NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 14 (01/04/2024 – 07/04/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công mạng người Việt tấn công vào tổ chức tài chính để thu thập dữ liệu tại Châu Á.

- **Cảnh báo:** Tấn công từ chối dịch vụ trên giao thức HTTP/2: Một luồng kết nối đủ để đánh sập máy chủ web.

2. Điểm yếu, lỗ hổng

- **781** 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: 280** 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://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công: Nhóm tấn công mạng người Việt tấn công vào tổ chức tài chính để thu thập dữ liệu tại Châu Á."

Một nhóm tấn công được cho là có nguồn gốc từ Việt Nam đã bị phát hiện trong quá trình tiến hành các cuộc tấn công nhằm vào quốc gia ở Đông Nam Á kể từ tháng 05/2023. Nhóm này được gọi là CoralRaider và là một nhóm APT có động cơ về tài chính, thường sử dụng mã độc để thu thập thông tin. Hiện tại, nhóm này nhằm mục tiêu vào các quốc gia như: Ấn Độ, Trung Quốc, Hàn Quốc, Bangladesh, Pakistan, Indonesia và Việt Nam.

Nhóm CoralRaider thường triển khai các chiến dịch tấn công nhằm lấy cắp thông tin đăng nhập, dữ liệu tài chính và tài khoản mạng xã hội của nạn nhân, bao gồm cả tài khoản kinh doanh và quảng cáo. Nhóm này sử dụng nhiều loại mã độc như RotBot (một biến thể của Quasar RAT) và mã độc đánh cắp dữ liệu XClient stealer làm payload. Ngoài ra, nhóm APT này cũng sử dụng các loại mã độc trojan truy cập từ xa và mã độc đánh cắp dữ liệu như: AsyncRAT, NetSupport RAT và Rhadamanthys.

Các nhóm tấn công mạng hoạt động tại nước ngoài thường tấn công các tài khoản mạng xã hội kinh doanh hoặc quảng cáo bằng một số loại mã độc đánh cắp dữ liệu nổi bật như Ducktail, NodeStealer và VietCredCare.

Sau đó, các đối tượng tấn công chiếm quyền kiểm soát và lợi dụng các tài khoản đã đánh cắp nhằm thực hiện các hành vi vi phạm pháp luật để kiếm lời trong một khoảng thời gian dài.

Trong chiến dịch tấn công, nhóm CoralRaider sử dụng Telegram để thu thập dữ liệu từ các đối tượng mục tiêu, sau đó trao đổi thông tin này trên các web đen để kiếm lợi nhuận. Thông qua các tin nhắn trên kênh bot C&C Telegram, tên bot, chuỗi PDB và ngôn ngữ tiếng Việt trong file payload, cơ quan bảo mật đã xác định được nhóm tấn công này có nguồn gốc từ Việt Nam.

Chiến dịch bắt đầu bằng một file Windows shortcut (LNK), được phát tán cho người dùng (tuy nhiên chưa rõ cách thức phát tán). Khi mở file LNK, một file ứng dụng HTML (HTA) được tải và thực thi từ xa từ một máy chủ của đối tượng tấn công, sau đó thực hiện một script Visual Basic được nhúng trong file HTA. Script này giải mã và thực thi một script PowerShell để vượt qua các biện pháp chống môi trường máy ảo và phân tích, vô hiệu hóa Windows User Access Control (UAC), tắt thông báo của Windows và ứng dụng, và tải và thực thi RotBot.

Nguồn: https://thehackernews.com/2024/04/vietnam-based-hackers-steal-financial.html

Tin tức An toàn thông tin

"Chiến dịch tấn công: Nhóm tấn công mạng người Việt tấn công vào tổ chức tài chính để thu thập dữ liệu tại Châu Á."

Mã độc RotBot được thiết lập để giao tiếp với bot trên Telegram và tải mã độc XClient nhằm thực thi mã độc trong bộ nhớ máy tính và đánh cắp thông tin như cookies, thông tin đăng nhập và thông tin tài chính từ các trình duyệt web như Brave, Cốc Cốc, Google Chrome, Microsoft Edge, Mozilla Firefox và Opera; cũng như dữ liệu từ các ứng dụng như Discord và Telegram và ảnh được lưu trữ trên thiết bị. Bên cạnh đó, mã độc XClient được thiết lập để đánh cắp thông tin từ các tài khoản Facebook, Instagram, TikTok và YouTube của nạn nhân, kể cả thông tin về cách thanh toán và quyền hạn trên các tài khoản quảng cáo/kinh doanh của Facebook.

Thông tin về nhóm tấn công đã được tiết lộ sau khi Bitdefender công bố chi tiết về một chiến dịch quảng cáo độc hại trên Facebook. Chiến dịch này lợi dụng sự phổ biến của các công cụ AI để lan truyền các mã độc như Rilide, Vidar, IceRAT và Nova Stealer. Chiến dịch này bắt đầu bằng việc sử dụng các tài khoản Facebook bị chiếm đoạt để tạo ra các trang hồ sơ giả mạo của các công cụ AI từ Google, OpenAI và Midjourney, sau đó chạy quảng cáo để phát tán mã độc.

Một trong số các trang giả mạo này đã thu hút được 1.2 triệu người theo dõi trước khi bị Facebook xóa. Các đối tượng điều hành các trang này chủ yếu đến từ Việt Nam, Mỹ, Indonesia, Anh và Úc.

Dưới đây là một số IoC được ghi nhận:

51[.]79[.]208[.]192

199[.]34[.]27[.]196

139[.]99[.]23[.]9

14[.]225[.]210[.]98

14[.]225[.]210[.]97

14[.]225[.]210[.]209

14[.]225[.]210[.]222

doc-0s-44-docstext[.]googleusercontent[.]com

doc-10-44-docstext[.]googleusercontent[.]com

Nguồn: https://thehackernews.com/2024/04/vietnam-based-hackers-steal-financial.html

Tin tức An toàn thông tin

"Cảnh báo: Tấn công từ chối dịch vụ trên giao thức HTTP/2: Một luồng kết nối đủ để đánh sập máy chủ web."

Một loạt lỗ hổng mới vừa được phát hiện trong giao thức HTTP/2, được gọi là "CONTINUATION Flood". Các lỗ hổng này cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ bằng cách đánh sập máy chủ web chỉ với một luồng kết nối TCP.

Giao thức HTTP/2 là phiên bản cải tiến của giao thức HTTP được chuẩn hóa vào năm 2015, nhằm cải thiện hiệu suất web. Nó được thiết kế để đem lại khả năng truyền dữ liệu hiệu quả hơn bằng cách sử dụng binary framing, cho phép trao đổi dữ liệu một cách hiệu quả, ghép kênh để có thể gửi và nhận nhiều yêu cầu và phản hồi trên cùng một kết nối, và nén header để giảm phí tổn.

Lỗi CONTINUATION Flood liên quan đến frame CONTINUATION trong giao thức HTTP/2, hiện không được hạn chế hoặc kiểm tra cẩn thận trong nhiều ứng dụng sử dụng giao thức này. Trong giao thức HTTP/2, các thông điệp sử dụng phần header và trailer được xếp thành các khối có thể phân mảnh thành nhiều frame trong quá trình trao đổi, và frame CONTINUATION được sử dụng để ghép chúng lại.

Sự thiếu sót trong kiểm tra frame trong nhiều ứng dụng web cho phép đối tượng tấn công gửi một chuỗi frame rất dài mà không đặt flag END_HEADERS, gây ra máy chủ bị sập do hết bộ nhớ hoặc tài nguyên CPU bị cạn kiệt khi xử lý frame này. Các lỗi này đã được đánh giá và gán mã định danh CVE tương ứng với nhiều cấp độ tấn công từ chối dịch vụ khác nhau như rò rỉ bộ nhớ, tiêu hao bộ nhớ, làm cạn CPU,... cụ thể như sau:

- CVE-2024-27983: Ảnh hưởng máy chủ Node.js HTTP/2, có thể dẫn tới rò rỉ bộ nhớ do tấn công race condition, gây ra từ chối dịch vụ.
- CVE-2024-27919: Ảnh hưởng đến mã code oghttp của Envoy, dẫn tới tiêu hao bộ nhớ do không làm mới yêu cầu khi chạm tới giới hạn header map.
- CVE-2024-2758: Tồn tại trên Tempesta FW, giới hạn rate không đủ ngăn chặn tấn công CONTINUATION Flood, gây ra từ chối dịch vụ.
- CVE-2024-31309: Ảnh hưởng Apache Traffic Server, gây hao tổn tài nguyên CPU.

Nguồn: https://www.bleepingcomputer.com/news/security/new-http-2-dos-attack-can-crash-web-servers-with-a-single-connection/?&web_view=true#google_vignette

Tin tức An toàn thông tin

"Cảnh báo: Tấn công từ chối dịch vụ trên giao thức HTTP/2: Một luồng kết nối đủ để đánh sập máy chủ web."

- CVE-2023-45288: Ảnh hưởng các gói GO net/http và net/http2=. Cho phép đối tượng tấn công gửi nhiều header tới máy chủ, gây ra hao tổn CPU.
- CVE-2024-28182: Ảnh hưởng thư viện nghttp2 và cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ khi không có lời gọi reset chuỗi phù hợp.
- CVE-2024-27316: Ảnh hưởng Apache Httpd. Hàng loạt frame CONTINUATION không có gán cờ END_HEADERS có thể được gửi tới máy chủ, dẫn tới việc gián đoạn quá trình xử lý yêu cầu.
- CVE-2024-30255: Ảnh hưởng Envoy 1.29.2 và cũ các phiên bản hơn. Cho phép đối tượng tấn công làm cạn tài nguyên CPU của máy chủ.
- CVE-2024-2653: Ảnh hưởng amphp/http. Frame CONTINUATION được thu thập trong một buffer không giới hạn, gây ra tràn bộ nhớ nếu giới hạn kích thước header bị vượt quá.

Hiện tại, một số nhà cung cấp như Red Hat, SUSE Linux, Arista Networks, Apache HTTP Server Project,... đã xác nhận bị ảnh hưởng bởi một trong số các CVE trên. Các nhà nghiên cứu bảo mật cảnh báo rằng các lỗ hổng trong giao thức HTTP/2 nghiêm trọng hơn so với cuộc tấn công "HTTP/2 Rapid Reset" trước đó.

Nguồn: https://www.bleepingcomputer.com/news/security/new-http-2-dos-attack-can-crash-web-servers-with-a-single-connection/?&web_view=true#google_vignette

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 **781** lỗ hổng, trong đó có 113 lỗ hổng mức Cao, 182 lỗ hổng mức Trung bình, 45 lỗ hổng mức Thấp và 441 lỗ hổng chưa đánh giá. Trong đó có ít nhất 201 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 173 lỗ hổng trong Linux, Nhóm 29 lỗ hổng trong Google, Nhóm 47 lỗ hổng trong Foxit, Nhóm 14 lỗ hổng trong Qualcomm, Nhóm 05 lỗ hổng trong Nvidia, Nhóm 13 lỗ hổng trong Cisco, Nhóm 12 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:

- Linux: CVE-2023-52630, CVE-2023-52631,...

- Google: CVE-2023-48426, CVE-2024-22004,...

- Foxit: CVE-2024-30322, CVE-2024-30323,...

- Qualcomm: CVE-2024-21473, CVE-2024-21468

- Nvidia: CVE-2024-0072, CVE-2024-0076,...

- Cisco: CVE-2024-20281, CVE-2024-20348,...

- IBM: CVE-2024-22328, CVE-2024-25029,...

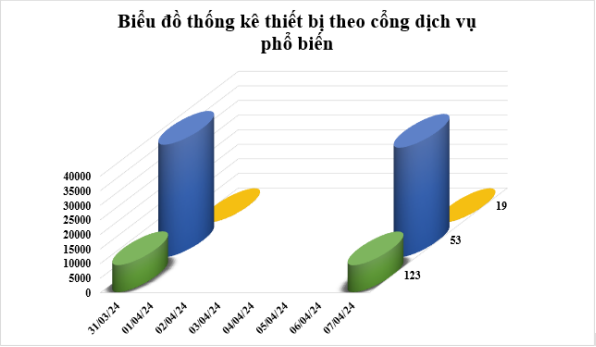
Thông tin điểm yếu, lỗ hổng

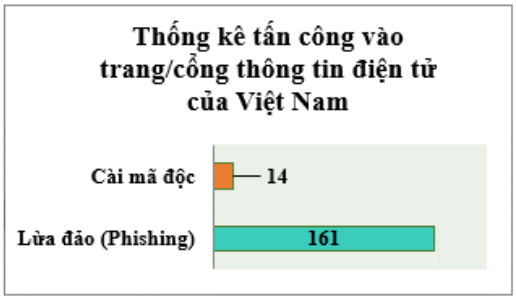
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-52630 CVE-2023-52631 CVE-2023-52632 ...	Nhóm 173 lỗ hổng trong Linux cho phép tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Google	CVE-2023-48426 CVE-2024-22004 CVE-2024-27231 ...	Nhóm 29 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Foxit	CVE-2024-30322 CVE-2024-30323 CVE-2024-30324	Nhóm 47 lỗ hổng trong Foxit 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	Qualcomm	CVE-2024-21473 CVE-2024-21468 CVE-2024-21470 ...	Nhóm 14 lỗ hổng trong Qualcomm 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
5	Nvidia	CVE-2024-0072 CVE-2024-0076 CVE-2023-31028 ...	Nhóm 05 lỗ hổng trong Nvidia 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
6	Cisco	CVE-2024-20281 CVE-2024-20348 CVE-2024-20347 ...	Nhóm 13 lỗ hổng trong Cisco cho phép đối tượng tấn công khai thác lỗi CSRF, khai thác lỗi XSS, khai thác lỗi SSRF, leo thang đặc quyền, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2024-22328 CVE-2024-25029 CVE-2024-28787 ...	Nhóm 12 lỗ hổng trong IBM phép đối tượng tấn công 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

Thống 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 **46.844** (giảm so với tuần trước **47.913**) 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.



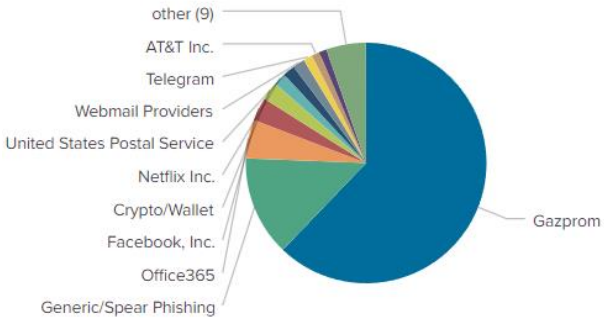


Tấn công Web

Trong tuần, có **175** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 161 trường hợp tấn công lừa đảo (Phishing), 14 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: 2113 IP	hzmksreiuojy.ru: 52 IP
disorderstatus.ru: 954 IP	xjpakmdcfuqe.biz: 23 IP
atomictrivia.ru: 511 IP	xjpakmdcfuqe.com: 19 IP
amnsreiuojy.ru: 115 IP	xjpakmdcfuqe.ru: 15 IP
restlesz.su: 90 IP	xjpakmdcfuqe.in: 09 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **280** 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	https://skhf11[.]com https://fdsd22[.]com	Website giả mạo sàn TMĐT Tiki
2	https://mbfic-plus[.]com	Website giả mạo Ngân hàng TMCP Quân đội
3	cskh-vib[.]nang-han-muc-the-visa[.]com khcn-uu-tien-3fv-vib[.]com kh-cn-uutien-3fv-vib[.]com stcard-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
4	https://quaysomediamart2024[.]vip	Website giả mạo Công ty Cổ phần MediaMart Việt Nam

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