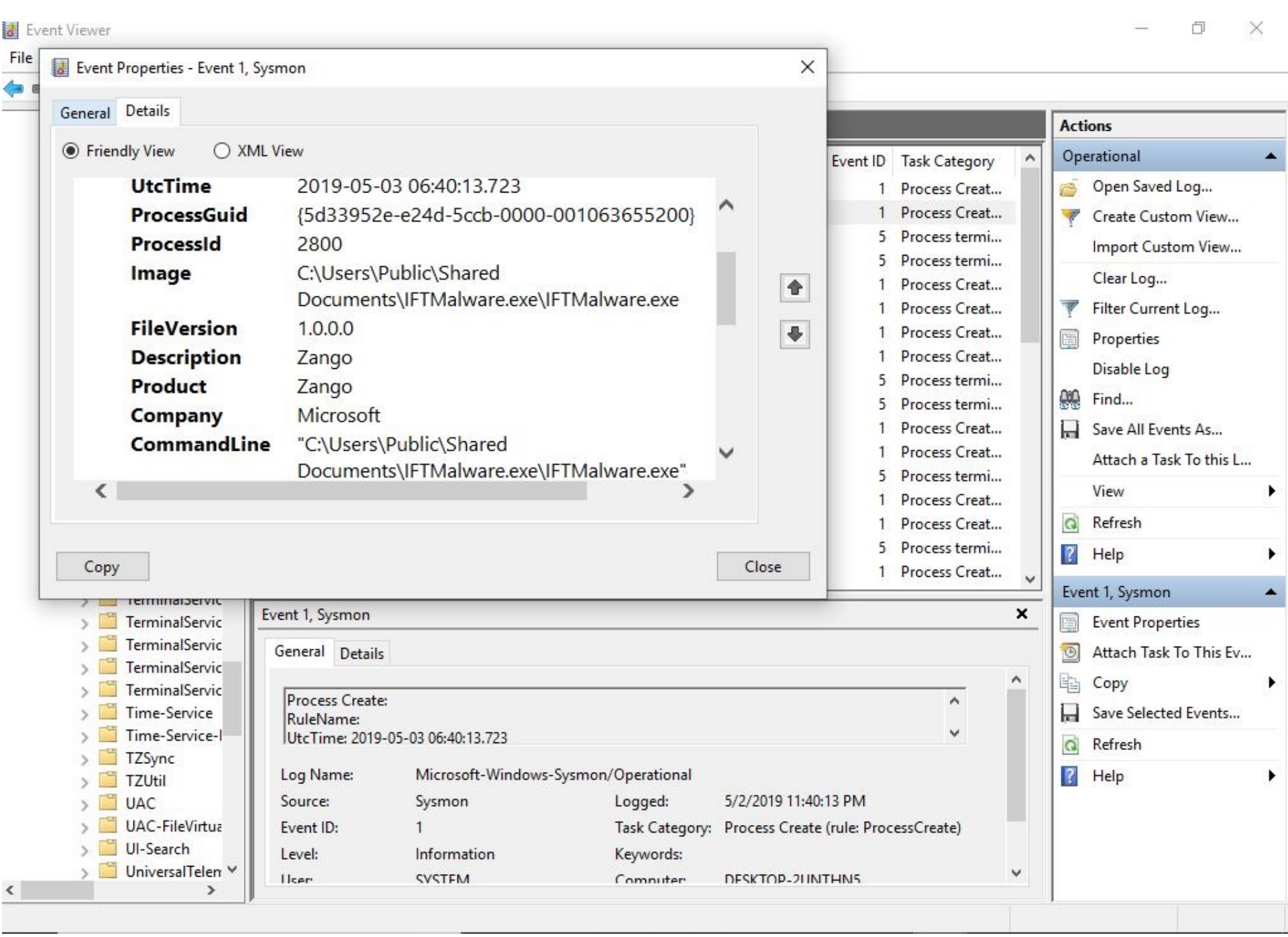
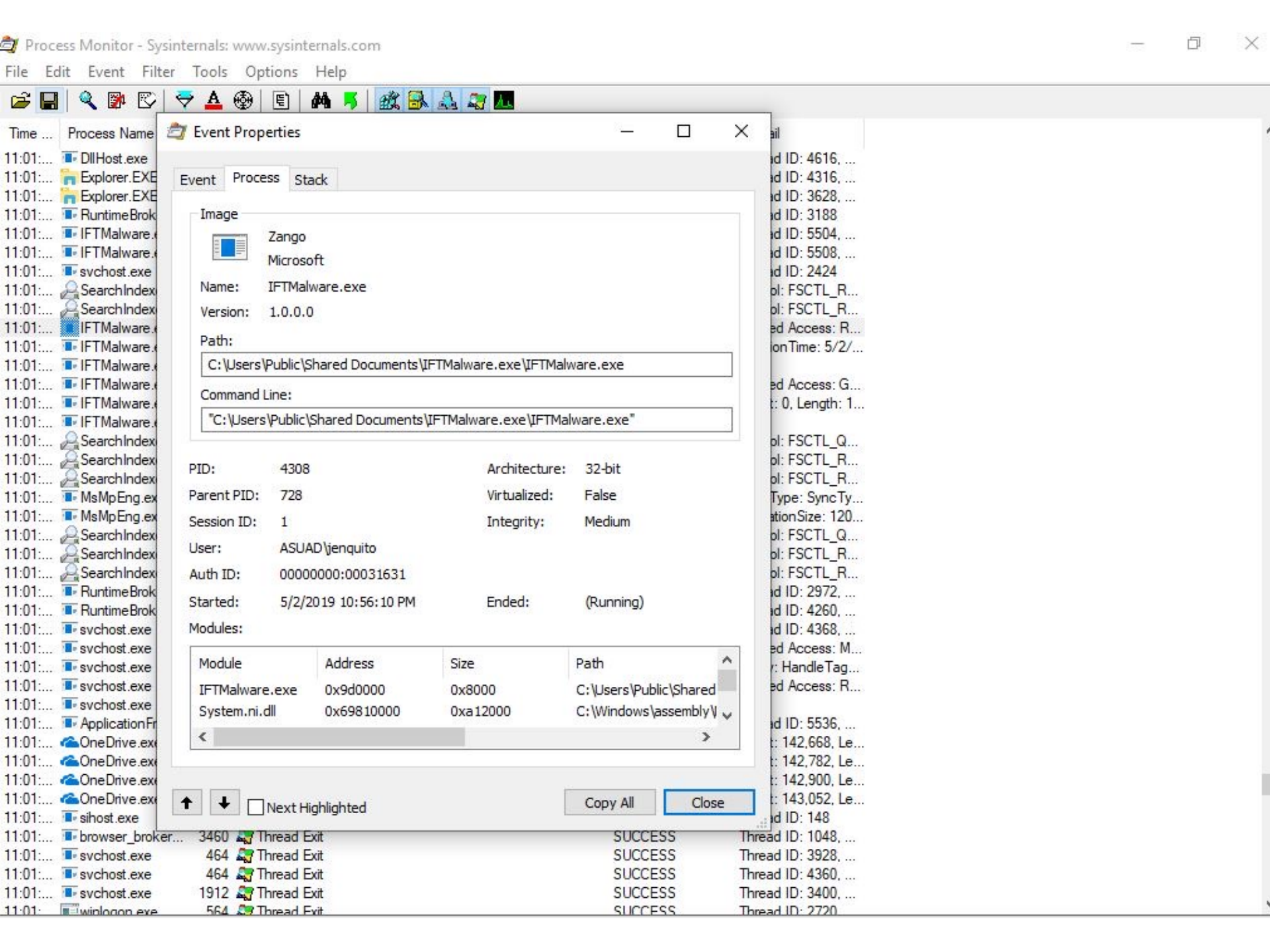
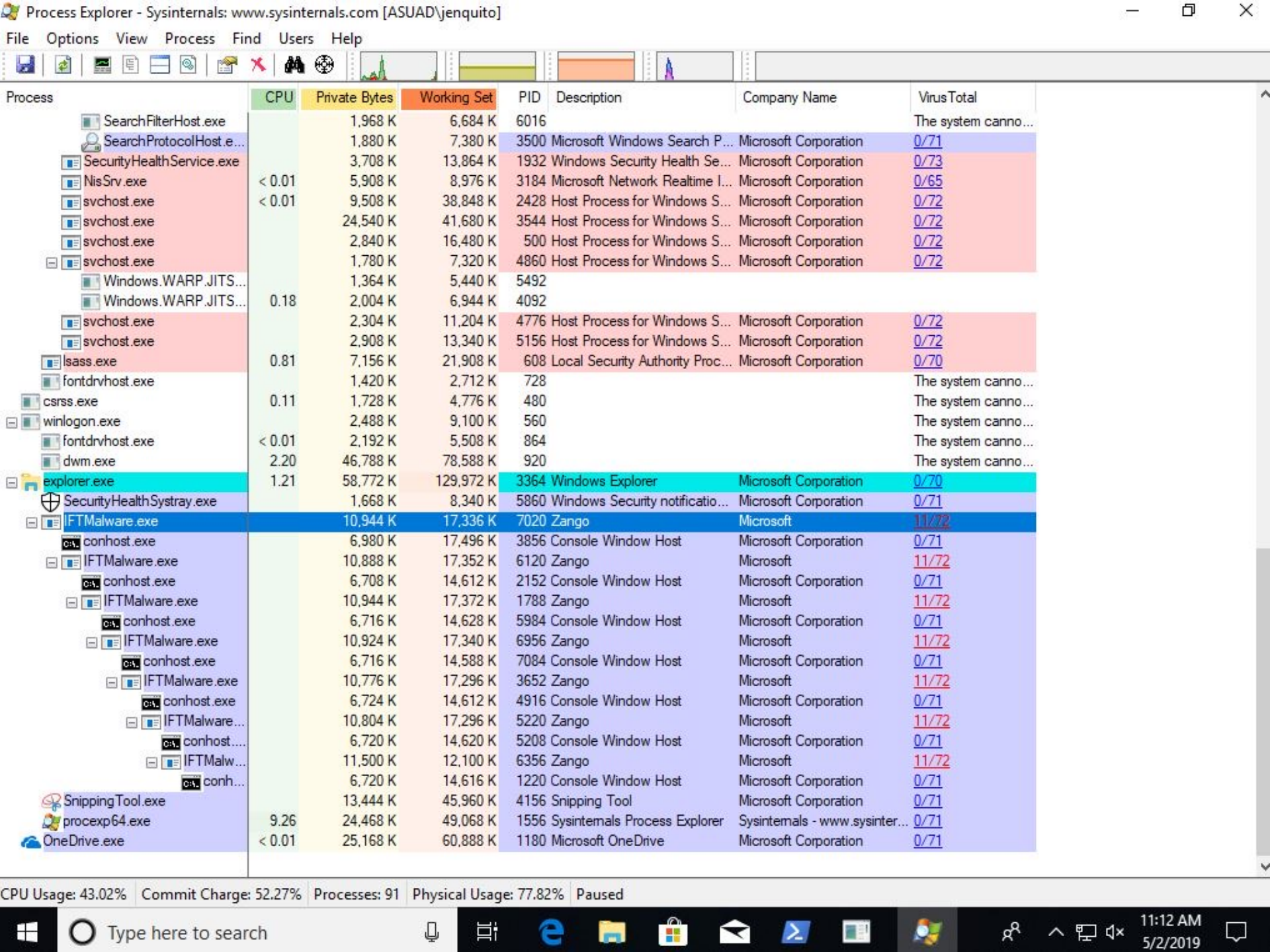
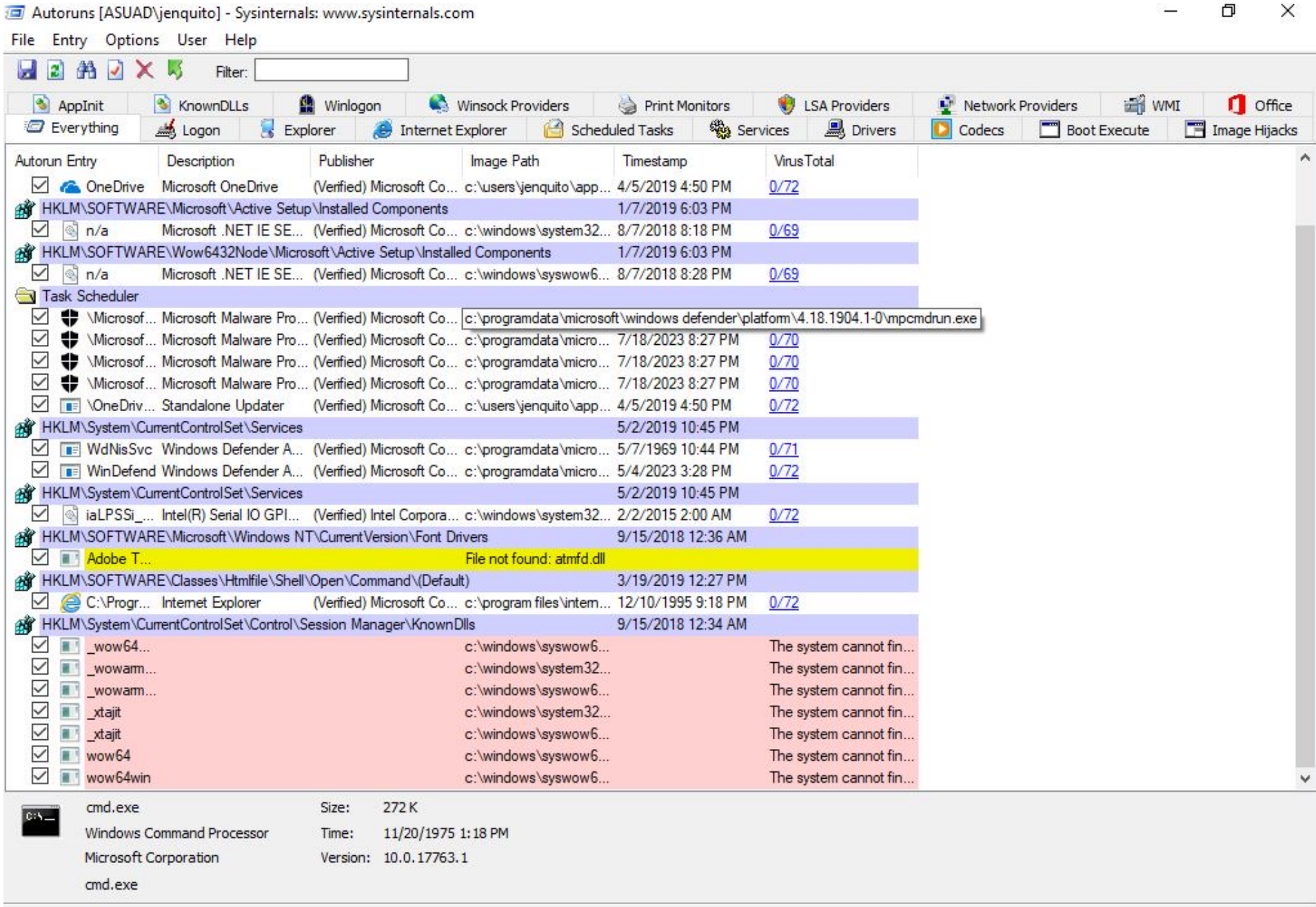

Event Viewer
File
Event Properties - Event 1, Sysmon
General
Details
Friendly View
XML View
UtcTime 2019-05-03 06:40:13.723
ProcessGuid {5d33952e-e24d-5ccb-0000-001063655200}
ProcessId 2800
Image C:\Users\Public\Shared Documents\IFTMalware.exe\IFTMalware.exe
FileVersion 1.0.0.0
Description Zango
Product Zango
Company Microsoft
CommandLine "C:\Users\Public\Shared Documents\IFTMalware.exe\IFTMalware.exe"
Copy
Close
Event ID
Task Category
1 Process Creat...
5 Process termi...
Actions
Operational
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Disable Log
Find...
Save All Events As...
Attach a Task To this L...
View
Refresh
Help
Event 1, Sysmon
Event Properties
Attach Task To This Ev...
Copy
Save Selected Events...
Refresh
Help
TerminalServic
Time-Service
TZSync
TZUtil
UAC
UAC-FileVirtua
UI-Search
UniversalTelen
Process Create:
RuleName:
UtcTime: 2019-05-03 06:40:13.723
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 5/2/2019 11:40:13 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: DESKTOP-2UNTHN5


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name
Event Properties
Event Process Stack
Image
Zango
Microsoft
Name: IFTMalware.exe
Version: 1.0.0.0
Path:
C:\Users\Public\Shared Documents\IFTMalware.exe\IFTMalware.exe
Command Line:
"C:\Users\Public\Shared Documents\IFTMalware.exe\IFTMalware.exe"
PID: 4308
Parent PID: 728
Session ID: 1
User: ASUAD\jenquito
Auth ID: 00000000:00031631
Started: 5/2/2019 10:56:10 PM
Architecture: 32-bit
Virtualized: False
Integrity: Medium
Ended: (Running)
Modules:
Module Address Size Path
IFTMalware.exe 0x9d0000 0x8000 C:\Users\Public\Shared
System.ni.dll 0x69810000 0xa12000 C:\Windows\assembly\
Next Highlighted
Copy All
Close


Process Explorer - Sysinternals: www.sysinternals.com [ASUAD\jenquito]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name VirusTotal
SearchFilterHost.exe 1,968 K 6,684 K 6016 The system canno...
SearchProtocolHost.e... 1,880 K 7,380 K 3500 Microsoft Windows Search P... Microsoft Corporation 0/71
SecurityHealthService.exe 3,708 K 13,864 K 1932 Windows Security Health Se... Microsoft Corporation 0/73
NisSrv.exe < 0.01 5,908 K 8,976 K 3184 Microsoft Network Realtime I... Microsoft Corporation 0/65
svchost.exe < 0.01 9,508 K 38,848 K 2428 Host Process for Windows S... Microsoft Corporation 0/72
svchost.exe 24,540 K 41,680 K 3544 Host Process for Windows S... Microsoft Corporation 0/72
svchost.exe 2,840 K 16,480 K 500 Host Process for Windows S... Microsoft Corporation 0/72
svchost.exe 1,780 K 7,320 K 4860 Host Process for Windows S... Microsoft Corporation 0/72
Windows.WARP.JITS... 1,364 K 5,440 K 5492
Windows.WARP.JITS... 0.18 2,004 K 6,944 K 4092
svchost.exe 2,304 K 11,204 K 4776 Host Process for Windows S... Microsoft Corporation 0/72
svchost.exe 2,908 K 13,340 K 5156 Host Process for Windows S... Microsoft Corporation 0/72
lsass.exe 0.81 7,156 K 21,908 K 608 Local Security Authority Proc... Microsoft Corporation 0/70
fontdrvhost.exe 1,420 K 2,712 K 728 The system canno...
csrss.exe 0.11 1,728 K 4,776 K 480 The system canno...
winlogon.exe 2,488 K 9,100 K 560 The system canno...
fontdrvhost.exe < 0.01 2,192 K 5,508 K 864 The system canno...
dwm.exe 2.20 46,788 K 78,588 K 920 The system canno...
explorer.exe 1.21 58,772 K 129,972 K 3364 Windows Explorer Microsoft Corporation 0/70
SecurityHealthSystray.exe 1,668 K 8,340 K 5860 Windows Security notificatio... Microsoft Corporation 0/71
IFTMalware.exe 10,944 K 17,336 K 7020 Zango Microsoft 11/72
conhost.exe 6,980 K 17,496 K 3856 Console Window Host Microsoft Corporation 0/71
IFTMalware.exe 10,888 K 17,352 K 6120 Zango Microsoft 11/72
conhost.exe 6,708 K 14,612 K 2152 Console Window Host Microsoft Corporation 0/71
IFTMalware.exe 10,944 K 17,372 K 1788 Zango Microsoft 11/72
conhost.exe 6,716 K 14,628 K 5984 Console Window Host Microsoft Corporation 0/71
IFTMalware.exe 10,924 K 17,340 K 6956 Zango Microsoft 11/72
conhost.exe 6,716 K 14,588 K 7084 Console Window Host Microsoft Corporation 0/71
IFTMalware.exe 10,776 K 17,296 K 3652 Zango Microsoft 11/72
conhost.exe 6,724 K 14,612 K 4916 Console Window Host Microsoft Corporation 0/71
IFTMalware... 10,804 K 17,296 K 5220 Zango Microsoft 11/72
conhost.... 6,720 K 14,620 K 5208 Console Window Host Microsoft Corporation 0/71
IFTMalw... 11,500 K 12,100 K 6356 Zango Microsoft 11/72
conh... 6,720 K 14,616 K 1220 Console Window Host Microsoft Corporation 0/71
SnippingTool.exe 13,444 K 45,960 K 4156 Snipping Tool Microsoft Corporation 0/71
procexp64.exe 9.26 24,468 K 49,068 K 1556 Sysinternals Process Explorer Sysinternals - www.sysinter... 0/71
OneDrive.exe < 0.01 25,168 K 60,888 K 1180 Microsoft OneDrive Microsoft Corporation 0/71
CPU Usage: 43.02% Commit Charge: 52.27% Processes: 91 Physical Usage: 77.82% Paused
Type here to search
11:12 AM
5/2/2019


Autoruns [ASUAD\jenquito] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
OneDrive Microsoft OneDrive (Verified) Microsoft Co... c:\users\jenquito\app... 4/5/2019 4:50 PM 0/72
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 1/7/2019 6:03 PM
n/a Microsoft .NET IE SE... (Verified) Microsoft Co... c:\windows\system32... 8/7/2018 8:18 PM 0/69
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 1/7/2019 6:03 PM
n/a Microsoft .NET IE SE... (Verified) Microsoft Co... c:\windows\syswow6... 8/7/2018 8:28 PM 0/69
Task Scheduler
\Microsof... Microsoft Malware Pro... (Verified) Microsoft Co... c:\programdata\microsoft\windows defender\platform\4.18.1904.1-0\mpcmdrun.exe
\Microsof... Microsoft Malware Pro... (Verified) Microsoft Co... c:\programdata\micro... 7/18/2023 8:27 PM 0/70
\Microsof... Microsoft Malware Pro... (Verified) Microsoft Co... c:\programdata\micro... 7/18/2023 8:27 PM 0/70
\Microsof... Microsoft Malware Pro... (Verified) Microsoft Co... c:\programdata\micro... 7/18/2023 8:27 PM 0/70
\OneDriv... Standalone Updater (Verified) Microsoft Co... c:\users\jenquito\app... 4/5/2019 4:50 PM 0/72
HKLM\System\CurrentControlSet\Services 5/2/2019 10:45 PM
WdNisSvc Windows Defender A... (Verified) Microsoft Co... c:\programdata\micro... 5/7/1969 10:44 PM 0/71
WinDefend Windows Defender A... (Verified) Microsoft Co... c:\programdata\micro... 5/4/2023 3:28 PM 0/72
HKLM\System\CurrentControlSet\Services 5/2/2019 10:45 PM
iaLPSSi_... Intel(R) Serial IO GPI... (Verified) Intel Corpora... c:\windows\system32... 2/2/2015 2:00 AM 0/72
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers 9/15/2018 12:36 AM
Adobe T... File not found: atmfd.dll
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default) 3/19/2019 12:27 PM
C:\Progr... Internet Explorer (Verified) Microsoft Co... c:\program files\intern... 12/10/1995 9:18 PM 0/72
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls 9/15/2018 12:34 AM
_wow64... c:\windows\syswow6... The system cannot fin...
_wowarm... c:\windows\system32... The system cannot fin...
_wowarm... c:\windows\syswow6... The system cannot fin...
_xtajit c:\windows\system32... The system cannot fin...
_xtajit c:\windows\syswow6... The system cannot fin...
wow64 c:\windows\syswow6... The system cannot fin...
wow64win c:\windows\syswow6... The system cannot fin...
cmd.exe Size: 272 K
Windows Command Processor Time: 11/20/1975 1:18 PM
Microsoft Corporation Version: 10.0.17763.1
cmd.exe