Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on May 21, 2024 and its most recent report on Form 10-K filed on September 7, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

splunk> .conf24

Hunting M365 Invaders

Tactical Insights for M365 Threat Detection

SEC1470B

.conf24

splunk>

Bring on the future.

Speakers

Mauricio Velazco

Principal Threat Research Engineer
Splunk

Michael Haag

Principal Threat Research Engineer
Splunk

Agenda

Introduction

Data Sources

Initial Access

Collection

Case Study: Midnight Blizzard

Demo

Takeaways

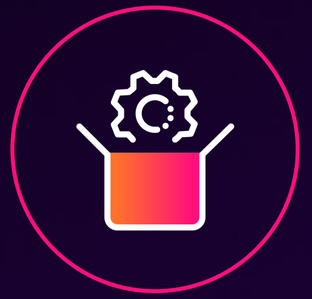
Introduction

Splunk Threat Research Team

Study Threats

Create Datasets

Build Detections



Release Tools

Share with Community

Microsoft® 365

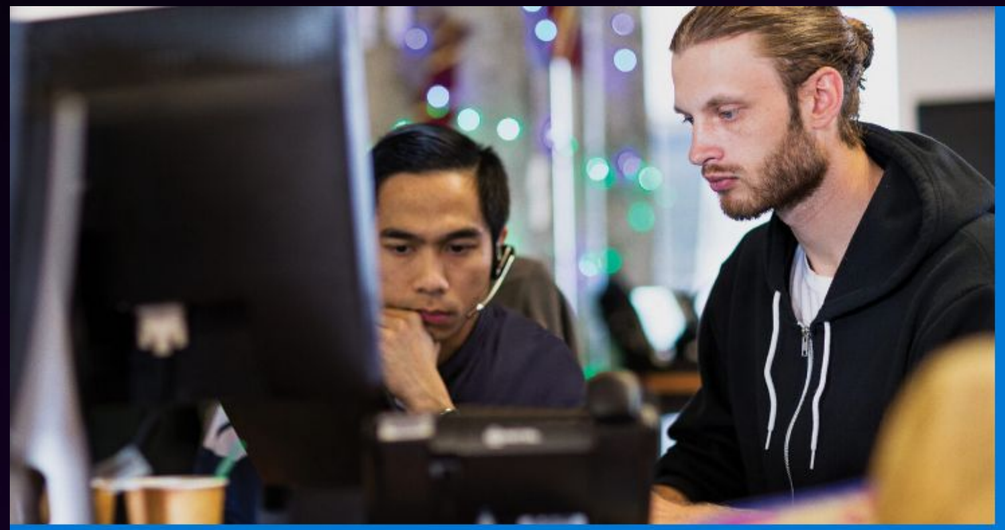
Cloud-based suite of productivity tools, including email, collaboration platforms, and office applications.

All integrated with Entra ID for identity and access management.

M365's centralized storage, ubiquity and widespread adoption make it a **common target of threat actors**.

[Title] is an independent conference and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation.

Financially Motivated



Research Threat intelligence Microsoft Defender Cybercrime

16 min read

Threat actors misuse OAuth applications to automate financially driven attacks

By Microsoft Threat Intelligence

December 12, 2023

Threat actors are misusing OAuth applications as an automation tool in financially motivated attacks. OAuth is an open standard for token-based authentication and authorization that enables applications to get access to data and resources based

Source: ttps://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/#:~:text=Threat%20actors%20are%20misusing%20OAuth,permissions%20set%20by%20a%20user.

Intelligence Motivated

Jonathan Greig

January 26th, 2024

Cybercrime | Industry | News | Nation-state

Get more insights with the Recorded Future Intelligence Cloud.

Learn more.

Microsoft says Russian hackers used previously identified tactic to breach senior exec emails

Russian hackers abused a popular authentication tool to gain access to the email accounts of senior executives at Microsoft, according to a new statement from the tech giant.

Microsoft has been tightlipped about an incident — announced late on Friday afternoon last week — that they said involved the months-long compromise of corporate email accounts. Prolific hackers allegedly connected to Russia's Foreign Intelligence Service (SVR) breached a legacy non-production test tenant account in late November before pivoting into their targets' email accounts. Microsoft only discovered the incident on January 12.

For the last week, Microsoft has offered little explanation on how the hackers managed to pivot from non-production test accounts into one's used by senior leaders of the company.

But Microsoft said in a blog post on Thursday night that the hackers managed to gain entry by abusing OAuth — a standard that allows applications to get access to data and resources based on permissions set by a user.

Source: https://therecord.media/microsoft-says-russian-hackers-used-previously-identified-technique-to-breach-executive-emails

Why Microsoft 365 Matters More Than Ever

- M365 adoption is skyrocketing
- Massive amounts of sensitive data now reside in M365
- Adversaries are actively targeting M365 with evolving tactics
- Recent breaches demonstrate the costly impacts of M365 compromise
- Remote work has expanded the attack surface and risks

Data Sources

Data Sources

Unified Audit Log

The UAL aggregates logs from various services, such as Microsoft ®Exchange Online, Microsoft ® SharePoint, Microsoft ® OneDrive, Microsoft® Teams and Microsoft Entra ID™.

It provides a **centralized view of user application activities** across the M365 environment.

Splunk Add-on for Microsoft Office 365

Entra ID Logs

Entra ID's sign-in and audit logs feature granular details relevant to authentication and identity management.

Provides more comprehensive details and includes categories not available in the UAL: **service principal, non-interactive and mange identity** sign-ins.

Splunk Add-on for Microsoft® Azure Splunk Add-on for Microsoft Cloud Services
Data Manager

Graph Activity Logs

Audit trail of all HTTP requests that the **Microsoft Graph API** received and processed for a tenant

After a brief stint in preview, they transitioned to general availability in April 2024.

Splunk Add-on for Microsoft Cloud Services
Data Manager

Unified Audit Log - MailItemsAccessed

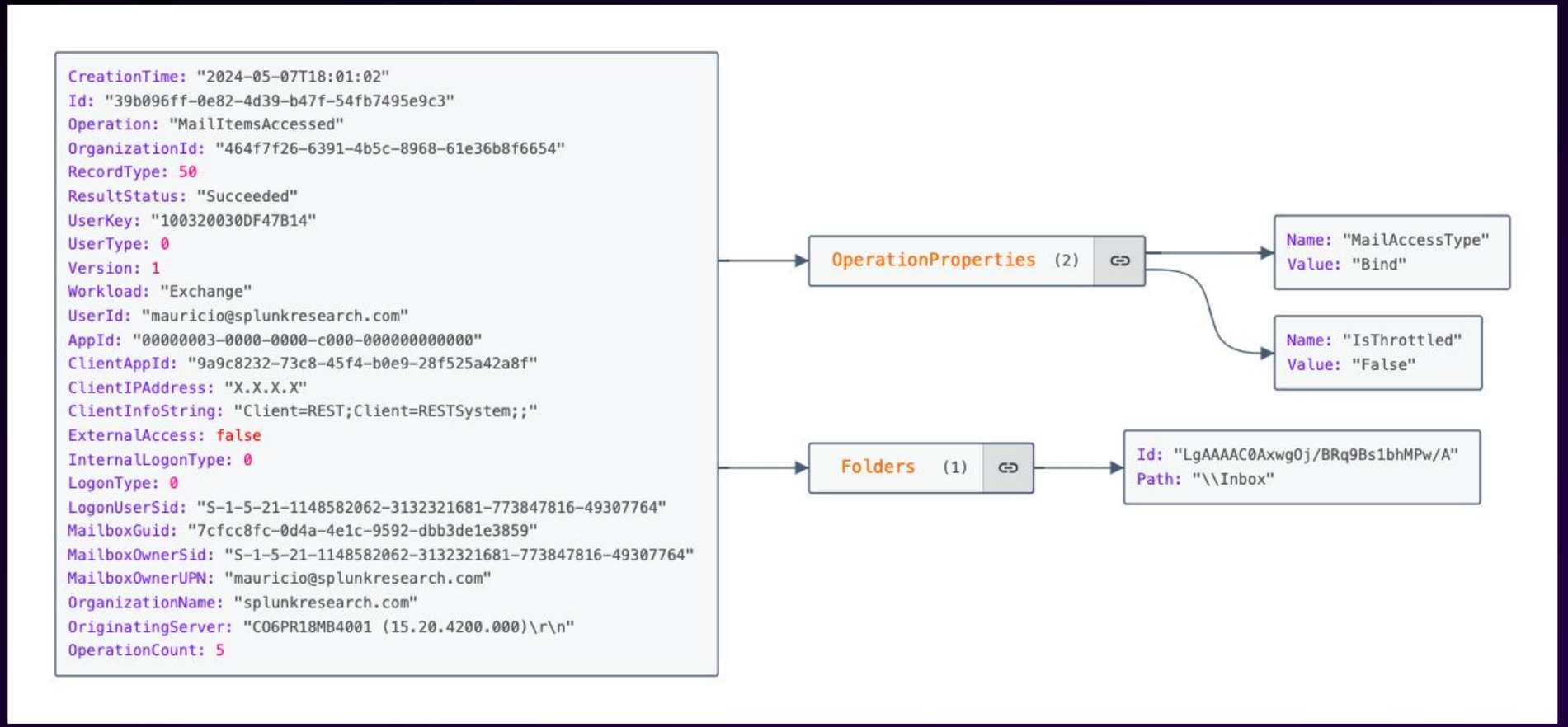


Image produced with jsoncrack.com

Entra Id Logs - ServicePrincipalSignInLogs

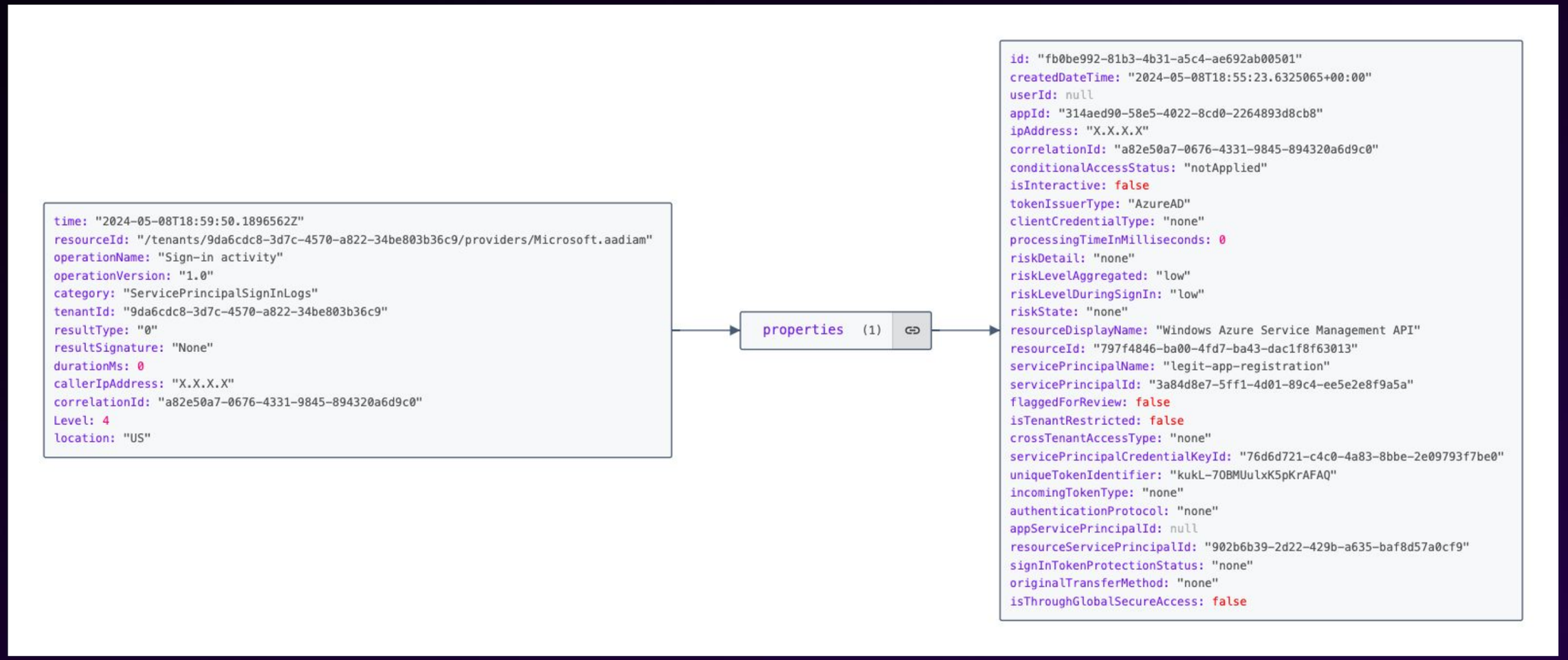


Image produced with jsoncrack.com

Graph Activity Logs - Graph Activity

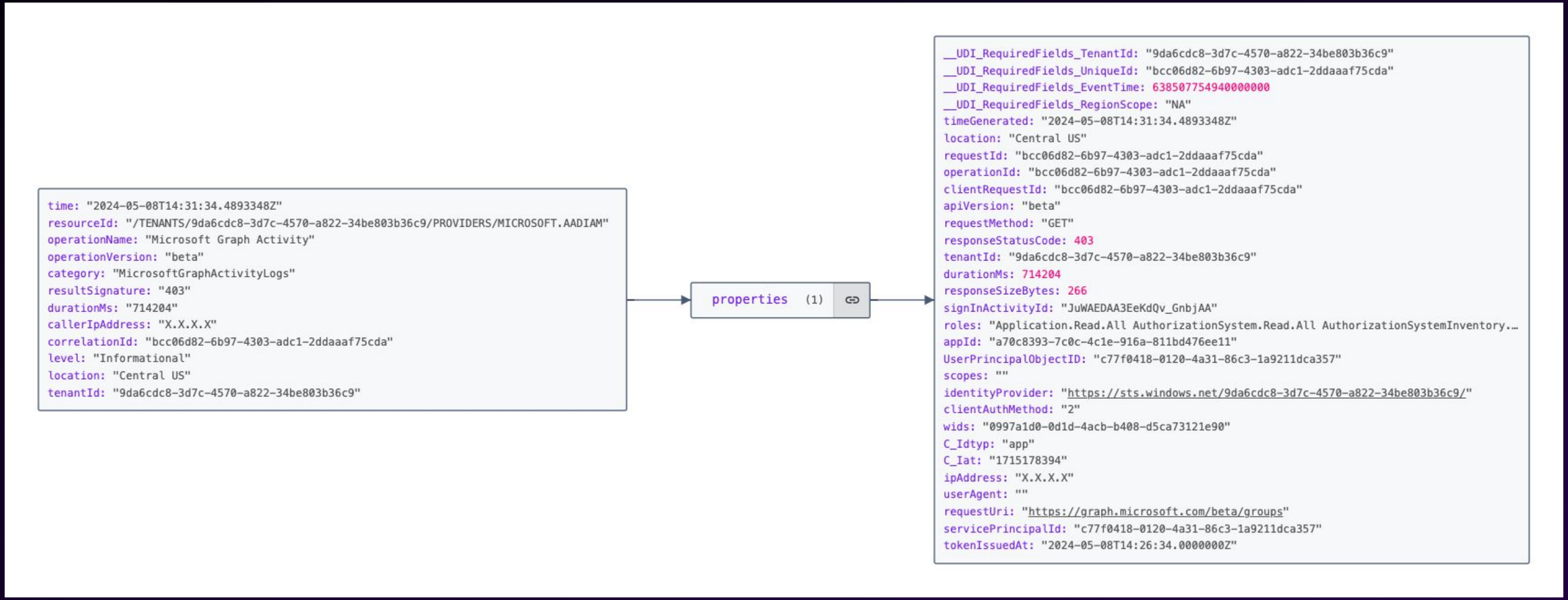
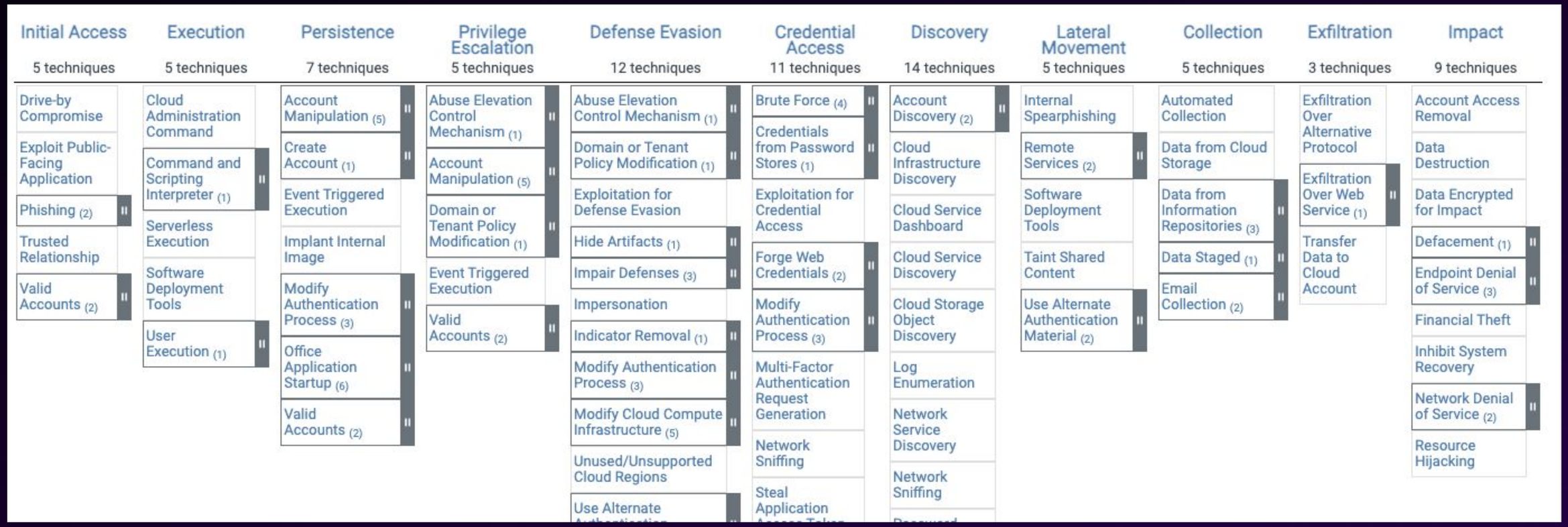


Image produced with jsoncrack.com

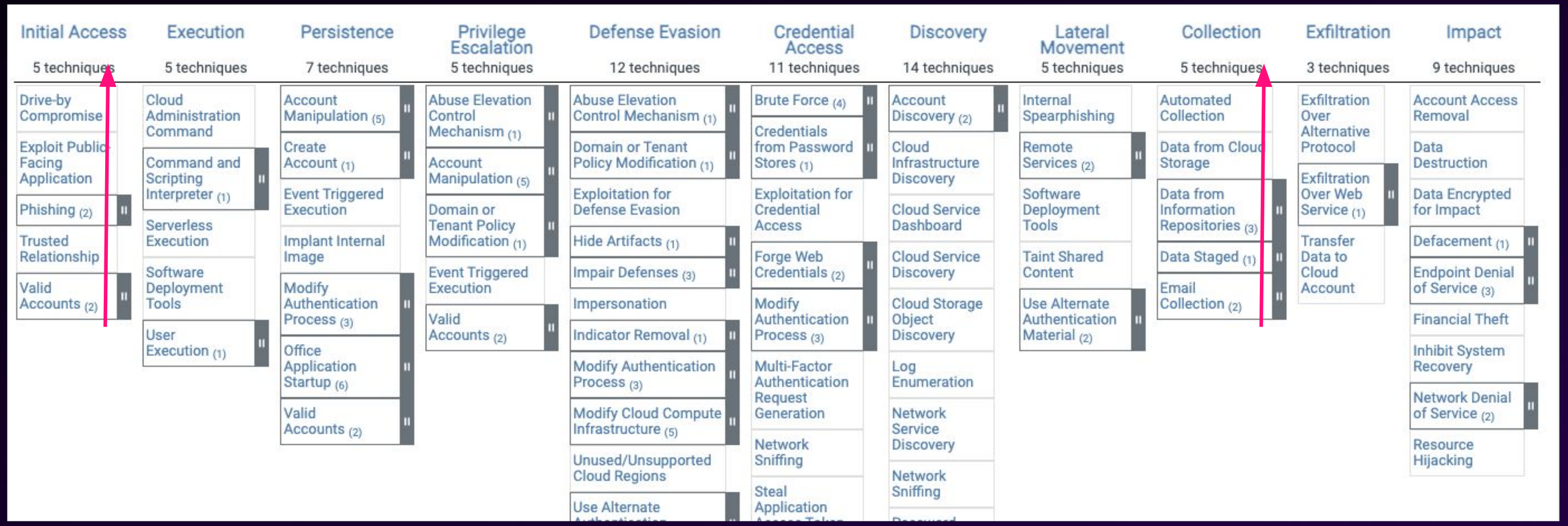
Source: https://www.pexels.com/photo/traffic-lights-and-street-signs-along-city-buildings-13084943/

MITRE ATT&CK® Cloud Matrix



https://attack.mitre.org/matrices/enterprise/cloud/

MITRE ATT&CK Cloud Matrix



https://attack.mitre.org/matrices/enterprise/cloud/

Initial Access

Initial Access

TA0001

Consists of techniques that use various attack vectors to **gain their initial foothold within a an environment**.

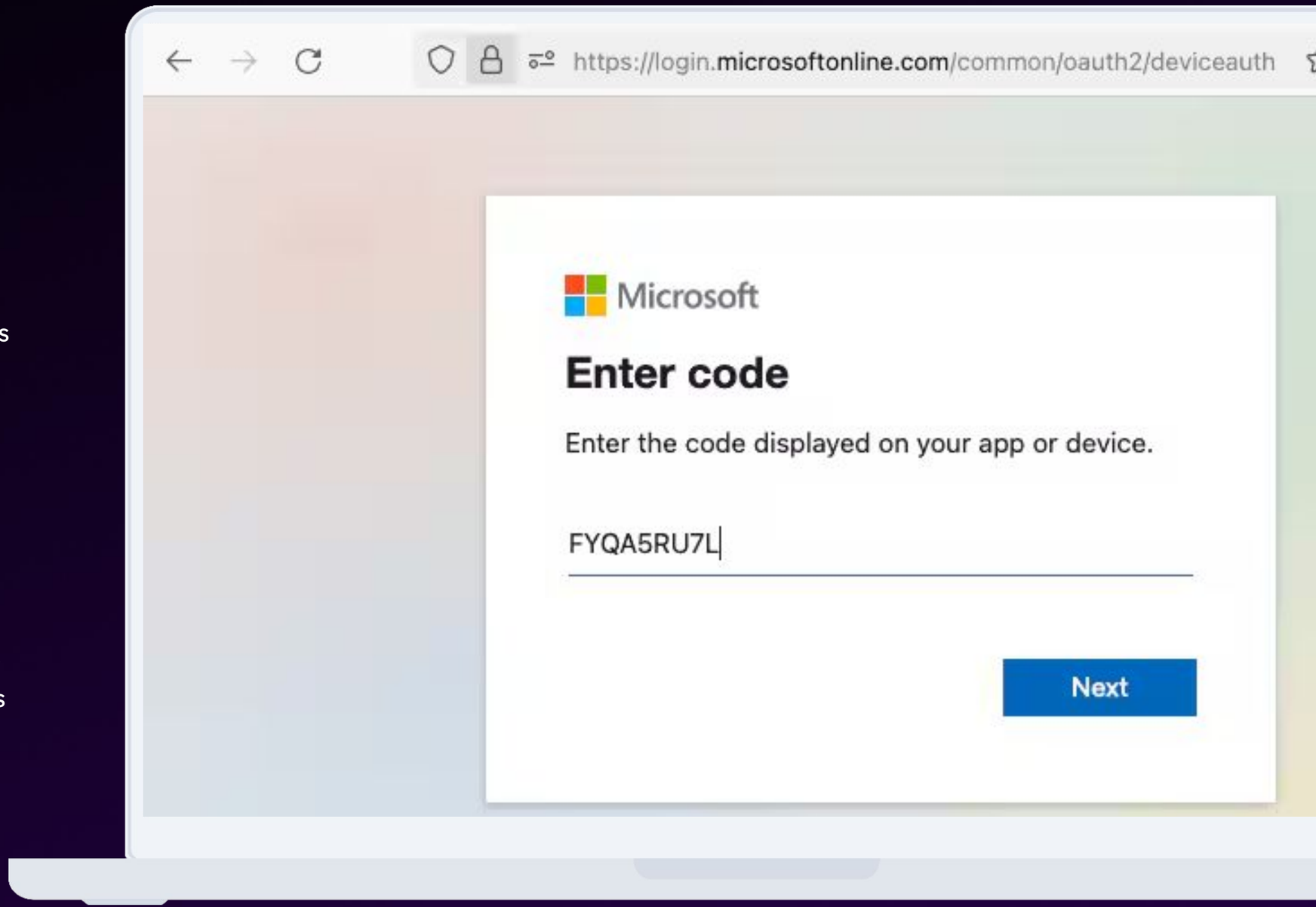
In the realm of cloud computing, **identity has become the new perimeter**. A compromised account can set the stage for further exploitation and data exfiltration.

Device Code Phishing

M365 and its authentication processes are built upon the OAuth protocol, which supports various authentication flows

One such flow, is the OAuth protocol extension known as **device authorization grant**, designed to accommodate devices that have constrained input capabilities.

This technique grants the attacker the ability to **bypass MFA** and gain unauthorized access to M365 services

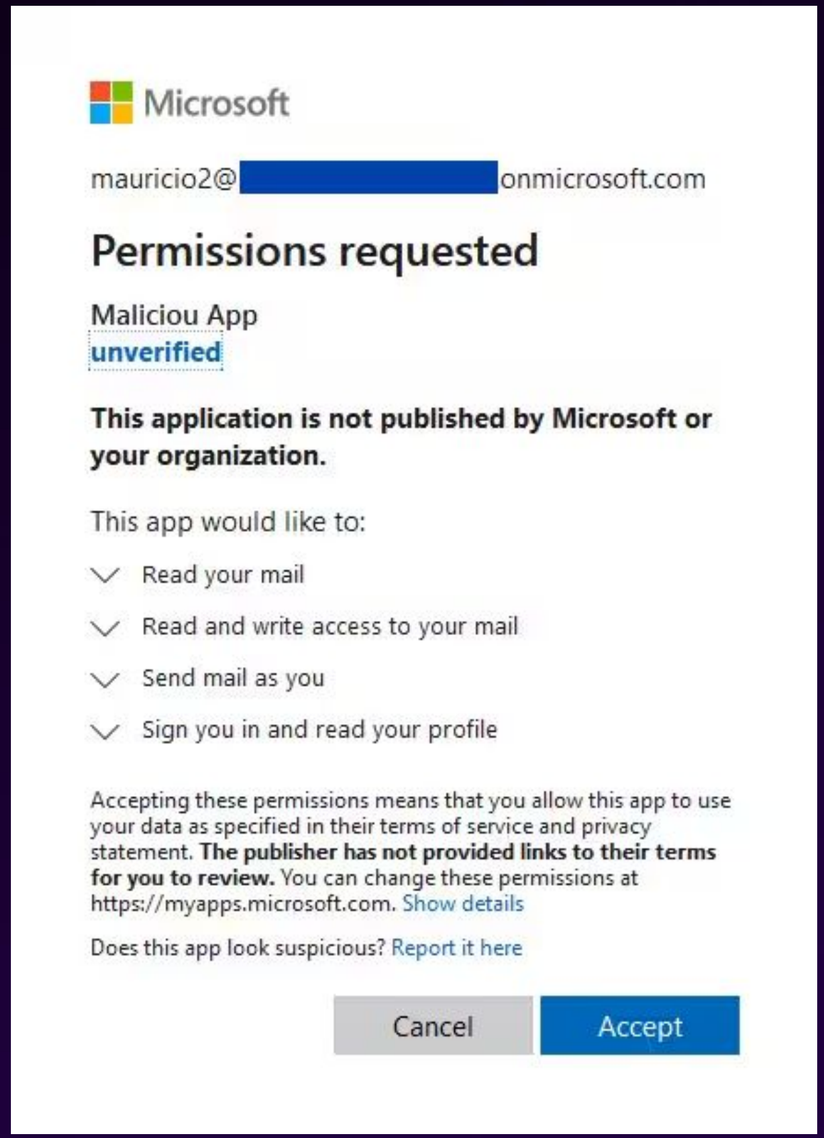


Illicit Consent Grant

OAuth also allows third-party applications to interact with organizational data.

Attackers exploit this by registering malicious Azure applications and then deceiving users into granting them consent

Once attackers obtain this unauthorized consent, they can acquire an access token, enabling them to access sensitive information **bypassing MFA**.

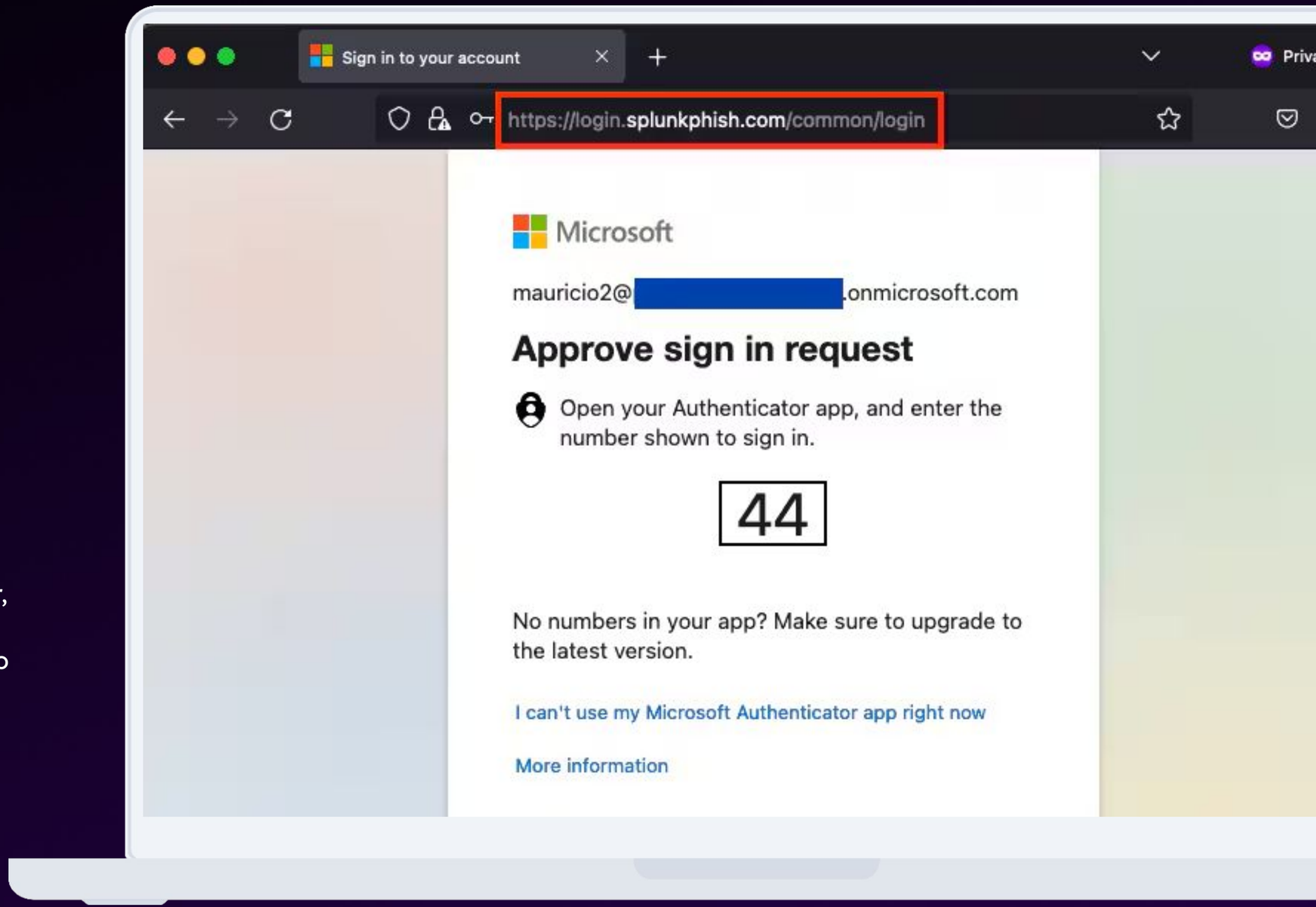


Adversary In The Middle

Phishing attacks have traditionally involved tricking people into visiting fake websites where they're asked to input their login details.

In an (AiTM) attack, attackers also trick victims into visiting a malicious site. However, the phishing site acts as a proxy server, forwarding and capturing victim's requests to the legitimate web.

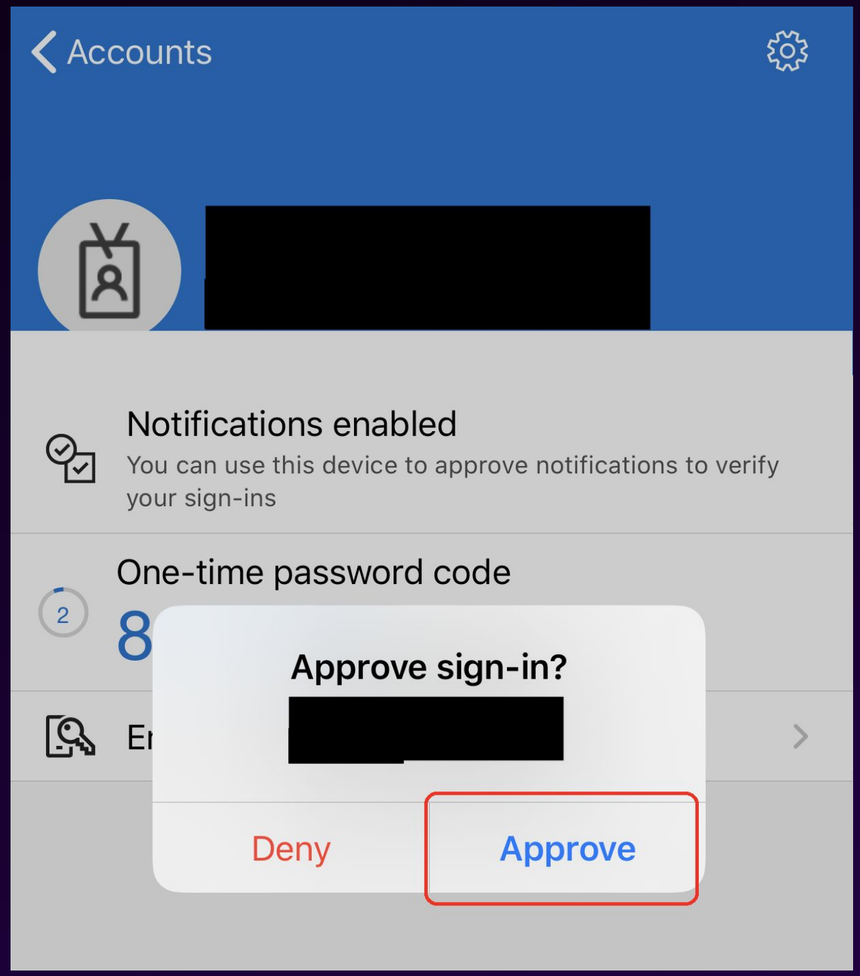
This method **bypasses MFA**, as the attacker gains a valid session cookie.



MFA Fatigue

A common method used to **bypass push-based MFA** involves attackers abusing stolen credentials to generate a flood of authentication requests.

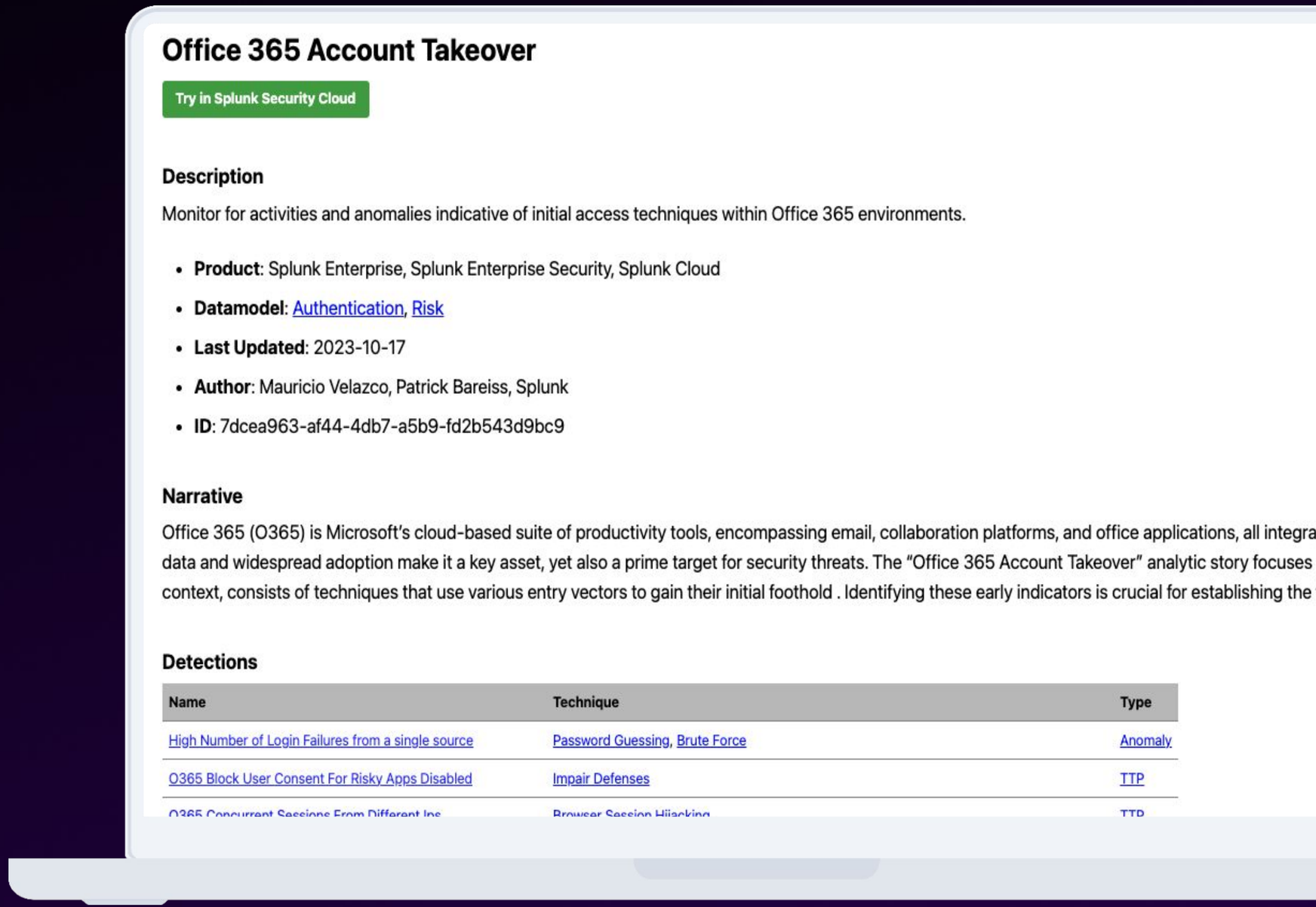
The hope is that the targeted user, overwhelmed or confused by the incessant prompts, will eventually approve one.



Office 365 Account Takeover

https://research.splunk.com/stories/office_365_account_takeover/

- 15 Analytics
- 11 unique MITRE Techniques



Collection

Collection

TA0009

Consists of the techniques adversaries execute for obtaining access to information of interest to their goal.

In the realm of M365, collection can be interpreted as unauthorized access to the victim's organization mailboxes.

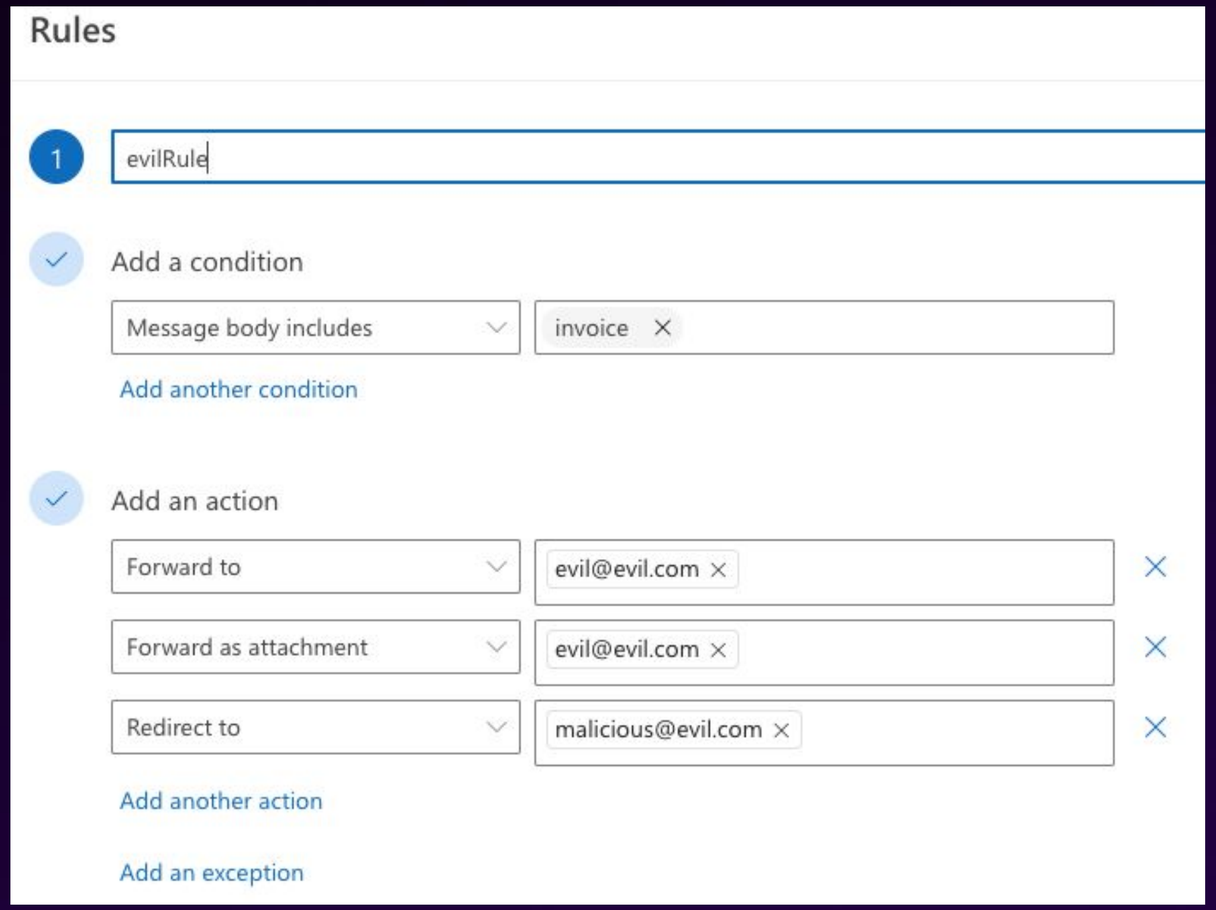
M365 was built on the foundations of Exchange, a platform that historically offered multiple mechanisms for mailbox access.

Inbox Rules

Inbox rules let users automate actions on incoming emails when they match specific criteria, such as containing certain words in the subject line.

These rules present an avenue for adversaries to discreetly manipulate email flow on a compromised account.

Business email compromise (BEC) actors commonly rely on this technique to collect information about their targets.

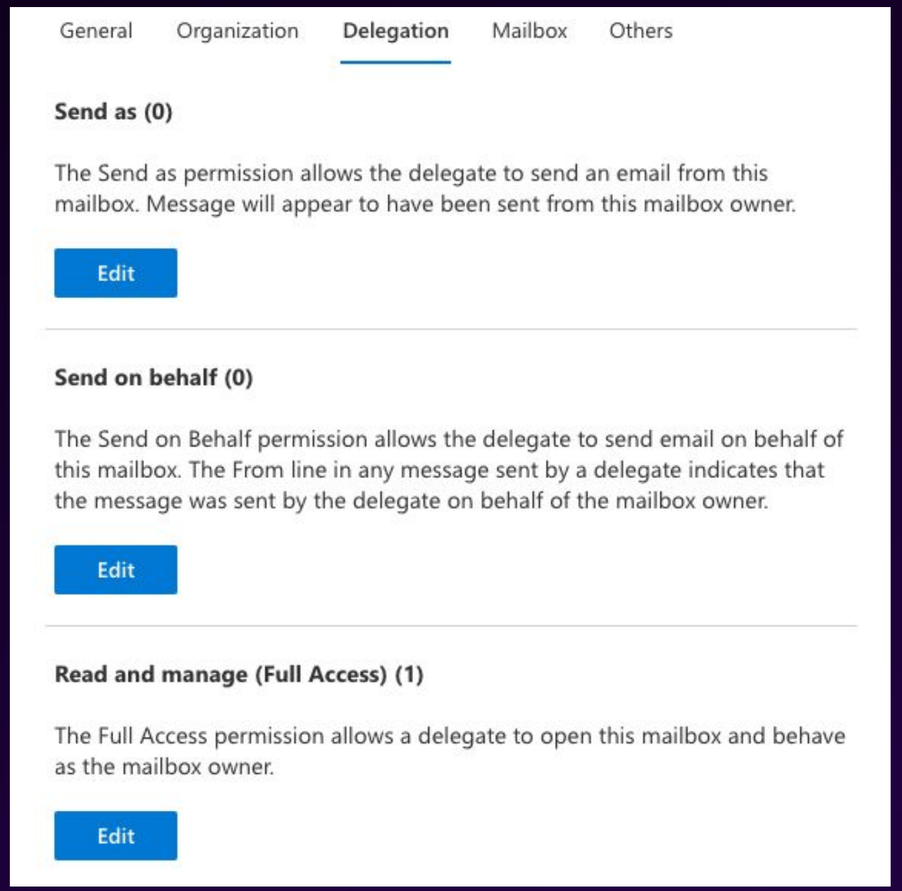


Mailbox Delegation

Delegation allows administrators to grant permissions to users, known as delegates, enabling delegates to gain comprehensive access to other user's mailboxes.

This feature, while facilitating administrative efficiency, also poses a risk if permissions are not properly audited.

Adversaries who successfully gain access to an M365 environment can abuse mailbox delegation to access a victim's mailbox.

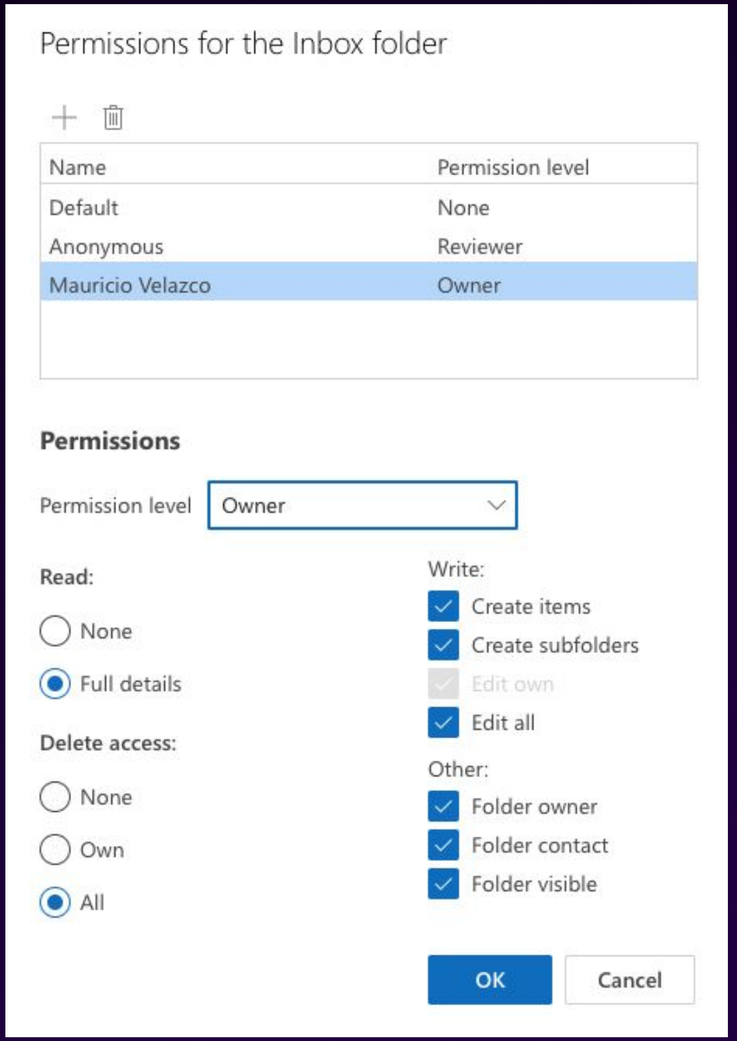


Mailbox Folder Permissions

Folder permissions allows users to fine-tune who can view or modify the contents of specific folders within a mailbox

If not properly monitored, it could allow adversaries to discreetly monitor email communications, posing a significant risk to data security.

APT29 leveraged this technique for email collection.



API Mailbox Access

Exchange Online provides system administrators with APIs like **EWS** and the **Microsoft Graph** for streamlined mailbox management.

With the right privileges in place, adversaries can abuse these powerful tools to gain varied levels of unauthorized email access.

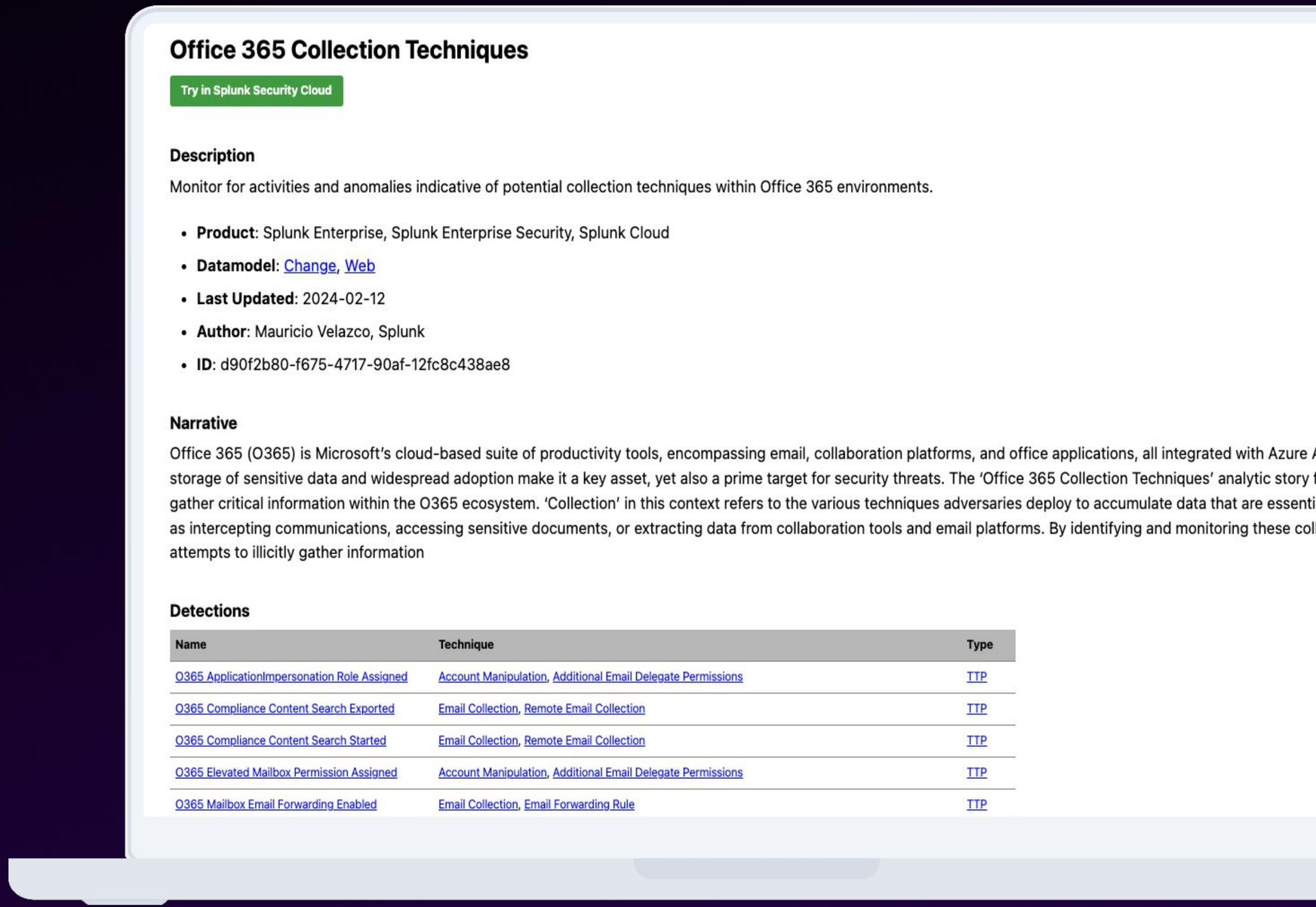
```
(base)
┌──[mvelazco@C02D25J0MD6R]-[~/Dev/o365]
└─ # python read_email_graph2.py
User: mauricio@splunkresearch.com, Subject: wire instruction #1
User: mauricio@splunkresearch.com, Subject: Confidential Email #6
User: mauricio@splunkresearch.com, Subject: Confidential Email #5
User: mauricio@splunkresearch.com, Subject: Confidential Email #4
User: mauricio@splunkresearch.com, Subject: Confidential Email #2


User: herman@splunkresearch.com, Subject: Test email after disabling
User: herman@splunkresearch.com, Subject: Test SMTP config
User: herman@splunkresearch.com, Subject: Test email after disabling
User: herman@splunkresearch.com, Subject: Test email after disabling
User: herman@splunkresearch.com, Subject: Test email attachment - 2
```

Office 365 Collection Techniques

https://research.splunk.com/stories/office_365_collection_techniques/

- 19 analytics
- 7 MITRE techniques



Office 365 Collection Techniques

Try in Splunk Security Cloud

Description

Monitor for activities and anomalies indicative of potential collection techniques within Office 365 environments.

- **Product**: Splunk Enterprise, Splunk Enterprise Security, Splunk Cloud
- **Datamodel**: Change, Web
- **Last Updated**: 2024-02-12
- **Author**: Mauricio Velazco, Splunk
- **ID**: d90f2b80-f675-4717-90af-12fc8c438ae8

Narrative

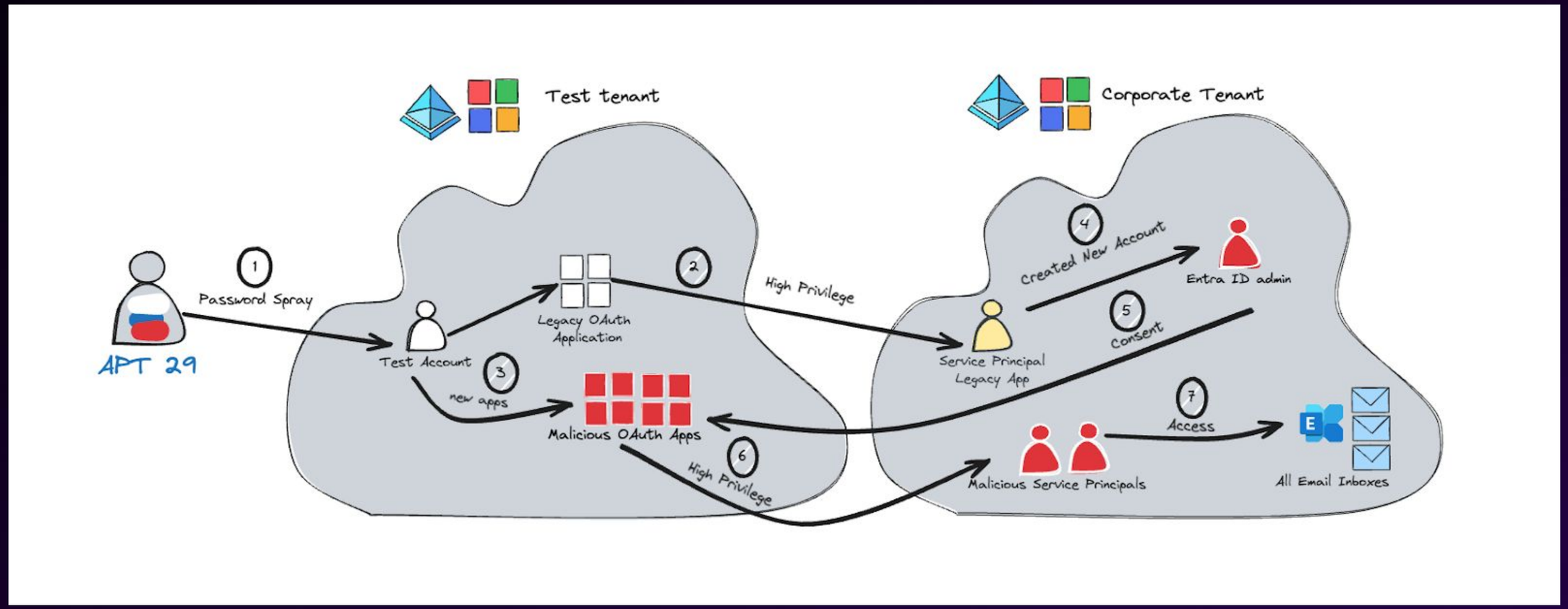
Office 365 (O365) is Microsoft's cloud-based suite of productivity tools, encompassing email, collaboration platforms, and office applications, all integrated with Azure A
storage of sensitive data and widespread adoption make it a key asset, yet also a prime target for security threats. The 'Office 365 Collection Techniques' analytic story f
gather critical information within the O365 ecosystem. 'Collection' in this context refers to the various techniques adversaries deploy to accumulate data that are essenti
as intercepting communications, accessing sensitive documents, or extracting data from collaboration tools and email platforms. By identifying and monitoring these col
attempts to illicitly gather information

Detections

Name	Technique	Type
O365 ApplicationImpersonation Role Assigned	Account Manipulation, Additional Email Delegate Permissions	TTP
O365 Compliance Content Search Exported	Email Collection, Remote Email Collection	TTP
O365 Compliance Content Search Started	Email Collection, Remote Email Collection	TTP
O365 Elevated Mailbox Permission Assigned	Account Manipulation, Additional Email Delegate Permissions	TTP
O365 Mailbox Email Forwarding Enabled	Email Collection, Email Forwarding Rule	TTP

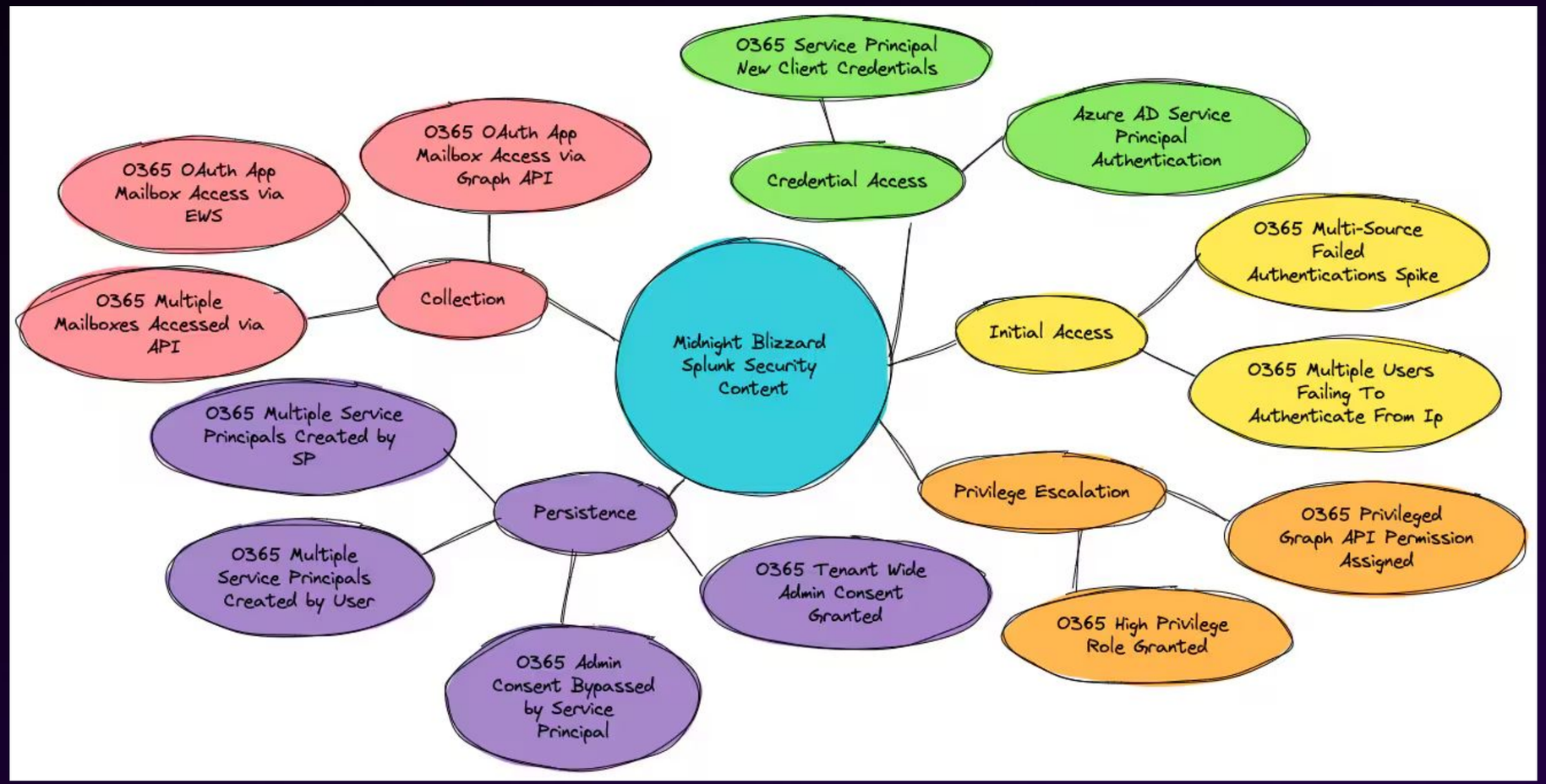
Case Study: Midnight Blizzard

Midnight Blizzard - Attack Chain



Source: https://cloudsecurityalliance.org/blog/2024/02/27/securing-your-microsoft-environment-after-the-midnight-blizzard-attack

Midnight Blizzard - Splunk Coverage

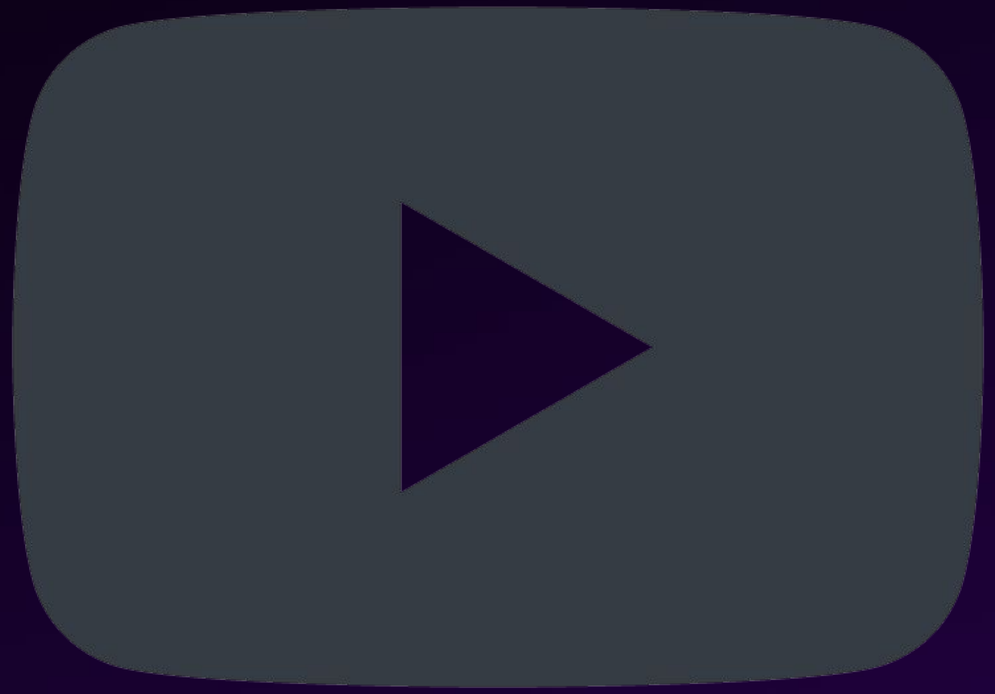


Source: https://www.splunk.com/en_us/blog/security/hunting-m365-invaders-navigating-the-shadows-of-midnight-blizzard.html

Demo

https://github.com/mvelazc0/msInvader

Demo



Takeaways

Key Takeaways

- M365 is a top target for adversaries seeking financial gain or data theft.
- Blue teams must proactively simulate and detect common M365 attack vectors.
- Splunk enhances M365 threat detection by analyzing multiple data sources.
- Continuous refinement of detection strategies is crucial to counter evolving threats.

Thank you