Threat Hunter Playbook

Search this book...

KNOWLEDGE LIBRARY

Windows

PRE-HUNT ACTIVITIES

Data Management

GUIDED HUNTS

Windows

- LSASS Memory Read Access
- DLL Process Injection via CreateRemoteThread and LoadLibrary
- Active Directory Object Access via Replication Services
- Active Directory Root Domain Modification for Replication Services
- Registry Modification to Enable Remote Desktop Conections
- Local PowerShell Execution
- WDigest Downgrade
- PowerShell Remote Session
- Alternate PowerShell Hosts
- Domain DPAPI Backup Key Extraction
- SysKey Registry Keys Access
- SAM Registry Hive Handle Request
- WMI Win32_Process Class and Create Method for Remote Execution
- WMI Eventing
- WMI Module Load
- Local Service Installation
- Remote Service creation
- Remote Service Control Manager Handle
- Remote Interactive Task Manager LSASS Dump
- Registry Modification for Extended

Active Directory Root Domain Modification for Replication Services

Hypothesis

Adversaries with enough permissions (domain admin) might be adding an ACL to the Root Domain for any user to abuse active directory replication services.

Technical Context

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.

Offensive Tradecraft

An adversary with enough permissions (domain admin) can add an ACL to the Root Domain for any user, despite being in no privileged groups, having no malicious sidHistory, and not having local admin rights on the domain controller. This is done to bypass detection rules looking for Domain Admins or the DC machine accounts performing active directory replication requests against a domain controller.

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

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

Additional reading

- https://github.com/OTRF/ThreatHunter-Playbook/tree/master/docs/library/active_directory_replication.md

Pre-Recorded Security Datasets

Metadata	Value
docs	https://securitydatasets.com/notebooks/atomic/windows/defense_evasion/SDWIN-190301125905.html
link	https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/defense_evasion/host/empire_powerview_ldap_ntsecuritydescriptor.zip

Download Dataset

```
import requests
from zipfile import ZipFile
from io import BytesIO

url = 'https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets
zipFileRequest = requests.get(url)
zipFile = ZipFile(BytesIO(zipFileRequest.content))
datasetJSONPath = zipFile.extract(zipFile.namelist()[0])
```

Read Dataset

```
import pandas as pd
from pandas.io import json

df = json.read_json(path_or_buf=datasetJSONPath, lines=True)
```

Analytics

A few initial ideas to explore your data and validate your detection logic:

Analytic I

Look for users accessing directory service objects with replication permissions GUIDs.

Data source	Event Provider	Relationship	Event
Windows active directory	Microsoft-Windows-Security-Auditing	User accessed AD Object	4662

Logic

```
SELECT `@timestamp`, Hostname, SubjectUserName, ObjectName, OperationType
FROM dataTable
WHERE LOWER(Channel) = "security"
    AND EventID = 4662
    AND ObjectServer = "DS"
    AND AccessMask = "0x40000"
    AND ObjectType LIKE "%19195a5b_6da0_11d0_afd3_00c04fd930c9%"
```

Pandas Query

```
(
df[['@timestamp','Hostname','SubjectUserName','ObjectName','OperationType']]

[(df['Channel'].str.lower() == 'security')
    & (df['EventID'] == 4662)
    & (df['ObjectServer'] == 'DS')
    & (df['AccessMask'] == '0x40000')
    & (df['ObjectType'].str.contains('.*19195a5b-6da0-11d0-afd3-00c04fd930c9.*'
```

```
]
)
```

Analytic II

Look for any user modifying directory service objects with replication permissions GUIDs.

Data source	Event Provider	Relationship	Event
Windows active directory	Microsoft-Windows-Security-Auditing	User modified AD Object	5136

Logic

```
SELECT `@timestamp`, Hostname, SubjectUserName, ObjectDN, AttributeLDAPDisplayN
FROM dataTable
WHERE LOWER(Channel) = "security"
    AND EventID = 5136
    AND lower(AttributeLDAPDisplayName) = "ntsecuritydescriptor"
    AND (AttributeValue LIKE "%1131f6aa_9c07_11d1_f79f_00c04fc2dcd2%"
        OR AttributeValue LIKE "%1131f6ad_9c07_11d1_f79f_00c04fc2dcd2%"
        OR AttributeValue LIKE "%89e95b76_444d_4c62_991a_0facbeda640c%")
```

Pandas Query

```
(
df[['@timestamp','Hostname','SubjectUserName','ObjectDN','AttributeLDAPDisplayN

    [(df['Channel'].str.lower() == 'security')
    & (df['EventID'] == 5136)
    & (df['AttributeLDAPDisplayName'].str.lower() == 'ntsecuritydescriptor')
    & (
        (df['AttributeValue'].str.contains('.*1131f6aa-9c07-11d1-f79f-00c04fc2c
        | (df['AttributeValue'].str.contains('.*1131f6ad-9c07-11d1-f79f-00c04fc
        | (df['AttributeValue'].str.contains('.*89e95b76-444d-4c62-991a-0facbec
    )
    ]
)
```

Known Bypasses

False Positives

Hunter Notes

Hunt Output

Type	Link
Sigma Rule	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/security/win_ad_object_writedac_access.yml

Sigma Rule	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/security/win_account_backdoor_dcsync_rights.yml

References

- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/1522b774-6464-41a3-87a5-1e5633c3fbbb
- https://docs.microsoft.com/en-us/windows/desktop/adschema/c-domain
- https://docs.microsoft.com/en-us/windows/desktop/adschema/c-domaindns
- http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc782376(v=ws.10)
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/f977faaa-673e-4f66-b9bf-48c640241d47

Previous
‹ Active Directory Object Access via Replication Services

Next
Registry Modification to Enable Remote Desktop Conections ›

By Roberto Rodriguez @Cyb3rWard0g