BỘ CÔNG AN
**CÔNG AN TỈNH QUẢNG NGÃI**

Số: 851/CAT-ANM

V/v cảnh báo chiến dịch tấn công mạng lợi dụng lỗ hổng bảo mật Microsoft SharePoint CVE-2025-53770

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

*Quảng Ngãi, ngày 29 tháng 7 năm 2025*

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Cục Thi hành án dân sự tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Tòa án nhân dân tỉnh;
- Cục Thống kê tỉnh; Bảo hiểm xã hội tỉnh; Cục Thuế tỉnh;
- Kho bạc Nhà nước tỉnh; Cảng vụ Hàng hải tỉnh;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- UBND các xã, phường, đặc khu;
- Trường Đại học Phạm Văn Đồng, Cao đẳng Cộng đồng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Công ty CP Lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi; Điện lực Quảng Ngãi.

Qua công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao phát hiện chiến dịch tấn công mạng lợi dụng lỗ hổng bảo mật Microsoft SharePoint CVE-2025-53770 vào hệ thống thông tin của các cơ quan Đảng, Nhà nước; ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn. Lỗ hổng bảo mật CVE-2025-53770 tồn tại trên sản phẩm Microsoft SharePoint On-premises, cho phép đối tượng tấn công thực thi mã từ xa. Đặc biệt, lỗ hổng này có thể đã, đang và sẽ được các nhóm tấn công có chủ đích (APT) sử dụng để khai thác diện rộng trong thời gian này *(có Phục lục kèm theo)*.

- Thông tin cụ thể về lỗ hổng như sau:

+ Điểm CVSS: 9.8/10; Mức độ: Rất nghiêm trọng;

+ Lỗ hổng khai thác lỗi bỏ qua xác thực được kích hoạt bằng cách đặt header "Referer" thành "/_layouts/SignOut.aspx"". Sau đó được khai thác để kích hoạt thực thi mã từ xa thông qua webshell "/_layouts/15/ToolPane.aspx".

+ Lỗ hổng ảnh hưởng đến các phiên bản Microsoft SharePoint Server 2019 và Microsoft SharePoint Enterprise Server 2016.

- Biện pháp khắc phục lỗ hổng là cập nhật các bản vá (Bản vá bảo mật do Microsoft: https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-

sharepoint-vulnerability-cve-2025-53770/) hoặc sử dụng các biện pháp giảm thiểu nguy cơ tấn công.

Nhằm bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin của các cơ quan Đảng, Nhà nước, tổ chức, doanh nghiệp trên địa bàn tỉnh, Công an tỉnh đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện:

**1.** Kiểm tra, rà soát và xác định máy chủ sử dụng phiên bản SharePoint có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft.

**2.** Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo kịp thời của các cơ quan chức năng và các tổ chức lớn về an ninh mạng để phát hiện kịp thời các nguy cơ tấn công mạng.

**3.** Trong trường hợp phát hiện dấu hiệu tấn công mạng khai thác lỗ hổng bảo mật trên, đề nghị các đơn vị liên hệ đầu mối Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, điện thoại: 0888.309.485, thư điện tử: anm-ca@quangngai.gov.vn) để báo cáo sự cố và được hướng dẫn hỗ trợ./.

***Nơi nhận:***
- Như trên;
- UBND tỉnh (báo cáo);
- Giám đốc CA tỉnh;
- Phòng Tham mưu;
- Lưu: VT, ANM.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

**Đại tá Võ Văn Dương**

# PHỤC LỤC
# CẢNH BÁO CHIẾN DỊCH TẤN CÔNG LỢI DỤNG LỖ HỔNG TRÊN SHAREPOINT VỚI MÃ ĐỊNH DANH CVE-2025-53770

*(Kèm theo Công văn số 851/CAT-ANM ngày 29/7/2025 của Công an tỉnh)*

**Tài liệu lưu hành nội bộ**

## I. GIỚI THIỆU VỀ LỖ HỔNG CVE-2025-53770 VÀ CHIẾN DỊCH TẤN CÔNG THỰC TẾ

### 1.1. Giới thiệu về lỗ hổng CVE-2025-53770

Vừa qua, Microsoft đã phát hành cảnh báo khẩn cấp về một lỗ hổng bảo mật nghiêm trọng trên các máy chủ **Microsoft SharePoint on-premises**, với mã định danh **CVE-2025-53770**. Đây là một lỗ hổng **zero-day**, đã bị khai thác tích cực ngoài thực tế từ ngày **18/7/2025** và có mức độ nghiêm trọng **CVSS 9.8**, cho phép thực thi mã từ xa mà không cần xác thực (unauthenticated RCE).

Các phiên bản bị ảnh hưởng bao gồm:

+ SharePoint Server 2016
+ SharePoint Server 2019
+ SharePoint Subscription Edition

Trong khi đó, **SharePoint Online trên nền tảng Microsoft 365 không bị ảnh hưởng** bởi lỗ hổng này.

**CVE-2025-53770** được phát hiện là một biến thể của hai lỗ hổng trước đó là **CVE-2025-49704** và **CVE-2025-49706**, vốn đã được Microsoft vá trước đó. Tuy nhiên, **kẻ tấn công đã tìm ra cách bypass các bản vá này**, kết hợp với một lỗ hổng bypass xác thực mới (**CVE-2025-53771**) để thực hiện tấn công không cần đăng nhập và chiếm toàn quyền kiểm soát hệ thống.

Tại trung tâm của chuỗi tấn công là endpoint:

```
/_layouts/15/ToolPane.aspx?DisplayMode=Edit
```

Kẻ tấn công gửi **HTTP POST request** đến endpoint này, **spoof (giả mạo) header Referer** để nó trỏ đến */SignOut.aspx* — một trang đăng xuất hợp pháp trong SharePoint. Bằng cách này, SharePoint **tin rằng yêu cầu là hợp lệ và bỏ qua bước xác thực**, cho phép upload file độc hại lên hệ thống.

### 1.2. Chiến dịch tấn công thực tế

- Theo thông tin từ **Microsoft Threat Intelligence** (2025-07-24), các lỗ hổng được nhóm **APT Storm-2603** khai thác trong chiến dịch này là:

+ **CVE-2025-49706** - Spoofing vulnerability;

+ **CVE-2025-49704** - Remote Code Execution vulnerability;

+ **CVE-2025-53770** - Zero-day bypass lỗ hổng cũ, cho phép thực hiện deserialization tấn công không cần xác thực.

- Chiến dịch được cho là bắt đầu từ **ngày 7 tháng 7 năm 2025**, với sự tham gia của các nhóm APT có nguồn gốc từ Trung Quốc, bao gồm:

+ **Storm-2603**: tập trung vào mã độc tống tiền (ransomware), từng triển khai **Warlock** và **Lockbit** trong các chiến dịch trước.

+ **Linen Typhoon** và **Violet Typhoon**: tập trung vào gián điệp và đánh cắp thông tin.

Trong chiến dịch hiện tại, **Storm-2603** đã thực hiện chuỗi tấn công như sau:

+ Khai thác lỗ hổng trên các máy chủ **SharePoint on-premise** để giành quyền truy cập ban đầu.

+ Vô hiệu hóa **Microsoft Defender** bằng chỉnh sửa registry.

+ Cài đặt webshell, tạo scheduled task, và tải các **.NET assembly** độc hại để duy trì quyền kiểm soát.

+ Trích xuất **mật khẩu plaintext** từ bộ nhớ LSASS bằng **Mimikatz**.

+ Di chuyển ngang qua hệ thống bằng **PsExec**, **Impacket** và **WMI**.

+ Chỉnh sửa **Group Policy Objects (GPO)** để triển khai **ransomware Warlock** trên toàn hệ thống.


Theo ghi nhận từ Trung tâm SANS Internet Storm, có hơn 100 đường dẫn đến webshell đang bị quét - cho thấy lỗ hổng đang bị khai thác hàng loạt trên Internet.

## II. DẤU HIỆU NHẬN DIỆN VÀ CÔNG CỤ RÀ QUÉT

### 2.1. Dấu hiệu nhận diện

Trong quá trình giám sát, phản ứng sự cố kết hợp với tình báo an ninh mạng, đơn vị giám sát an ninh mạng của A05 quốc tế đã phát hiện những chuỗi truy cập bất thường vào máy chủ SharePoint. Điểm chung của các yêu cầu HTTP này là thiếu trường cs-username trong log IIS - một dấu hiệu cho thấy có truy cập trái phép từ người dùng chưa xác thực.

Ví dụ về chuỗi log IIS ghi nhận:

| |
|---|
| 2025-07-17 18:xx:15 POST /_layouts/15/ToolPane.aspx DisplayMode=Edit&a=/ToolPane.aspx 443 - Mozilla Firefox /_layouts/SignOut.aspx 302 |
| 2025-07-18 17:xx:16 GET /_layouts/15/spinstall0.aspx - 443 - Mozilla Firefox /_layouts/SignOut.aspx 200 |

Trong đó, tệp *ToolPane.aspx* được khai thác để tải payload độc hại, sau đó *spinstall0.aspx* - một webshell - được truy cập nhằm kiểm soát hệ thống từ xa.

Webshell có tên **spinstall0.aspx** được ghi nhận đã được upload thành công vào thư mục mặc định của SharePoint:

| |
|---|
| C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\spinstall0.aspx |

Thông tin về mã độc:

- **SHA256 hash**: 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
- **Chức năng chính**:
  - Đọc và đánh cắp **machine keys** (ValidationKey và DecryptionKey) trong cấu hình ASP.NET.
  - Tạo ViewState giả mạo để **thực hiện RCE (Remote Code Execution)** mà không cần xác thực.
  - Thiết lập **persistency** bằng cách tải .NET assemblies độc hại và tạo scheduled task.

Kết hợp với các nguồn dữ liệu từ cộng đồng và kiểm tra, đánh giá trong quá trình giám sát, đơn vị giám sát an ninh mạng đề xuất một số tập luật theo chuẩn định dạng Sigma rule, triển khai trên hệ thống giám sát an ninh mạng như SIEM, EDR, XDR… như sau:

```
title: Potential SharePoint ToolShell CVE-2025-53770 Exploitation - File Create
id: ba479447-721f-42a9-9af2-6dcd517bbdb3
status: experimental
description: |
  Detects the creation of file such as spinstall0.aspx which may indicate successful exploitation of CVE-2025-53770.
  CVE-2025-53770 is a zero-day vulnerability in SharePoint that allows remote code execution.
references:
  - https://research.eye.security/sharepoint-under-siege/
  - https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-
```

```
vulnerability-cve-2025-53770/
author: Swachchhanda Shrawan Poudel (Nextron Systems)
date: 2025-07-21
tags:
    - attack.initial-access
    - attack.t1190
    - cve.2025-53770
    - detection.emerging-threats
logsource:
    product: windows
    category: file_event
detection:
    selection:
        TargetFilename|endswith: '\spinstall0.aspx'
    condition: selection
falsepositives:
    - Unknown
level: critical
```

```
title: Potential SharePoint ToolShell CVE-2025-53770 Exploitation Indicators
id: 7477881c-ec3b-49d6-aced-7255944e5c59
status: experimental
description: |
    Detects potential exploitation of CVE-2025-53770 by identifying indicators such as suspicious command lines discovered in Post-Exploitation activities.
    CVE-2025-53770 is a zero-day vulnerability in SharePoint that allows remote code execution.
references:
    - https://research.eye.security/sharepoint-under-siege/
    - https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
author: Swachchhanda Shrawan Poudel (Nextron Systems)
date: 2025-07-21
tags:
    - attack.initial-access
    - attack.t1190
    - cve.2025-53770
    - detection.emerging-threats
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        ParentImage|endswith: '\w3wp.exe'
    selection_encoded_aspx:
        - CommandLine|wide|base64offset|contains: 'spinstall0.aspx'
        - CommandLine|base64|contains: 'spinstall0.aspx'
    selection_encoded_path:
```

```
        CommandLine|wide|base64offset|contains:
            -
':\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS'
            -
':\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS'
            - ':\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\15\TEMPLATE\LAYOUTS'
            - ':\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\16\TEMPLATE\LAYOUTS'
    selection_ioc:
        CommandLine|contains:
            - '-EncodedCommand
JABiAGEAcwBlADYANABTAHQAcgBpAG4AZwAgAD0'
            - 'TEMPLATE\LAYOUTS\spinstall0.aspx'
    condition: (selection_img and 1 of selection_encoded_*) or selection_ioc
falsepositives:
    - Unknown
level: high
```

```
title: SharePoint ToolShell CVE-2025-53770 Exploitation - Web IIS
id: 48d053db-6a56-4866-b60d-0975647050ed
status: experimental
description: |
    Detects access to vulnerable SharePoint components potentially being exploited in
CVE-2025-53770 through IIS web server logs.
    CVE-2025-5370 is a zero-day vulnerability in SharePoint that allows remote code
execution.
references:
    - https://www.linkedin.com/posts/mauricefielenbach_sharepoint-incidentresponse-
windowssecurity-activity-7352653907363303425-bL2f
    - https://research.eye.security/sharepoint-under-siege/
    - https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-
vulnerability-cve-2025-53770/
author: Swachchhanda Shrawan Poudel (Nextron Systems)
date: 2025-07-21
tags:
    - attack.initial-access
    - attack.t1190
    - cve.2025-53770
    - detection.emerging-threats
logsource:
    category: webserver # IIS web server logs
detection:
    selection_exploit_post:
        cs-method: 'POST'
        cs-uri-stem|contains: '/_layouts/15/ToolPane.aspx'
        cs-uri-query|contains: 'DisplayMode=Edit&a=/ToolPane.aspx'
    selection_exploit_get:
```

```
      cs-method: 'GET'
      cs-uri-stem|contains: '/_layouts/15/spinstall0.aspx'
   selection_referer:
      cs-referer|contains: '/_layouts/SignOut.aspx'
   condition: 1 of selection_exploit_* and selection_referer
falsepositives:
   - Unknown
level: medium
```

Ngoài ra các tổ chức có thể sử dụng một số truy vấn phát hiện có thể sử dụng trực tiếp trên các hệ thống giám sát an ninh mạng phổ biến như Splunk, Elastic Stack như sau:

***Truy vấn trên Splunk***

```
index=iis source="*iis*"
| search cs_method="POST" cs_uri_stem="/_layouts/15/ToolPane.aspx" cs_uri_query="DisplayMode=Edit&a=/ToolPane.aspx"
| eval payload_size=tonumber(cs_bytes)
| where payload_size > 7000
| search cs_User_Agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0"
| stats count by src_ip, cs_uri_stem, payload_size
| sort -payload_size
```

```
index=iis
| search cs_method="POST" AND cs_uri_stem="/_layouts/15/ToolPane.aspx"
| where cs_bytes > 7000 AND cs_bytes < 10000
| search cs_Referer="/_layouts/SignOut.aspx"
| eval attack_pattern=if(like(cs_User_Agent, "%Windows NT 10.0; Win64; x64; rv:120.0%"), "CVE-2025-53770", "Other")
| where attack_pattern="CVE-2025-53770"
| table _time, src_ip, cs_uri_query, cs_bytes, sc_status
```

***Truy vấn trên Elastic Stack***

```
{
 "query": {
  "bool": {
   "must": [
     {"term": {"http.request.method": "POST"}},
     {"term": {"url.path": "/_layouts/15/ToolPane.aspx"}},
     {"term": {"url.query": "DisplayMode=Edit&a=/ToolPane.aspx"}},
     {"range": {"http.request.bytes": {"gte": 7000, "lte": 10000}}},
     {"term": {"user_agent.original": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0"}},
     {"term": {"http.request.referrer": "/_layouts/SignOut.aspx"}}
   ]}}
}
```

### 2.2. Công cụ rà quét

Công cụ được tác giả ZehprFish phát triển nhằm hỗ trợ đội ngũ giám sát an ninh mạng trong việc kiểm tra tự động các hệ thống SharePoint bằng cách gửi các truy vấn POST được thiết kế sẵn chứa mã khai thác. Quá trình quét tập trung vào việc phát hiện dấu hiệu rò rỉ thông tin khóa máy (machine key), gồm các trường ValidationKey, DecryptionKey, và CompatibilityMode – những thành phần bảo mật cốt lõi trong việc mã hóa và xác thực của ASP.NET. Khi máy chủ trả về chuỗi chứa các giá trị này theo định dạng phân tách bằng ký tự |, đây là bằng chứng rõ ràng cho thấy hệ thống đã bị khai thác.

Ngoài ra, scanner còn có khả năng phát hiện payload thứ cấp như file spinstall0.aspx. Scanner cũng xác định các chỉ số tấn công (IOC) như payload dạng nén base64, mẫu mã độc ASP.NET viết bằng C#, hoặc các header bất thường như User-Agent và Content-Length. Mỗi phát hiện được phân loại theo mức độ tin cậy từ **LOW**, **MEDIUM**, **HIGH** đến **CRITICAL**, với cảnh báo ngay lập tức nếu hệ thống bị lộ khóa mã hóa.

Các bước triển khai công cụ như sau, công cụ được triển khai trên một máy chủ Linux trong cùng dải mạng với máy chủ SharePoint hoặc được mở rule trên Firewall để có thể kết nối đến từ dải mạng khác trong hệ thống. Giả sử tổ chức đang sử dụng máy Ubuntu mới cài đặt (ví dụ Ubuntu 22.04 hoặc 24.04 LTS), các bước sau sẽ hướng dẫn người quản trị hoặc đội ngũ giám sát an ninh mạng của tổ chức thiết lập từ đầu.

- Bước 1: Cập nhật hệ thống

```
sudo apt update && sudo apt upgrade -y
```

- Bước 2: Cài đặt Python3 và pip

```
sudo apt install python3 python3-pip -y
python3 --version
pip3 --version
```

- Bước 3: Cài đặt Git để clone mã nguồn

```
sudo apt install git -y
```

- Bước 4: Clone công cụ từ GitHub

```
git clone https://github.com/ZephrFish/CVE-2025-53770-Scanner
cd CVE-2025-53770-Scanner
```

- Bước 5: Cài đặt các công cụ phụ thuộc

```
pip3 install -r requirements.txt
```

- Bước 6: Tạo tập tin danh sách máy chủ SharePoint cần thiết

```
nano hosts.txt
sharepoint1.example.com
192.168.56.101
internal-sharepoint.local
```

- Bước 7: Triển khai công cụ rà quét

| |
|---|
| chmod +x scanner.py |
| Rà quét cơ bản: |
| python3 scanner.py -i hosts.txt |
| Rà quét nâng cao (đa luồng, lưu log và kết quả): |
| python3 scanner.py -i hosts.txt -o results.json -l scan.log -t 20 -v |

- Bước 8: Xem kết quả rà quét

| |
|---|
| cat results.json \| jq |

## III. KHUYẾN NGHỊ VÀ KHẮC PHỤC

Để ứng phó với tình trạng khai thác lỗ hổng đang diễn ra trên các máy chủ SharePoint on-premises, tổ chức cần thực hiện một loạt biện pháp phòng thủ chủ động và xử lý sự cố khẩn cấp. Trước hết, nếu hệ thống SharePoint chưa được cập nhật bản vá mới nhất từ Microsoft, nên giả định rằng hệ thống đã bị xâm nhập. Các dấu hiệu tấn công bao gồm truy cập đáng ngờ đến đường dẫn */ToolPane.aspx*, đặc biệt là các yêu cầu HTTP POST đến */layouts/15/ToolPane.aspx?DisplayMode=Edit* có chứa tiêu đề Referer: */SignOut.aspx*. Ngoài ra, cần kiểm tra thư mục layouts trên máy chủ SharePoint để phát hiện các file .aspx bất thường, chẳng hạn như ***spinstall0.aspx***, vì đây là dấu hiệu phổ biến của web shell được triển khai sau khai thác. Cũng cần lưu ý đến các hành vi bất thường như tiến trình IIS (w3wp.exe) gọi shell PowerShell hoặc CMD.

Các tổ chức nên rà soát nhật ký mạng và SIEM để tìm kết nối đến các địa chỉ IP độc hại đã được ghi nhận, bao gồm *107.191.58[.]76, 104.238.159[.]149* và *96.9.125[.]147*, đặc biệt trong khung thời gian từ ngày 17 đến 21 tháng 7 năm 2025. Ngoài ra, cần theo dõi các hoạt động bất thường liên quan đến */layouts/SignOut.aspx*, vì các attacker đang sử dụng kỹ thuật spoofing để khai thác từ trang này.

Trong trường hợp chưa phát hiện dấu hiệu xâm nhập, các biện pháp chủ động cần thực hiện ngay bao gồm: áp dụng bản vá bảo mật mới nhất từ Microsoft cho các phiên bản SharePoint Server Subscription Edition và 2019 (lưu ý rằng bản vá cho 2016 vẫn đang chờ cập nhật). Cần bật chức năng AMSI (Antimalware Scan Interface) cho SharePoint và đảm bảo rằng máy chủ đang sử dụng Microsoft Defender hoặc phần mềm antivirus tương thích. Trong trường hợp không thể kích hoạt AMSI, các máy chủ SharePoint cần được tách ra khỏi môi trường internet cho đến khi có bản vá hoặc phương án khắc phục chính thức.

Một bước quan trọng không thể bỏ qua là xoay vòng lại các khóa máy (machine key), bao gồm ValidationKey và DecryptionKey, vốn được dùng để ký và mã hóa ViewState. Nếu attacker đã đánh cắp các khóa này, họ có thể tiếp tục truy cập hệ thống ngay cả sau khi đã vá lỗ hổng. Theo khuyến nghị của CISA và

Microsoft, việc xoay khóa cần được thực hiện trước và sau khi áp dụng bản vá, sau đó khởi động lại dịch vụ IIS.

Bên cạnh đó, các tổ chức cần kiểm tra và thay đổi mật khẩu tài khoản dịch vụ, đồng thời rà soát các tài khoản quản trị viên mới được tạo ra hoặc có hành vi đáng ngờ. Thực hiện các đợt threat hunting bằng EDR để phát hiện hành vi khai thác và phần mềm độc hại như webshell hoặc DLL tải về hệ thống. Đặc biệt, các mã độc dưới dạng DLL thường khó phát hiện hơn so với các file .aspx thông thường.

Tổ chức cũng cần đảm bảo hệ thống sao lưu đang hoạt động ổn định và nhật ký đủ dài để truy vết, tối thiểu từ ngày 17 tháng 7. Các máy chủ SharePoint đã hết vòng đời (EOL) như phiên bản 2013 hoặc cũ hơn cần được ngắt khỏi internet hoặc loại bỏ khỏi hệ thống. Đồng thời, cần cập nhật hệ thống ngăn chặn xâm nhập (IPS), tường lửa ứng dụng web (WAF) để chặn các mẫu khai thác tương ứng, và triển khai đầy đủ các chính sách logging theo hướng dẫn của CISA.

Cuối cùng, để giảm thiểu khả năng bị ransomware hoặc tái xâm nhập, tổ chức nên tiến hành kiểm tra toàn diện về cấu hình quyền truy cập, tối giản hóa phân quyền layout và quyền quản trị, thực hiện bảo vệ nhiều lớp và áp dụng các thực hành bảo mật tiên tiến, bao gồm hướng dẫn #StopRansomware từ CISA.

## IV. DANH SÁCH INDICATOR OF COMPROMISE (IOC)

| IoC | Mô tả |
|---|---|
| 107.191.58[.]76 | Nguồn IP khai thác |
| 104.238.159[.]149 | Nguồn IP khai thác |
| 96.9.125[.]147 | Nguồn IP khai thác |
| 139.144.199[.]41 | Nguồn IP khai thác |
| 89.46.223[.]88 | Nguồn IP khai thác |
| 45.77.155[.]170 | Nguồn IP khai thác |
| 154.223.19[.]106 | Nguồn IP khai thác |
| 185.197.248[.]131 | Nguồn IP khai thác |
| 149.40.50[.]15 | Nguồn IP khai thác |
| 64.176.50[.]109 | Nguồn IP khai thác |
| 149.28.124[.]70 | Nguồn IP khai thác |
| 206.166.251[.]228 | Nguồn IP khai thác |
| 95.179.158[.]42 | Nguồn IP khai thác |
| 86.48.9[.]38 | Nguồn IP khai thác |
| 128.199.240[.]182 | Nguồn IP khai thác |
| 212.125.27[.]102 | Nguồn IP khai thác |
| 91.132.95[.]60 | Nguồn IP khai thác |
| C:\PROGRA~1\COMMON~1\MICROS~1\ WEBSER~1\16\TEMPLATE\LAYOUTS\ spinstall0.aspx | Tập tin được tạo ra sau khi các câu lệnh mã hóa được thực thi |

| IoC | Mô tả |
|---|---|
| C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\ debug_dev.js | Tập tin được tạo ra sau khi các câu lệnh mã hóa được thực thi |
| 4A02A72AEDC3356D8CB38F01F0E0B9 F26DDC5CCB7C0F04A561337CF24AA84030 | .NET module hash |
| B39C14BECB62AEB55DF7FD55C814AF BB0D659687D947D917512FE67973100B70 | .NET module hash |
| 390665BDD93A656F48C463BB6C11A4D45B7 D5444BDD1D1F7A5879B0F6F9AAC7E | .NET module hash |
| 66AF332CE5F93CE21D2FE408DFFD49D4AE3 1E364D6802FFF97D95ED593FF3082 | .NET module hash |
| 7BAF220EB89F2A216FCB2D0E9AA021B2A10 324F0641CAF8B7A9088E4E45BEC95 | .NET module hash |