|  |  |  |
| --- | --- | --- |
| Event ID | Type | Note |
| 4624 | Authentication | Logon Success |
| 4625 | Authentication | Logon Failure |
| 4672 | Authentication | Administrator privileged logon event |
| 4673 | Process Privilege | Sensitive Privilege use |
| 4703 |  | Token right adjusted; enabled privileges; **CHECK IF ENABLED** |
| 4728 | Group Modification | User added to a security group; only logged on DCs; look for additions to admin groups such as Domain Admins |
| 4729 | Group Modification | User removed from an AD security group |
| 4732 | Group Modification | User added to a local security group |
| 4733 | Group Modification | User removed from a local security group |
| 4720 | User Modification | User account created; logged for both local SAM and domain accts |
| 4724 | User Modification | Attempt to reset an account's password |
| 4726 | User Modification | User account deletion |
| 4738 | User Modification | User account was changed; e.g. set to not require a password |
| 5154 | Network | New application listening for incoming connections |
| 4698 | Task Scheduler | New scheduled task created |
| 4697 | Service | New service created |

**WMI Event Subscription**

Consumer = script / command line

Filter = the query

filterToConsumerBinding = binding

|  |  |
| --- | --- |
| autorunsc64.exe -accepteula -a m | only displays WMI entries; the name returned here is for the CommandLineEventConsumer |

**Removing with PowerShell**

Get-WMIObject -Class \_\_EventFilter -Namespace root\subscription | where {$\_.name -like "maliciouspersistence" | Remove-WMIObject

**Removing with Autoruns**

Only deletes the CommandLineEventConsumer



**PsRemoting**

Enable-PSRemoting –force  
Set-Item WSMan:localhost\client\trustedhosts -value \*  
New-PSSession –ComputerName server1.domain.com –Credentials domain\serveradmin  
Exit-PsSession  
Disconnect-PsSession

**schtasks**

|  |  |
| --- | --- |
| /tn | Task Name |
| /query | Query |
| /v | verbose |
| /fo list | list output format |

Look at the "Task To Run" field for malicious executable/command

Delete a Task

schtasks /delete /tn MaliciousTaskName /f

**Registry Keys**

HKLM keys are run at system boot

HKCU keys are run at user logon

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]

**Querying Registry Keys**

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

* check if UserInit has anything but C:\Windows\system32\userinit.exe

**Registry Key Value Removal**

reg delete "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v EvilKey

**Investigation Process**

1. tcpview identify connected processes
2. proc exp
   1. unsigned binaries
3. strings
4. dll view
5. suspend malware
6. proc mon
7. kill malware