NCSC VN
National Cyber Security Center

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

# CẢNH BÁO TUẦN

**Số 01 (30/12/2024 – 05/01/2025)**

# NỘI DUNG TUẦN

## 1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Ghi nhận nhóm tấn công thuộc Triều Tiên triển khai mã độc OtterCookie trong chiến dịch tấn công "Contagious Interview".

- **Cảnh báo:** Ghi nhận phương thức tấn công "DoubleClickjacking" bỏ qua bảo mật Clickjacking trên website.

## 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: 6.685** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

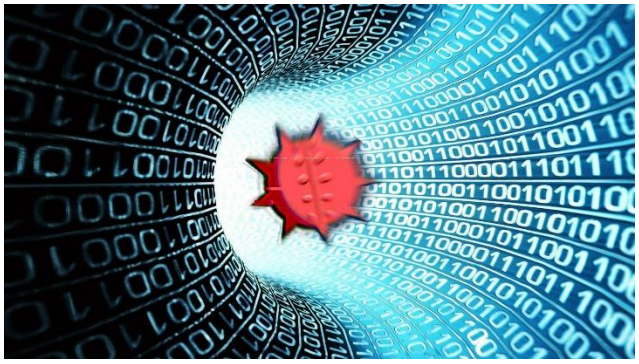
## 4. Tài liệu lưu trữ

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

https://khonggianmang.vn

# Tin tức An toàn thông tin

## "Chiến dịch tấn công APT: Ghi nhận nhóm tấn công thuộc Triều Tiên triển khai mã độc OtterCookie trong chiến dịch tấn công "Contagious Interview""



Nhóm đối tượng tấn công thuộc Triều Tiên đằng sau chiến dịch tấn công "Contagious Interview" gần đây đã được quan sát thấy trong lúc phát tán mã độc JavaScript có tên OtterCookie.

Chiến dịch tấn công còn có tên khác là DeceptiveDevelopment sử dụng kỹ thuật social engineering với nhóm đối tượng giả danh thành các nhân viên tuyển dụng để lừa người dùng đang tìm kiếm việc làm tải xuống mã độc như một bước trong quá trình phỏng vấn.

Các mã độc được cài vào trong gói npm hoặc ứng dụng họp video được lưu trên GitHub hoặc registry chính thức của gói, qua đó cho phép đối tượng phát tán mã độc như BeaverTail và InvisibleFerret. Hiện nhóm tấn công này đang được theo dõi dưới tên CL-STA-0240.

Vào tháng 09/2024, cơ quan bảo mật Group-IB đã công bố thông tin chi tiết về chuỗi tấn công, nhằm tô điểm việc sử dụng phiên bản cải tiến của BeaverTail có tính module bằng cách tách rời chức năng đánh cắp dữ liệu của mã độc ra một bộ script Python có tên CivetQ.

Đáng chú ý, chiến dịch Contagious Interview hiện đang được cho là tách biệt với chiến dịch "Operation Dream Job", cũng là một chiến dịch tấn công thực hiện bởi nhóm tấn công Triều Tiên với cùng phương thức lây nhiễm thông qua các mồi nhử liên quan tới việc làm.

Ngoài ra, trong phát hiện mới nhất, mã độc JavaScript được sử dụng để thực thi BeaverTail còn có chức năng tải xuống và thức thi mã độc OtterCookie, được phát hiện vào tháng 09/2024 và có phiên bản mới hơn vào tháng 11/2024.

Mã độc OtterCookie khi được thực thi sẽ kết nối tới máy chủ C&C thông qua thư viện JavaScript "Socket.IO", sau đó sẽ chờ chỉ thị mới.

Nguồn: https://thehackernews.com/2024/12/north-korean-hackers-deploy-ottercookie.html

# Tin tức An toàn thông tin

## “Chiến dịch tấn công APT: Ghi nhận nhóm tấn công thuộc Triều Tiên triển khai mã độc OtterCookie trong chiến dịch tấn công “Contagious Interview””

Mã độc được thiết kế để thực thi các câu lệnh shell có nhiệm vụ đánh cắp dữ liệu như file, nội dung trong clipboard và khóa ví tiền ảo.

Chiến dịch tấn công này được công bố trong bối cảnh các nhóm tấn công đang gia tăng nỗ lực cập nhật bộ công cụ sử dụng mà vẫn giữ lại chuỗi tấn công, điều này chứng tỏ chiến dịch tấn công có tính hiệu quả cao.

**Một số IoC được ghi nhận:**

| | |
|---|---|
| 45[.]159.248.55 | zkservice[.]cloud |
| w3capi[.]marketing | payloadrpc[.]com |

Nguồn: https://thehackernews.com/2024/12/north-korean-hackers-deploy-ottercookie.html

NCSC VN
National Cyber Security Center

# Tin tức An toàn thông tin

## "Cảnh báo: Ghi nhận phương thức tấn công "DoubleClickjacking" bỏ qua bảo mật Clickjacking trên website"


Gần đây, các chuyên gia bảo mật đã ghi nhận và công bố chi tiết của một lớp lỗ hổng dựa trên thời gian phổ biến sử dụng trình tự double-click để thực hiện tấn công clickjacking và chiếm dụng tài khoản trên các website.

Kỹ thuật này hiện được đặt tên là DoubleClickjacking. Cụ thể, thay vì dựa vào một lần click, kỹ thuật sử dụng trình tự double-click cho phép thao túng UI để vượt qua các biện pháp bảo mật clickjacking hiện có, bao gồm cả header X-Frame-Options hay cookie SameSite: Lax/Strict. Kỹ thuật tấn công Clickjacking, hay còn gọi là chỉnh sửa UI, là một kỹ thuật trong đó người dùng bị lừa vào việc bấm vào một yếu tố trông như an toàn trên website (thường là nút xác nhận), từ đó dẫn tới việc triển khai mã độc trên hệ thống hoặc trích xuất dữ liệu quan trọng.

Kỹ thuật DoubleClickjacking là một biến thể khai thác khoảng thời gian giữa lúc bắt đầu của lần click và kết thúc của lần click thứ 2 để vượt qua biện pháp bảo mật và chiếm dụng tài khoản của người dùng. Cụ thể các bước như sau:

- Người dùng truy cập vào trang web điều khiển bởi đối tượng tấn công có luồng hoạt động là mở lên một cửa sổ browser hoặc một tab mới mà không cần người dùng tương tác, hoặc chỉ cần một lần click chuột.
- Cửa sổ (tab) mới này có thể giả dạng thành một xác thức Captcha, yêu cầu người dùng click 2 lần để hoàn thành chúng.
- Khi người dùng thực hiện điều này, trang web độc hại sử dụng đối tượng trên JavaScript là "Window Location" để điều hướng người dùng tới trang độc hại.
- Cửa sổ trên cùng sẽ được đóng, qua đó người dùng đã vô tình cấp quyền truy cập cho đối tượng bằng cách đồng ý với thông báo cấp quyền trên trang chính.

Nguồn: https://thehackernews.com/2025/01/new-doubleclickjacking-exploit-bypasses.html

# Tin tức An toàn thông tin

## "Cảnh báo: Ghi nhận phương thức tấn công "DoubleClickjacking" bỏ qua bảo mật Clickjacking trên website"

Được biết, lỗ hổng và kỹ thuật này có thể bị loại bỏ bằng cách sử dụng giải pháp client-side cho phép tắt chức năng của các nút quan trọng trên website trừ khi di chuột theo một cách nhất định hoặc khi người dùng bấm nút trên bàn phím.

Thông tin về kỹ thuật này được công bố gần một năm sau khi một chuyên gia bảo mật đã chứng minh một biến thể khác của Clickjacking có tên "Cross window forgery" (hay gesture-jacking) hoạt động dựa trên việc người dùng bấm hoặc giữ nút Enter/Space trên một trang web độc hại để thực hiện các tác vụ độc hại như chiếm dụng tài khoản trên website đó.

Nguồn: https://thehackernews.com/2025/01/new-doubleclickjacking-exploit-bypasses.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 **524** lỗ hổng, trong đó có 143 lỗ hổng mức Cao, 299 lỗ hổng mức Trung bình, 24 lỗ hổng mức Thấp và 58 lỗ hổng chưa đánh giá. Trong đó có ít nhất 47 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 các sản phẩm của Four-Faiths, Palo Alto Networks và Microsoft, cụ thể là như sau:

- **CVE-2024-3393 (Điểm CVSS: 8.7 – Cao)**: Lỗ hổng tồn tại trên chức năng DNS Security của phần mềm Palo Alto Networks PAN-OS cho phép đối tượng tấn công sử dụng các gói tin độc hại để thực hiện tấn công từ chối dịch vụ bằng cách khiến tường lửa khởi động lại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

- **CVE-2024-12856 (Điểm CVSS: 7.2 – Cao)**: Lỗ hổng tồn tại trên router mẫu F3x24 và F3x36 của hãng Four-Faiths. Là lỗi command injection cho phép đối tượng tấn công thực thi lệnh OS tùy ý qua giao thức HTTP khi điều chỉnh thời gian hệ thống trên file apply.cgi. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.

- **CVE-2018-0802 (Điểm CVSS: 7.8 – Cao)**: Lỗ hổng tồn tại trên Microsoft Office 2007, 2010, 2013, 2016 trên thành phần Equation Editor do sai sót trong quá trình xử lý đối tượng trên bộ nhớ. Đối tượng tấn công khai thác lỗ hổng có thể thực thi mã từ xa. 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-2024-3393 | - Điểm CVSS: 8.7 (Cao)<br>- Ảnh hưởng: Palo Alto Networks PAN-OS<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ<br>- Lỗ hổng chưa 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-2024-3393 |
| 2 | CVE-2024-12856 | - Điểm CVSS: 7.2 (Cao)<br>- Ảnh hưởng: Route Four-Faith mẫu F3x24 và F3x36<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa<br>- Lỗ hổng chưa 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-2024-12856 |
| 3 | CVE-2018-0802 | - Điểm CVSS: 7.8 (Cao)<br>- Ảnh hưởng: Microsoft Office 2007, 2010, 2013, 2016<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-2018-0802 |
| 4 | CVE-2024-12356 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Privileged Remote Access (PRA) và Remote Support (RS) của hãng Beyondtrust.<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép<br>- Lỗ hổng chưa 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-2024-12356 |
| 5 | CVE-2024-50623 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Cleo Harmony, VLTrader, LexiCom<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-2024-50623 |

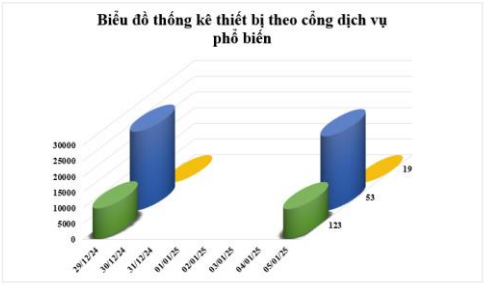
# TOP 10 lỗ hổng đáng chú ý trong tuần

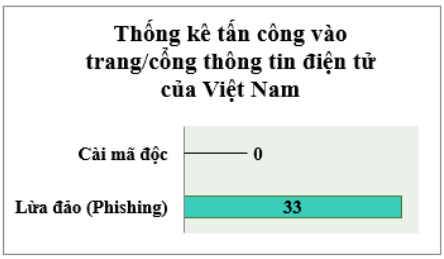
| TT | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|
| 6 | CVE-2024-45387 | - Điểm CVSS: 9.9 (Nghiêm trọng)<br>- Ảnh hưởng: Apache Traffic Control<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi SQL Injection<br>- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công | https://nvd.nist.gov/vuln/detail/CVE-2024-45387 |
| 7 | CVE-2024-50379 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Apache Tomcat<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-2024-50379 |
| 8 | CVE-2024-43441 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Apache HugeGraph-Server<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công bỏ qua biện pháp xác thực, truy cập và thực hiện các hành vi trái phép<br>- Lỗ hổng chưa 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-2024-43441 |
| 9 | CVE-2024-47575 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Ảnh hưởng: Fortinet FortiManager.<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-2024-47575 |
| 10 | CVE-2024-50945 | - Điểm CVSS: 7.5 (Cao)<br>- Ảnh hưởng: SimplCommerce<br>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép<br>- Lỗ hổng chưa 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-2024-50945 |

# 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 **33.165** (giảm so với tuần trước **34.860**) 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.



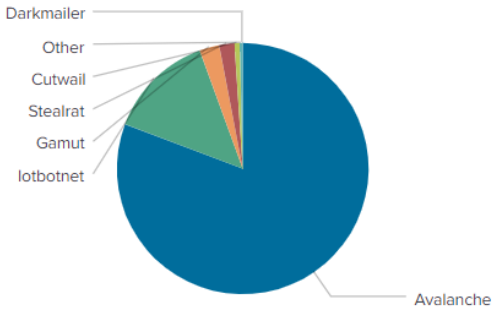




## Tấn công Web

Trong tuần, có **33** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 33 trường hợp tấn công lừa đảo (Phishing), 0 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

| | |
|---|---|
| disorderstatus.ru | b.deltaheavy.ru |
| differentia.ru | c.deltaheavy.ru |
| atomictrivia.ru | ydbnsrt.me |
| morphed.ru | soplifan.ru |
| thesecond.in | xjpakmdcfuqe.in |
| hzmksreiuojy.in | xjpakmdcfuqe.com |
| ygiudewsqhct.in | xjpakmdcfuqe.ru |
| a.deltaheavy.ru | cp.02dxbo9u.ru |
| xjpakmdcfuqe.biz | restless.su |
| devicesta.ru | svbmav.info |

# Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **6.685** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **213** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **6.472** trường hợp phản ánh cuộc gọi, tin nhắn lừa đảo thông qua tổng đài 156/5656

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

| STT | Website lừa đảo | Ghi chú |
|---|---|---|
| 1 | amazoni1[.]com/ | Website giả mạo sàn TMĐT Amazon |
| 2 | amazouo9[.]com | Website giả mạo sàn TMĐT Amazon |
| 3 | dichvucong[.]hokhauso[.]com/ | Website giả mạo Bộ Công An |
| 4 | Vietchinhphux[.]com | Website giả mạo Cổng Dịch vụ công Quốc gia |
| 5 | vnchinhphu[.]cc | Website giả mạo Cổng Dịch vụ công Quốc gia |
| 6 | giaohangtietkiem-express[.]com/ | Website giả mạo Công ty cổ phần giao hàng tiết kiệm |
| 7 | cucanninhmang24h[.]com/?gad_source=1&gclid=Cj0KCQiAyc67BhDSARIsAM95Qzs97Z8YMPy0mj-LRUFiVXcIBS4_SoL4JWQ7bHYdrtpEZdTKO2Jh6_AaAlXSEALw_wcB | Website giả mạo Cục An ninh mạng, Bộ Công an |
| 8 | csgt[.]dinhdanhpt[.]com | Website giả mạo Cục cảnh sát giao thông, Bộ Công An |
| 9 | baohanhdienmayxanh[.]vn/tho-dien-may-xanh-gioi-thieu-dich-vu-thay-loi-loc-nuoc-dung-chuan/ | Website giả mạo Điện máy xanh |
| 10 | dienlanhmayxanh[.]com/?gad_source=1&gclid=Cj0KCQiA7NO7BhDsARIsADg_hIbjU__x6wPykmUVIoLnSTew0wHZfe5OCAosfix0fNA7O5BQSz5tjGIaAhWKEALw_wcB | Website giả mạo Điện máy xanh |
| 11 | dienlanhmayxanh[.]com/sua-tu-lanh-tai-nha/ | Website giả mạo Điện máy xanh |
| 12 | Dienmayxanh452[.]com | Website giả mạo Điện máy xanh |
| 13 | vietcombank[.]asia/ | Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam |
| 14 | vietcombankvn[.]bm68[.]site/ | Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam |
| 15 | vay[.]giainganngа247[.]info/ | Website giả mạo Ngân hàng TMCP Quân đội |
| 16 | tc-shbfinance[.]com | Website giả mạo Ngân hàng TMCP Sài Gòn – Hà Nội |
| 17 | soppe68[.]org/account/login | Website giả mạo sàn TMĐT Shopee |
| 18 | www[.]shopeesallers[.]com/ | Website giả mạo sàn TMĐT Shopee |
| 19 | chinhphu[.]kbshkdt[.]org/ | Website giả mạo Văn phòng Chính phủ |
| 20 | chinhphu-vn[.]com | Website giả mạo Văn phòng Chính phủ |

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