NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 15 (10/04/2023 – 16/04/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Google phát hành bản cập nhật để khắc phục lỗ hổng Zero-Day trong trình duyệt Chrome.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT RTM Locker sử dụng ransomware nhằm mục tiêu vào các doanh nghiệp.

2. Điểm yếu, lỗ hổng

- **792** 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: 324** 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

"Nhóm tấn công APT RTM Locker sử dụng ransomware nhằm mục tiêu vào các doanh nghiệp"

Gần đây, các nhà nghiên cứu bảo mật đã phát hiện nhóm tấn công APT Read The Manual (RTM) đã sử dụng ransomware để cho phép đối tượng tấn công cài cắm RaaS (ransomware as a service) nhằm thực hiện các cuộc tấn công thu lợi nhuận bất hợp pháp. Ransomware-as-a-Service (RaaS) là thuật ngữ đề cập đến việc một số nhóm tấn công mạng cho các nhóm đối tượng khác nhau thuê ransomware. Bởi vậy, nhóm RTM đã thiết lập ra các chi nhánh thuê ransomeware của mình để tống tiền người dùng.

Nhóm APT Read The Manual bắt đầu hoạt động kể từ năm 2015 và được phát hiện lần đầu vào tháng 2/2017. Nhóm này sử dụng phần mềm độc hại có liên quan đến các ngân hàng, từ đó nhằm mục tiêu tấn công vào các doanh nghiệp ở Nga thông qua việc cài cắm mã độc vào thư rác, email lừa đảo. Ngoài ra, các đối tượng tấn công này còn có thể thực hiện tấn công Drive-by Download, đây là một kỹ thuật tấn công phổ biến cho phép cài đặt phần mềm độc hại vào máy tính của người dùng một cách âm thầm.

Vào tháng 3/2021, nhóm này đã thực hiện một chiến dịch tấn công tống tiền thông qua ba mối đe dọa gồm: RAT (Remote Access Trojan), mã độc trojan và một ransomware được gọi là Quoter. Tuy nhiên, các nghiên cứu mới nhất cho thấy rằng trong các cuộc tấn công gần đây của RTM Locker không liên quan đến ransomware Quoter.

Mục tiêu của nhóm RTM là hoạt động ngầm và tránh thực hiện các hoạt động gây sự chú ý. Nhóm RTM sẽ tự động khóa các chi nhánh thuê ransomware nếu các chi nhánh này không hoạt động trong 10 ngày. Điều này nhằm thúc đẩy các chi nhánh tích cực hoạt động, đồng thời để tránh các nguy cơ bị phát hiện.

RTM sử dụng các kỹ thuật tấn công tương tự các nhóm RaaS khác, buộc người dùng phải trả tiền để lấy lại những dữ liệu bị đánh cắp. Điều này cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, ngăn chặn các phần mềm chống vi-rút và sao lưu, xóa các bản sao ẩn trước khi bắt đầu quy trình mã hóa. Ngoài ra, mã độc cũng được thiết kế để dọn sạch Recycle Bin nhằm ngăn việc khôi phục, thay đổi hình nền, xóa nhật ký và thực thi lệnh tự xóa ở bước cuối.

Để giảm thiểu nguy cơ bị tấn công mạng các cá nhân, doanh nghiệp 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/rtm-locker-emerging-cybercrime-group.html?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Google phát hành bản cập nhật để khắc phục lỗ hổng Zero-Day trong trình duyệt Chrome"

Ngày 14/04/2023, Google đã phát hành bản cập nhật nhằm khắc phục lỗ hổng zero-day đang bị khai thác trong thực tế trên trình duyệt Chrome. Đây cũng là lỗ hổng đầu tiên trên Chrome được Google xử lý kể từ đầu năm.

Lỗ hổng CVE-2023-2033 ảnh hưởng ở mức Cao, liên quan đến lỗi Type confusion trong trong V8 ở Google Chrome phiên bản trước 112.0.5615.121. Lỗ hổng này cho phép đối tượng tấn công khai thác để gây hỏng bộ nhớ heap (heap corruption) thông qua HTML được tạo sẵn. Ngoài ra, việc khai thác thành công lỗi Type confusion cũng cho phép đối tượng tấn công có thể gây lỗi trình duyệt bằng cách đọc hoặc ghi bộ nhớ ngoài giới hạn bộ đệm, thực thi mã tùy ý trên các thiết bị bị xâm nhập.

CVE-2023-2033 có điểm tương đồng với với CVE-2022-1096, CVE-2022-1364, CVE-2022-3723 và CVE-2022-4262. Đây là bốn lỗ hổng Type confusion trong V8 đã được Google khắc phục trong năm 2022. Tính đến năm 2022, Google đã phát hiện ra tổng cộng 9 lỗ hổng zero-day trong Chrome.

Để tránh nguy cơ bị tấn công mạng và giảm thiểu các mối nguy hại tiềm ẩn, người dùng Chrome nên nâng cấp phiên bản 112.0.5615.121 cho Windows, macOS và Linux Ngoài ra, người dùng các trình duyệt dựa trên Chromium như Microsoft Edge, Brave, Opera và Vivaldi nên áp dụng các bản sửa lỗi.

Nguồn: https://thehackernews.com/2023/04/google-releases-urgent-chrome-update-to.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 792 lỗ hổng, trong đó có 212 lỗ hổng mức Cao, 157 lỗ hổng mức Trung bình, 02 lỗ hổng mức Thấp và 421 lỗ hổng chưa đánh giá. Trong đó có ít nhất 102 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 12 lỗ hổng trong Google, Nhóm 06 lỗ hổng trong Linux, Nhóm 09 lỗ hổng trong Apache, Nhóm 15 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong IBM, Nhóm 56 lỗ hổng trong Adobe, Nhóm 99 lỗ hổng trong Microsoft. 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-2022-47335, CVE-2022-47336,...*
- *Linux: CVE-2023-1829, CVE-2023-1872,...*
- *Apache: CVE-2023-27602, CVE-2023-27603,...*
- *Wordpress: CVE-2013-10023, CVE-2013-10024,...*
- *IBM: CVE-2022-34333, CVE-2022-43928,...*
- *Adobe: CVE-2023-21582, CVE-2023-22235,...*
- *Microsoft: CVE-2023-21727, CVE-2023-24884,..*

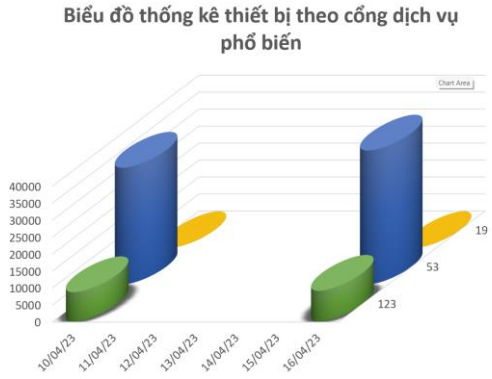
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2022-47335 CVE-2022-47336 CVE-2022-47337 …	Nhóm 12 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện tấn công XSS, khai thác lỗi heap thông qua HTML, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1829 CVE-2023-1872 CVE-2023-1989 …	Nhóm 06 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2023-27602 CVE-2023-27603 CVE-2023-29215 …	Nhóm 09 lỗ hổng trong Apache (Linkis, Airflow Hive Provider,..) 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
4	Wordpress	CVE-2013-10023 CVE-2013-10024 CVE-2013-10025 …	Nhóm 15 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.	Đã có thông tin xác nhận và bản vá
5	IBM	CVE-2022-34333 CVE-2022-43928 CVE-2022-43914 …	Nhóm 05 lỗ hổng trong IBM cho phép đối tượng tấn công thực hiện tấn công XSS, thu thập thông tin dữ liệu trái phép, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Adobe	CVE-2023-21582 CVE-2023-22235 CVE-2023-26388 …	Nhóm 56 lỗ hổng trong Adobe (Digital Editions, InCopy,…) cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	Microsoft	CVE-2023-21727 CVE-2023-24884 CVE-2023-24886 …	Nhóm 99 lỗ hổng trong Microsoft phép đối tượng tấn công thực thi mã từ xa, thực hiện nâng cao đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

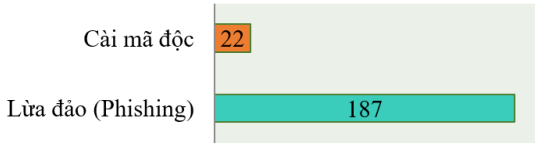
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **48,574** (tăng so với tuần trước **47,608**) 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.

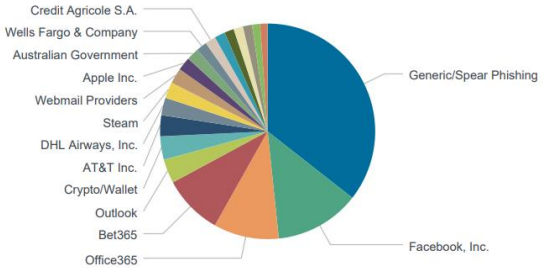


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 209 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 187 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: 14666 IP	xjpakmdcfuqe.ru:352 IP
disorderstatus.ru: 5196 IP	xjpakmdcfuqe.in:376 IP
atomictrivia.ru: 3608 IP	restlesz.su: 357 IP
xjpakmdcfuqe.biz: 466 IP	amnsreiuojy.ru: 799 IP
xjpakmdcfuqe.com: 413 IP	hzmksreiuojy.ru: 74 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 324 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	sieuthidienmayxanh24h.com	Website giả mạo siêu thị Điện máy xanh
2	momopay.fun	Website giả mạo ví điện tử Momo
3	shop63288.com	Website giả mạo sàn TMĐT Shopee

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