



## 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



### Contents

Hypothesis  
Technical Context  
Offensive Tradecraft  
Pre-Recorded Security  
Datasets  
Analytics  
Known Bypasses  
False Positives  
Hunter Notes  
References

# Remote Service creation

## Hypothesis

Adversaries might be creating new services remotely to execute code and move laterally in my environment

## Technical Context

## Offensive Tradecraft

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by by adversaries creating a new service. Adversaries can create services remotely to execute code and move laterally across the environment.

## Pre-Recorded Security Datasets

| Metadata | Value   |
|----------|---|
| docs     | <a href="https://securitydatasets.com/notebooks/atomic/windows/lateral_movement/SDWIN-190518210652.html">https://securitydatasets.com/notebooks/atomic/windows/lateral_movement/SDWIN-190518210652.html</a>   |
| link     | <a href="https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/lateral_movement/host/empire_psexec_dcerpc_tcp_svcctl.zip">https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/lateral_movement/host/empire_psexec_dcerpc_tcp_svcctl.zip</a> |

## Download Dataset

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

url = 'https://raw.githubusercontent.com/OTRF/Security-Datasets/master/
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

## Analytic I

Look for new services being created in your environment under a network logon session (3). That is a sign that the service creation was performed from another endpoint in the environment.

| Data source        | Event Provider                      | Relationship            | Event |
|--------------------|-------------------------------------|-------------------------|-------|
| Service            | Microsoft-Windows-Security-Auditing | User created Service    | 4697  |
| Authentication log | Microsoft-Windows-Security-Auditing | User authenticated Host | 4624  |

## Logic

```
SELECT o.`@timestamp`, o.Hostname, o.SubjectUserName, o.SubjectUserName
FROM dataTable o
INNER JOIN (
  SELECT Hostname, TargetUserName, TargetLogonId, IpAddress
  FROM dataTable
  WHERE LOWER(Channel) = "security"
    AND EventID = 4624
    AND LogonType = 3
    AND NOT TargetUserName LIKE "%$"
) a
ON o.SubjectLogonId = a.TargetLogonId
WHERE LOWER(o.Channel) = "security"
AND o.EventID = 4697
```

## Pandas Query

```
serviceInstallDf= (
df[['@timestamp', 'Hostname', 'SubjectUserName', 'SubjectLogonId', 'Service

[(df['Channel'].str.lower() == 'security')
 & (df['EventID'] == 4697)
]
)

networkLogonDf = (
df[['@timestamp', 'Hostname', 'TargetUserName', 'TargetLogonId', 'IpAdc

[(df['Channel'].str.lower() == 'security')
 & (df['EventID'] == 4624)
 & (df['LogonType'] == 3)
 & (~df['SubjectUserName'].str.endswith('$', na=False))
]
)

(
pd.merge(serviceInstallDf, networkLogonDf,
  left_on = 'SubjectLogonId', right_on = 'TargetLogonId', how = 'inner'
)
```

## Known Bypasses

## False Positives

## Hunter Notes

- If there are a lot of unique services being created in your environment, try to categorize the data based on the bussiness unit.
- Identify the source of unique services being created everyday. I have seen Microsoft applications doing this.
- Stack the values of the service file name associated with the new service.
- Document what users create new services across your environment on a daily basis

## References

- [https://www.powershellempire.com/?page\\_id=523](https://www.powershellempire.com/?page_id=523)

[← Previous](#)  
[Local Service Installation](#)

[Remote Service Control Manager](#) [Next](#)  
[Handle](#)

---

By Roberto Rodriguez @Cyb3rWard0g  
© Copyright 2022.