☰

Security Datasets

🔍 Search this book...

HOW-TO

Create Datasets ⌄

Consume Datasets ⌄

ATOMIC DATASETS

aws ⌄

linux ⌄

windows ⌃

   defense_evasion ⌄

   credential_access ⌄

   discovery ⌄

   persistence ⌄

   lateral_movement ⌃

      Empire Over-Pass-The-Hash

      Empire Invoke SMBExec

      Empire Invoke PsExec

      Empire Invoke DCOM ShellWindows

      Empire Invoke PSRemoting

      Empire Invoke Execute MSBuild

      Covenant Remote WMI Eventing ActiveScriptEventConsumers

      Covenant SC.exe Utility Query

      Covenant SharpSC Query

      Covenant Remote File Copy

      Covenant SharpSC Create

      Covenant SharpSC Start

      Covenant SharpSC Stop Service

      Covenant SharpWMI Exec

      Covenant PowerShell Remoting Command

      Empire Remote WMIC Add User

      Mimikatz Netlogon Unauthenticated NetrServerAuthenticate2

      DCOM ExecuteExcel4macro

      DCOM RegisterXLL

      Empire Invoke WMI

      Covenant Remote WMI Wbemcomn DLL Hijacking

      Covenant Remote DCOM Iertutil DLL Hijacking

      PurpleSharp Active Directory Playbook I

      Remote Scheduled Task Creation

      Remote Scheduled Task Modification

⛶   ⌗   ⤓

Contents

Covenant Remote File Copy

Metadata

Contributors	Roberto Rodriguez @Cyb3rWard0g
Creation Date	2020/08/06
Modification Date	2020/08/06
Tactics	TA0008
Techniques	T1021.002
Tags	SMB CreateRequest

Dataset Description

This dataset represents a threat actor remotely copying a file over SMB (CreateRequest).

Datasets Downloads

Type	Link
Host	https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/lateral_movement/host/covenant_copy_smb_CreateRequest.zip
Network	https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/lateral_movement/host/covenant_copy_smb_CreateRequest.zip

Simulation Metadata

Tools

type	Name	Module
C2	Covenant	Copy

Adversary View

```
[09/22/2020 18:53:30 UTC] Copy completed
(wardog) > Copy /source:"C:\Users\pgustavo\Desktop\GruntHTTP.exe" /desti

Successfully copied file from: C:\Users\pgustavo\Desktop\GruntHTTP.exe t
```

Explore Datasets

Download & Decompress Dataset

```
import requests
from zipfile import ZipFile
```

```
from io import BytesIO

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

Read JSON File

```
from pandas.io import json

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

Access Security Events

```
df.groupby(['Channel']).size().sort_values(ascending=False)
```

References

- https://www.mdsec.co.uk/2020/09/i-like-to-move-it-windows-lateral-movement-part-1-wmi-event-subscription/