



Threat Hunter Playbook

Q 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

Remote Session for Forwarded

☰

🔍

🔗

🔄

📄

Registry Modification to Enable Remote Desktop Conections

Hypothesis

Adversaries might be modifying registry key values to enable remote desktop connections in my environment

☰ Contents

Hypothesis

Technical Context

Offensive Tradecraft

Pre-Recorded Security Datasets

Analytics

Known Bypasses

False Positives

Hunter Notes

Hunt Output

References

Technical Context

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).

Offensive Tradecraft

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. There are several settings that must be configured to enable Remote Desktop connections. First, you must enable Remote Desktop connections by using the fDenyTSConnections setting. Setting fDenyTSConnections=False in the Microsoft-Windows-TerminalServices-LocalSessionManager component (HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server) specifies whether Remote Desktop connections are enabled.

An adversary can also specify how users are authenticated. Setting UserAuthentication=0 in the Microsoft-Windows-TerminalServices-RDP-WinStationExtensions component (HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp) helps make sure that users can connect remotely from computers that don't run Remote Desktop by using network-level authentication. This is the equivalent of Allow connections from computers running any version of Remote Desktop (less secure) security setting.

Pre-Recorded Security Datasets

Metadata	Value
docs	<a href="https://securitydatasets.com/notebooks/atomic/windows/defense_evasion/SDWIN-190518203650.html">https://securitydatasets.com/notebooks/atomic/windows/defense_evasion/SDWIN-190518203650.html</a>
link	<a href="https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/defense_evasion/host/empire_enable_rdp.tar.gz">https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/defense_evasion/host/empire_enable_rdp.tar.gz</a>

Download Dataset

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

url = 'https://raw.githubusercontent.com/OTRF/Security-Datasets/master/dataset.json'
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 1

Look for any process updating fDenyTSConnections or UserAuthentication registry key values

Data source	Event Provider	Relationship	Event
Windows registry	Microsoft-Windows-Sysmon/Operational	Process modified Windows registry key value	13

### Logic

```
SELECT `@timestamp`, Hostname, Image, TargetObject
FROM dataTable
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
      AND EventID = 13
      AND (TargetObject LIKE "%fDenyTSConnections"
            OR TargetObject LIKE "%UserAuthentication")
      AND Details = "DWORD (0x00000000)"
```

### Pandas Query

```
(
df[['@timestamp', 'Hostname', 'Image', 'TargetObject']]

[(df['Channel'] == 'Microsoft-Windows-Sysmon/Operational')
 & (df['EventID'] == 13)
 & (
(df['TargetObject'].str.contains('.*fDenyTSConnections', regex=True))
 | (df['TargetObject'].str.contains('.*UserAuthentication', regex=True))
)
 & (df['Details'] == 'DWORD (0x00000000)')
]
.head()
)
```

## Known Bypasses

# False Positives

## Hunter Notes

- if the activity defined above happens frequently in your environment, you cshould Stack the processeses modifying the registry key values.

## Hunt Output

Type	Link
Sigma Rule	<a href="https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_registry_modification.yml">https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_registry_modification.yml</a>

## References

- <https://attack.mitre.org/techniques/T1076/>
- [https://github.com/EmpireProject/Empire/blob/master/lib/modules/powershell/management/enable\\_rdp.py](https://github.com/EmpireProject/Empire/blob/master/lib/modules/powershell/management/enable_rdp.py)
- <https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-terminalservices-localsessionmanager-fdenytsconnections>
- <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/enable-remote-desktop-by-using-an-answer-file>