NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 18 (29/04/2024 – 05/05/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm Muddling Meerkat thao túng DNS bằng Great Firewall của Trung Quốc.

- **Cảnh báo:** Lỗ hổng an toàn thông tin tồn tại trên BIG-IP Next Central Manager cho phép chiếm dụng thiết bị.

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: 225** 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 Muddling Meerkat thao túng DNS bằng Great Firewall của Trung Quốc."

Một nhóm tấn công mới được gọi là Muddling Meerket, có sự hậu thuẫn từ Trung Quốc, đã bắt đầu thực hiện một chiến dịch thăm dò mạng lưới toàn cầu thông qua việc thao túng DNS kể từ tháng 10/2019. Gần đây, vào tháng 09/2023, nhóm này đã tái xuất một cách đột ngột.

Một điều đáng chú ý trong hoạt động của nhóm là việc nhóm này thao túng các ghi chép của MX (Mail Exchange) bằng cách chèn phản hồi giả mạo thông qua Tường lửa vĩ đại của Trung Quốc (GFW), một hành vi bất thường chưa từng thấy trên hệ thống kiểm duyệt Internet của quốc gia này.

Theo điều tra từ cơ quan bảo mật, hiện vẫn chưa rõ mục đích hoặc động cơ của hành vi này, tuy nhiên đã chứng minh được sự phức tạp và tinh vi của nhóm này trong việc thao túng hệ thống DNS toàn cầu. Cụ thể, thông qua việc phân tích dữ liệu DNS, các nhà nghiên cứu bảo mật đã phát hiện ra một hành vi được cho là vô hại hoặc có thể dễ dàng bị bỏ qua. Nhóm Muddling Meerket đã thực hiện thao túng truy vấn và phản hồi của DNS bằng cách sử dụng cache để ảnh hưởng đến cơ chế trả về địa chỉ của giao thức này. Chẳng hạn, nhóm tấn công có thể tạo ra các phản hồi giả trên ghi chép MX từ phía GFW để gây nhiễu cho quá trình điều hướng, làm cho email của người dùng được gửi đến nhầm địa chỉ.

Chức năng chính của GFW là lọc và chặn các nội dung không phù hợp với chính phủ Trung Quốc bằng cách chặn các truy vấn DNS và trả về các phản hồi không khả dụng. Tuy nhiên, hành vi của Muddling Meerkat đã khiến GFW cung cấp các phản hồi giả mạo nhằm mục đích kiểm thử khả năng phục hồi và hành vi của các mạng lưới khác.

Nguồn: https://www.bleepingcomputer.com/news/security/muddling-meerkat-hackers-manipulate-dns-using-chinas-great-firewall/amp/

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm Muddling Meerkat thao túng DNS bằng Great Firewall của Trung Quốc."

Nhằm che giấu hành vi của mình, nhóm tấn công đã tạo yêu cầu DNS ngẫu nhiên cho các subdomain của domain được chọn làm mục tiêu, thường những subdomain này không tồn tại trong thực tế. Dù hình thức này giống với tấn công "Slow Drip DDoS", nhưng mục tiêu của nhóm không phải là tấn công từ chối dịch vụ, mà là kiểm thử và gây khó khăn cho việc xác định nguồn gốc của các yêu cầu DNS bất thường này.

Muddling Meerkat đã chọn các tên miền có tên ngắn, được đăng ký trước năm 2000 để tránh bị chọn vào danh sách chặn DNS. Về mục tiêu của chiến dịch tấn công, có thể là để thực hiện bản đồ hóa mạng và đánh giá bảo mật DNS của chính họ để chuẩn bị cho các cuộc tấn công trong tương lai. Hoặc có thể nhằm mục đích tạo ra sự rối loạn trong DNS, từ đó che giấu các hành vi độc hại và gây khó khăn cho các chuyên gia trong việc xác định nguồn gốc của các yêu cầu DNS bất thường này.

Một số IoC được ghi nhận:

183[.]136[.]225[.]45

183[.]136[.]225[.]14

Nguồn: https://www.bleepingcomputer.com/news/security/muddling-meerkat-hackers-manipulate-dns-using-chinas-great-firewall/amp/

Tin tức An toàn thông tin

“Cảnh báo: Lỗ hổng an toàn thông tin tồn tại trên BIG-IP Next Central Manager cho phép chiếm dụng thiết bị.”

F5 đã vá hai lỗ hổng an toàn thông tin mức độ Cao trên BIG-IP Next Central Manager, các lỗ hổng này cho phép đối tượng tấn công khai thác để đạt được quyền điều khiển admin và tạo các tài khoản trái phép trên các tài sản được quản lý. Next Central Manager cho phép quản trị viên điều khiển các phiên/dịch vụ vật lý hoặc trên hạ tầng cloud của BIG-IP Next thông qua một giao diện quản lý tổng thể.

Hai lỗ hổng này là **CVE-2024-26026 (SQL Injection)** và **CVE-2024-21793 (Odata Injection)** tồn tại trên BIG-IP Next Central Manager API cho phép đối tượng tấn công thực thi các câu lệnh SQL lên thiết bị từ xa.

Tấn công SQL Injection là hình thức tấn công chèn các câu lệnh truy vấn SQL độc hại vào một trường nhập dữ liệu hoặc tham số nằm trong câu truy vấn của cơ sở dữ liệu. Lỗ hổng này gây ảnh hưởng tới tính bảo mật của ứng dụng và cho phép câu lệnh SQL độc hại được thực thi, qua đó cho phép truy cập trái phép, gây lộ lọt dữ liệu và chiếm dụng hệ thống.

Sau khi tiến hành điều tra, đã phát hiện ra các tài khoản trái phép được tạo ra bởi các đối tượng tấn công không xuất hiện trên Next Central Manager. Điều này làm cho chúng trở thành cách để duy trì kết nối trên các thiết bị mà đối tượng tấn công đã xâm nhập.

Theo khuyến nghị từ F5, trong trường hợp không thể ngay lập tức cập nhật bản vá, quản trị viên nên hạn chế quyền truy cập vào Next Central Manager, chỉ cho các tài khoản người dùng được xác định là đáng tin cậy trên hệ thống mạng bảo mật. Điều này giúp giảm thiểu nguy cơ bị ảnh hưởng bởi các cuộc tấn công khai thác hai lỗ hổng này.

Hiện chưa có bằng chứng cho thấy hai lỗ hổng này đã bị khai thác trên môi trường thực tế.Tuy nhiên, thông qua kết quả tìm kiếm trên Shodan, hiện có hơn 10.000 thiết bị BIG-IP của F5 đang có cổng quản trị mở ra cho mạng công cộng.

Nguồn: https://www.bleepingcomputer.com/news/security/new-big-ip-next-central-manager-bugs-allow-device-takeover/

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng an toàn thông tin tồn tại trên BIG-IP Next Central Manager cho phép chiếm dụng thiết bị."

Vào tháng 11/2023, F5 đã cảnh báo người dùng về một chiến dịch tấn công sử dụng hai lỗ hổng **CVE-2023-46747** và **CVE-2023-46748**. Cả hai lỗ hổng này đã được vá từ trước một tháng trước khi chiến dịch tấn công diễn ra. Chiến dịch này nhằm vào các thiết bị chưa cập nhật bản vá, nhằm thực thi mã từ xa rồi xóa bỏ dấu vết của việc xâm nhập.

Hai năm trước đó, CISA cũng đã cảnh báo về việc khai thác rộng rãi của lỗ hổng **CVE-2022-1388**, cũng tồn tại trên các thiết bị F5 BIG-IP, lỗ hổng này cho phép đối tượng tấn công chiếm quyền điều khiển thiết bị. Trong thời điểm đó, chiến dịch tấn công đã nhắm vào hệ thống mạng của cả chính phủ và các doanh nghiệp tư nhân.

Nguồn: https://www.bleepingcomputer.com/news/security/new-big-ip-next-central-manager-bugs-allow-device-takeover/

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 **1.564** lỗ hổng, trong đó có 137 lỗ hổng mức Cao, 285 lỗ hổng mức Trung bình, 12 lỗ hổng mức Thấp và 1.130 lỗ hổng chưa đánh giá. Trong đó có ít nhất 532 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 tới các sản phẩm của Cisco và CrushFTP, cụ thể như sau:

- CVE-2024-20359 (**Điểm CVSS: 6.0 – Trung bình**): Lỗ hổng an toàn thông tin tồn tại trên phần mềm Cisco Adaptive Security Appliance (ASA) và Cisco Firepower Threat Defense (FTD) cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền root. Lỗ hổng tồn tại do quá trình xác thực file sai cách khi file được đọc từ bộ nhớ flash của hệ thống. Đối tượng tấn công có thể khai thác lỗ hổng này bằng cách copy file độc hại, được tạo trước vào disk0: của thiết bị. Qua đó cho phép đối tượng thực thi mã tùy ý kể cả sau khi thiết bị được khởi động lại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- CVE-2024-20353 (**Điểm CVSS: 8.6 – Cao**): Lỗ hổng an toàn thông tin tồn tại trên phần mềm Cisco Adaptive Security Appliance (ASA) và Cisco Firepower Threat Defense (FTD) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. Lỗ hổng tồn tại do quy trình kiểm tra lỗi thiếu hoàn thiện khi thiết bị duyệt một HTTP header. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- CVE-2024-4040 (**Điểm CVSS:10 – Nghiêm trọng**): Lỗ hổng chèn template tồn tại bên phía máy chủ trên CrushFTP phiên bản trước 10.7.1 và 11.1.0 trên mọi nền tảng cho phép đối tượng tấn công đọc file từ filesystem nằm ngoài VFS Sandbox, bỏ qua biện pháp xác thực để đạt được quyền quản trị và thực thi mã từ xa trên máy chủ. 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-2024-20359	- Điểm CVSS: 6.0 (Trung bình) - Ảnh hưởng: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý trên hệ thống bị ảnh hưởng - Lỗ hổng đã có mã khai thác đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-20359
2	CVE-2024-20353	- Điểm CVSS: 8.6 (Cao) - Ảnh hưởng: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - 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-2024-20353
3	CVE-2024-4040	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: CrushFTP - 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-2024-4040
4	CVE-2024-27322	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Ngôn ngữ lập trình R - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-27322
5	CVE-2024-3400	- Điểm CVSS: 10 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3400

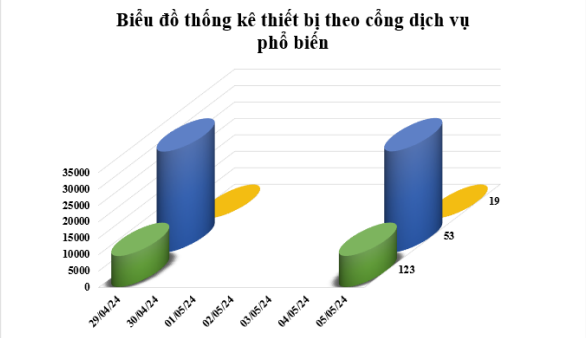
TOP 10 lỗ hổng đáng chú ý trong tuần

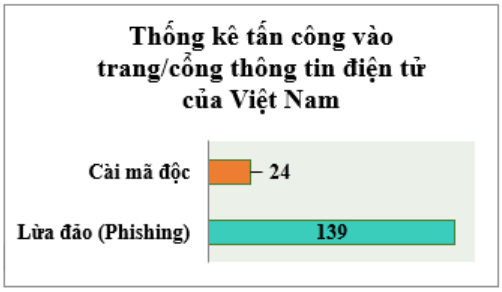
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-3094	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Tukaani XZ - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-3094
7	CVE-2024-27198	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: JetBrains TeamCity - Mô tả: Lỗ hổng cho phép đối tượng tấn công bỏ xác thực, thực hiện các hành vi trái phép trên thiết bị. - 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-2024-27198
8	CVE-2024-29988	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Windows Server 2022, Windows 10, Windows 11. - 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-2024-29988
9	CVE-2024-20337	- Điểm CVSS: 8.2 (Cao) - Ảnh hưởng: Cisco Secure Client - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công CRLF Injection, qua đó thực thi mã tùy ý trên trình duyệt, 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-2024-20337
10	CVE-2024-24996	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ivanti Avalanche - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-24996

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 **40.281** (tăng so với tuần trước **40.172**) 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.



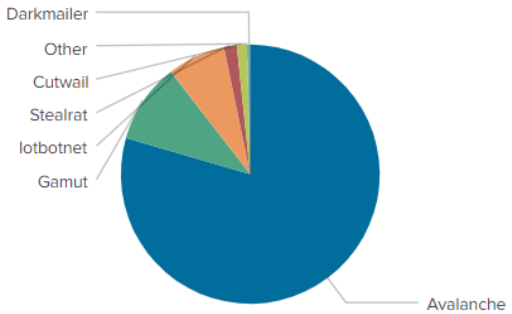


Tấn công Web

Trong tuần, có **163** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 139 trường hợp tấn công lừa đảo (Phishing), 24 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
atomictrivia.ru	db2017417b23.zapto.org
amnsreiuojy.ru	facialwaxmaxfaxlax3.com
restlesz.su	wlcalc.org
hzmksreiuojy.ru	vmcrjlkhbiynnasht.org
xjpakmdcfuqe.in	vbppedprxkrhfnhhn.org
xjpakmdcfuqe.biz	tylkxtkdhygbuiwfm.org
xjpakmdcfuqe.ru	suxrtwcnmcfjqywee.org
xjpakmdcfuqe.com	sonic4me.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **225** 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://homecreditvn[.]net	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
2	https://dienmayxanh542[.]com	Website giả mạo Điện máy xanh
3	https://dich-vu-dien-mayxanh[.]com	Website giả mạo Điện máy xanh
4	https://lazd8[.]com	Website giả mạo sàn TMĐT Lazada
5	http://vieetcombiank[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
6	https://visa-mb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
7	https://finacehoisomb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
8	https://mbdkb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
9	https://han-muc-khcn-uu-tien-vna1[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	http://vib[.]tanghanmuc-vn[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	http://vib[.]hanmucvn[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	khcn-my-diamon-han-muc-uu-tien[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
13	vib-mydiamon-khcn-uutien-vnc1[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
14	http://mail[.]labtpb[.]online	Website giả mạo Ngân hàng TMCP Tiên Phong
15	https://canhantpb[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
16	http://vpb[.]tang-han-muc-the-visa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
17	vpb[.]nanghanmucvisa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
18	https://shinhan[.]chamsocthekhachhang-thang4[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
19	https://tdkd07[.]com	Website giả mạo sàn TMĐT Tiki
20	https://dich-vu-kh-vip-vpbank[.]com/	Website giả mạo ngân hàng VPbank

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