NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 05 (27/01/2025 – 02/02/2025)

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:** Phát hiện kỹ thuật Syncjacking cho phép đối tượng tấn công chiếm quyền điều khiển thiết bị của người dùng thông qua tiện ích mở rộng của Chrome.

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

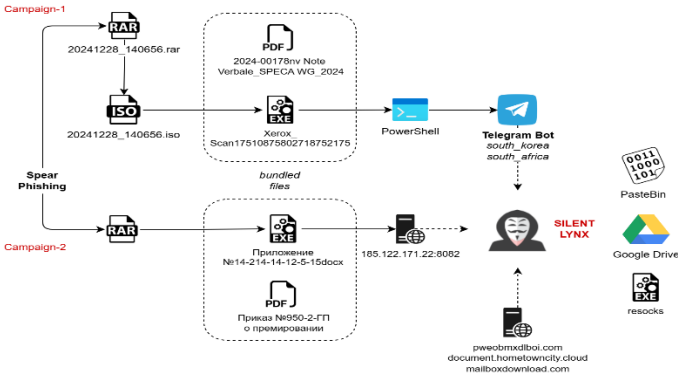
4. Tài liệu lưu trữ

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

https://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Phát hiện nhóm APT Silent Lynx thực hiện chiến dịch tấn công do thám nhằm vào Trung Á"



Gần đây, một cơ quan bảo mật đã phát hiện và ghi nhận hai chiến dịch tấn công có tính phức tạp nhằm vào một nhóm APT mới được phát hiện có tên Silent Lynx. Nhóm APT này có liên kết tới Kazakhstan đã thực hiện chiến dịch tấn công nhằm vào các tổ chức chính phủ thuộc quốc gia láng giềng và Kyrgyzstan với chuỗi tấn công đa giai đoạn để thực hiện mục tiêu thu thập thông tin về tình hình kinh tế, ngoại giao.

Cụ thể, Silent Lynx đã nhằm tới các tổ chức quan trọng như đại sứ quán, viện nghiên cứu và các tổ chức tài chính của các quốc gia thuộc chương trình SPECA. Trong chiến dịch mới nhất nhằm vào Kyrgyzstan, nhóm này đã sử dụng kỹ thuật spear-phishing để xâm nhập đầu vào, sử dụng các văn bản mồi như có nội dung liên quan tới sự kiện của Liên Hợp Quốc và các văn bản về đãi ngộ cho nhân viên được phát hành bởi chính phủ.

Trong các email này có chứa file .RAR độc hại có chứa reverse shell viết bằng Golang cùng với văn bản Word dùng làm ngụy trang hoặc một file ISO độc hại có chứa loader C++ cùng với file PDF ngụy trang.

Ngoài spear-phishing, nhóm APT này cũng sử dụng kết hợp nhiều kỹ thuật, công cụ khác trong các giai đoạn của chiến dịch, cụ thể là như sau:

- Sử dụng loader độc hại: Loader đứa chưa trong file C++ cho phép đối tượng tấn công thực thi mã từ xa và triển khai backdoor trên hệ thống người dùng.
- Sử dụng bot PowerShell: Script PowerShell sau khi được thực thi sẽ kết nối tới máy chủ C&C dựa trên bot của Telegram, cho phép đối tượng tấn công thực thi các câu lệnh hệ thống từ xa và trích xuất dữ liệu nhạy cảm của người dùng.
- Mã độc Golang: Cụ thể là reverse shell có chức năng thiết lập kết nối duy trì sử dụng khóa registry của Windows Run, sau đó sử dụng câu lệnh "curl" để tải xuống các payload bổ sung từ domain độc hại.

Nguồn: https://securityonline.info/silent-lynx-apt-group-a-new-espionage-threat-targeting-central-asia/?&web_view=true

Tin tức An toàn thông tin

"Chiến dịch tấn công APT Phát hiện nhóm APT Silent Lynx thực hiện chiến dịch tấn công do thám nhằm vào Trung Á"

Mục tiêu chính của Silent Lynx là xâm nhập, thu thập thông tin của các tổ chức chính phủ của các quốc tại Trung Á nhằm mục đích do thám. Được biết, nhóm này phụ thuộc vào bot của Telegram để triển khai C&C và trích xuất dữ liệu được thu thập. Ngoài ra, cơ quan bảo mật phát hiện nhóm này cũng đã chỉ một số điểm chung của nhóm với YoroTrooper về việc sử dụng công cụ PowerShell và mục tiêu thực hiện chiến dịch tấn công.

Một số IoC được ghi nhận:

hxxps:[//]pweobmxdlboi[.]com	hxxps:[//]document[.]hometowncity[.]cloud
hxxps:[//]mailboxdownload[.]com	hxxps[:]//api[.]telegram[.]org/bot8171872935:AAHLoudjpHz1bxA26bV5wPuOEL3LOHEl6Qk
hxxps[:]//api[.]telegram[.]org/bot7898508392:AAF5FPbJ1jlPQfqCIGnx-zNdw2R5tF_Xxt0	297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c
c045344b23fc245f35a0ff4a6d6fa744d580cde45c8cd0849153dee7dce1d80c	e6f76a73180b4f2947764f4de57b52d037b482ece1a88dab9d3290e76be8c098
99c6017c8658faf678f1b171c8eb5d5fa7e7d08e0a0901b984a8e3e1fab565cd	0

Nguồn: https://securityonline.info/silent-lynx-apt-group-a-new-espionage-threat-targeting-central-asia/?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện kỹ thuật Syncjacking cho phép đối tượng tấn công chiếm quyền điều khiển thiết bị của người dùng thông qua tiện ích mở rộng của Chrome"

Các chuyên gia bảo mật đã ghi nhận một kỹ thuật tấn công mới có tên "Browser Syncjacking" cho phép đối tượng tấn công sử dụng tiện ích mở rộng của Chrome để chiếm quyền điều khiển thiết bị. Kỹ thuật tấn công này được phát hiện bởi SquareX và có nhiều bước thực hiện, trong đó gồm có: chiếm dụng profile của Chrome, chiếm quyền điều khiển trình duyệt và có thể dẫn tới chiếm dụng thiết bị hoàn toàn.

Điểm đặc biệt của kỹ thuật này là khả năng ẩn mình mặc cho nó có nhiều giai đoạn, chỉ yêu cầu quyền hạn tối thiểu và không cần người dùng phải tương tác gì khác ngoài việc cài đặt tiện ích độc hại. Chuỗi tấn công của kỹ thuật bắt đầu bằng việc tạo một domain Google Workspace độc hại có chứa nhiều profile người dùng với các chức năng bảo mật như MFA bị tắt. Domain này sẽ được dùng để tạo một profile khác trên thiết bị của người dùng bị tấn công.

Sau khi lừa người dùng cài đặt tiện ích mở rộng, đối tượng tấn công sẽ đăng nhập người dùng vào một trong các profile này trên tab trình duyệt chạy ẩn phía sau; cùng lúc đó, tiện ích sẽ mở lên một trang hỗ trợ của Google, và với quyền Đọc/Ghi của nó, tiện ích sẽ nhúng nội dung vào trang, yêu cầu người dùng bật chức năng đồng bộ hóa trên Chrome.

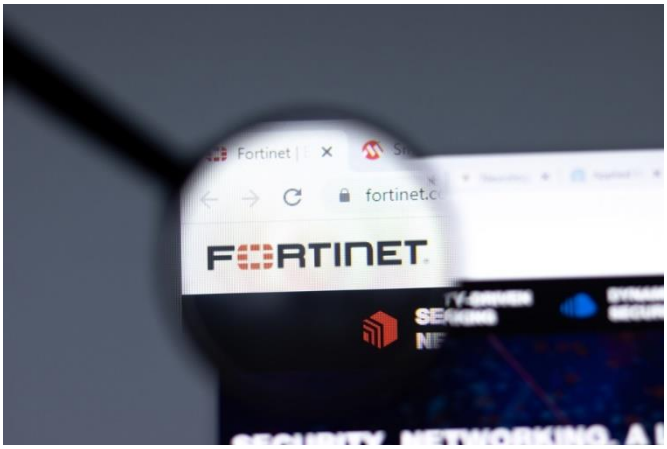
Sau khi thực hiện tác vụ trên, mọi dữ liệu lưu trên trình duyệt sẽ bị phơi bày cho đối tượng tấn công truy cập và sẽ chiếm quyền điều khiển trình duyệt của người dùng thông qua profile được cài cắm trước đó.

Kỹ thuật tấn công này nghiêm trọng ở việc đối tượng tấn công có thể khai thác Native Messaging Api của Chrome để thiết lập một kênh truyền thông tin trực tiếp giữa tiện ích độc hại và hệ điều hành của người dùng. Qua đó, đối tượng có thể duyệt thư mục, chỉnh sửa file, cài mã độc, thực thi mã từ xa, lưu lại dữ liệu nhập vào bởi người dùng, trích xuất dữ liệu và thậm chí là kích hoạt webcam, mic trên thiết bị.

Theo ý kiến của chuyên gia bảo mật, khả năng ẩn mình của kỹ thuật này khiến cho người dùng thông thường khó có thể phát hiện hành vi độc hại đang diễn ra trên thiết bị của mình do nó không có bất kì dấu hiệu trực tiếp nào.

Nguồn: https://www.bleepingcomputer.com/news/security/new-syncjacking-attack-hijacks-devices-using-chrome-extensions/

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 **762** lỗ hổng, trong đó có 249 lỗ hổng mức Cao, 361 lỗ hổng mức Trung bình, 27 lỗ hổng mức Thấp và 125 lỗ hổng chưa đánh giá. Trong đó có ít nhất 116 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 Apple, Mitel và Fortinet, cụ thể là như sau:

- **CVE-2025-24085 (Điểm CVSS: 7.8 – Cao):** Lỗ hổng tồn tại trên các sản phẩm của hãng Apple sử dụng hệ điều hành iOS, iPadOS, macOS, watchOS và tvOS cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế

- **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-2024-55591 (Điểm CVSS: 9.6 – Nghiêm trọng):** Lỗ hổng tồn tại trên Fortinet FortiOS và FortiProxy cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền để đạt được quyền super-admin thông qua các yêu cầu độc hại gửi tới module Node.js websocket. 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-2025-24085	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Hệ điều hành iOS, iPadOS, macOS, watchOS và tvOS - Mô tả: Lỗ hổng cho phép đối tượng tấn công - 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-2025-24085
2	CVE-2024-41710	- Điểm CVSS: 6.8 (Cao) - Ảnh hưởng: Mitel - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - 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
3	CVE-2024-55591	- Điểm CVSS: 9.6 (Nghiêm trọng) - Ảnh hưởng: FortiOS, FortiProxy. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện 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://www.cve.org/CVERecord?id=CVE-2024-55591
4	CVE-2024-40891	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: DSL CPE Zyxel - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành vi trái phép. - 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-2024-40891
5	CVE-2025-0065	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: TeamViewer - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - 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

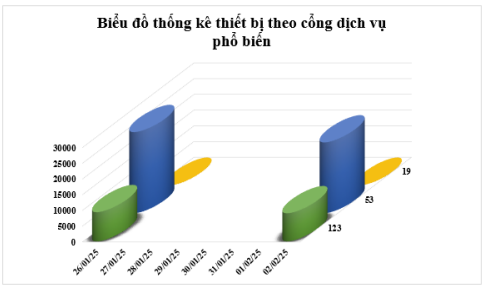
TOP 10 lỗ hổng đáng chú ý trong tuần

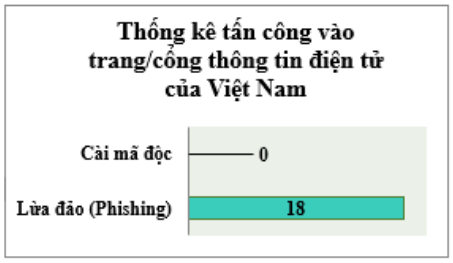
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2025-0683	- Điểm CVSS: 5.9 (Trung bình) - Ảnh hưởng: Contec Health CMS8000 Patient Monitors - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2025-0683
7	CVE-2025-22604	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Framework Cacti - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - 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
8	CVE-2025-22217	- Điểm CVSS: 8.6 (Cao) - Ảnh hưởng: Avi Load Balancer - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi SQL Injection. - 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-2025-22217
9	CVE-2025-24118	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Hệ điều hành iPadOS, macOS Sequoia/ Sonoma - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - 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
10	CVE-2025-0626	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Contec Health CMS8000 Patient Monitors - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - 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-2025-0626

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 **31.525** (giảm so với tuần trước **35.155**) 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.



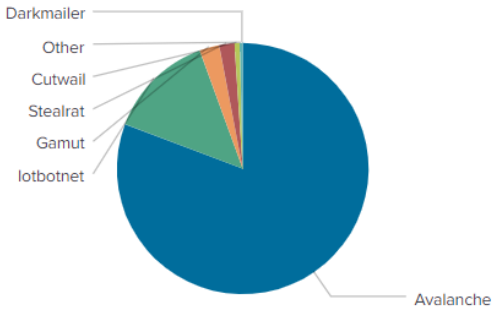


Tấn công Web

Trong tuần, có **18** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 18 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

differentia.ru	b.deltaheavy.ru
atomictrivia.ru	devicesta.ru
thesecond.in	c.deltaheavy.ru
morphed.ru	cp.f2a4ipk6.ru
hzmksreiuojy.in	xjpakmdcfuqe.com
ygiudewsqhct.in	ydbnsrt.me
xjpakmdcfuqe.biz	cp.wdzbt76z.ru
a.deltaheavy.ru	butterflyjobs.com
xjpakmdcfuqe.in	key-pack.com
differentia.ru	0-0-0-0-0-0-0-0-0-0-0-0-0-0-18-0-0-0-0-0-0-0-0-0-0-0-0-0-0.info

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **1.525** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **54** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **1.471** 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://global-sellings[.]com/AmazonRegisterAccoun	Website giả mạo sàn TMĐT Amazon
3	www[.]amzzcbe-cme[.]cm	Website giả mạo sàn TMĐT Amazon
4	tuyendungapple[.]com/	Website giả mạo Apple
5	https://congthongtinanninhmang[.]com/login	Website giả mạo Bộ Công An
6	congthongtinanninhmang[.]com/tickets/	Website giả mạo Bộ Công an
7	kiemtragplx[.]vn	Website giả mạo Bộ Giao thông Vận tải
8	kythuatdmayxanh[.]com/sua-bep-tu-bep-hong-ngoai-dien-may-xanh/?zarsrc=30&utm_source=zalo&utm_medium=zalo&utm_campaign=zalo	Website giả mạo Điện máy xanh
9	https://app[.]ebaynnhd[.]vip	Website giả mạo sàn TMĐT Ebay
10	giaohangnhanh[.]info/	Website giả mạo Giao hàng nhanh
11	vietcombank[.]asia/	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
12	https://www[.]shopeesallers[.]com	Website giả mạo sàn TMĐT Shopee
13	https://marketing-oder[.]com/	Website giả mạo sàn TMĐT Taobao
14	https://evn[.]it[.]com/	Tập đoàn Điện lực Việt Nam (EVN)
15	https://newmalle[.]cc	Website giả mạo Tiktok
16	https://newmalla[.]com	Website giả mạo Tiktok
17	tkshopvn[.]vip/2[.]html	Website giả mạo TikTok
18	http://vienthongviettel[.]vn	Website giả mạo Viettel
19	http://shop[.]vnggmes[.]com/	Website giả mạo VNG
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