



Product

Solutions

Resources

Open Source

Enterprise

Pricing

Search

Sign in

Sign up

SwiftOnSecurity / sysmon-config

Public

Notifications

Fork1.7k

Star4.8k

<> Code

Issues54

Pull requests28

Actions

Projects

Wiki

Security

Insights

Keyboard Layout Load #92

New issue

Closed

Neo23x0 wants to merge 2 commits into SwiftOnSecurity:master from Neo23x0:patch-4

Conversation2

Commits2

Checks0

Files changed1

+2-0

Changes from all commitsFile filterConversationsJump toSettings

▼	↕	2	■■■■■	sysmonconfig-export.xml	📄	⋮
⬆	@@ -673,6 +673,8 @@					
673	673	<TargetObject condition="end with">\FriendlyName</TargetObject> <!--Microsoft:Windows: New devices connected and remembered-->				
674	674	<TargetObject condition="is">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\InProgress\ (Default)</TargetObject> <!--Microsoft:Windows: See when WindowsInstaller is engaged, useful for timeline matching with other events-->				
675	675	<TargetObject condition="begin with">HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32</TargetObject> <!-- Microsoft:Windows: Malware sometimes disables tracing to obfuscate tracks-->				
	676	+	<TargetObject condition="contains">\Keyboard Layout\Preload</TargetObject> <!--Microsoft:Windows: Keyboard layout loaded into user session [https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/Keyboard-Layout/Preload/index] -->			
	677	+	<TargetObject condition="contains">\Keyboard Layout\Substitutes</TargetObject> <!-- Microsoft:Windows: Keyboard layout loaded into user session [https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/Keyboard-Layout/Preload/index] -->			
676	678	</RegistryEvent>				
677	679					
678	680	<RegistryEvent onmatch="exclude">				
		⬇				