**Plus971 Cybersecurity**

Windows Forensics

**31s August 2023**

**Windows artifacts that can give me information about file access**

1. Using the event viewer we can filter for specific file related events using the following ID’s in the folder ‘Applications and Services Logs’ /Microsoft/Windows/FileHistory-Core or ‘Applications and Services Logs’ /Microsoft/Windows/FileHistory-Engine:
   1. Event ID 4663 (File and object access)
   2. Event ID 4656 (Handle Manipulation)
   3. Event ID 4660 (Object Open)
   4. Event ID 4670 (Permissions on Object)
2. LNK files: are those shortcuts to recently accessed files in the quick access panel of the windows file explorer, these can give us a list of files that were accessed and when they were accessed.
3. If the computer is under the active directory and the organization has file access auditing enabled then a look at the logs will tell us exactly when a file was accessed. And how many times. - unrelated to windows artifacts
4. Application and system logs in event viewer: can provide information related to errors in file access, disk operations and such.
5. The limitation of the event viewer is that even if object access auditing is enabled, specific file names or paths are not in the log, only the time at which they occurred, however using the time and alert type we can create a timeline that outlines a correlation which can be used as evidence.
6. Shellbags: shelbags can be used to analyze recently accessed files and folders however only contain a limited number of records. Stored at: Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Shell\Bags
7. Add jump list

**Windows artifacts that give me information about a file transfer to USB**

1. USB Device history in windows registry: the registry stores info about drives that have been plugged in
2. Windows Event logs: can contain events related to USB operations, errors, etc.. these can be stored in
   1. Event ID 2003,6418, 6417 : event occurs when USB is plugged in or removed
   2. Event ID 6416,4663 : audit info about actions performed, only occurs if local policy is set accordingly.
   3. Locations:
      1. ‘Applications and Services Logs’/Hardware Events.
      2. ‘Applications and Services Logs’/Microsoft/Windows/ DriverFrameworks-UserMode/Operational
      3. ‘Applications and Services Logs’/Microsoft/Windows/USB-USBPORT/Operational
      4. ‘Applications and Services Logs’/Microsoft/Windows/ USB-USBXHCI/Operational.
3. LNK Files: as mentioned above it provides shortcuts for recently accessed files, but not only for the C Drive, but for all drives with mount points, these shortcut files can act as evidence as a thief would open the file in the drive to make sure it was copied correctly.
4. USBSTOR.INF: this file is located at C:\Windows\INF and keeps track of installed USB devices, this can provide a history of all connected USB devices.
5. File metadata and timestamps: using correlation, if we see that the file was last accessed a few seconds after the drive was inserted then we can make an argument that the file was copied onto it.
6. Volume shadow copies: if VSS is enabled we can examine shadow copies to recover older versions of the files and determine why they were modified.

**Windows artifacts that i can use to detect if an executable was run**

1. Registry run keys: executables can be added to the registry to run on startup as background services. The keys to search for are as follows:
   1. Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   2. Key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
   3. Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run (for 32-bit applications on a 64-bit system)
2. Windows Security Logs in event viewer:
   1. Starting an executable creates an event in the event viewer with the event ID : 4688 which is used to denote process creation
   2. This event logs info about the process such as parent process, user, command line argos, etc.
3. Shim Cache: is a set of binary files that records information the windows registry, the path to which is: Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

**Windows artifacts that i can use to detect if NAS was connected**

1. Check mapped drives in the registry under:
   1. HKEY\_CURRENT\_USER\Network
   2. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\NetCache
2. Windows Event Logs: look for events related to drive mapping or disconnecting:
   1. Event ID: 4098 (Network Share)
   2. 4103 (Mapped Network Drive)
   3. 4624 (Logon)
   4. Location: ‘Applications and Services Logs’/Microsoft/Windows/…
      1. "NetworkProfile/Operational": Contains network profile change events and information about network connections.
      2. "Wireless Network Assistant/Operational": Focuses on wireless network-related events and diagnostics.
      3. "Microsoft-Windows-WLAN-AutoConfig/Operational": Logs wireless LAN (Wi-Fi) auto-configuration events.
      4. "Microsoft-Windows-Diagnostics-Networking/Operational": Records network diagnostics and connectivity events.
3. Check the registry again for recent mount points at :
   1. HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

**Windows artifacts that I can use to detect if Powershell was used.**

1. Check the windows event viewer at the paths:
   1. ‘Applications and Services Logs’/Microsoft/Windows/Powershell
   2. ‘Applications and Services Logs’ /Microsoft/Windows/PowerShell-DesiredStateConfiguration-FileDownloadManager
   3. OrApplications and Services Logs’ /Windows PowerShell
2. Module and script Locations: PowerShell modules and scripts are often stored in specific directories. Examine these directories, such as:
   1. C:\Program Files\WindowsPowerShell\Modules
   2. C:\Users\<Username>\Documents\WindowsPowerShell\Scripts
3. You can check the history of what commands were run on powershell by pressing the up arrow.

**Windows artifacts that i can use to detect if cloud storage was connected**

1. Registry run keys : cloud services run services on startup to ensure that all files the service is responsible for are synced and downloaded across its services. These services can be viewed by going to the registry paths:
   1. Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   2. Key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
   3. Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run (for 32-bit applications on a 64-bit system)
2. Browser history is another way we can see if the user has accessed any cloud based storage services such as onedrive, gcloud, etc. if the user used a cloud based service such as onedrive for business or g suite for businesses then the admin can see:
   1. what is currently on their drive
   2. What they have uploaded, deleted, downloaded, etc…

**Windows artifacts that i can use to detect if RDP took place**

1. Registry: navigate to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
2. RDP Connection Logs: located at C:\Windows\System32\LogFiles\TerminalServices
3. Windows registry: under the security tab filter for:
   1. 4624 (Successful Logon)
   2. 4625 (Failed Logon)
   3. Under ‘Applications and Services Logs’/Microsoft/Windows/ RemoteDesktopServices-RdpCoreTS **or** RemoteDesktopServices-SessionServices
      1. Event ID 21 (Remote Desktop Services): Indicates that an RDP session has started.
      2. Event ID 22 (Remote Desktop Services): Indicates that an RDP session has ended.
      3. Event ID 1149 (Remote Desktop Services): Records information about an RDP login.