NCSC VN
National Cyber Security Center

## Trung tâm Giám sát an toàn không gian mạng quốc gia

# CẢNH BÁO TUẦN

**Số 04 (20/01/2025 – 26/01/2025)**

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT PlushDaemon nhằm vào nhà cung cấp VPN của Hàn Quốc trong chiến dịch tấn công gây ảnh hưởng tới chuỗi cung ứng.

- **Cảnh báo:** Cisco vá lỗ hổng leo thang đặc quyền tồn tại trên giải pháp Meeting Management.

## 2. Điểm yếu, lỗ hổng

- TOP **10** lỗ hổng đáng chú ý trong tuần.

## 3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 5.367** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

## 4. Tài liệu lưu trữ

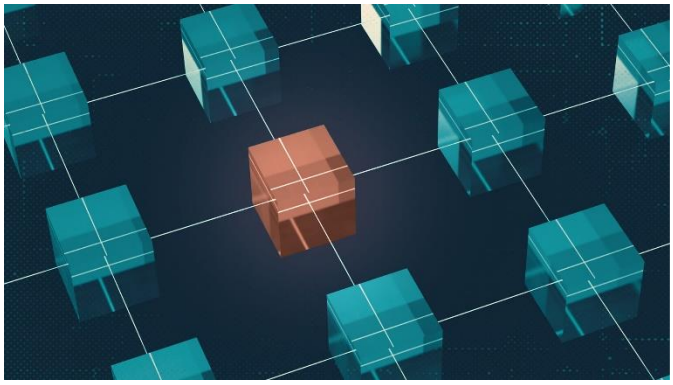
Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Chiến dịch tấn công APT: Nhóm APT PlushDaemon nhằm vào nhà cung cấp VPN của Hàn Quốc trong chiến dịch tấn công gây ảnh hưởng tới chuỗi cung ứng"



Gần đây, các chuyên gia đã bảo mật đã ghi nhận nhóm APT có nguồn gốc từ Trung Quốc với tên PlushDaemon đã được gán với chiến dịch tấn công nhằm vào chuỗi cung ứng nhằm vào nhà cung cấp VPN của Hàn Quốc kể từ năm 2023.

Chiến dịch tấn công diễn ra với việc nhóm APT này thay thế bộ cài chính thống của hãng bằng bộ cài gài mã độc có chức năng triển khai mã độc SlowStepper, đây là một backdoor có nhiều chức năng cùng với hơn 30 thành phần được thích hợp. Nhóm APT PlushDaemon là một nhóm tấn công có nguồn gốc Trung Quốc đã đi vào hoạt động kể từ năm 2019 nhằm vào các tổ chức, cá nhân tại Trung Quốc, Đài Loan, Hồng Kông, Hàn Quốc, Mỹ và New Zealand.

Điểm đáng chú ý của nhóm này là việc sử dụng mã độc SlowStepper, được mô tả là một bộ toolkit lớn với hơn 30 module được lập trình sử dụng ngôn ngữ C++, Python và Go. Một điểm khác của chiến dịch tấn công lần này của nhóm là việc chiếm dụng các kênh cập nhật phần mềm chính thống cũng hãng VPN, khai thác lỗ hổng tồn tại trên máy chủ web để xâm nhập vào hệ thống mục tiêu.

Phiên bản độc hại của bộ cài, hiện đã được gỡ bỏ khỏi website của hãng VPN bị ảnh hưởng, có chức năng phát tán mã độc SlowStepper cùng với phần mềm chính thống. Hiện chưa rõ chính xác mục tiêu trích xuất thông tin của hình thức tấn công chuỗi cung ứng này là gì, tuy nhiên các tổ chức, cá nhân tải xuống file .ZIP này đều đứng trước nguy cơ bị ảnh hưởng. Dữ liệu Telemetry được thu thập bởi ESET cho thấy có nhiều người dùng đã cố cài đặt phiên bản độc hại của phần mềm thuộc một công ty bán dẫn và một công ty phát triển phần mềm tại Hàn Quốc

Nguồn: https://thehackernews.com/2025/01/plushdaemon-apt-targets-south-korean.html?&web_view=true

# Tin tức An toàn thông tin

## "Chiến dịch tấn công APT: Nhóm APT PlushDaemon nhằm vào nhà cung cấp VPN của Hàn Quốc trong chiến dịch tấn công gây ảnh hưởng tới chuỗi cung ứng"

Dữ liệu Telemetry được thu thập bởi ESET cho thấy có nhiều người dùng đã cố cài đặt phiên bản độc hại của phần mềm thuộc một công ty bán dẫn và một công ty phát triển phần mềm tại Hàn Quốc.

Chuỗi tấn công của chiến dịch này bắt đầu bắt việc thực thi bộ cài "IPanyVPNsetup.exe", sau đó sẽ thiết lập kết nối duy trì trên hệ thống giữa các lần khởi động lại và thực thi loader "AutoMsg.dll" có chức năng thực thi shellcode nạp vào hệ thống DLL "EncMgr.pkg". DLL này sẽ trích xuất ra hai file có tác dụng nạp vào DLL độc hại "lregdll.dll" có tên PerfWatson.exe.

Mục tiêu cuối của quá trình này là để triển khai mã độc SlowStepper từ file winlogin.gif tồn tại trên file FeatureFlag.pkg. Mã độc này có sử dùng nhiều công cụ khác nhau được viết bởi ngôn ngữ Python và Go cho phép thu thập dữ liệu và che giấu hành vi giám sát thông qua việc ghi âm và video.

Các thông tin được nhóm tấn công này nhằm tới gồm có:

- Trình duyệt web: dữ liệu lưu trên trình duyệt Google Chrome, Microsoft Edge, Cốc Cốc, Firefox,…
- Camera hệ thống, thiết bị.
- Các file văn bản (.txt, .doc, .docx, .xls,…)
- Các ứng dụng nhắn tin như DingTalk, Telegram, WeChat.
- Các thông tin liên quan tới mạng wifi.

Tính phức tạp của nhóm tấn công còn được thể hiện thông qua sự đa dạng trong chuỗi tấn công sử dụng bởi nhóm này, vượt ra khỏi phạm vi gây ảnh hưởng tới chuỗi cung ứng hay khai thác lỗ hổng web để triển khai hình thức tấn công adversary-in-the-middle (AitM) cho truy cập đầu vào. Điều này được thực hiện thông qua việc chiếm dụng cơ chế cập nhật phần mềm của các ứng dụng sau khi chiếm dụng DNS mức router.

**Một số IoC được ghi nhận:**

| | |
|---|---|
| 202.189.8[.]72 | 47.96.17[.]237 |
| 47.74.159[.]166 | 8.130.87[.]195 |
| 47.113.200[.]18 | 47.104.138[.]190 |
| 202.189.8[.]87 | 202.189.8[.]69 |
| 47.92.6[.]64 | reverse.wcsset[.]com |
| 7051.gsm.360safe[.]company | st.360safe[.]company |
| 202.105.1[.]187 | 202.189.8[.]193 |
| 47.108.162[.]218 | agt.wcsset[.]com |
| 120.24.193[.]58 | 202.105.1[.]187 |

Nguồn: https://thehackernews.com/2025/01/plushdaemon-apt-targets-south-korean.html?&web_view=true

# Tin tức An toàn thông tin

## "Cảnh báo: Cisco vá lỗ hổng leo thang đặc quyền tồn tại trên giải pháp Meeting Management"


Gần đây, Cisco đã phát hành bản vá cho lỗ hổng an toàn thông tin mức nghiêm trọng tồn tại trên Meeting Management, cho phép đối tượng tấn công sau khi khai thác thành công có thể đạt được quyền quản trị trên các phiên làm việc bị ảnh hưởng.

Lỗ hổng có mã định danh CVE-2025-20156 (Điểm CVSS: 9.9) được phân loại là lỗ hổng leo thang đặc quyền trên REST API của giải pháp Cisco Meeting Management. Lỗ hổng này xảy ra do sự thiếu sót trong quá trình ủy quyền cho người dùng REST API.

Ngoài ra, Cisco cũng đã thực hiện vá lỗ cho lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ trên BroadWorks, lỗi này phát sinh do việc xử lý bộ nhớ thiếu bảo mật cho các yêu cầu SIP (CVE-2025-20165, Điểm CVSS: 7.5).

Lỗ hổng thứ ba được vá bởi Cisco có mã CVE-2025-20128 (Điểm CVSS: 5.3), là lỗi integer underflow gây ảnh hưởng tới quy trình giải mã "Object Linking and Embedding 2 (OLE2)" trên ClamAV có thể dẫn tới tấn công từ chối dịch vụ.

Được biết, các lỗ hổng trên đã được hãng Cisco ghi nhận tồn tại mã khai thác, nhưng chưa có chứng cứ nào cho thấy các lỗ hổng này bị khai thác trong môi trường thực tế.

Nguồn: https://thehackernews.com/2025/01/cisco-fixes-critical-privilege.html

# Nguy cơ tấn công mạng từ điểm yếu, lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất **870** lỗ hổng, trong đó có 337 lỗ hổng mức Cao, 400 lỗ hổng mức Trung bình, 20 lỗ hổng mức Thấp và 113 lỗ hổng chưa đánh giá. Trong đó có ít nhất 94 lỗ hổng cho phép chèn và thực thi mã lệnh.

Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm trọng cao hoặc đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của Mitel, Windows và Apple, cụ thể là như sau:

- **CVE-2024-41710 (Điểm CVSS: 6.8 – Cao):** Lỗ hổng tồn tại trên các thiết bị SIP của hãng Mitel cho phép đối tượng tấn công với quyền quản trị có thể thực hiện tấn công argument injection để dẫn tới việc thực thi mã từ xa. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.

- **CVE-2025-21298 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Windows OLE (Object Linking and Embedding) cho phép đối tượng tấn công thực thi mã từ xa. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

- **CVE-2025-24118 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên các thiết bị Apple sử dụng hệ điều hành iPadOS, macOS Sequoia/ Sonoma. Đây là lỗi phát sinh trong quy trình xử lý bộ nhớ cho phép các ứng dụng độc hại gây ra việc sập hệ thống hoặc ghi lên bộ nhớ kernel. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.

# TOP 10 lỗ hổng đáng chú ý trong tuần

| TT | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|
| 1 | CVE-2024-41710 | - Điểm CVSS: 6.8 (Cao)<br>- Ảnh hưởng: Mitel<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2024-41710 |
| 2 | CVE-2025-21298 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Microsoft Windows<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2025-21298 |
| 3 | CVE-2025-24118 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Hệ điều hành iPadOS, macOS Sequoia/ Sonoma<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép.<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2025-24118 |
| 4 | CVE-2024-49138 | - Điểm CVSS: 7.8 (Cao)<br>- Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2024-49138 |
| 5 | CVE-2025-0065 | - Điểm CVSS: 7.8 (Cao)<br>- Ảnh hưởng: TeamViewer<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2025-0065 |

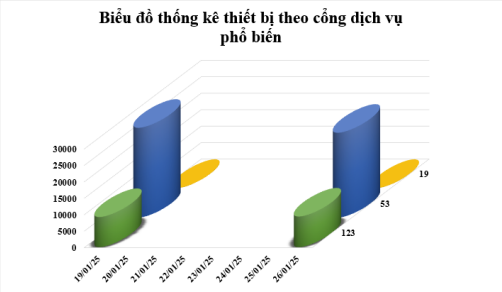
# TOP 10 lỗ hổng đáng chú ý trong tuần

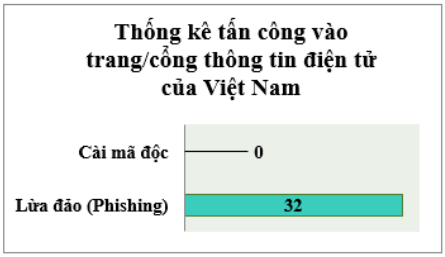
| TT | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|
| 6 | CVE-2024-57727 | - Điểm CVSS: 7.5 (Cao)<br>- Ảnh hưởng: SimpleHelp<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép.<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2024-57727 |
| 7 | CVE-2025-24160 | - Điểm CVSS: 4.3 (Trung bình)<br>- Ảnh hưởng: Hệ điều hành iPadOS, macOS Sequoia/ Sonoma, visionOS, iOS, watchOS, tvOS.<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2025-24160 |
| 8 | CVE-2023-6080 | - Điểm CVSS: 7.8 (Cao)<br>- Ảnh hưởng: Windows<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2023-6080 |
| 9 | CVE-2025-22604 | - Điểm CVSS: 9.1 (Nghiêm trọng)<br>- Ảnh hưởng: Framework Cacti<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2025-22604 |
| 10 | CVE-2025-0411 | - Điểm CVSS: 7.0 (Cao)<br>- Ảnh hưởng: 7-Zip<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2025-0411 |

# Thống kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

## Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **35.155** (giảm so với tuần trước **36.516**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.



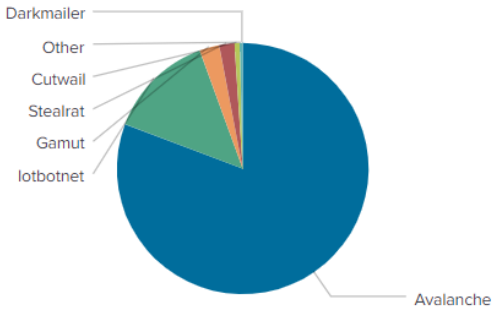




## Tấn công Web

Trong tuần, có **32** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 32 trường hợp tấn công lừa đảo (Phishing), 0 trường hợp tấn công cài cắm mã độc.

## Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.




### Địa chỉ được sử dụng trong các mạng botnet

| | |
|---|---|
| disorderstatus.ru | devicesta.ru |
| differentia.ru | xjpakmdcfuqe.in |
| atomictrivia.ru | c.deltaheavy.ru |
| morphed.ru | cp.wdzbt76z.ru |
| thesecond.in | gbhyze.info |
| cp.f2a4ipk6.ru | xjpakmdcfuqe.com |
| hzmksreiuojy.in | soplifan.ru |
| ygiudewsqhct.in | ydbnsrt.me |
| xjpakmdcfuqe.biz | b.deltaheavy.ru |
| a.deltaheavy.ru | 0-0-0-0-0-0-0-0-0-0-0-0-0-18-0-0-0-0-0-0-0-0-0-0-0-0-0.info |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **5.367** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **222** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **5.145** trường hợp phản ánh cuộc gọi, tin nhắn lừa đảo thông qua tổng đài 156/5656

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

| STT | Website lừa đảo | Ghi chú |
|---|---|---|
| 1 | https://shop[.]amz-dropshipping[.]com/login | Website giả mạo sàn TMĐT Amazon |
| 2 | https://congthongtinanninhmang[.]com/login | Website giả mạo Bộ Công An |
| 3 | cucantoanthongtin24h[.]com | Website giả mạo Cục An toàn thông tin, Bộ Công An |
| 4 | https://cucantoanthongtin24h[.]com/?gad_source=1&gclid=CjwKCAiAtNK8BhBBEiwA8wVt92YtBfS8x3hC-c0d177zwHq9UzT5Or5rkHGyZ4x9PXILbbiCHAYr6BoC-c0QAvD_BwE | Website giả mạo Cục An toàn thông tin, Bộ Công An |
| 5 | https://app[.]ebaynnhd[.]vip | Website giả mạo sàn TMĐT Ebay |
| 6 | zkjvk[.]com | Website giả mạo GOMarket |
| 7 | Https://lazada[.]haozuhua[.]com | Website giả mạo sàn TMĐT Lazada |
| 8 | https://tcb[.]khuyenmaithang-canhan-hotro247-thang01[.]com[.]vn/ | Ngân hàng TMCP Kỹ Thương Việt Nam |
| 9 | vib[.]han-muc-the-ngan-hang[.]com | Ngân hàng TMCP Quốc tế Việt Nam |
| 10 | vpbank[.]hotrodacbiet-khuyenmaithang-hotro247-thang01[.]com[.]vn | Ngân hàng TMCP Việt Nam Thịnh Vượng |
| 11 | https://www[.]shopeesallers[.]com | Website giả mạo sàn TMĐT Shopee |
| 12 | sp6708p[.]com/register | Website giả mạo sàn TMĐT Shopee |
| 13 | https://taoobao-order[.]com | Website giả mạo sàn TMĐT Taobao |
| 14 | http://talegrm[.]king88su[.]xyz/ | Website giả mạo Telegram |
| 15 | tkshopvn[.]vip/2[.]html | Website giả mạo TikTok |
| 16 | https://edu[.]vov[.]vn/ | Website giả mạo Trường Cao đẳng Phát thanh - Truyền hình II, Đài Tiếng nói Việt Nam |
| 17 | http://vienthongviettel[.]vn | Website giả mạo Viettel |
| 18 | vinmarket[.]net | Website giả mạo Vingroup |
| 19 | https://www[.]xmtap2[.]com:443/chat/text/chat_0QRMAF[.]html?l=vi | Website giả mạo VNPost |
| 20 | westernunionnvn9[.]wixsite[.]com/online | Website giả mạo Western Union |

NCSC VN
National Cyber Security Center

# Khuyến nghị đối với các cơ quan, đơn vị

**"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"**

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin tức an toàn thông tin,** Quý đơn vị cần thường xuyên cập nhật thông tin (như các chiến dịch tấn công của các nhóm APT, thông tin IoC kèm theo từng chiến dịch, điểm yếu lỗ hổng đang bị lợi dụng để khai thác,…), rà soát trên các hệ thống thống thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần Lỗ hổng bảo mật, Quý đơn vị cần lưu ý theo dõi và cập nhật bản vá cho các lỗ hổng liên quan đến sản phẩm đang sử dụng. Ngoài ra, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

3. Đối với các nguy cơ về tấn công từ chối dịch vụ, tấn công web trong phần **Thống kê nguy cơ, các cuộc tấn công tại Việt Nam**, Quý đơn vị cần rà soát, hạn chế tối đa việc mở các cổng dịch vụ có thể bị lợi dụng để thực hiện tấn công từ chối dịch vụ; thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và xử lý nguy cơ tấn công. Bên cạnh đó, đối với các IP/tên miền được đề cập trong mục **Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam**, Quý đơn vị cần kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại mà Cục ATTT đã chia sẻ.

***

4. Đối với các website giả mạo thống kê tại mục **Tấn công lừa đảo người dùng Việt Nam**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

024.3209.1616
ncsc@ais.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội