WE KNOW WHAT YOU DID (IN AZURE) LAST SUMMER

EXCLUSIVELY IN THE CLOUD VILLAGE

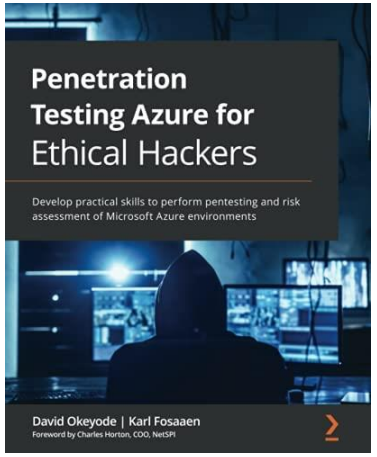
August 9

Karl Fosaaen Thomas Elling

Get-AzContext

Karl Fosaaen

- VP of Research
- Co-Author – Penetration Testing Azure for Ethical Hackers



Thomas Elling

- Director, Azure and Entra ID
- Technical Editor – Penetration Testing Azure for Ethical Hackers

What level of privacy do you expect from your cloud provider?

Should the existence of a resource in the cloud be attributable to an identity?

r/AZURE • 11 hr. ago
hippoheiko

Advice on Preventing Blob Hunting for My Azure Storage Account

Question

I hope this post finds you well. I am currently experiencing an unexpected behaviour with my Azure storage account and I'm seeking some advice on how to resolve it. I would like to prevent exposing the knowledge that my storage account exists. Is this possible?

Despite having completely disabled network settings and preventing public access, I've found that my endpoint - https://nameofstorageaccount.blob.core.windows.net/. - is still accessible. This has raised a concern for me as I want to ensure that the Storage Account is not reachable from the public internet.

Ideally, I would like to make it impossible for anyone to even know the existence of this storage account or its blobs, let alone access them.

If anyone has encountered a similar situation, or has expertise in Azure storage account security, your advice would be greatly appreciated. Specifically, I would like to know what steps I can take to make it not only inaccessible but unknown to others.

The current configuration (StorageV2, Standard performance) is as follows:

1. Public network access: Disabled
2. Secure transfer required: Enabled
3. Allow Blob anonymous access: Disabled
4. Allow storage account key access: Disabled
5. Allow recommend upper limit for SAS expiry interval: Disabled
6. Default to Entra authorisation in the Azure portal: Disabled

Thank you in advance for your time and assistance.

Previous Research

Entra ID User Enumeration

- Nyxgeek – Track the Planet – DEF CON 31
  - https://www.youtube.com/watch?v=4AY5uS3yFjE

Entra ID Tenant Enumeration Tooling

- DrAzureAD (Nestori Syynimaa) – AAD Internals
  - https://aadinternals.com/

AWS Resource to Account Mapping

- Daniel Grzelak – AWSeye
  - https://awseye.com/

MSIdentityTools

- Azure AD team - Resolve-MsIdTenant
  - https://github.com/AzureAD/MSIdentityTools

Previous Research

cloud_enum

- Chris Moberly - Multi-cloud OSINT tool
- https://github.com/initstring/cloud_enum

Jos Lieben

- LinkedIn Post – Domain > Tenant ID resolution via Admin Consent API

Anonymous Azure Resource Enumeration

- NetSPI - Anonymously Enumerating Azure Services (2018)
  - https://www.netspi.com/blog/technical-blog/cloud-pentesting/enumerating-azure-services/

Azure Resource Enumeration and Attribution

What can be enumerated/attributed?

- Tenant ownership of some Azure resource types:
  - Storage Accounts
  - Key Vaults
  - Azure DataBricks
  - App Services Applications
  - Azure Subscription IDs
  - SharePoint
  - Azure Threat Protection Usage
  - Azure Dev Ops Organizations

How can we do this?

- Following the authentication flow
  - Mostly HTTP requests and responses…
- Combine with Graph API functionality or other methods

Why would we do this?

- Attack surface enumeration and confirmation
- Useful for blue and red teams

Azure Tenant and Resource Overview

What is an Azure Tenant?

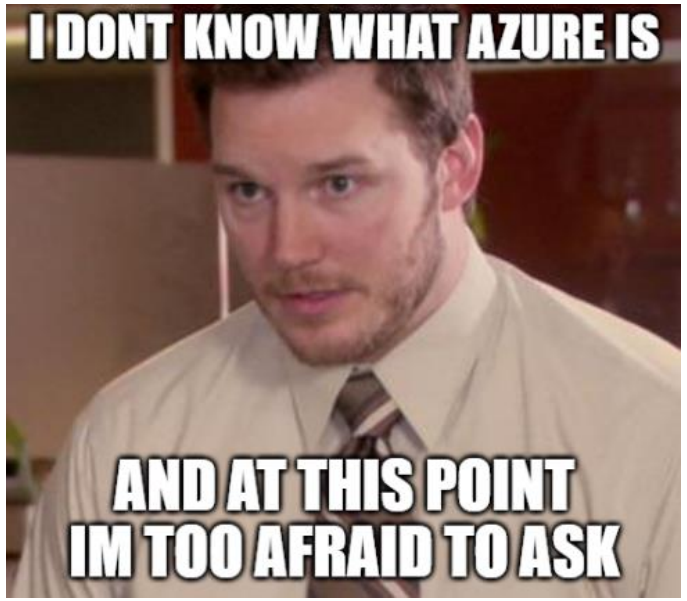
Azure's Identity Directory (Entra ID)

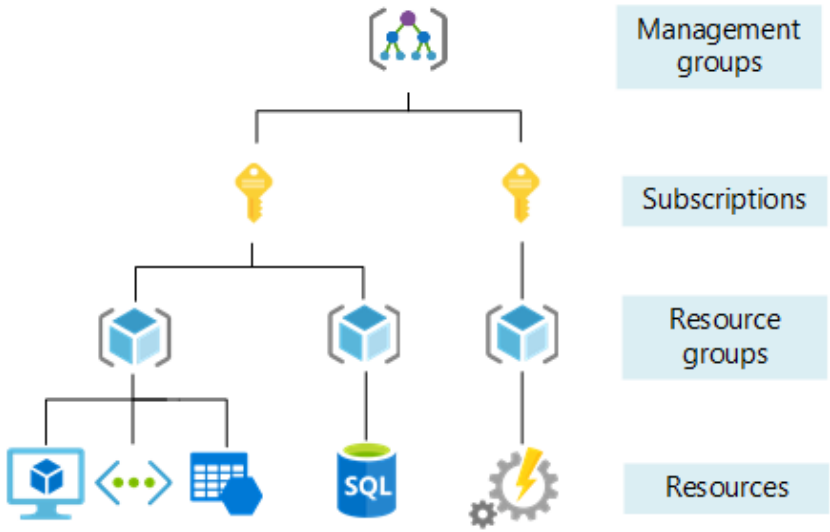
The core of Identity (RBAC / IAM) in Azure

- Security Principals
  - Users / Guest Users
- Service Principals
  - App Registrations
  - Enterprise Apps
- Managed Identities
- RBAC Roles
  - Entra ID and Resource Role Applications

Identifiers:

- Domains
  - microsoft.com
  - microsoft.onmicrosoft.com
- Tenant ID
  - 72f988bf-86f1-41af-91ab-2d7cd011db47

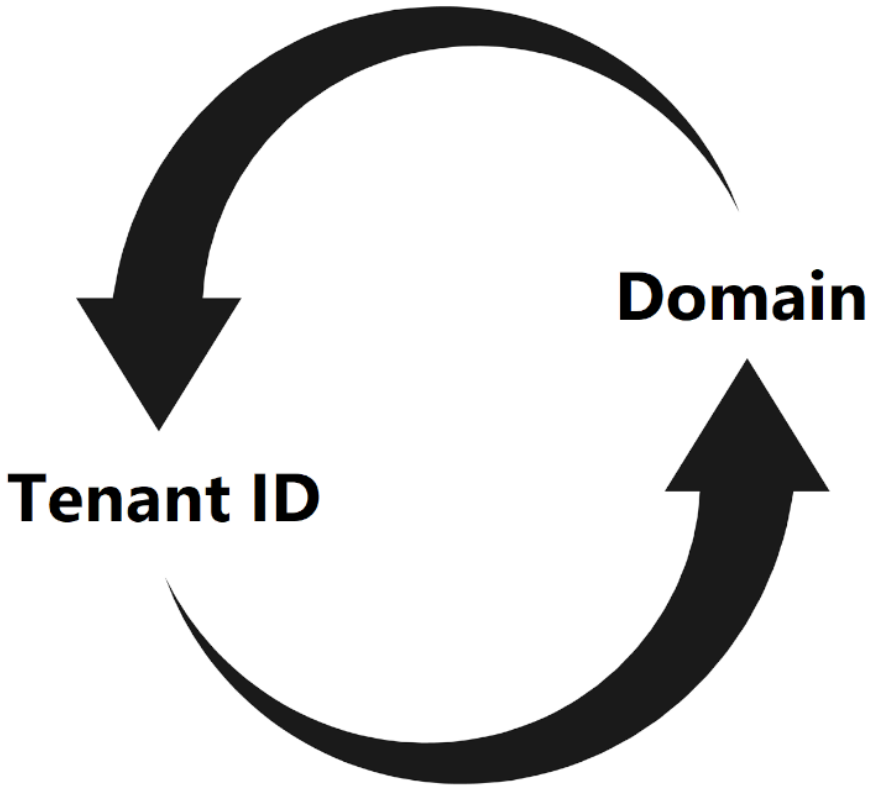




What is an Azure Tenant?

Tenant and ID Enumeration

- Domain to Tenant ID
  - Easiest Method
  - Multiple known ways to resolve
- Tenant ID to Domain
  - More complicated
  - Allows us to see additional linked domains
  - .onmicrosoft.com default domain
- What can we do with a Tenant ID?
  - Use as a key for resource attribution



Graph API - findTenantInformationByTenantId

Tenant ID to Domain

- Graph API has a convenient API call to convert a tenant id to domain
- GET */tenantRelationships/findTenantInformationByTenantId(tenantId='{id}')*
- Used in *Get-AADIntTenantDomain* command from AADInternals by @DrAzureAD (Nestori Syynimaa)
- API returns displayName and defaultDomainName
- Requires authentication and Graph scope *CrossTenantInformation.ReadBasic.All*

https://aadinternals.com/aadinternals/#get-aadinttenantdomain-m

https://learn.microsoft.com/en-us/graph/api/tenantrelationship-findtenantinformationbytenantid?view=graph-rest-1.0&tabs=http

Get-AADIntTenantDomain (M)

Since version 0.7.2
Returns the default domain for the given tenant id.

Example:

```
# Get access token and store to cache
Get-AADIntAccessTokenForMSGraph -SaveToCache

# Get the default domain of the given tenant id
Get-AADIntTenantDomain -TenantId 72f988bf-86f1-41af-91ab-2d7cd011db47
```

Output:

```
microsoft.onmicrosoft.com
```

findTenantInformationByTenantId

GET | v1.0

https://graph.microsoft.com/v1.0/tenantRelationships/findTenantInformationByTenantId(tenantId='977e0660-d4d3-4752-a79d-3ac9c4dbcf19')

Run query

No resource was found matching this query

Request Body | Request Headers | Modify Permissions | Access token

OK - 200 - 588 ms

Response preview | Response headers | Code snippets | Toolkit component | Adaptive cards


```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#microsoft.graph.tenantInformation",
    "tenantId": "977e0660-d4d3-4752-a79d-3ac9c4dbcf19",
    "federationBrandName": null,
    "displayName": "Dark Side Ops",
    "defaultDomainName": "Darksideops.cloud"
}
```

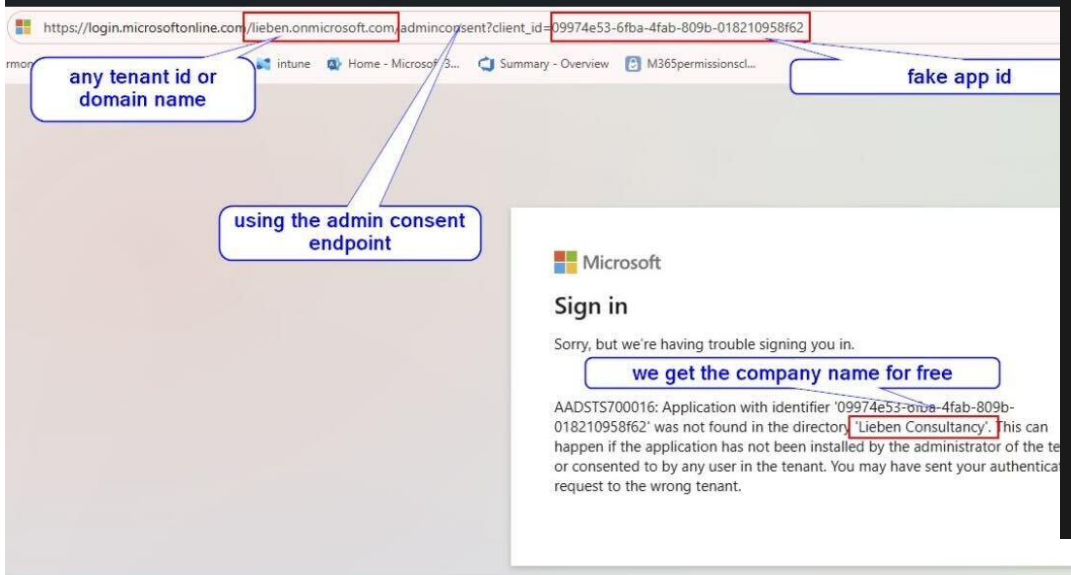
Jos Lieben • 2nd
Azure Cloud Architect at Natuurmonum...
5d •

+ Follow

Is this 'known' already?

domain -> tenant id i knew, but getting the company name for non-branded tenants without tenant access....hadn't read / found that anywhere yet. Dr. Nestori Syynimaa?

#EntraID #Security



47 5 comments • 1 repost

Request the permissions from a directory admin

When you're ready to request permissions from your organization's admin, you can redirect the user to the Microsoft identity platform *admin consent endpoint*.

none Copy

```
https://login.microsoftonline.com/{tenant}/v2.0/adminconsent
        ?client_id=00001111-aaaa-2222-bbbb-3333cccc4444
        &scope=https://graph.microsoft.com/Calendars.Read https://graph.microsoft.com/Mail.Send
        &redirect_uri=http://localhost/myapp/permissions
        &state=12345
```

Expand table

Parameter	Condition	Description
`tenant`	Required	The directory tenant that you want to request permission from. Can be provided in GUID or friendly name format OR generically referenced with `organizations` as seen in the example. Do not use 'common', as personal accounts cannot provide admin consent except in the context of a tenant. To ensure best compatibility with personal accounts that manage tenants, use the tenant ID when possible.
`client_id`	Required	The **Application (client) ID** that the Microsoft Entra admin center – App registrations experience assigned to your app.

Admin Consent API

1

Request (Pretty | Raw | Hex)

```
GET /72f988bf-86f1-41af-91ab-2d7cd011db47/adminconsent?client_id=
e531774f-1eb5-4351-a630-8417802ceca4&sso_reload=true HTTP/2
Host: login.microsoftonline.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Connection: close
```

Response (Pretty | Raw | Hex | Render)


```
"fEnableShowPickerCredObservable":true,"fFetchSessionsSkipDsso":tr
"fIsCiamUserFlowUxNewLogicEnabled":true,"fUseNonMicrosoftDefaultBr
:true,"sCompanyDisplayName":"Microsoft","fRemoveCustomCss":true,
"fFixUiCrashForApiRequestHandler":true,"fShowUpdatedKoreanPrivacyB
"fUsePostCssHotfix":true,"fUseHighContrastDetectionMode":true,
"fFixUserFlowBranding":true,"fIsQrCodePinSupported":true,"fEnableE
:true,"fEnableRefreshCookiesFix":true,"urlAcmaServerPath":
"https://login.microsoftonline.com","sTenantId":
"72f988bf-86f1-41af-91ab-2d7cd011db47","sMkt":"en-US","fIsDesktop"
```


2

Request (Pretty | Raw | Hex)

```
GET /f8cdef31-a31e-4b4a-93e4-5f571e91255a/adminconsent?client_id=
e531774f-1eb5-4351-a630-8417802ceca4&sso_reload=true HTTP/2
Host: login.microsoftonline.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
```

Response (Pretty | Raw | Hex | Render)


```
:true,"fShowAccessPassPeek":true,"fUpdateSessionPollingLogic":tru
"fEnableShowPickerCredObservable":true,"fFetchSessionsSkipDsso":t
"fIsCiamUserFlowUxNewLogicEnabled":true,"fUseNonMicrosoftDefaultB
:true,"sCompanyDisplayName":"Microsoft Services","fRemoveCustomCs
"fFixUiCrashForApiRequestHandler":true,"fShowUpdatedKoreanPrivacy
"fUsePostCssHotfix":true,"fUseHighContrastDetectionMode":true,
"fFixUserFlowBranding":true,"fIsQrCodePinSupported":true,"fEnable
:true,"fEnableRefreshCookiesFix":true,"urlAcmaServerPath":
"https://login.microsoftonline.com","sTenantId":
```


3

Request (Pretty | Raw | Hex)

```
GET /977e0660-d4d3-4752-a79d-3ac9c4dbcf19/adminconsent?client_id=
e531774f-1eb5-4351-a630-8417802ceca4&sso_reload=true HTTP/2
Host: login.microsoftonline.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
```

Response (Pretty | Raw | Hex | Render)


```
:true,"fShowAccessPassPeek":true,"fUpdateSessionPollingLogic":tru
"fEnableShowPickerCredObservable":true,"fFetchSessionsSkipDsso":t
"fIsCiamUserFlowUxNewLogicEnabled":true,"fUseNonMicrosoftDefaultB
:true,"sCompanyDisplayName":"Dark Side Ops","fRemoveCustomCss":tr
"fFixUiCrashForApiRequestHandler":true,"fShowUpdatedKoreanPrivacy
"fUsePostCssHotfix":true,"fUseHighContrastDetectionMode":true,
"fFixUserFlowBranding":true,"fIsQrCodePinSupported":true,"fEnable
:true,"fEnableRefreshCookiesFix":true,"urlAcmaServerPath":
```


https://learn.microsoft.com/en-us/entra/identity-platform/v2-admin-consent

Enumerating Azure Resources

Enumerating Azure Resources

How subdomains work for Azure

- Creation of the $StorageName Storage Account
  - $StorageName.blob.core.windows.net
    - Blob Service
  - $StorageName.file.core.windows.net
    - File Service
  - $StorageName.table.core.windows.net
    - Table Service
  - $StorageName.queue.core.windows.net
    - Queue Service
  - $StorageName.z4.web.core.windows.net
    - Static Web Hosting

Example Domains

- .azurewebsites.net
- .scm.azurewebsites.net
- .(blob/file/table/queue).core.windows.net
- .azuredatabricks.net
- .vault.azure.net
- .sharepoint.com
- .cloudapp.net
- .documents.azure.com
- .database.windows.net
- .azureedge.net
- .search.windows.net
- .azure-api.net

Enumerating Azure Resources

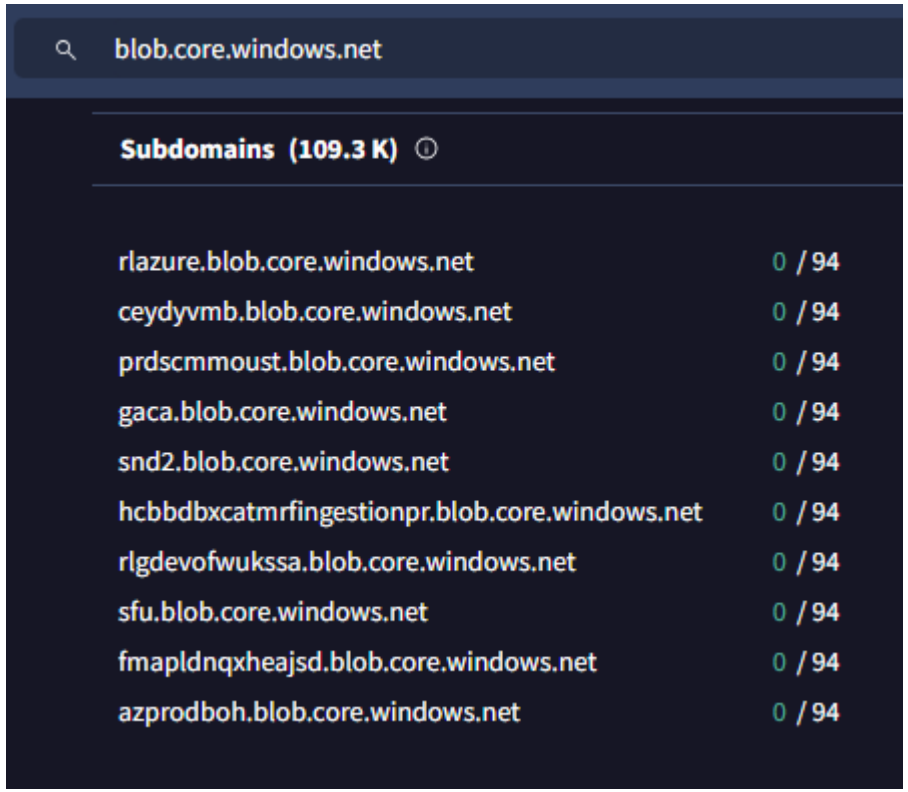
Keyword/Subdomain Enumeration

Sources – In order of usefulness

- Virus Total – Relations tab
- GitHub
- Grayhat warfare – Storage Accounts
- Certificate Transparency - crt.sh
  - Only works for specific services
- Common Crawl Dataset
- Shodan

Available Tooling

- BBot



Repeat for all subdomains

- Resource names are often shared across services
- One may be listed in VT under one subdomain, but not under others

Enumerating Azure Resources

General Process

- Enumerate/Generate list of potential subdomain keywords
- DNS lookup of hostnames:
  - notpayloads.azurewebsites.net
  - defnotpayloads.blob.core.windows.net
- Log active records, discard failed lookups
- Identify the tenant hosting the resource

A name is not proof of ownership:

AWS does not actually own aws.blob.core.windows.net

So how do we prove ownership?

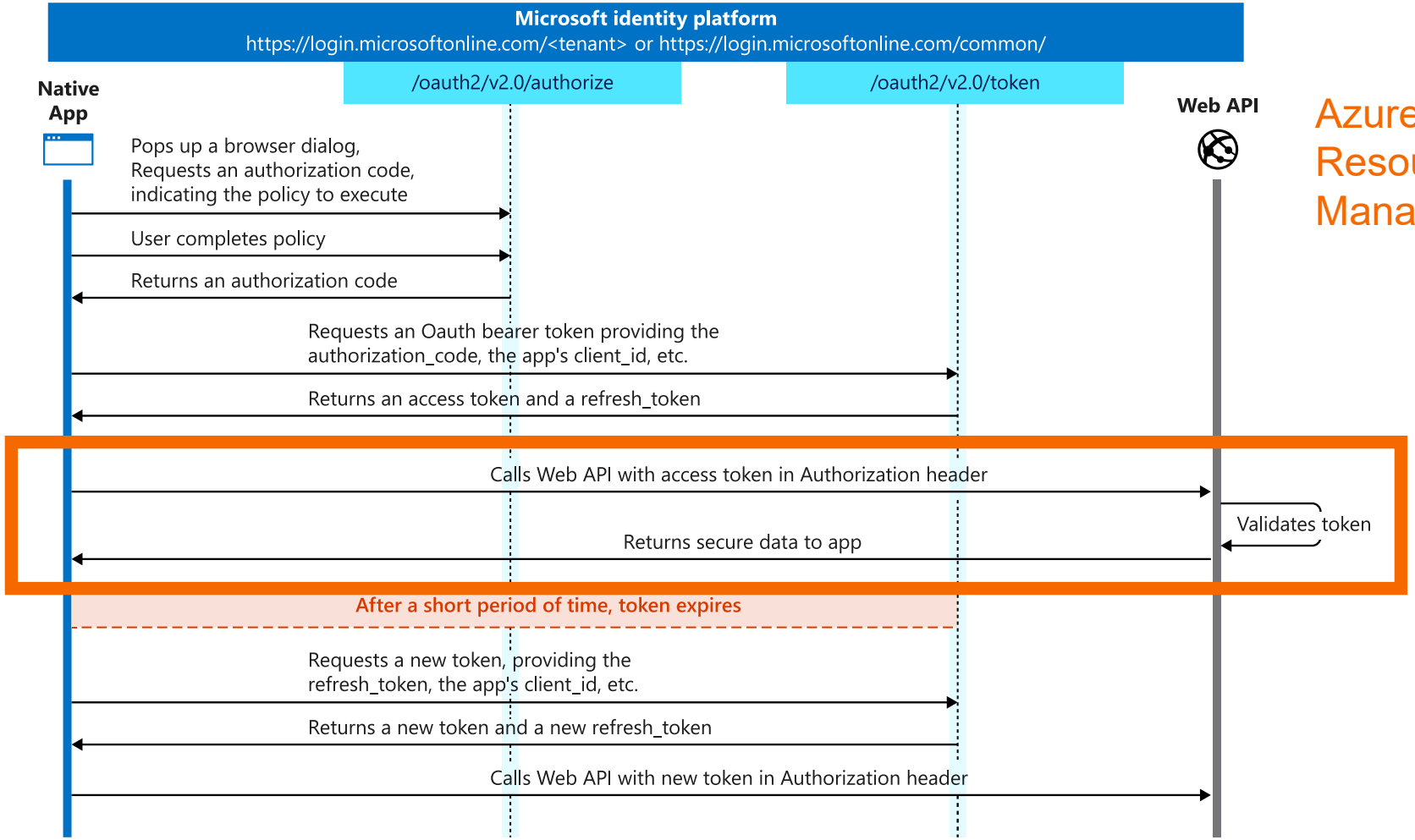
Tenant Resource Attribution

Attribution Overview

Browser authenticating to Azure Portal

Azure Resource Manager API

How does the server respond to specially crafted requests during the “Validates token” process?



https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-auth-code-flow

Attribution Overview

Microsoft Identity Platform and Azure

- Azure Resource Manager and other Azure resources use the Microsoft Identity Platform
- ARM APIs and Azure resources will require an access token acquired from Entra ID
- Azure ARM API endpoints will return a WWW-Authenticate header in the response with a bearer challenge depending on headers in the request, authorization etc.
- Challenge happens when no access token is submitted OR an invalid token (token with zero access to the resource) is submitted
- Challenge response will usually contain the expected Bearer authorization URI for the target resource
    - ***<u>The authorization URI will usually contain the Tenant ID of the corresponding resource</u>***
- Bearer challenges are documented and expected behavior
    - https://learn.microsoft.com/en-us/rest/api/storageservices/authorize-with-azure-active-directory#sample-response-to-bearer-challenge

```
WWW-Authenticate:

Bearer authorization_uri=https://login.microsoftonline.com/<tenant_id>/oauth2/authorize
resource_id=https://storage.azure.com
```

Attribution Overview

1. Specific Azure Resource
2. WWW-Authenticate Bearer Challenge
3. Entra Tenant ID
4. Get-AADIntTenantDomain
   Get-AADIntOpenIDConfiguration
   Get-AADIntLoginInformation

   Admin Consent API

- Entra Tenant ID
- Tenant Friendly Name
- OpenID Configuration Info
- Domain Name
- Federation Brand Name
- And more…

A graph of resources and associated Entra tenants can be created to map relationships

Attribution – Azure Provider String

Resource Description

- Any Resource path (see below) that contains the subscription ID can expose the parent tenant

Resource Domain

- https://management.azure.com/subscriptions/*

Attribution Method

- Responds with “WWW-Authenticate” Header
- Contains Tenant ID

Potential Exposures

- Useful for attributing resources from documentation, GitHub, etc. to the tenant they are hosted in

Attribution – Azure Provider String

```
try {
        Invoke-RestMethod -Uri "https://management.azure.com/subscriptions/155c4768-b71c-4e4b-a990-97407f43edda?api-version=2022-12-01"
}
catch {$_.Exception.Response.Headers.GetValues("WWW-Authenticate")}


Bearer authorization_uri="https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47", error="invalid_token", error_description="The authentication failed because of missing 'Authorization' header."
```

Attribution – Storage Accounts

Resource Description

- A service for hosting public and private files

Resource Domain

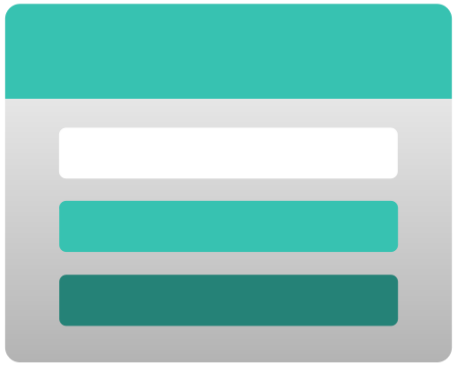
- *.blob.core.windows.net
  - File, Queue, Table also work

Attribution Method

- HTTP Request with “x-ms-version” Header
  - Responds with “WWW-Authenticate” Header (Contains Tenant ID)

Potential Exposures

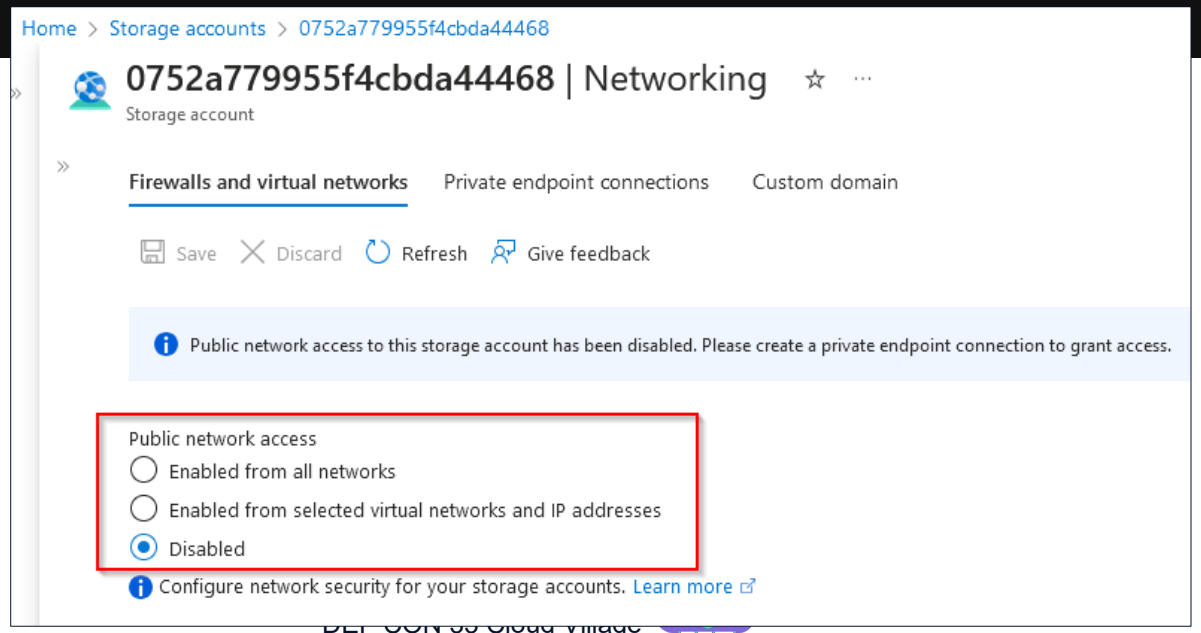
- Publicly available files could be enumerated
  - Containers would need to be enumerated
- Public HTML hosting attribution
  - Static HTML can be hosted at the root

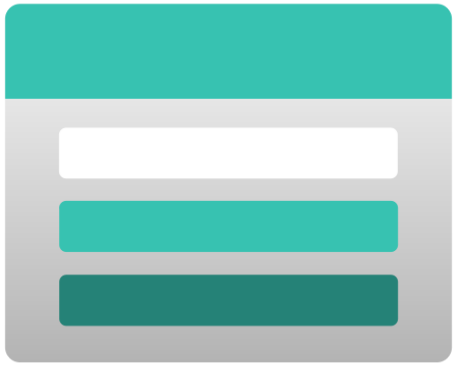


Attribution – Storage Accounts

```
try {
   Invoke-RestMethod -Uri "https://0752a779955f4cbda44468.blob.core.windows.net/?comp=blobs" -Method Get -Headers @{"x-ms-version"="2019-12-12"}
}
catch {$_.Exception.Response.Headers}

Key Value
--- -----
x-ms-error-code {NoAuthenticationInformation}
x-ms-version {2019-12-12}
WWW-Authenticate {Bearer authorization_uri=https://login.microsoftonline.com/977e0660-d4d3-4752-a79d-3ac9c4dbcf19/oauth2/authorize
resource_id=https://storage.azure.com}
Date {Sun, 19 Jan 2025 16:02:50 GMT}
```





Attribution – Key Vaults

Resource Description

- A service that provides secret storage

Resource Domain

- *.vault.azure.net

Attribution Method

- Responds with “WWW-Authenticate” Header
- Contains Tenant ID

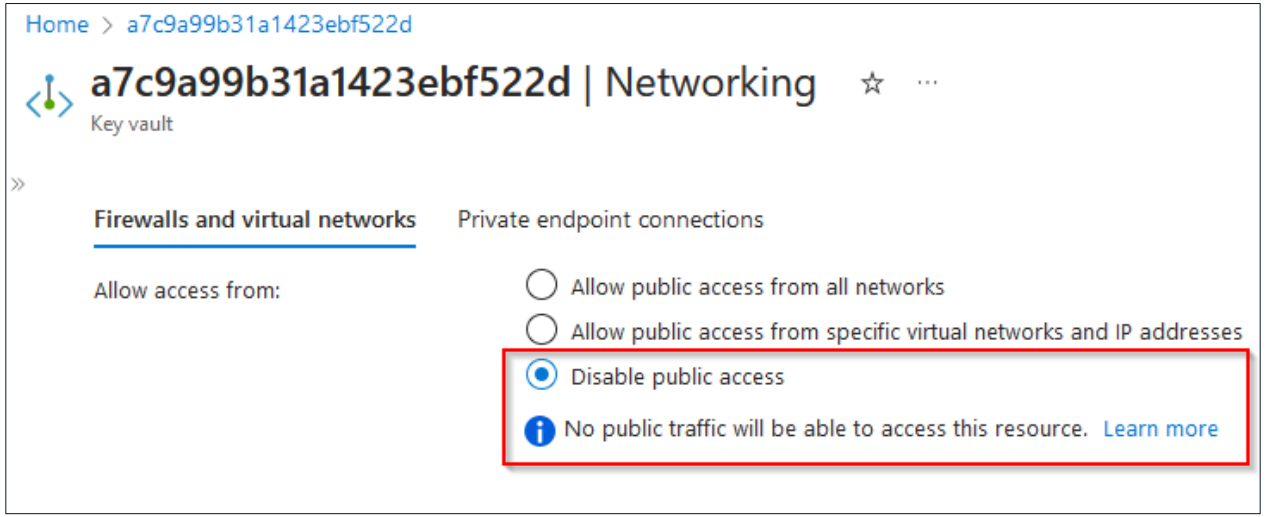
Potential Exposures

- Resource name exposure
- Would require access to a principal with access rights on the vault

Attribution – Key Vaults

```
try {
   Invoke-RestMethod -Uri "https://a7c9a99b31a1423ebf522d.vault.azure.net/keys" -Method Head
}
catch {$_.Exception.Response.Headers}

Key Value
--- -----
x-ms-keyvault-region {eastus}
WWW-Authenticate {Bearer authorization="https://login.microsoftonline.com/977e0660-d4d3-4752-a79d-3ac9c4dbcf19",
resource="https://vault.azure.net"}
Date {Sun, 19 Jan 2025 16:17:07 GMT}
```



Attribution – App Services

Resource Description

- Serverless application hosting
- Includes Function Apps

Resource Domain

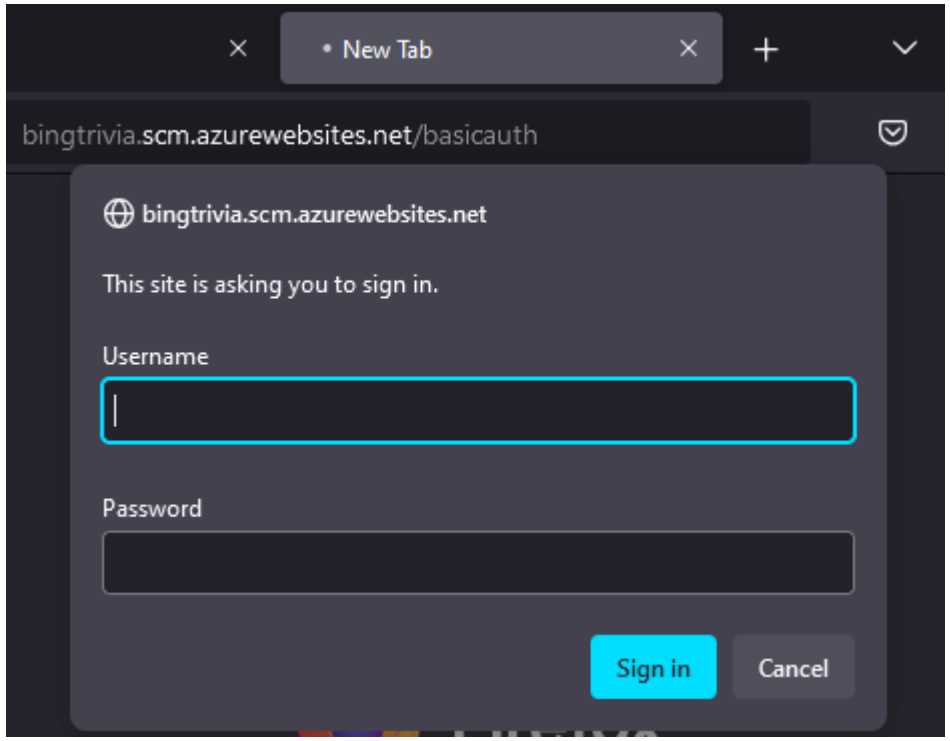
- *.azurewebsites.net – Integrated Entra ID Authentication
  - See - bingtrivia.azurewebsites.net
- *.scm.azurewebsites.net and *.scm.*.azurewebsites.net

Attribution Method

- HTTP Request to the Kudu (.scm.) interface
- Responds with a redirect - Location contains Tenant ID

Potential Exposures

- Application may not be intended for public use



Attribution – App Services (Previous)

```
try {
                Invoke-RestMethod -Uri "https://ttesta456cf3d.scm.azurewebsites.net" -Method Head -TimeoutSec 3 -
MaximumRedirection 0
}
catch {$_.Exception.Response.Headers}


Key Value
--- -----
Date {Sun, 24 Mar 2024 17:48:32 GMT}
Location {https://login.microsoftonline.com/977e0660-d4d3-4752-a79d-
3ac9c4dbcf19/oauth2/authorize?response_type=code&redirect_uri=https%3A%2F%2Fblu.sso.azurewebsites.windows.net%2F&client
_id…
```

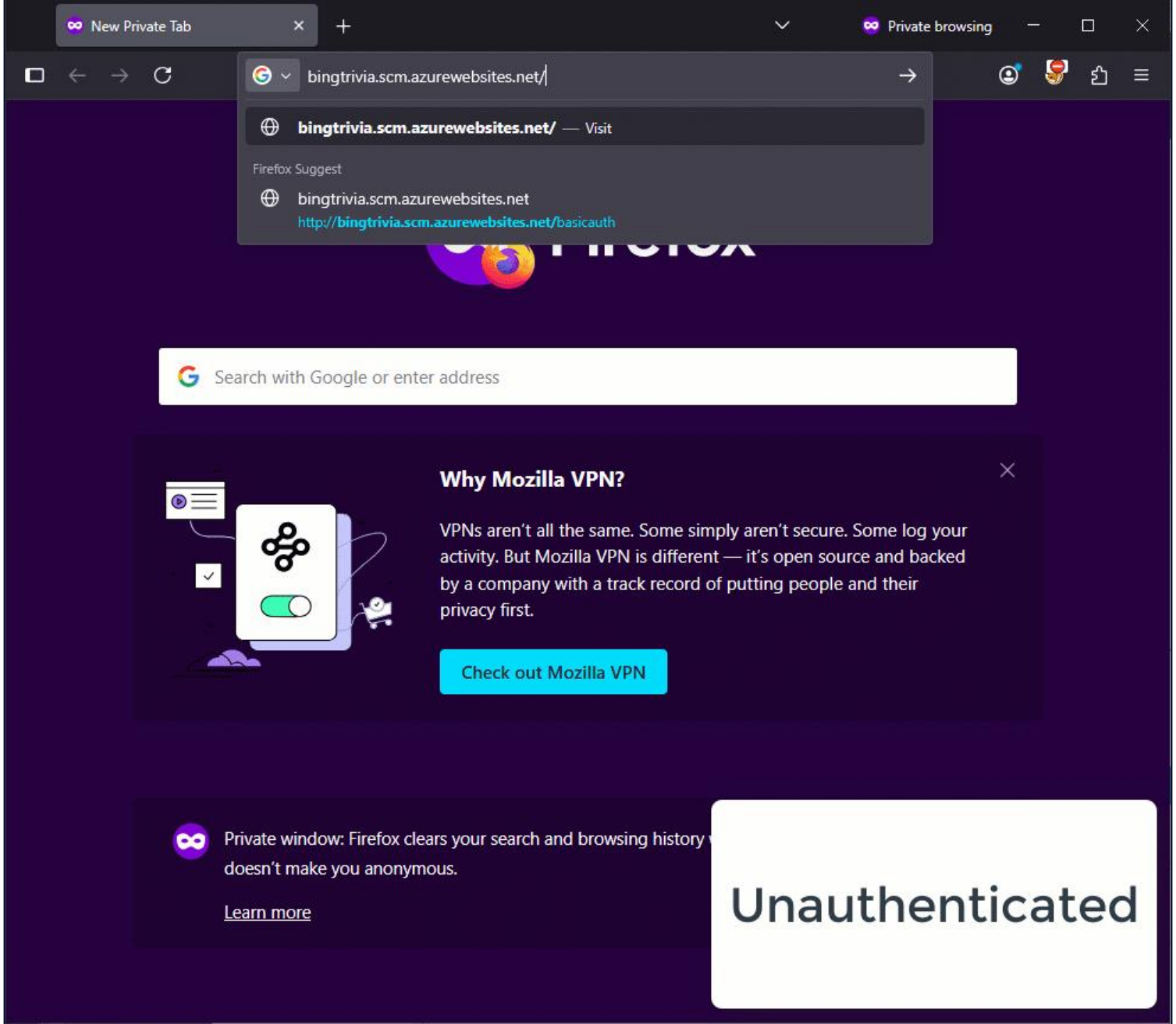
Attribution – App Services (Current)

```
$uri = "https://bingtrivia.scm.azurewebsites.net"

(Invoke-WebRequest -Uri $uri -MaximumRedirection 0 -ErrorAction SilentlyContinue -Method Head -
UseBasicParsing).Headers.Location


https://login.microsoftonline.com/common/oauth2/authorize?response_type=code&redirect_uri=https%3A%2F%2Fhk1.sso.azurewe
bsites.windows.net%2F&client_id=abfa0a7c-a6b6-4736-8310-5855508787cd&[Truncated]
```

*Can be “fixed” by providing a valid ESTSAUTHPERSISTENT cookie


New Private Tab
Private browsing
bingtrivia.scm.azurewebsites.net/
bingtrivia.scm.azurewebsites.net/ — Visit
Firefox Suggest
bingtrivia.scm.azurewebsites.net
http://bingtrivia.scm.azurewebsites.net/basicauth
Search with Google or enter address
Why Mozilla VPN?
VPNs aren't all the same. Some simply aren't secure. Some log your activity. But Mozilla VPN is different — it's open source and backed by a company with a track record of putting people and their privacy first.
Check out Mozilla VPN
Private window: Firefox clears your search and browsing history
doesn't make you anonymous.
Learn more
Unauthenticated

Attribution – Additional Services

SharePoint

- *.sharepoint.com or *-my.sharepoint.com

Azure Databricks

- *. azuredatabricks.net

Azure Machine Learning

- $Compute_Name.$REGION.instances.azureml.ms
  - API endpoint (/api/metrics/v1) redirects to the common tenant

Azure DevOps

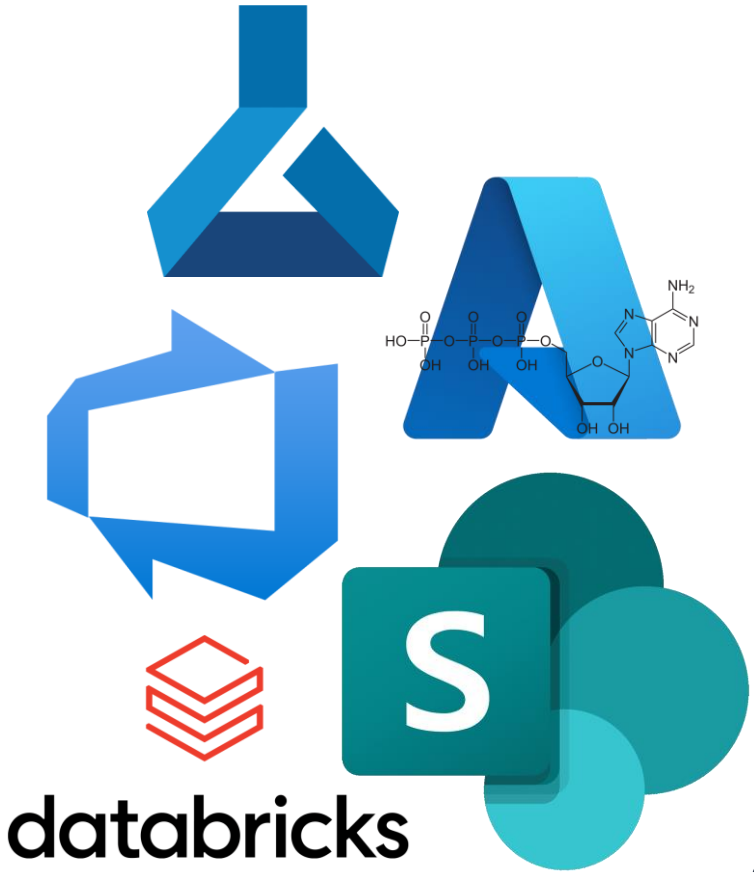
- https://dev.azure.com/$ADO_OrgName

Azure Threat Protection (ATP)

- $DOMAIN.atp.azure.com
  - netspi.atp.azure.com
- $DOMAINsensorapi.atp.azure.com
  - netspisensorapi.atp.azure.com
- Invoke-AADIntReconAsOutsider from AADInternals finds this

SSO Applications

- 3rd party applications with Entra ID integration



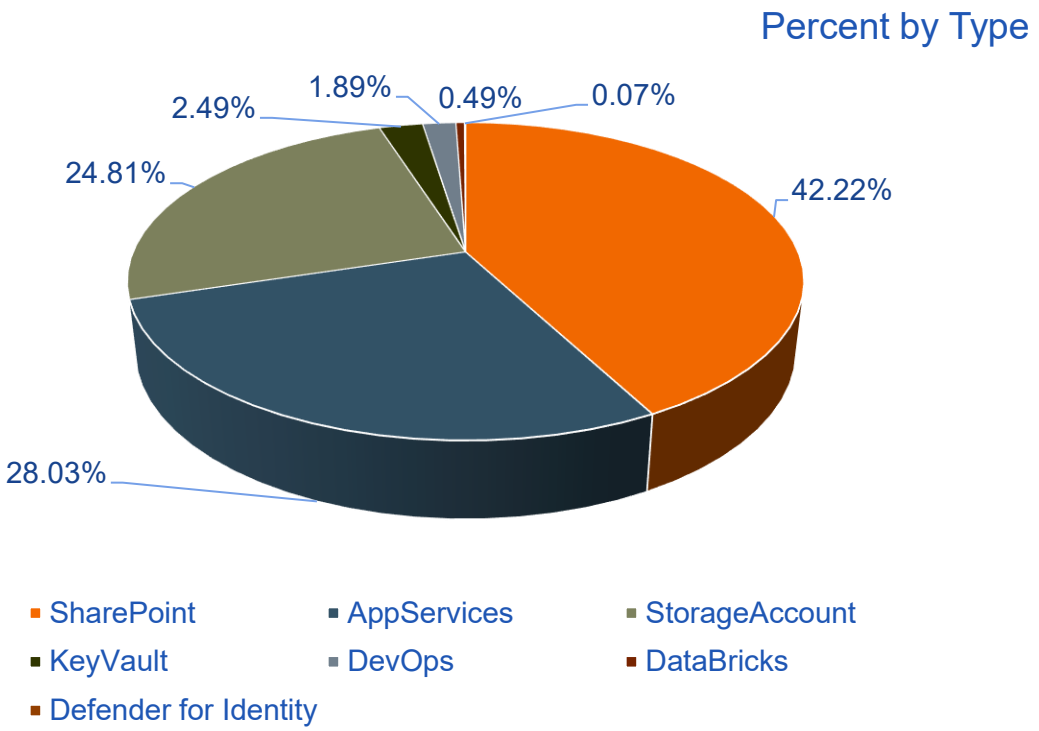
Attribution – Summary

Resource Type	Subdomains	Enumeration Technique	Attribution Technique
Azure Provider String	management.azure.com	Resource String Disclosure	“WWW-Authenticate” Header
Key Vaults	vault.azure.net	Subdomain Enumeration	“WWW-Authenticate” Header
Storage Accounts	blob.core.windows.net	Subdomain Enumeration	“WWW-Authenticate” Header
SharePoint	sharepoint.com	Subdomain Enumeration	“Report-To” Header
App Services	azurewebsites.net scm.azurewebsites.net	Subdomain Enumeration	“Location” Header in Redirect
Azure DataBricks	azuredatabricks.net	Subdomain Enumeration	“Location” Header in Redirect
Azure Machine Learning	instances.azureml.ms	Subdomain Enumeration	“Location” Header in Redirect
ATP	atp.azure.com	Subdomain Enumeration	Subdomain is tenant domain
DevOps	dev.azure.com	Directory Enumeration	“WWW-Authenticate” Header

Data Collection Results

What did we find?

- DNS Enumeration Results
  - 479,826 Live DNS entries
    - SharePoint – 202,596 – 42%
    - App Services – 134,483 – 28%
    - Storage Account – 119,047 – 25%
    - Key Vault – 11,948 – 2.5%
    - DevOps – 9,084 – 1.9%
    - Databricks – 2,347 – 0.5%
    - Defender for Identity – 321 – 0.1%



Conclusions

Impact

What can we do with Ownership data?

Defenders

- Rapid identification of ownership on a resource during investigations
- Example - logs indicate a user making a request to a Storage Account blob URI. The Storage Account attribution request above can return the tenant id, which can then be used to get further information to determine ownership.
- Shadow IT identification

Attackers

- Graphs and relationships
- OSINT
- Attack surface mapping
- Targeted attacks

ATEAM

Want to Replicate the Research?

Azure Tenant Enumeration and Attribution Module

- Link - https://github.com/NetSPI/ATEAM

Usage:

Scan a single resource:

```
python ateam.py -r "myapp"
```

Scan from a text file resource list:

```
python ateam.py -f resources.txt
```

ATEAM

Want to Replicate the Research?

Usage:

Azure Tenant Discovery Results

Generated on: 2025-07-28 14:41:43

Search in all columns...

Resource URI	Type	Tenant ID	Company Name	Discovered At
darksideops.vault.azure.net	KeyVault	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:43
darksideopslogic.vault.azure.net	KeyVault	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:40
darksideops.sharepoint.com	SharePoint	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:41
cloudshelldso.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:39
darksideops3.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:39
darksideopsazure.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:39
dso3.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:41
dsoazure.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:39
dsocertificates.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:40
dsosecretfiles.blob.core.windows.net	StorageAccount	977e0660-d4d3-4752-a79d-3ac9c4dbcf19	Dark Side Ops	2025-07-28 14:41:39
darksideops.scm.azurewebsites.net	AppServices-SCM	common		2025-07-28 14:41:39

Export results to HTML:

```
python ateam.py -e html
```

Post

kat traxler @NightmareJS · 10/14/21

Stop writing S3 enumeration tools

4 16

Scott Piper
@0xdabbad00

S3 bucket finders are the hello world of offensive cloud security.

1:12 PM · 10/14/21

MSRC Disclosure Timelines

Storage Account Attribution

- Mar 27, 2024 - Initial Report Date
- Apr 23, 2024 - Case Close Date
- Status – Complete, “by-design”

Key Vault Attribution

- Mar 27, 2024 - Initial Report Date
- May 28, 2024 - Case Close Date
- Status – Complete, “working as intended”

App Service Attribution

- Mar 27, 2024 - Initial Report Date
- May 22, 2024 - Case Close Date
- Status – Complete, “working as intended”

Combined Report – Azure Tenant Enumeration

This issue was reported to MSRC and we worked with MSRC on Coordinated Vulnerability Disclosure leading up to the presentation.

- Feb 14, 2025 - Initial Report Date
- Feb 26, 2025 - Case Close Date
    - Status – Complete, “valid, but does not pose an immediate threat”
- Feb 28, 2025 - Coordinated Vulnerability Disclosure process begins
- July 2025 - Coordination with MSRC and Product Team

Microsoft’s Response

We appreciate your effort in bringing this to Microsoft's attention. Upon reviewing the collection of these cases together, we have re-evaluated the 'by design' closure of these prior cases, and are investigating approaches to defend against these classes of reconnaissance techniques.

Questions?

Special Thanks

- Patrick Sayler – Beta testing and SharePoint enumeration
- MSRC and the Microsoft Product Teams

Find Us Online:

Karl Fosaaen

- @kfosaaen (Bluesky, Mastodon, Threads)
- Karl-Fosaaen (LinkedIn)

Thomas Elling

- thomaselling1 (LinkedIn)

Both:

https://www.netspi.com/blog/technical/
https://github.com/NetSPI/