NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 51 (18/12/2023 – 24/12/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT UAC-0099 khai thác lỗ hổng trên WinRAR trong chiến dịch tấn công nhằm vào các cơ quan tại Ukraine bằng mã độc LONEPAGE.

- **Cảnh báo:** Mã độc NKAbuse sử dụng blockchain NKN để tấn công DDoS.

2. Điểm yếu, lỗ hổng

- **910** 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: 343** 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 UAC-0099 khai thác lỗ hổng trên WinRAR trong chiến dịch tấn công nhằm vào các cơ quan tại Ukraine bằng mã độc LONEPAGE"

Nhóm APT có tên UAC-0099 liên tiếp thực hiện các cuộc tấn công mạng nhằm vào Ukraina bằng hình thức khai thác lỗ hổng bảo mật nghiêm trọng trên WinRAR để phát tán mã độc LONEPAGE. Nhóm UAC-0099 lần đầu bị phát hiện vào tháng 06/2023, trong khi đang thực hiện các hoạt động gián điệp mạng nhằm vào các tổ chức tiểu bang và cơ quan truyền thông

Nhóm UAC-0099 đã thực hiện chiến dịch tấn công lừa đảo bằng cách sử dụng tin nhắn có chứa các file đính kèm dạng HTA, RAR và LNK. Mục tiêu của chiến dịch tấn công này là triển khai LONEPAGE, một mã độc Visual Basic Script (VBS) có khả năng kết nối tới máy chủ C&C để tải xuống các payload bổ trợ như keylogger, bộ đánh cắp thông tin và mã độc có khả năng chụp ảnh màn hình. UAC-0099 đã thành công trong việc xâm nhập và kiểm soát trái phép nhiều thiết bị tại Ukraine trong giai đoạn khoảng năm 2022-2023.

Chiến dịch tấn công của nhóm UAC-0099 bao gồm ba phương thức chính, cụ thể, phương thức đầu tiên sử dụng file HTA, trong khi hai phương thức còn lại sử dụng file SFX (một loại file lưu trữ tự giải nén) và file ZIP chứa mã độc. File ZIP khai thác lỗ hổng bảo mật trên WinRAR (CVE-2023-38831, Điểm CVSS: 7,8) để triển khai mã độc LONEPAGE.

Đối với chuỗi tấn công sử dụng file SFX, nhóm này tạo một đường dẫn LNK giả mạo một file DOCX đính kèm nội dung là lệnh triệu tập tòa án để đánh lừa người dùng mở file. Điều này dẫn đến việc thực thi đoạn mã PowerShell độc hại để triển khai mã độc LONEPAGE. Đáng chú ý, file ZIP chứa mã độc được UAC-0099 tung ra vào ngày 05/08/2023, chỉ sau 3 ngày kể từ khi WinRAR tung ra bản vá cho lỗ hổng trên sản phẩm của mình.

Các chuyên gia bảo mật đánh giá nhóm UAC-0099 đã sử dụng chiến thuật tấn công đơn giản nhưng hiệu quả bằng cách tạo ra các công cụ gián điệp dựa trên PowerShell và thực thi các tệp VBS. Bên cạnh đó, cũng cảnh báo về một làn sóng tin nhắn lừa đảo mới, giả mạo thông báo từ một hãng viễn thông phổ biến tại Ukraina để lan truyền mã độc Remcos RAT, đồng thời cho rằng chiến dịch này có liên quan đến nhóm APT UAC-0050.

Nguồn: https://thehackernews.com/2023/12/uac-0099-using-winrar-exploit-to-target.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng Zero-Day trên Chrome đang bị khai thác trên không gian mạng"

Google vừa phát hành bản cập nhật bảo mật cho trình duyệt Chrome để khắc phục một lỗ hổng zero-day nghiêm trọng đang bị khai thác trên không gian mạng. Đó là lỗ hổng CVE-2023-7024, một lỗi tràn bộ đệm heap trong framework WebRTC, có thể dẫn đến việc thực thi mã từ xa hoặc gây sự cố cho ứng dụng. Hiện vẫn chưa có thông tin chi tiết về cách lỗ hổng này bị khai thác nhằm giảm thiểu nguy cơ bị tấn công.

Hơn nữa, framework WebRTC là một dự án mã nguồn mở được Mozilla Firefox và Apple Safari cũng sử dụng. Tuy nhiên, hiện vẫn chưa rõ liệu lỗ hổng này có ảnh hưởng đến các trình duyệt khác ngoài Chrome hoặc các trình duyệt dựa trên Chromium.

Việc công bố thông tin này đánh dấu lỗ hổng zero-day thứ 8 bị khai thác trên Chrome kể từ đầu năm 2023.

- CVE-2023-2033 (Điểm CVSS: 8.8) - Type confusion trên V8
- CVE-2023-2136 (Điểm CVSS: 9.6) – Lỗ hổng tràn số nguyên trên Skia
- CVE-2023-3079 (Điểm CVSS: 8.8) - Type confusion trên V8
- CVE-2023-4762 (Điểm CVSS: 8.8) - Type confusion trên V8
- CVE-2023-4863 (Điểm CVSS: 8.8) - Lỗ hổng tràn bộ đệm trên heap trên WebP
- CVE-2023-5217 (Điểm CVSS: 8.8) - Lỗ hổng tràn bộ đệm trên heap trên mã hóa vp8 trong libvpx
- CVE-2023-6345 (Điểm CVSS: 9.6) - Lỗ hổng tràn số nguyên trên Skia

Theo thống kê đã có 26,447 lỗ hổng an toàn thông tin được phát hiện trong năm 2023, nhiều hơn 1500 CVE so với năm ngoái, trong đó có 115 lỗ hổng đã bị khai thác bởi các đối tượng tấn công và các nhóm ransomware.

Đứng đầu danh sách các lỗ hổng phổ biến là: thực thi mã từ xa, bỏ qua chức năng bảo mật, thao túng bộ đệm, leo thang đặc quyền, lỗi xác thực đầu vào và phân tích cú pháp.

Người dùng được khuyến nghị cần nhanh chóng cập nhật Chrome lên phiên bản 120.0.6099.129/130 cho Windows và 20.0.6099.129 cho macOS/Linux để giảm thiểu nguy cơ bị tấn công. Đồng thời, người dùng sử dụng trình duyệt Chromium như Microsoft Edge, Brave, Opera và Vivaldi cũng được khuyến nghị cập nhật bản vá ngay khi khả dụng.

Nguồn: https://thehackernews.com/2023/12/urgent-new-chrome-zero-day.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 **910** lỗ hổng, trong đó có 360 lỗ hổng mức Cao, 437 lỗ hổng mức Trung bình, 22 lỗ hổng mức Thấp và 91 lỗ hổng chưa đánh giá. Trong đó có ít nhất 301 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 21 lỗ hổng trong Mozilla, Nhóm 05 lỗ hổng trong Linux, Nhóm 15 lỗ hổng trong Apache, Nhóm 213 lỗ hổng trong Wordpress, Nhóm 07 lỗ hổng trong Github, Nhóm 193 lỗ hổng trong Adobe, Nhóm 18 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:

- Mozilla: CVE-2023-6866, CVE-2023-6873,...

- Linux: CVE-2023-6546, CVE-2023-6931,...

- Apache: CVE-2023-41314, CVE-2023-29234, ...

- Wordpress: CVE-2023-25970, CVE-2023-29234,...

- Github: CVE-2023-46647, CVE-2023-46648,...

- Adobe: CVE-2023-47064, CVE-2023-47065,...

- IBM: CVE-2023-46177, CVE-2023-42017,...

Thông tin điểm yếu, lỗ hổng

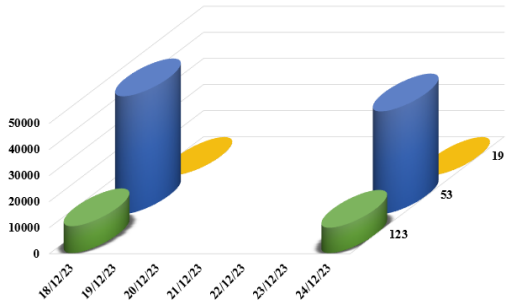
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-6866 CVE-2023-6873 CVE-2023-6862 …	Nhóm 21 lỗ hổng trong Mozilla cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép	Chưa có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-6546 CVE-2023-6931 CVE-2023-6932 …	Nhóm 05 lỗ hổng trong Linux cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Apple	CVE-2023-41314 CVE-2023-29234 CVE-2023-46279 …	Nhóm 15 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi mã từ xa, 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-2023-25970 CVE-2023-29384 CVE-2023-49772 …	Nhóm 213 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện SQL Injection, khai thác lỗ hổng CSRF, khai thác lỗ hổng XSS, khai thác lỗ hổng SSRF, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2023-46647 CVE-2023-46648 CVE-2023-6746 …	Nhóm 07 lỗ hổng trong Github cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Adobe	CVE-2023-47064 CVE-2023-47065 CVE-2023-48440 …	Nhóm 193 lỗ hổng trong Adobe cho phép đối tượng tấn công khai thác lỗ hổng XSS, truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2023-46177 CVE-2023-42017 CVE-2023-47702 …	Nhóm 18 lỗ hổng trong IBM phép đối tượng tấn công leo thực thi mã từ xa, 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

Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

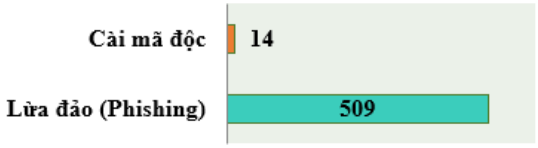
Tấn công DRDoS

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 **49.168**, (giảm so với tuần trước **55.537**) 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

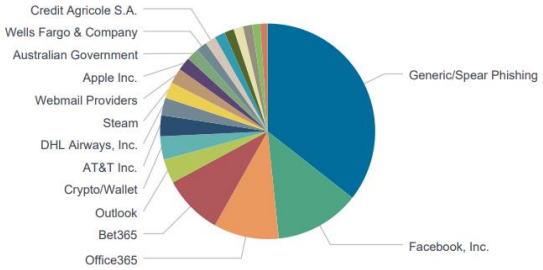


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **523** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 509 trường hợp tấn công lừa đảo (Phishing), 14 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: 13382 IP	hzmksreiuojy.ru: 242 IP
disorderstatus.ru: 5253 IP	xjpakmdcfuqe.biz: 174 IP
atomictrivia.ru: 2456 IP	xjpakmdcfuqe.com: 84 IP
amnsreiuojy.ru: 786 IP	xjpakmdcfuqe.ru: 66 IP
restlesz.su: 339 IP	xjpakmdcfuqe.in: 51 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **343** 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	mallshopvn.vip nykkky.com	Website giả mạo sàn TMĐT Amazon
2	nang-cap-online-vpbank.com dich-vu-online-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
3	tmko1.com tmko2.com tmko3.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
4	aeoonmail.com aaeeonmart.com	Website giả mạo Công ty TNHH Aeon Việt Nam
5	lazadavn.vn	Website giả mạo sàn TMĐT Lazada

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