Files Written

When executing the file being studied, it wrote to the following files.

- C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\UPnP Device Host\upnphost\udhisapi.dll
  C:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector

Registry Actions

Registry Keys Set

HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\A70D59A1-8EAD-4F40-AAAB-FBFC460800A4\FriendlyName

Process And Service Actions

Processes Terminated

- 2892 - "C:\Program Files (x86)\Common Files\Adobe\Updater6\Adobe_Updater.exe" -doActionAppID=reader9rdr-es_ES
  2948 - C:\Windows\system32\sc.exe start w32time task_started
  2916 - C:\Windows\system32\rundll32.exe dfdts.dll,DfdGetDefaultPolicyAndSMART
  2904 - taskhost.exe SYSTEM
  2112 - taskhost.exe $(Arg0)
  2192 - C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"