NCSC VN
National Cyber Security Center

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

# CẢNH BÁO TUẦN

**Số 11 (11/03/2024 – 17/03/2024)**

s

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT RedCurl sử dụng PCA Windows cho hoạt động gián điệp không gian mạng.

- **Cảnh báo:** Chiến dịch tấn công plugin "Popup Builder" trên WordPress ảnh hưởng hơn 3.900 trang web.

## 2. Điểm yếu, lỗ hổng

- **767** 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: 319** 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 RedCurl sử dụng PCA Windows cho hoạt động gián điệp không gian mạng."

Nhóm tấn công APT RedCurl, có nguồn gốc từ Nga, đã khai thác một công cụ hợp pháp trên Windows, gọi là Program Compatibility Assistant (PCA), để chạy các lệnh độc hại. PCA hay pcalua.exe là một công cụ được dùng để phát hiện và sửa lỗi tương thích của các chương trình trên phiên bản cũ của Windows. Tuy nhiên, nhóm tấn công này đã sử dụng nó để thực thi mã từ xa, bỏ qua các biện pháp bảo mật thông thường.

Nhóm APT RedCurl, còn có các tên gọi khác như Earth Kapre và Red Wolf, đã hoạt động từ năm 2018 với các chiến dịch gián điệp không gian mạng nhằm vào các doanh nghiệp tại nhiều quốc gia như Úc, Canada, Đức, Nga, Slovenia, Anh, Mỹ và Ukraine. Trong cuộc tấn công vào tháng 11/2022 và tháng 05/2023, RedCurl đã gây ra thiệt hại nghiêm trọng cho một ngân hàng lớn tại Nga và một công ty tại Úc, khiến dữ liệu quan trọng của doanh nghiệp và thông tin cá nhân của nhân viên bị đánh cắp.

Chiến dịch của nhóm tấn công này thường bắt đầu bằng việc gửi các email lừa đảo chứa các tệp tin độc hại như .ISO và .IMG. Sau đó, chúng sẽ sử dụng cmd.exe để tải xuống tiện ích "curl" từ máy chủ từ xa, tiện ích này sẽ được sử dụng làm kênh trung gian để tải xuống các tệp tin loader (ms.dll hoặc ps.dll).

Các tệp DLL độc hại sau đó sẽ sử dụng PCA để tạo ra một quy trình bộ tải khác để kết nối đến máy chủ chứa "curl" và tải xuống loader. Đồng thời, nhóm tấn công này cũng sử dụng phần mềm mã nguồn mở Impacket để thực thi mã từ xa mà không cần quyền truy cập.

Thông tin về cuộc tấn công này được tiết lộ cùng lúc với việc một nhóm APT khác, cũng được cho là có liên quan đến Nga, đang sử dụng một DLL giả mạo có tên là Pelmeni để triển khai mã độc backdoor Kazuar viết bằng .NET.

DLL độc hại Pelmeni thường giả mạo thành các thư viện liên quan như SkyTel, NVIDIA Geforce Experience, vncutil, ASUS và được tải vào bằng kỹ thuật DLL side-loading. Khi được kích hoạt bởi chương trình bị ảnh hưởng thì DLL sẽ giải mã và thực thi mã độc Kazuar.

Nguồn: https://thehackernews.com/2024/03/redcurl-cybercrime-group-abuses-windows.html

# Tin tức An toàn thông tin

## "Cảnh báo: Chiến dịch tấn công plugin "Popup Builder" trên WordPress ảnh hưởng hơn 3.900 trang web."

Một loạt các trang web đã bị ảnh hưởng bởi một chiến dịch mã độc sử dụng một lỗ hổng an toàn thông tin ở mức độ cao trong plugin Popup Builder trên WordPress. Trong vòng 3 tuần, hơn 3.900 trang web đã bị tác động bởi chiến dịch này. Chiến dịch được bắt đầu từ các tên miền mới, với tên miền cũ nhất được đăng ký vào ngày 12/02/2024.

Lỗ hổng CVE-2023-6000 trên Popup Builder đã bị khai thác để tạo người dùng quản trị không hợp lệ và cài đặt các plugin tùy ý, làm cho quá trình lây nhiễm trở nên dễ dàng cho kẻ tấn công. Trước đó, lỗ hổng này đã được sử dụng trong chiến dịch tấn công Balada Injector vào tháng 01/2024, làm ảnh hưởng tới khoảng 7000 trang web. Diễn biến mới nhất trong chiến dịch này là việc chèn đoạn mã độc hại, được chia thành hai biến thể nhằm mục tiêu điều hướng người dùng đến các trang web độc hại.

Chủ các trang web sử dụng WordPress được khuyến nghị cập nhật các plugin lên phiên bản mới nhất và thực hiện việc quét website để phát hiện các mã độc hoặc người dùng có hành vi đáng ngờ. Đồng thời, cần thực hiện các biện pháp xử lý phù hợp để bảo vệ trang web của mình.

Thông tin về cuộc tấn công được tiết lộ sau khi bộ phận bảo mật của WordPress công bố một lỗ hổng an toàn thông tin trên plugin Ultimate Member, có thể bị khai thác để chèn các đoạn mã script độc hại. Lỗ hổng này có mã CVE-2024-2123 (Điểm CVSS: 7.2), cho phép đối tượng tấn công khai thác lỗi XSS và ảnh hưởng đến các phiên bản cũ hơn 2.8.3 của plugin. Hiện lỗ hổng này đã được vá trong phiên bản 2.8.4 trở lên.

Vào tháng 02/2024, WordPress cũng đã xử lý một lỗ hổng tương tự với mã CVE-2024-1071 (Điểm CVSS là 9.8). Ngoài ra, một lỗ hổng khác liên quan đến việc tải lên file tùy ý trong Avada WordPress (CVE-2024-1468, điểm CVSS: 8.8) cũng đã được phát hiện. Đối tượng tấn công có thể khai thác lỗ hổng này để thực thi mã từ xa. Hiện lỗ hổng này đã được vá trong phiên bản 7.11.5 của Avada.

Nguồn: https://thehackernews.com/2024/03/malware-campaign-exploits-popup-builder.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 **767** lỗ hổng, trong đó có 195 lỗ hổng mức Cao, 299 lỗ hổng mức Trung bình, 30 lỗ hổng mức Thấp và 243 lỗ hổng chưa đánh giá. Trong đó có ít nhất 190 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 50 lỗ hổng trong Linux, Nhóm 58 lỗ hổng trong Google, Nhóm 03 lỗ hổng trong Apple, Nhóm 61 lỗ hổng trong Microsoft, Nhóm 09 lỗ hổng trong Fortinet, Nhóm 09 lỗ hổng trong Cisco, Nhóm 14 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-2024-26616, CVE-2021-47109,...
- Google: CVE-2024-0039, CVE-2024-0044,...
- Apple: CVE-2024-23300, CVE-2023-42938,...
- Microsoft: CVE-2024-26203, CVE-2024-21400,...
- Fortinet: CVE-2023-47534, CVE-2023-48788,...
- Cisco: CVE-2024-20319, CVE-2024-20318,...
- IBM: CVE-2024-22346, CVE-2024-27266,...

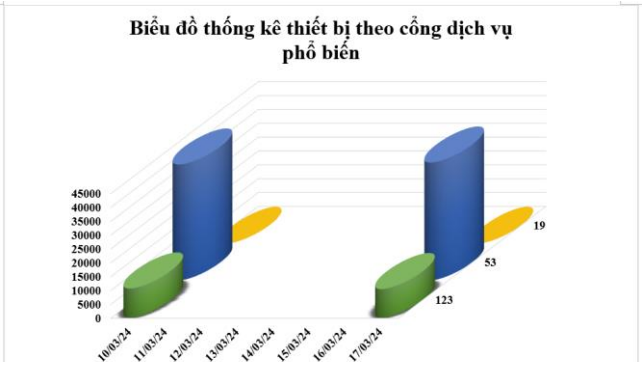
# Thông tin điểm yếu, lỗ hổng

| TT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| 1 | Linux | CVE-2024-26616<br>CVE-2021-47109<br>CVE-2021-47110<br>... | Nhóm 50 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-2024-0039<br>CVE-2024-0044<br>CVE-2024-0045<br>... | Nhóm 58 lỗ hổng trong Google cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ. | Chưa có thông tin xác nhận và bản vá |
| 3 | Apple | CVE-2024-23300<br>CVE-2023-42938<br>CVE-2024-23298 | Nhóm 03 lỗ hổng trong Apple 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 |
| 4 | Microsoft | CVE-2024-26203<br>CVE-2024-21400<br>CVE-2024-21421<br>... | Nhóm 61 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, khai thác lỗi XSS, thực hiện tấn công từ chối dịch vụ. | Chưa có thông tin xác nhận và bản vá |
| 5 | Fortinet | CVE-2023-47534<br>CVE-2023-48788<br>CVE-2023-36554<br>... | Nhóm 09 lỗ hổng trong Fortinet 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 |
| 6 | Cisco | CVE-2024-20319<br>CVE-2024-20318<br>CVE-2024-20327<br>… | Nhóm 09 lỗ hổng trong Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, khai thác lỗi XSS. | Chưa có thông tin xác nhận và bản vá |
| 7 | IBM | CVE-2024-22346<br>CVE-2024-27266<br>CVE-2021-38938<br>... | Nhóm 14 lỗ hổng trong IBM phép đối tượng tấn công leo thang đặc quyền, khai thác lỗi XSS, truy cập và thực hiện các hành động trái phép. | Đã có thông tin xác nhận và bản vá |

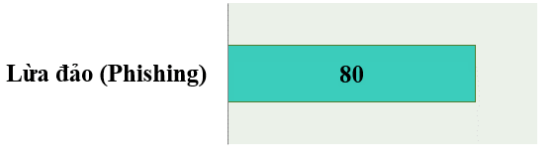
# Thống kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

## 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 **52.933** (tăng so với tuần trước **52.416**) 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**

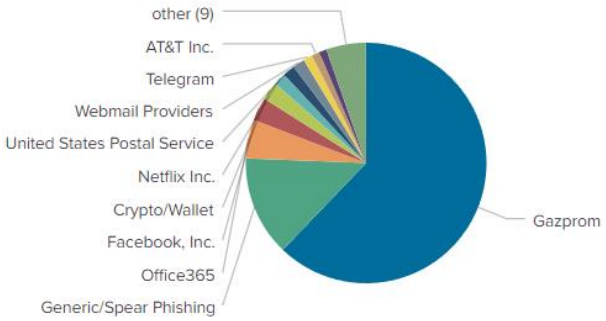



## Tấn công Web

Trong tuần, có **80** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 80 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: 1888 IP | hzmksreiuojy.ru: 37 IP |
| disorderstatus.ru: 1110 IP | xjpakmdcfuqe.biz: 23 IP |
| atomictrivia.ru: 521 IP | xjpakmdcfuqe.com: 22 IP |
| amnsreiuojy.ru: 133 IP | xjpakmdcfuqe.ru: 15 IP |
| restlesz.su: 97 IP | xjpakmdcfuqe.in: 12 IP |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **319** 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 | vn11568p[.]com<br>vn85548s[.]com<br>shoppeemall[.]net | Website giả mạo sàn TMĐT Shopee |
| 2 | dich-vu-the-vdiamond-vib[.]com<br>dich-vu-vip3-vib[.]com | Website giả mạo Ngân hàng Thương mại Cổ phần Quốc tế Việt Nam |
| 3 | tikib[.]vip<br>eufk22[.]com<br>atqa11[.]com<br>tdkd02[.]com<br>tdkd03[.]com | Website giả mạo sàn TMĐT Tiki |
| 4 | policeonline[.]club | Website giả mạo Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) |
| 5 | dichvucong[.]zlgov[.]com<br>dichvucong[.]tkgov[.]com<br>dichvucong[.]dulieuquocgia[.]com | Website giả mạo Dịch vụ công Quốc Gia |
| 6 | www[.]amadbfk[.]vip | Website giả mạo sàn TMĐT Amazon |
| 7 | taichinhmb[.]com<br>cskhmbcanhan[.]com<br>vib[.]chamsocthekhachang-tructuyen[.]com[.]vn | Website giả mạo Ngân hàng TMCP Quân đội |
| 8 | aeeonmaill[.]com | Website giả mạo Công ty TNHH Aeon Việt Nam |
| 9 | www[.]hdsaison-app[.]vip<br>www[.]hdsaison-com[.]cc<br>www[.]hdsaison-hi[.]cc<br>www[.]hdsaison-vn[.]cc<br>… | Website giả mạo Công ty Tài chính TNHH HD SAISON |

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