Scheduled Task/Job

Sub-techniques (5)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.[1]

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to System Binary Proxy Execution, adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.[2]

ID: T1053

Sub-techniques: T1053.002, T1053.003, T1053.005, T1053.006, T1053.007

ⓘ

Tactics: Execution, Persistence, Privilege Escalation

ⓘ

Platforms: Containers, Linux, Windows, macOS

ⓘ

Permissions Required: Administrator, SYSTEM, User

ⓘ

Effective Permissions: Administrator, SYSTEM, User

ⓘ

Supports Remote: Yes

Contributors: Alain Homewood, Insomnia Security; Andrew Northern, @ex_raritas; Bryan Campbell, @bry_campbell; Leo Loobeek, @leoloobeek; Prashant Verma, Paladion; Selena Larson, @selenalarson; Travis Smith, Tripwire; Zachary Abzug, @ZackDoesML

Version: 2.3

Created: 31 May 2017

Last Modified: 15 October 2024

Version Permalink

Procedure Examples

ID	Name	Description
S1052	DEADEYE	DEADEYE has used the scheduled tasks `\Microsoft\Windows\PLA\Server Manager Performance Monitor`, `\Microsoft\Windows\Ras\ManagerMobility`, `\Microsoft\Windows\WDI\SrvSetupResults`, and `\Microsoft\Windows\WDI\USOShared` to establish persistence.[3]
G1006	Earth Lusca	Earth Lusca used the command `schtasks /Create /SC ONLOgon /TN WindowsUpdateCheck /TR "[file path]" /ru system` for persistence.[4]
S0447	Lokibot	Lokibot's second stage DLL has set a timer using "timeSetEvent" to schedule its next execution.[5]
S0125	Remsec	Remsec schedules the execution one of its modules by creating a new scheduler task.[6]
S1034	StrifeWater	StrifeWater has create a scheduled task named `Mozilla\Firefox Default Browser Agent 409046Z0FF4A39CB` for persistence.[7]

Mitigations

ID	Mitigation	Description
M1047	Audit	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. [8]
M1028	Operating System Configuration	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl` . The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. [9]
M1026	Privileged Account Management	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. [10]
M1022	Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.
M1018	User Account Management	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Analytic 1 - Look for task scheduling commands being executed with unusual parameters. `index=security (sourcetype="WinEventLog:Security" OR sourcetype="linux_secure" OR sourcetype="macos_secure" OR sourcetype="container_logs")| eval CommandLine = coalesce(CommandLine, process)| where (sourcetype="WinEventLog:Security" AND EventCode IN (4697, 4702, 4698)) OR (sourcetype="linux_secure" AND CommandLine LIKE "%cron%" OR CommandLine LIKE "%at%") OR (sourcetype="macos_secure" AND CommandLine LIKE "%launchctl%" OR CommandLine LIKE "%cron%") OR (sourcetype="container_logs" AND (CommandLine LIKE "%cron%" OR CommandLine LIKE "%at%"))| where (sourcetype="WinEventLog:Security" AND (CommandLine LIKE "%/create%" OR CommandLine LIKE "%/delete%" OR CommandLine LIKE "%/change%")) OR (sourcetype="linux_secure" AND (CommandLine LIKE "%-f%" OR CommandLine LIKE "%-m%" OR CommandLine LIKE "%--env%")) OR (sourcetype="macos_secure" AND (CommandLine LIKE "%/Library/LaunchDaemons%" OR CommandLine LIKE "%/Library/LaunchAgents%" OR CommandLine LIKE "%/System/Library/LaunchDaemons%" OR CommandLine LIKE "%/System/Library/LaunchAgents%")) OR (sourcetype="container_logs" AND (CommandLine LIKE "%-f%" OR CommandLine LIKE "%--schedule%" OR CommandLine LIKE "%--env%"))`
DS0032	Container	Container Creation	Monitor for newly constructed containers that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Analytic 1 - Look for new container creation events with unusual parameters. `index=container_logs sourcetype="docker_events" OR sourcetype="kubernetes_events"| eval event_action=coalesce(action, status)| where (event_action="create" OR event_action="start")| search event_type="container"| search (parameters="*--privileged*" OR parameters="*--cap-add=*" OR parameters="*--volume=*" OR parameters="*--network=host*" OR parameters="*--device*")`
DS0022	File	File Creation	Monitor newly constructed files that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Analytic 1 - Look for new task files with unusual parameters. `index=security_logs OR index=system_logs(sourcetype="docker_events" OR sourcetype="kubernetes_events" OR sourcetype="wineventlog:security" OR sourcetype="linux_secure" OR sourcetype="syslog" OR sourcetype="file_monitoring")| eval platform=case(sourcetype=="docker_events" OR sourcetype=="kubernetes_events", "Containers", sourcetype=="wineventlog:security", "Windows", sourcetype=="linux_secure" OR sourcetype=="syslog", "Linux", sourcetype=="mac_os_events", "macOS")| search ((platform="Containers" AND (event_type="file_create" AND (file_path="*/etc/cron.d/*" OR file_path="*/etc/systemd/system/*"))) OR (platform="Windows" AND EventCode=4663 AND (ObjectName="C:\Windows\System32\Tasks\" *OR ObjectName="C:\Windows\Tasks*")) OR (platform="Linux" AND (file_path="/etc/cron.d/" *OR file_path="/etc/systemd/system/*")) OR (platform="macOS" AND (file_path="/Library/LaunchDaemons/" *OR file_path="/Library/LaunchAgents/*")))`

ID	Data Source	Data Component	Detects
		File Modification	Monitor for changes made to files that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Analytic 1 - Look for task file modifications with unusual parameters. `index=security_logs OR index=system_logs(sourcetype="docker_events" OR sourcetype="kubernetes_events" OR sourcetype="wineventlog:security" OR sourcetype="linux_secure" OR sourcetype="syslog" OR sourcetype="file_monitoring")| eval platform=case(sourcetype=="docker_events" OR sourcetype=="kubernetes_events", "Containers", sourcetype=="wineventlog:security", "Windows", sourcetype=="linux_secure" OR sourcetype=="syslog", "Linux", sourcetype=="mac_os_events", "macOS")| search ((platform="Containers" AND (event_type="file_modify" AND (file_path="/etc/cron.d/" OR file_path="/etc/systemd/system/" OR file_path="/etc/crontab"))) OR (platform="Windows" AND EventCode=4663 AND (ObjectName="C:\Windows\System32\Tasks\" OR ObjectName="C:\Windows\Tasks\")) OR (platform="Linux" AND (file_path="/etc/cron.d/" OR file_path="/etc/systemd/system/" OR file_path="/etc/crontab")) OR (platform="macOS" AND (file_path="/Library/LaunchDaemons/" OR file_path="/Library/LaunchAgents/")))`
DS0009	Process	Process Creation	Monitor for newly executed processes that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Note: Below is the relevant Events and SourcesWindows: • Sysmon Event ID 1: Process creation, particularly for schtasks.exe, at.exe, Taskeng.exe, crontab, etc. • Windows Event Log EventCode 4688: Process creation that might involve task scheduling. • Windows Task Scheduler Logs: Task creation, modification, or deletion. Linux/macOS: • Auditd logs: Monitoring for cron job creation or modifications. • Syslog: Logs related to cron jobs or scheduled tasks. • File integrity monitoring (FIM): For changes to /etc/cron, */var/spool/cron/*, or user-specific cron jobs. Containers:- Container logs: Detection of scheduled tasks or cron jobs within container environments. Analytic 1 - Look for task execution with unusual parameters. `(sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" OR sourcetype="WinEventLog:Security" OR sourcetype="linux_auditd" OR sourcetype="syslog") | where Image IN ("schtasks.exe", "at.exe", "Taskeng.exe", "cron", "crontab", "systemd-timers")`

ID	Data Source	Data Component	Detects
DS0003	Scheduled Job	Scheduled Job Creation	Monitor newly constructed scheduled jobs that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. On Windows systems, security event ID 4698 (A scheduled task was created) provides information on newly created scheduled tasks. It includes the TaskContent field, which contains an XML blob that captures key information on the scheduled task including the command to be executed. Analytic 1 - Scheduled Task Execution `source="*WinEventLog:Security" EventCode="4698" | where NOT (TaskName IN ("\Microsoft\Windows\UpdateOrchestrator\Reboot", "\Microsoft\Windows\Defrag\ScheduledDefrag"))| search TaskContent="powershell.exe" OR TaskContent="cmd.exe"`

References

1. Microsoft. (2005, January 21). Task Scheduler and security. Retrieved June 8, 2016.
2. Campbell, B. et al. (2022, March 21). Serpent, No Swiping! New Backdoor Targets French Entities with Unique Attack Chain. Retrieved April 11, 2022.
3. Rufus Brown, Van Ta, Douglas Bienstock, Geoff Ackerman, John Wolfram. (2022, March 8). Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments. Retrieved July 8, 2022.
4. Chen, J., et al. (2022). Delving Deep: An Analysis of Earth Lusca’s Operations. Retrieved July 1, 2022.
5. Muhammad, I., Unterbrink, H.. (2021, January 6). A Deep Dive into Lokibot Infection Chain. Retrieved August 31, 2021.
6. Kaspersky Lab's Global Research & Analysis Team. (2016, August 9). The ProjectSauron APT. Technical Analysis. Retrieved August 17, 2016.
7. Cybereason Nocturnus. (2022, February 1). StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations. Retrieved August 15, 2022.
8. PowerSploit. (n.d.). Retrieved December 4, 2014.
9. Microsoft. (2012, November 15). Domain controller: Allow server operators to schedule tasks. Retrieved December 18, 2017.
10. Microsoft. (2013, May 8). Increase scheduling priority. Retrieved December 18, 2017.