SSO Sloppy, SSO Suspect, SSO Vulnerable

Jenko Hwong
Cloud Village
August 12, 2023

jhwong@netskope.com
@jenkohwong
@jenko@infosec.exchange

© 2023 Jenko Hwong

Themes

Chains: Trust, Attack, Web APIs

Protocol Risk: Design & Implementatior

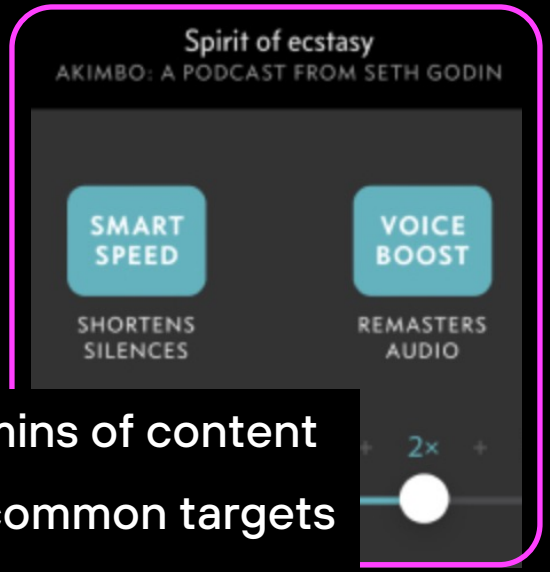
Concepts and Principles

Goals

Inform: 80mins of content

Entertain: common targets

Feel Better About Yourself

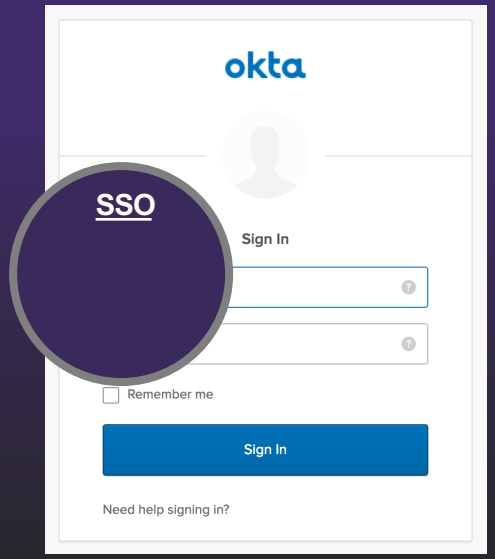


© 2023 Jenko Hwong

01 SSO

© 2023 Jenko Hwong

SSO, been there, done that...

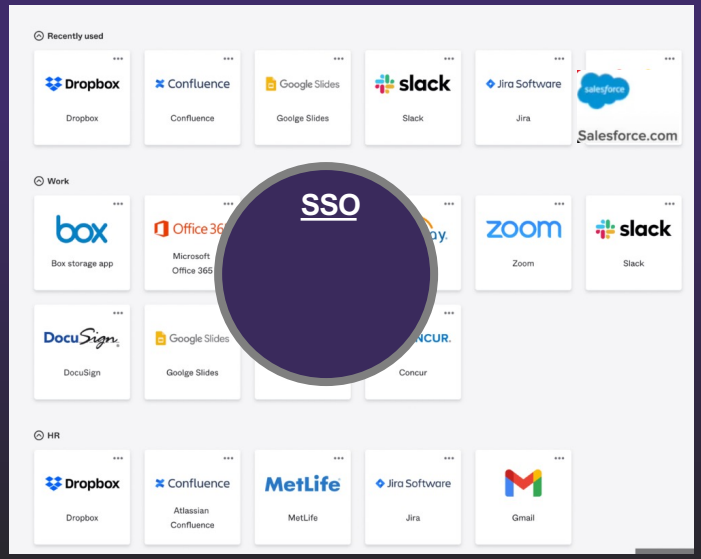


1. Login at SSO IDP

IDP-initiated flow

© 2023 Jenko Hwong

SSO, been there, done that...

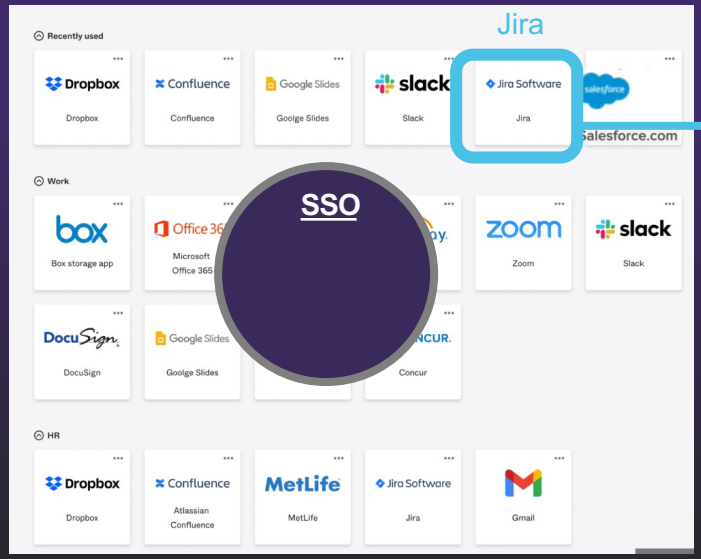


2. SSO App Dashboard

IDP-initiated flow

© 2023 Jenko Hwong

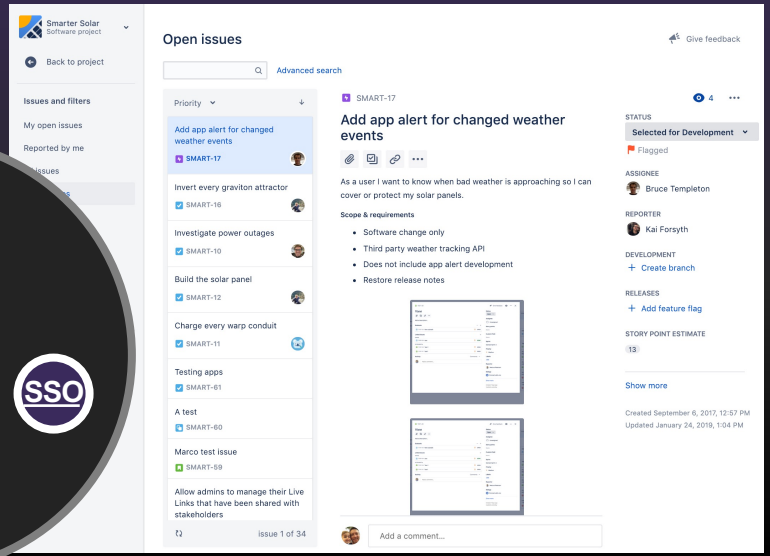
SSO, been there, done that...

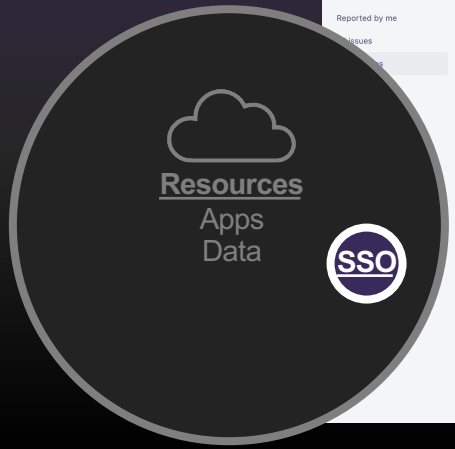


IDP-initiated flow

3a. Redirect to Jira (SP)
Signed auth/ID token
e.g. SAML assertion

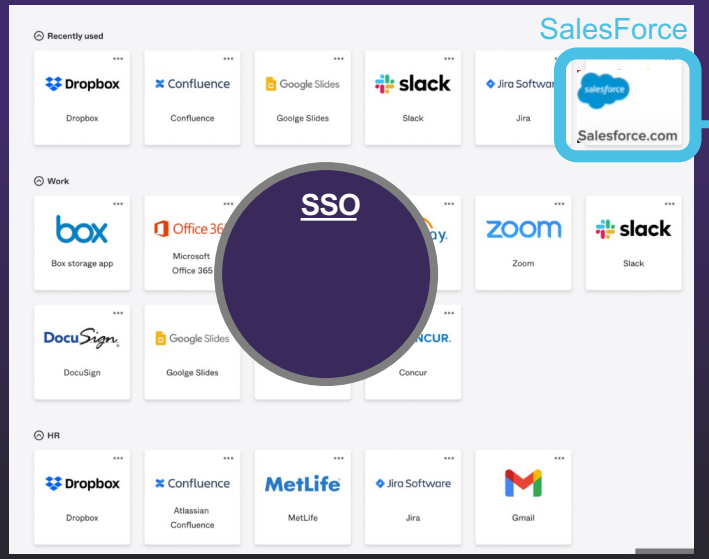
Jira





© 2023 Jenko Hwong

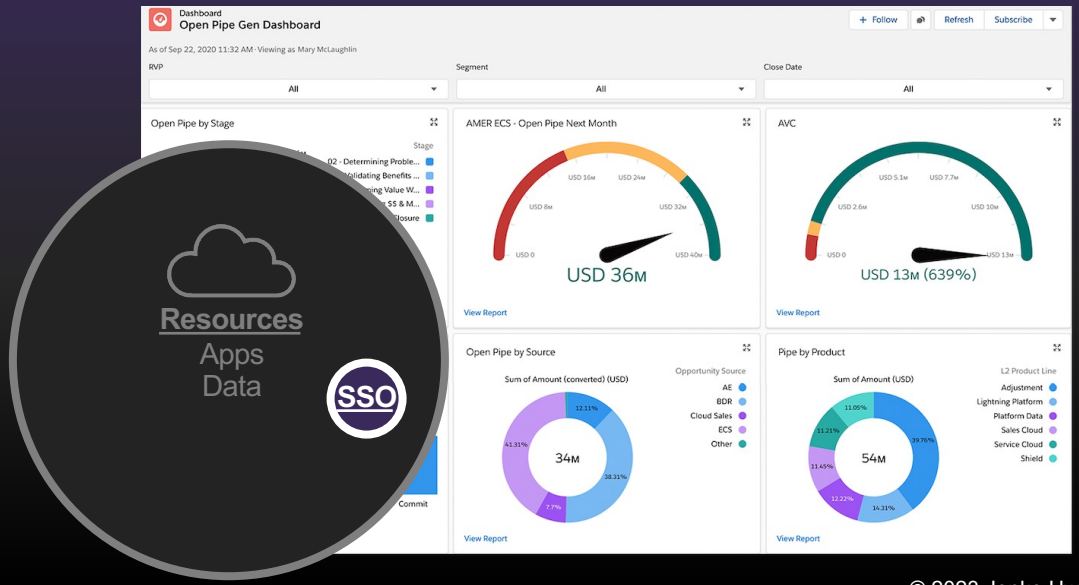
SSO, been there, done that...



IDP-initiated flow

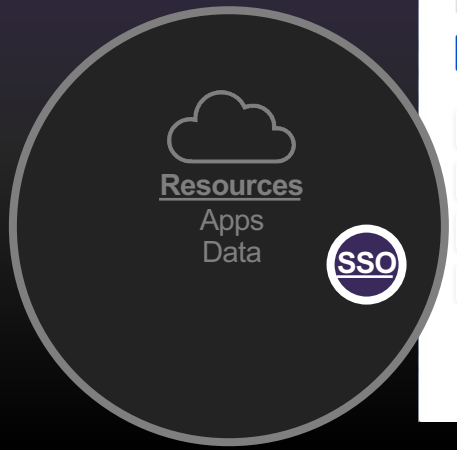
3b. Redirect to SalesForce (SP)
Signed auth/ID token
e.g. SAML assertion

SalesForce



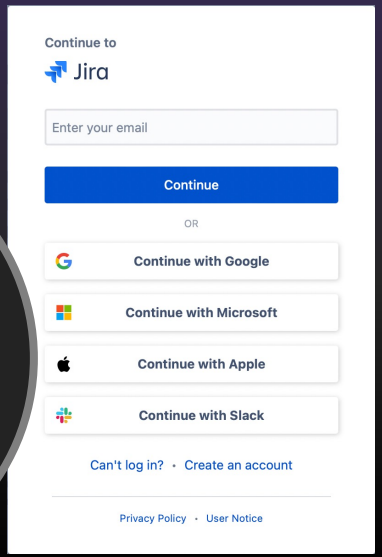
© 2023 Jenko Hwong

SSO, been there, done that...



SP-initiated flow

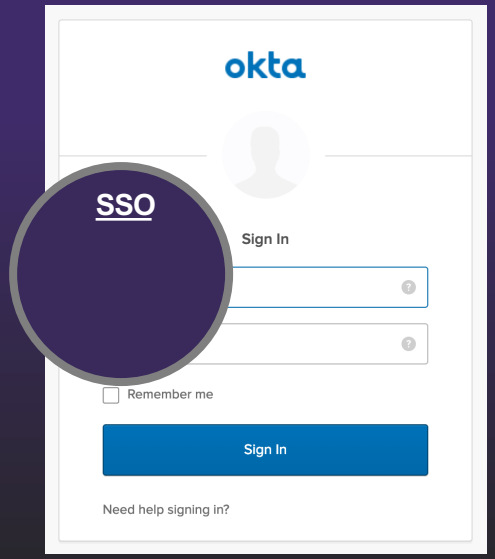
1. Login at SP (select SSO)



© 2023 Jenko Hwong

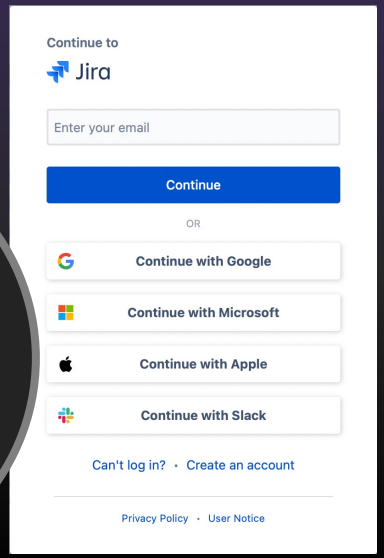
SSO, been there, done that...

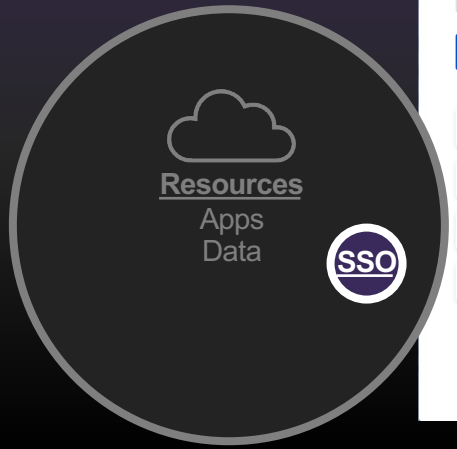
SP-initiated flow



[2. Login at SSO IDP]

Redirect to SSO/IDP



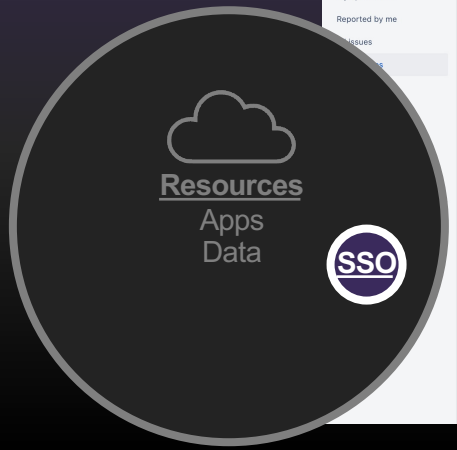


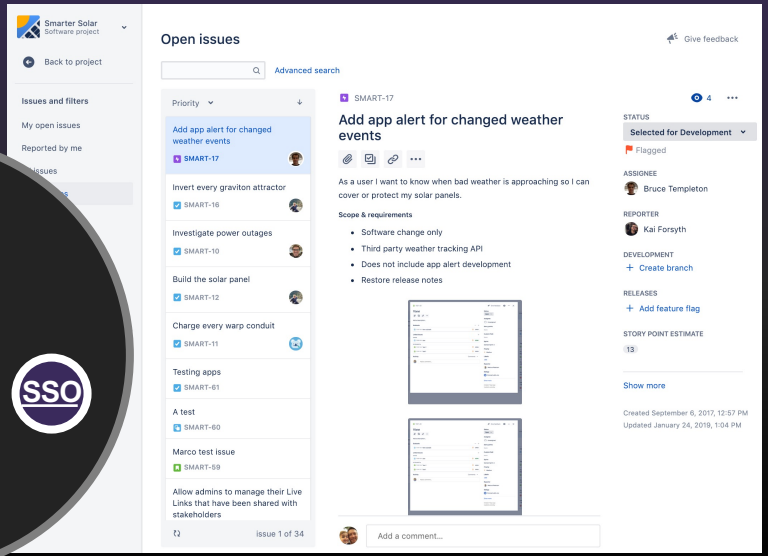
© 2023 Jenko Hwong

SSO, been there, done that...

SP-initiated flow

3. Redirect to Jira (SP)
Signed auth/ID token
e.g. SAML assertion





© 2023 Jenko Hwong

Conventional Wisdom

- SSO is a good thing and is a best practice
- Centrally-managed authentication policies (consistency, correctness)
- Enforce stronger password policies (credential rotation, MFA, strength)
- Reduce # of credentials (attack surface) - L8 weak link
- Convenience for end-user (which aligns with security!)

© 2023 Jenko Hwong

Conventional Wisdom?

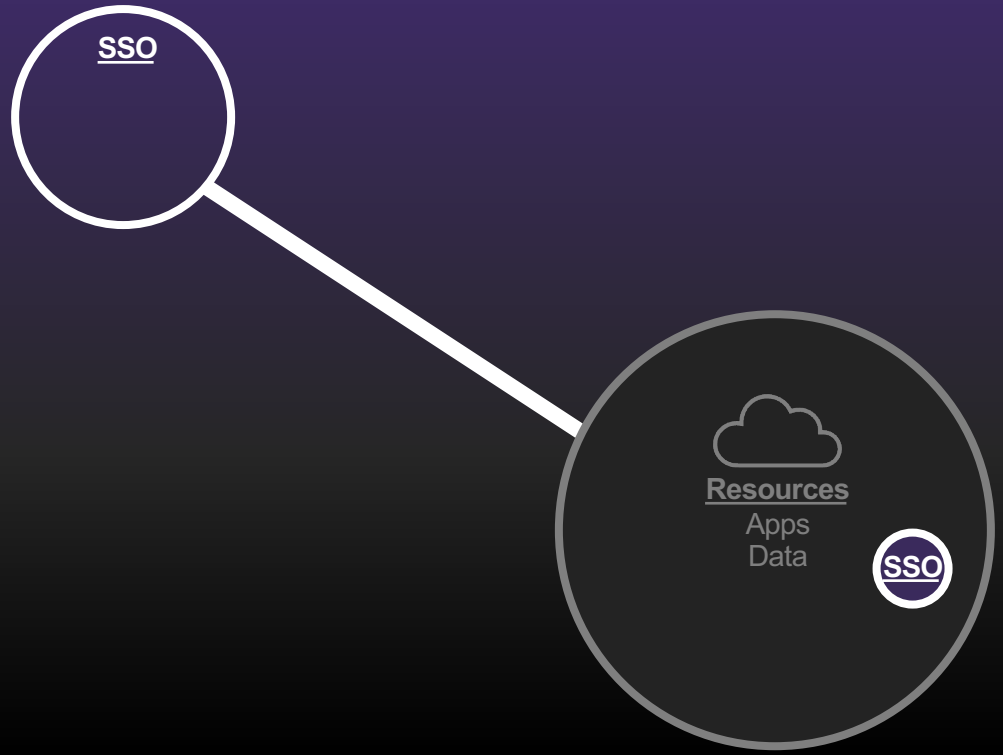
"The riskiest thing we can do is just maintain the status quo."
– Bob Iger

© 2023 Jenko Hwong

02 Attacks

© 2023 Jenko Hwong

Assumptions

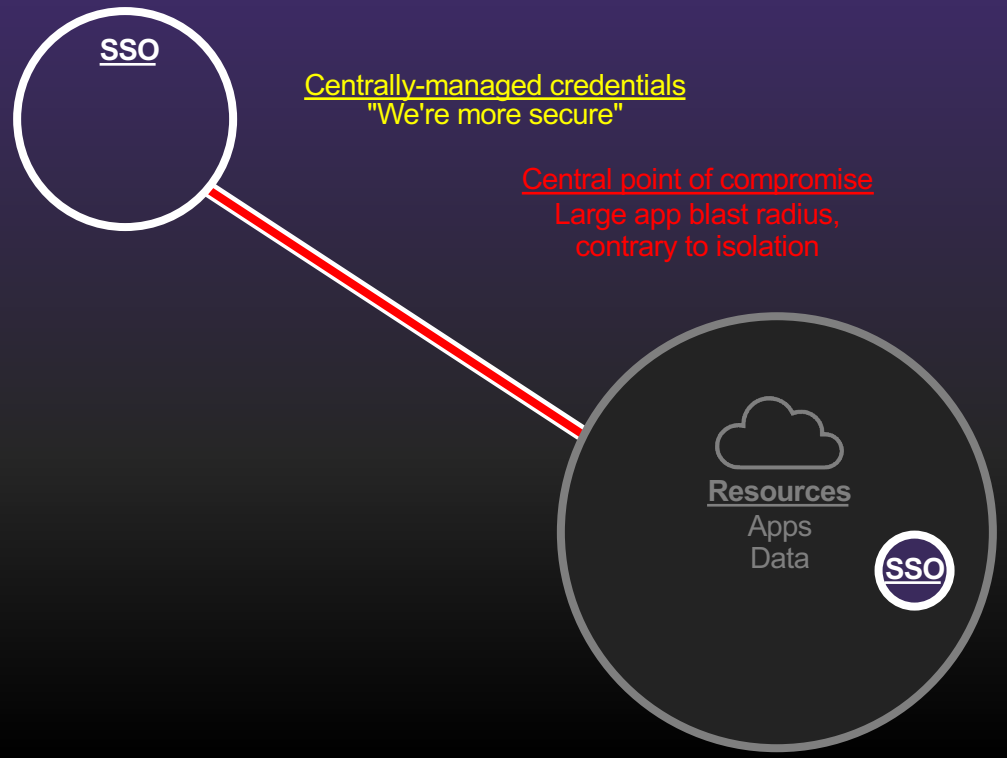


© 2023 Jenko Hwong

Assumptions

© 2023 Jenko Hwong

Assumptions → Risk

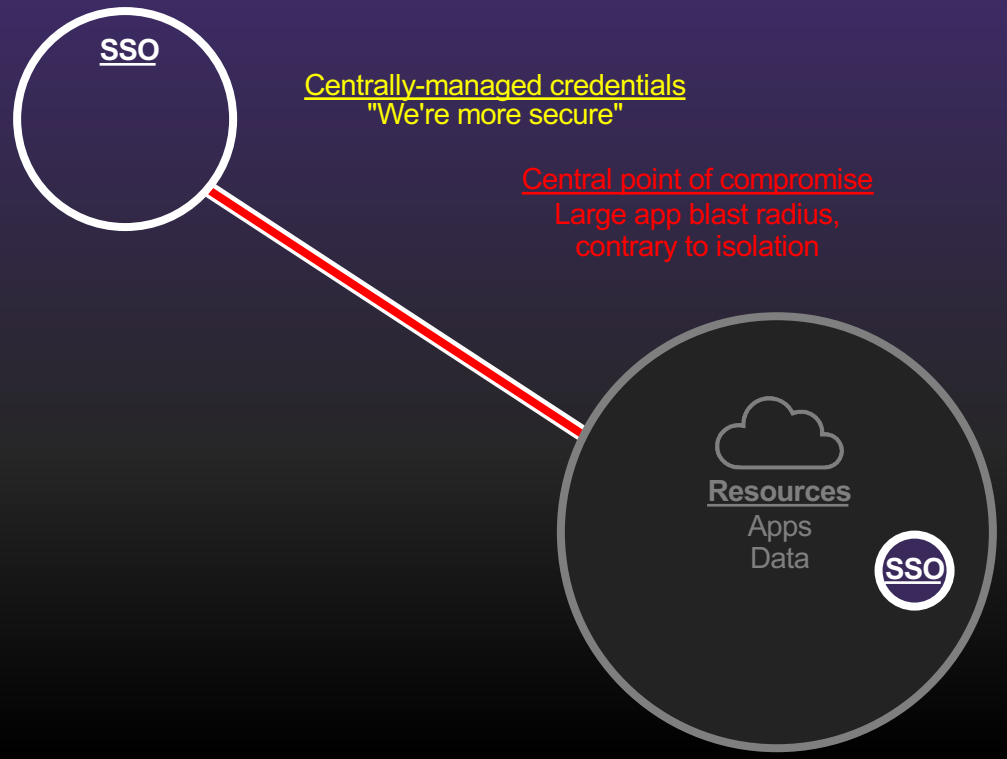


© 2023 Jenko Hwong

Assumptions → Risk → Abuse

Supply Chain Attacks (Trust)

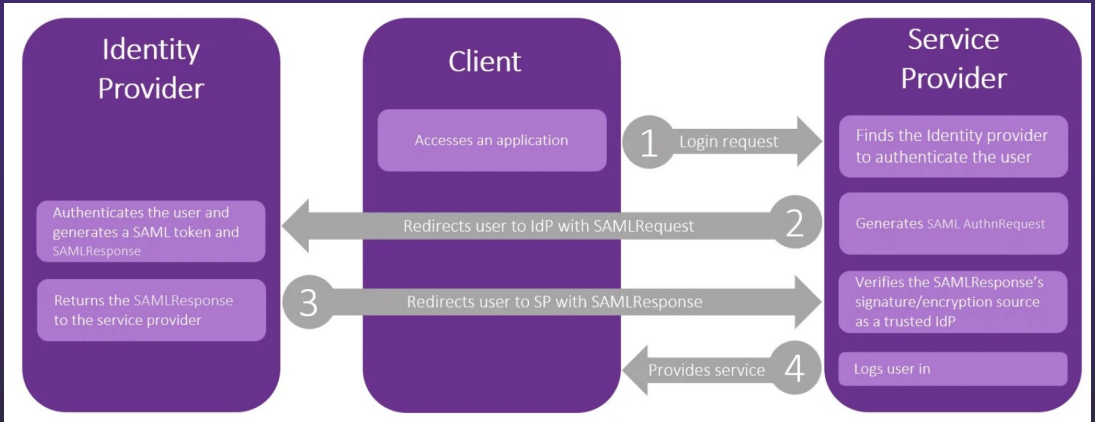
- Golden SAML: signing keys



© 2023 Jenko Hwong

Supply Chain Attacks: Golden SAML

SAML Flow

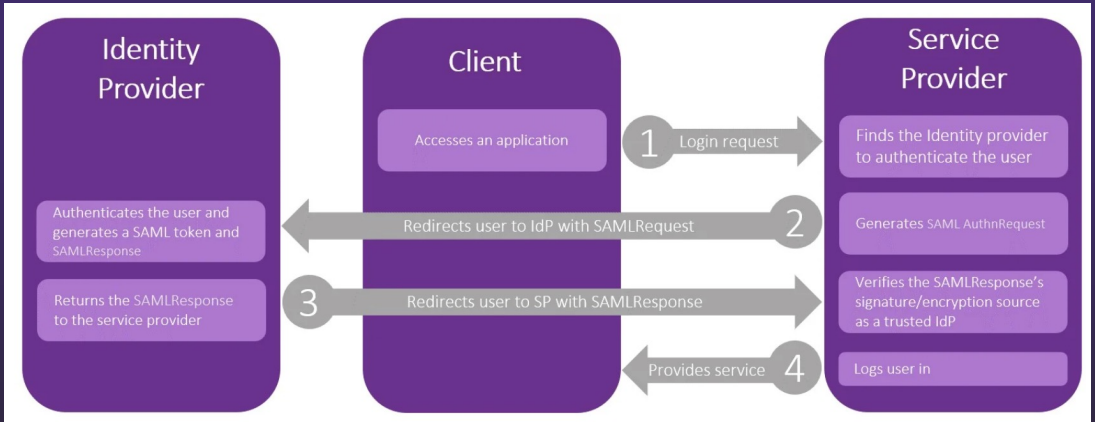


"Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps," Shaked Reiner, CyberArk (11/21/2017)
https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps

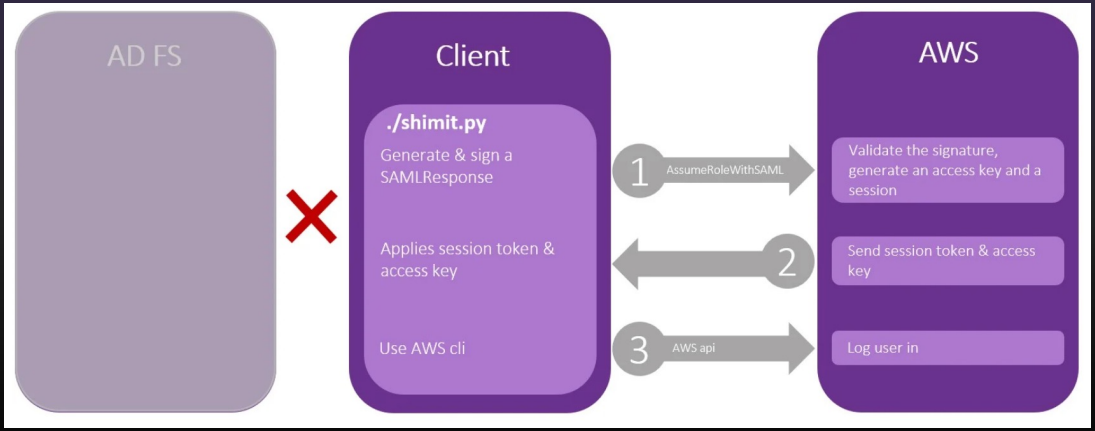
© 2023 Jenko Hwong

Supply Chain Attacks: Golden SAML

SAML Flow



Golden SAML Attack



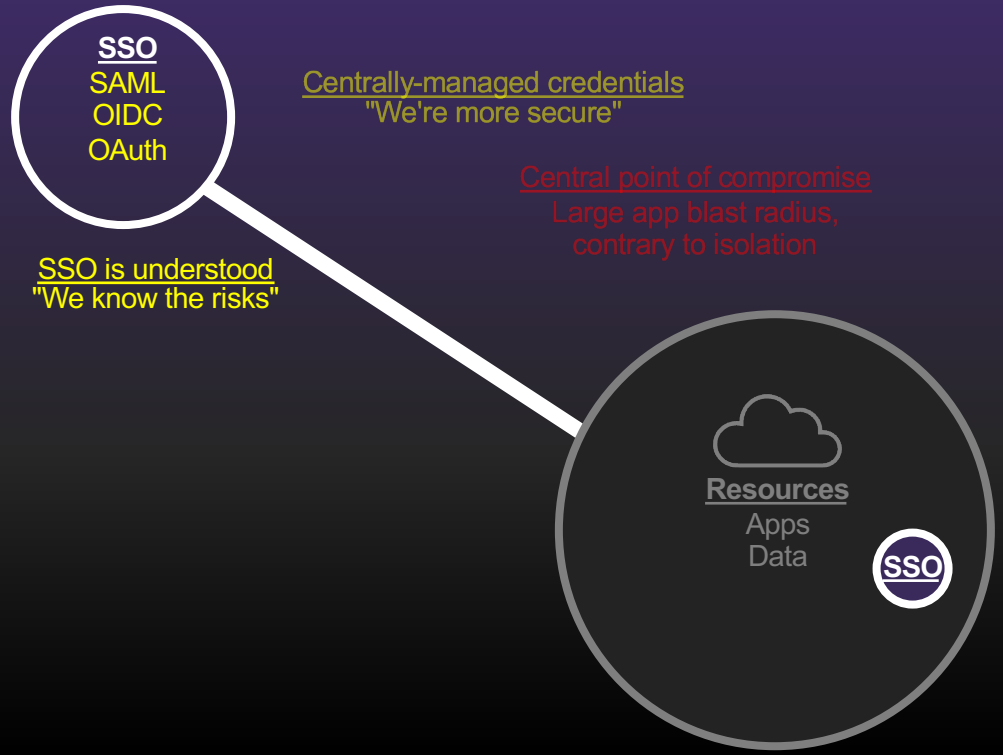
"Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps," Shaked Reiner, CyberArk (11/21/2017)
https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps

© 2023 Jenko Hwong

Assumptions

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

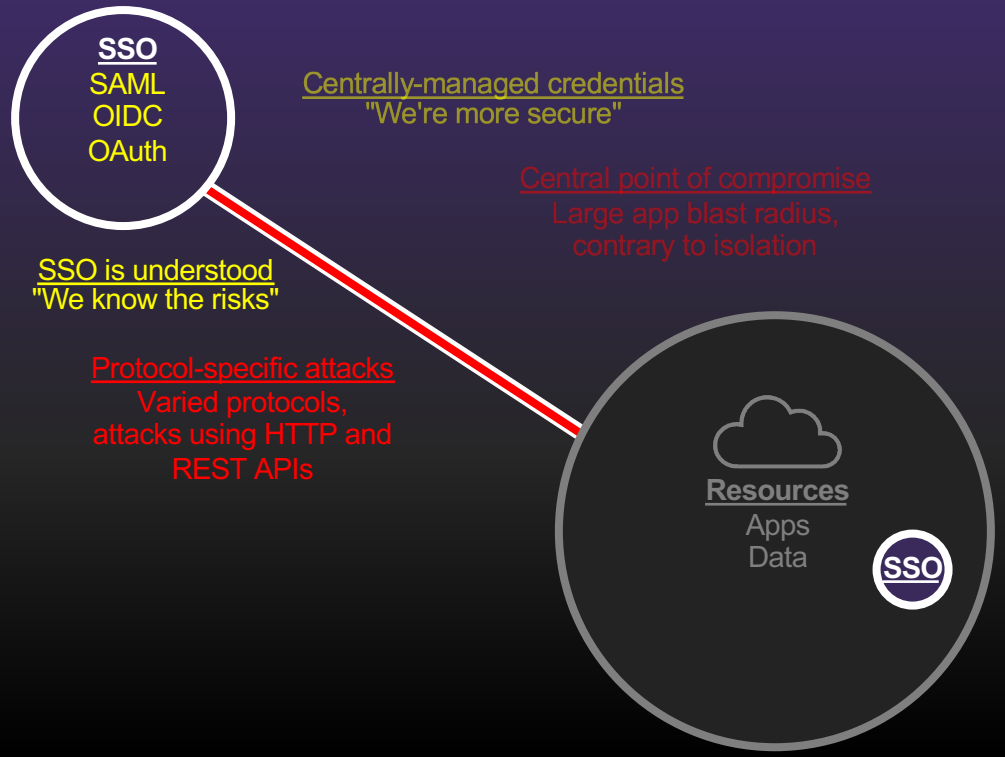


© 2023 Jenko Hwong

Assumptions → Risk

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

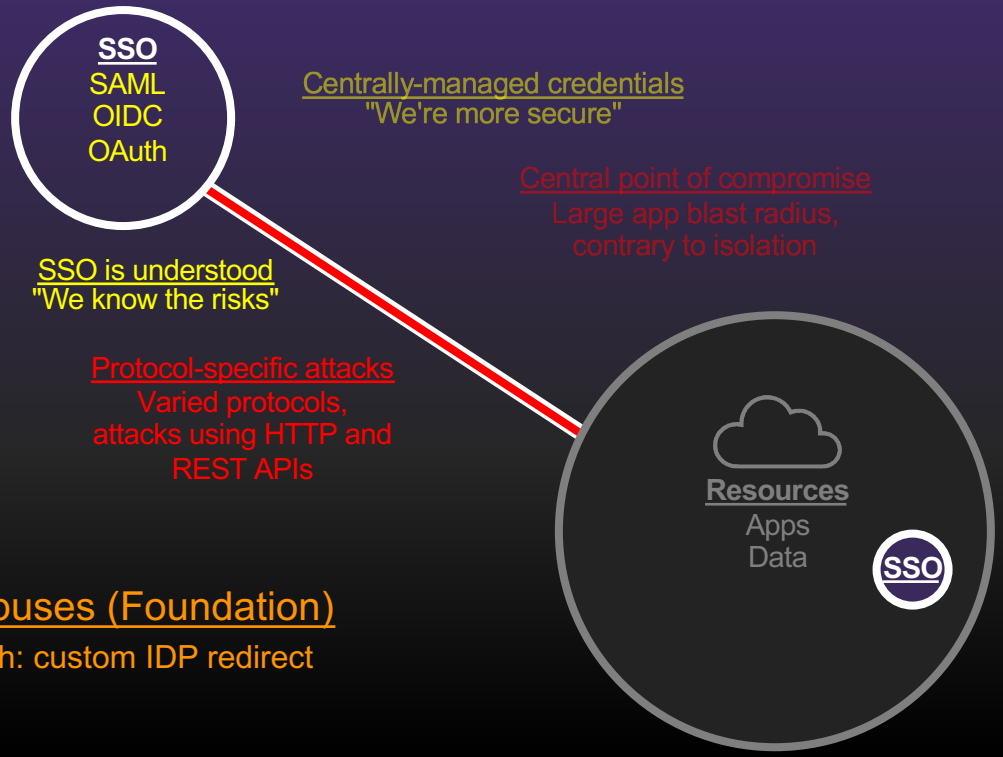


© 2023 Jenko Hwong

Assumptions → Risk → Abuse

Supply Chain Attacks (Trust)

- Golden SAML: signing keys



Protocol Abuses (Foundation)

- SAML Phish: custom IDP redirect

© 2023 Jenko Hwong

Protocol Abuses: SAML Phish

Victim View

"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

Protocol Ab

Victim View

Okta MFA Device Expiration Inbox ×

Okta <noreply@okta.com>
to me

Valid email from Okta

okta

Target Organization - MFA Device Expiration

Hi Jordan,

Your MFA Device is expiring in 24 hours, follow this link to refresh your device to avoid being locked out of your account.

Refresh MFA Token

This link expires in 7 days.

Link to *.okta.com

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link: targetorg.okta.com/help/login

This is an automatically generated message from Okta. Replies are not monitored or answered.

Reply Forward

© 2023 Jenko Hwong

https://jordanpotti.okta.com/sso/saml2/0oaq3csxlcc6N5YgO356

Link to *.okta.com

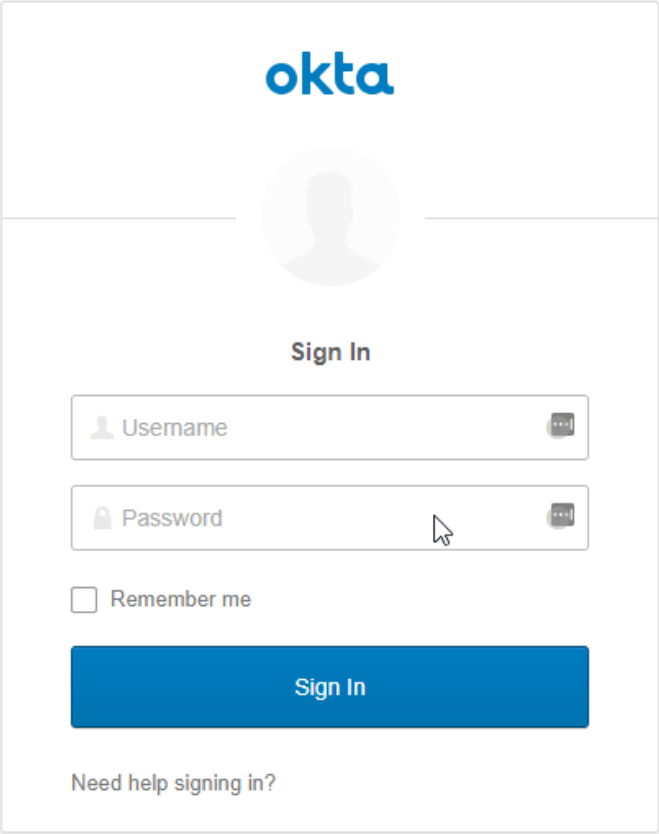
Signing In

"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

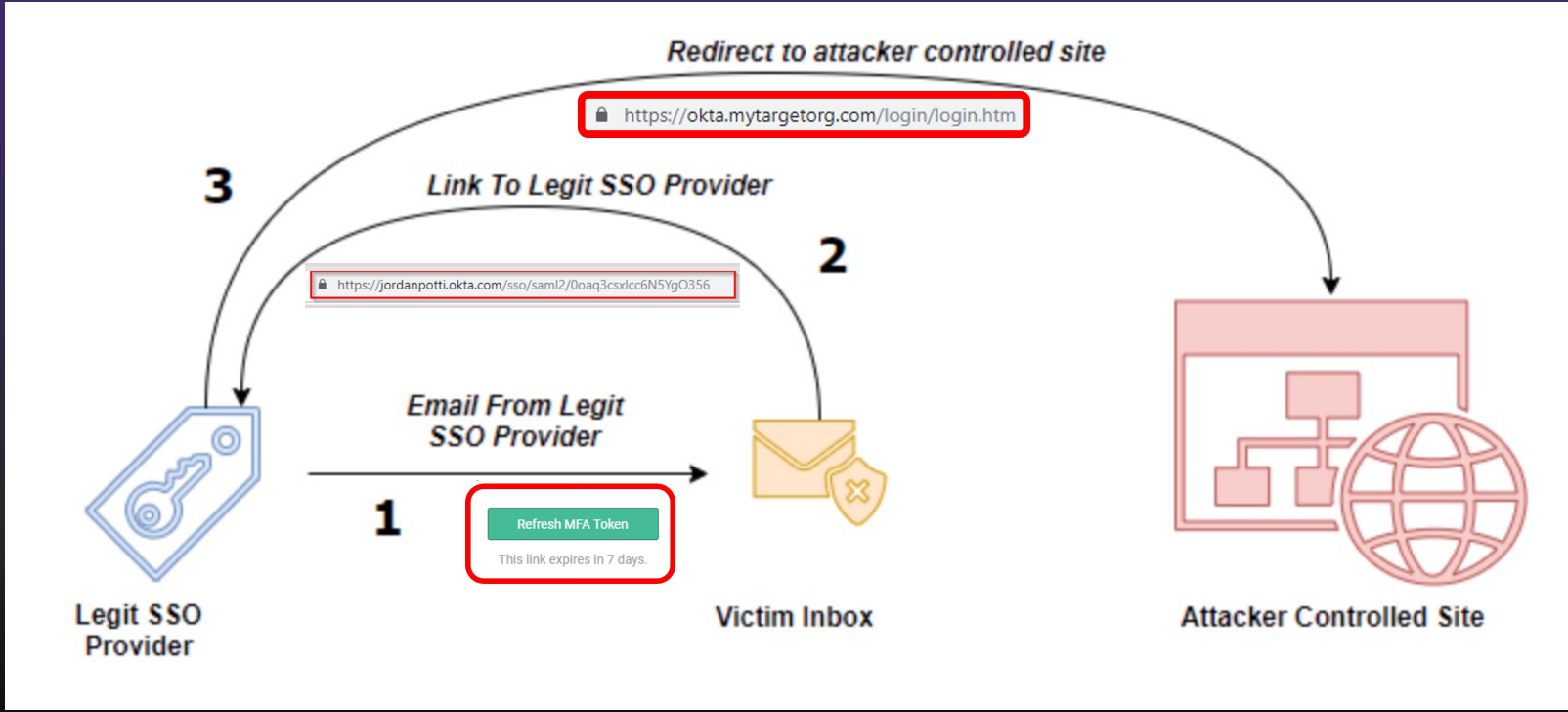
https://okta.mytargetorg.com/login/login.htm

HTTP redirect...to attacker domain



Protocol Abuses: SAML Phish

Attack Flow

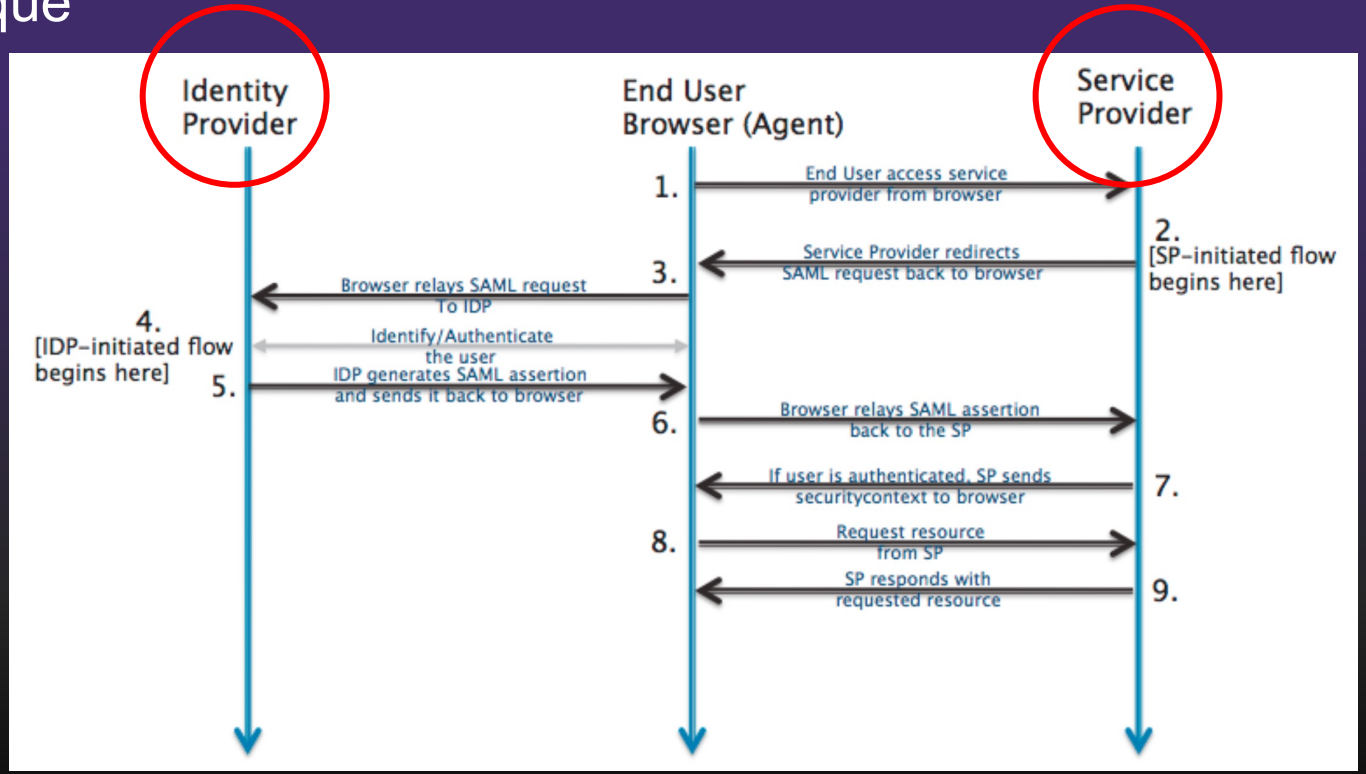


"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

Protocol Abuses: SAML Phish

Attack Technique

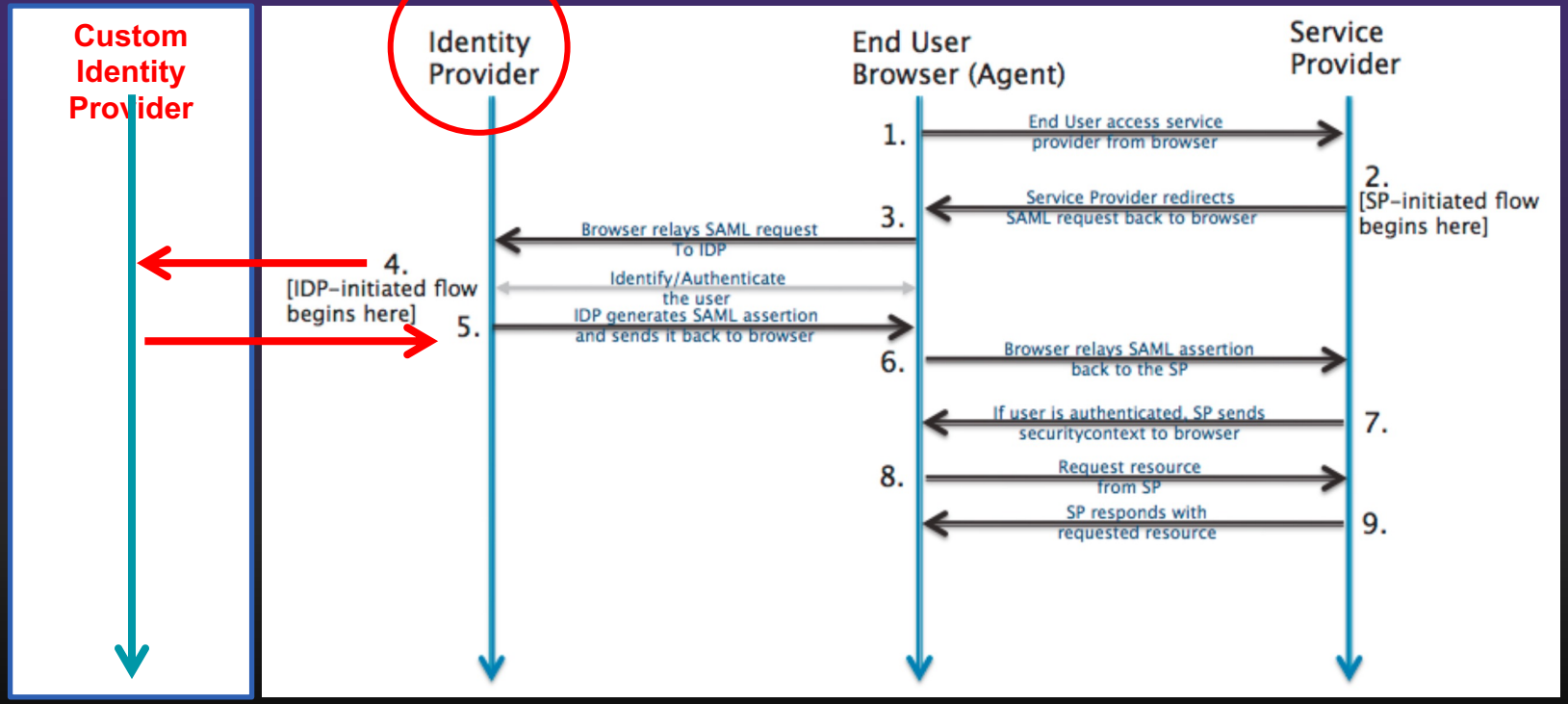


"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

Protocol Abuses: SAML Phish

Attack Technique



"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

Protocol AI

Attack Setup

Okta Email Template

Add Translation

Default Language English (en)

English (en)

Email Preview

Okta MFA Device Expiration

okta

Target Organization - MFA Device Expiration

Hi jordan,

Your MFA Device is expiring in 24 hours, follow this link to refresh your device to avoid being locked out of your account.

Refresh MFA Token

This link expires in 7 days.

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link:
targetorg.okta.com/help/login

This is an automatically generated message from Okta. Replies are not monitored or answered.

"Phishing with SAML and SSO P ... rs/

© 2023 Jenko Hwong

Protocol Abuses: SAML Phish

Attack Setup

Okta IDP Redirect URL

Add Identity Provider

Search...

Name	Type	Account Mode	Profile Master	Actions
test	Saml2	SSO		Active / Configure

IdP ID	0oaq3csxlcc6N5YgO356
SAML metadata	Download metadata
Assertion Consumer Service URL	https://jordanpotti.okta.com/sso/saml2/0oaq3csxlcc6N5YgO356
Audience URI	https://www.okta.com/saml2/service-provider/sppnodrqoozkoruqymoo

Show More

"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

Protocol Abus

Attack Setup

Okta IDP Redirect Target

1 day until you lose access to Okta. If you need more time, we can extend your trial Extend Trial

Edit Identity Provider

Name: test

Protocol: SAML2

AUTHENTICATION SETTINGS

IdP Username: idpuser.subjectNameId

Expression Language Reference

Filter: Only allow usernames that match defined RegEx Pattern

Match against: Okta Username

Choose the user attribute to match against the IdP username.

If no match is found:
- Create new user (JIT)
- Redirect to Okta sign-in page

SAML PROTOCOL SETTINGS

IdP Issuer URI: /login

IdP Single Sign-On URL: https://evilsite.com

IdP Signature Certificate: ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain View, O=Google Inc.
Certificate expires in 1795 days

Show Advanced Settings

Update Identity Provider Cancel

"Phishing with SAML and SSO Providers -providers/

© 2023 Jenko Hwong

Protocol Ab

Attack Setup

Okta Email Target Users

Add Person

First name: John

Last name: Doe

Username: john.doe

Primary email: john.doe@mytargetorg.com

Secondary email (optional):

Groups (optional): You haven't added any groups

Password: Set by user

☐ Send user activation email now

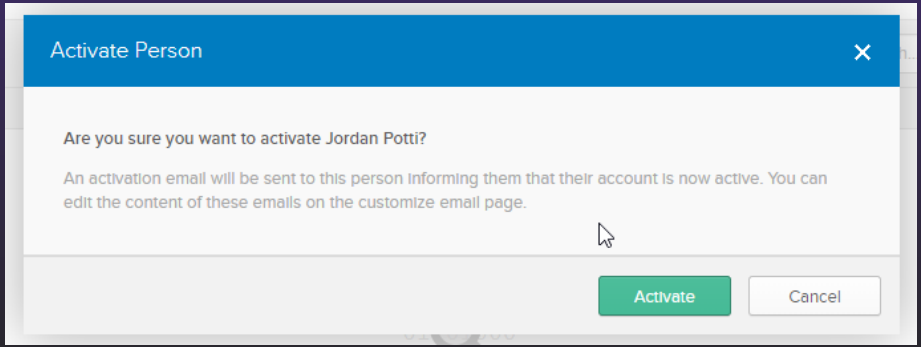
Save | Save and Add Another | Cancel

© 2023 Jenko Hwong

Protocol Abuses: SAML Phish

Attack Setup

Okta Email Campaign



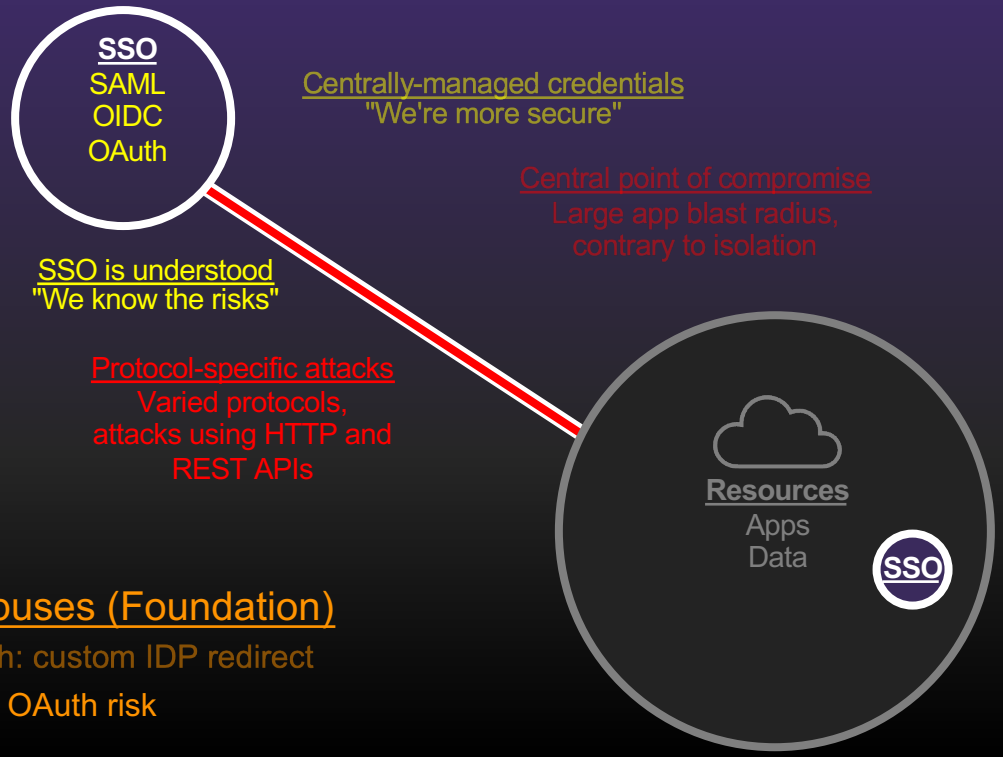
"Phishing with SAML and SSO Providers," Jordan Potti, (8/26/2019): https://jordanpotti.com/2019/08/26/phishing-with-saml-and-sso-providers/

© 2023 Jenko Hwong

Assumptions → Risk → Abuse

Supply Chain Attacks (Trust)

- Golden SAML: signing keys



Protocol Abuses (Foundation)

- SAML Phish: custom IDP redirect
- AWS SSO: OAuth risk

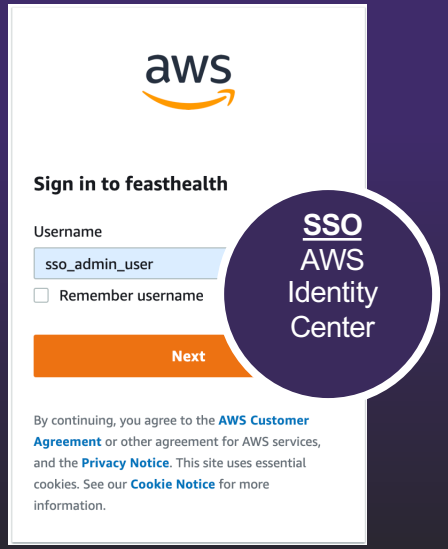
© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

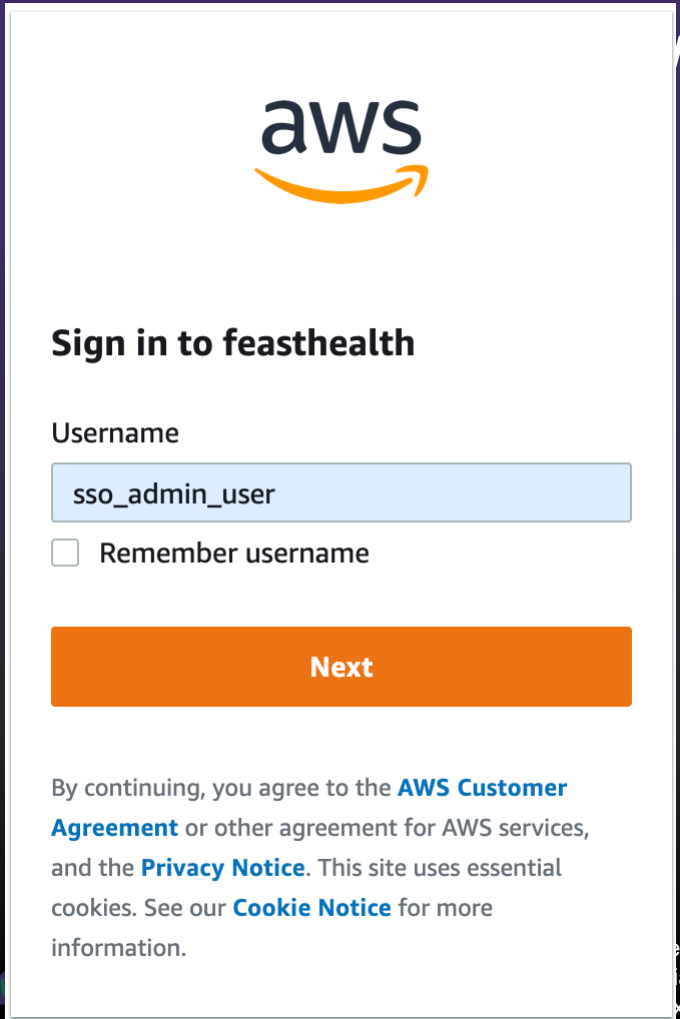


SSO
AWS Identity Center

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

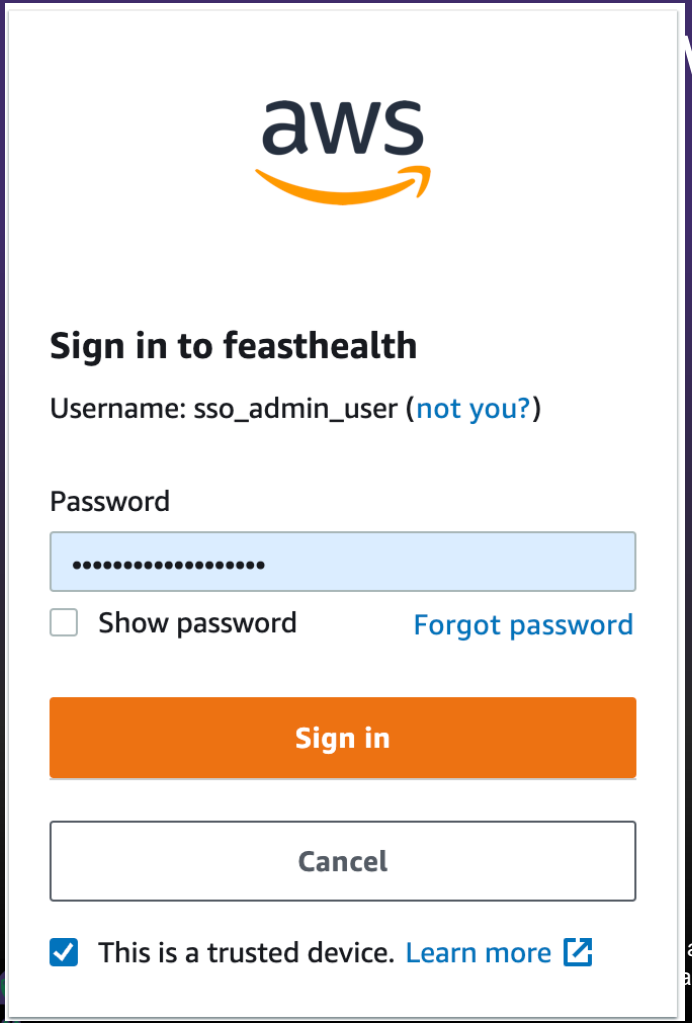
WS SSO



e authentication," Christophe Tafani-Dereeper (6/9/2021)
ia-aws-sso-device-code-authentication/
x Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

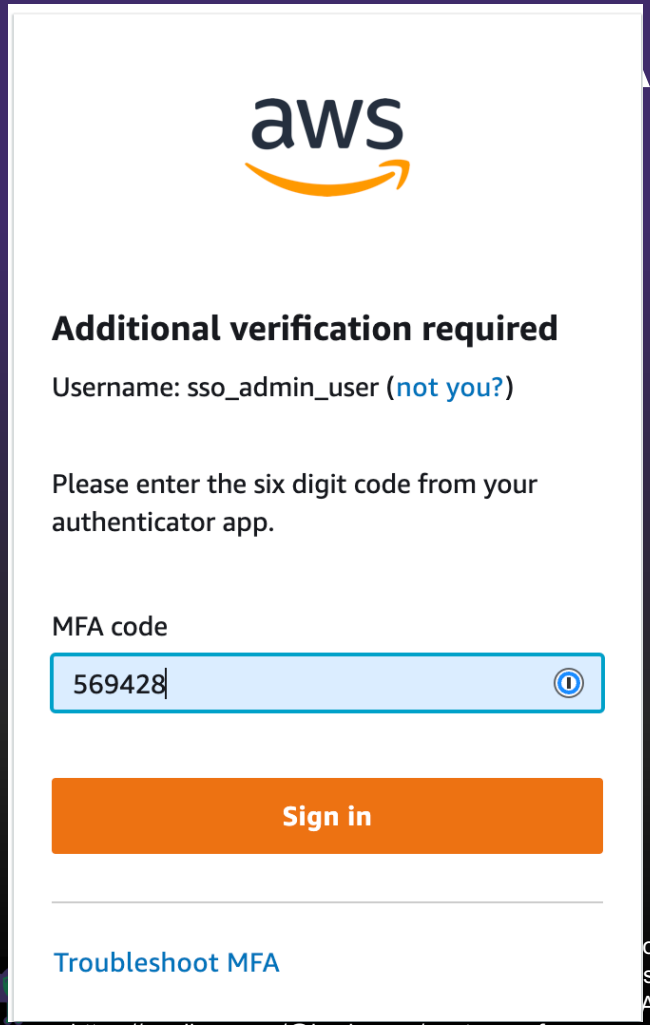
WS SSO



authentication," Christophe Tafani-Dereeper (6/9/2021)
a-aws-sso-device-code-authentication/
Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

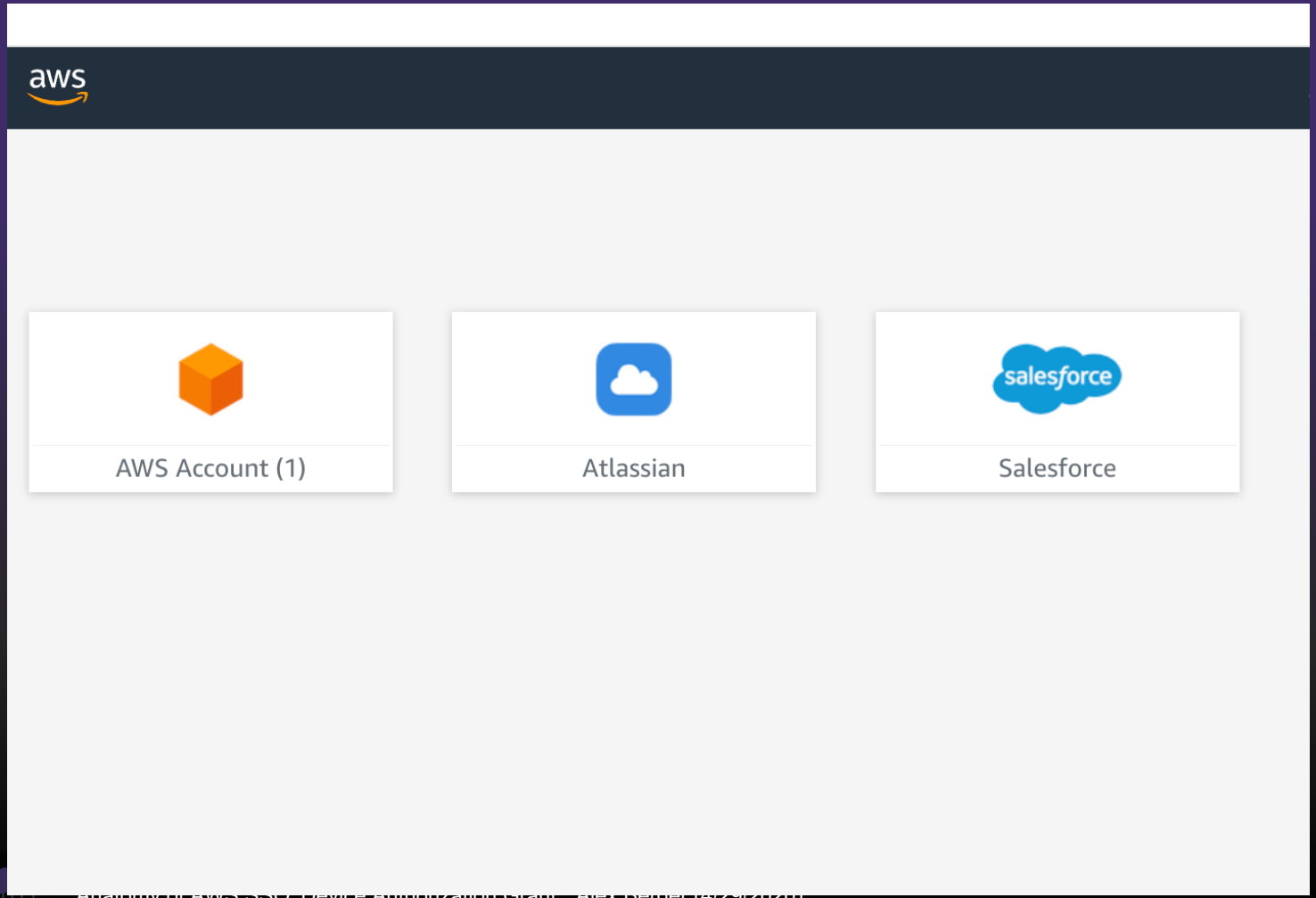
© 2023 Jenko Hwong

AWS SSO



ode authentication," Christophe Tafani-Dereeper (6/9/2021)
s-via-aws-sso-device-code-authentication/
Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong



"Anatomy of AWS SSO Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

salesforce '23

Search... Search

Home | Chatter | Campaigns | Leads | Accounts | Contacts | Opportunities | Forecasts | Contracts | Orders | Cases | Solutions | Products | Reports | Dashboards

Create New...

Recent Items

Joe Blogs

Recycle Bin

Joe Blogs

Joe Blogs

Thursday November 17, 2022

Hide Feed

Post | File | New Event | More

Share an update, @mention someone...

Share

Sort By Most Recent Activity

Joe Blogs

Joe Blogs changed Email from joeblogs@bulky.eml.cc to sso_admin_user_quest@bulky.eml.cc.

Comment · Like · Two days ago at 10:47 PM

Joe Blogs

Joe Blogs changed Email from joeblogs@bulky.eml.cc to sso_admin_user_quest@bulky.eml.cc.

Comment · Like · Two days ago at 10:47 PM

Recommendations

Download Salesforce

Run your business from your phone with Salesforce.

Skip >

Calendar

New Event

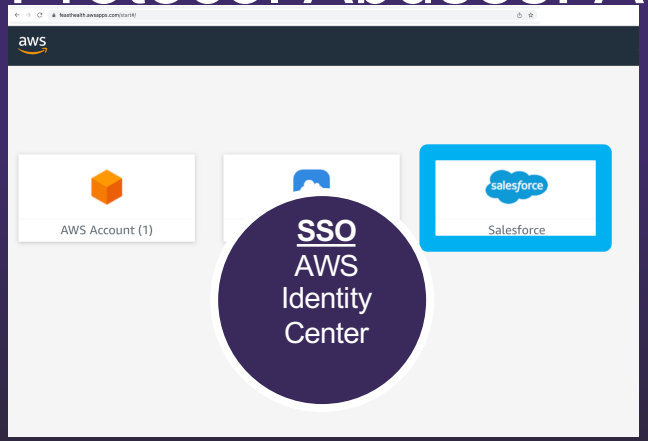
Today 11/17/2022

You have no events scheduled for the next 7 days.

https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

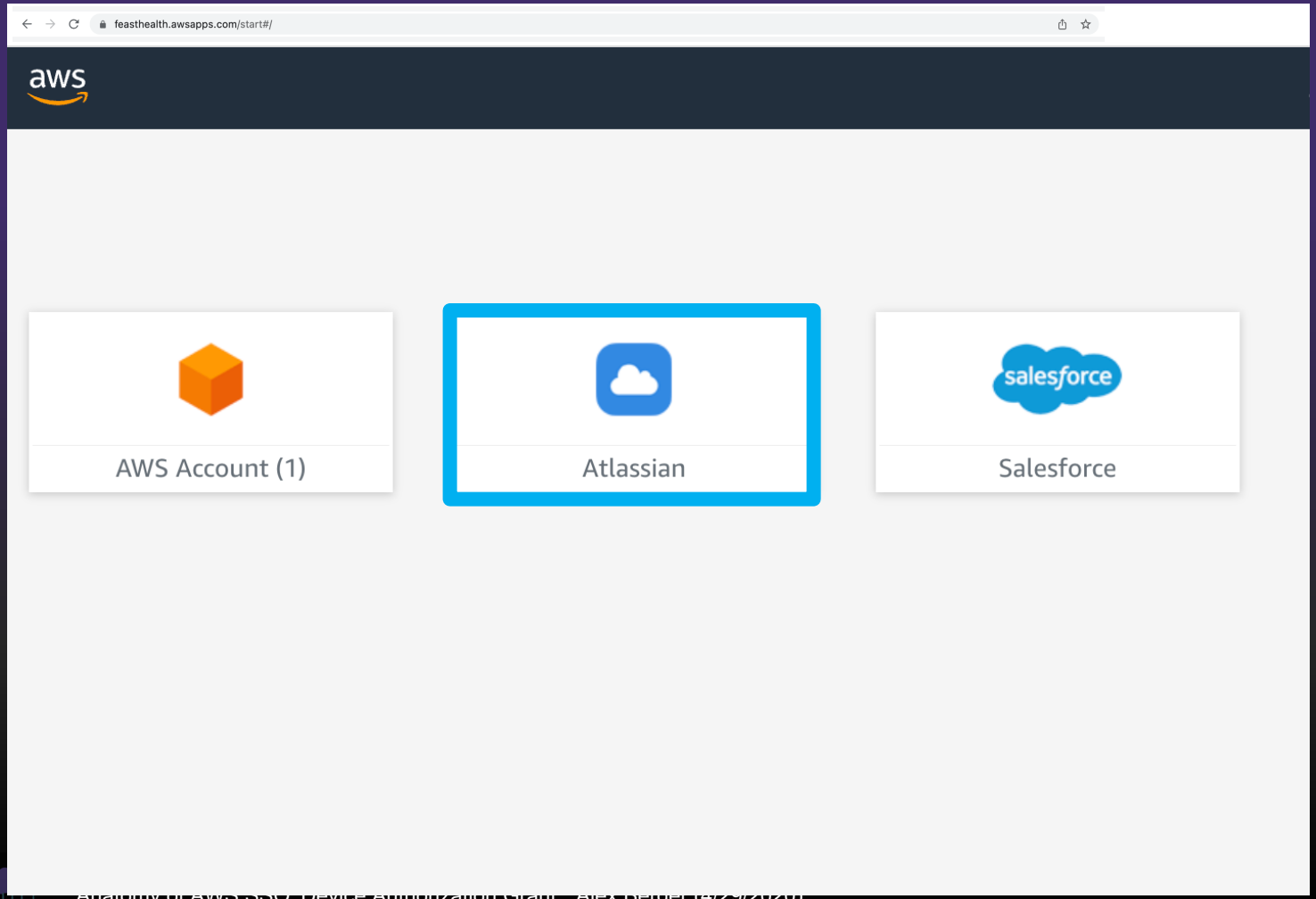
© 2023 Jenko Hwong

Protocol Abuses: AWS SSO



"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong



"Anatomy of AWS SSO Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Jira | Your work | Projects | Filters | Dashboards | People | Apps | Create | Search

Your work

Recent projects

AWS Cloud Deployment
Team-managed software
QUICK LINKS
My open issues 0
Done issues
1 board

CRM
Team-managed software
QUICK LINKS
My open issues 0
Done issues
1 board

Source Code Security Sc...
Team-managed software
QUICK LINKS
My open issues 0
Done issues
1 board

SSO Implementation
Company-managed software
QUICK LINKS
My open issues 0
Done issues
1 board

Worked on | Viewed | Assigned to me | Starred

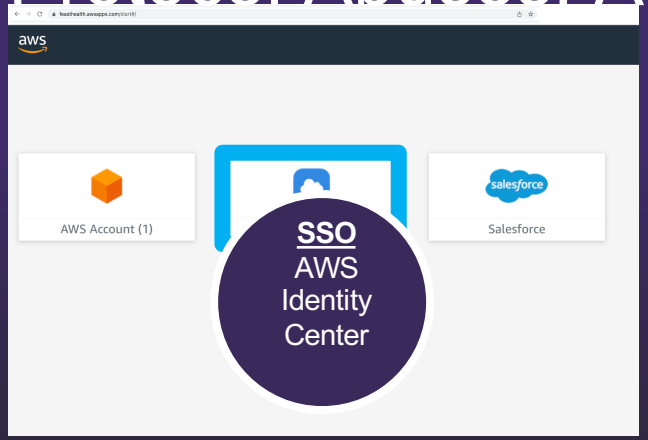
IN THE LAST WEEK

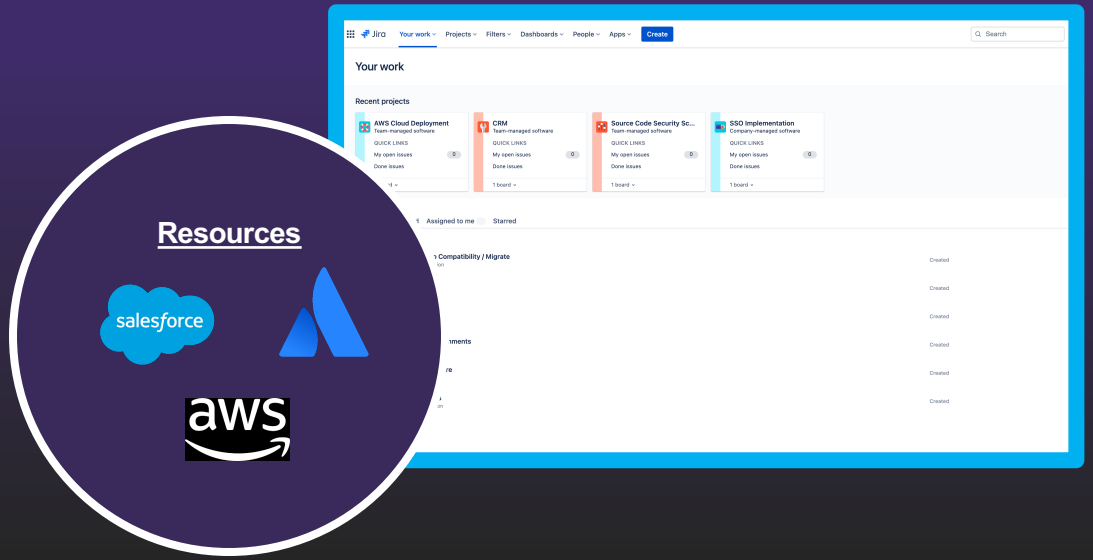
Determine SSO App Compatibility / Migrate SI-6 · SSO Implementation	Created
Production Cutover SI-5 · SSO Implementation	Created
Beta Test SI-4 · SSO Implementation	Created
Setup Test, Prod Environments SI-3 · SSO Implementation	Created
Design SSO Architecture SI-2 · SSO Implementation	Created
Evaluate SSO options SI-1 · SSO Implementation	Created

https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO





"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

feasthealth.awsapps.com/start#/

aws

Job | MFA devices | Sign out

Search

AWS Account (1)

Atlassian

Salesforce

BulkSecurity

#49XXXXXXXX32 | bulk_security_root@acme.com

AdministratorAccess

Management console

Command line or programmatic access

© 2023 Jenko Hwong

us-east-1.console.aws.amazon.com/console/home?region=us-east-1#

aws | Services | Search [Option+S] | N. Virginia | AdministratorAccess/sso_admin_user

GuardDuty | Detective | Security Hub

Console Home Info

Reset to default layout | + Add widgets

Introducing the new widget Applications. Find it at the bottom of your Console Home.

Recently visited Info

- IAM
- IAM Identity Center (successor to AWS Single ...
- Config
- VPC
- Resource Groups & Tag Editor
- EC2
- Directory Service
- GuardDuty
- AWS Budgets
- Detective
- AWS Organizations
- Security Hub

View all services

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

AWS Health Info

Open issues

0

Cost and usage Info

© 2023 Jenko Hwong

feasthealth.awsapps.com/start#/

aws

Job | MFA devices | Sign out

Search

AWS Account (1)

Atlassian

Salesforce

BulkSecurity

#49XXXXXXXX32 | bulk_security_root@acme.com

AdministratorAccess

Management console | Command line or programmatic access

© 2023 Jenko Hwong

Get credentials for AdministratorAccess

AWS account 49[redacted] (BulkSecurity)

Use any of the following options to access AWS resources programmatically or from the AWS CLI. You can retrieve new credentials as often as needed. Learn more

macOS and Linux | Windows | PowerShell

Option 1: Set AWS environment variables

Option 1: Set AWS environment variables Learn more

```
export AWS_ACCESS_KEY_ID="ASIAXGQ[illegible]
export AWS_SECRET_ACCESS_KEY="M+Gb[illegible]D"
export AWS_SESSION_TOKEN="IQoJb[illegible]ZP7G/
```

Option 2: Add a profile to your AWS credentials file

Paste the following text in your AWS credentials file (typically found at ~/.aws/credentials). Learn more

```
[495059067232_AdministratorAccess]
aws_access_key_id = ASIA[illegible]
aws_secret_access_key = M+[illegible]D
aws_session_token = IQ[illegible]Nw
```

Option 3: Use individual values in your AWS service client (Learn more)

AWS Access Key Id	ASIA[illegible]	Copy
AWS Secret access key	M+Gb[illegible]D	Copy
AWS session token	IQoJ[illegible]Kav	Copy

© 2023 Jenko Hwong

ATTACKER

```
$demo.sh
```

Amazon Web Services (AWS) | my-accounting - S3 bucket

s3.console.aws.amazon.com/s3/buckets/my-accounting?region=us-west-2&tab=objects

aws | Services | Search [Option+S] | Global | AdministratorAccess/sso_admin_user

GuardDuty | Detective | Security Hub | S3

Amazon S3

- Buckets
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3

- Block Public Access settings for this account

- Storage Lens
  - Dashboards
  - AWS Organizations settings

- Feature spotlight 3

- AWS Marketplace for S3

Amazon S3 > Buckets > ftx-bitcoin-bucket

ftx-bitcoin-bucket Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Copy S3 URI | Copy URL | Download | Open | Delete | Actions | Create folder

Upload

Find objects by prefix

1

Name	Type	Last modified	Size	Storage class
secrets.docx	docx	November 2, 2022, 06:35:57 (UTC-07:00)	10.3 KB	Standard

© 2022, Amazon Web Services, Inc. or its affiliates.

Protocol Abuses: AWS SSO

Browser/SAML

SSO
AWS
Identity
Center

Resources

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~

CLI/OAuth

SSO
AWS
Identity
Center

Resources

App/Client

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~

CLI/OAuth

SSO
AWS
Identity
Center

1. become an OAuth app
dynamic registration

```
{
   "authorizationEndpoint": null,
   "clientId": "R-j5yN-4-TPNs...tMQ",
   "clientIdIssuedAt": 1587156567,
   "clientSecret": "eyJr...x74",
   "clientSecretExpiresAt": 1594932567,
   "tokenEndpoint": null
}
```

App/Client

aws cli

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~

CLI/OAuth

SSO
AWS
Identity
Center

1. become an OAuth app
dynamic registration

2. initiate device code user +
device code

```
{
  "deviceCode": "8Acq...DUg",
  "expiresIn": 600,
  "interval": 1,
  "userCode": "RPXP-JSQA",
  "verificationUri": "https://device.sso.eu-central-1.amazonaws.com/",
  "verificationUriComplete": "https://device.sso.eu-central-
1.amazonaws.com/?user_code=RPXP-JSQA"
}
```

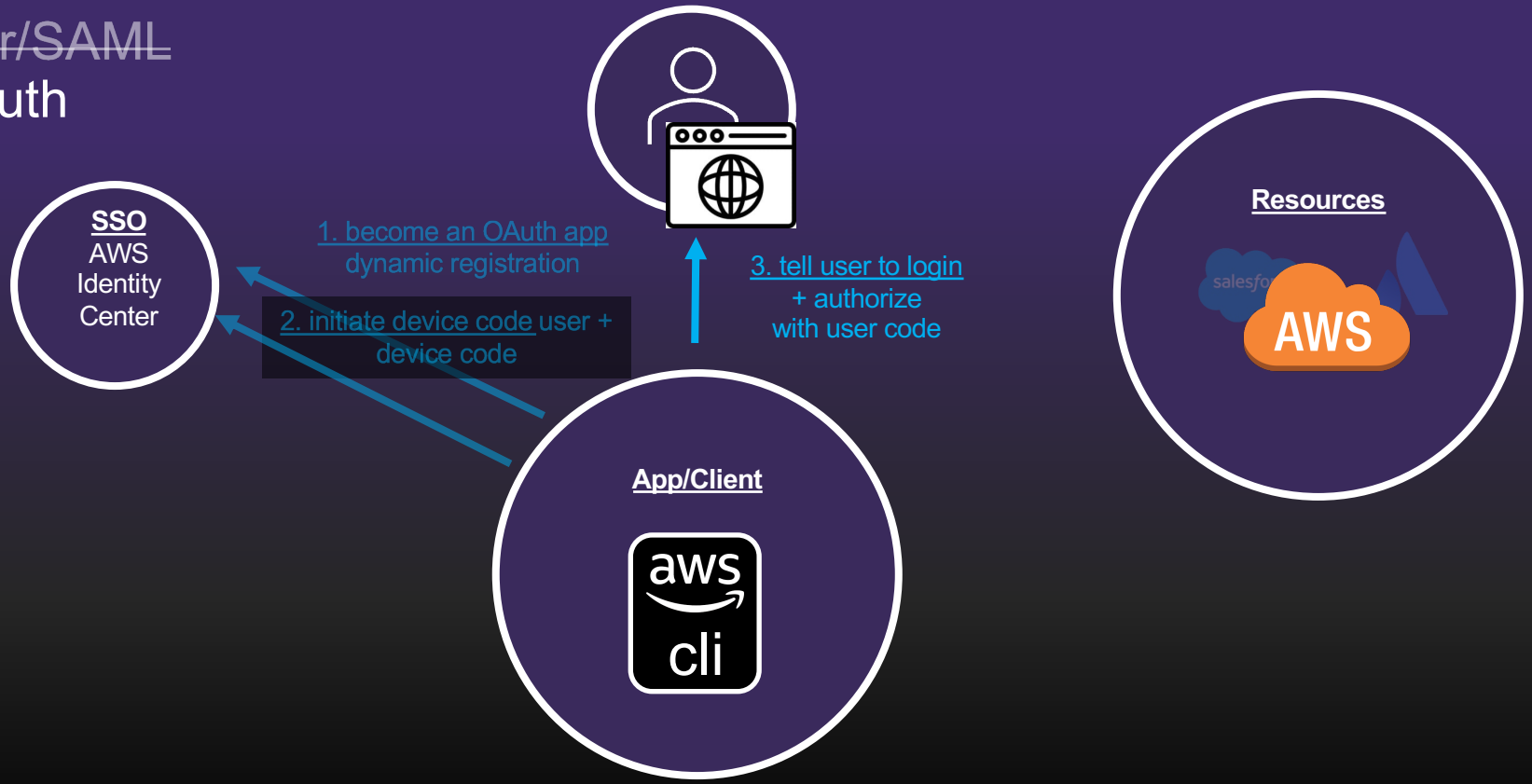

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~

CLI/OAuth



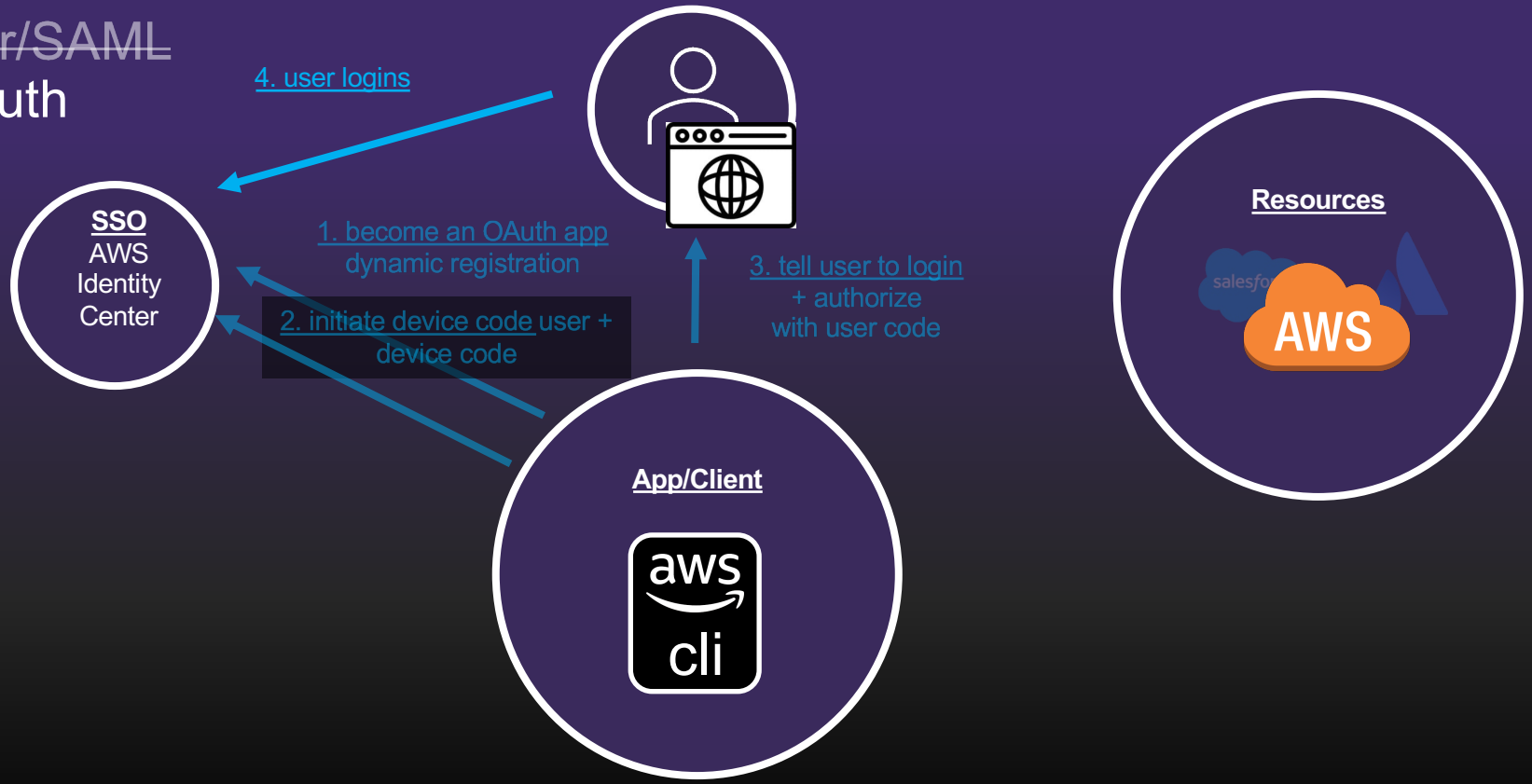
"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~

CLI/OAuth



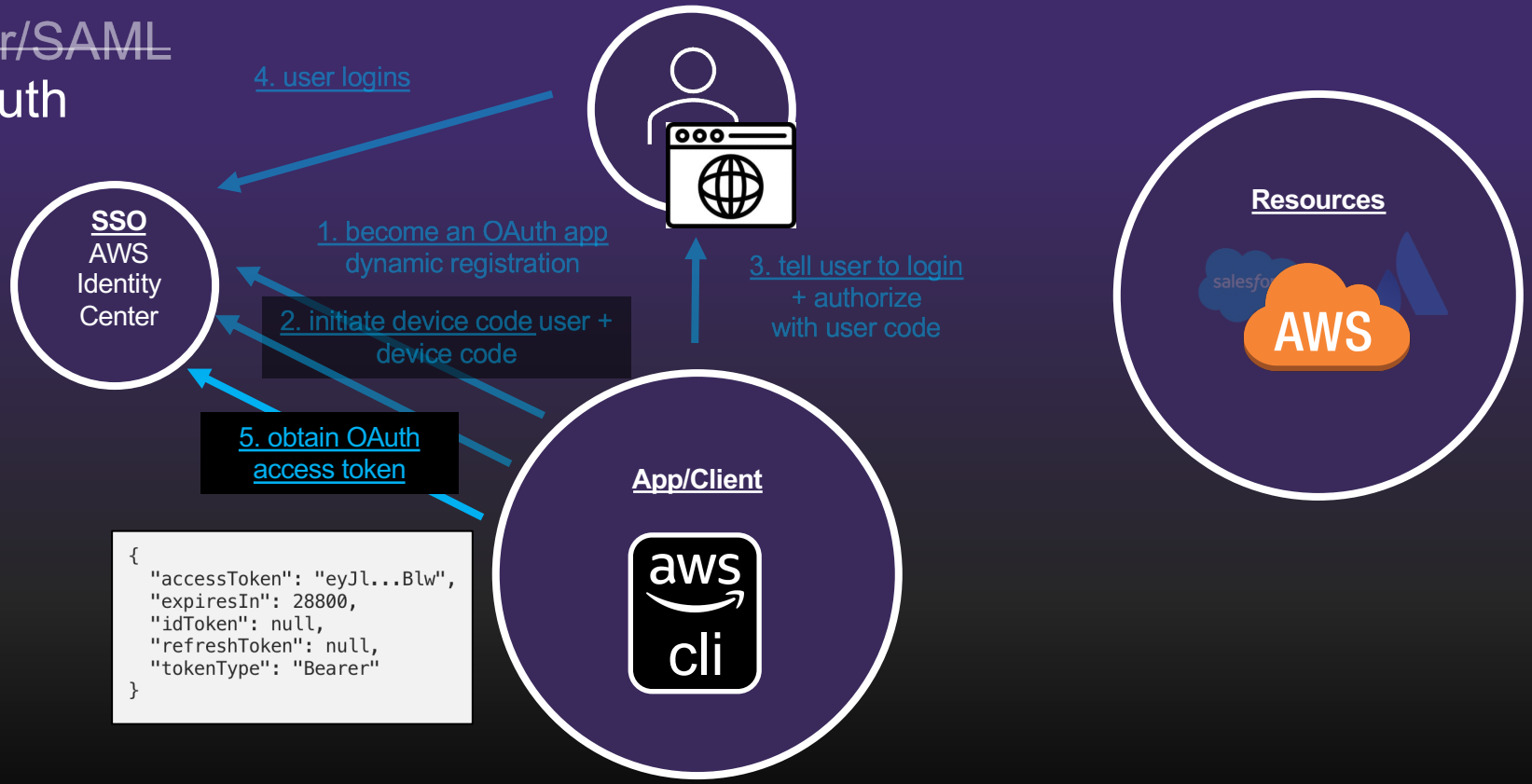
"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~

CLI/OAuth



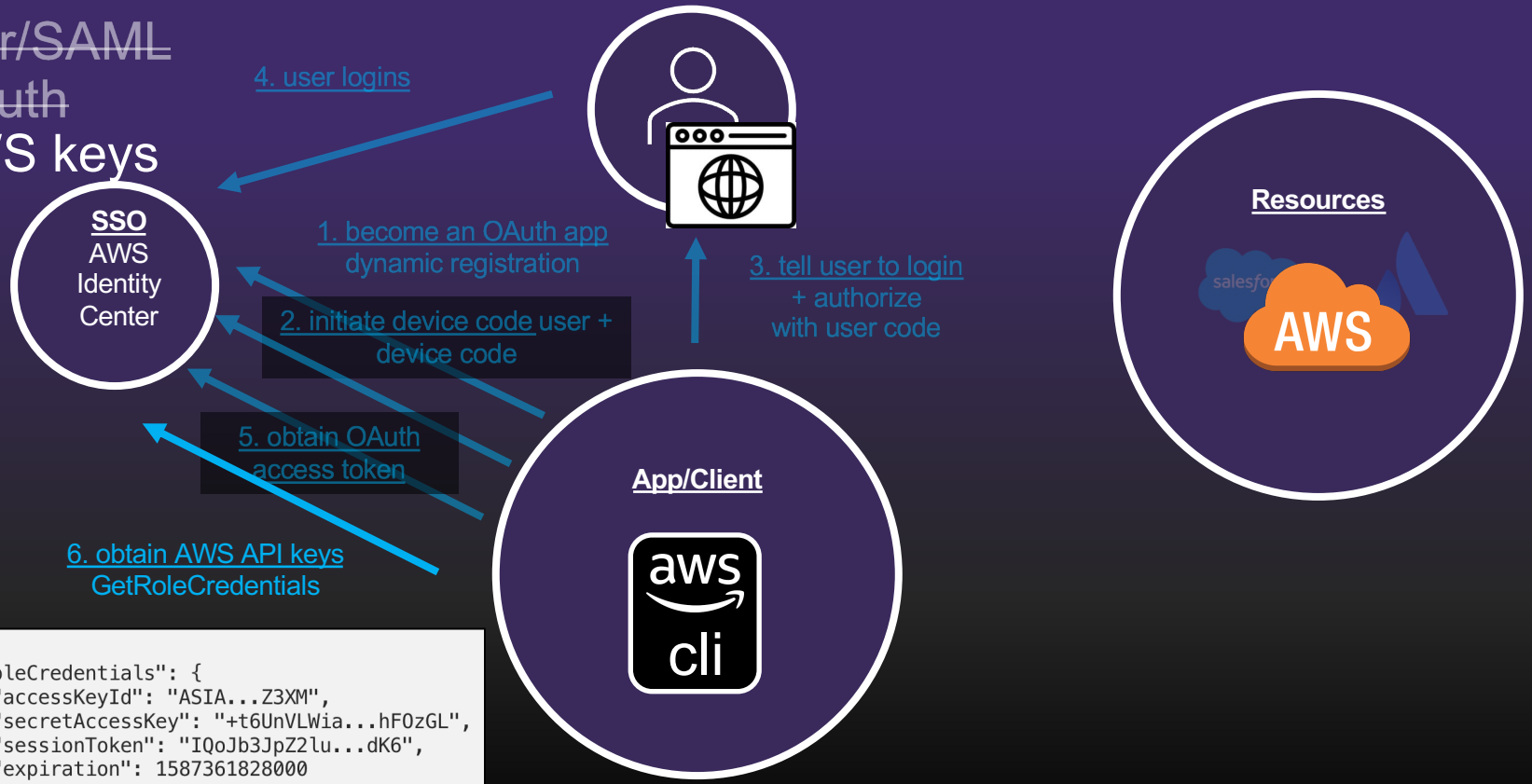

```
{
  "accessToken": "eyJl...Blw",
  "expiresIn": 28800,
  "idToken": null,
  "refreshToken": null,
  "tokenType": "Bearer"
}
```

"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~
~~CLI/OAuth~~
CLI/AWS keys



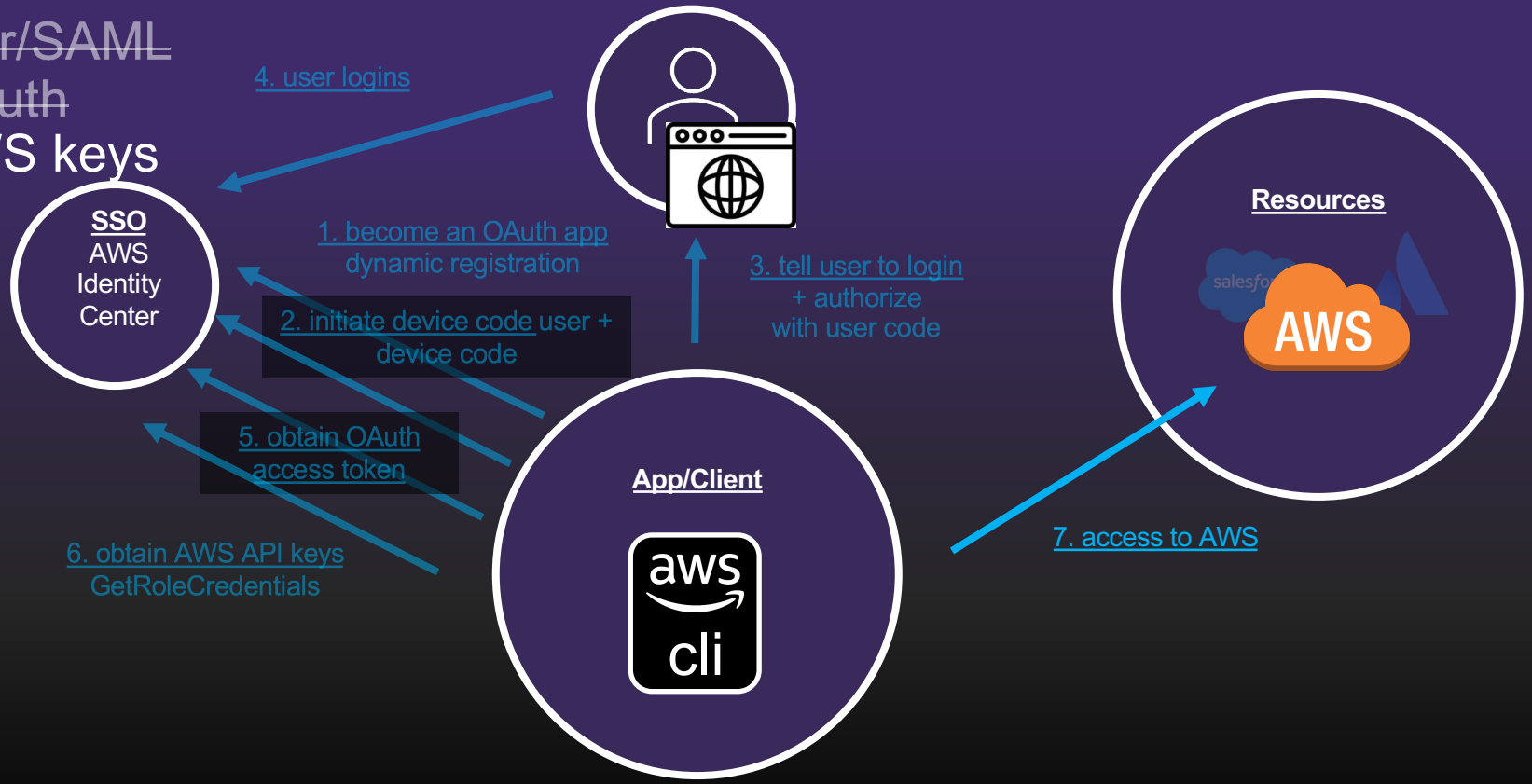

```
{
  "roleCredentials": {
    "accessKeyId": "ASIA...Z3XM",
    "secretAccessKey": "+t6UnVLWia...hFOzGL",
    "sessionToken": "IQoJb3JpZ2lu...dK6",
    "expiration": 1587361828000
  }
}
```

"Phishing cation," Christophe Tafani-Dereeper (6/9/2021)
https://blo o-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~
~~CLI/OAuth~~
CLI/AWS keys

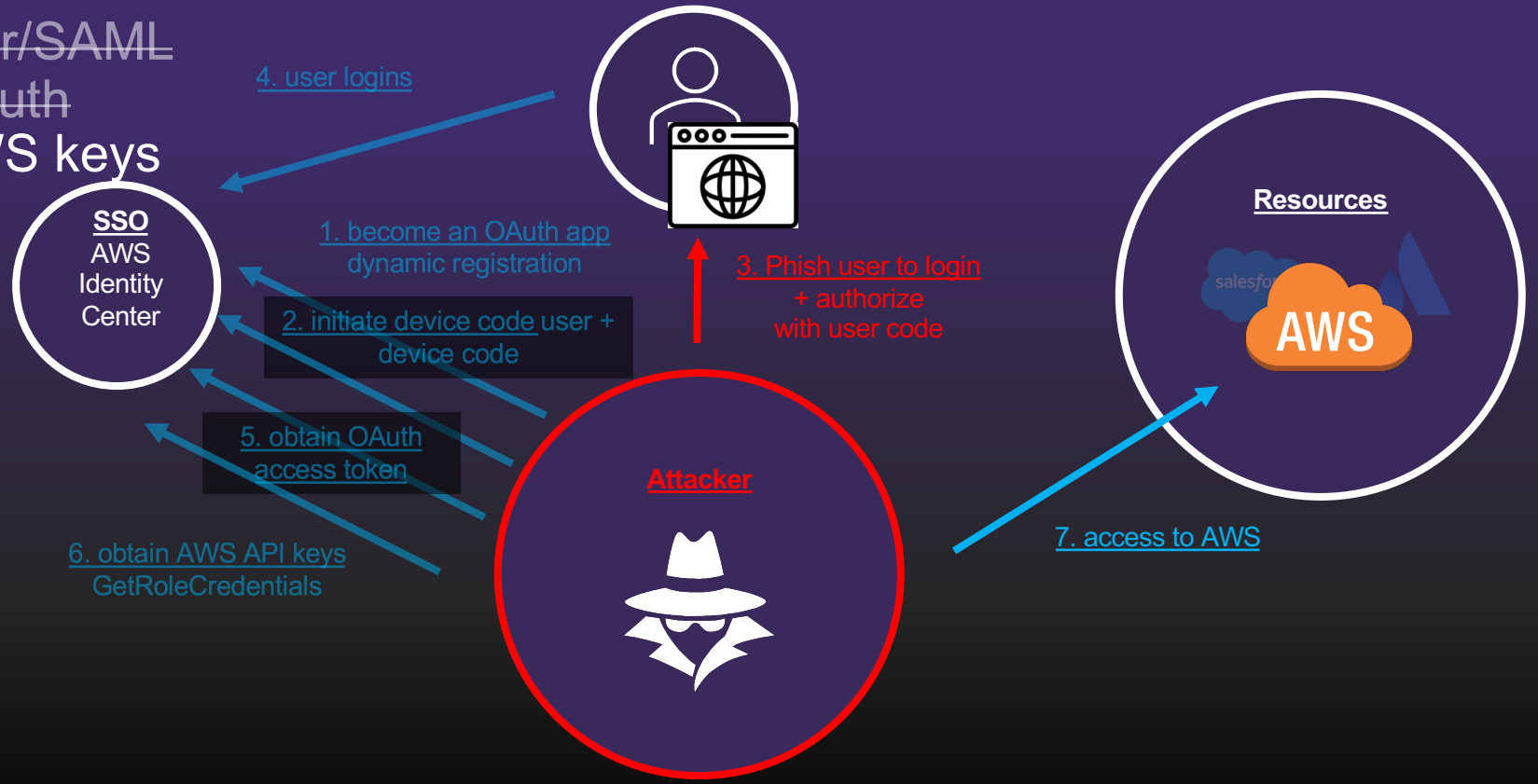


"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

© 2023 Jenko Hwong

Protocol Abuses: AWS SSO

~~Browser/SAML~~
~~CLI/OAuth~~
CLI/AWS keys



"Phishing for AWS credentials via AWS SSO device code authentication," Christophe Tafani-Dereeper (6/9/2021)
https://blog.christophetd.fr/phishing-for-aws-credentials-via-aws-sso-device-code-authentication/
"Anatomy of AWS SSO' Device Authorization Grant," Alex Berger (4/29/2020)
https://medium.com/@lex.berger/anatomy-of-aws-sso-device-authorization-grant-2839008c367a

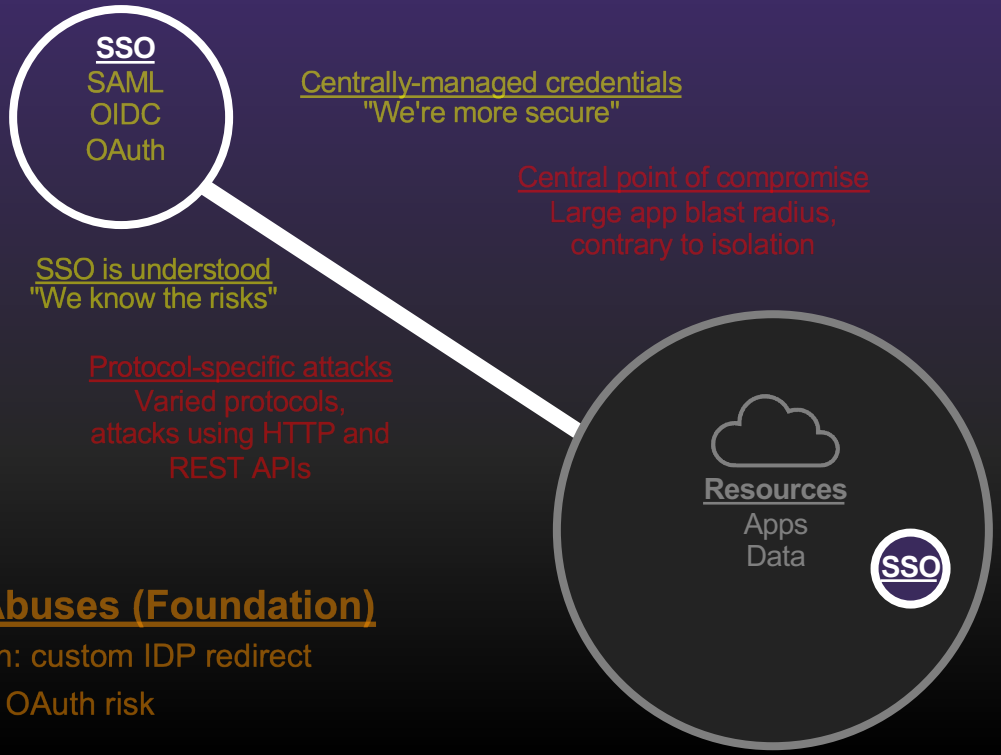
© 2023 Jenko Hwong

Assumptions

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

Piece-meal security 👍
"We've secured the pieces"



Centrally-managed credentials
"We're more secure"

Central point of compromise
Large app blast radius,
contrary to isolation

SSO is understood
"We know the risks"

Protocol-specific attacks
Varied protocols,
attacks using HTTP and
REST APIs

Protocol Abuses (Foundation)

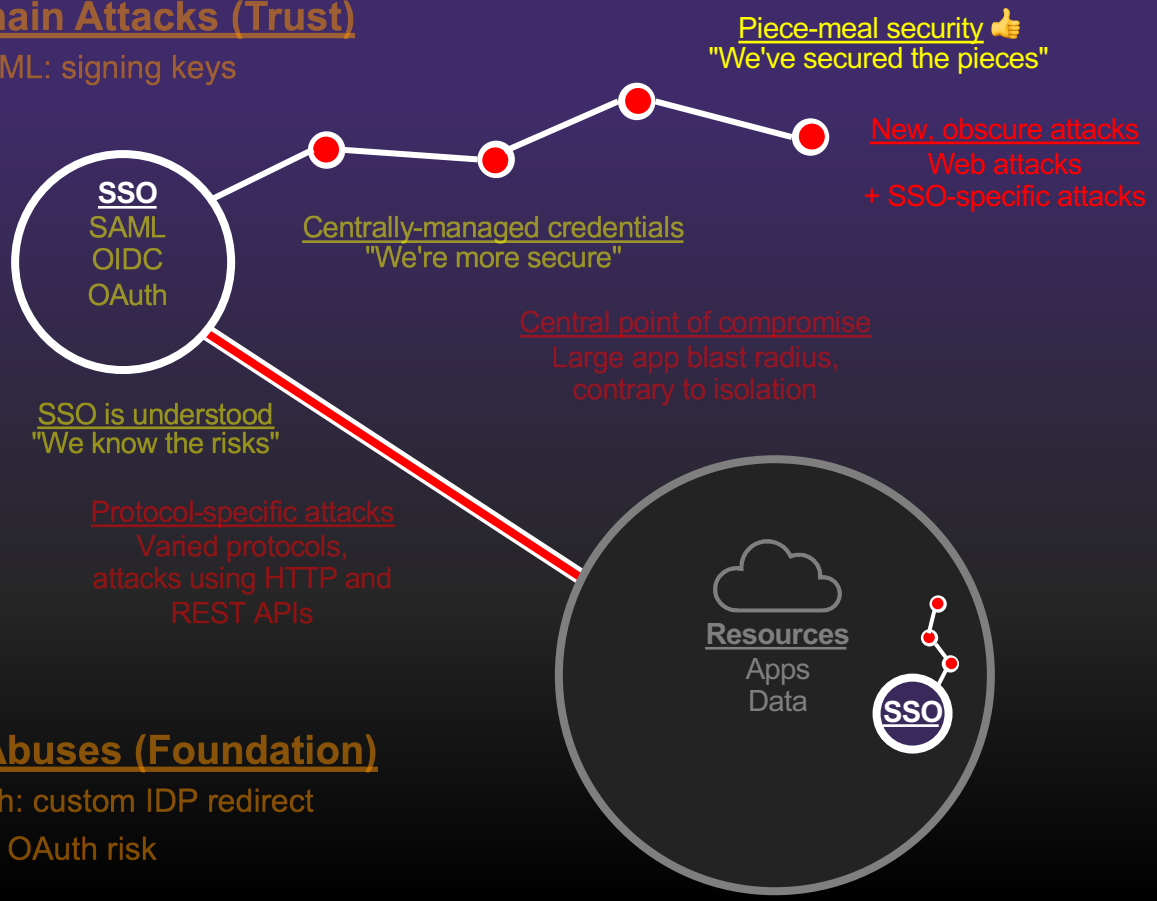
- SAML Phish: custom IDP redirect
- AWS SSO: OAuth risk

© 2023 Jenko Hwong

Assumptions → Risk

Supply Chain Attacks (Trust)

- Golden SAML: signing keys



Protocol Abuses (Foundation)

- SAML Phish: custom IDP redirect
- AWS SSO: OAuth risk

© 2023 Jenko Hwong

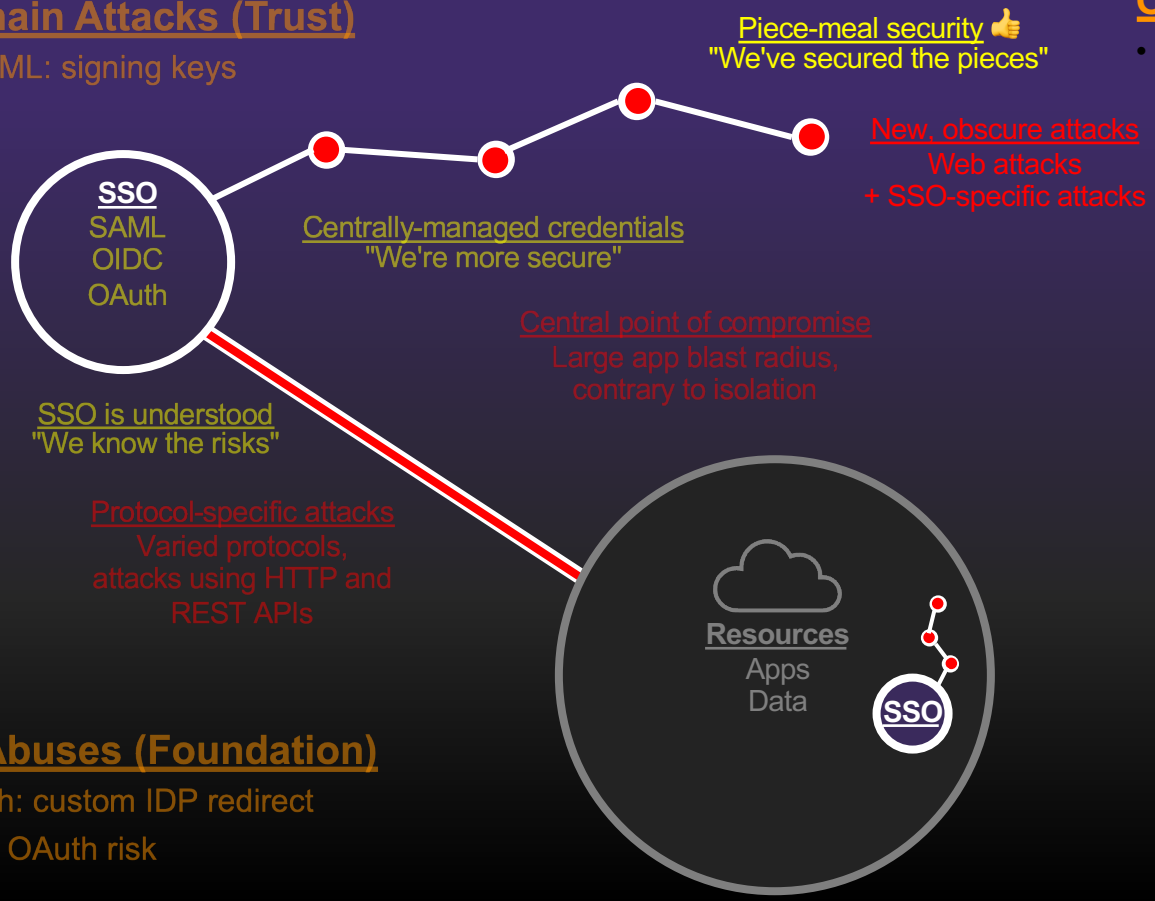
Assumptions → Risk → Abuse

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

Obfuscated Attacks (Magic)

- FB-Google SSO: web + OAuth == chain of confusion



Protocol Abuses (Foundation)

- SAML Phish: custom IDP redirect
- AWS SSO: OAuth risk

© 2023 Jenko Hwong

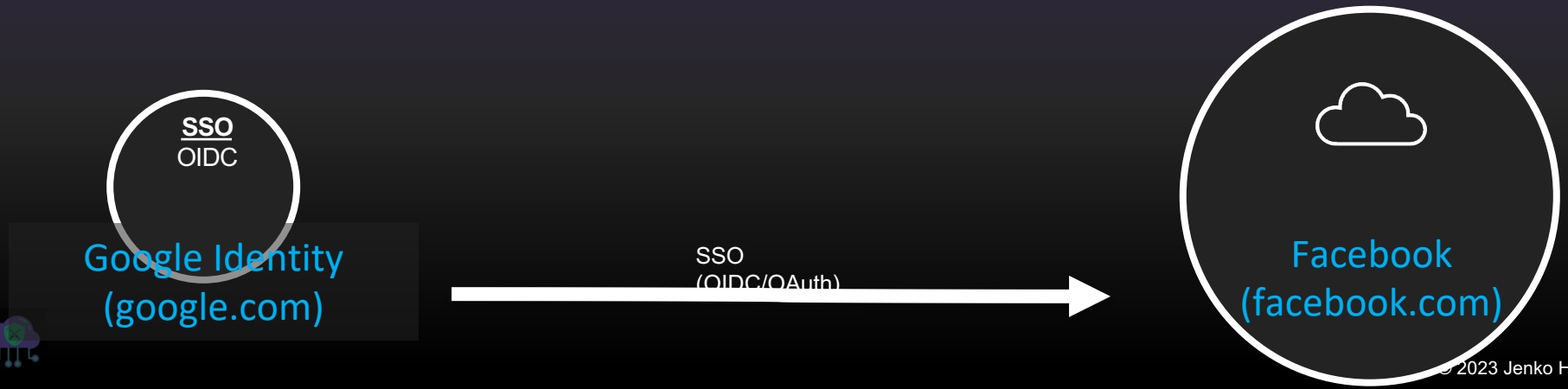
Obfuscated Attacks: FB ATO-Google SSO

© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

[1] Youssef Sammouda, 5/14/22: Multiple bugs chained to takeover Facebook Accounts which uses Gmail, https://ysamm.com/?p=763

[2] Malwarebytes, 5/17/22: https://www.malwarebytes.com/blog/news/2022/05/gmail-linked-facebook-accounts-vulnerable-to-attack-using-a-chain-of-bugs-now-fixed



© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

[1] Youssef Sammouda, 5/14/22: Multiple bugs chained to takeover Facebook Accounts which uses Gmail, https://ysamm.com/?p=763

[2] Malwarebytes, 5/17/22: https://www.malwarebytes.com/blog/news/2022/05/gmail-linked-facebook-accounts-vulnerable-to-attack-using-a-chain-of-bugs-now-fixed

Playground with user upload of custom HTML

Facebook Sandbox (fbsbx.com)

Hosted Captcha during password reset

SSO
OIDC

Google Identity (google.com)

SSO (OIDC/OAuth)

Facebook (facebook.com)

© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

[1] Youssef Sammouda, 5/14/22: Multiple bugs chained to takeover Facebook Accounts which uses Gmail, https://ysamm.com/?p=763

[2] Malwarebytes, 5/17/22: https://www.malwarebytes.com/blog/news/2022/05/gmail-linked-facebook-accounts-vulnerable-to-attack-using-a-chain-of-bugs-now-fixed

Facebook Sandbox (fbsbx.com)

Sandbox allows XSS+CSRF attacks

Captcha iFrame (Checkpoint State)
- account verification, pwd reset
- data leakage of referer as GET param

https://www.fbsbx.com/captcha/recaptcha/iFrame/?referer=https://www.facebook.com/checkpoint/?next=<google_oauth_resp_with_access_token>

Checkpoint State: OAuth token can be resent

Google Identity (google.com)

Facebook (facebook.com)

© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

Facebook Sandbox
(fbsbx.com)

1 Upload custom HTML
with **XSS+CSRF** attacks
(logout & login)

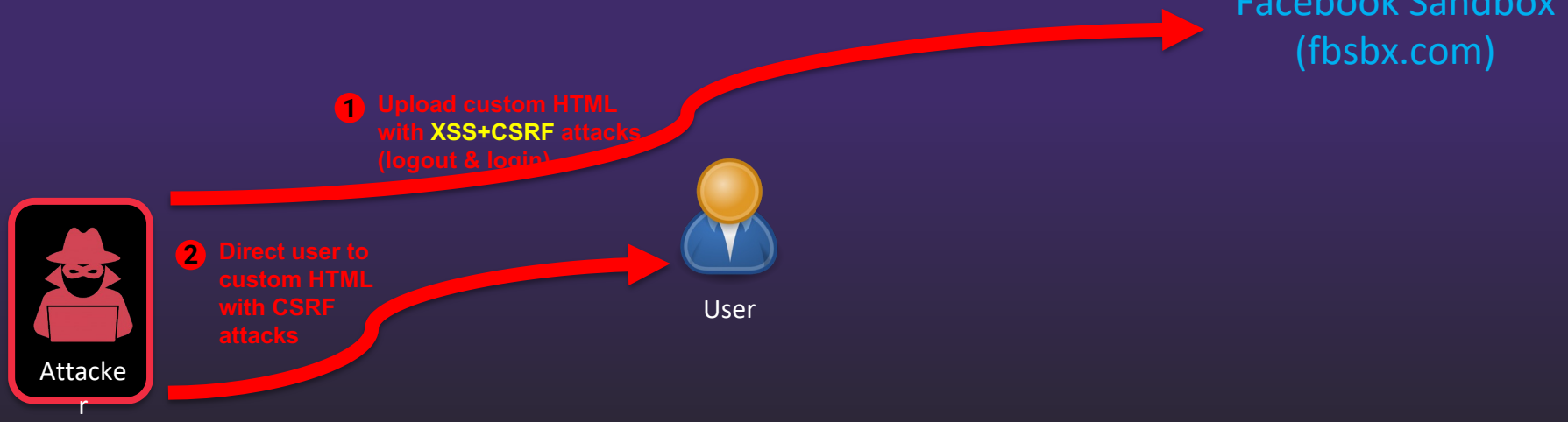
User

Google Identity
(google.com)

Facebook
(facebook.com)

© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

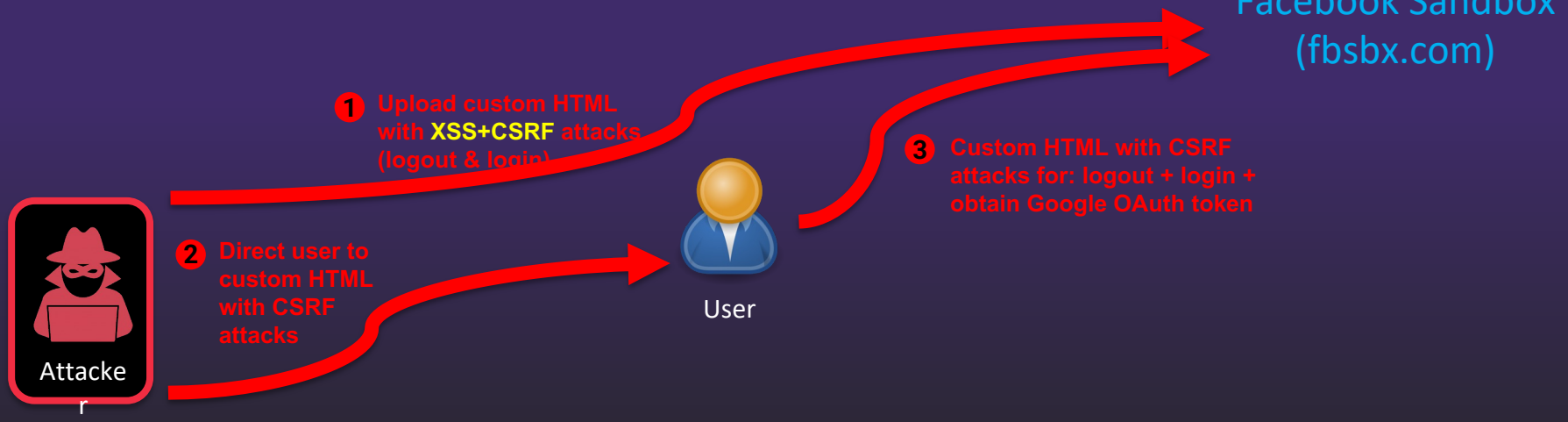


Google Identity
(google.com)

Facebook
(facebook.com)

© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

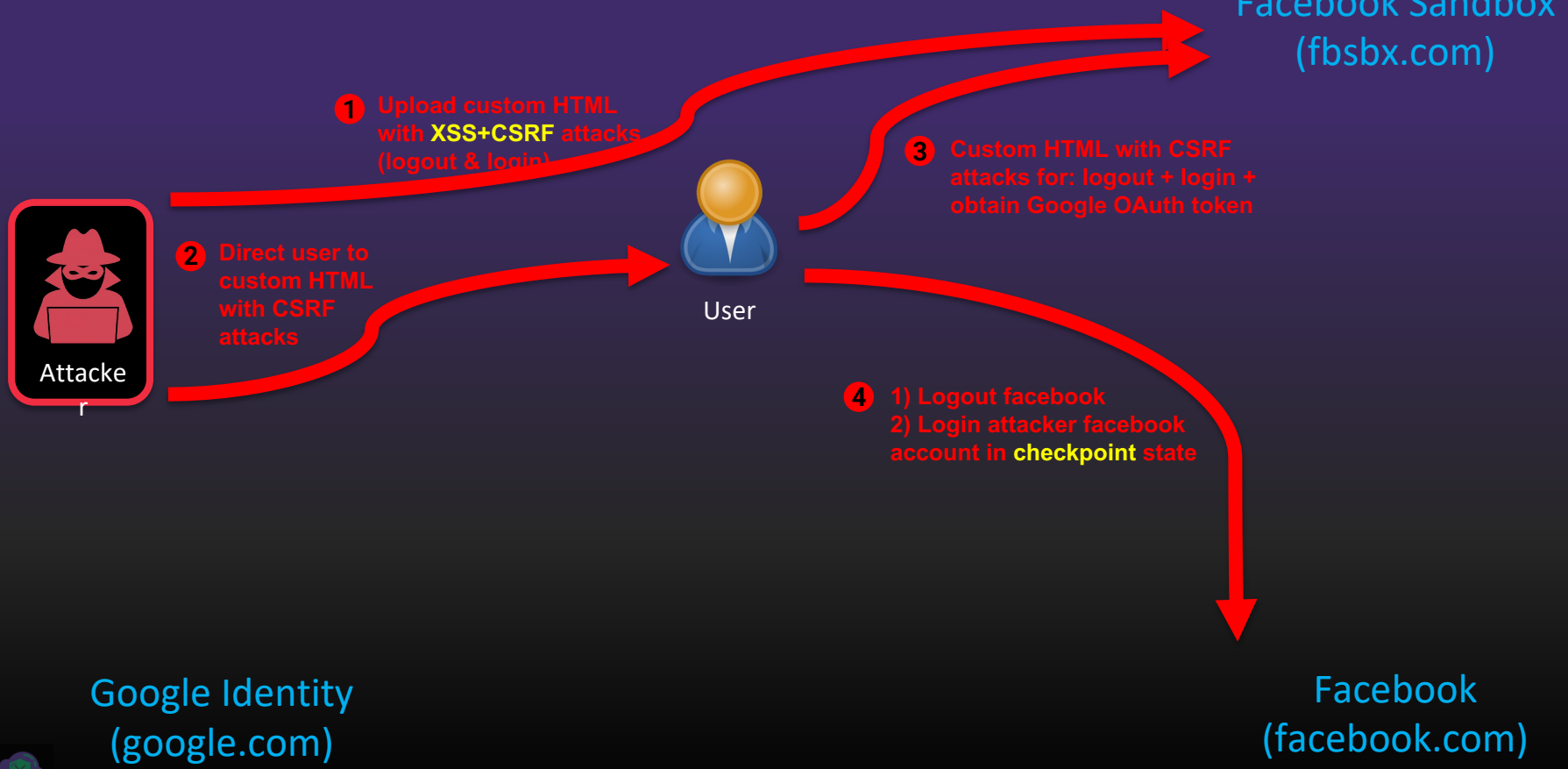


Google Identity
(google.com)

Facebook
(facebook.com)

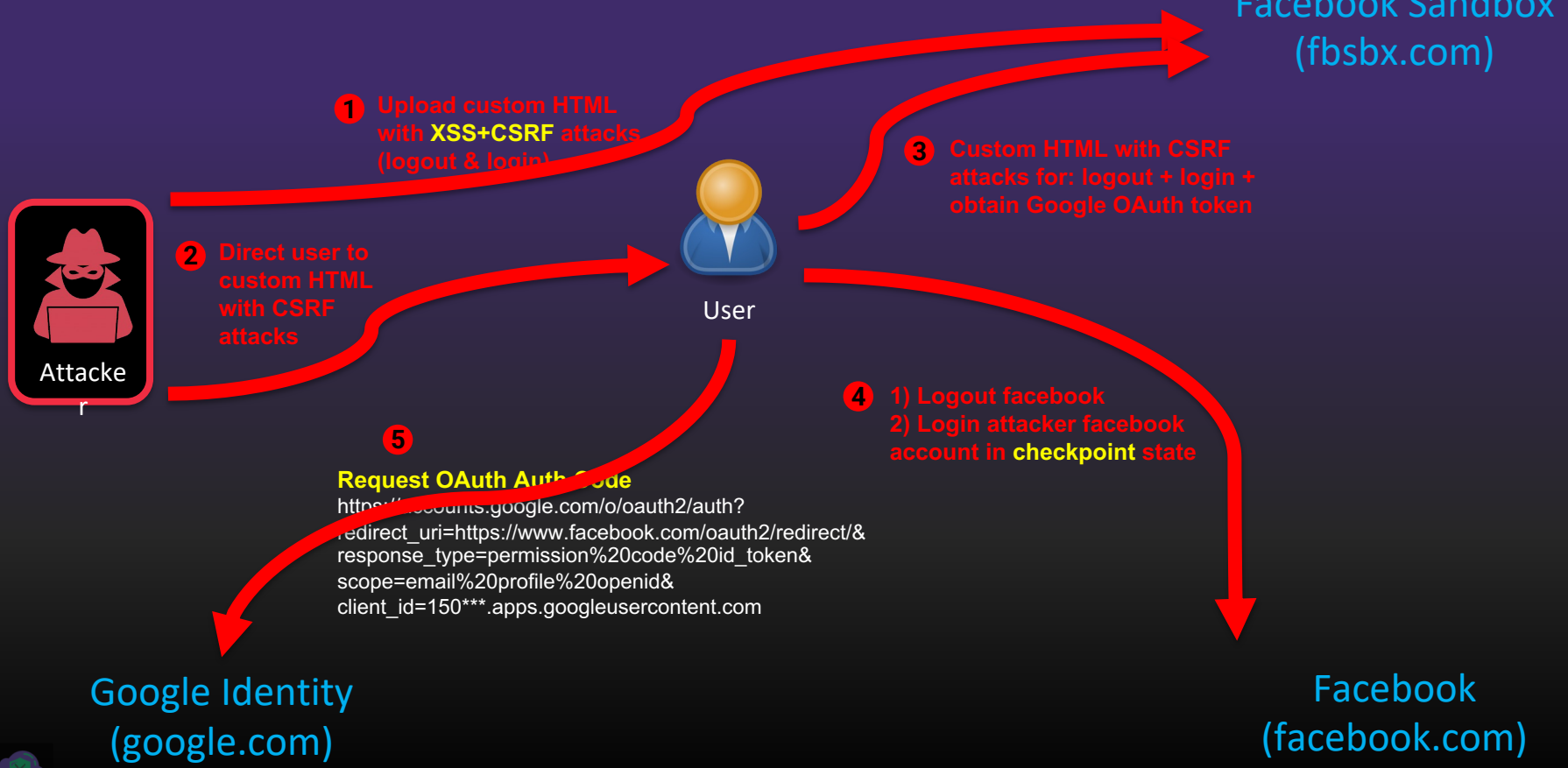
© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO



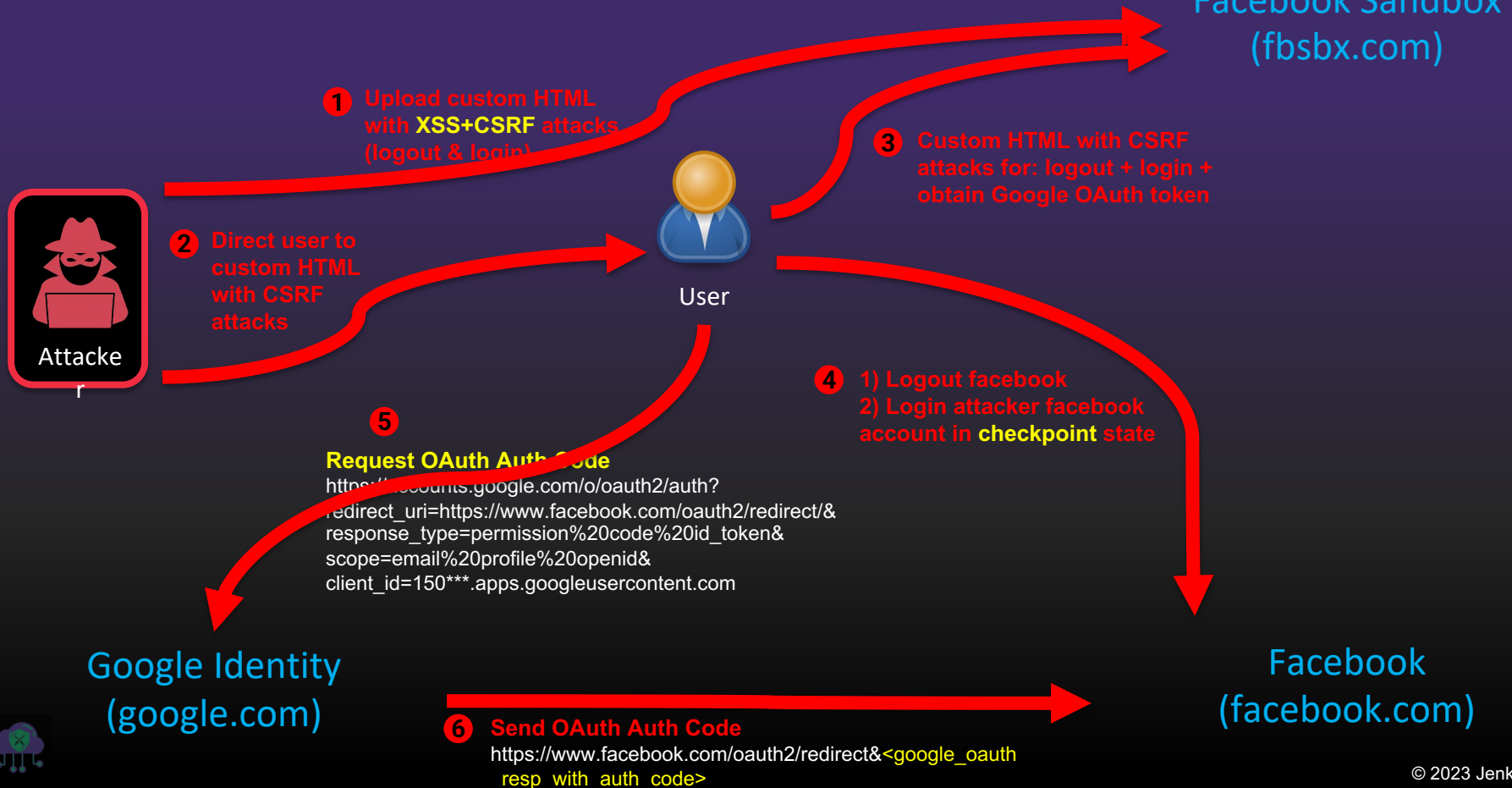
© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO



© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO



© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO

Facebook Sandbox
(fbsbx.com)

1 Upload custom HTML with **XSS+CSRF** attacks (logout & login)

2 Direct user to custom HTML with CSRF attacks

3 Custom HTML with CSRF attacks for: logout + login + obtain Google OAuth token

4 1) Logout facebook
2) Login attacker facebook account in **checkpoint** state

5 **Request OAuth Auth Code**
https://accounts.google.com/o/oauth2/auth?
redirect_uri=https://www.facebook.com/oauth2/redirect/&
response_type=permission%20code%20id_token&
scope=email%20profile%20openid&
client_id=150***.apps.googleusercontent.com

6 **Send OAuth Auth Code**
https://www.facebook.com/oauth2/redirect&<google_oauth_resp_with_auth_code>

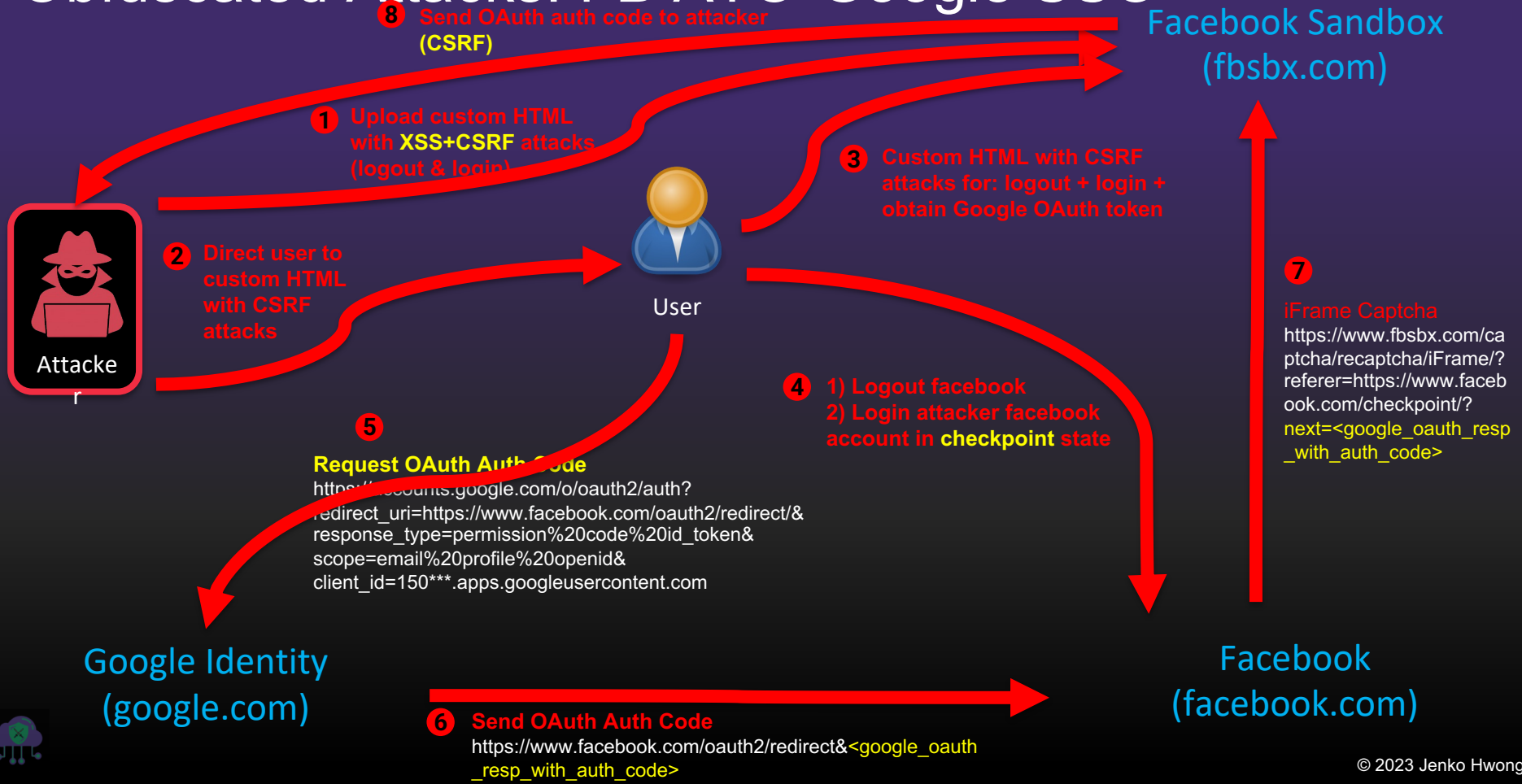
7 iFrame Captcha
https://www.fbsbx.com/captcha/recaptcha/iFrame/?referer=https://www.facebook.com/checkpoint/?next=<google_oauth_resp_with_auth_code>

Google Identity
(google.com)

Facebook
(facebook.com)

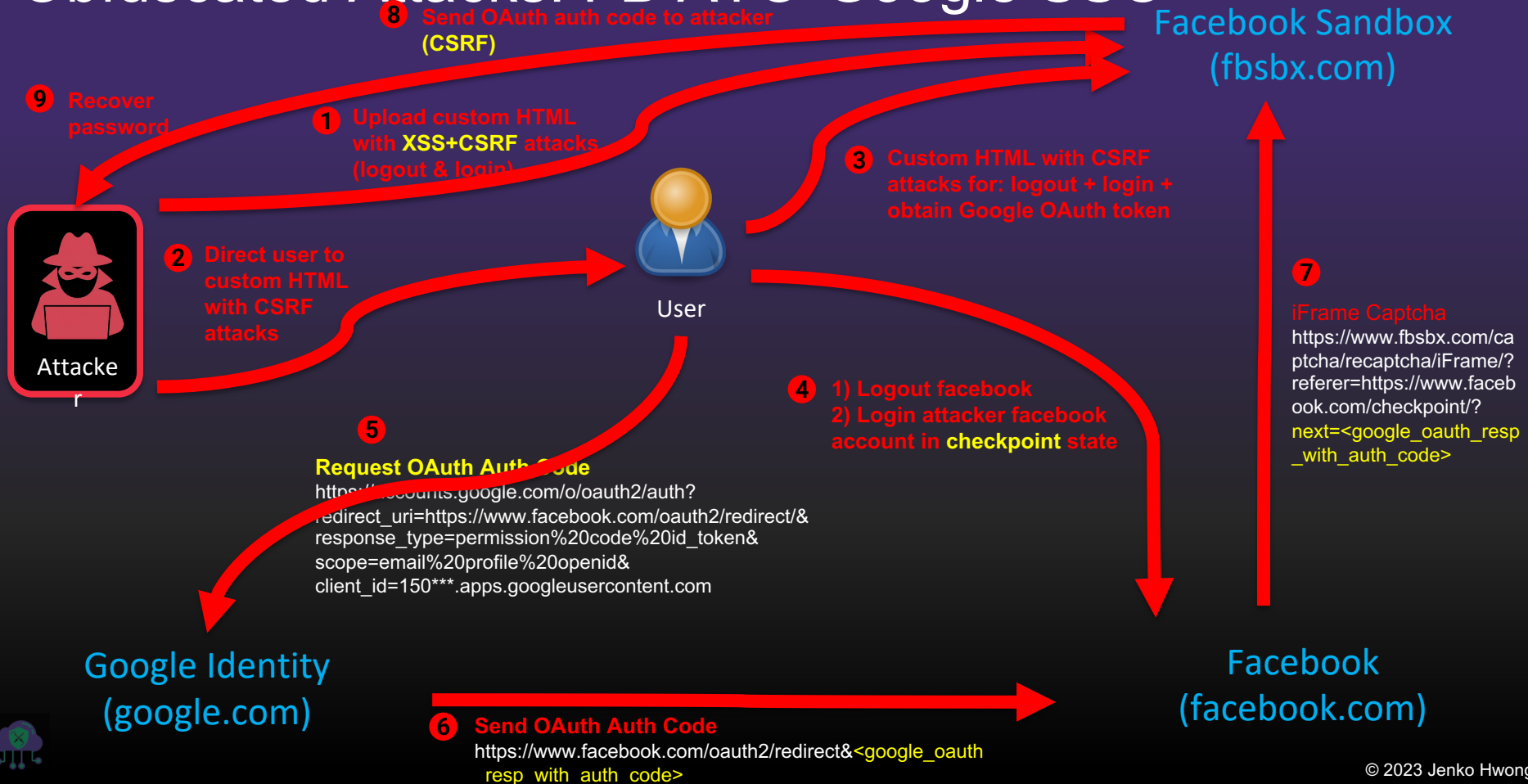
© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO



© 2023 Jenko Hwong

Obfuscated Attacks: FB ATO-Google SSO



© 2023 Jenko Hwong

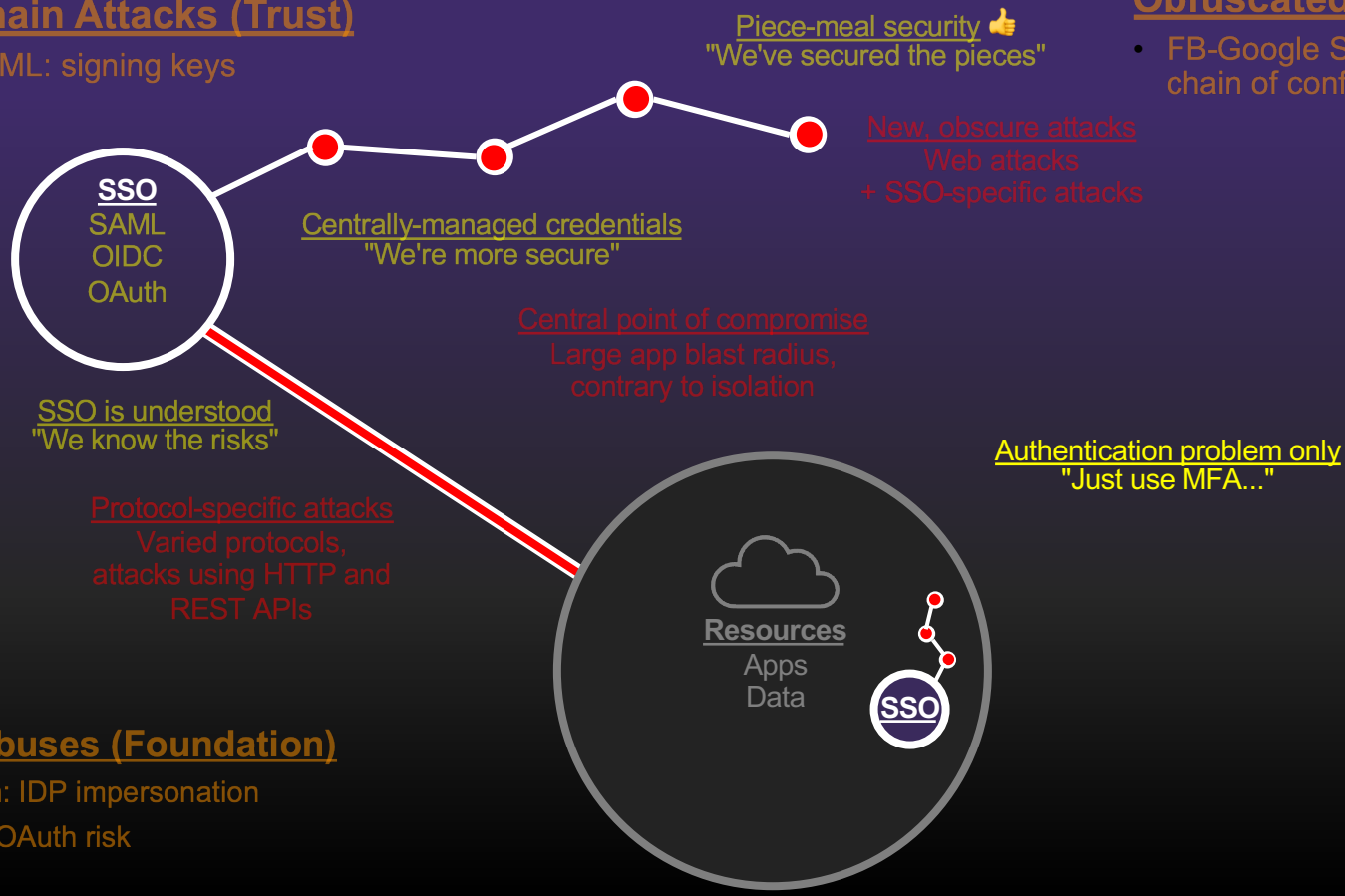
Assumptions

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

Obfuscated Attacks (Magic)

- FB-Google SSO: web + OAuth == chain of confusion



Protocol Abuses (Foundation)

- SAML Phish: IDP impersonation
- AWS SSO: OAuth risk

© 2023 Jenko Hwong

Assumptions → Risk

Supply Chain Attacks (Trust)

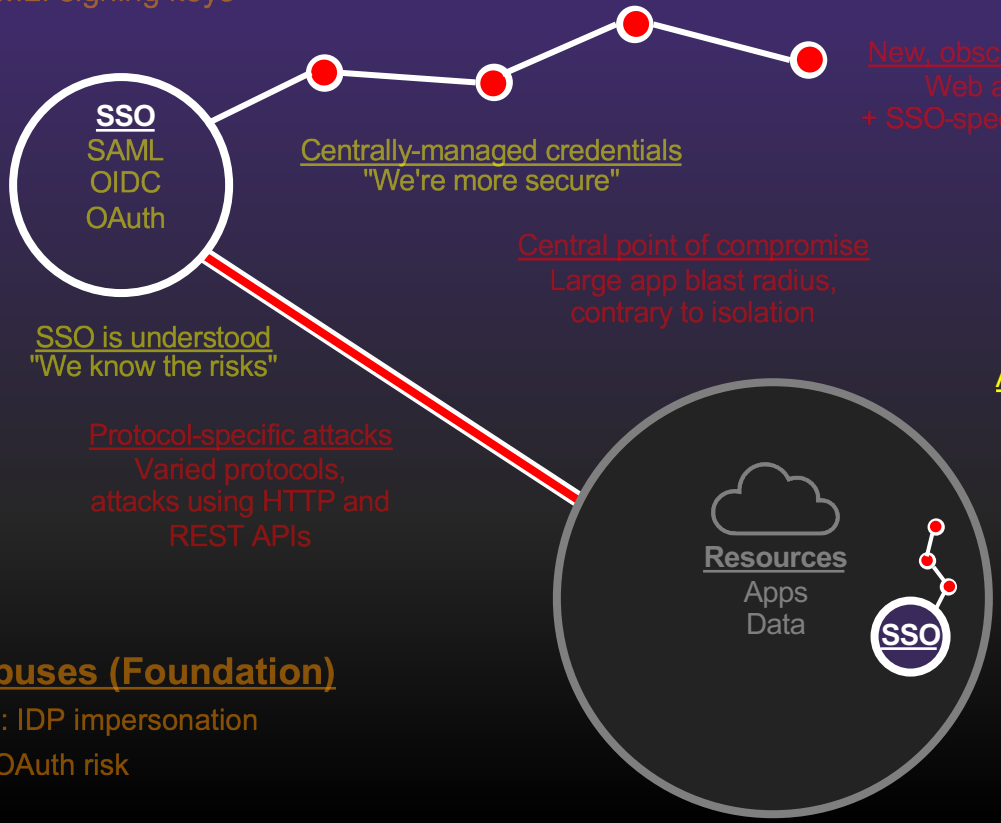
- Golden SAML: signing keys

Obfuscated Attacks (Magic)

- FB-Google SSO: web + OAuth == chain of confusion

Piece-meal security 👍
"We've secured the pieces"

New, obscure attacks
Web attacks
+ SSO-specific attacks



Centrally-managed credentials
"We're more secure"

Central point of compromise
Large app blast radius,
contrary to isolation

SSO is understood
"We know the risks"

Protocol-specific attacks
Varied protocols,
attacks using HTTP and
REST APIs

Authentication problem only
"Just use MFA..."

Wide-spread Impact
One compromised app
gives access to all apps/data

Protocol Abuses (Foundation)

- SAML Phish: IDP impersonation
- AWS SSO: OAuth risk

© 2023 Jenko Hwong

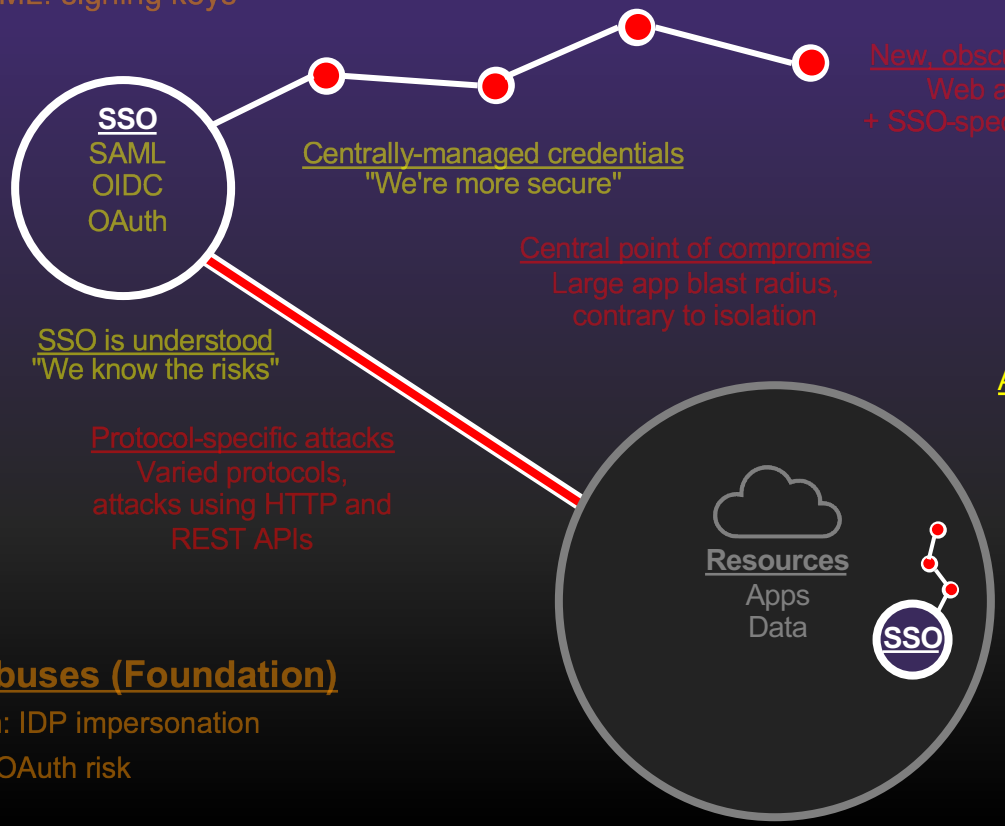
Assumptions → Risk → Abuse

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

Obfuscated Attacks (Magic)

- FB-Google SSO: web + OAuth == chain of confusion



Protocol Abuses (Foundation)

- SAML Phish: IDP impersonation
- AWS SSO: OAuth risk

Pivots (Blast Radius)

- Microsoft Device Code Phish: OAuth risk

© 2023 Jenko Hwong

Pivots: Microsoft Device Code Phish[1][2]

[1] Dr. Nestori Syynimaa (@DrAzureAD), 10/13/20, https://o365blog.com/post/phishing
[2] Ryan Marcotte Cobb, Tony Gore, 3/23/22, https://github.com/secureworks/family-of-client-ids-research

© 2023 Jenko Hwong

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Sign in to your account

login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4...

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

Sign-in options

Terms of use Privacy & cookies

Attacker

```
attacker-host:~ $ clear
```

ks Exploiting OAuth
ion Flows

7, 2021

twong
skope.com
nwong

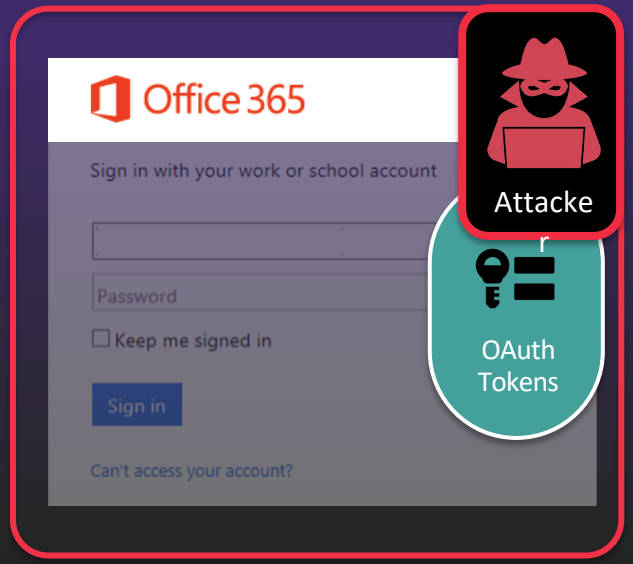
Notes Comments 220%

Pivots: Microsoft Device Code Phish[1][2]

1 Assumed Application Identity

Authorization

Cloud Data, Compute, Users



SSO & OAuth Conflicts

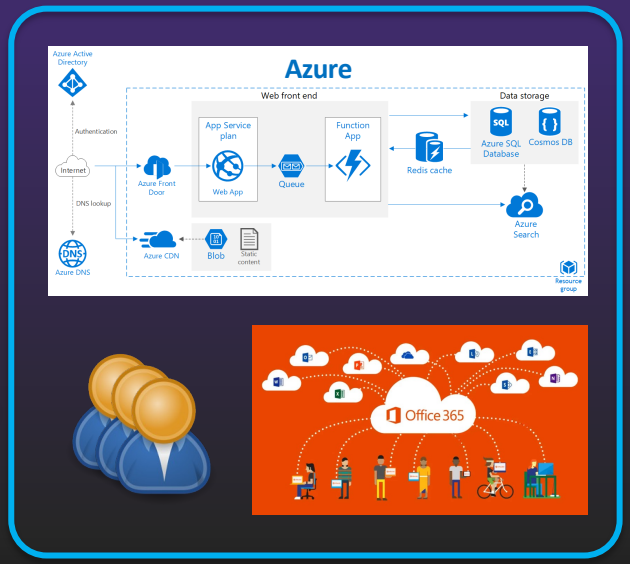
lateral movement[2]

5 Access

API Calls

Office 365 -> Azure

4 Token



2 Phish

3 Authenticate, ~~Authorize~~

https://microsoft.com/...

Azure

User

Username Password

[1] Dr. Nestori Syynimaa (@DrAzureAD), 10/13/20, https://o365blog.com/post/phishing
[2] Ryan Marcotte Cobb, Tony Gore, 3/23/22, https://github.com/secureworks/family-of-client-ids-research

© 2023 Jenko Hwong

Pivots: Microsoft Device Code Phish[1][2][3][4]

TeamFiltration Tool [4]

- Password spraying
- Data exfiltration across SSO apps

client_id	application_name
00b41c95-dab0-4487-9791-b9d2c32c80f2	Office 365 Management
04b07795-8ddb-461a-bbee-02f9e1bf7b46	Microsoft Azure CLI
1950a258-227b-4e31-a9cf-717495945fc2	Microsoft Azure PowerShell
1fec8e78-bce4-4aaf-ab1b-5451cc387264	Microsoft Teams
26a7ee05-5602-4d76-a7ba-eae8b7b67941	Windows Search
27922004-5251-4030-b22d-91ecd9a37ea4	Outlook Mobile
4813382a-8fa7-425e-ab75-3b753aab3abb	Microsoft Authenticator App
ab9b8c07-8f02-4f72-87fa-80105867a763	OneDrive SyncEngine
d3590ed6-52b3-4102-aeff-aad2292ab01c	Microsoft Office
872cd9fa-d31f-45e0-9eab-6e460a02d1f1	Visual Studio
af124e86-4e96-495a-b70a-90f90ab96707	OneDrive iOS App
2d7f3606-b07d-41d1-b9d2-0d0c9296a6e8	Microsoft Bing Search for Microsoft Edge
844cca35-0656-46ce-b636-13f48b0eecbd	Microsoft Stream Mobile Native
87749df4-7ccf-48f8-aa87-704bad0e0e16	Microsoft Teams - Device Admin Agent
cf36b471-5b44-428c-9ce7-313bf84528de	Microsoft Bing Search
0ec893e0-5785-4de6-99da-4ed124e5296c	Office UWP PWA
22098786-6e16-43cc-a27d-191a01a1e3b5	Microsoft To-Do client
4e291c71-d680-4d0e-9640-0a3358e31177	PowerApps
57336123-6e14-4acc-8dcf-287b6088aa28	Microsoft Whiteboard Client
57fcbcfa-7cee-4eb1-8b25-12d2030b4ee0	Microsoft Flow
66375f6b-983f-4c2c-9701-d680650f588f	Microsoft Planner
9ba1a5c7-f17a-4de9-a1f1-6178c8d51223	Microsoft Intune Company Portal
a40d7d7d-59aa-447e-a655-679a4107e548	Accounts Control UI
a569458c-7f2b-45cb-bab9-b7dee514d112	Yammer iPhone
b26aadf8-566f-4478-926f-589f601d9c74	OneDrive
c0d2a505-13b8-4ae0-aa9e-cddd5eab0b12	Microsoft Power BI
d326c1ce-6cc6-4de2-bebc-4591e5e13ef0	SharePoint
e9c51622-460d-4d3d-952d-966a5b1da34c	Microsoft Edge
eb539595-3fe1-474e-9c1d-feb3625d1be5	Microsoft Tunnel
ecd6b820-32c2-49b6-98a6-444530e5a77a	Microsoft Edge
f05ff7c9-f75a-4acd-a3b5-f4b6a870245d	SharePoint Android
f44b1140-bc5e-48c6-8dc0-5cf5a53c0e34	Microsoft Edge

[1] Dr. Nestori Syynimaa (@DrAzureAD), 10/13/20, https://o365blog.com/post/phishing
[2] Ryan Marcotte Cobb, Tony Gore, 3/23/22, https://github.com/secureworks/family-of-client-ids-research
[3] Melvin Langvik, Taking a Dump In The Cloud, https://www.youtube.com/watch?v=GpZTQHLKelg
[4] Melvin Langvik, TeamFiltration, https://github.com/Flangvik/TeamFiltration

© 2023 Jenko Hwong

Assumptions → Risk → Abuse

Supply Chain Attacks (Trust)

- Golden SAML: signing keys

Obfuscated Attacks (Magic)

- FB-Google SSO: web + OAuth == chain of confusion

Piece-meal security 👍
"We've secured the pieces"

New, obscure attacks
Web attacks
+ SSO-specific attacks

SSO
SAML
OIDC
OAuth

Centrally-managed credentials
"We're more secure"

Central point of compromise
Large app blast radius,
contrary to isolation

SSO is understood
"We know the risks"

Authentication problem only
"Just use MFA..."

Protocol-specific attacks
Varied protocols,
attacks using HTTP and
REST APIs

Wide-spread Impact
One compromised app
gives access to all apps/data

Resources
Apps
Data

SSO

Protocol Abuses (Foundation)

- SAML Phish: IDP impersonation
- AWS SSO: OAuth risk

Pivots (Blast Radius)

- Microsoft Device Code Phish: OAuth risk

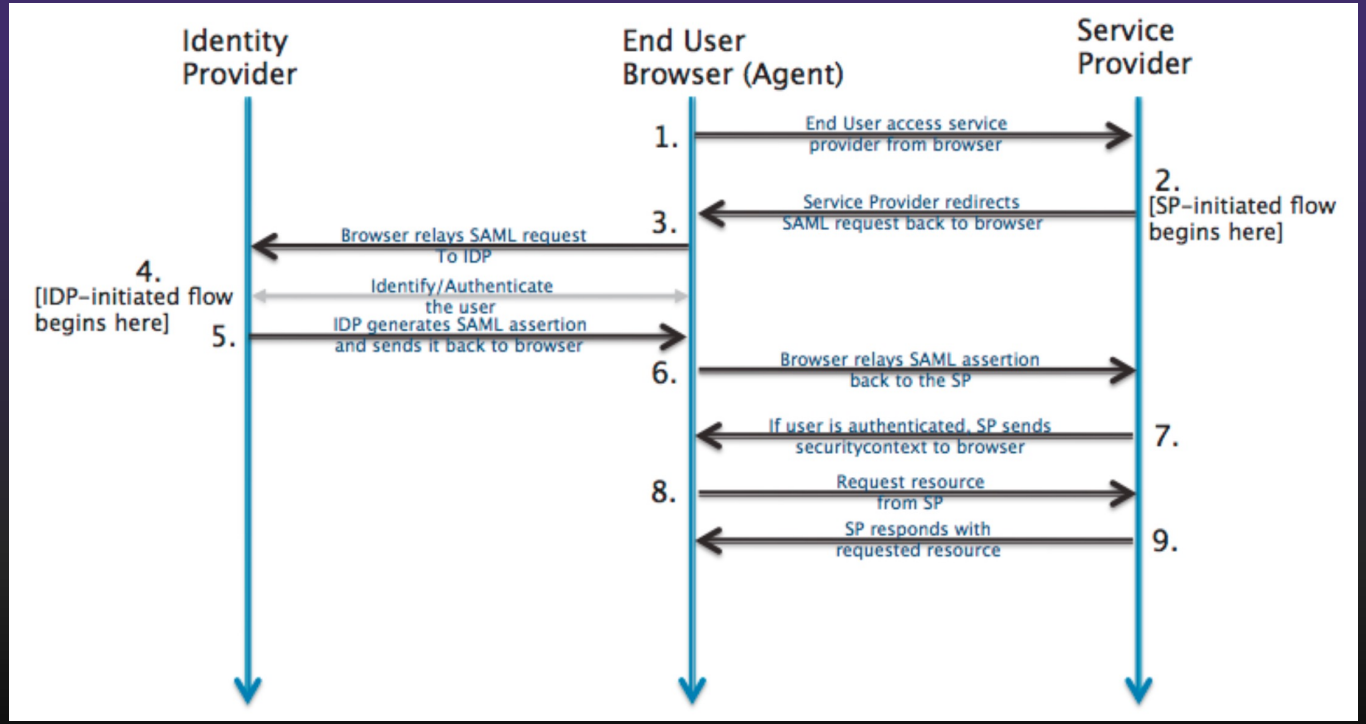
© 2023 Jenko Hwong

How/Why did we get here?

- Protocol Complexity
  - SAML
    - Local user account provisioning (SP)
    - User account information (dynamic lookup, replication/sync)
    - Endpoints, redirects, # attributes, validation/signing
  - OAuth: # parties, # flows, # R/T comms, REST-enabled
  - Varied implementations

© 2023 Jenko Hwong

SAML 2.0



https://developer.okta.com/docs/concepts/saml/#federated-identity

© 2023 Jenko Hwong

OAuth 2.0: Authorization Code Flow

```
     +----------+
     | Resource |
     |   Owner  |
     |          |
     +----------+
          ^
          |
         (B)
     +----|-----+          Client Identifier      +---------------+
     |         -+----(A)-- & Redirection URI ----->|               |
     |  User-   |                                 | Authorization |
     |  Agent  -+----(B)-- User authenticates --->|     Server    |
     |          |                                 |               |
     |         -+----(C)-- Authorization Code ---<|               |
     +-|----|---+                                 +---------------+
       |    |                                         ^      v
      (A)  (C)                                        |      |
       |    |                                         |      |
       ^    v                                         |      |
     +---------+                                      |      |
     |         |>---(D)-- Authorization Code ---------'      |
     |  Client |          & Redirection URI                 |
     |         |                                            |
     |         |<---(E)----- Access Token -------------------'
     +---------+       (w/ Optional Refresh Token)
```

REST APIs

Note: The lines illustrating steps (A), (B), and (C) are broken into two parts as they pass through the user-agent.

Figure 3: Authorization Code Flow

https://www.rfc-editor.org/rfc/rfc6749

© 2023 Jenko Hwong

OAuth 2.0: Device Code Flow

```
+----------+
| Resource |
|   Owner  |
|          |
+----------+
```

```
+----------+                                +----------------+
|          |>---(A)-- Client Identifier --->|                |
|          |                                |                |
|          |<---(B)-- Device Code,      ---<|                |
|          |          User Code,            |                |
|  Device  |          & Verification URI    |                |
|  Client  |                                |                |
|          |  [polling]                     |                |
|          |>---(E)-- Device Code       --->|                |
|          |          & Client Identifier   |                |
|          |                                |  Authorization |
|          |<---(F)-- Access Token      ---<|     Server     |
+----------+   (& Optional Refresh Token)   |                |
      v                                     |                |
      :                                     |                |
     (C) User Code & Verification URI       |                |
      :                                     |                |
      v                                     |                |
+----------+                                |                |
| End User |                                |                |
|    at    |<---(D)-- End user reviews  --->|                |
| Browser  |          authorization request |                |
+----------+                                +----------------+
```

REST APIs

Figure 1: Device Authorization Flow

https://www.rfc-editor.org/rfc/rfc8628

© 2023 Jenko Hwong

How/Why did we get here?

- Protocol Complexity
  - SAML
    - Local user account provisioning (SP)
    - User account information (dynamic lookup, replication/sync)
    - Endpoints, redirects, # attributes, validation/signing
  - OAuth: # parties, # flows, # R/T comms, REST-enabled
  - Varied implementations
- Leads to Obfuscation
  - Web attacks + (SAML|OIDC|OAuth custom)
  - SecOps controls lag: prevention, detection, remediation

© 2023 Jenko Hwong

How/Why did we get here?

- Protocol Complexity
  - SAML
    - Local user account provisioning (SP)
    - User account information (dynamic lookup, replication/sync)
    - Endpoints, redirects, # attributes, validation/signing
  - OAuth: # parties, # flows, # R/T comms, REST-enabled
  - Varied implementations
- Leads to Obfuscation
  - Web attacks + (SAML|OIDC|OAuth custom)
  - SecOps controls lag: prevention, detection, remediation
- And Mixing of Models, which leads to mistakes
  - Authentication (SSO/SAML) <=> Authorization (OAuth)
  - User/Manual <=> API/Automated
  - Browser Authentication (HTTP/UA) <=> API Authentication (Tokens, REST)

© 2023 Jenko Hwong

Thank you

Jenko Hwong

jhwong@netskope.com
@jenkohwong
@jenko@infosec.exchange

© 2023 Jenko Hwong