

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you join in?

https://threathunterplaybook.com/notebooks/windows/02_execution/WIN-190410151110.html

Go

AUG

SEP

DEC

2019

2020

2021

7 captures

25 Sep 2020 - 24 Jun 2022

Metad

Technical

About this capture

?

f

t

x

TARGETED NOTEBOOKS

Windows

Execution

- Alternate PowerShell
- Hosts
- WMI Win32_Process
- Class and Create
- Method for Remote
- Execution
- Basic PowerShell
- Execution
- Service Creation

Basic PowerShell Execution

Metadata

id	WIN-190410151110
author	Roberto Rodriguez @Cyb3rWard0g
creation date	2019/04/10
platform	Windows
playbook link	

Technical Description

Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Therefore, it is important to understand the basic artifacts left when PowerShell is used in your environment.

- Hypothesis
- Analytics
- Detection
- Blindspots
- Hunter Notes
- Hunt Output
- References

Enable Remote Desktop

Connections Registry

WDigest Downgrade

7 captures

25 Sep 2020 - 24 Jun 2022

Adversaries might be leveraging PowerShell to execute code within my environment

AUG 2019

SEP 2020

DEC 2021

Metad

Technical

About this capture

Analytics

Initialize Analytics Engine

```
from openhunt.mordorutils import *  
spark = get_spark()
```

Download & Process Mordor File

```
mordor_file = "https://raw.githubusercontent.com/OTR  
registerMordorSQLTable(spark, mordor_file, "mordorTa
```

[+] Processing a Spark DataFrame..

[+] Processing Data from Winlogbeat version 6..
[+] DataFrame Returned !

[+] Temporary SparkSQL View: mordorTable

Analytic I

FP		
Rate	Log Channel	Description

7 captures

25 Sep 2020 - 24 Jun 2022

PowerShell/Operational', classic AUG SEP DEC

'PowerShell'] PowerShell log, 25 2020 2021

event ID 400 2019

Metad

Technical

About this capture

indicates when a new PowerShell host process has started. You can filter on powershell.exe as a host application if you want to or leave it without a filter to captuer every single PowerShell host

Contents

- Hypothesis
- Analytics
- Detection
- Blindspots
- Hunter Notes
- Hunt Output
- References

```
df = spark.sql(
    '''
    SELECT `@timestamp`, computer_name, channel
    FROM mordorTable
    WHERE (channel = "Microsoft-Windows-PowerShell/Opera
        AND (event_id = 400 OR event_id = 4103)
    '''
)
df.show(10,False)
```

@timestamp	computer_name	channel
2019-05-18 14:20:49.575	HR001.shire.com	Windows P
2019-05-18 14:20:50.108	HR001.shire.com	Microsoft
2019-05-18 14:20:50.963	HR001.shire.com	Microsoft
2019-05-18 14:20:50.984	HR001.shire.com	Microsoft
2019-05-18 14:20:50.989	HR001.shire.com	Microsoft
2019-05-18 14:20:51.038	HR001.shire.com	Microsoft
2019-05-18 14:20:51.287	HR001.shire.com	Microsoft
2019-05-18 14:20:51.306	HR001.shire.com	Microsoft
2019-05-18 14:20:51.341	HR001.shire.com	Microsoft
2019-05-18 14:20:51.589	HR001.shire.com	Microsoft

7 captures

25 Sep 2020 - 24 Jun 2022

AUG

SEP

25

2020

DEC

2021

About this capture

Analytic II

FP	Log	
Rate	Channel	Description
High	['Security']	Looking for non-interactive powershell session might be a sign of PowerShell being executed by another application in the background

```
df = spark.sql(
    '''
    SELECT `@timestamp`, computer_name, NewProcessName
    FROM mordorTable
    WHERE channel = "Security"
           AND event_id = 4688
           AND NewProcessName LIKE "%powershell.exe"
           AND NOT ParentProcessName LIKE "%explorer.exe"
    '''
)
df.show(10,False)
```

@timestamp	computer_name	NewProcessName
2019-05-18 14:20:46.325	HR001.shire.com	C:\Window

Analytic III

7 captures

25 Sep 2020 - 24 Jun 2022

Rate

Log Channel

Description

AUG 2019

SEP 25 2020

DEC 2021

Metad

Technical

About this capture

High	['Microsoft-Windows-Sysmon/Operational']	Looking for non-interactive powershell session might be a sign of PowerShell being executed by another application in the background				
------	--	--	--	--	--	--

Hypothesis

Analytics

Detection

Blindspots

Hunter Notes

Hunt Output

References

```
df = spark.sql(
    '''
    SELECT `@timestamp`, computer_name, Image, ParentImage
    FROM morderTable
    WHERE channel = "Microsoft-Windows-Sysmon/Operational"
           AND event_id = 1
           AND Image LIKE "%powershell.exe"
           AND NOT ParentImage LIKE "%explorer.exe"
    '''
)
df.show(10,False)
```

@timestamp	computer_name	Image
2019-05-18 14:20:46.353	HR001.shire.com	C:\Window

Analytic IV

FP

Rate	Log Channel	Description
------	-------------	-------------

7 captures

25 Sep 2020 - 24 Jun 2022

Sysmon/Operational | PowerShell DLL | AUG 2019

SEP 25 2020

DEC 2021

Contents

Metad | Technical | About this capture

```
df = spark.sql(
    '''
    SELECT `@timestamp`, computer_name, Image, ImageLoad
    FROM mordorTable
    WHERE channel = "Microsoft-Windows-Sysmon/Operational"
        AND event_id = 7
        AND (lower(Description) = "system.management.aut
    '''
)
df.show(10,False)
```

@timestamp	computer_name	Image
2019-05-18 14:20:48.649	HR001.shire.com	C:\Window

Analytic V

FP		
Rate	Log Channel	Description
Medium	['Microsoft-Windows-Sysmon/Operational']	Monitoring for PSHost* pipes is another interesting way to find PowerShell execution

```
df = spark.sql(
    '''
    SELECT `@timestamp`, computer_name, Image, PipeName
    FROM mordorTable
```

7 captures

25 Sep 2020 - 24 Jun 2022

```
df.show(10,False)
```

AUG 2019

SEP 2020

DEC 2021

▼ About this capture

Contents

Metad

Technical

Hypothesis

Analytics

Detection

Blindspots

Hunter Notes

Hunt Output

References

@timestamp	computer_name	Image
2019-05-18 14:20:49.334	HR001.shire.com	C:\Window

Analytic VI

FP		
Rate	Log Channel	Description
Medium	[‘Microsoft-Windows-Sysmon/Operational’]	The “PowerShell Named Pipe IPC” event will indicate the name of the PowerShell AppDomain that started. Sign of PowerShell execution

```
df = spark.sql(
    '''
    SELECT `@timestamp`, computer_name, message
    FROM mordorTable
    WHERE channel = "Microsoft-Windows-PowerShell/Operat
        AND event_id = 53504
    '''
)
df.show(10,False)
```

7 captures

25 Sep 2020 - 24 Jun 2022

2019-05-18 14:20:49.47|HR001.shire.com|Windows Po

AUG

SEP

DEC

25

2020

2021

About this capture

Detection Blindspots

Hunter Notes

- Explore the data produced in your environment with the analytics above and document what normal looks like from a PowerShell perspective.
- If execution of PowerShell happens all the time in your environment, I suggest to categorize the data you collect by business unit to build profiles and be able to filter out potential noise.
- You can also stack the values of the command line arguments being used. You can hash the command line arguments too and stack the values.

Hunt Output

Category	Type	Name
signature	SIGMA	sysmon_powershell_execution_modu
signature	SIGMA	sysmon_powershell_execution_pipe
signature	SIGMA	sysmon_non_interactive_powershell_

Contents

7 captures

25 Sep 2020 - 24 Jun 2022

AUG 2019

SEP 202025

DEC 2021

Meta...
Technical
About this capture

References

- [https://posts.specterops.io/abusing-powershell-desired-state-configuration-for-lateral-movement-ca42ddbe6f06](https://github.com/darkoperator/Presentations/blob/master/PS(• <a href=)

<< WMI Win32_Process Class and Create Method for Remote	
Execution	By Roberto Rodriguez @Cyb3rWard0g

© Copyright 2020.