NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 39 (25/9/2023 – 01/10/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT BlackTech xâm nhập vào router của Cisco nhằm vào các tổ chức tại Mỹ và Nhật Bản.

- **Cảnh báo:** Lỗ hổng bảo mật Nghiêm trọng trong Exim: Nguy cơ tấn công từ xa hệ thống máy chủ Email.

2. Điểm yếu, lỗ hổng

- **656** lỗ hổng được công bố và cập nhật.

- **07** lỗ hổng, nhóm lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Tấn công lừa đảo người dùng Việt Nam: 363** 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://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT BlackTech xâm nhập vào router của Cisco nhằm vào các tổ chức tại Mỹ và Nhật Bản"

Gần đây, nhóm APT BlackTech, được cho là có hậu thuẫn từ Trung Quốc, đã bị phát hiện trong quá trình xâm nhập vào các router mạng để tiến hành tấn công nhiều tổ chức khác nhau. Theo cơ quan điều tra, nhóm này đã thực hiện chiến dịch tấn công từ năm 2010 và gần đây đã thay đổi firmware của router Cisco để che giấu hoạt động trong khi nhắm mục tiêu tấn công vào các công ty có trụ sở chính tại Mỹ và Nhật Bản.

Phương thức tấn công

- BlackTech thường nhắm vào các router nhánh, những thiết bị nhỏ thường dùng trong văn phòng chi nhánh, đồng thời sử dụng kết nối tin cậy giữa nạn nhân và các người dùng khác trong mạng lưới mục tiêu.
- Sau khi chiếm được quyền quản trị viên, nhóm này bắt đầu điều chỉnh firmware để che giấu hoạt động và duy trì kết nối trong mạng.
- BlackTech sử dụng các biến thể của backdoor firmware để có thể bật/tắt tùy ý thông qua các gói tin TCP hoặc UDP.
- Trong một số trường hợp, BlackTech đã thay thế firmware cho một số router IOS của Cisco bằng phiên bản độc hại, từ đó duy trì kết nối backdoor và che giấu các hoạt động tấn công.

Thông tin về BlackTech

- Nhóm APT BlackTech thường sử dụng mã độc tùy chỉnh và công cụ dual-use. Đây là công cụ vừa giúp ích cho người dùng, vừa cho phép đối tượng tấn công sử dụng trong các chiến dịch tấn công.
- Chiến thuật living-off-the-land thường được nhóm này dùng để tận dụng các tính năng có sẵn trên các thiết bị và phần mềm bị xâm nhập. Ví dụ, họ có thể tắt chức năng ghi nhật ký trên các router để che giấu hoạt động của mình.
- Để tránh bị phát hiện, BlackTech thường xuyên cập nhật các công cụ tấn công và sử dụng các chứng thư số (Code Signing Certificates) để các phần mềm giả mạo trông đáng tin cậy hơn.

Sự lan rộng toàn cầu của các nhóm tấn công Trung Quốc

- Các nhóm tấn công có liên quan đến Trung Quốc đang toàn cầu hóa mục tiêu tấn công.
- Một chiến dịch gián điệp mạng trong nhiều năm của nhóm TAG-74 do Trung Quốc hậu thuẫn nhằm vào các tổ chức giáo dục, chính trị và chính phủ tại Hàn Quốc.
- Đáng chú ý, chiến dịch tấn công kéo dài 5 năm của nhóm EvilBamBoo nhằm vào cá nhân, tổ chức tại các vùng như Tibet, Uyghur và Đài Loan đang tạo ra nhiều mối lo ngại về an toàn thông tin. Hơn nữa, sự xuất hiện của các mã độc như ValleyRAT, Sainbox RAT và Purple Fox đang đang tạo thêm nhiều rủi ro về tấn công mạng đối với cá nhân và tổ chức trong khu vực.

Nguồn: https://cyware.com/news/blacktech-apt-breaks-in-cisco-routers-targets-us-and-japanese-companies-8e3cd028

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng bảo mật Nghiêm trọng trong Exim: Nguy cơ tấn công từ xa hệ thống máy chủ Email"

Một số lỗ hổng bảo mật đã được công bố trong Exim mail cho phép đối tượng tấn công thực thi mã từ xa và tiếp cận thông tin máy chủ.

Danh sách các lỗ hổng cụ thể là như sau:

- CVE-2023-42114 (Điểm CVSS: 3.7) – Lỗ hổng tiết lộ thông tin do lỗi đọc ngoài giới hạn trên Exim NTLM Challenge.
- CVE-2023-42115 (Điểm CVSS: 9.8) - Lỗ hổng cho phép thực thi mã từ xa do lỗi ghi ngoài giới hạn trên Exim AUTH.
- CVE-2023-42116 (Điểm CVSS: 8.1) - Lỗ hổng cho phép thực thi mã từ xa do tràn bộ nhớ đệm trên Stack của Exim SMTP Challenge.
- CVE-2023-42117 (Điểm CVSS: 8.1) - Lỗ hổng cho phép thực thi mã từ xa do việc không trung hòa đúng cách của các yếu tố đặc biệt trên Exim.
- CVE-2023-42118 (Điểm CVSS: 7.5) - Lỗ hổng cho phép thực thi mã từ xa do lỗi Integer Underflow trên Exim libspf2.
- CVE-2023-42119 (Điểm CVSS: 3.1) - Lỗ hổng tiết lộ thông tin do lỗi đọc ngoài giới hạn trên Exim dnsdb.

Nguồn: https://thehackernews.com/2023/09/new-critical-security-flaws-expose-exim.html

Trong danh sách trên, lỗ hổng nghiêm trọng nhất là CVE-2023-42115, lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa trên các phiên bản bị ảnh hưởng của Exim. Cụ thể, lỗ hổng này tồn tại ở dịch vụ SMTP trên cổng TCP 25 và phát sinh do sự thiếu sót trong quá trình xác thực hợp lệ của dữ liệu do người dùng cung cấp. Hậu quả của sự thiếu sót này là khả năng ghi dữ liệu ra ngoài giới hạn, cho phép đối tượng tấn công thực thi mã từ xa dưới danh tính của tài khoản dịch vụ.

Exim đã công bố bản vá các lỗ hổng CVE-2023-42114, CVE-2023-42115 và CVE-2023-42116. Tuy nhiên, đội ngũ bảo mật Exim còn đang chờ thông tin chi tiết về ba lỗ hổng còn lại. Trong trường hợp chưa có bản vá của các lỗ hổng này, các chuyên gia khuyến nghị người dùng nên hạn chế sử dụng ứng dụng Exim.

Đáng chú ý, đây không phải là lần đầu tiên Exim gặp vấn đề về bảo mật. Trước đó, đã phát hiện 21 lỗ hổng bảo mật có mã định danh là 21Nails, các lỗ hổng này cho phép đối tượng tấn công không cần xác thực việc thực thi mã từ xa mà vẫn chiếm được quyền root trên máy chủ Exim.

Vào tháng 05/2020, chính phủ Mỹ đã thông báo về việc các nhóm tấn công liên quan đến nhóm Sandworm đã khai thác thành công lỗ hổng CVE-2019-10149 trên Exim để xâm nhập vào các hệ thống mạng quan trọng. Báo cáo này càng trở nên quan trọng hơn bởi sự xuất hiện của một phương thức mới gọi là "spoofing chuyển tiếp", đối tượng tấn công sử dụng phương thức này để lợi dụng các lỗ hổng trong tác vụ chuyển tiếp email gửi các thông điệp giả mạo, ảnh hưởng đến tính toàn vẹn của dữ liệu.

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 **656** lỗ hổng, trong đó có 226 lỗ hổng mức Cao, 190 lỗ hổng mức Trung bình, 15 lỗ hổng mức Thấp và 225 lỗ hổng chưa đánh giá. Trong đó có ít nhất 146 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam: Nhóm 05 lỗ hổng trong Linux, Nhóm 77 lỗ hổng trong Apple, Nhóm 02 lỗ hổng trong Google, Nhóm 78 lỗ hổng trong Wordpress, Nhóm 13 lỗ hổng trong GitLab, Nhóm 18 lỗ hổng trong Cisco, Nhóm 25 lỗ hổng trong Huawei. Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- Linux: CVE-2023-42753, CVE-2023-5158,...

- Apple: CVE-2023-40431, CVE-2023-40443,...

- Google: CVE-2023-5186, CVE-2023-5186

- Wordpress: CVE-2023-4490, CVE-2023-4521,...

- GitLab: CVE-2023-0989, CVE-2023-2233,...

- Cisco: CVE-2023-20033, CVE-2023-20254,...

- Huawei: CVE-2023-41297, CVE-2023-41296,...

Thông tin điểm yếu, lỗ hổng

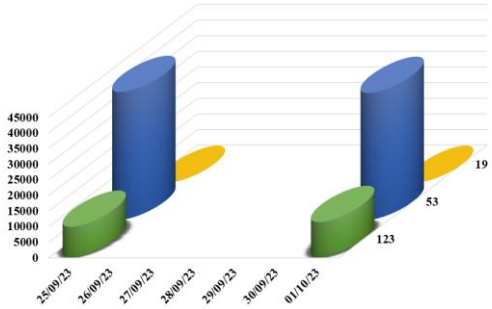
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-42753 CVE-2023-5158 CVE-2023-42756 ...	Nhóm 05 lỗ hổng trong Linux cho phép đối tượng tấn công thực hiện leo thang đặc quyền, tấn công từ chối dịch vụ, khai thác lỗi Buffer Overflow, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
2	Apple	CVE-2023-40431 CVE-2023-40443 CVE-2023-38586 ...	Nhóm 77 lỗ hổng trong Apple cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-5186 CVE-2023-5187	Nhóm 02 lỗ hổng trong Google cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-4490 CVE-2023-4521 CVE-2023-3547 ...	Nhóm 78 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công SQL Injection, tấn công CSRF, thực thi mã từ xa, khai thác lỗi XSS.	Chưa có thông tin xác nhận và bản vá
5	GitLab	CVE-2023-0989 CVE-2023-2233 CVE-2023-3115 ...	Nhóm 13 lỗ hổng trong GitLab cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Cisco	CVE-2023-20033 CVE-2023-20254 CVE-2023-20176 ...	Nhóm 18 lỗ hổng trong Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
7	Huawei	CVE-2023-41297 CVE-2023-41296 CVE-2022-48606 ...	Nhóm 25 lỗ hổng trong Huawei cho phép đối tượng tấn công thực hiện tấn công Command Injection, tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

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

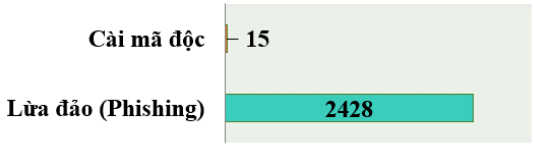
Tấn công DRDoS

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 **51.810**, (tăng so với tuần trước **50.584**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

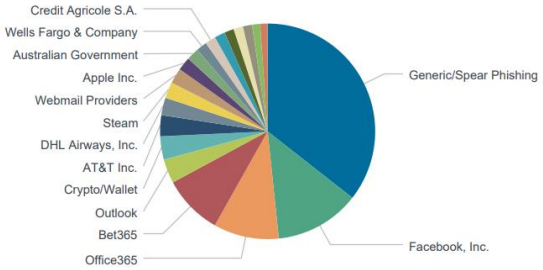


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **2443** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 2428 trường hợp tấn công lừa đảo (Phishing), 15 trường hợp tấn công cài cắm mã độc.



Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,v.v…Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và tính phí) như các mạng xã hội, Payment, Apple, Paypal,v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để đánh cắp tài khoản.

Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru: 14124 IP	hzmksreiuojy.ru: 224 IP
disorderstatus.ru: 6736 IP	xjpakmdcfuqe.biz: 221 IP
atomictrivia.ru: 3274 IP	xjpakmdcfuqe.com: 131 IP
amnsreiuojy.ru: 743 IP	xjpakmdcfuqe.ru: 98 IP
restlesz.su: 344 IP	xjpakmdcfuqe.in: 90 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **363** 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 website của ngân hàng, các trang thương mại điện tử…

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	nnkon878.com	Website giả mạo sàn TMĐT Shopee
2	uhy89mb.com	Website giả mạo sàn TMĐT Lazada
3	www.dichvutruyenhinhcab24h.online	Website giả mạo SCTV
4	app.amazon-line.com	Website giả mạo sàn TMĐT Amazon
5	Sendwop.com	Website giả mạo sàn TMĐT Sendo

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 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, những đơn vị đã có tài khoản trên "Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động" tại địa chỉ https://service.khonggianmang.vn, quản trị viên có thể thêm các sản phẩm đang sử dụng để giám sát và nhận cảnh báo ngay khi có lỗ hổng mới phát sinh.

***

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**, Quý đơn vị cần chú ý quan tâm không truy cập vào các trang web được nêu để tránh nguy cơ bị tấn công lừa đảo, nâng cao nhận thức bản thân và tuyên truyền cho bạn bè, người thân và những người xung quanh tránh việc trở thành nạn nhân của những cuộc tấn công lừa đảo này.

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