NCSC VN
National Cyber Security Center

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

# CẢNH BÁO TUẦN

**Số 17 (22/04/2024 – 28/04/2024)**

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công ToddyCat sử dụng công cụ nâng cao nhằm đánh cắp dữ liệu.

- **Cảnh báo:** Lỗ hổng trên plugin WP-Automatic bị khai thác để tạo tài khoản Admin trên các trang WordPress.

- **Cảnh báo**: Chiến dịch tấn công mạng ArcaneDoor ảnh hưởng đến các thiết bị mạng Cisco.

## 2. Điểm yếu, lỗ hổng.

- TOP **10** lỗ hổng đáng chú ý trong tuần.

## 3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 293** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

## 4. Tài liệu lưu trữ

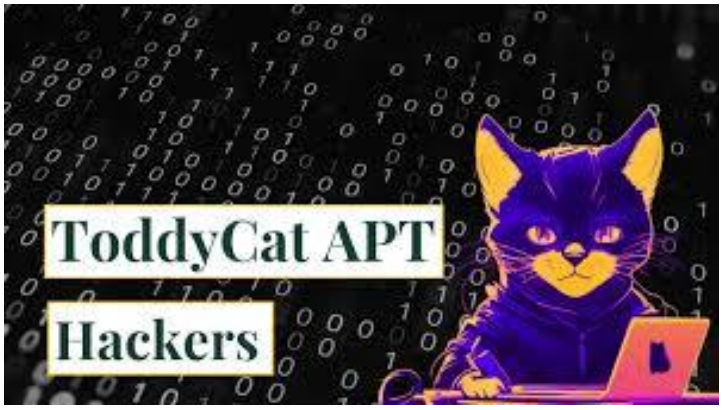
Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Chiến dịch tấn công APT: Nhóm tấn công ToddyCat sử dụng công cụ nâng cao nhằm đánh cắp dữ liệu."




Nhóm tấn công ToddyCat đã bị phát hiện khi họ sử dụng một loạt công cụ để xâm nhập vào môi trường hệ thống người dùng và đánh cắp dữ liệu quan trọng. Các cơ quan bảo mật cho biết rằng nhóm này đã sử dụng nhiều công cụ khác nhau để thu thập dữ liệu quy mô lớn từ các tổ chức chính phủ và quốc phòng ở khu vực Châu Á Thái Bình Dương.

Nhóm ToddyCat được phát hiện lần đầu vào tháng 06/2022 khi họ tiến hành hàng loạt cuộc tấn công vào các tổ chức chính phủ và quân đội ở Châu Âu và Châu Á. Cuộc tấn công bắt đầu từ tháng 12/2020 và tiếp diễn trong một khoảng thời gian dài. Trong chiến dịch này, nhóm ToddyCat đã sử dụng một loại backdoor thụ động được gọi là Samurai, cho phép họ kiểm soát từ xa các hệ thống bị nhiễm mã độc.

Sau khi phân tích kỹ về hoạt động của nhóm ToddyCat, đã phát hiện nhóm này sử dụng một số công cụ như LoFiSe và Pcexter để trích xuất dữ liệu và đưa lên Microsoft OneDrive. Trong chiến dịch tấn công mới nhất, ToddyCat đã mở rộng danh mục công cụ bằng cách thêm vào phần mềm thu thập dữ liệu thông qua các kênh tunnel. Thường thì điều này xảy ra sau khi nhóm này đã có quyền truy cập vào các tài khoản có đặc quyền trên hệ thống. Các công cụ và kỹ thuật này bao gồm:

- Reverse SSH tunnel sử dụng OpenSSH
- SoftEther VPN, được đặt lại tên file thành "boot.exe," "mstime.exe," "netscan.exe," and "kaspersky.exe"
- Ngrok và Krong dùng để mã hóa và điều hướng lưu lượng của C&C tới cổng chỉ định trên hệ thống.
- FRP client, một reverse proxy tốc độ cao được viết bằng Golang
- Cuthead, một file thực thi .NET có mục đích dò tìm văn bản có định dạng file hoặc tên file khớp yêu cầu đặt ra; hoặc dựa trên thời gian file này được sửa đổi.

Nguồn: https://thehackernews.com/2024/04/russian-hacker-group-toddycat-uses.html

# Tin tức An toàn thông tin

## "Chiến dịch tấn công APT: Nhóm tấn công ToddyCat sử dụng công cụ nâng cao nhằm đánh cắp dữ liệu."

- WAExp, chương trình .NET dùng để thu thập dữ liệu của ứng dụng WhatsApp rồi lưu lại thành file nén.
- TomBerBil để trích xuất cookies và thông tin xác thực từ trình duyệt web Chrome, Edge.

Nhóm tấn công duy trì nhiều kết nối đến cùng một thiết bị bị nhiễm mã độc, tất cả đều kết nối đến hạ tầng C&C được điều khiển bởi đối tượng. Họ sử dụng các công cụ khác nhau như biện pháp dự phòng để luôn duy trì kết nối, trong trường hợp một trong các tunnel này bị phát hiện và ngừng hoạt động.

Chuyên gia bảo mật khuyến nghị rằng người quản trị nên sử dụng tường lửa để chặn tài nguyên và địa chỉ IP của các dịch vụ Cloud có khả năng tạo tunnel lưu lượng. Ngoài ra, người dùng cũng nên tránh lưu mật khẩu trên trình duyệt web để tăng cường an ninh cho hạ tầng của tổ chức.

**Một số IoC được ghi nhận:**

103.27.202[.]85

118.193.40[.]42

Ha[.]bbmouseme[.]com

Nguồn: https://thehackernews.com/2024/04/russian-hacker-group-toddycat-uses.html

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Cảnh báo: Lỗ hổng trên plugin WP-Automatic bị khai thác để tạo tài khoản Admin trên các trang WordPress."


Một số đối tượng tấn công đang khai thác một lỗ hổng an toàn thông tin nghiêm trọng nhằm vào plugin ValvePress Automatic trên WordPress để chiếm quyền kiểm soát các trang web. Lỗ hổng có mã CVE-2024-27956 (Điểm CVSS: 9.9 – Nghiêm trọng) gây ảnh hưởng cho tất cả phiên bản plugin cũ hơn 3.92.0. Hiện lỗ hổng này đã được vá trong phiên bản 3.92.1 của plugin được phát hành vào 27/02/2024, tuy nhiên, thông tin không được ghi lại trong nội dung bản vá. Đây là lỗi SQL Injection cho phép đối tượng tấn công chiếm quyền kiểm soát website bằng cách tạo tài khoản có quyền hạn admin, tải lên các file độc hại và có thể qua đó toàn quyền kiểm soát website.

Lỗ hổng này tồn tại do cơ chế xác thực người dùng của plugin có thể bị phá vỡ một cách đơn giản để thực thi các truy vấn SQL lên cơ sở dữ liệu lưu trữ website bằng các yêu cầu được nhập vào.

Trong các cuộc tấn công sử dụng lỗ hổng CVE-2024-27956, đối tượng tấn công sử dụng lỗ hổng này để thực hiện các hành vi độc hại trên các trang web WordPress. Các đối tượng này có thể thực hiện các truy vấn trái phép trên cơ sở dữ liệu và tạo tài khoản admin trên các trang WordPress. Họ cũng có thể cài đặt các plugin độc hại hoặc chỉnh sửa mã nguồn để gây hại cho trang web.

Một cách phổ biến để tránh bị phát hiện là đổi tên các tệp tin bị ảnh hưởng. Ví dụ, tệp tin "/wp-content/plugins/wp-automatic/inc/csv.php" có thể được đổi tên thành "/wp-content/plugins/wp-automatic/inc/csv65f82ab408b3.php". Hành động này cũng có thể được thực hiện để tránh sự can thiệp từ các đối tượng tấn công khác.

Nguồn: https://thehackernews.com/2024/04/hackers-exploiting-wp-automatic-plugin.html

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Cảnh báo: Lỗ hổng trên plugin WP-Automatic bị khai thác để tạo tài khoản Admin trên các trang WordPress."

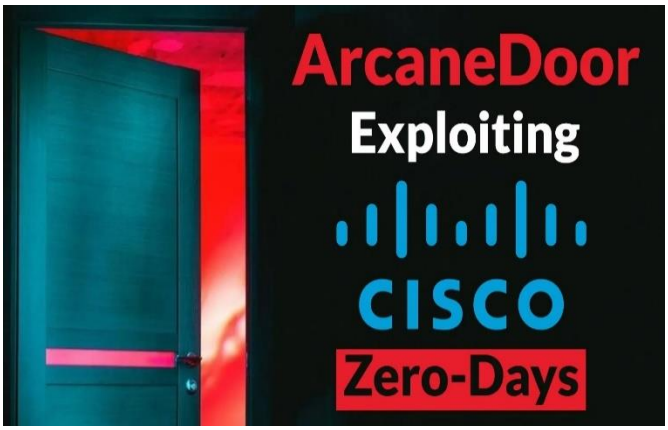
Lỗ hổng CVE-2024-27956 đã được WordPress công bố chi tiết vào ngày 13/03/2024, và từ đó đã ghi nhận hơn 5,5 triệu lần thử tấn công sử dụng lỗ hổng này trong thực tế. Việc tiết lộ về việc khai thác lỗ hổng này diễn ra trong bối cảnh nhiều lỗ hổng an toàn thông tin khác cũng đã được công bố chi tiết trên các plugin khác như Email Subcriber của Icegram Express (CVE-2024-2876 – Điểm CVSS: 9.8); Forminator (CVE-2024-28890 – Điểm CVSS: 9.8); và User Registration (CVE-2024-2417 – Điểm CVSS: 8.8), có khả năng bị lợi dụng để trích xuất dữ liệu quan trọng từ cơ sở dữ liệu, tải lên các file tự do, và cấp quyền admin cho tài khoản người dùng đã được xác thực.

Đồng thời, lỗ hổng CVE-2024-32514 (Điểm CVSS: 9.9) cũng được công bố bởi WordPress. Lỗ hổng này tồn tại trên plugin Poll Maker cho phép đối tượng tấn công với quyền truy cập subscriber hoặc cao hơn có thể tải lên file tùy ý vào máy chủ, qua đó cho phép đối tượng tấn công thực thi mã từ xa. Hiện lỗ hổng này vẫn chưa được vá.

Nguồn: https://thehackernews.com/2024/04/hackers-exploiting-wp-automatic-plugin.html

# Tin tức An toàn thông tin

## "Cảnh báo: Chiến dịch tấn công mạng ArcaneDoor ảnh hưởng đến các thiết bị mạng Cisco."




Chiến dịch tấn công mạng ArcaneDoor ảnh hưởng đến các thiết bị mạng Cisco. Khi truy cập được vào các thiết bị này, đối tượng tấn công có thể điều hướng lại hoặc điều chỉnh lưu lượng mạng, theo dõi liên lạc trong mạng lưới và thực hiện hành động trái phép.

Trong thời gian vừa qua, đã cho thấy sự gia tăng của các chiến dịch tấn công nhằm vào thiết bị mạng trong lĩnh vực cung cấp dịch vụ viễn thông và tổ chức năng lượng. Vào đầu năm 2024, trong một cuộc điều tra phân tích đã phát hiện được một nhóm tấn công mới hiện đang được theo dõi dưới tên UAT4356 bởi Talos và STORM-1849 bởi Microsoft Threat Intelligence Center.

Được biết UAT4356 đã triển khai hai backdoor trong chiến dịch lần này, có tên "Line Runner" và "Line Dance", cả hai được sử dụng để thực hiện các hành vi độc hại lên thiết bị bị ảnh hưởng, bao gồm: điều chỉnh cấu hình, do thám, theo dõi/trích xuất lưu lượng mạng và leo thang đặc quyền.

Thông qua quá trình điều tra phân tích, các nhà phân tích thấy rằng các nhóm tấn công thường triển khai mã độc, thực thi mã từ xa trên thiết bị bị ảnh hưởng. Hai lỗ hổng bị khai thác gồm có:

- **CVE-2024-20353 (Điểm CVSS: 8.6 – Cao)** tồn tại trên Cisco Adaptive Security Appliance (ASA) Software và Cisco Firepower Threat Defense (FTD) Software cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.
- **CVE-2024-20359 (Điểm CVSS: 6.0 -Trung bình)** tồn tại trên Cisco Adaptive Security Appliance (ASA) Software và Cisco Firepower Threat Defense (FTD) Software cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền root.

Nguồn: https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

# Tin tức An toàn thông tin

## "Cảnh báo: Chiến dịch tấn công mạng ArcaneDoor ảnh hưởng đến các thiết bị mạng Cisco."

**Dưới đây là một số IoC được ghi nhận**

| | |
|---|---|
| 192.36.57[.]181 | 185.167.60[.]85 |
| 185.227.111[.]17 | 176.31.18[.]153 |
| 172.105.90[.]154 | 185.244.210[.]120 |
| 45.86.163[.]224 | 172.105.94[.]93 |
| 213.156.138[.]77 | 89.44.198[.]189 |
| 45.77.52[.]253 | 103.114.200[.]230 |
| 212.193.2[.]48 | 51.15.145[.]37 |
| 89.44.198[.]196 | 131.196.252[.]148 |
| 213.156.138[.]78 | 121.227.168[.]69 |
| 213.156.138[.]68 | 194.4.49[.]6 |
| 185.244.210[.]65 | 216.238.75[.]155 |

Nguồn: https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

# 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 **529** lỗ hổng, trong đó có 160 lỗ hổng mức Cao, 193 lỗ hổng mức Trung bình, 20 lỗ hổng mức Thấp và 156 lỗ hổng chưa đánh giá. Trong đó có ít nhất 100 lỗ hổng cho phép chèn và thực thi mã lệnh.


Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm trọng cao hoặc đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

Trong đó, đáng chú ý có 03 lỗ hổng ảnh hưởng tới các sản phẩm của Cisco và CrushFTP, cụ thể như sau:

- CVE-2024-20359 (**Điểm CVSS: 6.0 – Trung bình**): Lỗ hổng an toàn thông tin tồn tại trên phần mềm Cisco Adaptive Security Appliance (ASA) và Cisco Firepower Threat Defense (FTD) cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền root. Lỗ hổng tồn tại do quá trình xác thực file sai cách khi file được đọc từ bộ nhớ flash của hệ thống. Đối tượng tấn công có thể khai thác lỗ hổng này bằng cách copy file độc hại, được tạo trước vào disk0: của thiết bị. Qua đó cho phép đối tượng thực thi mã tùy ý kể cả sau khi thiết bị được khởi động lại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- CVE-2024-20353 (**Điểm CVSS: 8.6 – Cao**): Lỗ hổng an toàn thông tin tồn tại trên phần mềm Cisco Adaptive Security Appliance (ASA) và Cisco Firepower Threat Defense (FTD) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. Lỗ hổng tồn tại do quy trình kiểm tra lỗi thiếu hoàn thiện khi thiết bị duyệt một HTTP header. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- CVE-2024-4040 (**Điểm CVSS:10 – Nghiêm trọng**): Lỗ hổng chèn template tồn tại bên phía máy chủ trên CrushFTP phiên bản trước 10.7.1 và 11.1.0 trên mọi nền tảng cho phép đối tượng tấn công đọc file từ filesystem nằm ngoài VFS Sandbox, bỏ qua biện pháp xác thực để đạt được quyền quản trị và thực thi mã từ xa trên máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

# TOP 10 lỗ hổng đáng chú ý trong tuần

| TT | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|
| 1 | CVE-2024-20359 | - Điểm CVSS: 6.0 (Trung bình)<br>- Ảnh hưởng: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD)<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý trên hệ thống bị ảnh hưởng.<br>- Lỗ hổng đã có mã khai thác đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-20359 |
| 2 | CVE-2024-20353 | - Điểm CVSS: 8.6 (Cao)<br>- Ảnh hưởng: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD)<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-20353 |
| 3 | CVE-2024-4040 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: CrushFTP<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-4040 |
| 4 | CVE-2024-21345 | - Điểm CVSS: 8.8 (Cao)<br>- Ảnh hưởng: Windows Server 2022<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-21345 |
| 5 | CVE-2024-21111 | - Điểm CVSS: 7.8 (Cao)<br>- Ảnh hưởng: Oracle VM VirtualBox<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.<br>- Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-21111 |

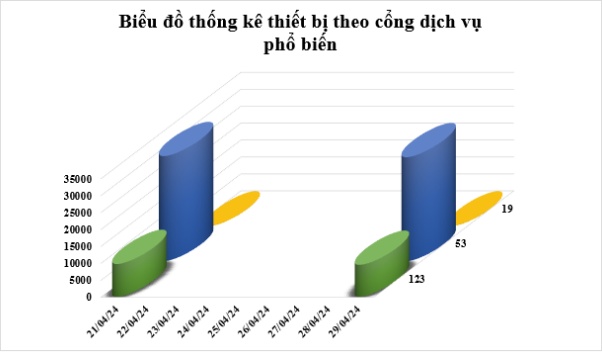
# TOP 10 lỗ hổng đáng chú ý trong tuần

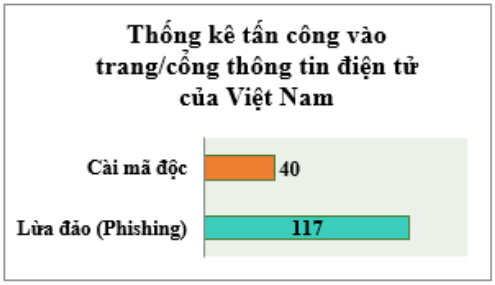
| TT | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|
| 6 | CVE-2024-21762 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Fortinet FortiOS, FortiProxy<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-21762 |
| 7 | CVE-2024-26218 | - Điểm CVSS: 7.8 (Cao)<br>- Ảnh hưởng: Windows<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-26218 |
| 8 | CVE-2024-3094 | - Điểm CVSS: 10.0 (Nghiêm trọng)<br>- Ảnh hưởng: Tukaani XZ<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế. | https://nvd.nist.gov/vuln/detail/CVE-2024-3094 |
| 9 | CVE-2024-27956 | - Điểm CVSS: 9.9 (Nghiêm trọng)<br>- Ảnh hưởng: ValvePress Automatic plugin trên WordPress.<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công SQL Injection.<br>- Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-27956 |
| 10 | CVE-2024-3400 | - Điểm CVSS: 10 (Nghiêm trọng)<br>- Ảnh hưởng: Palo Alto Networks PAN-OS<br>- Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa.<br>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công. | https://nvd.nist.gov/vuln/detail/CVE-2024-3400 |

# 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 **40.172** (giảm so với tuần trước **40.763**) 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.



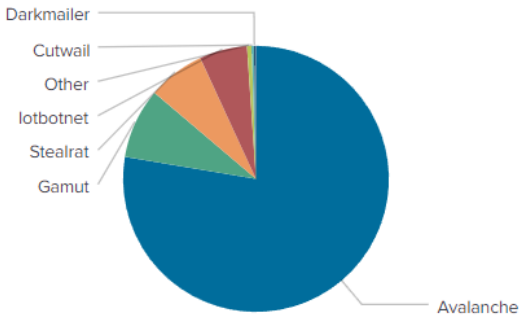




## Tấn công Web

Trong tuần, có **157** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 117 trường hợp tấn công lừa đảo (Phishing), 40 trường hợp tấn công cài cắm mã độc.

## Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.




### Địa chỉ được sử dụng trong các mạng botnet

| | |
|---|---|
| differentia.ru | restless.su |
| disorderstatus.ru | andall.servicesql.info |
| atomictrivia.ru | imageshells.com |
| amnsreiuojy.ru | facialwaxmaxfaxlax3.com |
| restlesz.su | db2017417b23.zapto.org |
| hzmksreiuojy.ru | uyhgqunqkxnx.pw |
| xjpakmdcfuqe.com | mildwave.com |
| xjpakmdcfuqe.biz | focusdate.com |
| xjpakmdcfuqe.ru | www.csbtd.com |
| xjpakmdcfuqe.in | wwgfyvvdtmeq.pw |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **293** 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 các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

| STT | Website lừa đảo | Ghi chú |
|---|---|---|
| 1 | https://homecreditvn[.]net | Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam |
| 2 | http://dichvucong[.]hhghv.com/ | Website giả mạo Dịch vụ công Quốc Gia |
| 3 | https://dichvucong[.]hhlpa.com/ | Website giả mạo Dịch vụ công Quốc Gia |
| 4 | https://dienmayxanh542[.]com | Website giả mạo Điện máy xanh |
| 5 | https://dich-vu-dien-mayxanh[.]com | Website giả mạo Điện máy xanh |
| 6 | https://lazd8[.]com | Website giả mạo sàn TMĐT Lazada |
| 7 | https://finacehoisomb[.]com | Website giả mạo Ngân hàng TMCP Quân đội |
| 8 | https://mbdkb[.]com | Website giả mạo Ngân hàng TMCP Quân đội |
| 9 | https://khoi-khach-hang-ca-nhan-vni-diamon[.]com | Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam |
| 10 | http://vib.tanghanmuc-vn[.]com | Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam |
| 11 | http://vib.hanmucvn[.]com | Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam |
| 12 | http://mail.labtpb[.]online | Website giả mạo Ngân hàng TMCP Tiên Phong |
| 13 | https://canhantpb[.]com | Website giả mạo Ngân hàng TMCP Tiên Phong |
| 14 | https://vpb.tanghanmucvisa-vn[.]com | Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng |
| 15 | http://vpb.tang-han-muc-the-visa-vn[.]com | Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng |
| 16 | https://shinhan.chamsocthekhachhang-thang4[.]online | Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam |
| 17 | https://vnsendo[.]shop/ | Website giả mạo sàn TMĐT Sendo |
| 18 | https://investshopeemall[.]net/ | Website giả mạo sàn TMĐT Shopee |
| 19 | https://sp56788[.]com/ | Website giả mạo sàn TMĐT Shopee |
| 20 | https://tdkd08[.]com/ | Website giả mạo sàn TMĐT Tiki |

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, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

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**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

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