Welcome

Sean Metcalf
CTO, Trimarc

Agenda

• Attacking Active Directory
• The Most Common AD Security Issues
• Attacking & Defending Office 365/Azure AD
Attacking Active Directory
Attackers Require...

- Account (credentials)
- Rights (privileges)
- Access (connectivity to resources)

Attacker Capability Depends on the Defender...
Traditional AD Administration

- All admins are Domain Admins.
- Administration from anywhere – servers, workstations, Starbucks.
- Need a service account with AD rights – Domain Admin!
- Need to manage user accounts – Account Operators!
- Need to run backups (anywhere) – Backup Operators!
- Management system deploys software & patches all workstations, servers, & Domain Controllers.
- Agents, everywhere!

- Full Compromise… Likely
As an Attacker, Do I Need Domain Admin?

No.
Avenues to Compromise

• GPO permissions
  – Modify a GPO to own everything that applies it

• AD Permissions
  – Delegation a decade ago is still in place, so are the groups

• Improper group nesting
  – Group inception = innocuous groups with super powers

• Over-permissioned accounts
  – Regular users are admins

• Service account access
  – Domain Admins (of course!)

• Kerberos Delegation
  – Who really knows what this means?

• Password Vaults
  – Management issues (user accounts with admin rights, improper protection of server, etc)

• Backup Process
  – What servers backup Active Directory? How is this backup data protected?
In the Real World, Rights are Everywhere

• Workstation Admins have full control on workstation computer objects and local admin rights.

• Server Admins have full control on server computer objects and local admin rights.

• Often, Server Admins are Exchange Admins.

• Sometimes Server Admins have rights to Domain Controllers.

• Help Desk Admins have local admin rights and remote control on user workstations.

• Local admin accounts & passwords often the same among workstations, and sometimes the same among servers.

• “Temporary” admin group assignments often become permanent.
3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights
- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights
3rd Party Product Permission Requirements

- **Domain** user access
- **Operations** systems access
- **Mistaken** identity – trust the installer
- **AD** object rights
- **Install** permissions on systems
- **Needs** System rights

- **Active Directory** privileged rights
- **Domain** permissions during install
- **More** access required than often needed.
- **Initial** start/run permissions
- **Needs** full AD rights
Over-permissioned Delegation

• Use of built-in groups for delegation
• Clicking the "easy button": Full Control at the domain root.
• Let's just "make it work"
• Delegation tools in AD are challenging to get right
Reviewing Active Directory Permissions

- PowerShell for OU Permission Report:

- ACLight (Batch file that calls PowerShell):
  - https://github.com/cyberark/ACLight

- Bloodhound:
  - https://github.com/BloodHoundAD/BloodHound
Common AD Security Issues

We find really interesting things…
Local Administrator Passwords Not Managed on Workstations or Servers

• Workstation build usually sets the standard organization Administrator password.

• Compromise one workstation to compromise them all

Mitigation: Ensure local Administrator passwords regularly change on workstations and servers (using something like Microsoft LAPS).
# Domain Password Policy

## Account Policies/Password Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>7 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
## Domain Password Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>8 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
# Domain Password Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>10 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Set to at least 12 characters, preferably 15.

At least use Fine-Grained Password Policies for Admins & Service Accounts
Regular Users in AD Admin Groups

• User account is a member of Administrators, Domain Admins, or nested group.

Administrators Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Active Directory Domain Services Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Admins</td>
<td>trimarcresearch.com/Users</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>trimarcresearch.com/Users</td>
</tr>
<tr>
<td>Jack Duncan</td>
<td>trimarcresearch.com/Accounts/Users</td>
</tr>
<tr>
<td>trimarcadmin</td>
<td>trimarcresearch.com/Users</td>
</tr>
</tbody>
</table>
No Account Naming Standard

• Security through obscurity?
• Does not fool attackers
• Discovering AD admin accounts is trivial

Mitigation:
• Use designators to clearly identify admin rights:
  – -ada
  – -sa
  – -wa
Account Operators

Account Operators Properties

Members:

Name          Active Directory Domain Services Folder
Ruth Parker   trimarcresearch.com/Administration/Admin Acco...
Account Operators

By default, this built-in group has no members, and it can create and manage users and groups in the domain, including its own membership and that of the Server Operators group. This group is considered a service administrator group because it can modify Server Operators, which in turn can modify domain controller settings. As a best practice, leave the membership of this group empty, and do not use it for any delegated administration. This group cannot be renamed, deleted, or moved.
Admin Group Nesting Issues

---

### Domain Admins Properties

<table>
<thead>
<tr>
<th>Object</th>
<th>Security</th>
<th>Attribute Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Members</td>
<td>Member Of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managed By</td>
</tr>
</tbody>
</table>

**Members:**

- **Name:** ADA Admins
  - **Security:** Active Directory Domain Services Folder
  - **Attribute Editor:** lab.adsecurity.org/AD Management

- **Name:** ADSAAdministrator
  - **Security:** lab.adsecurity.org/Users
  - **Attribute Editor:** lab.adsecurity.org/AD Management

- **Name:** LukeSkywalker
  - **Security:** lab.adsecurity.org/AD Management
  - **Attribute Editor:**

### Critical Server Admins Properties

<table>
<thead>
<tr>
<th>Object</th>
<th>Security</th>
<th>Attribute Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Members</td>
<td>Member Of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managed By</td>
</tr>
</tbody>
</table>

**Members:**

- **Name:** Server Admins
  - **Security:** Active Directory Domain Services Folder
  - **Attribute Editor:** lab.adsecurity.org/AD Management

- **Name:** HanSolo
  - **Security:** lab.adsecurity.org/AD Management
  - **Attribute Editor:**

- **Name:** WesleyCrusher
  - **Security:** lab.adsecurity.org/Accounts
  - **Attribute Editor:**

---

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Default Domain Controllers Policy is.. default

<table>
<thead>
<tr>
<th>Local Policies/Security Options</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Controller</strong></td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Setting</td>
</tr>
<tr>
<td>Domain controller: LDAP server signing requirements</td>
<td>None</td>
</tr>
<tr>
<td><strong>Domain Member</strong></td>
<td>Setting</td>
</tr>
<tr>
<td>Policy</td>
<td>Setting</td>
</tr>
<tr>
<td>Domain member: Digitally encrypt or sign secure channel data (always)</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Microsoft Network Server</strong></td>
<td>Setting</td>
</tr>
<tr>
<td>Policy</td>
<td>Setting</td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign communications (always)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign communications (if client agrees)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
AD Admin Accounts Have Old Passwords.

<table>
<thead>
<tr>
<th>SamAccountName</th>
<th>Enabled</th>
<th>PasswordLastSet</th>
<th>Password Age (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>admAEEdwards</td>
<td>Yes</td>
<td>1/12/2013 2:20:06 PM</td>
<td>6.5</td>
</tr>
<tr>
<td>admBWalker</td>
<td>No</td>
<td>6/11/2017 10:14:08 AM</td>
<td>2.2</td>
</tr>
<tr>
<td>admCGriffin</td>
<td>Yes</td>
<td>3/1/2019 12:41:18 PM</td>
<td>0.4</td>
</tr>
<tr>
<td>AGPMService</td>
<td>Yes</td>
<td>5/3/2009 3:17:32 PM</td>
<td>10.2</td>
</tr>
<tr>
<td>SCCMsvc</td>
<td>Yes</td>
<td>11/14/2011 5:23:12 PM</td>
<td>7.6</td>
</tr>
<tr>
<td>VMWareAdmin</td>
<td>Yes</td>
<td>8/28/2012 10:23:41 AM</td>
<td>7.0</td>
</tr>
<tr>
<td>VulnerabilityScanner</td>
<td>Yes</td>
<td>9/19/2015 4:43:19 PM</td>
<td>3.9</td>
</tr>
</tbody>
</table>
Service Accounts in Domain Admins

- Service Accounts rarely actually need Domain Admin rights
- Better to delegate the required rights for the accounts.

Mitigation:
- Remove from Domain Admins
- Delegate appropriate rights
- Use separate accounts for different tiers:
  - Workstations
  - Servers
  - Domain Controllers
Default Domain Administrator Account SPN

- There is no good reason for admin accounts to have Kerberos SPNs.
- Attack: Kerberoast these accounts to own AD.
Server GPOs Linked to Domain Controllers
Server GPOs Linked to Domain Controllers

Only use GPOs dedicated to Domain Controllers, don’t link GPOs already linked to other OUs.
Modify Rights to GPOs at Domain/DC Level

Only AD Admins should have modify rights on GPOs linked to the Domain/Domain Controllers.
# Domain Permission Delegation Issues

<table>
<thead>
<tr>
<th>Domain</th>
<th>TRDLAB\trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityReference</td>
<td>TRDLAB\Domain Computers</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>Full Control</td>
</tr>
<tr>
<td>ObjectType</td>
<td>user</td>
</tr>
<tr>
<td>InheritedObjectClass</td>
<td>All</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>IsInherited</td>
<td>False</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>TRDLAB\ServerAdmins</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityReference</td>
<td>TRDLAB\ServerAdmins</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>ReadProperty, WriteProperty, ExtendedRight, GenericExecute</td>
</tr>
<tr>
<td>ObjectType</td>
<td>computer</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>All</td>
</tr>
<tr>
<td>IsInherited</td>
<td>False</td>
</tr>
<tr>
<td>ObjectFlags</td>
<td>InheritedObjectAceTypePresent</td>
</tr>
<tr>
<td>InheritanceFlags</td>
<td>ContainerInherit</td>
</tr>
<tr>
<td>PropagationFlags</td>
<td>InheritOnly</td>
</tr>
<tr>
<td>FlaggedForReview</td>
<td>False</td>
</tr>
</tbody>
</table>
# AdminSDHolder Permission Delegation Issues

<table>
<thead>
<tr>
<th>Domain</th>
<th>lab.trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>ObjectDN</td>
<td><code>CN=AdminSDHolder,CN=System,DC=lab,DC=trimarcresearch,DC=com</code></td>
</tr>
<tr>
<td>IdentityReference</td>
<td>TRDPROD\User Admins</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>ReadProperty, WriteProperty, GenericExecute</td>
</tr>
<tr>
<td>InheritedObjectClass</td>
<td>All</td>
</tr>
<tr>
<td>ObjectClass</td>
<td>All</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>IsInherited</td>
<td>False</td>
</tr>
<tr>
<td>ObjectFlags</td>
<td>None</td>
</tr>
<tr>
<td>InheritanceFlags</td>
<td>None</td>
</tr>
<tr>
<td>PropagationFlags</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>prod.trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>ObjectDN</td>
<td><code>CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com</code></td>
</tr>
<tr>
<td>IdentityReference</td>
<td>TRDPROD\User Admins</td>
</tr>
<tr>
<td>ActiveDirectoryRights</td>
<td>ReadProperty, WriteProperty, GenericExecute</td>
</tr>
<tr>
<td>InheritedObjectClass</td>
<td>All</td>
</tr>
<tr>
<td>ObjectClass</td>
<td>All</td>
</tr>
<tr>
<td>AccessControlType</td>
<td>Allow</td>
</tr>
<tr>
<td>IsInherited</td>
<td>False</td>
</tr>
<tr>
<td>ObjectFlags</td>
<td>None</td>
</tr>
<tr>
<td>InheritanceFlags</td>
<td>ContainerInherit</td>
</tr>
<tr>
<td>PropagationFlags</td>
<td>None</td>
</tr>
</tbody>
</table>
Admins Use Regular Workstations for AD Administration

1 workstation
30 accounts in the local Administrators group.
50 accounts w/ local admin via software management system.
20 accounts with control of the computer via security agent(s).

======

~ 100 accounts with effective admin rights on the workstation

How many GPOs apply to the workstation & how many accounts have modify rights?

Who has control of your workstation?
Accounts with Delegated Rights to AD

• Group membership
• AD delegated permissions
• Group Policy delegation
• Group Policy User Rights Assignments (DC GPOs)
Domain Controllers with minimal event auditing

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit object access</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Not Defined</td>
</tr>
</tbody>
</table>

**Policy**

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

**Setting**

Enabled
Kerberos Delegation

• Delegation = Impersonation

• Kerberos Delegation:
  – **Unconstrained**: Impersonate users connecting to service to ANY Kerberos service.
  – **Constrained**: Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
  – **Constrained with Protocol Transition**: Impersonate any user to SPECIFIC Kerberos services on servers. (aka “Kerberos Magic”)
  – **Resource-based Constrained Delegation**: Enables delegation configured on the resource instead of the account.
Kerberos Delegation

• Delegation = Impersonation

• Kerberos Delegation:
  – **Unconstrained:**
    Impersonate users connecting to service to ANY Kerberos service.
  – **Constrained:**
    Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
  – **Constrained with Protocol Transition:**
    Impersonate any user to SPECIFIC Kerberos services on servers. (aka “Kerberos Magic”)
  – **Resource-based Constrained Delegation:**
    Enables delegation configured on the resource instead of the account.

*Account is sensitive and cannot be delegated*
Cross-Forest Administration

Forest A

Trust

Forest B

RDP

Result:
Full Compromise of the Production Active Directory

Forest A Domain Admin Account
Cross-Forest Administration

- Production \(\leftarrow\) one-way \(\rightarrow\) trust \(\rightarrow\) External
- Production forest AD admins manage the External forest.
- External forest administration is done via RDP.
- Production forest admin creds end up on systems in the External forest.
- Attacker compromises External to compromise Production AD.

Mitigation:
- Manage External forest with External admin accounts.
- Use non-privileged Production forest accounts with External admin rights.
The Cloud Is Magic!
From On-Premises to Cloud

- Server
- Domain
- Domain Admin
- Pass the Hash
- Private IPs
- RDP / SSH
- Services
- Subscription
- Subscription Admin
- Credential Pivot
- Public IPs
- Management APIs

Faust and Johnson – Cloud Post Exploitation Techniques Infiltrate 2017 https://vimeo.com/214855977
Cloud Challenges

• Security controls: On-prem vs cloud
• Cloud environment is constantly changing.
• Rapid changes often mean learning curve is steeper.
• Security capability and best practices depend on Cloud service offering.
• Sharing data appropriately and securely.
• Services & data that’s private vs public isn’t always obvious.
“I’m going to migrate my on-prem Active Directory to Azure AD”

It doesn’t quite work like that…
Active Directory vs Azure AD

**On-premises Active Directory**
- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
  - Kerberos
  - NTLM
- LDAP
- Group Policy

**Azure AD (Office 365)**
- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
  - OAuth/OpenID Connect based protocols
- AD Graph API (REST API)
- MDM (InTune)
On-Prem: AD to Cloud Sync

• AD provides Single Sign On (SSO) to cloud services.
• Most organizations aren’t aware of all cloud services active in their environment.
• Some directory sync tools synchronizes all users & attributes to cloud services.
• Most sync engines only require AD user rights to send user and group information to cloud service.
• If you have Office 365, you almost certainly have Azure AD Connect synchronizing on-prem AD user to Azure AD.
On-Prem: AD to Cloud Sync Examples

- **Adobe** User Sync tool
- **Atlassian** Active Directory Attributes Sync
- **Dropbox** Active Directory Connector
- **Duo** Directory Sync
- **Envoy** Active Directory integration (PowerShell)
- **Google** Cloud Directory Sync
- **Facebook** Workplace Active Directory Sync
- **Forcepoint** (Websense) Directory Synchronization Client
- **Mimecast** Directory Sync Tool
- **Proofpoint** Essentials AD Sync Tool
- **Rackspace** Directory Sync (syncs passwords too!)
- **Zoom** AD Sync to Zoom
Attacking On-Prem Cloud Integration

Permissions for the created AD DS account for express settings

The **account** created for reading and writing to AD DS have the following permissions when created by express settings:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>
### On-Prem: Acme’s Azure AD Connect

```powershell
PS C:\> get-aduser -filter {samaccountname -like "MSOL*"}
-prop DistinguishedName,description | fl *
```

<table>
<thead>
<tr>
<th>Description</th>
<th>Account created by the Windows Azure Active Directory Sync tool with installation 'trd977930921' running on computer 'AZURESYNC' configured to synchronize to tenant 'theacmeio.onmicrosoft.com'. This account must have directory replication permission in Azure Directory and write permission on certain attributes to enable Hybrid Deployment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DistinguishedName</td>
<td>CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io</td>
</tr>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>GivenName</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>MSOL_trd977930921</td>
</tr>
<tr>
<td>ObjectClass</td>
<td>user</td>
</tr>
<tr>
<td>ObjectGUID</td>
<td>cdcb6dd0-65e2-40bc-bc60-461408831036</td>
</tr>
<tr>
<td>SamAccountName</td>
<td>MSOL_trd977930921</td>
</tr>
<tr>
<td>SID</td>
<td>S-1-5-21-143179592-3749324205-2095737646-1138</td>
</tr>
</tbody>
</table>
On-Prem: Acme’s Azure AD Connect
On-Prem: Acme’s Azure AD Connect

PS C:\> get-aduser -filter {samaccountname -like "MSOL*"} -prop DistinguishedName,description | fl *

Description : Account created by the Windows Azure Active Directory Sync service 'trd977930921' running on computer 'AZURESYNC' configured in 'theacmeio.onmicrosoft.com'. This account must have directory and write permission on certain attributes to ensure correct synchronisation.

DistinguishedName : CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io
Enabled : True
GivenName :

PS C:\> get-adcomputer AzureSync

DistinguishedName : CN=AZURESYNC,OU=Servers,DC=theacme,DC=io
DNSHostName :
Enabled : True
Name : AZURESYNC
ObjectClass : computer
ObjectGUID : 42f88cbe-c51f-4f5c-9059-58d3449a7a30

On-Prem: Acme’s Azure AD Connect

```powershell
PS C:\> Find-GPOComputerAdmin -OUName 'OU=Servers,DC=theacme,DC=io'

ComputerName : 
ObjectName : ServerAdmins
ObjectDN : **CN=Server Admins,OU=Groups,DC=theacme,DC=io**
ObjectSID : S-1-5-21-143179592-3749324205-2095737646-1103
IsGroup : True
GPODisplayName : Server Baseline Policy
GPOGuid : {002404EA-6ACB-495D-97E6-2AEC89ED91A8}
GPOPath : `\theacme.io\SysVol\theacme.io\Policies\{002404EA-6ACB-495D-97E6-2AEC89ED91A8\}
GPOType : GroupPolicyPreferences
```
On-Prem: Acme’s Azure AD Connect
On-Prem: Acme’s Azure AD Connect Scenario

• Azure AD Connect service account is granted password hash sync rights.

• AAD Connect runs on “AzureSync” which is in the Servers OU.

• The Servers OU has 2 GPOs applied:
  • “Server Baseline Policy” GPO adds the Server Admins group (in the Groups OU).
  • “Server Config” GPO has 3 Server Tier groups with modify rights.

Attack Options:

• Compromise account that is a member of the Server Admins group or any of the Server Tier groups.

• Compromise account delegated rights to modify groups in the Groups OU.
OnPrem Sync Defense

• You may have sync engines other than AAD Connect…

• Protect any sync engine server that handles AD password data like a Domain Controller (Tier 0).

• Protect any associated service account like it’s a Domain Admin account.

• Ensure only AD admins manage these systems.
AD Recon vs Azure AD Recon

On-Prem AD:
– AD user can enumerate all user accounts & admin group membership with network access to a Domain Controller.

Azure AD:
• Azure AD user can enumerate all user accounts & admin group membership with access to Office 365 services (the internet by default).
• User enumeration* often possible without an account!
Azure AD User Enumeration

• Office 365 Authentication Page (Python) [Account Discovery]
  – https://github.com/LMGsec/o365creeper

• OWA (Golang)
  – https://github.com/busterb/msmailprobe

• ActiveSync (Python)
  – https://bitbucket.org/grimhacker/office365userenum/src

• MSOnline/AzureAD PowerShell Module (PowerShell)
  – https://github.com/nyxgeek/o365recon
Password Spraying Overview

“Winter2018”

Sleep x seconds/minutes

“Spring2019”

No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.
No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.
Password Spraying Overview

- Ruler (Exchange) [Golang]

- SprayingToolkit (Lync/Skype for Business/OWA) [Python]
  - https://github.com/byt3bl33d3r/SprayingToolkit

- LyncSniper (Lync/Skype for Business) [PowerShell]
  - https://github.com/mdsecresearch/LyncSniper

- MailSniper (OWA/EWS) [PowerShell]
  - https://github.com/dafthack/MailSniper

Legacy Authentication enables O365 Password Spraying

Legacy = Outlook =<2010, POP, IMAP, SMTP, etc
Attacking the Cloud: Password Spraying

Password Spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx. Sit tight... 5 threads remaining

[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:01:04
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:01:35
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User: theacme.io\thrawn@theacme.io Password: Summer2019!
[*] A total of 1 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:01:58
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:02:21
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Results have been written to C:\temp\owa-sprayed-creds.txt.
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 08/02/2019 04:02:44
[*] Trying Exchange version Exchange2010
[*] A total of 0 credentials were obtained.
Attacking the Cloud: Password Spraying

Results have been written to C:\temp\owa-sprayed-creds.txt

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
Current date and time: 08/02/2019 04:01:35
Trying Exchange version Exchange2010
SUCCESS! User: theacme.io\thrawn@theacme.io Password:Summer2019!
A total of 1 credentials were obtained.

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
Current date and time: 08/02/2019 04:04:26
Trying Exchange version Exchange2010
SUCCESS! User: theacme.io\obiwan@theacme.io Password:TheForce19
A total of 1 credentials were obtained.

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
Current date and time: 08/02/2019 04:04:03
Trying Exchange version Exchange2010
SUCCESS! User: theacme.io\bobbafett@theacme.io Password:Mandalorian19!
A total of 1 credentials were obtained.

Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
Current date and time: 08/02/2019 04:05:34
Trying Exchange version Exchange2010
SUCCESS! User: theacme.io\bailey@theacme.io Password:Password1
A total of 1 credentials were obtained.

Results have been written to C:\temp\owa-sprayed-creds.txt.
Detecting Password Spraying

Microsoft:
“Nearly 100% of password spray attacks are using legacy authentication.”

Azure AD Sign-in Logs require Azure AD Premium (P1 or P2)

Access denied

You do not have access

To see sign-in data, upgrade your organization’s subscription to include Azure AD Premium. License status: Azure AD Free

Start a free Premium Trial

Soon…
Detecting Password Spraying

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Name</th>
<th>Application</th>
<th>Status</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/1/2019, 9:09:12 PM</td>
<td>Thrawn</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:11 PM</td>
<td>Qui-Gon Jinn</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:11 PM</td>
<td>Lando Calrissian</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:07 PM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>obi-wan Kenobi</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>leia</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>Rey</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:06 PM</td>
<td>kylo</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:01 PM</td>
<td>Padme Amidala</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:01 PM</td>
<td>Bailey</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:00 PM</td>
<td>Han Solo</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:09:00 PM</td>
<td>Adm Ackbar</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
<tr>
<td>8/1/2019, 9:08:53 PM</td>
<td>Finn</td>
<td>Office 365 Exchange On...</td>
<td>Failure</td>
<td>52.168.138.234</td>
</tr>
</tbody>
</table>

*Azure AD Sign-in Logs require Azure AD Premium (P1 or P2)
Detecting Password Spraying

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>User</th>
<th>Application</th>
<th>Result</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/2/2019, 12:02:06 AM</td>
<td>Boba Fett</td>
<td>Office 365 Exchange Online</td>
<td>Failure</td>
<td>52.168.138.234</td>
<td>Not Applied</td>
</tr>
</tbody>
</table>

*Azure AD Sign-in Logs require Azure AD Premium (P1 or P2)*
Detecting Password Spraying

<table>
<thead>
<tr>
<th>Basic info</th>
<th>Device info</th>
<th>MFA info</th>
<th>Conditional Access</th>
<th>Troubleshooting and support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request ID</td>
<td>8e270d9b-9dc4-41c5-9273-e69395680400</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correlation ID</td>
<td>94558595-8ecc-484b-b7a6-6eaaa3e9d74e</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Boba Fett</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>5688de1a-10ec-4b5c-b98d-73cff3c2e7f0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Office 365 Exchange Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application ID</td>
<td>000000002-0000-0ff1-ce00-000000000000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>52.168.138.234</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Washington, Virginia, US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>8/2/2019, 12:02:06 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sign-in error code</td>
<td>50126</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure reason</td>
<td>Invalid username or password or Invalid on-premise username or password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client app</td>
<td>Other clients; Older Office clients</td>
<td>Other clients; Older Office clients</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sign-in error code 50126

Failure reason Invalid username or password or Invalid on-premise username or password

Client app Other clients; Older Office clients

Legacy Authentication
Password Spraying Defense

• Disable Legacy Authentication (Especially if this is a new tenant!)
  • Baseline Policy: Disable Legacy Authentication
  • Conditional Access

• Enforce MFA for admins
  • Baseline Policy: Require MFA for admins (preview)
  • Conditional Access

• Disable service access for users
  • Configure on each user’s mailbox config
  • Exchange authentication policy
Password Spraying Defense (ADFS)

• Enable Smart Lockout (2012R2/2016)
• Block Legacy Authentication with ADFS Authorization rules
• Install Azure AD Connect Health with ADFS on ADFS servers
  • Alerts about common ADFS issues (cert expiring, missing updates, performance, etc)
  • Will also alert on bad Password Attempts and Risky IPs!

<table>
<thead>
<tr>
<th>TIMESTAMP</th>
<th>TRIGGER TYPE</th>
<th>IP ADDRESS</th>
<th>BAD PASSWORD ERROR COUNT</th>
<th>EXTRANET LOCKOUT ERROR COUNT</th>
<th>UNIQUE USERS ATTEMPTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/28/2018 6:00 PM</td>
<td>hour</td>
<td>104.208.238.9</td>
<td>0</td>
<td>284</td>
<td>14</td>
</tr>
<tr>
<td>2/28/2018 6:00 PM</td>
<td>hour</td>
<td>104.44.252.135</td>
<td>0</td>
<td>27</td>
<td>1</td>
</tr>
<tr>
<td>2/28/2018 6:00 PM</td>
<td>hour</td>
<td>168.61.144.85</td>
<td>0</td>
<td>164</td>
<td>2</td>
</tr>
</tbody>
</table>
Password Spraying Defense: Azure AD Password Protection

- **Requirements**
  - Azure AD Premium (P1)
  - DCs need to be 2012 or later
  - No Domain or Forest functional level requirement
  - Sysvol needs to be using DFSR ([http://aka.ms/dfsrmig](http://aka.ms/dfsrmig))

- **Deploy in Audit Mode first**

- **Passwords are fuzzy matched, substring matched & scored. Must be 5 or higher**

- **After passwords have been changed, look to extend password age**
From On-Prem to Cloud Administration
## Attacking Cloud Administration

### Global administrator - Assignments

<table>
<thead>
<tr>
<th>NAME</th>
<th>USERNAME</th>
<th>TYPE</th>
<th>SCOPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sean Metcalf</td>
<td><a href="mailto:sean@theacme.io.onmicrosoft.com">sean@theacme.io.onmicrosoft.com</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Mark Morowczynski</td>
<td><a href="mailto:mark@theacme.io">mark@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Sean Metcalf</td>
<td><a href="mailto:seanmetcalf@theacme.io">seanmetcalf@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Han Solo</td>
<td><a href="mailto:hansolo@theacme.io">hansolo@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Boba Fett</td>
<td>SUCCESS! User:theacme.io\<a href="mailto:bobafett@theacme.io">bobafett@theacme.io</a> Password:Mandalorian19!</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mace Windu</td>
<td><a href="mailto:mace@theacme.io">mace@theacme.io</a></td>
<td>User</td>
<td>Directory</td>
</tr>
<tr>
<td>Thrawn</td>
<td>SUCCESS! User:theacme.io\<a href="mailto:thrawn@theacme.io">thrawn@theacme.io</a> Password:Summer2019!</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attacking Cloud Administration

Global Reader

From Global Admin to **Global Reader**

- Currently in Private Preview
- Provides read access to O365 services that Global Admin can read/write.
- Enables accounts that “required” Global Admin to be switched to read-only.
- Global Reader read-only access is still being expanded to cover all O365 services.

Cloud Administration – Finding a Weakness

Workstation

Web Browser

(DNS)

HTTP(S)

Cloud Website
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft
Attacking Cloud Administration: Token Theft
Protect Cloud Admin Accounts

According to Microsoft (as of August 2019):

Admin Accounts with MFA: 7.94%!
Protect Cloud Admin Accounts

• Anyone with elevated rights to cloud services (i.e. “admin”) needs to have an account just for Cloud Administration.

• Good: Turn MFA on!

• Better: Conditional Access or Baseline Policy for Admins (Public Preview)
  • Will change based on feedback
  • Learn more at: https://aka.ms/aadbaseline

• Best: Azure AD Privilege Identity Management
  • No standing admin access
  • Admin access requires elevation + MFA
  • Approval workflows and elevation scheduling
  • Alerts on admin activity taking place outside of PIM
  • Applies/Protect Azure Resources as well!
  • Can buy Azure AD P2 license for just your admins
  • https://aka.ms/deploymentplans
Protect Cloud Administration

• Isolate Cloud Administration to special systems:
  • Cloud Admin Server
  • Cloud VDI
  • Cloud Admin Workstation

• Ensure SSL/TLS decryption devices whitelist all cloud admin URLs & are well protected (Tier 0).
Password Reuse/Replay

Our team is currently looking into reports of stolen passwords. Stay tuned for more.

112. Han Solo hansolo LeiaIKnow19! hansolo@theacme.io
113. Luke Skywalker lukeskywalker TheForce19 lukeskywalker@Plus.com
Password Reuse/Replay Detection

Password Hash (of the AD Hash) Sync Enabled: Users with Leaked Credential

Havel Been Pwned.com

Check if you have an account that has been compromised in a data breach

- Domain name: enter the domain you’d like to search
- Subscribe me:
- Notification email: enter your email address

Risk level: High
Detection type: Offline
Risk event type: Users with leaked credentials
Risk events closed: 2 of 2
Turn on Azure AD Connect Password Hash Sync

• Leaked Credential Reporting
  • Dark Web, Law Enforcement, and Security Researchers

• When something catastrophic happens
  • WannaCry, NotPetya

• Understand How Password Hash Sync Works
  • http://aka.ms/aadphs

• After enabling will see “NEW” leaks going forward
  • Don’t “leak” one yourself “just to make sure it’s working”
Attacking the Cloud: App PrivEsc & Persistence

• Illicit Consent Grant Attack (OAuth Espionage)
  • Users fooled into granting permissions to an app that looks like a familiar app.
  • FireEye PwnAuth
• MDSec Office 365 Toolkit
  • https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/

• Overprivileged Enterprise Apps with broad permissions.
Illicit Consent Grant Attack: MDSec O365 Attack Toolkit

https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/
Illicit Consent Grant Attack: Pawn Storm

Enterprise App Permissions

• Enterprise App (tenant-wide) permissions can be granted by Admins.

• Ideal persistence technique since app permissions not reviewed like group membership.
Enterprise App Permissions

This app would like to:

- Read and write all applications
- Read and write directory data
- Use Exchange Web Services with full access to all mailboxes
- Read and write calendars in all mailboxes
- Read and write contacts in all mailboxes
- Read and write all user mailbox settings
- Read and write mail in all mailboxes
- Send mail as any user
- Read all users' full profiles
- Sign in and read user profile

Awesome Notes

needs access to

- Contacts
- Location
- Microphone

Google play

ACCEPT
App Attack Detection & Defense

• Provide training to users around App Consent.
• Regularly review app permissions:
  • Admin Consent
  • User Consent
• Use PowerShell!

Get-AzureADPSPermissions.ps1
https://gist.github.com/pignore/t/41793f8c6211d2df5051d77ca3728c09
O365 Phase 1 Go Do Right Now Checklist

- Require MFA for all cloud admin accounts.
- Configure PIM for all cloud admin accounts
- Enable “Password Hash Sync” (Azure AD Connect).
- Ensure all apps use Modern Authentication (ADAL) to connect to Office 365 services.
- Enable user and admin activity logging in Office 365 (UnifiedAuditLogIngestionEnabled).
- Enable mailbox activity auditing on all O365 mailboxes.
- Conditional Access: Block Legacy Auth (for those that are not using it today!).
- Integrate Azure AD Logs with your SIEM or use Azure Log Analytics or Azure Sentinel
- Deploy Azure AD Banned Password for your on-prem AD
- Enable Azure AD Connect Health for ADFS and ADFS Smart Lockout
- Ensure all users are registered for MFA.
O365 Phase 2 Go Do Soon Security Checklist

- Enable self-service password reset (SSPR).
- Enable MFA for all users via Conditional Access or Risk Based.
- Disable Legacy Authentication Entirely via Conditional Access
- FIDO for admin accounts
- Follow admin account best practices for cloud admins
- Audit consented permissions for apps & user access to apps.
- Review App Permissions
- Monitor App registrations.
- Review the recommendations in Microsoft Secure Score and implement as many as possible.
Traditional AD Administration must evolve with the threats to effectively protect Active Directory.

Most organizations have done "something" to better secure their environment, thought it’s often not enough.

Cloud is a new paradigm that requires special attention (& resources).

The cloud isn’t inherently secure.

Security responsibilities are shared between provider and customer.

Security controls need to be researched, tested, and implemented.

Security in the cloud may cost extra.