
 Jonathan Johnson and Jonathan Johnson Pre Mitre EU update

01e9ddf · 3 years ago 

92 lines (70 loc) · 2.8 KB

Preview

Code

Blame

Raw







Protocol:

- [Schedueled Task \(MS-TSCH\)](#)

Interface UUID:

- 1FF70682-0A51-30E8-076D-740BE8CEE98B (GUID_ATSvc)
- 378E52B0-C0A9-11CF-822D-00AA0051E40F (GUID_SASec)
- 86D35949-83C9-4044-B424-DB363231FD0C (GUID_ITaskSchedulerService)

Server Binary:

ATSvc/SASec:

- taskcomp.dll (loads into) svchost.exe

ITaskSchedulerService

- schedsvc.dll (loads into) svchost.exe

Endpoint:

ATSvc/SASec:

- ncacn_np: `\pipe\atsvc`

ITaskSchedulerService:

- ncacn_ip_tcp
- ncacn_np: `\pipe\atsvc`

ATT&CK Relation:

- [T1053 - Scheduled Task](#)
- SASec is used to get or set account information that is associated with tasks.

Indicator of Activity (IOA):

- Network:
 - Methods:
 - ITaskSchedulerServices:
 - `SchRpcRegisterTask`
 - `SchRpcEnumTasks`
 - ATSVS:
 - `NetrJobAdd`
- Host:
 - Inbound network connection to `svchost.exe` over pipe `\pipe\atsvc` or `TCP_IP` port
 - Registry Key Creation:
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree`

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
- Sysmom Event 12/13
- File Creation:
 - C:\Windows\System32\Tasks OR C:\Windows\Tasks OR C:\Windows\SYSTEM64\Tasks
 - Sysmon Event 11

Prevention Opportunities:

RPC Filter Example:

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=1FF70682-0A51-30E8-076D-740BE8CEE!
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;DA)
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=1FF70682-0A51-30E8-076D-740BE8CEE!
add filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=378E52B0-C0A9-11CF-822D-00AA0051E!
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;DA)
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=378E52B0-C0A9-11CF-822D-00AA0051E!
add filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=86D35949-83C9-4044-B424-DB363231F!
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;DA)
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=86D35949-83C9-4044-B424-DB363231F!
add filter
quit
```

Notes:

By default local administrators can create/start scheduled tasks remotely.

If remote scheduled tasks is an operational need, create a group specific to this action. Apply changes to the rpc filter, remove DAs from the SDDL string.

Useful Resources:

- <https://posts.specterops.io/abstracting-scheduled-tasks-3b6451f6a1c5>