NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 27 (01/07/2024 – 07/07/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Kimsuky sử dụng tiện ích độc hại TRANSLATEXT trên Chrome nhằm đánh cắp dữ liệu người dùng.

- **Cảnh báo:** Lỗ hổng Nghiêm trọng trong CocoaPods gây nguy hiểm đến các ứng dụng iOS và macOS.

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: 1.927** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

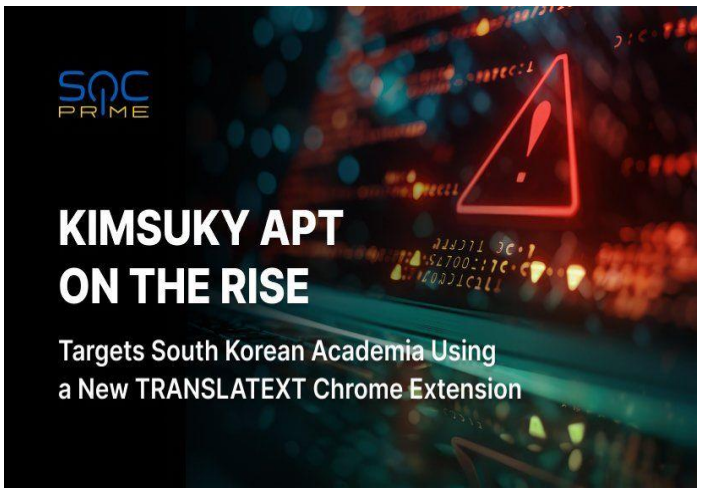
4. Tài liệu lưu trữ

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

https://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Kimsuky sử dụng tiện ích độc hại TRANSLATEXT trên Chrome nhằm đánh cắp dữ liệu người dùng"



Nhóm tấn công APT Kimsuky đã bị phát hiện đang triển khai một tiện ích mở rộng mới trên Google Chrome, có tên là TRANSLATEXT, nhằm mục đích đánh cắp thông tin nhạy cảm.

Tiện ích TRANSLATEXT được phát hiện vào tháng 3 năm 2024, có khả năng thu thập địa chỉ email, tên người dùng, mật khẩu, cookie và chụp ảnh màn hình trình duyệt. Chiến dịch tấn công của nhóm nhằm vào các tổ chức giáo dục tại Hàn Quốc, đặc biệt là những đơn vị nghiên cứu về chính trị Triều Tiên.

Kimsuky là một nhóm APT đến từ Triều Tiên bắt đầu hoạt động từ năm 2012 và là một phần của Lazarus, nổi tiếng với các cuộc tấn công gián điệp mạng và tài chính.

Nhóm này còn được biết đến với nhiều tên gọi khác nhau như APT43, ARCHIPELAGO, Black Banshee, Emerald Sleet, Springtail và Velvet Chollima.

Trong thời gian gần đây, Kimsuky đã khai thác lỗ hổng CVE-2017-11882 trong Microsoft Office để phát tán phần mềm keylogger, sử dụng các mồi nhử liên quan đến tuyển dụng việc làm trong các cuộc tấn công vào lĩnh vực quốc phòng và hàng không vũ trụ.

Kimsuky thường sử dụng spear-phishing và kỹ thuật xâm nhập xã hội để tiếp cận các hệ thống. Chiến dịch thường bắt đầu bằng một tệp ZIP giả danh về lịch sử quân đội Hàn Quốc, chứa các tài liệu bằng chữ Hàn và một tệp thực thi. Khi khởi động, tệp thực thi này sẽ tải xuống một script PowerShell từ máy chủ của đối tượng tấn công để thu thập thông tin từ máy tính nạn nhân và gửi lên GitHub. Đồng thời, tệp thực thi cũng sẽ tải thêm mã PowerShell thông qua tệp shortcut (LNK) của Windows. Quy trình này giúp Kimsuky duy trì và mở rộng quyền kiểm soát trên máy tính nạn nhân một cách kín đáo và hiệu quả.

Nguồn: https://thehackernews.com/2024/06/kimsuky-using-translatext-chrome.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Kimsuky sử dụng tiện ích độc hại TRANSLATEXT trên Chrome nhằm đánh cắp dữ liệu người dùng"

Tài khoản GitHub được sử dụng cho chiến dịch này được tạo vào ngày 13 tháng 2 năm 2024, lưu trữ tiện ích TRANSLATEXT dưới tên "GoogleTranslate.crx", mặc dù phương thức phân phối hiện tại vẫn chưa xác định. TRANSLATEXT đã giả mạo Google Translate và sử dụng mã JavaScript để vượt qua các biện pháp bảo mật của Google, Kakao và Naver; thu thập địa chỉ email, thông tin đăng nhập và cookie; chụp ảnh màn hình trình duyệt và trích xuất dữ liệu bị đánh cắp. Tiện ích này cũng có thể thực hiện các lệnh từ URL Blogger Blogspot để chụp ảnh màn hình các tab mới mở và xóa toàn bộ cookie khỏi trình duyệt.

Mục tiêu chính của nhóm APT Kimsuky là các vị trí quan trọng trong lĩnh vực giáo dục và chính phủ. Việc sử dụng các công cụ như TRANSLATEXT trong các chiến dịch tấn công là minh chứng cho sự tinh vi và khả năng che giấu của nhóm Kimsuky, đồng thời đặt ra thách thức lớn đối với các biện pháp bảo mật hiện tại.

Một số IoC ghi nhận được:

bba3b15bad6b5a80ab9fa9a49b643658
38e27983c757374d9bae36a2e2520e8e
hxxp://sdfa.liveblog365[.]com/ares/hades.txt
hxxp://sdfa.liveblog365[.]com/ares/babyhades.txt
hxxp://ney.r-e[.]kr/mar/tys.txt
hxxp://ney.r-e[.]kr/mar/tys.php
hxxps://webman.w3school.cloudns[.]nz
hxxps://onewithshare.blogspot[.]com/2023/04/10.html
hxxps://raw.githubusercontent[.]com/HelperDav/Web/main/update.xml
hxxps://github[.]com/cmastern

Nguồn: https://thehackernews.com/2024/06/kimsuky-using-translatext-chrome.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng Nghiêm trọng trong CocoaPods gây nguy hiểm đến các ứng dụng iOS và macOS"

Gần đây, ba lỗ hổng an toàn thông tin Nghiêm trọng đã được phát hiện trong trình quản lý phụ thuộc CocoaPods, đây là công cụ phổ biến dành cho các dự án sử dụng ngôn ngữ lập trình Swift và Objective-C. Những lỗ hổng này có thể bị khai thác để thực hiện các cuộc tấn công vào chuỗi cung ứng, ảnh hưởng nghiêm trọng đến toàn bộ người dùng bằng cách chiếm quyền kiểm soát các gói ứng dụng (pod) trong CocoaPods để chèn mã độc hại vào các ứng dụng iOS/macOS.

Lỗ hổng **CVE-2024-38368 (Điểm CVSS: 9.3)** cho phép kẻ tấn công lợi dụng quy trình 'Claim Your Pods' để chiếm quyền kiểm soát các gói ứng dụng (pod) không có người quản lý. Vấn đề này bắt nguồn từ việc di dời máy chủ Trunk vào năm 2014, khiến hàng nghìn gói ứng dụng trở thành không có chủ. Đối tượng tấn công có thể sử dụng API công khai và địa chỉ email được cung cấp trong mã nguồn của CocoaPods ("unclaimed-pods@cocoapods.org") để chiếm quyền kiểm soát các gói ứng dụng này và chèn mã độc hại vào mã nguồn.

Lỗ hổng **CVE-2024-38366 (Điểm CVSS: 10.0)** là lỗ hổng nghiêm trọng nhất, cho phép đối tượng tấn công khai thác quy trình xác thực email không an toàn để thực thi mã tùy ý từ xa trên máy chủ Trunk. Điều này cho phép thay đổi hoặc thay thế các gói ứng dụng mà không cần sự can thiệp của người dùng. Việc này đặc biệt nguy hiểm vì đối tượng tấn công có thể thực hiện bất kỳ thao tác nào với gói ứng dụng bị chiếm đoạt.

Nguồn: https://thehackernews.com/2024/07/critical-flaws-in-cocoapods-expose-ios.html

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng Nghiêm trọng trong CocoaPods gây nguy hiểm đến các ứng dụng iOS và macOS"

Lỗ hổng **CVE-2024-38367 (Điểm CVSS: 8.2)** nằm trong thành phần xác thực email của dịch vụ. Đối tượng tấn công có thể gửi liên kết xác thực email giả mạo, khi người dùng bấm vào, họ sẽ bị chuyển hướng đến miền do đối tượng tấn công kiểm soát, thu thập token phiên của nạn nhân. Hơn nữa, lỗ hổng này có thể được nâng cấp thành một cuộc tấn công chiếm đoạt tài khoản không cần sự tương tác của người dùng thông qua việc giả mạo header HTTP và khai thác các công cụ bảo mật email bị cấu hình sai.

Cả ba lỗ hổng này đã được CocoaPods vá vào tháng 10 năm 2023, đồng thời cài đặt lại tất cả các phiên người dùng để ngăn chặn các khả năng khai thác tiếp theo. Trước đó, vào tháng 3 năm 2023, một công ty bảo mật đã phát hiện một sub-domain bị bỏ quên ("cdn2.cocoapods[.]org") liên quan đến CocoaPods có thể đã bị đối tượng tấn công chiếm dụng thông qua GitHub Pages để lưu trữ payload độc hại.

Đối với người dùng CocoaPods, việc cập nhật lên phiên bản mới nhất và sử dụng các biện pháp bảo mật bổ sung là cực kỳ quan trọng để bảo vệ hệ thống của họ khỏi các mối đe dọa tiềm ẩn.

Nguồn: https://thehackernews.com/2024/07/critical-flaws-in-cocoapods-expose-ios.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 **531** lỗ hổng, trong đó có 106 lỗ hổng mức Cao, 144 lỗ hổng mức Trung bình, 25 lỗ hổng mức Thấp và 256 lỗ hổng chưa đánh giá. Trong đó có ít nhất 99 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 OpenSSH, GeoServer và Splunk cụ thể là như sau:

- **CVE-2024-6387 (Điểm CVSS: 8.1 – Cao):** Lỗ hổng tồn tại trên máy chủ OpenSSH cho phép đối tượng tấn công khai thác lỗi Race Condition, cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-36401 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên GeoServer cho phép đối tượng tấn công thực thi mã từ xa thông qua việc truyền vào dữ liệu độc hại tới các phiên GeoServer cấu hình mặc định. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-36991 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng tồn tại trên Splunk Enterpise phiên bản Windows cho phép đối tượng tấn công khai thác lỗi Path Traversal để truy cập và thực hiện các hành vi trái phép trên hệ thống. Hiện lỗ hổng đã 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-2024-6387	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: OpenSSH - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - 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-2024-6387
2	CVE-2024-26229	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền - 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-2024-26229
3	CVE-2024-36991	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Splunk Enterprise trên Windows. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - 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-2024-36991
4	CVE-2024-29943	- Điểm CVSS: Chưa xác định - Ảnh hưởng: JavaScript - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-29943
5	CVE-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: GeoServer - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - 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-2024-36401

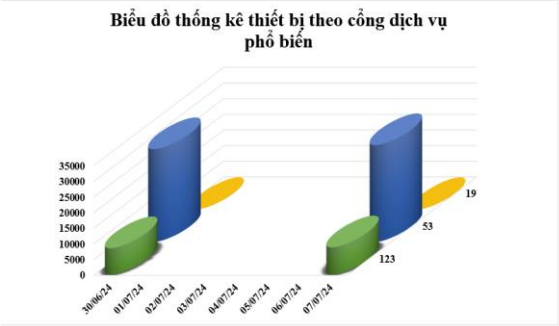
TOP 10 lỗ hổng đáng chú ý trong tuần

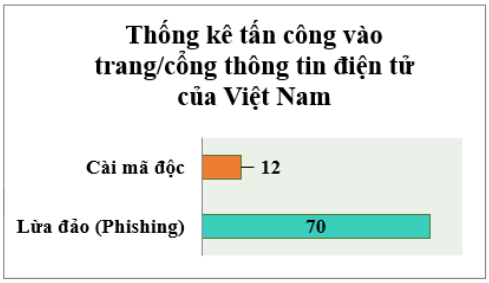
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-20399	- Điểm CVSS: 6.7 (Trung bình) - Ảnh hưởng: Cisco NX-OS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-20399
7	CVE-2024-4040	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: CrushFTP - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành vi trái phép. - 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-2024-4040
8	CVE-2024-37726	- Điểm CVSS: Chưa xác định - Ảnh hưởng: MSI Center - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - 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-2024-37726
9	CVE-2024-5806	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Progress MOVEit Transfer. - Mô tả: Lỗ hổng bỏ qua xác thực cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - 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-2024-5806
10	CVE-2024-39943	- Điểm CVSS: 9.9 (Nghiêm trọng) - Ảnh hưởng: rejetto HFS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - 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-2024-39943

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 **39.780** (tăng so với tuần trước **38.212**) 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.



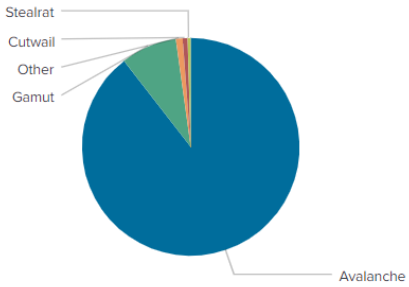


Tấn công Web

Trong tuần, có **82** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 70 trường hợp tấn công lừa đảo (Phishing), 12 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

differentia.ru	andall.servicesql.info
disorderstatus.ru	restless.su
amnsreiuojy.ru	sql.onlyslq.lol
atomictrivia.ru	jpalertcert.com
xjpakmdcfuqe.biz	griefcube.cc
hzmksreiuojy.ru	aurasport.net
restlesz.su	umyugu88.ru
xjpakmdcfuqe.in	sirec.in
xjpakmdcfuqe.com	groceryshootworld.com
xjpakmdcfuqe.ru	focusdate.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **1.927** phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam phản ánh về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) qua hệ thống tại địa chỉ https://canhbao.khonggianmang.vn. Qua kiểm tra, phân tích có nhiều trường hợp lừa đảo giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

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

STT	Website lừa đảo	Ghi chú
1	https://baohiemxahoi[.]vnagov[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://mojgov[.]weebly[.]com	Website giả mạo Bộ Tư pháp
3	https://giiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://vgiao[.]hangtietkiem[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://tcvnhomefic[.]com	Website giả mạo Ngân hàng TMCP Quân đội
6	http://vib[.]uudaikhachhang-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
7	http://vib-gold-card[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
8	http://nang-hang-the-vip2-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
9	https://www[.]vpbank[.]chamsockhachhang-uudai-the-truc-tuyen[.]online	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
10	https://lapdatinternet[.]net/	Website giả mạo SCTV
11	https://vnc75635s[.]com	Website giả mạo sàn TMĐT Shopee
12	https://vnc69977s[.]com	Website giả mạo sàn TMĐT Shopee
13	https://www[.]shopeesop[.]com	Website giả mạo sàn TMĐT Shopee
14	https://tdkt07[.]com	Website giả mạo sàn TMĐT Tiki
15	https://tikijaj2[.]com	Website giả mạo sàn TMĐT Tiki
16	https://tikt88[.]com	Website giả mạo sàn TMĐT Tiki
17	https://businesseventskp[.]top	Website giả mạo sàn TMĐT Tiki
18	chinhphu[.]cc	Website giả mạo Văn phòng Chính phủ
19	quandoi-viettel[.]com	Website giả mạo Viettel
20	giaodichdaquocgia[.]us	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