TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 33 (16/08/2021 – 22/08/2021)

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 – ais.@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp.Hà Nội

NCSC VN
National Cyber Security Center

NỘI DUNG TUẦN

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

TIN CẢNH BÁO

- **Cảnh báo:** Botnet Mozi tiếp tục nhằm mục tiêu đến bộ định tuyến của các hãng Netgear, Huawei và ZTE

- **Chiến dịch tấn công APT:** Nhóm tấn công APT InkySquid khai thác các lỗ hổng trong trình duyệt web để phát tán phần mềm độc hại

ĐIỂM YẾU, LỖ HỔNG

- **396** 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.

SỐ LIỆU, THỐNG KÊ

- Tấn công DRDoS
- Tấn công Web
- Tấn công lừa đảo người dùng Việt Nam

Hot News!

Tài liệu lưu trữ:

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

https://service.khonggianmang.vn

TIN CẢNH BÁO

Cảnh báo: Botnet Mozi tiếp tục nhằm mục tiêu đến bộ định tuyến của các hãng Netgear, Huawei và ZTE

Botnet Mozi được biết đến là một botnet chuyên nhằm mục tiêu đến các thiết bị IoT. Gần đây, các chuyên gia bảo mật đã phát hiện botnet này còn có thể duy trì được sự tồn tại trên bộ định tuyến của các hãng Netgear, Huawei và ZTE.

Các cổng mạng là mục tiêu đặc biệt hấp dẫn đối với các đối tượng tấn công vì chúng có thể trở thành điểm truy cập ban đầu vào các mạng của doanh nghiệp. Bằng cách lây nhiễm vào các bộ định tuyến, đối tượng tấn công có thể thực hiện các cuộc tấn công man-in-the-middle (MITM) thông qua xâm nhập HTTP và DNS giả mạo, xâm nhập các thiết bị đầu cuối và triển khai ransomware hoặc gây ra sự cố mất an toàn thông tin trong các hệ thống vận hành. Mozi đã được nâng cấp để hỗ trợ các lệnh mới cho phép phần mềm độc hại chiếm quyền điều khiển các phiên HTTP và thực hiện giả mạo DNS để chuyển hướng lưu lượng truy cập đến miền do kẻ tấn công kiểm soát.

Một phân tích X-Force của IBM được công bố vào tháng 9 năm 2020 đã công bố rằng Mozi chiếm gần 90% lưu lượng truy cập mạng IoT được quan sát từ tháng 10 năm 2019 đến tháng 6 năm 2020, cho thấy rằng các tác nhân đe dọa đang ngày càng khai thác các thiết bị IoT để mở rộng phạm vi tấn công. Theo đánh giá sơ bộ từ các chuyên gia bảo mật ít nhất 24 quốc gia đã bị nhằm mục tiêu, trong đó dẫn đầu là Bulgaria và Ấn Độ.

Các doanh nghiệp và người dùng sử dụng bộ định tuyến Netgear, Huawei và ZTE nên bảo mật thiết bị bằng mật khẩu mạnh và thường xuyên cập nhật phiên bản.

Nguồn: https://thehackernews.com/2021/08/mozi-iot-botnet-now-also-targets.html?&web_view=true

Nhóm tấn công APT InkySquid khai thác các lỗ hổng trong trình duyệt web để phát tán phần mềm độc hại

Nhóm này đã sử dụng cách khai thác này kể từ năm 2020 trong các cuộc tấn công vào trình duyệt Internet Explorer để tải xuống mã Javascrip độc hại thường được ẩn bên trong mã hợp pháp.

Theo các nhà nghiên cứu bảo mật, vào tháng 4 năm 2021 đã phát hiện mã độc hại được tải qua ww.dailynk.com tới các miền phụ của jquery.services, từ đó các đối tượng tấn công có thể lưu trữ các phần mềm độc hại mới. Có 2 URL độc hại đã được tìm thấy là:

- hxxps://www.dailynk[.]com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1
- hxxps://www.dailynk[.]com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2

Các lỗ hổng bảo mật mà nhóm này đã khai thác bao gồm: CVE-2021-1380 (điểm CVSS: 7.5), CVE-2021-26411 (điểm CVSS: 8.8): lỗ hổng tồn tại trong Internet Explorer.

Dữ liệu mà đối tượng tấn công thu thập được có thể là thông tin người dùng, tên máy, phiên bản hệ điều hành, địa chỉ IP,….

Nguồn: https://gbhackers.com/north-korean-hacker-group-uses-browser-exploits/?web_view=true

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 396 lỗ hổng, trong đó có 03 lỗ hổng mức cao, 05 lỗ hổng mức trung bình, 02 lỗ hổng mức thấp và 386 lỗ hổng chưa đánh giá. Trong đó có ít nhất 50 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 42 lỗ hổng trong phần mềm Adobe, Nhóm 41 lỗ hổng trong các Wordpress Plugin, Nhóm 20 lỗ hổng trong phần mềm Google, Nhóm 11 lỗ hổng phần mềm Mozilla, Nhóm 11 lỗ hổng trong Mediatek, Nhóm 10 lỗ hổng trong các sản phẩm của Dell, Nhóm 06 lỗ hổng trong thiết bị Cisco. 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-2021-35988, CVE-2021-35986,...

- WordPress: CVE-2021-24540, CVE-2021-24534,...

- Google: CVE-2021-37690, CVE-2021-0579,...

- Mozilla: CVE-2021-29990, CVE-2021-29983,...

- Mediatek: CVE-2021-0626, CVE-2021-0408,...

- Dell: CVE-2021-21594, CVE-2021-36280,...

- Cisco: CVE-2021-34730, CVE-2021-34715,...

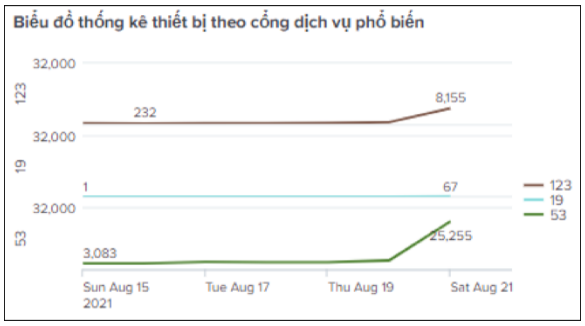
Thông tin điểm yếu, lỗ hổng

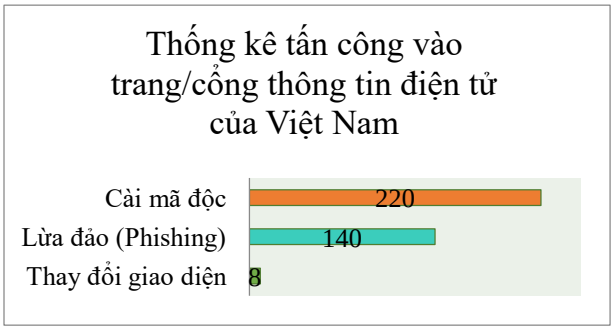
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Adobe	CVE-2021-35988 CVE-2021-35986 CVE-2021-35985 …	Nhóm 42 lỗ hổng trong phần mềm Adobe (Acrobat Reader DC) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
2	WordPress	CVE-2021-24540 CVE-2021-24534 CVE-2021-24380 …	Nhóm 41 lỗ hổng trong các Wordpress Plugin (Wonder Video Embed WordPress plugin,…) cho phép đối tượng tấn công thực hiện tấn công Stored XSS, Reflected XSS.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2021-37690 CVE-2021-0579 CVE-2021-0584 …	Nhóm 20 lỗ hổng trong phần mềm Google (TensorFlow, Google- Android) cho phép đối tượng tấn công thu thập thông tin, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
4	Mozilla	CVE-2021-29990 CVE-2021-29983 CVE-2021-29984 …	Nhóm 11 lỗ hổng phần mềm Mozilla (Firefox, Thunderbird) cho phép đối tượng tấn công thu thập thông tin, thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
5	Mediatek	CVE-2021-0626 CVE-2021-0408 CVE-2021-0407 …	Nhóm 11 lỗ hổng trong Mediatek cho phép đối tượng tấn công thu thập thông tin, leo thang đặc quyền, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	Dell	CVE-2021-21594 CVE-2021-36280 CVE-2021-36279 …	Nhóm 10 lỗ hổng trong các sản phẩm của Dell (PowerScale OneFS,…) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
7	Cisco	CVE-2021-34730 CVE-2021-34715 CVE-2021-34716 …	Nhóm 06 lỗ hổng trong thiết bị Cisco (Cisco Small Business,…) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công từ chối dịch vụ, chiếm quyền kiểm soát thiết bị.	Đã có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công tại 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 **58,191** (tăng so với tuần trước **57,762**) 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.



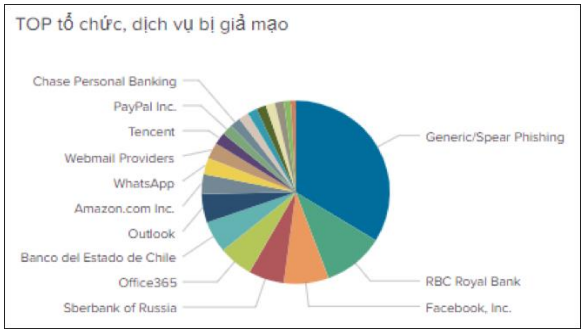


Tấn công Phishing

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, Paypment, Apple, Paypal ..v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

Tấn công Web

Trong tuần, có 368 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 08 trường hợp tấn công thay đổi giao diện, 140 trường hợp tấn công lừa đảo (Phishing), 220 trường hợp tấn công cài cắm mã độc.



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

differentia.ru	a.asense.in
disorderstatus.ru	ww2.bbbjdnxbgp3.ru
atomictrivia.ru	a.deltaheavy.ru
morphed.ru	sdk.asense.in
ydbnsrt.me	soplifan.ru

New

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 87 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, lừa đảo liên quan đến COVID…..

Dưới đây một số trường hợp điển hình người dùng cần nâng cao tương tự.

STT	Website lừa đảo	Ghi chú
1	https://h5.manycash.online//#/Index/Home	Lừa đảo cho vay online
2	https://21ak22.com/	Website chuyên phát tán phần mềm crack có kèm ransomware
3	https://garena.giaidauonline.vn/	Lừa đảo lấy thông tin cá nhân của gamer từ mã otp kích hoạt
4	http://usename.biz/ http://newname.vqpclaaw.nethost-4611.000nethost.com/ http://newname.work/ http://newname.asia/ http://newname.biz	Giả mạo website của Vietcombank
5	https://mercedes-vietnam.com.vn/	Giả mạo website Mercedes-benz
6	https://vn211.com/	Lừa đảo đầu tư tiền ảo
7	http://www.saigoncom.vip/	Website giả mạo ngân hàng TMCP Sài Gòn
8	https://tuoi-tre.com/	Trang Web giả mạo báo Tuổi Trẻ đăng thông tin sai sự thật
9	https://haegin.net/	Giả mạo trang Coupon của Play together
10	https://lienquanmobilefree.com/	Lừa đảo tài khoản game liên quân mobile
11	https://tradevn.tech/	Sàn giao dịch lừa đảo, đăng phần mềm WinRAR crack ảnh hưởng đến đại lý phân phối ở VN
12	http://ibongdanews.co/	Trang web giả mạo website Báo Thế giới và Việt Nam
13	https://muaho8.com/index/user/login.html	Web bán hàng lừa đảo
14	https://teslay.com/index/login/index	Lừa đảo nạp tiền vào tài khoản

Khuyến nghị đối với các cơ quan, đơn vị

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin cảnh báo** 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 **Nguy cơ tấn công mạng từ điểm yếu lỗ hổng**, 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.

***

4. 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.

***

Thông tin liên hệ:

Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 - ais@mic.gov.vn