

Cyber Security Audit Report

Name: KHADER

Lab: AEROSPACE

Audit Timestamp: 2025-04-06 14:10:24

Table of Contents

1. System Information
2. Network Details
3. Security Information
4. Users Accounts
5. Last Windows Update
6. RDP & Remote Services
7. Critical Windows Services
8. Desktop Files
9. USB Device Connection History
10. Installed Programs
11. Startup Applications
12. Shared Folders
13. Unwanted Softwares
14. Logs

This report contains confidential information intended solely for the recipient. Unauthorized use or distribution is prohibited.

CYBER SECURITY AUDIT REPORT

System Information

S.No	Parameter	Value
1	System Serial Number	NHQ7NSI0020431B4673400
2	PC Name	JoeyTheDog
3	OS Name	Microsoft Windows 11 Home Single Language
4	Windows Version	10.0.26100
5	BIOS Version	V1.07
6	Machine Type	64-bit
7	Processor	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
8	Product ID	00327-35907-93161-AAOEM
9	Service Pack Status	No Service Pack Installed
10	OS Configuration	Standalone Workstation
11	Plug and Play Status	Plug and Play Enabled (Manual Start)
12	Windows Directory	C:\WINDOWS
13	System Directory	C:\WINDOWS\system32
14	Clear Desktop Status	Desktop is Cluttered (26 files/folders)
15	OS Install Date	2025-03-30
16	Domain	WORKGROUP
17	System Last Updated On	30 March 2025
18	Windows License Status	Unknown License Status
19	BitLocker Status	BitLocker is Disabled (Drive is not encrypted)
20	Internet Connectivity	Connected
21	Geo-Location Status	Geo-Location Status Unknown (Registry Value: 2)
22	Bluetooth Status	Bluetooth Enabled
23	Local IP Address	192.168.0.191
24	Public IP Address	49.204.17.137
25	CPU Usage	1.4%
26	Memory Usage	80.4%

Network Details

S.No	Parameter	Value
1	MAC Address	8C-8D-28-32-2E-A8
2	Connection Type	Ethernet
3	Active Network Interface	Intel(R) Wi-Fi 6 AX201 160MHz
4	Wi-Fi Interface	Wi-Fi
5	Wi-Fi Status	Wi-Fi is ON
6	Wi-Fi SSID	JoeyDeNw_EXT
7	IP Address	192.168.0.191
8	Network Type	Project Network or Unknown

Security Information

S.No	Parameter	Value
1	Timestamp	2025-04-06 14:10:24
2	Antivirus Installed	Antivirus Installed: Norton Security Ultra, Windows Defender, Norton
3	Windows Firewall Status	Domain Profile: Enabled Private Profile: Enabled Public Profile: Disabled
4	Last Windows Defender Scan Time	01 April 2025 09:22:49
5	USB Storage Device Access	USB Access: Allowed
6	AutoPlay Status	AutoPlay is Enabled
7	Remote Desktop Protocol (RDP)	Disabled (RDP is OFF)
8	Telnet	Not Installed
9	Default Share Status	Enabled (Security Risk)
10	Shared Folder Status	Not Configured (Safe)
11	Passwords not saved in web/system	Passwords Saved (See Credential Manager)
12	BIOS Password	BIOS Password May Be Set (Check BIOS Manually)
13	Windows Login Password	Windows Login Password Set (User: amaan)
14	Password Policy	Partial Password Policy (No password history enforced) Minimum password age (days): 0 ■ Maximum password age (days): 45 ■ Minimum password length: 10 ■ Length of password history maintained: None

15	System Lockout Policy	System Lockout Policy is Configured Lockout Threshold: 10 Lockout Duration (minutes): 10 Lockout Observation Window (minutes): 10
16	Open TCP Ports	Port 49670 (TCP) - Unknown Port 49669 (TCP) - Unknown Port 49666 (TCP) - Unknown Port 445 (TCP) - SMB Port 135 (TCP) - RPC Port 139 (TCP) - NetBIOS Port 49668 (TCP) - Unknown Port 49667 (TCP) - Unknown
17	UDP Services	Port 61058 (UDP) - Unknown - Process IDs: 18372 Port 58580 (UDP) - Unknown - Process IDs: 11932 Port 58579 (UDP) - Unknown - Process IDs: 11932 Port 49669 (UDP) - Unknown - Process IDs: 4672 Port 49487 (UDP) - Unknown - Process IDs: 2268 Port 5353 (UDP) - mDNS - Process IDs: 4672, 2268 Port 1900 (UDP) - UPnP - Process IDs: 11932

Users Accounts

Administrator, amaan, DefaultAccount, Guest, WDAGUtilityAccount

Last Windows Update

- KB5049622 3/29/2025
- KB5053598 3/29/2025
- KB5052915 3/30/2025

RDP & Remote Services Status

Total Services Checked: 10

S.No	Service Name	Status
1	Bluetooth Support Service	Running
2	Geolocation Service	Running
3	Plug and Play	Running
4	HV Host Service	Stopped

5	Remote Desktop Services	Running
6	Remote Procedure Call (RPC)	Running
7	Routing and Remote Access	Running
8	Wi-Fi Direct Services	Stopped
9	Xbox Game Monitoring	Unknown
10	Default Share Status	Running

Critical Windows Services Status

Total Services Checked: 18

S.No	Service Name	Status
1	DNS Client	Running
2	DNS Server	Unknown
3	Geolocation Service	Running
4	Distributed Transaction Coordinator	Running
5	Plug and Play	Running
6	Remote Access Auto Connection Manager	Running
7	Remote Access Connection Manager	Running
8	Routing and Remote Access	Running
9	Remote Registry	Stopped
10	RPC Endpoint Mapper	Running
11	Remote Procedure Call (RPC) Locator	Stopped
12	Remote Procedure Call (RPC)	Running
13	Remote Desktop Configuration	Running
14	Microsoft Storage Spaces SMP	Stopped
15	OpenSSH Authentication Agent	Unknown
16	Remote Desktop Services	Running
17	Problem Reports Control Panel Support	Running
18	Telnet Client	Unknown

Desktop Files

Number of Desktop Files: 26

S.No	File Name
1	.ipynb_checkpoints
2	180168M_032025 (1).pdf
3	26-March-2025-main
4	automation-test-main
5	Code
6	daa.py
7	desktop.ini
8	download.pdf
9	final audit
10	Japan Cover Letter 2024 Amaan img.png

USB Device Connection History

No USB storage devices found.

Installed Programs

Total Installed Programs: 110

S.No	Program Name	Version
1	DriverSetupUtility	1.00.3026
2	Acer Configuration Manager	2.5.22250
3	Acer Jumpstart	3.5.22220.20
4	Adobe Acrobat (64-bit)	25.001.20435
5	Adobe Genuine Service	8.6.0.79
6	Adobe Premiere Pro 2024	24.2.1
7	Anaconda3 2024.02-1 (Python 3.11.7 64-bit)	2024.02-1
8	App Explorer	0.273.4.917
9	Care Center Service	4.00.3042
10	Dynamic Application Loader Host Interface Service	1.0.0.0
11	GoTrust ID Plugin 2.0.10.26	2.0.10.26
12	Google Chrome	135.0.7049.41
13	Intel(R) Chipset Device Software	10.1.18263.8193

14	Intel(R) Chipset Device Software	10.1.18263.8193
15	Intel(R) Icls	1.0.0.0
16	Intel(R) LMS	1.0.0.0
17	Intel(R) Management Engine Components	2004.14.0.1447
18	Intel(R) Management Engine Components	1.0.0.0
19	Intel(R) Management Engine Components	1.0.0.0
20	Intel(R) Management Engine Driver	1.0.0.0
21	Java 8 Update 411 (64-bit)	8.0.4110.9
22	Java Auto Updater	2.8.411.9
23	Killer Ethernet Performance Driver Suite UWD	2.2.1410
24	McAfee Security Scan Plus	4.2.707.1
25	Microsoft 365 - en-us	16.0.18623.20156
26	Microsoft Edge	135.0.3179.54
27	Microsoft Edge WebView2 Runtime	134.0.3124.93
28	Microsoft GameInput	10.1.22621.3036
29	Microsoft OneDrive	25.046.0310.0005
30	Microsoft Teams Meeting Add-in for Microsoft Office	1.24.14501
31	Microsoft Update Health Tools	5.72.0.0
32	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40664	12.0.40664.0
33	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40664	12.0.40664.0
34	Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664	12.0.40664
35	Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40664	12.0.40664
36	Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40664	12.0.40664
37	Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40664	12.0.40664
38	Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31326	14.32.31326.0
39	Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.32.31326	14.32.31326.0
40	Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31326	14.32.31326
41	Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31326	14.32.31326
42	Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31326	14.32.31326
43	Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31326	14.32.31326
44	Microsoft Visual Studio Code (User)	1.99.0
45	Mozilla Firefox 75.0 (x64 en-US)	75.0
46	Mozilla Maintenance Service	75.0
47	NVIDIA Backend	39.5.0.0
48	NVIDIA Container	1.40

49	NVIDIA FrameView SDK 1.3.8513.32290073	1.3.8513.32290073
50	NVIDIA GPX Common OSS binaries (POCO, OpenSSL, libprotobuf 7.1	7.1
51	NVIDIA GeForce Experience 3.28.0.417	3.28.0.417
52	NVIDIA Graphics Driver 565.90	565.90
53	NVIDIA HD Audio Driver 1.4.2.6	1.4.2.6
54	NVIDIA Install Application	2.1002.422.0
55	NVIDIA LocalSystem Container	1.40
56	NVIDIA Message Bus for NvContainer	1.34
57	NVIDIA NVAPI Monitor plugin for NvContainer	1.0
58	NVIDIA NetworkService Container	1.40
59	NVIDIA NodeJS	3.28.0.417
60	NVIDIA NvModuleTracker	6.14.26040.64835
61	NVIDIA Optimus Update 39.5.0.0	39.5.0.0
62	NVIDIA PhysX System Software 9.23.1019	9.23.1019
63	NVIDIA SHIELD Streaming	7.1.33903191
64	NVIDIA SHIELD Wireless Controller Driver	3.20.3.58
65	NVIDIA Session Container	1.40
66	NVIDIA ShadowPlay 3.28.0.417	3.28.0.417
67	NVIDIA Telemetry Client	18.1.13.0
68	NVIDIA TelemetryApi helper for NvContainer	1.40
69	NVIDIA Update 39.5.0.0	39.5.0.0
70	NVIDIA Update Core	39.5.0.0
71	NVIDIA User Container	1.40
72	NVIDIA Virtual Audio 4.65.0.3	4.65.0.3
73	NVIDIA Virtual Host Controller	3.05.0.1
74	NVIDIA Watchdog Plugin for NvContainer	1.40
75	NitroSense Service	3.01.3016
76	Norton Security Ultra	22.24.8.36
77	Nvidia Share	3.28.0.417
78	Office 16 Click-to-Run Extensibility Component	16.0.18623.20156
79	Office 16 Click-to-Run Licensing Component	16.0.18623.20156
80	Office 16 Click-to-Run Localization Component	16.0.12527.20482
81	PyCharm Community Edition 2023.3.3	233.13763.11
82	Python 3.12.3 (64-bit)	3.12.3150.0
83	Python 3.12.3 Add to Path (64-bit)	3.12.3150.0

84	Python 3.12.3 Core Interpreter (64-bit debug)	3.12.3150.0
85	Python 3.12.3 Core Interpreter (64-bit symbols)	3.12.3150.0
86	Python 3.12.3 Core Interpreter (64-bit)	3.12.3150.0
87	Python 3.12.3 Development Libraries (64-bit debug)	3.12.3150.0
88	Python 3.12.3 Development Libraries (64-bit)	3.12.3150.0
89	Python 3.12.3 Documentation (64-bit)	3.12.3150.0
90	Python 3.12.3 Executables (64-bit debug)	3.12.3150.0
91	Python 3.12.3 Executables (64-bit symbols)	3.12.3150.0
92	Python 3.12.3 Executables (64-bit)	3.12.3150.0
93	Python 3.12.3 Standard Library (64-bit debug)	3.12.3150.0
94	Python 3.12.3 Standard Library (64-bit symbols)	3.12.3150.0
95	Python 3.12.3 Standard Library (64-bit)	3.12.3150.0
96	Python 3.12.3 Tcl/Tk Support (64-bit debug)	3.12.3150.0
97	Python 3.12.3 Tcl/Tk Support (64-bit symbols)	3.12.3150.0
98	Python 3.12.3 Tcl/Tk Support (64-bit)	3.12.3150.0
99	Python 3.12.3 Test Suite (64-bit debug)	3.12.3150.0
100	Python 3.12.3 Test Suite (64-bit symbols)	3.12.3150.0
101	Python 3.12.3 Test Suite (64-bit)	3.12.3150.0
102	Python 3.12.3 pip Bootstrap (64-bit)	3.12.3150.0
103	Python Launcher	3.12.1150.0
104	Quick Access Service	3.00.3038
105	Realtek Audio Driver	6.0.8981.1
106	Rocket League	Unknown Version
107	Steam	2.10.91.91
108	Telegram Desktop	5.12.3
109	User Experience Improvement Program Service	4.00.3114
110	WinRAR 7.01 (64-bit)	7.01.0

Startup Applications

Total Startup Applications: 393

S.No	Application Name	Path	Source
1	AdobeGCInvoker-1.0	"C:\Program Files (x86)\Common Files\Adobe\AdobeGCCClient\AGCInvokerUtility.exe"	Registry

2	MicrosoftEdgeAutoLaunch_75 EEE27B96CB44DF3D365E0D 42034901	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start	Registry
3	OneDrive	"C:\Users\amaan\AppData\Local\Microsoft\OneDrive\ OneDrive.exe" /background	Registry
4	RtkAudUService	"C:\WINDOWS\System32\DriverStore\FileRepository\ realtekservice.inf_amd64_9971779a1c712866\RtkAu dUService64.exe" -background	Registry
5	SecurityHealth	%windir%\system32\SecurityHealthSystray.exe	Registry
6	Steam	"C:\Program Files (x86)\Steam\steam.exe" -silent	Registry
7	\ACCAgent	C:\Program Files (x86)\Acer\Care Center\LiveUpdateChecker.exe -auto	Task Scheduler
8	\ACCBBackgroundApplication	C:\Program Files (x86)\Acer\Care Center\LiveUpdateAgent.exe	Task Scheduler
9	\AcerCMUpdateTask2.5.22250	C:\Program Files (x86)\Acer\Care Center\ACCStd.exe	Task Scheduler
10	\AcerCMUpdateTask2.5.22250	"C:\Program Files (x86)\Acer\Amundsen\2.5.22250\awc.exe" /task	Task Scheduler
11	\AcerCMUpdateTask2.5.22250	"C:\Program Files (x86)\Acer\Amundsen\2.5.22250\awc.exe" /task	Task Scheduler
12	\Adobe Acrobat Update Task	"C:\Program Files (x86)\Acer\Amundsen\2.5.22250\awc.exe" /task	Task Scheduler
13	\Adobe Acrobat Update Task	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	Task Scheduler
14	\Adobe-Genuine-Software-Inte grity-Scheduler-1.0	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	Task Scheduler
15	\AdobeGCInvoker-1.0	C:\Program Files (x86)\Common Files\Adobe\AdobeGCCClient\AGSService.exe	Task Scheduler
16	\App Explorer	C:\Program Files (x86)\Common Files\Adobe\AdobeGCCClient\AGCInvokerUtility.exe -mode=scheduled	Task Scheduler
17	\GoTrust ID Driver	%LOCALAPPDATA%\Host App Service\Engine\HostAppServiceUpdater.exe /LOGON	Task Scheduler
18	\GoTrust ID Driver	C:\Program Files\GoTrust ID Plugin\Resource\GO-Trust_ID_Driver.exe	Task Scheduler
19	\GoTrust ID Driver	C:\Program Files\GoTrust ID Plugin\Resource\GO-Trust_ID_Driver.exe	Task Scheduler
20	\GoogleSystem\GoogleUpdate r\GoogleUpdaterTaskSystem1 36.0.7079.0{90C7907D-593C- 443B-A1D6-B218A0FF8D6E}	"C:\Program Files\Acer\User Experience Improvement Program Service\Framework\UEIPOOBECheck.exe"	Task Scheduler

21	\GoogleSystem\GoogleUpdate r\GoogleUpdaterTaskSystem1 36.0.7079.0{90C7907D-593C- 443B-A1D6-B218A0FF8D6E}	"C:\Program Files (x86)\Google\GoogleUpdater\136.0 .7079.0\updater.exe" --wake --system	Task Scheduler
22	\McUpdaterModuleTask	C:\Program Files\GoTrust ID Plugin\Resource\GO-Trust_ID_Driver.exe	Task Scheduler
23	\MicrosoftEdgeUpdateTaskMa chineCore	C:\Program Files (x86)\McAfee Security Scan\4.2.707\McUpdaterModule.exe	Task Scheduler
24	\MicrosoftEdgeUpdateTaskMa chineCore	C:\Program Files (x86)\Microsoft\EdgeUpdate\Micros oftEdgeUpdate.exe /c	Task Scheduler
25	\MicrosoftEdgeUpdateTaskMa chineUA	C:\Program Files (x86)\Microsoft\EdgeUpdate\Micros oftEdgeUpdate.exe /c	Task Scheduler
26	\Microsoft\Office\Office Apps Prewarm	"C:\Program Files (x86)\Google\GoogleUpdater\136.0 .7079.0\updater.exe" --wake --system	Task Scheduler
27	\Microsoft\Office\Office Apps Prewarm Recurring	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe /prewarm	Task Scheduler
28	\Microsoft\Office\Office Automatic Updates 2.0	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe /prewarm	Task Scheduler
29	\Microsoft\Office\Office Automatic Updates 2.0	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe /frequentupdate SCHEDULEDTASK displaylevel=False	Task Scheduler
30	\Microsoft\Office\Office Automatic Updates 2.0	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe /frequentupdate SCHEDULEDTASK displaylevel=False	Task Scheduler
31	\Microsoft\Office\Office ClickToRun Service Monitor	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe /frequentupdate SCHEDULEDTASK displaylevel=False	Task Scheduler
32	\Microsoft\Office\Office Feature Updates	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe /WatchService	Task Scheduler
33	\Microsoft\Office\Office Feature Updates	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Task Scheduler
34	\Microsoft\Office\Office Feature Updates	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Task Scheduler
35	\Microsoft\Office\Office Feature Updates	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Task Scheduler
36	\Microsoft\Office\Office Feature Updates	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Task Scheduler
37	\Microsoft\Office\Office Feature Updates	C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe	Task Scheduler

38	\\Microsoft\\Office\\Office Feature Updates Logon	C:\\Program Files\\Microsoft Office\\root\\Office16\\sdxhelper.exe	Task Scheduler
39	\\Microsoft\\Office\\Office Feature Updates Logon	C:\\Program Files\\Microsoft Office\\root\\Office16\\sdxhelper.exe /onlogon	Task Scheduler
40	\\Microsoft\\Office\\Office Performance Monitor	C:\\Program Files\\Microsoft Office\\root\\Office16\\sdxhelper.exe /onlogon	Task Scheduler
41	\\Microsoft\\Windows\\.NET Framework\\.NET Framework NGEN v4.0.30319	C:\\Program Files\\Microsoft Office\\root\\VFS\\ProgramFilesCommonX64\\Microsoft Shared\\Office16\\operfmon.exe	Task Scheduler
42	\\Microsoft\\Windows\\.NET Framework\\.NET Framework NGEN v4.0.30319 64	COM handler	Task Scheduler
43	\\Microsoft\\Windows\\.NET Framework\\.NET Framework NGEN v4.0.30319 64 Critical	COM handler	Task Scheduler
44	\\Microsoft\\Windows\\.NET Framework\\.NET Framework NGEN v4.0.30319 Critical	COM handler	Task Scheduler
45	\\Microsoft\\Windows\\Active Directory Rights Management Services Client\\AD RMS Rights Policy Template Management (Automated)	COM handler	Task Scheduler
46	\\Microsoft\\Windows\\Active Directory Rights Management Services Client\\AD RMS Rights Policy Template Management (Automated)	COM handler	Task Scheduler
47	\\Microsoft\\Windows\\Active Directory Rights Management Services Client\\AD RMS Rights Policy Template Management (Manual)	COM handler	Task Scheduler
48	\\Microsoft\\Windows\\AppID\\EDP Policy Manager	COM handler	Task Scheduler
49	\\Microsoft\\Windows\\AppID\\EDP Policy Manager	COM handler	Task Scheduler
50	\\Microsoft\\Windows\\AppID\\PolicyConverter	COM handler	Task Scheduler
51	\\Microsoft\\Windows\\AppID\\VerifiedPublisherCertStoreCheck	%windir%\\system32\\appidpolicyconverter.exe	Task Scheduler
52	\\Microsoft\\Windows\\AppListBackup\\Backup	%windir%\\system32\\dstokenclean.exe	Task Scheduler
53	\\Microsoft\\Windows\\AppListBackup\\BackupNonMaintenance	COM handler	Task Scheduler

54	\Microsoft\Windows\Application Experience\MareBackup	%windir%\system32\appidcertstorecheck.exe	Task Scheduler
55	\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser	Multiple actions	Task Scheduler
56	\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser Exp	%windir%\system32\sc.exe start InventorySvc	Task Scheduler
57	\Microsoft\Windows\Application Experience\PcaPatchDbTask	%windir%\system32\compattelrunner.exe -m:appraiser.dll -f:DoScheduledTelemetryRun express	Task Scheduler
58	\Microsoft\Windows\Application Experience\SdbinstMergeDb Task	%windir%\system32\rundll32.exe %windir%\system32\PcaSvc.dll,PcaPatchSdbTask	Task Scheduler
59	\Microsoft\Windows\Application Experience\SdbinstMergeDb Task	%windir%\system32\sdbinst.exe -mm	Task Scheduler
60	\Microsoft\Windows\Application Experience\StartupAppTask	%windir%\system32\sdbinst.exe -mm	Task Scheduler
61	\Microsoft\Windows\Application Data\CleanupTemporaryState	%windir%\system32\AppHostRegistrationVerifier.exe	Task Scheduler
62	\Microsoft\Windows\Application Data\DsSvcCleanup	%windir%\system32\rundll32.exe Windows.Storage.ApplicationData.dll,CleanupTemporaryState	Task Scheduler
63	\Microsoft\Windows\Application Data\appuriverifierdaily	%windir%\system32\rundll32.exe Startupscan.dll,SusRunTask	Task Scheduler
64	\Microsoft\Windows\Application Data\appuriverifierinstall	%windir%\system32\AppHostRegistrationVerifier.exe	Task Scheduler
65	\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup	COM handler	Task Scheduler
66	\Microsoft\Windows\AppxDeploymentClient\UCPD velocity	%windir%\system32\rundll32.exe %windir%\system32\AppxDeploymentClient.dll,AppxPreStageCleanupRunTask	Task Scheduler
67	\Microsoft\Windows\Autochk\Proxy	%windir%\system32\UCPDMgr.exe	Task Scheduler
68	\Microsoft\Windows\BitLocker\BitLocker Encrypt All Drives	%windir%\system32\rundll32.exe /d acproxy.dll,PerformAutochkOperations	Task Scheduler
69	\Microsoft\Windows\BitLocker\BitLocker MDM policy Refresh	COM handler	Task Scheduler
70	\Microsoft\Windows\Bluetooth\UninstallDeviceTask	COM handler	Task Scheduler

71	\\Microsoft\\Windows\\Broker\\Infrastructure\\BgTaskRegistrationMaintenanceTask	BthUdTask.exe \$(Arg0)	Task Scheduler
72	\\Microsoft\\Windows\\CertificateServicesClient\\AikCertEnrollTask	%windir%\\system32\\rundll32.exe %windir%\\system32\\CapabilityAccessManager.dll,CapabilityAccessManagerDoStoreMaintenance	Task Scheduler
73	\\Microsoft\\Windows\\CertificateServicesClient\\AikCertEnrollTask	COM handler	Task Scheduler
74	\\Microsoft\\Windows\\CertificateServicesClient\\CryptoPolicyTask	COM handler	Task Scheduler
75	\\Microsoft\\Windows\\CertificateServicesClient\\KeyPreGenTask	COM handler	Task Scheduler
76	\\Microsoft\\Windows\\CertificateServicesClient\\KeyPreGenTask	COM handler	Task Scheduler
77	\\Microsoft\\Windows\\CertificateServicesClient\\KeyPreGenTask	COM handler	Task Scheduler
78	\\Microsoft\\Windows\\CertificateServicesClient\\KeyPreGenTask	COM handler	Task Scheduler
79	\\Microsoft\\Windows\\CertificateServicesClient\\KeyPreGenTask	COM handler	Task Scheduler
80	\\Microsoft\\Windows\\CertificateServicesClient\\SystemTask	COM handler	Task Scheduler
81	\\Microsoft\\Windows\\CertificateServicesClient\\SystemTask	COM handler	Task Scheduler
82	\\Microsoft\\Windows\\CertificateServicesClient\\SystemTask	COM handler	Task Scheduler
83	\\Microsoft\\Windows\\CertificateServicesClient\\UserTask	COM handler	Task Scheduler
84	\\Microsoft\\Windows\\CertificateServicesClient\\UserTask	COM handler	Task Scheduler
85	\\Microsoft\\Windows\\CertificateServicesClient\\UserTask	COM handler	Task Scheduler
86	\\Microsoft\\Windows\\CertificateServicesClient\\UserTask	COM handler	Task Scheduler
87	\\Microsoft\\Windows\\CertificateServicesClient\\UserTask-Roam	COM handler	Task Scheduler

88	\\Microsoft\\Windows\\Certificate ServicesClient\\UserTask-Roam	COM handler	Task Scheduler
89	\\Microsoft\\Windows\\Chkdsk\\ProactiveScan	COM handler	Task Scheduler
90	\\Microsoft\\Windows\\Chkdsk\\SyspartRepair	COM handler	Task Scheduler
91	\\Microsoft\\Windows\\Clip\\License Validation	%windir%\\system32\\bcdboot.exe %windir% /sysrepair	Task Scheduler
92	\\Microsoft\\Windows\\CloudExperienceHost\\CreateObjectTask	%SystemRoot%\\system32\\ClipUp.exe -p -s -o	Task Scheduler
93	\\Microsoft\\Windows\\CloudRestore\\Backup	COM handler	Task Scheduler
94	\\Microsoft\\Windows\\CloudRestore\\Backup	COM handler	Task Scheduler
95	\\Microsoft\\Windows\\CloudRestore\\Restore	COM handler	Task Scheduler
96	\\Microsoft\\Windows\\ConsentUX\\UnifiedConsent\\UnifiedConsentSyncTask	COM handler	Task Scheduler
97	\\Microsoft\\Windows\\ConsentUX\\UnifiedConsent\\UnifiedConsentSyncTask	COM handler	Task Scheduler
98	\\Microsoft\\Windows\\Customer Experience Improvement Program\\Consolidator	COM handler	Task Scheduler
99	\\Microsoft\\Windows\\Customer Experience Improvement Program\\UsbCeip	%SystemRoot%\\System32\\wsqmcons.exe	Task Scheduler
100	\\Microsoft\\Windows\\DUSM\\dusmtask	COM handler	Task Scheduler
101	\\Microsoft\\Windows\\Data Integrity Scan\\Data Integrity Check And Scan	COM handler	Task Scheduler
102	\\Microsoft\\Windows\\Data Integrity Scan\\Data Integrity Check And Scan	COM handler	Task Scheduler
103	\\Microsoft\\Windows\\Data Integrity Scan\\Data Integrity Scan	COM handler	Task Scheduler
104	\\Microsoft\\Windows\\Data Integrity Scan\\Data Integrity Scan for Crash Recovery	COM handler	Task Scheduler

105	\Microsoft\Windows\Defrag\ScheduledDefrag	COM handler	Task Scheduler
106	\Microsoft\Windows\Device Information\Device	%windir%\system32\defrag.exe -c -h -o -\$	Task Scheduler
107	\Microsoft\Windows\Device Information\Device	%windir%\system32\devicecensus.exe SystemCxt	Task Scheduler
108	\Microsoft\Windows\Device Information\Device User	%windir%\system32\devicecensus.exe SystemCxt	Task Scheduler
109	\Microsoft\Windows\Device Setup\Metadata Refresh	%windir%\system32\devicecensus.exe UserCxt	Task Scheduler
110	\Microsoft\Windows\Device DirectoryClient\HandleCommand	COM handler	Task Scheduler
111	\Microsoft\Windows\Device DirectoryClient\HandleWnsCommand	COM handler	Task Scheduler
112	\Microsoft\Windows\Device DirectoryClient\IntegrityCheck	COM handler	Task Scheduler
113	\Microsoft\Windows\Device DirectoryClient\LocateCommand UserSession	COM handler	Task Scheduler
114	\Microsoft\Windows\Device DirectoryClient\RegisterDeviceAccountChange	COM handler	Task Scheduler
115	\Microsoft\Windows\Device DirectoryClient\RegisterDeviceAccountChange	COM handler	Task Scheduler
116	\Microsoft\Windows\Device DirectoryClient\RegisterDeviceLocationRightsChange	COM handler	Task Scheduler
117	\Microsoft\Windows\Device DirectoryClient\RegisterDevicePeriodic24	COM handler	Task Scheduler
118	\Microsoft\Windows\Device DirectoryClient\RegisterDevicePolicyChange	COM handler	Task Scheduler
119	\Microsoft\Windows\Device DirectoryClient\RegisterDevicePolicyChange	COM handler	Task Scheduler
120	\Microsoft\Windows\Device DirectoryClient\RegisterDeviceProtectionStateChanged	COM handler	Task Scheduler
121	\Microsoft\Windows\Device DirectoryClient\RegisterDeviceSettingChange	COM handler	Task Scheduler

122	\\Microsoft\\Windows\\DeviceDir ectoryClient\\RegisterDeviceSe ttingChange	COM handler	Task Scheduler
123	\\Microsoft\\Windows\\DeviceDir ectoryClient\\RegisterDeviceW nsFallback	COM handler	Task Scheduler
124	\\Microsoft\\Windows\\DeviceDir ectoryClient\\RegisterUserDevi ce	COM handler	Task Scheduler
125	\\Microsoft\\Windows\\DeviceDir ectoryClient\\RegisterUserDevi ce	COM handler	Task Scheduler
126	\\Microsoft\\Windows\\DeviceDir ectoryClient\\RegisterUserDevi ce	COM handler	Task Scheduler
127	\\Microsoft\\Windows\\Diagnosis\\ RecommendedTroubleshootin gScanner	COM handler	Task Scheduler
128	\\Microsoft\\Windows\\Diagnosis\\ RecommendedTroubleshootin gScanner	COM handler	Task Scheduler
129	\\Microsoft\\Windows\\Diagnosis\\ RecommendedTroubleshootin gScanner	COM handler	Task Scheduler
130	\\Microsoft\\Windows\\Diagnosis\\ RecommendedTroubleshootin gScanner	COM handler	Task Scheduler
131	\\Microsoft\\Windows\\Diagnosis\\ Scheduled	COM handler	Task Scheduler
132	\\Microsoft\\Windows\\Diagnosis\\ UnexpectedCodepath	COM handler	Task Scheduler
133	\\Microsoft\\Windows\\DirectX\\D XGIAdapterCache	%windir%\\system32\\directxdatabaseupdater.exe	Task Scheduler
134	\\Microsoft\\Windows\\DirectX\\D XGIAdapterCache	%windir%\\system32\\dxgiadaptercache.exe	Task Scheduler
135	\\Microsoft\\Windows\\DirectX\\D XGIAdapterCache	%windir%\\system32\\dxgiadaptercache.exe	Task Scheduler
136	\\Microsoft\\Windows\\DirectX\\Dir ectXDatabaseUpdater	%windir%\\system32\\UCConfigTask.exe	Task Scheduler
137	\\Microsoft\\Windows\\DirectX\\Dir ectXDatabaseUpdater	%windir%\\system32\\directxdatabaseupdater.exe	Task Scheduler
138	\\Microsoft\\Windows\\DiskClean up\\SilentCleanup	%windir%\\system32\\dxgiadaptercache.exe	Task Scheduler

139	\\Microsoft\\Windows\\DiskDiagnostic\\Microsoft-Windows-DiskDiagnosticDataCollector	%windir%\\system32\\cleanmgr.exe /autocleanstoragesense /d %systemdrive%	Task Scheduler
140	\\Microsoft\\Windows\\DiskDiagnostic\\Microsoft-Windows-DiskDiagnosticResolver	%windir%\\system32\\rundll32.exe dfdts.dll,DfdGetDefaultPolicyAndSMART	Task Scheduler
141	\\Microsoft\\Windows\\DiskFootprint\\Diagnostics	%windir%\\system32\\DFDWiz.exe	Task Scheduler
142	\\Microsoft\\Windows\\DiskFootprint\\StorageSense	%windir%\\system32\\disksnapshot.exe -z	Task Scheduler
143	\\Microsoft\\Windows\\EDP\\EDP App Launch Task	%SystemRoot%\\System32\\dusmtask.exe	Task Scheduler
144	\\Microsoft\\Windows\\EDP\\EDP Auth Task	COM handler	Task Scheduler
145	\\Microsoft\\Windows\\EDP\\EDP Inaccessible Credentials Task	COM handler	Task Scheduler
146	\\Microsoft\\Windows\\EDP\\StorageCardEncryption Task	COM handler	Task Scheduler
147	\\Microsoft\\Windows\\Enterprise Mgmt\\MDMMaintenanceTask	COM handler	Task Scheduler
148	\\Microsoft\\Windows\\ExploitGuard\\ExploitGuard MDM policy Refresh	%windir%\\system32\\MDMAgent.exe	Task Scheduler
149	\\Microsoft\\Windows\\ExploitGuard\\ExploitGuard MDM policy Refresh	COM handler	Task Scheduler
150	\\Microsoft\\Windows\\ExploitGuard\\ExploitGuard MDM policy Refresh	COM handler	Task Scheduler
151	\\Microsoft\\Windows\\Feedback\\Siuf\\DmClient	COM handler	Task Scheduler
152	\\Microsoft\\Windows\\Feedback\\Siuf\\DmClientOnScenarioDownload	%windir%\\system32\\dmclient.exe	Task Scheduler
153	\\Microsoft\\Windows\\FileHistory\\File History (maintenance mode)	%windir%\\system32\\dmclient.exe utcwnf	Task Scheduler
154	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\BootstrapUsage DataReporting	COM handler	Task Scheduler
155	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileConfigs	COM handler	Task Scheduler

156	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
157	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
158	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
159	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
160	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
161	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
162	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataFlushing	COM handler	Task Scheduler
163	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataFlushing	COM handler	Task Scheduler
164	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataFlushing	COM handler	Task Scheduler
165	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataReceiver	COM handler	Task Scheduler
166	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataReporting	COM handler	Task Scheduler
167	\\Microsoft\\Windows\\Flighting\\OneSettings\\RefreshCache	COM handler	Task Scheduler
168	\\Microsoft\\Windows\\Flighting\\OneSettings\\RefreshCache	COM handler	Task Scheduler
169	\\Microsoft\\Windows\\Flighting\\OneSettings\\RefreshCache	COM handler	Task Scheduler
170	\\Microsoft\\Windows\\HelloFace\\FODCleanupTask	COM handler	Task Scheduler
171	\\Microsoft\\Windows\\InstallService\\RestoreDevice	COM handler	Task Scheduler

172	\\Microsoft\\Windows\\InstallService\\ScanForUpdates	COM handler	Task Scheduler
173	\\Microsoft\\Windows\\InstallService\\ScanForUpdates	COM handler	Task Scheduler
174	\\Microsoft\\Windows\\InstallService\\ScanForUpdates	COM handler	Task Scheduler
175	\\Microsoft\\Windows\\InstallService\\ScanForUpdatesAsUser	COM handler	Task Scheduler
176	\\Microsoft\\Windows\\InstallService\\SmartRetry	COM handler	Task Scheduler
177	\\Microsoft\\Windows\\InstallService\\SmartRetry	COM handler	Task Scheduler
178	\\Microsoft\\Windows\\InstallService\\SmartRetry	COM handler	Task Scheduler
179	\\Microsoft\\Windows\\InstallService\\SmartRetry	COM handler	Task Scheduler
180	\\Microsoft\\Windows\\InstallService\\SmartRetry	COM handler	Task Scheduler
181	\\Microsoft\\Windows\\InstallService\\SmartRetry	COM handler	Task Scheduler
182	\\Microsoft\\Windows\\InstallService\\WakeUpAndContinueUpdates	COM handler	Task Scheduler
183	\\Microsoft\\Windows\\InstallService\\WakeUpAndScanForUpdates	COM handler	Task Scheduler
184	\\Microsoft\\Windows\\International\\Synchronize Language Settings	COM handler	Task Scheduler
185	\\Microsoft\\Windows\\International\\Synchronize Language Settings	COM handler	Task Scheduler
186	\\Microsoft\\Windows\\Kernel\\La57Cleanup	COM handler	Task Scheduler
187	\\Microsoft\\Windows\\Language Components\\Installer\\Installation	%windir%\\system32\\la57setup.exe	Task Scheduler
188	\\Microsoft\\Windows\\Language Components\\Installer\\ReconcileLanguageResources	COM handler	Task Scheduler
189	\\Microsoft\\Windows\\Language Components\\Installer\\Uninstallation	COM handler	Task Scheduler

190	\\Microsoft\\Windows\\License Manager\\TempSignedLicenseExchange	COM handler	Task Scheduler
191	\\Microsoft\\Windows\\Location\\Notifications	COM handler	Task Scheduler
192	\\Microsoft\\Windows\\Location\\WindowsActionDialog	%windir%\\System32\\LocationNotificationWindows.exe	Task Scheduler
193	\\Microsoft\\Windows\\MU\\LPRemove	%SystemRoot%\\System32\\MbaeParserTask.exe	Task Scheduler
194	\\Microsoft\\Windows\\Maintenance\\WinSAT	%windir%\\System32\\WindowsActionDialog.exe	Task Scheduler
195	\\Microsoft\\Windows\\Management\\Autopilot\\DetectHardwareChange	COM handler	Task Scheduler
196	\\Microsoft\\Windows\\Management\\Autopilot\\DetectHardwareChange	COM handler	Task Scheduler
197	\\Microsoft\\Windows\\Management\\Autopilot\\RemediateHardwareChange	COM handler	Task Scheduler
198	\\Microsoft\\Windows\\Management\\Provisioning\\Cellular	COM handler	Task Scheduler
199	\\Microsoft\\Windows\\Management\\Provisioning\\Logon	%windir%\\system32\\ProvTool.exe /turn 7 /source CellStateChangeTask	Task Scheduler
200	\\Microsoft\\Windows\\Management\\Provisioning\\MdmDiagnosticsCleanup	%windir%\\system32\\ProvTool.exe /turn 5 /source LogonIdleTask	Task Scheduler
201	\\Microsoft\\Windows\\Management\\Provisioning\\Retry	%windir%\\system32\\MdmDiagnosticsTool.exe /clean	Task Scheduler
202	\\Microsoft\\Windows\\Management\\Provisioning\\RunOnReboot	%windir%\\system32\\ProvTool.exe /turn 5 /source ProvRetryTask	Task Scheduler
203	\\Microsoft\\Windows\\Maps\\MapsToastTask	%windir%\\system32\\ProvTool.exe /turn 5 /source ContinueSessionTask	Task Scheduler
204	\\Microsoft\\Windows\\Maps\\MapsUpdateTask	COM handler	Task Scheduler
205	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
206	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
207	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler

208	\Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
209	\Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic	COM handler	Task Scheduler
210	\Microsoft\Windows\Mobile Broadband Accounts\MNO Metadata Parser	COM handler	Task Scheduler
211	\Microsoft\Windows\Multimedia\SystemSoundsService	%windir%\system32\lpremove.exe	Task Scheduler
212	\Microsoft\Windows\Network Connectivity Status Indicator\NcsIdentifyUserProxies	COM handler	Task Scheduler
213	\Microsoft\Windows\Network Connectivity Status Indicator\NcsIdentifyUserProxies	COM handler	Task Scheduler
214	\Microsoft\Windows\Network Connectivity Status Indicator\NcsIdentifyUserProxies	COM handler	Task Scheduler
215	\Microsoft\Windows\NlaSvc\WiFiTask	COM handler	Task Scheduler
216	\Microsoft\Windows\PI\Secure-Boot-Update	COM handler	Task Scheduler
217	\Microsoft\Windows\PI\Sqm-Tasks	COM handler	Task Scheduler
218	\Microsoft\Windows\PerformanceTrace\RequestTrace	%SystemRoot%\System32\WiFiTask.exe nla	Task Scheduler
219	\Microsoft\Windows\Plug and Play\Device Install Group Policy	COM handler	Task Scheduler
220	\Microsoft\Windows\Plug and Play\Device Install Reboot Required	COM handler	Task Scheduler
221	\Microsoft\Windows\Plug and Play\Device Install Reboot Required	COM handler	Task Scheduler
222	\Microsoft\Windows\Plug and Play\Sysprep Generalize Drivers	COM handler	Task Scheduler
223	\Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem	%SystemRoot%\System32\drvinst.exe 6	Task Scheduler

224	\Microsoft\Windows\Printing\EduPrintProv	COM handler	Task Scheduler
225	\Microsoft\Windows\Printing\PrintJobCleanupTask	COM handler	Task Scheduler
226	\Microsoft\Windows\Printing\PrinterCleanupTask	%windir%\system32\eduprintprov.exe	Task Scheduler
227	\Microsoft\Windows\PushToInstall\LoginCheck	COM handler	Task Scheduler
228	\Microsoft\Windows\PushToInstall\Registration	%windir%\system32\sc.exe start pushtoinstall login	Task Scheduler
229	\Microsoft\Windows\PushToInstall\Registration	%windir%\system32\sc.exe start pushtoinstall registration	Task Scheduler
230	\Microsoft\Windows\Ras\MobilityManager	%windir%\system32\sc.exe start pushtoinstall registration	Task Scheduler
231	\Microsoft\Windows\ReFS\DedupSvc\Initialization	COM handler	Task Scheduler
232	\Microsoft\Windows\Recovery Environment\VerifyWinRE	COM handler	Task Scheduler
233	\Microsoft\Windows\Registry\RegIdleBackup	COM handler	Task Scheduler
234	\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask	COM handler	Task Scheduler
235	\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask	%windir%\system32\RAServer.exe /offerraupdate	Task Scheduler
236	\Microsoft\Windows\SMB\UninstallSMB1ClientTask	COM handler	Task Scheduler
237	\Microsoft\Windows\SMB\UninstallSMB1ServerTask	%windir%\system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -NonInteractive -NoProfile -WindowStyle Hidden "&%windir%\system32\WindowsPowerShell\v1.0\Modules\SmbShare\DisableUnusedSmb1.ps1 -Scenario Client"	Task Scheduler
238	\Microsoft\Windows\Servicing\OOBEFodSetup	%windir%\system32\RAServer.exe /offerraupdate	Task Scheduler
239	\Microsoft\Windows\Servicing\StartComponentCleanup	%windir%\system32\OOBEFodSetup.exe	Task Scheduler
240	\Microsoft\Windows\Setup\SetupCleanupTask	COM handler	Task Scheduler
241	\Microsoft\Windows\SharedPC\Account Cleanup	COM handler	Task Scheduler

242	\Microsoft\Windows\Shell\CreateObjectTask	COM handler	Task Scheduler
243	\Microsoft\Windows\Shell\FamilySafetyMonitor	COM handler	Task Scheduler
244	\Microsoft\Windows\Shell\FamilySafetyRefreshTask	%windir%\System32\wpcmon.exe	Task Scheduler
245	\Microsoft\Windows\Shell\IndexerAutomaticMaintenance	COM handler	Task Scheduler
246	\Microsoft\Windows\Shell\ThemeAssetTask_SyncFODState	COM handler	Task Scheduler
247	\Microsoft\Windows\Shell\ThemesSyncedImageDownload	COM handler	Task Scheduler
248	\Microsoft\Windows\Shell\UpdateUserPictureTask	COM handler	Task Scheduler
249	\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask	%windir%\system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -NonInteractive -NoProfile -WindowStyle Hidden "& %windir%\system32\WindowsPowerShell\v1.0\Modules\SmbShare\DisableUnusedSmb1.ps1 -Scenario Server"	Task Scheduler
250	\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTaskLogon	COM handler	Task Scheduler
251	\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTaskNetwork	COM handler	Task Scheduler
252	\Microsoft\Windows\SpacePort\SpaceAgentTask	COM handler	Task Scheduler
253	\Microsoft\Windows\SpacePort\SpaceAgentTask	%windir%\system32\SpaceAgent.exe	Task Scheduler
254	\Microsoft\Windows\SpacePort\SpaceManagerTask	%windir%\system32\SpaceAgent.exe	Task Scheduler
255	\Microsoft\Windows\SpacePort\SpaceManagerTask	%windir%\system32\spaceman.exe /Work	Task Scheduler
256	\Microsoft\Windows\Speech\SpeechModelDownloadTask	%windir%\system32\spaceman.exe /Work	Task Scheduler
257	\Microsoft\Windows\StateRepository\MaintenanceTasks	%windir%\system32\speech_onecore\common\SpeechModelDownload.exe	Task Scheduler
258	\Microsoft\Windows\StorageTiers Management\StorageTiers Management Initialization	%windir%\system32\rundll32.exe %windir%\system32\Windows.StateRepositoryClient.dll,StateRepository DoMaintenanceTasks	Task Scheduler

259	\Microsoft\Windows\Storage Tiers Management\Storage Tiers Optimization	COM handler	Task Scheduler
260	\Microsoft\Windows\Subscription\EnableLicenseAcquisition	%windir%\system32\defrag.exe -c -h -g -# -m 8 -i 13500	Task Scheduler
261	\Microsoft\Windows\Subscription\EnableLicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe -e	Task Scheduler
262	\Microsoft\Windows\Subscription\EnableLicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe -e	Task Scheduler
263	\Microsoft\Windows\Subscription\LicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe -e	Task Scheduler
264	\Microsoft\Windows\Subscription\LicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe	Task Scheduler
265	\Microsoft\Windows\Subscription\LicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe	Task Scheduler
266	\Microsoft\Windows\Sustainability\PowerGridForecastTask	%SystemRoot%\system32\ClipRenew.exe	Task Scheduler
267	\Microsoft\Windows\Sustainability\PowerGridForecastTask	COM handler	Task Scheduler
268	\Microsoft\Windows\Sustainability\SustainabilityTelemetry	COM handler	Task Scheduler
269	\Microsoft\Windows\Sysmain\HybridDriveCachePrepopulate	COM handler	Task Scheduler
270	\Microsoft\Windows\Sysmain\HybridDriveCacheRebalance	COM handler	Task Scheduler
271	\Microsoft\Windows\Sysmain\ResPriStaticDbSync	COM handler	Task Scheduler
272	\Microsoft\Windows\Sysmain\WsSwapAssessmentTask	COM handler	Task Scheduler
273	\Microsoft\Windows\SystemRestore\SR	%windir%\system32\rundll32.exe sysmain.dll,PfSvWsSwapAssessmentTask	Task Scheduler
274	\Microsoft\Windows\TPM\Tpm-HASCertRetr	%windir%\system32\tzsync.exe	Task Scheduler
275	\Microsoft\Windows\TPM\Tpm-Maintenance	COM handler	Task Scheduler
276	\Microsoft\Windows\TPM\Tpm-Maintenance	COM handler	Task Scheduler
277	\Microsoft\Windows\TPM\Tpm-Maintenance	COM handler	Task Scheduler
278	\Microsoft\Windows\TPM\Tpm-Maintenance	COM handler	Task Scheduler

279	\Microsoft\Windows\TPM\Tpm-PreAttestationHealthCheck	COM handler	Task Scheduler
280	\Microsoft\Windows\Task Manager\Interactive	%windir%\system32\srtasks.exe ExecuteScheduledSPPCreation	Task Scheduler
281	\Microsoft\Windows\TextServicesFramework\MsCtfMonitor	COM handler	Task Scheduler
282	\Microsoft\Windows\Time Synchronization\ForceSynchronize Time	COM handler	Task Scheduler
283	\Microsoft\Windows\Time Synchronization\ForceSynchronize Time	COM handler	Task Scheduler
284	\Microsoft\Windows\Time Synchronization\SynchronizeTime	COM handler	Task Scheduler
285	\Microsoft\Windows\Time Zone\SynchronizeTimeZone	%windir%\system32\sc.exe start w32time task_started	Task Scheduler
286	\Microsoft\Windows\UNP\Run UpdateNotificationMgr	COM handler	Task Scheduler
287	\Microsoft\Windows\UNP\Run UpdateNotificationMgr	%windir%\System32\UNP\UpdateNotificationMgr.exe	Task Scheduler
288	\Microsoft\Windows\UPnP\UPnPHostConfig	%windir%\System32\MLEngineStub.exe HandleUusFailoverEvaluationSignalFromWnf	Task Scheduler
289	\Microsoft\Windows\USB\Usb-Notifications	sc.exe config upnphost start= auto	Task Scheduler
290	\Microsoft\Windows\USB\Usb-Notifications	COM handler	Task Scheduler
291	\Microsoft\Windows\USB\Usb-Notifications	COM handler	Task Scheduler
292	\Microsoft\Windows\USB\Usb-Notifications	COM handler	Task Scheduler
293	\Microsoft\Windows\UpdateOrchestrator\Report policies	%windir%\System32\UNP\UpdateNotificationMgr.exe	Task Scheduler
294	\Microsoft\Windows\UpdateOrchestrator\Report policies	%systemroot%\system32\usoclient.exe ReportPolicies	Task Scheduler
295	\Microsoft\Windows\UpdateOrchestrator\Schedule Maintenance Work	%systemroot%\system32\usoclient.exe ReportPolicies	Task Scheduler
296	\Microsoft\Windows\UpdateOrchestrator\Schedule Scan	%systemroot%\system32\usoclient.exe StartMaintenanceWork	Task Scheduler
297	\Microsoft\Windows\UpdateOrchestrator\Schedule Scan Static Task	%systemroot%\system32\usoclient.exe StartScan	Task Scheduler

298	\Microsoft\Windows\UpdateOrchestrator\Schedule Scan Static Task	%systemroot%\system32\usoclient.exe StartScan	Task Scheduler
299	\Microsoft\Windows\UpdateOrchestrator\Schedule Scan Static Task	%systemroot%\system32\usoclient.exe StartScan	Task Scheduler
300	\Microsoft\Windows\UpdateOrchestrator\Schedule Scan Static Task	%systemroot%\system32\usoclient.exe StartScan	Task Scheduler
301	\Microsoft\Windows\UpdateOrchestrator\Schedule Scan Static Task	%systemroot%\system32\usoclient.exe StartScan	Task Scheduler
302	\Microsoft\Windows\UpdateOrchestrator\Schedule Wake To Work	%systemroot%\system32\usoclient.exe StartScan	Task Scheduler
303	\Microsoft\Windows\UpdateOrchestrator\Schedule Work	%systemroot%\system32\usoclient.exe StartWork	Task Scheduler
304	\Microsoft\Windows\UpdateOrchestrator\Start Oobe Expedite Work	%systemroot%\system32\usoclient.exe StartWork	Task Scheduler
305	\Microsoft\Windows\UpdateOrchestrator\StartOobeAppsScan AfterUpdate	%systemroot%\system32\usoclient.exe StartWork	Task Scheduler
306	\Microsoft\Windows\UpdateOrchestrator\StartOobeAppsScan_LicenseAccepted	%systemroot%\system32\usoclient.exe StartOobeAppsScanAfterUpdate	Task Scheduler
307	\Microsoft\Windows\UpdateOrchestrator\UIEOrchestrator	%systemroot%\system32\usoclient.exe StartOobeAppsScan	Task Scheduler
308	\Microsoft\Windows\UpdateOrchestrator\USO_UxBroker	%systemroot%\system32\UIEOrchestrator.exe /SendHeartbeat	Task Scheduler
309	\Microsoft\Windows\UpdateOrchestrator\USO_UxBroker	%systemroot%\system32\MusNotification.exe	Task Scheduler
310	\Microsoft\Windows\UpdateOrchestrator\UUS Failover Task	%systemroot%\system32\MusNotification.exe	Task Scheduler
311	\Microsoft\Windows\User Profile Service\HiveUploadTask	COM handler	Task Scheduler
312	\Microsoft\Windows\WCM\WiFi Task	COM handler	Task Scheduler
313	\Microsoft\Windows\WDI\ResolutionHost	%SystemRoot%\System32\WiFiTask.exe	Task Scheduler
314	\Microsoft\Windows\WOF\WIM-Hash-Management	COM handler	Task Scheduler

315	\\Microsoft\\Windows\\WOF\\WIM-Hash-Management	COM handler	Task Scheduler
316	\\Microsoft\\Windows\\WOF\\WIM-Hash-Validation	COM handler	Task Scheduler
317	\\Microsoft\\Windows\\WaaS\\Medic\\PerformRemediation	COM handler	Task Scheduler
318	\\Microsoft\\Windows\\Windows Defender\\Windows Defender Cache Maintenance	COM handler	Task Scheduler
319	\\Microsoft\\Windows\\Windows Defender\\Windows Defender Cleanup	C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.25020.1009-0\\MpCmdRun.exe -IdleTask -TaskName WdCacheMaintenance	Task Scheduler
320	\\Microsoft\\Windows\\Windows Defender\\Windows Defender Scheduled Scan	C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.25020.1009-0\\MpCmdRun.exe -IdleTask -TaskName WdCleanup	Task Scheduler
321	\\Microsoft\\Windows\\Windows Defender\\Windows Defender Verification	C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.25020.1009-0\\MpCmdRun.exe Scan -ScheduleJob -ScanTrigger 55 -IdleScheduledJob	Task Scheduler
322	\\Microsoft\\Windows\\Windows Error Reporting\\QueueReporting	C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.25020.1009-0\\MpCmdRun.exe -IdleTask -TaskName WdVerification	Task Scheduler
323	\\Microsoft\\Windows\\Windows Error Reporting\\QueueReporting	%windir%\\system32\\wermgr.exe -upload	Task Scheduler
324	\\Microsoft\\Windows\\Windows Error Reporting\\QueueReporting	%windir%\\system32\\wermgr.exe -upload	Task Scheduler
325	\\Microsoft\\Windows\\Windows Error Reporting\\QueueReporting	%windir%\\system32\\wermgr.exe -upload	Task Scheduler
326	\\Microsoft\\Windows\\Windows Error Reporting\\QueueReporting	%windir%\\system32\\wermgr.exe -upload	Task Scheduler
327	\\Microsoft\\Windows\\Windows Filtering Platform\\BfeOnServiceStartTypeChange	%windir%\\system32\\wermgr.exe -upload	Task Scheduler
328	\\Microsoft\\Windows\\Windows Media Sharing\\UpdateLibrary	%windir%\\system32\\rundll32.exe bfe.dll,BfeOnServiceStartTypeChange	Task Scheduler
329	\\Microsoft\\Windows\\Windows ColorSystem\\Calibration Loader	"%ProgramFiles%\\Windows Media Player\\wmpnscfg.exe"	Task Scheduler
330	\\Microsoft\\Windows\\Windows ColorSystem\\Calibration Loader	COM handler	Task Scheduler

331	\\Microsoft\\Windows\\WindowsUpdate\\Refresh Group Policy Cache	COM handler	Task Scheduler
332	\\Microsoft\\Windows\\WindowsUpdate\\Scheduled Start	COM handler	Task Scheduler
333	\\Microsoft\\Windows\\WindowsUpdate\\Scheduled Start	%systemroot%\\System32\\sc.exe start wuauserv	Task Scheduler
334	\\Microsoft\\Windows\\WindowsUpdate\\Scheduled Start	%systemroot%\\System32\\sc.exe start wuauserv	Task Scheduler
335	\\Microsoft\\Windows\\WindowsUpdate\\Scheduled Start	%systemroot%\\System32\\sc.exe start wuauserv	Task Scheduler
336	\\Microsoft\\Windows\\Wininet\\CacheTask	%systemroot%\\System32\\sc.exe start wuauserv	Task Scheduler
337	\\Microsoft\\Windows\\WlanSvc\\CDSSync	COM handler	Task Scheduler
338	\\Microsoft\\Windows\\WlanSvc\\MoProfileManagement	COM handler	Task Scheduler
339	\\Microsoft\\Windows\\WlanSvc\\MoProfileManagement	COM handler	Task Scheduler
340	\\Microsoft\\Windows\\Work Folders\\Work Folders Logon Synchronization	COM handler	Task Scheduler
341	\\Microsoft\\Windows\\Work Folders\\Work Folders Maintenance Work	COM handler	Task Scheduler
342	\\Microsoft\\Windows\\Workplace Join\\Automatic-Device-Join	COM handler	Task Scheduler
343	\\Microsoft\\Windows\\Workplace Join\\Automatic-Device-Join	%SystemRoot%\\System32\\dsregcmd.exe \$(Arg0) \$(Arg1) \$(Arg2)	Task Scheduler
344	\\Microsoft\\Windows\\Workplace Join\\Device-Sync	%SystemRoot%\\System32\\dsregcmd.exe \$(Arg0) \$(Arg1) \$(Arg2)	Task Scheduler
345	\\Microsoft\\Windows\\Workplace Join\\Recovery-Check	COM handler	Task Scheduler
346	\\Microsoft\\Windows\\Workplace Join\\Recovery-Check	%SystemRoot%\\System32\\dsregcmd.exe /checkrecovery	Task Scheduler
347	\\Microsoft\\Windows\\WwanSvc\\NotificationTask	%SystemRoot%\\System32\\dsregcmd.exe /checkrecovery	Task Scheduler
348	\\Microsoft\\Windows\\WwanSvc\\OobeDiscovery	%SystemRoot%\\System32\\WiFiTask.exe wwan	Task Scheduler
349	\\Microsoft\\Windows\\WwanSvc\\OobeDiscovery	COM handler	Task Scheduler
350	\\Microsoft\\Windows\\WwanSvc\\OobeDiscovery	COM handler	Task Scheduler

351	\Microsoft\Windows\capabilityaccessmanager\maintenanceta sks	COM handler	Task Scheduler
352	\Microsoft\Windows\input\Input SettingsRestoreDataAvailable	%WinDir%\System32\WinBioPlugIns\FaceFodUninst aller.exe	Task Scheduler
353	\Microsoft\Windows\input\Local UserSyncDataAvailable	COM handler	Task Scheduler
354	\Microsoft\Windows\input\Mou seSyncDataAvailable	COM handler	Task Scheduler
355	\Microsoft\Windows\input\Pen SyncDataAvailable	COM handler	Task Scheduler
356	\Microsoft\Windows\input\Rem oteMouseSyncDataAvailable	COM handler	Task Scheduler
357	\Microsoft\Windows\input\Rem otePenSyncDataAvailable	COM handler	Task Scheduler
358	\Microsoft\Windows\input\Rem oteTouchpadSyncDataAvailabl e	COM handler	Task Scheduler
359	\Microsoft\Windows\input\Touc hpadSyncDataAvailable	COM handler	Task Scheduler
360	\Microsoft\Windows\input\sync pensettings	COM handler	Task Scheduler
361	\Microsoft\XblGameSave\XblG ameSaveTask	COM handler	Task Scheduler
362	\Mozilla\Firefox Default Browser Agent 308046B0AF4A39CB	%windir%\System32\XblGameSaveTask.exe standby	Task Scheduler
363	\NVIDIA GeForce Experience SelfUpdate_{B2FE1952-0186- 46C3-BAEC-A80AA35AC5B8}	C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe -d "C:\Program Files\NVIDIA Corporation\NvDriverUpdateCheck" -l 3 -f C:\Program Data\NVIDIA\NvContainerDriverUpdateCheck.log	Task Scheduler
364	\NitroSense	C:\Program Files (x86)\Microsoft\EdgeUpdate\Micros oftEdgeUpdate.exe /ua /installsource scheduler	Task Scheduler
365	\Norton Security Ultra\Norton Security Ultra Autofix	C:\Program Files\Mozilla Firefox\default-browser-agent.exe do-task	Task Scheduler
366	\Norton Security Ultra\Norton Security Ultra Error Analyzer	C:\Program Files\Norton Security\Engine\22.24.8.36\SymErr.exe /ui	Task Scheduler
367	\Norton Security Ultra\Norton Security Ultra Error Processor	C:\Program Files\Norton Security\Engine\22.24.8.36\SymErr.exe /analyze	Task Scheduler
368	\Norton WSC Integration	"C:\Program Files\Acer\NitroSense Service\PSLauncher.exe"	Task Scheduler

369	\NvDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	"C:\Program Files\Norton Security\Engine\22.24.8.36\WSCStub.exe" /taskschd	Task Scheduler
370	\NvNodeLauncher_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	"C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA GeForce Experience.exe"	Task Scheduler
371	\NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	C:\Program Files (x86)\NVIDIA Corporation\NvNode\nvnodejslauncher.exe --launcher=TaskScheduler	Task Scheduler
372	\NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe	Task Scheduler
373	\NvTmRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe	Task Scheduler
374	\NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe	Task Scheduler
375	\NvTmRep_CrashReport3_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe	Task Scheduler
376	\NvTmRep_CrashReport4_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}	C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe	Task Scheduler
377	\Oem\AcerJumpstartTask	C:\Program Files\Norton Security\Engine\22.24.8.36\SymErr.exe /submit	Task Scheduler
378	\Oem\AcerJumpstartTask	"C:\Program Files (x86)\Acer\Acer Jumpstart\hermes.exe" /default	Task Scheduler
379	\OneDrive Reporting Task-S-1-5-21-408419827-1937999014-645067451-1001	C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe	Task Scheduler
380	\OneDrive Standalone Update Task-S-1-5-21-4054349220-3449028549-667842490-500	%localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe /reporting	Task Scheduler
381	\OneDrive Standalone Update Task-S-1-5-21-408419827-1937999014-645067451-1001	%localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe	Task Scheduler
382	\OneDrive Startup Task-S-1-5-21-408419827-1937999014-645067451-1001	%localappdata%\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe	Task Scheduler
383	\Power Button	C:\Users\amaan\AppData\Local\Microsoft\OneDrive\25.041.0303.0002\OneDriveLauncher.exe /startInstances	Task Scheduler
384	\Quick Access	"C:\Program Files\Acer\Quick Access Service\PowerButton_NB.exe" -s	Task Scheduler

385	\Remediation\AntimalwareMigrationTask	"C:\Program Files (x86)\Acer\Acer Jumpstart\hermes.exe" /default	Task Scheduler
386	\SecurityScannerScheduler	"C:\Program Files\Acer\Quick Access Service\QALauncher.exe"	Task Scheduler
387	\Software Update Application	C:\Program Files (x86)\McAfee Security Scan\4.2.707\SSScheduler.exe	Task Scheduler
388	\Software Update Application	"C:\ProgramData\OEM\UpgradeTool\ListCheck.exe"	Task Scheduler
389	\Software Update Application	"C:\ProgramData\OEM\UpgradeTool\ListCheck.exe"	Task Scheduler
390	\Software Update Application	"C:\ProgramData\OEM\UpgradeTool\ListCheck.exe"	Task Scheduler
391	\StorPSCTL	"C:\ProgramData\OEM\UpgradeTool\ListCheck.exe"	Task Scheduler
392	\UEIPIinvitation	"C:\Program Files\Acer\User Experience Improvement Program Service\Framework\TriggerFramework.exe"	Task Scheduler
393	\UbtFrameworkService	"C:\Program Files\Acer\StorPSCTL\StorPSCTL.exe"	Task Scheduler

Shared Folders

Total Shared Folders: 3

S.No	Shared Name	Local Path	Description
1	C\$	C:\	Default share
2	D\$	D:\	Default share
3	IPC\$	Remote	IPC

Unwanted Software Detection

Total Unwanted Software Found: 1

S.No	Software Name
1	NVIDIA NVAPI Monitor plugin for NvContainer

USB Logs

- **No logs found.**

Security Logs

- **Event ID:** 4688
Timestamp: 2025-03-30T03:24:47.5210000
Source: Microsoft-Windows-Security-Auditing
Description: A new process has been created.
- **Event ID:** 4696
Timestamp: 2025-03-30T03:24:47.5210000
Source: Microsoft-Windows-Security-Auditing
Description: A primary token was assigned to process.
- **Event ID:** 4826
Timestamp: 2025-03-30T03:24:47.5210000
Source: Microsoft-Windows-Security-Auditing
Description: Boot Configuration Data loaded.
- **Event ID:** 4688
Timestamp: 2025-03-30T03:24:47.5250000
Source: Microsoft-Windows-Security-Auditing
Description: A new process has been created.
- **Event ID:** 4688
Timestamp: 2025-03-30T03:24:48.1560000
Source: Microsoft-Windows-Security-Auditing
Description: A new process has been created.

System Logs

- **Event ID:** 12
Timestamp: 2025-03-30T03:24:45.2810000
Source: Microsoft-Windows-Kernel-General
Description: The operating system started at system time 2025-03-29T21:54:44.500000000Z.
- **Event ID:** 25
Timestamp: 2025-03-30T03:24:45.2810000
Source: Microsoft-Windows-Kernel-General
Description: The system time was initialized to 2025-03-29T21:54:44.500000000Z.

- **Event ID:** 6009
Timestamp: 2025-03-30T03:25:11.8240000
Source: EventLog
Description: Microsoft (R) Windows (R) 10.00. 26100 Multiprocessor Free.
- **Event ID:** 6005
Timestamp: 2025-03-30T03:25:11.8240000
Source: EventLog
Description: The Event log service was started.
- **Event ID:** 153
Timestamp: 2025-03-30T03:24:45.2810000
Source: Microsoft-Windows-Kernel-Boot
Description: Virtualization-based security (policies: 0) is disabled.

Application Logs

- **Event ID:** 1531
Timestamp: 2025-03-30T03:24:52.1180000
Source: Microsoft-Windows-User Profiles Service
Description: The User Profile Service has started successfully.
- **Event ID:** 5615
Timestamp: 2025-03-30T03:25:01.3650000
Source: Microsoft-Windows-WMI
Description: Windows Management Instrumentation Service started successfully
- **Event ID:** 5617
Timestamp: 2025-03-30T03:25:01.8350000
Source: Microsoft-Windows-WMI
Description: Windows Management Instrumentation Service subsystems initialized successfully
- **Event ID:** 63
Timestamp: 2025-03-30T03:25:02.0660000
Source: Microsoft-Windows-WMI
Description: A provider, InvProv, has been registered in the Windows Management Instrumentation namespace ROOT\CIMV2 to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.
- **Event ID:** 63
Timestamp: 2025-03-30T03:25:02.0680000
Source: Microsoft-Windows-WMI
Description: A provider, InvProv, has been registered in the Windows Management Instrumentation namespace ROOT\CIMV2 to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user

requests.

DNS Logs

- **No logs found.**