MUNICH CYBER TACTICS
TECHNIQUES AND PROCEDURES | 25

MCTTP

Microsoft Security

Defending Against the Evolving OAuth Attack Landscape

Daniel Goltz
Dr Nestori Syynimaa

Who are we?

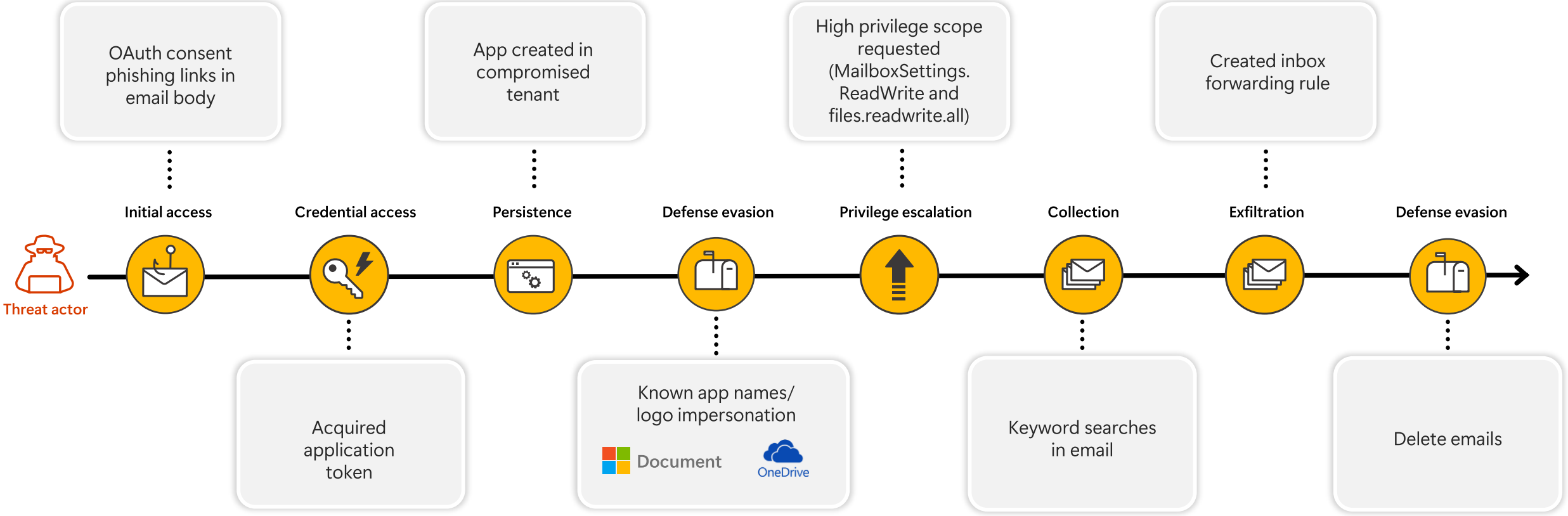
Daniel Goltz
Principal Security Engineering Manager
Microsoft Red Team

Dr. Nestori Syynimaa (@DrAzureAD)
Principal Identity Security Researcher
Microsoft Threat Intelligence Center (MSTIC)

Agenda

- **OAuth Threat Landscape Overview**
- **Token-Based Authentication 101**
- **Attack Scenarios & Demos**
- **Detecting & Preventing**

Real World OAuth Attack



The Evolving OAuth Attack Landscape

OAuth: A Critical Attack Surface

OAuth-connected apps have become a critical attack surface. More apps, more interconnectivity, and implicit trust = more opportunities for attackers. We can no longer treat OAuth access as “set and forget.”

SaaS Proliferation

Explosive growth in SaaS apps – enterprises use ~150 apps on average today (up from ~10 a decade ago).

App-to-App Connectivity

Employees routinely connect apps together for productivity. One click can grant an app permissions to read or write email, files, and more. This expanded trust boundary creates new attack paths.

Advanced Threat Adoption

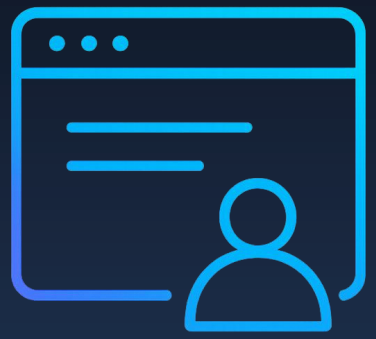
Nation-state and financially motivated actors are increasingly exploiting OAuth. Modern attackers have added OAuth abuse to their playbooks for persistence and lateral movement in the cloud.

GenAI and User Ease

Threat actors also benefit from those advanced tools to easily launch sophisticated attacks. Meanwhile, with ease of access, securing GenAI poses new challenges.

Token-Based Authentication 101

Key concepts



User/App

- Consumes services

Service Provider (SP)

- Provides services

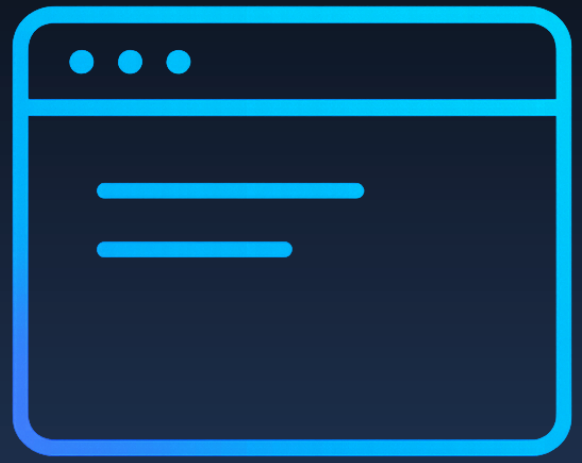
Identity Provider (IdP)

- Provides identity and access management

OAuth Permissions

Delegated Permissions

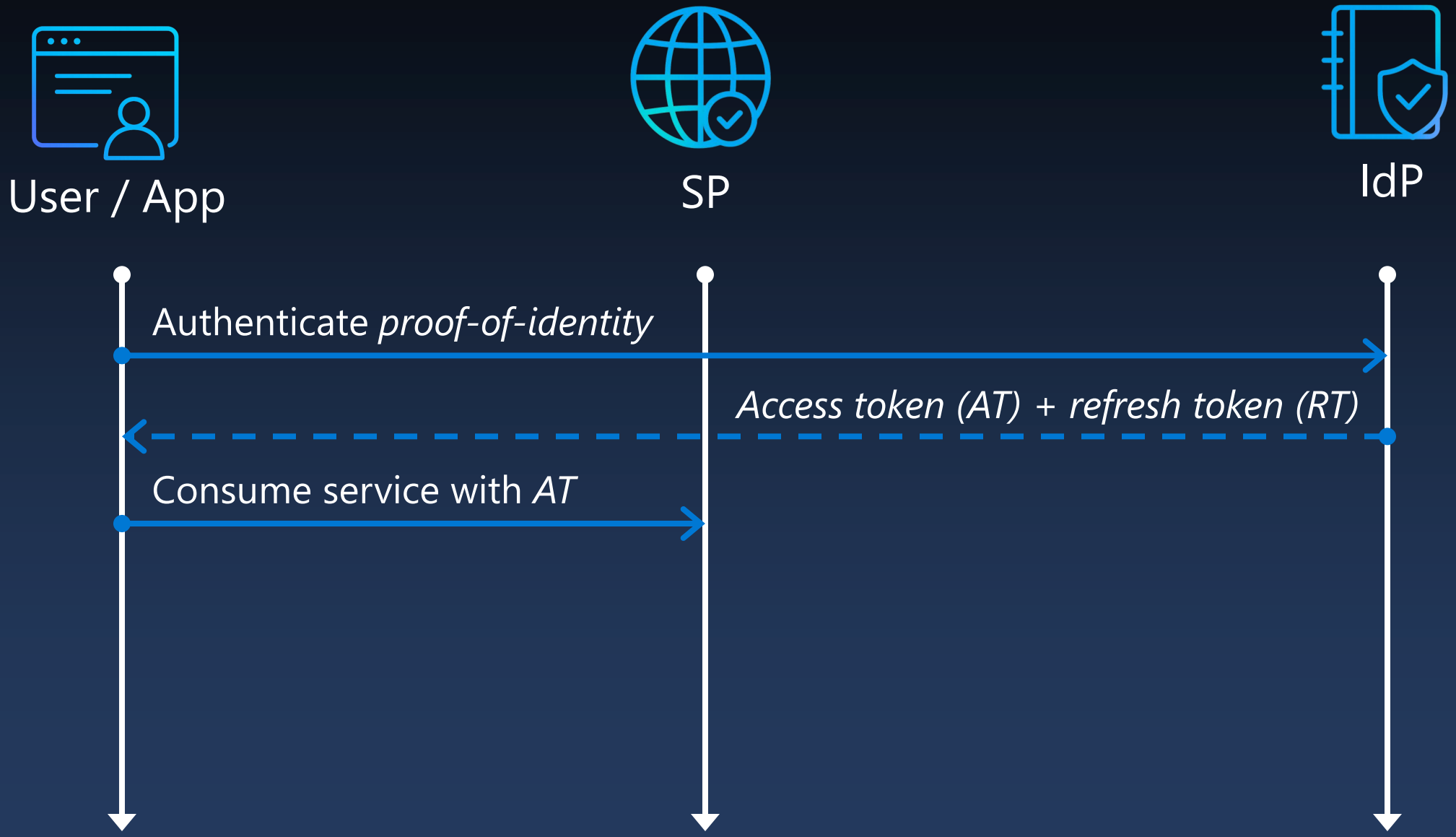
Delegated permissions allow apps to act on-behalf-of users who provide their consent.



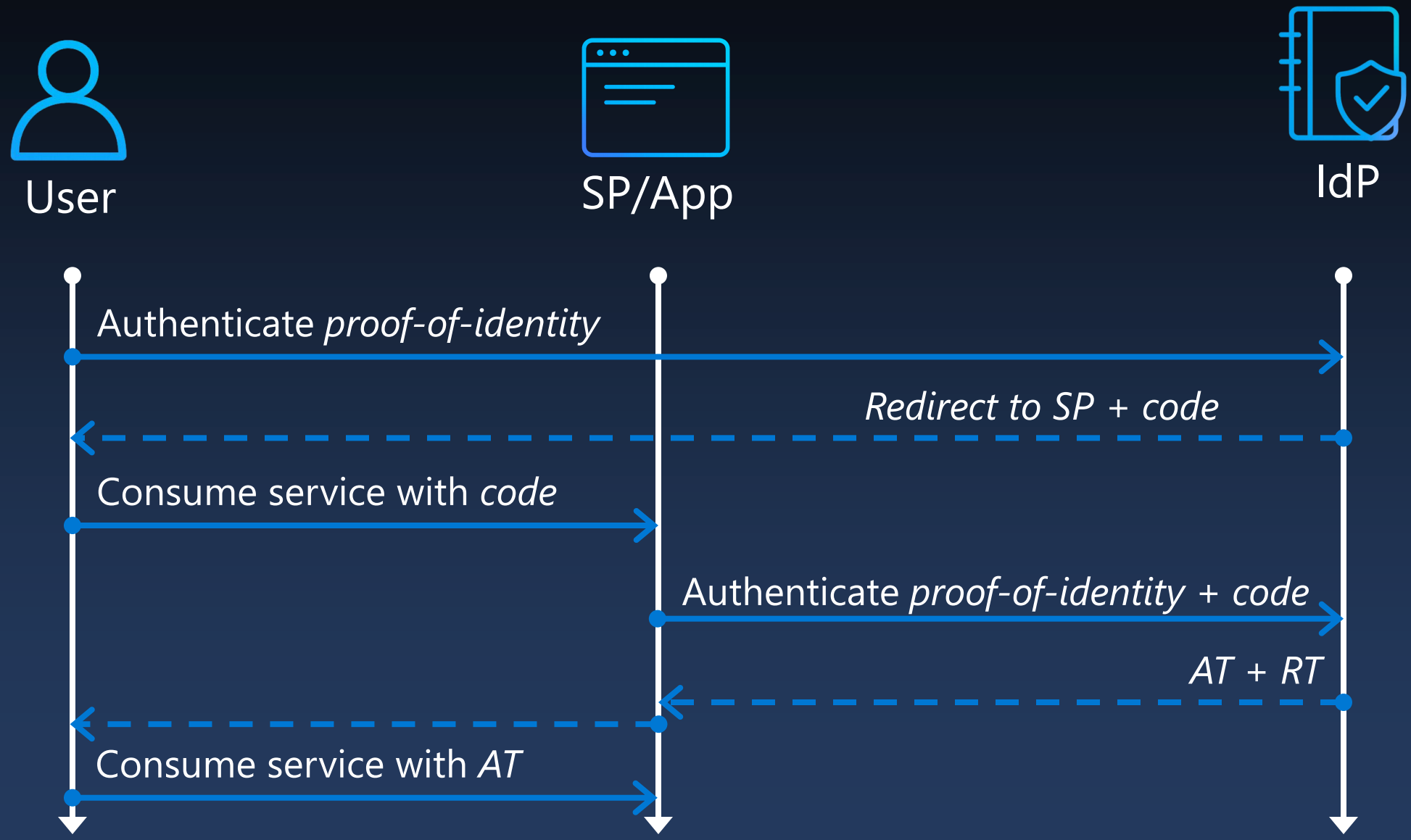
App-Only Permissions

App-only permissions grant apps their own identity through admin consent.

OAuth ROPC flow



OAuth authorization code flow



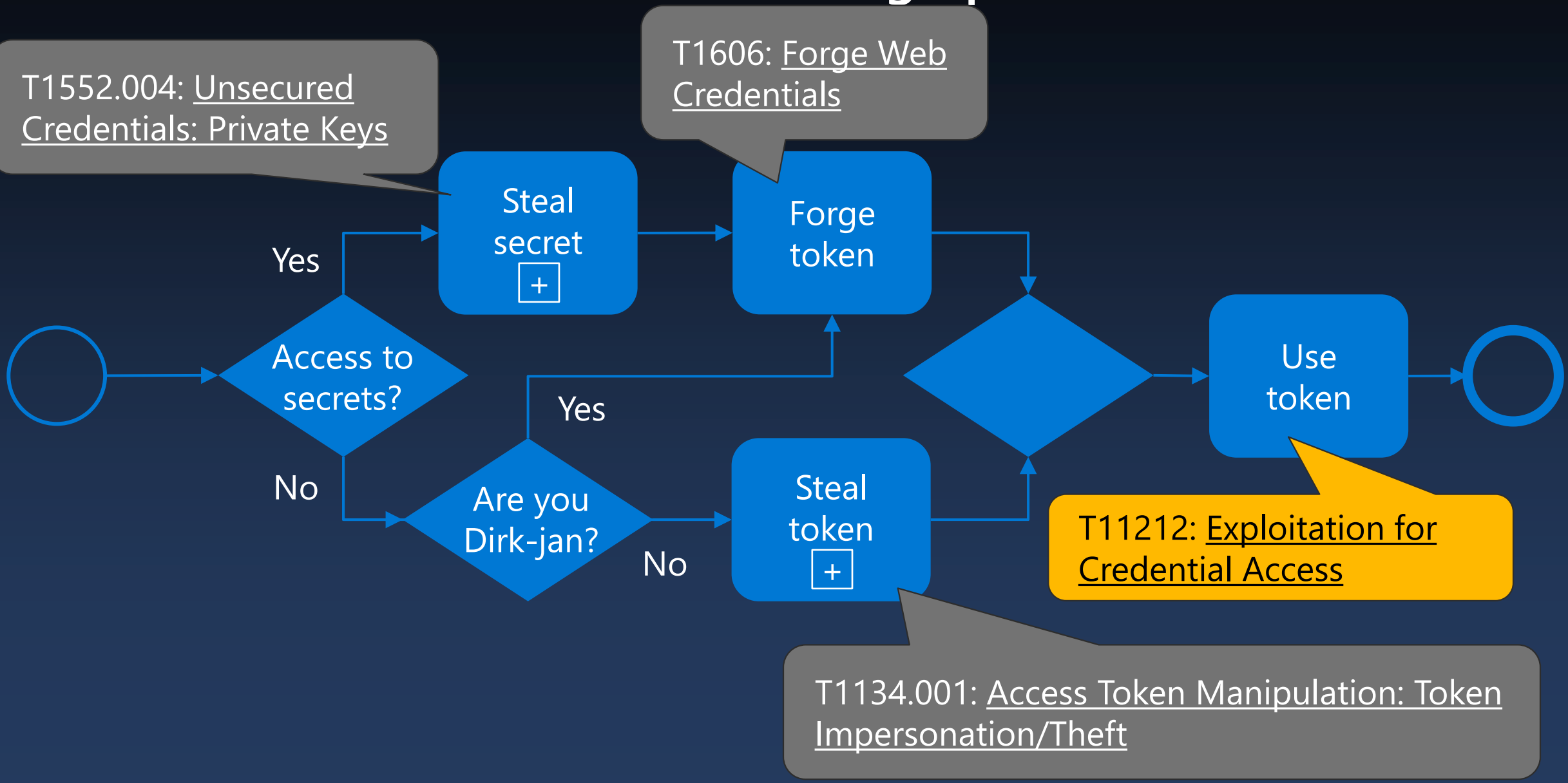
OAuth Attack Vectors

OAuth Attack Vectors – How Attackers Exploit Them

Main **attack vectors** we see with OAuth and tokens:

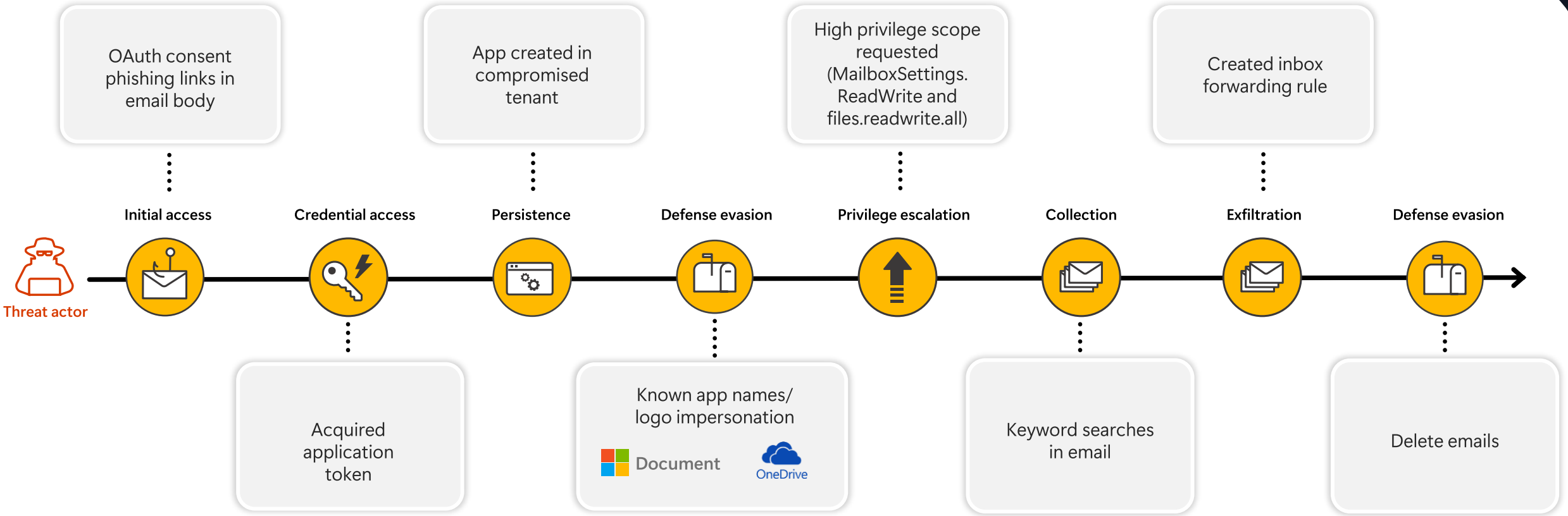
1. Consent Phishing (Malicious OAuth Apps)
2. Token Theft
3. Stolen Keys & Token Forgery
4. Compromised OAuth App Credentials
5. Emerging Threats: SaaS Harvesters & Cryptojacking

Token-based authentication attack graph

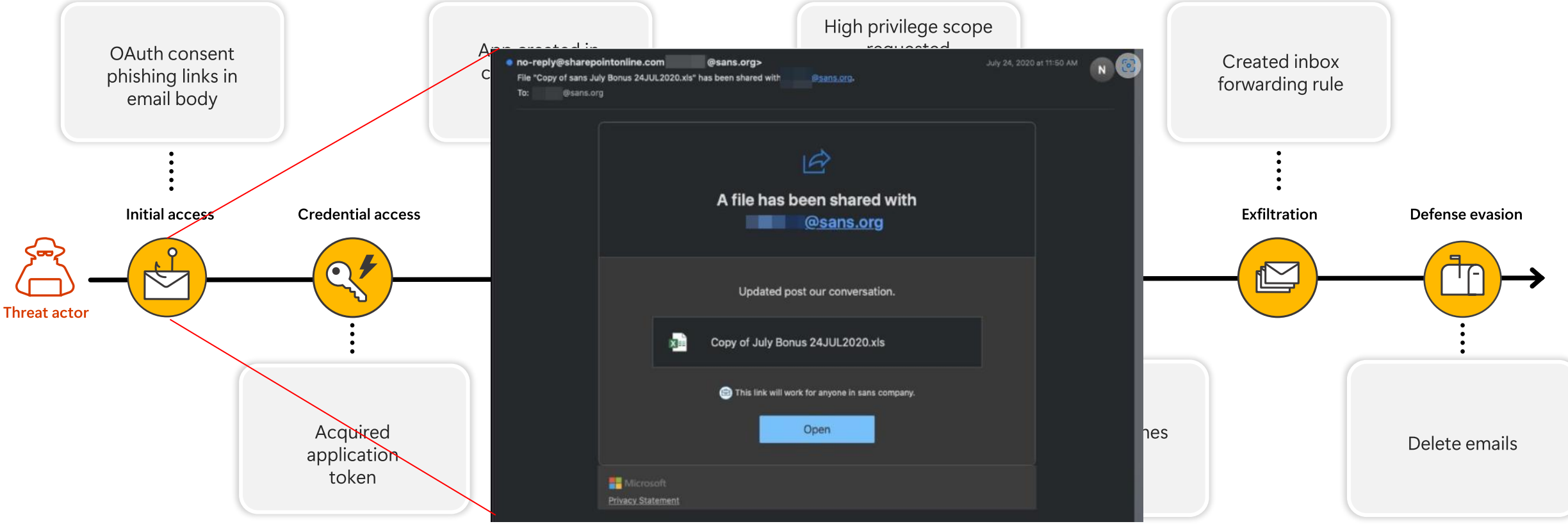


Demos

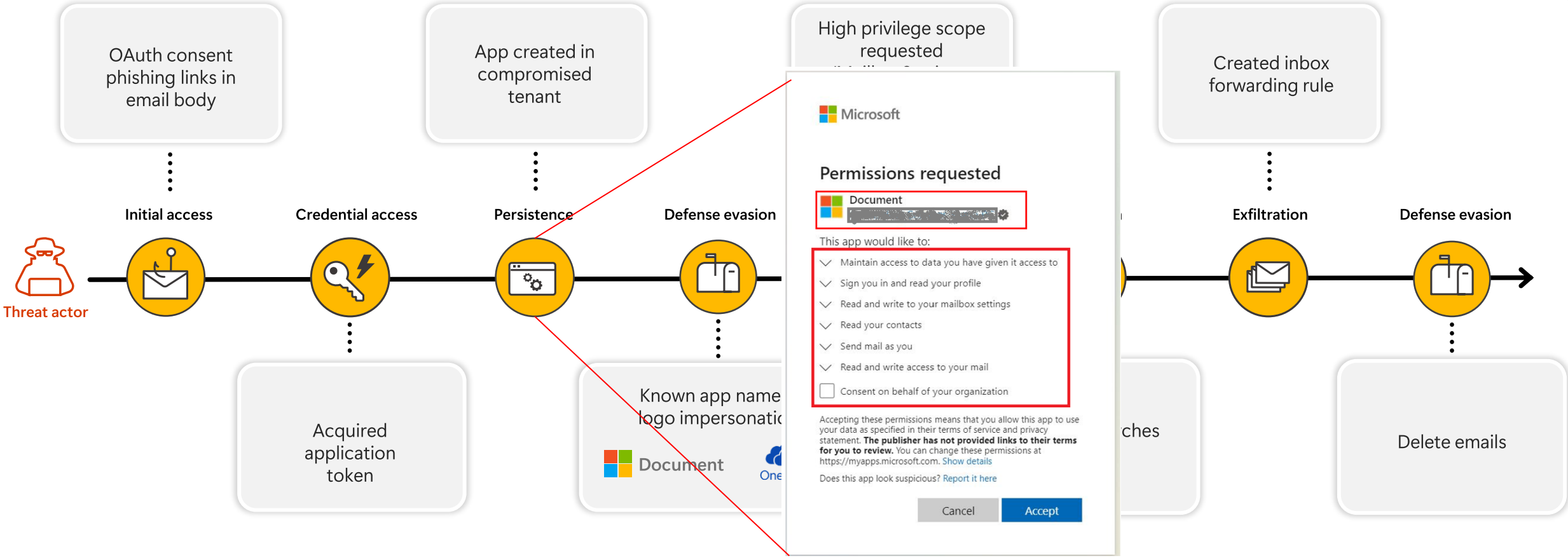
Case study: OAuth Consent Phishing (Malicious App) Attack Flow



Case study: OAuth Consent Phishing (Malicious App) Attack Flow



Case study: OAuth Consent Phishing (Malicious App) Attack Flow



Emerging Threat: SaaS Harvesters at Scale

Financially motivated attackers who focus on accessing SaaS applications at scale with the intent to profit, usually by selling data or extorting the victims.

https://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/

Emerging Threat: Cryptojacking In The Cloud

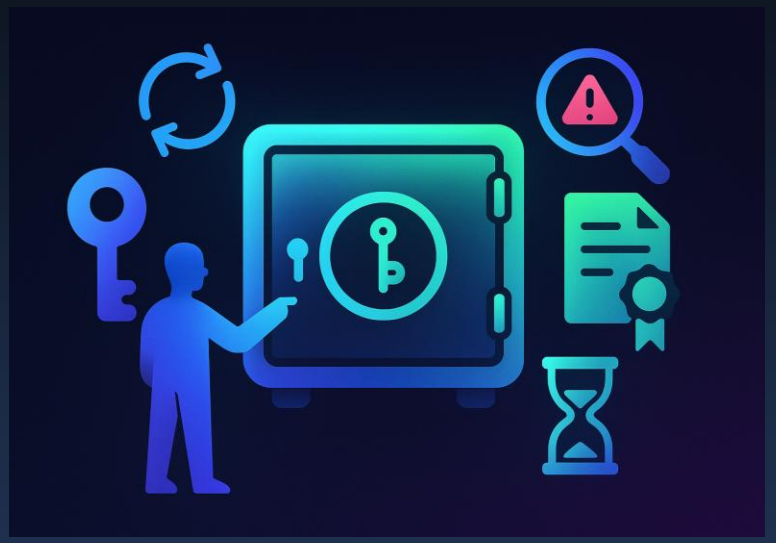
https://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/

Detecting & Preventing

Prevention Strategies – Stopping OAuth Attacks Up Front

Control Access

- User Consent Governance
- Least Privilege for Apps
- Conditional access controls



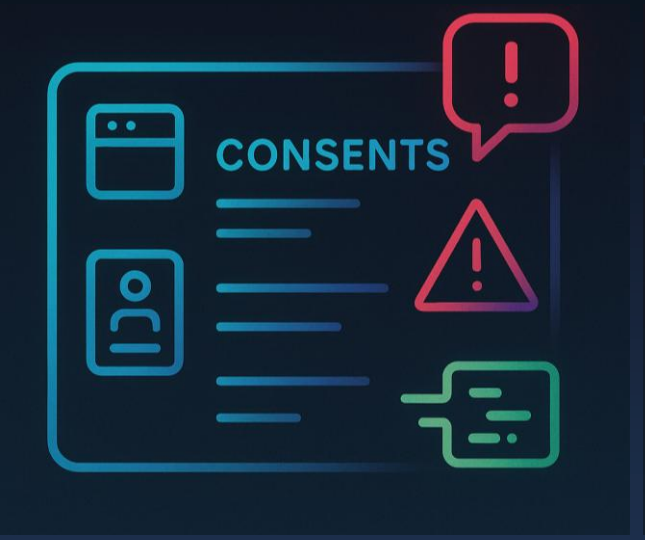
Secure Credentials

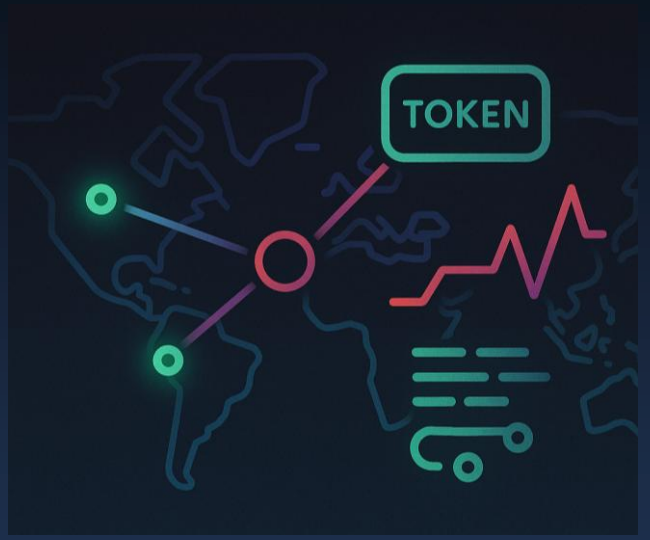
- Protect app secrets
- Zero Trust mindset

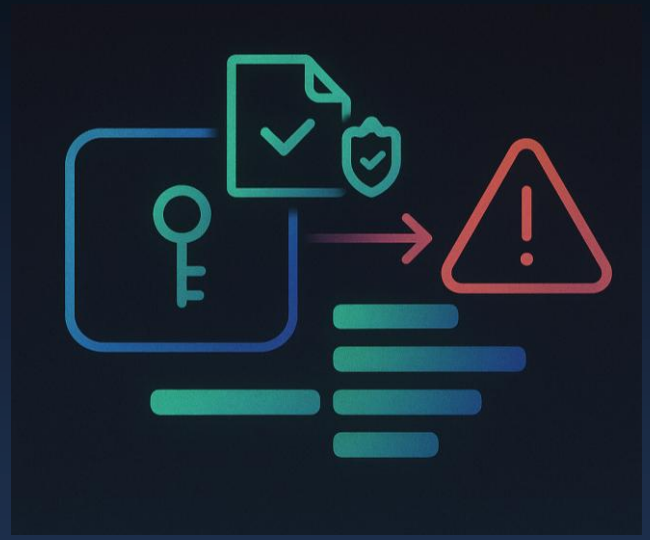
Evaluate & Maintain

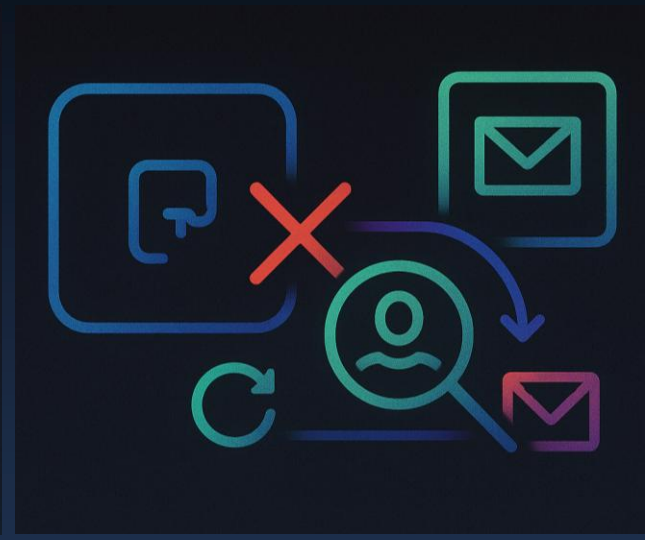
- Vet third-party apps
- Constant cleanup & hygiene

Detection & Response – Finding Malicious OAuth Activity









Visibility & Logging

Enable detailed logs for consents, app creations, and service principal sign-ins, and generate alerts for suspicious events.

Anomaly Detection

Identify unusual token usage (time, location, volume) and watch for abnormal API activity like mass downloads or forwarding rules.

App Change Monitoring

Track when apps gain new credentials, owners, or elevated permissions, which may indicate attacker tampering.

Rapid Response

Act fast to revoke malicious apps and tokens, then investigate the wider context to uncover related accounts or additional backdoors.

Key Takeaways

1. OAuth Attacks Are Here to Stay.
2. Non-Human Identities = First-Class Identities
3. Single Click, Full Compromise
4. Defense in Depth is Vital
5. Be Prepared for the Next Evolution

How many OAuth apps have access to your data right now?

Do you know what permissions they have and who added them?

Do you allow users to bring their own devices?

Questions


Microsoft Security
Thank you!