

## Abusing debug privilege. Create process with arbitrary parent Let's hunt it!



Search for spawning of unusual child processes by different system processes:

```
event_id:1 AND source_name:"Microsoft-Windows-Sysmon" AND event_data.ParentImage:{"\\winlogon.exe"
"\\services.exe" "\\lsass.exe" "\\csrss.exe" "\\smss.exe" "\\wininit.exe" "\\spoolsv.exe" "\\searchindexer.exe")
AND event_data.Image:{"\\cmd.exe" "\\powershell.exe"} AND event_data.User:"NT AUTHORITY\\SYSTEM" AND
-event_data.CommandLine:{"*route* *ADD*}
```

task	event_data.ParentImage	event_data.ParentUser	event_data.Image	event_data.User	event_data.IntegrityLevel
Process Create (rule: Process Create)	C:\\Windows\\System32\\winlo gon.exe	NT AUTHORITY\\SYSTEM	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe	NT AUTHORITY\\SYSTEM	System
Process Create (rule: Process Create)	C:\\Windows\\System32\\lsass .exe	NT AUTHORITY\\SYSTEM	C:\\Windows\\System32\\cmd.exe	NT AUTHORITY\\SYSTEM	System