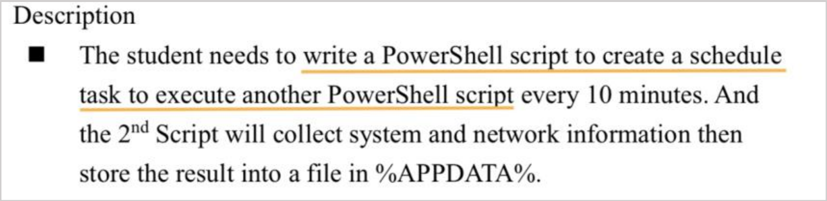
Scheduled Task/Job—Schedule task

1. Attack scenario introduction

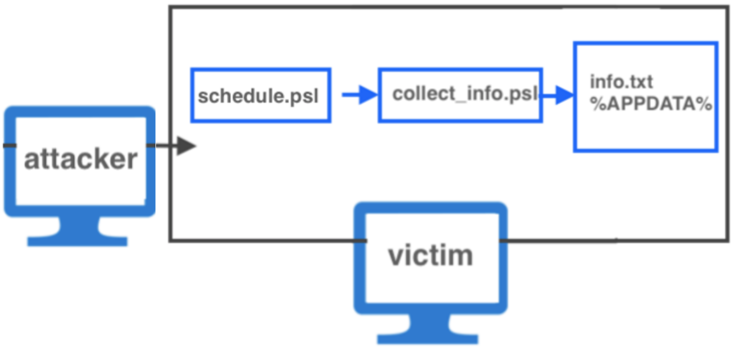
(1) Group : UNC2452 No.20

(2) Scenario :



Description

- The student needs to write a PowerShell script to create a schedule task to execute another PowerShell script every 10 minutes. And the 2nd Script will collect system and network information then store the result into a file in %APPDATA%.



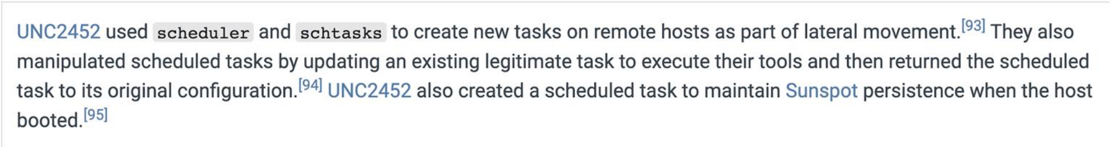
(3) Introduction :

① Schedule programs/scripts to be executed.

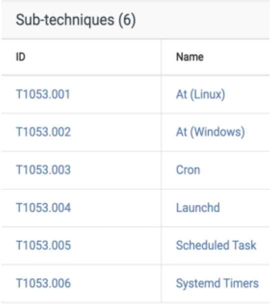
② Can be classified into time-based and event-based such as startup or logon

③ In general, Privilege Escalation is required and can be used in Persistence, Lateral movement, Exfiltration, or facilitating initial access.

(4) MITRE ATT&CK techniques :



UNC2452 used `scheduler` and `schtasks` to create new tasks on remote hosts as part of lateral movement.[93] They also manipulated scheduled tasks by updating an existing legitimate task to execute their tools and then returned the scheduled task to its original configuration.[94] UNC2452 also created a scheduled task to maintain Sunspot persistence when the host booted.[95]



Sub-techniques (6)

ID	Name
T1053.001	At (Linux)
T1053.002	At (Windows)
T1053.003	Cron
T1053.004	Launchd
T1053.005	Scheduled Task
T1053.006	Systemd Timers

The scheduler varies between different OS.

For windows, At.exe is deprecated as of win8, Cron is for Unix-like computer OS, while Lanched is job scheduler in MacOS.

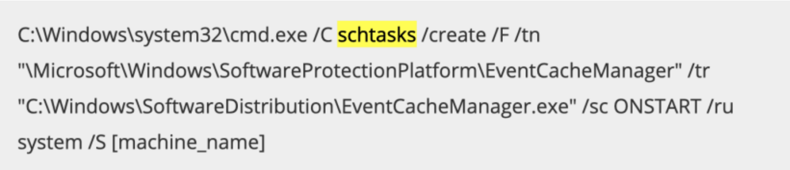
(5) Are the tools comprised with modules?

No, but there are useful PowerShell module such as PowerSploit.

(6) techniques that used

① Schtasks : Partial Code from the blog mentioned in MITRE [1]

https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/



```
C:\Windows\system32\cmd.exe /C schtasks /create /F /tn
"\Microsoft\Windows\SoftwareProtectionPlatform\EventCacheManager" /tr
"C:\Windows\SoftwareDistribution\EventCacheManager.exe" /sc ONSTART /ru
system /S [machine_name]
```

② Usage of schtasks

schtasks /create /sc <scheduletype such as DAILY, ONCE>

/tn <taskname> /tr <taskrun : path>

[/s <computer/IP> [/u<user> /p <password>]]

[/ru {[<domain>\]<user> | system}] [/rp <password>]

> /ru will run the task with permissions of the specified user account, which is also valid when scheduling remotely. The valid options include:
>
> Domain - Specifies an alternate user account.
>
> System - Specifies the local System account.

[/d<WEEKLY, MONTHLY>] [/m<JAN-DEC>] [/i<1-99(minutes)>]

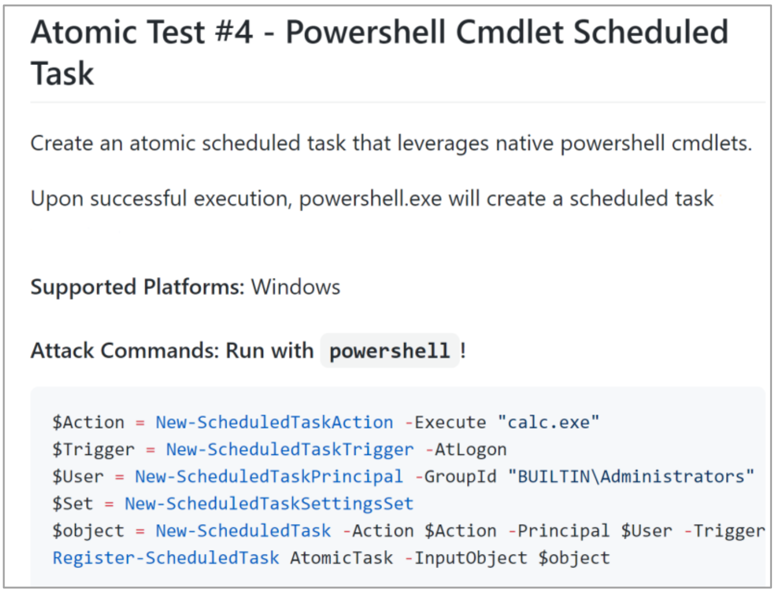
[/st<start time>][/ri<interval>] [{/et|/du} [/k]]

[/sd<start date> /ed<end date>]

[/z<delete upon completion>] [/f<suppress warnings if file already exists>]

③ Powershell Cmdlet Scheduled Task [2]

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1053.005/T1053.005.md



Atomic Test #4 - Powershell Cmdlet Scheduled Task

Create an atomic scheduled task that leverages native powershell cmdlets.

Upon successful execution, powershell.exe will create a scheduled task

Supported Platforms: Windows

Attack Commands: Run with `powershell`!

```
$Action = New-ScheduledTaskAction -Execute "calc.exe"
$Trigger = New-ScheduledTaskTrigger -AtLogon
$User = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Administrators"
$Set = New-ScheduledTaskSettingsSet
$object = New-ScheduledTask -Action $Action -Principal $User -Trigger
Register-ScheduledTask AtomicTask -InputObject $object
```

2. How you reproduced the attack scenario.

(1) Tools : A VM of Win10, PowerShell

(2) How it works :

There are 3 files working in the scenario.

① schedule.ps1 [3] https://devblogs.microsoft.com/scripting/use-powershell-to-create-scheduled-task-in-new-folder/ :

Create a scheduled task by 2 Functions. The first function is to create scheduled task, while the other is for configuration (optional).

```
-----------------------------------------------------------------------------------------------
Function CreateScheduledTask ($TASKNAME, $TASKPATH){
   $ACTION = New-ScheduledTaskAction –Execute “wscript.exe”
                    –Argument $Hidden –ExecutionPolicy ByPass –File $SCRIPT
   $TRIGGER = New-ScheduledTaskTrigger -Once -At (Get-Date) –
                    RepetitionInterval (New-TimeSpan -Minutes 10)
   Register-ScheduledTask ……
}
Function ConfigureScheduledTaskSettings ($TASKNAME, $TASKPATH){……}
-----------------------------------------------------------------------------------------------
```

In the first function, using “wscript.exe $Hidden” is to hide the powershell window, where $Hidden is the filepath of HiddenPowershell.vbs.

If using powershell.exe, the powershell window will popup though arguments –ExecutionPolicy ByPass and –WindowStyle Hidden are passed.

(Reason: powershell.exe is a console application created by the OS when the process starts. The powershell.exe code that processes -WindowStyle Hidden is therefore executed after the console window is opened hence the flash. To fix this, we would need the equivalent of wscript i.e. a win32 host application instead of a console host application.)[4]https://github.com/PowerShell/PowerShell/issues/3028

② HiddenPowershell.vbs [5] https://github.com/UNT-CAS/HiddenPowershell/blob/master/HiddenPowershell.vbs

The filepath is set by variable $Hidden in schedule.ps1.

It wraps the powershell script in the vbs script.

③ collect_info.ps1 [6] https://attack.mitre.org/techniques/T1016/

$USER = $env:username

$PATH_STORED = "/Users/$USER/AppData/computer_info.txt"

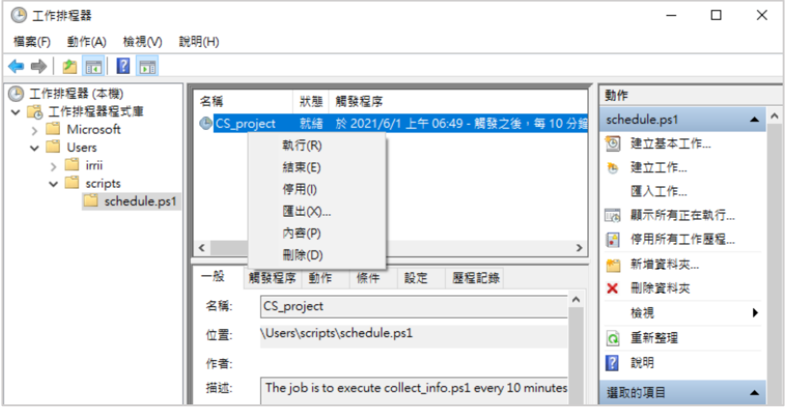
The result of “systeminfo”, “ipconfig /all”, “Get-NetNeighbor”, “arp -a”, “route print” are stored at $PATH_STORED.

(3) How to implement :

Copy the whole directory “scripts” to “/Users” and execute the command “/Users/scripts/schedule.ps1” with PowerShell (Administrator).

Next, view the information collected at /Users/$USER/AppData/computer_info.txt

(If you don’t want to wait 10 minutes for the result, go to the same path as the following picture of Task Scheduler and execute immediately.)



名稱	狀態	觸發程序
CS_project	就緒	於 2021/6/1 上午 06:49 - 觸發之後，每 10 分鐘

名稱: CS_project

位置: \Users\scripts\schedule.ps1

作者:

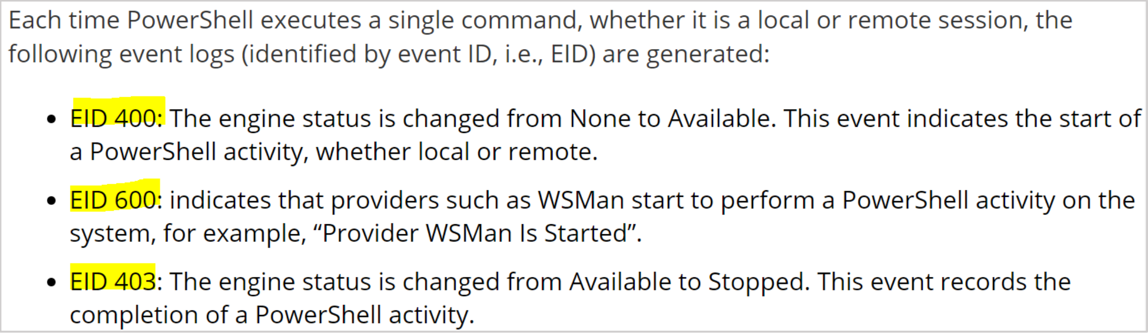
描述: The job is to execute collect_info.ps1 every 10 minutes

3. Observed activities.

There are 3 places mentioned below to view the event logs.

(1) Event viewer – Windows Powershell

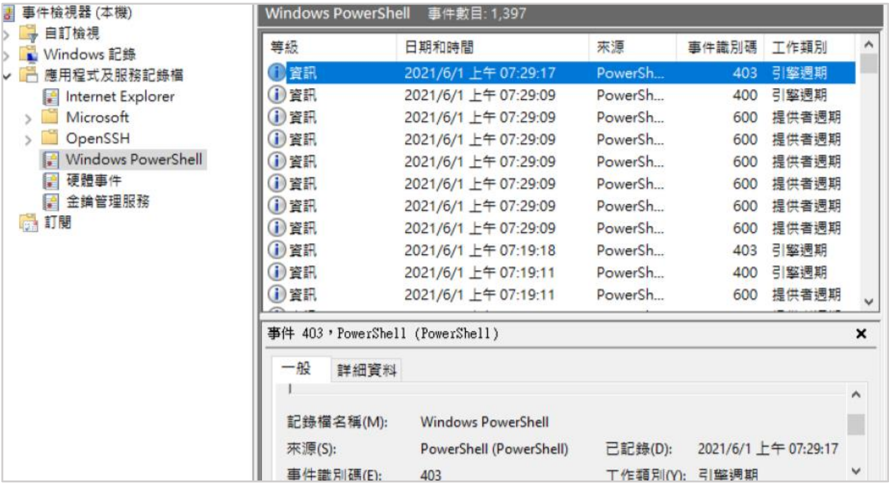
Go to "Applications and Services Logs/Windows PowerShell", and view the EID mentioned below. [7] https://nsfocusglobal.com/Attack-and-Defense-Around-PowerShell-Event-Logging



Each time PowerShell executes a single command, whether it is a local or remote session, the following event logs (identified by event ID, i.e., EID) are generated:

- EID 400: The engine status is changed from None to Available. This event indicates the start of a PowerShell activity, whether local or remote.
- EID 600: indicates that providers such as WSMan start to perform a PowerShell activity on the system, for example, "Provider WSMan Is Started".
- EID 403: The engine status is changed from Available to Stopped. This event records the completion of a PowerShell activity.

(EID related to PowerShell activities)



Windows PowerShell 事件數目: 1,397

等級	日期和時間	來源	事件識別碼	工作類別
資訊	2021/6/1 上午 07:29:17	PowerSh...	403	引擎週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	400	引擎週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	600	提供者週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	600	提供者週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	600	提供者週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	600	提供者週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	600	提供者週期
資訊	2021/6/1 上午 07:29:09	PowerSh...	600	提供者週期
資訊	2021/6/1 上午 07:19:18	PowerSh...	403	引擎週期
資訊	2021/6/1 上午 07:19:11	PowerSh...	400	引擎週期
資訊	2021/6/1 上午 07:19:11	PowerSh...	600	提供者週期

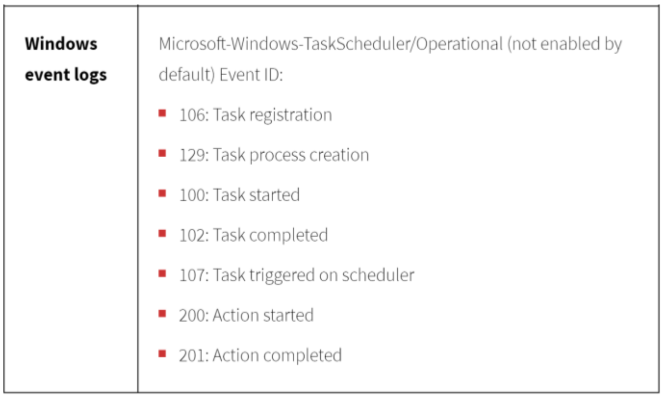
事件 403，PowerShell (PowerShell)

記錄檔名稱(M): Windows PowerShell
來源(S): PowerShell (PowerShell) 已記錄(D): 2021/6/1 上午 07:29:17
事件識別碼(E): 403 工作類別(Y): 引擎週期

(Check out the events of EID 400, 600, 403)

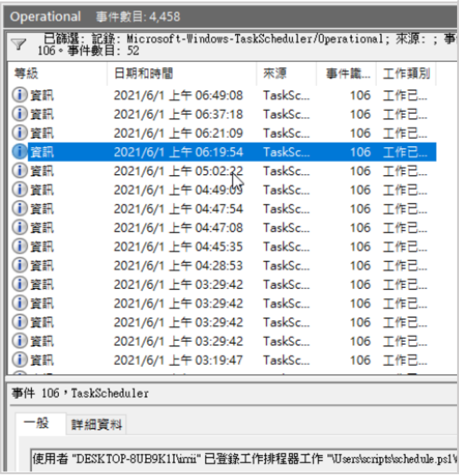
(2) Event viewer –Scheduled task log

Go to "Applications and Services Logs/Microsoft/Windows/Taskscheduler/Optional", and be careful of EID below [8] https://redcanary.com/threat-detection-report/techniques/scheduled-task/



Windows event logs	Microsoft-Windows-TaskScheduler/Operational (not enabled by default) Event ID: ▪ 106: Task registration ▪ 129: Task process creation ▪ 100: Task started ▪ 102: Task completed ▪ 107: Task triggered on scheduler ▪ 200: Action started ▪ 201: Action completed

(EID related to scheduled task)



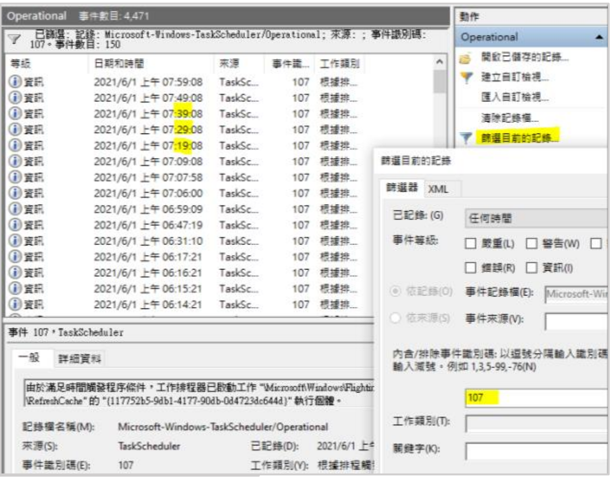
Operational 事件數目: 4,458

已篩選: 記錄: Microsoft-Windows-TaskScheduler/Operational; 來源: ; 事
106。事件數目: 52

等級	日期和時間	來源	事件識...	工作類別
資訊	2021/6/1 上午 06:49:08	TaskSc...	106	工作已...
資訊	2021/6/1 上午 06:37:18	TaskSc...	106	工作已...
資訊	2021/6/1 上午 06:21:09	TaskSc...	106	工作已...
資訊	2021/6/1 上午 06:19:54	TaskSc...	106	工作已...
資訊	2021/6/1 上午 05:02:22	TaskSc...	106	工作已...
資訊	2021/6/1 上午 04:49:09	TaskSc...	106	工作已...
資訊	2021/6/1 上午 04:47:54	TaskSc...	106	工作已...
資訊	2021/6/1 上午 04:47:08	TaskSc...	106	工作已...
資訊	2021/6/1 上午 04:45:35	TaskSc...	106	工作已...
資訊	2021/6/1 上午 04:28:53	TaskSc...	106	工作已...
資訊	2021/6/1 上午 03:29:42	TaskSc...	106	工作已...
資訊	2021/6/1 上午 03:29:42	TaskSc...	106	工作已...
資訊	2021/6/1 上午 03:29:42	TaskSc...	106	工作已...
資訊	2021/6/1 上午 03:29:42	TaskSc...	106	工作已...
資訊	2021/6/1 上午 03:19:47	TaskSc...	106	工作已...

事件 106，TaskScheduler

使用者 "DESKTOP-8UB9K1I\imii" 已登錄工作排程器工作 "\Users\scripts\schedule.ps1\



Operational 事件數目: 4,471

已篩選: 記錄: Microsoft-Windows-TaskScheduler/Operational; 來源: ; 事件識別碼:
107。事件數目: 150

等級	日期和時間	來源	事件識...	工作類別
資訊	2021/6/1 上午 07:59:08	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:49:08	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:39:08	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:29:08	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:19:08	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:09:08	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:07:58	TaskSc...	107	根據排...
資訊	2021/6/1 上午 07:06:00	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:59:09	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:47:19	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:31:10	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:17:21	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:16:21	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:15:21	TaskSc...	107	根據排...
資訊	2021/6/1 上午 06:14:21	TaskSc...	107	根據排...

事件 107，TaskScheduler

由於滿足時間觸發程序條件，工作排程器已啟動工作 "\Microsoft\Windows\Flightin
\RefreshCache" 的 "{117752b5-9db1-4177-90db-0d4723dc644d}" 執行個體。

記錄檔名稱(M): Microsoft-Windows-TaskScheduler/Operational
來源(S): TaskScheduler 已記錄(D): 2021/6/1 上午
事件識別碼(E): 107 工作類別(Y): 根據排程觸

篩選目前的記錄

已記錄: (G) 任何時間

事件等級: □ 嚴重(L) □ 警告(W) □ □ 錯誤(R) □ 資訊(I)

● 依記錄(O) 事件記錄檔(E): Microsoft-Wi

○ 依來源(S) 事件來源(V):

內含/排除事件識別碼: 以逗號分隔輸入識別碼
輸入減號。例如 1,3,5-99,-76(N)

107

工作類別(T):

關鍵字(K):

(Check out the events of EID 106, 107)

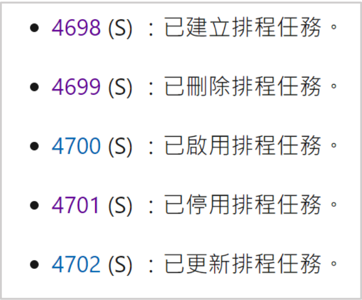
(3) Windows event logs

Firstly download gpedit-msc.bat from [9] https://github.com/GDaily/gpedit-msc/releases .

Secondly enable “Audit Object Access” with Security Access Control Lists (SACL).

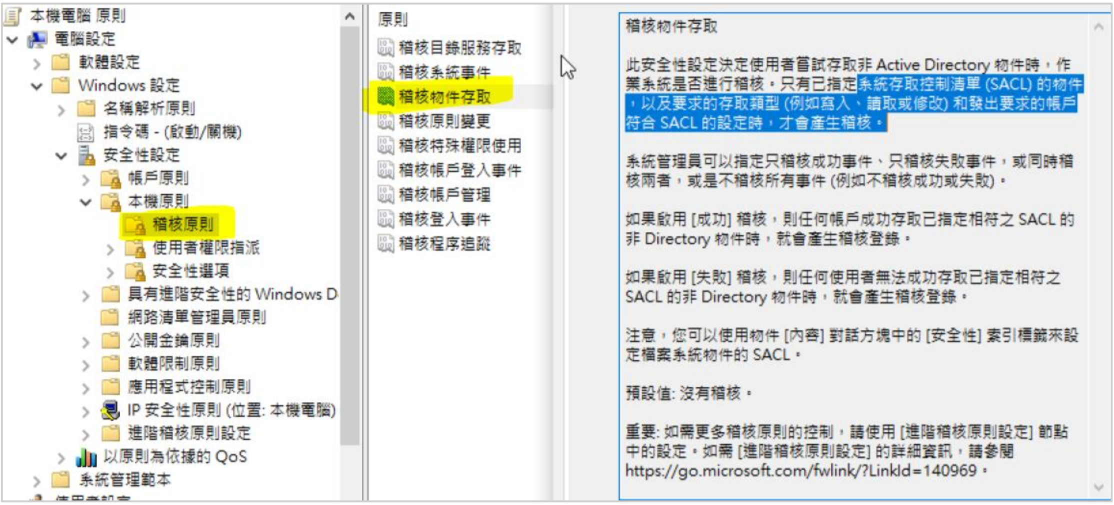
Lastly apply an EID filter on “4698, 4699, 4700, 4701, 4702” according to [9]

https://docs.microsoft.com/zh-tw/windows/security/threat-protection/auditing/audit-other-object-access-events



- 4698 (S) ：已建立排程任務。
- 4699 (S) ：已刪除排程任務。
- 4700 (S) ：已啟用排程任務。
- 4701 (S) ：已停用排程任務。
- 4702 (S) ：已更新排程任務。

(EID related to scheduled task)



稽核物件存取

此安全性設定決定使用者嘗試存取非 Active Directory 物件時，作業系統是否進行稽核。只有已指定系統存取控制清單 (SACL) 的物件，以及要求的存取類型 (例如寫入、讀取或修改) 和發出要求的帳戶符合 SACL 的設定時，才會產生稽核。

系統管理員可以指定只稽核成功事件、只稽核失敗事件，或同時稽核兩者，或是不稽核所有事件 (例如不稽核成功或失敗)。

如果啟用 [成功] 稽核，則任何帳戶成功存取已指定相符之 SACL 的非 Directory 物件時，就會產生稽核登錄。

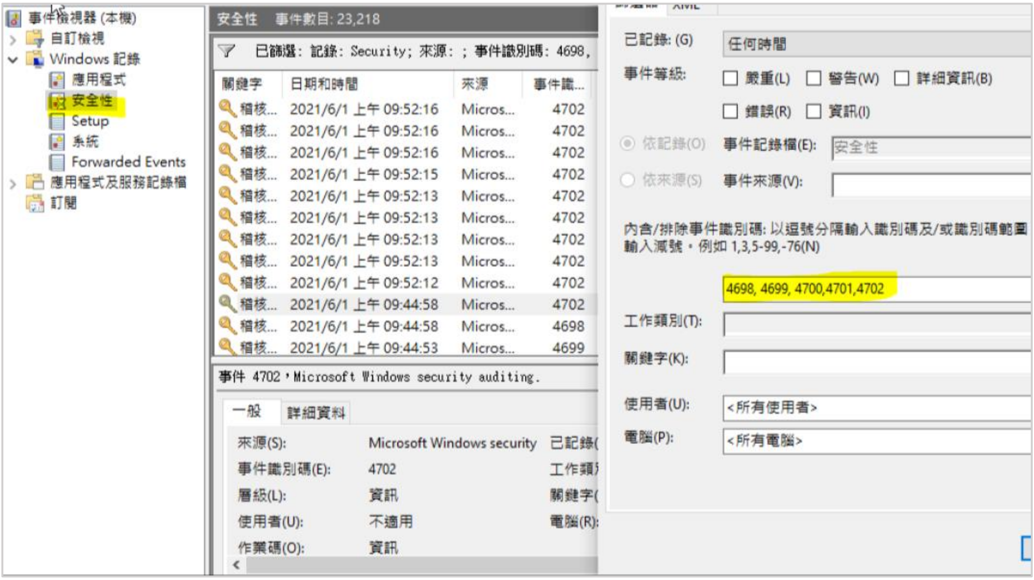
如果啟用 [失敗] 稽核，則任何使用者無法成功存取已指定相符之 SACL 的非 Directory 物件時，就會產生稽核登錄。

注意，您可以使用物件 [內容] 對話方塊中的 [安全性] 索引標籤來設定檔案系統物件的 SACL。

預設值: 沒有稽核。

重要: 如需更多稽核原則的控制，請使用 [進階稽核原則設定] 節點中的設定。如需 [進階稽核原則設定] 的詳細資訊，請參閱 https://go.microsoft.com/fwlink/?LinkId=140969。

(Policy setting : go to “Windows Settings > Security Settings > Local Policies > Audit Policy ”)



安全性 事件數目: 23,218

已篩選: 記錄: Security; 來源: ; 事件識別碼: 4698,

關鍵字	日期和時間	來源	事件識...
稽核...	2021/6/1 上午 09:52:16	Micros...	4702
稽核...	2021/6/1 上午 09:52:16	Micros...	4702
稽核...	2021/6/1 上午 09:52:16	Micros...	4702
稽核...	2021/6/1 上午 09:52:15	Micros...	4702
稽核...	2021/6/1 上午 09:52:13	Micros...	4702
稽核...	2021/6/1 上午 09:52:13	Micros...	4702
稽核...	2021/6/1 上午 09:52:13	Micros...	4702
稽核...	2021/6/1 上午 09:52:13	Micros...	4702
稽核...	2021/6/1 上午 09:52:12	Micros...	4702
稽核...	2021/6/1 上午 09:44:58	Micros...	4702
稽核...	2021/6/1 上午 09:44:58	Micros...	4698
稽核...	2021/6/1 上午 09:44:53	Micros...	4699

事件 4702，Microsoft Windows security auditing.

來源(S):	Microsoft Windows security	已記錄(
事件識別碼(E):	4702	工作類
層級(L):	資訊	關鍵字(
使用者(U):	不適用	電腦(R):
作業碼(O):	資訊	

已記錄: (G) 任何時間

事件等級: □ 嚴重(L) □ 警告(W) □ 詳細資訊(B)
□ 錯誤(R) □ 資訊(I)

● 依記錄(O) 事件記錄檔(E): 安全性

○ 依來源(S) 事件來源(V):

內含/排除事件識別碼: 以逗號分隔輸入識別碼及/或識別碼範圍
輸入減號。例如 1,3,5-99,-76(N)

4698, 4699, 4700,4701,4702

工作類別(T):

關鍵字(K):

使用者(U): <所有使用者>

電腦(P): <所有電腦>

(Check out the events with EID 4698, 4699, 4700, 4701, 4702)

4. Possible solutions to detect such an attack scenario.

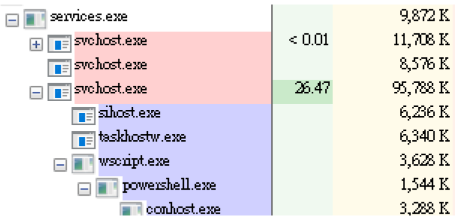
(1) Check the system logs of PowerShell, Scheduled task, and Security Events.

(2) Process tree for behavior analysis

On Windows 10, tasks are run directly by *"svchost.exe"* , which is responsible for the *"Task Scheduler"* Service.

Thus, how the task behaves can be identified according to the process tree.

Also, a CPU-consuming process can be identified.

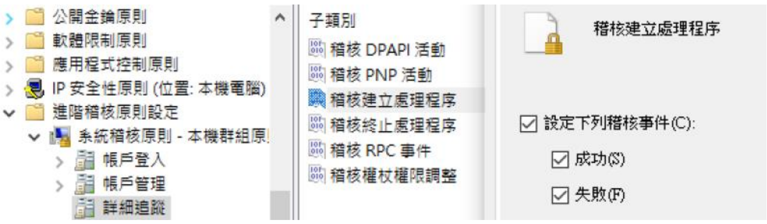


```
⊟ services.exe                          9,872 K
  ⊞ svchost.exe             < 0.01     11,708 K
    svchost.exe                         8,576 K
  ⊟ svchost.exe              26.47     95,788 K
      sihost.exe                        6,236 K
      taskhostw.exe                     6,340 K
    ⊟ wscript.exe                       3,628 K
      ⊟ powershell.exe                  1,544 K
          conhost.exe                   3,288 K
```

(Process tree viewed by process explorer)

(3) Process Command line monitoring

Firstly, include the command line in "process creation events" so that the file path can be viewed on the panel.



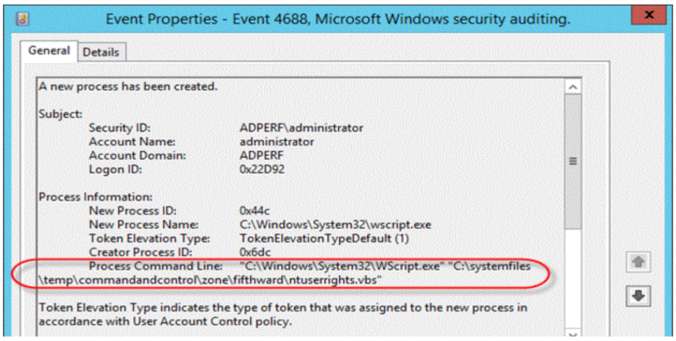
公開金鑰原則
軟體限制原則
應用程式控制原則
IP 安全性原則 (位置: 本機電腦)
進階稽核原則設定
系統稽核原則 - 本機群組原
帳戶登入
帳戶管理
詳細追蹤

子類別
稽核 DPAPI 活動
稽核 PNP 活動
稽核建立處理程序
稽核終止處理程序
稽核 RPC 事件
稽核權杖權限調整

稽核建立處理程序

☑ 設定下列稽核事件(C):
☑ 成功(S)
☑ 失敗(F)

(go to "Security Settings > Advanced Audit Configuration/Detailed Tracking" and check "Audit Process Creation ".)



Event Properties - Event 4688, Microsoft Windows security auditing.

General | Details

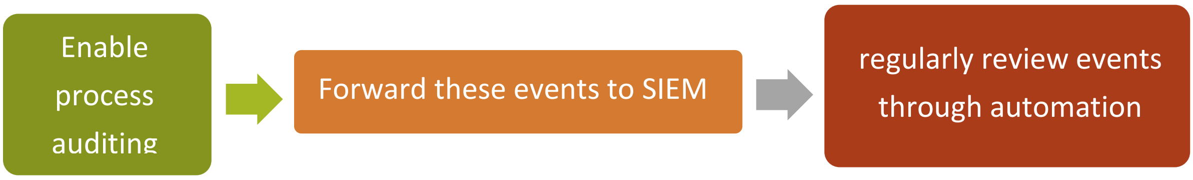
```
A new process has been created.

Subject:
        Security ID:            ADPERF\administrator
        Account Name:           administrator
        Account Domain:         ADPERF
        Logon ID:               0x22D92

Process Information:
        New Process ID:         0x44c
        New Process Name:       C:\Windows\System32\wscript.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x6dc
        Process Command Line:   "C:\Windows\System32\WScript.exe" "C:\systemfiles
\temp\commandandcontrol\zone\fifthward\ntuserrights.vbs"

Token Elevation Type indicates the type of token that was assigned to the new process in
accordance with User Account Control policy.
```

After that, we can forward the process logs to analysis tools to detect anomaly.



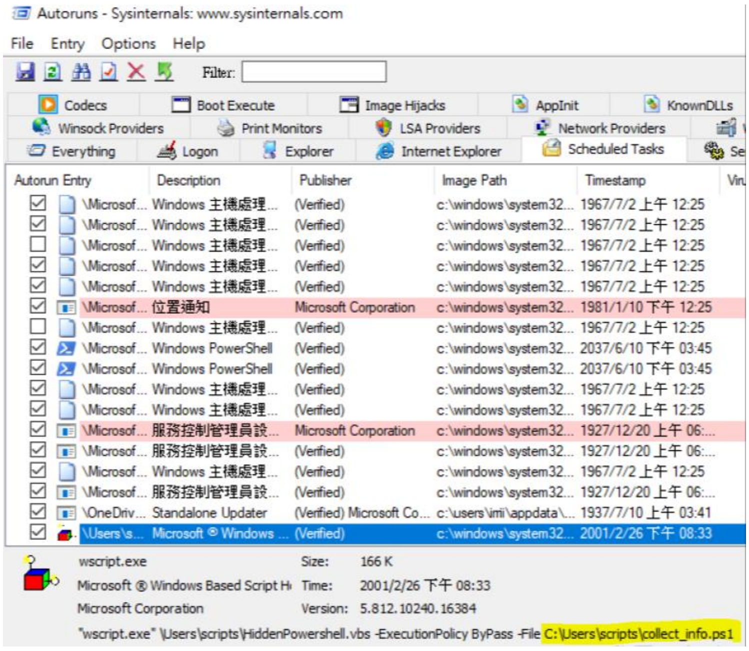
Enable process auditing

Forward these events to SIEM

regularly review events through automation

(4) Sysinternals Autoruns

It is a small-sized tool which will check Registries and file system locations easily used for auto-start configuration and then list current scheduled tasks as well as auto-start programs.



Autoruns - Sysinternals: www.sysinternals.com

	Autorun Entry	Description	Publisher	Image Path	Timestamp	Viru
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☐	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	位置通知	Microsoft Corporation	c:\windows\system32...	1981/1/10 下午 12:25	
☐	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	Windows PowerShell	(Verified)	c:\windows\system32...	2037/6/10 下午 03:45	
☑	\Microsof...	Windows PowerShell	(Verified)	c:\windows\system32...	2037/6/10 下午 03:45	
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	服務控制管理員設...	Microsoft Corporation	c:\windows\system32...	1927/12/20 上午 06:...	
☑	\Microsof...	服務控制管理員設...	(Verified)	c:\windows\system32...	1927/12/20 上午 06:...	
☑	\Microsof...	Windows 主機處理...	(Verified)	c:\windows\system32...	1967/7/2 上午 12:25	
☑	\Microsof...	服務控制管理員設...	(Verified)	c:\windows\system32...	1927/12/20 上午 06:...	
☑	\OneDriv...	Standalone Updater	(Verified) Microsoft Co...	c:\users\irrii\appdata\...	1937/7/10 上午 03:41	
☑	\Users\s...	Microsoft ® Windows ...	(Verified)	c:\windows\system32...	2001/2/26 下午 08:33	

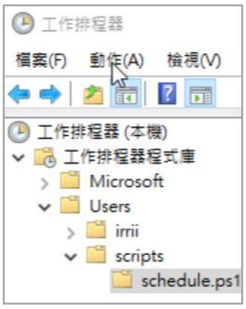
wscript.exe Size: 166 K

Microsoft ® Windows Based Script H Time: 2001/2/26 下午 08:33

Microsoft Corporation Version: 5.812.10240.16384

"wscript.exe" \Users\scripts\HiddenPowershell.vbs -ExecutionPolicy ByPass -File C:\Users\scripts\collect_info.ps1

(The task marked is the abnormal)



(In Task Scheduler, correct path is required to find an abnormal task.)