RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART3-W01**

Anticipate and Defend Against Adversaries Targeting SaaS and IaaS

Brian Vecci

Field CTO

Varonis Systems, Inc.

@brianthevecci

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.

Agenda

- State of SaaS risks
- How these risks are exploited
- Q&A

RSAConference2022

State of SaaS Risks

Broken Access Control Takes the Crown in 2021

- The **OWASP** Top 10 is a standard awareness document for developers and web application security
- **Broken access control** is considered the most critical security risk to web applications

2021

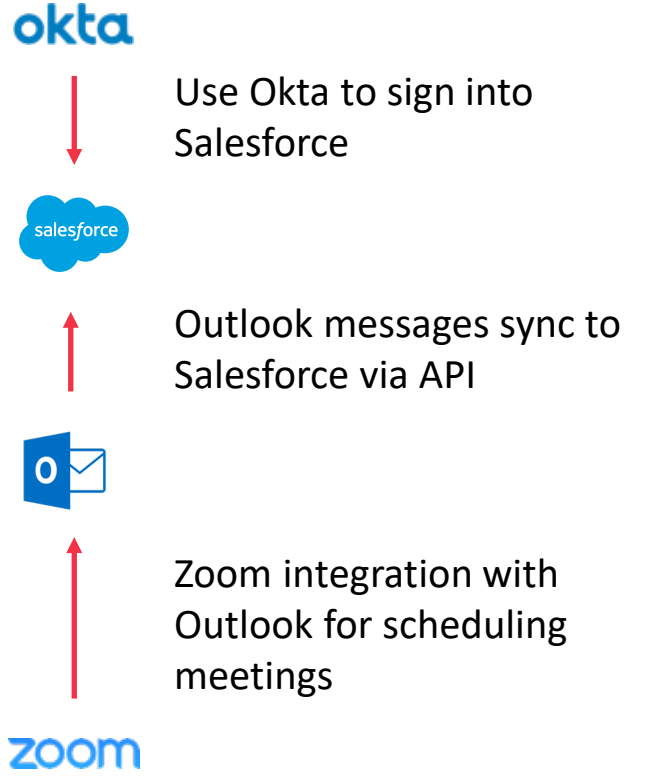
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

SaaS challenges

- Data Protection
- Configuration Risk
- Interconnectivity Risk

Everything is connected



RSAConference2022

API Abuse

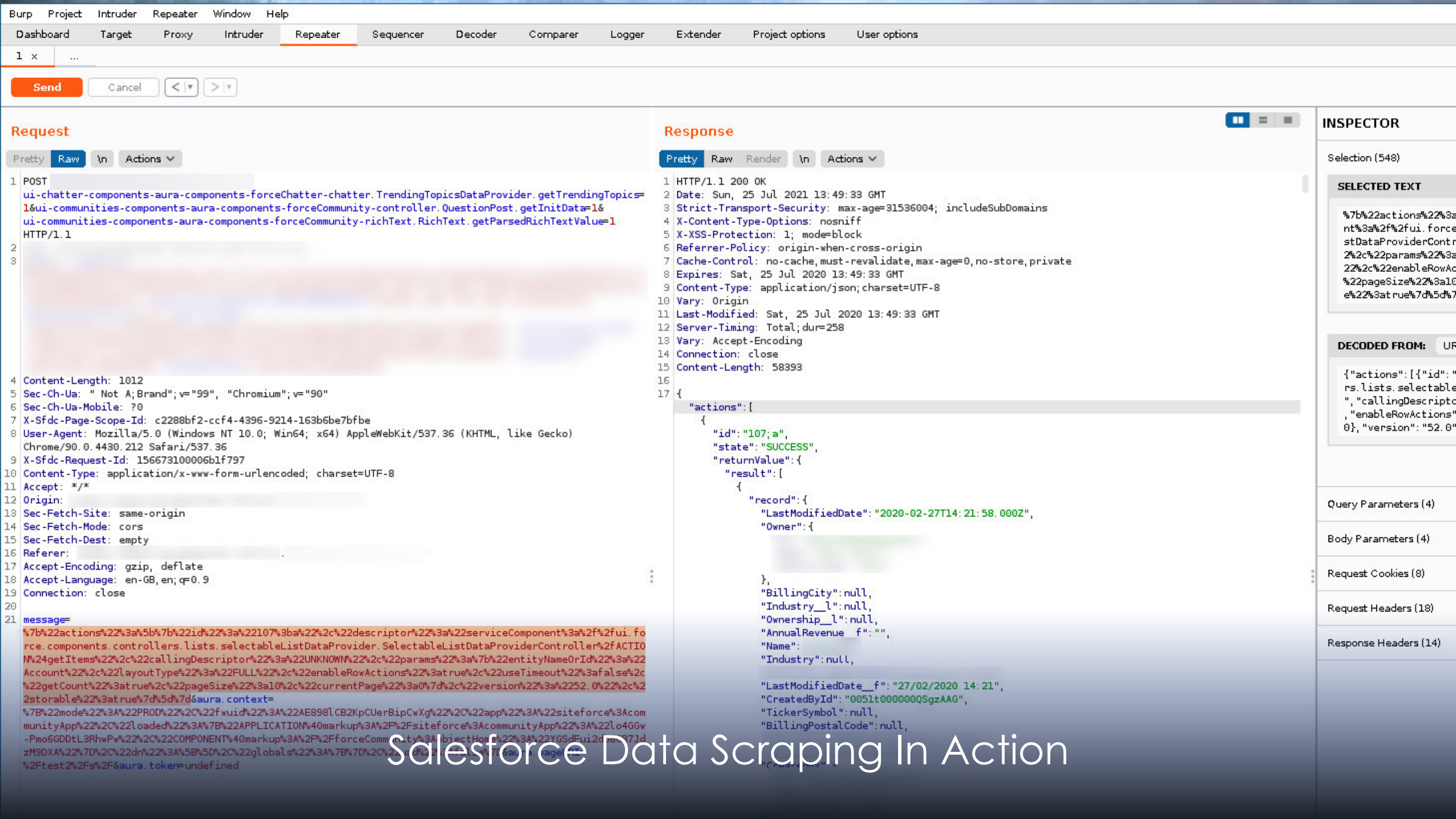

Rise of the Machines
1 out of 4 identities in SaaS apps are non-human

Salesforce Community API misconfiguration

So there's this guest profile in Salesforce Communities…

Check for misconfigurations

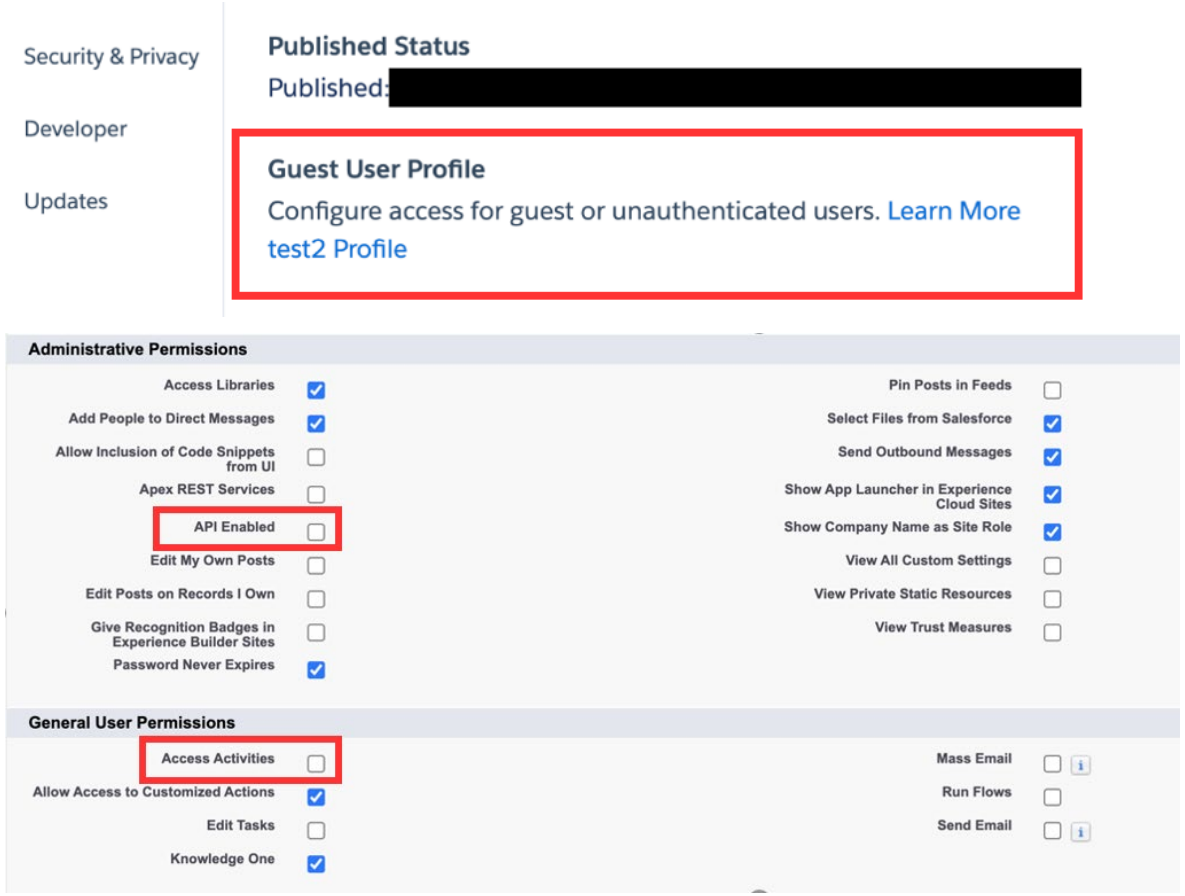
- Use Google URL searches
- Operators like “inurl” will narrow the results
- Common Salesforce Community URLs include:
  - /s/topic
  - /s/article
  - /s/contactsupport



Salesforce Data Scraping In Action

What you can do to fix the exposure

- Check the rights on the Guest User profile in the Site Builder settings
- Remove Guest User rights
  - API Enabled
  - Access Activities
- Set Default Record Ownership to Admins
- Enable “Secure guest user record access” in the Sharing Settings

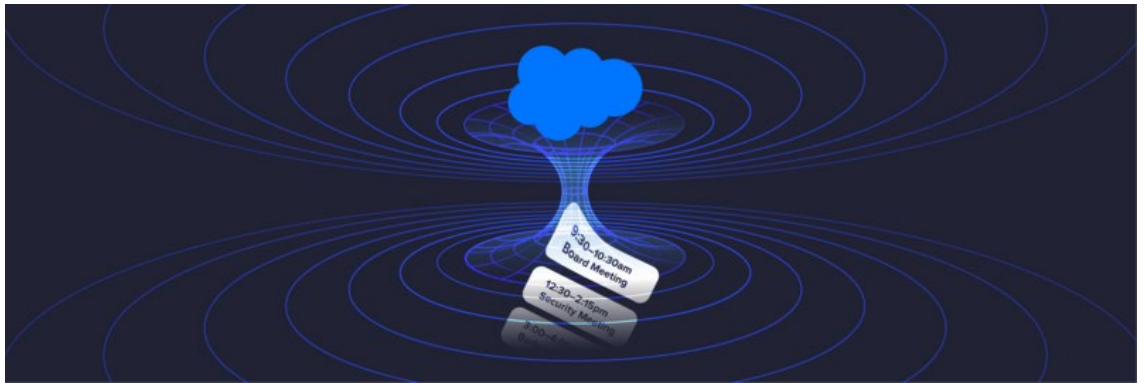


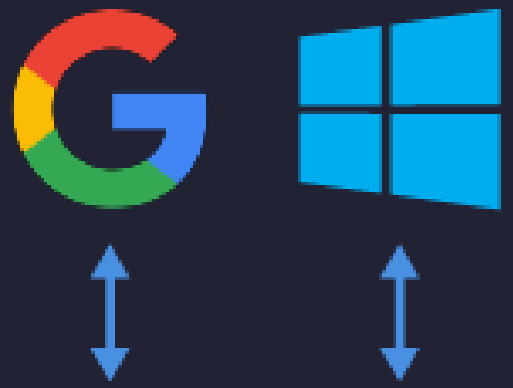
Dial M for Misconfiguration

44% of cloud user privileges are misconfigured

Einstein's Wormhole

- Varonis researchers discovered a bug called **Einstein's Wormhole**, which can expose administrator's calendars to the internet
- **Einstein Activity Capture** (EAC) synchronizes emails and calendar events between Microsoft Exchange or Google accounts and Salesforce
- If **misconfigured**, calendar events and their sensitive contents can be exposed publicly

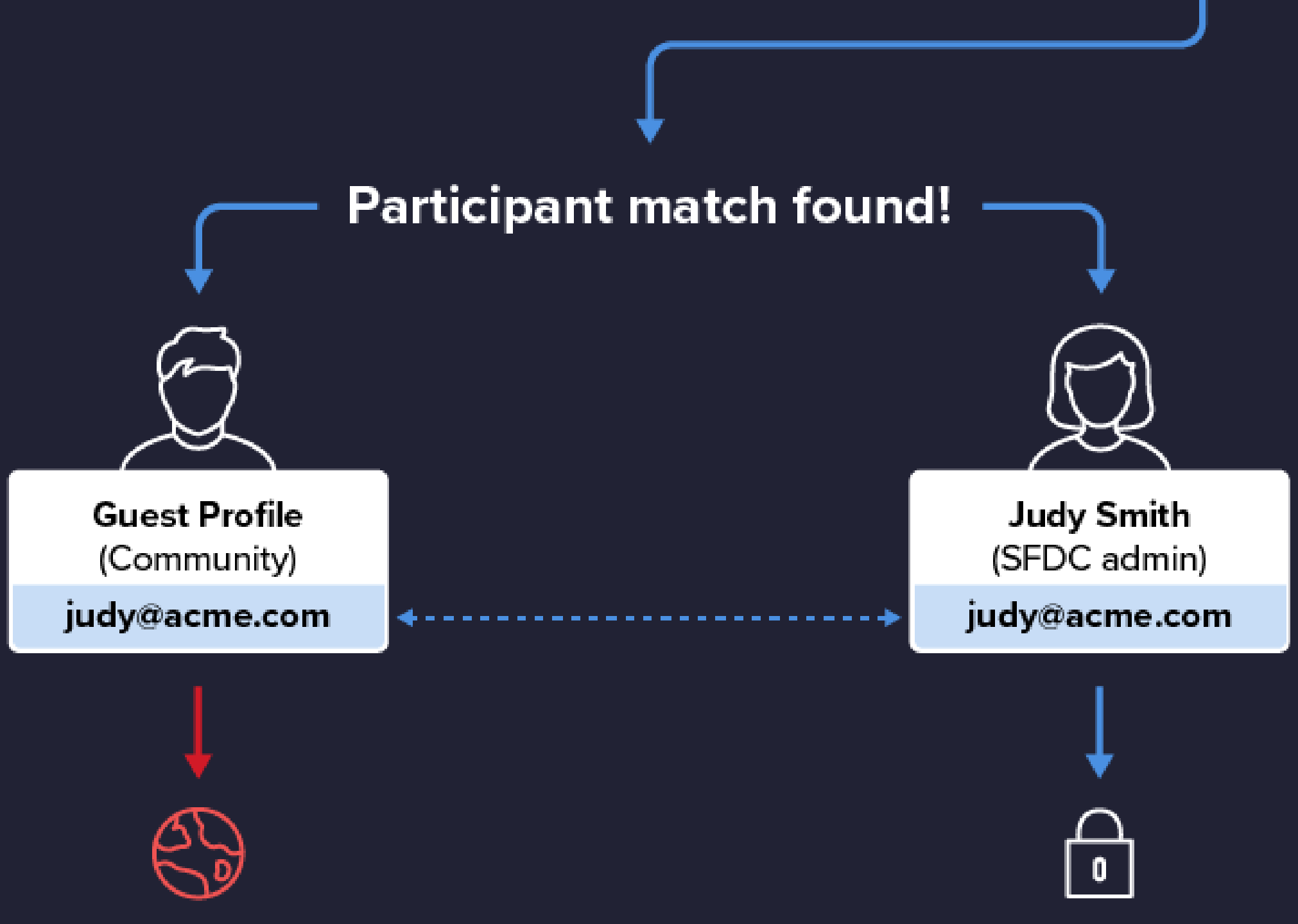




Einstein checks Google / Exchange for new calendar events

Calendar event added to the organizer's Salesforce calendar

Einstein scans the participant list for matching Salesforce users, leads, and contacts


Participant match found!
Guest Profile
(Community)
judy@acme.com
Judy Smith
(SFDC admin)
judy@acme.com

Guest Profile
(Community)

judy@acme.com

Judy Smith
(SFDC admin)

judy@acme.com

Create PUBLIC event

Roadmap Meeting

Attendees: ...

Description: ...

Zoom link: ...

Password: ...

Create private event

Roadmap Meeting

Attendees: ...

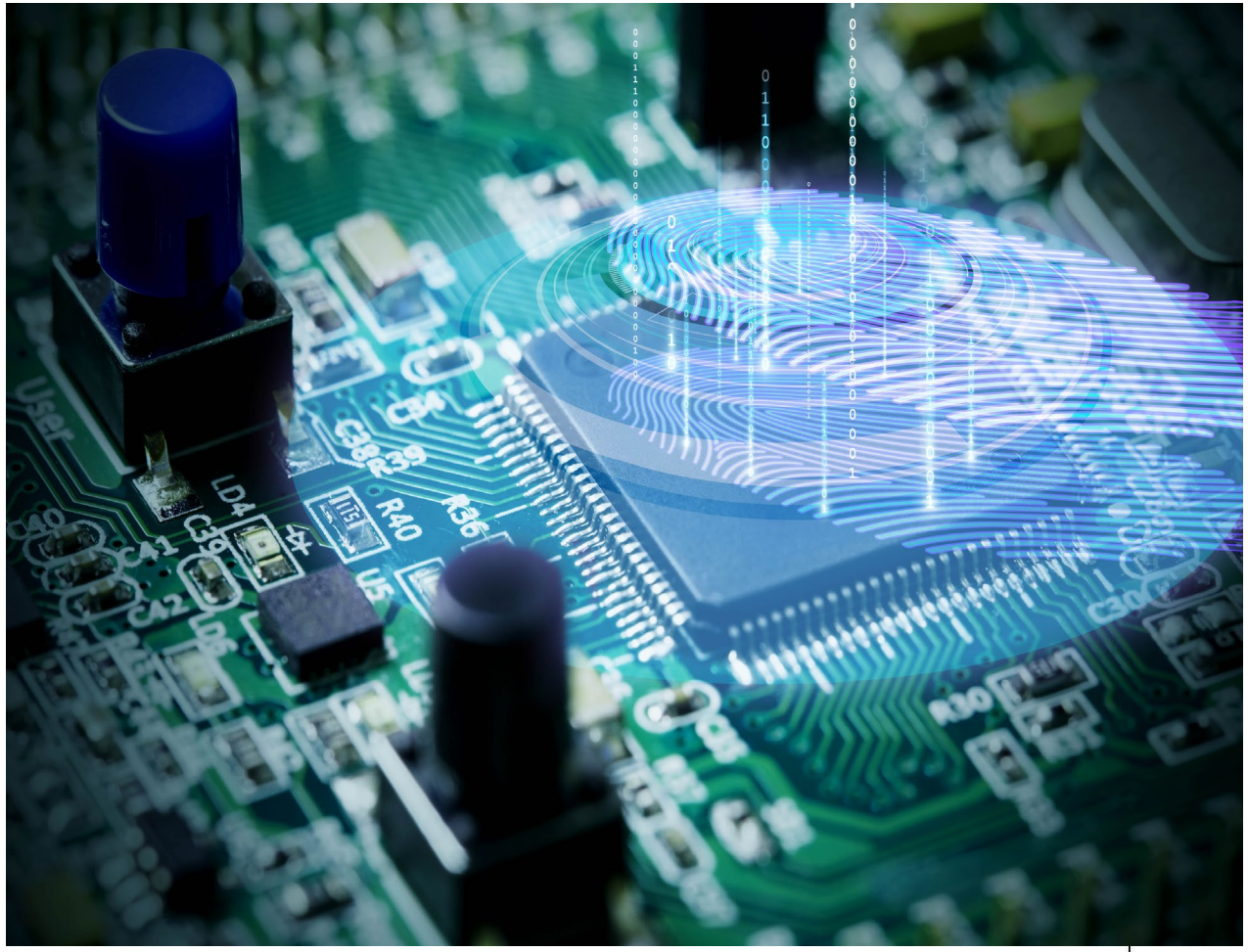
Description: ...

Zoom link: ...

Password: ...

The Fix Is In

- Salesforce already corrected the underlying bug
- Change your guest user's email to a dummy email using the script
- Delete the sensitive objects associated with the guest account (this is tough, we can help)



RSAConference2022

SSO Impersonation


The Shadow Knows
3 out of 5 privileged cloud users are shadow admins

SSO is the new (h)Active Directory

- SSO makes it easy and convenient to centrally manage users' various cloud solution access
- A compromised SSO admins opens the door to re-assigning resources
- Attackers can pivot to different resources by assigning cloud data apps and impersonating users
- Data exfiltration is as easy as sharing data with attacker-controlled accounts

Attack Flow

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

Phishing Mail

okta

Impersonation to other users using SSO

Google Workspace

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

box

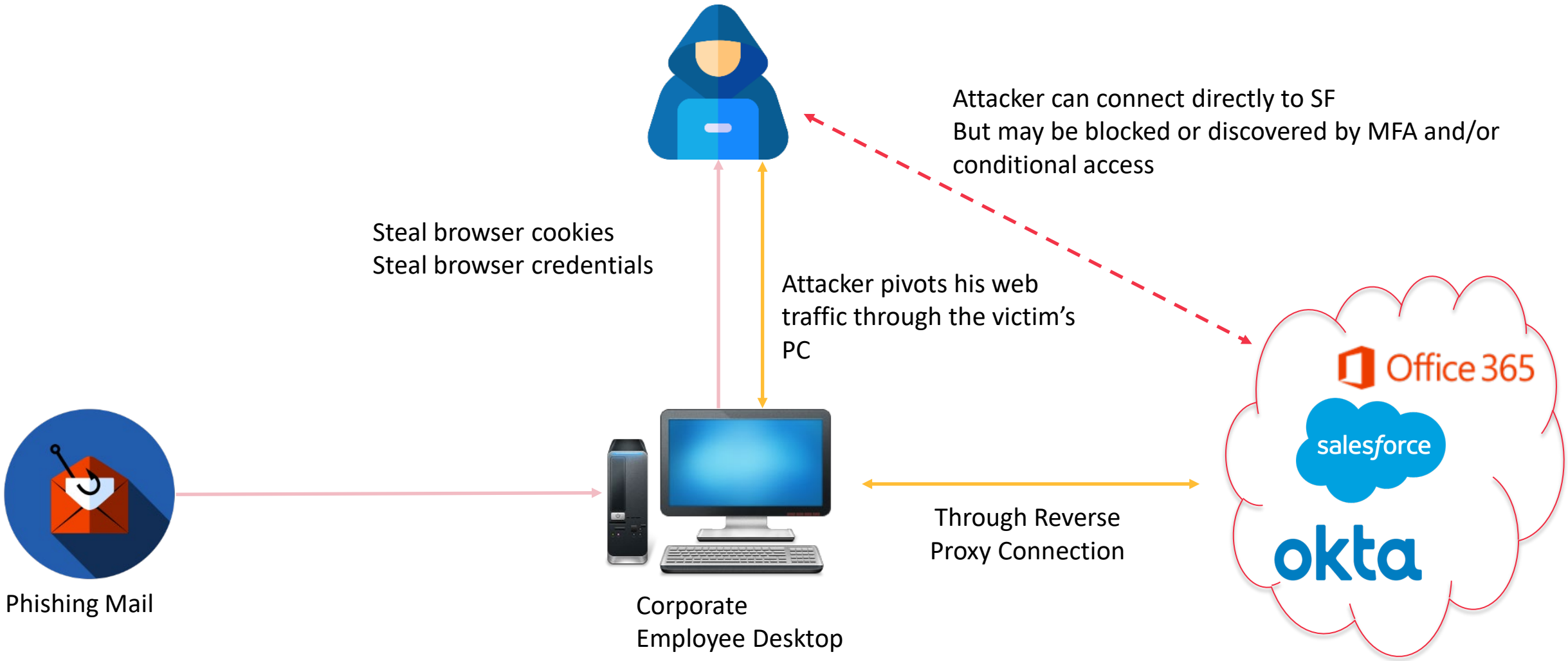
Share customers contracts using a public custom URL

RSAConference2022

Authentication Monitoring Evasion

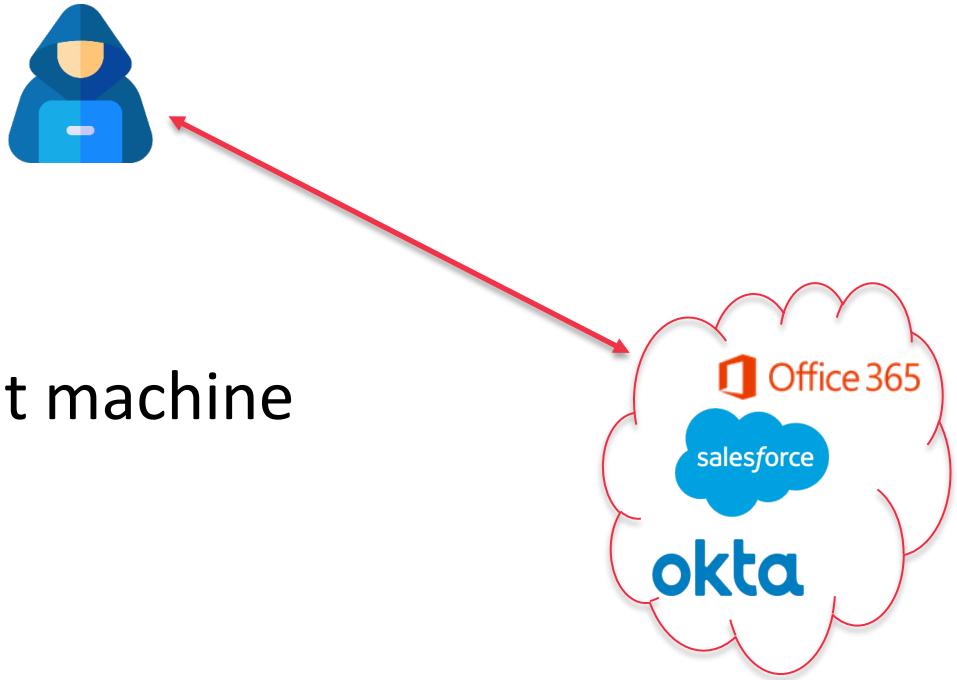

Watch the vault not the door

Attack Flow


Attacker can connect directly to SF
But may be blocked or discovered by MFA and/or conditional access
Steal browser cookies
Steal browser credentials
Attacker pivots his web traffic through the victim's PC
Office 365
salesforce
okta
Through Reverse Proxy Connection
Phishing Mail
Corporate Employee Desktop

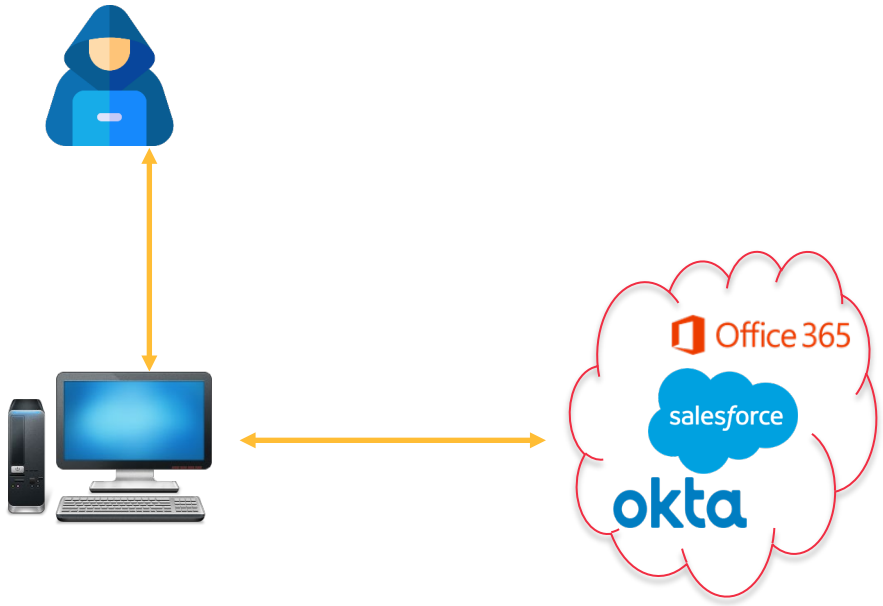
Why Use Reverse Web Proxy Technique

- 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

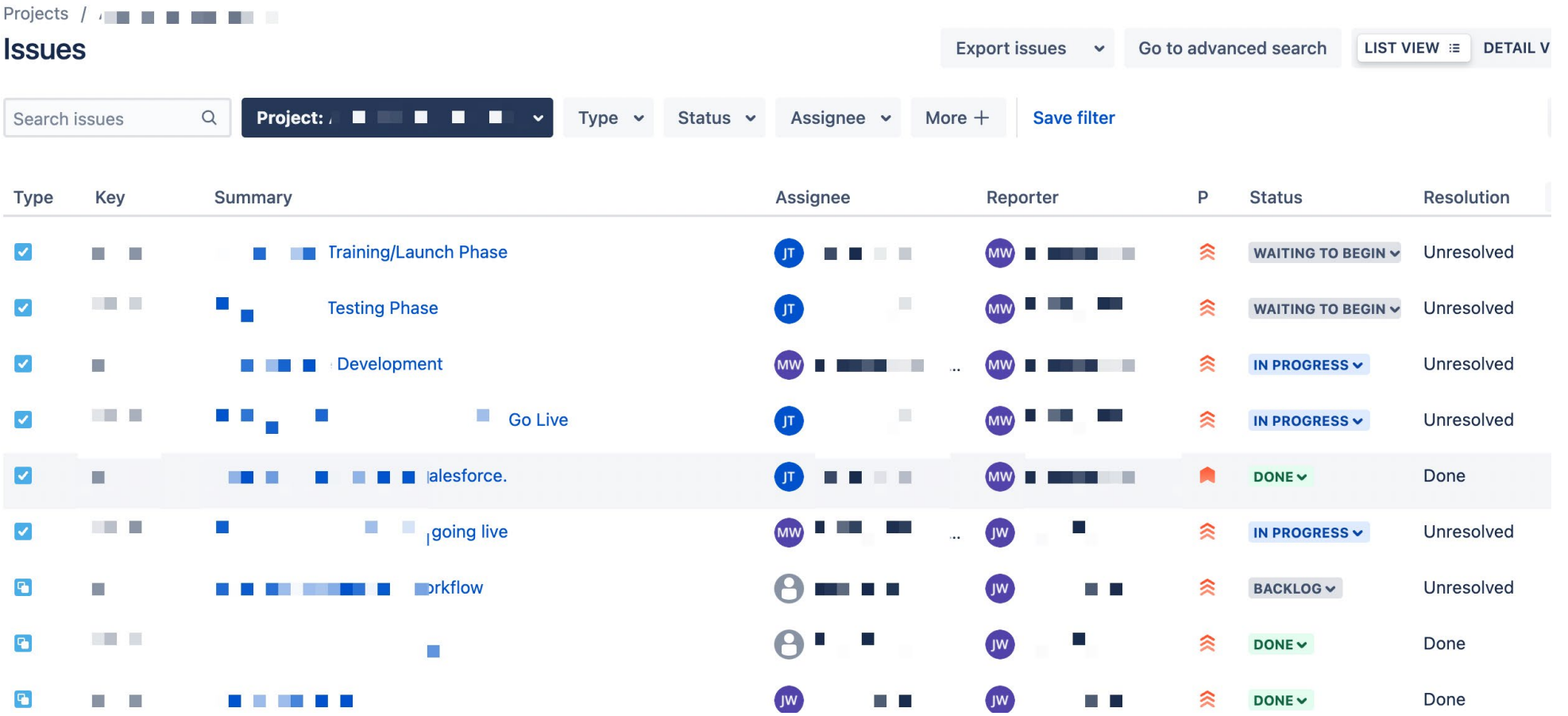


Why Use Reverse Web Proxy Technique

- 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
  - No alerts generate by activity?

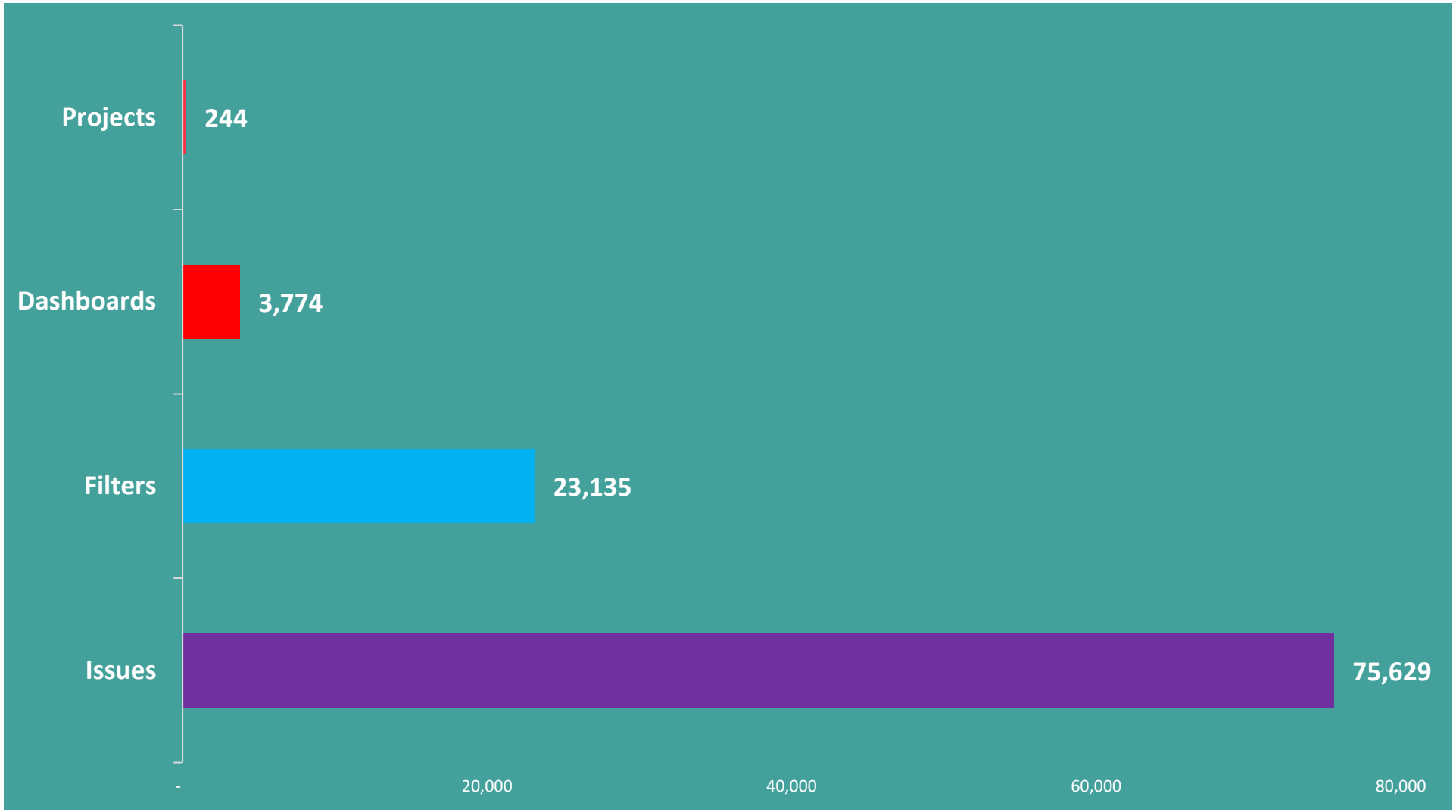


One more thing…



Jira

How many Jira public objects did we find?



Scanner scope:

- ✓ **812** subdomains scanned
- ✓ **689** had public objects

Potentially sensitive data:

- ✓ **2,922** email addresses
- ✓ **5,424** IPv4 addresses
- ✓ **60,411** URLs


Thanks to our top-notch research team

Q&A

Thank You
More questions? Come visit us at Booth #5545