Exploiting The Microsoft Cloud (Azure & M365)

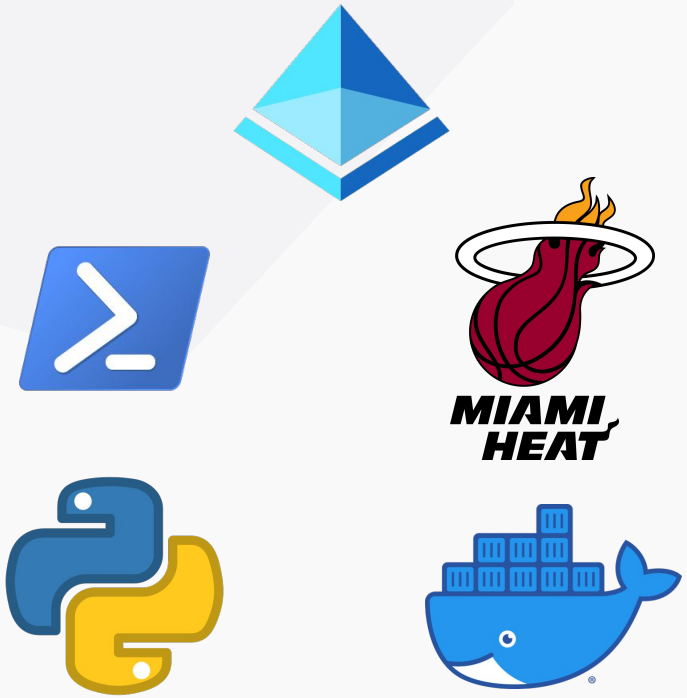
By: Alberto Rodriguez

2021

whoami

Alberto Rodriguez (@_ar0d_)

- Director & Operator @ SIXGEN
- Lead Instructor @ HackerU
- Ex Cyber Operations Officer (17A) @ US Army
- Ex SOC & Threat Simulation Lead



Agenda

- Why this talk?
- The Microsoft Cloud
- Reconnaissance
- Attacks
  - Password Attacks
  - Phishing
  - O-Day
- Quick Wins! (Defenders…. #TYFYS)

Why?

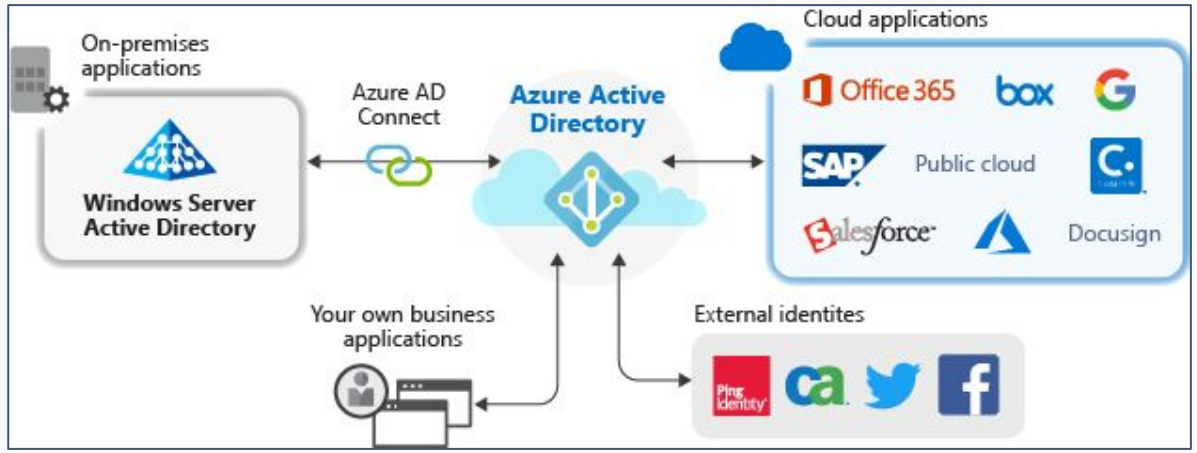
Why this talk?

- Microsoft Cloud vs Google Cloud vs AWS (or all)
- On-premise AD is not going away :)
- Windows is still a common/preferred OS by users
- Still new to many!

The Microsoft Cloud

M365 vs O365 vs Azure

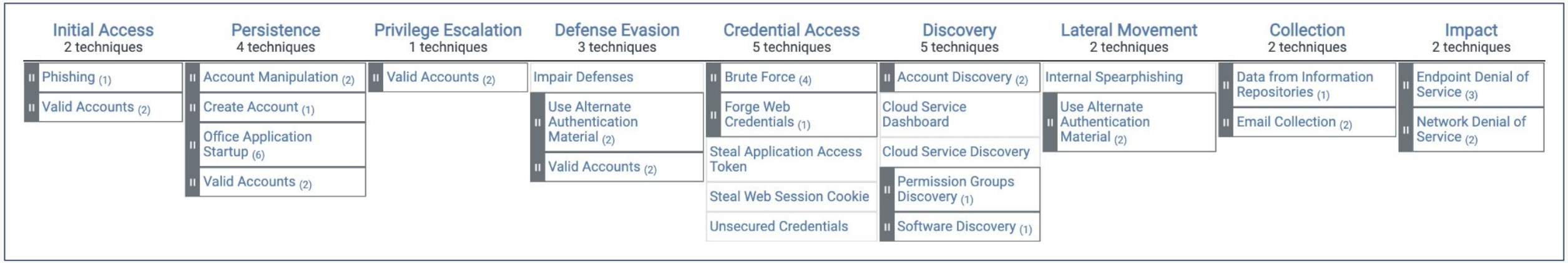
- **Software** as a Service vs **X** as a Service
- Sensitive Data
- Azure Active Directory
  (not the same as on-premise AD)
- Windows 11 (requires a Microsoft account and an internet connection at setup… sort of...)



https://docs.microsoft.com/en-gb/azure/active-directory/manage-apps/what-is-application-management

The Microsoft Cloud

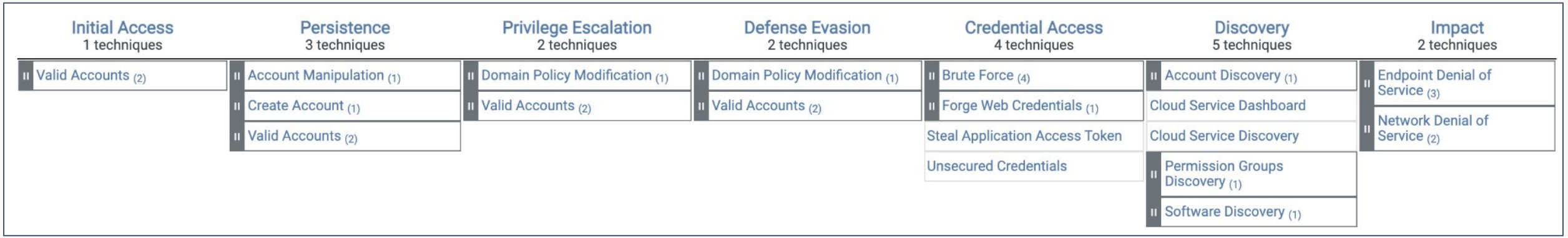
ATT&CK - O365



https://attack.mitre.org/matrices/enterprise/cloud/office365/

The Microsoft Cloud

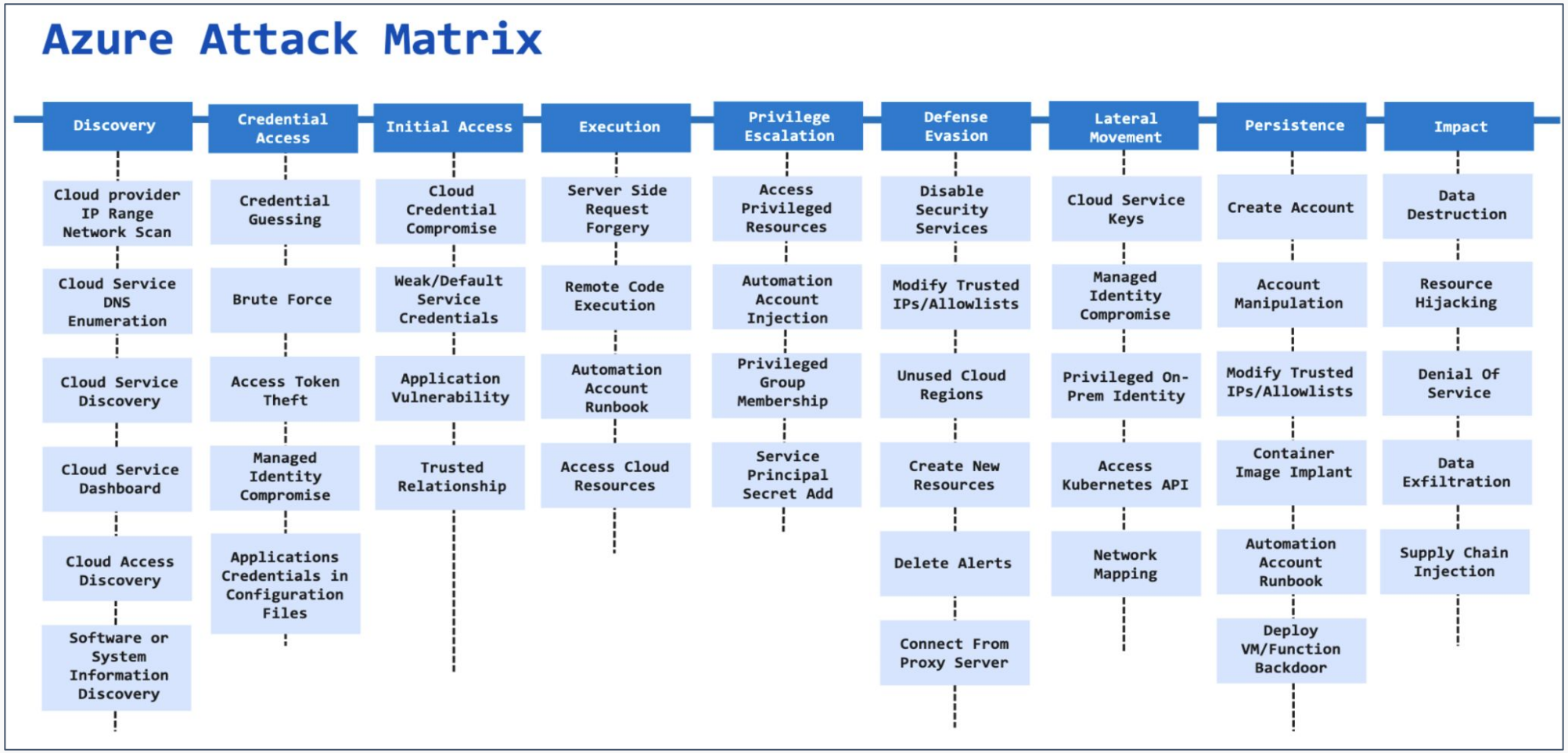
ATT&CK - Azure AD



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

The Microsoft Cloud

They're adding up...



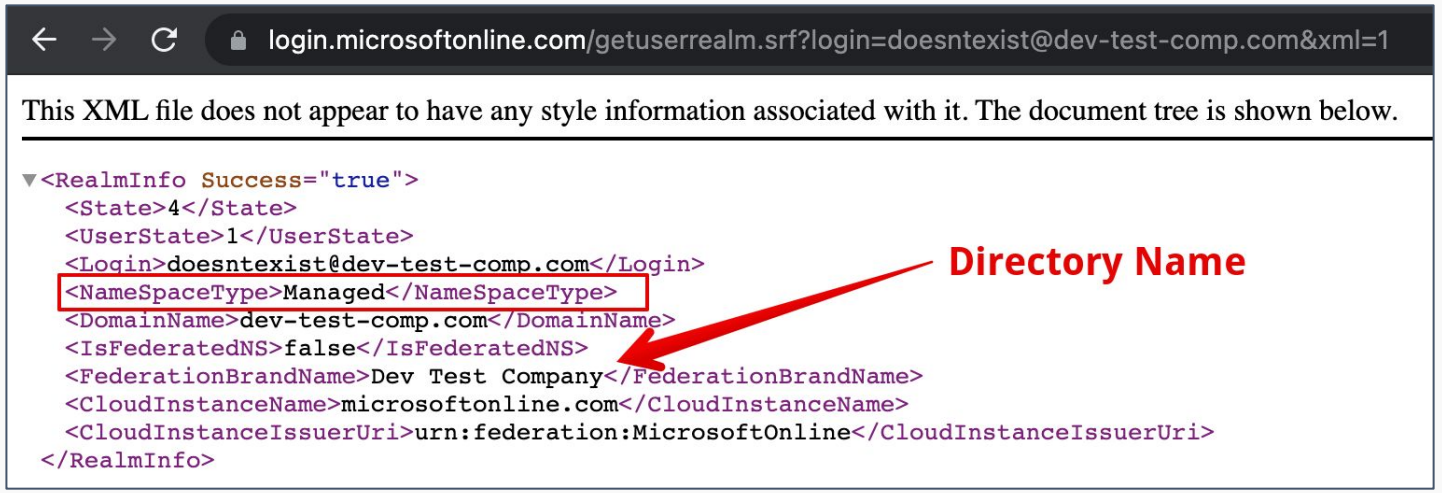
https://github.com/davidokeyode/presentations/blob/master/Azure-Belgium-User-Group.pdf

Reconnaissance

Microsoft Org?

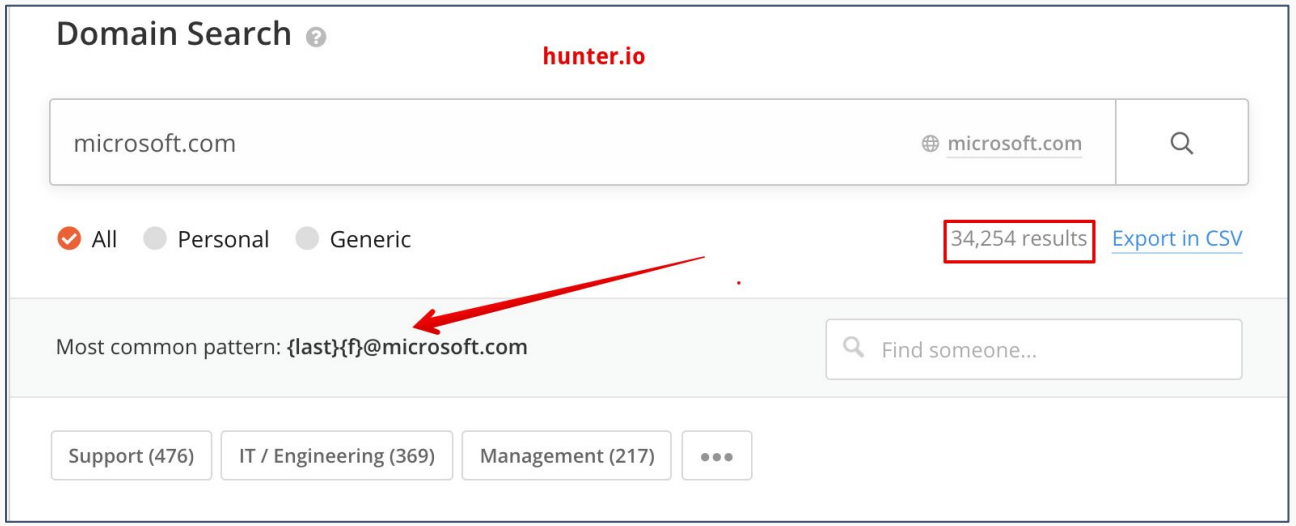
- Check if the company uses **Azure AD**:
  https://login.microsoftonline.com/getuserrealm.srf?login=**username@company.onmicrosoft.com**&xml=1

- **User** Enumeration
  - "Passive" Approach
    - Public Services
    - Breaches
    - Social Media
  - Active Interaction Approach



Reconnaissance

Users: Passive vs Active




```
root@azure-pwn-vps:~/o365enum# python3 o365enum.py -u user.list -p [redacted] -m msol
username,valid
jdoe@dev-test-comp.com,1
asmith@dev-test-comp.com,0
soneal@dev-test-comp.com,0
ljames@dev-test-comp.com,0
mjordan@dev-test-comp.com,0
kdurant@dev-test-comp.com,0
cpaul@dev-test-comp.com,0
drios@dev-test-comp.com,1
achester@dev-test-comp.com,0
dwade@dev-test-comp.com,0
amourning@dev-test-comp.com,0
jkapono@dev-test-comp.com,0
```

Microsoft Online

Reconnaissance

Users: "But what about Azure Smart Lockout"

"Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in"

Example:FIREPROX

Mike Felch - @ustayready

- Rotates IP address with every request
- Configure separate regions
- All HTTP methods supported
- All parameters and URI's are passed through
- Create, delete, list, or update proxies
- Spoof X-Forwarded-For source IP header by requesting with an X-My-X-Forwarded-For header

Reconnaissance

DNS

DOMAIN	SERVICE
azurewebsites.net	App Services
scm.azurewebsites.net	App Services – Management
p.azurewebsites.net	App Services
cloudapp.net	App Services
file.core.windows.net	Storage Accounts-Files
blob.core.windows.net	Storage Accounts-Blobs

DOMAIN	SERVICE
table.core.windows.net	Storage Accounts-Tables
redis.cache.windows.net	Databases-Redis
documents.azure.com	Databases-Cosmos DB
database.windows.net	Databases-MSSQL
vault.azure.net	Key Vaults
onmicrosoft.com	Microsoft Hosted Domain

Karl Fosaaen

Reconnaissance

DNS

- Not just ***.company.com**
- Azure Services has TONS of domains to check against

```
PS [redacted] Invoke-EnumerateAzureSubDomains -base army

Subdomain                                    Service
---------                                    -------
armygithub.azurewebsites.net                 App Services
army-site.azurewebsites.net                  App Services
armydev.azurewebsites.net                    App Services
azurearmy.azurewebsites.net                  App Services
azurearmy.scm.azurewebsites.net              App Services - Management
armygithub.scm.azurewebsites.net             App Services - Management
army-site.scm.azurewebsites.net              App Services - Management
armydev.scm.azurewebsites.net                App Services - Management
army-dev.azureedge.net                       CDN
armydemo.database.windows.net                Databases-MSSQL
armysql.database.windows.net                 Databases-MSSQL
secretarmy.mail.protection.outlook.com       Email
myarmy.mail.protection.outlook.com           Email
armypublic.mail.protection.outlook.com       Email
webarmy.mail.protection.outlook.com          Email
armytest.mail.protection.outlook.com         Email
testarmy.mail.protection.outlook.com         Email
accountingarmy.mail.protection.outlook.com   Email
army.mail.protection.outlook.com             Email
armyit.mail.protection.outlook.com           Email
dataarmy.mail.protection.outlook.com         Email
dataarmy.onmicrosoft.com                     Microsoft Hosted Domain
accountingarmy.onmicrosoft.com               Microsoft Hosted Domain
myarmy.onmicrosoft.com                       Microsoft Hosted Domain
itarmy.onmicrosoft.com                       Microsoft Hosted Domain
testarmy.onmicrosoft.com                     Microsoft Hosted Domain
privatearmy.onmicrosoft.com                  Microsoft Hosted Domain
armypublic.onmicrosoft.com                   Microsoft Hosted Domain
myarmy.sharepoint.com                        SharePoint
accountingarmy.sharepoint.com                SharePoint
testarmy.sharepoint.com                      SharePoint
armydemo.blob.core.windows.net               Storage Accounts - Blobs
army.blob.core.windows.net                   Storage Accounts - Blobs
army.file.core.windows.net                   Storage Accounts - Files
armydemo.file.core.windows.net               Storage Accounts - Files
army.queue.core.windows.net                  Storage Accounts - Queues
armydemo.queue.core.windows.net              Storage Accounts - Queues
armydemo.table.core.windows.net              Storage Accounts - Tables
army.table.core.windows.net                  Storage Accounts - Tables
```

MicroBurst - Karl Fosaaen

Attacks

Gaining Credentials

- **Password Spraying (Many Users -> One Password)**

```
root@azure-pwn-vps:~/MSOLSpray# python3 MSOLSpray.py --userlist user.list --password 'miamiHEAT305!!!'
There are 13 users in total to spray,
Now spraying Microsoft Online.
Current date and time: Mon Jul 19 05:43:11 2021
WARNING! The user asmith@dev-test-comp.com doesn't exist.
WARNING! The user soneal@dev-test-comp.com doesn't exist.
WARNING! The user ljames@dev-test-comp.com doesn't exist.
WARNING! The user mjordan@dev-test-comp.com doesn't exist.
WARNING! The user kdurant@dev-test-comp.com doesn't exist.
WARNING! The user cpaul@dev-test-comp.com doesn't exist.
SUCCESS! drios@dev-test-comp.com : miamiHEAT305!!!
WARNING! The user achester@dev-test-comp.com doesn't exist.
WARNING! The user dwade@dev-test-comp.com doesn't exist.
WARNING! The user amourning@dev-test-comp.com doesn't exist.
WARNING! The user jkapono@dev-test-comp.com doesn't exist.
```

Seasons
Sports
Company Name

Attacks

Gaining Credentials Cont.

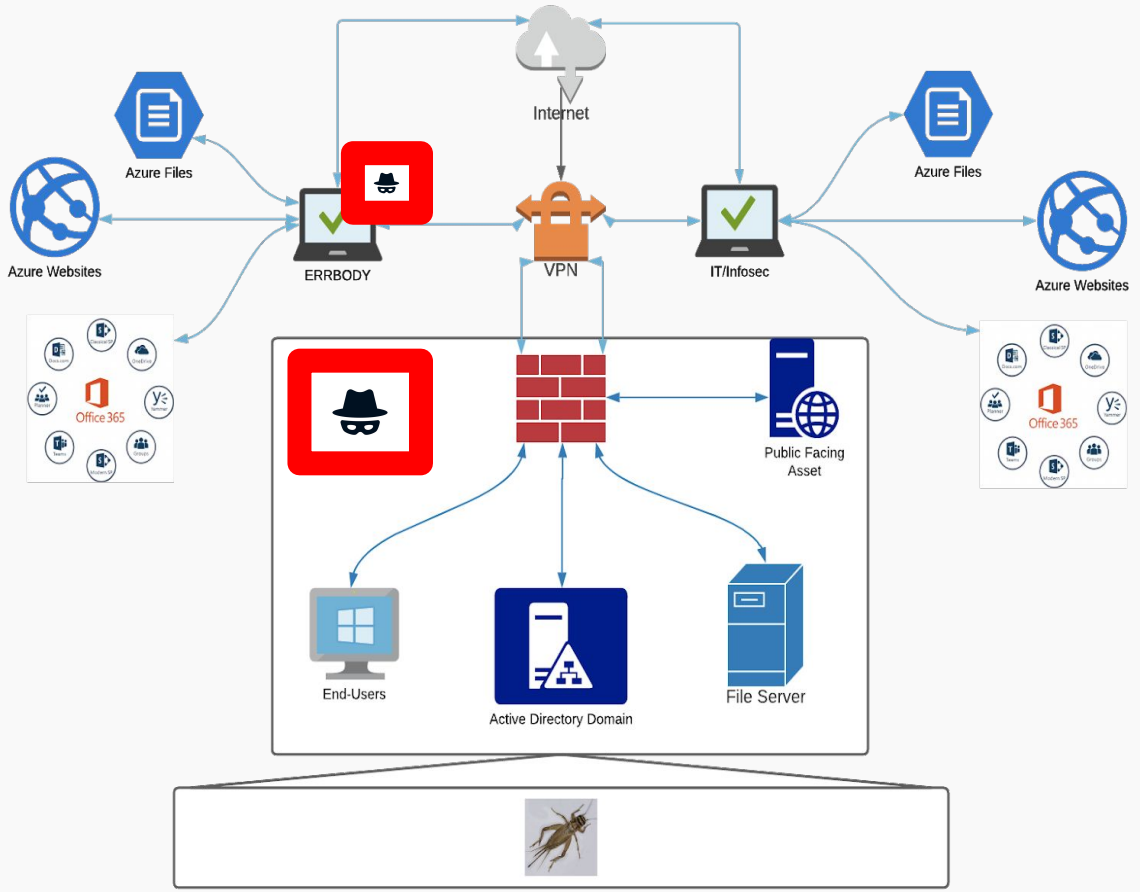
- **Credential Stuffing (One user tied to one password #breaches)**

```
root@azure-pwn-vps:~/OSINT# cat breached-creds.json
      "email": "mjohnson@[redacted]",
      "password": [redacted]
      "email": "bgehres@[redacted]",
      "password": [redacted]
      "email": "aancona@[redacted]",
      "password": [redacted]
      "email": "thawkins@[redacted]",
      "password": [redacted]
      "email": "eramsey@[redacted]",
      "password": "",
      "email": "tgiuliani@[redacted]",
      "password": [redacted]
      "email": "tprice@[redacted]",
      "password": "",
      "email": "dwheeler@[redacted]",
      "password": [redacted]
      "email": "twyatt@[redacted]",
      "password": [redacted]
```

Attacks

Phishing

- **Phish for internal access**
- Phish for valid credentials
- Phish for cloud access



Attacks

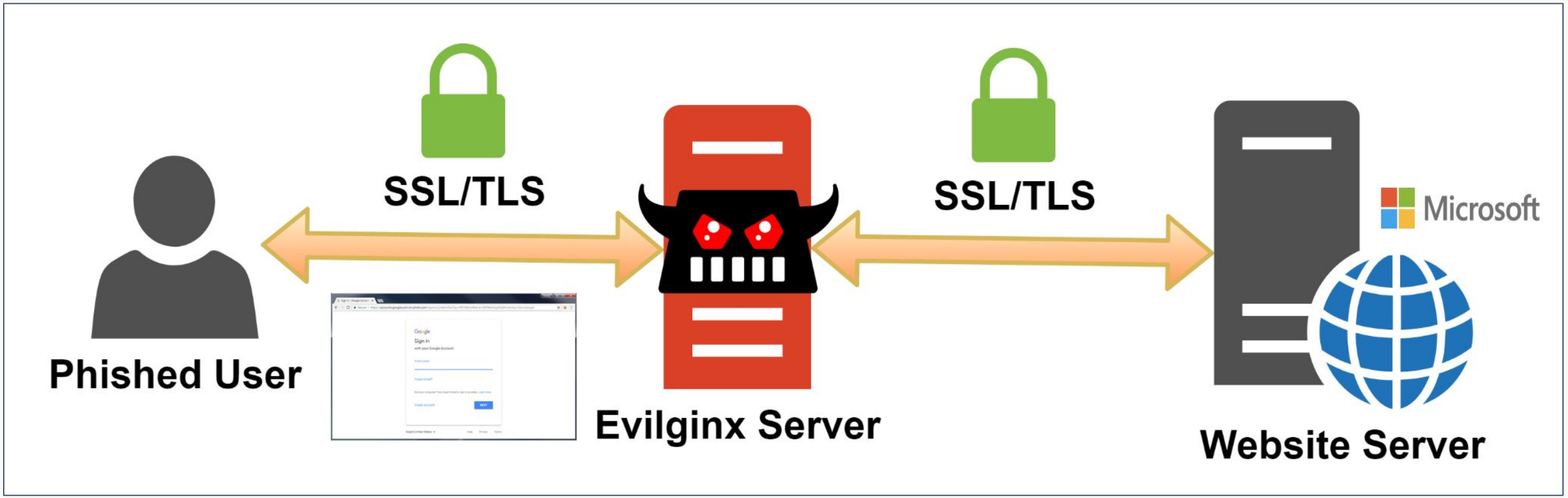
Phishing Cont.

- Phish for internal access
- **Phish for valid credentials**
  - Send enticing emails
  - Place malicious links in forums
  - Malicious links in “chat” platforms
- Phish for cloud access

DEMO is near….

Attacks

Phishing Cont.

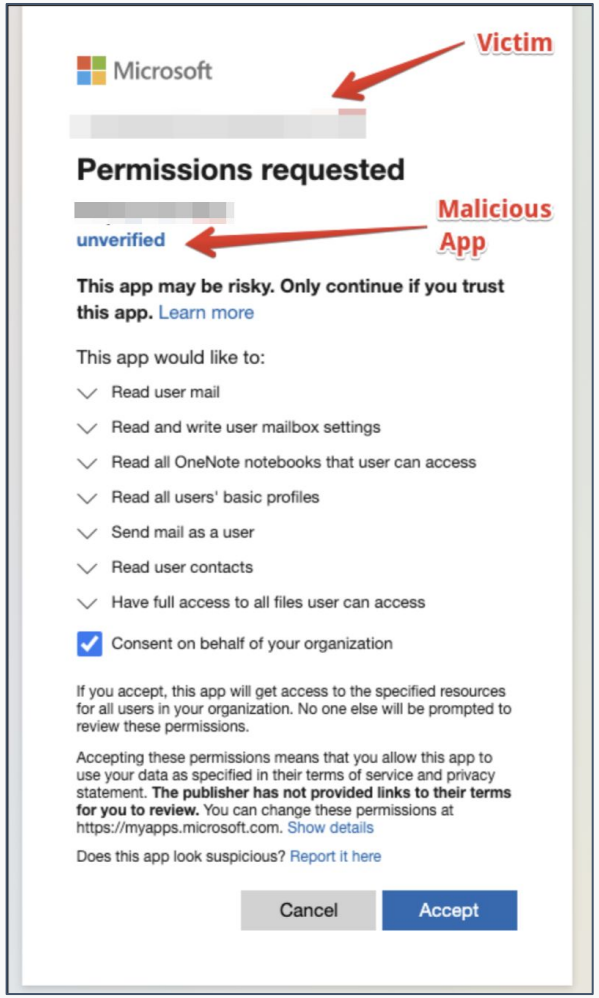


https://github.com/kgretzky/evilginx2

Attacks

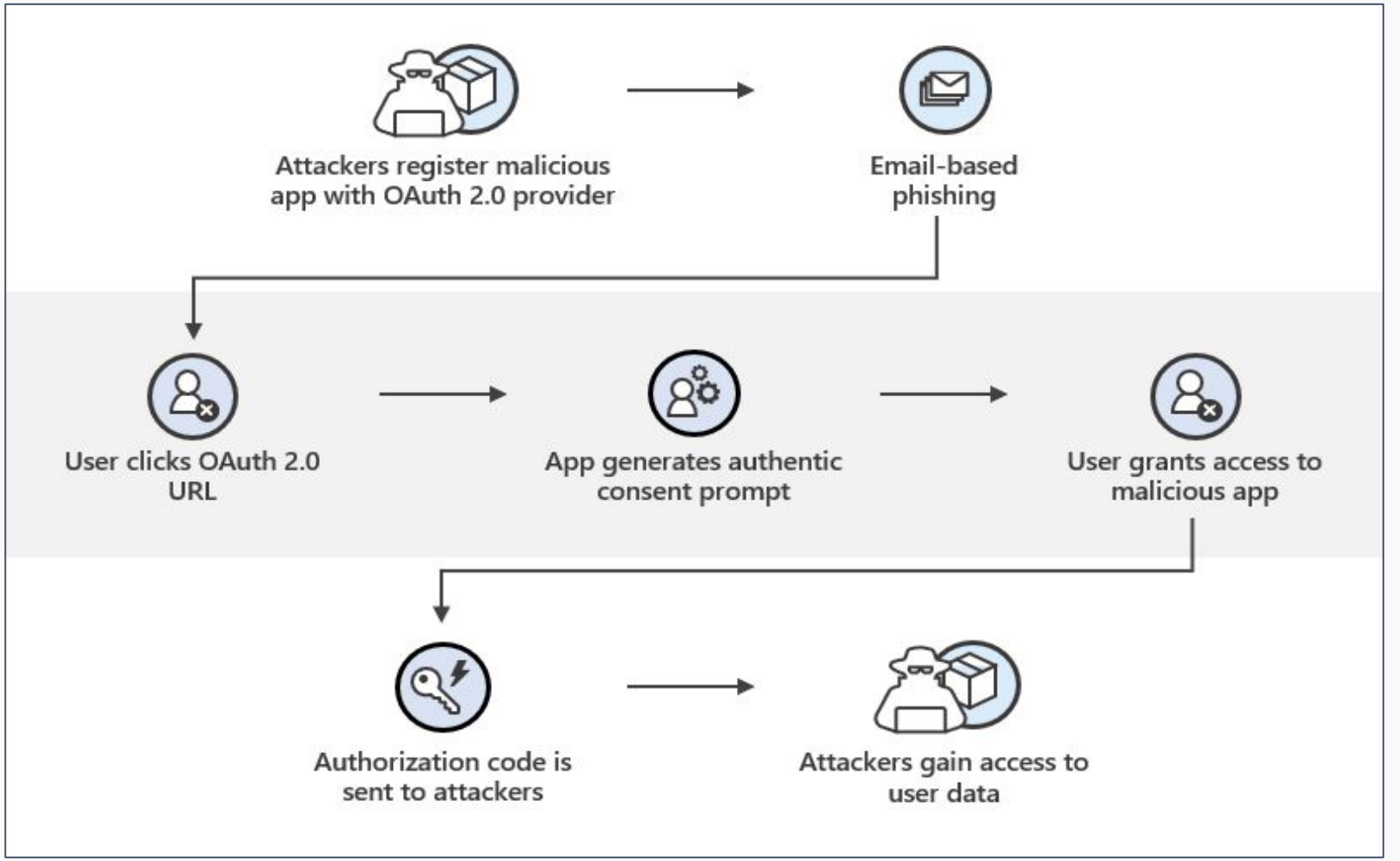
Phishing Cont.

- Phish for internal access
- Phish for valid credentials
  - Send enticing emails
  - Place malicious links in forums
  - Malicious links in “chat” platforms
- **Phish for cloud access**



Attacks

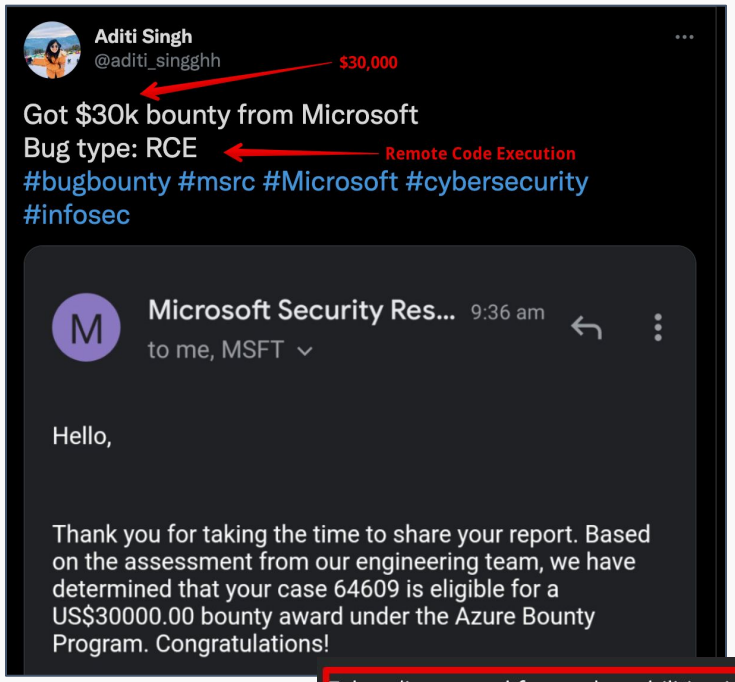
Phishing Cont.



Microsoft 365 Defender Threat Intelligence Team

Attacks

0-Days



UPDATED A remote code execution (RCE) vulnerability in Microsoft Exchange Online remains unresolved after security researchers bypassed two patches for successive exploits.

Rated as critical, the zero-day flaw impacts multiple Software as a Service (SaaS) providers as well as on-premise installations of Exchange Server.

The bug in Exchange Online, part of the Office 365 suite, could be exploited to gain "access to millions of corporate email accounts", said Steven Seeley of the Qihoo 360 Vulcan Team in a blog post published yesterday (January 12).

Office 365's user base is burgeoning along with demand for cloud deployments more generally, reaching 200 million active users by the end of 2019.

Read more of the latest Microsoft security news

Seeley said he was motivated to probe the environment for RCEs given that six other such bugs in Microsoft Exchange Server had emerged in the last two years, most notably CVE-2020-0688 and CVE-2019-1373, the latter prompting him to "focus on the powershell remoting interface".

That the vulnerabilities were all authenticated did not diminish the severity "since a malicious tenant can be created with ease and the necessary permissions applied" – a "fundamental" yet often "overlooked" difference between targeting cloud-based versus on-premise environments, said S

Talos discovered four vulnerabilities in Azure Sphere, two of which could lead to unsigned code execution, and the two others for privilege escalation. The discovery of these vulnerabilities continues our research into Azure Sphere — conducted as part of the Azure Sphere Security Research Challenge — and follows the multiple vulnerabilities we disclosed in July.

In accordance with our coordinated disclosure policy, Cisco Talos worked with Microsoft to ensure that these issues are resolved and that an update is available for affected customers. Microsoft plans to assigns CVEs for these issues on Oct. 13. We will update this blog when these have been assigned.

Security researchers have earned a $3,000 bug bounty after discovering a mechanism to takeover Microsoft Azure DevOps accounts using just one click.

Sean Yeoh, engineering lead at Assetnote, a platform for continuous security monitoring, writes that his team uncovered the problem after first discovering that the subdomain `project-cascade.visualstudio.com` was vulnerable to an Azure Zone DNS takeover.

The security weakness – identified through automated scanning – was found in what is known technically as a "dangling DNS zone", opening the door to exploitation.

"The NS [Name Server] records for `project-cascade.visualstudio.com` were pointing to Azure DNS, however they were no longer registered on Azure DNS," Yeoh explains in a technical write up.

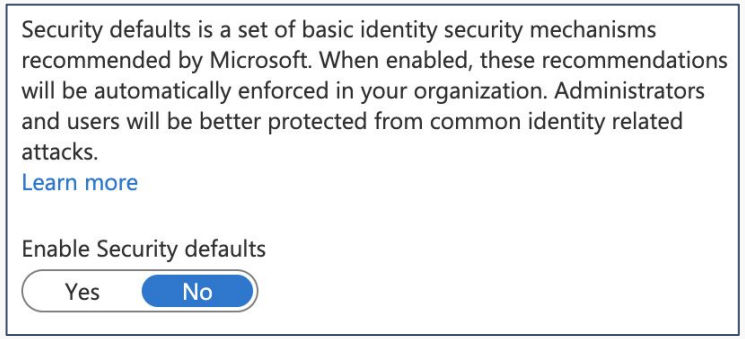
"As the lookups were being refused, we were able to to register the subdomain under an Azure account that we owned. By doing so, we were able to create arbitrary DNS records for the subdomain `project-cascade.visualstudio.com`."

Hacking the authentication flow

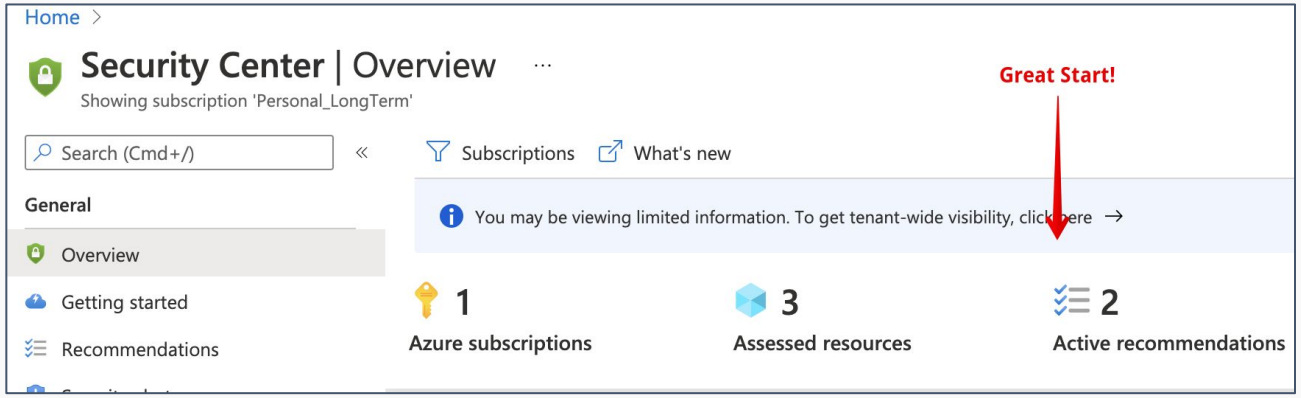
Quick Wins

Harden!

- MFA 1000000000%
- Conditional Access Policies
  - Careful with “allows” #MobileDevices
- Privileged Identity Management (PIM!)

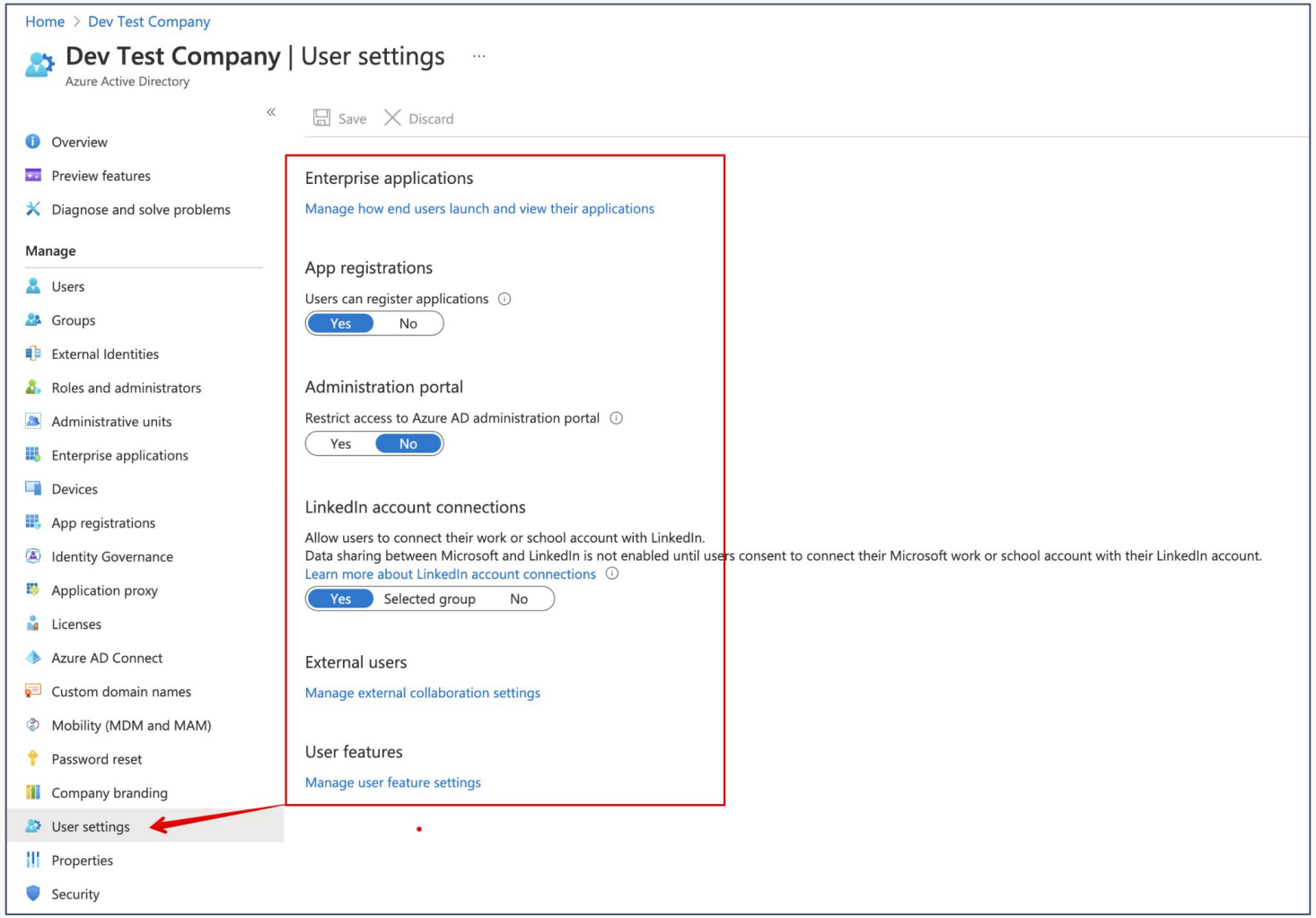


“Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical roles with **PIM**.”



Quick Wins

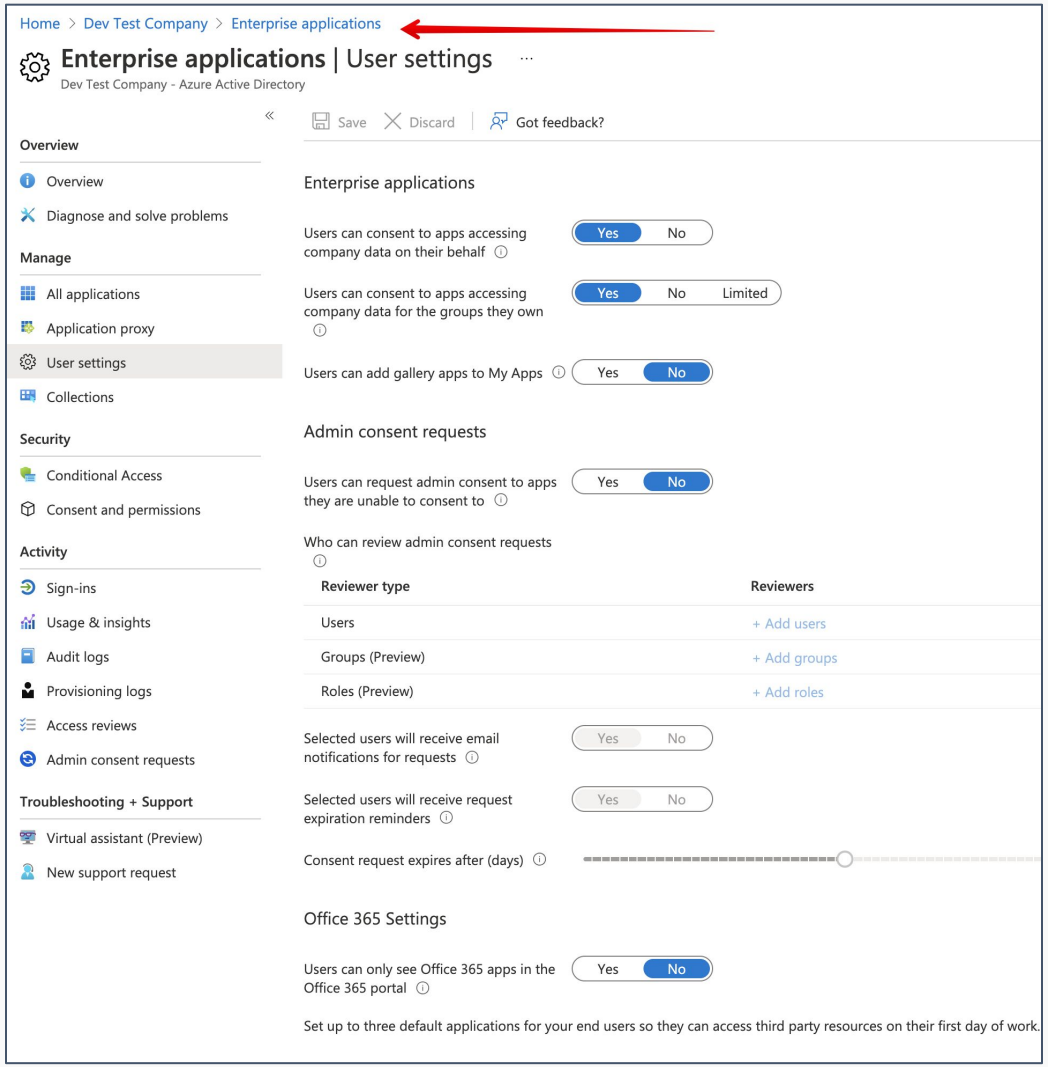
Harden Cont.



Quick Wins

Harden Cont.

- Enterprise Apps!



Quick Wins

Logging!

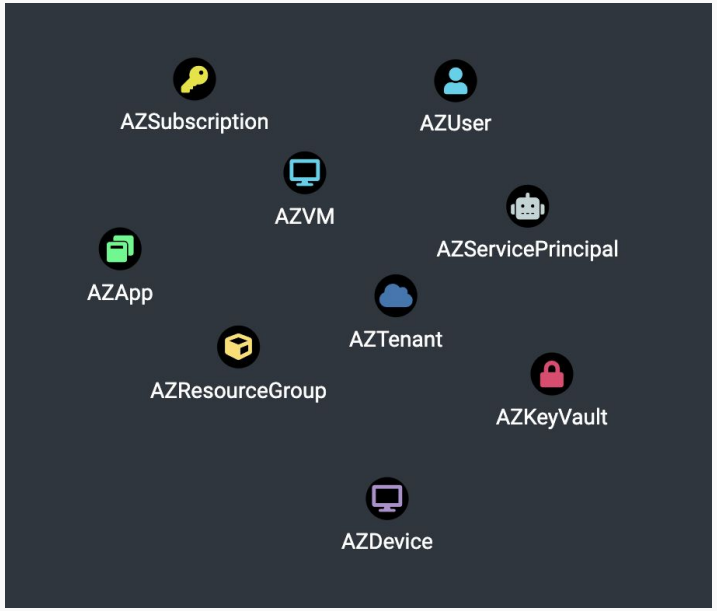
- "Audit logging is turned on by default for Microsoft 365 and Office 365 enterprise organizations"
  - New Orgs
  - Verify!

https://github.com/ANSSI-FR/DFIR-O365RC

- ANALYZE THE LOGS

Quick Wins

Attack Surface



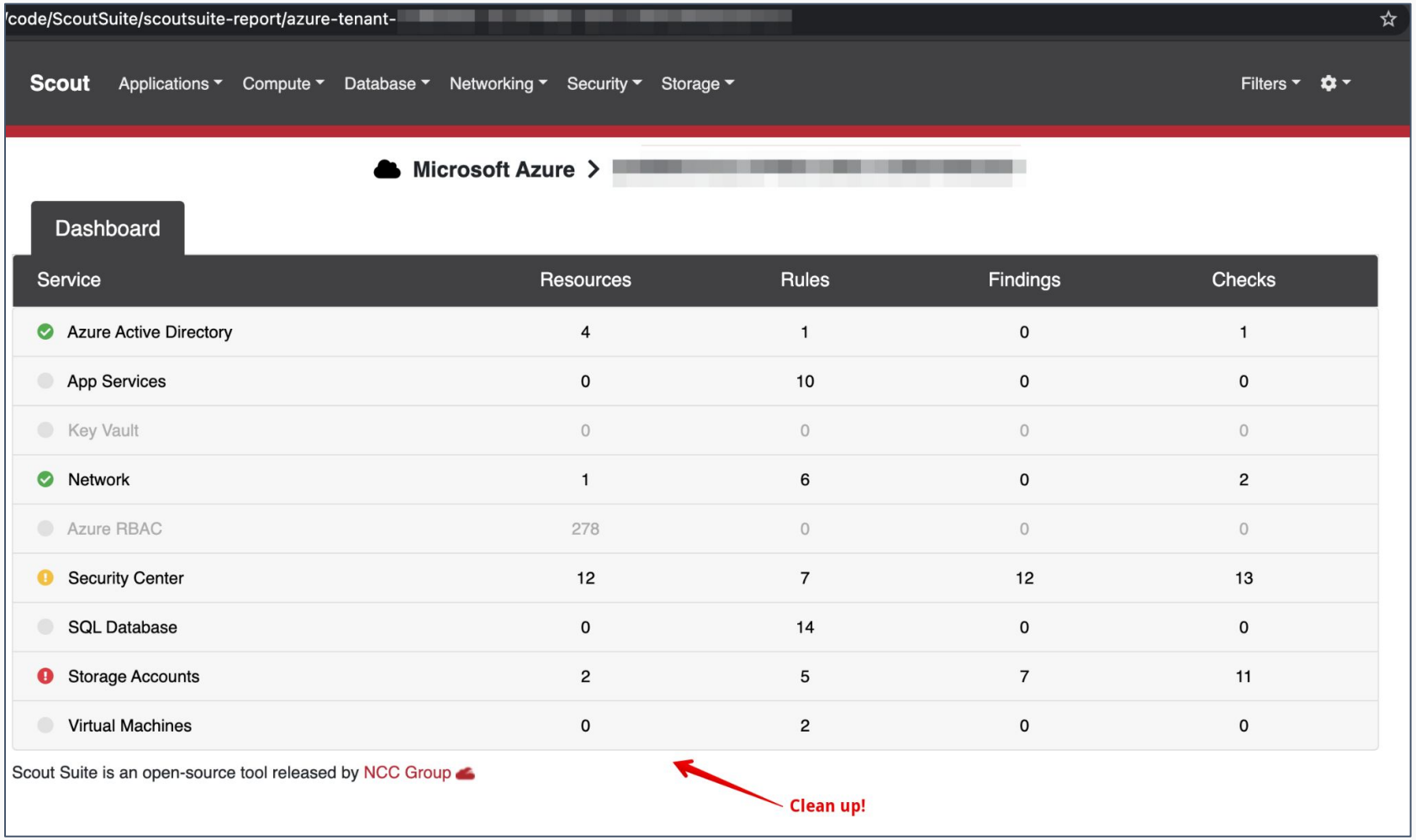
STORMSPOTTER

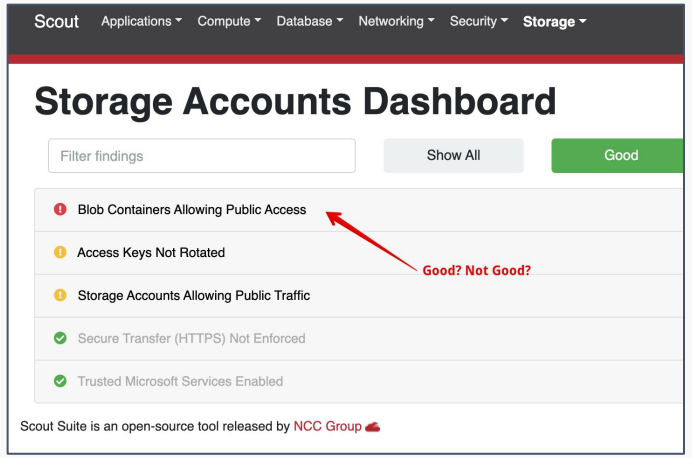
ROADtools

SCOUTSUITE

Quick Wins

Attack Surface Cont.





Thank You!

Questions?

CONTACT

Alberto Rodriguez

All links/references can be found here:
https://github.com/ar0dd/LaListaDeMCA

Twitter: @__ar0d__
LinkedIn: https://linkedin.com/in/albertojoser