Defining the Undefined:
What is Tier Zero? – Part 2

Alexander Schmitt, Jonas B. Knudsen, Elad Shamir

Agenda

- Recap
- AD Containers
- GPOs
- Special users
- RODCs

Who is talking about this?

- SpecterOps Research resources with decades of experience abusing and defending access to Tier Zero
- BloodHound Enterprise resources with experience mapping Attack Paths across identities and resources in AD / Azure
- Today's Special: TEAL Consulting with decades of experience defending access to Tier Zero

Recap – Part 1

- History of Tier Zero
- Our definition of Tier Zero:
  Tier Zero is a set of assets in control of enterprise identities and their security dependencies
  - *Control: a relationship that can contribute to compromising the controlled asset or impact its operability.*
- Microsoft’s original list of Tier Zero AD groups

Suggestions From The Community

Suggestions from the community

Domain root object

AdminSDHolder object

krbtgt user account

RID-500 account

OUs

GPOs

Read-Only Domain Controllers

TrustedDomain objects

AAD Connect object(s)

https://github.com/BloodHoundAD/TierZeroTable/issues

Suggestions from the community

Domain root object

AdminSDHolder object

krbtgt user account

RID-500 account

OUs

GPOs

Read-Only Domain Controllers

TrustedDomain objects

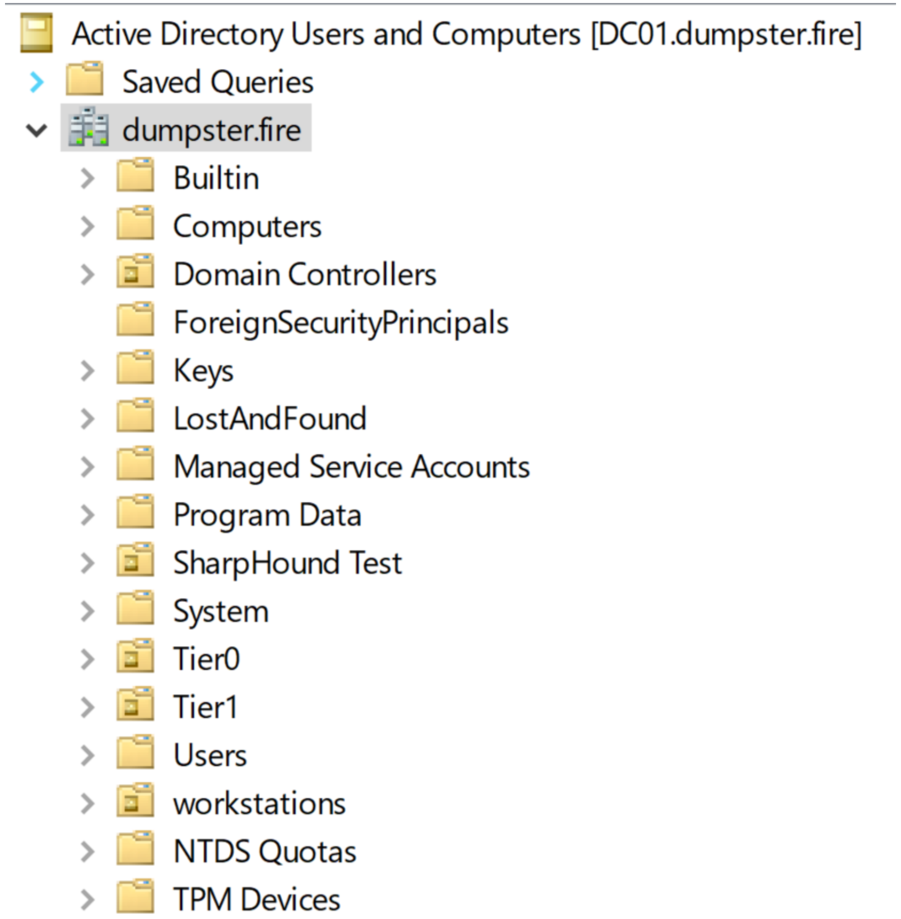
AAD Connect object(s)

https://github.com/BloodHoundAD/TierZeroTable/issues

Included in today's discussion

AD Containers

AD Containers



Active Directory Users and Computers [DC01.dumpster.fire]

- Saved Queries
- dumpster.fire
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Keys
  - LostAndFound
  - Managed Service Accounts
  - Program Data
  - SharpHound Test
  - System
  - Tier0
  - Tier1
  - Users
  - workstations
  - NTDS Quotas
  - TPM Devices

AD Containers

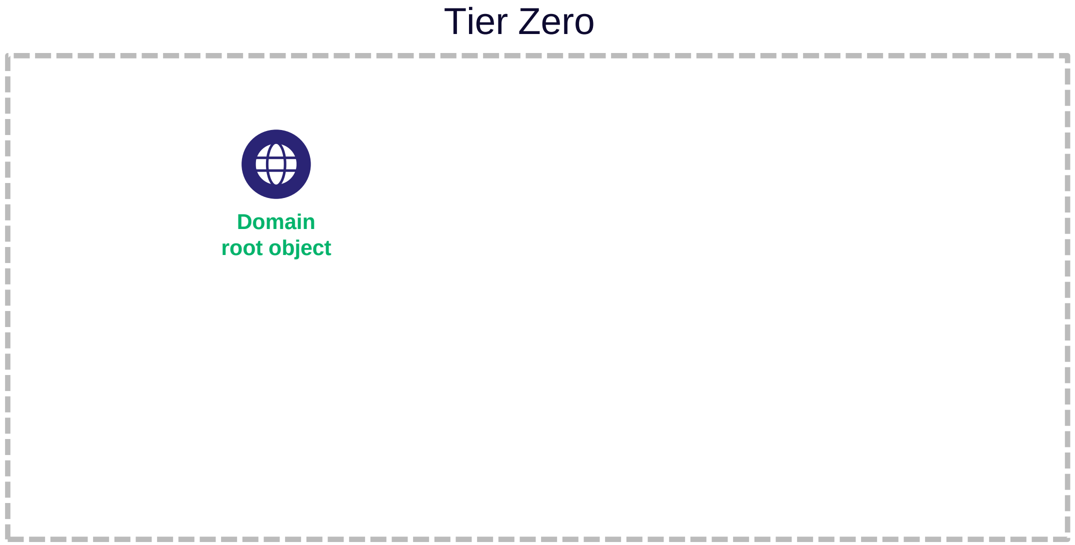
- AD Container is Tier Zero if:
  - Contains one (or more) Tier Zero objects that can be compromised by an attacker with control over the container

AD Containers

- ~~AD Container is Tier Zero if:~~
  - ~~Contains one (or more) Tier Zero objects that can be compromised by an attacker with control over the container~~
- Keep it simple:
  - AD Container is Tier Zero if it contains Tier Zero objects
  - Use the power of naming conventions

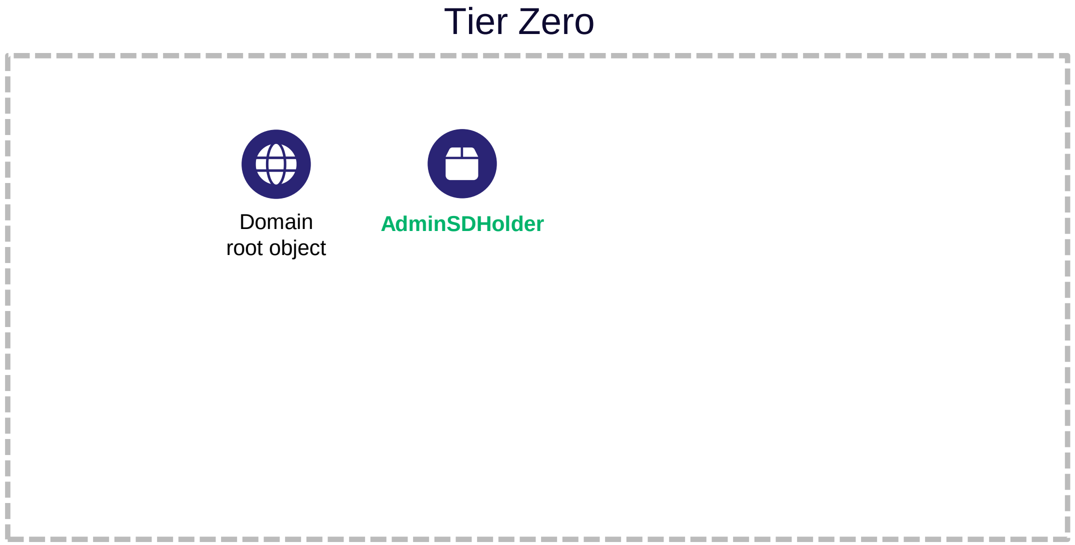
AD Containers

Name	**Domain root object**
Identification	Top object in the Default Naming Context
Description	• Contains all AD objects of the default naming context for the domain
Contains Tier Zero objects?	Yes
Is it Tier Zero?	Yes



AD Containers

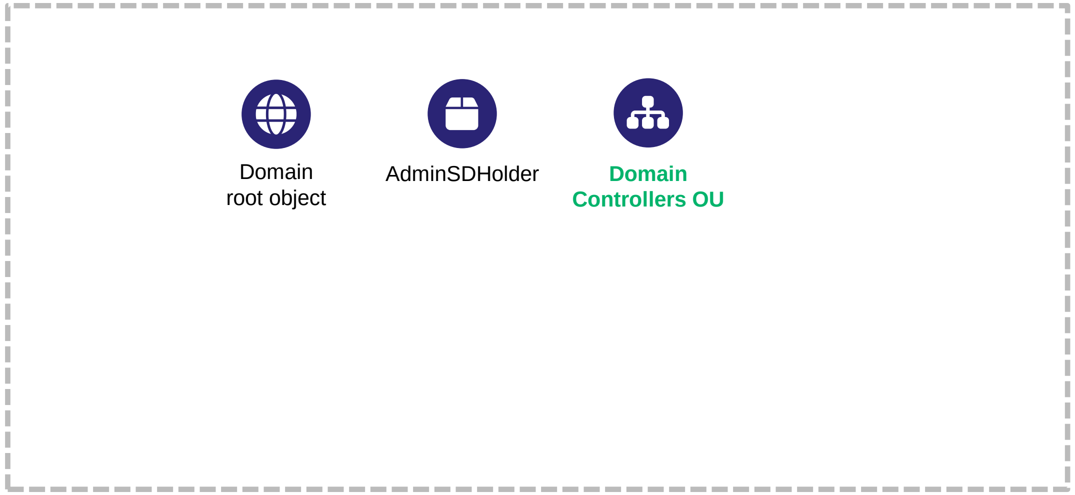
Name	**AdminSDHolder**
Identification	CN=AdminSDHolder,CN=System,<Domain DN>
Description	• Template of permissions for protected principals
Contains Tier Zero objects?	No
Is it Tier Zero?	Yes



AD Containers

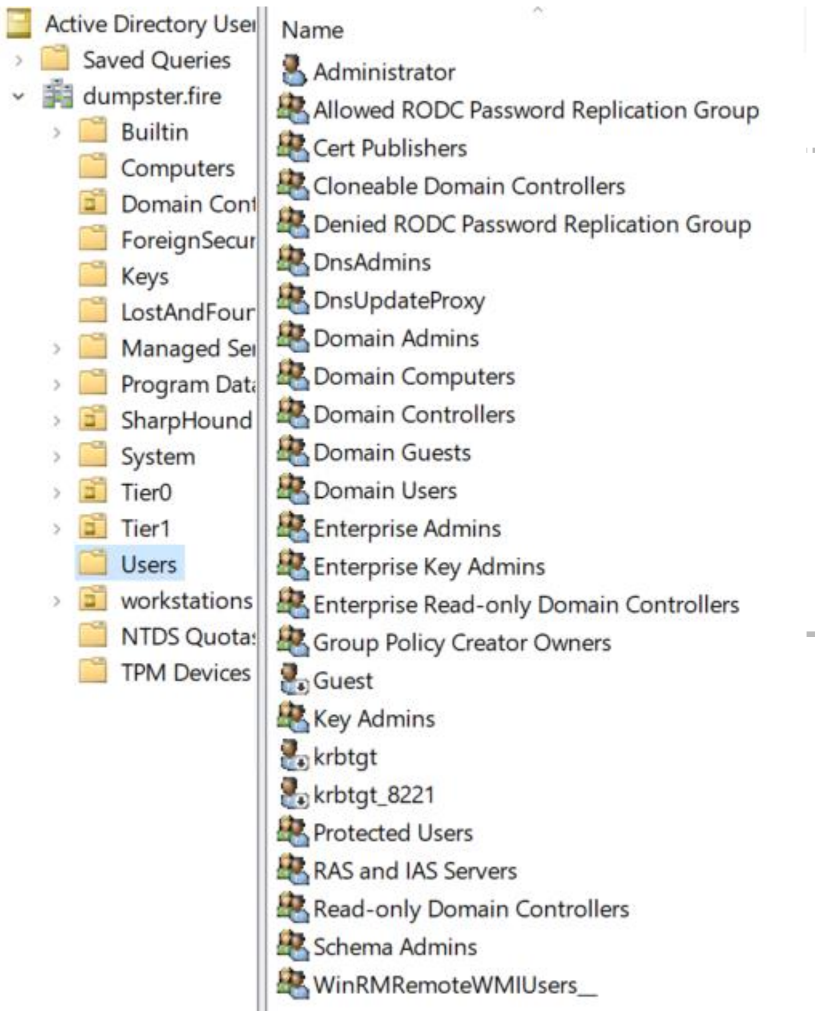
Name	**Domain Controller OU**
Identification	OU=Domain Controllers,<Domain DN>
Description	• Contains the DCs of the domain
Contains Tier Zero objects?	Yes
Is it Tier Zero?	Yes

Tier Zero



AD Containers

Name	**Users container**
Identification	CN=Users,<Domain DN>
Description	• Default location for users • Contains default AD groups
Contains Tier Zero objects?	Yes
Is it Tier Zero?	Yes



Active Directory User
- Saved Queries
- dumpster.fire
  - Builtin
  - Computers
  - Domain Cont
  - ForeignSecur
  - Keys
  - LostAndFour
  - Managed Se
  - Program Dat
  - SharpHound
  - System
  - Tier0
  - Tier1
  - Users
  - workstations
  - NTDS Quota
  - TPM Devices

Name
- Administrator
- Allowed RODC Password Replication Group
- Cert Publishers
- Cloneable Domain Controllers
- Denied RODC Password Replication Group
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Key Admins
- Enterprise Read-only Domain Controllers
- Group Policy Creator Owners
- Guest
- Key Admins
- krbtgt
- krbtgt_8221
- Protected Users
- RAS and IAS Servers
- Read-only Domain Controllers
- Schema Admins
- WinRMRemoteWMIUsers__

Group Policy Objects (GPO)

GPOs

- GPO is Tier Zero if:
  - Linked to a container (Domain, OU, or Site) containing one (or more) Tier Zero users or computers not protected with GPO inheritance

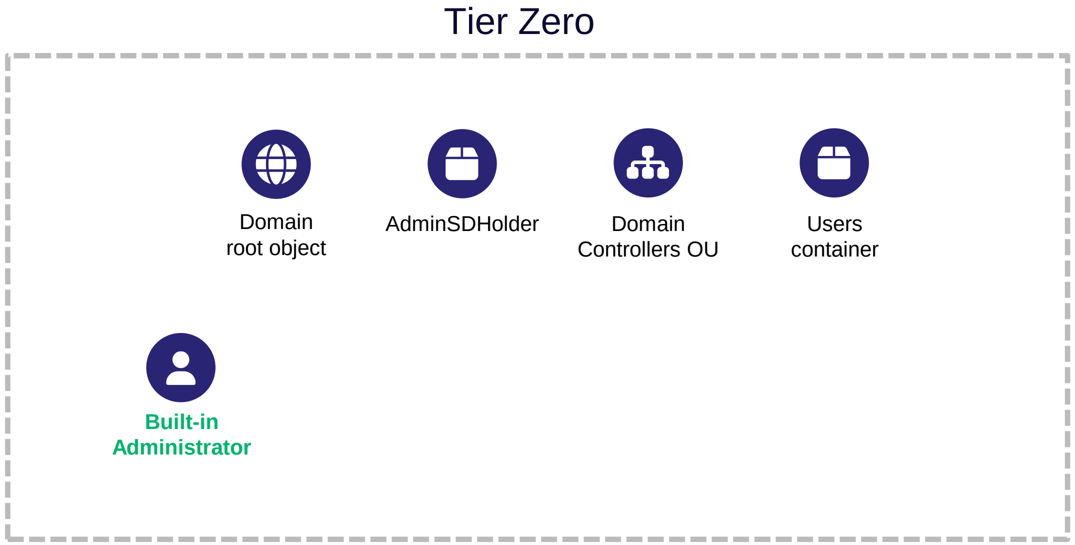
GPOs

- ~~GPO is Tier Zero if:~~
  - ~~Linked to a container (Domain, OU, or Site) containing one (or more) Tier Zero users or computers not protected with GPO inheritance~~
- Keep it simple:
  - GPO is Tier Zero if it is linked to a Tier Zero object (Domain, OU, or Site)
  - Use the power of naming conventions

Special Users

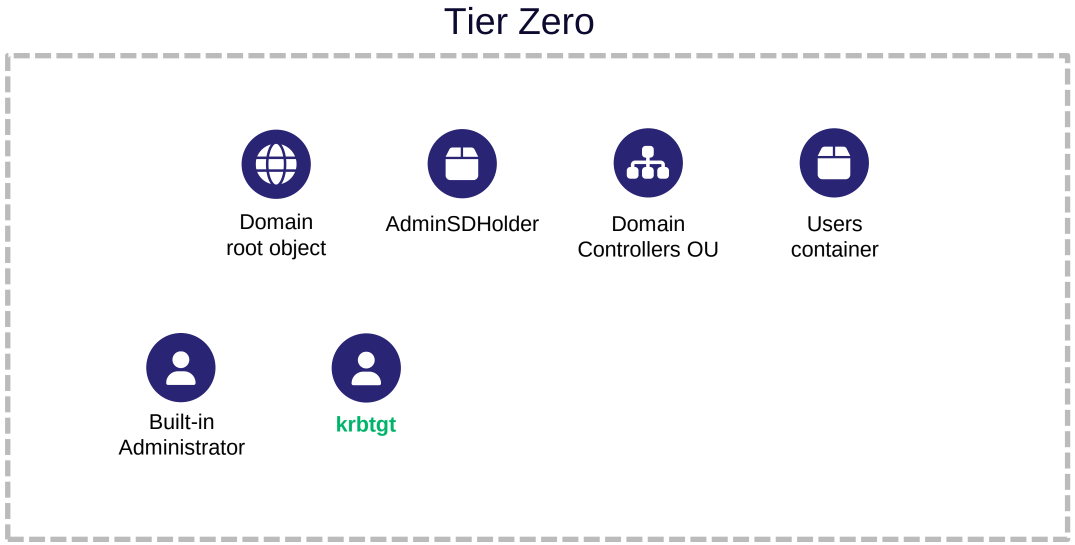
Special users

Name	**Administrator**
Identification	S-1-5-21-<domain>-500
Description	• Built-in Administrator account for domain • Member of Administrators by default
Tier Zero Compromise?	Yes
Is it Tier Zero?	Yes



Special users

Name	**krbtgt**
Identification	S-1-5-21-<domain>-502
Description	• Credentials used for encrypting Kerberos TGTs
Tier Zero Compromise?	Yes
Is it Tier Zero?	Yes



Read-Only Domain Controllers

Read-Only Domain Controllers

- The Read-Only Domain Controller (RODC) is Microsoft’s solution for physical locations that don’t have adequate security to host a domain controller but still require directory services
    - Examples: branch office, retail store, mine site
- Does not have write access to objects
- Has a “filtered” copy of the directory
- Can retrieve the credentials of principals specified in its msDS-RevealOnDemandGroup attribute (allow list) but not of principals specified in its msDS-NeverRevealGroup attribute (deny list)

Read-Only Domain Controllers

The Read-Only Domain Controller can access the credentials of all accounts present in its msDS-RevealOnDemandGroup attribute
and not present in its msDS-NeverRevealGroup attribute

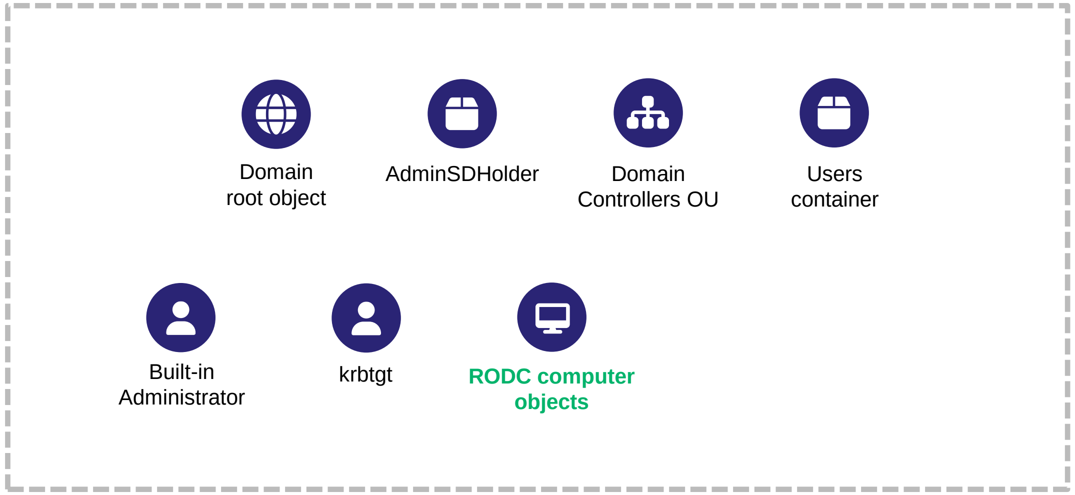
Read-Only Domain Controllers

- Components:
    - RODC Host
    - RODC AD Computer Object
    - RODC krbtgt object
    - RODC-related AD groups
        - Allowed RODC Password Replication Group
        - Denied RODC Password Replication Group
        - Read-only Domain Controllers (covered in Episode 1)
        - Enterprise Read-only Domain Controllers

Read-Only Domain Controllers

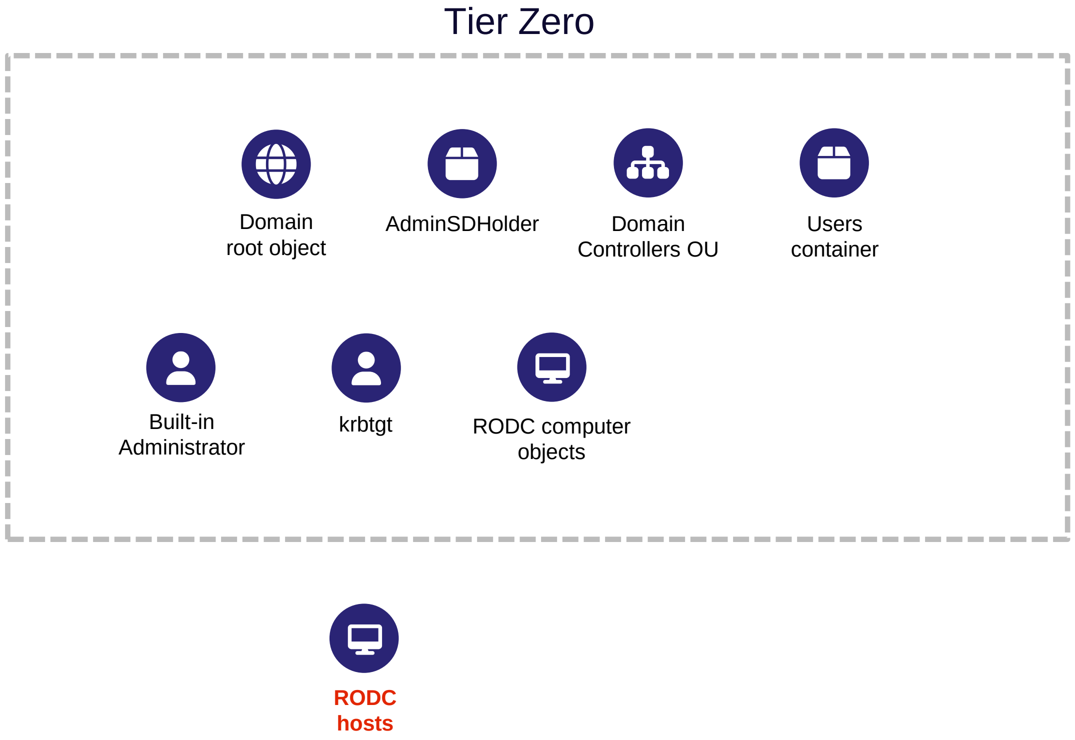
Name	**RODC computer object**
Identification	msDS-isRODC set to True
Description	• The AD computer object of a RODC • Powerful attributes
Tier Zero Compromise?	Yes
Is it Tier Zero?	Yes

Tier Zero



Read-Only Domain Controllers

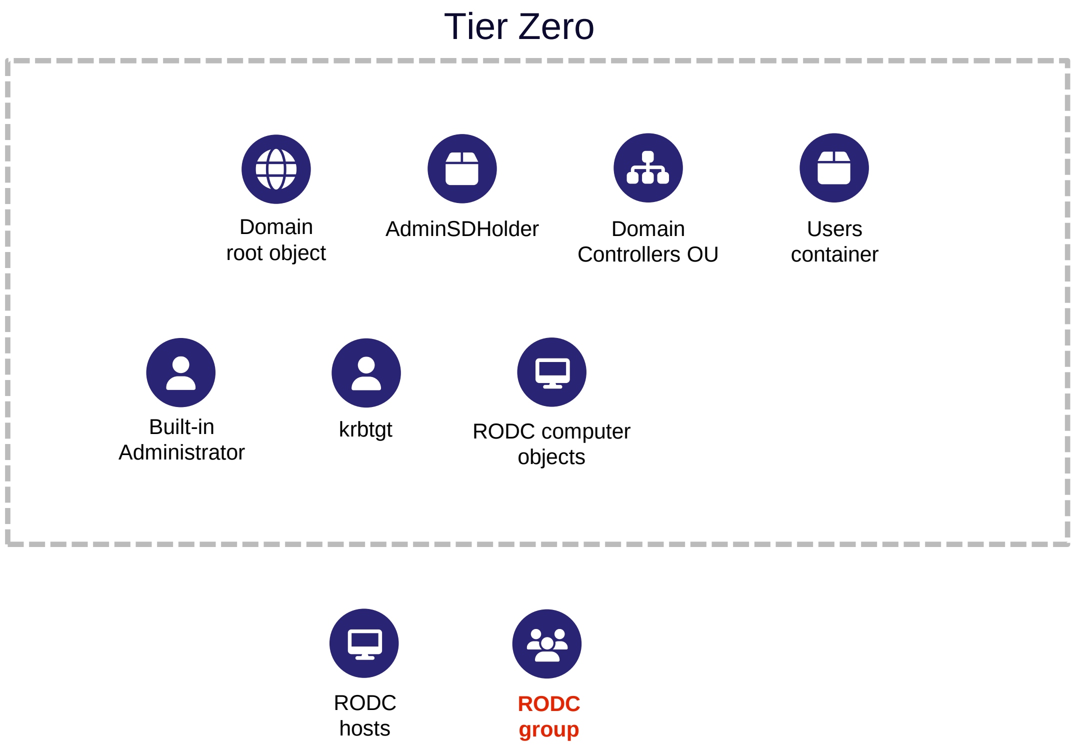
Name	**RODC hosts**
Identification	Not an AD object
Description	- The RODC computer and operating system
Tier Zero Compromise?	No
Is it Tier Zero?	No



Read-Only Domain Controllers

Name	**Read-only Domain Controllers (Group)**
Identification	S-1-5-21-<domain>-521
Description	• RODCs of the domain • No compromising privileges
Tier Zero Compromise?	No
Is it Tier Zero?	No

Covered in Part 1



Tier Zero

Domain root object

AdminSDHolder

Domain Controllers OU

Users container

Built-in Administrator

krbtgt

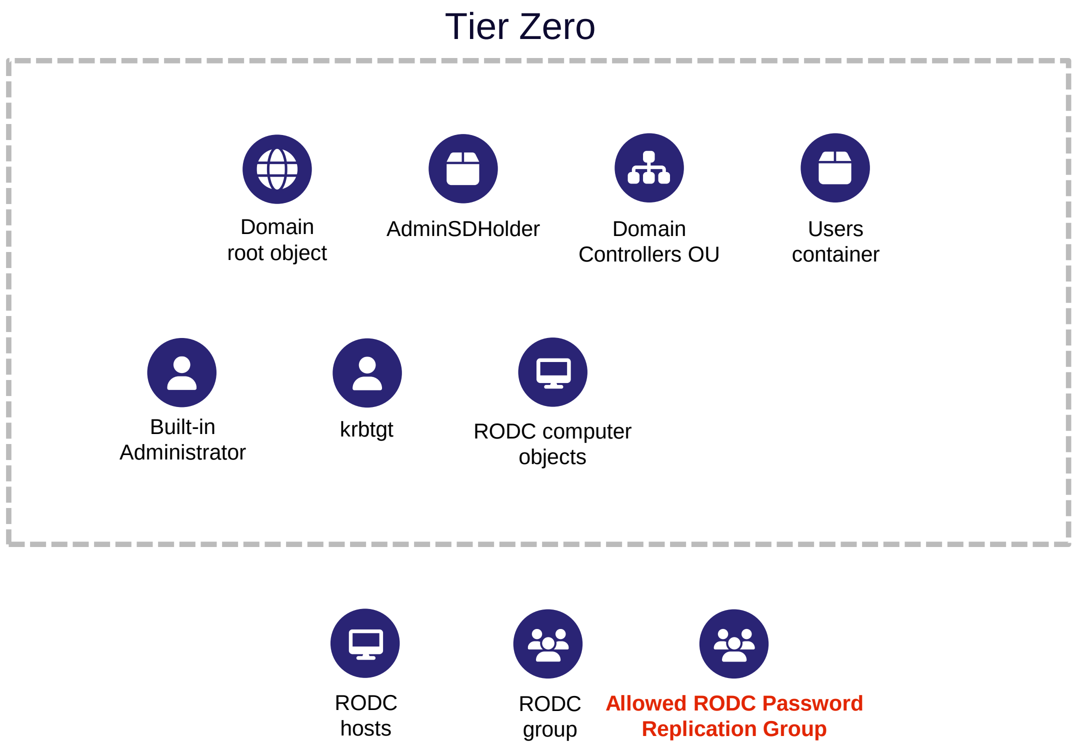
RODC computer objects

RODC hosts

RODC group

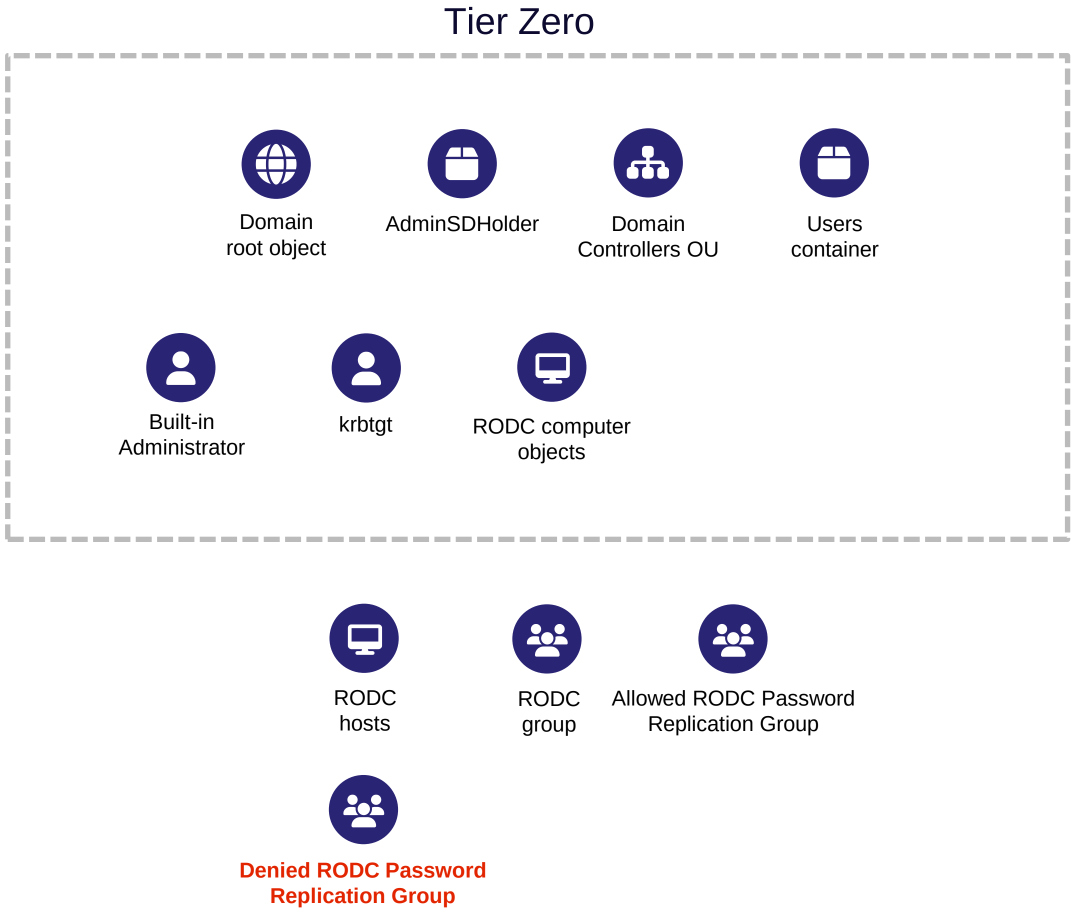
Read-Only Domain Controllers

Name	**Allowed RODC Password Replication Group**
Identification	S-1-5-21-<domain>-571
Description	• Default group for principals that can have their credentials retrieved by RODCs
Tier Zero Compromise?	No
Is it Tier Zero?	No



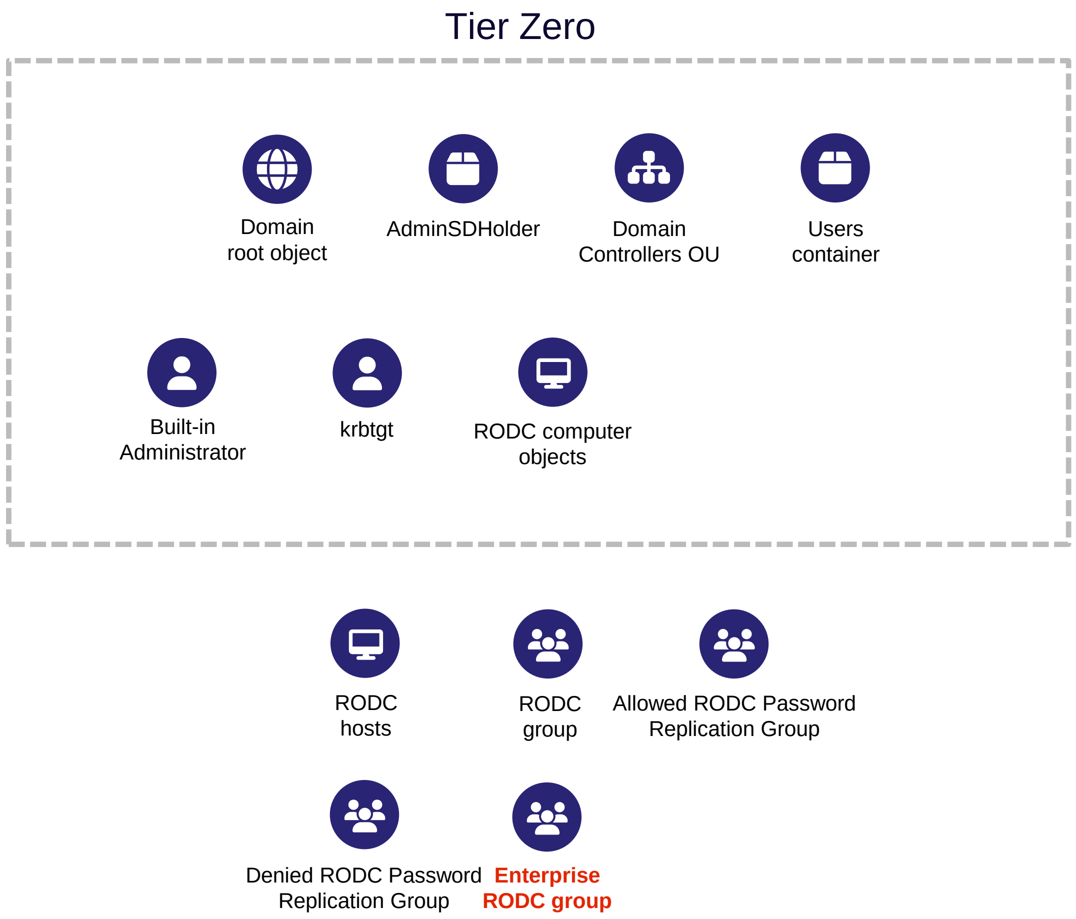
Read-Only Domain Controllers

Name	**Denied RODC Password Replication Group**
Identification	S-1-5-21-<domain>-572
Description	• Default group for principals that **cannot** have their credentials retrieved by RODCs
Tier Zero Compromise?	No
Is it Tier Zero?	No



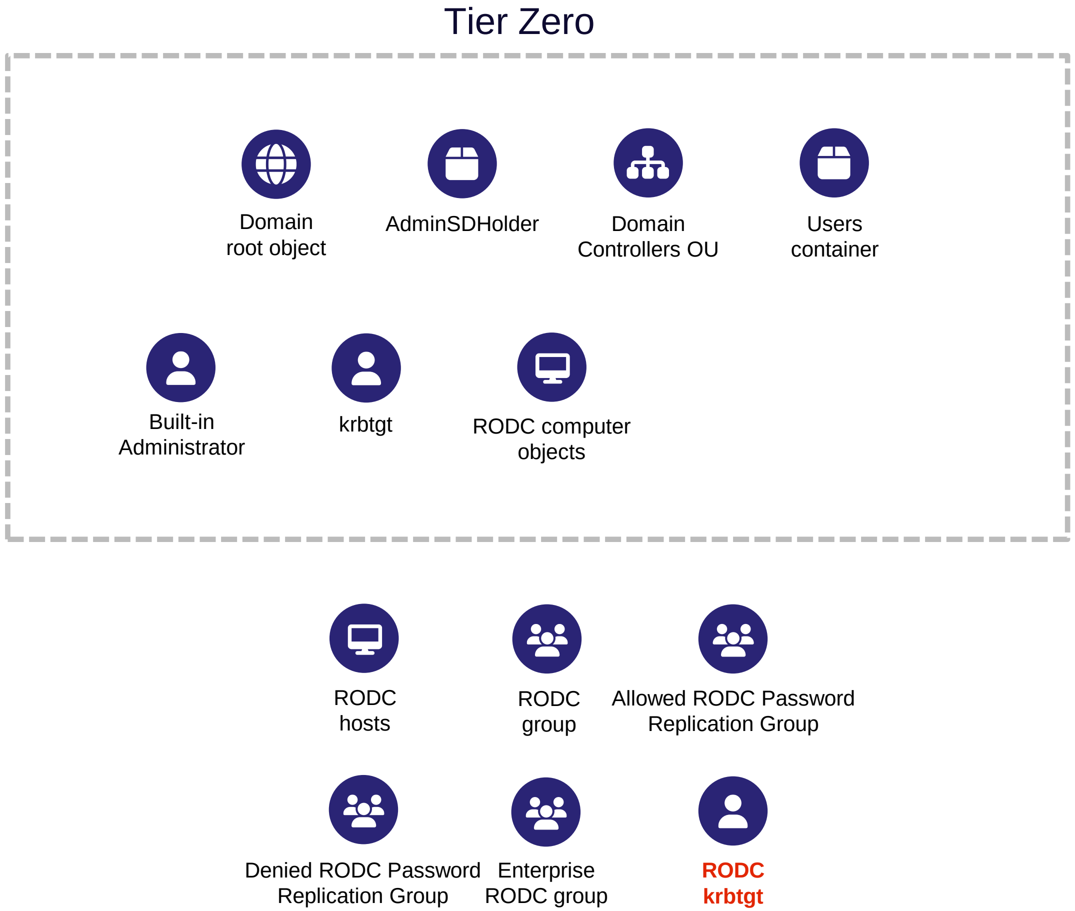
Read-Only Domain Controllers

Name	**Enterprise Read-only Domain Controllers**
Identification	S-1-5-21-<root domain>-498
Description	• Members are RODCs in the forest • Has GetChanges
Tier Zero Compromise?	No
Is it Tier Zero?	No

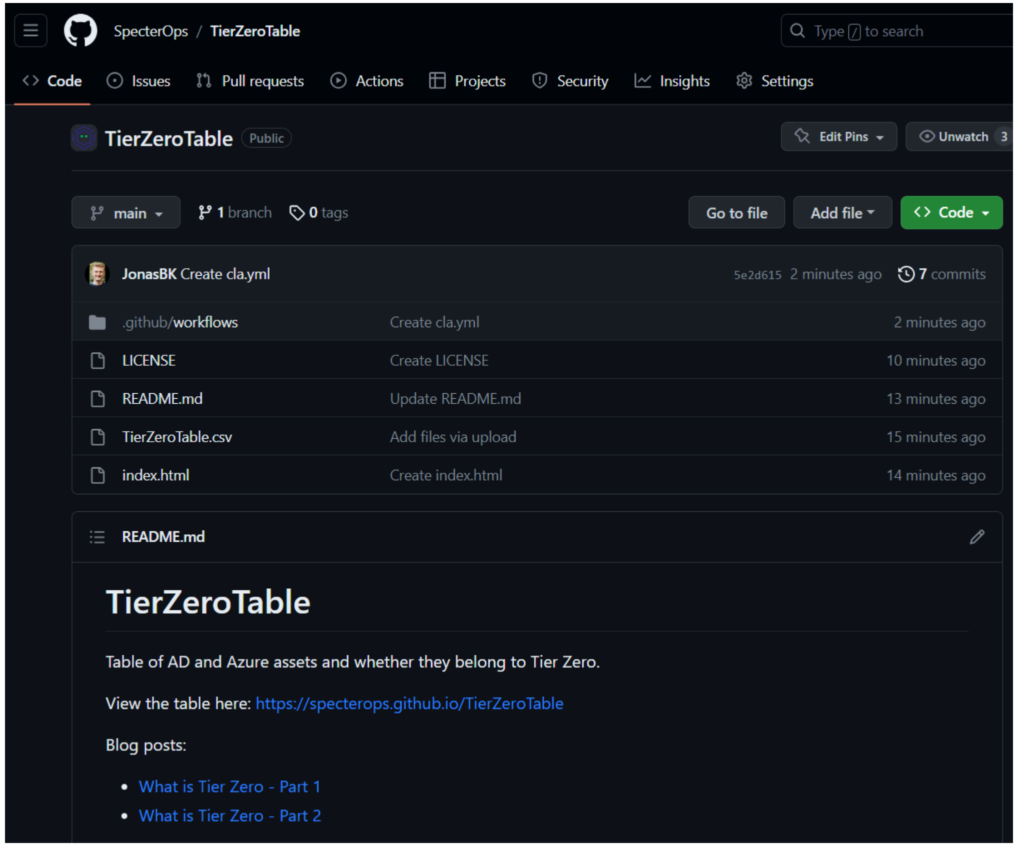


Read-Only Domain Controllers

Name	**krbtgt_<x digits>**
Identification	msDS-SecondaryKrbTgtNumber set to <x digits>
Description	- The krbtgt account for a RODC
Tier Zero Compromise?	No
Is it Tier Zero?	No



Tier Zero Table



JonasBK Create cla.yml 5e2d615 2 minutes ago 7 commits

.github/workflows	Create cla.yml	2 minutes ago
LICENSE	Create LICENSE	10 minutes ago
README.md	Update README.md	13 minutes ago
TierZeroTable.csv	Add files via upload	15 minutes ago
index.html	Create index.html	14 minutes ago

README.md

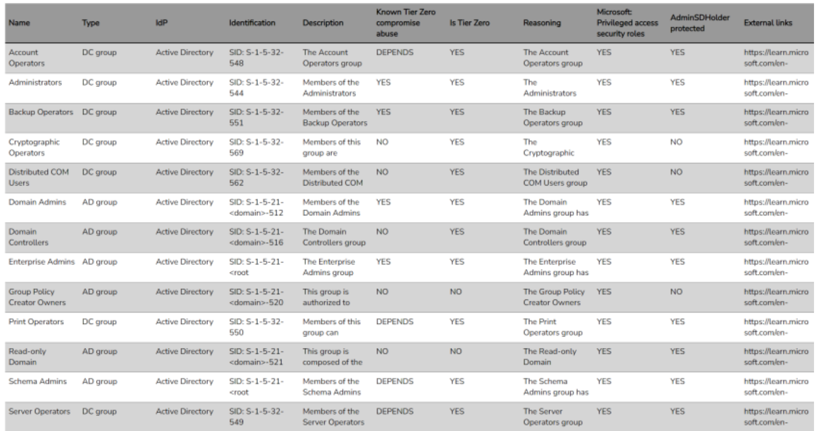
TierZeroTable

Table of AD and Azure assets and whether they belong to Tier Zero.

View the table here: https://specterops.github.io/TierZeroTable

Blog posts:

- What is Tier Zero - Part 1
- What is Tier Zero - Part 2



Name	Type	IdP	Identification	Description	Known Tier Zero compromise abuse	Is Tier Zero	Reasoning	Microsoft: Privileged access security roles	AdminSDHolder protected	External links
Account Operators	DC group	Active Directory	SID: S-1-5-32-548	The Account Operators group	DEPENDS	YES	The Account Operators group	YES	YES	https://learn.microsoft.com/en-
Administrators	DC group	Active Directory	SID: S-1-5-32-544	Members of the Administrators	YES	YES	The Administrators	YES	YES	https://learn.microsoft.com/en-
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551	Members of the Backup Operators	YES	YES	The Backup Operators group	YES	YES	https://learn.microsoft.com/en-
Cryptographic Operators	DC group	Active Directory	SID: S-1-5-32-569	Members of this group are	NO	YES	The Cryptographic	YES	NO	https://learn.microsoft.com/en-
Distributed COM Users	DC group	Active Directory	SID: S-1-5-32-562	Members of the Distributed COM	NO	YES	The Distributed COM Users group	YES	NO	https://learn.microsoft.com/en-
Domain Admins	AD group	Active Directory	SID: S-1-5-21-<domain>-512	Members of the Domain Admins	YES	YES	The Domain Admins group has	YES	YES	https://learn.microsoft.com/en-
Domain Controllers	AD group	Active Directory	SID: S-1-5-21-<domain>-516	The Domain Controllers group	NO	YES	The Domain Controllers group	YES	YES	https://learn.microsoft.com/en-
Enterprise Admins	AD group	Active Directory	SID: S-1-5-21-<root	The Enterprise Admins group	YES	YES	The Enterprise Admins group has	YES	YES	https://learn.microsoft.com/en-
Group Policy Creator Owners	AD group	Active Directory	SID: S-1-5-21-<domain>-520	This group is authorized to	NO	NO	The Group Policy Creator Owners	YES	NO	https://learn.microsoft.com/en-
Print Operators	DC group	Active Directory	SID: S-1-5-32-550	Members of this group can	DEPENDS	YES	The Print Operators group	YES	YES	https://learn.microsoft.com/en-
Read-only Domain	AD group	Active Directory	SID: S-1-5-21-<domain>-521	This group is composed of the	NO	NO	The Read-only Domain	YES	YES	https://learn.microsoft.com/en-
Schema Admins	AD group	Active Directory	SID: S-1-5-21-<root	Members of the Schema Admins	DEPENDS	YES	The Schema Admins group has	YES	YES	https://learn.microsoft.com/en-
Server Operators	DC group	Active Directory	SID: S-1-5-32-549	Members of the Server Operators	DEPENDS	YES	The Server Operators group	YES	YES	https://learn.microsoft.com/en-

- https://github.com/SpecterOps/TierZeroTable
- Submit contributions or refinements

Topics for the next sessions

- Azure AD Roles
- Microsoft Identity additions (ADFS, ADCS, SCCM)
- Third-party solutions (PAM, EDR, Backup providers)

Questions