

Windows Task Scheduler Monitor

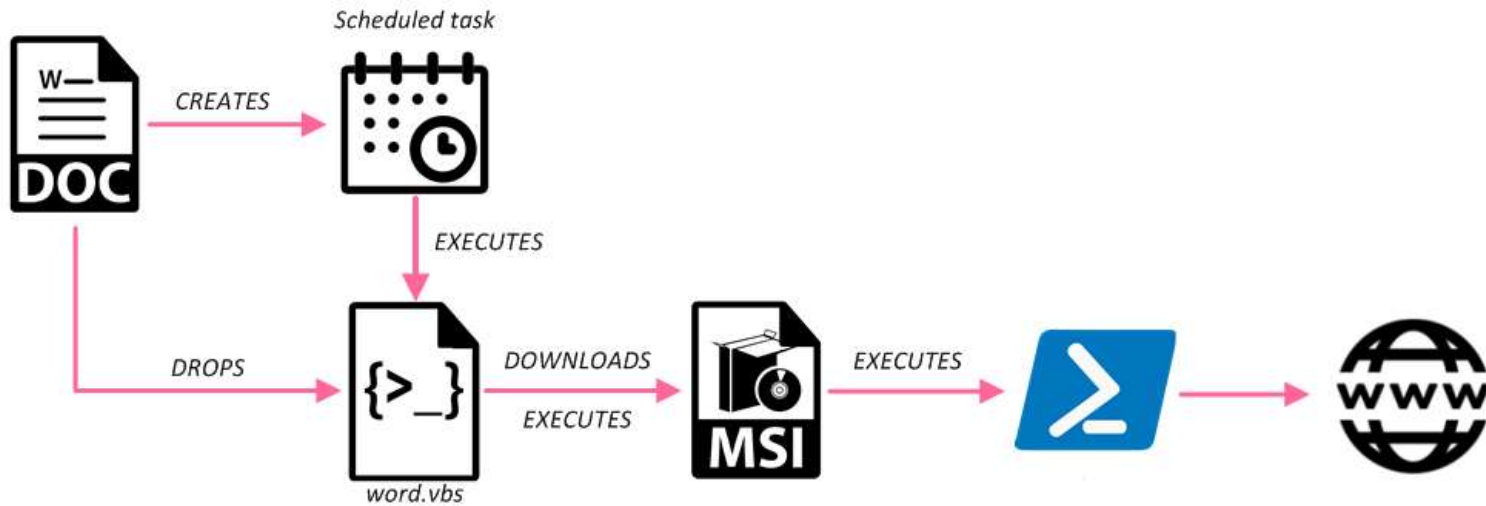
April 11, 2020

Marc Ochsenmeier

[@ochsenmeier](#)

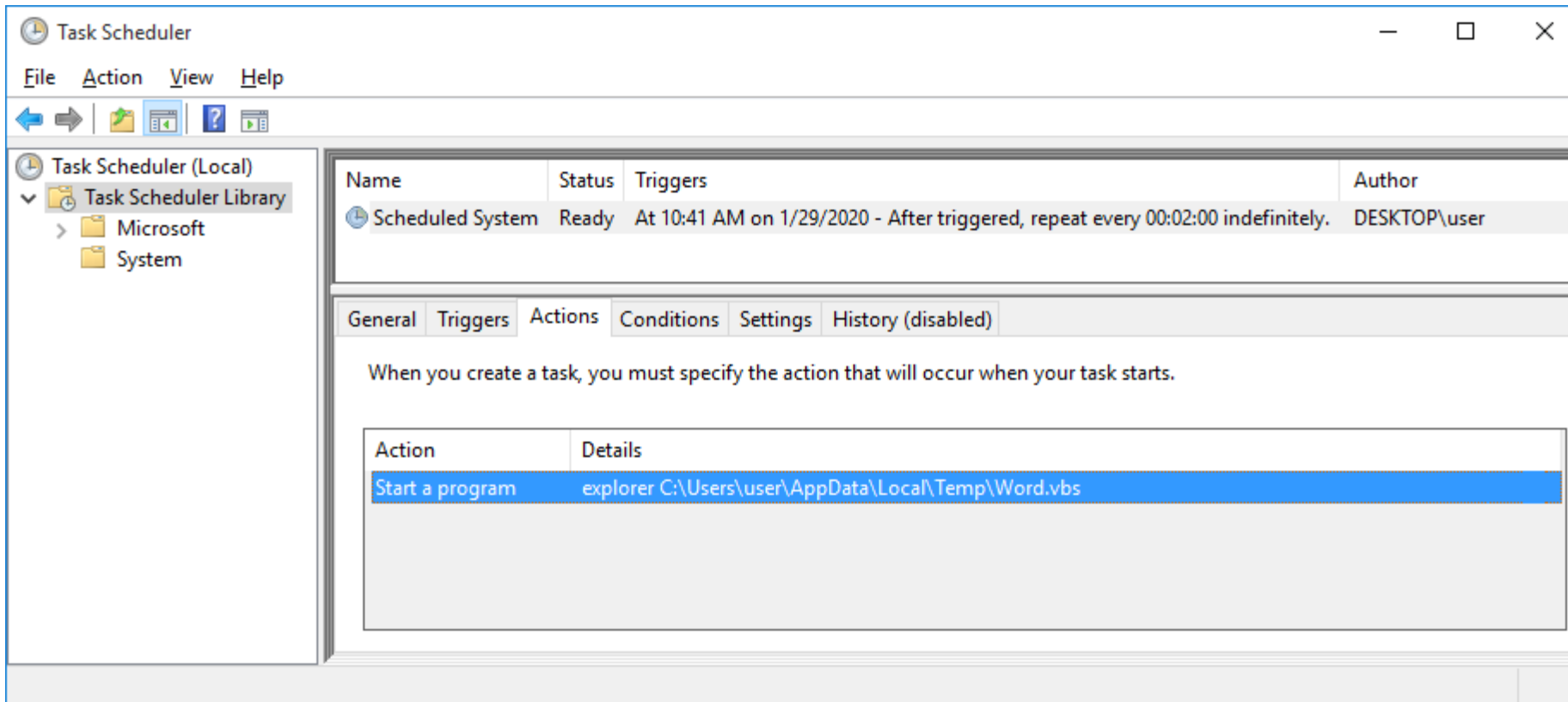
www.winitor.com

- Malware creates scheduled Task > [MITRE - T1053](#)



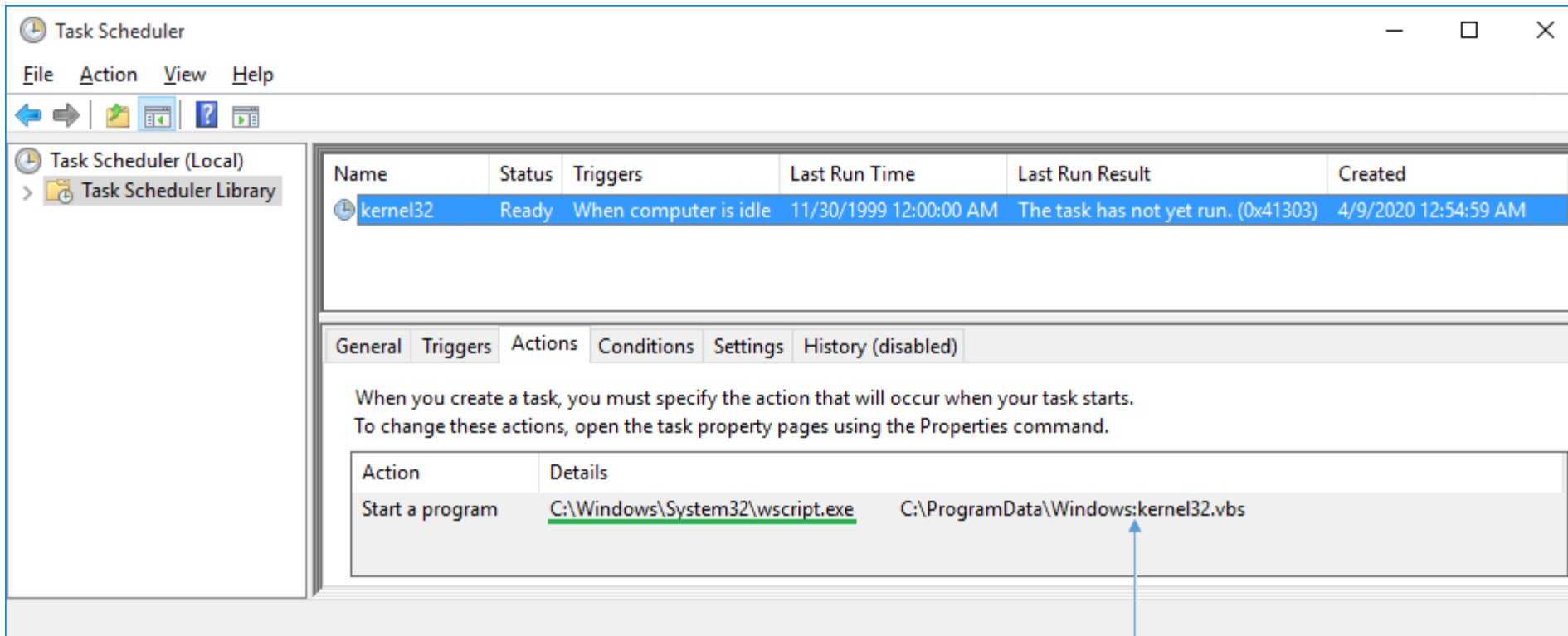
<https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/>

- Malware creates scheduled Task > [MITRE - T1053](#)



<https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/>

- Malware creates scheduled Task > [MITRE - T1053](#)



<https://blog.talosintelligence.com/2017/03/dnsmessenger.html>

- Malware often creates scheduled Task(s) to...
 - Achieve persistence
 - Launch next step of infection
 - Obfuscate Kill chain
 - Bypass UAC
 - Bypass File permissions

The image displays two screenshots from Sysinternals tools. The top screenshot is Process Explorer, showing a list of processes. The bottom screenshot is Process Monitor, showing a log of system events.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-CHRRD1G\user]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Integrity	ASLR
csrss.exe		1.624 K	2.376 K	528				n/a
wininit.exe		1.284 K	1.680 K	612				n/a
services.exe		4.396 K	6.772 K	688				n/a
svchost.exe		5.948 K	9.796 K	1364	Host Process for Windows Services	Microsoft Corporation	System	ASLR
notepad.exe		2.584 K	2.176 K	3140	Notepad	Microsoft Corporation	Medium	ASLR
notepad.exe		2.416 K	3.388 K	7776	Notepad	Microsoft Corporation	High	ASLR

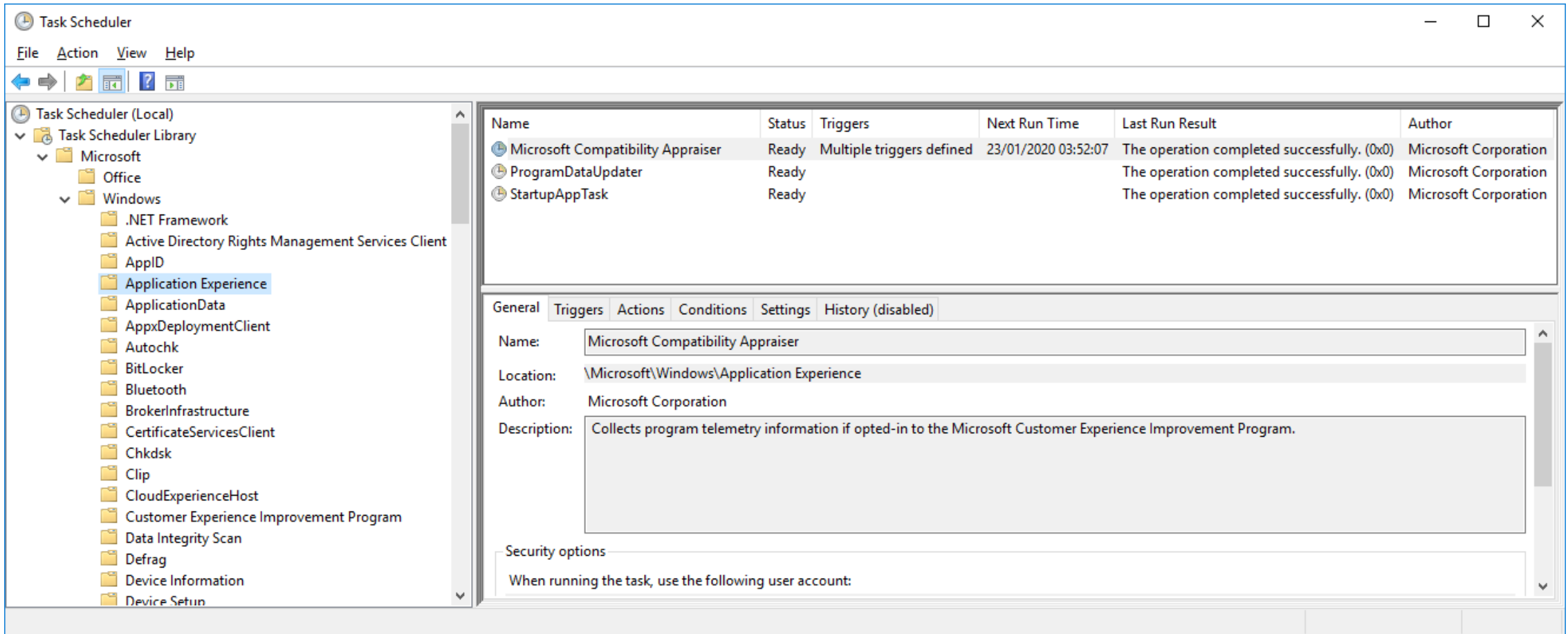
CPU Usage: 2.70% | Commit Charge: 10.32% | Processes: 120 | Physical Usage: 10.89%

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Detail
13:42:35,1629442	Explorer.EXE	4984	Thread Create		Thread ID: 6376
13:42:36,2513409	svchost.exe	1364	Process Create	C:\Windows\System32\notepad.exe	PID: 6048, Command line: C:\Windows\System32\notepad.exe
13:42:36,2513478	notepad.exe	6048	Process Start		Parent PID: 1364, Command line: C:\Windows\System32\notepad.exe, ...
13:42:36,2596391	notepad.exe	6048	Load Image	C:\Windows\System32\sechost.dll	Image Base: 0x7f897f0000, Image Size: 0x5b000
13:42:36,2597478	notepad.exe	6048	Load Image	C:\Windows\System32\mact4.dll	Image Base: 0x7f898110000, Image Size: 0x11f000

Showing 174 of 139.306 events (0.1%) | Backed by virtual memory

- Windows uses Task Scheduler intensively



- Enumerate scheduled Tasks

```
C:\Windows\System32\cmd.exe
C:\Windows\System32\Tasks>schtasks /fo list
Folder: \Microsoft\Office
HostName: DESKTOP-CHRRD1G
TaskName: \Microsoft\Office\Office 15 Subscription Heartbeat
Next Run Time: 20/01/2020 06:52:36
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Office
HostName: DESKTOP-CHRRD1G
TaskName: \Microsoft\Office\OfficeTelemetryAgentFallBack2016
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Office
HostName: DESKTOP-CHRRD1G
TaskName: \Microsoft\Office\OfficeTelemetryAgentLogOn2016
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Windows\.NET Framework
HostName: DESKTOP-CHRRD1G
TaskName: \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Windows\Application Experience
HostName: DESKTOP-CHRRD1G
TaskName: \Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser
Next Run Time: 20/01/2020 03:10:45
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Windows\Application Experience
HostName: DESKTOP-CHRRD1G
TaskName: \Microsoft\Windows\Application Experience\StartupAppTask
```

```
C:\Windows\System32\cmd.exe - powershell
PS C:\Windows\System32\Tasks> Get-ScheduledTask

TaskPath                TaskName                State
-----
\Microsoft\Office\      Office 15 Subscription Heartbeat Ready
\Microsoft\Office\      OfficeTelemetryAgentFallBack2016 Ready
\Microsoft\Office\      OfficeTelemetryAgentLogOn2016 Ready
\Microsoft\Windows\.NET Framework\ .NET Framework NGEN v4.0.30319 Ready
\Microsoft\Windows\.NET Framework\ .NET Framework NGEN v4.0.30319 64 Ready
\Microsoft\Windows\.NET Framework\ .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\.NET Framework\ .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Ready
\Microsoft\Windows\AppID\ PolicyConverter Disabled
\Microsoft\Windows\AppID\ VerifiedPublisherCertStoreCheck Disabled
\Microsoft\Windows\Application Experience\ Microsoft Compatibility Appraiser Ready
\Microsoft\Windows\Application Experience\ ProgramDataUpdater Ready
\Microsoft\Windows\Application Experience\ StartupAppTask Ready
\Microsoft\Windows\ApplicationData\ appuriverifierdaily Ready
\Microsoft\Windows\ApplicationData\ appuriverifierinstall Ready
\Microsoft\Windows\ApplicationData\ CleanupTemporaryState Ready
\Microsoft\Windows\ApplicationData\ DsSvcCleanup Ready
\Microsoft\Windows\AppxDeploymentClient\ Pre-staged app cleanup Disabled
\Microsoft\Windows\Data Integrity Scan\ Data Integrity Scan Ready
\Microsoft\Windows\Data Integrity Scan\ Data Integrity Scan for Crash ... Ready
\Microsoft\Windows\Defrag\ ScheduledDefrag Disabled
\Microsoft\Windows\Device Information\ Device Ready
\Microsoft\Windows\Diagnosis\ Scheduled Ready
\Microsoft\Windows\DiskCleanup\ SilentCleanup Ready
\Microsoft\Windows\DiskDiagnostic\ Microsoft-Windows-DiskDiagnost... Ready
```

```
Windows PowerShell
PS C:\Users\user> (Get-ScheduledTask).count
105
```

- Enumerate scheduled Tasks

The screenshot shows the Autoruns application window with the following details:

- Window Title: Autoruns - Sysinternals: www.sysinternals.com
- Menu: File, Entry, Options, Help
- Filter: (empty)
- Navigation: KnownDLLs, Winlogon, Winsock Providers, Print Monitors, LSA Providers, Network Providers, WMI, Office, Everything, Logon, Explorer, Internet Explorer, Scheduled Tasks, Services, Drivers, Codecs, Boot Execute, Image Hijacks, AppInit
- Table of Scheduled Tasks:

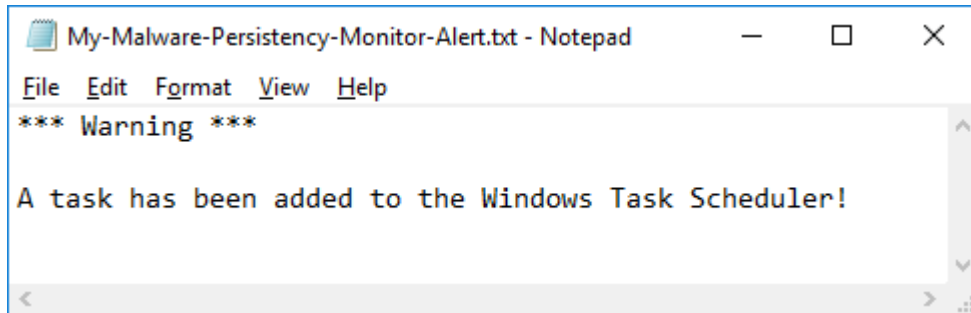
Autorun Entry	Description	Publisher	Image Path
<input checked="" type="checkbox"/> \Microsoft\Windows\Diagnosis\Scheduled	Scripted Diagnostics Scheduled Task	(Verified) Microsoft Windows	c:\windows\system32\sdiagschd.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\DiskCleanup\SilentCleanup	Disk Space Cleanup Manager for Windows	(Verified) Microsoft Windows	c:\windows\system32\cleanmgr.exe
<input checked="" type="checkbox"/> \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector	Windows Disk Failure Diagnostic Module	(Verified) Microsoft Windows	c:\windows\system32\dfds.dll
<input type="checkbox"/> \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver	Windows Disk Diagnostic User Resolver	(Verified) Microsoft Windows	c:\windows\system32\dfdewiz.exe
<input checked="" type="checkbox"/> \Microsoft\Windows\DiskFootprint\Diagnosics	DiskSnapshot.exe	(Verified) Microsoft Windows	c:\windows\system32\disksnapshot.exe
<input checked="" type="checkbox"/> \Microsoft\Windows\Feedback\Siuf\DmClient	Microsoft Feedback SIUF Deployment Ma...	(Verified) Microsoft Windows	c:\windows\system32\dmclient.exe
<input type="checkbox"/> \Microsoft\Windows\File Classification Infrastructure\Property Definition Sync	Microsoft® File Server Resource Manage...	(Verified) Microsoft Windows	c:\windows\system32\smclient.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\FileHistory\File History (maintenance mode)	File History Task Handler	(Verified) Microsoft Windows	c:\windows\system32\fhtask.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\LanguageComponentsInstaller\Installation	LanguageComponentsInstaller Task	(Verified) Microsoft Windows	c:\windows\system32\languagecomponentsinstaller.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\Location\Notifications	Location Notification	(Verified) Microsoft Windows	c:\windows\system32\locationnotificationwindows.exe
<input checked="" type="checkbox"/> \Microsoft\Windows\Location\WindowsActionDialog	Windows Action Dialog Broker	(Verified) Microsoft Windows	c:\windows\system32\windowsactiondialog.exe
<input checked="" type="checkbox"/> \Microsoft\Windows\Maintenance\WinSAT	Windows System Assessment Tool API	(Verified) Microsoft Windows	c:\windows\system32\winsatapi.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\Maps\Maps ToastTask	MapsToastTask Task	(Verified) Microsoft Windows	c:\windows\system32\mapstoasttask.dll
<input type="checkbox"/> \Microsoft\Windows\Maps\MapsUpdateTask	MapsUpdateTask Task	(Verified) Microsoft Windows	c:\windows\system32\mapsupdatetask.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents	Microsoft Windows Memory Diagnostic Ta...	(Verified) Microsoft Windows	c:\windows\system32\memorydiagnostic.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic	Microsoft Windows Memory Diagnostic Ta...	(Verified) Microsoft Windows	c:\windows\system32\memorydiagnostic.dll
<input checked="" type="checkbox"/> \Microsoft\Windows\Mobile Broadband Accounts\MNO Metadata Parser	Mobile Broadband Account Experience Pa...	(Verified) Microsoft Windows	c:\windows\system32\mbaeparsertask.exe
<input checked="" type="checkbox"/> \Microsoft\Windows\MUI\ILRemove	MUI Language pack cleanup	(Verified) Microsoft Windows	c:\windows\system32\lremove.exe

Task details for cleanmgr.exe:

- cleanmgr.exe
- Size: 202 K
- Disk Space Cleanup Manager for Win Time: 7/9/2015 7:19 PM
- Microsoft Corporation Version: 10.0.10240.16384
- Command: "%windir%\system32\cleanmgr.exe" /autodean /d %systemdrive%

Status: Ready. No Filter.

- Monitor new entry in Windows Task Scheduler
 - Provide visible immediate Notification
 - Ease malware early triage
 - Trigger automation
 - Accelerate remediation

A screenshot of a Notepad window titled "My-Malware-Persistency-Monitor-Alert.txt - Notepad". The window contains the following text:

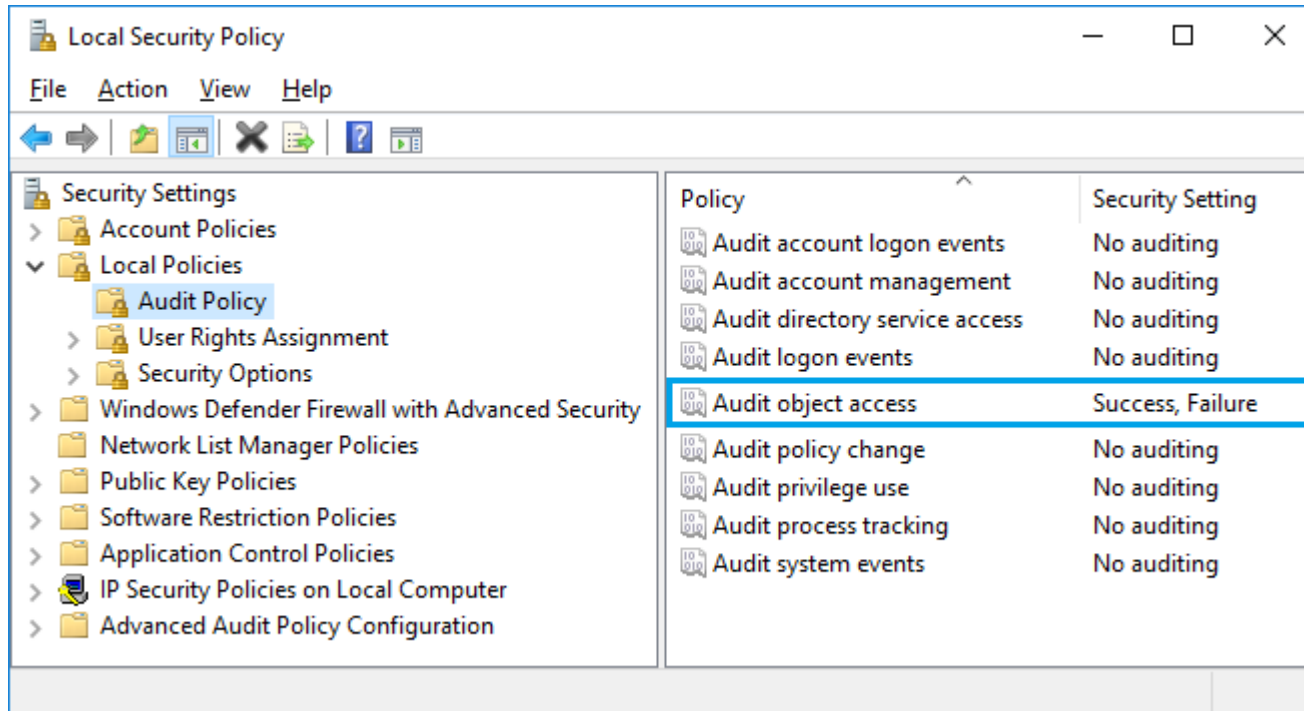
```
File Edit Format View Help
*** Warning ***

A task has been added to the Windows Task Scheduler!
```

- Install a Task Scheduler Monitor
 - 1. Enable Audit Policy
 - 2. Bind the appropriate Windows event(s)
 - 3. Setup the appropriate Task(s) | Action(s)
 - 4. Configure the appropriate condition(s)



- Install a Task Scheduler Monitor
 - 1 - Enable Audit Policy

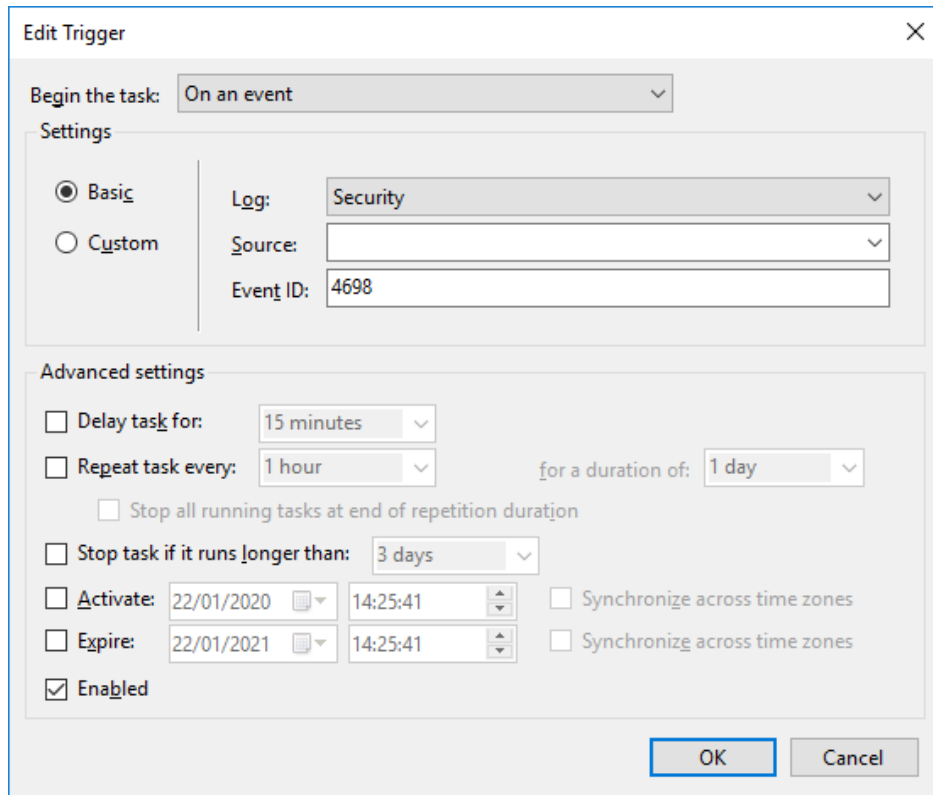


- Install a Task Scheduler Monitor
 - 2- Bind a Task to the appropriate Windows event(s)

ID	Description	Windows 7 / Server 2008 R2	Windows 10 / Server 2016
106	Scheduled task registered	x	
140	Scheduled task updated	x	
141	Scheduled task deleted	x	
4698	Scheduled task created		x
4699	Scheduled task deleted		x
4700	Scheduled task enabled		x
4701	Scheduled task disabled		x
4702	Scheduled task updated		x

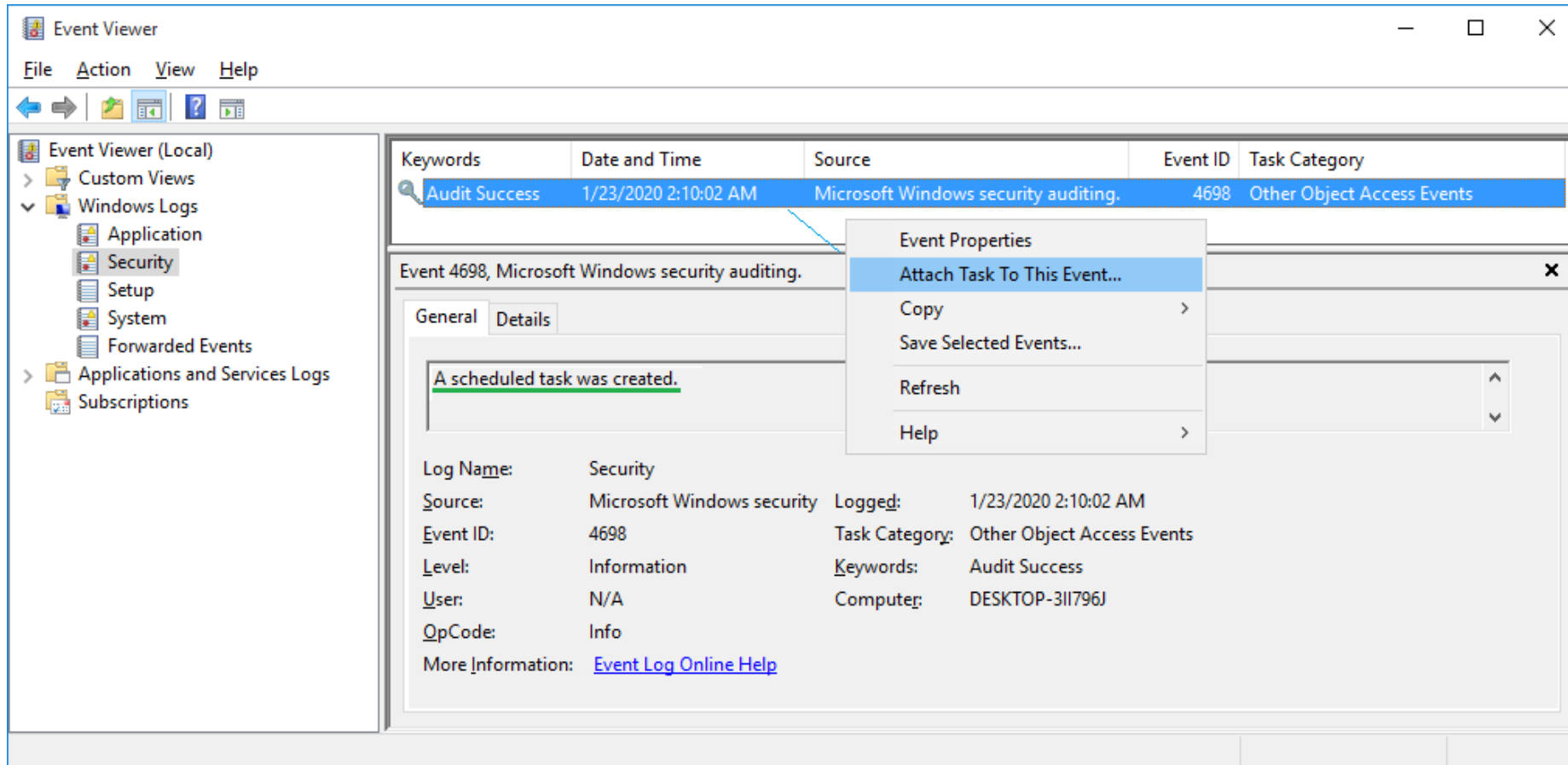
Advanced Audit Policy – which GPO corresponds with which Event ID
<https://girl-germs.com/?p=363>

- Install a Task Scheduler Monitor
 - 2 - Bind a Task to the appropriate Windows event(s)

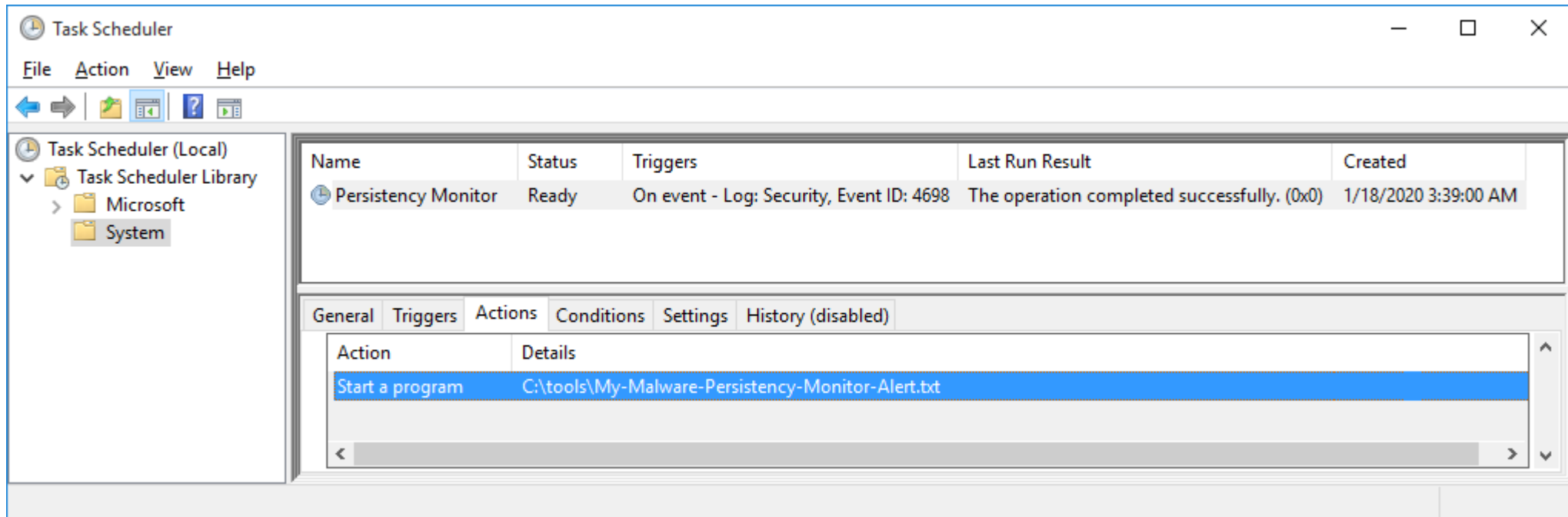


The screenshot shows the 'Edit Trigger' dialog box in Windows Task Scheduler. The 'Begin the task' dropdown is set to 'On an event'. Under the 'Settings' section, the 'Basic' radio button is selected. The 'Log' dropdown is set to 'Security', the 'Source' dropdown is empty, and the 'Event ID' text box contains '4698'. The 'Advanced settings' section includes several options: 'Delay task for' (15 minutes), 'Repeat task every' (1 hour) for a duration of '1 day', 'Stop all running tasks at end of repetition duration', 'Stop task if it runs longer than' (3 days), 'Activate' (22/01/2020 14:25:41), 'Expire' (22/01/2021 14:25:41), and 'Synchronize across time zones' (unchecked). The 'Enabled' checkbox is checked. 'OK' and 'Cancel' buttons are at the bottom.

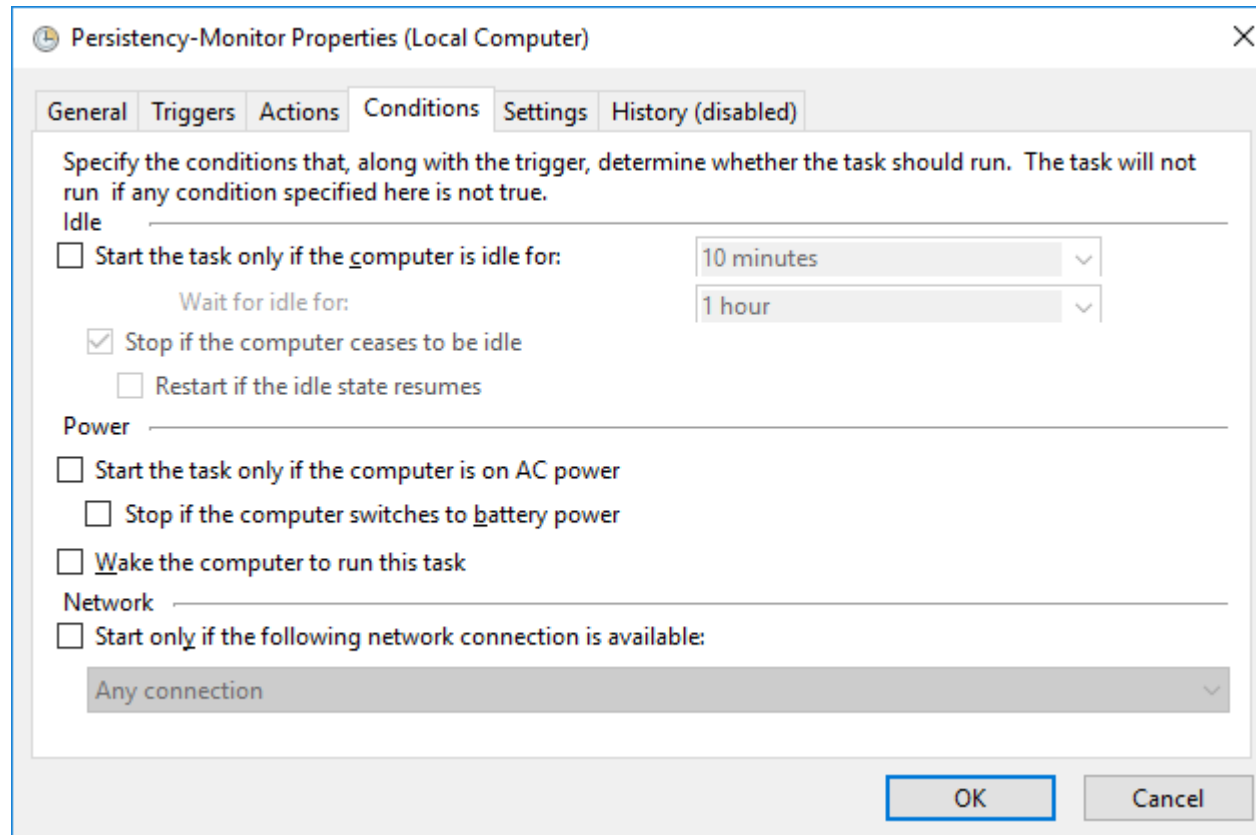
- Install a Task Scheduler Monitor
 - 2 - Bind the appropriate Windows Event to a Task



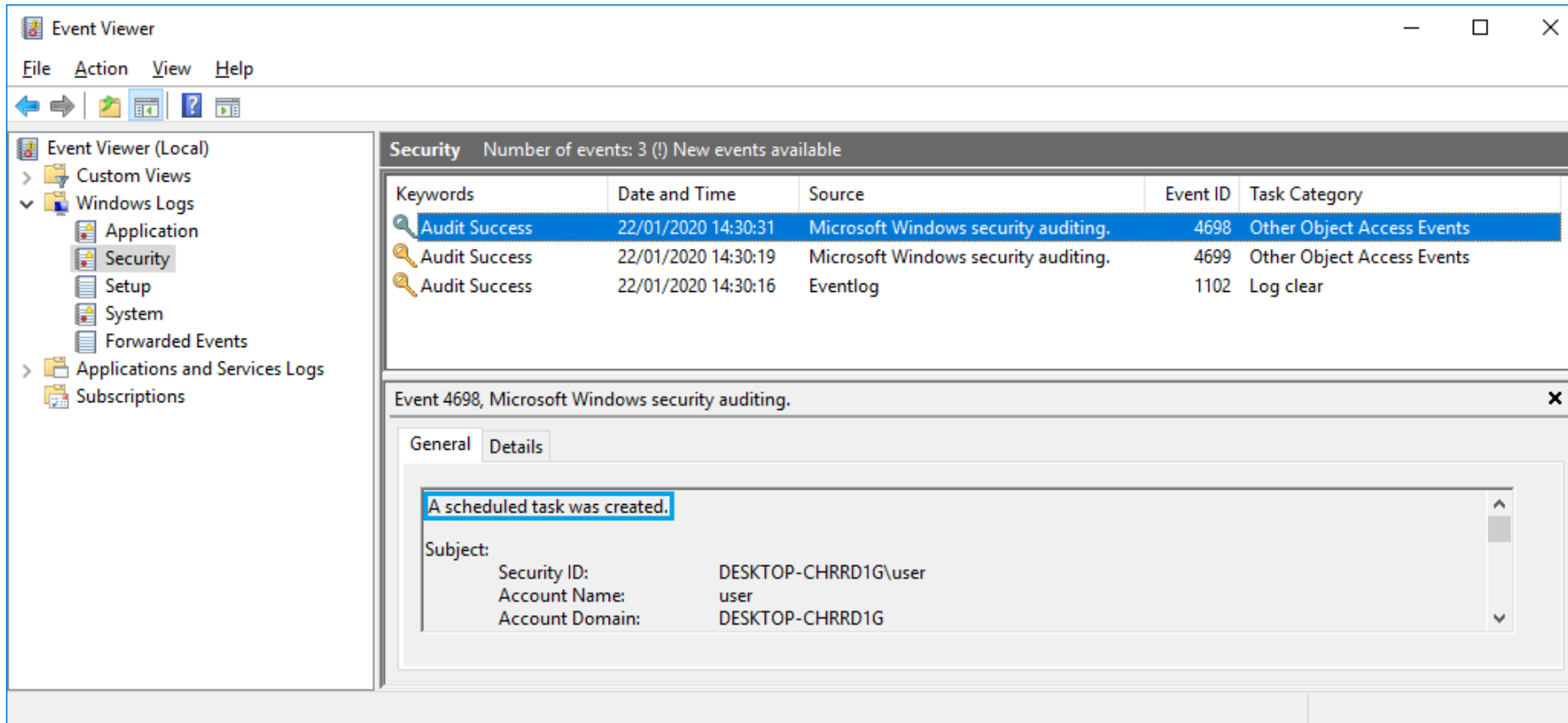
- Install a Task Scheduler Monitor
 - Setup the appropriate action(s)



- Install a Task Scheduler Monitor
 - 3 - Configure the appropriate condition(s)



- Events related to the Task Scheduler



The screenshot shows the Windows Event Viewer application. The left pane displays the tree view with 'Security' selected under 'Windows Logs'. The main pane shows a table of security events. The first event, ID 4698, is highlighted and its details are shown in the bottom pane. The event message is 'A scheduled task was created.' and the subject information is as follows:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	22/01/2020 14:30:31	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	22/01/2020 14:30:19	Microsoft Windows security auditing.	4699	Other Object Access Events
Audit Success	22/01/2020 14:30:16	Eventlog	1102	Log clear

Event 4698, Microsoft Windows security auditing.

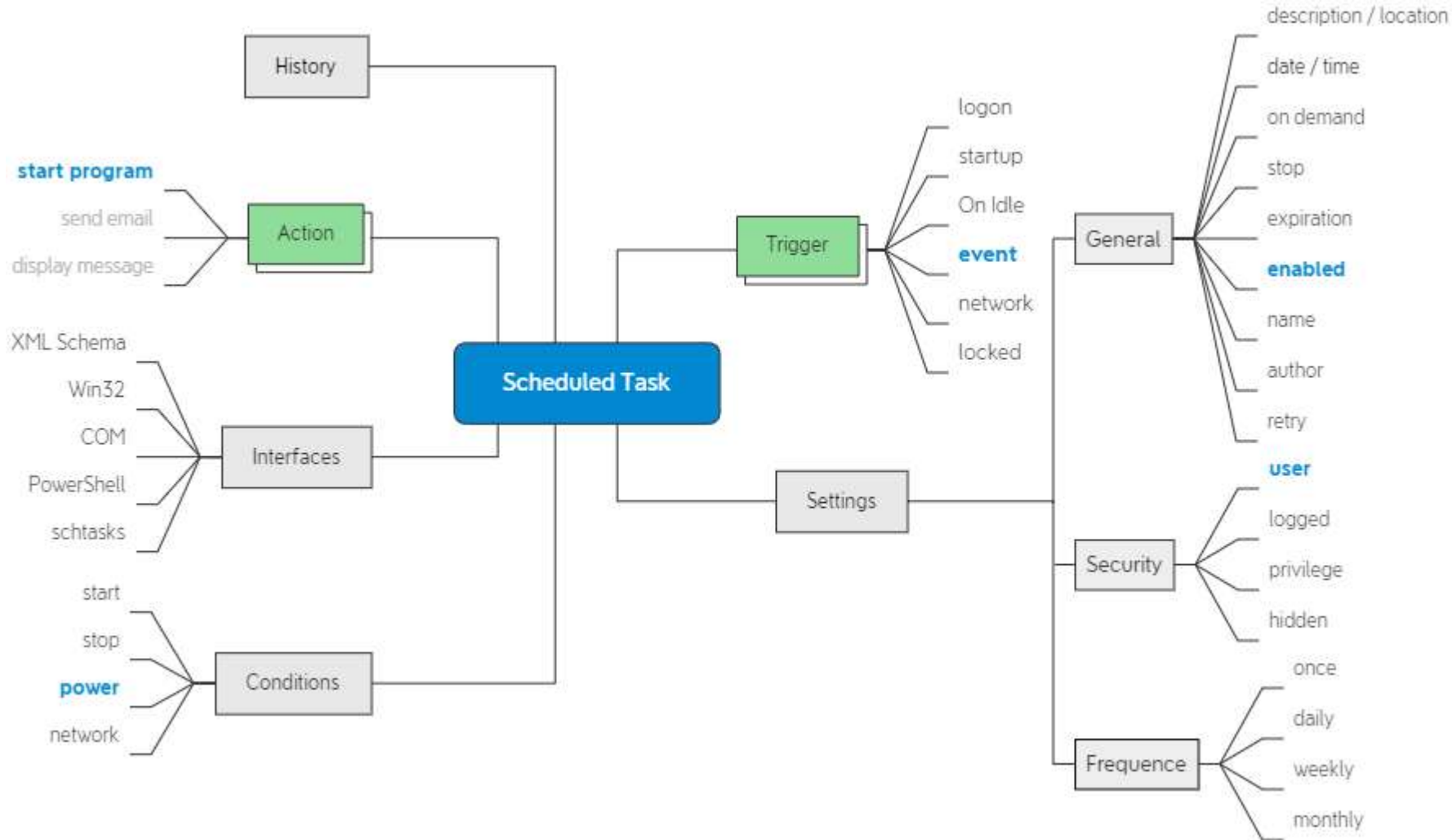
General Details

A scheduled task was created.

Subject:

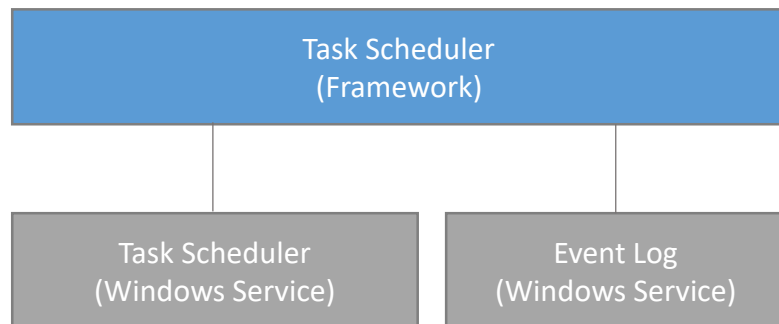
Security ID:	DESKTOP-CHRRD1G\user
Account Name:	user
Account Domain:	DESKTOP-CHRRD1G

- Configuration of a scheduled Task

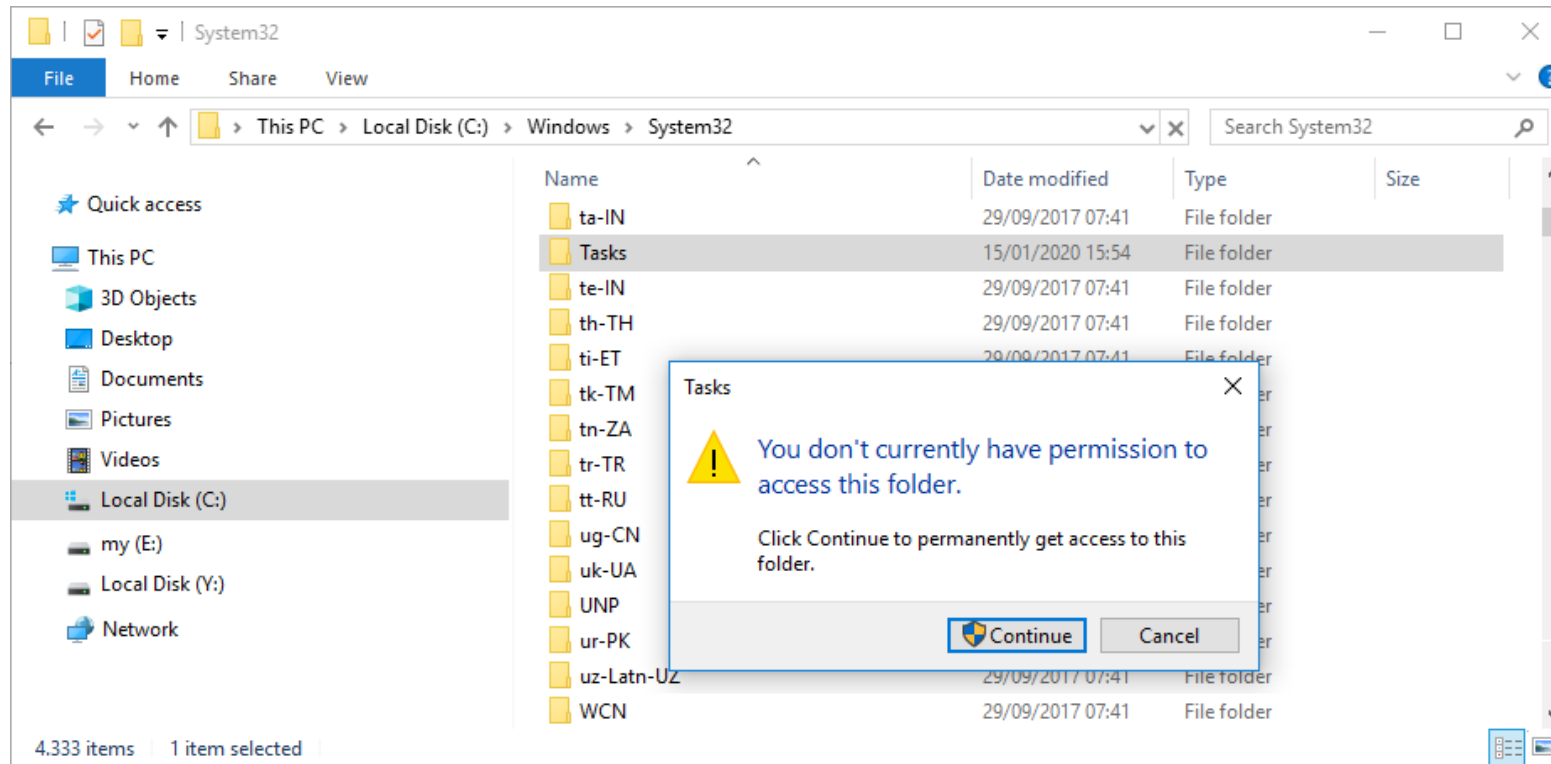


- Architecture

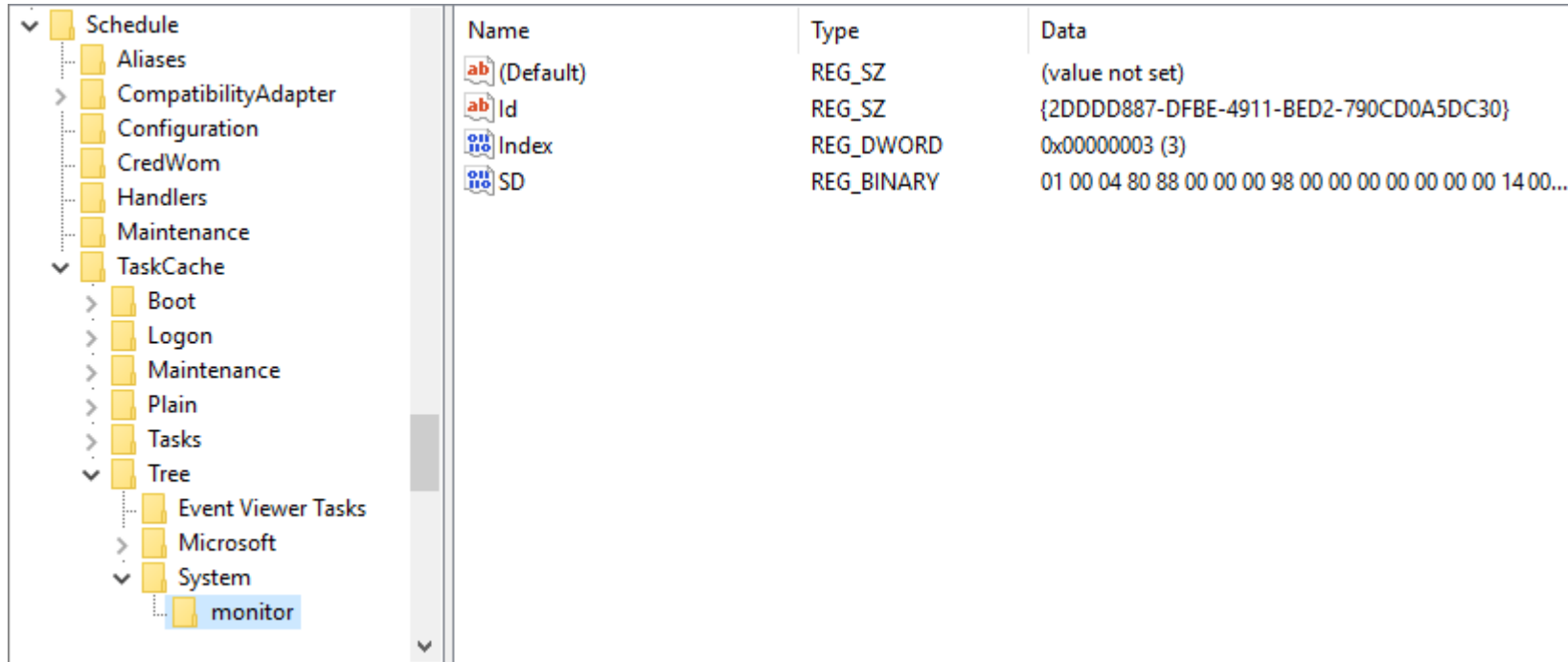
- The Task Scheduler is NOT the Windows Task Manager
- The Task Scheduler is NOT the Windows Task Scheduler Service
- The Task Scheduler is NOT the Windows Thread Scheduler



- Repository
 - Legacy: \Windows\Tasks
 - Preferred: \Windows\System32\Tasks



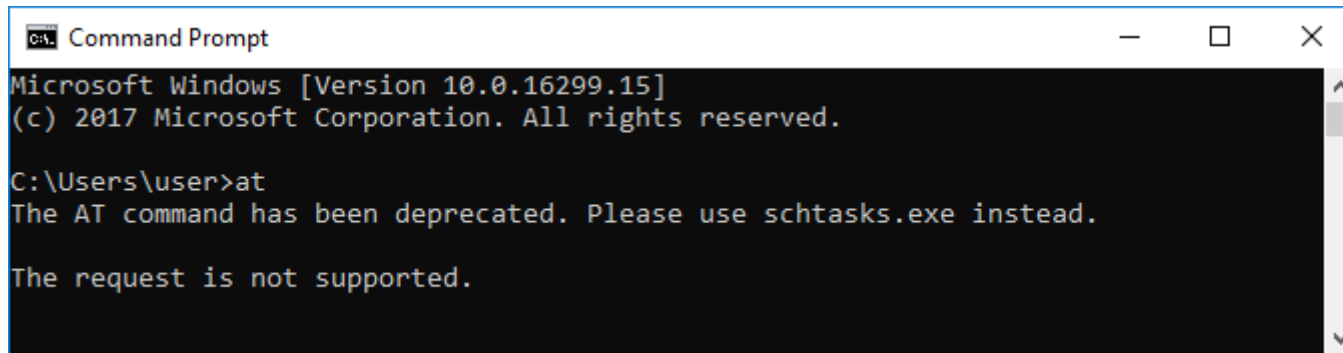
- Repository
 - Computer related settings



Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{2DDDD887-DFBE-4911-BED2-790CD0A5DC30}
Index	REG_DWORD	0x00000003 (3)
SD	REG_BINARY	01 00 04 80 88 00 00 00 98 00 00 00 00 00 00 14 00...

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree

- Some more details
 - at.exe is obsolete
 - eventtriggers.exe is replaced



```
Command Prompt
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user>at
The AT command has been deprecated. Please use schtasks.exe instead.

The request is not supported.
```

• References

- <https://attack.mitre.org/techniques/T1053/>
- <https://support.microsoft.com/en-us/help/939039/description-of-the-scheduled-tasks-in-windows-vista>
- <https://docs.microsoft.com/de-de/archive/blogs/wincat/trigger-a-powershell-script-from-a-windows-event>
- <https://blog.malwarebytes.com/cybercrime/2015/03/scheduled-tasks/>
- <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
- <https://girl-germs.com/?p=363>
- <https://docs.microsoft.com/en-us/windows/win32/taskschd/schtasks>
- <https://docs.microsoft.com/en-us/windows/win32/api/taskschd/index>