NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 46 (13/11/2023 – 19/11/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT DarkCasino mới xuất hiện khai thác lỗ hổng trên WinRAR.

- **Cảnh báo:** Phát hiện lỗ hổng an toàn thông tin trên phần mềm email Zimbra đang bị khai thác bởi 4 nhóm tấn công khác nhau.

2. Điểm yếu, lỗ hổng

- **794** 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: 406** 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 DarkCasino mới xuất hiện khai thác lỗ hổng trên WinRAR"

Nhóm APT DarkCasino đã bắt đầu hoạt động kể từ năm 2021 với động cơ nhằm vào kinh tế. DarkCasino có trình độ kỹ thuật và khả năng học tập nhanh chóng, tích hợp nhiều hình thức tấn công APT khác nhau vào chuỗi tấn công của mình. Các chiến dịch tấn công do nhóm thực hiện có mật độ thường xuyên, thể hiện khát vọng đánh cắp tài sản trực tuyến của nhóm.

Gần đây, DarkCasino đã được phát hiện đang thực hiện khai thác lỗ hổng zero-day CVE-2023-38831 (Điểm CVSS: 7.8) cho phép đối tượng tấn công triển khai các payload độc hại.

Vào tháng 08/2023, cơ quan bảo mật đã phát hiện một chiến dịch tấn công có sử dụng lỗ hổng này nhằm vào các diễn đàn giao dịch để phát tán payload có tên DarkMe, một mã độc trojan Visual Basic có liên kết với DarkCasino. Mã độc có khả năng thu thập thông tin của thiết bị, chụp ảnh, thao túng tệp tin và Windows Registry, thực thi câu lệnh và tự cập nhật trên thiết bị nhiễm mã độc.

Trước đó, DarkCasino đã được coi là một chiến dịch lừa đảo thực hiện bởi nhóm Evilnum nhằm vào các nền tảng tín dụng, tiền ảo tại Châu Âu và Châu Á, tuy nhiên, qua thời gian theo dõi chuyên sâu thì nhóm DarkCasino đã được xếp loại thành một đối tượng mới riêng biệt. Trong thời gian gần đây, với sự thay đổi về biện pháp lừa đảo, các chiến dịch tấn công của nhóm APT này đã vươn tầm quốc tế, gây ảnh hưởng tới các quốc gia như Hàn Quốc và Việt Nam.

Được biết, lỗ hổng CVE-2023-38831 đã được khai thác bởi nhiều nhóm APT khác như APT28, APT29, APT40, Dark Pink, Ghostwriter, Konni, và Sandworm. Trong đó, chuỗi tấn công của Ghostwriter được coi là đã mở đường cho PicassoLoader, một mã độc trung gian đóng vai trò làm bộ tải cho các payload độc hại khác.

Nhận định từ chuyên gia bảo mật cho rằng việc lỗ hổng CVE-2023-38831 trên WinRAR bị khai thác đã đem lại những mối lo ngại bất định về tình hình tấn công APT vào nửa cuối năm 2023. Bổ sung thêm, chuyên gia cho biết rằng lỗ hổng an toàn thông tin này cũng đã được khai thác bởi nhiều nhóm khác nhau để thực hiện các chiến dịch tấn công nhằm vào chính phủ với mục tiêu vượt qua hệ thống bảo mật, đạt được mục tiêu đặt ra của đối tượng.

Nguồn: https://thehackernews.com/2023/11/experts-uncover-darkcasino-new-emerging.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng an toàn thông tin trên phần mềm email Zimbra đang bị khai thác bởi 4 nhóm tấn công khác nhau"

Lỗ hổng an toàn thông tin trên phần mềm email Zimbra Collaboration đang bị khai thác bởi 4 nhóm tấn công khác nhau nhằm đánh cắp dữ liệu email, thông tin đăng nhập của người dùng và các token xác thực. Phần lớn các chiến dịch này đều diễn ra sau khi bản vá ban đầu được công bố trên GitHub.

Lỗ hổng an toàn thông tin với mã CVE-2023-37580 (Điểm CVSS: 6.1) là một lỗ hổng XSS gây ảnh hưởng tới các phiên bản cũ hơn 8.8.15 Patch 41. Bản vá cho lỗ hổng này đã được Zimbra phát hành vào ngày 25/07/2023.

Việc khai thác thành công lỗ hổng cho phép đối tượng tấn công thực thi các đoạn script độc hại trên trình duyệt người dùng, thông qua việc lừa người dùng bấm vào một đường dẫn URL được thiết kế để thực thi một yêu cầu XSS tới Zimbra, kết quả của việc khai thác này được phản hồi về cho người dùng. Theo phát hiện từ các chuyên gia các chiến dịch này đã diễn ra kể từ ngày 29/06/2023, 2 tuần trước khi Zimbra đưa ra cảnh báo cho người dùng.

Ba trong số bốn chiến dịch được phát hiện đã được thực hiện từ trước khi có bản vá, chiến dịch còn lại diễn ra sau khi bản vá được phát hành.

Chiến dịch đầu tiên được ghi nhận có mục tiêu là các tổ chức chính phủ tại Hy Lạp, gửi đi các email có chứa URL khai thác tới người dùng, sau khi nhấn vào đường dẫn sẽ triển khai mã độc đánh cắp email đã từng được sử dụng trong chiến dịch EmailThief hồi tháng 02/2022.

Bộ xâm nhập với mã định danh TEMP_HERETIC này cũng có khả năng khai thác lỗ hổng zero-day trên Zimbra để triển khai tấn công.

Đối tượng tấn công thứ hai khai thác CVE-2023-37580 là Winter Vivern, nhằm vào các tổ chức chính phủ tại Moldova và Tunisia sau khi bản vá cho lỗ hổng này được phát hành trên GitHub.

Đáng chú ý rằng, nhóm đối tượng này cũng có liên quan tới việc khai thác các lỗ hổng an toàn thông tin trên Roundcube vào đầu năm nay.

Đối tượng thứ ba đã khai thác lỗ hổng này vào ngày 25/06 để lừa đảo chiếm đoạt thông tin đăng nhập của tổ chức chính phủ tại Việt Nam. Đối với trường hợp này, URL khai thác chỉ tới một đoạn script hiển thị ra website lừa đảo để lấy thông tin xác thực webmail của người dùng và đăng tải thông tin này lên một URL lưu trữ trên domain của chính phủ mà kẻ tấn công đã xâm nhập từ trước đó.

Cuối cùng, một tổ chức chính phủ tới Pakistan đã bị ảnh hưởng bởi lỗ hổng an toàn thông tin này vào ngày 25/08, dẫn tới việc đánh cắp token xác thực trên Zimbra và truyền về domain độc hại dựng lên bởi đối tượng.

Một khuôn mẫu trong cả bốn chiến dịch này là đối tượng tấn công thường xuyên khai thác các lỗ hổng XSS trên máy chủ mail, qua đó cho thấy các ứng dụng này cần phải được kiểm tra kỹ lưỡng, đặc biệt là cho thấy tầm quan trọng của việc cập nhật bản vá mới nhất cho các máy chủ mail sớm nhất có thể. Ngoài ra, cũng có thể nhận thấy rằng các đối tượng tấn công thường xuyên theo dõi các trang lưu trữ mã nguồn mở để tìm cơ hội khác thác lỗ hổng đã có bản vá được công bố trên các trang này nhưng lại chưa được phát hành cho người dùng thông thường.

Nguồn: https://thehackernews.com/2023/11/zero-day-alert-lace-tempest-exploits.html

NCSC VN
National Cyber Security Center

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 **794** lỗ hổng, trong đó có 116 lỗ hổng mức Cao, 92 lỗ hổng mức Trung bình, 03 lỗ hổng mức Thấp và 583 lỗ hổng chưa đánh giá. Trong đó có ít nhất 150 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 03 lỗ hổng trong Linux, Nhóm 33 lỗ hổng trong Microsoft, Nhóm 70 lỗ hổng trong Adobe, Nhóm 154 lỗ hổng trong Wordpress, Nhóm 10 lỗ hổng trong Zoom, Nhóm 17 lỗ hổng trong Fortinet, 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:

- Linux: CVE-2023-6111, CVE-2023-6121,...

- Microsoft: CVE-2023-36014, CVE-2023-36024,...

- Adobe: CVE-2023-22268, CVE-2023-36024,...

- Wordpress: CVE-2023-46207, CVE-2023-35041,...

- Zoom: CVE-2023-39199, CVE-2023-39203,...

- Fortinet: Cve-2023-45582, CVE-2023-42783,...

- IBM: CVE-2023-45167, CVE-2023-38364,...

Thông tin điểm yếu, lỗ hổng

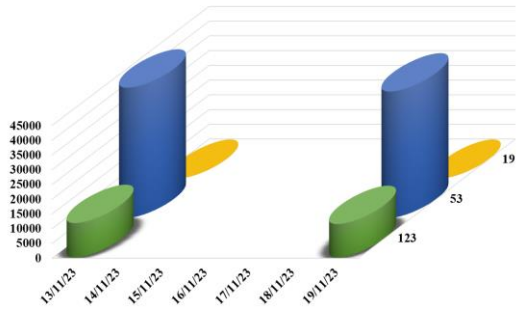
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-6111 CVE-2023-6121 CVE-2023-6176	Nhóm 03 lỗ hổng trong Linux cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-36014 CVE-2023-36024 CVE-2023-36027 …	Nhóm 33 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, khai thác lỗi XSS.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-22268 CVE-2023-22272 CVE-2023-22273 …	Nhóm 70 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, thực hiện SQL Injection, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-46207 CVE-2023-35041 CVE-2023-26514 …	Nhóm 154 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi XSS, khai thác lỗi CSRF, khai thác lỗi CSRF, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Apache	CVE-2023-39199 CVE-2023-39203 CVE-2023-43590 …	Nhóm 10 lỗ hổng trong Zoom cho phép đối tượng tấn công leo thang đặc quyền, 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
6	Samsung	CVE-2023-45582 CVE-2023-42783 CVE-2023-45585 …	Nhóm 17 lỗ hổng trong Fortinet cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-45167 CVE-2023-38364 CVE-2023-38363 …	Nhóm 06 lỗ hổng trong IBM 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

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

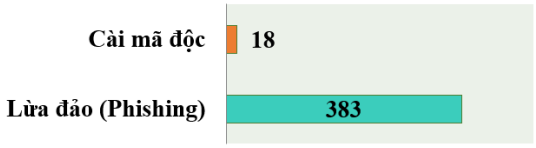
Tấn công DRDoS

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 **54.229**, (tăng so với tuần trước **51.390**) 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

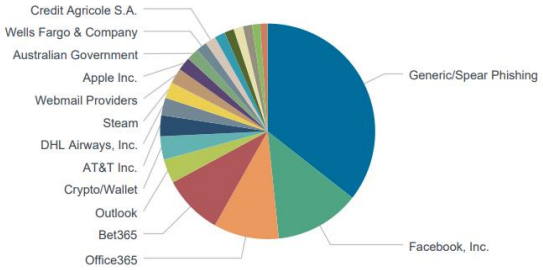


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **401** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 383 trường hợp tấn công lừa đảo (Phishing), 18 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: 13009 IP	hzmksreiuojy.ru: 201 IP
disorderstatus.ru: 4104 IP	xjpakmdcfuqe.biz: 194 IP
atomictrivia.ru: 1909 IP	xjpakmdcfuqe.com: 78 IP
amnsreiuojy.ru: 751 IP	xjpakmdcfuqe.ru: 38 IP
restlesz.su: 324 IP	xjpakmdcfuqe.in: 34 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **406** 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	vn11268shp.com	Website giả mạo sàn TMĐT Shopee
2	ama-zmart.top	Website giả mạo sàn TMĐT Amazon
3	vieclamlazada.vn	Website giả mạo sàn TMĐT Lazada
4	ebaayshopping.site	Website giả mạo Ebay
5	aeeonmart.com	Website giả mạo Công ty TNHH Aeon Việt Nam
6	dich-vu-the-ai-vpbank.com vpbank.com.vn dich-vu-the-ez-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
7	shinhanbank.tanghanmucthang11.com.vn	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam

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