Threat Hunter Playbook

Playbook Title: "Windows Event Logs Cleared via Windows Command (wevtutil cl)"

Date Created: 2022-07-10

Hypothesis: Attackers will try to cover their tracks using Windows Commands (such as "wevtutil cl")

Mitre Tactic: T1070 "Indicator Removal on Host"

Mitre Sub Technique: T1070.001 "Indicator Removal on Host: Clear Windows Event Logs" (via Windows Command "wevtutil cl")

Simulation Details (if any): None

Proposed Search Query: `index=sysmon event.code=1 process.command_line="wevtutil cl *"`

Hunter Limitations/Observation Notes: The Proposed Search Query did not produce any valuable results. However, it would be prudent to run a simulation to test this command and build the detection.

Hunt Findings: Although the query did not produce results, I believe the developed query should be made into a detection because attackers could possibly use the command to clear the Windows Event logs.

Proposed Detection Title: "ALERT: Windows Command ("wevtutil cl") used to clear Windows Event logs"

Proposed Detection Query:

```
index=sysmon event.code=1 process.command_line="wevtutil cl *" | rename process.command_line as command | table _time host.name event.code user.name command | sort _time
```