NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 08 (20/02/2023 – 26/02/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Mã độc ChromeLoader nhằm mục tiêu đến game thủ thông qua các trò chơi Nintendo và Steam.

- **Chiến dịch tấn công APT:** Hà Lan bắt giữ 3 đối tượng tình nghi đánh cắp số lượng lớn dữ liệu cá nhân.

2. Điểm yếu, lỗ hổng

- **391** 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: 464** 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

"Hà Lan bắt giữ 3 đối tượng tình nghi đánh cắp số lượng lớn dữ liệu cá nhân"

Hà Lan cho biết đã bắt giữ 3 đối tượng tình nghi có liên quan đến chiến dịch tấn công nhằm đánh cắp thông tin dữ liệu người dùng và bán cho các nhóm tấn công để thực hiện tống tiến, rửa tiền. Ngày 23/1/2023, Hà Lan đã bắt giữ 3 đối tượng tình nghi gồm hai thanh niên 21 tuổi đến từ Zandvoot, Rotterdam và một thanh niên khác 18 tuổi không rõ địa chỉ thường trú.

Theo báo cáo điều tra cho thấy, các đối tượng tấn công đã đánh cắp hơn 10 triệu dữ liệu cá nhân của người dùng bao gồm: tên, địa chỉ, ngày sinh, số điện thoại, tài khoản ngân hàng, thẻ tín dụng, mật khẩu, giấy phép đăng ký, thông tin hộ chiếu,....Các cơ quan chức năng đã bắt đầu cuộc điều tra kể từ tháng 3/2021 sau khi một lượng lớn các công ty ở Hà Lan bị tấn công và trở thành nạn nhân của các vụ tống tiền.

Hàng nghìn doanh nghiệp và tổ chức lớn, nhỏ ở cả trong nước và quốc tế đã trở thành mục tiêu của các đối tượng tấn công. Ngoài ra, nhóm tấn công còn nhằm mục tiêu vào các ngành dịch vụ, sản thương mại điện tử, mạng xã hội,....

Nhiều công ty đã trả tiền chuộc dao động từ 100.000 đến 700.000 Euro đối với mỗi cuộc tấn công khác nhau. Tuy nhiên, dữ liệu bị đánh cắp vẫn bị bán ra ngoài hoặc thậm chí bị xóa dù cho các công ty đã trả tiền chuộc. Cơ quan chức năng đã đưa ra cảnh báo về mục tiêu của việc đánh cắp thông tin và mua bán dữ liệu là một khoản lợi nhuận lớn cho các đối tượng tấn công.

Nguồn:https://thehackernews.com/2023/02/dutch-police-arrest-3-hackers-involved.html

Tin tức An toàn thông tin

"Cảnh báo: Mã độc ChromeLoader nhằm mục tiêu đến game thủ thông qua các trò chơi Nintendo và Steam"

Gần đây, các nhà nghiên cứu đã phát hiện ra ChromeLoader đang phân phối mã độc thông qua các tệp VHD thay vì sử dụng các tệp IOS như trước đây. Tệp VHD này được phát hiện thông qua kết quả tìm kiếm của Google đối với các truy vấn đến những trò chơi phổ biến như Nintendo và Steam. ChromeLoader (còn được gọi là Choziosi Loader hoặc ChromeBack) xuất hiện lần đầu vào tháng 1/2022 cho phép đối tượng tấn công đánh cắp thông tin đăng nhập nhằm chiếm quyền điều khiển trình duyệt, thu thập dữ liệu trái phép, triển khai ransomware và phân phối file giải nén độc hại.

Mục tiêu chính của ChromeLoader là xâm nhập vào các trình duyệt web như Google Chrome để sửa đổi cài đặt gốc của trình duyệt và điều hướng người dùng đến các trang web chèn quảng cáo độc hại. ChromeLoader có khả năng xâm nhập vào cả hệ thống Windows và macOS. Việc chuyển sang sử dụng tệp VHD là một dấu hiệu cho thấy chiến dịch tấn công đã trải qua nhiều thay đổi trong vài tháng qua.

Nhiều tựa game đã bị nhằm mục tiêu cho mục đích phát tán mã độc được phát hiện bao gồm Elden Ring, ROBLOX, Dark Souls 3, Red Dead Redemption 2, Need for Speed, Call of Duty, Portal 2, Minecraft, Legend of Zelda, Pokemon, Mario Kart, Animal Crossing,...Các nhà nghiên cứu cho biết khi một tệp VHD được tải xuống người dùng có thể nhầm tệp VHD độc hại này với một chương trình liên quan đến trò chơi.

Để giảm thiểu rủi ro và phòng tránh nguy cơ tấn công mạng người dùng nên tải xuống phần mềm từ các nguồn chính thức.

Nguồn: https://thehackernews.com/2023/02/chromeloader-malware-targeting-gamers.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 391 lỗ hổng, trong đó có 28 lỗ hổng mức Cao, 15 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 348 lỗ hổng chưa đánh giá. Trong đó có ít nhất 53 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 08 lỗ hổng trong Google, Nhóm 02 lỗ hổng trong Tp-link, Nhóm 08 lỗ hổng trong Apache, Nhóm 51 lỗ hổng trong Wordpress, Nhóm 02 lỗ hổng trong Dell, Nhóm 26 lỗ hổng trong Adobe, Nhóm 08 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-2023-0927, CVE-2023-0928,...*
- *Tp-link: CVE-2023-23040, CVE-2023-0936,....*
- *Apache: CVE-2023-25613, CVE-2023-25621,...*
- *Wordpress: CVE-2012-10007, CVE-2023-0942,...*
- *Dell: CVE-2023-23695, CVE-2023-24575,...*
- *Adobe: CVE-2023-21574, CVE-2023-21575,...*
- *IBM: CVE-2022-43927, CVE-2022-43929,...*

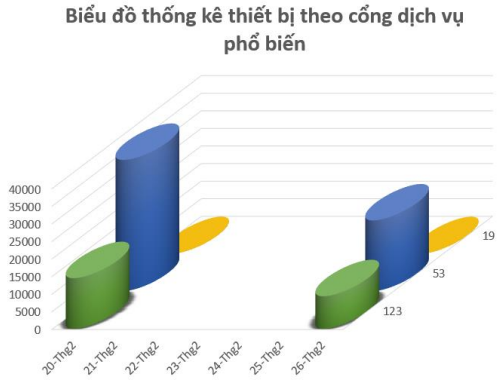
Thông tin điểm yếu, lỗ hổng

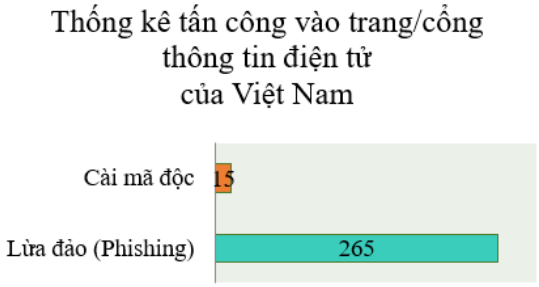
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-0927 CVE-2023-0928 CVE-2023-0929 …	Nhóm 08 lỗ hổng trong Google (Chrome) cho phép đối tượng tấn công khai thác lỗi heap thông qua một trang HTML độc hại.	Chưa có thông tin xác nhận và bản vá
2	Tp-link	CVE-2023-23040 CVE-2023-0936	Nhóm 02 lỗ hổng trong Tp-link 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-2023-25613 CVE-2023-25621 CVE-2023-25691 …	Nhóm 08 lỗ hổng trong Apache (Airflow Google Provider, Kerby,…) 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-2012-10007 CVE-2023-0942 CVE-2023-0540 …	Nhóm 51 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã tùy ý, 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-2023-23695 CVE-2023-24575	Nhóm 02 lỗ hổng trong Dell (Secure Connect Gateway,…) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Adobe	CVE-2023-21574 CVE-2023-21575 CVE-2023-21619 …	Nhóm 26 lỗ hổng trong Adobe (Photoshop, InDesign,…) cho phép đối tượng tấn công thực thi mã tùy ý, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-43927 CVE-2022-43929 CVE-2023-24964 ...	Nhóm 08 lỗ hổng trong IBM (InfoSphere Information Server,…) 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.	Đã có thông tin xác nhận và bản vá

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

Tấn công DRDoS

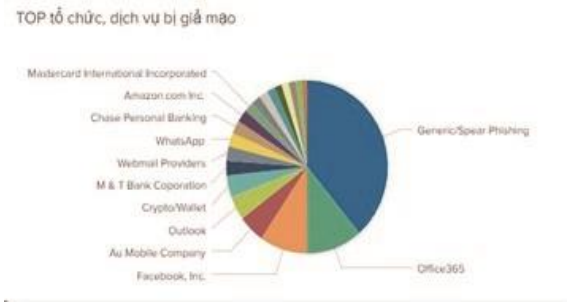
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **50,826** (tăng so với tuần trước **45,154**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.





Tấn công Web

Trong tuần, có 280 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 265 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: 7947 IP	xjpakmdcfuqe.ru:116 IP
disorderstatus.ru: 3247 IP	xjpakmdcfuqe.in:122 IP
atomictrivia.ru: 1588 IP	restlesz.su: 234 IP
xjpakmdcfuqe.biz: 242 IP	amnsreiuojy.ru: 571 IP
xjpakmdcfuqe.com: 182 IP	hzmksreiuojy.ru: 46 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 464 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	vayqualuongshinhan.com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
2	sieuthidienmayxanh247.com	Website giả mạo Điện máy xanh
3	jaccscom.com bxrtxfr.xyz hdcreditvnn.com vaynhanhvn.net	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