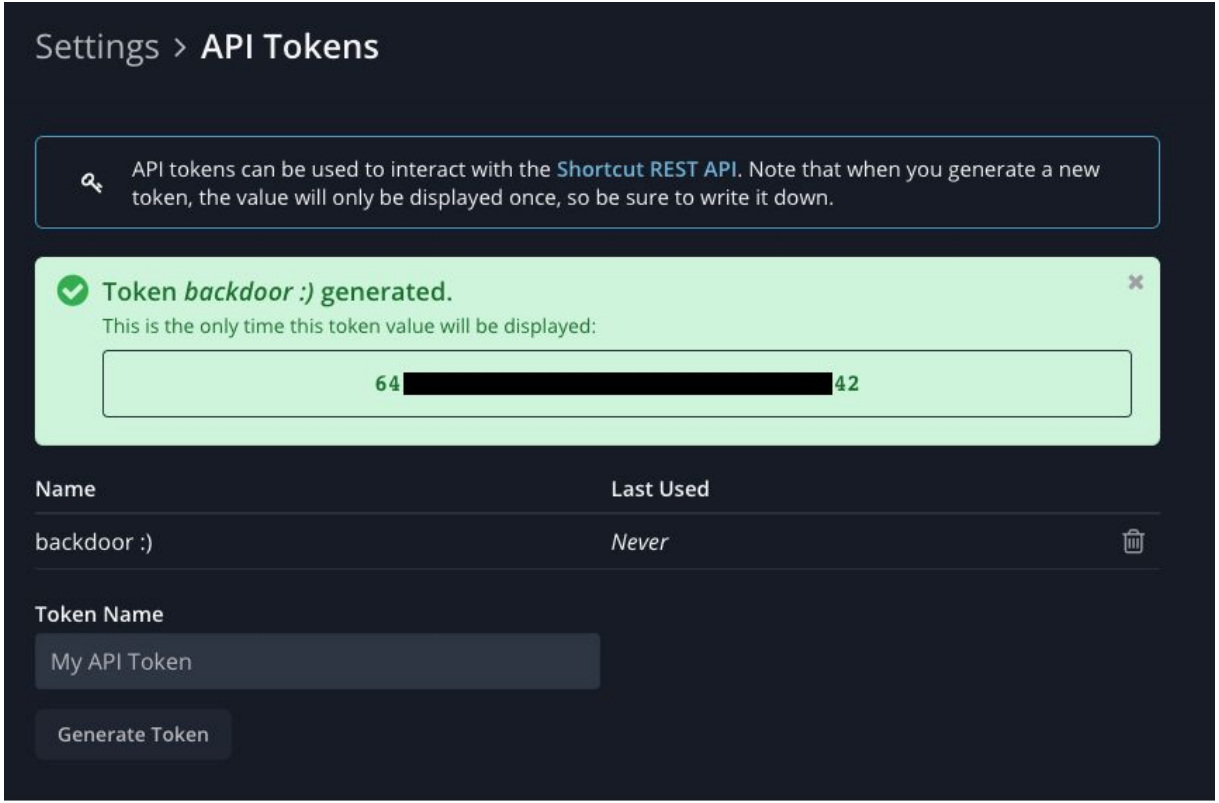
Persistence:
Link sharing



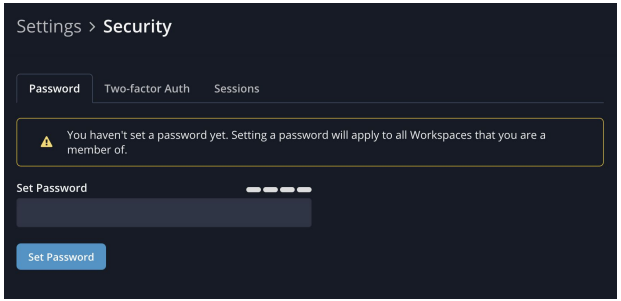


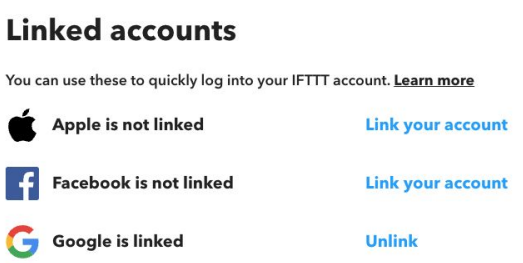


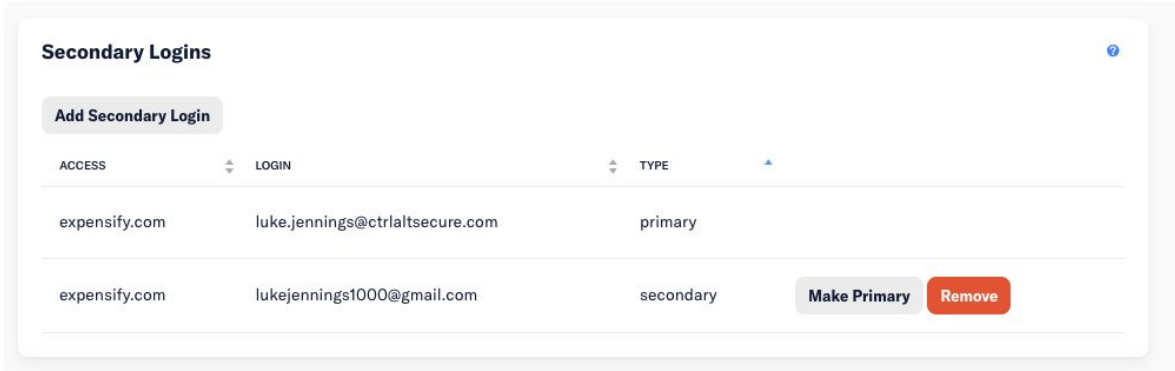
Persistence: API keys



Persistence: Ghost logins

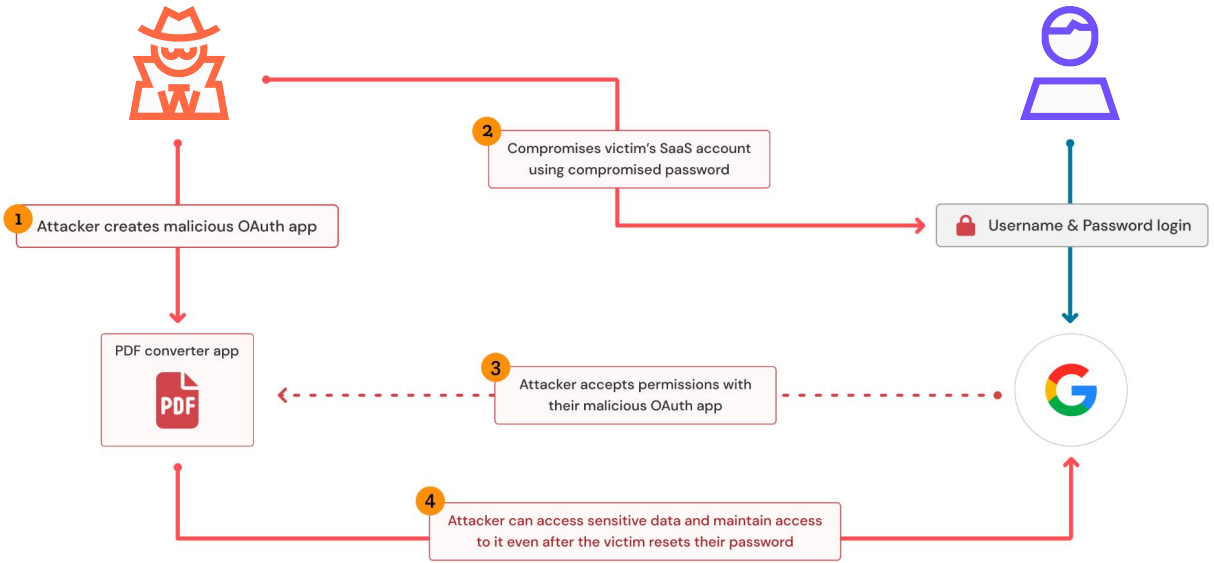






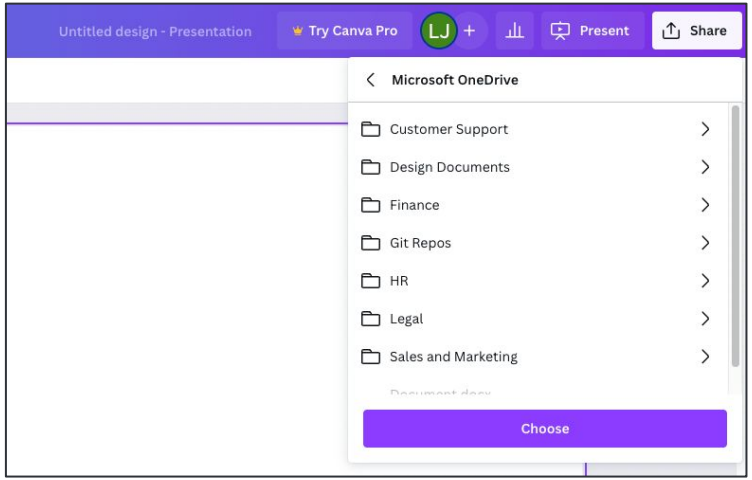
Persistence: OAuth integrations

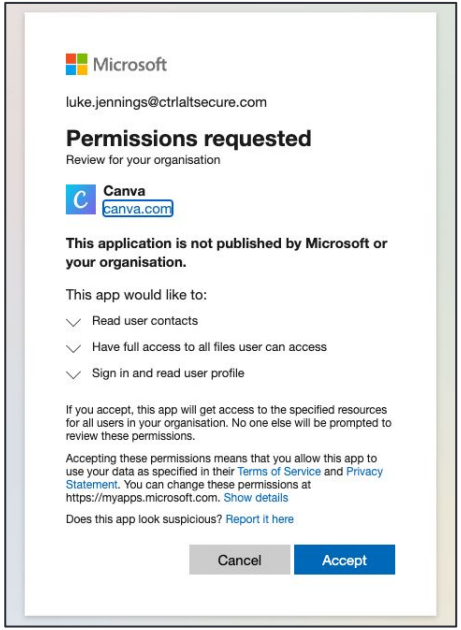
- Custom OAuth apps
- Legit SaaS apps
- Impersonate client-side apps



Persistence: OAuth integrations

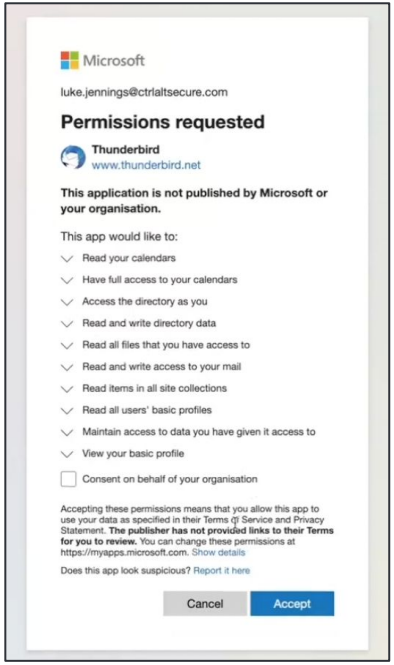
- Custom OAuth apps
- Legit SaaS apps
- Impersonate client-side apps





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-aq8lmia8j95dhl1a2bvharmfk3t1hgqj.apps.googleusercontent.com",
85        clientSecret: "kSmqreRr0qwBWJgbf5Y-PjSU",
86        authorizationEndpoint: "https://accounts.google.com/o/oauth2/auth",
87        tokenEndpoint: "https://www.googleapis.com/oauth2/v3/token",
88      },
89    ],
```

```
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

Power Automate

Retool

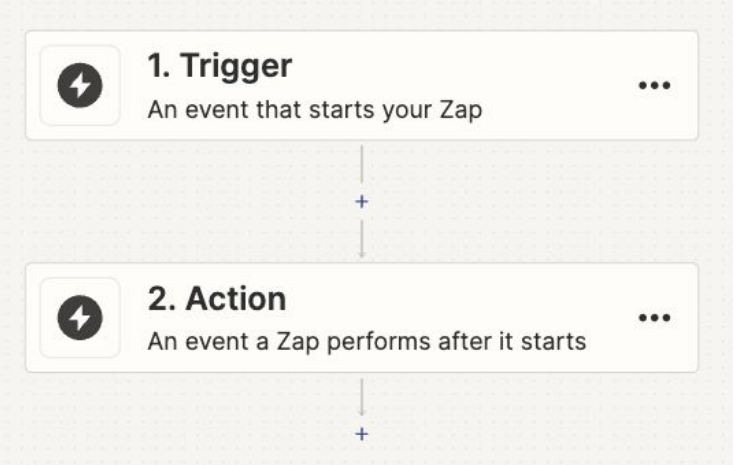
zapier

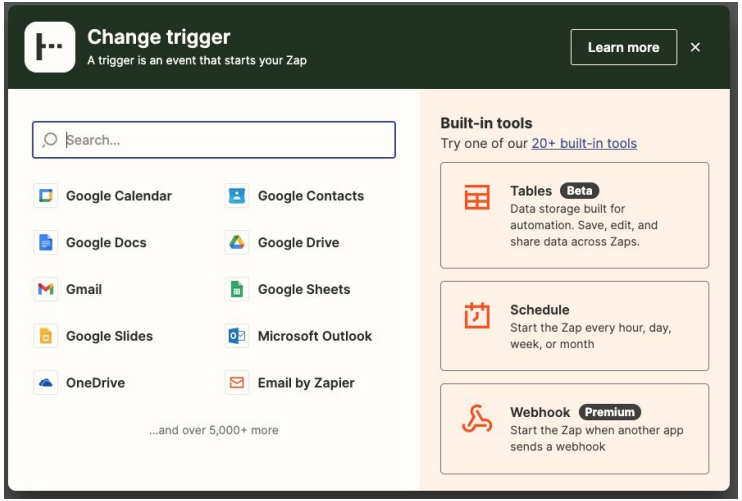
make

tines

IFTTT

Fivetran





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

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
SAML enumeration	Domain phishing	Shadow extension	API keys	Link hijacking	API keys	Password scraping
Subdomain tenant discovery	Password sprays	OAuth abuse	SAML tokens	Abuse existing OAuth integrations	OAuth tokens	API secret theft
Bug bounty enumeration	SAML spoofing	Client-side app spoofing	Evil twin integrations	Malicious mail rules	Evil twin integrations	
DNS reconnaissance	Account onboarding		Malicious mail rules		Malicious mail rules	
Username enumeration	Credential stuffing		Link sharing		Link sharing	
	App spoofing		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	
	MDaaS					

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/

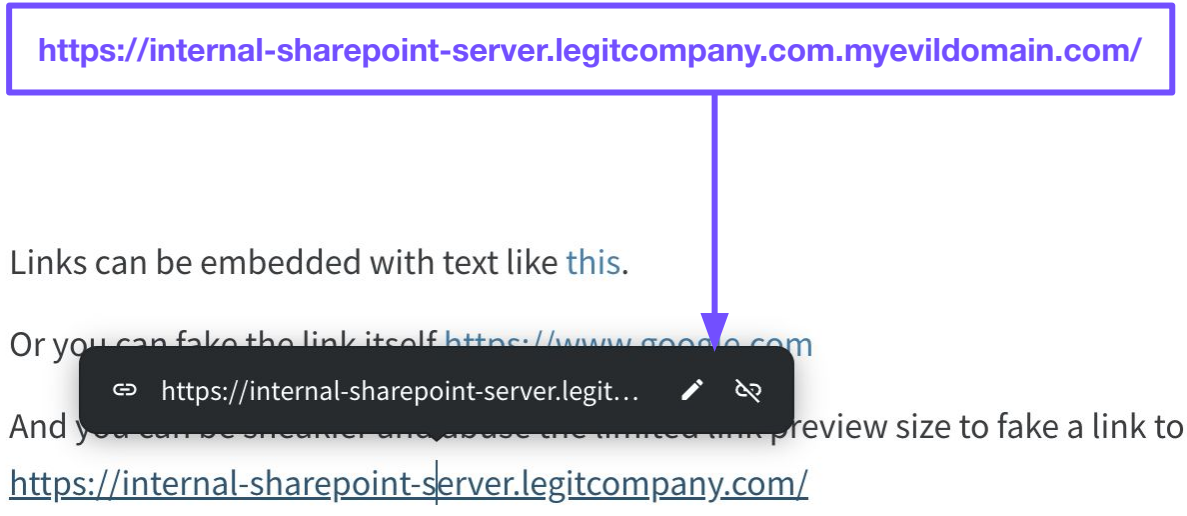
Lateral movement: Link backdooring

Links can be embedded with

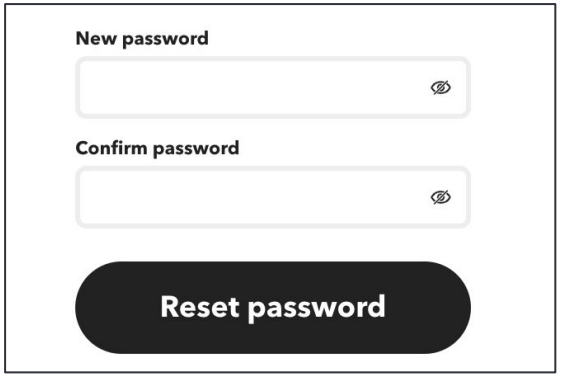
Or you can fake the link itself https://www.google.com

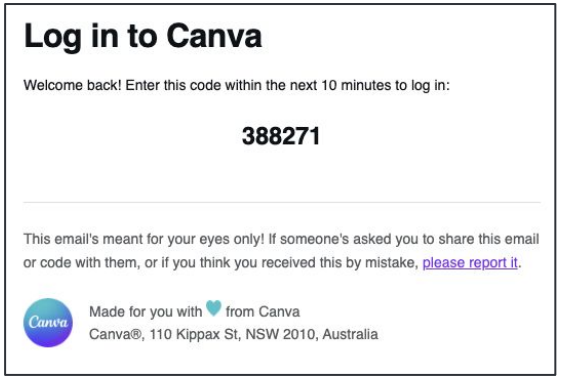
And you can be sneakier and abuse the limited link preview size to fake a link to https://internal-sharepoint-server.legitcompany.com/

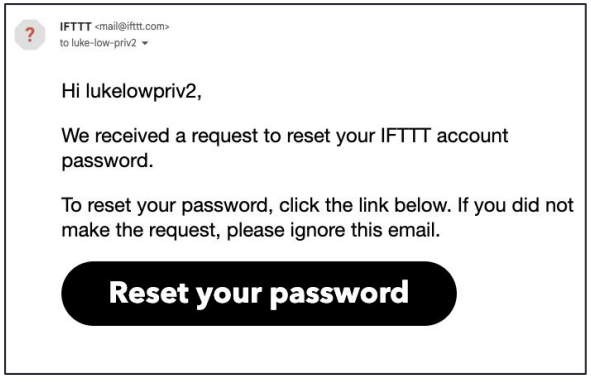
Lateral movement: Link backdooring



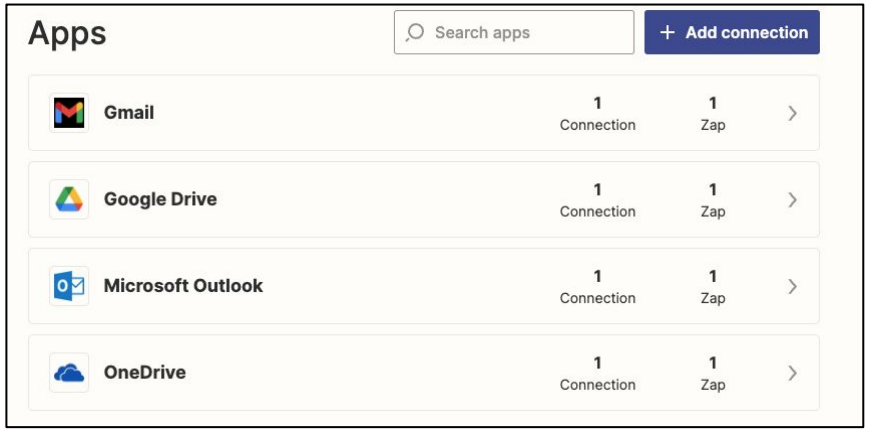
Lateral movement: Account recovery

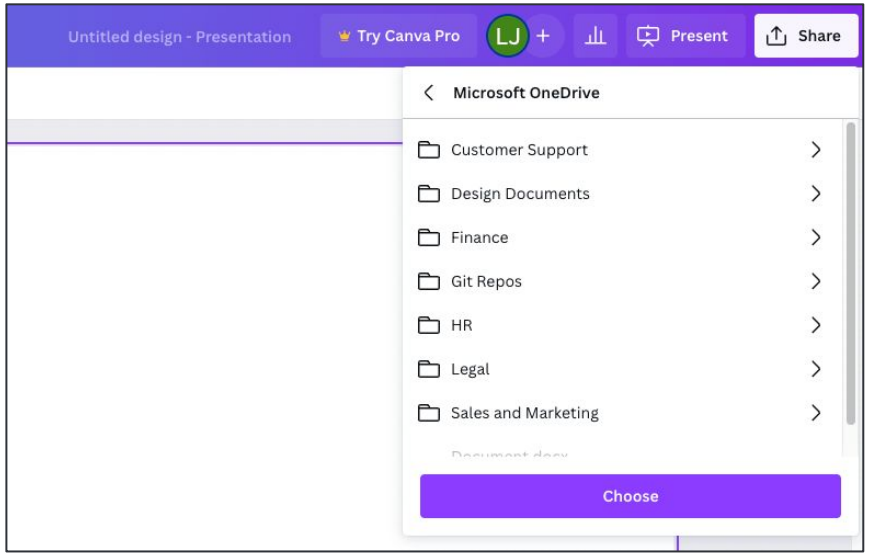






Lateral movement: Abuse existing integrations





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								

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

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

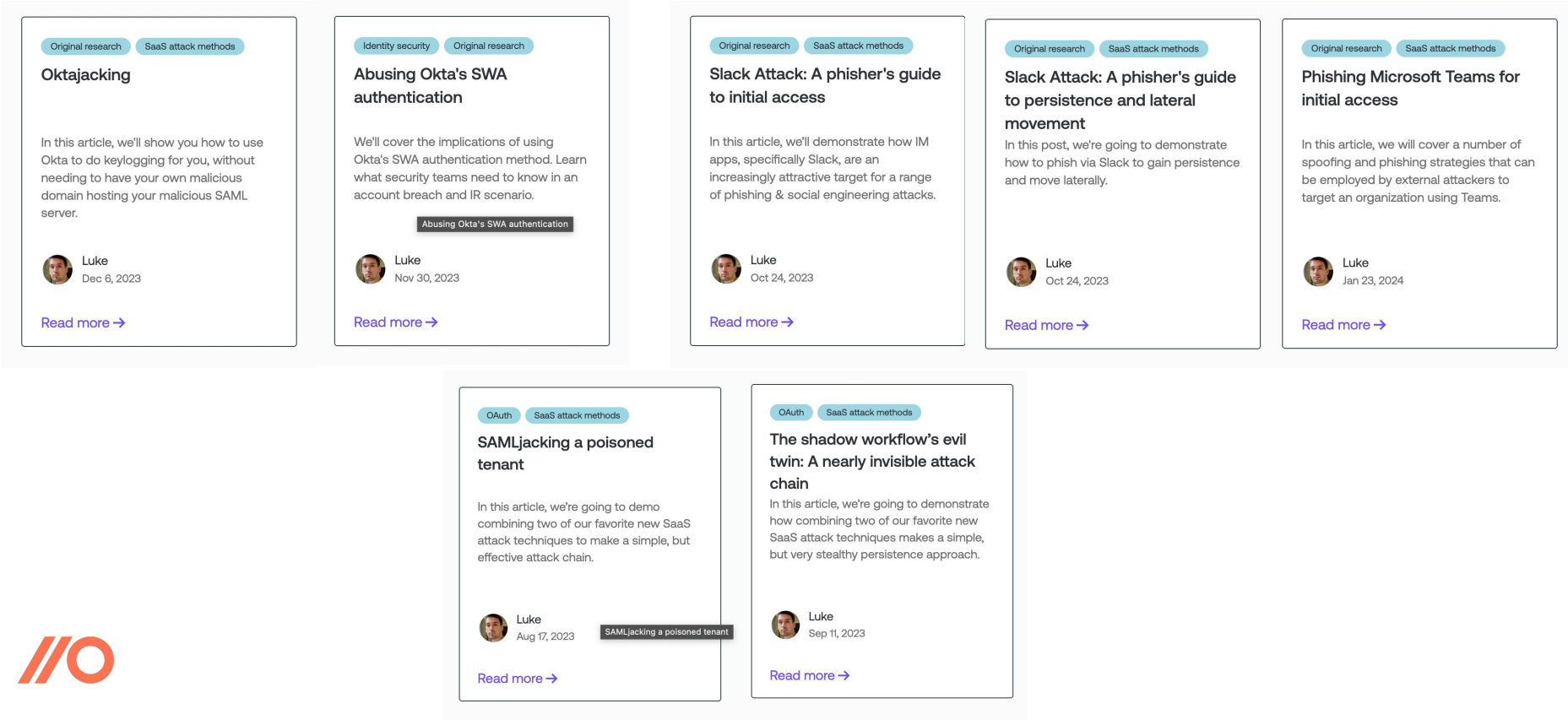
- Okta

References

- Okta Cross-Tenant Impersonation

https://pushsecurity.com/blog

Introducing the SaaS attack matrix



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