Sign in

The-DFIR-Report / **Sigma-Rules** Public

Notifications | Fork 31 | Star 188

Code | Issues | Pull requests 4 | Actions | Projects | Security | Insights

Sigma-Rules / **win_mofcomp_execution.yml**

28 lines (28 loc) · 697 Bytes

Code | Blame | Raw

```yaml
title: MOFComp Execution
id: fd7aed23-7585-44fb-9920-5da82c740e6e
status: Experimental
description: Detects abuse of mofcomp to load WMI classes i.e. to create WMI event subscriptions
author: _pete_0, TheDFIRReport
references:
  - https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/
date: 2022/07/11
modified: 2022/07/11
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith:
      - '\mofcomp.exe'
    ParentImage|endswith:
      - '\cmd.exe'
      - '\powershell.exe'
  condition: selection
fields:
  - ParentCommandLine
falsepositives:
  - System administrator activities
level: high
tags:
  - attack.execution
  - attack.t1546.003
```