https://image.slidesharecdn.com/kheirkhabarovoffzonefinal-181117201458/95/hunting-for-privilege-escalation-in-windows-environment-50-638.jpg

Always Install Elevated. Let's hunt it!



Search for spawning of cmd or Powershell by MSI package:

source_name:"Microsoft-Windows-Sysmon" AND event_id:1AND event_data.lmage:("\\cmd.exe" "\\powershell.exe") AND event_data.Parentlmage:("\\Windows\\Installer\\" AND *msi* AND *tmp)

task	event_data.ParentOfParent	event_data.ParentImage	event_data.CommandLine	event_data.User	event_data.IntegrityLevel
ProcessCreate (rule: ProcessCreate)	C:\Windows\System32\msiexec .exe	C:\Mindows\Installer\MSI7 F54.tmp	C:\Windows\system32\cmd.ex	NT AUTHORITY\SYSTEM	System
Process Create (rule: ProcessCreate)	C:\Windows\System32\msiexec .exe	C:\Windows\Installer\MSI7 838.tmp	C:\Windows\system32\cmd.ex	WIN10X64_1803\priv user	Medium

Search for spawning of processes from cmd/Powershell, spawned from MSI package:

source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.ParentImage:("\\cmd.exe" "\\powershell.exe") AND event_data.ParentOfParent:("\\Windows\\Installer\\" AND *msi* AND *tmp)

task X >	event_data_ParentOfParent	event_data.Parentlmage	event_data.lmage	event_data.User	event_data.IntegrityLevel
Process Create (rule: ProcessCreate)	C:\Windows\Installer\MSI783 8.tmp	C:\Windows\System32\cmd.e	C:\Windows\System32\w hoami.exe	WIN10X64_1803\priv user	Medium
Process Create (rule: ProcessCreate)	C:\Windows\Installer\MSIA7E C:tmp	C:\Windows\System32\cmd.e	C:\Windows\System32\w hoami.exe	NT AUTHORITY\SYSTEM	System