NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 09 (27/02/2023 – 05/03/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Lỗ hổng bảo mật Nghiêm trọng ảnh hưởng đến FortiOS và FortiProxy.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Blind Eagle nhằm mục tiêu vào các ngành công nghiệp quan trọng ở Colombia.

2. Điểm yếu, lỗ hổng

- **543** 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: 296** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Nhóm tấn công APT Blind Eagle nhằm mục tiêu vào các ngành công nghiệp quan trọng ở Colombia"

Gần đây, nhóm tấn công APT Blind Eagle hay còn được gọi là APT-C-36 đã trở lại trong một chiến dịch tấn công mới nhằm mục tiêu vào các ngành công nghiệp quan trọng ở Colombia.

Ngày 20/2/2023, các nhà nghiên cứu đã phát hiện ra nhóm Blind Eagle đang mạo danh cơ quan thuế của chính phủ Colombia để nhằm mục tiêu vào các ngành công nghiệp chính. Ngoài ra nhiều nghiên cứu cho thấy nhóm tấn công đang mở rộng chiến dịch đến một số tổ chức ở Chile, Tây Ban Nha, Ecuador.

Chiến dịch được bắt đầu bằng một email lừa đảo có chứa tệp đính kèm PDF với tiêu đề email được viết bằng tiếng Tây Ban Nha. Tệp PDF này chứa một URL giả mạo website Tổng cục Thuế và Hải quan quốc gia (DIAN) của Colombia. Sau khi người dùng truy cập vào URL và tải xuống một payload giai đoạn 2 cho phép đối tượng tấn công có thể triển khai AsyncRAT từ dịch vụ của Discord.

Nhóm tấn công APT Blind Eagle chủ yếu sử dụng AsyncRAT, njRAT , QuasarRAT , LimeRAT và RemcosRAT trong các chiến dịch của chúng. Ngoài ra, nhóm còn sử dụng các dịch vụ Dynamic DNS (DDNS) chẳng hạn như DuckDNS để kết nối các RAT của chúng nhằm điều khiển từ xa các máy chủ bị xâm nhập.

Chiến dịch Blind Eagle vẫn đang tiếp tục hoạt động nhằm mục đích đánh cắp thông tin dữ liệu và thực hiện các hành động trái phép. Các cơ quan, tổ chức cần thực hiện kiểm tra, rà soát để giảm thiểu rủi ro và phòng tránh nguy cơ tấn công mạng.

Nguồn: https://cyware.com/news/blind-eagle-re-appears-in-a-phishing-campaign-to-target-colombian-entities-61f20ba8

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng bảo mật Nghiêm trọng ảnh hưởng đến FortiOS và FortiProxy"

Vừa qua, Fortinet đã phát hành bản vá cho 15 lỗ hổng bảo mật, bao gồm một lỗ hổng bảo mật Nghiêm trọng ảnh hưởng đến FortiOS và FortiProxy. Lỗ hổng CVE-2023-25610 (điểm CVSS: 9.3) cho phép đối tượng tấn công không cần xác thực chiếm quyền truy cập hệ thống trái phép, thực thi mã tùy ý, thực hiện tấn công từ chối dịch vụ.

Lỗ hổng này ảnh hưởng đến các phiên bản FortiOS và FortiProxy sau đây:

- FortiOS phiên bản từ 7.2.0 đến 7.2.3
- FortiOS phiên bản từ 7.0.0 đến 7.0.9
- FortiOS phiên bản từ 6.4.0 đến 6.4.11
- FortiOS phiên bản từ 6.2.0 đến 6.2.12
- FortiOS 6.0
- FortiProxy phiên bản từ 7.2.0 đến 7.2.2
- FortiProxy phiên bản từ 7.0.0 đến 7.0.8
- FortiProxy phiên bản từ 2.0.0 đến 2.0.11
- FortiProxy 1.2
- FortiProxy 1.1

Để đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, tổ chức, doanh nghiệp nên kiểm tra, rà soát các sản phẩm FortiOS và FortiProxy đang sử dụng có khả năng bị ảnh hưởng. Ngoài ra, thực hiện nâng cấp lên các phiên bản mới nhất để tránh nguy cơ bị tấn công, tăng cường giám sát và sẵn sàng các phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Nguồn: https://thehackernews.com/2023/03/new-critical-flaw-in-fortios-and.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 543 lỗ hổng, trong đó có 65 lỗ hổng mức Cao, 64 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 413 lỗ hổng chưa đánh giá. Trong đó có ít nhất 101 lỗ hổng cho phép chèn và thực thi mã

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 14 lỗ hổng trong Google, Nhóm 20 lỗ hổng trong Linux, Nhóm 55 lỗ hổng trong Apple, Nhóm 54 lỗ hổng trong Wordpress, Nhóm 05lỗ hổng trong Dell, Nhóm 09 lỗ hổng trong Huawei, Nhóm 08 lỗ hổng trong IBM. 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:

- Google: CVE-2022-20455, CVE-2022-20551,...

- Linux: CVE-2023-26544, CVE-2023-26545,....

- Apple: CVE-2020-9846, CVE-2023-25621,...

- Wordpress: CVE-2022-4795, CVE-2022-4829,...

- Dell: CVE-2023-24567, CVE-2023-23689,...

- Huawei: CVE-2022-48255, CVE-2022-48254,...

- IBM: CVE-2022-43923, CVE-2020-5001,...

Thông tin điểm yếu, lỗ hổng

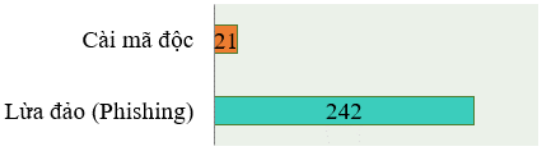
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2022-20455 CVE-2022-20481 CVE-2022-20551 …	Nhóm 14 lỗ hổng trong Google (Android) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-26545 CVE-2023-26544 CVE-2023-26605 …	Nhóm 20 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Apple	CVE-2020-9846 CVE-2022-32784 CVE-2022-32830 …	Nhóm 55 lỗ hổng trong Apple (macOS,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-4795 CVE-2022-4829 CVE-2023-0168 …	Nhóm 54 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã tùy ý, thực hiện tấn công XSS, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2023-24567 CVE-2023-23689 CVE-2023-25536 …	Nhóm 05 lỗ hổng trong Dell (PowerScale OneFS, NetWorker,…) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Huawei	CVE-2022-48230 CVE-2022-48254 CVE-2022-48255 …	Nhóm 09 lỗ hổng trong Huawei (BiSheng-WNM FW, Leia-B29,…) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-43923 CVE-2020-5001 CVE-2020-5026 ...	Nhóm 08 lỗ hổng trong IBM (Maximo Application Suite,…) cho phép đối tượng tấn công đánh cắp thông tin dữ liệu, chèn mã JavaScript tùy ý, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

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

Tấn công DRDoS

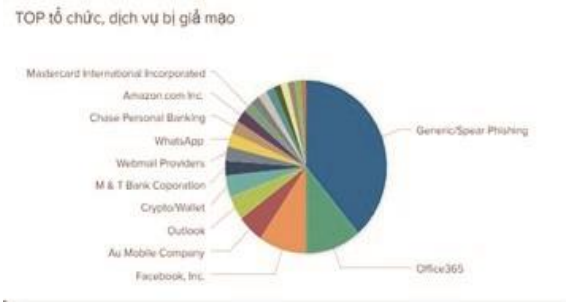
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **54,042** (tăng so với tuần trước **50,826**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.

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



Tấn công Web

Trong tuần, có 263 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 242 trường hợp tấn công lừa đảo (Phishing), 21 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: 19305 IP	xjpakmdcfuqe.ru:419 IP
disorderstatus.ru: 8333 IP	xjpakmdcfuqe.in:395 IP
atomictrivia.ru: 3947 IP	restlesz.su: 367 IP
xjpakmdcfuqe.biz: 665 IP	amnsreiuojy.ru: 1048 IP
xjpakmdcfuqe.com: 492 IP	hzmksreiuojy.ru: 51 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 296 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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	jaccscom.com bxrtxfr.xyz hdcreditvnn.com vaynhanhvn.net …	Website giả mạo, lừa đảo

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