NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 14 (03/04/2023 – 09/04/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Lỗ hổng bảo mật "By-Design" trong Microsoft Azure cho phép đối tượng tấn công thu thập thông tin tài khoản.

- **Chiến dịch tấn công APT:** Google cảnh báo về nhóm tấn công APT ARCHIPELAGO có liên quan đến Bắc Triều Tiên.

2. Điểm yếu, lỗ hổng

- **651** 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: 275** 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

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Lỗ hổng bảo mật "By-Design" trong Microsoft Azure cho phép đối tượng tấn công thu thập thông tin tài khoản"

Lỗ hổng bảo mật "By - Design" trong Microsoft Azure cho phép đối tượng tấn công truy cập vào các dữ liệu nội bộ sau khi chiếm quyền điều khiển tài khoản lưu trữ và thực thi mã từ xa. Đối tượng tấn công đã tận dụng công cụ Azure để đánh cắp mã thông báo truy cập nhằm thực hiện các hành động trái phép vào hệ thống.

Thông qua phương thức ủy quyền Shared Key được biết đến với cơ chế khai thác đường dẫn để làm nền tảng cho các cuộc tấn công và được mặc định trong tài khoản lưu trữ. Azure tạo ra hai khóa truy cập tài khoản lưu trữ 512 bit khi khởi tạo tài khoản này. Các khóa được dùng để cấp quyền truy cập vào cấu hình và dữ liệu của tài khoản lưu trữ thông qua phương thức ủy quyền Shared Key hoặc mã thông báo SAS (Shared Access Signatures).

Nguồn: https://thehackernews.com/2023/04/newly-discovered-by-design-flaw-in.html

Theo các nghiên cứu, những mã thông báo truy cập bị đánh cắp có khả năng cho phép đối tượng tấn công có được quyền truy cập vào tài khoản với vai trò là người dùng cục bộ nhằm thực hiện leo thang đặc quyền, truy cập vào tài nguyên nội bộ và thực thi reverse shell (đảo ngược shell) trên máy ảo hóa.

Để giảm thiểu rủi ro bị đánh cắp dữ liệu bảo mật, các cá nhân, tổ chức nên xem xét sử dụng xác thực danh tính và thư mục (Azure Active Directory) thay vì Azure Shared Key. Ngoài ra cần thực hiện kiểm tra, rà soát và chuẩn bị sẵn các phương án xử lý để phòng ngừa các cuộc tấn công mạng.

Tin tức An toàn thông tin

"Cảnh báo: Google cảnh báo về nhóm tấn công APT ARCHIPELAGO có liên quan đến Bắc Triều Tiên"

Vừa qua, các chuyên gia đã cảnh báo về nhóm APT ARCHIPELAGO được chính phủ Bắc Triều Tiên hậu thuẫn có liên quan đến các cuộc tấn công mạng nhằm mục tiêu vào cá nhân và tổ chức chính phủ, quân đội ở Hàn Quốc và Hoa Kỳ.

ARCHIPELAGO hay còn được biết đến với tên gọi APT43 lần đầu được các chuyên gia phát hiện vào năm 2012. ARCHIPELAGO đã thực hiện các chiến thuật tấn công từ lừa đảo thông tin xác thực cơ bản sang các kỹ thuật nâng cao. Ví dụ như mở rộng tùy chỉnh của Chrome và sử dụng Google Drive để ra lệnh và kiểm soát C&C.

Các cuộc tấn công mạng do ARCHIPELAGO sử dụng các email lừa đảo có đính kèm các liên kết độc hại, nhằm chuyển hướng người dùng đến các trang đăng nhập giả mạo để thu thập thông tin đăng nhập trái phép.

ARCHIPELAGO sử dụng kỹ thuật tấn công BitB (Browser In The Browser) để hiển thị các trang đăng nhập giả mạo. Các tin nhắn lừa đảo giả mạo cảnh báo bảo mật tài khoản Google nhằm kích hoạt quá trình lây nhiễm, với các mã độc lưu trữ tập thể như BabyShark trên Google Drive ở dạng tệp trống hoặc hình ảnh đĩa quang ISO.

Ngoài ra, một kỹ thuật được ARCHIPELAGO sử dụng là các tiện ích mở rộng giả mạo của Google Chrome để thu thập thông tin dữ liệu như trong các chiến dịch trước đó.

Để giảm thiểu nguy cơ bị tấn công mạng các cơ quan, tổ chức nên kiểm tra trước khi truy cập vào bất kỳ đường link nào, thường xuyên sử dụng công cụ quét virus để sớm phát hiện và loại bỏ các phần mềm độc hại trên thiết bị của mình.

Nguồn: https://thehackernews.com/2023/04/google-tag-warns-of-north-korean-linked.html?&web_view=true

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 651 lỗ hổng, trong đó có 73 lỗ hổng mức Cao, 54 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 523 lỗ hổng chưa đánh giá. Trong đó có ít nhất 123 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 14 lỗ hổng trong Google, Nhóm 05 lỗ hổng trong Linux, Nhóm 08 lỗ hổng trong Apache, Nhóm 104 lỗ hổng trong Wordpress, Nhóm 08 lỗ hổng trong IBM, 01 lỗ hổng trong Samsung, 01 lỗ hổng trong Ubuntu. 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-2023-1810, CVE-2023-1811,…*
- *Linux: CVE-2023-1855, CVE-2023-1838,…*
- *Apache: CVE-2023-26269, CVE-2023-28706,...*
- *Wordpress: CVE-2023-23996, CVE-2023-23998,...*
- *IBM: CVE-2023-27284, CVE-2023-26283,...*
- *Samsung: CVE-2023-28613.*
- *Ubuntu: CVE-2020-11935.*

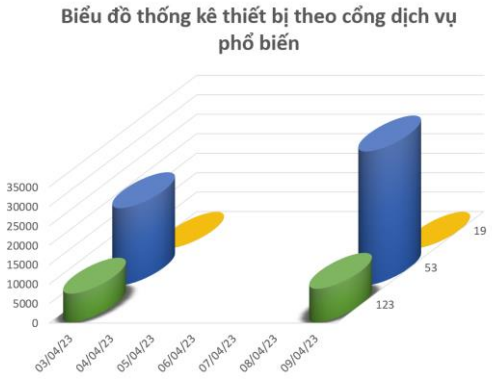
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-1810 CVE-2023-1811 CVE-2023-1812 …	Nhóm 14 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện truy cập bộ nhớ ngoài, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1855 CVE-2023-1838 CVE-2023-1582 …	Nhóm 05 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện tấn công thực hiện tấn công thu thập thông tin, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2023-26269 CVE-2023-28706 CVE-2023-28710 …	Nhóm 04 lỗ hổng trong Apache 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
4	Wordpress	CVE-2023-23996 CVE-2023-23998 CVE-2023-24002 …	Nhóm 104 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	IBM	CVE-2023-27284 CVE-2023-27286 CVE-2023-26283 …	Nhóm 08 lỗ hổng trong IBM cho phép đối tượng tấn công thực thi mã tùy ý, làm tràn bộ đệm, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2023-28613	01 lỗ hổng trong Samsung 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	Ubuntu	CVE-2020-11935	01 lỗ hổng trong Ubuntu phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá

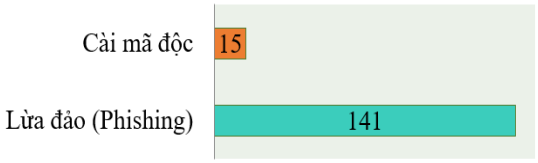
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **47,608** (tăng so với tuần trước **48,402**) 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.

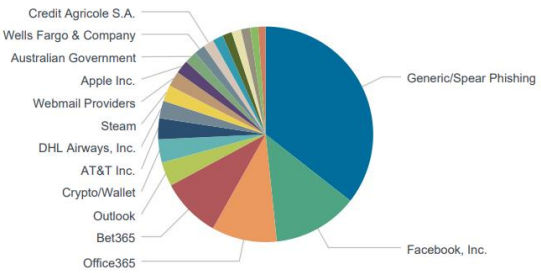


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 156 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 141 trường hợp tấn công lừa đảo (Phishing), 15 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: 10368 IP	xjpakmdcfuqe.ru:214 IP
disorderstatus.ru: 5196 IP	xjpakmdcfuqe.in:269 IP
atomictrivia.ru: 2480 IP	restlesz.su: 257 IP
xjpakmdcfuqe.biz: 339 IP	amnsreiuojy.ru: 531 IP
xjpakmdcfuqe.com: 260 IP	hzmksreiuojy.ru: 42 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 275 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	vie-tcapital.com	Website giả mạo Ngân hàng TMCP Bản Việt
2	lashopp061.com	Website giả mạo sàn TMĐT Shopee
3	vinfast888.net phattai6666.com rik11.fun alibabavn.shop congtykiman.org vincomonevip.net trungtamthuongmaihanoi.com minhchinhmega.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