NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 32 (05/08/2024 – 11/08/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Moonstone Sleet của Triều Tiên tiếp tục chiến dịch phát tán mã độc thông qua npm.

- **Cảnh báo:** Chiến dịch tấn công thông qua Windows Update có thể "gỡ bỏ" các bản vá hệ thống.

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: 966** 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 Moonstone Sleet của Triều Tiên tiếp tục chiến dịch phát tán mã độc qua npm"

Nhóm tấn công Moonstone Sleet, được Triều Tiên hậu thuẫn, mới đây đã phát tán các gói npm độc hại lên registry JavaScript với mục tiêu xâm nhập vào hệ thống Windows. Điều này cho thấy sự dai dẳng và liên tục của chiến dịch mà nhóm này đang triển khai.

Vào ngày 7/7/2024, hai gói tin độc hại có tên harthat-api và harthat-hash đã được phát hành lên registry npm. Tuy nhiên, cả hai gói này không thu hút bất kỳ lượt tải xuống nào và đã bị gỡ bỏ chỉ sau một thời gian ngắn. Đáng chú ý, mã độc trong các gói này đã tái sử dụng mã nguồn từ một repository GitHub nổi tiếng có tên node-config, vốn là một công cụ phổ biến trong cộng đồng lập trình.

Moonstone Sleet thường xuyên triển khai các chuỗi tấn công bằng cách phát tán các tệp ZIP giả mạo qua LinkedIn thông qua các tài khoản công ty giả hoặc trên các nền tảng freelancer, từ đó lừa người dùng thực thi mã độc bằng cách tải và chạy các gói npm giả mạo. Khi thực thi, gói npm độc hại sẽ sử dụng lệnh curl để kết nối với một máy chủ do kẻ tấn công kiểm soát, từ đó tải về các payload bổ sung như SplitLoader. Trong một cuộc tấn công khác, Moonstone Sleet đã sử dụng một loader npm độc hại để đánh cắp thông tin đăng nhập từ quy trình LSASS của Windows.

Các gói mã độc mới phát hiện của nhóm này được lập trình để thực hiện một script pre-install được chỉ định trong file package.json. Script này kiểm tra xem hệ thống có đang chạy Windows hay không (thông qua tham số "Windows_NT"). Nếu đúng, nó sẽ kết nối với máy chủ C&C để tải về một tệp DLL, sau đó sử dụng binary rundll32.exe để sideload tệp này vào hệ thống. Mặc dù tệp DLL này chưa thực hiện các hành vi độc hại ngay lập tức, điều này có thể là một thử nghiệm về cơ sở hạ tầng phát tán mã độc, hoặc có khả năng mã độc thực tế chưa được tích hợp vào tệp DLL trước khi nó bị phát hiện và gỡ bỏ.

Nguồn: https://thehackernews.com/2024/08/north-korean-hackers-moonstone-sleet.html

Tin tức An toàn thông tin

“Chiến dịch tấn công APT: Nhóm APT Moonstone Sleet của Triều Tiên tiếp tục chiến dịch phát tán mã độc qua npm.”

Thông tin về hoạt động của Moonstone Sleet lần này xuất hiện trong bối cảnh Hàn Quốc đã cảnh báo về các chiến dịch tấn công khác từ các nhóm tin tặc Triều Tiên như Andariel và Kimsuky. Các nhóm này đã nhắm mục tiêu vào ngành xây dựng và máy móc của Hàn Quốc, phát tán các mã độc như Dora RAT và TrollAgent (còn gọi là Troll Stealer). Đáng chú ý, chuỗi tấn công của Dora RAT đã khai thác cơ chế cập nhật của phần mềm VPN nội địa để phát tán mã độc, gây ra nguy cơ lớn cho các hệ thống bị tấn công.

Một số IoC được ghi nhận:

harthat-api-v1.3.1.zip
harthat-hash-v1.3.3.zip
142.111.77[.]196
d2a74db6b9c900ad29a81432af72eee8ed4e22bf61055e7e8f7a5f1a33778277

Nguồn: https://thehackernews.com/2024/08/north-korean-hackers-moonstone-sleet.html

Tin tức An toàn thông tin

"Cảnh báo: Chiến dịch tấn công thông qua Windows Update có thể "gỡ bỏ" các bản vá hệ thống"

Tại sự kiện Black Hat 2024, một chuyên gia bảo mật từ SafeBreach đã tiết lộ một hình thức tấn công hạ cấp qua Windows Update. Phương pháp này khai thác hai lỗ hổng zero-day (CVE-2024-38202 và CVE-2024-21302) nhằm làm mất hiệu lực các bản vá trên Windows 10, Windows 11 và Windows Server, khiến các lỗ hổng đã được vá trước đó quay trở lại.

Microsoft đã phát hành cảnh báo về hai lỗ hổng zero-day chưa được vá (CVE-2024-38202 và CVE-2024-21302) trong buổi thuyết trình tại Black Hat, đồng thời cung cấp các biện pháp giảm thiểu nguy cơ cho đến khi bản vá chính thức được phát hành.

Trong hình thức tấn công này, đối tượng tấn công có thể buộc hệ thống quay về các phiên bản phần mềm cũ, khiến các lỗ hổng đã được vá trước đó xuất hiện trở lại và có thể bị khai thác. Cụ thể, quy trình cập nhật của Windows có thể bị khai thác để hạ cấp các thành phần quan trọng của hệ điều hành, như thư viện liên kết động (DLL) và NT Kernel. Dù các thành phần này đã bị hạ cấp, Windows Update vẫn báo cáo rằng hệ thống được cập nhật đầy đủ, và các công cụ khôi phục hoặc quét không phát hiện ra vấn đề.

Khi các lỗ hổng zero-day này bị khai thác, đối tượng tấn công có thể hạ cấp Secure Kernel của Credential Guard, Isolated User Mode Process và hypervisor của Hyper-V. Điều này làm lộ ra các lỗ hổng leo thang đặc quyền đã được vá trước đó. Các chuyên gia bảo mật cho biết, phương pháp tấn công này có thể biến những lỗ hổng đã được vá thành lỗ hổng zero-day, khiến khái niệm "hệ thống đã được vá" không còn ý nghĩa trên tất cả các máy tính Windows.

Tính nghiêm trọng của hình thức tấn công này là nó không thể bị phát hiện, không bị chặn bởi các giải pháp Endpoint Detection & Response (EDR), và không thể được nhận diện bởi người dùng vì Windows Update vẫn báo cáo rằng hệ thống đã được cập nhật đầy đủ, dù thực tế đã bị hạ cấp.

Nguồn: https://www.bleepingcomputer.com/news/microsoft/windows-update-downgrade-attack-unpatches-fully-updated-systems/

Tin tức An toàn thông tin

"Cảnh báo: Chiến dịch tấn công thông qua Windows Update có thể "gỡ bỏ" các bản vá hệ thống"

Chuyên gia bảo mật đã thông báo cho Microsoft về các lỗ hổng từ tháng 2 năm 2024, nhưng đến nay, Microsoft vẫn chưa phát hành bản vá cho CVE-2024-38202 (leo thang đặc quyền trên Windows Update Stack) và CVE-2024-21302 (leo thang đặc quyền trên Windows Secure Kernel Mode). Lỗ hổng CVE-2024-38202 cho phép đối tượng tấn công có quyền người dùng cơ bản "gỡ bỏ" các bản vá hoặc vượt qua bảo mật Virtualization Based Security (VBS). Trong khi đó, lỗ hổng CVE-2024-21302 cho phép đối tượng tấn công sử dụng quyền quản trị thay thế các file hệ thống Windows bằng các phiên bản cũ hơn.

Hiện chưa có báo cáo về việc hai lỗ hổng này bị khai thác thực tế. Người dùng được khuyến nghị thực hiện các biện pháp giảm thiểu rủi ro khai thác cho đến khi bản vá chính thức được phát hành. Chuyên gia bảo mật cũng nhấn mạnh rằng hình thức tấn công này có thể không chỉ ảnh hưởng đến Windows mà còn có thể tiềm tàng nguy cơ đối với các hệ điều hành khác.

Nguồn: https://www.bleepingcomputer.com/news/microsoft/windows-update-downgrade-attack-unpatches-fully-updated-systems/

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 **773** lỗ hổng, trong đó có 200 lỗ hổng mức Cao, 254 lỗ hổng mức Trung bình, 26 lỗ hổng mức Thấp và 293 lỗ hổng chưa đánh giá. Trong đó có ít nhất 90 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 1Password và Microsoft, cụ thể là như sau:

- **CVE-2018-0824 (Điểm CVSS: 8.8 - Cao):** Lỗ hổng tồn tại trên "Microsoft COM for Windows" cho phép đối tượng tấn công thực thi mã từ xa thông qua lỗi xử lý đối tượng tuần tự thất bại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế.
- **CVE-2024-42219 (Điểm CVSS: 7.0 – Cao):** Lỗ hổng tồn tại trên ứng dụng 1Password cho hệ điều hành macOS, xảy ra do quá trình xác thực liên lạc giữa các tiến trình XPC thất bại. Cho phép đối tượng tấn công truy cập và trích xuất các thông tin lưu trong ứng dụng. Hiện lỗ hổng chưa có mã khai thác và chưa có ghi nhận khai thác trong môi trường thực tế bởi các nhóm tấn công
- **CVE-2024-42218 (Điểm CVSS: 6.3 – Trung bình):** Lỗ hổng tồn tại trên ứng dụng 1Password cho hệ điều hành macOS. Đối tượng tấn công có thể khai thác lỗ hổng bằng cách vượt qua các biện pháp bảo mật của macOS, qua đó cho phép đối tượng tấn công truy cập và trích xuất các thông tin lưu trong ứng dụng. Hiện lỗ hổng chưa có mã khai thác và chưa có ghi nhận 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-2018-0824	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Windows 7, Windows 8 Windows 10, Windows 11, Windows Server 2012. - 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-2018-0824
2	CVE-2024-42219	- Điểm CVSS: 7.0 (Cao) - Ảnh hưởng: 1Password - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - 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-2024-42219
3	CVE-2024-42218	- Điểm CVSS: 6.3 (Trung bình) - Ảnh hưởng: 1Password - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - 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-2024-42218
4	CVE-2024-38077	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Windows Server 2022, Windows Server 2012, Windows Server 2016, Windows Server 2019. - 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-2024-38077
5	CVE-2024-38856	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Apache OFBiz - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, 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-2024-38856

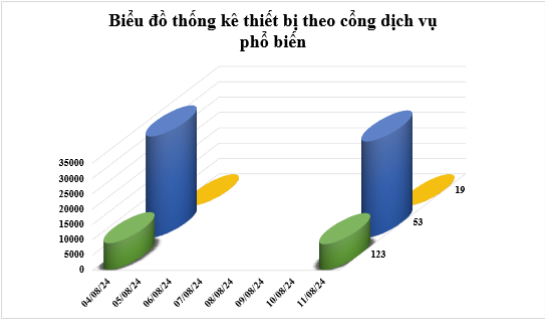
TOP 10 lỗ hổng đáng chú ý trong tuần

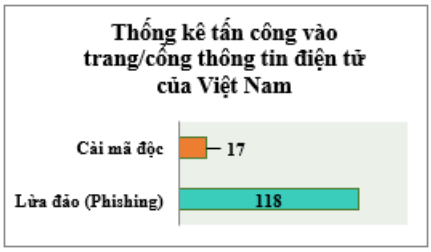
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-38100	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows Server 2016, Windows Server 2019, Windows Server 2022. - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-38100
7	CVE-2024-6782	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Calibre - 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-2024-6782
8	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
9	CVE-2024-20832	- Điểm CVSS: 6.4 (Trung bình) - Ảnh hưởng: Samsung. - Mô tả: Lỗ hổng cho phép đối tượng tấn công có quyền cục bộ khả năng thực thi mã tùy ý trên thiết bị. - 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-2024-20832
10	CVE-2024-3105	- Điểm CVSS: 9.9 (Nghiêm trọng) - Ảnh hưởng: Wordpress. - 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-2024-3105

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 **39.745** (giảm so với tuần trước **41.696**) 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.



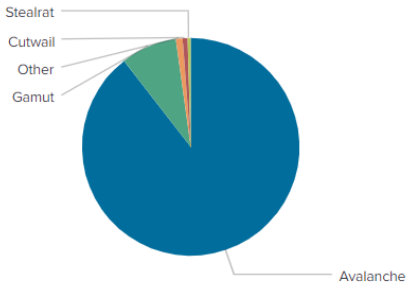


Tấn công Web

Trong tuần, có **135** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 118 trường hợp tấn công lừa đảo (Phishing), 17 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	andall.servicesql.info
disorderstatus.ru	restless.su
atomictrivia.ru	xiaoe.com
amnsreiuojy.ru	griefcube.cc
hzmksreiuojy.ru	spaines.pw
xjpakmdcfuqe.biz	sirec.in
restlesz.su	db2017417b23.zapto.org
xjpakmdcfuqe.com	zssryih.com
xjpakmdcfuqe.in	yxjsibeugmmj.com
xjpakmdcfuqe.ru	yvdcrvba.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **966** 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://vssid[.]pddgov[.]cc	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://www[.]govn[.]cc	Website giả mạo Bộ Công An
3	https://ggiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://www[.]dautuphattrienvnfic[.]com	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
5	https://dienmayxanh389[.]com	Website giả mạo Điện máy xanh
6	https://kbthuhoivontreo[.]com	Website giả mạo Kho bạc Nhà nước
7	https://www[.]baovietvay[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
8	https://baovietn[.]vip	Website giả mạo Ngân hàng TMCP Bảo Việt
9	https://ocb[.]hotrokhachhang-tructuyenthe[.]com	Website giả mạo Ngân hàng TMCP Phương Đông
10	https://hotro0nline28[.]com	Website giả mạo Ngân hàng TMCP Quân đội
11	https://mbbkh-canhan[.]com	Website giả mạo Ngân hàng TMCP Quân đội
12	https://mmbonline01[.]com	Website giả mạo Ngân hàng TMCP Quân đội
13	https://vib[.]cham-soc-the-truc-tuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
14	https://taichinheximbak[.]com	Website giả mạo Ngân Hàng TMCP Xuất Nhập Khẩu Việt Nam
15	https://www[.]shopeesopp[.]com	Website giả mạo sàn TMĐT Shopee
16	https://tikinew[.]club	Website giả mạo sàn TMĐT Tiki
17	https://tikijaj3[.]com	Website giả mạo sàn TMĐT Tiki
18	https://tikicareers[.]vip	Website giả mạo sàn TMĐT Tiki
19	https://chinhphu[.]thongtincutru[.]org	Website giả mạo Văn phòng Chính phủ
20	https://vnviettel[.]com	Website giả mạo Viettel

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