Clearing Logs

Hypothesis:
Clearing of audit / event logs could indicate an adversary attempting to cover their tracks.

Adversaries may delete or alter generated event files on a host system, including potentially captured files such as quarantined malware. This may compromise the integrity of the security solution, causing events to go unreported, or make forensic analysis and incident response more difficult due to lack of sufficient data to determine what occurred.

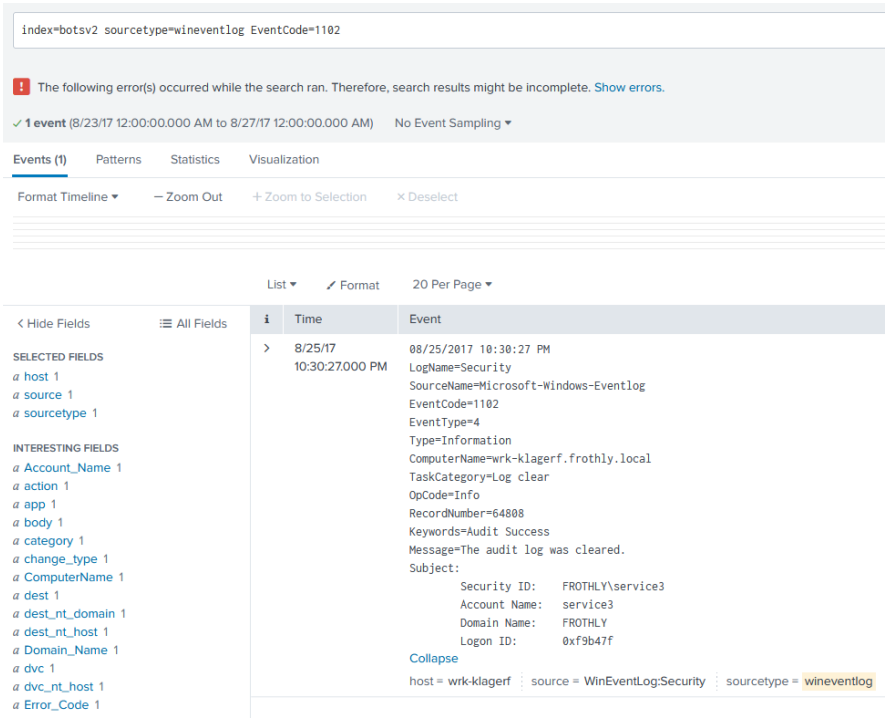
Here are some questions to think about that may help as we conduct our hunt:

- What data sources (sourcetypes) are needed to identify event or audit logs are being cleared?
- Are there specific event codes or values that would identify that event or audit log clearing is occurring?
- Who was clearing event logs?
- What systems were used to clear event logs?
- When were event logs cleared?
- Are they generally cleared before or after an adversary completes its work?

Cleared Event Logs

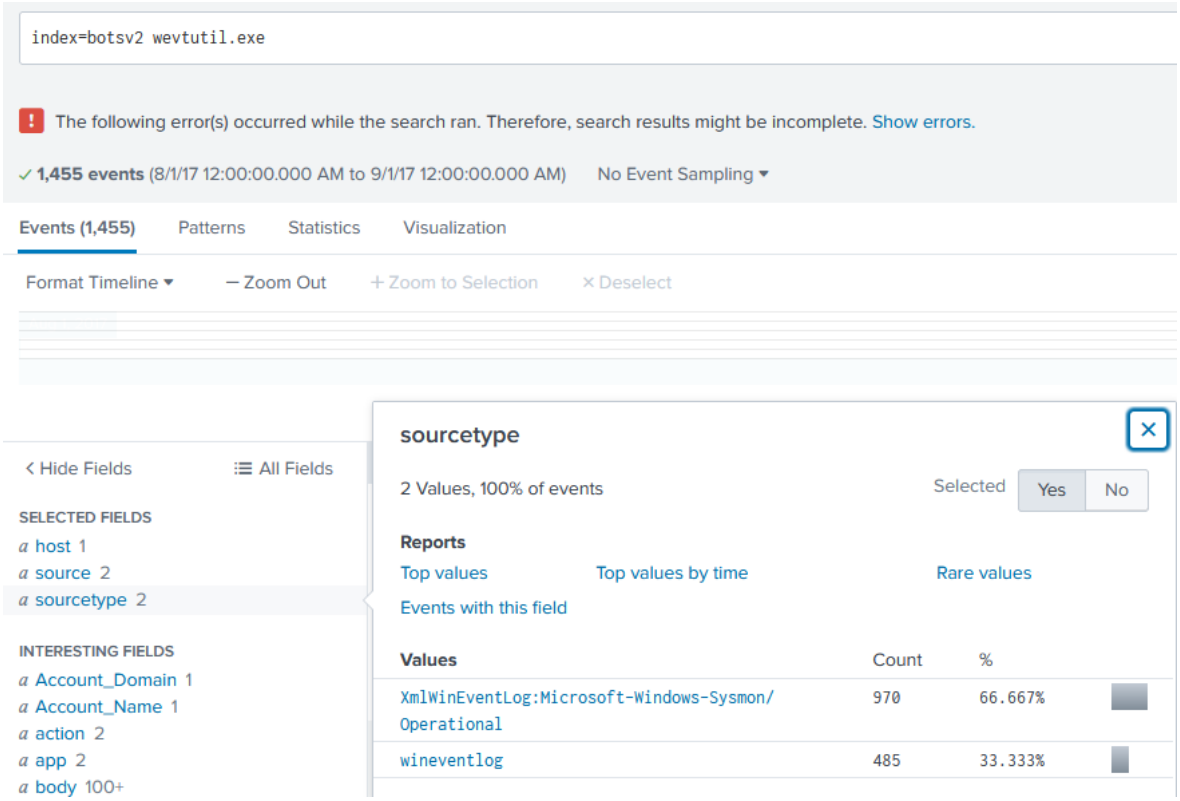
- We can do a quick Google search for “windows event log cleared” and we can see that for Security logs, the event code 1100 and 1102. For System logs, it is event code 104.

- If we search within the Windows event logs for EventCode 1102, we can see that Kevin’s workstation, wrk-klagerf, was cleared. We can also see that the service3 account was the account that cleared the log.



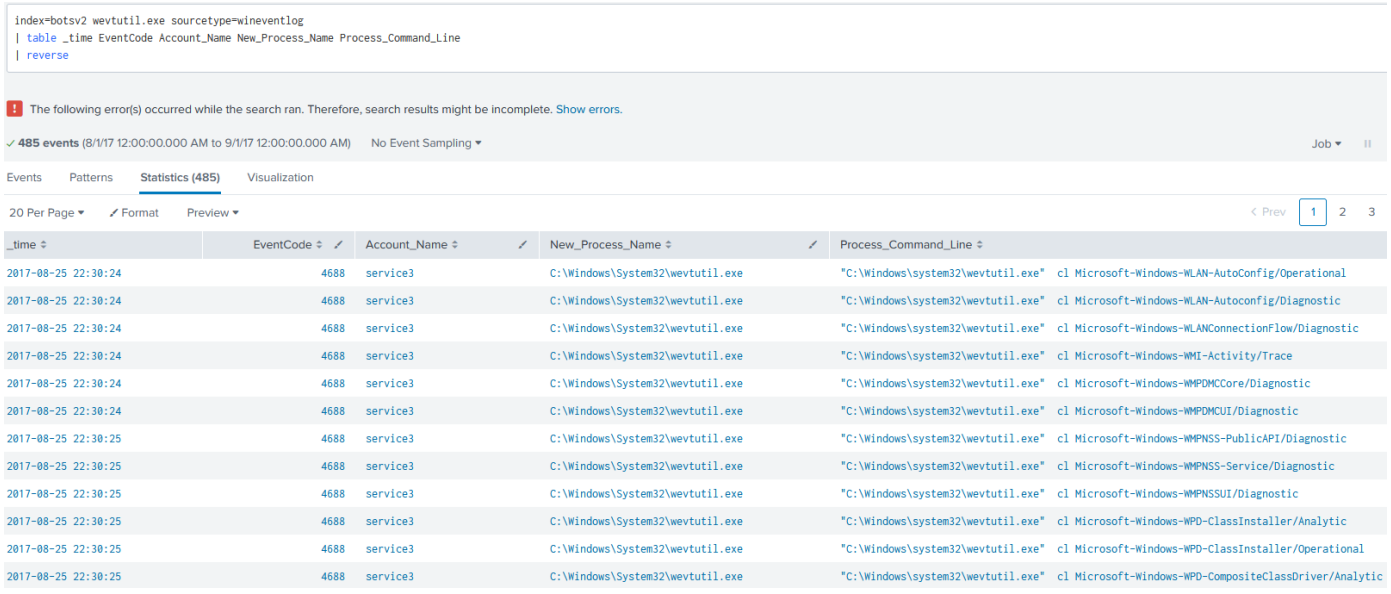
wevtutil.exe

- Let's hunt for these events for any wevtutil.exe references.
- We can also see that we have both Sysmon and Windows Event Logs with references



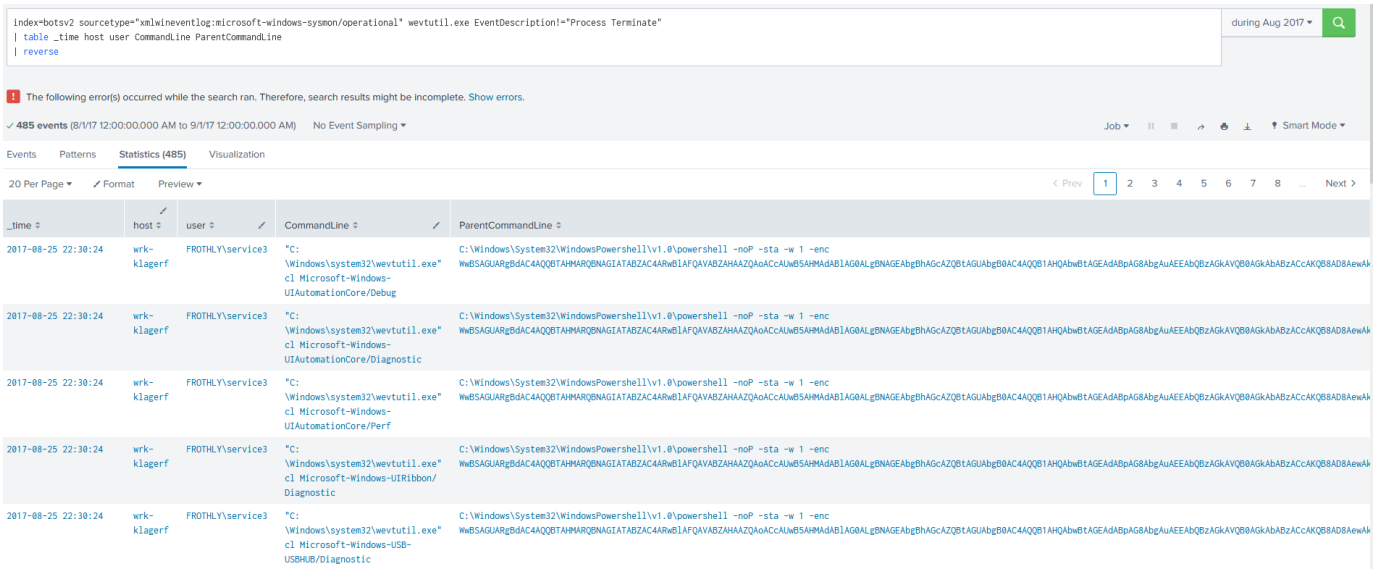
to this exe.

- If we drill down on the Windows Event Log sourcetype,we can see that these events are all coming from EventCode 4688 - A New Process Has Been Created.
- We can also see that in the Process_Command_Line field that wevtutil.exe is called in each one. The events uses the cl argument and each call a distinct log file which clears each and every log file called. We can see 485 events so it is safe to say almost every possible Windows log we can imagine is being cleared during this sequence.



_time	EventCode	Account_Name	New_Process_Name	Process_Command_Line
2017-08-25 22:30:24	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WLAN-AutoConfig/Operational
2017-08-25 22:30:24	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WLAN-Autoconfig/Diagnostic
2017-08-25 22:30:24	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WLANConnectionFlow/Diagnostic
2017-08-25 22:30:24	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMI-Activity/Trace
2017-08-25 22:30:24	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMPDMCCore/Diagnostic
2017-08-25 22:30:24	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMPDMCUI/Diagnostic
2017-08-25 22:30:25	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMPNSS-PublicAPI/Diagnostic
2017-08-25 22:30:25	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMPNSS-Service/Diagnostic
2017-08-25 22:30:25	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMPNSSUI/Diagnostic
2017-08-25 22:30:25	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WPD-ClassInstaller/Analytic
2017-08-25 22:30:25	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WPD-ClassInstaller/Operational
2017-08-25 22:30:25	4688	service3	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WPD-CompositeClassDriver/Analytic

- If we take a look at the Sysmon data with the same basic search, we can see similar results with a couple of small differences. When we initially looked at the sourcetype Sysmon, we had 970 events, but now we only have 485. We added criteria that Event Descriptions were NOT Process Terminate as they were less interesting than the Process Starts that make up the bulk of these events.
- When we look at the field CommandLine, we can see the same thing we saw with the 4688 process events, that the wevtutil.exe is executing with the clear log argument and hitting numerous logs. The ParentCommandLine appears be encoded PowerShell.



Now we answer the questions asked to know what we have learned:

- What data sources (sourcetypes) are needed to identify event or audit logs are being cleared? ***Wineventlog, Sysmon***
- Are there specific event codes or values that would identify that event or audit log clearing is occurring? ***1102***
- Who was clearing event logs? ***Service3***
- What systems were used to clear event logs? ***admin workstation wrk-klagerf***
- When were event logs cleared? ***8/25/17 10:30:27.000 PM***
- Are they generally cleared before or after an adversary completes its work? ***After work***