Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

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

Notifications Fork 31 Star 188

Code Issues Pull requests 4 Actions Projects Security Insights

**Files**

7526056

Go to file

- Deleting Windows Defender sche...
- Enable WDigest using PowerShell
- Enable WDigest using PowerShell...
- Enabling RDP service via reg.exe c...
- Enabling restricted admin mode
- Execution of ZeroLogon PoC exec...
- LICENSE
- PSEXEC Custom Named Service B...
- QBot Exec via Scheduled Task wit...
- Qbot Exec via Scheduled Task
- README.md
- Registry Query for WDigest
- SSH over port 443 with known S...
- Webshell Usage with ManageEng...
- adfind_discovery
- custom_cobalt_strike_command_...
- defaultaccount_usage
- dns_query_for_ufileio_domain.yml
- exchange_webshell_creation
- lazagne_dumping_credentials
- mimkiatz_command_line_with_tic...
- scheduled_task_executing_power...
- sigma-mapping.yml
- suspicious_scheduled_task_creati...
- win_chcp_codepage_locale_looku...
- win_cobaltstrike_operator_bloope...
- win_cobaltstrike_operator_bloope...
- win_hiding_local_user_accounts.yml
- win_mofcomp_execution.yml
- win_network_anydesk.yml
- win_network_splashtop.yml
- win_software_byot.yml
- win_software_splashtop.yml
- win_suspicious_commands_by_sq...

Sigma-Rules / **win_mofcomp_execution.yml**

**The DFIR Report** Update win_mofcomp_execution.yml 12783e2 · 2 years ago History

Code Blame 28 lines (28 loc) · 697 Bytes 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 subs
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
```