Living Off the Land Attacks with Scheduled Task

logrhythm.com/blog/living-off-the-land-attacks-with-scheduled-task

March 11, 2020

In our previous living off the land (LotL) blog post, we discussed why attackers use tools that already exist in the environment to plan an attack. But what role does Microsoft Scheduled Tasks in an attacker's plan?

In this post, we're going to test our lab environment as an example and take a threat hunting approach to learn what happens as it pertains to Microsoft Scheduled Tasks and a potential LotL attack.

What is Scheduled Tasks?

Scheduled Tasks (and its predecessor AT.EXE) have been in the Windows OS since Windows 98 in one form or another. Fundamentally, they give users the ability to schedule the launch of programs or scripts at a specified time, or on a repeating schedule. This is a useful feature for general maintenance of the Windows OS itself, and for automating certain types of tasks, such as cleaning things up on startup or shutdown or running a regular backup.

Scheduled Tasks are also a great tool for adversaries to use, since they are present on all Windows operating systems, they are easy to use, and most users do not even realize they're present. Even those who are aware might struggle to work out which tasks are valid parts of the OS or applications they have installed, and which, if any, are malicious. Scheduled Tasks are currently used by a range of threat groups predominantly to achieve persistence. They could also be used to check in via command and control channels of a regular basis for new content for a trojan or dropper.

LogRhythm Labs recently released the MITRE ATT&CK® technique detection Scheduled Task (T1053) to help detect attackers using this tool. There are many different ways to detect when a Scheduled Task is created, run, and deleted, but for the purposes of this blog post, we're focusing on command line arguments involving Scheduled Task (schtasks.exe) and the deprecated AT.EXE.

First and foremost, if you notice AT.EXE process running, you should investigate this immediately. According to Microsoft, Scheduled Tasks replaced AT.EXE, but AT.EXE is still present to support legacy operations. Today, AT.EXE should not be used, and if it is in your environment, it likely means you need to update your legacy scheduled task, or something malicious is issuing AT commands. Cleaning up these legacy tasks would be a good first step in aiding visibility of Scheduled Task abuse by attackers.

Threat Hunting with Scheduled Tasks

A great starting point in formulating a threat hunting strategy is to read up on the technique from ATT&CK, and especially the detection section here.

Following the detection advice there, we can move to the LogRhythm WebUI and perform a search to see if there are any recent processes named “schtasks.exe” or “at.exe”.

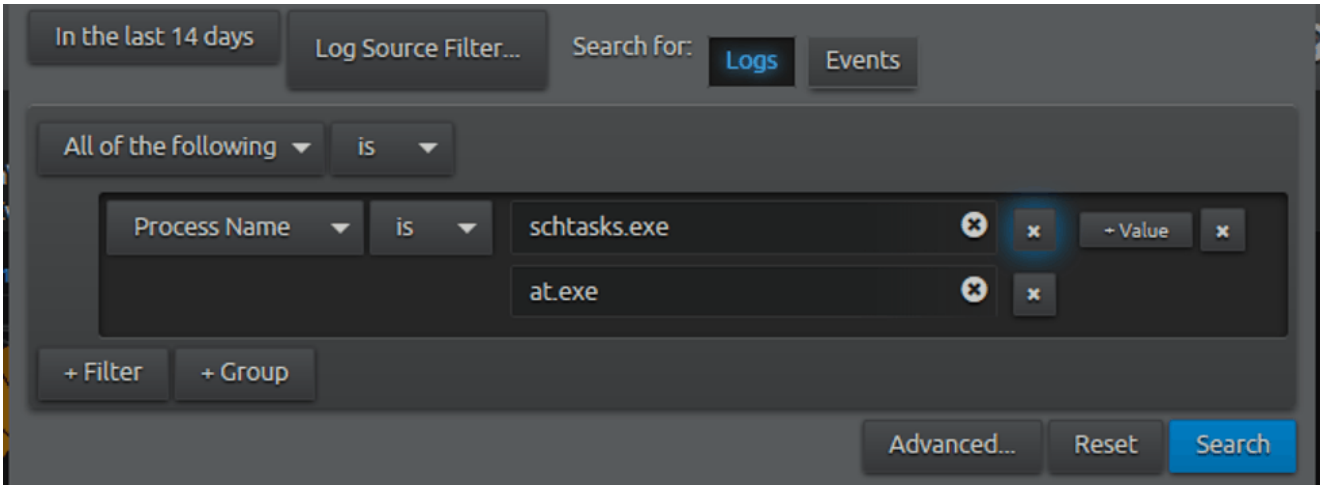

Figure 1: LogRhythm WebUI search for schtasks.exe processes

We see that there’s quite a bit of activity in the last 14 days, and we can also see some frequent occurrences in the “Top Log Source Host” and “Top Common Event” widgets. Common occurrences can indicate a normal occurrence, or abnormal occurrence. Either way, we’ll need to dig deeper. In our custom Advanced Analysis view, we can quickly see that the periodic activity is occurring, but not equally distributed across log sources by evidence of counts.

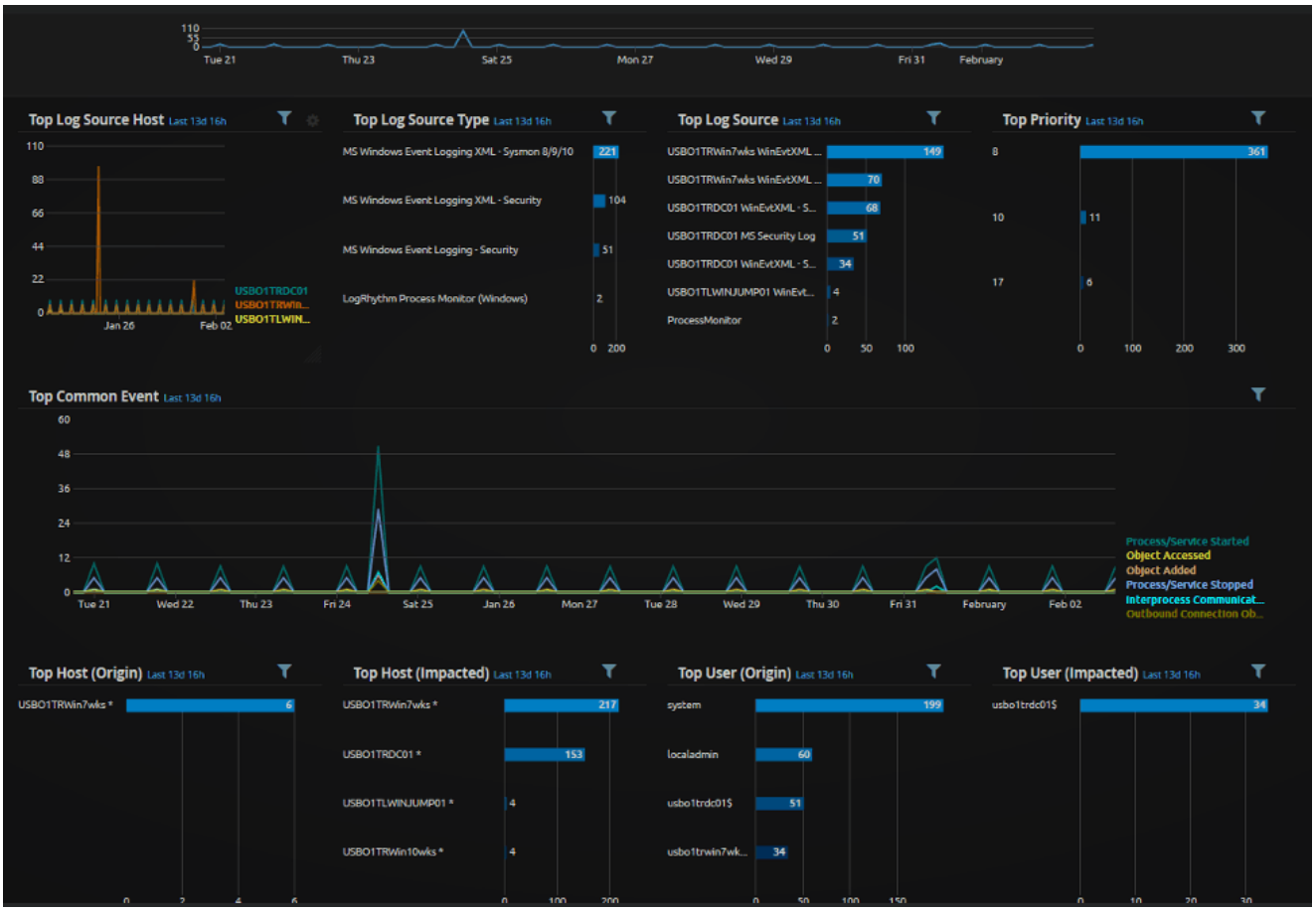

Figure 2: LogRhythm WebUI shows frequent occurrences of Top Log Source Host widget

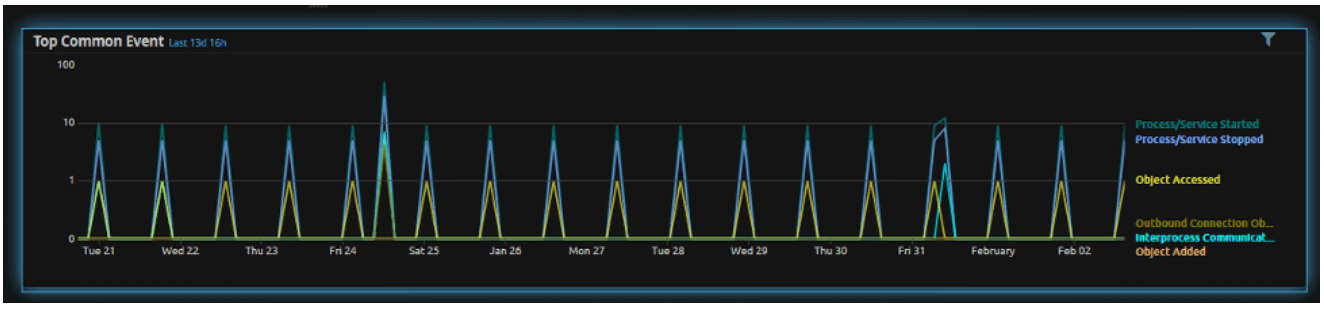

Figure 3: LogRhythm WebUI shows frequent occurrences of Top Common Event widget

By filtering on the most common occurrence of the command line, we can see that the periodic activity is associated with this command.

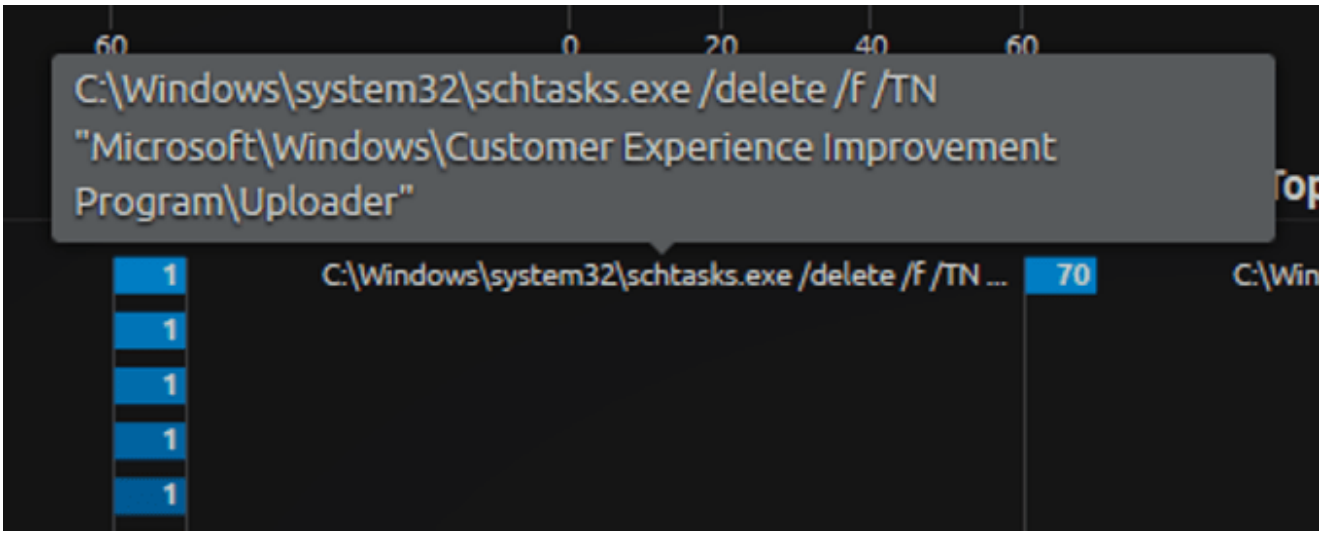

Figure 4: You can see periodic activity by filtering on the most common occurrence

Also, by filtering on the command, we can quickly see that the parent process is named "wsqmcons.exe".

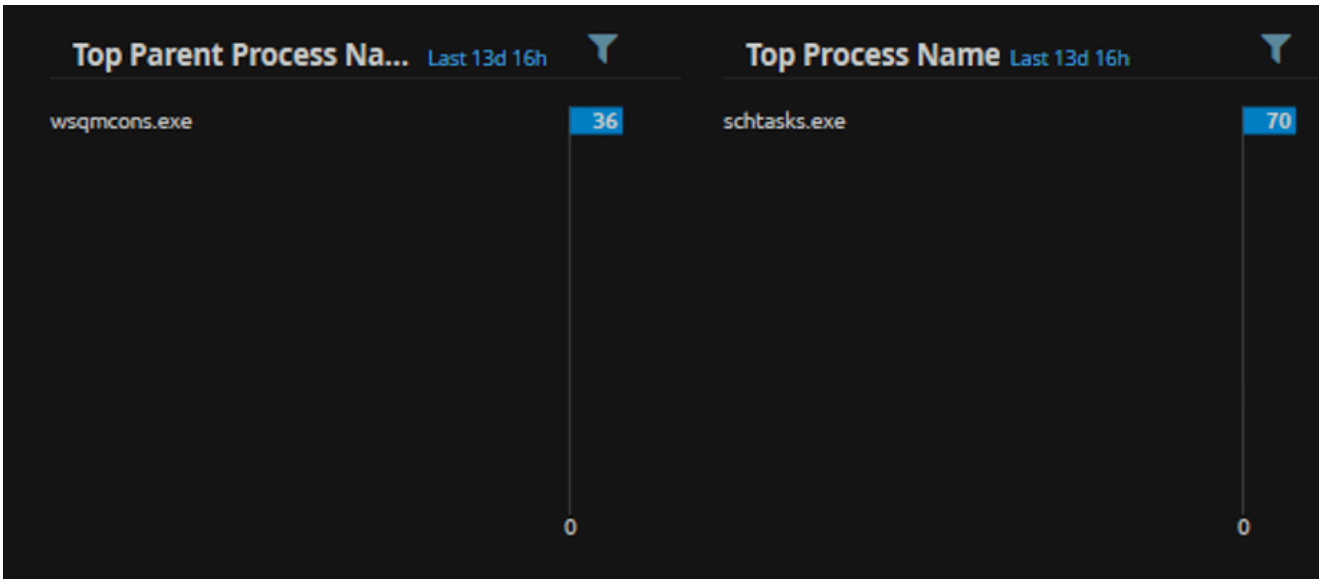

Figure 5: Filtering on the command shows the parent process name

Let's recap what we have found so far. We've found several occurrences of Scheduled Tasks being executed in our environment, across different hosts, and under varying user accounts. We initially focus on the most commonly appearing command line that is configuring Scheduled Tasks, which is deleting a task, and the parent process doing the deletion is the wsqmcons.exe process. So, we have a few pieces of evidence already, but we need to dig deeper to find out what is really happening here.

In looking closer at one of the logs, we see that the user is "System" and wsqmcons.exe resides in the System32 directory, as shown in the following two screen shots.

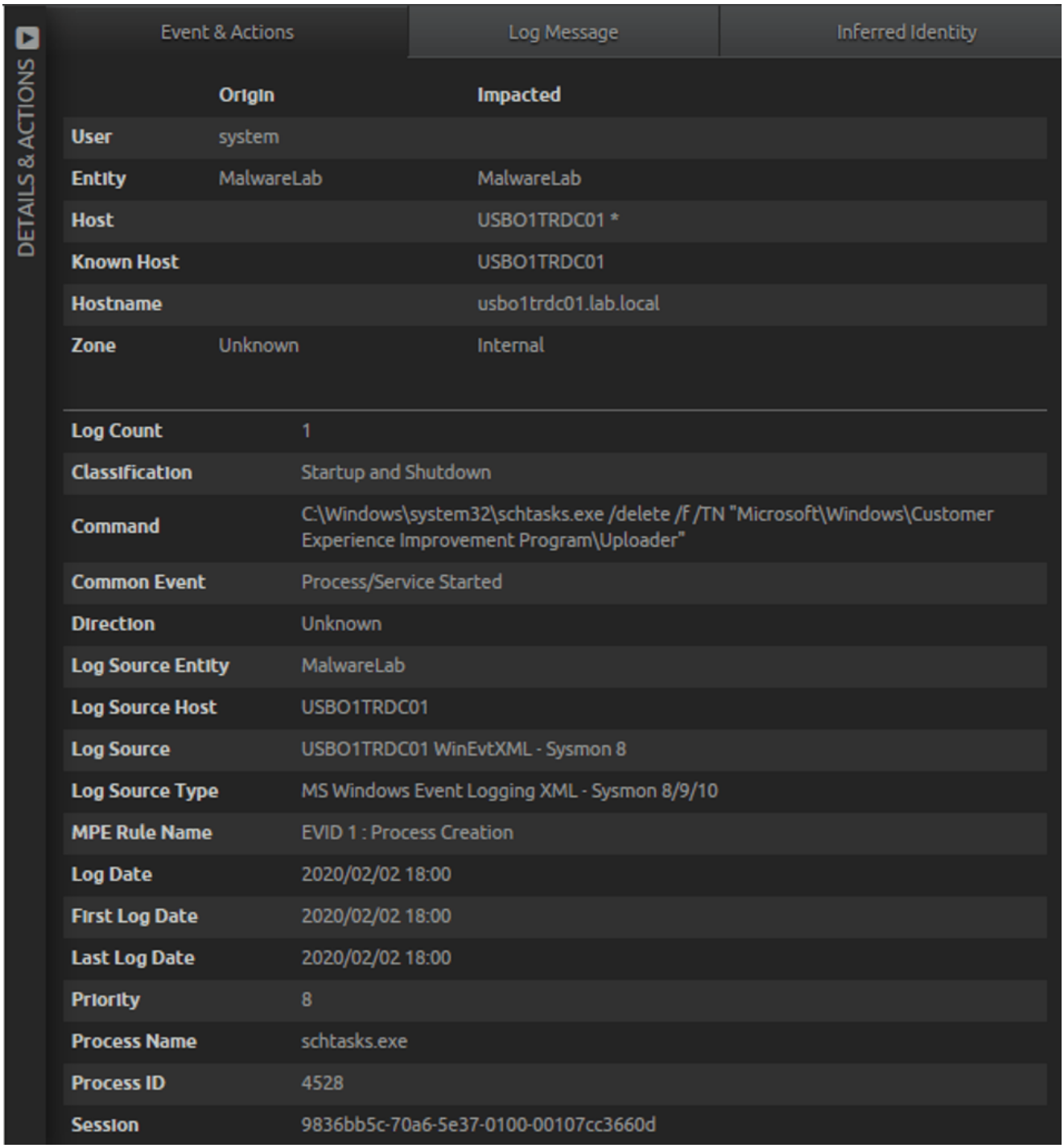

Figure 6: The user as reflected in this log is "System"

Severity	Information
Subject	C:\Windows\System32
Vendor Message ID	1
Version	6.3.9600.18001 (winblue_ltsb.150731-0600)
Log Sequence Number	229705
Domain (Impacted)	NT AUTHORITY
Hash	2E9E198247BF0E9BD94B42286798A5AC
Vendor Info	Process Create (rule: ProcessCreate)
Parent Process ID	3864
Parent Process Name	wsqmcons.exe
Parent Process Path	C:\Windows\System32\
Session Type	System

Figure 7: The parent process is wsqmcons.exe in the System32 directory

By asking the question of what the activity of this process is for the past 14 days (14*24 = 336 hours), we want to determine if this parent process also has any activity that might be worth noting in our threat hunt.

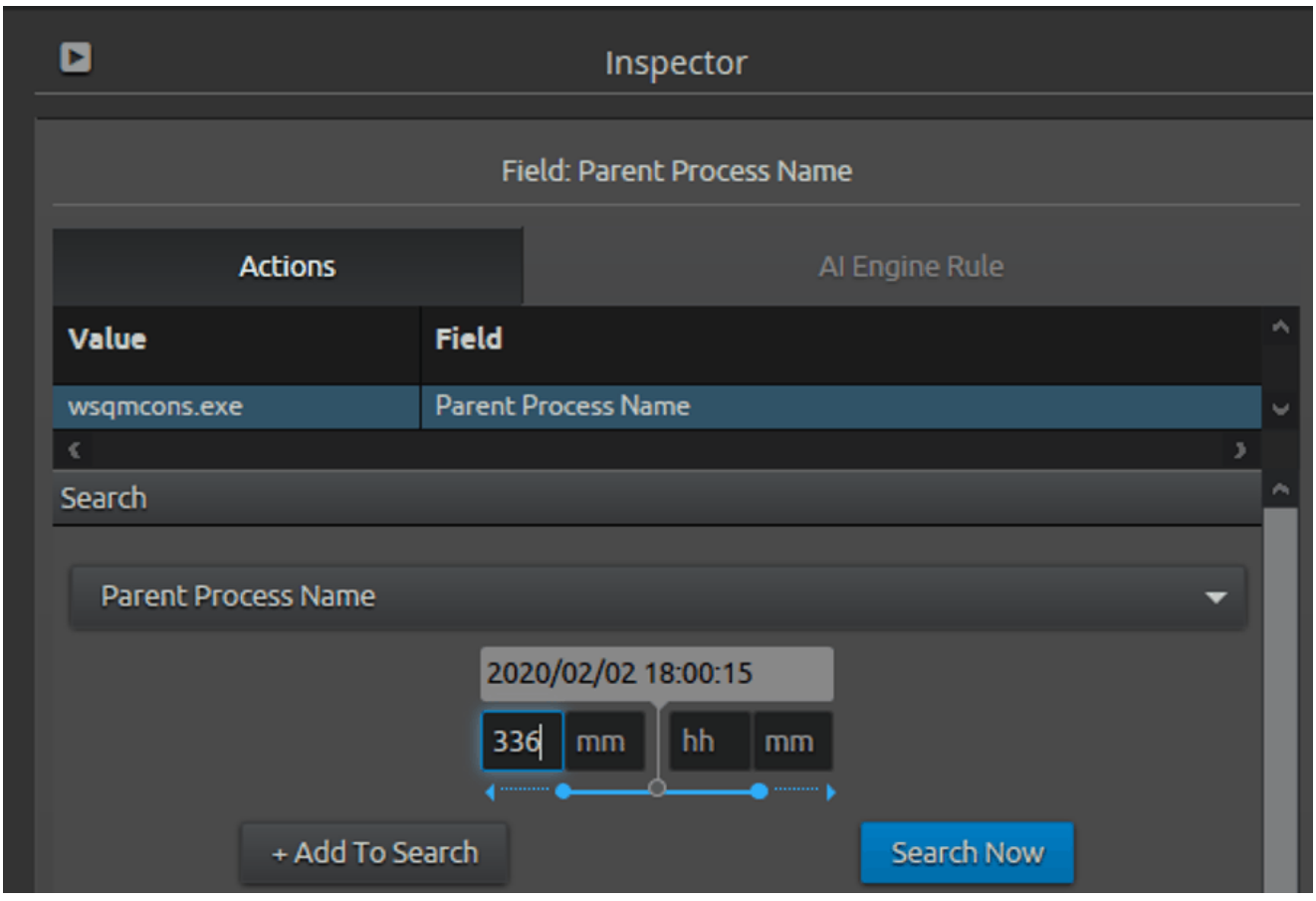

Figure 8: This query explores the activity over the last 14 days

Our results don't net anything new, but show the periodic activity. Now, it's time to query Google to find out more about what wsqmcons could be. By highlighting wsqmcons, and then right clicking to perform a Google search, we get a few results.

Figure 9: Results show periodic activity

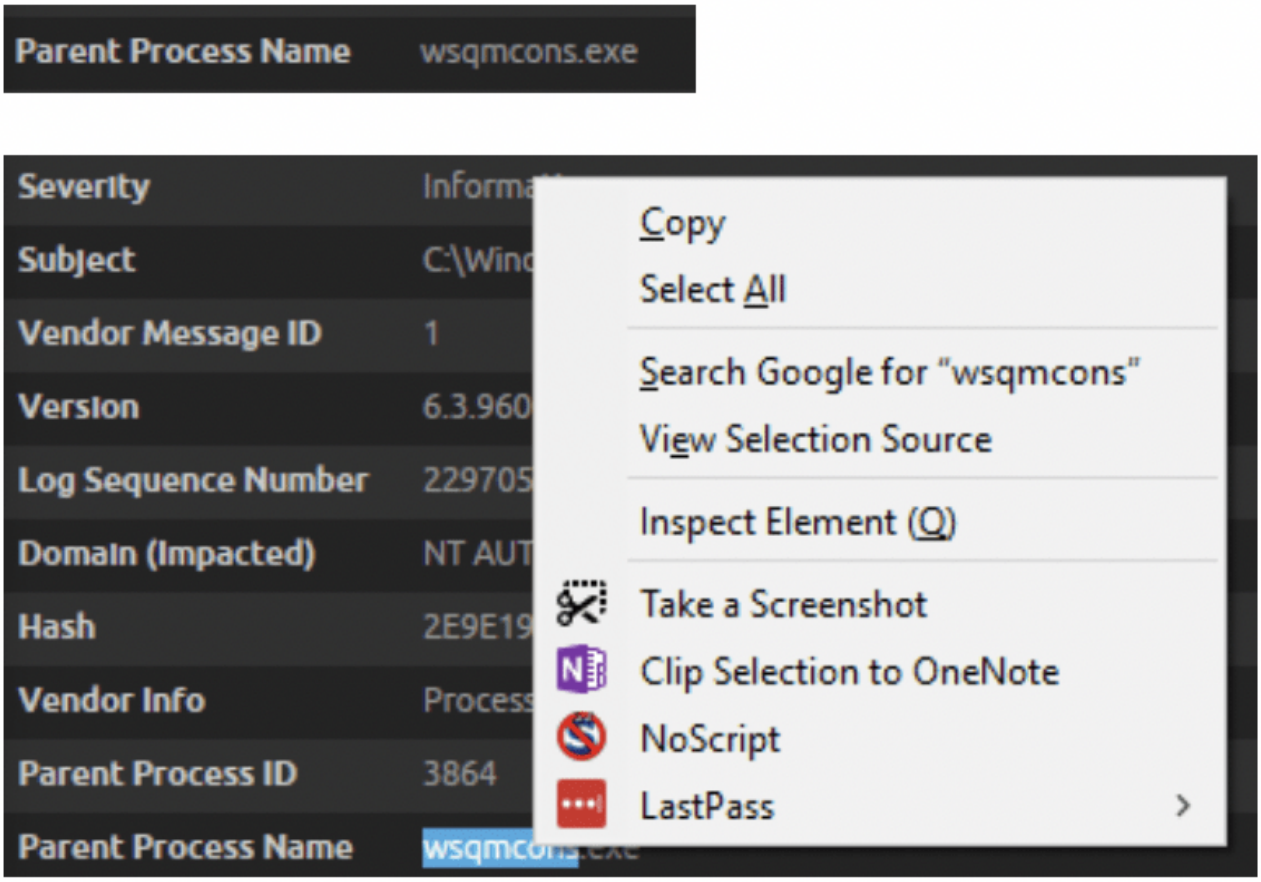

Figure 10: Query Google to search for "wsqmcons.exe"

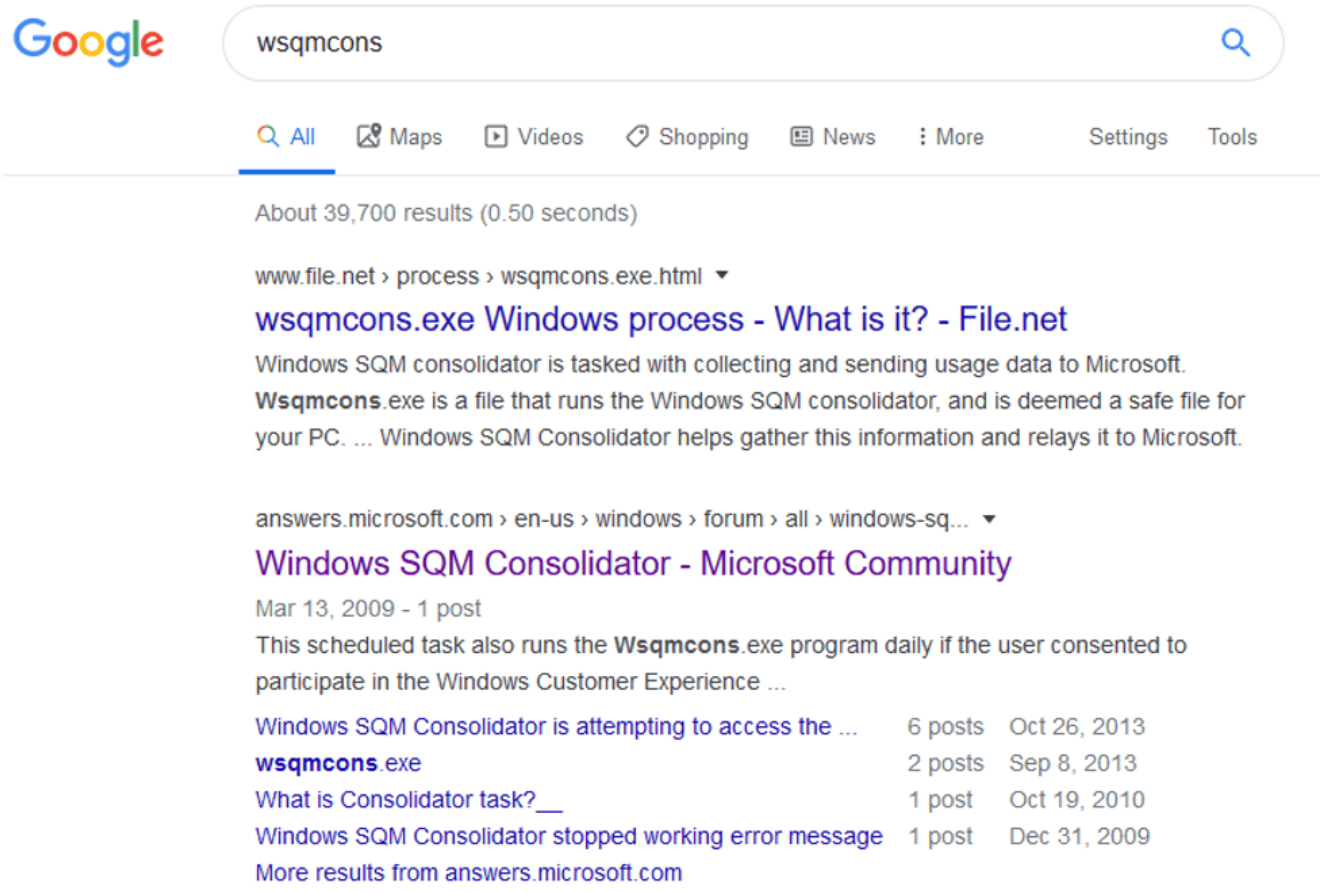

Figure 11: Google search results of wsqmcons.exe

It's best to read from sources of authority first, so we'll add microsoft.com to the search query, and we receive a result for "Windows SQM Consolidator."

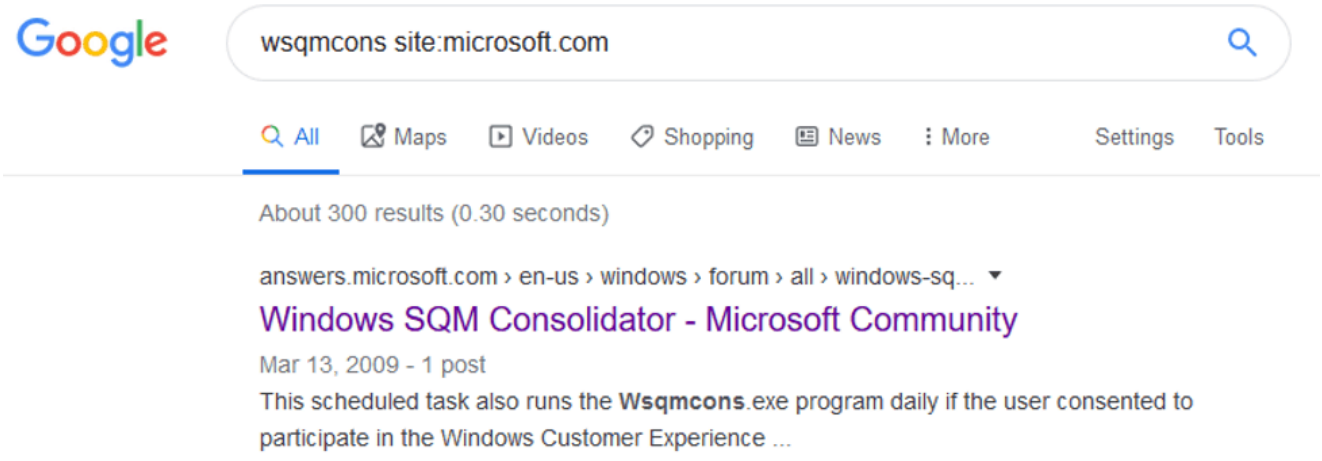

Figure 12: The search query for "Windows SQM Consolidator"

According to Microsoft, "This scheduled task runs the Wsqmcons.exe program when you install Windows Vista. This scheduled task also runs the Wsqmcons.exe program daily if the user consented to participate in the Windows Customer Experience Improvement Program. This program collects and sends usage data to Microsoft. The Wsqmcons.exe program is located in the System32 folder."

Note, the date of this article is March 2009. This service has been around a long time. Does that mean it's trustworthy and the Scheduled Task should be whitelisted? Not necessarily. It depends on your company's risk tolerance of an application sending metadata that it has collected about your system, possibly about you, back to the company. This type of collection is typically referred to as "Telemetry." As a best practice, corporate assets should not send any sort of telemetry.

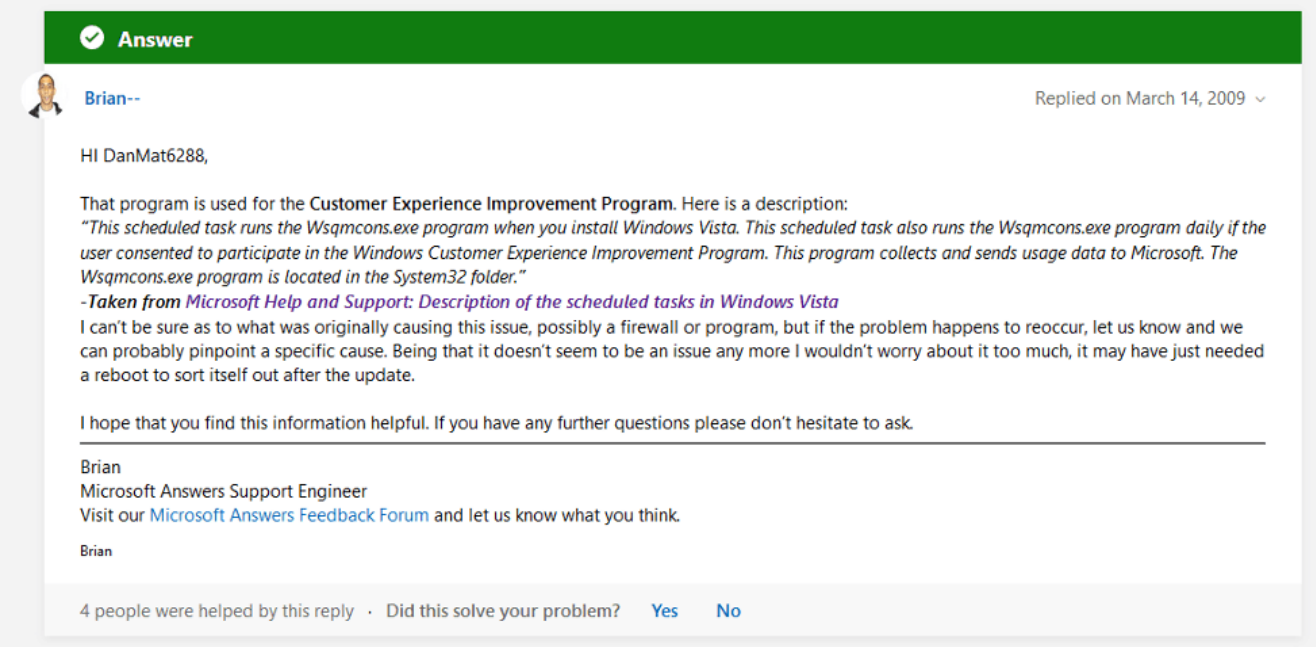

Figure 13: Search results for Windows SQM Consolidator

Consolidator	Customer Experience Improvement Program	This scheduled task runs the Wsqmcons.exe program when you install Windows Vista. This scheduled task also runs the Wsqmcons.exe program daily if the user consented to participate in the Windows Customer Experience Improvement Program. This program collects and sends usage data to Microsoft. The Wsqmcons.exe program is located in the System32 folder.
OptinNotification	Customer Experience Improvement Program	This scheduled task runs the \System32 \wsqmcons.exe -n 0x1C577FA2B69CAD0 command when you log on to a user account. This scheduled task prompts the Microsoft Windows Software Quality Metrics opt-in notification.

Figure 14: The results indicate a telemetry collection, which organizations should avoid

What can you do about Microsoft collecting telemetry as part of its "Customer Experience Improvement Program?" Quite a bit. Microsoft provides guidance on how to manage the privacy settings of the "Customer Experience Improvement Program," including how to configure and set a GPO to disable this sort of collection and telemetry data being sent. Review the "Procedures for controlling the Windows Customer Experience Improvement Program" if you are interested in disabling the "Customer Experience Improvement Program" in your environment.

Assess the Threat Hunting Findings

So, did we find something interesting in this threat hunt using the MITRE ATT&CK Scheduled Task technique? We found telemetry occurring, and this is something we don't want to run in our environment. As a best practice, we enabled a GPO to disable this sort of collection and telemetry in our environment, and you likely should too if you find wsqmcons running in your environment.

While we didn't find an attacker living off the land in this case, the above process provides a good template for hunting for this kind of activity. This might be a hunt that defenders conduct on a periodic basis. Alternatively, the MITRE ATT&CK Schedule Task detection rule is available to LogRhythm's customers in our out-of-the-box content. This will automatically alert if tasks are created or deleted in your environment. Check out the links below for more details of the MITRE module.