Threat Hunter Playbook

Playbook Title: Hunting for Adversary's Schedule

Mitre Tactic: T1053

Mitre Sub Technique: T1053.005

Hypothesis:
Adversaries might create/change scheduled tasks on local/remote endpoints using GUI/command line tools to execute additional/new executables/hta files/js files for maintaining persistence in the environment

**Proposed Detection Query:

> Leverage sysmon data to hunt for scheduled tasks

```
 index=sysmon AND event.code=11 AND "process.executable"="C:\\Windows\\system32\\svchost.exe" AND
"file.path"="C:\\Windows\\System32\\Tasks\\*"   "file.path"!="C:\\Windows\\System32\\Tasks\\Microsoft\\*"
"file.path"!="C:\\Windows\\System32\\Tasks\\CreateExplorerShellUnelevatedTask"
"file.path"!="C:\\Windows\\System32\\Tasks\\GoogleUpdateTaskUserS*"
"file.path"!="C:\\Windows\\System32\\Tasks\\MicrosoftEdgeUpdateTaskMachineCore"
"file.path"!="C:\\Windows\\System32\\Tasks\\MicrosoftEdgeUpdateTaskMachineUA"
"file.path"!="C:\\Windows\\System32\\Tasks\\Mozilla"  "file.path"!="C:\\Windows\\System32\\Tasks\\Mozilla\\*"
"file.path"!="C:\\Windows\\System32\\Tasks\\OneDrive*"  "file.path"!="C:\\Windows\\System32\\Tasks\\npcapwatchdog"
"file.path"!="C:\\Windows\\System32\\Tasks\\AVG*" "file.path"!="C:\\Windows\\System32\\Tasks\\CCleaner*" | transaction file.path
        | table file.path,host.name
> (("process.command_line"="*/c start /B C*" OR "process.command_line"="* /create*" OR "process.command_line"="*\/sc\ onevent*")
OR ("process.parent.command_line"="\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" " AND
"process.executable"="C:\\Windows\\System32\\cmd.exe" AND "process.command_line"="*/c start /B C*" ))AND
"process.parent.executable"!="C:\\Program Files\\Microsoft Office\\root\\Integration\\Integrator.exe"
```

Simulation Details: Does not apply to us

Hunter Limitations/Observation Notes:
When searching for Scheduled tasks, we observed that we do not have all the data required, windows event logs, and "Microsoft-Windows-TaskScheduler/Operational" channel events. Also, we only see only one workstation wkst01 has cleanup.exe, but no events for wkst02

Hunt Findings:
We observed a scheduled Task named "Daily MagnumTempus IT Cleanup" on computers wkst02 and wkst01