NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 46 (11/11/2024 – 17/11/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công mạng Việt Nam tấn công các tổ chức tại châu Âu và châu Á bằng mã độc PXA Stealer.

- **Cảnh báo:** Lỗ hổng nghiêm trọng trên tường lửa PAN-OS bị khai thác trong thực tế.

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: 5.249** 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 tấn công mạng Việt Nam tấn công các tổ chức tại châu Âu và châu Á bằng mã độc PXA Stealer"

Các chuyên gia bảo mật vừa phát hiện một nhóm tấn công mạng có nguồn gốc từ Việt Nam, đang thực hiện chiến dịch đánh cắp thông tin từ các tổ chức chính phủ và giáo dục tại châu Âu, châu Á, nhóm này sử dụng một mã độc mới được viết bằng Python có tên PXA Stealer.

Chiến dịch này tập trung vào việc thu thập các dữ liệu nhạy cảm, bao gồm thông tin xác thực của tài khoản trực tuyến, ứng dụng VPN/FTP, thông tin tài chính, cookie trình duyệt và dữ liệu từ các phần mềm chơi game. Theo ghi nhận, mã độc PXA Stealer có khả năng giải mã mật khẩu chính của trình duyệt và sử dụng mật khẩu này để đánh cắp thông tin đăng nhập được lưu trữ.

Dấu hiệu kết nối từ Việt Nam được xác định thông qua một số chú thích viết bằng tiếng Việt trong mã nguồn và một tài khoản Telegram có tên "Lone None". Đáng chú ý, tài khoản này sử dụng ảnh đại diện là logo của Bộ Công an Việt Nam.

Trong quá trình điều tra, các chuyên gia bảo mật phát hiện nhóm đối tượng này có hoạt động buôn bán thông tin tài khoản Facebook, Zalo và SIM điện thoại trên kênh Telegram "Mua Bán Scan MINI." Kênh này trước đó đã được xác định thuộc sở hữu của nhóm CoralRaider. Không chỉ vậy, tài khoản Lone None còn tham gia vào một nhóm Telegram khác của CoralRaider với tên gọi "Cú Black Ads - Dropship." Tuy nhiên, mối liên hệ chính thức giữa hai nhóm này hiện vẫn chưa được xác nhận.

Công cụ và phương pháp tấn công

Nhóm tấn công này sử dụng các công cụ tự động để quản lý tài khoản, bao gồm: Công cụ tạo tài khoản Hotmail hàng loạt, công cụ thu thập email, công cụ chỉnh sửa cookie Hotmail hàng loạt.

Các công cụ này thường được cung cấp kèm mã nguồn, cho phép người dùng tuỳ chỉnh theo ý muốn. Bên cạnh đó, chúng còn được quảng bá trên các trang như **aehack[.]com** và hướng dẫn sử dụng được chia sẻ qua YouTube.

Chiến dịch tấn công sử dụng các email phishing có chứa file đính kèm định dạng ZIP, bên trong bao gồm:

- Một **loader** viết bằng Rust.
- Một thư mục ẩn chứa các script batch cho Windows.
- Một file PDF ngụy trang.

Nguồn: https://thehackernews.com/2024/11/vietnamese-hacker-group-deploys-new-pxa.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm tấn công mạng Việt Nam tấn công các tổ chức tại châu Âu và châu Á bằng mã độc PXA Stealer"

Khi file ZIP được mở, các script batch sẽ kích hoạt file PDF ngụy trang (một mẫu đơn xin việc Glassdoor) đồng thời thực thi các lệnh PowerShell để: Tải về và chạy payload nhằm vô hiệu hóa phần mềm diệt virus trên thiết bị và triển khai mã độc **PXA Stealer**.

Điểm đáng chú ý của PXA Stealer

Mã độc này đặc biệt tập trung vào việc đánh cắp cookie Facebook, sử dụng chúng để xâm nhập tài khoản và khai thác **Facebook Ads Manager** cùng **Graph API** để thu thập thêm thông tin liên quan đến tài khoản và các hoạt động quảng cáo. Việc nhắm mục tiêu vào tài khoản quảng cáo Facebook và các doanh nghiệp là một đặc điểm phổ biến trong các nhóm tin tặc có nguồn gốc từ Việt Nam.

Thông tin về chiến dịch PXA Stealer được công bố trong bối cảnh một cơ quan bảo mật khác đã công bố thông tin chi tiết về một chiến dịch tấn công mạng được ghi nhận từ giữa tháng 4/2023, phát tán mã độc StrelaStealer tới các tổ chức châu Âu thông qua các email lừa đảo giả dạng hóa đơn.

Các mã độc đánh cắp thông tin hiện đang ngày càng trở nên phổ biến, thể hiện rõ qua sự phát triển không ngừng của các chủng mã độc nổi bật như RECORDSTEALER (hay còn gọi là RecordBreaker, Raccoon Stealer V2) và Rhadamanthys. Bên cạnh đó, các mã độc mới thuộc dạng này cũng liên tục xuất hiện, điển hình như Amnesia Stealer và Glove Stealer.

Một số IoC được ghi nhận:

hxxps[://]tvdseo[.]com/file/synaptics[.]zip	hxxps[://]tvdseo[.]com/file/PXA/PXA_PURE_ENC
hxxps[://]tvdseo[.]com/file/Adonis/AdFnis_Bot	hxxps[://]tvdseo[.]com/file/PXA/PXA_PURE_ENC
hxxps[://]tvdseo[.]com/file/Adonis/Adonis_XW_ENC	hxxps[://]tvdseo[.]com/file/Adonis/Adonis_Bot0
hxxps[://]tvdseo[.]com/file/STC/STC_XW_ENC	hxxps[://]tvdseo[.]com/file/STC/STC_PURE[.]b64
hxxps[://]tvdseo[.]com/file/STC/STC_OTO	hxxps[://]tvdseo[.]com/file/PXA/Cookie_Ext[.]zip
hxxps[://]tvdseo[.]com/file/STC/STC_BOT	hxxps[://]tvdseo[.]com/file/PXA/PXA_BOT
hxxps[://]tvdseo[.]com/file/STC/STC_PUP	hxxps[://]tvdseo[.]com/file/PXA/PXA_BOT
hxxps[://]tvdseo[.]com/file/STC/STC_PURE_ENC	hxxps[://]tvdseo[.]com/file/Adonis/Adonis_Bot
tvdseo[.]com	hxxps[://]tvdseo[.]com/file/STC/Cookie_Ext[.]zip

Nguồn: https://thehackernews.com/2024/11/vietnamese-hacker-group-deploys-new-pxa.html

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng nghiêm trọng trên tường lửa PAN-OS bị khai thác trong thực tế"

Gần đây, Palo Alto Networks đã công bố một danh sách IoC mới, chỉ một ngày sau khi xác nhận sự khai thác thực tế của một lỗ hổng zero-day ảnh hưởng đến giao diện quản lý tường lửa PAN-OS. Theo đó, hãng ghi nhận các hành vi độc hại xuất phát từ các địa chỉ IP 136.144.17[.], 173.239.218[.]251 và 216.73.162[.], nhắm đến các địa chỉ IP công cộng sử dụng để triển khai giao diện quản lý PAN-OS. Tuy nhiên, những địa chỉ IP này có thể thuộc mạng VPN, nơi có thể có cả người dùng hợp pháp.

Lỗ hổng zero-day này hiện chưa có mã định dạng và có điểm CVSS là 9.3, được xếp vào mức Nghiêm trọng. Lỗ hổng cho phép đối tượng tấn công khai thác lỗi trên giao diện quản lý để triển khai webshell lên hệ thống, từ đó mở ra khả năng truy cập từ xa lâu dài và thực thi mã từ xa. Tính phức tạp của cuộc tấn công được đánh giá là "thấp" và không yêu cầu người dùng phải tương tác hay có quyền truy cập đặc biệt để có thể bi khai thác.

Ngoài ra, điểm CVSS của lỗ hổng này có thể giảm xuống còn 7.5 nếu giao diện quản lý được cấu hình để chỉ cho phép một số IP nhất định truy cập. Điều này buộc đối tượng tấn công phải có quyền truy cập hoặc sử dụng những IP này trước khi thực hiện khai thác.

Trước đó, Palo Alto Networks đã khuyến nghị người dùng tăng cường các biện pháp bảo mật cho giao diện quản lý sau khi nhận được báo cáo về một lỗ hổng cho phép thực thi mã từ xa. Hiện tại, chưa có thông tin chi tiết về cách thức lỗ hổng zero-day này được phát hiện, cũng như về đối tượng tấn công và mục tiêu của các cuộc tấn công liên quan.

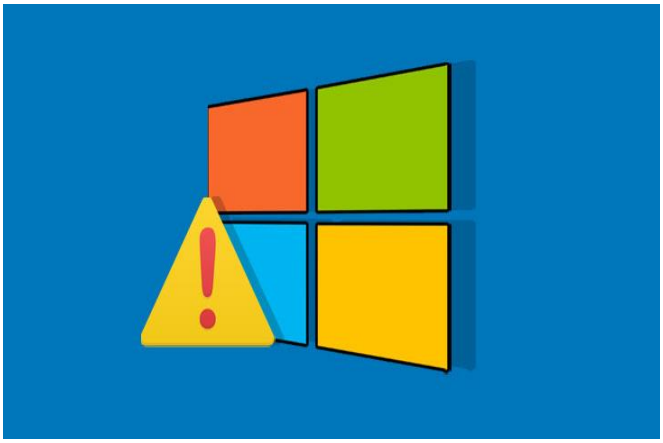
Lỗ hổng hiện vẫn chưa được vá, vì vậy người dùng cần chủ động giới hạn truy cập vào giao diện quản lý tường lửa để giảm thiểu nguy cơ bị khai thác.

Thông tin này được công bố trong bối cảnh ba lỗ hổng an toàn thông tin mức nghiêm trọng khác của hãng, gồm CVE-2024-5910, CVE-2024-9463 và CVE-2024-9465, đang bị khai thác trong thực tế. Tuy nhiên, hiện tại chưa có bằng chứng nào cho thấy sự khai thác của các lỗ hổng này có liên quan đến nhau.

Nguồn: https://thehackernews.com/2024/11/pan-os-firewall-vulnerability-under.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 **919** lỗ hổng, trong đó có 315 lỗ hổng mức Cao, 371 lỗ hổng mức Trung bình, 24 lỗ hổng mức Thấp và 209 lỗ hổng chưa đánh giá. Trong đó có ít nhất 104 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 Microsoft, Apache và Laravel, cụ thể là như sau:

- **CVE-2024-43451 (Điểm CVSS: 6.5 – Trung bình):** Lỗ hổng tồn tại trên Microsoft Windows 10, Windows 11, Windows Server 2022 cho phép đối tượng tấn công đánh cắp mã băm NTLM từ hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2021-44228 (Điểm CVSS: 10.0 – Nghiêm trọng):** Hay còn được gọi là Log4Shell là lỗ hổng tồn tại trên Apache cho phép đối tượng tấn công thực thi mã từ xa nạp vào từ máy chủ LDAP khi chức năng thay thế message lookup được sử dụng thông qua việc điều khiển tham số thông điệp log, control log. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-52301 (Điểm CVSS: Chưa xác định):** Lỗ hổng tồn tại trên framework Laravel cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép lên môi trường web thông qua các câu truy vấn độc hại. Hiện lỗ hổng chưa có mã khai thác và đang bị khác thác trong thực tế bởi các nhóm tấn công.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-43451	- Điểm CVSS: 6.5 (Trung bình) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2022 - 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-2024-43451
2	CVE-2021-44228	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Apache - 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-2021-44228
3	CVE-2024-52301	- Điểm CVSS: Chưa xác định - Ảnh hưởng: Laravel framework - 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-2024-52301
4	CVE-2024-35250	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện 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-2024-35250
5	CVE-2024-47575	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: FortiManager - 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-2024-47575

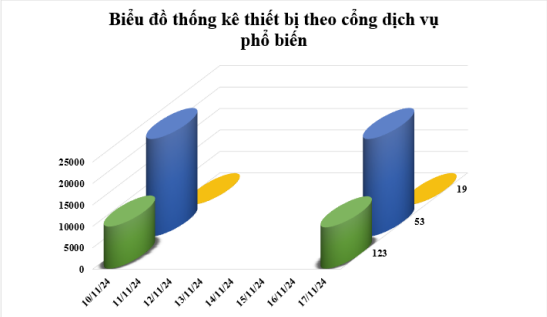
TOP 10 lỗ hổng đáng chú ý trong tuần

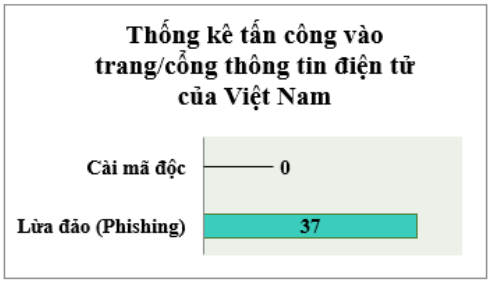
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-9264	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Grafana - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi Command Injection - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-9264
7	CVE-2024-10924	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Plugin "Really Simple Security" cho WordPress - 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-2024-10924
8	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 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-2024-4577
9	CVE-2024-49039	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Windows 10 - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện 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-2024-49039
10	CVE-2024-21534	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Gói "jsonpath-plus" - 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-2024-21534

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 **32.424** (giảm so với tuần trước **32.599**) 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.



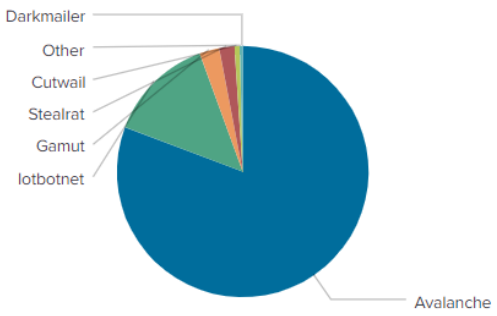


Tấn công Web

Trong tuần, có **37** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 37 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

disorderstatus.ru	gjogvvpsf.biz
differentia.ru	morphed.ru
atomictrivia.ru	ygiudewsqhct.in
a.asense.in	hzmksreiuojy.in
sdk.asense.in	hzmksreiuojy.ru
statis.multispacesext.net	a.deltaheavy.ru
ydqlnw.info	xjpakmdcfuqe.biz
thesecond.in	egksyqv.info
amnsreiuojy.ru	restlesz.su
cp.ceddi8ub.ru	mrkniokqsi.ru

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **5.249** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **220** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **5.029** 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://sellings-global[.]com/fedex	Website giả mạo sàn TMĐT Amazon
2	https://www[.]applecenter[.]info[.]vn/	Website giả mạo Apple
3	https://dichvucongbca[.]com/	Website giả mạo Bộ Công an
4	https://www[.]ihomeficvn[.]com	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
5	lazada[.]ac	Website giả mạo sàn TMĐT Lazada
6	hdbank[.]uudaikhachhang-trungtamcapnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
7	https://mmmbonline[.]com	Website giả mạo Ngân hàng TMCP Quân đội
8	https://www[.]iplus-fianc24h[.]online	Website giả mạo Ngân hàng TMCP Quân đội
9	vib[.]khach-hang-nang-han-muc-ca-nhan[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	https://vpbank[.]uudaikhachhang-uudaithe-thang11[.]com[.]vn/	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
11	https://sp56188p[.]com/my	Website giả mạo sàn TMĐT Shopee
12	https://nzu62352s[.]com/order	Website giả mạo sàn TMĐT Shopee
13	https://sp5583p[.]com/my	Website giả mạo sàn TMĐT Shopee
14	www[.]evnspc[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
15	https://www[.]tikifreeship[.]cc	Website giả mạo sàn TMĐT Tiki
16	https://af[.]tiktok25881[.]shop/	Website giả mạo TikTok
17	https://evaluatetravels[.]com/recharge	Website giả mạo Traveloka
18	https://viettel-post[.]cfd/vn/	Website giả mạo ViettelPost
19	https://nhantienquoctej13[.]vercel[.]app/dichvunhantien	Website giả mạo Western Union
20	https://zloweb[.]me/	Website giả mạo Zalo

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