NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 34 (21/8/2023 – 27/8/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Lazarus sử dụng lỗ hổng trong ManaEngine để triển khai QuiteRAT.

- **Cảnh báo:** Chiến dịch LABRAT sử dụng lỗ hổng trong GitLab để tấn công Cryptojacking và Proxyjacking.

2. Điểm yếu, lỗ hổng

- **535** 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: 369** 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://service.khonggianmang.vn

https://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Lazarus sử dụng lỗ hổng trong ManaEngine để triển khai QuiteRAT"

Nhóm APT Lazarus, được cho là có sự hậu thuẫn của Triều Tiên, đã bắt đầu triển khai một chiến dịch mới nhằm vào hạ tầng Internet quan trọng và các tổ chức y tế tại Châu u. Theo thông tin từ các chuyên gia, nhóm APT này đã tiến hành cuộc tấn công bằng cách khai thác lỗ hổng CVE-2022-47966 trong ManageEngine ServiceDesk từ tháng 1, chỉ trong vòng 5 ngày sau khi lỗ hổng này được công bố.

Thông tin chi tiết:

Nhóm Lazarus đã khai thác lỗ hổng để xác lập quyền truy cập ban đầu, kích hoạt việc tải và chạy một binary độc hại thông qua quy trình Java Runtime, từ đó mở đầu quá trình cài đặt mã độc trên máy chủ bị tấn công..

Binary này là phiên bản biến thể của phần mềm độc hại MagicRAT, có tên gọi là QuiteRAT.

Nhóm Lazarus cũng đã giới thiệu một mã độc mới trong chiến dịch này, có tên gọi là CollectionRAT, với khả năng thực thi các lệnh tùy ý trên hệ thống bị nhiễm mã độc.

Ngoài ra, theo các chuyên gia bảo mật, đã xác định được liên kết giữa mã độc CollectionRAT và mã độc Jupiter/EarlyRAT mà trước đó đã được xác định là có liên quan với nhóm APT Andariel APT, nhóm này hoạt động dưới sự hậu thuẫn của nhóm APT Lazarus.

Từ MagicRAT tới QuiteRAT:

Tương tự MagicRAT, QuiteRAT được xây dựng trên nền tảng Qt framework, một framework mã nguồn mở đa nền tảng dành cho việc phát triển ứng dụng. Đây là framework sở hữu các chức năng như thực thi mã tùy ý.

Tuy nhiên, kích cỡ của file framework chỉ từ 4 đến 5MB, nhỏ hơn đáng kể so với mã độc MagicRAT nặng 18MB.

Theo phân tích, sự khác biệt lớn về kích thước có thể liên quan đến quyết định của nhóm APT Lazarus về việc chỉ tích hợp các thư viện cần thiết của Qt vào QuiteRAT, khác với MagicRAT được tích hợp toàn bộ framework Qt.

Trong khi MagicRAT tích hợp các cơ chế duy trì tồn tại thông qua việc cấu hình các nhiệm vụ được lên lịch, QuiteRAT lại không có tính năng này. Thay vào đó, QuiteRAT phụ thuộc vào máy chủ C&C để cung cấp hướng dẫn duy trì sự tồn tại của mã độc trên thiết bị.

Tổng kết

Đây là chiến dịch thứ ba của nhóm Lazarus trong năm 2023, và một điểm đáng chú ý là nhóm tấn công đã sử dụng cơ sở hạ tầng giống nhau cho tất cả các chiến dịch này. Các chuyên gia bảo mật khuyến nghị cần theo dõi và phân tích các nguy cơ để có thể ngăn chặn sự lây nhiễm từ QuiteRAT một cách kịp thời.

Nguồn: https://cyware.com/news/lazarus-exploits-manageengine-to-deploy-quiterat-fd174c2c

Tin tức An toàn thông tin

"Cảnh báoPhát hiện mã độc giả mạo ứng dụng "OfficeNote" trên macOS"

Một biến thể mới của mã độc XLoader đã xuất hiện trên Apple macOS. Mã độc này bị phát hiện đang che giấu các chức năng độc hại dưới vỏ bọc của ứng dụng văn phòng "OfficeNote".

Phiên bản mới của mã độc XLoader được ngụy trang dưới hình ảnh của một ổ đĩa thông thường của Apple có tên "OfficeNote.dmg" và có chữ ký của nhà phát triển "MAIT JAKHU (54YDV8NU9C)".

XLoader lần đầu được phát hiện vào năm 2020 và được xem là phiên bản cập nhật của Formbook. Mã độc này có khả năng đánh cắp thông tin và keylog được cung cấp dưới dạng malware-as-a-service (MaaS – mã độc dạng dịch vụ). Biến thể của mã độc xuất hiện trên macOS vào tháng 07/2021 và được phát tán thông qua chương trình Java trên file .JAR.

Theo các chuyên gia bảo mật, việc Apple ngừng cung cấp Java Runtime Environment (JRE) kèm theo macOS mới đã khiến cho các tệp .JAR độc hại không thể thực thi trên macOS mới vì những tệp này yêu cầu sử dụng JRE. Trong phiên bản mới nhất của XLoader, mã độc này đã vượt qua sự hạn chế này bằng cách chuyển sang sử dụng các ngôn ngữ lập trình C và Objective C, với tệp ảnh ổ đĩa được ký vào ngày 17/07/2023. Hiện tại, Apple đã thu hồi chữ ký của tệp ảnh này.

Một công ty bảo mật đã phát hiện nhiều dấu vết được tải lên trang VirusTotal trong suốt tháng 7 năm nay, cho thấy sự tồn tại của một chiến dịch lây lan rộng của mã độc này.

Sau khi thực thi, OfficeNote hiển thị một thông báo lỗi "không thể mở do không thể tìm thấy tệp gốc". Điều này là một chiêu trò để lừa đảo trong khi thực tế, mã độc này đang cài đặt một ứng dụng tên là "Launch Agent" ẩn trong hệ thống để duy trì việc kết nối.

XLoader được tạo ra để thu thập dữ liệu từ clipboard cũng như thông tin trong các thư mục của các trình duyệt như Google Chrome và Firefox. Mã độc này cũng được cấu hình để chạy các lệnh ngủ nhằm trì hoãn việc thực thi, từ đó không để lại bất kỳ dấu vết nào quá lộ liễu để tránh bị phát hiện.

Theo nhận định từ các chuyên gia, nếu các thông tin này bị đánh cắp có thể bị rao bán cho các đối tượng tấn công khác, gây ra những hậu quả lâu dài đối với người dùng.

Nguồn: https://thehackernews.com/2023/08/new-variant-of-xloader-macos-malware.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 **535** lỗ hổng, trong đó có 158 lỗ hổng mức Cao, 119 lỗ hổng mức Trung bình, 03 lỗ hổng mức Thấp và 255 lỗ hổng chưa đánh giá. Trong đó có ít nhất 63 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 04 lỗ hổng trong Microsoft, Nhóm 26 lỗ hổng trong Tenda, Nhóm 09 lỗ hổng trong Google, Nhóm 47 lỗ hổng trong Wordpress, Nhóm 07 lỗ hổng trong Python, Nhóm 07 lỗ hổng trong TP-LINK, Nhóm 06 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:

- Microsoft: CVE-2023-36787, CVE-2023-36741,...

-Tenda: CVE-2023-39670,CVE-2023-39672,...

- Google: CVE-2023-4430, CVE-2023-4429,...

-Wordpress: CVE-2023-4404, CVE-2023-3604,...

-Python: CVE-2022-25024, CVE-2022-48560,..

-TP-LINK: CVE-2023-39747,CVE-2023-39751,...

-IBM: CVE-2023-38734, CVE-2023-40370,...

Thông tin điểm yếu, lỗ hổng

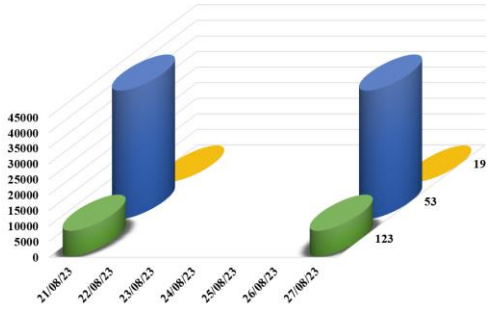
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-36787 CVE-2023-36741 CVE-2020-19725 ...	Nhóm 04 lỗ hổng trong Apple cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
2	Tenda	CVE-2023-39670 CVE-2023-39672 CVE-2023-39673 ...	Nhóm 26 lỗ hổng trong Tenda cho phép đối tượng tấn công thực hiện lỗi Buffer Overflow, 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
3	Google	CVE-2023-4430 CVE-2023-4429 CVE-2023-4428 ...	Nhóm 09 lỗ hổng trong Google cho phép đối tượng tấn công thực hiện lỗi XSS, leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-4404 CVE-2023-3604 CVE-2023-28994 ...	Nhóm 47 lỗ hổng trong Wordpress cho phép đối tượng tấn công leo thang đặc quyền, thực hiện lỗi XSS, truy cập và thực hiện các hành động trái phép	Chưa có thông tin xác nhận và bản vá
5	Python	CVE-2022-25024 CVE-2022-48560 CVE-2022-48564 ...	Nhóm 07 lỗ hổng trong Python cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	TP-LINK	CVE-2023-39747 CVE-2023-39751 CVE-2023-39745 ...	Nhóm 07 lỗ hổng trong TP-LINK cho 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
7	IBM	CVE-2023-38734 CVE-2023-40370 CVE-2023-38732 ...	Nhóm 06 lỗ hổng trong IBM phép đối tượng tấn công truy cập và 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

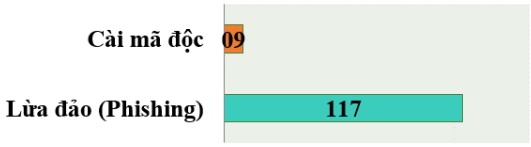
Tấn công DRDoS

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 **50.012**, (tăng so với tuần trước **49.587**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

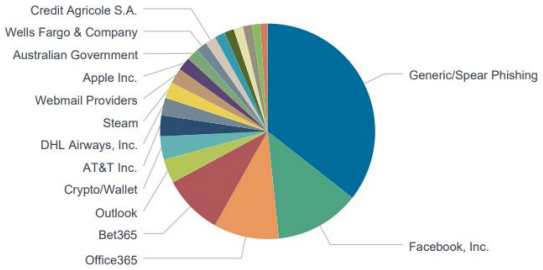


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 126 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 117 trường hợp tấn công lừa đảo (Phishing), 09 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: 10437 IP	xjpakmdcfuqe.ru: 60 IP
disorderstatus.ru: 4401 IP	xjpakmdcfuqe.in: 65 IP
atomictrivia.ru: 2086 IP	restlesz.su: 282 IP
xjpakmdcfuqe.biz: 171 IP	amnsreiuojy.ru: 519 IP
xjpakmdcfuqe.com: 80 IP	hzmksreiuojy.ru: 53 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **369** 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	macysbyi.com	Website giả mạo Ebay
2	viet.cgovn.cc vietgov5.cc	Website giả mạo Dịch vụ công Quốc Gia
3	hdfn.online	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
4	mbbffn.online	Website giả mạo Ngân hàng TMCP Quân đội
5	clmm.pe	Website giả mạo Ví điện tử Momo

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
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