TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 34 (23/08/2021 – 29/08/2021)

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:** Cisco sẽ không phát hành bản cập nhật phần mềm cho lỗ hổng zero-day trên các bộ định tuyến EOL VPN

- **Chiến dịch tấn công APT:** Sự trở lại của nhóm tấn công APT FIN8 với backdoor mới.

ĐIỂM YẾU, LỖ HỔNG

- **380** 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: Cisco sẽ không phát hành bản cập nhật phần mềm cho lỗ hổng zero-day trên các bộ định tuyến EOL VPN

Gần đây, Cisco đã thông báo rằng sẽ không phát hành các bản cập nhật phần mềm cho lỗ hổng bảo mật của dịch vụ Universal Plug-and-Play (UPnP) trong Bộ định tuyến Cisco Small Business RV110W, RV130, RV130W và RV215W. UPnP là dịch vụ khá phổ biến được sử dụng trong hầu hết các thiết bị mạng gia đình. Nó cũng đã là mục tiêu trước đây của botnet Mirai.

Lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa tùy ý mà không cần xác thực, tấn công từ chối dịch vụ. Kẻ tấn công có thể khai thác lỗ hổng này bằng cách gửi UPnP request tới một thiết bị bị ảnh hưởng.

Lỗ hổng chỉ ảnh hưởng đến các bộ định tuyến RV Series nếu chúng đã được cấu hình UPnP. Dịch vụ UPnP mặc định sẽ bật trên giao diện mạng LAN và tắt trên mạng WAN. Để kiểm tra xem tính năng UPnP có được kích hoạt trên giao diện mạng LAN của thiết bị hay không, người dùng nên mở giao diện quản lý trên nền tảng web và chọn vào Basic Settings> UPnP. Nếu "Disable check box" đang không được tích chọn thì có nghĩa là UPnP được bật trên thiết bị. Nếu UPnP được kích hoạt, đối tượng tấn công có thể khai thác để mở các cổng trên tường lửa dẫn đến điều hướng được lưu lượng truy cập từ Internet.

Cisco cảnh báo rằng bất kỳ giải pháp thay thế hoặc giảm thiểu nào đều có thể gây ảnh hưởng. Vì vậy, thay vì phát hành bản vá, Cisco khuyến nghị người dùng chuyển sang bộ định tuyến Cisco Small Business RV132W, RV160 hoặc RV160W.

Nguồn: https://www.zdnet.com/article/cisco-not-planning-to-fix-critical-0-day-rce-vulnerability-in-eol-vpn-routers/?&web_view=true

Sự trở lại của nhóm tấn công APT FIN8 với backdoor mới.

FIN8 được biết đến là nhóm tấn công APT nhằm mục tiêu vào nhiều ngành công nghiệp. Gần đây, các chuyên gia bảo mật đã phát hiện nhóm này sử dụng một backdoor mới nhằm mục tiêu vào một tổ chức tài chính có trụ sở tại Hoa Kỳ. Backdoor này được đặt tên là Sardonic. Sardonic có thể thiết lập tính ổn định trên máy bị nhiễm và thu thập thông tin hệ thống, thực hiện các lệnh tùy ý, tải thêm các plugin.

Trong cuộc tấn công lần này, đối tượng tấn công đã xâm nhập mạng mục tiêu và thực hiện leo thang đặc quyền. Tuy nhiên, do các dòng lệnh độc hại đã bị chặn nên việc phát tán Sardonic đã không thành công.

Kể từ năm 2016, FIN8 đã sử dụng nhiều kỹ thuật khác nhau như lừa đảo trực tuyến cùng với các phần mềm độc hại khác nhau như BadHatch/PunchTrack để lấy cắp thông tin thẻ thanh toán từ hệ thống POS.

Cụ thể vào tháng 3 năm 2016, FIN8 bắt đầu nhằm mục tiêu vào các ngành bán lẻ, công nghệ, bảo hiểm và hóa chất có trụ sở tại Nam Phi, Hoa Kỳ, Canada, Panama, Puerto Rico bằng phần mềm độc hại BadHatch.

Theo các chuyên gia, FIN8 đang phát triển chiến thuật tấn công và cơ sở hạ tầng để phân phối phần mềm độc hại. Các tổ chức nên cảnh giác với các hệ thống PoS của mình, hướng dẫn nhân viên để xác định email lừa đảo và tăng cường các giải pháp bảo mật email.

Nguồn: https://cyware.com/news/fin8-returns-with-new-sardonic-backdoor-1529fe9c

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 380 lỗ hổng, trong đó có 15 lỗ hổng mức cao, 91 lỗ hổng mức trung bình, 21 lỗ hổng mức thấp và 253 lỗ hổng chưa đánh giá. Trong đó có ít nhất 53 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 58 lỗ hổng trong phần mềm Adobe, Nhóm 20 lỗ hổng trong các thiết bị Cisco, Nhóm 17 lỗ hổng trong GitLab, Nhóm 14 lỗ hổng trong phần mềm Google, Nhóm 09 lỗ hổng trong thư viện Xstream, Nhóm 08 lỗ hổng phần mềm IBM, Nhóm 06 lỗ hổng trong thiết bị Totolink. 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-2021-28624, CVE-2021-35989,...

- Cisco: CVE-2021-1577, CVE-2021-1578,...

- GitLab: CVE-2021-22251, CVE-2021-22249,...

- Google: CVE-2021-30602, CVE-2021-30598,...

- XStream: CVE-2021-39154, CVE-2021-39153,...

- IBM: CVE-2021-29704, CVE-2021-29802,...

- Totolink: CVE-2021-34218, CVE-2021-34207,...

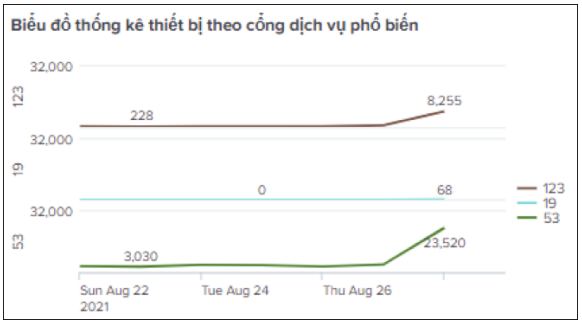
Thông tin điểm yếu, lỗ hổng

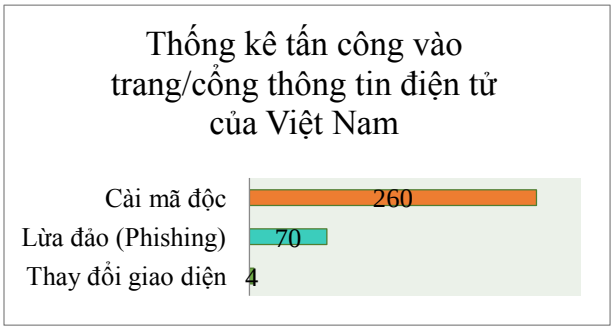
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Adobe	CVE-2021-28624 CVE-2021-35989 CVE-2021-35990 …	Nhóm 58 lỗ hổng trong phần mềm Adobe (Bridge, Illustrator ,…) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, thực thi mã tùy ý, tấn công từ chối dịch vụ, tấn công SSRF, XSS.	Đã có thông tin xác nhận và bản vá
2	Cisco	CVE-2021-1577 CVE-2021-1578 CVE-2021-1579 …	Nhóm 20 lỗ hổng trong các thiết bị Cisco (APIC, Cloud APIC,…) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, leo thang đặc quyền, thực thi mã tùy ý, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
3	GitLab	CVE-2021-22251 CVE-2021-22249 CVE-2021-22246 …	Nhóm 17 lỗ hổng trong GitLab EE, cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, tấn công XSS.	Đã có thông tin xác nhận và bản vá
4	Google	CVE-2021-30602 CVE-2021-30598 CVE-2021-30597 …	Nhóm 14 lỗ hổng trong phần mềm Google (Chrome) cho phép đối tượng tấn công truy cập trái phép và gây hư hỏng bộ nhớ, thực thi mã tùy ý, tấn công giả mạo Url bar.	Đã có thông tin xác nhận và bản vá
5	XStream	CVE-2021-39154 CVE-2021-39153 CVE-2021-39147 …	Nhóm 09 lỗ hổng trong thư viện XStream cho phép đối tượng tấn công thực thi mã tùy ý, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	IBM	CVE-2021-29704 CVE-2021-29802 CVE-2021-29727 …	Nhóm 08 lỗ hổng phần mềm IBM (Security SOAR, API Connect,...) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, leo thang đặc quyền, tấn công chèn mã.	Đã có thông tin xác nhận và bản vá
7	Totolink	CVE-2021-34218 CVE-2021-34207 CVE-2021-34215 …	Nhóm 06 lỗ hổng trong thiết bị Totolink (A3002R firmware) cho phép đối tượng tấn công thu thập thông tin qua Directory Indexing, tấn công XSS.	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 **55,618** (giảm so với tuần trước **58,191**) 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.



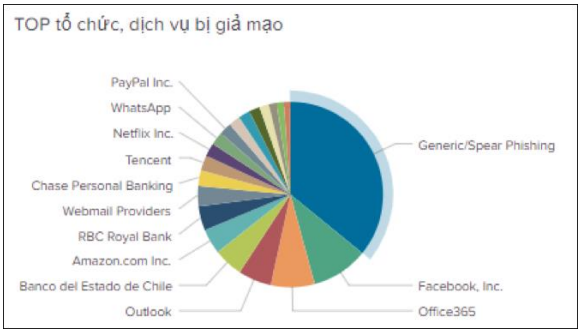


Tấn công Phishing

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 334 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 04 trường hợp tấn công thay đổi giao diện, 70 trường hợp tấn công lừa đảo (Phishing), 260 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 151 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://liximomo.fun/	Trang web giả mạo Momo lừa tiền
2	https://www.vietelshop.online/	Lừa đảo bán sim online
3	https://clmm.me/	Web lừa đảo cờ bạc qua ví điện tử Momo
4	https://playtogethershop.com/quay/43 https://iplaytogethershop.com/login.html https://www.playtogether.store https://muathengay.com/blog/cach-nap-game-play-together-gia-re-uy-tin-nhanh-chong http://thecaoplaytogether.com/ https://pay.heagin.com/	Lừa đảo nạp thẻ game Play Together
5	https://hackvn.pro/doc-trom-tin-nhan-facebook	Website lừa đảo hướng dẫn hack tài khoản facebook
6	Error! Hyperlink reference not valid. https://khoataikhoangarena.xyz/	Lừa đảo tài khoản game Garena
7	https://westernuinon.weebly.com/ http://bom.to/Fzcr7rPMM33XYJ	Giả mạo Western Union
8	https://muabanhanh.io/	Trang web lừa đảo khi nạp tiền
9	lis666.sinh5.com	Giả mạo NYSE

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 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