



Settings



Post



Florian Roth   
@cyb3rops



Long shot - Sigma rule to detect RPC service process anomalies based on sub processes

Could you guys check if and how often you see sub processes with this parent command line?  
(starts with; use a \* at the end)

CVE-2022-26809

C:\WINDOWS\system32\svchost.exe -k RPCSS

```
proc_creation_win_rpcss_anomalies.yml U X file_access_win_browser_credential_stealing.yml net_connection_win_dllhost_net_
1 title: Remote Procedure Call Service Anomaly
2 id: a7cd7306-df8b-4398-b711-6f3e4935cf16
3 status: experimental
4 description: Detects suspicious remote procedure call (RPC) service anomalies based on the spawned sub processes
5 author: Florian Roth
6 references:
7   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809
8   - https://www.bleepingcomputer.com/startups/RpcSs.exe-14544.html
9 date: 2022/04/13
10 logsource:
11   category: process_creation
12   product: windows
13 detection:
14   selection:
15     ParentCommandLine|startswith: 'C:\WINDOWS\system32\svchost.exe -k RPCSS'
16   condition: selection
17 falsepositives:
18   - Unknown
19 level: high
20 tags:
21   - attack.initial_access
22   - attack.ti190
23   - attack.execution
24   - attack.ti569.002
25
```

2:24 PM · Apr 13, 2022

74 Reposts 2 Quotes 253 Likes 45 Bookmarks



45



Don't miss what's happening  
People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.  
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies