NCSC VN
National Cyber Security Center

## Trung tâm Giám sát an toàn không gian mạng quốc gia

# CẢNH BÁO TUẦN

**Số 10 (04/03/2024 – 10/03/2024)**

s

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Lotus Bane - Chủ mưu của chiến dịch tấn công các tổ chức tài chính tại Việt Nam.

- **Cảnh báo:** Canva cảnh báo về ba lỗ hổng mới trong phông chữ.

## 2. Điểm yếu, lỗ hổng

- **579** 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: 254** 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

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Chiến dịch tấn công: Nhóm APT Lotus Bane - Chủ mưu của chiến dịch tấn công các tổ chức tài chính tại Việt Nam."

Một tổ chức tài chính ở Việt Nam đã trở thành mục tiêu của nhóm APT Lotus Bane trong một chiến dịch tấn công được phát hiện lần đầu vào tháng 03/2023, nhóm này bị nghi ngờ là đã hoạt động kể từ năm 2022.

Hiện vẫn chưa xác định rõ về cách thức lây nhiễm mã độc của nhóm Lotus Bane, tuy nhiên, đã có những dấu hiệu cho thấy nhóm này sử dụng các kỹ thuật tấn công như DLL side-loading và trao đổi dữ liệu qua named pipe. Những kỹ thuật này được sử dụng để thực thi các tập tin độc hại và tạo ra lịch trình tác vụ từ xa, nhằm mục đích di chuyển ngang hệ thống. Mục tiêu của việc di chuyển ngang hệ thống là để lấy được quyền truy cập vào các tài nguyên quan trọng hoặc để lan truyền mã độc hoặc tấn công đến các vị trí khác trong hệ thống.

Đáng chú ý, các kỹ thuật tấn công mà nhóm Lotus Bane sử dụng có nhiều điểm tương đồng với nhóm OceanLotus, một nhóm tấn công có nguồn gốc từ Việt Nam (có nhiều tên gọi khác như APT32, Canvas Cyclone, Bismuth và Cobalt Kitty). Tuy nhiên, ngoài điểm chung là cùng sử dụng các mã độc như PIPEDANCE để kết nối named pipe thì đối tượng mục tiêu của hai nhóm tấn công này khác nhau. Do đó, khả năng hai nhóm này là một rất khó xảy ra.

Mã độc PIPEDANCE được phát hiện vào tháng 02/2023 trong một chiến dịch nhằm vào một tổ chức ở Việt Nam vào cuối tháng 12/2022. Mặc dù Lotus Bane chủ yếu nhằm vào lĩnh vực ngân hàng tại khu vực Châu Á-Thái Bình nhưng lại phát hiện chiến dịch tấn công này xuất phát từ Việt Nam. Điều này cho thấy cho thấy Lotus Bane rất tinh vi và phạm vi hoạt động có thể lan rộng hơn dự kiến. Thông tin về Lotus Bane được công bố trong bối cảnh có nhiều tổ chức tài chính tại Châu Á Thái Bình Dương, Châu Âu, Mỹ Latin và Bắc Mỹ cùng một lúc trở thành mục tiêu của các nhóm APT như Blind Eagle và Lazarus Group trong thời gian gần đây.

Gần đây, một nhóm APT có động cơ tài chính đáng chú ý là UNC1945 đã tiến hành các cuộc tấn công nhắm vào các máy chủ switch ATM với mục tiêu lây nhiễm mã độc CAKETAP trên hệ thống. Mã độc này có khả năng ngăn chặn dữ liệu được truyền từ máy chủ ATM tới máy chủ chứa module bảo mật phần cứng và kiểm tra dữ liệu với các điều kiện đã được đặt trước. Nếu các điều kiện được đáp ứng, mã độc sẽ sửa đổi dữ liệu trước khi gửi lại tới máy chủ ATM.

Trước đó, hai nhóm UNC2891 và UNC1945 đã triển khai rootkit CAKETAP trên các hệ thống chạy Oracle Solaris vào tháng 02/2022. Họ sử dụng rootkit này để ngăn chặn tin nhắn gửi từ mạng lưới switch ATM và thực hiện việc rút tiền trái cấp phép tại nhiều ngân hàng khác nhau bằng cách sử dụng thẻ giả.

Nguồn: https://thehackernews.com/2024/03/new-apt-group-lotus-bane-behind-recent.html

# Tin tức An toàn thông tin

## "Cảnh báo: Canva cảnh báo về ba lỗ hổng mới trong phông chữ."

Nền tảng thiết kế trực tuyến Canva đã phát hiện ba lỗ hổng an toàn thông tin liên quan đến font chữ của mình. Trong quá trình tìm kiếm các biện pháp để cải thiện tính bảo mật của nền tảng, bao gồm phần mềm, chuỗi cung ứng, công cụ và quy trình, Canva đã tập trung vào các phạm vi tấn công ít được chú ý như font chữ, một phần quan trọng và phổ biến trong việc xử lý đồ họa. Qua đó, Canva đã phát hiện ra ba lỗ hổng an toàn thông tin, cụ thể là:

CVE-2023-45139 (Điểm CVSS: 7.5): Lỗ hổng tồn tại trong FontTools, một thư viện quản lý phông chữ bằng ngôn ngữ Python. Thư viện này có khả năng sử dụng các tệp XML không đáng tin cậy khi xử lý một bảng SVG nhằm giảm kích cỡ phông chữ bằng việc loại bỏ các phần không cần thiết. Điều này dẫn đến việc một phông chữ có kích cỡ nhỏ hơn được tạo ra bằng cách sử dụng một bảng SBG có chứa một đối tượng được nén thành một tệp mật khẩu.

CVE-2024-25081 (Điểm CVSS: 4.2) và CVE-2024-25082 (Điểm CVSS: 4.2): Đây là hai lỗ hổng liên quan tới việc đặt tên và nén của file. Cụ thể, những lỗi này có thể tồn tại trên các công cụ như FontForge và ImageMagick, cho phép người dùng thay đổi tên tập tin của phông chữ. Điều này giúp người dùng có thể dễ dàng tìm kiếm một phông chữ cụ thể trong hệ thống có tên phức tạp.

Tuy nhiên, việc lưu tên tập tin có thể gây ra rủi ro về an toàn thông tin khi xử lý dữ liệu không bảo mật, vì nó cho phép kẻ tấn công tạo ra một shell để thực thi, khiến FontForge mở các tập tin công cụ mà không cần quyền truy cập.

Khi FontForge truy cập và chỉnh sửa file phông chữ trong file nén, nó tạo ra một thư mục tạm để thực hiện công việc. Quá trình duyệt TOC (bảng mục lục) của FontForge có thể bị khai thác bởi việc lấy tên file từ chức năng ArchiveParseTOC. Đối tượng tấn công có thể tạo ra một file nén được đặt tên độc hại, vượt qua các biện pháp bảo mật thông thường và thực hiện tấn công chèn lệnh. Điều này có thể ảnh hưởng đến cả máy chủ và ứng dụng trên thiết bị.

Canva nhấn mạnh rằng phông chữ là một điểm yếu phổ biến vì các tổ chức và cá nhân thường muốn sử dụng phông chữ độc đáo với các thiết lập tùy chỉnh. Mỗi loại phông chữ lại có các thông số kỹ thuật đặc biệt của riêng nó. Vì vậy, Canva đề xuất rằng phông chữ nên được coi như là dữ liệu không an toàn và cần được xử lý một cách cẩn thận. Đồng thời, hiện vẫn còn nhiều hạn chế về mặt bảo mật trong lĩnh vực này.

Nguồn: https://www.theregister.com/2024/03/08/canva_font_security/?&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 **579** lỗ hổng, trong đó có 99 lỗ hổng mức Cao, 157 lỗ hổng mức Trung bình, 20 lỗ hổng mức Thấp và 303 lỗ hổng chưa đánh giá. Trong đó có ít nhất 80 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 59 lỗ hổng trong Linux, Nhóm 03 lỗ hổng trong Google, Nhóm 71 lỗ hổng trong Apple, Nhóm 05 lỗ hổng trong Dell, Nhóm 22 lỗ hổng trong Qualcomm, Nhóm 08 lỗ hổng trong Cisco, Nhóm 21 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-2021-47102, CVE-2023-52584,...*

*- Google: CVE-2024-2173, CVE-2024-2174,...*

*- Apple: CVE-2024-23225, CVE-2024-23296,...*

*- Dell: CVE-2024-0155, CVE-2024-0156,...*

*- Qualcomm: CVE-2023-28578, CVE-2023-28582,...*

*- Cisco: CVE-2024-20337, CVE-2024-20338,...*

*- IBM: CVE-2024-25016, CVE-203-32331,...*

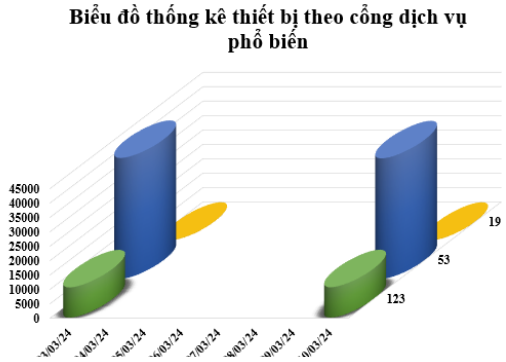
# Thông tin điểm yếu, lỗ hổng

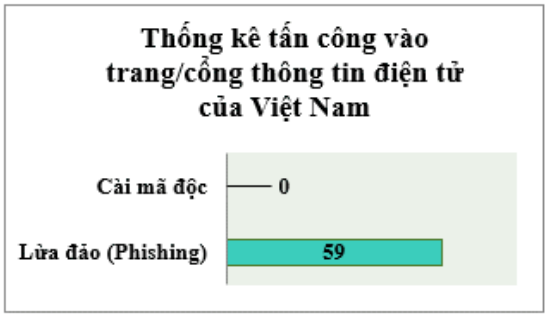
| TT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| 1 | Linux | CVE-2021-47102<br>CVE-2023-52584<br>CVE-2021-47082<br>… | Nhóm 59 lỗ hổng trong Linux cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép. | Chưa có thông tin xác nhận và bản vá |
| 2 | Google | CVE-2024-2173<br>CVE-2024-2174<br>CVE-2024-2176 | Nhóm 03 lỗ hổng trong Google 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 |
| 3 | Apple | CVE-2024-23225<br>CVE-2024-23296<br>CVE-2024-23201<br>… | Nhóm 71 lỗ hổng trong Apple cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, 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 |
| 4 | Dell | CVE-2024-0155<br>CVE-2024-0156<br>CVE-2024-22452<br>… | Nhóm 05 lỗ hổng trong Dell cho phép đối tượng tấn công thực thi mã từ xa, leo thăng đặc quyền, truy cập và thực hiện các hành động trái phép. | Chưa có thông tin xác nhận và bản vá |
| 5 | Qualcomm | CVE-2023-28578<br>CVE-2023-28582<br>CVE-2023-43552<br>... | Nhóm 22 lỗ hổng trong Qualcomm 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 |
| 6 | Cisco | CVE-2024-20337<br>CVE-2024-20338<br>CVE-2024-20345<br>… | Nhóm 08 lỗ hổng trong Cisco cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗ hổng XSS, truy cập và thực hiện các hành động trái phép. | Chưa có thông tin xác nhận và bản vá |
| 7 | IBM | CVE-2024-25016<br>CVE-2023-32331<br>CVE-2022-22399<br>... | Nhóm 21 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗ hổng XSS 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 **52.416** (giảm so với tuần trước **52.509**) 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.



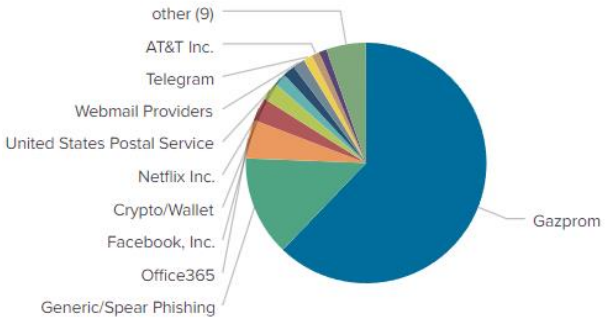




## Tấn công Web

Trong tuần, có **59** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 59 trường hợp tấn công lừa đảo (Phishing), 0 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: 8273 IP | hzmksreiuojy.ru: 130 IP |
| disorderstatus.ru: 4324 IP | xjpakmdcfuqe.biz: 149 IP |
| atomictrivia.ru: 1967 IP | xjpakmdcfuqe.com: 94 IP |
| amnsreiuojy.ru: 527 IP | xjpakmdcfuqe.ru: 89 IP |
| restlesz.su: 241 IP | xjpakmdcfuqe.in: 87 IP |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **254** 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 | sendovn[.]com | Website giả mạo sàn TMĐT Sendo |
| 2 | tdkd01[.]com<br>tah0a[.]com | Website giả mạo sàn TMĐT Tiki |
| 3 | lzd2024[.]com | Website giả mạo sàn TMĐT Lazada |
| 4 | ebayget[.]cc | Website giả mạo sàn TMĐT Ebay |
| 5 | abbankquick[.]com<br>www[.]abb-vnbank[.]cc | Website giả mạo Ngân hàng TMCP An Bình |
| 6 | www[.]shopeesmarket[.]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