NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 06 (13/02/2023 – 19/02/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Apple cảnh báo về 3 lỗ hổng mới ảnh hưởng đến các thiết bị iPhone, iPad và Mac.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Earth Kitsune triển khai backdoor WhiskerSpy trong các cuộc tấn công mới.

2. Điểm yếu, lỗ hổng

- **717** 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: 1336** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Nhóm tấn công APT Earth Kitsune triển khai backdoor WhiskerSpy trong các cuộc tấn công mới"

Nhóm tấn công có tên là Earth Kitsune đã được phát hiện đang triển khai backdoor WhiskerSpy trong các cuộc tấn công Social engineering. Kể từ năm 2019, Earth Kitsune đã phát tán các mã độc nhằm vào nhiều website ở Triều Tiên và khai thác các lỗ hổng bảo mật trong Google Chrome, Internet Explorer để kích hoạt các chuỗi lây nhiễm.

Gần đây, các chuyên gia đã công bố rằng Earth Kitsune đang chuyển hướng sang các cuộc tấn công Social engineering để đánh lừa người dùng truy cập vào các trang web độc hại. Nhóm nhằm mục tiêu vào các tổ chức khác nhau trên khắp Triều Tiên, Brazil, Trung Quốc, Nhật Bản, ….

Cuối năm 2022, Earth Kitsune đã tấn công vào một trang web của Triều Tiên thông qua backdoor WhiskerSpy. Khi người dùng vào xem video trên trang web sẽ hiển thị thông báo lỗi giả mạo để lừa người dùng tải xuống mã độc được ngụy trang dưới dạng Advanced Video Codec - AVC1. Các trang web đã được cấu hình để phát tán các mã độc cho người dùng truy cập thông qua các địa chỉ IP được đặt tại Thẩm Dương (Trung Quốc), Nagoya (Nhật Bản), Brazil, điều này làm cho cuộc tấn khó bị phát hiện.

Earth Kitsune đã lợi dụng lỗ hổng chiếm quyền điều khiển Dynamic Library Link (DLL) trong OneDrive và tiện ích mở rộng của Google Chrome để cài cắm mã độc mỗi khi trình duyệt web được khởi chạy. Backdoor WhiskerSpy cho phép đối tượng tấn công xóa, liệt kê, tải xuống tệp lệnh, chụp ảnh màn hình, chèn mã sell và thực thi mã tùy ý.

Để phòng tránh các cuộc tấn công như vậy, các cơ quan, tổ chức cần tăng cường kiểm tra, rà soát và sẵn sàng các phương án xử lý kịp thời khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Nguồn: https://thehackernews.com/2023/02/north-korean-cyber-espionage-group.html

Tin tức An toàn thông tin

"Cảnh báo: Apple cảnh báo về 3 lỗ hổng mới ảnh hưởng đến các thiết bị iPhone, iPad và Mac"

Vừa qua, Apple đã đưa ra cảnh báo về 3 lỗ hổng bảo mật mới ảnh hưởng đến iOS, iPadOS và macOS. Lỗ hổng đầu tiên là CVE-2023-23520 cho phép đối tướng tấn công đọc các tệp tùy ý với đặc quyền root. Hai lỗ hổng khác được các nhà nghiên cứu ghi nhận là CVE-2023-23530 và CVE-2023-23531 cho phép đối tượng tấn công vượt qua cơ chế bảo mật của sandbox để thực thi mã tùy ý và thực hiện nâng cao đặc quyền.

Đối tượng tấn công có thể lợi dụng những lỗ hổng này để có khả năng truy cập trái phép vào tin nhắn, lịch, định vị, lịch sử cuộc gọi, micro, máy ảnh và ảnh của các thiết bị. Điều đáng lo ngại hơn là các lỗ hổng này có thể cho phép đối tượng tấn công cài đặt ứng dụng tùy ý hoặc thấm chí xóa sạch thiết bị.

Hiện tại, Apple đã phát hành bản cập nhật mới nhất cho các thiết bị và khuyến nghị người dùng cập nhật phần mềm để bảo vệ các thiết bị của mình.

Nguồn: https://thehackernews.com/2023/02/apple-warns-of-3-new-vulnerabilities.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 717 lỗ hổng, trong đó có 110 lỗ hổng mức Cao, 61 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 546 lỗ hổng chưa đánh giá. Trong đó có ít nhất 124 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 02 lỗ hổng trong Google, Nhóm 09 lỗ hổng trong Dlink, Nhóm 03 lỗ hổng trong Apache, Nhóm 36 lỗ hổng trong Wordpress, Nhóm 11 lỗ hổng trong Dell, Nhóm 78 lỗ hổng trong Microsofr, Nhóm 13 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-2023-20927, CVE-2023-20949,...*
- *Dlink: CVE-2023-24348, CVE-2023-24349,....*
- *Apache: CVE-2023-25141, CVE-2023-22832,...*
- *Wordpress: CVE-2022-43469, CVE-2022-4471,...*
- *Dell: CVE-2023-23698, CVE-2022-34454,...*
- *Microsoft: CVE-2023-21689, CVE-2023-21690,...*
- *IBM: CVE-2022-40232, CVE-2022-40231,...*

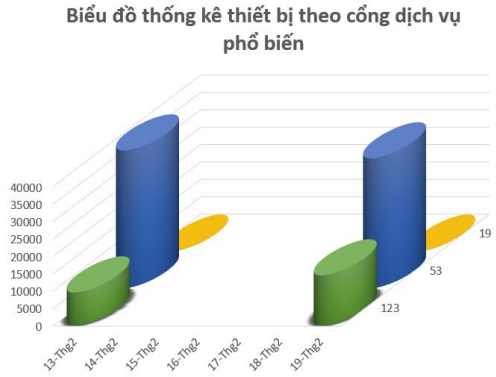
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-20927 CVE-2023-20949	Nhóm 02 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Dlink	CVE-2023-24348 CVE-2023-24349 CVE-2023-24350 …	Nhóm 09 lỗ hổng trong Dlink (DIR-605L, …) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Apache	CVE-2022-42735 CVE-2023-22832 CVE-2023-25141	Nhóm 03 lỗ hổng trong Apache (ShenYu, NiFi,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-43469 CVE-2022-4471 CVE-2022-4473 …	Nhóm 36 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2023-23698 CVE-2022-34454 CVE-2022-33934 …	Nhóm 11 lỗ hổng trong Dell (PowerScale OneFS, SupportAssist,…) cho phép đối tượng tấn công có quyền truy cập thông tin cá nhân trái phép, thực thi mã tùy ý, thực hiện nâng cao đặc quyền.	Chưa có thông tin xác nhận và bản vá
6	Microsoft	CVE-2023-21689 CVE-2023-21690 CVE-2023-21692 …	Nhóm 78 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin trái phép, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-36775 CVE-2022-40231 CVE-2022-40232 ...	Nhóm 13 lỗ hổng trong IBM (Tivoli Workload Scheduler,…) cho phép đối tượng tấn công thực thi mã từ xa, làm rò rỉ thông tin dữ liệu, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

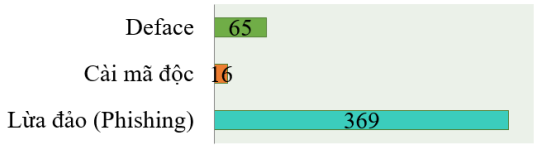
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **45,154** (giảm so với tuần trước **48,527**) 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.

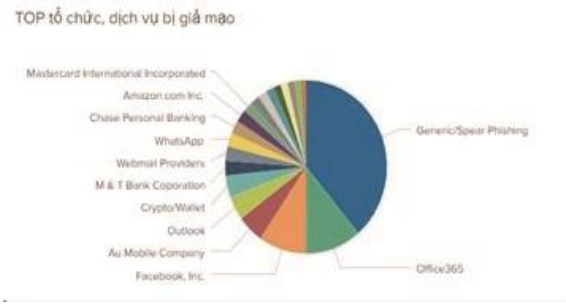


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 450 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 65 trường hợp tấn công thay đổi giao diện (Deface), 369 trường hợp tấn công lừa đảo (Phishing), 16 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: 13150 IP	xjpakmdcfuqe.ru:220 IP
disorderstatus.ru: 5890 IP	xjpakmdcfuqe.in: 238 IP
atomictrivia.ru: 2864 IP	restlesz.su: 270 IP
xjpakmdcfuqe.biz: 376 IP	amnsreiuojy.ru: 881 IP
xjpakmdcfuqe.com: 244 IP	hzmksreiuojy.ru: 44 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 1336 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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	tpbankn.com tpbankc.com	Website giả mạo Ngân hàng TMCP Tiên Phong
2	m.nbm65.com	Website giả mạo, lừa đảo

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