


Security Datasets

 Search this book...

HOW-TO

Create Datasets

Consume Datasets

ATOMIC DATASETS

aws

linux

windows

defense_evasion

credential_access

Empire DCSync

Rubeus Userland ASKTGT PTT

Empire Mimikatz LogonPasswords

Empire Mimikatz Extract Kerberos Keys

Empire Mimikatz Backup Keys

Empire Mimikatz SAM Extract Hashes

Empire Reg Dump SAM Hive

RDP TaskManager LSASS Dump

Covenant DCSync

Empire Mimikatz Lsadump LSA Patch

Rubeus Elevated ASKTGT CreateNetOnly

Empire Powerdump Extract Hashes

Lsass Memory Dump via Comsvcs.dll

Lsass Memory Dump via Syscalls

SAM Copy via ESENTUTL VSS

Psexec Reg LSA Secrets Dump

UI Prompt For Credentials Function

PurpleSharp Active Directory Playbook I

discovery

persistence

lateral_movement

privilege_escalation

execution

collection

COMPOUND DATASETS

Golden SAML AD FS Mail Access



UI Prompt For Credentials Function

Metadata

Contributors	Roberto Rodriguez @Cyb3rWard0g
Creation Date	2020/10/20
Modification Date	2020/10/20
Tactics	TA0006,TA0009
Techniques	T1056.002
Tags	art.2b162bfd-0928-4d4c-9ec3-4d9f88374b52

Dataset Description

This dataset represents adversaries leveraging functions such as CredUIPromptForCredentials to create and display a configurable dialog box that accepts credentials information from a user.

Datasets Downloads

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

Simulation Metadata

Tools

type	Name	Module
Manual	powershell	powershell

Adversary View

```
PS > $cred = $host.UI.PromptForCredential('Windows Security Update',
PS > write-warning $cred.GetNetworkCredential().Password
WARNING: testing
PS >
```

Explore Datasets

Download & Decompress Dataset



Contents

Metadata

Dataset Description

Datasets Downloads

Simulation Metadata

Adversary View

Explore Datasets

References

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

url = https://raw.githubusercontent.com/OTRF/Security-Datasets/master/atomic/windows/credential_access/SDWIN-201020013208.zip
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://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1056.002/T1056.002.md#atomic-test-2—powershell—prompt-user-for-password>
- <https://docs.microsoft.com/en-us/windows/win32/api/wincred/nf-wincred-creduipromptforcredentialsa>

[Previous](#)
[Psexec Reg LSA Secrets Dump](#)

[Next](#)
[PurpleSharp Active Directory Playbook I](#)

By Roberto Rodriguez @Cyb3rWard0g
© Copyright 2022.