

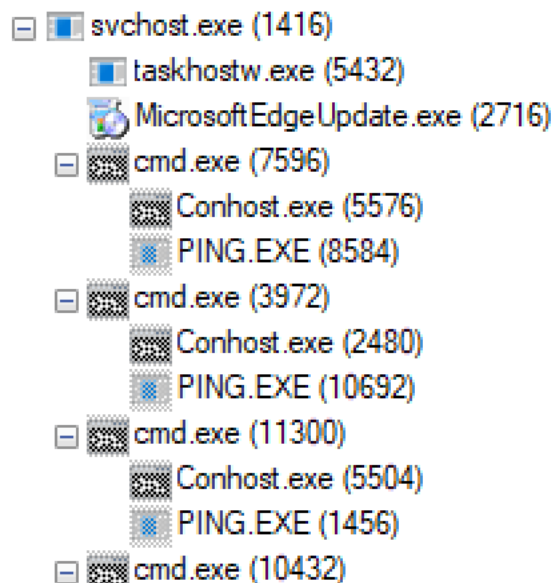
#Tarrask - Hidden Scheduled Task

Deep dive

Version: 0.4

Witold Lawacz

- ❑ [Tarrask – Defense Evasion](#)
- ❑ [The Case of the Disappearing Scheduled Task](#)



```
C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /c
C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
ping 8.8.8.8
C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
ping 8.8.8.8
C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
ping 8.8.8.8
C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
```

```
C:\Windows\system32>schtasks.exe /query /V /FO CSV /TN TestTask4
ERROR: The system cannot find the file specified.

C:\Windows\system32>schtasks.exe /query /V /FO CSV | findstr 8.8.8.8

C:\Windows\system32>whoami
nt authority\system
```

Agenda

- **Scheduled Task Artifacts**
- **Hiding Scheduled Task**
- **Detecting Hidden Scheduled Tasks**
- **Analyzing Hidden Scheduled Tasks**
- **Tools**
- **Key Takeaways**

Scheduled Task Artifacts (Chosen)

[Registry]

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\<%TaskID%>\

- **SecurityDescriptor** (Unknown)
- **Actions** (User Context + Program + Arguments + Working Dir + ...)

```
| Signature [2 bytes]
| run_as_account_size [4 bytes] | run_as_account [run_as_account_size]
| Unknown [6 bytes] |
| program_path_size [4 bytes] | program_path [program_path_size]
| program_parameters_size [4 bytes] | program_parameters [program_parameters_size]
| working_dir_size [4 bytes] | working_dir [working_dir_size]
```

00000000	03	00	0C	00	00	00	41	00	A	.	
00000008	75	00	74	00	68	00	6F	00	u	.	t	.	h	.	o	.
00000010	72	00	66	66	00	00	00	00	r	.	f
00000018	36	00	00	00	43	00	3A	00	6	.	.	.	C	.	.	.
00000020	5C	00	57	00	69	00	6E	00	\	.	W	.	i	.	n	.
00000028	64	00	6F	00	77	00	73	00	d	.	o	.	w	.	s	.
00000030	5C	00	53	00	79	00	73	00	\	.	S	.	y	.	s	.
00000038	74	00	65	00	6D	00	33	00	t	.	e	.	m	.	3	.
00000040	32	00	5C	00	63	00	6D	00	2	.	\	.	c	.	m	.
00000048	64	00	2E	00	65	00	78	00	d	.	.	e	.	x	.	.
00000050	65	00	3E	00	00	00	2F	00	e	.	>
00000058	63	00	20	00	70	00	69	00	r	.	.	.	n	.	i	.

SYSTEM (Full Control)
Administrators (Read, Delete)



UTF16LE

NOTE: run_as_account seems to accept Author (which is a pointer to Author registry value, or arbitrary user name (not tested yet))

SYSTEM (Full Control)
Administrators (Read, Delete)



- **Path** (A Task key or key with sub-key(s) pointing to Task entry under “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree” node)

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Malware-Key\Sub-Key\MalwareTask

T\CurrentVersion\Schedule\TaskCache\Tasks\{6AA2E298-C47C-45AE-BF6F-E2D9A555345C}		
Name	Type	Data
Path	REG_SZ	\Microsoft\Windows\DiskCleanup\SilentCleanup

NT\CurrentVersion\Schedule\TaskCache\Tasks\{0C9D6996-8FE8-4AE0-B0A-8D68B8F32588}		
Name	Type	Data
Path	REG_SZ	\TestTask4

Task Location = ...TaskCache\Tree + ...TaskCache\Tasks\<%TaskID%>\<%Path%>

Scheduled Task Artifacts (Chosen)

[Registry]

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\<%Path%>

- **ID** (Task ID, the location of Task under “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks” node)

NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4

Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{0C9D6996-8FE8-4AE0-BB0A-8D68B8F32588}
Index	REG_DWORD	0x00000003 (3)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{0C9D6996-8FE8-4AE0-BB0A-8D68B8F32588}

Tasks

{0016B09F-CFDA-4F5B-A70B-84A75599B89B}

{00446CF1-8668-472D-BEDD-D0BB88DBA009}

{008539BF-83F9-4483-9E0A-EEEE6EAC0A08}

{051DF697-AF10-4DB6-9B93-E1A4E35F00F7}

{077333D6-06BA-4EA4-BDF4-1CD1439558F2}

{082A60E5-6BFA-49FB-89FB-C6CCAFB344A2}

{082F4875-D88C-40EA-8706-87480962C446}

{0C9D6996-8FE8-4AE0-BB0A-8D68B8F32588}

{0CBABB27-6DFC-4155-BAE7-AE919B92FEF2}

{0CEC0B91-4AE9-4E8A-ACB2-3B4C811F442C}

{0E2DCCB3-7B11-40CF-B973-90F22732E317}

Name	Type	Data
(Default)	REG_SZ	(value not set)
Actions	REG_BINARY	03 00 0c 00 00 00 41 00 75 00 74 00
Author	REG_SZ	WORKGROUP\SYSTEM
Date	REG_SZ	2022-04-19T07:30:32.5313892
DynamicInfo	REG_BINARY	03 00 00 00 d0 69 a2 11 fa 53 d8 01
Hash	REG_BINARY	93 62 20 36 ef 44 54 99 b0 e7 bb 5d
Path	REG_SZ	\TestTask4
Schema	REG_DWORD	0x00010002 (65538)
Triggers	REG_BINARY	17 00 00 00 00 00 00 01 07 04 00
URI	REG_SZ	\TestTask4

- **Author** (User Context to execute Task)

rm.py -rp "python_registry" -r -s "hives/win10" -p "tasks"

RegMagnet Attempts to translate Actions blob containing User Context to human readable data.

It seems it support arbitrary user names like LocalSystem



Value name:

Author

Value data:

WORKGROUP\SYSTEM

```
TaskCache\Tasks\{03B65EB4-84C4-4442-9E92-DB8BFA0891ED},Actions,b'\x03\x00\x0c\x00\x00\x00A\x00u\x00t\x00h\x00o\x00r\x00ff\x00\x00...
TaskCache\Tasks\{03B65EB4-84C4-4442-9E92-DB8BFA0891ED},Actions_,[RunAs: Author] %systemroot%\system32\usoclient.exe StartInstall
TaskCache\Tasks\{03BAB3F3-7CFB-408A-9756-70F45BE325AC},Actions,b'\x03\x00\x16\x00\x00\x00L\x00o\x00c\x00a\x00l\x00S\x00y\x00s\x00t\x00e\x00m\x00ff\x00\x00...
TaskCache\Tasks\{03BAB3F3-7CFB-408A-9756-70F45BE325AC},Actions_,[RunAs: LocalSystem] %windir%\system32\rundll32.exe /d acprox.dll,PerformAutochkOperations
```

Scheduled Task Artifacts (Chosen)

[Registry]

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\<%Path%>

- **SD** (Binary SDDL describing access permissions (Task Scheduler, schtasks, Autoruns...they all use it to determine whether or not a Task should be shown/executed/other allowed/denied etc.)

Value name:									
SD									
Value data:									
00000060	00	00	24	00	89	00	12	00	. . \$
00000068	01	05	00	00	00	00	00	05
00000070	15	00	00	00	38	1F	C6	C3 8 . Æ Å
00000078	43	9E	93	DA	C0	51	BF	0F	C . . Ú À Q ¿ .
00000080	E9	03	00	00	61	00	72	00	é . . . a . r .
00000088	01	02	00	00	00	00	00	05
00000090	20	00	00	00	20	02	00	00
00000098	01	05	00	00	00	00	00	05
000000A0	15	00	00	00	38	1F	C6	C3 8 . Æ Å
000000A8	43	9E	93	DA	C0	51	BF	0F	C . . Ú À Q ¿ .
000000B0	01	02	00	00				

TaskHunter: Can print human readable permissions from a Task's **SD** value ([Get-ScheduledTaskInfo](#))

[+] SDDL (Tree.Task_Path.**SD**) Permissions:

[-] O:BAG:SYD:(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FA;;;BA)(A;;;FR;;;SY)

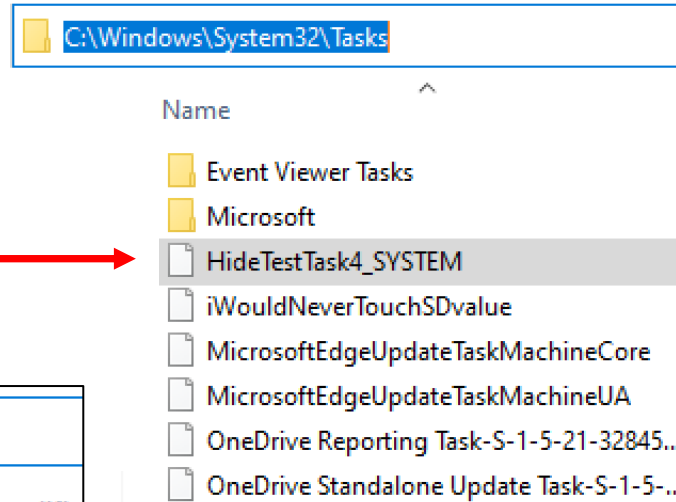
[-] **BUILTIN\Administrators**: AccessAllowed Inherited (ChangePermissions, CreateSubKey, Delete, EnumerateSubKeys, ExecuteKey, FullControl, FullControl, FullControl, GenericExecute, GenericRead, Notify, QueryValues, Read, ReadAttributes, ReadPermissions, SetValue, Synchronize, TakeOwnership, write, WriteAttr
ibutes, writeKey)

Scheduled Task Artifacts (Chosen)

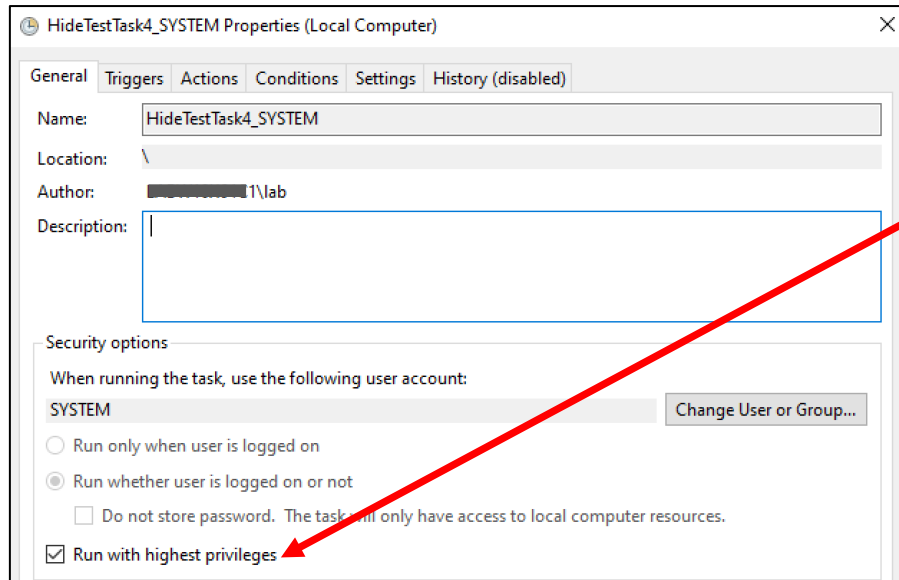
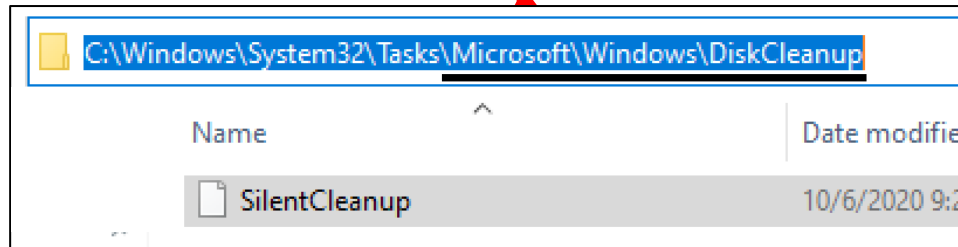
[Disk]

C:\Windows\System32\Tasks

■ **<%Path%>**



- Task information/metadata is stored in XML format
- RunLevel is stored only in XML file (LeastPrivilege/HighestAvailable)



```
<Principals>
  <Principal id="Author">
    <RunLevel>HighestAvailable</RunLevel>
    <UserId>S-1-5-18</UserId>
  </Principal>
</Principals>

<Actions Context="Author">
  <Exec>
    <Command>cmd.exe</Command>
    <Arguments>/c REG DELETE "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4" /v SD /f</Arguments>
  </Exec>
</Actions>
```

Scheduled Task Artifacts (Chosen)

[Memory]

svchost.exe

- An instance of **svchost.exe** responsible for running scheduled tasks (having loaded module **schedsvc.dll** loaded by **HKLM\System\CurrentControlSet\Services\Schedule**, having child processes like **taskhostw.exe** and Command Line like **-k netsvcs -p -s Schedule**

The image shows two windows side-by-side. The left window is titled 'svchost.exe (1136) (0x1862f92b000 - 0x1862f92d000)' and displays a memory dump. The right window is titled 'Results - svchost.exe (1136)' and displays a table of 34 results.

svchost.exe (1136) Memory Dump:

```
000006b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000006c0 4e 00 54 00 20 00 54 00 41 00 53 00 4b 00 5c 00 N.T. .T.A.S.K.\
000006d0 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 M.i.c.r.o.s.o.f.
000006e0 74 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 t.\.W.i.n.d.o.w.
000006f0 73 00 5c 00 41 00 70 00 6c 00 69 00 63 00 s.\.A.p.p.l.i.c.
00000700 61 00 74 00 69 00 6f 00 6e 00 20 00 45 00 78 00 a.t.i.o.n. .E.x.
00000710 70 00 65 00 72 00 69 00 65 00 6e 00 63 00 65 00 p.e.r.i.e.n.c.e.
00000720 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 \.M.i.c.r.o.s.o.
00000730 66 00 74 00 20 00 43 00 6f 00 6d 00 70 00 61 00 f.t. .C.o.m.p.a.
00000740 74 00 69 00 62 00 69 00 6c 00 69 00 74 00 79 00 t.i.b.i.l.i.t.y.
00000750 20 00 41 00 70 00 70 00 72 00 61 00 69 00 73 00 .A.p.p.r.a.i.s.
00000760 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 e.r.....
00000770 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000780 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2a 40 .....*@
00000790 03 00 0c 00 00 00 41 00 75 00 74 00 68 00 6f 00 .....A.u.t.h.o.
000007a0 72 00 66 66 00 00 00 00 36 00 00 00 43 00 3a 00 r.f.f....6...C.t.
000007b0 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 \.W.i.n.d.o.w.s.
000007c0 5c 00 53 00 79 00 73 00 74 00 65 00 6d 00 33 00 \.S.y.s.t.e.m.3.
000007d0 32 00 5c 00 63 00 6d 00 64 00 2e 00 65 00 78 00 2.\.c.m.d...e.x.
000007e0 65 00 3e 00 00 00 2f 00 63 00 20 00 70 00 69 00 e.>...c. .p.i.
000007f0 6e 00 67 00 20 00 38 00 2e 00 38 00 2e 00 38 00 n.g. .8...8...8.
00000800 2e 00 38 00 20 00 3e 00 20 00 54 00 65 00 73 00 .8. .>. .T.e.s.
00000810 74 00 54 00 61 00 73 00 6b 00 34 00 2e 00 74 00 t.T.a.s.k.4...t.
00000820 78 00 74 00 14 00 00 00 43 00 3a 00 5c 00 4d 00 x.t.....C.t.\.M.
00000830 41 00 4c 00 57 00 41 00 52 00 45 00 00 00 00 00 A.L.W.A.R.E....
00000840 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000850 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 40 .....
00000860 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Results - svchost.exe (1136):

Address	Length	Result
0x1862f2b9c10	14	tTask4
0x1862f92b7e6	62	/c ping 8.8.8.8 > TestTask4.txt
0x1862fe6f2a0	20	\TestTask4
0x1862fe959b0	118	C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
0x1862fed7d00	34	NT TASK\TestTask4
0x1862ff3d370	34	NT TASK\TestTask4
0x1862ff63df8	46	NT TASK\DeleteTestTask4
0x1862ff64360	20	\TestTask4
0x1862ffad2f0	40	HideTestTask4_SYSTEM
0x1862ffaf120	18	TestTask4
0x1862ffaf6f0	40	HideTestTask4_SYSTEM
0x1862ffafea0	18	TestTask4
0x1863023cb78	56	NT TASK\HideTestTask4_SYSTEM
0x1863023cd48	232	cmd.exe /c REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\...
0x18630261ce8	34	NT TASK\TestTask4
0x186302696d2	388	/c SHTASKS /Create /f /tn "HideTestTask4_SYSTEM" /sc onstart /tr "cmd.exe /c REG DELETE HKLM\SOF...
0x186302698e2	388	/c SHTASKS /Create /f /tn "HideTestTask4_SYSTEM" /sc onstart /tr "cmd.exe /c REG DELETE HKLM\SOF...
0x18630269f12	388	/c SHTASKS /Create /f /tn "HideTestTask4_SYSTEM" /sc onstart /tr "cmd.exe /c REG DELETE HKLM\SOF...
0x1863026a332	388	/c SHTASKS /Create /f /tn "HideTestTask4_SYSTEM" /sc onstart /tr "cmd.exe /c REG DELETE HKLM\SOF...
0x1863026a962	388	/c SHTASKS /Create /f /tn "HideTestTask4_SYSTEM" /sc onstart /tr "cmd.exe /c REG DELETE HKLM\SOF...
0x18630286cb8	34	%T TASK\TestTask4
0x18630286ed0	118	C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt

Scheduled Task Artifacts (Chosen)

[Memory] svchost.exe - Task (in-memory)

2344163_863.bin x																	0123456789ABCDEF
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
0:	4E	00	54	00	20	00	54	00	41	00	53	00	4B	00	5C	00	N.T. .T.A.S.K.\
16:	54	00	65	00	73	00	74	00	54	00	61	00	73	00	6B	00	...e.s.t.T.a.s.k
32:	34	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00
48:	00	1D	CC	89	C6	02	00	00	00	00	00	00	FF	FF	FF	FF	..i%e.....ÿÿÿÿ
64:	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00
80:	60	1D	CC	89	C6	02	00	00	02	00	00	00	00	00	00	00	..i%e.....
96:	70	1D	CC	89	C6	02	00	00	00	00	00	00	FF	FF	FF	FF	p.i%e.....ÿÿÿÿ
112:	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00
128:	A8	1D	CC	89	C6	02	00	00	48	1D	CC	89	C6	02	00	00	..i%e...H.i%e...
144:	10	00	00	00	00	00	00	00	3C	00	00	00	FF	FF	FF	FF<...ÿÿÿÿ
160:	E6	07	04	00	02	00	1A	00	0B	00	34	00	28	00	00	00	æ.....4.(...
176:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
192:	04	00	00	00	00	00	00	00	50	1D	CC	89	C6	02	00	00P.i%e...
208:	31	00	00	00	00	00	00	00	05	00	00	00	00	00	00	00	1.....
224:	00	00	00	00	00	00	00	00	68	1D	CC	89	C6	02	00	00h.i%e...
240:	31	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1.....
256:	1C	10	00	00	00	00	00	00	01	00	00	00	00	00	00	00
272:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
288:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
304:	B0	1D	CC	89	C6	02	00	00	31	00	00	00	00	00	00	00	°.i%e...1.....
320:	E0	1D	CC	89	C6	02	00	00	E8	1D	CC	89	C6	02	00	00	à.i%e...è.i%e...
336:	01	00	00	00	00	00	00	00	20	1E	CC	89	C6	02	00	00i%e...
352:	20	1F	CC	89	C6	02	00	00	31	00	00	00	00	00	00	00	..i%e...1.....
368:	43	00	3A	00	5C	00	57	00	69	00	6E	00	64	00	6F	00	C::\W.i.n.d.o.
384:	77	00	73	00	5C	00	53	00	79	00	73	00	74	00	65	00	w.s.\S.y.s.t.e.
400:	6D	00	33	00	32	00	5C	00	63	00	6D	00	64	00	2E	00	m.3.2.\c.m.d...
416:	65	00	78	00	65	00	00	00	01	00	00	00	00	00	00	00	e.x.e.....
432:	58	1E	CC	89	C6	02	00	00	90	1E	CC	89	C6	02	00	00	X.i%e.....i%e...
448:	08	1F	CC	89	C6	02	00	00	00	00	00	00	00	00	00	00	..i%e.....
464:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
480:	43	00	3A	00	5C	00	57	00	69	00	6E	00	64	00	6F	00	C::\W.i.n.d.o.
496:	77	00	73	00	5C	00	53	00	79	00	73	00	74	00	65	00	w.s.\S.y.s.t.e.
512:	6D	00	33	00	32	00	5C	00	63	00	6D	00	64	00	2E	00	m.3.2.\c.m.d...
528:	65	00	78	00	65	00	00	00	43	00	3A	00	5C	00	57	00	e.x.e...C::\W.
544:	69	00	6E	00	64	00	6F	00	77	00	73	00	5C	00	53	00	i.n.d.o.w.s.\S.
560:	79	00	73	00	74	00	65	00	60	00	33	00	32	00	5C	00	y.s.t.e.m.3.2.\
576:	63	00	6D	00	64	00	2E	00	65	00	78	00	65	00	20	00	c.m.d...e.x.e..
592:	2F	00	63	00	20	00	70	00	69	00	6E	00	67	00	20	00	/c. .p.i.n.g. .
608:	38	00	2E	00	38	00	2E	00	38	00	2E	00	38	00	20	00	8...8...8...8..
624:	3E	00	20	00	54	00	65	00	73	00	74	00	54	00	61	00	>. .T.e.s.t.T.a.
640:	73	00	6B	00	34	00	2E	00	74	00	78	00	74	00	00	00	s.k.4...t.x.t...
656:	43	00	3A	00	5C	00	4D	00	41	00	4C	00	57	00	41	00	C::\M.A.L.W.A
672:	52	00	45	00	00	00	00	00	0F	00	02	00	00	00	00	00	R.E.....
688:	44	44	44	04	80	F4	03	00	00	40	00	00					DDD.€ô...@..

- Task Signature
- Task Name
- You can get task names from process dump file with simple command (But it's harder to find other details):

```
grep -Poa "N.T. .T.A.S.K.\\|.*?\x00\x00" svchost.exe.dmp | sort -u
```
 - Determined markers allow educated byte search, and Action/Command line retrieval (I have implemented it in GetTasks tool)
 - It's hard to differentiate between a properly removed and hidden task (as both leave similar entries in memory, and I lack a proper memory struct for them)
- Program path marker
- Program path
- Action marker (Followed by Program path)
- Program path
- Program arguments
- Working directory

Hiding Scheduled Task

The removal of Task's SD value, makes the task to disappear from Task Scheduler/Autoruns/schtasks...
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4\SD

Survives a reboot

```
* REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4" /v SD /f (Under SYSTEM account)
* SHTASKS /Create /f /tn "HideTestTask4_SYSTEM" /sc onstart /tr "cmd.exe /c REG DELETE \"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4\" /v SD /f" /ru system /RL HIGHEST (Under Admin account)
```

Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4

Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{0C9D6996-8FE8-4AE0-BB0A-8D68B8F32588}
Index	REG_DWORD	0x00000003 (3)

Task Scheduler (Local)

Task Scheduler Library

Name	Status	Triggers
HideTestTask4_SYSTEM	Ready	At system startup
iWouldNeverTouchSDvalue	Ready	
MicrosoftEdgeUpdateTaskMachineCore	Running	Multiple triggers defined
MicrosoftEdgeUpdateTaskMachineUA	Ready	At 11:51 AM every day - After triggered, repeat every 1 hour for a d
OneDrive Reporting Task-S-1-5-21-328...	Ready	At 11:44 PM on 5/4/2022 - After triggered, repeat every 1.00:00:00 i
OneDrive Standalone Update Task-S-1...	Ready	At 10:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 i
TestTask	Ready	At 12:29 AM every day - After triggered, repeat every 1 hour indefir

SD ???

TestTask4 ???

```
C:\Windows\system32>schtasks.exe /query /V /FO CSV /TN TestTask4
ERROR: The system cannot find the file specified.

C:\Windows\system32>schtasks.exe /query /V /FO CSV | findstr 8.8.8.8

C:\Windows\system32>whoami
nt authority\system
```



Removal of C:\Windows\system32\Tasks\TestTask4
Task keeps running

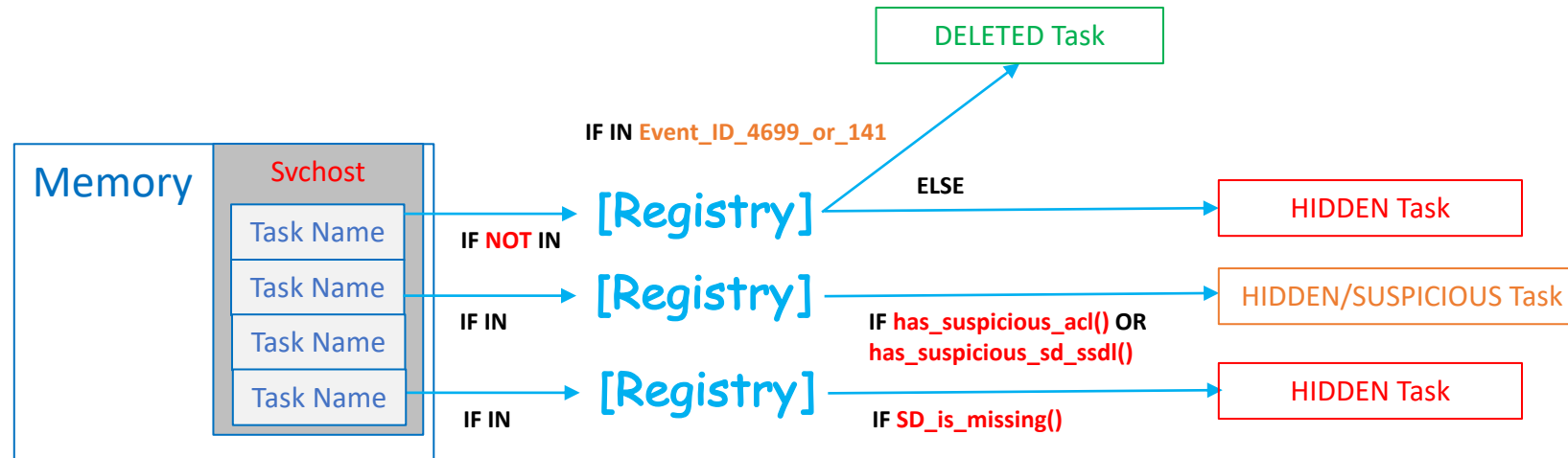
Survives a reboot

Removal of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4
Removal of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}

Does NOT survives a reboot

Detecting Hidden Scheduled Tasks

- Look for Tasks without ...`\Tree\<%Path%\SD` value (Covers the use-case of tasks surviving a reboot)
- Look for in-memory Tasks and map their local artefacts (If they are not found, the Task is either Hidden or properly removed)



Detecting Hidden Scheduled Tasks

- **TaskHunter.ps1** (A PoC tool, finds and dumps Task Scheduler memory, to pull Scheduled Tasks and analyse their local artefacts in order to flag Hidden/Suspicious entries)

```
[*] Starting Tarrask Hunter...
```

```
[*] Search for Task Scheduler process to dump...
```

```
[-] Dumping: svchost.exe [1416]
[-] CMD: rundll32.exe comsvcs.dll MiniDump 1416 C:\MALWARE\Actions\1416_svchost_task_scheduler.dmp full
[-] Dumped to C:\MALWARE\Actions\1416_svchost_task_scheduler.dmp
```

```
[*] Parsing process dump: C:\MALWARE\Actions\1416_svchost_task_scheduler.dmp
```

```
[-] Loading dump file...
[-] Searching Task names...
[-] Found: 300 Task entries [Unique Task Names: 216]
```

```
[*] Scanning OS for Hidden Tasks...
```

```
[*] Search for Hidden Tasks...
```

```
[+] Creating Microsoft-Windows-Security-Auditing CACHE [Time consuming]...
[-] cached entries
```

```
[+] Scanning Windows Registry...
```

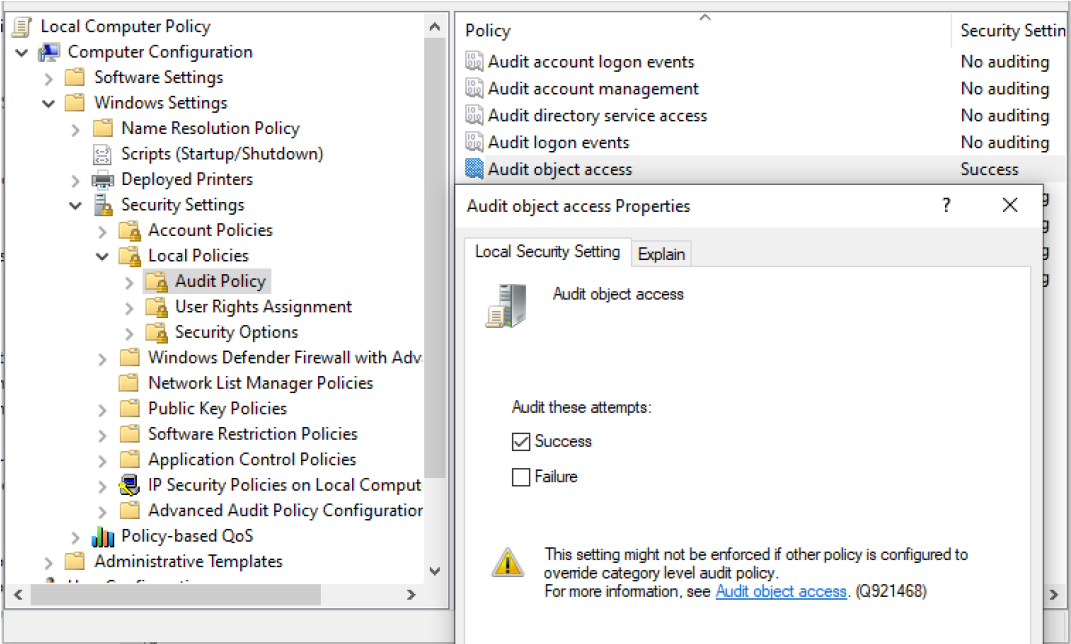
```
[-] HIDDEN (Task's Key NOT FOUND -> HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{ca4730d0-52b0-400f-9580-9c2e862ce8aa}
[-] REMOVED (Task properly DELETED -> HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\iWASremoved_2
[-] HIDDEN (Task's SD contains unexpected user: [REDACTED]\lab] -> HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\iWouldNeverTouchSDvalue
....
[-] HIDDEN (Task's Key NOT FOUND -> HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\XblGameSave\XblGameSaveTaskLogon
[-] HIDDEN (Task's SD Value NOT FOUND -> HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4\SD
```

```
[*] Get_Tasks Comman-Line:
```

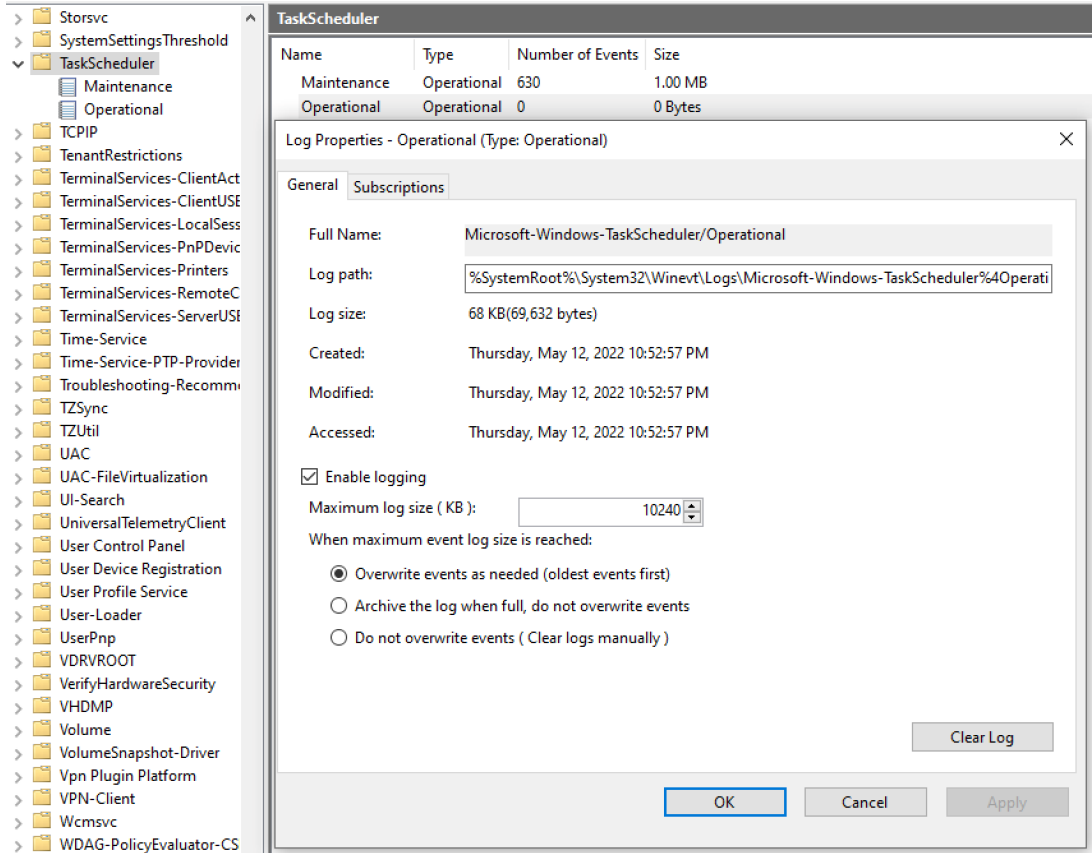
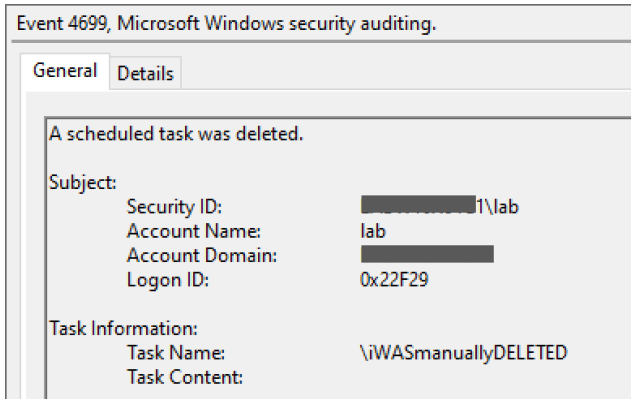
```
-i 1416_svchost_task_scheduler.dmp --dump-task --csv -v -n "{ca4730d0-52b0-400f-9580-9c2e862ce8aa}" - "-"iWouldNeverTouchSDvalue" - "-"Microsoft\Windows\EnterpriseMgmt\*" - "-"Microsoft\Windows\UpdateOrchestrator\Backup Scan" - "-"Microsoft\Windows\UpdateOrchestrator\Battery Leve
l Install" - "-"Microsoft\Windows\UpdateOrchestrator\Enable UWF" - "-"Microsoft\Windows\UpdateOrchestrator\Reboot" - "-"Microsoft\Windows\UpdateOrchestrator\Schedule Update" - "-"Microsoft\Windows\WwanSvc\WiFiTask" - "-"Microsoft\XblGameSave\XblGameSaveTaskLogon" - "-"TestTask4"
```

Detecting Hidden Scheduled Tasks

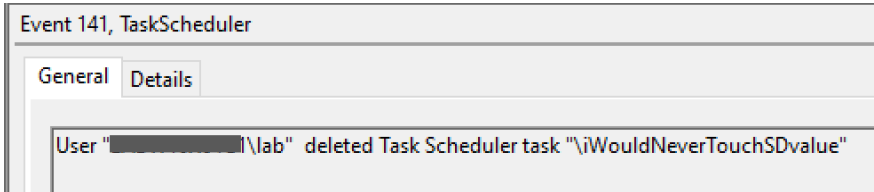
- **Audit Policy** (The auditing of **Object Access** (Event ID 4699) or **TaskScheduler/Operational** (Event ID 141) would help in differentiating properly removed tasks from hidden ones)



%SystemRoot%\System32\Winevt\Logs\Security.evtx



%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx







Analyzing Hidden Scheduled Tasks

- **get_tasks.py** (GetTasks, a PoC tool, parses Task Scheduler memory, to pull Scheduled Tasks and print information about Task Actions and more...)

```
get_tasks.py -i svchost.dmp -f dumped_tasks/ -o dumped_tasks/tasks.csv --dump-task --csv -v -n "\TestTask4-/-\HideTestTask4_SYSTEM"
```

```
[+] Processing dump file: /mnt/hgfs/repos/ma/tasks/test2/removed/svchost.mdp
[-] Task to lookup: b'\\x00T\x00e\x00s\x00t\x00T\x00a\x00s\x00k\x004\x00'
[Base Offset: 11894259 / Relative: 8207] -> TASK: NT TASK\HideTestTask4_SYSTEM00000000뽕뵡00000000000000찰뵡000000찰뵡00000000000000
-- Size: 724
-- Path: \HideTestTask4_SYSTEM NORMAL Task
-- Path(hex): b'5c0048006900640065006500730074005400610073006b0034005f00530059005300540045004d00'
-- Program: cmd.exe
-- Program(hex): b'63006d0064002e00650078006500'
-- Action: cmd.exe /c REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4" /v SD /f
-- Action(hex): b'63006d0064002e0065007800650020002f00630020005200450047002000440045004c004500540045002000220048004b004c004d005c00'
[Base Offset: 12132138 / Relative: 10271] -> TASK: NT TASK\TestTask400000000油00000000000000潤000000潑00000000000000淨000000消000000
-- Size: 908
-- Path: \TestTask4 HIDDEN Task
-- Path(hex): b'5c0054006500730074005400610073006b003400'
-- Program: C:\Windows\System32\cmd.exe
-- Program(hex): b'43003a005c00570069006e0064006f00770073005c00530079007300740065006d00330032005c0063006d0064002e00650078006500'
-- Action: C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
-- Action(hex): b'43003a005c00570069006e0064006f00770073005c00530079007300740065006d00330032005c0063006d0064002e00650078006500'
1 Task Offset: 11894259, 8207: \HideTestTask4_SYSTEM
```

Name	Size
 11894259_8207.bin	724 bytes
 12132138_10271.bin	908 bytes
 27272437_8207.bin	724 bytes
 tasks.csv	856 bytes

```
-h, --help          show this help message and exit
-i INPUT_FILE       Path to process memory dump file
-f OUT_DIR          Output directory where dumped tasks are stored
-o OUTPUT_FILE      CSV file path
-n TASK_NAME        Task name (or names delimited by "-|-") or * to search all
                    tasks
-d, --dump-tasks    Dump Task buffer
--csv               Dump Task Info to a CSV file indicated in -o
-v, --verbose       Enable Debug mode/Verbose mode
```

```
1 Task_Offset_11894259-8207;\HideTestTask4_SYSTEM;cmd.exe /c REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4" /v SD /f
2 Task_Offset_12132138-10271;\TestTask4;C:\Windows\System32\cmd.exe /c ping 8.8.8.8 > TestTask4.txt
3 Task_Offset_27272437-8207;\HideTestTask4_SYSTEM;cmd.exe /c REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TestTask4" /v SD /f
```

Tools

- [TaskHunter](#) (@wit0k)
- [GetTasks](#) (@wit0k)
- [UnlockScheduledTask.ps1](#) (@withakay)
- [Tarrask_Hidden_SchTask.ps1](#) (@knight0x07)

Key Takeaways

Threat Detection

- Monitor for **RegDeleteValue** requests to “*HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\.*\SD*”, especially for processes other than svchost related to Task Scheduler, as this can effectively hide a scheduled task
- Monitor for **RegistryWrite** requests to “*HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\.*\SD*”, especially for processes other than svchost related to Task Scheduler, as this can effectively allow additional users to execute specific tasks
- Monitor file removal events in “*C:\Windows\System32\Tasks*” especially for processes other than svchost related to Task Scheduler
- A user requires elevated access to be able to use highest run level to create tasks under SYSTEM account
- Use TaskHunter to look for Hidden tasks in company wide scan (After small modification, the tool could be detonated and re-used by any EDR, if EDR itself has no such capabilities)

Incident Response

- “*sc stop Schedule*” followed by “*sc start Schedule*” (under SYSTEM account allows restarting Task Scheduler, hence dropping all hidden tasks having no reboot persistence, without a reboot)
- The removal of XML file related to Tasks does not unload the Task, and the Task is still visible in Task Scheduler
- The removal of Task’s SD value does not unload task operations, it only makes it invisible to tools like “*schtasks*”, “*Autoruns*” or even **Task Scheduler** itself (it keeps executing it)
- XML files in “*C:\Windows\System32\Tasks*” keep the RunLevel associated with scheduled tasks (This info seems to be not cached in registry)
- It seems that Microsoft itself run a bunch of hidden tasks (I guess this is how these guys from Hafnium found out about this persistence method)

To Do

- What is the value “*HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks*SecurityDescriptor*” used for ?
- Is there a way to differentiate Deleted task from Hidden based on in-memory artifact only?
- Can Actions registry value be manipulated to insert arbitrary username without authentication prompt?
- Volatility plugin