NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 37 (09/09/2024 – 15/09/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Ba nhóm tấn công của Trung Quốc đứng sau chiến dịch tấn công mạng nhằm vào các quốc gia Đông Nam Á.

- **Cảnh báo:** Ivanti phát hành bản vá cho lỗ hổng RCE nghiêm trọng trên phần mềm Endpoint Management.

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: 486** 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: Ba nhóm tấn công của Trung Quốc đứng sau chiến dịch tấn công mạng nhằm vào các quốc gia Đông Nam Á"

Ba nhóm tấn công có liên quan với Trung Quốc đã được ghi nhận thực hiện các chiến dịch tấn công nhằm vào nhiều tổ chức chính phủ tại Đông Nam Á trong một chiến dịch do nhà nước hậu thuẫn mang tên "Crimson Palace", cho thấy sự mở rộng phạm vi hoạt động gián điệp không gian mạng của Trung Quốc.

Chiến dịch này bao gồm ba nhóm tấn công, được theo dõi với tên: Nhóm Alpha (STAC1248), Nhóm Bravo (STAC1870), và Nhóm Charlie (STAC1305). STAC là viết tắt của "security threat activity cluster" (cụm hoạt động đe dọa an ninh). Được biết các nhóm đối tượng đã khai thác hệ thống của các tổ chức và mạng lưới dịch vụ công trong khu vực để phát tán mã độc và công cụ độc hại, ngụy trang dưới các điểm truy cập tin cậy.

Một điểm đáng chú ý của chiến dịch là việc sử dụng hệ thống của một tổ chức làm điểm chuyển tiếp C&C và nơi lưu trữ công cụ tấn công. Đồng thời, một máy chủ Microsoft Exchange bị xâm nhập của một tổ chức khác đã bị lợi dụng để lưu trữ mã độc.

Chiến dịch "Crimson Palace" lần đầu được ghi nhận vào tháng 6/2024, với các đợt tấn công diễn ra từ tháng 3/2023 đến tháng 4/2024. Đến khoảng thời gian từ tháng 1/2024 đến tháng 6/2024,

Trong giai đoạn đầu của các cuộc tấn công diễn ra vào tháng 03/2024 được thực hiện bởi nhóm Bravo, cách hoạt động của nhóm này có nhiều điểm chung với nhóm APT Unfading Sea Haze. Đến khoảng thời gian từ tháng 01/2024 đến tháng 6/2024, một làn sóng tấn công mới của nhóm này đã nhắm vào 11 tổ chức và cơ quan trong khu vực.

Các chuyên gia bảo mật cũng ghi nhận một đợt tấn công khác từ nhóm Charlie (còn gọi là APT Earth Longzhi) được thực hiện từ tháng 9/2023 đến tháng 6/2024. Nhóm này đã sử dụng các framework C&C như Cobalt Strike, Havoc, và XieBroC2 để thực hiện các hành vi độc hại sau khai thác và phát tán các payload bổ trợ như SharpHound nhằm lập bản đồ hạ tầng Active Directory.

Nguồn: https://thehackernews.com/2024/09/experts-identify-3-chinese-linked.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Ba nhóm tấn công của Trung Quốc đứng sau chiến dịch tấn công mạng nhằm vào các quốc gia Đông Nam Á"

Mặc dù mục tiêu chính vẫn là thu thập dữ liệu, tuy nhiên, nhóm Charlie đã tập trung nhiều hơn vào việc thiết lập lại và mở rộng sự xâm nhập vào hệ thống mạng bằng cách vượt qua lớp bảo mật từ phần mềm EDR và khôi phục kết nối khi các cài đặt C&C trước đó bị chặn.

Một yếu tố đáng chú ý khác là việc nhóm Charlie chủ yếu sử dụng kỹ thuật DLL hijacking để thực thi mã độc, một kỹ thuật thường được nhóm Alpha sử dụng, cho thấy có sự chia sẻ kỹ thuật giữa các nhóm tấn công. Các đối tượng tấn công còn sử dụng phần mềm mã nguồn mở như RealBlindingEDR và Alcatraz để vô hiệu hóa các quy trình chống virus và làm mờ các file thực thi (như .exe, .dll, và .sys), nhằm mục đích tránh bị phát hiện.

Cuối cùng, các chuyên gia bảo mật đã ghi nhận mã độc keylogger mới có tên TattleTale, lần đầu xuất hiện vào tháng 8/2023. Mã độc này có khả năng thu thập dữ liệu từ các trình duyệt Google Chrome và Microsoft Edge, đồng thời thu thập tên domain controller và đánh cắp LSA (Local Security Authority) Query Information Policy, nơi chứa thông tin nhạy cảm như chính sách mật khẩu, cài đặt bảo mật và mật khẩu lưu trữ.

Tóm lại, chiến dịch "Crimson Palace" bao gồm ba nhóm tấn công phối hợp với nhau, mỗi nhóm đảm nhiệm một giai đoạn trong chuỗi tấn công: xâm nhập và thu thập thông tin (Nhóm Alpha), thâm nhập sâu vào hệ thống bằng các cơ chế C&C (Nhóm Bravo), và đánh cắp dữ liệu (Nhóm Charlie). Theo nhận định của các chuyên gia, trong suốt quá trình thực hiện chiến dịch, các nhóm tấn công đã liên tục thử nghiệm và nâng cao các kỹ thuật, công cụ. Khi các biện pháp đối phó được triển khai, chúng kết hợp công cụ tự phát triển với các công cụ mã nguồn mở thường được sử dụng bởi các chuyên gia kiểm thử an ninh mạng để duy trì quyền truy cập.

Một số IoC được ghi nhận:

178.128.221.202:443	gsenergyspeedtest.com	192.142.18.15
192.142.18.27	192.142.18.25	hpupdate.net
45.15.143.151	198.244.237.13	123.253.35.100
cancelle.net	dmsz.org	gandeste.net
103.56.5.224	49.157.28.114	103.19.16.248:443
141.136.44.219	145.14.158.235	107.148.41.114
66.42.56.233	test1.zhangliyong.cn	191.96.53.132: 443
45.9.191.183	www.pmshyptest.com	64.176.50.42:8444
191.96.53.132	45.77.46.245:443	64.176.37.107:443
95.179.249.205	198.13.47.158:443	128.199.107.213

Nguồn: https://thehackernews.com/2024/09/experts-identify-3-chinese-linked.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Ivanti phát hành bản vá cho lỗ hổng RCE nghiêm trọng trên phần mềm Endpoint Management"

Gần đây, Ivanti đã vá lỗ hổng Nghiêm trọng trên phần mềm Endpoint Management (EPM), lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa (RCE) lên máy chủ.

Ivanti EPM là giải pháp quản lý thiết bị cho phép quản trị viên kiểm soát các thiết bị client trên nhiều nền tảng như Windows, macOS, Chome OS và các hệ điều hành của thiết bị IoT.

Lỗ hổng được vá có mã CVE-2024-29847 (Điểm CVSS: 10.0) tồn tại do điểm yếu trong việc xử lý các dữ liệu không tin cậy trên cổng agent. Trước đó, lỗ hổng này đã được đề cập trong các bản vá của Ivanti EPM 2024 và Ivanti EPM 2022 Service Update 6 (SU6). Đối tượng tấn công khai thác lỗ hổng này có thể truy cập trái phép vào máy chủ EPM. Hiện tại, Ivanti cho biết chưa ghi nhận trường hợp nào bị ảnh hưởng và chưa có thông tin khai thác công khai nào được xác nhận.

Bên cạnh lỗ hổng này, Ivanti cũng đã vá nhiều lỗi khác trên Ivanti EPM, Workspace Control (IWC) và Cloud Service Appliance (CSA). Vào tháng 01/2024, công ty đã phát hành bản vá cho một lỗ hổng RCE tương tự (CVE-2023-39336) trên Ivanti EPM, cho phép đối tượng tấn công truy cập trái phép vào máy chủ và kiểm soát các thiết bị được quản lý.

Việc phát hành nhiều bản vá trong thời gian gần đây là kết quả của việc Ivanti nâng cao công tác rà quét nội bộ và kiểm thử bằng các phương pháp khai thác thủ công. Công ty cũng đã cải thiện công tác công bố thông tin để xử lý các vấn đề phát sinh nhanh hơn.

Thông tin này được Ivanti công bố trong bối cảnh nhiều lỗ hổng zero-day bị khai thác trong thực tế vào những năm gần đây. Trong đó, lỗ hổng command injection CVE-2024-21887 và lỗ hổng vượt qua xác thực CVE-2023-46805 đã được sử dụng để tấn công các sản phẩm VPN của Ivanti. Thêm vào đó, Ivanti cũng đã cảnh báo về lỗ hổng zero-day SSRF (CVE-2024-21893), bị khai thác nhiều lần vào tháng 02/2024, cho phép kẻ tấn công vượt qua xác thực trên các sản phẩm ICS, IPS và gateway ZTA.

Nguồn: https://www.bleepingcomputer.com/news/security/ivanti-fixes-maximum-severity-rce-bug-in-endpoint-management-software/

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 **542** lỗ hổng, trong đó có 206 lỗ hổng mức Cao, 193 lỗ hổng mức Trung bình, 28 lỗ hổng mức Thấp và 115 lỗ hổng chưa đánh giá. Trong đó có ít nhất 78 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

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của SonicWall, Ivanti và GeoServer, cụ thể là như sau:

- **CVE-2024-40766 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên SonicWall SonicOS cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-7262 (Điểm CVSS: 9.8– Nghiêm trọng):** Lỗ hổng tồn tại trong Ivanti EPM cho phép đối tượng tấn công thực thi mã từ xa bằng cách giải tuần tự các dữ liệu không được tin cậy trên giao diện agent. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-7971 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên GeoServer cho phép đối tượng tấn công thực thi mã từ xa bằng cách truyền các dữ liệu độc hại vào tham số yêu cầu OGC trên các phiên bản cài đặt mặc định của ứng dụng. 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-2024-40766	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: SonicWall SonicOS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - 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-2024-40766
2	CVE-2024-29847	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ivanti EPM - 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-2024-29847
3	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
4	CVE-2024-8522	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Plugin LearnPress của WordPress - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi SQL Injection, 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-2024-8522
5	CVE-2024-38127	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows Server 2022. - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-38127

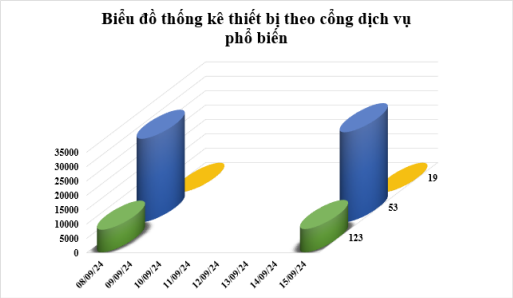
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-28000	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache. - 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-2024-28000
7	CVE-2024-8504	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: VICIdial - 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-2024-8504
8	CVE-2024-4577	- Điểm CVSS: 9.8 (Cao) - Ảnh hưởng: Ngôn ngữ lập trình PHP - 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-2024-4577
9	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: OpenSSH - 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-2024-6387
10	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Microsoft Windows 10, Windows Server 2022 - 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-2024-38063

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 **39.438** (tăng so với tuần trước **36.907**) 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.

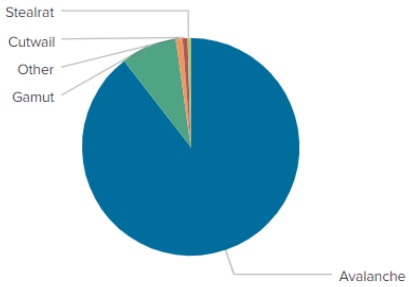


Tấn công Web

Trong tuần, có **83** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 72 trường hợp tấn công lừa đảo (Phishing), 11 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	restless.su
hzmksreiuojy.ru	andall.servicesql.info
xjpakmdcfuqe.biz	spaines.pw
differentia.ru	butterflyjobs.com
restlesz.su	wdxzlv.org
disorderstatus.ru	uyhgqunqkxnx.pw
xjpakmdcfuqe.com	mc-live.online
xjpakmdcfuqe.ru	focusdate.com
xjpakmdcfuqe.in	c6i0ilgden1ve8eb1here4s.ddns.net
atomictrivia.ru	xtgfujmknprb.ru

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **486** 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://vngiao[.]hangtietkiem[.]online	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
2	https://giaohangtietkiemvietnam[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://org[.]govqp[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
5	https://www[.]ebayu[.]top	Website giả mạo sàn TMĐT Ebay
6	https://play[.]appgoogle[.]cc	Website giả mạo Google
7	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
8	https://acb[.]hotrokhachhang-uudai-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
9	https://acb[.]uudaikhachhangthe-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
10	https://baovietcv[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
11	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
12	https://mbdk555[.]com	Website giả mạo Ngân hàng TMCP Quân đội
13	https://tienichshiinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
14	https://www[.]lapmangsctv[.]com[.]vn	Website giả mạo SCTV
15	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
16	https://kpt32165s[.]com	Website giả mạo sàn TMĐT Shopee
17	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
18	https://tiktikshopvn[.]com	Website giả mạo sàn TMĐT Tiki
19	https://muasamtiki24h[.]com	Website giả mạo sàn TMĐT Tiki
20	https://chinhphu[.]hodancu[.]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