The table below prescribes the criteria utilized in review of the Dominion DS 5.5B voting system. This review is designed to ascertain whether any component contained malicious software of any kind.
User Activity and Malicious Software Review
Installed Programs: This is used to determine if there are any suspicious programs installed on the systems. This could be for malicious software or indications of Internet usage. This could include things like VNC player, or software that was not listed in the Dominion documentation.
Auto-Run commands: This includes software or other objects that are run automatically upon system load. We will be looking for things that might indicate internet activity, including Zoom or other software that may load automatically and require internet connectivity.
Event Logs: This is where a bulk of the examination will be looking for Windows events that will detail external connections or other faults to help identify internet connectivity or malicious software usage or activity.
UserAssist: This is detailed information from the Windows registry, about programs executed on the system including when last used and how many times. This will be used to examine programs executed on the systems. This should help track down potentially malicious executions on the system, as well as potentially find indicators of network connected programs (Webex, Zoom, VNC etc.)
Jump Lists: List of recently opened items including files, folders, websites etc. We will examine these areas to look for indicators of malicious software activities and internet connectivity.
Recycle Bin: Used to determine if there are any deleted files that would indicate malicious software activity or internet connectivity.
USB: This will tell you every USB device connected to the system, to help identify potentially malicious file activity.
FileName Search: A check of filenames, verifying files associated with products, and looking for known malicious files.