NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 39 (23/09/2024 – 29/09/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Trung Quốc khai thác lỗ hổng GeoServer để tấn công các quốc gia Châu Á Thái Bình Dương bằng mã độc EAGLEDOOR.

- **Cảnh báo:** Lỗ hổng vượt qua xác thực trên Ivanti vTM bị khai thác trong các chiến dịch tấn công.

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: 338** 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: Nhóm APT Trung Quốc khai thác lỗ hổng GeoServer để tấn công các quốc gia Châu Á Thái Bình Dương bằng mã độc EAGLEDOOR"

Gần đây, một chiến dịch tấn công mạng từ Trung Quốc đã nhắm vào các tổ chức chính phủ ở Đài Loan và có khả năng lan ra các quốc gia khác trong khu vực Châu Á - Thái Bình Dương. Chiến dịch khai thác lỗ hổng nghiêm trọng trên OSGeo GeoServer GeoTools bị phát hiện vào tháng 7/2024 bởi Trend Micro. Nhóm APT Earth Baxia bị nghi đứng sau chiến dịch này dựa trên các email lừa đảo, tài liệu ngụy trang và phương thức tấn công. Các đối tượng bị ảnh hưởng bao gồm các tổ chức chính phủ, doanh nghiệp viễn thông và ngành năng lượng tại Philippines, Hàn Quốc, Việt Nam, Đài Loan và Thái Lan.

Chuỗi tấn công của chiến dịch này sử dụng hai kỹ thuật chính: gửi các email spear-phishing và khai thác lỗ hổng CVE-2024-36401 trên GeoServer.

Mục đích là để phát tán mã độc Cobalt Strike và một loại backdoor mới được đặt tên là EAGLEDOOR, cho phép đối tượng tấn công thu thập thông tin và triển khai các payload độc hại.

Nhóm APT Earth Baxia đã sử dụng hai kỹ thuật "GrimResource" và "AppDomainManager Injection" để triển khai thêm các payload bổ sung. Trong đó, GrimResource được dùng để tải về mã độc từ một file MSC mồi nhử tên RIPCOY, đính kèm trong file ZIP. Một số nguồn tin cho thấy nhóm APT41 cũng đã từng áp dụng hai kỹ thuật này để tấn công các tổ chức ở Đài Loan, quân đội Philippines và các doanh nghiệp năng lượng tại Việt Nam. Các chuyên gia bảo mật nhận định rằng hai chiến dịch này có thể liên quan đến nhau do sử dụng chung các domain C&C của mã độc Cobalt Strike.

Mục tiêu chính của chiến dịch do nhóm APT Earth Baxia thực hiện là phát tán một biến thể tùy chỉnh của mã độc Cobalt Strike, đóng vai trò làm nền tảng để triển khai backdoor EAGLEDOOR ("Eagle.dll") thông qua kỹ thuật DLL side-loading.

Nguồn: https://thehackernews.com/2024/09/chinese-hackers-exploit-geoserver-flaw.html

"Chiến dịch tấn công APT: Nhóm APT Trung Quốc khai thác lỗ hổng GeoServer để tấn công các quốc gia Châu Á Thái Bình Dương bằng mã độc EAGLEDOOR"

Mã độc này hỗ trợ bốn phương thức liên lạc với máy chủ C&C, bao gồm DNS, HTTP, TCP và Telegram. Ba giao thức đầu tiên dùng để gửi trạng thái của nạn nhân, còn chức năng chính được thực hiện thông qua API Bot của Telegram để tải lên và tải xuống tệp, cũng như thực thi các payload bổ sung. Dữ liệu thu thập được sẽ được chuyển ra ngoài qua curl.exe.

Chiến dịch tấn công của Earth Baxia cho thấy sự tinh vi và khả năng linh hoạt khi nhóm này không chỉ khai thác các lỗ hổng mới mà còn tận dụng dịch vụ đám mây công cộng để lưu trữ mã độc, giúp hoạt động của chúng khó bị phát hiện hơn.

Một số IoC được ghi nhận:

recordar-simmco.s3.sa-east-1.amazonaws[.]com	167.172.89[.]142	proradead.s3.sa-east-1.amazonaws[.]com
wordpresss-data.s3.me-south-1.amazonaws[.]com	167.172.84[.]142	status.s3cloud-azure[.]com
ecgglass-arq.s3.sa-east-1.amazonaws[.]com	152.42.243[.]170	api.s2cloud-amazon[.]com
souzacambos.s3.sa-east-1.amazonaws[.]com	188.166.252[.]85	visualstudio-microsoft[.]com
cooltours.s3.sa-east-1.amazonaws[.]com	xiiltrionsoledadprod.s3.sa-east-1.amazonaws[.]com	us2.s3bucket-azure[.]online
s3-contemp.s3.sa-east-1.amazonaws[.]com	app-dimensiona.s3.sa-east-1.amazonaws[.]com	static.trendmicrotech[.]com
homologacao-sisp.s3.sa-east-1.amazonaws[.]com	bjj-files-production.s3.sa-east-1.amazonaws[.]com	msa.hinet[.]ink
doare-assets.s3.sa-east-1.amazonaws[.]com	footracker-statics.s3.sa-east-1.amazonaws[.]com	bobs8.oss-cn-hongkong.aliyuncs[.]com
kcalmoments.s3.me-south-1.amazonaws[.]com	static.krislab[.]site	rocean.oca[.]pics
speedshare.oss-cn-hongkong.aliyuncs[.]com	ms1.hinet[.]lat	360photo.oss-cn-hongkong.aliyuncs[.]com

Nguồn: https://thehackernews.com/2024/09/chinese-hackers-exploit-geoserver-flaw.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng vượt qua xác thực trên Ivanti vTM bị khai thác trong các chiến dịch tấn công"

Cơ quan An ninh mạng và Cơ sở hạ tầng Hoa Kỳ (CISA) vừa ghi nhận một lỗ hổng Nghiêm trọng trên Ivanti vTM, cho phép đối tượng tấn công tạo tài khoản quản trị viên giả mạo trên các thiết bị Virtual Traffic Manager (vTM).

Lỗ hổng Nghiêm trọng có mã CVE-2024-7593, là lỗi bỏ qua xác thực do việc triển khai thuật toán xác thực không chính xác. Điều này cho phép đối tượng tấn công từ xa chưa được xác thực có thể truy cập trái phép vào các trang quản trị của thiết bị vTM được kết nối với Internet. Nếu khai thác thành công lỗ hổng này có thể dẫn đến việc đối tượng tấn công vượt qua cơ chế xác thực và tạo ra các tài khoản quản trị viên tùy ý.

Mặc dù Ivanti đã phát hành bản vá cho lỗ hổng CVE-2024-7593 vào ngày 13 tháng 8 năm 2024, kèm theo mã khai thác PoC, nhưng công ty này vẫn chưa cung cấp thông tin cụ thể về số lượng các cuộc tấn công lợi dụng lỗ hổng này.

Ivanti khuyên người dùng nên kiểm tra kỹ nhật ký kiểm toán (Audit Logs Output) để phát hiện dấu hiệu bị tấn công. Đặc biệt, cần chú ý tới sự xuất hiện của các tài khoản quản trị viên bất thường như "user1" hoặc "user2", được tạo thông qua giao diện người dùng hoặc sử dụng mã khai thác công khai. Các chuyên gia khuyến nghị quản trị viên nên giới hạn quyền truy cập giao diện quản lý vTM trong mạng nội bộ hoặc dùng IP riêng để giảm nguy cơ bị tấn công.

Lỗ hổng này là một trong nhiều lỗ hổng của Ivanti bị khai thác trong các chiến dịch tấn công gần đây, nhắm vào các sản phẩm như VPN, hệ thống ICS, IPS, và các cổng ZTA của hãng. Ivanti cũng cảnh báo về các cuộc tấn công đang khai thác hai lỗ hổng vừa được vá trên Cloud Services Appliance (CSA).

Để đối phó với các cuộc tấn công này, Ivanti đã nâng cao khả năng quét và kiểm thử nội bộ. Hãng cam kết cải thiện quy trình công bố thông tin để phát hiện và xử lý các lỗ hổng bảo mật nhanh chóng hơn, từ đó bảo vệ hệ thống của hàng nghìn khách hàng doanh nghiệp trên toàn cầu.

Nguồn: https://www.bleepingcomputer.com/news/security/critical-ivanti-vtm-auth-bypass-bug-now-exploited-in-attacks/

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 **636** lỗ hổng, trong đó có 224 lỗ hổng mức Cao, 151 lỗ hổng mức Trung bình, 18 lỗ hổng mức Thấp và 243 lỗ hổng chưa đánh giá. Trong đó có ít nhất 37 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 Ivanti, GeoServer và NVIDIA, cụ thể là như sau:

- **CVE-2024-8190 (Điểm CVSS: 7.2 – Cao):** Lỗ hổng tồn tại trên Ivanti Cloud Services cho phép đối tượng tấn công sở hữu tài khoản có quyền quản trị khả năng thực thi mã từ xa. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-36401 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên GeoServer cho phép đối tượng tấn công thực thi mã từ xa sau khi khai thác lỗ hổng bằng cách đưa vào các dữ liệu độc hại trên phiên bản cài đặt mặc định của sản phẩm, thông qua các tham số OGC. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-0132 (Điểm CVSS: 9.0– Nghiêm trọng):** Lỗ hổng tồn tại trên NVIDIA Container Toolkit là lỗi Time-of-check Time-of-Use (TOCTOU) trên cấu hình mặc định của sản phẩm. Đối tượng tấn công có thể khai thác lỗ hổng với các container image độc hại để truy cập vào hệ thống, qua đó dẫn tới khả năng thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, tấn công leo thang đặc quyền, thực thi các hành vi trái phép khác. Hiện lỗ hổng chưa 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-2024-8190	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: Ivanti Cloud Services - 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-2024-8190
2	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-2024-36401
3	CVE-2024-0132	- Điểm CVSS: 9.0 (Nghiêm trọng) - Ảnh hưởng: NVIDIA Container Toolkit - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, tấn công leo thang đặc quyền, truy cập và thực thi các hành vi trái phép. - 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-2024-0132
4	CVE-2024-38200	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Microsoft Office - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - 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-2024-38200
5	CVE-2024-47176	- Điểm CVSS: 8.3 (Cao) - Ảnh hưởng: CUPS (hệ thống in mã nguồn mở) - 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-2024-47176

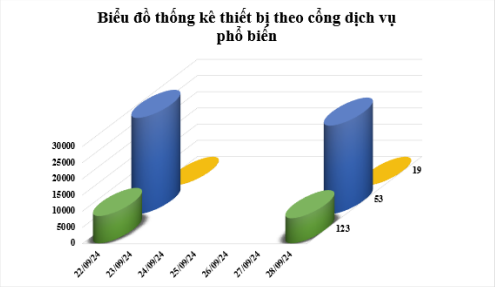
TOP 10 lỗ hổng đáng chú ý trong tuần

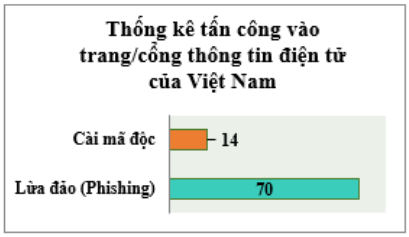
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-7593	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ivanti vTM - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-7593
7	CVE-2024-38014	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - 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-2024-38014
8	CVE-2024-43461	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công giả mạo website, đánh lừa người dùng cung cấp thông tin quan trọng. - 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-2024-43461
9	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: lỗ hổng cho phép đối tượng tấn công thực hiện tấn công Spoofing. - 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-2024-38112
10	CVE-2024-8963	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Ivanti CSA - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - 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-2024-8963

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 **35.095** (giảm so với tuần trước **38.187**) 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.



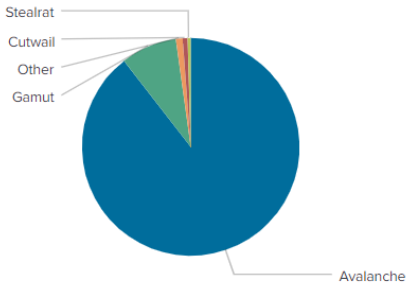


Tấn công Web

Trong tuần, có **84** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 70 trường hợp tấn công lừa đảo (Phishing), 14 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

amnsreiuojy.ru	andall.servicesql.info
hzmksreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	yk37wagdg.life
xjpakmdcfuqe.com	maxisurf.net
restlesz.su	cmnsgscccrej.pw
xjpakmdcfuqe.ru	uyhgqunqkxnx.pw
xjpakmdcfuqe.in	pudglvytdysvadjts.org
restless.su	krkksgulmmrbppjia.com
api.garageserviceoperation.com	focusdate.com
butterflyjobs.com	elitiorecfreetoo.cc

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **338** 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	vssid[.]svgov[.]cc	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://vngiao[.]hangtietkiem[.]online	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://giaohangtietkiemvietnam[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://org[.]govqp[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
6	dichvucong[.]bcavnvnvngov[.]com	Website giả mạo Dịch vụ công Quốc Gia
7	https://www[.]ebayu[.]top	Website giả mạo sàn TMĐT Ebay
8	https://github-scanner[.]com	Website giả mạo Github
9	https://play[.]appgoogle[.]cc	Website giả mạo Google
10	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
11	https://baovietcv[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
12	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
13	ocb[.]chamsocthekhachhang-uudai-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phương Đông
14	https://tienichshiinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
15	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
16	www[.]shopeeace[.]com	Website giả mạo sàn TMĐT Shopee
17	nzu66938s[.]com	Website giả mạo sàn TMĐT Shopee
18	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
19	https://muasamtiki24h[.]com	Website giả mạo sàn TMĐT Tiki
20	https://vnpttechnology[.]weebly[.]com	Website giả mạo VNPT- Tập đoàn Bưu chính Viễn thông Việt Nam

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