NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 21 (27/05/2024 – 02/06/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Microsoft tiết lộ về nhóm tấn công mới "Moonstone Sleet" của Triều Tiên.

- **Cảnh báo:** Chuyên gia bảo mật cảnh báo về nguy cơ bị tấn công trên Plugin WordPress.

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: 283** 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: Microsoft tiết lộ về nhóm tấn công mới "Moonstone Sleet" của Triều Tiên"

Nhóm tấn công mới có tên Moonstone Sleet đã nhằm vào các cá nhân và tổ chức trong lĩnh vực phần mềm, công nghệ thông tin, giáo dục và quốc phòng bằng ransomware, tương tự như nhóm APT Lazarus Group. Nhóm này tạo ra các công ty ma và cơ hội việc làm giả để phát tán các công cụ hợp pháp nhưng bị cài trojan, mã độc game và ransomware. Moonstone Sleet sử dụng cả kỹ thuật phổ biến của các nhóm tấn công Triều Tiên và kỹ thuật mới của riêng mình.

Ban đầu được theo dõi dưới tên Storm-1789, Moonstone Sleet đã được xác định là một nhóm riêng biệt nhờ hạ tầng và kỹ thuật tấn công riêng, có nhiều điểm tương đồng với Lazarus Group.

Cả hai nhóm đều sử dụng mã nguồn của mã độc nổi tiếng như Comebacker. Bên cạnh đó, Moonstone Sleet cũng ứng tuyển vào các vị trí phát triển phần mềm tại các công ty hợp pháp nhằm tạo doanh thu bất hợp pháp cho Triều Tiên hoặc đạt quyền truy cập vào các tổ chức từ bên trong.

Từ tháng 08/2023, nhóm tấn công sử dụng phiên bản chỉnh sửa của công cụ PuTTY. Họ gửi một file .ZIP chứa PuTTY bị nhiễm trojan và file url.txt chứa địa chỉ IP cùng mật khẩu. Khi người dùng nhập thông tin này vào PuTTY, payload được giải mã và thực thi. Payload này là SplitLoader, thực hiện một loạt tác vụ để tải và chạy file từ máy chủ C&C.

Một chuỗi tấn công khác sử dụng các gói npm độc hại phát tán qua LinkedIn hoặc các trang web việc làm tự do. Nhóm tấn công tạo các công ty giả để gửi file .ZIP chứa gói npm ngụy trang thành bài kiểm tra kỹ năng kỹ thuật. Các gói npm này kết nối đến máy chủ C&C để tải payload hoặc trích xuất thông tin xác thực từ tiến trình Windows LSASS. Đáng chú ý, chiến thuật này từng được sử dụng trong chiến dịch Contagious Interview, đây là một phương pháp phát tán mã độc phổ biến của nhóm APT Triều Tiên có tên Jade Sleet.

Nguồn: https://thehackernews.com/2024/05/microsoft-uncovers-moonstone-sleet-new.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Microsoft tiết lộ về nhóm tấn công mới "Moonstone Sleet" của Triều Tiên"

Ngoài ra, Moonstone Sleet còn sử dụng một trò chơi độc hại phát tán qua tin nhắn hoặc email. Nhóm này giả mạo nhà phát triển game cần đầu tư hoặc trợ giúp từ nhà phát triển khác và sử dụng tên của một công ty blockchain hợp pháp hoặc ma. Trong trò chơi này, họ cài đặt loader mã độc YouieLoad để tải payload tiếp theo vào bộ nhớ, tạo dịch vụ độc hại để quét hệ thống mạng và thu thập dữ liệu trình duyệt.

Nhóm APT Moonstone Sleet sử dụng một công ty ma tên là StarGlow Ventures trong chiến dịch tấn công social engineering. Công ty này giả danh là một công ty phát triển phần mềm hợp pháp, đăng tin tuyển dụng các dự án liên quan đến web, ứng dụng di động, blockchain và AI. Chiến dịch kéo dài trong 4 tháng đầu năm 2024, sử dụng email nhúng pixel theo dõi để xây dựng độ tin cậy và xác định người dùng tương tác với email, chuẩn bị cho các cuộc tấn công tương lai nhằm thu lợi nhuận.

Moonstone Sleet đã tung ra công cụ ransomware mới gọi là FakePenny, được phát hiện trong hệ thống của một công ty công nghệ quốc phòng vào tháng 04/2024. Nhóm này yêu cầu tiền chuộc là 6.6 triệu đô la bằng Bitcoin.

Thông tin về nhóm Moonstone Sleet được tiết lộ sau khi Hàn Quốc cáo buộc Triều Tiên, đặc biệt là Lazarus Group, đã đánh cắp 1.014 GB dữ liệu bao gồm tên, số căn cước công dân và ghi chép tài chính từ một hệ thống mạng của tòa án Hàn Quốc từ ngày 07/01/2021 đến 09/02/2023.

Một số IoC được ghi nhận:

bestonlinefilmstudio[.]org	blockchain-newtech[.]com
ccwaterfall[.]com	chaingrown[.]com
defitankzone[.]com	detankwar[.]com
freenet-zhilly[.]org	matrixane[.]com
pointdnt[.]com	starglowventures[.]com
mingeloem[.]com	0

Nguồn: https://thehackernews.com/2024/05/microsoft-uncovers-moonstone-sleet-new.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Chuyên gia bảo mật cảnh báo về nguy cơ bị tấn công trên Plugin WordPress"

Các chuyên gia bảo mật đã đưa ra cảnh báo về hàng loạt các lỗ hổng an toàn thông tin mức độ cao tồn tại trên plugin của WordPress và đang bị khai thác trong thực tế bởi các nhóm tấn công để tạo ra các tài khoản quản trị trái phép.

Những lỗ hổng cho phép đối tượng tấn công khai thác lỗi XSS, do việc lọc dữ liệu đầu vào và đầu ra không đảm bảo an toàn thông tin, dẫn tới việc website bị chèn các script độc hại. Cụ thể, các lỗ hổng này là:

- **CVE-2023-6961 (Điểm CVSS: 7.2)** – Lỗ hổng Unauthenticated Stored Cross-Site Scripting tồn tại trong WP Meta SEO phiên bản cũ hơn 4.5.12.
- **CVE-2023-40000 (Điểm CVSS: 8.3)** - Lỗ hổng Unauthenticated Stored Cross-Site Scripting tồn tại trong LiteSpeed Cache phiên bản cũ hơn 5.7.
- **CVE-2024-2194 (Điểm CVSS: 7.2)** - Lỗ hổng Unauthenticated Stored Cross-Site Scripting tồn tại trong WP Statistics phiên bản cũ hơn 14.5.

Nhóm tấn công khai thác các lỗ hổng này bắt đầu bằng cách chèn payload vào tệp JavaScript trên một domain độc hại, với mục tiêu tạo tài khoản quản trị, thêm mã độc backdoor, và triển khai các script giám sát.

Mã độc backdoor bằng ngôn ngữ PHP được chèn vào các tệp plugin và theme trên trang web, trong khi các script giám sát được lập trình để gửi yêu cầu HTPT GET chứa thông tin về host HTTP đến máy chủ C&C với địa chỉ IP "ur.mystiqueapi[.]com/?ur". Hầu hết các cố gắng khai thác lỗ hổng này đều bắt nguồn từ địa chỉ IP thuộc sở hữu của Hệ thống Tự động IP Volume Inc (Autonomous System (AS) IP Volume Inc), chủ yếu có nguồn gốc từ Hà Lan.

Lưu ý rằng, trước đó, WPScan - một công cụ bảo mật của WordPress - cũng đã tiết lộ thông tin về một chiến dịch tấn công tương tự, sử dụng lỗ hổng CVE-2023-40000 để tạo tài khoản quản trị trái phép trên các trang web bị ảnh hưởng.

Để giảm thiểu nguy cơ bị tấn công, người dùng sử dụng WordPress cho trang web của mình cần kiểm tra các plugin đã cài đặt, cập nhật chúng lên phiên bản mới nhất và kiểm tra lại trang web để phát hiện và loại bỏ mã độc cũng như những tài khoản quản trị đáng ngờ.

Nguồn: https://thehackernews.com/2024/05/researchers-uncover-active-exploitation.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 **1.010** lỗ hổng, trong đó có 76 lỗ hổng mức Cao, 181 lỗ hổng mức Trung bình, 09 lỗ hổng mức Thấp và 744 lỗ hổng chưa đánh giá. Trong đó có ít nhất 163 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 CheckPoint, Palo Alto Networks và Wordpress, cụ thể là như sau:

- **CVE-2024-24919 (Điểm CVSS: 8.6 – Cao):** Lỗ hổng tồn tại trên Check Point Security Gateways cho phép đối tượng tấn công truy cập và đọc các thông tin trên thiết bị ảnh hưởng có sử dụng chức năng remote Access VPN hoặc Mobile Access Software Blades. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.
- **CVE-2024-3400 (Điểm CVSS: 9.1 – Nghiêm trọng)**: Lỗ hổng Command Injection tồn tại trên Palo Alto Networks PAN-OS cho phép đối tượng thực thi mã tùy ý với quyền root trên tường lửa sử dụng PAN-OS. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công
- **CVE-2024-5204 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trong plugin "Swiss Toolkit For WP" của WordPress cho phép đối tượng tấn công với quyền hạn đóng góp trên website có thể đăng nhập vào website sử dụng tài khoản bất kì tồn tại trên website. Hiện lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-24919	- Điểm CVSS: 8.6 (Cao) - Ảnh hưởng: Check Point Security Gateways - 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-2024-24919
2	CVE-2024-3400	- Điểm CVSS: 10 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3400
3	CVE-2024-5204	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: WordPress. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép trên các tài khoản tồn tại trong website. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-5204
4	CVE-2024-4367	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Mozilla Firefox, Mozilla Firefox ESR, Mozilla Thunderbird. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện script JavaScript tùy ý trên trình duyệt. - 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-2024-4367
5	CVE-2024-3094	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Tukaani Xz. - 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-2024-3094

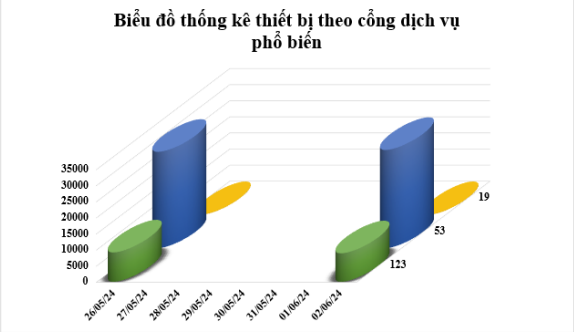
TOP 10 lỗ hổng đáng chú ý trong tuần

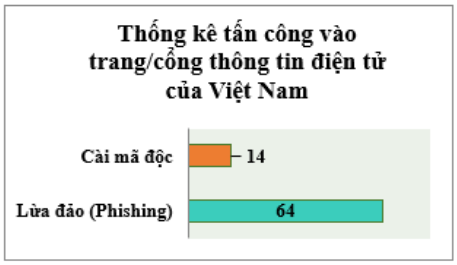
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-5274	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-5274
7	CVE-2024-21887	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - 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-2024-21887
8	CVE-2024-23108	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Fortinet FortiSIEM. - 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-2024-23108
9	CVE-2024-21412	-- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2022. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý, 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-2024-21412
10	CVE-2024-1086	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Linux. - 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-2024-1086

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 **39.409** (tăng so với tuần trước **39.100**) 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.



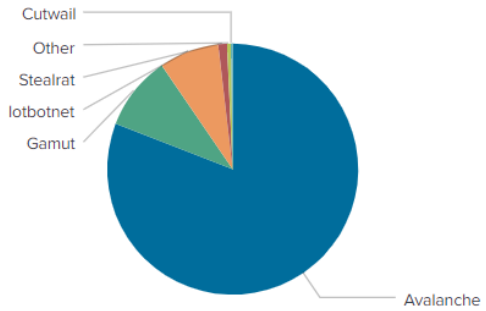


Tấn công Web

Trong tuần, có **78** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 64 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

differentia.ru	ivz7x63ymy.ru
disorderstatus.ru	restless.su
atomictrivia.ru	omfghellobrosjda38.org
amnsreiuojy.ru	andall.servicesql.info
xjpakmdcfuqe.biz	bbuildersget.com
restlesz.su	jpalertcert.com
hzmksreiuojy.ru	db2017417b23.zapto.org
xjpakmdcfuqe.com	www.hnmrw.net
xjpakmdcfuqe.ru	cardzstorezone.com
xjpakmdcfuqe.in	and4.junglebeariwtc4.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **283** 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://miaoniter[.]com/	Website giả mạo sàn TMĐT Amazon
2	https://amazonl3[.]com/	Website giả mạo sàn TMĐT Amazon
3	https://www[.]amatvip36sc[.]cc/	Website giả mạo sàn TMĐT Amazon
4	https://vssid[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
5	https://da6555[.]com/	Website giả mạo sàn TMĐT Lazada
6	https://da2323[.]com	Website giả mạo sàn TMĐT Lazada
7	https://mbfn-fic[.]com/	Website giả mạo Mbbank
8	https://mbcanhan-cskh[.]com/	Website giả mạo Mbbank
9	https://www[.]mbdkb[.]com/	Website giả mạo Mbbank
10	https://phattai247[.]com/	Website giả mạo Mbbank
11	https://tinchaphd[.]com/	Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
12	hdb[.]vntanghanmucvisadebit[.]com	Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
13	hdb[.]tang-han-muc-tin-dung-vn[.]com	Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
14	kh-vibquocte[.]com	Ngân hàng TMCP Quốc tế Việt Nam
15	https://tpb-vayuudai[.]com/	Ngân hàng TMCP Tiên Phong
16	https://soppe68[.]shop/	Website giả mạo sàn TMĐT Shopee
17	https://sp15569p[.]com/	Website giả mạo sàn TMĐT Shopee
18	https://tdkt01[.]com/	Website giả mạo sàn TMĐT Tiki
19	https://vntiki11[.]com/	Website giả mạo sàn TMĐT Tiki
20	https://ca-nhan-vpb[.]com/	Website giả mạo Vpbank

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