NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 03 (16/01/2023 – 22/01/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Lỗ hổng Realtek – hơn 134 triệu cuộc tấn công thiết bị IoT.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT BackdoorDiplomacy sử dụng backdoor Turian để nhằm mục tiêu vào chính phủ Iran.

2. Điểm yếu, lỗ hổng

- **589** 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: 173** 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 BackdoorDiplomacy sử dụng backdoor Turian để nhằm mục tiêu vào chính phủ Iran"

Gần đây, một làn sóng tấn công mới đã được phát hiện nhằm vào các cơ quan chính phủ Iran được cho là do nhóm BackdoorDiplomacy thực hiện.

BackdoorDiplomacy (hay còn gọi là Playful Taurus, APT15) bắt đầu một chiến dịch với phần mềm độc hại được nâng cấp thêm và thêm các công cụ mới trong chiến dịch. Trong làn sóng gần đây, nhóm có khả năng đã xâm nhập vào các mạng của chính phủ Iran thuộc 4 tổ chức khác nhau, trong đó có Bộ Ngoại giao. Nhóm đã chuyển dịch vụ lưu trữ của các mạng này qua cơ sở hạ tầng C&C độc hại và sử dụng chúng để thiết lập kết nối với phần mềm độc hại. Nhóm đã lạm dụng các chứng chỉ liên quan đến hoạt động hết hạn thuộc về cơ quan bị nhằm mục tiêu để tránh bị phát hiện.

BackdoorDiplomacy sử dụng các biến thể mới của backdoor có tên là Turian, được sử dụng vào tháng 6 năm 2021. Các nhà nghiên cứu đã tìm thấy một mẫu của biến thể mới hơn được tích hợp VMProtect có chứa chức năng mã hóa API và chức năng giải mã XOR.

BackdoorDiplomacy liên tục phát triển các TTP của nó trong chiến dịch gián điệp. Hơn nữa, nhóm còn thường xuyên triển khai TTP tương tự với các công cụ được sửa đổi để nhằm mục tiêu vào các tổ chức chính phủ và ngoại giao khác trên khắp Bắc và Nam Mỹ, Châu Phi, Trung Đông.

Nguồn: https://cyware.com/news/backdoordiplomacy-apt-uses-turian-backdoor-to-target-iranian-government-09f1da2a

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng Realtek – hơn 134 triệu cuộc tấn công thiết bị IoT"

Các nhà nghiên cứu đang cảnh báo về sự gia tăng đột biến của các cuộc tấn công khai thác lỗ hổng bảo mật thực thi mã từ xa đã được vá trong Realtek Jungle SDK kể từ đầu tháng 8 năm 2022. Tính đến tháng 12 năm 2022, đã ghi nhận 134 triệu vụ khai thác với 87% các cuộc tấn công xảy ra trong 4 tháng qua. Gần 50% các cuộc tấn công bắt nguồn từ Hoa Kỳ (48,3%), tiếp theo là Việt Nam (17,8%), Nga (14,6%), Hà Lan (7,4%), Pháp (6,4%), Đức (2,3%). Hơn nữa 98% các cuộc tấn công khai thác lỗ hổng bảo mật bắt nguồn từ Nga đã nhằm vào các tổ chức ở Úc.

Lỗ hổng bảo mật có mã CVE-2021-35394 (có điểm CVSS:9.8), cho phép đối tượng tấn công thực thi mã tùy ý với mức đặc quyền cao và chiếm quyền kiểm soát thiết bị. Lỗ hổng ảnh hưởng đến nhiều loại thiết bị như D-Link, LG, Belkin, ASUS và NETGEAR.

Bên cạnh đó, lỗ hổng CVE-2021-35394 được khai thác trong mạng botnet như Mirai, Gafgyt và Mozi, cũng như một mạng botnet tấn công từ chối dịch vụ phân tán DDoS dựa trên Golang có tên là RedGoBot.

Sự gia tăng của các cuộc tấn công khai thác lỗ hổng CVE-2021-35394 cho thấy đối tượng tấn công rất quan tâm đến các lỗ hổng trong chuỗi cung ứng, điều mà người dùng bình thường có thể khó xác định và khắc phục.

Nguồn: https://thehackernews.com/2023/01/realtek-vulnerability-under-attack-134.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 589 lỗ hổng, trong đó có 70 lỗ hổng mức Cao, 63 lỗ hổng mức Trung bình, 05 lỗ hổng mức Thấp và 451 lỗ hổng chưa đánh giá. Trong đó có ít nhất 73 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 28 lỗ hổng trong Adobe, Nhóm 74 lỗ hổng trong Oracle, Nhóm 12 lỗ hổng trong Apache, Nhóm 22 lỗ hổng trong Cisco, Nhóm 14 lỗ hổng trong Dell, Nhóm 01 lỗ hổng trong Github, Nhóm 09 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:

- Adobe: CVE-2023-21606, CVE-2023-21607,...

- Oracle: CVE-2023-21893, CVE-2023-21852,...

- Apache: CVE-2006-20001, CVE-2022-36760,...

- Cisco: CVE-2023-20020, CVE-2023-20043,...

- Dell: CVE-2022-32490, CVE-2022-34393,...

- Github: CVE-2022-23739.

- IBM: CVE-2021-39089, CVE-2022-47990,...

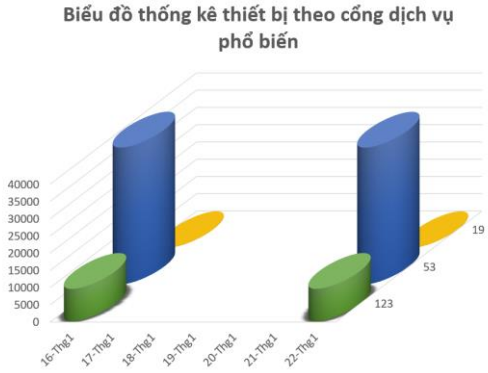
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Adobe	CVE-2023-21606 CVE-2023-21607 CVE-2023-21608 …	Nhóm 28 lỗ hổng trong Adobe (Acrobat Reader, InDesign,…) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công leo thang đặc quyền, làm rò rỉ thông tin dữ liệu.	Chưa có thông tin xác nhận và bản vá
2	Oracle	CVE-2023-21893 CVE-2023-21852 CVE-2023-21853 …	Nhóm 74 lỗ hổng trong Oracle (E-Business Suite, Fusion Middleware,…) cho phép đối tượng tấn công không cần xác thực có quyền truy cập mạng qua HTTP để xâm nhập vào hệ thống, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2006-20001 CVE-2022-36760 CVE-2022-37436 …	Nhóm 12 lỗ hổng trong Apache cho phép đối tượng tấn công với quyền của người dùng cục bộ có quyền truy cập đọc vào một cơ sở dữ liệu để thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Cisco	CVE-2023-20020 CVE-2023-20043 CVE-2023-20044 …	Nhóm 22 lỗ hổng trong Cisco (BroadWorks, Identity Services Engine,…) cho phép đối tượng tấn công thực thi các lệnh 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-2022-32490 CVE-2022-34393 CVE-2022-34401 …	Nhóm 14 lỗ hổng trong Dell (BIOS, EMC,…) cho phép đối tượng tấn công thực thi mã hoặc lệnh tùy ý.	Chưa có thông tin xác nhận và bản vá
6	Github	CVE-2022-23739	01 lỗ hổng trong Github (Enterprise Server) 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-2021-39089 CVE-2022-47990 CVE-2023-22592 ...	Nhóm 09 lỗ hổng trong IBM (CP4S, Spectrum Virtualize ,…) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, cài mã JavaScript tùy ý, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

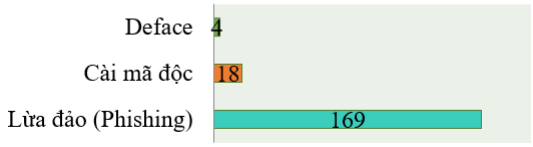
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **46,658** (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.

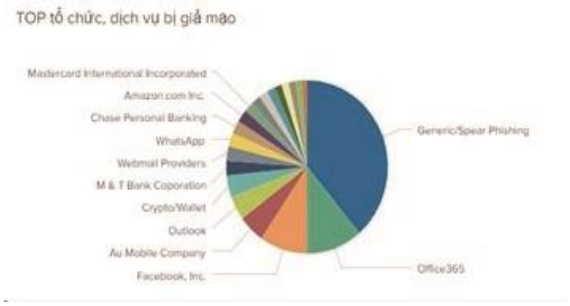


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 191 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 04 trường hợp tấn công thay đổi giao diện (Deface), 169 trường hợp tấn công lừa đảo (Phishing), 18 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: 24574 IP	xjpakmdcfuqe.ru:507 IP
disorderstatus.ru: 10248 IP	xjpakmdcfuqe.in: 460 IP
atomictrivia.ru: 4997 IP	restlesz.su: 285 IP
xjpakmdcfuqe.biz: 1006 IP	amnsreiuojy.ru: 1619 IP
xjpakmdcfuqe.com: 644 IP	hzmksreiuojy.ru: 85 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 173 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
0	0	0

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