NCSC VN
National Cyber Security Center

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

# CẢNH BÁO TUẦN

**Số 04 (23/01/2023 – 29/01/2023)**

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Cảnh báo:** Microsoft đang khuyến cáo người dùng bảo mật On-Premises Exchange Servers.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Gamaredon tấn công Ukraine thông qua Telegram.

## 2. Điểm yếu, lỗ hổng

- **633** 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: 113** 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

## "Nhóm tấn công APT Gamaredon tấn công Ukraine thông qua Telegram"


Gần đây, Gamaredon tiếp tục được phát hiện nhằm vào Ukraine thông qua các cuộc tấn công sử dụng ứng dụng nhắn tin phổ biến Telegram. Cơ sở hạ tầng mạng của nhóm dựa vào các tài khoản Telegram với nhiều giai đoạn để lập hồ sơ nạn nhân và xác định vị trí địa lý, sau đó dẫn nạn nhân đến máy chủ giai đoạn tiếp theo.

Theo các chuyên gia nghiên cứu phát hiện, một kênh Telegram mã hóa cứng được sử dụng để lấy địa chỉ IP của máy chủ lưu trữ phần mềm độc hại. Mẫu từ xa được thiết kế để tìm nạp tập lệnh VBA, tệp lệnh này sẽ thả tệp VBScript sau đó kết nối với địa chỉ IP được chỉ định trong kệnh Telegram để tìm nạp giai đoạn tiếp theo – tập lệnh PowerShell lần lượt tiếp cận với một địa chỉ IP khác để lấy tệp PHP.

Tệp PHP này có nhiệm vụ liên hệ với một kênh Telegram khác để truy xuất địa chỉ IP thứ 3 chứa payload cuối cùng, đây là phần mềm độc hại đánh cắp thông tin.

Nhóm thay đổi địa chỉ IP một cách linh hoạt, điều này khiến việc tự động hóa phân tích thông qua các kỹ thuật sandbox. Việc các địa chỉ IP bị nghi ngờ chỉ thay đổi trong giờ làm việc ở Đông Âu cho thấy rõ ràng rằng đối tượng tấn công hoạt động từ một điểm và rất có thể thuộc về một đơn vị mạng tấn công triển khai các hoạt động độc hại nhằm vào Ukraine.

Nguồn:https://thehackernews.com/2023/01/gamaredon-group-launches-cyberattacks.html?&web_view=true

# Tin tức An toàn thông tin

## "Cảnh báo: Microsoft đang khuyến cáo người dùng bảo mật On-Premises Exchange Servers"

Microsoft đang kêu gọi khách hàng cập nhật máy chủ Exchange cũng như thực hiện các bước để nâng cao độ bảo mật, như bật Windows Extended Protection và cấu hình certificate-based signing của payload PowerShell.

Microsoft cũng nhấn mạnh các biện pháp giảm thiểu do công ty đưa ra chỉ là giải pháp tạm thời và chúng có thể không đủ để bảo vệ và chống lại mọi biến thể của cuộc tấn công, đòi hỏi người dùng phải cài đặt các bản cập nhật bảo mật để bảo mật máy chủ.

Exchange Server đã được chứng minh là một công cụ tấn công nổi tiếng trong những năm gần đây, với một số lỗi bảo mật trong phần mềm được vũ khí hóa dưới dạng zero-day để xâm nhập vào hệ thống. Chỉ trong 2 năm qua, một số lỗ hổng bảo mật đã được phát hiện trong Exchange Server như ProxyLogon, ProxyOracle, ProxyShell, Proxy Token, ProxyNotShell.

Hầu hết các cuộc tấn công được cho là mang tính cơ hội hơn là tập trung và nhằm mục tiêu, với sự lây nhiễm lên đến đỉnh điểm trong nỗ lực triển khai web shells và phần mềm quản lý và giám sát từ xa (RMM) như ConnectWise Control và Go To Resolve.

Việc khai thác các lỗ hổng Microsoft Exchange cũng là một chiến thuật lặp đi lặp lại được sử dụng bởi UNC2596 (còn gọi là Tropical Scorpius), với một cuộc tấn công tận dụng trình tự khai thác ProxyNotShell để loại bỏ downloader BUGHATCH.

Mặc dù giai đoạn lây nhiễm ban đầu tiếp tục phát triển và các tác nhân đe dọa nhanh chóng khai thác bất kỳ cơ hội mới nào, nhưng các hoạt động hậu khai thác của chúng đã trở nên quen thuộc. Cách bảo vệ tốt nhất chống lại các cuộc tấn công mạng là kiến trúc phòng thủ chuyên sâu.

Nguồn: https://thehackernews.com/2023/01/microsoft-urges-customers-to-secure-on.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 633 lỗ hổng, trong đó có 53 lỗ hổng mức Cao, 55 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 525 lỗ hổng chưa đánh giá. Trong đó có ít nhất 179 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 03 lỗ hổng trong Adobe, 01 lỗ hổng trong Trend Micro, Nhóm 03 lỗ hổng trong Apache, Nhóm 08 lỗ hổng trong Cisco, 01 lỗ hổng trong Dell, Nhóm 04 lỗ hổng trong Github, Nhóm 06 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:***

*- Adobe: CVE-2023-22240, CVE-2023-22241,...*

*- Trend Micro: CVE-2022-48191.*

*- Apache: CVE-2023-22884, CVE-2020-36658,...*

*- Cisco: CVE-2023-20044, CVE-2022-20964,...*

*- Dell: CVE-2022-34405.*

*- Github: CVE-2023-22483, CVE-2023-22484,...*

*- IBM: CVE-2022-43864, CVE-2022-43917,...*

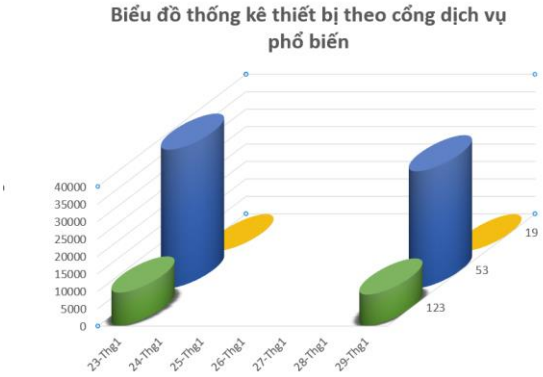
# Thông tin điểm yếu, lỗ hổng

| TT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| **1** | Adobe | CVE-2023-22240<br>CVE-2023-22241<br>CVE-2023-22242 | Nhóm 03 lỗ hổng trong Adobe (Acrobat Reader) cho phép đối tượng tấn công thực thi mã tùy ý. | Chưa có thông tin xác nhận và bản vá |
| **2** | Trend Micro | CVE-2022-48191 | 01 lỗ hổng trong Trend Micro (Trend Micro Maximum Security 2022) cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. | Đã có thông tin xác nhận và bản vá |
| **3** | Apache | CVE-2023-22884<br>CVE-2020-36658<br>CVE-2020-36659 | Nhóm 03 lỗ hổng trong Apache (Airflow, LDAP) cho phép đối tượng tấn công , truy cập/thực hiện các hành động trái phép. | Đã có thông tin xác nhận và bản vá |
| **4** | Cisco | CVE-2023-20044<br>CVE-2022-20964<br>CVE-2023-20008<br>… | Nhóm 08 lỗ hổng trong Cisco (CX Cloud Agent,…) cho phép đối tượng tấn công thực thi các lệnh 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-2022-34405 | 01 lỗ hổng trong Dell (Realtek) cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. | Chưa có thông tin xác nhận và bản vá |
| **6** | Github | CVE-2023-22483<br>CVE-2023-22484<br>CVE-2023-22486<br>… | Nhóm 04 lỗ hổng trong Github (CommonMark) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép. | Chưa có thông tin xác nhận và bản vá |
| **7** | IBM | CVE-2022-43864<br>CVE-2022-43917<br>CVE-2022-22462<br>... | Nhóm 06 lỗ hổng trong IBM (Identity Manager,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép. | Đã có thông tin xác nhận và bản vá |

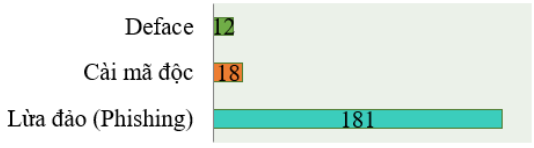
# Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

## 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 **40,895** (giảm so với tuần trước **46,658**) 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.

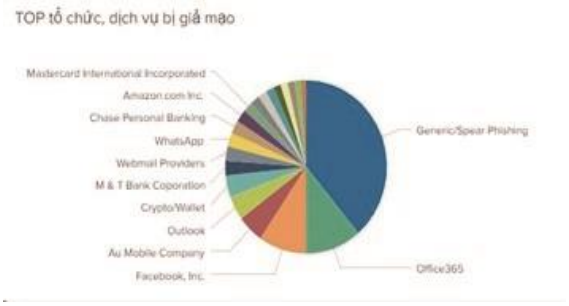



Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam




## Tấn công Web

Trong tuần, có 211 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 12 trường hợp tấn công thay đổi giao diện (Deface), 181 trường hợp tấn công lừa đảo (Phishing), 18 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: 5757 IP | xjpakmdcfuqe.ru:90 IP |
| disorderstatus.ru: 2556 IP | xjpakmdcfuqe.in: 460 IP |
| atomictrivia.ru: 1218 IP | restlesz.su: 122 IP |
| xjpakmdcfuqe.biz: 195 IP | amnsreiuojy.ru: 209 IP |
| xjpakmdcfuqe.com: 107 IP | hzmksreiuojy.ru: 16 IP |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 113 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 | clmm.nl<br>chanlemmo.com<br>dtcltx.com | Giả mạo website Ví điện tử Momo |
| 2 | mp220303.com | Giả mạo website sàn TMĐT Lazada |
| 3 | hdsaisonvn.com<br>vib84.com<br>a666.vn<br>76996.co<br>hdbankfinance.shop<br>6699uu.com<br>zvc.cc<br>79wing.com<br>thao88.com | 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