Windows Task Scheduler Monitor

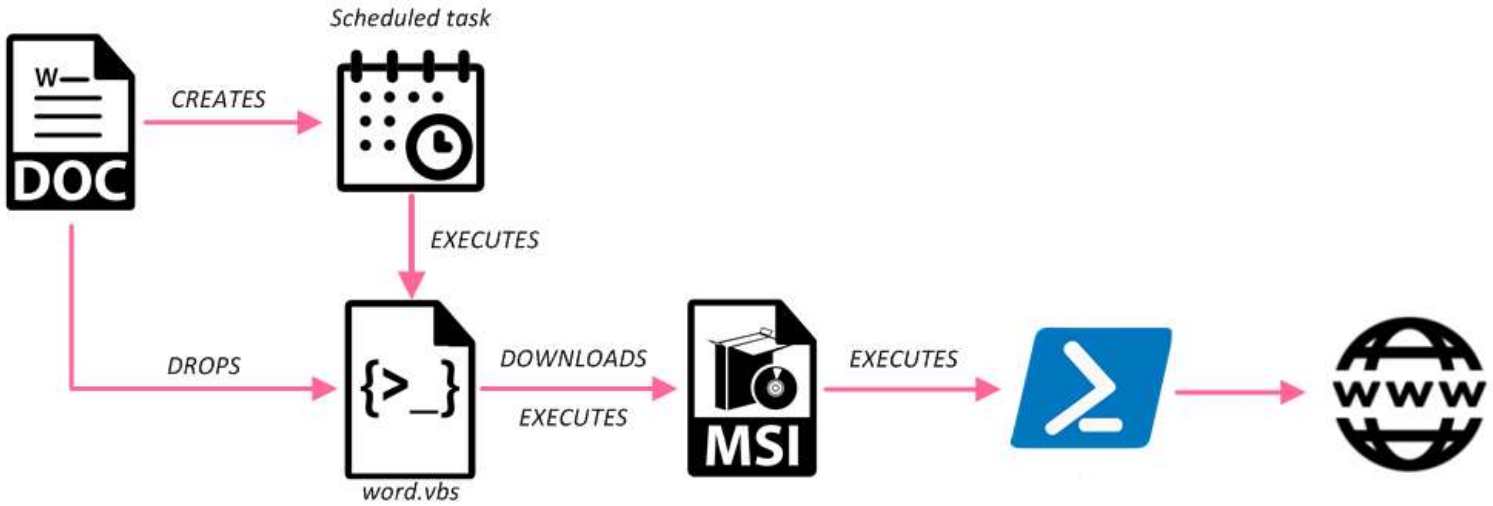
April 11, 2020

Marc Ochsenmeier

@ochsenmeier

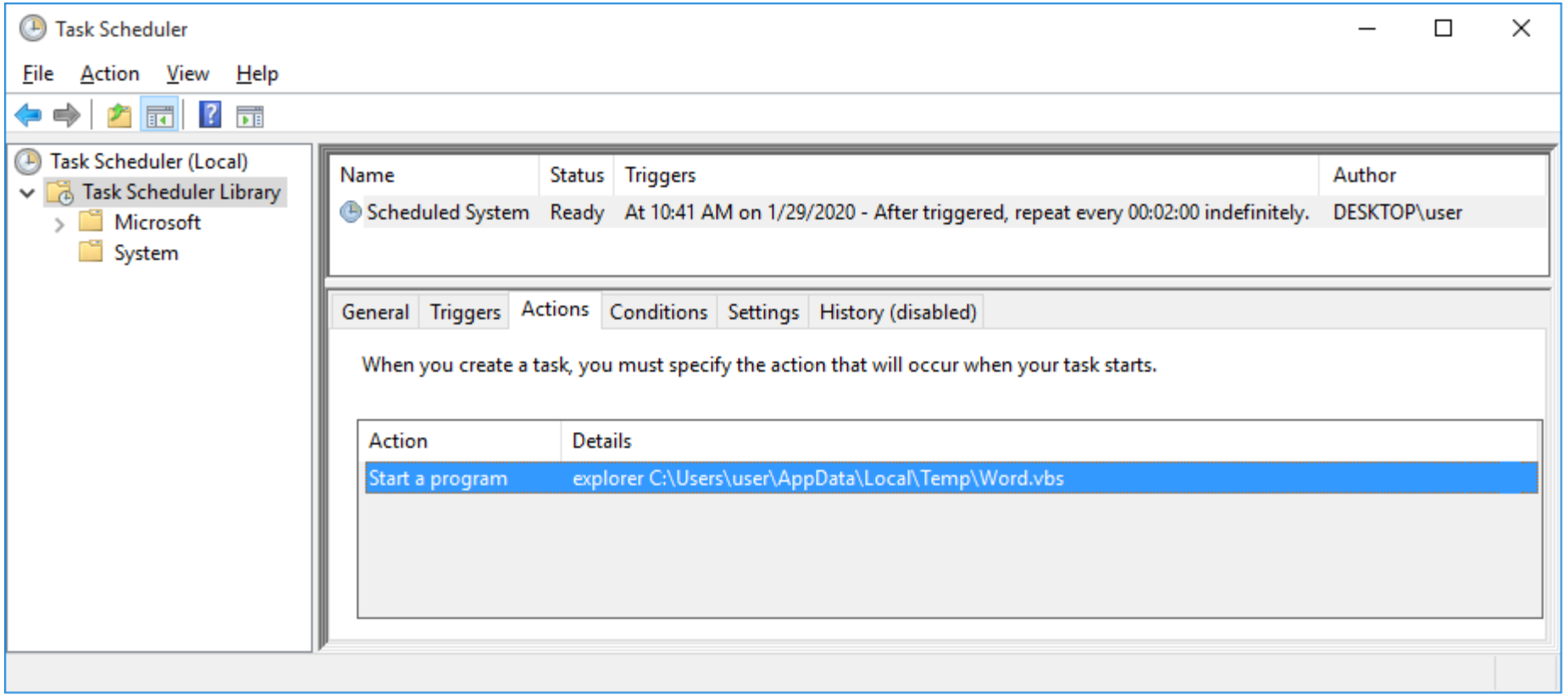
www.winitor.com

- Malware creates scheduled Task > [MITRE - T1053]



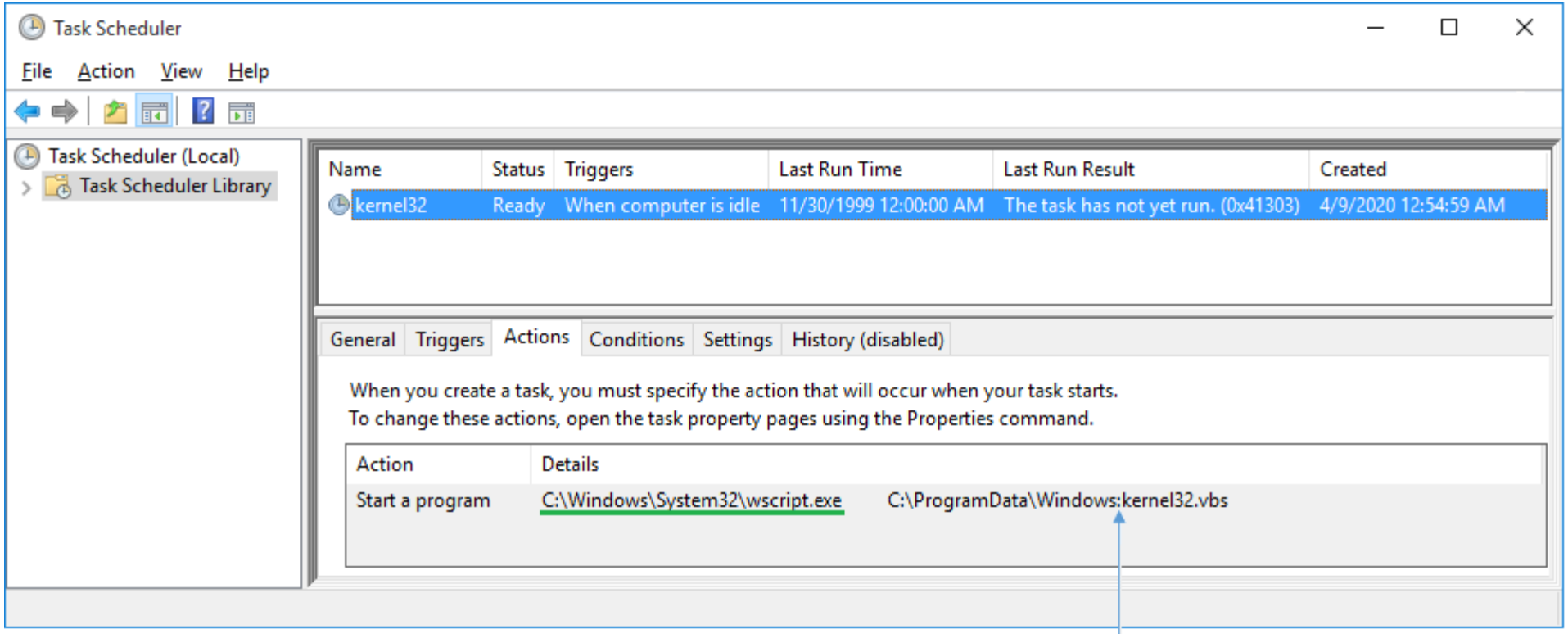
https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/

- Malware creates scheduled Task > MITRE - T1053



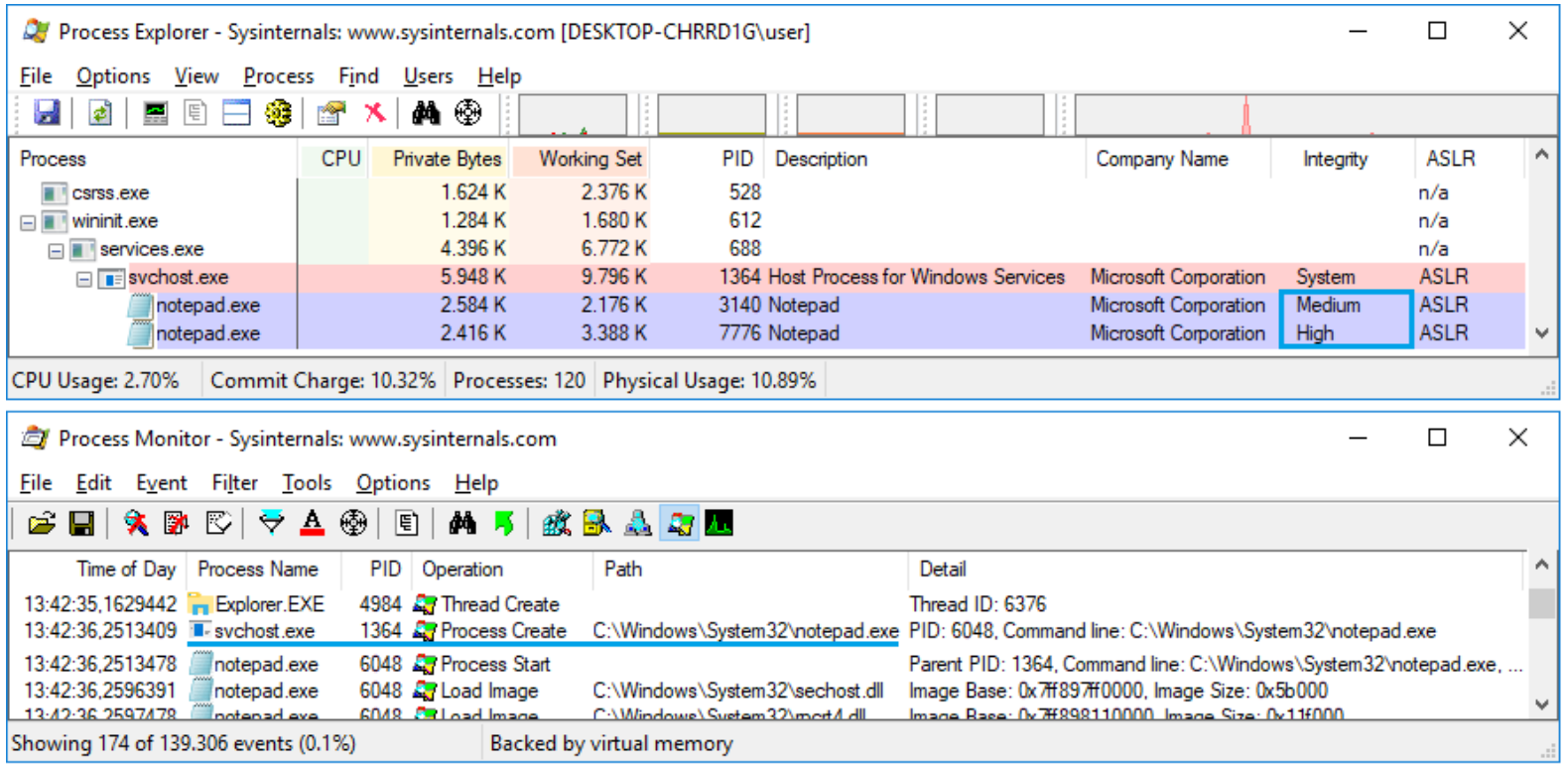
https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/

- Malware creates scheduled Task > MITRE - T1053



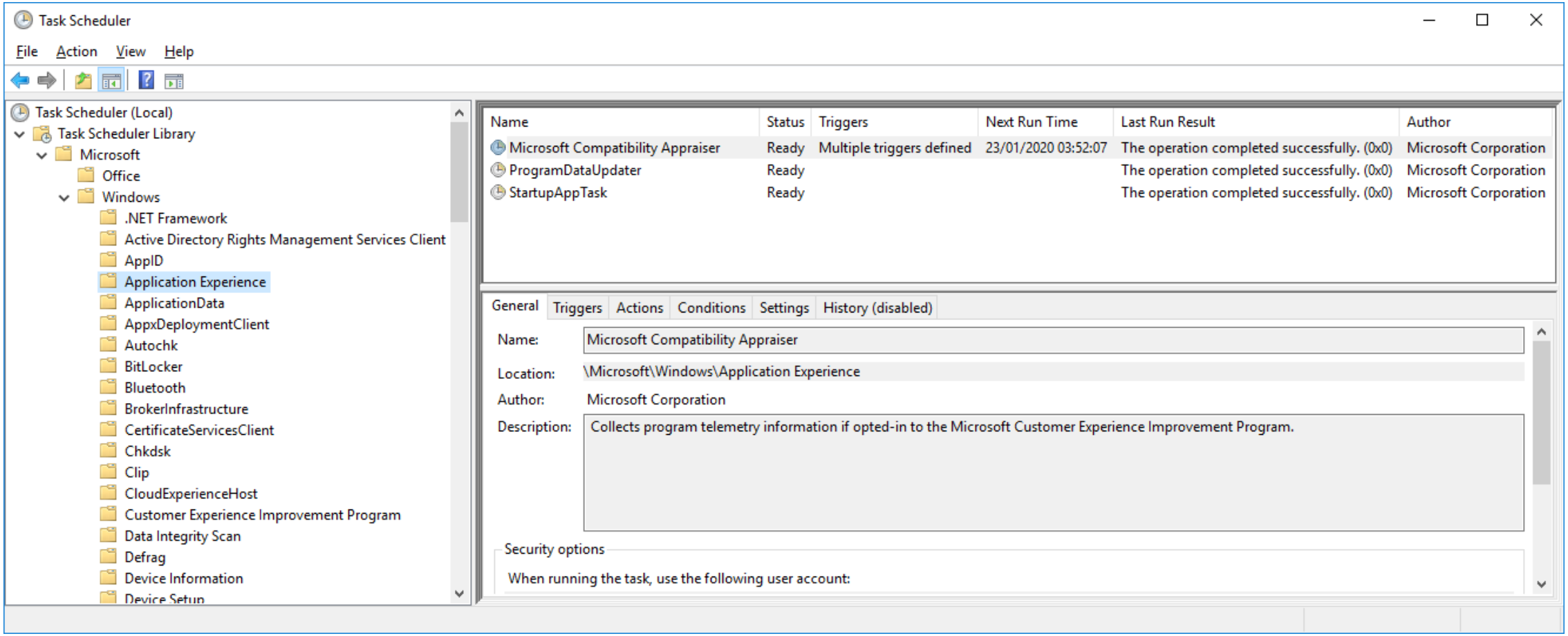
https://blog.talosintelligence.com/2017/03/dnsmessenger.html

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

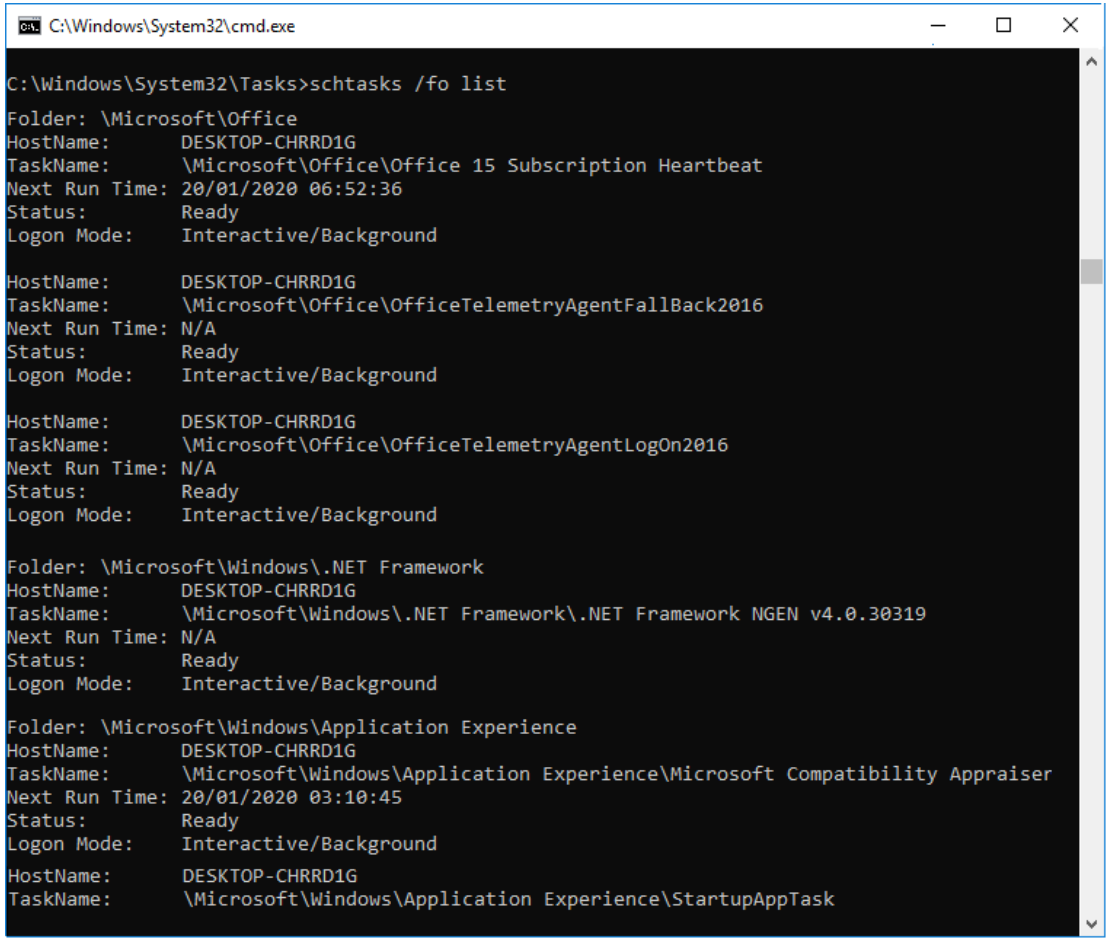


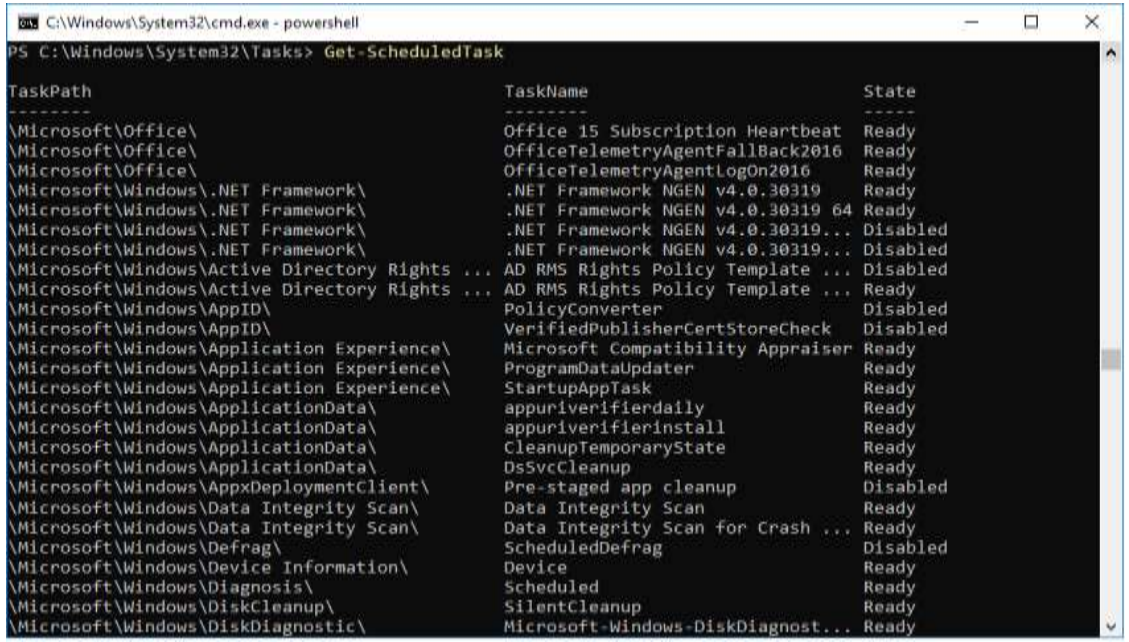
Windows Task Scheduler Monitor

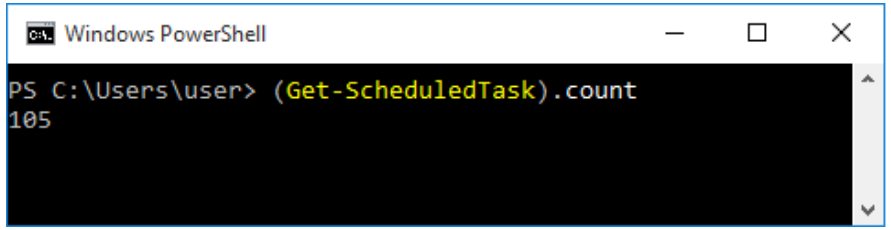
- Windows uses Task Scheduler intensively



- Enumerate scheduled Tasks

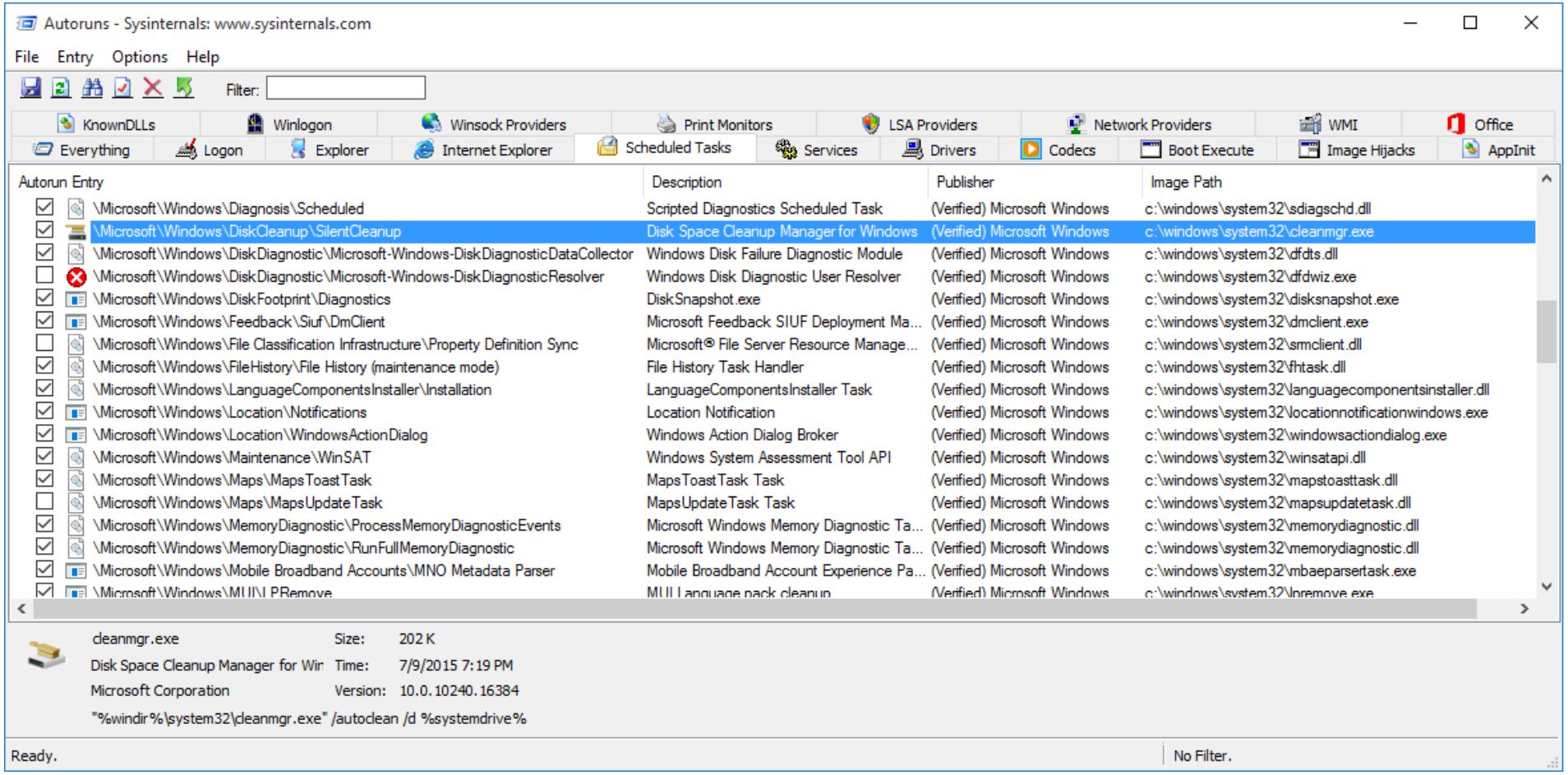






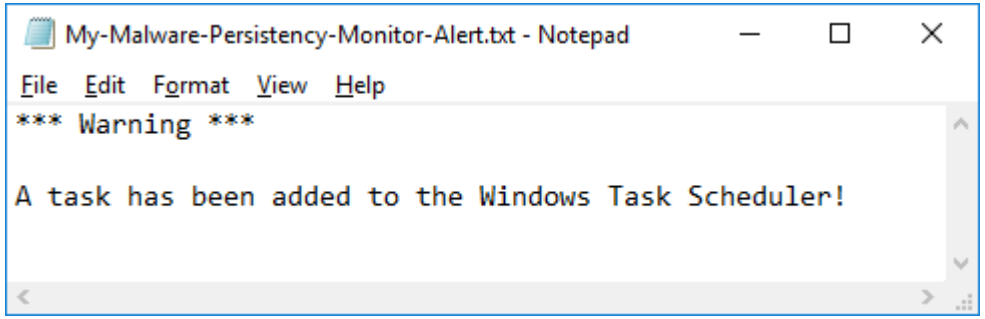
Windows Task Scheduler Monitor

- Enumerate scheduled Tasks



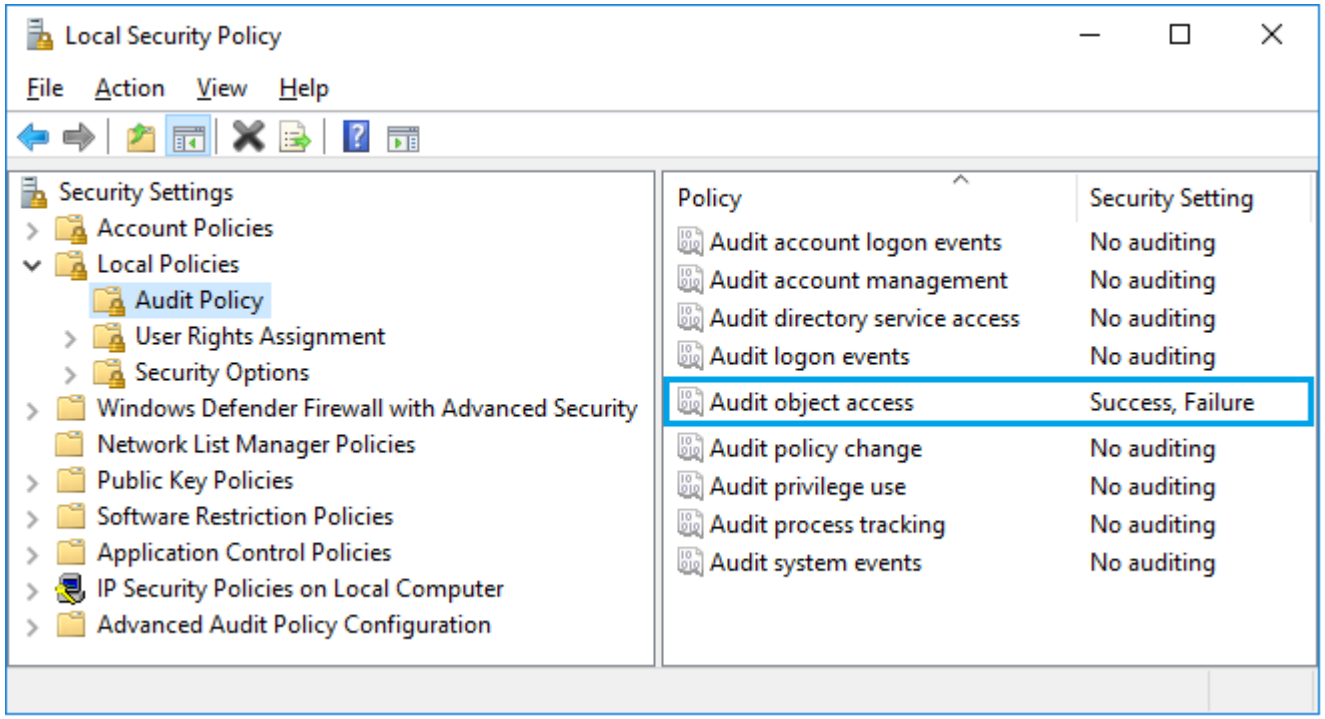
Windows Task Scheduler Monitor

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



- 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

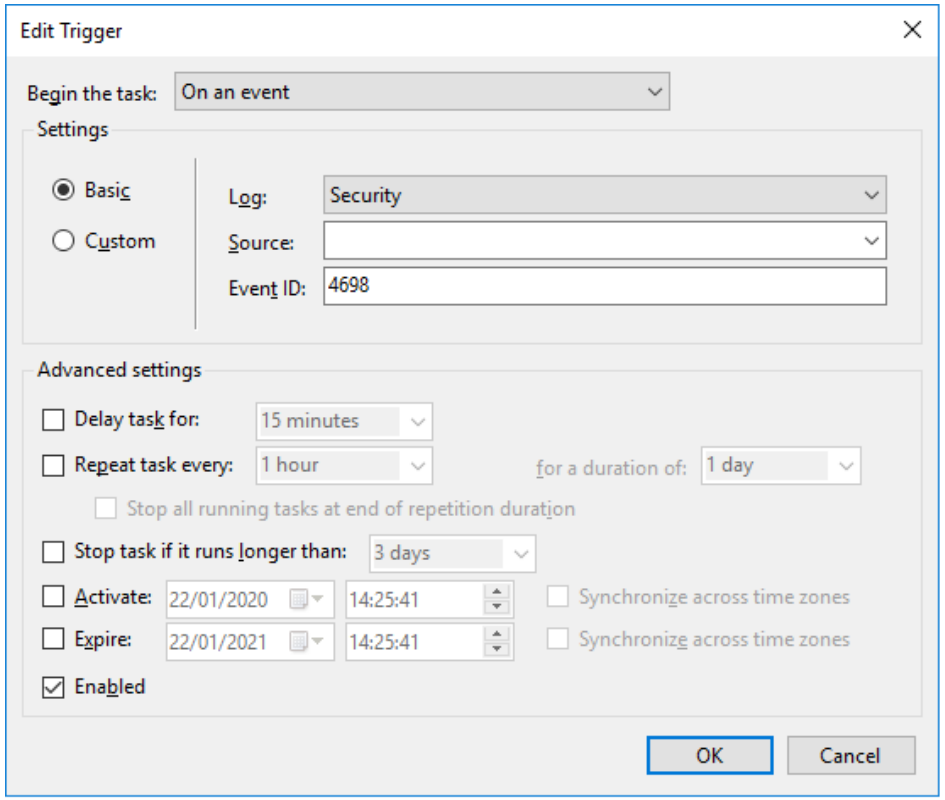


- Install a Task Scheduler Monitor
  - 2- Bind a Task to the appropriate Windows event(s)

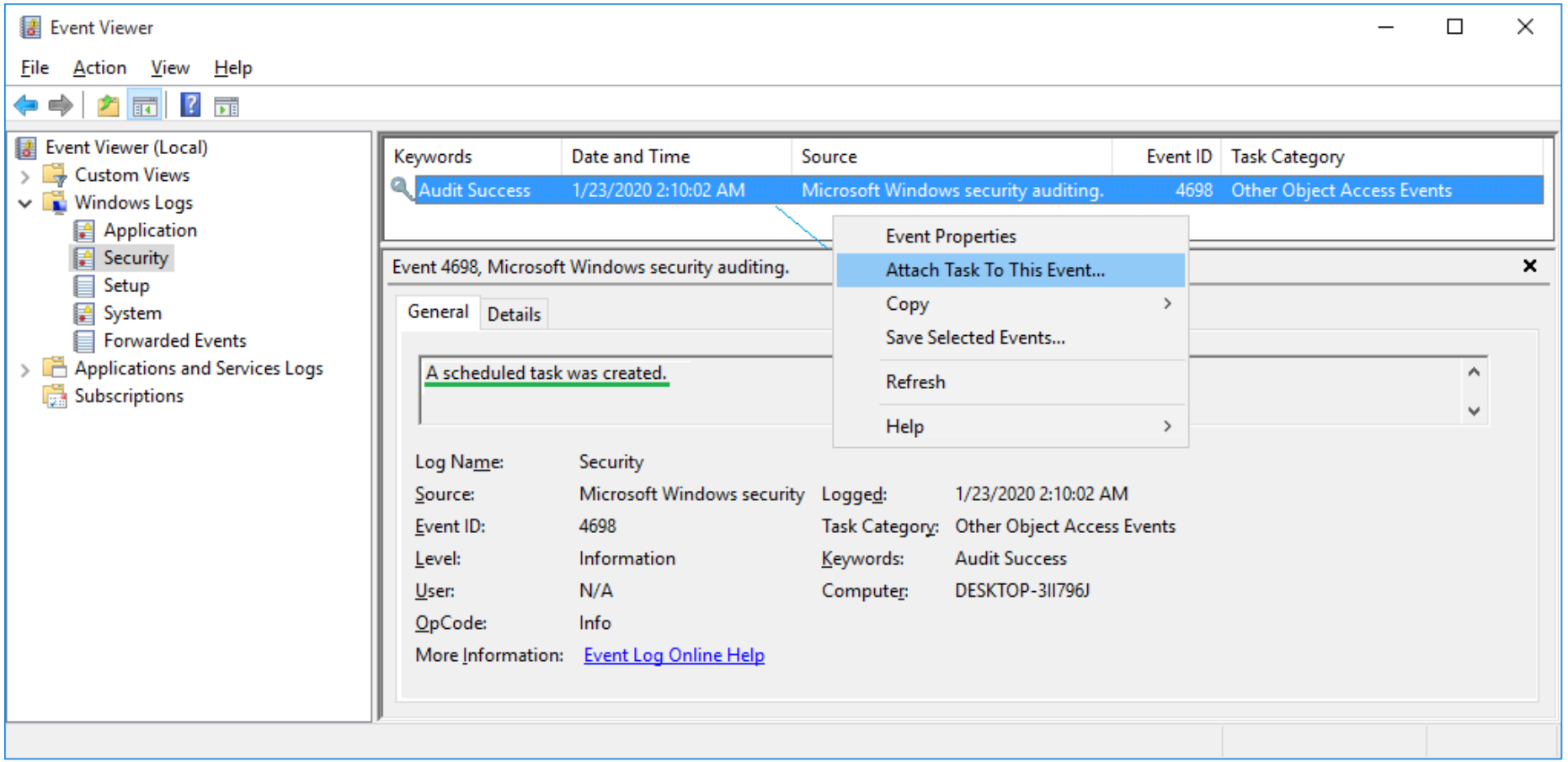
ID	Description	Windows 7 / Server 2008 R2	Windows 10 / Server 2016
106	Scheduled task registered	x	
140	Scheduled task updated	x	
141	Scheduled task deleted	x	
4698	Scheduled task created		x
4699	Scheduled task deleted		x
4700	Scheduled task enabled		x
4701	Scheduled task disabled		x
4702	Scheduled task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

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

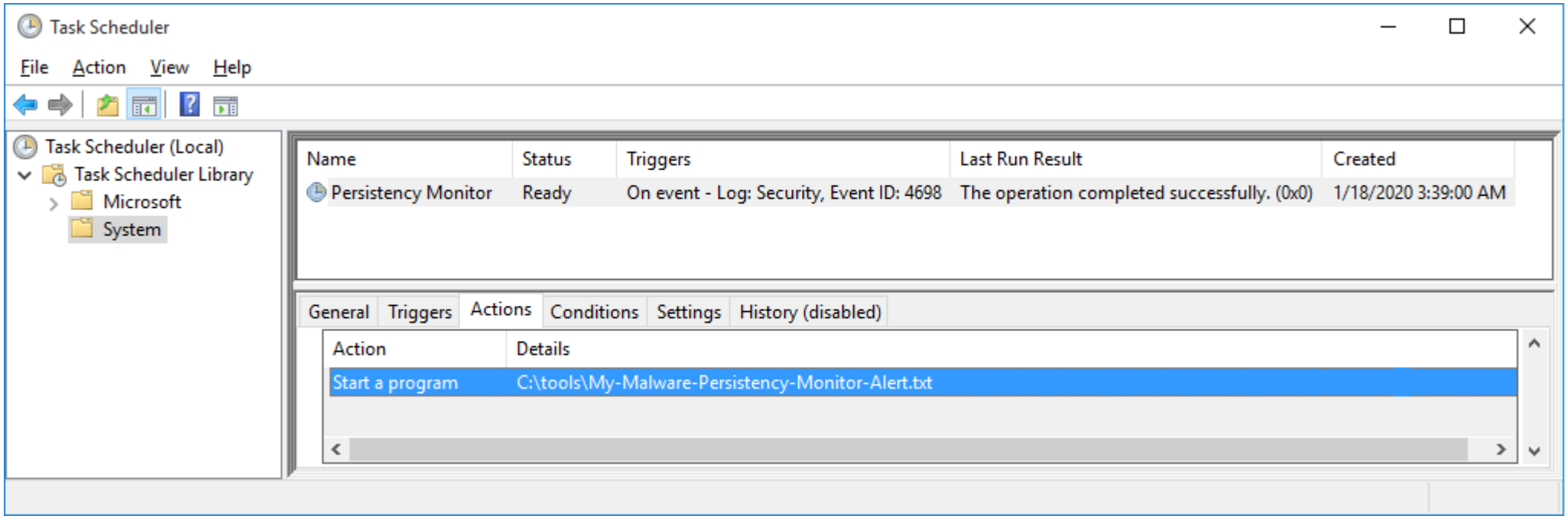
- Install a Task Scheduler Monitor
  - 2 - Bind a Task to the appropriate Windows event(s)



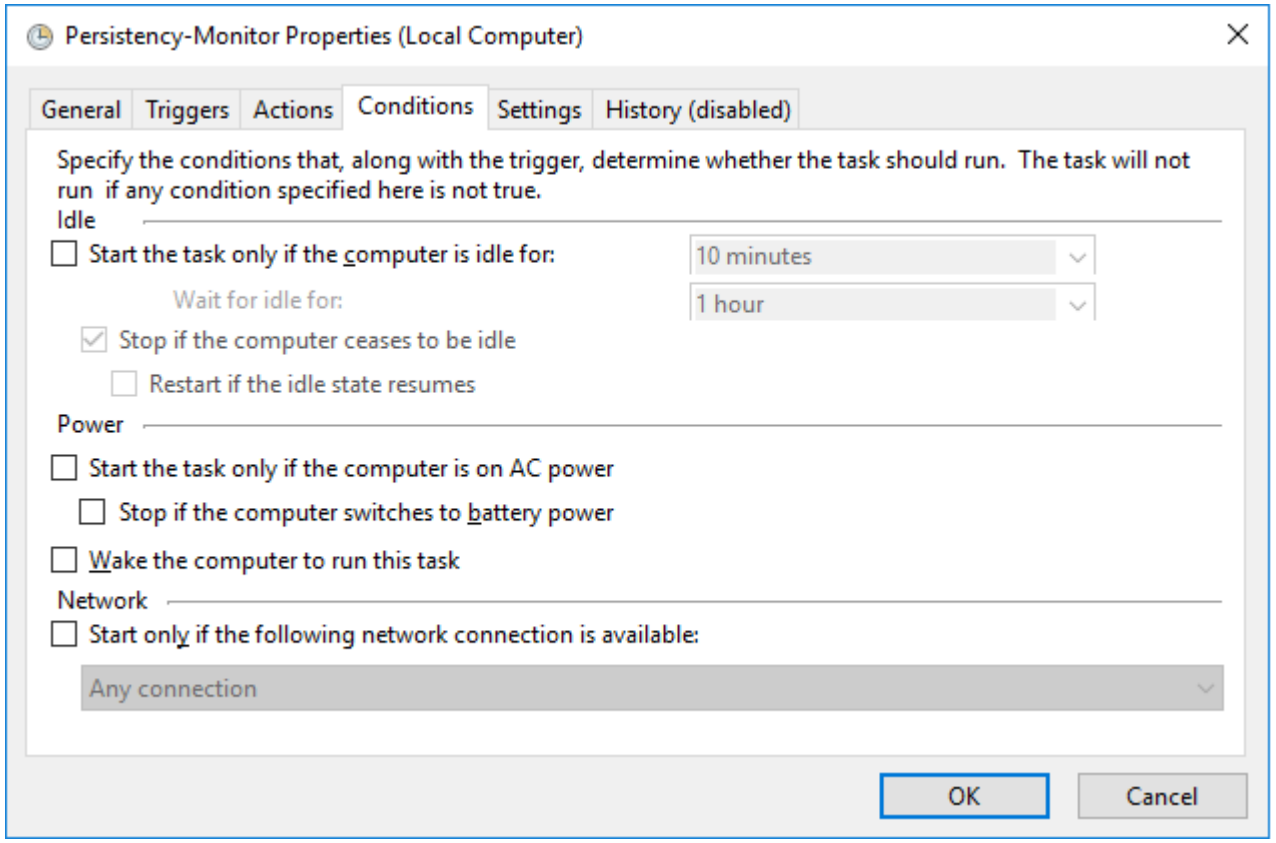
- Install a Task Scheduler Monitor
  - 2 - Bind the appropriate Windows Event to a Task



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

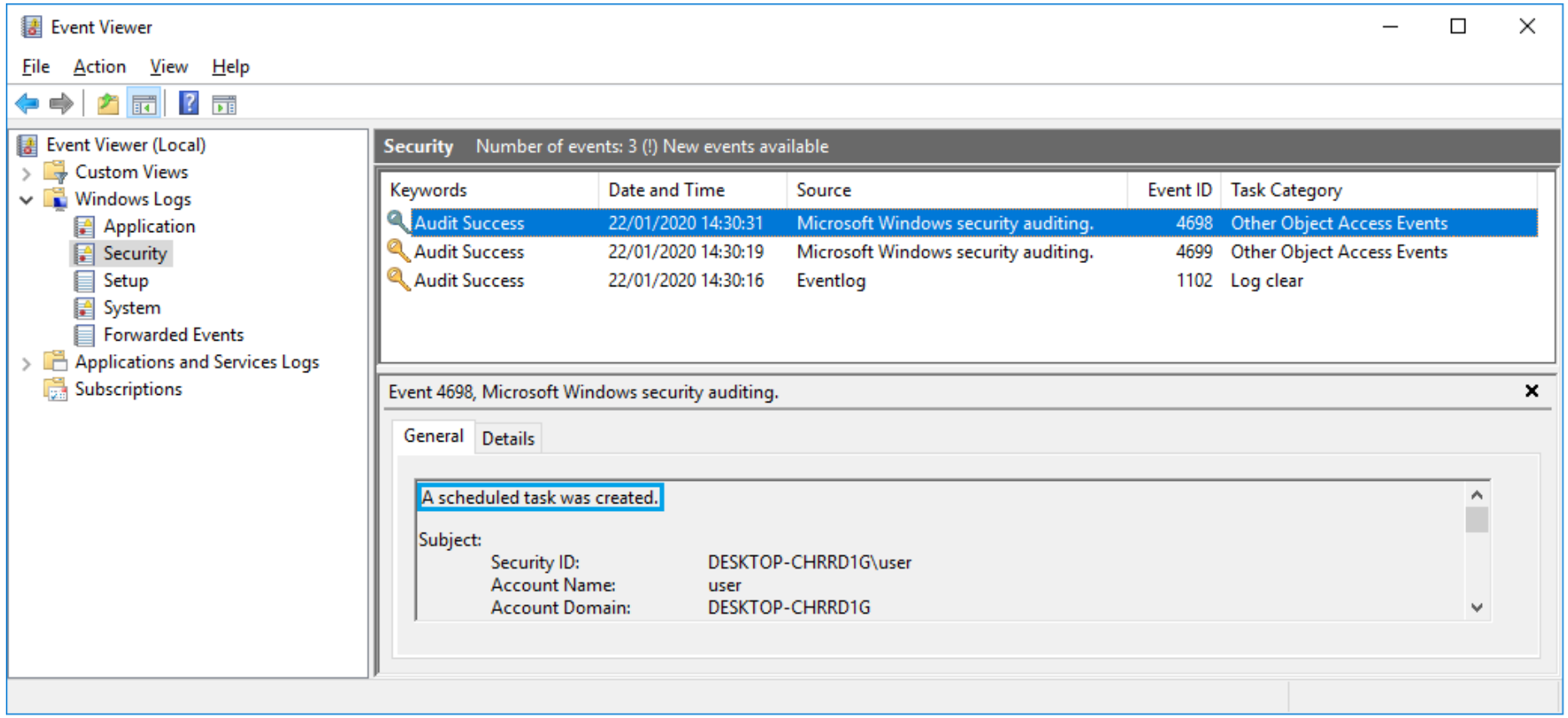


- Install a Task Scheduler Monitor
  - 3 - Configure the appropriate condition(s)

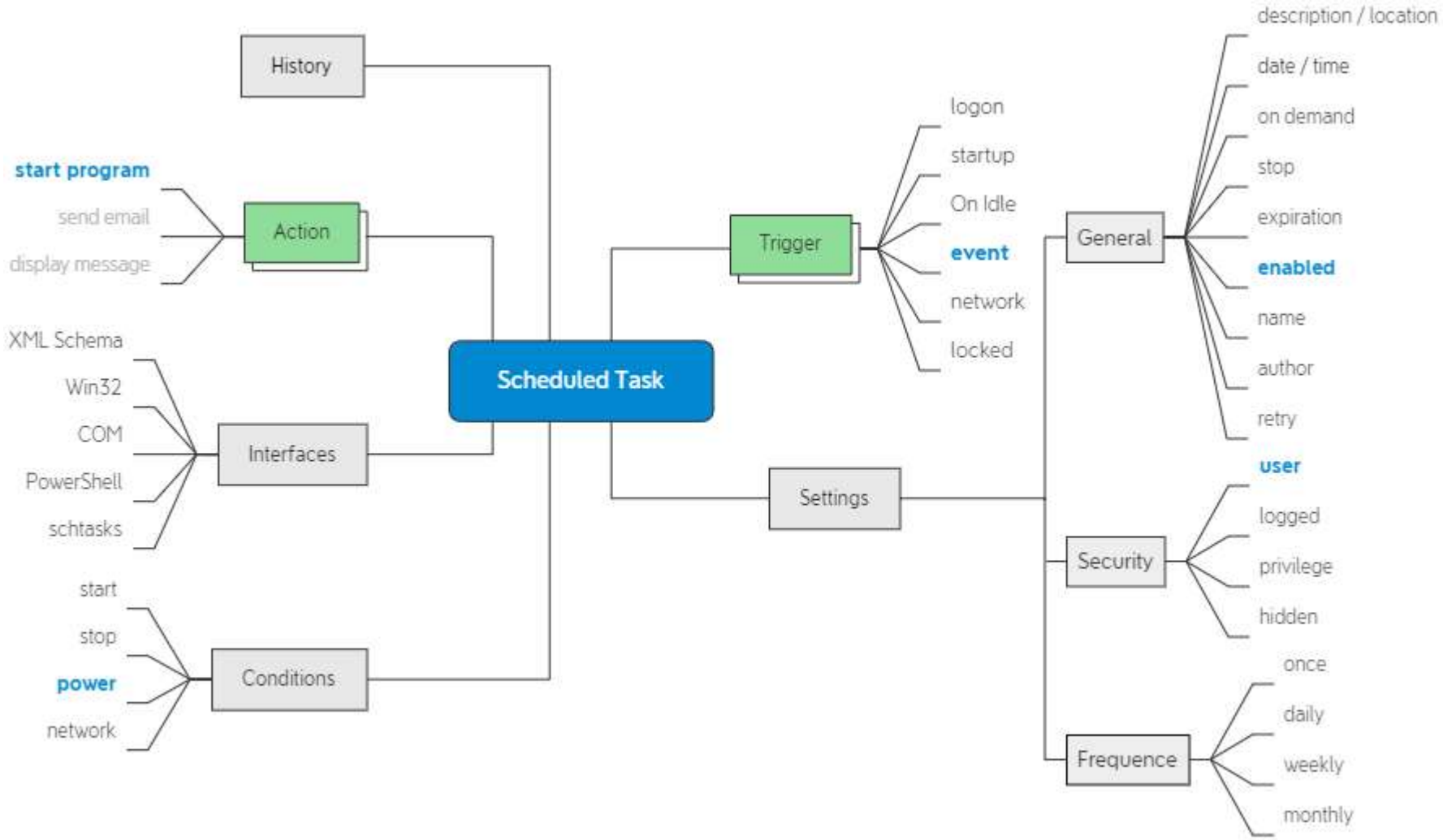


Windows Task Scheduler Monitor

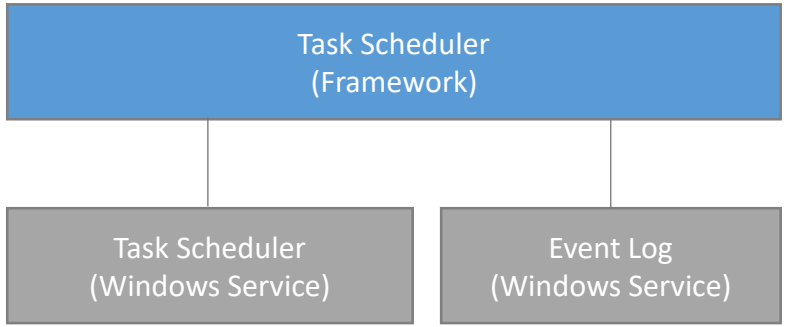
- Events related to the Task Scheduler



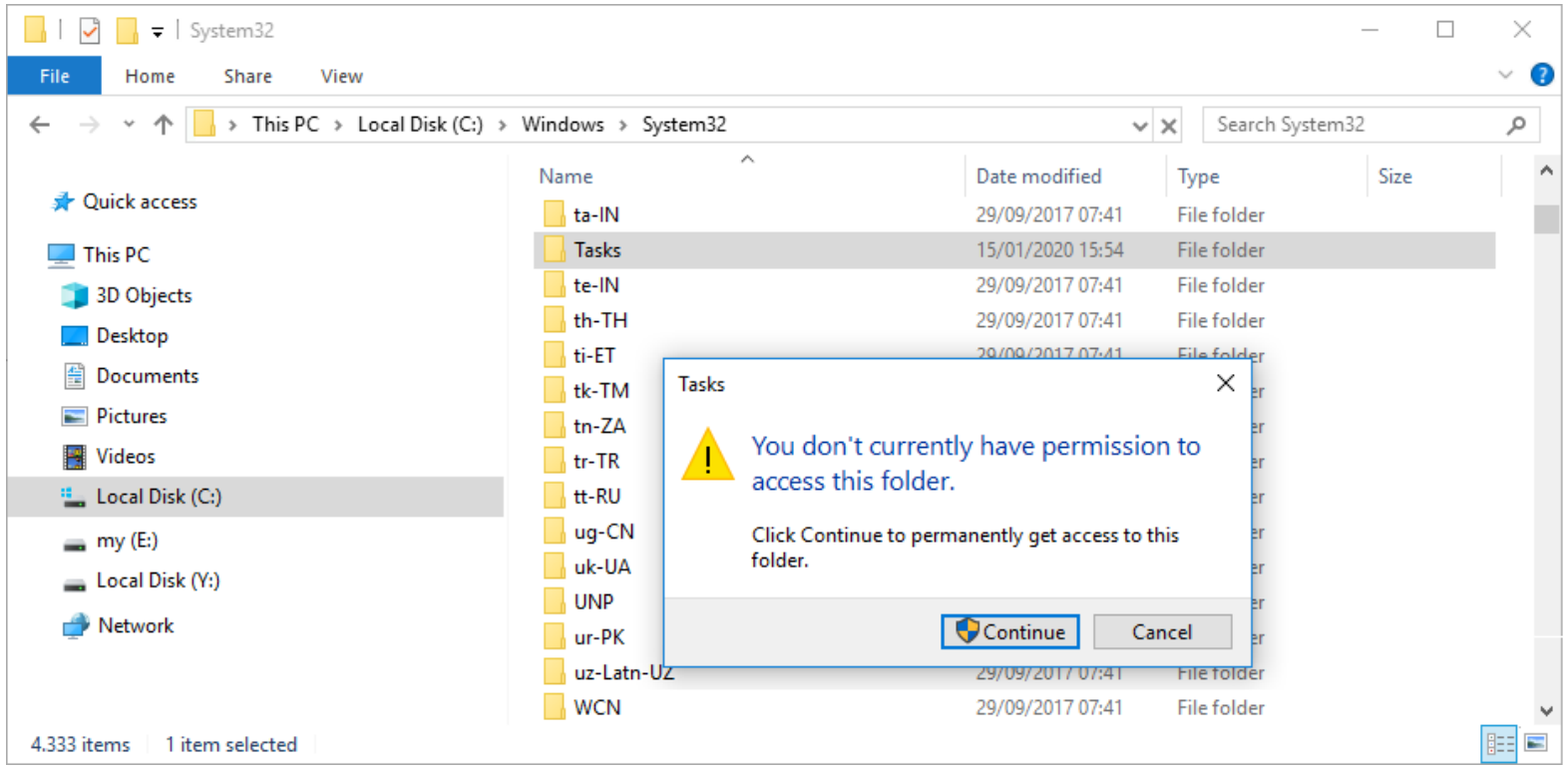
- Configuration of a scheduled Task



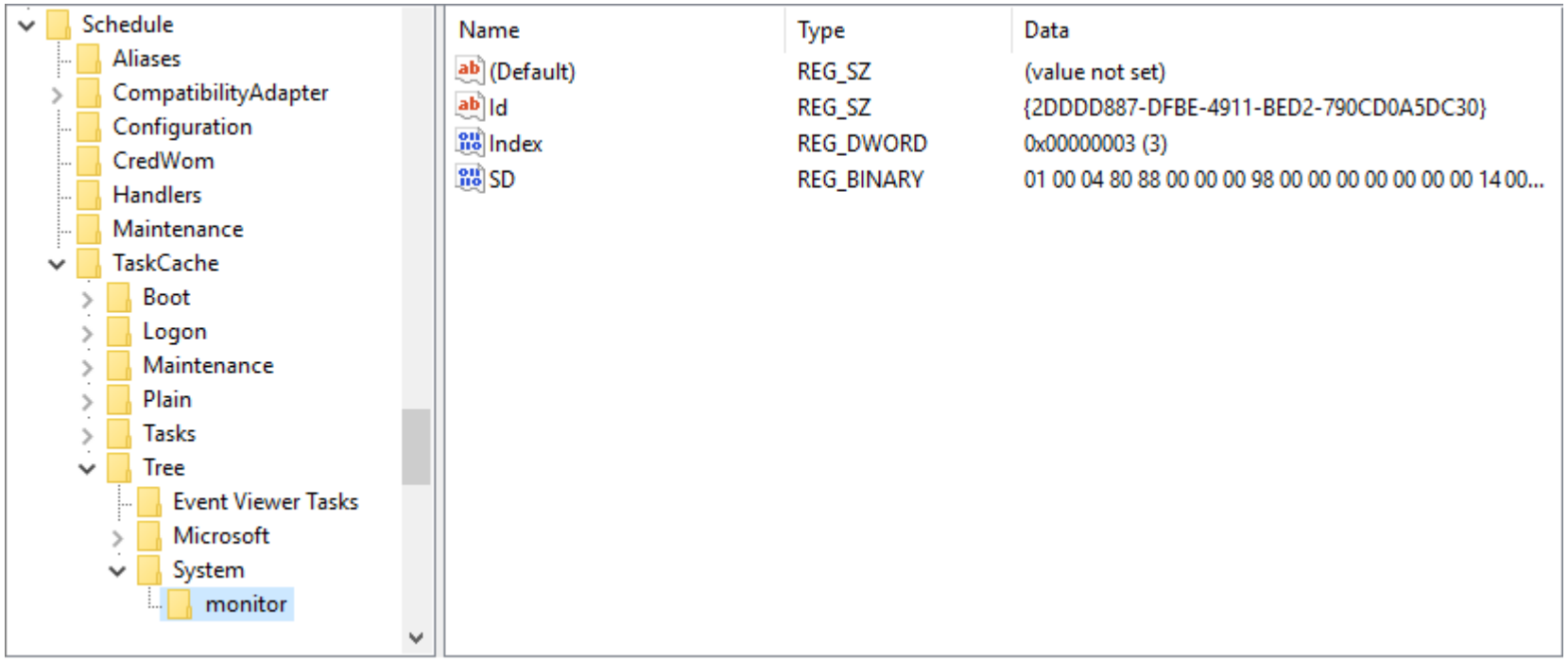
- Architecture
  - The Task Scheduler is NOT the Windows Task Manager
  - The Task Scheduler is NOT the Windows Task Scheduler Service
  - The Task Scheduler is NOT the Windows Thread Scheduler



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



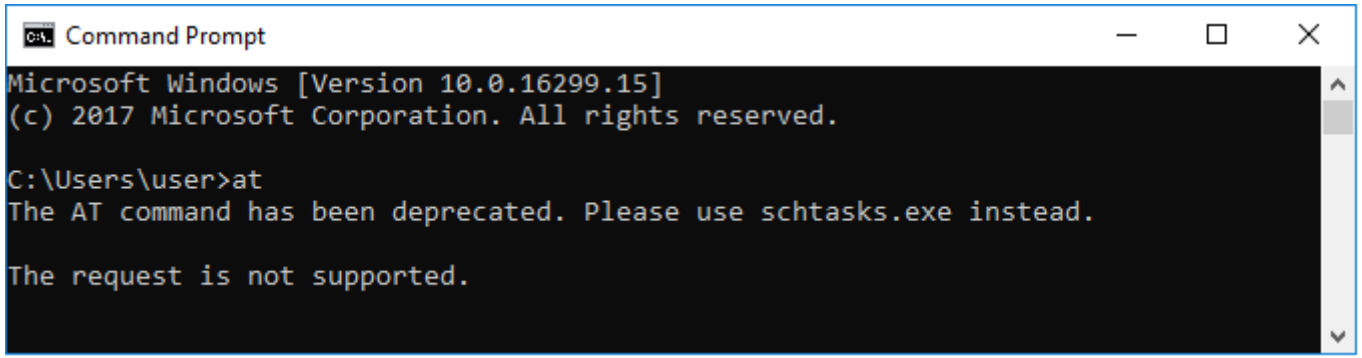
- Repository
  - Computer related settings



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

Windows Task Scheduler Monitor

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



- 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