NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 51 (16/12/2024 – 22/12/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Phát hiện nhóm UAC-0125 khai thác Cloudflare Workers để phát tán mã độc giả danh ứng dụng Army+.

- **Cảnh báo:** Ghi nhận lỗ hổng an toàn thông tin nghiêm trọng tồn tại trên Fortinet EMS cho phép đối tượng tấn công khai thác có thể triển khai các công cụ cho phép truy cập từ xa.

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: 6.227** 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: Phát hiện nhóm UAC-0125 khai thác Cloudflare Workers để phát tán mã độc giả danh ứng dụng Army+"

Gần đây, phía cơ quan CERT-UA thuộc Ukraine đã ghi nhận thông tin về nhóm đối tượng tấn công UAC-0125 đang khai thác dịch vụ Cloudflare Workers để đánh lừa các quân nhân của quốc gia này tải xuống mã độc giả danh ứng dụng Army+, một ứng dụng thuộc sở hữu của Bộ Quốc Phòng phát hành phục vụ mục tiêu số hóa quốc gia.

Người dùng khi truy cập vào các trang Cloudflare Workers giả mạo sẽ được yêu cầu tải xuống file thực thi của ứng dụng, file này tạo bởi Nullsoft Scriptable Install System (NSIS) là một công cụ mã nguồn mở dùng để tạo các bộ cài cho hệ điều hành.

Khi thực thi file, một file bù nhìn sẽ được mở lên cho người dùng, cùng lúc đó một đoạn script PowerShell có chức năng cài OpenSSH lên thiết bị, tạo cặp khóa RSA, bổ sung khóa công khai vừa tạo vào file "authorized_keys" rồi chuyển khóa bí mật tới máy chủ C&C thông qua mạng ẩn danh TOR.

Mục tiêu của chiến dịch này là đạt được quyền truy cập từ xa tới thiết bị, hệ thống của người dùng; hiện chưa rõ cách thức đường dẫn tới các website này được phát tán như nào.

Ngoài ra, cơ quan bảo mật cũng đã ghi nhận nhóm UAC-0125 có liên kết tới cụm UAC-0002 (hay APT44, FROZENBARENTS, Sandworm, Seashell Blizzard và Voodoo Bear) là một nhóm APT có liên kết với Unit 74455 hậu thuẫn bởi Nga. Đồng thời, trong tháng 12/2024, Fortra cũng đã ghi nhận xu hướng leo thang của việc lợi dụng các dịch vụ chính thống trong chiến dịch tấn công khai thác Cloudflare Workers và Pages để lưu các website đăng nhập Microsoft 365, xác thực captcha giả mạo nhằm mục đích đánh cắp thông tin xác thực của người dùng.

Xu hướng được ghi nhận chỉ ra việc tăng 198% về số lượng tấn công phishing nhằm vào Cloudflare Pages (tăng từ 460 lên tới 1.370); còn trên Cloudflare Workers đã tăng 40% (từ 2.447 lên tới 4.999).

Nguồn: https://thehackernews.com/2024/12/uac-0125-abuses-cloudflare-workers-to.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Phát hiện nhóm UAC-0125 khai thác Cloudflare Workers để phát tán mã độc giả danh ứng dụng Army+"

Thông tin về chiến dịch được công bố trong bối cảnh hội đồng Châu Âu đưa ra án phạt cho 16 cá nhân và 3 đơn vị thuộc Nga. Án phạt cũng nhằm Doppelganger, một mạng lưới tin giả thuộc Nga đưa tin về tình hình chiến sự giữa Nga – Ukraine.

Một số IoC được ghi nhận:

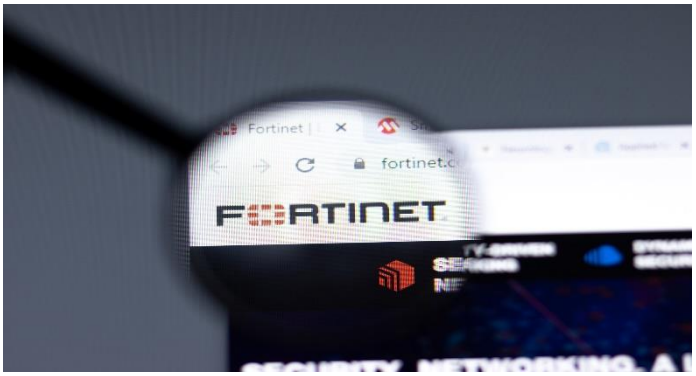
desktopapluscom.workers[.]dev	desktopaplus.workers[.]dev
armyplus-desktop.workers[.]dev	aplusdesktop.workers[.]dev
armylpus.workers[.]dev	aplusmodgovua.workers[.]dev
wvtmsouaa2gt6jmcuxj5hkfrqdss5lhecoqijt5dl7gfruueu3i5mkad[.]onion	0

Nguồn: https://thehackernews.com/2024/12/uac-0125-abuses-cloudflare-workers-to.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Ghi nhận lỗ hổng an toàn thông tin nghiêm trọng tồn tại trên Fortinet EMS cho phép đối tượng tấn công khai thác có thể triển khai các công cụ cho phép truy cập từ xa"



Gần đây, đã ghi nhận một lỗ hổng an toàn thông tin (hiện đã có bản vá) tồn tại trên Fortinet FortiClient EMS bị khai thác bởi các đối tượng tấn công trong chiến dịch tấn công với mục đích triển khai các phần mềm cho phép truy cập từ xa như AnyDesk và ScreenConnect.

Lỗ hổng có mã định danh CVE-2023-48788 (Điểm CVSS: 9.3), là lỗi SQL Injection cho phép đối tượng thực thi mã, câu lệnh độc hại mà không cần phải ủy quyền thông qua các gói dữ liệu độc hại được gửi tới giải pháp.

Việc khai thác trong chiến dịch được ghi nhận vào tháng 10/2024, nhằm vào một máy chủ Windows kết nối công cộng của một công ty, trong đó có 2 cổng đang mở phục vụ cho giải pháp FortiClient EMS.

Cụ thể, trong chiến dịch này, đối tượng tấn công đã khai thác lỗ hổng CVE-2023-48788 làm vector xâm nhập đầu vào, sau đó tiến hành cài đặt file thực thi của ScreenConnect để cho phép việc truy cập từ xa sau này tới thiết bị bị ảnh hưởng. Ngoài ra, đối tượng tấn công này còn tải lên các payload độc hại bổ sung để rà quét, lây lan tới các thiết bị cùng mạng thông qua việc liệt kê tài nguyên mạng, thu thập thông tin xác thực trong lúc né tránh phát hiện sử dụng các kỹ thuật chuyên dụng.

Một số công cụ đáng chú ý được phát tán gồm có:

- webbrowserpassview.exe, công cụ khôi phục mật khẩu làm lộ mật khẩu được lưu trên trình duyệt Internet Explorer (phiên bản 4.0 – 11.0), Mozilla Firefox (mọi phiên bản), Google Chrome, Safari và Opera;
- Mimikatz
- netpass64.exe, công cụ khôi phục mật khẩu;
- netscan.exe, công cụ rà quét mạng.

Nguồn: https://thehackernews.com/2024/12/hackers-exploiting-critical-fortinet.html

Tin tức An toàn thông tin

“Cảnh báo: Ghi nhận lỗ hổng an toàn thông tin nghiêm trọng tồn tại trên Fortinet EMS cho phép đối tượng tấn công khai thác có thể triển khai các công cụ cho phép truy cập từ xa”

Được biết, đối tượng đằng sau chiến dịch đã tấn công nhằm vào nhiều công ty tại các quốc gia như Brazil, Croatia, Pháp, Ấn Độ, Indonesia, Mông Cổ, Namibia, Peru, Tây Ban Nha, Thụy Sĩ, Thổ Nhĩ Kì và Các Tiểu vương quốc Ả Rập Thống nhất với các subdomain của ScreenConnect.

Vào ngày 23/10/2024, Kaspersky cũng đã ghi nhận nỗ lực khai thác lỗ hổng này một cách chuyên sâu hơn với việc thực thi script PowerShell lưu trên domain “webhook[.]site” để thu thập các gói tin phản hồi trả về từ các mục tiêu chịu ảnh hưởng của lỗ hổng này.

Thông tin về lỗ hổng trên giải pháp của Fortinet được công bố trong bối cảnh 8 tháng đã trôi qua kể từ khi một chiến dịch khác khai thác lỗ hổng được ghi nhận.

Nguồn: https://thehackernews.com/2024/12/hackers-exploiting-critical-fortinet.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 **668** lỗ hổng, trong đó có 300 lỗ hổng mức Cao, 263 lỗ hổng mức Trung bình, 14 lỗ hổng mức Thấp và 91 lỗ hổng chưa đánh giá. Trong đó có ít nhất 133 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 Windows và Apache, cụ thể là như sau:

- **CVE-2024-49138 (Điểm CVSS: 7.8 - Cao):** Lỗ hổng tồn tại trên Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-35250 (Điểm CVSS: 7.8 – Cao):** Lỗ hổng tồn tại trên Windows 10, Windows 11 tại thành phần Windows Kernel-Mode Driver, cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-53677 (Điểm CVSS: 9.5 – Nghiêm trọng):** Lỗ hổng tồn tại trên Apache Struts, đối tượng tấn công có thể thực thi mã từ xa thông qua việc khai thác lỗi tải lên file cho phép đối tượng khai thác lỗi path traversal và tải lên các file độc hại. 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-2024-49138	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - 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-2024-49138
2	CVE-2024-35250	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - 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-2024-35250
3	CVE-2024-53677	- Điểm CVSS: 9.5 (Nghiêm trọng) - Ảnh hưởng: Apache Struts - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - 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-2024-53677
4	CVE-2024-7479	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: TeamViewer Remote Clients - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - 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-2024-7479
5	CVE-2024-40725	- Điểm CVSS: 5.3 (Trung bình) - Ảnh hưởng: Apache HTTP Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - 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-2024-40725

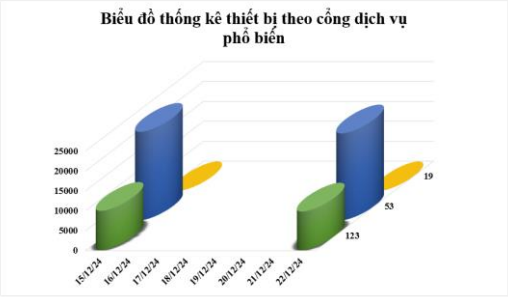
TOP 10 lỗ hổng đáng chú ý trong tuần

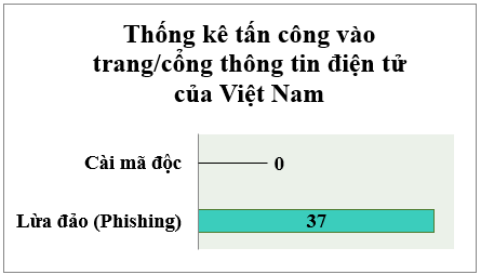
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-50379	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Apache Tomcat - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-50379
7	CVE-2024-50623	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Cleo Harmony, VLTrader và LexiCom - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - 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
8	CVE-2024-12356	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Privileged Remote Access (PRA) và Remote Support (RS) của hãng Beyondtrust - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi Command Injection. - 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
9	CVE-2024-12727	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Sophos Firewall - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - 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-2024-12727
10	CVE-2024-20767	- Điểm CVSS: 7.4 (Cao) - Ảnh hưởng: Adobe Cold Fusion - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - 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-2024-20767

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 **31.516** (giảm so với tuần trước **32.060**) 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.



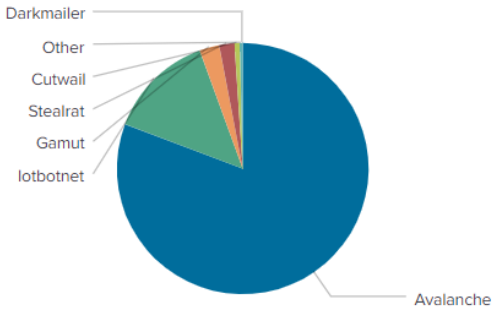


Tấn công Web

Trong tuần, có **37** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 37 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	ipjfhqda.info
differentia.ru	ygiudewsqhct.in
atomictrivia.ru	gjogvvpsf.biz
a.asense.in	hzmksreiuojy.in
sdk.asense.in	xjpakmdcfuqe.biz
thesecond.in	a.deltaheavy.ru
statis.multispacesext.net	hzmksreiuojy.ru
amnsreiuojy.ru	yunalwv.biz
cp.02dxbo9u.ru	restlesz.su
morphed.ru	b.deltaheavy.ru

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **6.227** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **227** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **6.000** 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	https://amazouo9[.]com/	Website giả mạo sàn TMĐT Amazon
2	https://dichvucong[.]hokhauso[.]com	Website giả mạo Bộ Công An
3	dichvucong[.]thongtincancuoc[.]org	Website giả mạo Bộ Công An
4	https://mofvn[.]com/	Website giả mạo Bộ Tài chính
5	dichvugiaohangtietkiemvn[.]store	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	https://giaohangtietkiem[.]com[.]vn/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
7	https://aeonmaills[.]shop	Website giả mạo Công ty TNHH Aeon Việt Nam
8	https://www[.]cuisin[.]sa[.]com/	Website giả mạo Cục An toàn thông tin, Bộ Thông tin và Truyền thông
9	https://cucanninhmang24h[.]com/?gad_source=1&gclid=CjwKCAiAyJS7BhBiEiwAyS9uNc-iPjBdOOzmxG_eHcDcmdg_Ekr23sT1FbmDx9b70p4qSck4Y-8jRhoCX6gQAvD_BwE	Website giả mạo Cục An toàn thông tin, Bộ Thông tin và Truyền thông
10	https://dienmayxanh-services[.]com/	Website giả mạo Điện máy xanh
11	https://magiamgiadienmayxanh[.]com/dmx/	Website giả mạo Điện máy xanh
12	Lazadass[.]com	Website giả mạo sàn TMĐT Lazada
13	cskh-techcombank[.]com	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
14	https://shinhan[.]chamsocthe-uudai-khachhang-tructuyen[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
15	https://shinhan[.]hotrotructuyen-khachhangcanhanthang12[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
16	https://kph25332s[.]com/	Website giả mạo sàn TMĐT Shopee
17	https://landing[.]evnpoint[.]com/	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
18	www[.]ozonvIetnam[.]com	Website giả mạo sàn TMĐT Tiki
19	https://tikihethongmuasam12h[.]com/my	Website giả mạo sàn TMĐT Tiki
20	quocte[.]click	Website giả mạo Western Union

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