NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 48 (25/11/2024 – 01/12/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT "Earth Estries" sử dụng mã độc GHOSTSPIDER trong chiến dịch tấn công nhằm vào ngành viễn thông tại hơn 12 quốc gia.

- **Cảnh báo:** Lỗ hổng nghiêm trọng tồn tại trên plugin "Anti-Spam" của WordPress khiến hơn 200.000 website đứng trước nguy cơ bị ảnh hưởng bởi tấn công thực thi mã 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: 5.237** 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 APT "Earth Estries" sử dụng mã độc GHOSTSPIDER trong chiến dịch tấn công nhằm vào ngành viễn thông tại hơn 12 quốc gia"

Gần đây, các chuyên gia bảo mật đã ghi nhận nhóm tấn công Earth Estries đang sử dụng mã độc backdoor mới có tên "GHOSTSPIDER" trong chiến dịch tấn công nhằm vào công ty thuộc ngành điện tử viễn thông tại các quốc gia Đông Nam Á. Trong chiến dịch, nhóm đối tượng còn sử dụng mã độc backdoor đa nền tảng MASOL RAT (Backdr-NQ) lên các hệ thống Linux thuộc hệ thống mạng của chính phủ tại các quốc gia này.

Theo thống kê từ chuyên gia bảo mật, Earth Estries đã thành công xâm nhập vào hơn 20 tổ chức thuộc lĩnh vực điện tử viễn thông, công nghệ, tư vấn, hóa học, vận chuyển và các đơn vị thuộc chính phủ cũng như các tổ chức phi lợi nhuận. Hiện danh scác quốc gia bị ảnh hưởng được ghi nhận cụ thể như sau: Afghanistan, Brazil, Eswatini, Ấn Độ, Indonesia, Malaysia, Pakistan, Philippines, Nam Phi, Đài Loan, Thái Lan, Mỹ và Việt Nam.

Nhóm tấn công Earth Estries đã đi vào hoạt động kể từ năm 2020 với các tên khác như FamousSparrow, GhostEmperor, Salt Typhoon và UNC2286, nhằm vào các đơn vị chính phủ, công ty điện tử viễn thông tại Mỹ, các quốc gia cùng Châu Á Thái Bình Dương, Trung Đông và Nam Phi.

Một số công cụ đáng chú ý được sử dụng bởi nhóm là rootkit Demodex và mã độc Deed RAT (SNAPPYBEE), là phiên bản mã độc cải tiến của ShadowPad và được sử dụng bởi nhiều nhóm APT thuộc Trung Quốc. Ngoài ra, nhóm Earth Estries còn sử dụng các mã độc backdoor, đánh cắp thông tin như Crowdoor, SparrowDoor, HemiGate, TrillClient và Zingdoor.

Việc xâm nhập đầu vào của nhóm được thực hiện thông qua khai thác các lỗ hổng an toàn thông tin tồn tại trên Ivanti Connect Secure (CVE-2023-46805 và CVE-2024-21887), Fortinet FortiClient EMS (CVE-2023-48788), Sophos Firewall (CVE-2022-3236), Microsoft Exchange Server (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, và CVE-2021-27065 hay ProxyLogon). Sau đó, nhóm đối tượng sẽ triển khai các mã độc như Deed RAT, Demodex và GHOSTSPIDER với mục đích gián điệp không gian mạng dài hạn.

Nguồn: https://thehackernews.com/2024/11/chinese-hackers-use-ghostspider-malware.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT "Earth Estries" sử dụng mã độc GHOSTSPIDER trong chiến dịch tấn công nhằm vào ngành viễn thông tại hơn 12 quốc gia"

Được biết, hạ tầng C&C phức tạp với nhiều backdoor được quản lý bởi các đội hạ tầng khác nhau đã tô điểm cho tính phức phức tạp trong hoạt động của nhóm đối tượng tấn công. Trong đó, GHOSTSPIDER kết nối tới hạ tầng này sử dụng giao thức liên lạc tự tạo được bảo vệ bởi TLS và tải xuống các module bổ sung chức năng cần thiết cho mục tiêu tấn công của nhóm đối tượng.

Ý kiến từ các chuyên gia bảo mật cho rằng: "Earth Estries thực hiện các chiến dịch tấn công một cách kín đáo bắt đầu từ các thiết bị nằm ở viền của không gian mạng và phát tán tới môi trường cloud khiến việc phát hiện trở nên khó khăn. Nhóm đối tượng còn sử dụng kết hợp nhiều biện pháp thiết lập mạng vận hành có vai trò che giấu dấu vết hoạt động của nhóm, qua đó cho thấy nhóm đối tượng này có một cách tiếp cận tinh vi tới việc xâm nhập, theo dõi mục tiêu của mình".

Ngoài ra, các công ty điện tử viễn thông gần đây đã trở thành mục tiêu của nhiều nhóm tấn công có liên kết tới Trung Quốc như Granite Typhoon và Liminal Panda.

Một số IOC được ghi nhận:

103[.]91[.]64[.]214	165[.]154[.]227[.]192	pulseathermakf[.]com	96[.]9[.]211[.]27
23[.]81[.]41[.]166	158[.]247[.]222[.]165	www[.]infraredsen[.]com	139[.]59[.]108[.]43
172[.]93[.]165[.]14	91[.]245[.]253[.]27	billing[.]clothworls[.]com	143[.]198[.]92[.]175
103[.]75[.]190[.]73	45[.]125[.]67[.]144	helpdesk[.]stnekpro[.]com	139[.]59[.]236[.]31
43[.]226[.]126[.]164	172[.]93[.]165[.]10	jasmine[.]lhousewares[.]com	vpn114240349[.]softether[.]net
193[.]239[.]86[.]168	146[.]70[.]79[.]18	private[.]royalnas[.]com	imap[.]dateupdata[.]com
146[.]70[.]79[.]105	205[.]189[.]160[.]3	vpn487875652[.]softether[.]net	139[.]99[.]114[.]108

Nguồn: https://thehackernews.com/2024/11/chinese-hackers-use-ghostspider-malware.html

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng nghiêm trọng tồn tại trên plugin "Anti-Spam" của WordPress khiến hơn 200.000 website đứng trước nguy cơ bị ảnh hưởng bởi tấn công thực thi mã từ xa"

Gần đây, các chuyên gia bảo mật đã ghi nhận thông tin về hai lỗ hổng an toàn thông tin mức Nghiêm trọng gây ảnh hưởng tới plugin "Anti-Spam" và "FireWall" cho WordPress. Đối tượng tấn công sau khi khai thác thành công lỗ hổng có thể cài và bật các plugin độc hại trên website, qua đó cho phép thực thi mã từ xa.

Hai lỗ hổng có mã CVE-2024-10542 (Điểm CVSS: 9.8) và CVE-2024-10781 (Điểm CVSS: 10.0) và đã được xử lý trong phiên bản 6.44, 6.45 được phát hành trong tháng.

Được biết, các plugin bị ảnh hưởng bởi lỗ hổng được coi là "plugin thông dụng cho việc chống spam" nhằm chặn các bình luận, lượt đăng kí, khảo sát… mang tính spam.

Chi tiết về cả hai lỗ hổng là về lỗi bỏ qua biện pháp xác ủy quyền, từ đó cho phép đối tượng tấn công cài và bật các plugin tùy ý, qua đó khiến website chịu ảnh hưởng bởi các lỗ hổng an toàn thông tin tồn tại trên plugin đó.

Đối với lỗ hổng CVE-2024-10781, vấn đề nằm tại việc thiếu sót trong việc kiểm soát giá trị rỗng trên "api_key" tại hàm "function"; còn lỗ hổng CVE-2024-10542 bắt nguồn từ việc bỏ qua biện pháp ủy quyền thông qua hình thức DNS Spoofing trên hàm checkWithoutToken().

Người dùng được khuyến nghị là nên cập nhật bản vá sớm nhất có thể cho các website của mình để giảm nguy cơ bị chịu ảnh hưởng bởi các chiến dịch tấn công khai thác hai lỗ hổng này.

Thông tin này được công bố trong bối cảnh Sucuri cảnh báo về nhiều chiến dịch tấn công khai thác website WordPress để chèn các đoạn mã độc hại có chức năng điều hướng người dùng tới các web độc hại khác thông qua quảng cáo, rà quét thông tin đăng nhập, phát tán mã độc có chức năng ghi nhận mật khẩu admin và thực thi mã PHP tùy ý trên máy chủ.

Nguồn: https://thehackernews.com/2024/11/critical-wordpress-anti-spam-plugin.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 **511** lỗ hổng, trong đó có 198 lỗ hổng mức Cao, 197 lỗ hổng mức Trung bình, 26 lỗ hổng mức Thấp và 90 lỗ hổng chưa đánh giá. Trong đó có ít nhất 89 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 ProjectSend và Palo Alto Networks, cụ thể là như sau:

- **CVE-2024-11680 (Điểm CVSS: Chưa xác định):** Lỗ hổng tồn tại trên ProjectSend tồn tại do thiếu sót trong khâu xác thực, đối tượng tấn công khai thác thành công lỗ hổng có thể truy cập và thực hiện các hành vi trái phép như tạo tài khoản tùy ý, tải lên các webshell độc hại và nhúng JavaScript độc hại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế
- **CVE-2024-0012 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên PAN-OS của hãng Palo Alto Networks cho phép đối tượng tấn công sau khi khai thác thành công có thể leo thang đặc quyền. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-9474 (Điểm CVSS: 7.2 – Cao):** Lỗ hổng tồn tại trên PAN-OS của hãng Palo Alto Networks cho phép đối tượng tấn công sau khi khai thác thành công có thể leo thang đặc quyền. 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-2024-11680	- Điểm CVSS: Chưa xác định - Ảnh hưởng: ProjectSends - 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-2024-11680
2	CVE-2024-0012	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng 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-2024-0012
3	CVE-2024-9474	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng 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-2024-9474
4	CVE-2024-35250	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng 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
5	CVE-2024-10914	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Dlink - 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-2024-10914

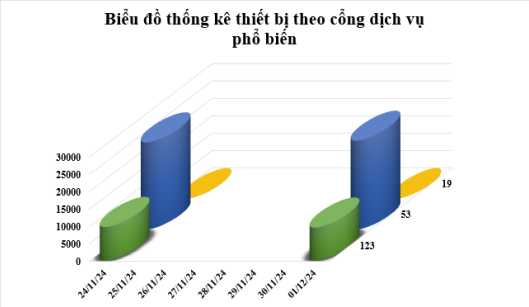
TOP 10 lỗ hổng đáng chú ý trong tuần

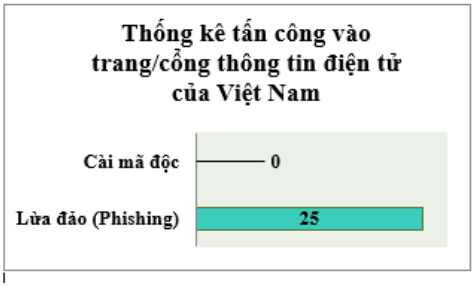
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-9680	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Firefox - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-9680
7	CVE-2024-49039	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows - Mô tả: Lỗ hổng cho phép đối tượng 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-2024-49039
8	CVE-2024-23113	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Fortinet - 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-2024-23113
9	CVE-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: GeoServer - 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-2024-23113
10	CVE-2024-29014	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: SonicWall SMA100 NetExtender Windows - 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-2024-29014

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 **35.190** (tăng so với tuần trước **34.886**) 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.



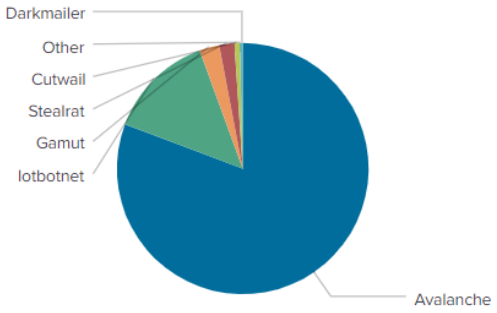


Tấn công Web

Trong tuần, có **25** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 25 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	gjogvvpsf.biz
differentia.ru	ygiudewsqhct.in
atomictrivia.ru	hzmksreiuojy.in
a.asense.in	yunalwv.biz
sdk.asense.in	a.deltaheavy.ru
ydqlnw.info	hzmksreiuojy.ru
statis.multispacesext.net	xjpakmdcfuqe.biz
thesecond.in	b.deltaheavy.ru
amnsreiuojy.ru	c.deltaheavy.ru
morphed.ru	gytujflc.biz

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **5.237** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **285** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **4.952** 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://amazoni1[.]com	Website giả mạo sàn TMĐT Amazon
2	shop[.]amz-dropshipping[.]com	Website giả mạo sàn TMĐT Amazon
3	https://logistic[.]amz-dropshipping[.]com	Website giả mạo sàn TMĐT Amazon
4	https://amazoui[.]top/	Website giả mạo sàn TMĐT Amazon
5	https://amazoni1[.]com/	Website giả mạo sàn TMĐT Amazon
6	https://www[.]applecenter[.]info[.]vn/	Website giả mạo Apple
7	https://dichvucong[.]xqrgov[.]com/	Website giả mạo Bộ Công An
8	dichvucong[.]thongtincancuoc[.]org	Website giả mạo Bộ Công An
9	https://vietchinhphu[.]com/	Website giả mạo Cổng Dịch vụ công Quốc gia
10	https://giaohangtietkiemvietnam[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
11	https://ctygiaohangtietkiemm[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
12	Giaohangtietkiemm[.]net	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
13	https://cucanninhmang[.]net/	Website giả mạo Cục An toàn thông tin, Bộ Thông tin và Truyền thông
14	ghn888[.]com	Website giả mạo Giao hàng nhanh
15	https://da5651[.]com/user/transaction-history	Website giả mạo sàn TMĐT Lazada
16	https://www[.]lazada2024[.]com/home	Website giả mạo sàn TMĐT Lazada
17	vcb[.]chamsockhachhang-capnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
18	hdbank[.]hotrokhachhang-capnhatuudai-trungtamcapnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
19	hdb[.]vi-han-muc-the-ca-nhan[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
20	https://evaluatetravels[.]com/my/history-recharge-withdraw	Website giả mạo Traveloka

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