Threat Hunter Playbook

Search this book...

KNOWLEDGE LIBRARY

Windows

- Active Directory Replication
- Active Directory Federation Services (ADFS) Distributed Key Manager (DKM) Keys
- Data Protection API
- Logon Session
- LSA Policy Objects
- Mimikatz OpenProcess Modules
- Process Security and Access Rights
- Security Account Manager (SAM) Database
- Security Account Manager Remote Protocol (SAMRP)
- Security Assertion Markup Language (SAML)
- Service Control Manager
- SysKey
- Task Scheduler Service

PRE-HUNT ACTIVITIES

Data Management

Active Directory Replication

Active Directory replication is the process by which the changes that originate on one domain controller are automatically transferred to other domain controllers that store the same data.

Active Directory data takes the form of objects that have properties, or attributes. Each object is an instance of an object class, and object classes and their respective attributes are defined in the Active Directory schema. The values of the attributes define the object, and a change to a value of an attribute must be transferred from the domain controller on which it occurs to every other domain controller that stores a replica of that object.

An adversary can abuse this model and request information about a specific account via the replication request. This is done from an account with sufficient permissions (usually domain admin level) to perform that request. Usually the accounts performing replication operations in a domain are computer accounts (i.e dcaccount$). Therefore, it might be abnormal to see other non-dc-accounts doing it.

The following access rights / permissions are needed for the replication request according to the domain functional level:

Contents

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Get-Changes	1131f6aa-9c07-11d1-f79f-00c04fc2dcd2
DS-Replication-Get-Changes-All	1131f6ad-9c07-11d1-f79f-00c04fc2dcd2
DS-Replication-Get-Changes-In-Filtered-Set	89e95b76-444d-4c62-991a-0facbeda640c

More information about the control access rights can be found here

DC-to-DC AD Replication via Directory Replication Service (DRS) Remote Protocol

The DC-to-DC interaction for replication and management of data in Active Directory is performed via the Directory Replication Service (DRS) Remote Protocol. If A DC wants to connect to a DC in a particular domain, the DC constructs a service principal name (SPN) specifying the fixed DRS RPC interface GUID "E3514235-4B06-11D1-AB04-00C04FC2DCD2". The format of the SPN constructed by the DC is the following:

//

is the fixed Directory Replication Service (DRS) RPC interface GUID, which, as mentioned before, has the well-known value of "E3514235-4B06-11D1-AB04-00C04FC2DCD2".

Directory Replication Services Auditing

Events generated by the replication activity on the targeted DC are available and easy to collect at scale. These events are related to the replication access control performed by the targeted DC and provided via event id 4662 from the security log channel.

- The main operation performed for AD replication purposes is categorized as `Object Access`. When an adversary performs a replication operation against a DC, the type of active directory object being accessed is of class Domain-DNS and points to the root domain distinguished name (i.e DC=shire,DC=com) or GUID.
- Event 4662 displays the AD object class with its `Ldap-Display-Name`, `domainDNS` value or `Schema-Id-Guid 19195a5b-6da0-11d0-afd3-00c04fd930c9`.
- The type of access in event 4662 is provided by the `access mask` field and it is of value `0x100` which translates to access type `Control Access`.
- The access type `Control Access` allows adversary to have access to the AD object

only after extended rights checks supported by the object are performed. Here is where the replication extended rights from the table above are checked and captured by event 4662. Those extended rights are captured in the `properties` field.

- The `Properties` field in 4662 provides two things, the first part is the type of access that was used. Typically, it has the same value as `Accesses field` which in this case is simply `Control Access`.
- The second part is a tree of GUID values of Active Directory classes or property sets, for which operation was performed. In our case we see the extended rights guid first and then the GUID of the class `Domain-DNS`. Therefore, when looking for this type of activity in event logs produced by the targeted DC, it is easy to find replication extended rights in event 4662.

Extra Notes:

- Remember that adversaries willing to perform a DCSync or activer directory replication attack, could also use any domain account to perform the task, despite being in no privileged groups, having no malicious sidHistory, and not having local admin rights on the domain controller itself.
- An adversary will just need to add the three ad replication access rights shown in the table

above to the unprivileged account to create a DCSync user backdoor.

References

- https://github.com/MicrosoftDocs/windows-itpro-docs/blob/master/windows/security/threat-protection/auditing/event-4662.md
- https://docs.microsoft.com/en-us/windows/desktop/adschema/c-domaindns
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/1522b774-6464-41a3-87a5-1e5633c3fbbb

Previous
Windows

Next
Active Directory Federation Services (ADFS) Distributed Key Manager (DKM) Keys

By Roberto Rodriguez @Cyb3rWard0g