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

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

Go







7 captures

25 Sep 2020 - 24 Jun 2022

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 Windows platform 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

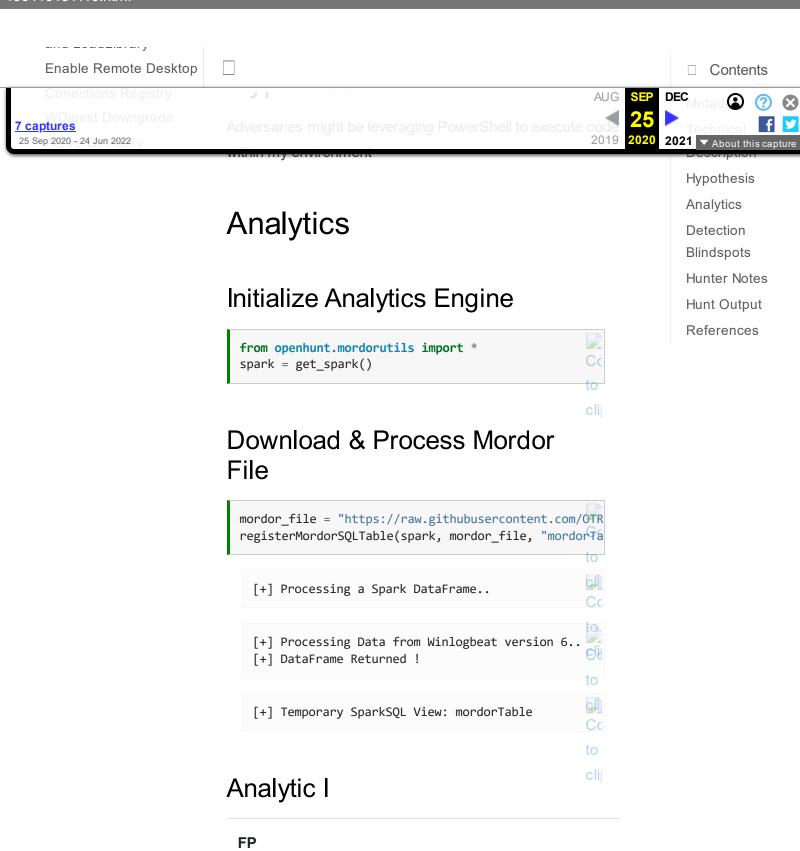
Detection

Blindspots

Hunter Notes

Hunt Output

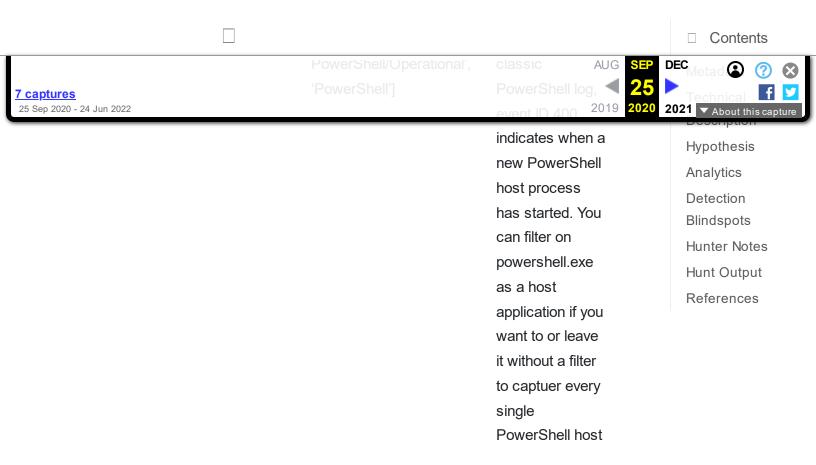
References

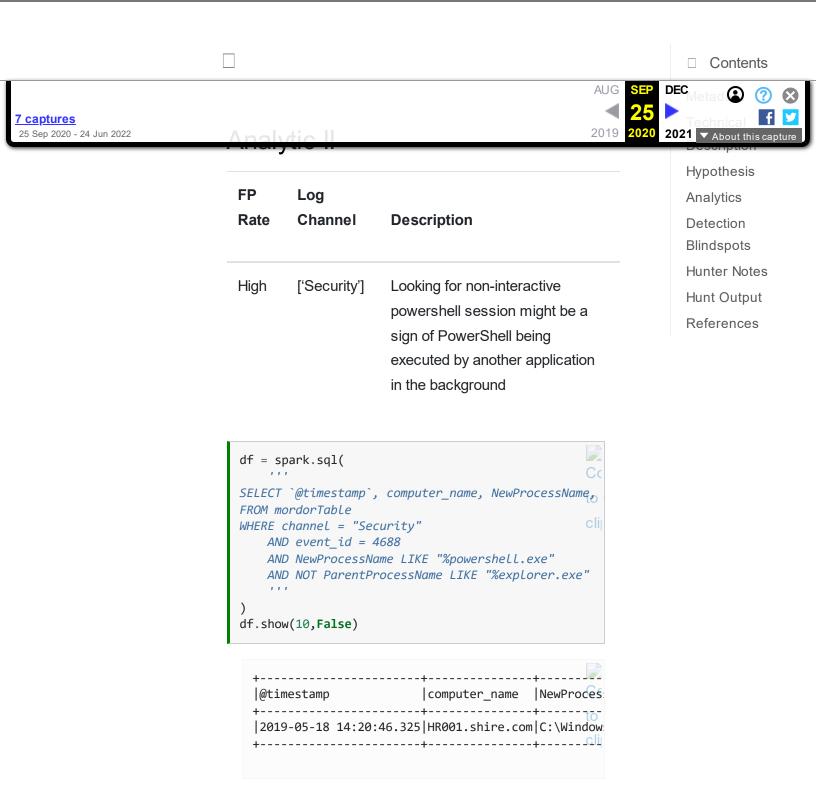


Description

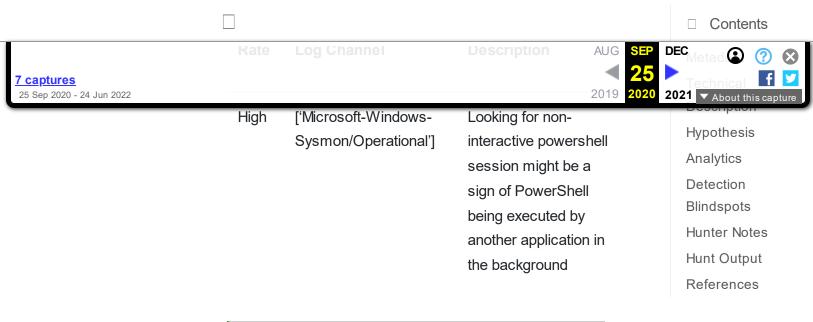
Log Channel

Rate





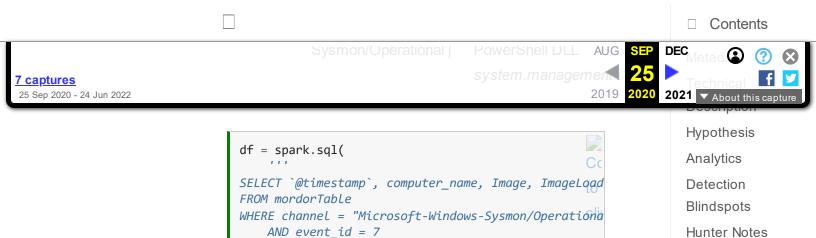
Analytic III



```
|@timestamp | computer_name | Image | Image | Computer_name | Image |
```

Analytic IV

FP Rate	Log Channel	Description	
	Log onamor	Becompacin	



AND (Lower(Description) = "system.management.aut

Hunt Output References

Analytic V

df.show(10,False)

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
```



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



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	Туре	Name
signature	SIGMA	sysmon_powershell_execution_modu
signature	SIGMA	sysmon_powershell_execution_pipe
signature	SIGMA	sysmon_non_interactive_powershell_

Hypothesis

Analytics

Detection

Blindspots

Hunter Notes

Hunt Output

References

