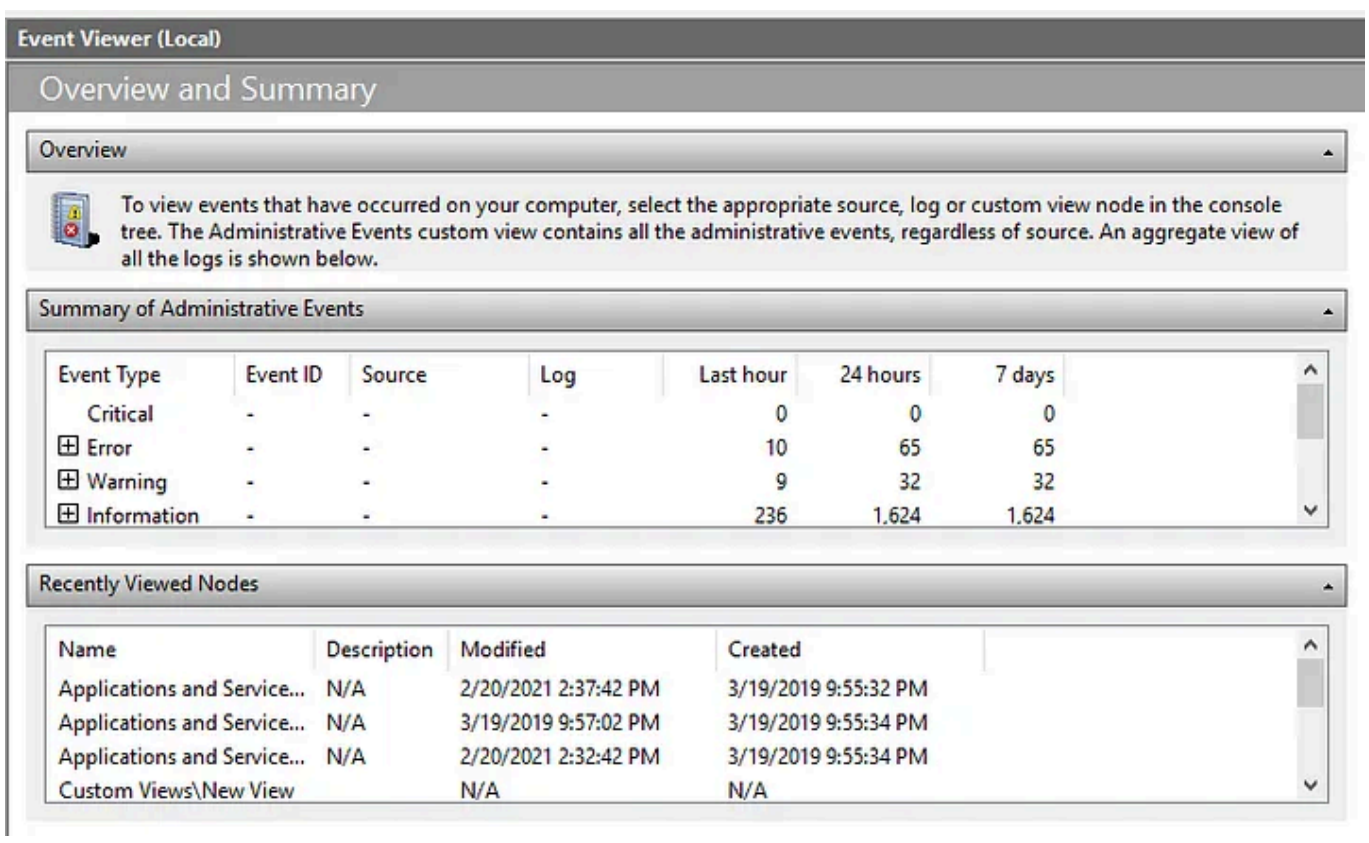
Finding Forensic Goodness In Obscure Windows Event Logs

Nasreddine Bencherchali · Follow
5 min read · Feb 20, 2021



Event Viewer

If you've been doing some digital forensics or threat hunting for some time. You'll know that one of the key sources of information are the Windows event logs. Most of the talks around the windows event logs only mention the "main" sources of logs such as "System" or "Application", even though windows provide many sources.

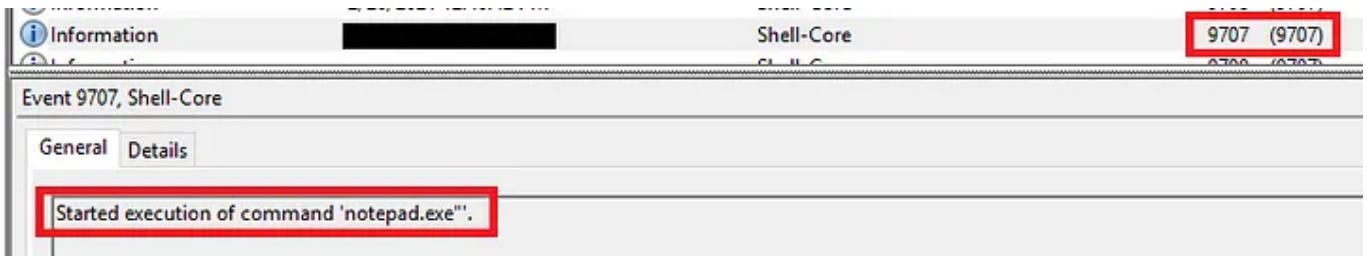
To get the full logging experience one need to enable additional logging from the ***Group Policy Editor*** or even installs something like ***Sysmon*** but what to do in the case where one cannot install or enable the aforementioned logs? Or let's say you're performing an investigation and the machine has only default logging enabled ? Does the windows event log contains other useful information other than the one provided by the main sources (Application, System and Security) ?

Today we'll take a look at some of those event logs and see if there is anything interesting.

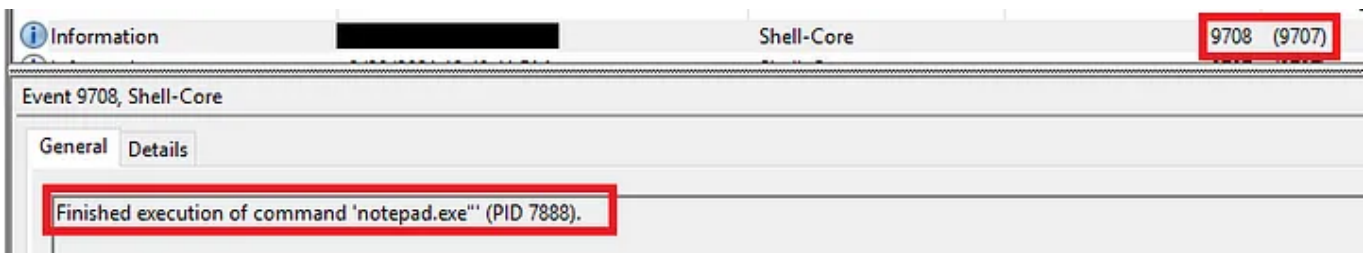
Please note that what gets logged by default in the "System" or "Security" logs has been covered before. What i want to do in this blog post is to take a look at other windows event log files and try to see if there is any interesting data.

Microsoft-Windows-Shell-Core/Operational

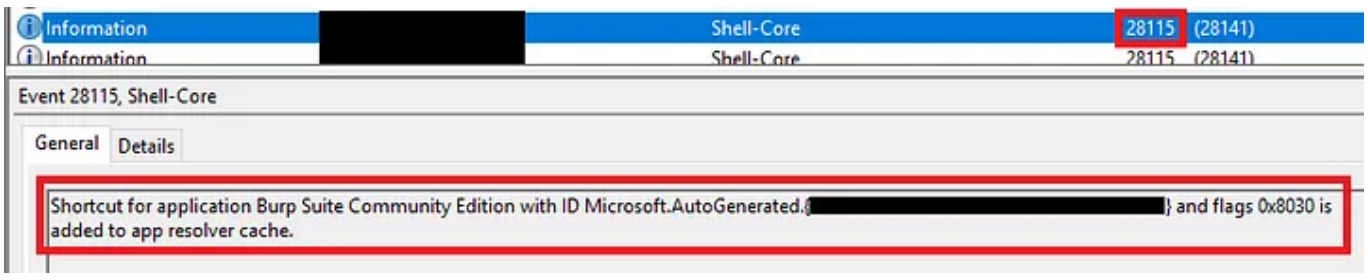
- **EID 9707:** Detects the start of the execution of a process from both the "Software\Microsoft\Windows\CurrentVersion\Run" and "Software\Microsoft\Windows\CurrentVersion\RunOnce" registry keys with the full command line.



- **EID 9708 :** Detects when the aforementioned process finishes execution with the corresponding PID (Useful when the process is still running on the system).



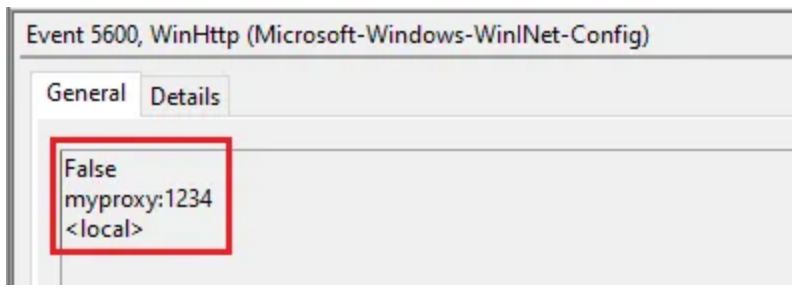
- **EID 28115 :** Triggered when a shortcut is added to the "App Resolver Cache". Indicates when an application is installed.



Both EID **9707** and **9708** can be used to search for any malware using the "**Run**" and "**RunOnce**" key as persistence mechanisms.

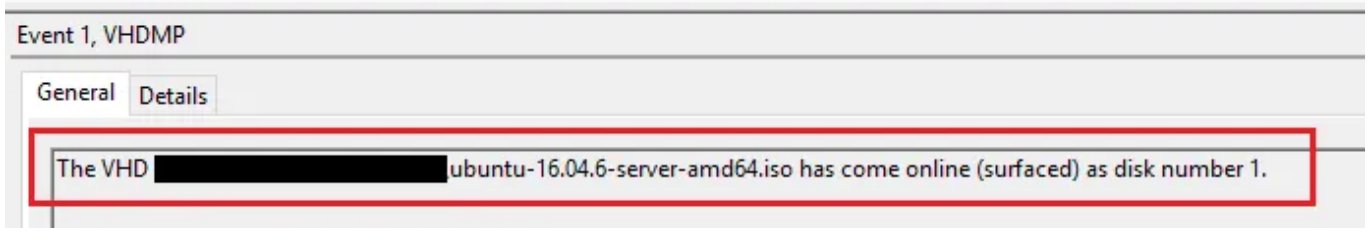
Microsoft-Windows-WinINet-Config/ProxyConfigChanged

- **EID 5600 :** Indicates change in the proxy configuration. For example if i change my proxy configuration from the "Internet Option" menu. The event will get generated.

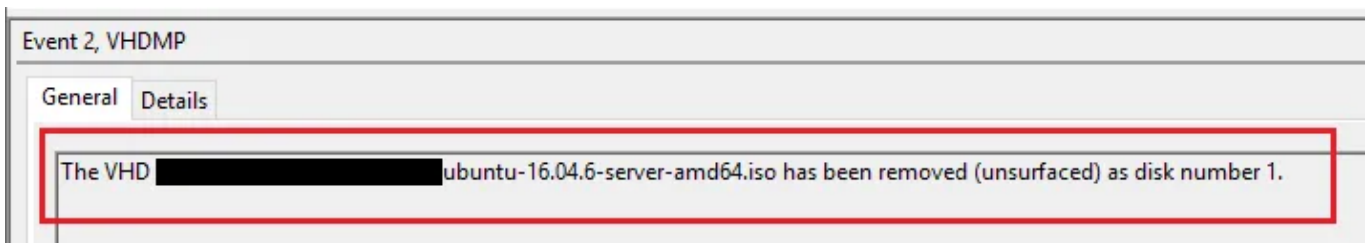


Microsoft-Windows-VHDMP-Operational

- **EID 1 :** Triggers when you mount a VHD (Virtual Hard Disk).



- **EID 2 :** Triggers when you unmount a VHD (Virtual Hard Disk).



- **EID 12 :** Contains information about the type, path, handle count of the mounted device.

OAlerts (Office Alerts)

- **EID 300 :** Triggers when a prompt is shown inside an office application. For example when the prompt to save the office (excel, word…etc) document is shown an event is generated. Contains information about the name of the files (In the case of saving a file), the office version, the office application that triggered the alert (Word, PowerPoint, Excel…etc).

This event can be used to determine if a suspicious for example file has been opened or altered in some way by a user.

Microsoft-Windows-WLAN-AutoConfig/Operational

- **EID 8001 :** Triggers when a successful connection to a wireless network occurs.
- **EID 8003 :** Triggers when we’re successfully disconnected from a wireless network.

Microsoft-Windows-Winlogon/Operational

- **EID 811/812 :** Triggers when a user logon to a machine. You can check for the “<SessionEnv>” subscriber notification in EID 811 to indicates that a user logged on via RDP.

Note that as far as i can tell the *“SessionEnv”* subscriber is also logged when a user logon to a machine for the first time (I.E doesn’t have a session). To distinguish between the two (RDP or Local) look for the EID 1/2 shortly after the “SessionEnv” subscriber to indicate a local logon and if not present that means its an RDP logon.

- **EID 1/2 :** In my test lab this event is triggered only when a user log in to a computer on which he doesn’t have a session (I.E session disconnected/ doesn’t exist). EID 2 can be used to determine how many times a user typed an incorrect password.

For example, if a user provided a wrong password and EID 2 will be generated with the “Result Code : 1326”. Which indicates an incorrect password.

If the password is correct, then the “Result Code : 0” is generated.

Microsoft-Windows-Windows Firewall With Advanced Security/Firewall

- **EID 2004 :** Trigger when “A rule has been **added** to the Windows Defender Firewall exception list.
- **EID 2005 :** Triggers when “A rule has been **modified** in the Windows Defender Firewall exception list.”
- **EID 2006 :** Triggers when “A rule has been **deleted** in the Windows Defender Firewall exception list.”

Contains information about :

- The “Rule Name” that’s been altered.
- The “Modifying Application” that initiated the change.
- The “Action” and “Direction”
- The “User”.
- …Etc.

Microsoft-Windows-UniversalTelemetryClient/Operational

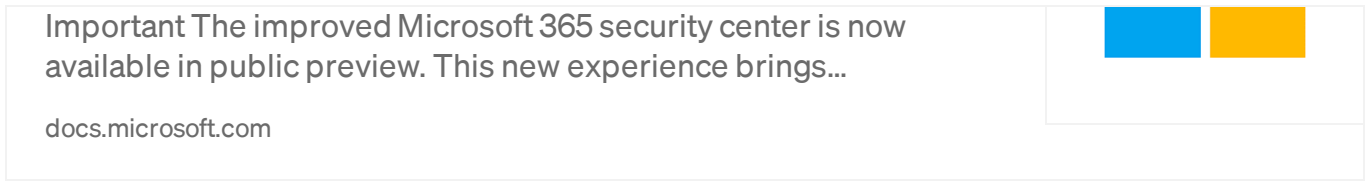
- **EID 55 :** Indicates whether the computer has Internet or Not.

You can use the difference between two events to determine why a process didn’t run (Maybe it needed internet) or answer the question did the malware send information to the C2 since the start of the infection for example.

Microsoft-Windows-Security-Mitigations/KernelMode

Another event log worth looking is the “Microsoft-Windows-Security-Mitigations/*”. This event log contains log about the “Exploit Protection” feature. A complete list of the EID’s available can be found below.

Apply mitigations to help prevent attacks through vulnerabilities - Windows security



. . .

Conclusion

We've taken a look at a couple of event logs that can be very useful during an investigation or a threat hunt. If you have other suggestions of events that should be added or noticed an error of some kind drop me a DM on twitter @nas_bench

Happy Hunting.

Forensics Dfir Threat Hunting Windows Windows Event Logs

Written by Nasreddine Bencherchali

Follow

2.1K Followers

I write about #Detection, #Sigma and #Windows. Follow https://github.com/nasbench/Misc-Research for interesting Windows tidbits