NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 01 (01/01/2024 – 07/01/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm UAC-0050 áp dụng chiến thuật lừa đảo mới trong chiến dịch phát tán mã độc Remcos RAT.

- **Cảnh báo:** SpectralBlur: Mã Độc Backdoor mới từ Triều Tiên đe dọa macOS.

2. Điểm yếu, lỗ hổng

- **585** 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: 304** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm UAC-0050 áp dụng chiến thuật lừa đảo mới trong chiến dịch phát tán mã độc Remcos RAT"

Nhóm APT UAC-0050 đã thực hiện các cuộc tấn công lừa đảo để phát tán mã độc Remcos RAT thông qua chiến dịch mới nhằm tránh bị phát hiện bởi phần mềm bảo mật. Bắt đầu hoạt động từ năm 2020, UAC-0050 chủ yếu tập trung nhằm vào Ukraina và Ba Lan thông qua các chiến dịch giả mạo tổ chức hợp pháp để lừa người dùng mở các file độc hại.

Remcos RAT (Remote Control RAT) là một loại phần mềm độc hại được sử dụng cho mục đích giám sát và kiểm soát từ xa. Remcos RAT nổi tiếng với khả năng thu thập dữ liệu hệ thống và thông tin đăng nhập từ các trình duyệt web như Internet Explorer, Mozilla Firefox và Google Chrome. Nó đã trở thành một trong những công cụ hàng đầu trong bộ sưu tập vũ khí của nhóm UAC-0050.

Ngày 21 tháng 12 năm 2023, kết quả phân tích một file LNK của mã độc Remcos RAT cho thấy đối tượng tấn công nhằm vào quân đội Ukraina thông qua email lừa đảo, giả mạo vai trò tư vấn với Lực lượng Phòng vệ Israel (IDF). Sau đó, tệp LNK này thu thập thông tin về phần mềm antivirus trên máy tính mục tiêu và tiến hành tải và thực thi một ứng dụng HTML từ xa có tên "6.hta" bởi máy chủ từ xa sử dụng mshata.exe, một binary trên Windows được dùng cho việc thực thi file HTA.

Bước tiếp theo của cuộc tấn công là sử dụng script PowerShell để tải xuống hai tệp "word_update.exe" và "ofer.docx". Chạy "word_update.exe" sẽ tạo một bản sao của chính nó và thiết lập tính duy trì của hệ thống. Tệp nhị phân này sử dụng ống không tên (unnamed pipes) để giao tiếp và cuối cùng khởi chạy phần mềm độc hại Remcos RAT. Việc triển khai mã độc Remcos RAT (phiên bản 4.9.2 Pro) có khả năng thu thập dữ liệu hệ thống, cookies và thông tin đăng nhập từ một số trình duyệt web.

Các nhà nghiên cứu cảnh báo rằng việc sử dụng ống trong hệ điều hành Windows là một chiến lược tinh vi, giúp nhóm UAC-0050 tránh bị phát hiện từ các hệ thống bảo mật. Điều này đánh dấu một bước tiến đáng kể trong sự phát triển của nhóm APT trong việc triển khai các chiến lược tấn công mạng.

Nguồn: https://thehackernews.com/2024/01/uac-0050-group-using-new-phishing.html?&web_view=true

Tin tức An toàn thông tin

"Cảnh báo: SpectralBlur: Mã Độc Backdoor mới từ Triều Tiên đe dọa macOS"

Mã độc backdoor mới trên Apple macOS, được đặt tên là SpectralBlur, đã được các chuyên gia bảo mật phát hiện. Đáng chú ý, SpectralBlur có nhiều điểm chung với một chủng mã độc liên quan đến các cuộc tấn công của Triều Tiên. Mã độc này có khả năng tải lên/tải xuống file, thực thi shell, cập nhật cấu hình, xóa file và chuyển sang trạng thái ngủ đông thông qua các lệnh từ máy chủ C&C.

SpectralBlur nổi bật với đặc điểm giống với KANDYKORN (hoặc SockRacket), một loại trojan truy cập từ xa (RAT) có khả năng điều khiển hệ thống từ xa với khả năng chiếm quyền kiểm soát các hệ thống bị ảnh hưởng. Hơn nữa, hoạt động của KANDYKORN liên quan đến một chiến dịch của nhóm BlueNoroff (hay TA444), một phần của nhóm APT Lazarus, với mục tiêu triển khai backdoor RustBucket và payload cuối cùng mang tên ObjCShellz.

Gần đây, các chuyên gia bảo mật đã ghi nhận việc đối tượng tấn công tích hợp các thành phần của KANDYKORN và RustBucket để lan truyền mã độc. Những phát hiện mới nhất chỉ ra rằng các đối tượng Triều Tiên đang tăng cường chiến lược tấn công, đặc biệt là đối với các hệ thống liên quan đến lĩnh vực tiền ảo và blockchain trên macOS.

Sự tương đồng giữa chức năng của KANDYKORN và SpectralBlur cho thấy rằng hai mã độc này có thể được phát triển bởi các lập trình viên khác nhau nhưng có cùng mục tiêu chung. Điểm nổi bật của SpectralBlur là khả năng gây gián đoạn cho quá trình phân tích và tránh bị phát hiện bằng cách sử dụng grantpt để thiết lập một terminal giả mạo và thực thi các lệnh shell từ máy chủ C&C.

Thông tin về mã độc này được tiết lộ sau khi phát hiện 21 chủng mã độc mới nhắm vào macOS trong năm 2023, bao gồm ransomware, mã độc đánh cắp thông tin, mã độc RAT và các mã độc được hậu thuẫn bởi chính quyền. Số liệu này tăng so với 13 chủng mã độc được phát hiện trong năm 2022. Dự đoán từ chuyên gia cho thấy sự phát triển và phổ biến của macOS trong doanh nghiệp có thể dẫn đến xuất hiện nhiều mã độc mới trên hệ điều hành này trong năm 2024.

Nguồn:
https://thehackernews.com/2024/01/spectralblur-new-macos-backdoor-threat.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 **585** lỗ hổng, trong đó có 254 lỗ hổng mức Cao, 182 lỗ hổng mức Trung bình, 29 lỗ hổng mức Thấp và 120 lỗ hổng chưa đánh giá. Trong đó có ít nhất 56 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 22 lỗ hổng trong Google, Nhóm 05 lỗ hổng trong Wireshark, Nhóm 04 lỗ hổng trong Apache, Nhóm 135 lỗ hổng trong Wordpress, Nhóm 04 lỗ hổng trong Linux, Nhóm 08 lỗ hổng trong Samsung, Nhóm 26 lỗ hổng trong Qualcomm. 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:

- Google: CVE-2023-32889,...

- Wireshark: CVE-2024-0207,...

- Apache: CVE-2023-49299,...

- Wordpress: CVE-2022-48639,...

- Linux: CVE-2023-6270, CVE-2023-0193,...

- Samsung: CVE-2024-20808,...

- Qualcomm: CVE-2023-33025,...

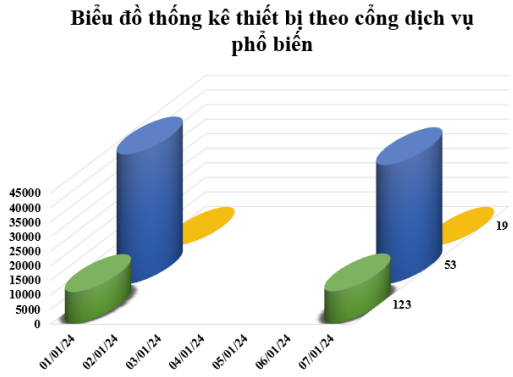
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-32889 CVE-2023-48419 CVE-2023-48418 …	Nhóm 22 lỗ hổng trong Google cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
2	Wireshark	CVE-2024-0207 CVE-2024-0208 CVE-2024-0209 …	Nhóm 05 lỗ hổng trong Wireshark cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Apache	CVE-2023-49299 CVE-2023-51784 CVE-2023-51785 …	Nhóm 04 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi mã từ xa truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-46839 CVE-2023-51475 CVE-2023-25054 …	Nhóm 135 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗ hổng SQL Injection, khai thác lỗ hổng CSRF, khai thác lỗ hổng XSS.	Chưa có thông tin xác nhận và bản vá
5	Linux	CVE-2023-6270 CVE-2024-0193 CVE-2023-7192 …	Nhóm 04 lỗ hổng trong Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Samsung	CVE-2024-20808 CVE-2024-20809 CVE-2024-20803 …	Nhóm 08 lỗ hổng trong Samsung cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	Qualcomm	CVE-2023-33025 CVE-2023-33030 CVE-2023-33032 …	Nhóm 26 lỗ hổng trong Qualcomm phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa 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 **52.017**, (giảm so với tuần trước **55.435**) 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.

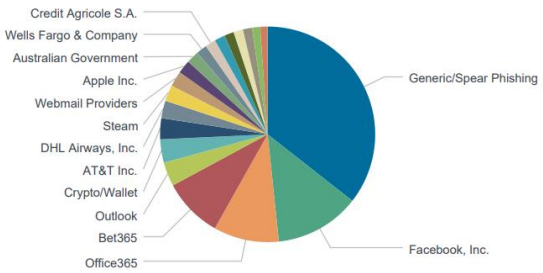


Tấn công Web

Trong tuần, có **244** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 229 trường hợp tấn công lừa đảo (Phishing), 15 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: 11454 IP	hzmksreiuojy.ru: 185 IP
disorderstatus.ru: 4934 IP	xjpakmdcfuqe.biz: 133 IP
atomictrivia.ru: 2230 IP	xjpakmdcfuqe.com: 62 IP
amnsreiuojy.ru: 830 IP	xjpakmdcfuqe.ru: 43 IP
restlesz.su: 273 IP	xjpakmdcfuqe.in: 37 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **304** phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam phản ánh 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	khcn-han-muc-tin-dung-ca-nhan.com	Website giả mạo Ngân hàng TMCP Hàng hải Việt Nam
2	dadw55.com dadw11.com tikivn.live	Website giả mạo sàn TMĐT Tiki
3	sp8668vn.com shop80pot.com showzyeye.com tb55988.com sp315693vn.com	Website giả mạo sàn TMĐT Shopee
4	www.vieclamlazada.com.vn	Website giả mạo sàn TMĐT Lazada
5	cltxmm.us	Website giả mạo Ví điện tử Momo
6	vibcskh.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
7	nang-han-muc-ido-vpbank.com cskh-the-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng

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 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
ncsc@ais.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội