```
                              ## CISA Code & Media Analysis ##

                             ############ README ###############
## Edit rules and queries as needed for your hunt and based on your environment.
## Ensure your EDR/SIEM instance has enough memory to run these AND/OR condition
based queries. May take longer to run than conventional Sigma rule query.
## Do not edit "logsource-product:" unless you are editing this rule to meet
specific logsources/fields and know your environment.
## TLP GREEN + Please use local installation of Sigma to convert this rule.
## TLP CLEAR may convert rules using online converter of choice.
                             ####################################

title: Detects CVE-2025-53770 IOCs and Activity Based on Submitted Files 251132.r2
incident: 251133.r2
tlp: CLEAR
id: a9327942-4cf7-48e4-9ea4-ad0b54db4bf7
status: test
description: Detects ToolShell CVE-2025-53770 Exploitation of SharePoint servers.
Detects IOCs and Activity Based on Submitted Files 251132.r2.
references:
    - 251132.r2
author: CISA Code & Media Analysis
date: 2025-07-23
modified: 2025-07-23
tags:
    - cve.2025.53770
logsource:
    product: cma
detection:
    keywords_1:
        - 'CVAUGFnZSBMYW5ndWFnZT0i'
        - '%@Page Language="'
    keywords_2:
        - 'Jwb3dlcnNoZWxsLmV4ZS'
        - 'powershell.exe'
    keywords_3:
        - 'ItZW5j'
        - '-enc'
        - 'LUVuY29kZWRDb21tYW5k'
        - '-EncodedCommand'
    keywords_4:
        - '0Jhc2U2NFN0cmluZy'
        - 'Base64String'
    keywords_5:
        - 'FJlcXVlc3QuRm9ybV'
        - 'Request.Form'
    keywords_6:
        - 'sicCJ'
        - '"p"'
```

```
    keywords_7:
        - '*.exe'
    keywords_8:
        - 'powershell*'
    keywords_9:
        - '-Command'
    keywords_10:
        - 'Get-ChildItem'
        - 'ForEach-Object'
    keywords_11:
        - '*\TEMPLATE\LAYOUTS\*'

    keywords_12:
        - '*.exe'
    keywords_13:
        - 'certutil*'
    keywords_14:
        - '-decode'

    keywords_15:
        -
'c:\progra~1\common~1\micros~1\webser~1\16\template\layouts\owa\resources\*'
        - 'c:\progra~1\common~1\micros~1\webser~1\16\template\layouts\*'
        - '\template\layouts\*'
        - '\template\layouts\owa\*'
    keywords_16:
        - '*.aspx'
        - '*.txt'

    keywords_17:
        - '*\TEMPLATE\LAYOUTS\*'
    keywords_18:
        - 'spinstall*'
    keywords_19:
        - '*.aspx'

    condition: keywords_1 and keywords_2 and keywords_3 and keywords_4 and
keywords_5 and keywords_6 or keywords_7 and keywords_8 and keywords_9 and
keywords_10 and keywords_11 or keywords_12 and keywords_13 and keywords_14 or
keywords_15 and keywords_16 or keywords_17 and keywords_18 and keywords_19

falsepositives:
    - Rate of FP low-moderate with some strings.
    - Use this rule in an infected environment/logs.
    - Analyst may need to make adjustments to the query as required.
level: critical
```