NCSC VN
National Cyber Security Center

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

# CẢNH BÁO TUẦN

**Số 28 (10/7/2023 – 16/07/2023)**

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Trung Quốc sử dụng PlugX để thực hiện kỹ thuật HTML Smuggling xâm nhập vào các cơ quan, tổ chức tại Châu Âu.

- **Cảnh báo:** Azure và Google Cloud trở thành mục tiêu trong chiến dịch đánh cắp thông tin xác thực trên dịch vụ đám mây.

## 2. Điểm yếu, lỗ hổng

- **912** 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: 336** 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://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Chiến dịch tấn công APT: Nhóm APT Trung Quốc sử dụng PlugX để thực hiện kỹ thuật HTML Smuggling xâm nhập vào các cơ quan, tổ chức tại Châu Âu"

Gần đây, một nhóm APT Trung Quốc đã tiến hành một chiến dịch tấn công thông qua việc sử dụng kỹ thuật HTML Smuggling để xâm nhập vào Bộ Ngoại giao và Đại sứ quán tại châu Âu.

Chiến dịch này được gọi là SmugX, bắt đầu hoạt động kể từ tháng 12 năm 2022 và là một phần của xu hướng dịch chuyển mục tiêu tấn công sang châu Âu của các nhóm APT Trung Quốc. Mục tiêu của chiến dịch này là triển khai mã độc PlugX, một trojan truy cập từ xa, trên các hệ thống bị nhằm mục tiêu.

Chiến dịch sử dụng các phương thức cài cắm mã độc kiểu mới, nổi bật là kỹ thuật HTML Smuggling để cài đặt và triển khai các biến thể mới của mã độc PlugX. Đây là một mã độc quen thuộc của nhiều nhóm tấn công tại Trung Quốc. Mặc dù sử dụng payload tương tự như phiên bản cũ nhưng với cách thức lây nhiễm mã độc mới đã giúp chiến dịch không bị phát hiện cho tới thời gian gần đây.

Hiện nay, việc xác định danh tính của nhóm tấn công đằng sau chiến dịch SmugX vẫn chưa được làm rõ. Dựa trên các manh mối hiện có thì đối tượng tình nghi được các chuyên gia bảo mật hướng đến là nhóm Mustang Panda, có chung đặc điểm với các nhóm APT Earth Preta, RedDelta và Camaro Dragon. Tuy nhiên, vẫn chưa đủ chứng cứ để kết luận một cách chính xác.

Nguồn: https://thehackernews.com/2023/07/chinese-hackers-use-html-smuggling-to.html

Kết quả phân tích mã độc trên VirusTotal còn cho thấy mã độc được thiết kế để nhằm vào các nhà ngoại giao và quan chức chính phủ tại Czechia, Hungary, Slovakia, Anh Quốc, Ukraine,Pháp và Thụy Điển.

Nhóm tấn công đã triển khai một tệp mồi có tên "China Tries to Block Prominent Uyghur Speaker at UN.docx". Khi tệp này sau khi được thực thi sẽ thu thập dữ liệu và gửi đến một máy chủ ngoài hệ thống thông qua một pixel theo dõi ẩn danh được nhúng vào thiết bị.

Quá trình lây nhiễm đa giai đoạn sử dụng kỹ thuật DLL side-loading để giải mã và triển khai payload PlugX.

Mã độc PlugX còn có tên gọi khác là Korplug, một trojan kiểu module được phát hiện vào năm 2008, có chứa nhiều plugin với các chức năng riêng biệt cho phép đối tượng tấn công đánh cắp file, chụp màn hình, keylogging và thực thi câu lệnh.

Trong quá trình điều tra mã độc, nhóm tấn công điều khiển chiến dịch này đã gửi một lệnh batch script có tên "del_RoboTask Update.bat" từ máy chủ C&C với mục đích xóa đi các dấu vết của chiến dịch, cụ thể là xóa đi: file thực thi hợp lệ, DLL loader của PlugX và registry key được sử dụng trong việc thiết lập duy trì rồi cuối cùng là tự xóa đi mã độc.

# Tin tức An toàn thông tin

## "Cảnh báo: Azure và Google Cloud trở thành mục tiêu trong chiến dịch đánh cắp thông tin xác thực trên dịch vụ đám mây"

Trong tháng 6 năm 2023, TeamTNT đã triển khai chiến dịch tấn công đánh cắp thông tin xác thực đám mây, tập trung vào Azure và Google Cloud Platform (GCP). Chiến dịch này có nhiều điểm tương đồng với một chiến dịch trước đó của TeamTNT tên là Silentbob. SilentBob sử dụng các dịch vụ đám mây bị cấu hình sai để triển khai mã độc và liên kết với các cuộc tấn công SCARLETEEL.

TeamTNT đang quét thông tin xác thực trên nhiều môi trường đám mây, bao gồm AWS, Azure và GCP. Đối tượng tấn công chọn các phiên bản Docker công khai để triển khai module nhân bản kiểu worm, đây là bước tiếp theo của chiến dịch tấn công trước đó đã nhằm vào Jupyter Notebook hồi tháng 12 năm 2022.

Có tới tám phiên bản của tập lệnh thu thập thông tin trái phép đã được phát hiện từ ngày 15/06/2023 đến 11/07/2023, cho thấy cuộc tấn công đang diễn ra một cách tích cực. Những phiên bản mới này ra đời nhằm thu thập thông tin trái phép từ các dịch vụ như AWS, Azure, Google Cloud Platform, Censys, Docker, Filezilla, Git, Grafana, Kubernetes, Linux, Ngrok, PostgreSQL, Redis, S3QL và SMB. Thông tin đăng nhập bị đánh cắp sau đó được chuyển đến máy chủ từ xa.

**Sự kết nối mật thiết giữa SCARLETEEL và TeamTNT**

Một số nhà nghiên cứu bảo mật cho rằng kỹ thuật tấn công của SCARLETEEL có nhiều điểm tương đồng với các chiến dịch của TeamTNT. Chiến dịch SilentBob của TeamTNT thường chiếm quyền truy cập, đánh cắp thông tin đăng nhập trái phép, xâm nhập vào các hệ thống được kết nối. Tương tự, SCARLETEEL đánh cắp thông tin đăng nhập từ các tệp cấu hình Terraform, cũng như SilentBob.

Mặc dù SCARLETEEL và TeamTNT có điểm giống nhau về cơ sở hạ tầng được sử dụng nhưng cũng có một số điểm khác biệt về chiến thuật, kỹ thuật và quy trình TTPs, đặc biệt là việc sử dụng endpoint AWS tùy chỉnh.

Bởi vậy, các cơ quan, tổ chức cần tiến hành rà soát để áp dụng kịp thời các biện pháp bảo mật phù hợp.

Nguồn: https://thehackernews.com/2023/07/teamtnts-cloud-credential-stealing.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 **912** lỗ hổng, trong đó có 210 lỗ hổng mức Cao, 170 lỗ hổng mức Trung bình, 05 lỗ hổng mức Thấp và 527 lỗ hổng chưa đánh giá. Trong đó có ít nhất 119 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 135 lỗ hổng trong Microsoft, Nhóm 07 lỗ hổng trong Linux, Nhóm 28 lỗ hổng trong Google, Nhóm 130 lỗ hổng trong Wordpress, Nhóm 20 lỗ hổng trong Adobe, Nhóm 03 lỗ hổng trong Cisco, Nhóm 19 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:***

- *Microsoft: CVE-2023-29347, CVE-2023-32043,...*
- *Linux: CVE-2023-3106, CVE-2023-3108,...*
- *Google: CVE-2023-21246, CVE-2023-21247,...*
- *Wordpress: CVE-2020-36757, CVE-2020-36760,...*
- *Adobe: CVE-2023-29315, CVE-2023-29316,...*
- *Cisco: CVE-2023-20207, CVE-2023-20210,...*
- *IBM: CVE-2023-27867, CVE-2023-27868,...*

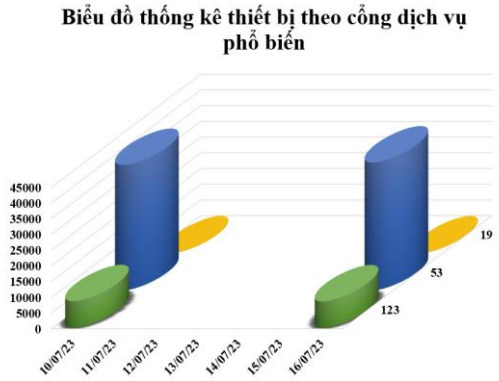
# Thông tin điểm yếu, lỗ hổng

| TT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| **1** | Microsoft | CVE-2023-35332<br>CVE-2023-32043<br>CVE-2023-29347<br>… | Nhóm 135 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền, làm rỏ rỉ thông tin dữ liệu, thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), truy cập và thực hiện các hành động trái phép. | Đã có thông tin xác nhận và bản vá |
| **2** | Linux | CVE-2023-3106<br>CVE-2023-3108<br>CVE-2023-32250<br>… | Nhóm 07 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép. | Đã có thông tin xác nhận và bản vá |
| **3** | Google | CVE-2023-21246<br>CVE-2023-21247<br>CVE-2023-21248<br>… | Nhóm 28 lỗ hổng trong Google (Android) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép. | Chưa có thông tin xác nhận và bản vá |
| **4** | Wordpress | CVE-2020-36761<br>CVE-2020-36760<br>CVE-2020-36757<br>… | Nhóm 130 lỗ hổng trong Wordpress cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép. | Đã có thông tin xác nhận và bản vá |
| **5** | Adobe | CVE-2023-29315<br>CVE-2023-29316<br>CVE-2023-29317<br>… | Nhóm 20 lỗ hổng trong Adobe 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-2023-20207<br>CVE-2023-20210<br>CVE-2023-20185 | Nhóm 03 lỗ hổng trong Cisco 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 |
| **7** | IBM | CVE-2023-27867<br>CVE-2023-27868<br>CVE-2023-27869<br>… | Nhóm 19 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép. | Chưa có thông tin xác nhận và bản vá |

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

## Tấn công DRDoS

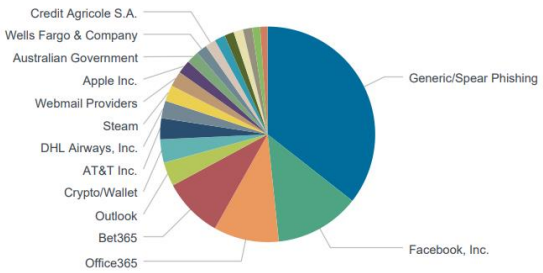
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **49.275,** (tăng so với tuần trước **48.557**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 545 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 521 trường hợp tấn công lừa đảo (Phishing), 24 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: 10914 IP | xjpakmdcfuqe.ru: 74 IP |
| disorderstatus.ru: 2787 IP | xjpakmdcfuqe.in: 39 IP |
| atomictrivia.ru: 1287 IP | restlesz.su: 288 IP |
| xjpakmdcfuqe.biz: 354 IP | amnsreiuojy.ru: 374 IP |
| xjpakmdcfuqe.com: 123 IP | hzmksreiuojy.ru: 32 IP |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **336** 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 | dienmayxanhsuachua.life<br>dienmayxanh-hcm.com<br>dienmayxanh268.com | Website giả Điện máy xanh |
| 2 | shopelnie.com<br>vn119shop.com<br>shopee.sootoou.com<br>timx2918.com<br>vn335shop.com<br>vn277shop.com | Website giả mạo sàn TMĐT Shopee |
| 3 | tikia.vip<br>tk9998.com<br>vntkm.com | Website giả mạo sàn TMĐT Tiki |
| 4 | dichvucongbaohiemxahoi.com<br>dangkyhosotructuyen2023.com<br>handico.vaytienmat-nhanh24h.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 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