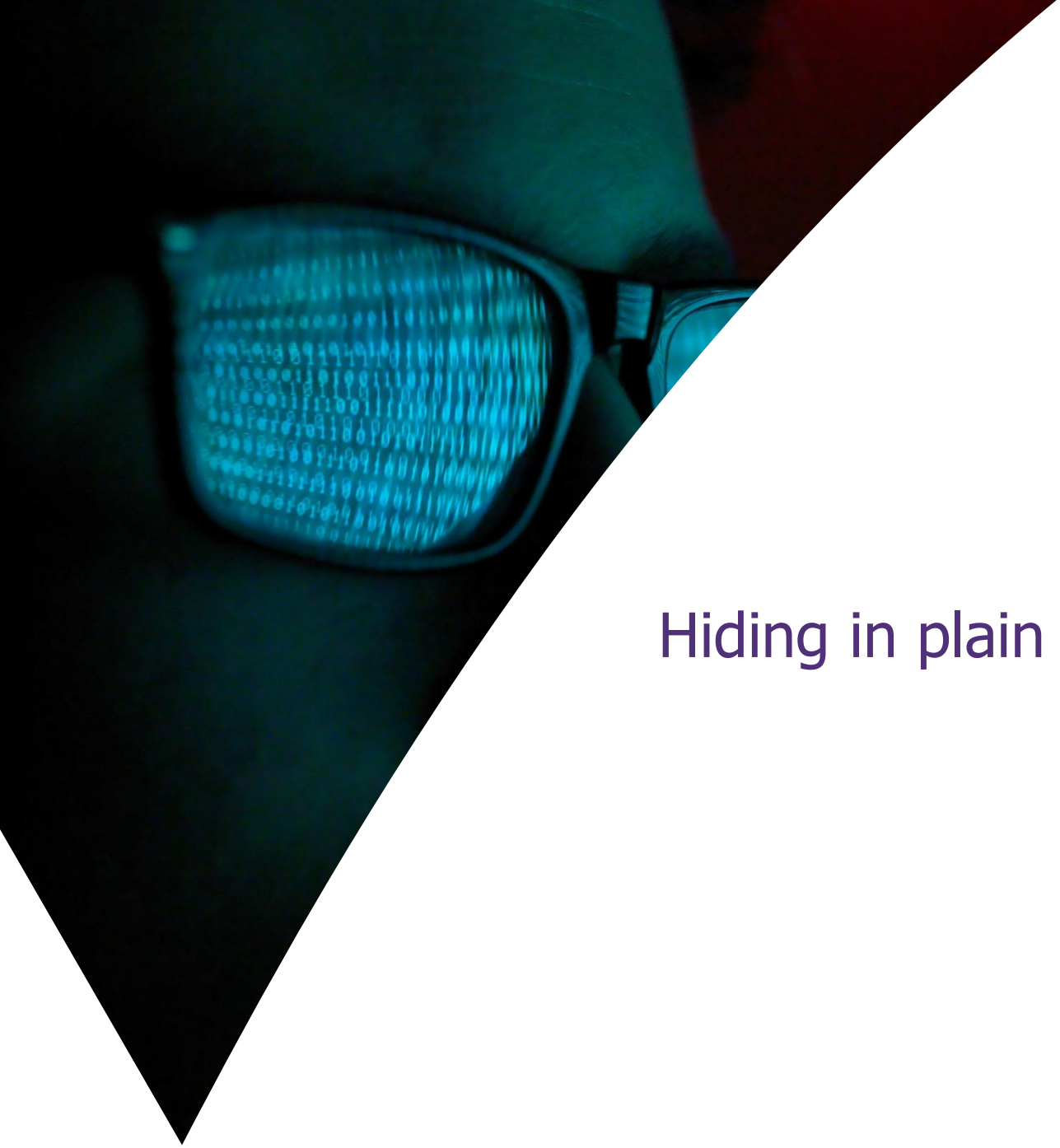


Hiding in plain sight: abusing Graph API for the win

Botconf 2023 lightning talks

Jean MARSAULT – @iansus

Assignment context

- French commercial CERT – Incident response for large client in retail during March 2023
- Initial intrusion through unpatched appliance
- Access sold 1 week later
- Full domain admin *privesc* in 5 hours
- Attacker caught during lateralization / persistence establishment

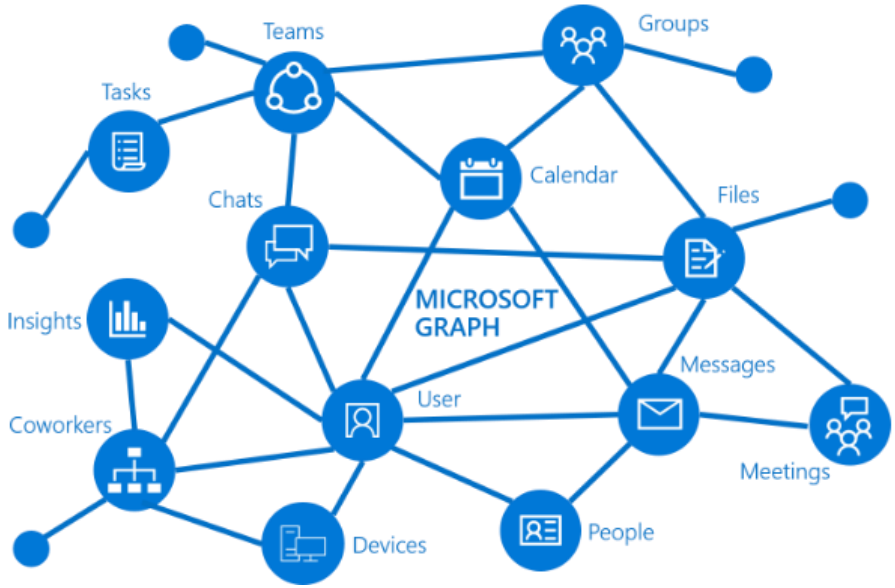
Focus on persistence

For once, we had **full visibility** on killchain through non-rotated logs

- Persistence on patient 0 through Linux userland rootkit
- On compromised assets, if connected to the Internet, **custom beacon deployment**

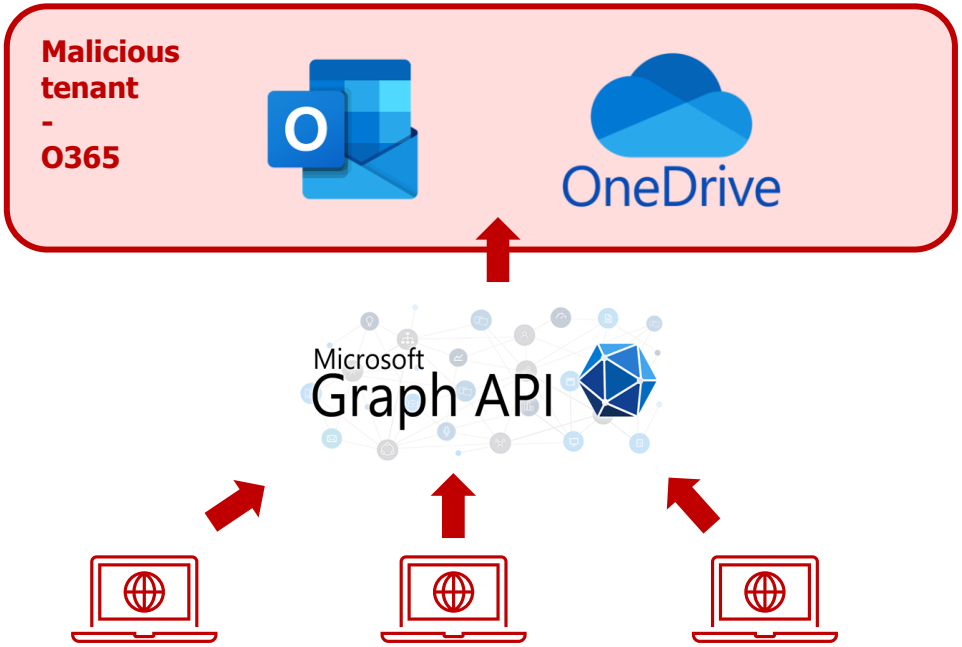
Tired of having your IP / domain blocked? Microsoft Graph API to the rescue!

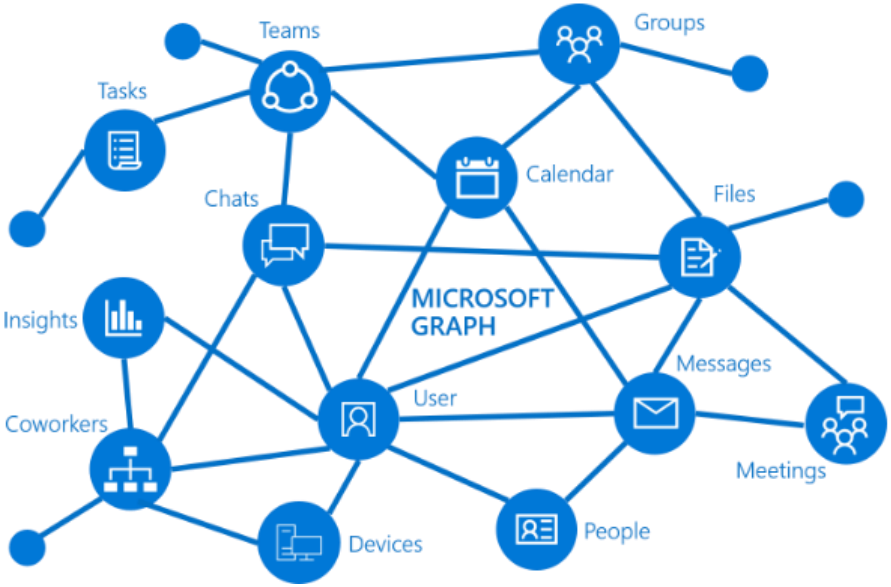
- Microsoft Graph API provides access to **lots** of Microsoft services
- Hard to block outgoing communications because **used everywhere**
- Sometimes **whitelisted** in direct outgoing communications (without proxy) due to load issues
- Perfect channel for **C2 communications**



Tired of having your IP / domain blocked? Microsoft Graph API to the rescue!

- Microsoft Graph API provides access to **lots** of Microsoft services
- Hard to block outgoing communications because **used everywhere**
- Sometimes **whitelisted** in direct outgoing communications (without proxy) due to load issues
- Perfect channel for **C2 communications**



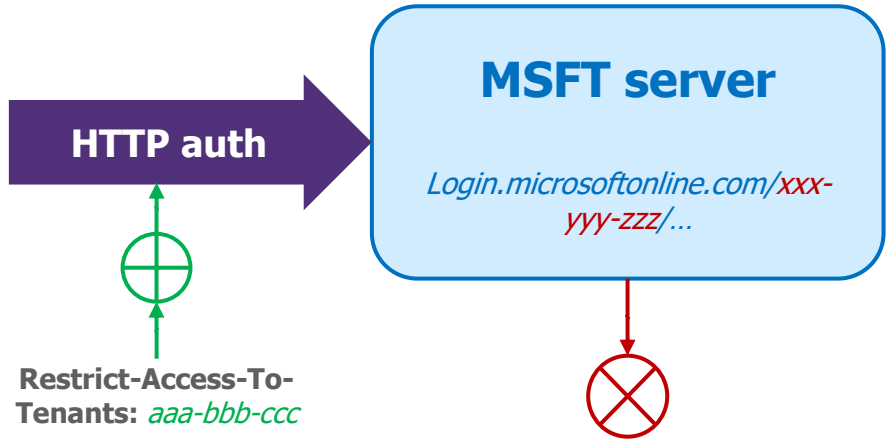


- In our case, the beacon talks to a **malicious Azure tenant** created by the attacker
- Uses **Outlook** subscription and the **drafts folder** as dead-drop for commands and outputs
- Uses **OneDrive** for file upload/download

It feels hopeless for the blue team…
Unless you know of Microsoft Tenant Restriction!

What it is

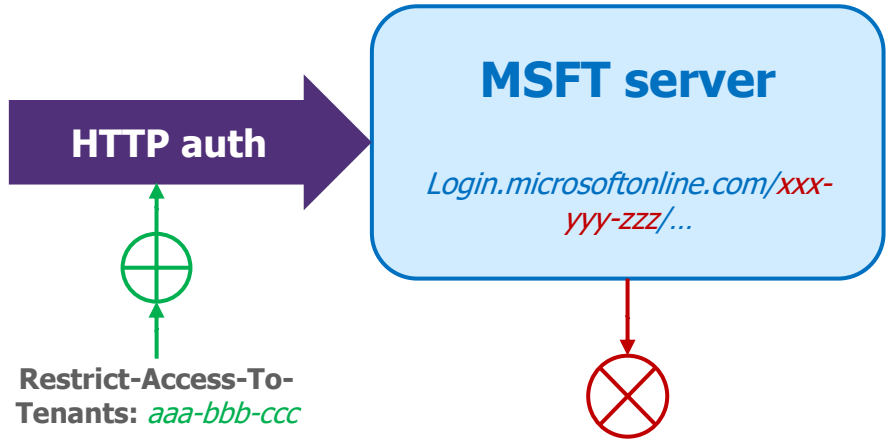
- Tenant restriction is a **security feature** from Microsoft
- Embeds a **whitelist** of *tenant-ids* for which auth is allowed
- Microsoft server checks the *tenant-id* in the **auth URI** against the provided whitelist and **denies access** if no match
- HTTP headers *Restrict-Access-To-Tenants* and *Restrict-Access-Context*



It feels hopeless for the blue team…
Unless you know of Microsoft Tenant Restriction!

What it is

- Tenant restriction is a **security feature** from Microsoft
- Embeds a **whitelist** of *tenant-ids* for which auth is allowed
- Microsoft server checks the *tenant-id* in the **auth URI** against the provided whitelist and **denies access** if no match
- HTTP headers *Restrict-Access-To-Tenants* and *Restrict-Access-Context*



Forcepoint

zscaler™

BROADCOM®

In practical

- Many **proxy software** are compatible with this feature
- Makes use of **SSL interception** of Microsoft auth domains
  - login.microsoftonline.com
  - login.microsoft.com
  - login.windows.net
- Performs **HTTP header injection** to outgoing requests