NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 03 (15/01/2024 – 21/01/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT UNC3886 của Trung Quốc âm thầm khai thác lỗ hổng Zero-Day của VMware trong suốt 2 năm.

- **Cảnh báo:** Phát hiện lỗ hổng trên Apache ActiveMQ trong chiến dịch tấn công Godillza Web Shell.

2. Điểm yếu, lỗ hổng

- **762** 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: 351** 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 APT UNC3886 của Trung Quốc âm thầm khai thác lỗ hổng Zero-Day của VMware trong suốt 2 năm"

Nhóm APT UNC3886 được cho là có liên quan đến Trung Quốc, đang khai thác một lỗ hổng zero-day trong VMware vCenter Server từ cuối năm 2021. Nổi bật với khả năng khai thác các lỗ hổng bảo mật mà không bị phát hiện trong nhiều chiến dịch tấn công mạng, nhóm UNC3886 đã khai thác thành công nhiều lỗ hổng bảo mật trong thiết bị VMware và Fortinet.

Lỗ hổng CVE-2023-34048 ở mức nghiêm trọng khi có điểm CVSS: 9.8, đây là một lỗ hổng viết nằm ngoài phạm vi, cho phép đối tượng tấn công thực thi mã hóa từ xa khi có quyền truy cập mạng vCenter Server. Mặc dù lỗ hổng này đã được vá vào ngày 24 tháng 10 năm 2023 nhưng VMware đã cập nhật thông báo mới nhất để xác nhận rằng lỗ hổng CVE-2023-34048 đã bị khai thác trong môi trường thực tế.

UNC3886 lần đầu bị phát hiện vào tháng 9 năm 2022 khi đang khai thác các lỗ hổng bảo mật trong VMware để thực hiện backdoor vào hệ thống Windows và Linux nhằm triển khai nhiều họ mã độc như VIRTUALPITA và VIRTUALPIE. Sau khi khai thác thành công lỗ hổng CVE-2023-34048, đối tượng tấn công có thể đạt được quyền truy cập đặc quyền vào hệ thống vCenter, liệt kê các máy chủ ESXi và máy ảo.

Cuộc tấn công tiếp theo bao gồm việc thu thập thông tin đăng nhập "vpxuser" và cài đặt malware VIRTUALPITA và VIRTUALPIE để kết nối trực tiếp với máy chủ. Qua đó, mở đường cho việc khai thác một lỗ hổng VMware khác (CVE-2023-20867) để thực hiện lệnh tùy ý và truyền tải tệp tin.

UNC3886 không chỉ tấn công VMware mà còn khai thác lỗ hổng trong Fortinet FortiOS để triển khai phần mềm độc hại THINCRUST và CASTLETAP. Nhóm này đặc biệt chú ý đến công nghệ tường lửa và ảo hóa, hướng đến việc thực hiện các lệnh tùy ý và thu thập dữ liệu nhạy cảm. Nguyên nhân là do các công nghệ này không có hỗ trợ cho các giải pháp phát hiện và phản ứng trên điểm cuối (EDR), giúp nhóm APT duy trì sự tồn tại trong môi trường mục tiêu trong thời gian dài.

Để giảm thiểu nguy cơ tấn công mạng, các chuyên gia bảo mật khuyến nghị người dùng VMware vCenter Server cần thực hiện nâng cấp phần mềm lên phiên bản mới nhất.

Nguồn: https://thehackernews.com/2024/01/chinese-hackers-silently-weaponized.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: SpectralBlur: Phát hiện lỗ hổng trên Apache ActiveMQ trong chiến dịch tấn công Godillza Web Shell"

Các chuyên gia bảo mật đang cảnh báo về một làn sóng gia tăng đáng kể trong hoạt động của các nhóm tấn công mạng, đặc biệt là khi chúng tích cực khai thác một lỗ hổng trên Apache ActiveMQ để triển khai web shell mang tên là Godzilla. Web shell này được ẩn giấu dưới định dạng nhị phân không rõ nguồn gốc nhằm qua mặt các công cụ quét và biện pháp bảo mật dựa trên chữ ký.

Đáng chú ý, mặc dù định dạng file nhị phân này chưa được xác định, động cơ JSP của ActiveMQ vẫn tiếp tục biên dịch và thực thi web shell, tạo điều kiện cho các đối tượng tấn công xâm nhập mà không bị phát hiện bởi các công cụ bảo mật.

Lỗ hổng đang bị khai thác có mã CVE-2023-46604 (Điểm CVSS: 10.0) là một lỗ hổng nghiêm trọng trên Apache ActiveMQ cho phép đối tượng tấn công thực thi mã từ xa. Trong chuỗi tấn công mới nhất được phát hiện, các thiết bị đã bị tấn công thông qua việc cài đặt các web shell sử dụng JSP, được đặt trong thư mục "admin" khi cài đặt ActiveMQ. Từ khi thông tin về lỗ hổng này được công bố vào cuối tháng 10/2023, đã có nhiều đối tượng tấn công sử dụng lỗ hổng này để triển khai các loại mã độc như ransomware, rootkit, đào tiền ảo và botnet DDoS.

Web shell có tên Godzilla là một backdoor với nhiều tính năng, có khả năng xử lý các yêu cầu HTTP POST, thực thi nội dung và trả về kết quả dưới dạng phản hồi HTTP. Quá trình tấn công cho thấy mã web shell được chuyển đổi thành mã Java trước khi thực thi bởi Jetty Servlet Engine, cho phép đối tượng tấn công kết nối và có quyền kiểm soát đầy đủ trên hệ thống mục tiêu.

Trong chiến dịch này, payload JSP có mục tiêu cuối cùng là cho phép đối tượng tấn công kết nối đến web shell thông qua giao diện quản lý của Godzilla. Điều này giúp các nhóm tấn công chiếm hoàn toàn quyền kiểm soát thiết bị mục tiêu, cho phép thực thi các lệnh shell tùy ý và xem thông tin mạng, đồng thời thực hiện các thao tác quản lý tập tin.

Hiện nay, lỗ hổng CVE-2023-46604 đã được cập nhật bản vá để khắc phục, tuy nhiên, các chuyên gia bảo mật khuyến nghị người dùng Apache ActiveMQ nên cập nhật phiên bản mới nhất sớm nhất có thể để giảm thiểu khả năng bị tấn công bởi các đối tượng khai thác lỗ hổng này.

Nguồn:
https://thehackernews.com/2024/01/apache-activemq-flaw-exploited-in-new.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 **762** lỗ hổng, trong đó có 250 lỗ hổng mức Cao, 297 lỗ hổng mức Trung bình, 27 lỗ hổng mức Thấp và 188 lỗ hổng chưa đánh giá. Trong đó có ít nhất 138 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 13 lỗ hổng trong Linux, Nhóm 15 lỗ hổng trong Google, Nhóm 04 lỗ hổng trong Adobe, Nhóm 43 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong Gitlab, Nhóm 12 lỗ hổng trong Tenda, Nhóm 08 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:

- Linux: CVE-2024-0562, CVE-2024-0582,...

- Google: CVE-2023-48340,...

- Adobe: CVE-2024-20709,...

- Wordpress: CVE-2022-1617,...

- Gitlab: CVE-2023-5356, CVE-2023-7028,...

- Tenda: CVE-2024-0531, CVE-2023-0532,...

- IBM: CVE-2024-22317, CVE-2023-40683,...

Thông tin điểm yếu, lỗ hổng

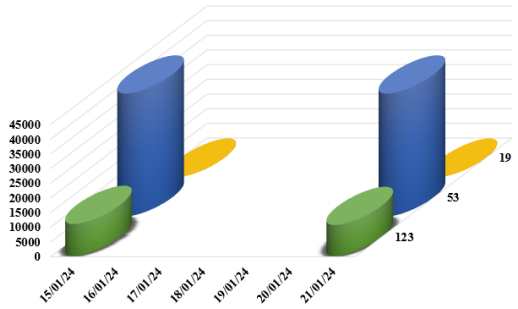
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2024-0562 CVE-2024-0582 CVE-2024-0646 …	Nhóm 13 lỗ hổng trong Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Google	CVE-2023-48340 CVE-2023-48341 CVE-2023-48343 …	Nhóm 15 lỗ hổng trong Google 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
3	Adobe	CVE-2024-20709 CVE-2024-20721 CVE-2023-51463 …	Nhóm 04 lỗ hổng trong Adobe cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗ hổng XSS.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-1617 CVE-2023-2655 CVE-2022-1609 …	Nhóm 43 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗ hổng SQL Injection, khai thác lỗ hổng XSS, khai thác lỗ hổng CSRF, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
5	Gitlab	CVE-2023-5356 CVE-2023-7028 CVE-2023-2030 …	Nhóm 05 lỗ hổng trong Gitlab 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
6	Tenda	CVE-2024-0531 CVE-2024-0532 CVE-2024-0533 …	Nhóm 12 lỗ hổng trong Tenda 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	IBM	CVE-2024-22317 CVE-2023-40683 CVE-2023-47718 …	Nhóm 08 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗ hổng CSRF, khai thác lỗ hổng SSRF, 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

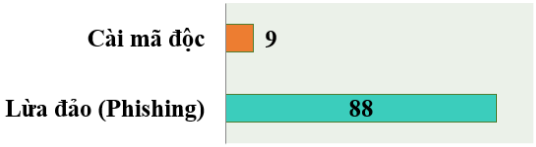
Tấn công DRDoS

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 **52.500**, (giảm so với tuần trước **52.856**) 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

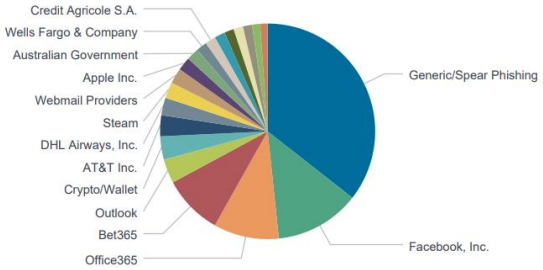


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **97** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 88 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: 14889 IP	hzmksreiuojy.ru: 187 IP
disorderstatus.ru: 5447 IP	xjpakmdcfuqe.biz: 449 IP
atomictrivia.ru: 2572 IP	xjpakmdcfuqe.com: 177 IP
amnsreiuojy.ru: 979 IP	xjpakmdcfuqe.ru: 126 IP
restlesz.su: 286 IP	xjpakmdcfuqe.in: 168 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **351** 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	agribank.dangkyungtuyen.com	Website giả mạo Agribank - Ngân hàng nông nghiệp và phát triển nông thôn
2	dich-vu-update-vpbank.com cskh-ca-nhan-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
3	nang-cap-hang-vvip-vib.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
4	p63899vn.com	Website giả mạo sàn TMĐT Shopee
5	baoviet-vn.cc	Website giả mạo Ngân hàng TMCP Bảo Việt
6	lazada.gg	Website giả mạo sàn TMĐT Lazada
7	amajwzon456.top	Website giả mạo sàn TMĐT Amazon
8	vinpearl1.vingroupsny.com	Website giả mạo Tập đoàn Vingroup
9	etkf44.com	Website giả mạo Điện máy xanh

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