NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 02 (09/01/2023 – 15/01/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** 02 lỗ hổng bảo mật nghiêm trọng trong Cisco EoL Business Routers.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Dark Pink nhằm mục tiêu vào APAC.

2. Điểm yếu, lỗ hổng

- **772** 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: 204** 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

Tin tức An toàn thông tin

"Nhóm tấn công APT Dark Pink nhằm mục tiêu vào APAC"

Một nhóm tấn công mới đã được phát hiện nhằm mục tiêu vào các tổ chức chính phủ và quân đội ở Châu Á Thái Bình Dương. Chiến dịch đang được theo dõi dưới tên Dark Pink.

Theo các chuyên gia, chiến dịch Dark Pink có liên quan đến 7 cuộc tấn công thành công từ tháng 6 đến tháng 12 năm 2022. Nhóm bắt đầu hoạt động vào giữa năm 2021 và các cuộc tấn công gia tăng một năm sau đó bằng cách sử dụng bộ công cụ tùy chỉnh, được tạo ra để đánh cắp thông tin quan trọng từ các mạng bị xâm nhập. Nhóm sử dụng email lừa đảo trực tuyến để khởi động các cuộc tấn công và API Telegram.

Nhóm Dark Pink tấn công vào hai cơ quan quân đội ở Philippines và Malaysia, cơ quan chính phủ ở Campuchia, Indonesia, Bosnia, Herzegovina và một tổ chức tôn giáo ở Việt Nam.

Nhóm Dark Pink truy cập vào các trang tuyển dụng để giả mạo ứng tuyển vào vị trí trong bộ phận PR và truyền thông. Tuy nhiên, mục đích của nhóm là triển khai KamiKakaBot và TelePowerBot để thực thi lệnh được gửi qua bot Telegram. Sau đó, nhóm sử dụng công cụ Ctealer và Cucky để đánh cắp thông tin đăng nhập và cookie từ trình duyệt web.

Chiến dịch đã sử dụng nhiều chuỗi lây nhiễm, trong đó quyền truy cập ban đầu có được thông qua các tin nhắn lừa đảo sử dụng liên kết đến tệp hình ảnh ISO bị lây nhiễm để triển khai phần mềm độc hại.

Chiến dịch Dark Pink đã sử dụng chiến thuật lừa đảo trực tuyến để phân phối một bộ công cụ tùy chỉnh, điều này cho thấy tầm quan trọng và hiệu quả của phương pháp tấn công này. Do đó, các tổ chức nên tăng cường tuyến phòng thủ của mình bằng cách sử dụng các giải pháp bảo mật email để phát hiện và ngăn chặn các email lừa đảo trước khi chúng xâm nhập vào bên trong mạng.

Nguồn: https://cyware.com/news/dark-pink-apt-group-targets-apac-b1da113a

Tin tức An toàn thông tin

"Cảnh báo 02 lỗ hổng bảo mật nghiêm trọng trong Cisco EoL Business Routers"

Cisco đã công bố về 02 lỗ hổng bảo mật () ảnh hưởng đến EoL Small Business RV016, RV042, RV042G và RV082. Cisco tuyên bố rằng 02 lỗ hổng này sẽ không được khắc phục ngay cả khi lỗ hổng đã bị khai thác trong thực tế. Lỗ hổng tồn tại do lỗi xác thực đầu vào trên giao diện quản lý dựa trên web của bộ định tuyến, cho phép bỏ qua xác thực hoặc thực thi các lệnh độc hại.

- Lỗ hổng bảo mật CVE-2023-20025 (điểm CVSS: 9.0 Cao) tồn tại do việc xác thực đầu vào của người dùng không đúng cách. Đối tượng tấn công có thể thực thi mã từ xa bằng cách gửi yêu cầu HTTP giả mạo.

- Lỗ hổng bảo mật CVE-2023-20026 (điểm CVSS:6,6 Trung bình) cho phép đối tượng tấn công có thông tin xác thực quản trị viên hợp lệ, truy cập dữ liệu trái phép.

Cisco không phát hành các bản cập nhật phần mềm để khắc phục 02 lỗ hổng này. Vì vậy, biện pháp khắc phục thay thế là quản trị viên nên tắt tính năng quản lý từ xa và chặn quyền truy cập cổng 443 và 60443.

Nguồn: https://thehackernews.com/2023/01/cisco-issues-warning-for-unpatched.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 772 lỗ hổng, trong đó có 284 lỗ hổng mức Cao, 141 lỗ hổng mức Trung bình, 05 lỗ hổng mức Thấp và 342 lỗ hổng chưa đánh giá. Trong đó có ít nhất 54 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 10 lỗ hổng trong Siemens, Nhóm 11 lỗ hổng trong Linux, Nhóm 07 lỗ hổng trong Wordpress, Nhóm 02 lỗ hổng trong Github, Nhóm 07 lỗ hổng trong Huawei, Nhóm 15 lỗ hổng trong Google, Nhóm 04 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:

- *Siemens: CVE-2022-47935, CVE-2022-47967,...*
- *Linux: CVE-2022-4382, CVE-2022-4382,...*
- *Wordpress: CVE-2022-38467, CVE-2022-45353,...*
- *Github: CVE-2022-46258, CVE-2015-10031.*
- *Huawei: CVE-2022-46762, CVE-2022-46761,...*
- *Google: CVE-2023-0134, CVE-2023-0129,...*
- *IBM: CVE-2022-35281, CVE-2022-22470,...*

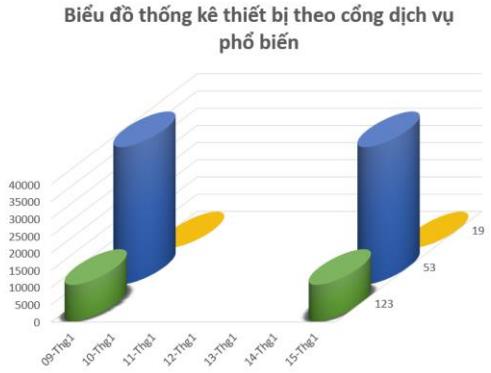
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Siemens	CVE-2022-47935 CVE-2022-47967 CVE-2022-3159 …	Nhóm 10 lỗ hổng trong Siemens (Automation License Manager,…) cho phép đối tượng tấn công thực thi mã từ xa, đọc và ghi các tệp tùy ý, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2022-2196 CVE-2022-4379 CVE-2022-4382 …	Nhóm 11 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE-2022-38467 CVE-2022-45353 …	Nhóm 07 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Github	CVE-2022-46258 CVE-2015-10031	Nhóm 02 lỗ hổng trong Github (491-Project, Enterprise Server) cho phép đối tượng tấn truy cập đọc/ghi để sửa đổi các tệp trái phép, SQL injection.	Đã có thông tin xác nhận và bản vá
5	Huawei	CVE-2022-47974 CVE-2022-46761 CVE-2022-46762 …	Nhóm 07 lỗ hổng trong Huawei (emui) cho phép đối tượng tấn có thể ngắt kết nối dịch vụ, ảnh hưởng đến tính khả dụng của hệ thống, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Google	CVE-2023-0128 CVE-2023-0129 CVE-2023-0134 …	Nhóm 15 lỗ hổng trong Google (Chrome) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-22470 CVE-2022-40615 CVE-2022-35281 ...	Nhóm 04 lỗ hổng trong IBM (Security Verify Governanc,…) cho phép đối tượng tấn công lưu trữ thông tin đăng nhập của người dùng, sửa đổi hoặc xóa thông tin trong cơ sở dữ liệu, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

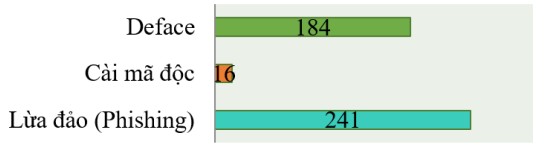
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **47,360** (tăng so với tuần trước **45,612**) 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.

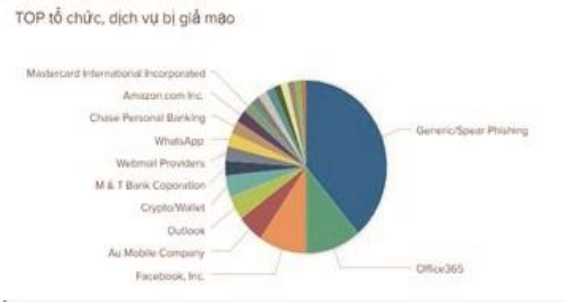


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 441 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 184 trường hợp tấn công thay đổi giao diện (Deface), 241 trường hợp tấn công lừa đảo (Phishing), 16 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: 32698 IP	xjpakmdcfuqe.ru:676 IP
disorderstatus.ru: 12124 IP	xjpakmdcfuqe.in: 622 IP
atomictrivia.ru: 6172 IP	restlesz.su: 347 IP
xjpakmdcfuqe.biz: 1777 IP	amnsreiuojy.ru: 1576 IP
xjpakmdcfuqe.com: 953 IP	hzmksreiuojy.ru: 168 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 204 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	cf222.art	Trang web 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
ais@mic.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội