Author(s): Syynimaa, Nestori

Title: Exploring Azure Active Directory Attack Surface : Enumerating Authentication Methods with Open-Source Intelligence Tools

Year: 2022

Version: Published version

Please cite the original version:

Syynimaa, N. (2022). Exploring Azure Active Directory Attack Surface : Enumerating Authentication Methods with Open-Source Intelligence Tools. In J. Filipe, M. Smialek, A. Brodsky, & S. Hammoudi (Eds.), ICEIS 2022 : Proceedings of the 24th International Conference on Enterprise Information Systems : Volume 2 (pp. 142-147). SCITEPRESS Science And Technology Publications. https://doi.org/10.5220/0011077100003179

Exploring Azure Active Directory Attack Surface: Enumerating Authentication Methods with Open-Source Intelligence Tools

Nestori Syynimaa[ID][a]

Secureworks, Counter Threat Unit, U.S.A.
Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland

Keywords: Azure Active Directory, Azure Ad, OSINT, Attack, Enumeration, SAML, Kerberos.

Abstract: Azure Active Directory (Azure AD) is Microsoft's identity and access management service used globally by 90 per cent of Fortune 500 companies and many other organisations. Recent attacks by nation-state adversaries have targeted these organisations by exploiting known attack vectors. In this paper, open-source intelligence (OSINT) is gathered from organisations using Azure AD to explore the current attack surface. OSINT is collected from Fortune 500 companies and top 2000 universities globally. The collected OSINT includes authentication methods used by the organisation and the full name and phone number of the primary technical contact. The findings reveal that most organisations are using Azure AD and that majority of these organisations are using authentication methods exploited during the recent attacks by nation-state adversaries.

1 INTRODUCTION

1.1 Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management (IAM) service (Microsoft, 2021b). Azure AD is used as IAM by Microsoft 365 and Azure. As such, all organisations consuming these services are using Azure AD. According to Microsoft, in 2017, 90 per cent of Fortune 500 companies used Azure AD (Simons, 2017).

Azure AD is often confused with Active Directory (AD), Microsoft's *on-premises* directory service. In 2014, AD was used by 95 per cent of Fortune 500 companies (InfoSecurity Magazine, 2014). The novel research reported in this paper focuses on Azure AD.

1.2 Hybrid Identities

Azure AD can be used as a cloud-only service, where users' identities are stored only in the cloud. However, many organisations use so-called *hybrid identities*, where their on-premises identities are synchronised to Azure AD. Hybrid identities are easier for users to use, as they only need to use one set of credentials in both cloud and on-premises based services. Also, hybrid identities are easier for administrators to manage, as they only need to manage one identity per user.

There are multiple different authentication methods to be used with Azure AD hybrid identities. These are Password Hash Synchronisation (PHS), Pass-Through Authentication (PTA), and Federation (AD FS) (Microsoft, 2021c).

PHS synchronises users' password hashes from the on-premises Active Directory (AD) to Azure AD. This allows users to use the same username and password in Azure AD they are using with on-premises AD. If organisations are unwilling to synchronise their passwords, they can use PTA or AD FS. *PTA* is based on an agent installed in the on-premises environment. The agent connects to Azure AD, and when users log in to Azure AD, the agent receives users' credentials. The agent tries to log in with the provided credentials and returns the result to Azure AD. If credentials are correct, the user is logged in. AD FS authentication is based on trust between Azure AD and on-premises AD FS. Users log in to AD FS, which then passes the user information in the Security Assertion Markup Language (SAML) token. (Microsoft, 2022c).

---

[a] https://orcid.org/0000-0002-6848-094X

From the hybrid authentication methods, only AD FS provides a single-sign-on (SSO) functionality as-is. However, PHS and PTA can be coupled with Azure AD seamless SSO, a Kerberos based SSO (Microsoft, 2022a).

1.3 Known Attack Vectors

All hybrid authentication methods have known attack vectors (see Palhière, 2020; Syynimaa, 2020a; Van Horenbeeck, Daalmans, Lecomte, & Scoles, 2021), used in recent attacks by nation-state adversaries (MSRC, 2020).

The requirement for all hybrid authentication methods is directory synchronisation, where the organisation's users, groups, and devices are synchronised from on-premises AD to Azure AD (Microsoft, 2021a).

The credentials used to perform the synchronisation have elevated privileged permissions to both on-premises AD and Azure AD. When using PHS authentication, the synchronisation credentials can be used to steal password hashes of any AD user, enabling pass-the-hash attacks (Palhière, 2020). If Seamless SSO is used with PHS, the credentials can be used to retrieve the password hash used to encrypt Kerberos tickets, enabling Silver Ticket attacks. Finally, compromising the AD FS server allows exporting token signing certificate, enabling Golden-SAML attacks. (Syynimaa, 2020c).

1.4 Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) has many definitions (Glassman & Kang, 2012), but generally, it refers to intelligence produced from publicly available information. Azure AD also has public Application Programming Interfaces (APIs) which can be used to gather OSINT (Syynimaa, 2020b).

1.5 Research Question

This study aims to find the present attack surface for the known hybrid-identity attack vectors using OSINT. Therefore, the research questions of this study are:
- What is the Azure AD adoption rate?
- Which authentication methods organisations are using?
- What other information is openly available?

1.6 Structure of the Paper

The rest of the paper is structured as follows. The research method and used tools are described in Section 2. The research results are presented in Section 3, followed by a discussion in Section 4.

2 METHODOLOGY

Two datasets with internet domains were acquired to answer the research questions: The list of Fortune 500 companies (Dofo, 2019) and global universities (World University Rankings, 2022). The latter list contains 2000 the most highly ranked universities out of 19 788 for 2022.

The *AADInternals* toolkit (Syynimaa, 2022) was used to perform the OSINT queries for each organisation. AADInternals is a PowerShell module based toolkit.

The research took place between Nov 24 2021, and Jan 26 2022.

2.1 Azure AD Tenant Id

Azure AD Tenant Id is the Global Unique Identifier (GUID) of the organisation's Azure AD environment. If the organisation has Azure AD Tenant Id, it uses Azure AD. The *Get-AADIntTenantId* command was used to retrieve the Tenant Ids (see Figure 1).

Figure 1: Retrieving Tenant Id.

2.2 Directory Synchronisation

The *Get-AADIntSARATenantInfo* command was used to check whether the directory synchronisation was enabled (see Figure 2). This command requires that the user is authenticated to *any* Azure AD tenant.

Figure 2: Checking is directory synchronisation enabled.

2.3 Seamless Single-Sign-on

The *Get-CredentialType* command was used to check whether Seamless SSO was enabled (see Table 3). This command is an internal command of the tool and not exposed outside it. It can be located at

AccessToken_utils.ps1 from the module installation location.

```
PS C:\> $credType = Get-CredentialType -UserName "nn@
PS C:\> $credType.EstsProperties.DesktopSsoEnabled
True
```

Figure 3: Checking is seamless single-sign-on enabled.

2.4 Number and Federation Information of Domains

Each Azure AD tenant can have multiple domains to be used as email addresses or login names. If AD FS is used for a particular domain, its type is *federated*. First, the *Get-AADIntTenantDomains* command was used to retrieve all tenant domains. After this, the *Get-UserRealmV2* command was used to retrieve the type of each domain (see Figure 4). This command is also an internal command located at *AccessToken_utils.ps1*.

```
PS C:\> $domains = Get-AADIntTenantDomains -Domain "
PS C:\> $domain = $domains[0]
PS C:\> $domainInfo = Get-UserRealmV2 -UserName "nn@$domain"
PS C:\> $domainInfo.NameSpaceType
Federated
```

Figure 4: Retrieving domains and federation info.

2.5 Tenant Organisation Information

Each tenant has a primary technical contact defined in their Azure AD tenant's organisation information. This information is valuable for adversaries, as the technical contact likely holds the Global Admin privileges to Azure AD.

```
PS C:\> Get-AADIntAccessTokenForAdmin -SaveToCache
AccessToken saved to cache.

Tenant                              User
------                              ----


PS C:\> Get-AADIntTenantOrganisationInformation -Domain "

TenantId            :
CompanyName         :
StreetAddress       :
ApartmentOrSuite    :
City                :
StateOrProvince     :
PostalCode          :
CountryCode         :
PhoneNumber         :
FirstName           :
LastName            :
```

Figure 5: Retrieve organisation information.

The *Get-AADIntTenantOrganisationInformation* command was used to retrieve this information (see Figure 5). This command requires that the user is authenticated to *any* Azure AD tenant.

3 RESULTS

In this Section, the collected data is presented in tabular format.

3.1 Azure AD Adoption Rate

From Fortune 500 organisations, 88 per cent use Azure AD (Table 1). This is two percentage points less than in 2017. The difference can be explained by the used dataset, as it may contain outdated or missing domain names.

Of the top 2000 universities, 95 per cent use Azure AD (Table 1). The higher adoption rate may be explained due to pricing, as most Microsoft cloud licenses are free-of-charge to educational institutions (Microsoft, 2022b).

Table 1: Azure AD Adoption Rate.

Organisation type	Azure AD	
Fortune 500 (*n*=500)	441	88 %
Top 2000 Universities (*n*=2000)	1892	95 %

3.2 Directory Synchronisation

From Fortune 500 companies using Azure AD, 84 per cent use directory synchronisation (Table 2). This rate is lower than anticipated, as hybrid identities are seen as a productivity improvement (Forrester, 2020). Of the top 2000 universities using Azure AD, only 52 per cent use directory synchronisation (Table 2). More homogenous and complex environments may explain the big difference to Fortune 500 companies compared to academic institutions, which typically already have an identity management system.

Table 2: Directory Synchronisation.

Organisation type	Sync	
Fortune 500 (*n*=441)	420	84 %
Top 2000 Universities (*n*=1892)	1042	52 %

3.3 Seamless Single-Sign-on

From Fortune 500 companies using Azure AD, 27 per cent use seamless single-sign-on (Table 3). At the first look, this seems a low percentage. However, when combined with the other SSO solution (AD FS) percentage, they cover 95 per cent of companies using Azure AD. Of the top 2000 universities using Azure AD, only 14 per cent use directory synchronisation (Table 3). Even when combined with AD FS percentage, this covers only 42 per cent of

universities. This implies that most universities are not using any SSO solution.

Table 3: Seamless Single-Sign-On.

Organisation type	SSO	
Fortune 500 (*n*=441)	118	27 %
Top 2000 Universities (*n*=1892)	258	14 %

3.4 Domains and Federation

From Fortune 500 companies using Azure AD, 98 per cent have domains registered to Azure AD (Table 4). The missing 2 per cent are organisations that haven't had any Exchange Online licenses. From the top 2000 universities using Azure AD, practically all have registered domains to Azure AD (Table 4).

Table 4: Domains.

Organisation type	Domains	
Fortune 500 (*n*=441)	432	98 %
Top 2000 Universities (*n*=1892)	1884	100 %

From Fortune 500 companies using Azure AD, 66 per cent use federation at least for one domain (Table 5). Of the top 2000 universities using Azure AD, only 28 per cent use federation (Table 5).

Table 5: Federated Domains.

Organisation type	Federation	
Fortune 500 (*n*=432)	293	68 %
Top 2000 Universities (*n*=1884)	535	28 %

An interesting finding was that some organisations used both SSO solutions (Table 6). From Fortune 500 organisations using Azure AD, 11 used both SSOs and from top universities, nine organisations.

Table 6: Organisations with both SSO solutions.

Organisation type	Two SSOs	
Fortune 500 (*n*=441)	11	2,49 %
Top 2000 Universities (*n*=1892)	9	0,48 %

3.5 Tenant Organisation Information

From Fortune 500 companies using Azure AD, 98 per cent has organisation information available (Table 7), including the full name of the primary technical contact. This was expected to be 100 per cent, but this information was not available for some organisations. From the top 2000 universities using Azure AD, the information was available only for 77 per cent (Table 7).

Table 7: Organisation Information.

Organisation type	Information	
Fortune 500 (*n*=441)	434	98 %
Top 2000 Universities (*n*=1892)	1463	77 %

Organisation information also includes the phone number of the primary technical contact. From Fortune 500 companies using Azure AD, 87 per cent had this information available (Table 8). From the top 2000 universities using Azure AD, the information was available for 56 per cent (Table 8).

Table 8: Phone number.

Organisation type	Phone num.	
Fortune 500 (*n*=441)	383	87 %
Top 2000 Universities (*n*=1892)	1059	56 %

4 DISCUSSION

4.1 Implications

The study results show that Azure AD is used by a great majority of Fortune 500 companies and top 2000 universities. This finding is in line with information shared by Microsoft (see Simons, 2017). Results also show which authentication methods and hybrid configuration the studied organisations are using. This revealed breadth and depth of the attack surface the adversaries could exploit. For instance, virtually all Fortune 500 companies using Azure AD have implemented SSO, a commonly used attack vector in recent attacks by nation-state adversaries.

Besides exposing the attack surface, OSINT reveals information that could be used for social engineering. For instance, technical contact names and phone numbers can be used in spear-phishing attacks. Moreover, listing all domains of the organisation allows searching the internet for existing email addresses with the same domain. These accounts can then be used in phishing campaigns.

4.2 Recommendations

By definition, OSINT is intelligence that anyone can access. As such, organisations using Azure AD can not prevent access to this information. However, most tenant organisation information can be freely edited. To hide the identity of the technical contact, organisations should use a general name, such as "IT Department", instead of the actual name of the contact. Moreover, the phone number should be

changed to a public number, such as the headquarters' phone number.

4.3 Future Work

Microsoft has over 140 portals administering their cloud services, such as Azure and Microsoft 365, and over 50 portals for consuming them (Fowler, 2022). Each of these portals uses APIs to access the back-end services. Studying these APIs could reveal candidates for gathering new OSINT.

4.4 Limitations

Two openly available data sets were used to conduct this research. The data sets were not curated, so they may contain outdated or missing data. However, our findings are in line with other available information regarding the Azure AD adoption rate, which indicates that the datasets were accurate.

4.5 Acknowledgements

This research used an unpublished version (v0.6.7) of the AADInternals toolkit to gather OSINT. The tool will be published in March 2022 after Microsoft has fixed vulnerabilities found and reported during this research. This paper does not contain any OSINT gathered exploiting these vulnerabilities. The author would like to thank Microsoft Security Response Center (MSRC) for cooperating with reported vulnerabilities.

4.6 Conclusions

This paper demonstrated how anyone could gather open-source intelligence (OSINT) from any organisation using Azure AD. The OSINT was collected from Fortune 500 organisations and 2000 the most highly ranked universities.

The findings revealed that most of the studied organisations are using Azure AD. It was possible to collect information about which hybrid identity authentication methods organisations were using. This information is extremely valuable to threat actors, as it reveals which attack vectors can be used to compromise the target organisation. Especially organisations using AD FS and seamless SSO are exciting targets, as compromising on-premises environment allows threat actors to impersonate any user of the target organisation.

For some organisations, information of the primary technical contact, including full name and phone number, could be gathered. This information is also extremely valuable, as these people often have Global Administrator privileges to Azure AD. Therefore, they are primary targets for social engineering attacks.

REFERENCES

Dofo. (2019). Domain Names of Fortune 500 Companies. Retrieved from https://dofo.com/blog/fortune-500-domain-names/

Forrester. (2020). The Total Economic Impact™ Of Securing Apps With Microsoft AzureActive Directory. 28. Retrieved from https://aka.ms/aadtei

Fowler, Adam. (2022). Microsoft Portals. Retrieved from https://msportals.io/

Glassman, Michael, & Kang, Min Ju. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior, 28*(2), 673-682. doi:https://doi.org/10.1016/j.chb.2011.11.014

InfoSecurity Magazine. (2014). Active Directory Flaw Could Threaten 95% of Fortune 500 with Massive Information Heist. *InfoSecurity Magazine*(July 16). Retrieved from https://www.infosecurity-magazine.com/news/active-directory-flaw-could/

Microsoft. (2021a). Azure AD Connect sync: Understand and customize synchronization. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis

Microsoft. (2021b). What is Azure Active Directory? Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (2021c). What is hybrid identity with Azure Active Directory? Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

Microsoft. (2022a). Azure Active Directory Seamless Single Sign-On. Retrieved from https://docs.micro soft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

Microsoft. (2022b). Get Office 365 free for your entire school. Retrieved from https://www.microsoft.com/en-us/microsoft-365/academic/compare-office-365-education-plans

Microsoft. (2022c). What is a Primary Refresh Token? Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-primary-refresh-token

MSRC. (2020). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved from https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

Palhière, Aymeric. (2020). Azure AD Introduction for Red Teamers. Retrieved from https://www.synacktiv.com/en/publications/azure-ad-introduction-for-red-teamers.html

Simons, Alex. (2017, Nov 13 2017). How organizations are connecting their on-premises identities to Azure AD. Retrieved from https://www.microsoft.com/en-us/microsoft-365/blog/2017/11/13/how-organizations-are-connecting-their-on-premises-identities-to-azure-ad/

Syynimaa, Nestori. (2020a). AAD & M365 kill chain. Retrieved from https://o365blog.com/aadkillchain/

Syynimaa, Nestori. (2020b). Just looking: Azure Active Directory reconnaissance as an outsider. Retrieved from https://o365blog.com/post/just-looking/

Syynimaa, Nestori. (2020c). Unnoticed sidekick: Getting access to cloud as an on-prem admin. Retrieved from https://o365blog.com/post/on-prem_admin/

Syynimaa, Nestori. (2022). AAD Internals. Retrieved from https://o365blog.com/aadinternals/

Van Horenbeeck, Michael, Daalmans, Peter, Lecomte, Thijs, & Scoles, Damian. (2021). *Microsoft 365 Security for IT Pros* (T. Lecomte Ed. Second edition (2022) ed.): VH Consulting & Training BV.

World University Rankings. (2022). Global 2000 list by the Center for World University Rankings, 2021-22 Edition. Retrieved from https://cwur.org/2021-22.php