Threat Research

Detecting Microsoft 365 and Azure Active Directory Backdoors

September 30, 2020 | by Mike Burns

MANDIANT DETECTION INCIDENT RESPONSE BACKDOOR

Mandiant has seen an uptick in incidents involving Microsoft 365 (M365) and Azure Active Directory (Azure AD). Most of these incidents are the result of a phishing email coercing a user to enter their credentials used for accessing M365 into a phishing site. Other incidents have been a result of password spraying, password stuffing, or simple brute force attempts against M365 tenants. In almost all of these incidents, the user or account was not protected by multi-factor authentication (MFA).

These opportunistic attacks are certainly the most common form of compromise for M365 and Azure AD, and are usually the initial vector to establish persistence. During both incident response (IR) engagements and proactive cloud assessments we are often asked:

- What are some other types of attacks that Mandiant is seeing against M365 and Azure AD?
- Is it possible for an on-premises compromise to "vertically" move to M365 and Azure AD?
- If a global administrator account is compromised, is it possible to maintain persistence even after the compromised account has been detected, a password reset has occurred, and MFA has been applied?

AADInternals PowerShell Module

In some incidents, Mandiant has witnessed attackers utilizing a PowerShell module called AADInternals, which can allow an attacker to vertically move from on-premises to Azure AD, establish backdoors, steal passwords, generate user security tokens, and bypass MFA protections. This PowerShell module has allowed attackers to maintain persistence in the tenant even after initial eradication efforts were conducted.

To see this module in action and understand how it works, Dr. Nestori Syynimaa's PSCONFEU 2020 presentation, Abusing Azure Active Directory: Who would you like to be today?, provides an in-depth overview of the module.

To detect the use of AADInternals, it is important to understand how some of these attacks work. Once an understanding is established, abnormal usage can be detected through a combination of log analysis and host-based indicators.

Backdoor 1: Abusing Pass-Through Authentication

Attacker Requirements

- Local Administrative Access to a server running Pass-through Authentication

  Or

- M365 global administrator credentials

that occurs between Azure AD and the server running the PTA Agent in the on-premises environment. Commonly, the PTA Agent runs on the same on-premises server as Azure AD Connect (AAD Connect).

When PTA is enabled, every logon that occurs against Azure AD gets redirected to the PTA Agent on-premises. The PTA Agent asks an on-premises Active Directory Domain Controller if a password is valid for an authenticating account. If valid, the PTA Agent responds back to Azure AD to grant the requestor access. Figure 1 provides the workflow of Pass-through Authentication and where AADInternals can intercept the request.

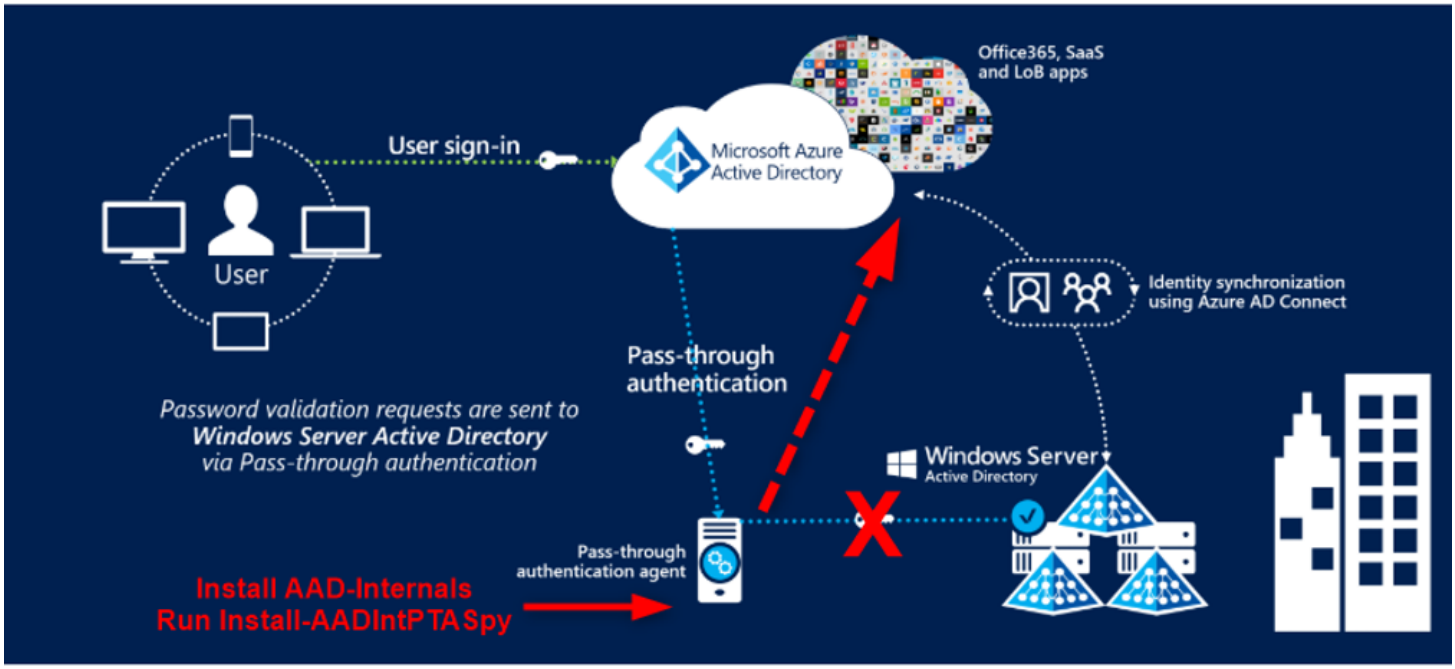


Figure 1: Pass-through Authentication workflow

Once the function is running, every PTA attempt against Azure AD will be intercepted by the installed `AADIntPTASpy` module. The module will record the user's password attempt and reply back to Azure AD on behalf of the PTA Agent. This reply advises Azure AD the password attempt was valid and grants the user access to the cloud, even if the password is incorrect. If an attacker has implanted `AADIntPTASpy`, they can log in as any user that attempts to authenticate using PTA—and will be granted access.

Additionally, all password attempts that are registered by the `AADIntPTASpy` module are recorded within a log file on the server (Default location: `C:\PTASpy\PTASPy.csv`). Figure 2 shows how the log file can be decoded to reveal a user's password in cleartext.

```
PS C:\Users\Administrator> Get-AADIntPTASpyLog -DecodePasswords

UserName                Password          Time
--------                --------          ----
garth.barks@b           sadffdsaf         6/20/2020 4:03:09 AM
garth.barks@b           sadffdsaf         6/20/2020 4:03:11 AM
garth.barks@b           ThisIsMyOnPremPW  6/20/2020 4:14:53 AM

PS C:\Users\Administrator>
```

could allow an attacker to pivot their attack to other areas of the network—or use these credentials against other internet accessible portals that may leverage single-factor authentication (e.g., VPN gateway).

An attacker can use this module in one of two ways:

Method 1: On-Premises Compromise

An attacker has gained access to an on-premises domain and is able to laterally move to the AADConnect / PTA Agent Server. From this server, an attacker can potentially leverage the AADInternals PowerShell module and invoke the `Install-AADIntPTASpy` function.

Method 2: Cloud Compromise

If an attacker has successfully compromised an Azure AD global admin account, an attack can be conducted from an attacker's own infrastructure. An attacker can install a PTA Agent on a server they manage and register the agent using the compromised global administrator account (Figure 3).

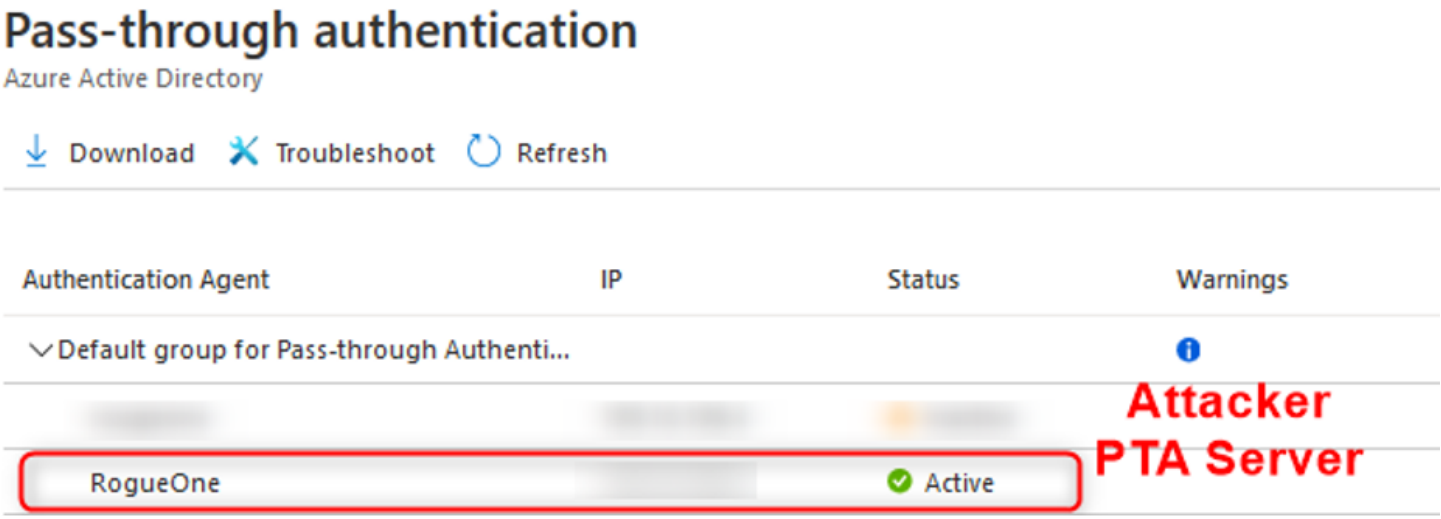


Figure 3: Azure AD Portal—registered Pass-through Authentication agents

Once registered with Azure AD, the rogue server will begin to intercept and authorize all login attempts. As with Method 1, this server can also be used to harvest valid credentials.

Backdoor 2: Abusing Identity Federation

Attacker Requirements

- Local administrative access to AD and server running Active Directory Federation Services

  Or

- M365 global administrator credentials

Another method of authenticating to M365 is through the usage of federation services. When a M365 domain is configured as a federated domain, a trust is configured between M365 and an external identify provider. In many cases, this trust is established with an Active Directory Federation Services (ADFS) server for an on-premises Active Directory domain.

Once validated, the ADFS server provides the user a security token. This token is then trusted by M365 and grants the access to the platform.

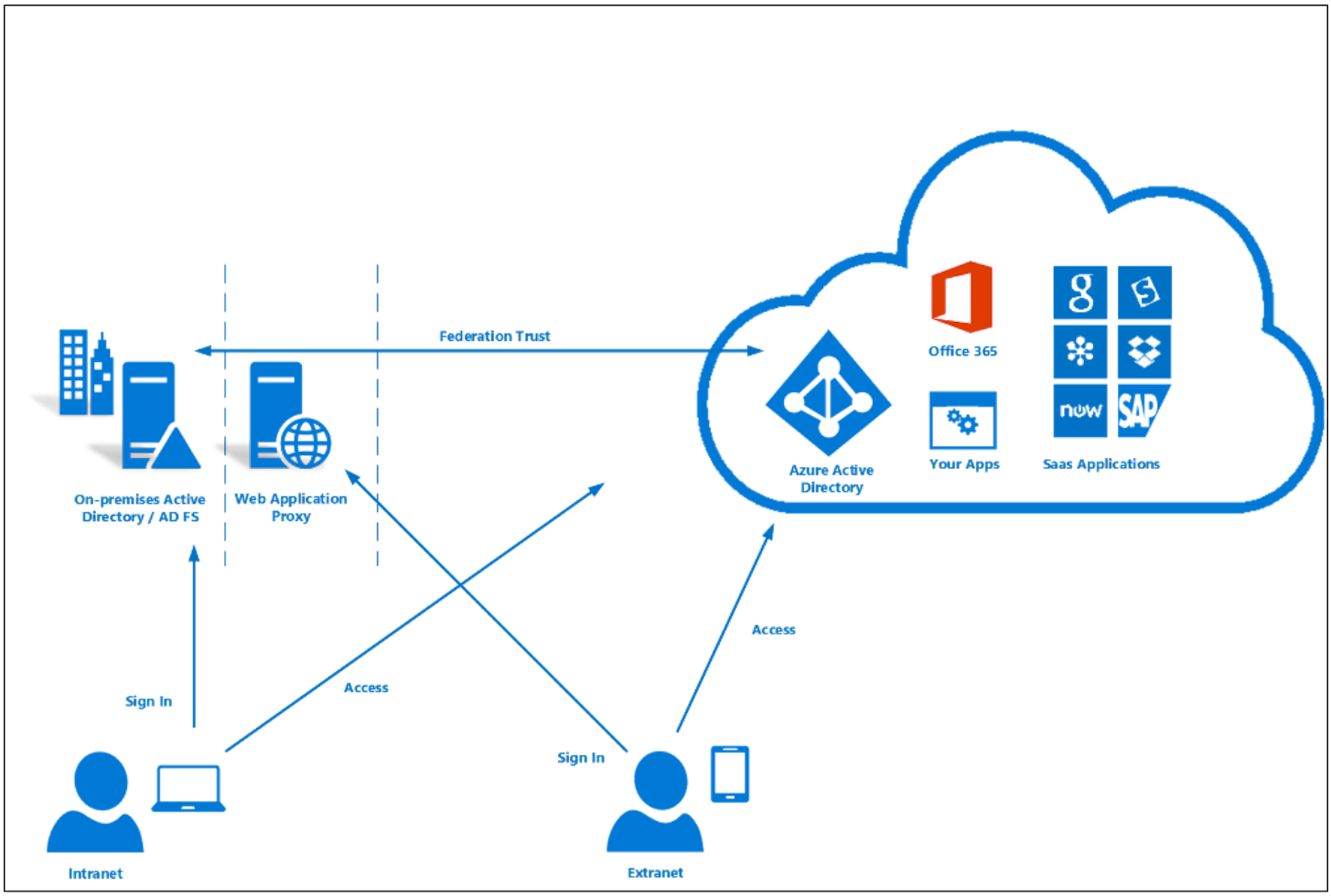


Figure 4: Microsoft 365 Federation Sign-in workflow

AADInternals has a PowerShell function to craft security tokens, which mimics the ADFS authentication process. When providing the function a valid UserPrincipalName, Immutable ID and IssuerURI, an attacker can generate a security token as any user of the tenant. What's even more concerning is that once this security token is generated, this can allow an attacker to bypass MFA.

As with Backdoor 1, this attack can either be performed from a compromised on-premises environment or from an attacker's own infrastructure.

Method 1: On-Premises Compromise

Once an attacker has gained access to an on-premises domain with elevated access, they can begin to collect the required information to craft their own security tokens to backdoor into M365 as any user. An attacker will require:

- A valid UserPrincipalName and Immutable.
  - Both of these attributes can be pulled from the on-premises Active Directory domain.
- IssuerURI of the ADFS server and ADFS Signing certificate.
  - This can be obtained from an ADFS server when directly logged into the server or remotely

access to M365 (Figure 5).

```
PS C:\Users\mike> Open-AADIntOffice365Portal -ImmutableID "5C                    =" -Issuer "https://sts.attacker-        com/adfs/services/trust" -PfxFileName
C:\users\mike\ADFSCert.pfx
```

Figure 5: AADInternals Open-AADIntOffice365Portal command

Method 2: Cloud Compromise

If an attacker has a compromised an M365 Global Administrator account, using their own infrastructure, an attacker can use their administrative access to collect user information and reconfigure the tenant to establish their backdoor. In this method, an attacker will require:

- A valid UserPrincipalName and valid ImmutableId.
  - Figure 6 shows how the `Get-MsolUser` command can obtain a user's ImmutableId from Azure AD.

```
PS C:\Users\mike.burns> Get-MsolUser | select UserPrincipalName,ImmutableId

UserPrincipalName                                  ImmutableId
-----------------                                  -----------
t
n
garth.barks@          .com                         5Cj7                    w==
n
```

Figure 6: Get-MsolUser—list user UPN & ImmutableId

- IssuerURI
  - This can be obtained by converting a managed domain to a federated domain. Figures 7 through 10 show how the AADInternals `ConvertTo-AADIntBackdoor` command (Figure 8) can be used to allow attacker to register their own IssuerURI for a federated domain.

```
PS C:\Users\Administrator> Get-msoldomain

Name                                   Status   Authentication
----                                   ------   --------------
Bu       .onmicrosoft.com              Verified Managed
b        .com                          Verified Managed
attack-          .com                  Verified Managed
         .mail.onmicrosoft.com         Verified Managed
```

Figure 7: Get-msoldomain—list of registered domains and authentication

```
Credential
PS C:\Users\Administrator> $at=Get-AADIntAccessTokenForAADGraph -Credentials $cred
PS C:\Users\Administrator> ConvertTo-AADIntBackdoor -AccessToken $at attack-b       .com
Are you sure to create backdoor with attack-       .com? Type YES to continue or CTRL+C to abort: yes

IssuerUri              Domain
---------              ------
http://any.sts/4       attack       5.com
```

Figure 8: ConvertTo-AADIntBackdoor—convert domain to federated authentication

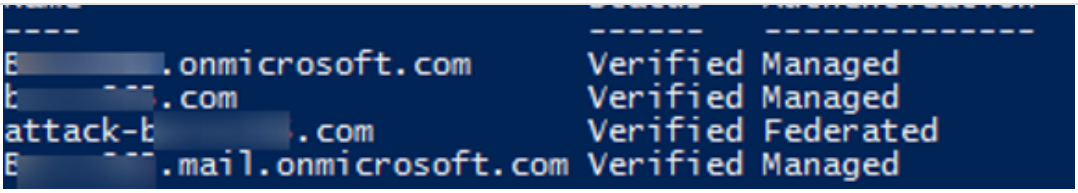


Figure 9: Changed authentication method

Figure 10: Azure AD Portal registered domains

Note: To not interrupt production and authentication with an existing federated domain (and to remain undetected), an attacker may opt to register a new domain with the tenant.

Figure 11: AADInternals Open-AADIntOffice365Portal Command using new Federated domain

Once an attacker has properly configured the tenant, using the ImmutableId of any user, a security token can be generated by executing the `Open-AADIntOffice365Portal` command (Figure 11). This will allow an attacker to login as that user without the need for a valid certificate or a legitimate IssuerURI.

Fortunately for defenders, this method will generate a number of events in the unified audit log, which can be leveraged for monitoring and alerting.

Mitigation and Detection

Once persistence is established, it can be extremely difficult to detect login activity that is utilizing one of the previously described methods. In lieu of this, it is recommended to monitor and alert on M365 unified audit logs and Azure AD sign-in activity to detect anomalous activity.

Detection in FireEye Helix

Being that Mandiant has seen this methodology being used in the wild, we felt it was necessary to build these detections into our FireEye Helix security platform. Helix engineers have created sever new detection rules that monitor for detectable activity of an attacker making use of the AADInternals PowerShell module.

The following five rules will monitor a server's event logs and alert upon the installation and usage of the AADInternals PowerShell module (Figure 12). The detection of these activities could be high fidelity alerts that an attacker is preparing to configure backdoors into M365 and Azure AD environments.

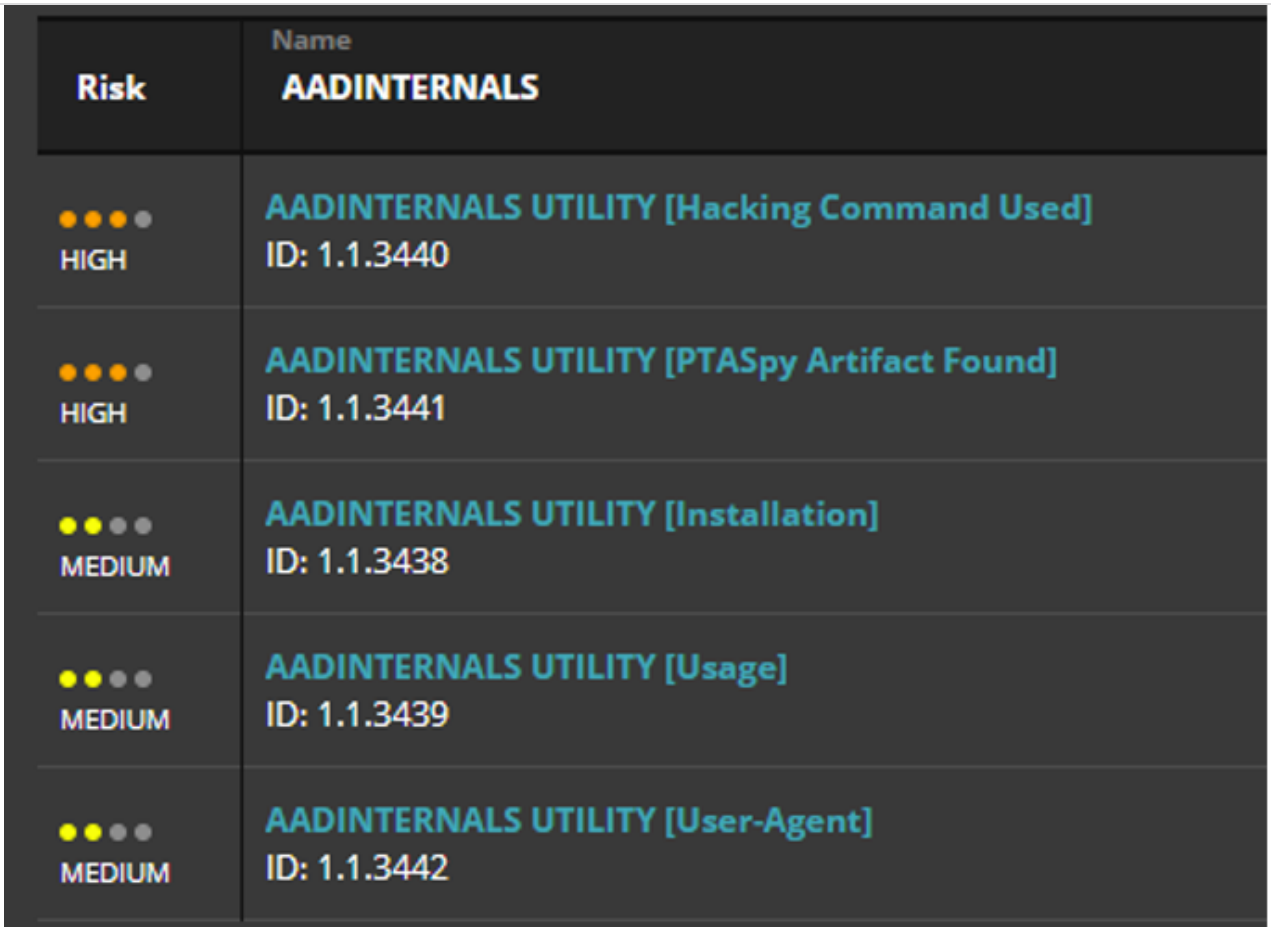
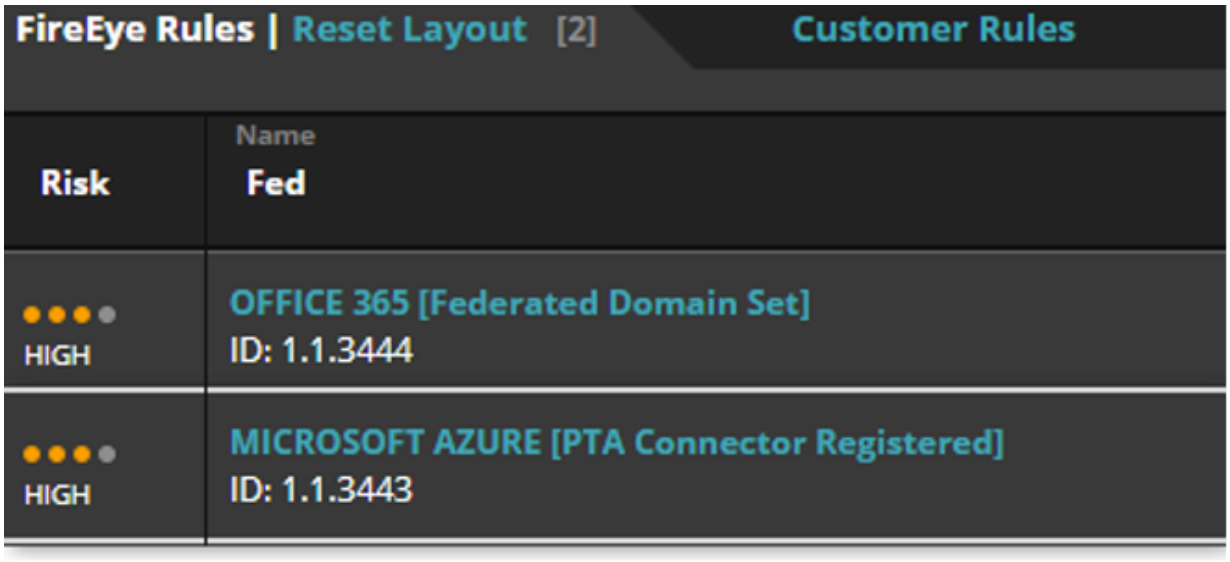


Figure 12: AADInternals Helix rules

If an attacker has successfully configured a backdoor using AADInternals, Helix will alert upon the following events registered in the Office 365 unified audit log and Azure Activity Log as indication of a possible event (Figure 13 and Figure 14). It is important to note that these alerts could be triggered upon legitimate administrator activity. When responding to these alerts, first check with your M365 and Azure AD administrator to verify the activity before raising a security event.



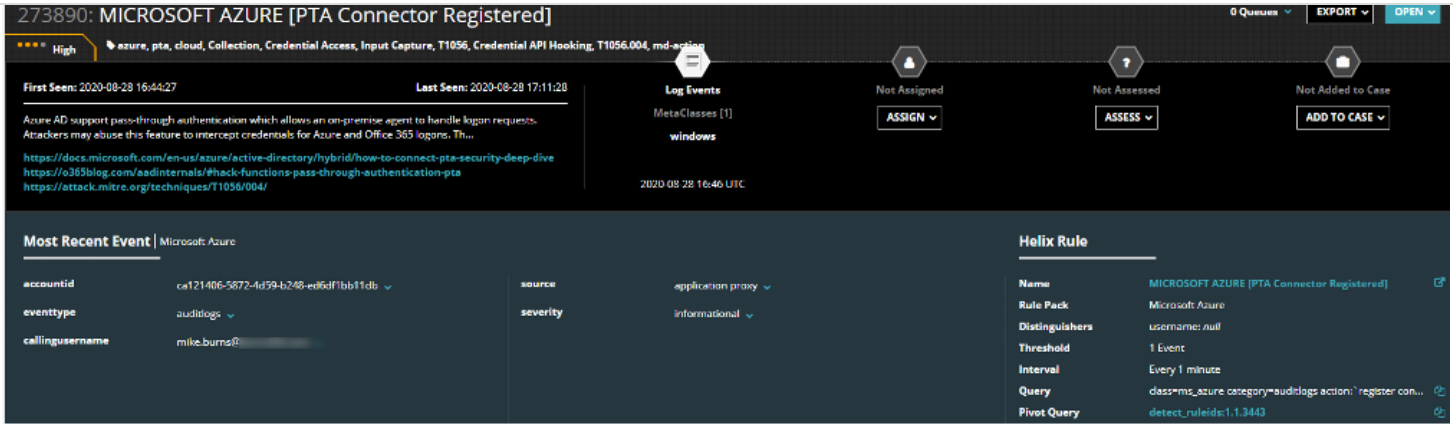


Figure 14: PTA Connector Registered alert description

Hunting for Backdoors in M365 Unified Audit Logs and Azure AD Logs

If you suspect a global administrator account was compromised and you want to review Azure AD for indicators of potential abuse, the following should be reviewed (note that these same concepts can be used for proactive log monitoring):

- From Azure AD Sign-ins logs, monitor logon activity from On-Premises Directory Synchronization Service Accounts. This account is used by the Azure AD Connect service (Figure 15).

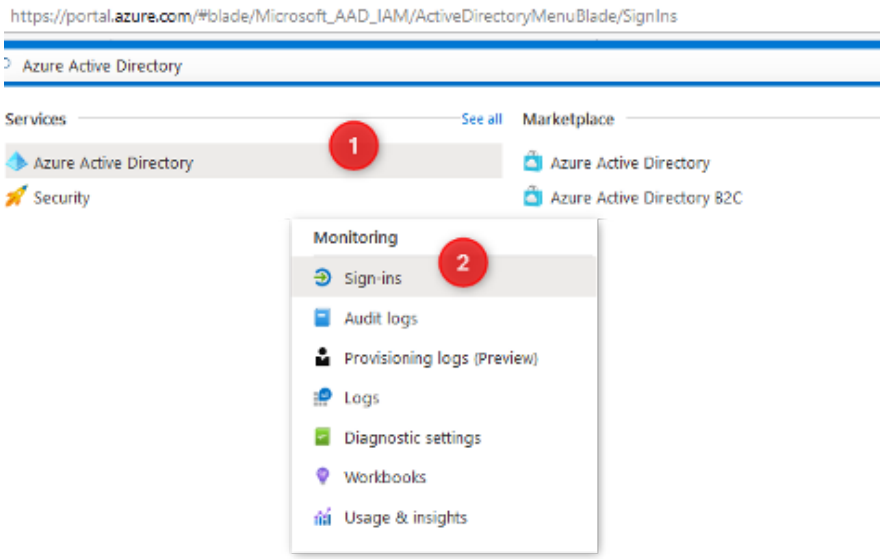
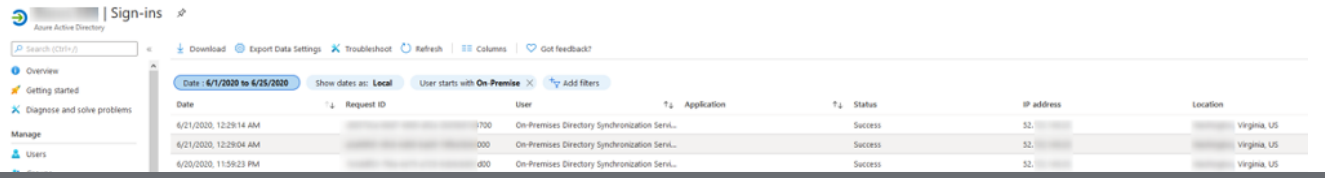


Figure 15: Azure AD Sign-ins

- Baseline the IP addresses used by this account and make sure the IPs match those assigned to the on-premises WAN infrastructure. If the attacker has configure a PTA Agent on their own infrastructure, seeing an IP that does not match your baseline could be an indicator that a rogue PTA Agent has been configured by the attacker (Figure 16).



These events are typically only generated when a new PTA agent is connected to the tenant. This could be an indicator that an attacker has connected a rogue PTA server hosted on an attacker's infrastructure (Figure 17).

Figure 17: Azure AD Sign-in logs—Azure AD Application Proxy Connector

If using Azure Sentinel, this event will also be registered in the Azure AuditLogs table as a "`Register Connector`" OperationName (Figure 18).

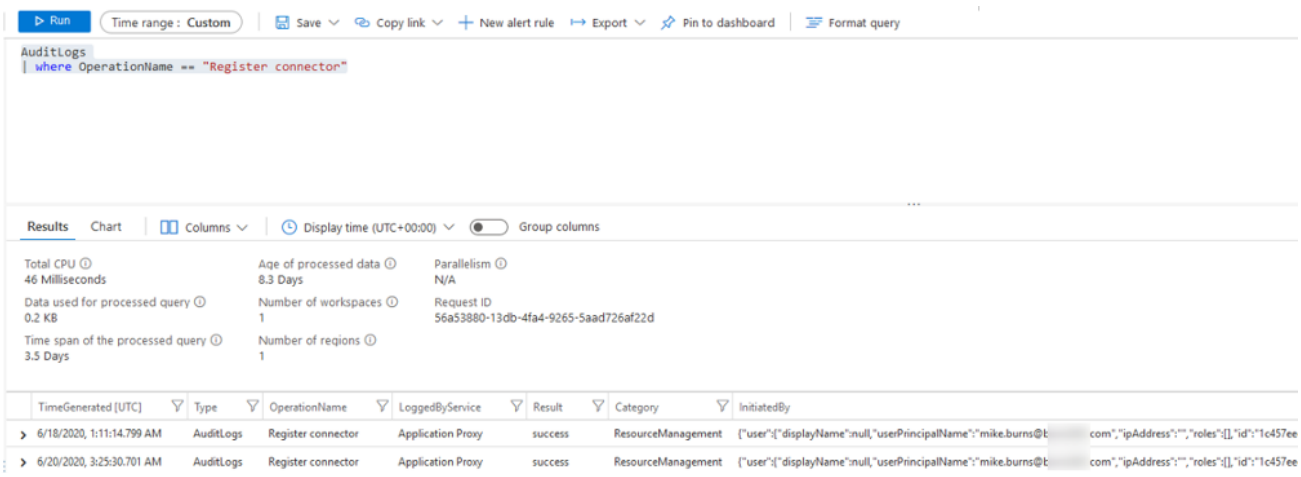


Figure 18: Register Connector—Azure Sentinel logs

- In the Azure Management Portal under the Azure AD Connect blade, review all registered servers running PTA Agent. The Authentication Agent and IP should match your infrastructure (Figure 19).
  - Log in to https://portal.azure.com
    - Select Azure AD Connect > Pass-through Authentication

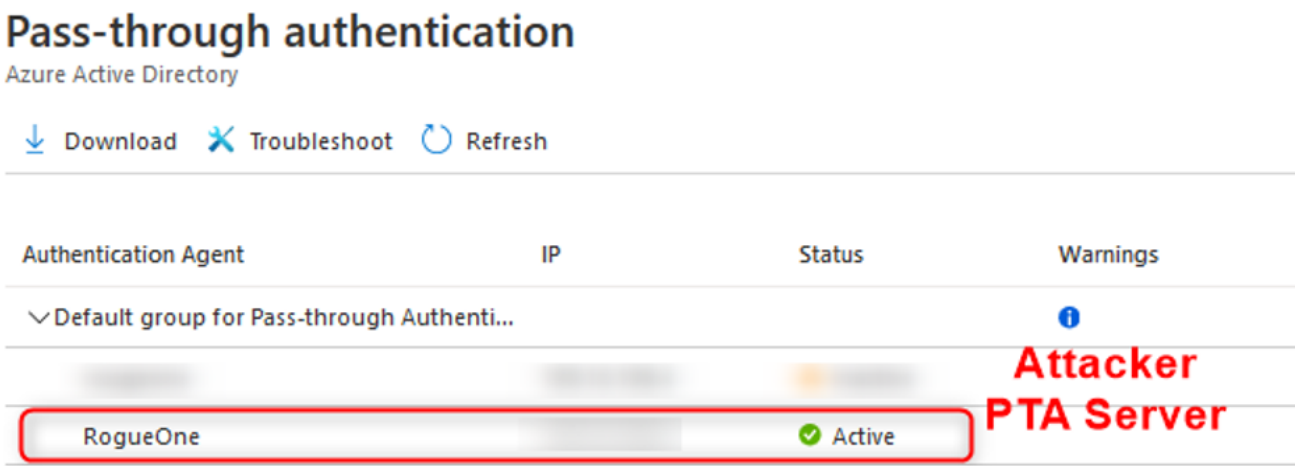


Figure 19: Azure Active Directory Pass-through Authentication agent status

- Monitor and alert for "Directory Administration Activity" in Office 365 Security & Compliance Center's unified audit log. When an attacker is able to create a domain federation within a

- Create New Alert Policy (Figure 20)

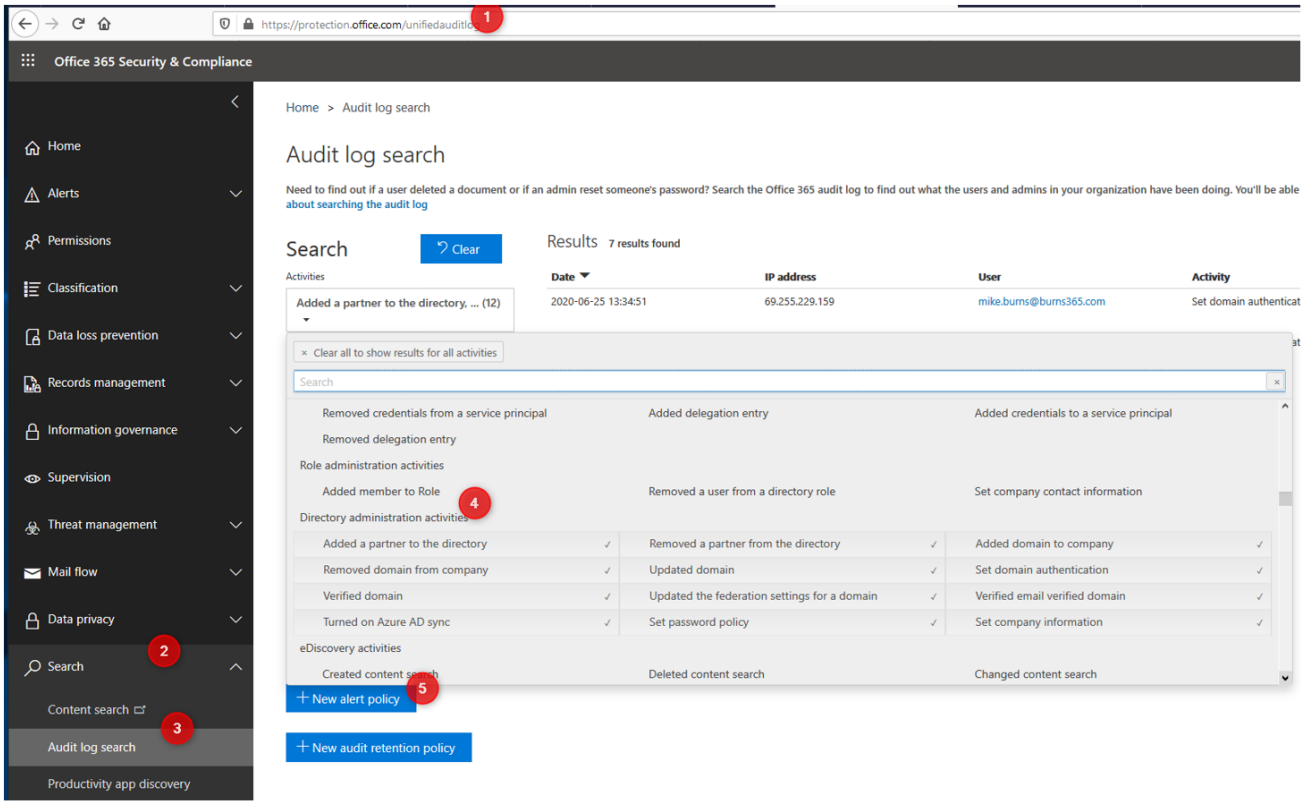


Figure 20: Unified Audit Log > Create new alert policy

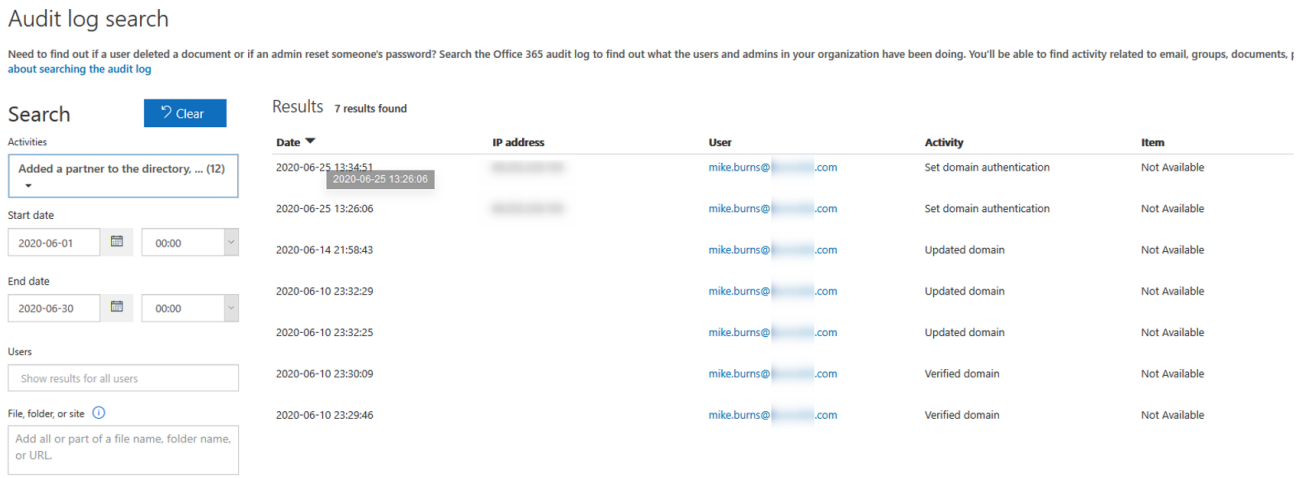


Figure 21: Unified Audit Log filtered for domain related events

- Using Azure Sentinel, more granular Directory Administration Activities can be modified for suspicious activity. This includes additions, deletions and modifications of domains and their authentication settings (Figure 22).
  - Monitoring for `OfficeActivity` Operations in Azure Sentinel can allow an organization to validate if this is normalized activity or if an attacker is working on setting up a backdoor for PTA or federation.
    - Table: OfficeActivity
      - Operation: Set-AcceptedDomain

- Operation: Remove-FederatedDomain

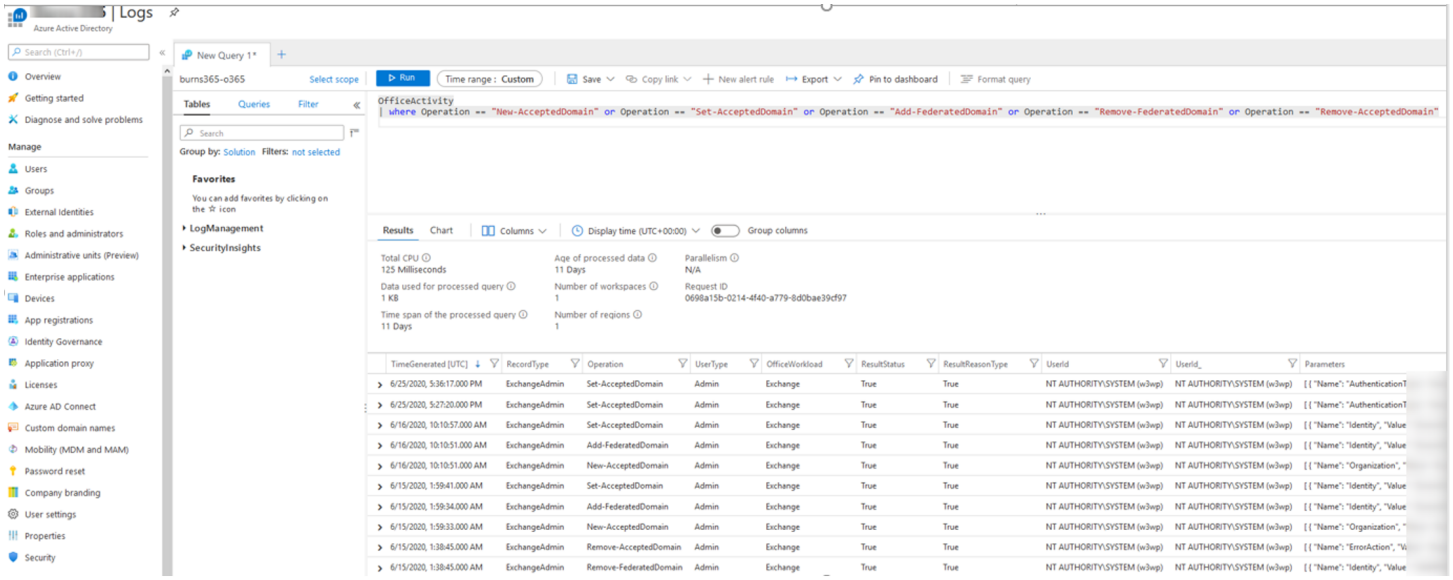


Figure 22: OfficeActivity Operations Azure Sentinel logs

Detection On-Premises

If an attacker is able to compromise on-premises infrastructure and access a server running AD Connect or ADFS services with the intention of leveraging a tool such as AADInternals to expand the scope of their access to include cloud, timely on-premises detection and containment is key. The following methods can be leveraged to ensure optimized visibility and detection for the scope of activities described in this post:

- Treat ADFS and Azure AD Connect servers as Tier 0 assets.
  - Use a dedicated server for each. Do not install these roles and server in addition to other. All too often we are seeing Azure AD Connect running on a file server.
- Ensure PowerShell logging is optimized on AD Connect and ADFS servers
- Review Microsoft-Windows-PowerShell/Operational logs on ADFS and AADConnect Server Logs.
  - If PowerShell logging is enabled, search for Event ID 4101. This event ID will record the event where AADInternals was installed (Figure 23).

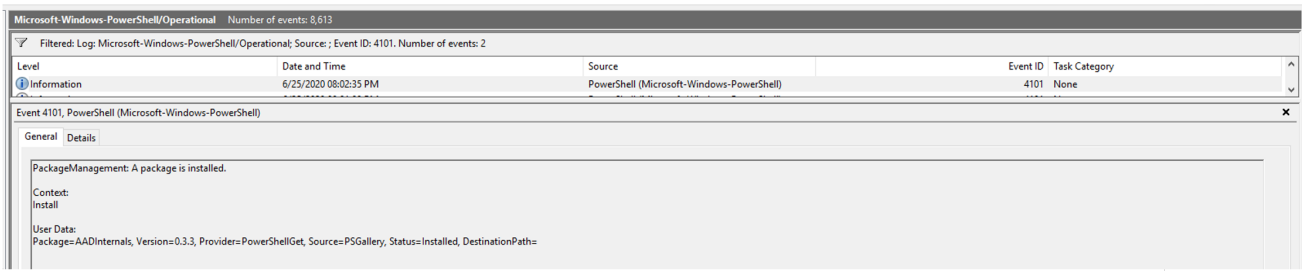


Figure 23: EventID 410—Installed Module

- Additionally, with this logging enabled, you will be able to review the PowerShell commands used by an attacker.
  - In PowerShell, run Get-Module -All and look for the presence of AADInternals (Figure 24).

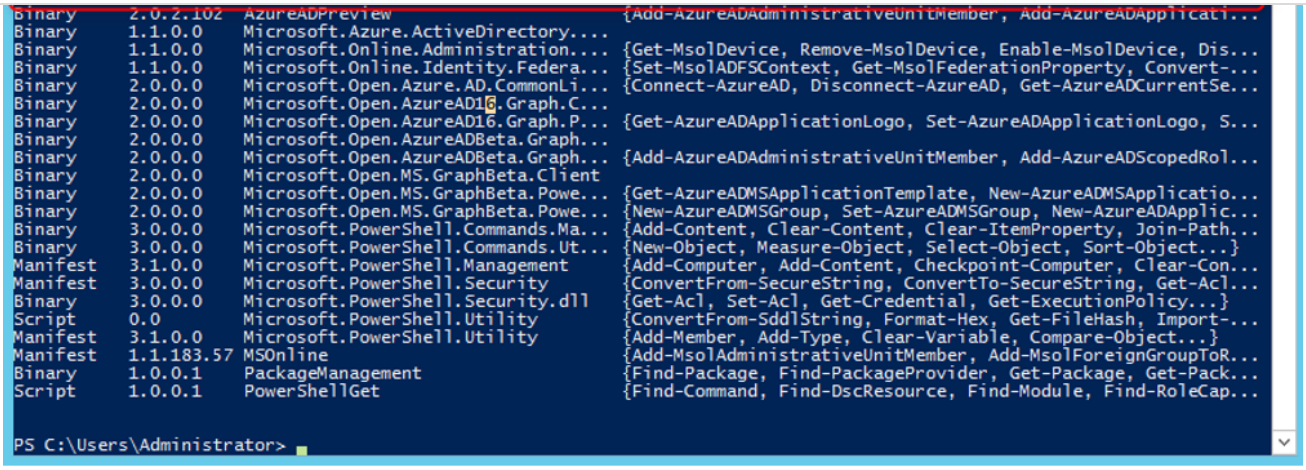


Figure 24: Get-Module command to list installed modules

- Alert for the presence of C:\PTASpy and C:\PTASpy\PTASpy.csv.
  - This is the default location of the log file that contains records of all the accounts that were intercepted by the tool. Remember, an attacker may also use this to harvest credentials, so it is important to reset the password for these accounts (Figure 25).

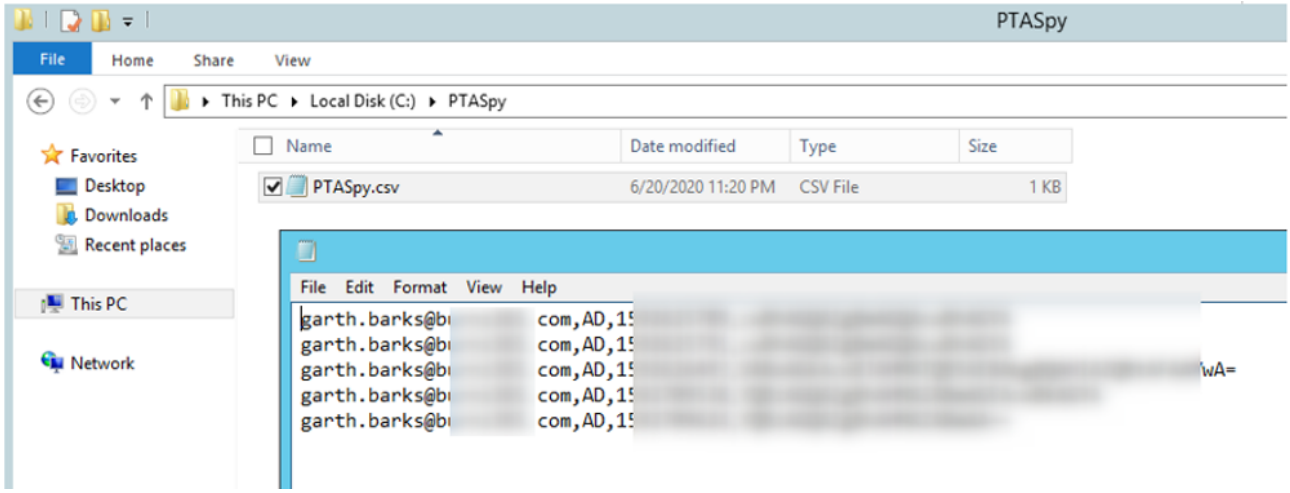


Figure 25: PTASpy.csv log activity

Mitigations

In order for this attack to be successful, an attacker must gain administrative privileges on a server running Azure AD Connect and/or gain global administrator rights within M365. Simple practices such as limiting and properly protecting global administrator accounts as well as properly protecting Tier 0 assets can greatly reduce the risk of an attacker successfully using the AADInternals PowerShell against your organization.

- Limit or restrict access to Azure AD Connect servers.
  - Any server acting as an identity provider or facilitating identity federation should be treated as a Tier 0 asset.
- Create separate dedicated global administrator accounts.
  - Global administrators should be cloud-only accounts.
  - These accounts should not retain any licensing

- Establish a roadmap to block legacy authentication.
- Limit which accounts are synced from on-premises to the cloud.
  - Do not sync privileged or service accounts to the cloud.
- Use Azure administrative roles.
  - Not everybody or everything needs to be a global admin to administer the environment.
- Use password hash sync over Pass-through Authentication.
  - Many organizations are reluctant to sync their password to Azure AD. The benefits from this service greatly outweigh the risks. Being able to use global and custom banned passwords lists, for both the cloud and on-premises, is a tremendous benefit.
- Forward all M365 unified audit logs and Azure logs to a SIEM and build detections.
  - Ensure you are forwarding the logs recommended in this post and building the appropriate detections and playbooks within your security operations teams.
  - Specifically monitor for:
    - Set-AcceptedDomain
    - Set-MsolDomainFederationSettings
    - Add-FederatedDomain
    - New-Accepted Domain
    - Remove-Accepted Domain
    - Remove-FederatedDomain
- Periodically review all identity providers and custom domains configured in the M365 tenant.
  - If an attacker is successful at gaining global administrative privileges, they may choose to add their own identity provider and custom domain to maintain persistence.

Acknowledgements

I want to give a special thanks to Daniel Taylor, Roberto Bamberger and Jennifer Kendall at Microsoft for collaborating with Mandiant on the creation of this blog post.

PREVIOUS POST

NEXT POST

Awards and Honors
Email Preferences

Technical Support
Incident?
Report Security Issue
Contact Support
Customer Portal
Communities
Documentation Portal

Site Language
English