NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 29 (15/07/2024 – 21/07/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Void Banshee khai thác lỗ hổng Microsoft MHTML để phát tán mã độc Atlantida Stealer.

- **Cảnh báo:** Cisco cảnh báo về lỗ hổng nghiêm trọng ảnh hưởng đến phiên bản On-Prem của phần nềm Smart Software Manager.

- **Thông tin:** Cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike.

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: 1.353** 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 APT Void Banshee khai thác lỗ hổng Microsoft MHTML để phát tán mã độc Atlantida Stealer."

Nhóm APT Void Banshee đã bị phát hiện lợi dụng một lỗ hổng mới được công bố chi tiết trong động cơ trình duyệt Microsoft MHTML (khai thác lỗi zero-day) để phát tán mã độc đánh cắp thông tin có tên Atlantida.

Lỗ hổng này có mã CVE-2024-38112, được sử dụng trong chuỗi tấn công nhiều giai đoạn với các tệp đường dẫn internet (URL) làm trọng điểm. Microsoft đã đề cập đến lỗ hổng này trong bản vá Patch Tuesday gần đây. Theo Microsoft, đây là một lỗi giả mạo (spoofing) tồn tại trong động cơ trình duyệt MSHTML (hay Trident) được sử dụng trong trình duyệt Internet Explorer. Tuy nhiên, Zero Day Initiative (ZDI) lại cho rằng đây là một lỗ hổng thực thi mã từ xa.

Trong chiến dịch của nhóm APT, các email spear-phishing có chứa đường dẫn đến các tệp ZIP được lưu trên trang web của nhóm tấn công đã được sử dụng. Các tệp ZIP này chứa các tệp URL khai thác lỗ hổng CVE-2024-38112 để điều hướng người dùng đến một trang web lưu trữ tệp HTML Application (HTA) độc hại.

Khi người dùng mở tệp HTA, một tập lệnh Visual Basic Script (VBS) sẽ được thực thi, tải xuống và thực thi một tập lệnh PowerShell có chức năng tải trình tải trojan .NET. Trình tải này sau đó sử dụng shellcode để giải mã và thực thi mã độc Atlantida trong bộ nhớ của tiến trình RegAsm.exe.

Mã độc Atlantida, được phát triển từ các mã độc mã nguồn mở như NecroStealer và PredatorTheStealer, có chức năng trích xuất tệp, chụp ảnh màn hình, vị trí địa lý và dữ liệu nhạy cảm từ các trình duyệt web và các ứng dụng khác, bao gồm Telegram, Steam, FileZilla và các ví tiền điện tử.

Nguồn: https://thehackernews.com/2024/07/void-banshee-apt-exploits-microsoft.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Void Banshee khai thác lỗ hổng Microsoft MHTML để phát tán mã độc Atlantida Stealer."

Không có nhiều thông tin về nhóm APT Void Banshee, ngoại trừ việc nhóm này có lịch sử nhằm mục tiêu vào khu vực Bắc Mỹ, Châu Âu và Đông Nam Á để thực hiện các chiến dịch đánh cắp dữ liệu và trục lợi tài chính.

Thông tin về nhóm và việc khai thác lỗ hổng này được công bố sau khi Cloudflare tiết lộ rằng nhiều nhóm tấn công đang nhanh chóng kết hợp các khai thác PoC (proof-of-concept) vào chiến dịch của mình. Trong trường hợp của lỗ hổng CVE-2024-27198, lỗ hổng đã bị khai thác chỉ sau 22 phút kể từ lúc thông tin được công bố.

Ngoài ra, thông tin trong bài viết này cũng tiếp nối sự phát hiện về một chiến dịch tấn công khác sử dụng quảng cáo trên Facebook để phát tán mã độc SYS01stealer thông qua các giao diện Windows giả, nhằm chiếm đoạt tài khoản doanh nghiệp trên Facebook và tiếp tục phát tán mã độc.

Một số IoC được ghi nhận:

hxxps[://]fullgasesspa[.]cl/tet/download[.]php
hxxp[://]cbmelipilla[.]cl/te/test1[.]html
hxxps[://]cbmelipilla[.]cl/te/hhhh2[.]php
hxxps[://]hostalaskapatagonia[.]com/tt/tedfd[.]te
hxxps[://]hostalaskapatagonia[.]com/tt/become[.]txt
hxxp[://]h[.]com:8000/test1[.]html
185[.]172[.]128[.]95

Nguồn: https://thehackernews.com/2024/07/void-banshee-apt-exploits-microsoft.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Cisco cảnh báo về lỗ hổng nghiêm trọng ảnh hưởng đến phiên bản On-Prem của phần nềm Smart Software Manager."

Trong tuần qua, Cisco đã phát hành bản vá cho hai lỗ hổng an toàn thông tin nghiêm trọng ảnh hưởng đến Smart Software Manager On-Prem (Cisco SSM On-Prem), trong đó có một lỗ hổng nghiêm trọng cho phép đối tượng tấn công thay đổi mật khẩu của bất kỳ người dùng nào, bao gồm cả tài khoản quản trị viên.

Lỗ hổng có mã CVE-2024-20419 (Điểm CVSS: 10.0) xuất phát từ việc triển khai không đúng cách quy trình thay đổi mật khẩu trên Smart Software Manager On-Prem (Cisco SSM On-Prem). Lỗ hổng này cho phép đối tượng tấn công gửi các yêu cầu HTTP được tinh chỉnh đến thiết bị bị ảnh hưởng để khai thác lỗ hổng. Khi khai thác thành công, đối tượng tấn công có thể truy cập vào giao diện web UI hoặc API với quyền của người dùng bị xâm phạm.

Lỗ hổng này ảnh hưởng đến tất cả các phiên bản Cisco SSM On-Prem từ 8-202206 trở xuống và đã được vá trong phiên bản 8-202212. Riêng phiên bản 9 của giải pháp này không bị ảnh hưởng.

Cisco thông báo rằng không có biện pháp khắc phục nào ngoài việc cập nhật bản vá, và hiện chưa có ghi nhận về việc lỗ hổng này bị khai thác trong môi trường thực tế. Ngoài ra, Cisco cũng đã khắc phục một lỗ hổng nghiêm trọng khác trong Secure Email Gateway (SEG), mã **CVE-2024-20401** (Điểm CVSS: 9.8). Lỗ hổng này liên quan đến việc ghi file cho phép đối tượng tấn công tạo thêm người dùng với quyền root và gây ra sự cố nghiêm trọng cho thiết bị bằng cách gửi các email có file đính kèm độc hại. Để lỗ hổng này phát huy tác dụng, thiết bị SEG phải đang chạy phiên bản Cisco AsyncOS bị ảnh hưởng và đáp ứng các điều kiện sau:

- Chức năng phân tích file (thuộc Cisco Advanced Malware Protection) hoặc chức năng lọc nội dung phải được bật và áp dụng cho chính sách email gửi tới.
- Phiên bản của công cụ Content Scanner Tools cũ hơn 23.3.0.4823.

Bản vá cho lỗ hổng **CVE-2024-20401** đã có sẵn trong các phiên bản Content Scanner Tools từ 23.3.0.4823 trở lên và được tích hợp mặc định trong Cisco AsyncOS cho Cisco Secure Email Software các phiên bản từ 15.5.1-055 trở lên.

Nguồn: https://thehackernews.com/2024/07/cisco-warns-of-critical-flaw-affecting.html

Tin tức An toàn thông tin

"Thông tin: Cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike."

Trong quá trình giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông, đã phát hiện rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike. Sự cố trên đã gây ảnh hưởng tới nhiều cơ quan, tổ chức trên thế giới, trong đó bao gồm Đức, Singapore, Tây Ban Nha, Ấn Độ, Israel, Nam Phi,….

Cụ thể, các máy tính chạy hệ điều hành Windows 10 và cài đặt phần mềm Falcon Sensor của hãng CrowdStrike đều gặp lỗi màn hình xanh (Blue Screen Of Death – BSOD và không thể khởi động lại để hoạt động bình thường. Điều này gây ảnh hưởng tới hệ thống thông tin và hoạt động của cá nhân, cơ quan, tổ chức. Nhà phát triển CrowdStrike đã đưa ra thông báo xác nhận rủi ro và thực hiện khôi phục phần mềm Falcon Sensor để tránh gây thêm ảnh hưởng tới thiết bị của người dùng.

Hướng dẫn khắc phục đối với các thiết bị đã bị ảnh hưởng:

Bước 1: Khởi động lại máy tính và vào chế độ Safe Mode hoặc Windows Recovery Environment.

Bước 2: Truy cập thư mục "C:\Windows\System32\drivers\CrowdStrike"

Bước 3: Xóa bỏ các tập tin có định dạng "C-00000291*.sys" (tập tin có định dạng .sys và tên bắt đầu bằng chuỗi C-00000291)

Bước 4: Khởi động lại máy tính và sử dụng như bình thường.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý Đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý Đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi rủi ro an toàn thông tin trên. Chủ động theo dõi các thông tin liên quan nhằm thực hiện khắc phục rủi ro trong trường hợp bị ảnh hưởng.
2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng
3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

Nguồn: https://khonggianmang.vn/alert/canh-bao-rui-ro-an-toan-thong-tin-lien-quan-en-san-pham-cua-crowd-

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 **989** lỗ hổng, trong đó có 406 lỗ hổng mức Cao, 277 lỗ hổng mức Trung bình, 18 lỗ hổng mức Thấp và 288 lỗ hổng chưa đánh giá. Trong đó có ít nhất 121 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 OpenSSH, GeoServer và ngôn ngữ lập trình PHP, cụ thể là như sau:

- **CVE-2024-36401 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên GeoServer cho phép đối tượng tấn công thực thi mã từ xa thông qua việc truyền vào dữ liệu độc hại tới các phiên GeoServer cấu hình mặc định. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-6387 (Điểm CVSS: 8.1 – Cao):** Lỗ hổng tồn tại trên máy chủ OpenSSH cho phép đối tượng tấn công khai thác lỗi Race Condition, 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-2024-4577 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên ngôn ngữ lập trình PHP phiên bản 8.1.* (cũ hơn 8.1.29), 8.2.* (cũ hơn 8.2.20), 8.3.* (cũ hơn 8.3.8), khi được sử dụng trong Apache và PHP-CGI của Windows. Đối tượng tấn công có thể khai thác lỗ hổng bằng cách gửi đi các tham số độc hại cho PHP duyệt, qua đó có thể làm lộ mã nguồn của script, thực thi code PHP tùy ý trên máy chủ. Hiện lỗ hổng đã có mã khai thác và 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-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: GeoServer - 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-2024-36401
2	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: OpenSSH - 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-2024-6387
3	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 tùy ý, 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
4	CVE-2024-22274	- Điểm CVSS: 7.2 (Cao) - 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-2024-22274
5	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11. - 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-2024-38112

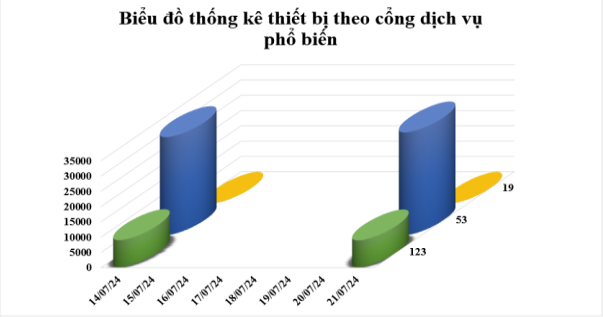
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-20419	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Cisco Smart Software Manager On-Prem (SSM On-Prem). - 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-2024-20419
7	CVE-2024-33544	- Điểm CVSS: 9.3 (Nghiêm trọng) - Ảnh hưởng: AA-Team WZone - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công SQL 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-2024-33544
8	CVE-2024-27198	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: JetBrains TeamCity - 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-2024-27198
9	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
10	CVE-2024-20401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Cisco Secure Email Gateway - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, 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-2024-20401

Thống kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

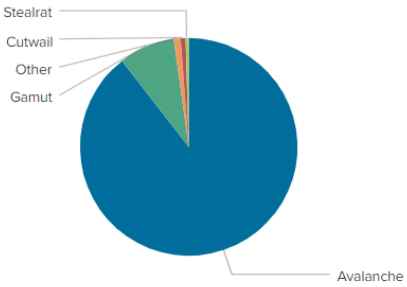
Tấn công DRDoS

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 **42.408** (tăng so với tuần trước **40.952**) 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 **100** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 89 trường hợp tấn công lừa đảo (Phishing), 11 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	spaines.pw
amnsreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	www.hnmrw.net
hzmksreiuojy.ru	mcnodes.zapto.org
restlesz.su	focusdate.com
xjpakmdcfuqe.com	elitiorecfreetoo.cc
xjpakmdcfuqe.ru	datefree.info
xjpakmdcfuqe.in	aurasport.net

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **1.353** 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://vssid[.]govnn[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://icchanoi[.]net/	Website giả mạo Công ty Cổ phần Đầu tư Quốc tế ICC Hà Nội
3	https://homecredit[.]hethongvaynhanh247[.]com/	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
4	https://mfacebook-com[.]vn/	Website giả mạo Facebook
5	https://bethivetranh2024[.]weebly[.]com	Website giả mạo Facebook
6	https://www[.]hethongnhanvien[.]com	Website giả mạo sàn TMĐT Lazada
7	https://da1215[.]com	Website giả mạo sàn TMĐT Lazada
8	https://lazadaevent[.]com/	Website giả mạo sàn TMĐT Lazada
9	https://www[.]momoshopvip[.]com	Website giả mạo MoMo
10	https://www[.]baovietcom[.]vip/	Website giả mạo Ngân hàng TMCP Bảo Việt
11	https://vietinbankamc[.]vn	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
12	https://khtechcanhan[.]com/	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
13	https://mcqdvn[.]com	Website giả mạo Ngân hàng TMCP Quân đội
14	https://centralmarketing[.]online/	Website giả mạo Ngân hàng Worldbank Việt Nam
15	https://nze98582s[.]com/	Website giả mạo sàn TMĐT Shopee
16	https://www[.]tikifreeship[.]vip/	Website giả mạo sàn TMĐT Tiki
17	https://tdke00[.]com/	Website giả mạo sàn TMĐT Tiki
18	https://www[.]vntiki[.]vip	Website giả mạo sàn TMĐT Tiki
19	https://tdke02[.]com	Website giả mạo sàn TMĐT Tiki
20	https://xacnhanthutuchoantra[.]us/	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