Mandiant & OUTSIDER SECURITY

Cloud security researcher vs threat actor

NorthSec 2026

Contents

Speakers

Dirk-jan Mollema

Outsider Security

Sanne Maasakkers

Mandiant / Google Threat Intelligence Group

01 Researcher vs Threat Actor

Overlap and differences in approach

01

Researchers

Find, use and publish techniques to aid in pentesting, or finding vulnerabilities in products. These techniques usually focus on initial access, lateral movement, or persistence.

02

Financial gain threat actors

Threat actors who are exploiting cloud platforms to steal data, demand ransom, and cryptomining. They achieve this by gaining access through methods like credential access, password spraying, phishing, and vishing.

03

Nation-state threat actors

Nation-state threat actors exploit cloud platforms to gain military, economic, or political advantages by targeting sensitive data, including user information, files, and internal intelligence.

Techniques versus vulnerabilities

Vulnerabilities found by researchers **get patched,** preventing threat actors from finding and abusing them.

Novel vulnerabilities being used by threat actors are rare, but they have their own cloud zero-days too. Example: **token signing key stealing** by Storm-0558 / UNC4920.

Techniques shared by researchers may be adopted by both the offensive security community but also by threat actors. **Defenders** can use these techniques to create **defenses or detection rules.**

Technique adoption

Most cloud techniques will probably be adopted quite soon, but **visibility is limited**. In the cases we found, there was a couple of months difference at least (based on limited visibility).

The **high-value techniques will likely get fixed**, the remaining attack surface is only abused when “needed” by actors.

Many espionage groups still do not focus that much on targeting the cloud, because of the **complexity**, already **established on-prem techniques** and the balance between **risk and reward**.

Pushing vendors

Most vendors and corporations consider attacks **theoretical** until abuse is observed in the wild.

Lack of mitigations, proper detection and secure by default often only receives attention after **public incidents** force vendors to react.

Research pushes the **overall security of the field forward**, ideally without having negative consequences for users of the product.

02
Cases

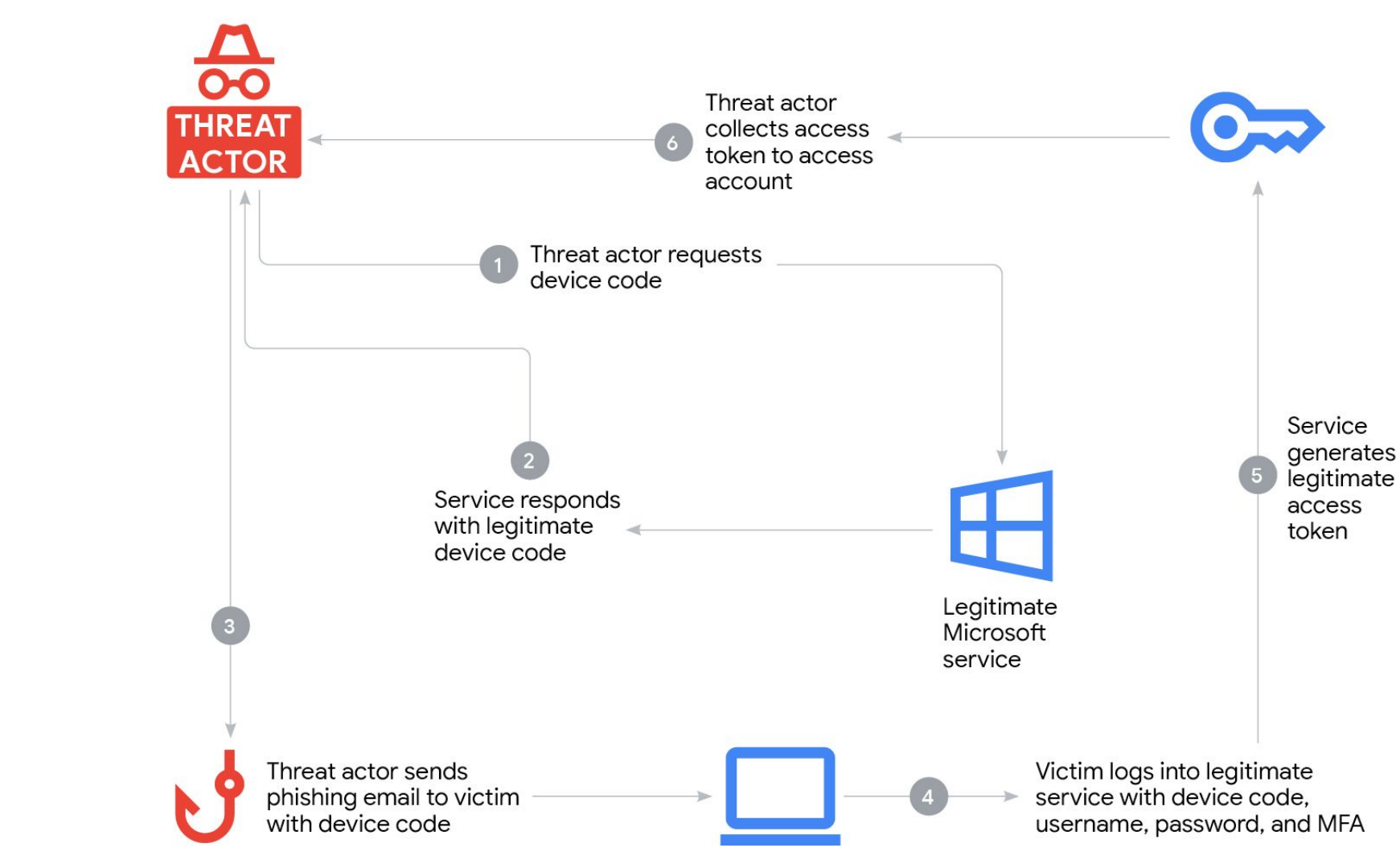
Abuse of cloud attack techniques by threat actors

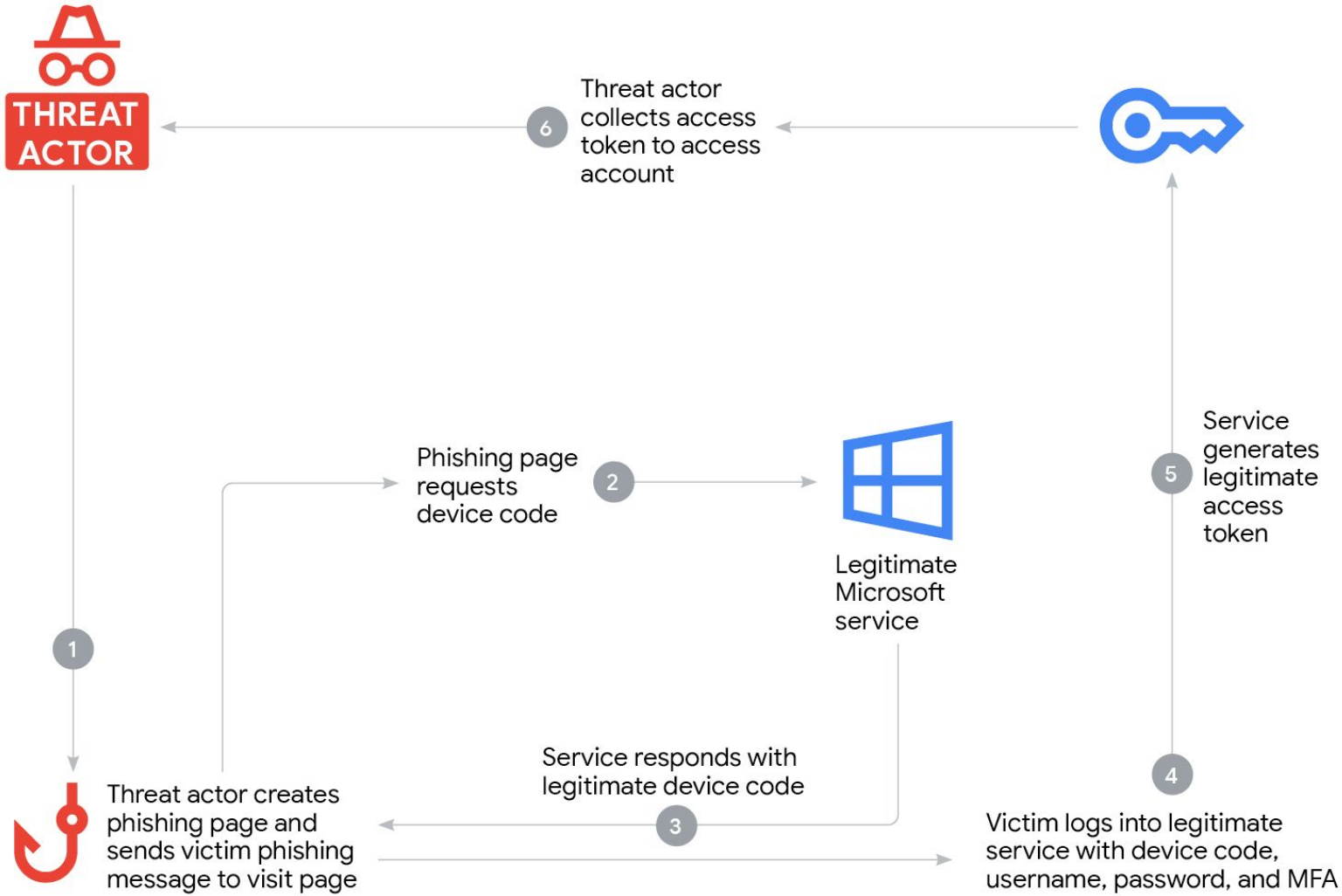
Researcher

Phishing for PRTs

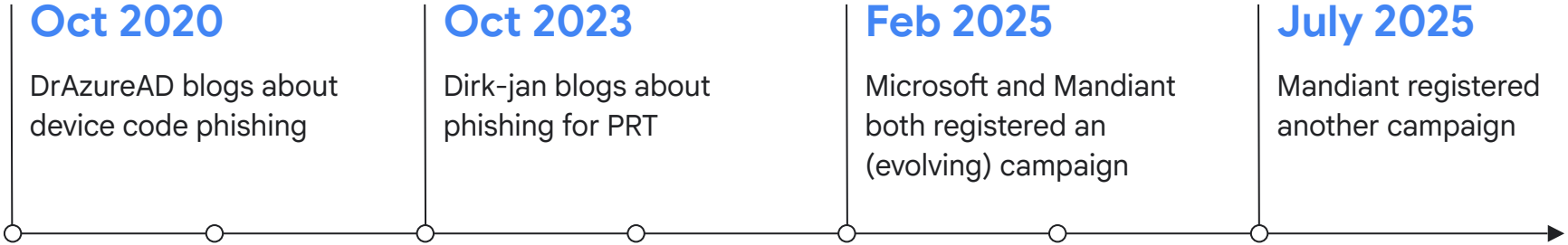
Threat actor

Device code phishing

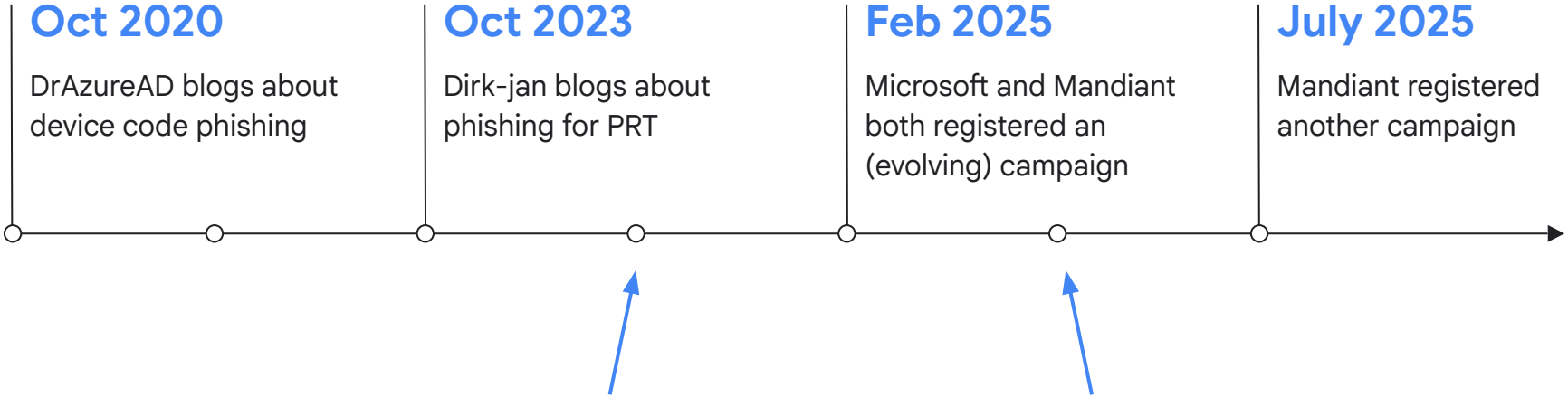

THREAT ACTOR
6
Threat actor collects access token to access account
1
Threat actor requests device code
2
Service responds with legitimate device code
3
Threat actor sends phishing email to victim with device code
4
Victim logs into legitimate service with device code, username, password, and MFA
5
Service generates legitimate access token
Legitimate Microsoft service


THREAT ACTOR
6
Threat actor collects access token to access account
Phishing page requests device code
2
Legitimate Microsoft service
5
Service generates legitimate access token
1
Service responds with legitimate device code
3
4
Threat actor creates phishing page and sends victim phishing message to visit page
Victim logs into legitimate service with device code, username, password, and MFA

Timeline


Oct 2020
DrAzureAD blogs about device code phishing
Oct 2023
Dirk-jan blogs about phishing for PRT
Feb 2025
Microsoft and Mandiant both registered an (evolving) campaign
July 2025
Mandiant registered another campaign

Timeline


Oct 2020
DrAzureAD blogs about device code phishing
Oct 2023
Dirk-jan blogs about phishing for PRT
Feb 2025
Microsoft and Mandiant both registered an (evolving) campaign
July 2025
Mandiant registered another campaign

Phishing for PRT

Primary Refresh Tokens are Single Sign On tokens and **can be used to sign in** to any application and any Entra connected website. This **links a user identity to a device identity** and is used in Conditional Access to enforce device based controls, like if it is compliant or hybrid joined for example.

It is resistant to credential phishing attacks, but you can **obtain a PRT with device code phishing**. By using this specific technique the threat actor has a much more powerful token that provides access to any app the victim can access.

Threat actor

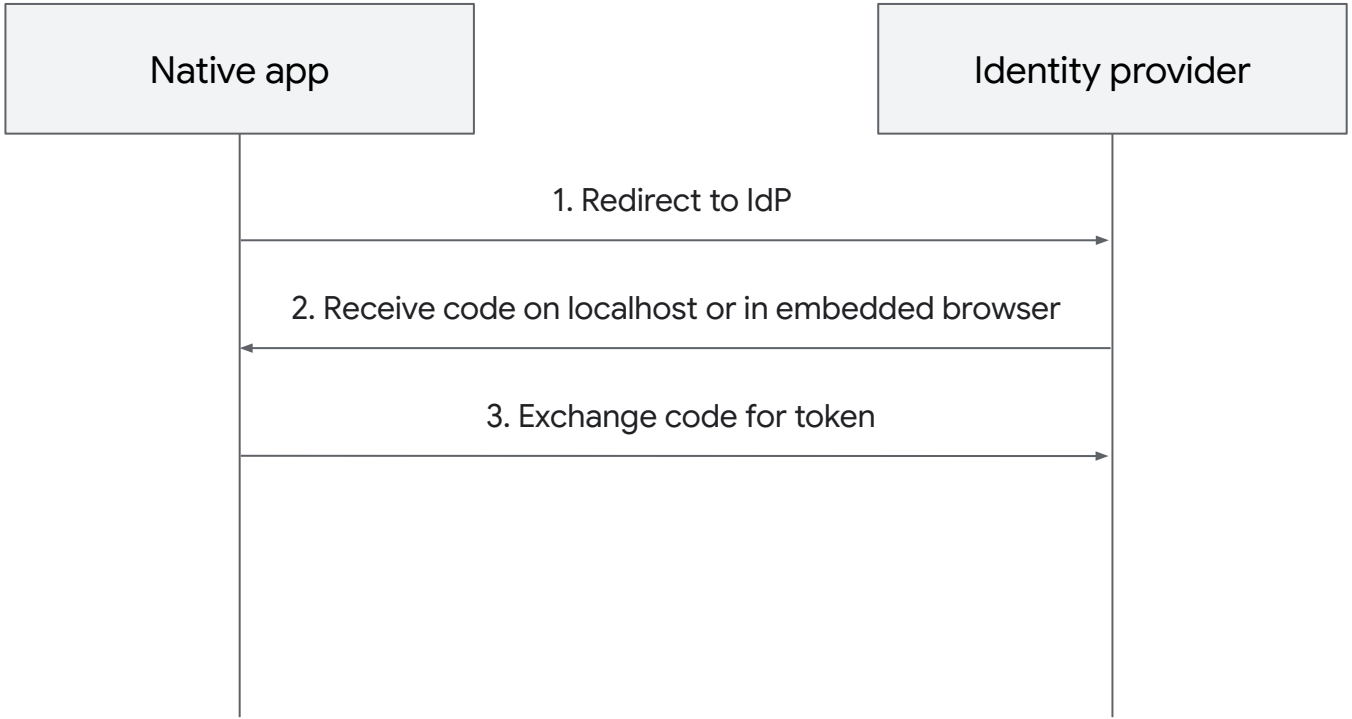
Authorization code phishing
aka ConsentFix

Authorization code phishing

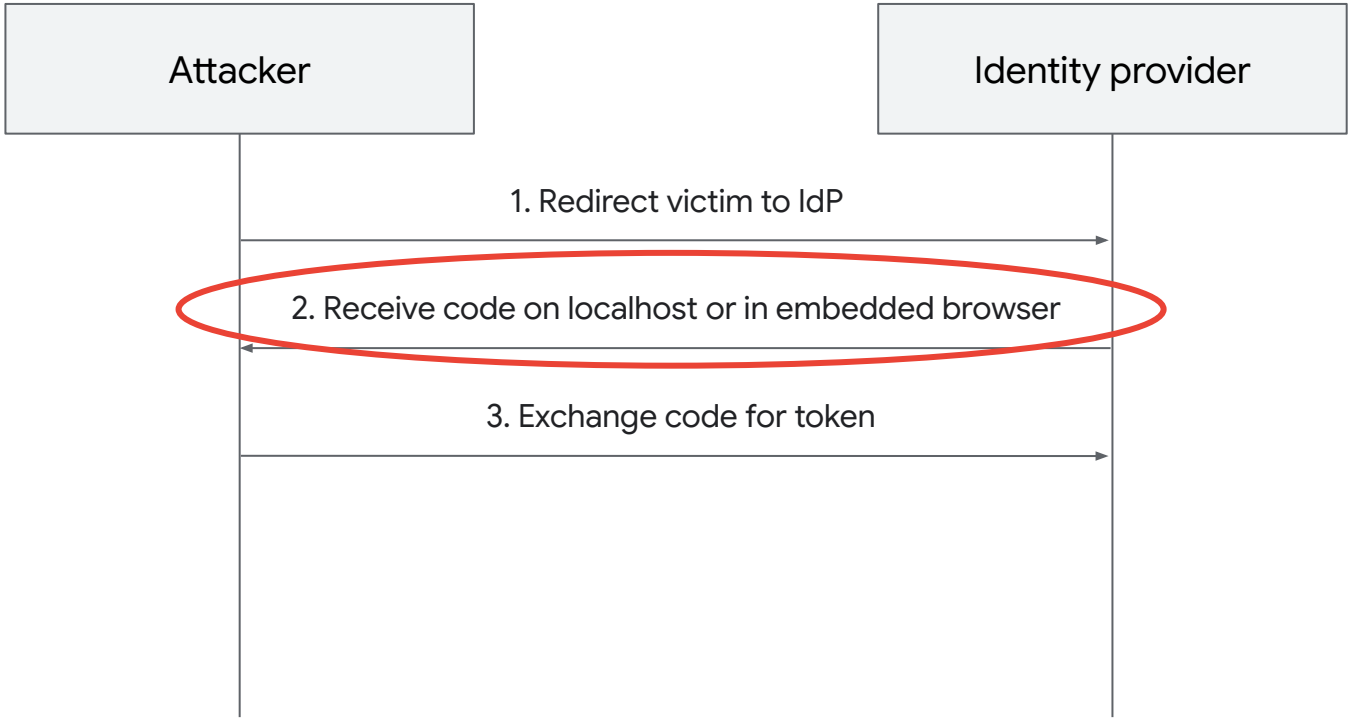
The **authorization code flow** is an OAuth2 flow that is used to sign in to websites and native apps.

The name is derived from the “**authorization code**” that is generated by the Identity Provider and sent to the application, which then exchanges that for **tokens**.

Authorization code flow



Authorization code phishing



Problem loading page

localhost/?code=1.AXkAqGH3BAqwkEusQSxUwSH8y

Azure phishy

Looks like there's a problem with this site

Firefox can't connect to the server at **localhost**

What can you do about it?

Try connecting on a different device. Check your modem or router. Disconnect and reconnect to Wi-Fi.

Try Again

Authorization code phishing

Authorization code phishing timelines

Volexity observed suspected Russian threat actors switching to **authorization code phishing** when **device code phishing** was getting less effective in March / April 2025.

Push Security published this under the name ConsentFix in December 2025. This campaign was using the same concept but in a more automated fashion.

The Volexity report also highlights attackers targeting the **device registration service** and the same **client ID used for PRT phishing**.

Unlike device code phishing, authorization code phishing complies with most Conditional Access policies and is **not easily blocked**, not even by most device based controls. It does require more **extensive user interaction**.

Researcher

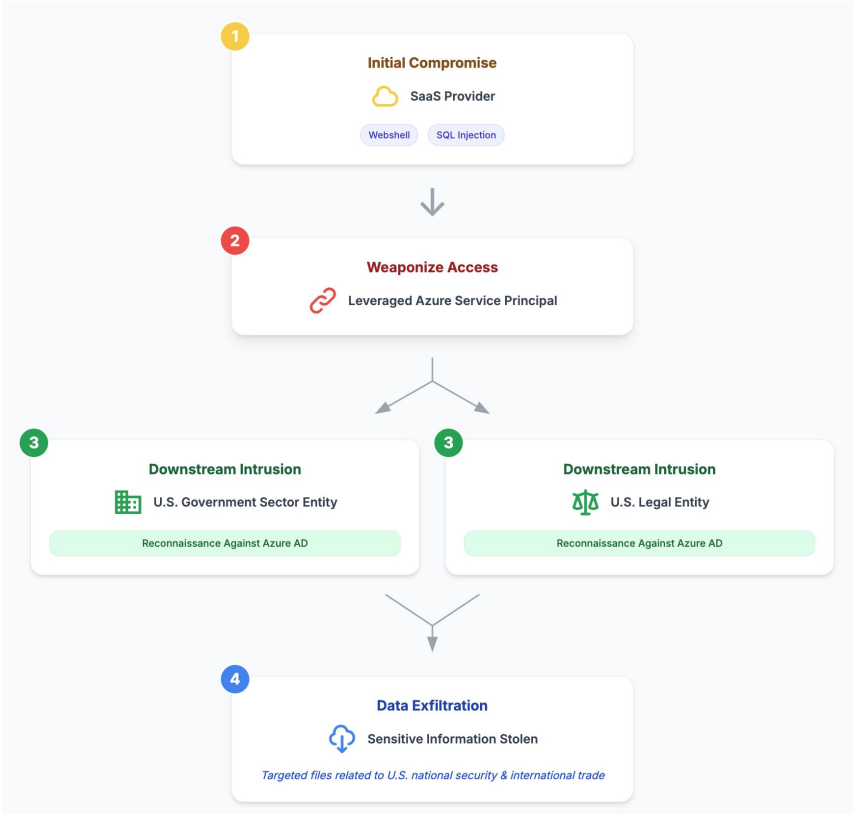
Cloud application backdoors

Threat actor

Downstream customer compromise with applications

Attack chain

Mandiant assesses that a threat actor has **compromised SaaS providers** likely to gain access to downstream targets that fall within the legal and government sectors in the United States, searching for **information related to US national security and international trade**. This assessment is made with medium confidence, based on Mandiant investigating two intrusions that stemmed from third party access of a targeted SaaS organization.



Threat activity

In one instance, after gaining access, **the threat actor made hundreds of Graph API requests** to extract user lists from the victim's Entra ID tenant. The actors also added new secrets to other cloud applications, indicating efforts to maintain access to the victim's Entra ID.

In another instance, the threat actor performed **reconnaissance using AzureHound**, an Azure-specific utility used with BloodHound to gather information about Entra ID and Azure Resource Manager (AzureRM) environments.

Timeline

Highlights of the intrusion timeline:

T0 First suspicious authentication using the Service Principal of a backup app

+6d Authentication to Graph API, Exchange Online and SharePoint for exfiltration

+1d Threat actor obtains persistence by modifying the KeyCredentials property

Multi-tenant applications

When installing an application from a third party vendor, a **trust relationship** is created between the **customer** tenant and the **vendor** tenant.

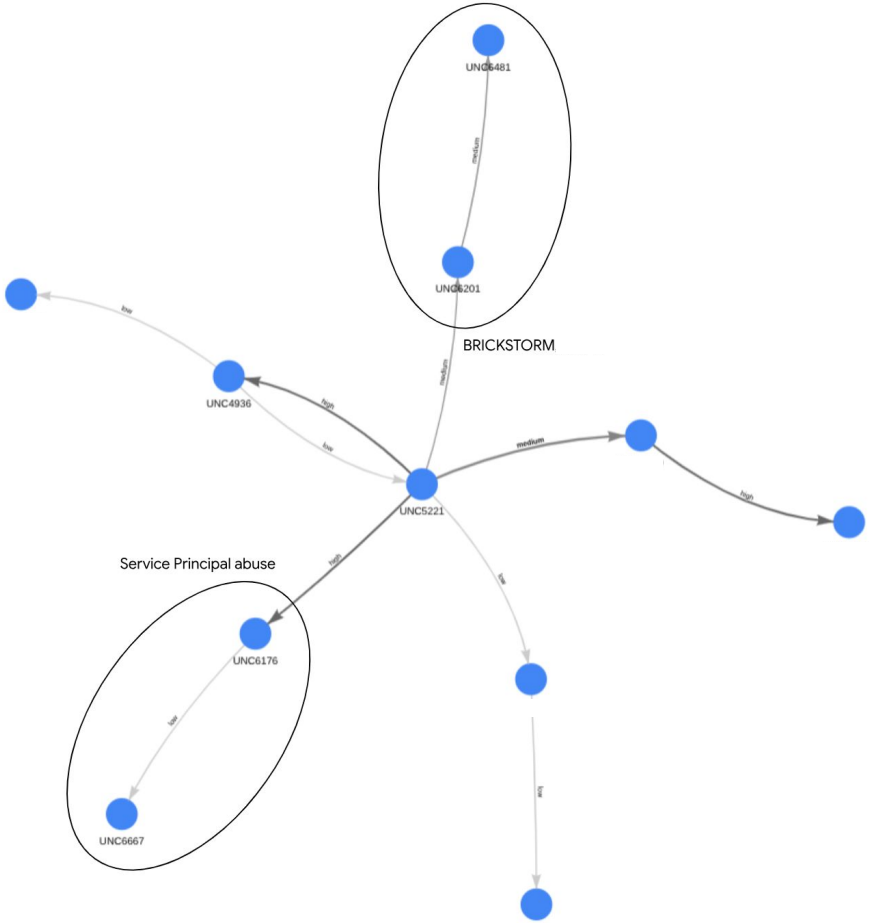
Depending on the permissions the vendor application needs, this may grant them access to company data such as **email**, **files** or even **administrative** tenant access.

Compromise of the vendor tenant can be used to move to downstream customer tenants.

Application abuse within a single tenant

Applications often are granted **extensive permissions** within the environment. Access to **business data** for automation purposes is a common configuration.

Threat actors can abuse applications for persistence and for automated data exfiltration over APIs by **assigning credentials** to existing applications.


UNC6481
medium
UNC6201
BRICKSTORM
low
UNC4936
high
low
medium
UNC5221
medium
high
Service Principal abuse
high
UNC6176
low
UNC6667
low
low

Shift in activity

Between 2025 and 2026, some threat actors shifted from just edge device exploitation to pivoting to **Microsoft 365 and Entra ID** for (long term) data exfiltration.

The use of highly specialized knowledge has been observed more and more. This includes **'niche' industry insights** that are typically inaccessible to those outside the specific industry.

Shift in activity

This could indicate possible **collaboration** with researchers, as we know that:

- Offensive cyber programs can be partly **outsourced** to private cybersecurity companies.
- Newly discovered zero-day vulnerabilities found by citizens or companies **must be reported to the state** before being patched or publicly disclosed.
- The government and state-linked enterprises use hacking competitions (like CTFs) and elite corporate vulnerability research labs to **identify top talent and harvest exploit techniques**.

Researcher

Open source tools

Threat actor

Using open source tools

AADInternals

Open source PowerShell based tool for offensive Entra ID operations. Popular by threat actors because of its easy accessibility (PowerShell) and many built-in exploitation capabilities.

Contains exploits that need to run on victim infrastructure, but also modules for interacting with the cloud from attacker devices.

Written by Finnish security researcher Dr Nestori Syynimaa.

AADInternals

Open source PowerShell based tool for offensive Entra ID operations. Popular by threat actors because of its easy accessibility (PowerShell) and many built-in exploitation capabilities.

Contains exploits that need to run on victim infrastructure, but also modules for interacting with the cloud from attacker devices.

Written by Finnish security researcher Dr Nestori Syynimaa.

Since 2021, various threat actors have utilized this tool for both financial gain and espionage. In most cases, the threat actor used AADInternals to lateral move from the on-premise environment to the cloud, so hands-on keyboard activity where the tool was used was observed. Comparing the changelog of the tool with usage, a nation-state threat actor adopted the tool within 2 months*

* This could be earlier, but detection of the cloud-only features of the tool is complicated due to limited telemetry.

ROADtools

Python based framework with different tools. Most popular tools include roadrecon and roadtx.

- roadrecon is a **recon focused** tool that makes a snapshot from the tenant and visualizes all the identities and admins from an offline database.
- roadtx is a tool for **requesting and using tokens**, registering fake devices and performing pass-the-token attacks.

No built-in exploits, limited logging since tools usually executed on the attackers infrastructure.

ROADtools

Python based framework with different tools. Most popular tools include roadrecon and roadtx.

- roadrecon is a **recon focused** tool that makes a snapshot from the tenant and visualizes all the identities and admins from an offline database.
- roadtx is a tool for **requesting and using tokens**, registering fake devices and performing pass-the-token attacks.

No built-in exploits, limited logging since tools usually executed on the attackers infrastructure.

Threat actors were observed to be using ROADtools shortly after publication on GitHub.

Last year, a threat actor was observed to be using roadrecon. After getting an authentication token, the threat actor authenticated to the tenant with roadrecon. It is hard to detect roadrecon activity based on logging, but the command was observed to be executed from attacker infra.

Newly introduced Azure AD graph activity logs provide visibility into roadrecon usage.

ROADtools

Python based framework with different tools. Most popular tools include roadrecon and roadtx.

- roadrecon is a **recon focused** tool that makes a snapshot from the tenant and visualizes all the identities and admins from an offline database.
- roadtx is a tool for **requesting and using tokens**, registering fake devices and performing pass-the-token attacks.

No built-in exploits, limited logging since tools usually executed on the attackers infrastructure.

Not everyone is successful in running it..

They then tried to use a tool called ROADtools Token eXchange (roadtx):

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python313\Scripts\roadtx.exe prtauth -r msgraph -c msteams
```

And then erroneously tried to run the same tool (as an executable) via Python:

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python313\python.exe C:\Users\Administrator\AppData\Local\Programs\Python\Python313\Scripts\roadtx.exe prtauth -r msgraph -c msteams
```

Then ran it again:

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python313\Scripts\roadtx.exe describe
```

And then tried to run it again, erroneously, using Python:

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python313\python.exe C:\Users\Administrator\AppData\Local\Programs\Python\Python313\Scripts\roadtx.exe describe
```

Takeaways

- The **motivation** of security researchers and threat actors are significantly different in cloud attacks
- This results in a **selective adoption** of published techniques: threat actors quickly adopt readily available tools, but are more selective in applying deeper concepts and theoretical attack paths.
- Advanced attackers do **evolve in tactics and techniques** if other option doesn't work, including novel techniques that are not well known in the research community.
- We **do not have full visibility** into abuse of cloud services
    - Full telemetry only available to the vendor.
    - Non-critical vulnerabilities often get patched without notification or details.
    - Detection is limited to what the vendor offers.
    - Many cloud tools will run on attacker hosts, limits visibility into exact methods used.

References

- https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia
- https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign
- https://aadinternals.com/post/phishing/
- https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens/
- https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
- https://pushsecurity.com/blog/consentfix
- https://github.com/dirkjanm/roadtools
- https://www.huntress.com/blog/rare-look-inside-attacker-operation

Thank you