NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 49 (04/12/2023 – 10/12/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Kimsuky triển khai backdoor tấn công các viện nghiên cứu tại Hàn Quốc.

- **Cảnh báo:** Lỗ hổng an toàn thông tin CVE-2023-45866 cho phép đối tượng tấn công chiếm quyền kiểm soát thiết bị Android, Linux, macOS và iOS.

2. Điểm yếu, lỗ hổng

- **745** 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: 294** 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 Kimsuky triển khai backdoor tấn công các viện nghiên cứu tại Hàn Quốc"

Nhóm APT đến từ Triều Tiên có tên là Kimsuky, hay còn gọi là APT43, ARCHIPELAGO, Black Banshee và Emerald Sleet vừa tiến hành một cuộc tấn công spear-phishing nhằm vào các viện nghiên cứu tại Hàn Quốc. Mục tiêu cuối cùng của cuộc tấn công này là triển khai backdoor lên các hệ thống bị xâm nhập.

Quá trình tấn công bắt đầu bằng việc sử dụng các tệp JSE độc hại, chứa script PowerShell, payload được mã hóa Base64 và một tệp PDF giả mạo để làm mồi nhử. Tiếp theo, nhóm này tập trung vào việc sử dụng file PDF để đánh lạc hướng người dùng trong khi script PowerShell được thực thi ẩn danh để triển khai backdoor.

Mã độc sử dụng trong chiến dịch này được định cấu hình để thu thập thông tin của hệ thống mạng và dữ liệu liên quan như tên host, tên người dùng và phiên bản hệ điều hành. Những thông tin này sau đó được chuyển đến một máy chủ từ xa. Mã độc còn có khả năng thực thi lệnh, triển khai các đặc điểm bổ sung và tự ngắt kết nối, biến nó thành backdoor cho việc truy cập từ xa vào hệ thống bị ảnh hưởng.

Nhóm APT Kimsuky bắt đầu hoạt động từ năm 2012, ban đầu tập trung vào chính phủ Hàn Quốc và sau đó mở rộng hoạt động sang Châu u, Nga và Mỹ.

Trong tháng 10/2023, Kimsuky đã bị Mỹ xử phạt vì tội thu thập thông tin hỗ trợ cho mục tiêu chiến lược của Triều Tiên, cụ thể là về vấn đề chính trị toàn cầu, chính sách đối ngoại và các nỗ lực ngoại giao của nước này.

Hơn nữa, nhóm APT Kimsuky còn sử dụng các URL độc hại để tải xuống file .ZIP giả mạo là bản cập nhật cho trình duyệt Chrome, triển khai VBScript độc hại từ Google Drive, sử dụng dịch vụ lưu trữ này như một kênh để trích xuất thông tin và làm máy chủ C&C.

Nguồn: https://thehackernews.com/2023/12/n-korean-kimsuky-targeting-south-korean.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng an toàn thông tin CVE-2023-45866 cho phép đối tượng tấn công chiếm quyền kiểm soát thiết bị Android, Linux, macOS và iOS"

Lỗ hổng bảo mật nghiêm trọng với mã định danh CVE-2023-45866 vừa bị khai thác bởi các đối tượng tấn công nhằm chiếm quyền kiểm soát đối với các thiết bị sử dụng hệ điều hành Android, Linux, macOS, và iOS.

Lỗ hổng CVE-2023-45866 là một lỗ hổng bỏ qua xác thực, cho phép đối tượng tấn công kết nối với thiết bị và chèn các nội dung gõ từ bàn phím để thực thi mã từ xa. Cụ thể, để khai thác lỗ hổng, đối tượng tấn công đánh lừa thiết bị người dùng tin rằng nó đang kết nối tới một bàn phím Bluetooth bằng việc lợi dụng cơ chế kết nối không xác thực của Bluetooth. Việc khai thác thành công lỗ hổng này cho phép đối tượng tấn công ở gần người dùng kết nối với thiết bị của họ và lan truyền các nội dung gõ phím để cài đặt ứng dụng và thực thi mã từ xa.

Đáng chú ý, việc khai thác lỗ hổng này không cần sử dụng phần cứng chuyên dụng và có thể thực hiện từ một máy tính sử dụng Linux với bộ chuyển đổi Bluetooth. Thông tin chi tiết về lỗ hổng này sẽ được công bố trong thời gian sớm nhất.

Lỗ hổng CVE-2023-45866 ảnh hưởng đến một loạt thiết bị sử dụng các hệ điều hành như Android (phiên bản từ 4.2.2 trở về trước), iOS, Linux và macOS. Đặc biệt, trên các thiết bị macOS và iOS, đặc điểm này gây ảnh hưởng lớn đối với các thiết bị sử dụng Bluetooth và bàn phím Magic Keyboard. Lỗ hổng này có thể vượt qua chế độ LockDown của Apple, mô phỏng khả năng bảo vệ người dùng trước những mối đe dọa kỹ thuật số phức tạp.

Trong tháng 11/2023, Google cũng đã đề cập về lỗ hổng bảo mật này trong báo cáo và nhấn mạnh lỗ hổng này có thể dẫn tới leo thang đặc quyền từ xa (ở khoảng cách lân cận) mà không cần tới quyền thực thi.

Nguồn: https://thehackernews.com/2023/12/new-bluetooth-flaw-let-hackers-take.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 **745** lỗ hổng, trong đó có 230 lỗ hổng mức Cao, 187 lỗ hổng mức Trung bình, 04 lỗ hổng mức Thấp và 324 lỗ hổng chưa đánh giá. Trong đó có ít nhất 60 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 195 lỗ hổng trong Google, Nhóm 14 lỗ hổng trong Microsoft, Nhóm 05 lỗ hổng trong Linux, Nhóm 33 lỗ hổng trong Wordpress, Nhóm 17 lỗ hổng trong Dell, Nhóm 10 lỗ hổng trong GitLab, Nhóm 23 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:

- Google: CVE-2023-21162, CVE-2023-21163,...

- Microsoft: CVE-2023-48315,...

- Linux: CVE-2023-6560, CVE-2023-6606,...

- Wordpress: CVE-2023-5952, CVE-2023-5762,...

- Dell: CVE-2023-44305, CVE-2023-44304,...

- GitLab: CVE-2023-5332, CVE-2023-5226,...

- IBM: CVE-2023-45168, CVE-2023-29258,...

Thông tin điểm yếu, lỗ hổng

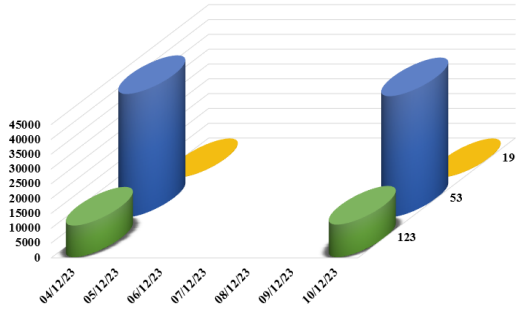
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-21162 CVE-2023-21163 CVE-2023-21164 …	Nhóm 195 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
2	Apple	CVE-2023-48315 CVE-2023-48316 CVE-2023-48691 …	Nhóm 14 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Foxit Software	CVE-2023-6560 CVE-2023-6606 CVE-2023-6610 …	Nhóm 05 lỗ hổng trong Linux 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
4	Wordpress	CVE-2023-5952 CVE-2023-5762 CVE-2023-5953 …	Nhóm 33 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã từ xa, thực hiện SQL Injection, khai thác lỗi XSS, khai thác lỗi SSRF.	Chưa có thông tin xác nhận và bản vá
5	Apache	CVE-2023-44305 CVE-2023-44304 CVE-2023-44302 …	Nhóm 17 lỗ hổng trong Dell cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, 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	GitLab	CVE-2023-5332 CVE-2023-5226 CVE-2023-5995 …	Nhóm 10 lỗ hổng trong GitLab 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
7	IBM	CVE-2023-45168 CVE-2023-29258 CVE-2023-38727 …	Nhóm 23 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, khai thác lỗi XSS, 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

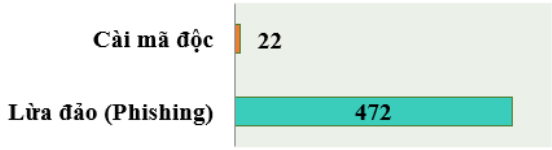
Tấn công DRDoS

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 **51.921**, (giảm so với tuần trước **52.324)** 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

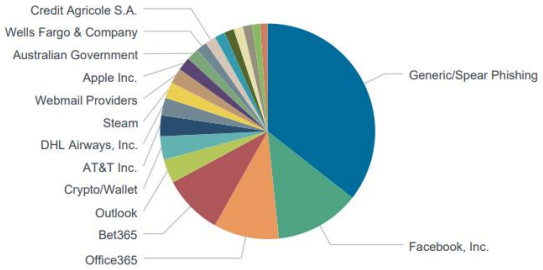


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **494** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 472 trường hợp tấn công lừa đảo (Phishing), 22 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: 13301 IP	hzmksreiuojy.ru: 249 IP
disorderstatus.ru: 4639 IP	xjpakmdcfuqe.biz: 231 IP
atomictrivia.ru: 2289 IP	xjpakmdcfuqe.com: 105 IP
amnsreiuojy.ru: 860 IP	xjpakmdcfuqe.ru: 88 IP
restlesz.su: 318 IP	xjpakmdcfuqe.in: 66 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **294** 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	vxvw22.com vxvw11.com takk6.com	Website giả mạo sàn TMĐT Tiki
2	kiemduyetvien.cc	Website giả mạo sàn TMĐT Lazada
3	vn22647shp.com	Website giả mạo sàn TMĐT Shopee
4	dich-vu-the-vdiamond-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