```
                              ## 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 ToolShell CVE-2025-53770 Exploitation IOCs and Activity
incident: 251133.r1
tlp: CLEAR
id: aba8967f-6613-47a8-87d1-e5d7aae31e9b
status: test
description: Detects ToolShell CVE-2025-53770 Exploitation of SharePoint servers.
Previous related CVEs are CVE-2025-49706 and CVE-2025-49704. CVE-2025-53770 is new
and stealthy webshell called SharpyShell, that extracts and leaks cryptographic
secrets from the SharePoint server using a simple GET request.
references:
    -
https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-expl
oitation-sharepoint-vulnerability-cve-2025-53770
    - https://research.eye.security/sharepoint-under-siege/
    - https://x.com/codewhitesec/status/1944743478350557232/photo/1
    - 251132.r1
author: CISA Code & Media Analysis
date: 2025-07-21
modified: 2025-07-22
tags:
    - cve.2025.53770
logsource:
    product: cma
detection:
    keywords:
        - '92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514'

        - '107.191.58.76'
        - '104.238.159.149'
        - '96.9.125.147'
        -
'Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0
/_layouts/SignOut.aspx'
        - '-EncodedCommand JABiAGEAcwBlADYANABTAHQAcgBpAG4AZwAgAD0'
        - 'TEMPLATE\LAYOUTS\spinstall0.aspx'
        - '/_layouts/15/ToolPane.aspx DisplayMode=Edit'
        - '/_layouts/15/spinstall0.aspx'
        - 'spinstall'
```

```
    - 'yoserial'

keywords_1:
    - 'POST'
    - 'GET'
keywords_2:
    - '/_layouts/15/ToolPane.aspx'
keywords_3:
    - 'DisplayMode=Edit'

keywords_4:
    - 'POST'
    - 'GET'
    - 'curl'
keywords_5:
    - '/_layouts/'
    - 'layouts'
keywords_6:
    - 'ToolPane.aspx'
    - 'SignOut.aspx'
    - 'spinstall'
    - 'info3.aspx'

keywords_7:
    - 'HTTP'
keywords_8:
    - 'X-TXT-NET'

keywords_9:
    - '.exe'
keywords_10:
    - '-ap'
keywords_11:
    - 'SharePoint'
keywords_12:
    - '8080'
keywords_13:
    - '.dll'
keywords_14:
    - 'pipe'
keywords_15:
    - 'inetpub'
keywords_16:
    - 'config'

keywords_17:
    - 'ysoserial'
keywords_18:
    - 'ViewState'
keywords_19:
```

```
        - 'TypeConfuseDelegate'
    keywords_20:
        - 'powershell'
    keywords_21:
        - '-EncodedCommand'

    keywords_22:
        - 'BiAGEAcwBlADYANABTAHQAcgBpAG4AZwAgAD0'
        - 'base64String='
    keywords_23:
        - 'BkAGUAYwBvAGQAZQBk'
        - 'decoded'
    keywords_24:
        - 'BGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBn'
        - 'FromBase64String'
    keywords_25:
        - 'cwBwAGkAbgBzAHQAYQBsAGwAMAAuAGEAcwBwAHg'
        - 'AuAGEAcwBwAHg'
        - 'spinstall0.aspx'
        - '.aspx'

    keywords_26:
        - 'V3JpdGUoY2cuVm'
    keywords_27:
        - 'bisifCIrY2cuRG'
    keywords_28:
        - 'mFsaW'


    condition: keywords or keywords_1 and keywords_2 and keywords_3 or keywords_4
and keywords_5 and keywords_6 or keywords_7 and keywords_8 or keywords_9 and
keywords_10 and keywords_11 and keywords_12 and keywords_13 and keywords_14 and
keywords_15 and keywords_16 or keywords_17 and keywords_18 and keywords_19 and
keywords_20 and keywords_21 or keywords_22 and keywords_23 and keywords_24 and
keywords_25 or keywords_26 and keywords_27 and keywords_28

falsepositives:
    - Rate of FP 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
```