TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 41 (11/10/2021 – 17/10/2021)

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

NỘI DUNG TUẦN

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

TIN CẢNH BÁO

- **Cảnh báo:** Telegram Bots được sử dụng trong các chiến dịch tấn công để lấy cắp OTP

- **Chiến dịch tấn công APT:** Lỗ hổng bảo mật zero-day trong Windows trở thành mục tiêu khai thác trong chiến dịch tấn công mạng diện rộng.

ĐIỂM YẾU, LỖ HỔNG

- **406** 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: Telegram Bots được sử dụng trong các chiến dịch tấn công để lấy cắp OTP

Xác thực 2 yếu tố (2FA) là một trong những phương pháp đơn giản và phổ biến được sử dụng để bảo vệ quyền riêng tư trực tuyến của người dùng. Do đó, tội phạm mạng đã bắt đầu nhằm mục tiêu đến tính năng này để tấn công.

Gần đây, các nhà nghiên cứu từ Intel 471 cho biết các dịch vụ cho phép kẻ tấn công đánh cắp mật khẩu OTP đang ngày một gia tăng. Các dịch vụ này bắt đầu hoạt động vào tháng 6 bằng cách sử dụng các bot hoặc hoặc các kênh 'hỗ trợ khách hàng' trên Telegram. Các bot được sử dụng để tự động liên hệ với những đối tượng mục tiêu nhằm lừa họ để lấy được mã OTP. Ngoài ra, các bot khác đang nhằm mục tiêu tới người dùng mạng xã hội thông qua các vụ tấn công lừa đảo và hoán đổi SIM.

Các nhà nghiên cứu đã phát hiện ra hai bot được quan tâm: BloodOTPbot và SMSRanger. BloodOTPbot là một bot dựa trên SMS được sử dụng để tạo các cuộc gọi tự động mạo danh nhân viên ngân hàng. SMSRanger được sử dụng để nhắm mục tiêu vào các dịch vụ cụ thể bao gồm PayPal, Apple Pay và Google Play cũng như các nhà cung cấp dịch vụ không dây.

Telegram đã trở thành một nền tảng đáng quan tâm của các đối tượng tấn công vì những lợi ích mà nó mang lại. Ở Áo, một bot Telegram đã được sử dụng để tạo các chứng chỉ vắc-xin giả miễn phí, những chứng chỉ giả này cũng được bán ở Brazil, Úc, Hòa Ký, Anh, Ireland, Phần Lan, Bồ Đào Nha,…

Các vụ tấn công gần đây thông qua nền tảng Telegram cho thấy rằng ngay cả xác thực hai yếu tố (2FA) cũng không tránh khỏi các mối đe dọa. Do đó, người dùng cần sử dụng các phương thức bảo mật khác thay cho OTP dựa trên cuộc gọi điện thoại hoặc tin nhắn văn bản.

Nguồn: https://cyware.com/news/telegram-bots-used-in-latest-campaigns-to-steal-otps-bd401a98

Lỗ hổng bảo mật zero-day trong Windows trở thành mục tiêu khai thác trong chiến dịch tấn công mạng diện rộng.

Các nhà nghiên cứu đã phát hiện lỗ hổng zero-day (CVE-2021-40449) trong Microsoft Windows đã được khai thác trong chiến dịch tấn công mạng APT để nâng cao đặc quyền và chiếm quyền sử dụng Windows Server. Khai thác thành công lỗ hổng, đối tượng tấn công phát tán một trojan truy cập từ xa mới có tên là MysterySnail với mục tiêu đánh cắp dữ liệu trên máy chủ bị xâm nhập.

Phần mềm độc hại này thu thập thông tin cơ bản về máy mục tiêu: tên máy tính, OEM code-page/default identifier, mã định danh mặc định, tên sản phẩm Windows, địa chỉ IP cục bộ, tên người dùng đã đăng nhập.

Các nhà nghiên cứu cho rằng, phần mềm độc hại này không quá phức tạp và có chức năng tương tự như nhiều phần mềm khác. Nhưng bằng cách nào đó nó được chú ý với số lượng tương đối lớn các lệnh điều khiển được sử dụng, các khả năng bổ sung như giám sát các ổ đĩa và có khả năng hoạt động như một proxy. Trong quá trình phân tích MysterySnail RAT của Kaspersky, họ đã liên kết chiến dịch với hoạt động APT của nhóm IronHusky (Trung Quốc).

Các cuộc tấn công mới nhất được phát hiện là nhằm mục tiêu trên diện rộng. Các nhà nghiên cứu bảo mật đã tìm thấy các biến thể của MysterySnail được sử dụng trong các chiến dịch gián điệp rộng rãi nhằm mục tiêu các công ty CNTT, nhà thầu quân sự và quốc phòng.

Nguồn: https://threatpost.com/windows-zero-day-exploited-espionage/175432/?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 406 lỗ hổng, trong đó có 04 lỗ hổng mức cao, 62 lỗ hổng mức trung bình, 14 lỗ hổng mức thấp và 326 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 70 lỗ hổng trong sản phẩm của Microsoft, Nhóm 29 lỗ hổng trong phần mềm Google Chrome, Nhóm 16 lỗ hổng trong các Wordpress plugin, Nhóm 14 lỗ hổng trong sản phẩm của Aruba, Nhóm 07 lỗ hổng trong các sản phẩm của IBM, Nhóm 07 lỗ hổng trong phần mềm Adobe, Nhóm 06 lỗ hổng trong phần mềm Apache. 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:

- Microsoft: CVE-2021-41354, CVE-2021-41353,...

- Google: CVE-2021-37965, CVE-2021-37963,...

- Wordpress: CVE-2021-39330, CVE-2021-39337,...

- Aruba: CVE-2021-40988, CVE-2021-40990,...

- IBM: CVE-2020-4654, CVE-2021-29906,...

- Adobe: CVE-2021-40728, CVE-2021-40729,...

- Apache: CVE-2021-38295, CVE-2021-41832,...

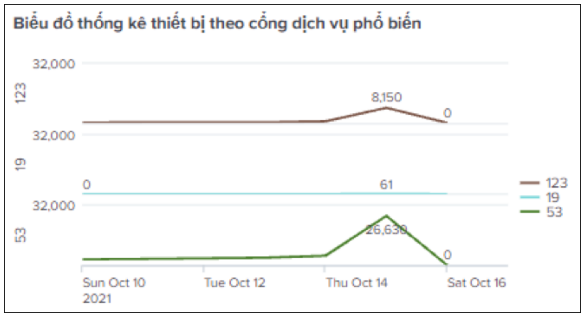
Thông tin điểm yếu, lỗ hổng

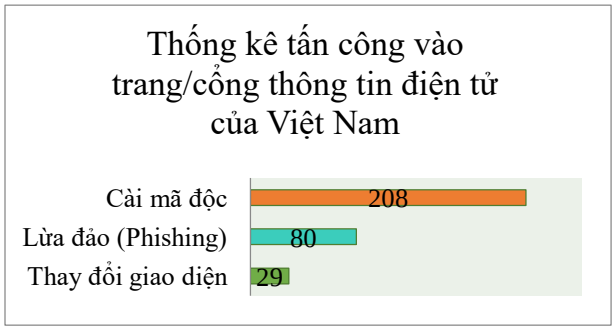
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2021-41354 CVE-2021-41353 CVE-2021-40457 …	Nhóm 70 lỗ hổng trong sản phẩm của Microsoft (Windows, Exchange Server,…) cho phép đối tượng tấn công thu thập thông tin, tấn công XSS, tấn công giả mạo, thực thi mã từ xa, tấn công từ chối dịch vụ, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
2	Google	CVE-2021-37965 CVE-2021-37963 CVE-2021-37964 …	Nhóm 29 lỗ hổng trong phần mềm Google Chrome cho phép đối tượng tấn công thu thập thông tin, tấn công giả mạo, chèn và thực thi mã, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE-2021-39330 CVE-2021-39337 CVE-2021-24651 …	Nhóm 16 lỗ hổng trong các Wordpress plugin cho phép đối tượng tấn công tải lên file thực thi, tấn công stored-XSS, chiếm quyền kiểm soát trang web, tấn công SQL injection.	Đã có thông tin xác nhận và bản vá
4	Aruba	CVE-2021-40988 CVE-2021-40990 …	Nhóm 14 lỗ hổng trong sản phẩm của Aruba (ClearPass Policy Manager,…) cho phép đối tượng tấn công thu thập thông tin, tấn công path traversal, SQL injection, thực thi lệnh từ xa, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá cho một số lỗ hổng
5	IBM	CVE-2020-4654 CVE-2021-29906 CVE-2021-29679 …	Nhóm 07 lỗ hổng trong các sản phẩm của IBM (Sterling File Gateway,…) cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
6	Adobe	CVE-2021-40728 CVE-2021-40729 CVE-2021-40724 …	Nhóm 07 lỗ hổng trong phần mềm Adobe (Acrobat Reader DC,…) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, thực thi mã tùy ý, tấn công CSRF, XSS.	Đã có thông tin xác nhận và bản vá
7	Apache	CVE-2021-38295 CVE-2021-41832 CVE-2021-41830 …	Nhóm 06 lỗ hổng trong phần mềm Apache (CouchDB,…) cho phép đối tượng tấn công leo thang đặc quyền, tấn công từ chối dịch vụ.	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 **56,103** (giảm so với tuần trước **59,601**) 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.



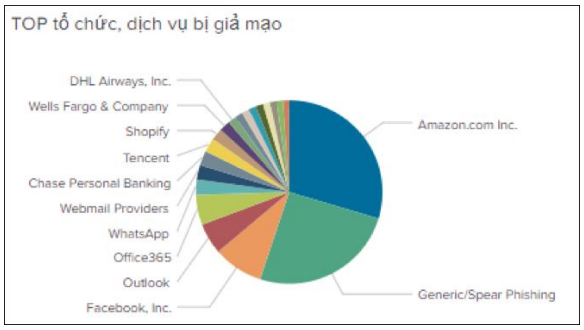


Tấn công Phishing

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 đánh cắp tài khoản.

Tấn công Web

Trong tuần, có 317 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 29 trường hợp tấn công thay đổi giao diện, 80 trường hợp tấn công lừa đảo (Phishing), 208 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 95 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 là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	http://enrichs.me/	Website lừa đảo cờ bạc qua ví điện tử Momo
2	https://newvnhill.site/ https://newvnpop.site	Giả mạo thông tin lừa đảo người dùng chuyển tiền
3	https://tiki56.com	Giả mạo website sàn TMĐT Tiki
4	https://vongquay-lienminh.com/	Giả mạo http://lienminh.garena.vn/ đánh cắp thông tin cá nhân, tài khoản khách hàng để thu lợi
5	https://acb.v-pay.info/ https://acb.v-ipay.top/ https://v-acb.top/	Giả mạo website ngân hàng ACB
6	https://scb.ipay-online.vip/	Giả mạo website ngân hàng SCB
7	http://www.smrtbiddv.com/	Giả mạo website ngân hàng BIDV
8	https://chuongtrinhgionghatvietnamnhi2021.weebly.com/	Website lấy cắp thông tin người dùng facebook, giả mạo chiếm đoạt tài sản

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