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

WDigest Downgrade

Hypothesis

Adversaries might have updated the property value UseLogonCredential of HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest to 1 in order to be able to extract clear text passwords from memory contents of lsass.

Technical Context

Windows 8.1 introduced a registry setting that allows for disabling the storage of the users logon credential in clear text for the WDigest provider.

Offensive Tradecraft

This setting can be modified in the property UseLogonCredential for the registry key HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest. If this key does not exists, you can create it and set it to 1 to enable clear text passwords.

Pre-Recorded Security Datasets

Metadata	Value
docs	https://securitydatasets.com/notebooks/atomic/windows/defense_evasion/SDWIN-190518201922.html
link	https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/defense_evasion/host/empire_wdigest_downgrade.tar.gz

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 any process updating UseLogonCredential registry key value.

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 "%UseLogonCredential"
    AND Details = 1
```

Pandas Query

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

[(df['Channel'] == 'Microsoft-Windows-Sysmon/Operational')
    & (df['EventID'] == 13)
    & (df['TargetObject'].str.endswith('UseLogonCredential', na=False))
    & (df['Details'] == 1)
]
.head()
)
```

Known Bypasses

False Positives

Hunter Notes

Hunt Output

Type	Link
Sigma Rule	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_wdigest_enable_uselogoncredenti

References

- https://github.com/samratashok/nishang/blob/master/Gather/Invoke-MimikatzWDigestDowngrade.ps1
- https://blog.stealthbits.com/wdigest-clear-text-passwords-stealing-more-than-a-hash/

‹ Previous
Local PowerShell Execution

Next ›
PowerShell Remote Session

By Roberto Rodriguez @Cyb3rWard0g