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 | file_access_win_browser_credential_stealing.yml | net_connection_win_dllhost_net_

```yaml
title: Remote Procedure Call Service Anomaly
id: a7cd7306-df8b-4398-b711-6f3e4935cf16
status: experimental
description: Detects suspicious remote procedure call (RPC) service anomalies based on the spawned sub processes
author: Florian Roth
references:
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809
    - https://www.bleepingcomputer.com/startups/RpcSs.exe-14544.html
date: 2022/04/13
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    ParentCommandLine|startswith: 'C:\WINDOWS\system32\svchost.exe -k RPCSS'
  condition: selection
falsepositives:
  - Unknown
level: high
tags:
  - attack.initial_access
  - attack.t1190
  - attack.execution
  - attack.t1569.002
```

2:24 PM · Apr 13, 2022

74 Reposts **2** Quotes **253** Likes **45** Bookmarks

45