NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 21 (20/05/2024 – 26/05/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công Trung Quốc nhằm mục tiêu tấn công vào các quốc gia vùng Biển Đông.

- **Cảnh báo:** QNAP phát hành bản vá khắc phục lỗ hổng an toàn thông tin trên QTS và QuTS hero.

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: 274** 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 tấn công Trung Quốc nhằm mục tiêu tấn công vào các quốc gia vùng Biển Đông"

Gần đây, các chuyên gia bảo mật đã tiết lộ chi tiết về nhóm APT **Unfading Sea Haze**, được cho là hoạt động từ năm 2018. Chiến dịch tấn công mới nhất của nhóm này nhằm vào các tổ chức chính phủ và quốc phòng tại các quốc gia vùng Biển Đông. Tính đến nay, nhóm này đã xâm nhập thành công vào tổng cộng tám mục tiêu.

Nhóm tấn công Unfading Sea Haze đã có thể xâm nhập vào hệ thống bằng cách khai thác những lỗ hổng bảo mật nghiêm trọng của người dùng, bao gồm việc sử dụng mật khẩu yếu và bỏ qua việc cập nhật các bản vá bảo mật cho các thiết bị và dịch vụ web. Mặc dù nhóm này có mục tiêu tương tự với chính phủ Trung Quốc, nhưng các đặc điểm đặc trưng của các cuộc tấn công này không giống với các nhóm tấn công khác đã được xác định trước đó.

Nhóm **Unfading Sea Haze** sử dụng các biến thể của mã độc Gh0st RAT, một loại trojan phổ biến thường được các nhóm tấn công Trung Quốc sử dụng. Một kỹ thuật đặc biệt được nhóm sử dụng trong chiến dịch này là thực thi mã JScript qua công cụ SharpJSHandler, tương tự với kỹ thuật của mã độc backdoor FunnySwitch của nhóm APT41. Cả hai kỹ thuật này đều nạp hợp ngữ .NET và thực thi mã JScript.

Quá trình xâm nhập ban đầu của nhóm chưa được xác định rõ ràng, nhưng đã có ghi nhận nhóm sử dụng email spear-phishing chứa file nén độc hại để tái xâm nhập vào các hệ thống đã bị xâm phạm. Các file nén này chứa file Windows shortcut (LNK), khi khởi động sẽ bắt đầu chuỗi lây nhiễm bằng cách thực thi lệnh tải xuống payload từ máy chủ C&C. Payload này là mã độc SerialPktdoor, được thiết kế để thực thi script PowerShell, quản lý file và tài khoản trên hệ thống.

Để duy trì kết nối với hệ thống bị xâm nhập, nhóm **Unfading Sea Haze** sử dụng các tác vụ lên lịch với tên tiến trình hợp lệ của Windows, thực hiện kỹ thuật DLL side-loading để nạp DLL độc hại.

Nguồn: https://thehackernews.com/2024/05/researchers-warn-of-chinese-aligned.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm tấn công Trung Quốc nhằm mục tiêu tấn công vào các quốc gia vùng Biển Đông"

Nhóm này cũng thao túng tài khoản Administrator cục bộ để vô hiệu hóa và đặt lại mật khẩu, duy trì quyền truy cập vào hệ thống. Ngoài ra, nhóm sử dụng các công cụ Remote Monitoring and Management (RMM) như ITarian RMM kể từ tháng 09/2022 để xâm nhập vào hệ thống mạng của người dùng.

Nhóm này thể hiện sự tinh vi qua việc sử dụng nhiều biến thể của mã độc Gh0st RAT như SilentGh0st, InsidiousGh0st, TranslucentGh0st, FluffyGh0st, và EtherealGh0st. Nhóm cũng sử dụng loader Ps2dllLoader để vượt qua bảo mật Antimalware Scan Interface (AMSI) và phát tán SharpJSHandler, công cụ này hoạt động bằng cách theo dõi các yêu cầu HTTP và thực thi mã JavaScript nhúng trong đó.

Ngoài các công cụ và mã độc chính, nhóm **Unfading Sea Haze** còn sử dụng mã độc backdoor Stubbedoor để thực thi hợp ngữ .NET tải từ máy chủ C&C. Các công cụ khác được nhóm sử dụng bao gồm keylogger xkeylog, mã độc đánh cắp dữ liệu trình duyệt, công cụ giám sát kết nối thiết bị cầm tay, và chương trình trích xuất dữ liệu DustyExfilTool đã được sử dụng từ tháng 03/2018 đến tháng 01/2022. Nhóm cũng sử dụng mã độc SharpZulip, lợi dụng API của Zulip để thu thập câu lệnh từ xa từ kênh "NDFUIBNFWDNSA".

Nhóm **Unfading Sea Haze** thực hiện trích xuất dữ liệu thủ công để chắt lọc thông tin quan trọng, bao gồm dữ liệu từ các ứng dụng nhắn tin như Telegram và Viber. Dữ liệu sau đó được nén lại dưới dạng file có mật khẩu trước khi gửi đi. Quá trình này cho thấy nhóm tấn công không chỉ dựa vào các công cụ tự động mà còn thực hiện các bước thủ công để đảm bảo thu thập được thông tin cần thiết.

Một số IoC được ghi nhận:

fc.adswt[.]com	mail.simpletra[.]com	mail.adswt[.]com
api.simpletra[.]com	bit.kozow[.]com	bitdefenderupdate[.]org
auth.bitdefenderupdate[.]com	mail.pcygphil[.]com	mail.bomloginset[.]com
dns-log.d-n-s.org[.]uk	linklab.blinklab[.]com	link.theworkguyoo[.]com
mail.theworkguyoo[.]com	sopho.kozow[.]com	news.nevuer[.]com
payroll.mywire[.]org	employee.mywire[.]org	airst.giize[.]com
cdn.g8z[.]net	managS.twilightparadox[.]com	dns.g8z[.]net
message.ooguy[.]com	spcg.lunaticfridge[.]com	helpdesk.fxnxs[.]com
newy.hifiliving[.]com	images.emldn[.]com	word.emldn[.]com
provider.giize[.]com	rest.redirectme[.]net	api.bitdefenderupdate[.]org
upupdate.ooguy[.]com	167.71.199[.]105	188.166.224[.]242
159.223.78[.]147	128.199.166[.]143	164.92.146[.]227
192.153.57[.]24	209.97.167[.]177	112.113.112[.]5
193.149.129[.]128	128.199.66[.]11	45.61.137[.]109
139.59.107[.]49	152.42.198[.]152	0

Nguồn: https://thehackernews.com/2024/05/researchers-warn-of-chinese-aligned.html

Tin tức An toàn thông tin

"Cảnh báo: QNAP phát hành bản vá khắc phục lỗ hổng an toàn thông tin trên QTS và QuTS hero"

Công ty QNAP vừa phát hành bản vá khắc phục một số lỗ hổng an toàn thông tin mức độ trung bình ảnh hưởng đến hệ điều hành QTS và QuTS hero, một trong số đó có thể bị tấn công để thực thi mã từ xa trên các thiết bị NAS của hãng. Danh sách lỗ hổng ảnh hưởng tới QTS 5.1.x và QuTS hero h5.1.x như sau:

- **CVE-2024-21902:** Lỗ hổng Incorrect Permission Assignment for Critical Resource, cho phép đối tượng tấn công sử dụng tài khoản người dùng đã xác thực đọc hoặc sửa đổi tài nguyên qua mạng.
- **CVE-2024-27127:** Lỗ hổng double free cho phép đối tượng tấn công sử dụng tài khoản người dùng đã xác thực khả năng thực thi mã tùy ý thông qua mạng.
- **CVE-2024-27128, CVE-2024-27129, và CVE-2024-27130:** Bộ các lỗ hổng buffer overflow cho phép đối tượng tấn công sử dụng tài khoản người dùng đã xác thực khả năng thực thi mã tùy ý thông qua mạng.

Các lỗ hổng này yêu cầu sử dụng tài khoản hợp pháp trên thiết bị NAS để khai thác và đã được vá trong phiên bản QTS 5.1.7.2770 và QuTS hero h5.1.7.2770. Lỗ hổng CVE-2024-27130 do hàm "strcpy" trong "No_Support_ACL" được sử dụng không an toàn bởi yêu cầu get_file_size trong script share.cgi, script này được dùng khi chia sẻ file media với người dùng ngoài hệ thống. Để khai thác, đối tượng tấn công cần tham số "SSID" phù hợp, tham số này chỉ được tạo ra khi người dùng NAS chia sẻ file. Cả QTS 4.x và 5.x đều kích hoạt chức năng Address Space Layout Randomization (ASLR), khiến việc khai thác lỗ hổng khó khăn hơn.

Bản vá của QNAP được phát hành 4 ngày sau khi một cơ quan bảo mật tại Singapore công bố thông tin về 15 lỗ hổng, trong đó có 4 lỗ hổng cho phép đối tượng tấn công bỏ qua xác thực và thực thi mã tùy ý. Bốn lỗ hổng này, với mã định danh từ CVE-2023-50361 đến CVE-2023-50364, đã được QNAP vá vào ngày 25/04/2024.

Lưu ý rằng, lỗ hổng CVE-2024-27131 (giả mạo log bằng cách sử dụng x-forwarded-for để ghi lại sự kiện tải xuống dưới dạng yêu cầu từ một nguồn gốc tùy ý) hiện vẫn chưa được QNAP sửa.

Nhà sản xuất bổ sung thông tin rằng đây là một phần của thiết kế ban đầu và yêu cầu điều chỉnh trong giao diện người dùng (UI) của QuLog Center. Chức năng này sẽ được sửa trong phiên bản QTS 5.2.0.

Khuyến nghị người dùng cập nhật phiên bản mới nhất cho QTS và QuTS hero sớm nhất có thể nhằm bảo vệ họ khỏi các mối đe dọa của các lỗ hổng đã được khai thác trước đó trên QNAP NAS.

Nguồn: https://thehackernews.com/2024/05/qnap-patches-new-flaws-in-qts-and-quts.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 **1.540** lỗ hổng, trong đó có 421 lỗ hổng mức Cao, 564 lỗ hổng mức Trung bình, 74 lỗ hổng mức Thấp và 481 lỗ hổng chưa đánh giá. Trong đó có ít nhất 229 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 Veeam, NextGen và GitHub, cụ thể là như sau:

- **CVE-2024-29849 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Veeam Backup Enterprise Manage cho phép đối tượng tấn công sau khi khai thác có thể đăng nhập vào trình quản trị web dưới tài khoản người dùng bất kì. Hiện lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.
- **CVE-2023-43208 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên NextGen Healthcare Mirth Connect trước phiên bản 4.1, xảy ra do việc vá lỗi chưa hoàn chỉnh của lỗ hổng CVE-2023-37679. Đối tượng tấn công khai thác thành công lỗ hổng có thể thực thi mã từ xa. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.
- **CVE-2024-4985 (Điểm CVSS: N/A):** Lỗ hổng bỏ qua chức năng xác thực tồn tại trên sản phẩm GitHub Enterprise Server (GHES) sử dụng xác thực SAML single sign-on (SSO). Đối tượng tấn công khai thác lỗ hổng có thể giả mạo yêu cầu SAML để yêu cầu quyền truy cập vào tài khoản quản trị của sản phẩm, qua đó cho phép đối tượng truy cập và thực hiện các hành vi trái phép. Hiện lỗ hổng đang bị khai thác trong môi trường thực tế.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-29849	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Veeam Backup Enterprise Manage - Mô tả: Lỗ hổng 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-2024-29849
2	CVE-2023-43208	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: NextGen Healthcare Mirth Connect - 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-2023-43208
3	CVE-2024-4985	- Điểm CVSS: N/A - Ảnh hưởng: GitHub Enterprise Server (GHES) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép sau khi đạt quyền truy cập vào tài khoản quản trị. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-4985
4	CVE-2024-4367	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Mozilla Firefox, Firefox ESR, Mozilla Thunderbird. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã JavaScript 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-2024-4367
5	CVE-2024-22120	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Zabbix - 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-2024-22120

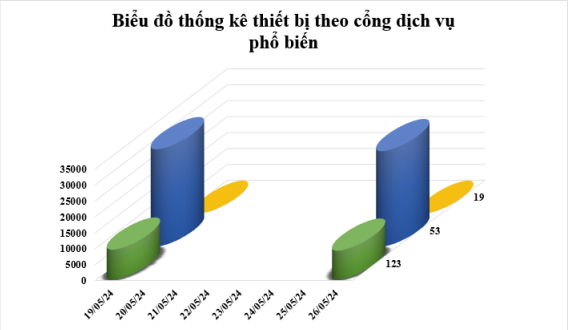
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-32002	- Điểm CVSS: 9.0 (Nghiêm trọng) - Ảnh hưởng: Git - 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-2024-32002
7	CVE-2024-4323	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Fluent Bit. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã tùy 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-2024-4323
8	CVE-2024-4761	- Điểm CVSS: Chưa xác định - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi ghi ngoài bộ nhớ. - 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-2024-4761
9	CVE-2024-4947	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome. - 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-2024-4947
10	CVE-2024-27130	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: QNAP QTS, QNAP QuTS hero. - 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-2024-27130

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 **39.100** (giảm so với tuần trước **40.030**) 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.

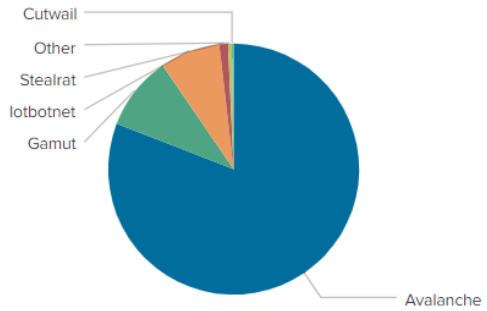


Tấn công Web

Trong tuần, có **118** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 69 trường hợp tấn công lừa đảo (Phishing), 49 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	xjpakmdcfuqe.ru
disorderstatus.ru	omfghellobrosjda38.org
atomictrivia.ru	andall.servicesql.info
amnsreiuojy.ru	restless.su
restlesz.su	cicqdaqtrws.info
hzmksreiuojy.ru	76236osm1.ru
xjpakmdcfuqe.biz	facialwaxmaxfaxlax3.com
xjpakmdcfuqe.com	griefcube.cc
ivz7x63ymy.ru	bbuildersget.com
xjpakmdcfuqe.in	menufantimemean.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **274** 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://miaoniter[.]com/	Website giả mạo sàn TMĐT Amazon
2	https://amazonl3[.]com/	Website giả mạo sàn TMĐT Amazon
3	https://www[.]amatvip36sc[.]cc/	Website giả mạo sàn TMĐT Amazon
4	https://vssid[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
5	https://da6555[.]com/	Website giả mạo sàn TMĐT Lazada
6	https://mbfn-fic[.]com/	Website giả mạo Mbbank
7	https://mbcanhan-cskh[.]com/	Website giả mạo Mbbank
8	https://www[.]mbdkb[.]com/	Website giả mạo Mbbank
9	https://phattai247[.]com/	Website giả mạo Mbbank
10	https://tinchaphd[.]com/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
11	https://ocb[.]chamsocthekhachhang-uudai-tructuyen[.]com/	Website giả mạo Ngân hàng TMCP Phương Đông
12	https://khvib-canhan[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
13	https://tpb-vayuudai[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
14	https://tpbankvn[.]workplace[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
15	https://soppe68[.]shop/	Website giả mạo sàn TMĐT Shopee
16	https://sp15569p[.]com/	Website giả mạo sàn TMĐT Shopee
17	https://www[.]shopee123[.]vip	Website giả mạo sàn TMĐT Shopee
18	https://tdkt01[.]com/	Website giả mạo sàn TMĐT Tiki
19	https://vntiki11[.]com/	Website giả mạo sàn TMĐT Tiki
20	https://ca-nhan-vpb[.]com/	Website giả mạo 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