NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 26 (24/06/2024 – 30/06/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** 75 tổ chức tại Đài Loan bị ảnh hưởng bởi chiến dịch gián điệp mạng của nhóm APT RedJuliett.

- **Cảnh báo:** Phát hiện lỗ hổng an toàn thông tin nghiêm trọng trên công cụ Ollama AI.

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: 1.843** 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: 75 tổ chức tại Đài Loan bị ảnh hưởng bởi chiến dịch gián điệp mạng của nhóm APT RedJuliett."

Gần đây, đã phát hiện một chiến dịch gián điệp mạng quy mô lớn, có khả năng được hậu thuẫn bởi chính phủ Trung Quốc. Chiến dịch này do nhóm tấn công RedJuliett thực hiện, còn được biết đến dưới các biệt danh Flax Typhoon và Ethereal Panda, nhằm vào các tổ chức giáo dục, công nghệ, chính phủ và ngoại giao tại Đài Loan từ tháng 11/2023 đến tháng 4/2024.

RedJuliett thường khai thác các thiết bị và ứng dụng kết nối Internet như tường lửa, bộ cân bằng tải và VPN doanh nghiệp để xâm nhập hệ thống, sử dụng các kỹ thuật tấn công như SQL Injection và Directory Traversal trên ứng dụng web và SQL. Sau khi xâm nhập, nhóm này dùng phần mềm SoftEther để điều hành lưu lượng độc hại và áp dụng kỹ thuật "living-off-the-land" để tránh bị phát hiện.

Để duy trì kết nối và kiểm soát hệ thống, RedJuliett triển khai các web shell như China Chopper, devilzShell, AntSword và Godzilla. Họ cũng khai thác lỗ hổng Dirty Cow (CVE-2016-5195) trên Linux để leo thang đặc quyền và củng cố quyền kiểm soát.

Hạ tầng hoạt động của RedJuliett bao gồm các máy chủ do nhóm kiểm soát, thuê từ các nhà cung cấp máy chủ ảo (VPS) và các hệ thống đã bị xâm nhập của ba trường đại học tại Đài Loan. Nhóm này sử dụng SoftEther để quản lý máy chủ và điều hành các hoạt động độc hại một cách hiệu quả và khó bị phát hiện.

Mục tiêu hoạt động của nhóm RedJuliett là hỗ trợ Bắc Kinh thu thập thông tin tình báo về các quốc gia Đông Á. Ngoài Đài Loan, nhóm còn nhắm đến Djibouti, Hong Kong, Kenya, Lào, Malaysia, Philippines, Rwanda, Hàn Quốc, và Hoa Kỳ. Đã ghi nhận 24 tổ chức, bao gồm các cơ quan chính phủ tại Đài Loan, Lào, Kenya và Rwanda, bị nhóm tấn công này thiết lập kết nối. Ước tính ít nhất 75 tổ chức tại Đài Loan đã trở thành mục tiêu do thám và khai thác diện rộng của nhóm.

Nguồn: https://thehackernews.com/2024/06/redjuliett-cyber-espionage-campaign.html?&web_view=true#update

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: 75 tổ chức tại Đài Loan bị ảnh hưởng bởi chiến dịch gián điệp mạng của nhóm APT RedJuliett."

RedJuliett tập trung chủ yếu vào việc thu thập thông tin tình báo về chính sách kinh tế, quan hệ thương mại và ngoại giao của Đài Loan đối với các quốc gia khác. Giống như các nhóm APT khác từ Trung Quốc, nhóm này tập trung vào khai thác các thiết bị kết nối Internet do chúng thường có hạn chế về hiển thị và bảo mật, cho phép mở rộng quy mô xâm nhập ban đầu một cách hiệu quả.

Chiến dịch gián điệp mạng của RedJuliett là một minh chứng rõ ràng về sự tinh vi và phức tạp của các nhóm tấn công nhà nước hậu thuẫn. Điều này đặt ra thách thức lớn đối với các tổ chức và quốc gia trong việc nâng cao khả năng bảo mật của mình, đặc biệt là đối với các thiết bị và ứng dụng kết nối Internet khi đối phó với các chiến dịch tấn công phức tạp tương tự.

Một số IoC được ghi nhận:

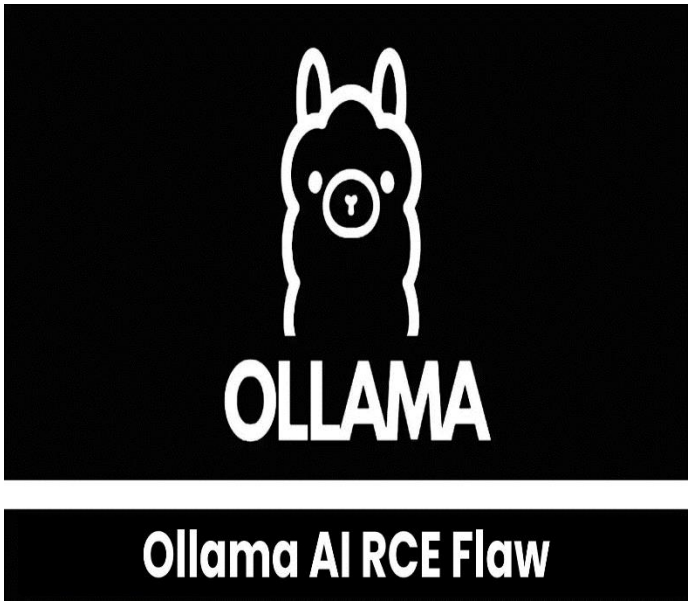
38.147.190[.]192
122.10.89[.]230
140.120.98[.]115
154.197.99[.]202
61.238.103[.]155
137.220.36[.]87
154.197.98[.]3
176.119.150[.]92

Nguồn: https://thehackernews.com/2024/06/redjuliett-cyber-espionage-campaign.html?&web_view=true#update

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng an toàn thông tin nghiêm trọng trên công cụ Ollama AI."



Các chuyên gia bảo mật đã ghi nhận và vá một lỗ hổng an toàn thông tin trên nền tảng cơ sở hạ tầng mã nguồn mở của Ollama AI. Lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa. Ollama là một dịch vụ đóng gói, triển khai và thực thi các mô hình ngôn ngữ lớn (Large Language Model – LLM) trên các hệ điều hành Windows, Linux và macOS.

Lỗ hổng CVE-2024-37032 còn được biết đến với tên gọi Probllama, đã được phát hiện vào ngày 05/05/2024 và khắc phục trong phiên bản 0.1.34 phát hành vào ngày 07/05/2024

Về bản chất, lỗ hổng này xuất phát từ việc thiếu kiểm tra đầu vào đầy đủ, dẫn đến lỗi đánh lạc hướng đường dẫn (payload path traversal) mà đối tượng tấn công có thể lợi dụng để ghi đè lên các tệp tin bất kỳ trên máy chủ và thực thi mã từ xa.

Để khai thác lỗ hổng này, đối tượng tấn công phải gửi các yêu cầu HTTP đặc biệt tới máy chủ API của Ollama để tấn công API endpoint '/api/pull', dùng để tải mô hình từ kho lưu trữ chính thức hoặc một kho lưu trữ riêng. Việc tấn công endpoint này cho phép kẻ tấn công tạo tệp mô hình độc hại với payload đánh lạc hướng đường dẫn.

Đối tượng tấn công khai thác lỗ hổng này không chỉ để gây hại tới các tệp tin trên hệ thống mà còn để thực thi mã từ xa, bằng cách ghi đè lên tệp cấu hình "etc/ld.so.preload" của trình liên kết động "ld.so", chèn vào đó một thư viện chia sẻ độc hại và thực thi nó trước khi mỗi chương trình được khởi chạy.

Mặc dù nguy cơ thực thi mã từ xa giảm đáng kể trong các cài đặt mặc định của Linux, nơi máy chủ API được ràng buộc với localhost, nhưng điều này không áp dụng đối với các triển khai Docker. Trên môi trường Docker, máy chủ API được mở rộng công khai với quyền root và lắng nghe trên địa chỉ 0.0.0.0 theo cấu hình mặc định.

Nguồn: https://thehackernews.com/2024/06/critical-rce-vulnerability-discovered.html

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng an toàn thông tin nghiêm trọng trên công cụ Ollama AI."

Ngoài ra, Ollama thiếu cơ chế xác thực, cho phép đối tượng tấn công khai thác các máy chủ truy cập công khai để đánh cắp hoặc can thiệp vào các mô hình trí tuệ nhân tạo và đe dọa các máy chủ tự động suy luận AI. Các chuyên gia bảo mật đã phát hiện hơn 1000 trường hợp Ollama mở và không được bảo vệ bởi biện pháp an ninh nào, vì vậy họ khuyên người dùng sử dụng giải pháp phần mềm trung gian như Reverse Proxy với cơ chế xác thực để tăng cường bảo mật.

Thông tin về lỗ hổng CVE-2024-37032 được tiết lộ sau khi công ty bảo mật AI cảnh báo về hơn 60 lỗ hổng an ninh ảnh hưởng tới các công cụ AI/ML mã nguồn mở khác nhau, có thể bị tấn công leo thang đặc quyền, chiếm quyền kiểm soát hệ thống và thực hiện các hành vi không đúng quy định. Trong đó, lỗ hổng nghiêm trọng nhất là CVE-2024-22476 (Điểm CVSS: 10.0), một lỗ hổng xâm nhập SQL trong phần mềm NIntel Neural Compressor cho phép đối tượng tấn công tải xuống các tệp tin tùy ý từ hệ thống của máy chủ người dùng.

Nguồn: https://thehackernews.com/2024/06/critical-rce-vulnerability-discovered.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 **687** lỗ hổng, trong đó có 115 lỗ hổng mức Cao, 166 lỗ hổng mức Trung bình, 20 lỗ hổng mức Thấp và 386 lỗ hổng chưa đánh giá. Trong đó có ít nhất 88 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 SolarWinds và VMware, cụ thể là như sau:

- **CVE-2024-28995 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng directory tranversal tồn tại trên SolarWinds Serv-U 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-2024-37079 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng heap-overflow tồn tại trong giao thức DCERPC trên VMware vCenter Server cho phép đối tượng tấn công thực thi mã từ xa sau khi khai thác sử dụng gói tin độc hại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-37080 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng heap-overflow tồn tại trong giao thức DCERPC trên VMware vCenter Server cho phép đối tượng tấn công thực thi mã từ xa sau khi khai thác sử dụng gói tin độc hại. Hiện lỗ hổng 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-2024-28995	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: SolarWinds Serv-U - 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-2024-28995
2	CVE-2024-37079	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: VMware vCenter Server - 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-2024-37079
3	CVE-2024-37080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: VMware vCenter Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-37080
4	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
5	CVE-2024-29973	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Zyxel. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã OS tùy ý. - 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-2024-29973

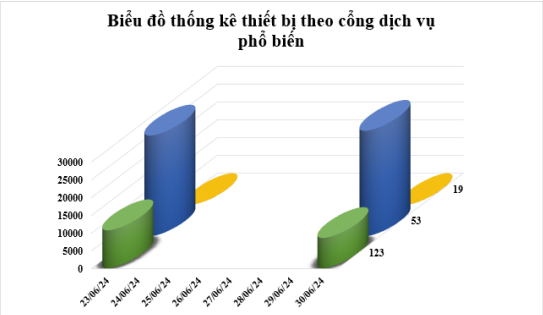
TOP 10 lỗ hổng đáng chú ý trong tuần

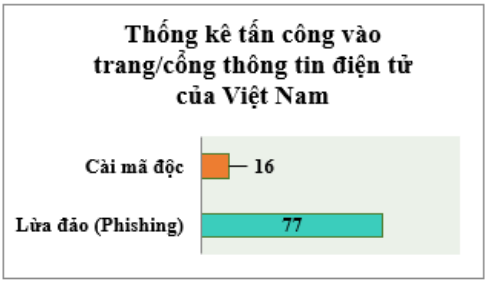
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-34102	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Adobe Commerce - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-34102
7	CVE-2024-5805	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Progress MOVEit Gateway - 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 đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-5805
8	CVE-2024-3400	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-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-2024-3400
9	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ngôn ngữ lập trình PHP. - 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-2024-4577
10	CVE-2024-21887	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - 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-2024-21887

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 **38.212** (giảm so với tuần trước **39.057**) 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.



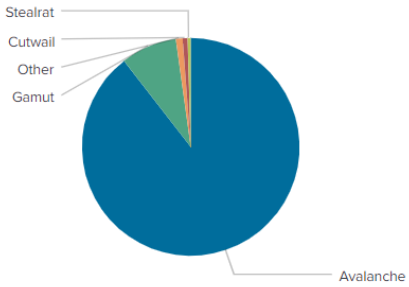


Tấn công Web

Trong tuần, có **93** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 77 trường hợp tấn công lừa đảo (Phishing), 16 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	jpalertcert.com
disorderstatus.ru	restless.su
atomictrivia.ru	jtkjixnmj.org
amnsreiuojy.ru	umyugu88.ru
xjpakmdcfuqe.biz	sql.onlyslq.lol
restlesz.su	kenkenlimted.top
hzmksreiuojy.ru	griefcube.cc
xjpakmdcfuqe.in	xnqwuwlq.org
xjpakmdcfuqe.com	vgbfurkmbjw.org
xjpakmdcfuqe.ru	jpalertcert.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **1.843** 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://vn156475p[.]com	Website giả mạo sàn TMĐT Amazon
2	https://vssidgov[.]com	Bảo hiểm Xã hội Việt Nam
3	nappthe[.]vn	Website giả mạo Công Ty Cổ Phần Giải Trí Và Thể Thao Điện Tử Việt Nam
4	https://nqsncoau[.]buzz/	Website giả mạo Cty tài chính tnhh ngân hàng việt nam thịnh vượng smbc
5	https://www[.]iazada[.]com/	Website giả mạo sàn TMĐT Lazada
6	https://la5959[.]com	Website giả mạo sàn TMĐT Lazada
7	https://tcbcanhan[.]com	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
8	hdbank[.]tructuyen-uudai-thekhachhang[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
9	nang-cap-qcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	vib-solution[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	vpbank[.]uudai-tructuyen-chamsockhachhang-the[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
12	https://www[.]seleeashopee[.]com	Website giả mạo sàn TMĐT Shopee
13	sp7335p[.]com	Website giả mạo sàn TMĐT Shopee
14	https://vnc63661s[.]com	Website giả mạo sàn TMĐT Shopee
15	https://tdkt06[.]com	Website giả mạo sàn TMĐT Tiki
16	https://fajiafu30[.]com/	Website giả mạo sàn TMĐT Tiki
17	https://sh2tiki[.]com	Website giả mạo sàn TMĐT Tiki
18	https://nhantienquoctev3[.]vercel[.]app/	Website giả mạo Western Union
19	https://chuyentienquoctenhanh[.]vercel[.]app/	Website giả mạo Western Union
20	chuyentienquocte1313[.]vercel[.]app	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