TID	Condition(s)	Description	Rule(s)	Reference
▪ T1546.015	Triggers when a windows scheduled task with COM-enabled handler has multiple COM payloads	Usually the Task COM Handlers have their payload located under HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\%Class_ID% (which requires admin rights to write in); however one can Hijack it by creating respective entry with the same class id under HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\%Class_ID%. It seems the ones under HKCU execute first … Hence having 1 COM handler from HKLM is expected, but having >1 could be an indication of a hijack.	▪ COM_Hijack_multi_payloads	https://attack.mitre.org/techniques/T1546/015/
	Triggers when a Scheduled Task has more than 1 action under Actions	Usually the Scheduled Tasks have not more than 1 action, everything above that count could be suspicious.	▪ Suspicious_Task_multi_actions	n/a
▪ T1564	Triggers when an SD value holding a Security Descriptor bytes for a scheduled task is missing or empty.	This technique has been abused by Hafnium threat group in tarrask malware. Deleting or erasing the content of SD value (holding a Security Descriptor bytes) is effectively hiding the task from Task Scheduler GUI.	▪ Hidden_Task_security_descriptor_abuse	https://github.com/wit0k/tarrask