NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 25 (17/06/2024 – 23/06/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** UNC3886 khai thác lỗ hổng Zero-Day trên Fortinet và VMware để triển khai chiến dịch gián điệp kéo dài.

- **Cảnh báo:** VMware cập nhật bản vá cho Cloud Foundation, vCenter Server, và vSphere ESXi.

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: 965** 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: UNC3886 khai thác lỗ hổng Zero-Day trên Fortinet và VMware để triển khai chiến dịch gián điệp kéo dài"

Nhóm APT Trung Quốc UNC3886 đã bị phát hiện đang khai thác các lỗ hổng zero-day trên các thiết bị của Fortinet, Ivanti và VMware, sử dụng nhiều cơ chế duy trì kết nối để thực hiện hành vi gián điệp trên các thiết bị bị xâm nhập.

Các lỗ hổng bị khai thác bao gồm CVE-2022-41328 (Fortinet FortiOS), CVE-2022-22948 (VMware vCenter) và CVE-2023-20867 (VMware Tools), nhằm triển khai mã độc backdoor và đánh cắp thông tin xác thực. Nhóm UNC3886 chủ yếu nhằm vào các tổ chức ở Bắc Mỹ, Đông Nam Á và Châu Đại Dương, bao gồm các ngành viễn thông, công nghệ, hàng không vũ trụ, quốc phòng, năng lượng và các tổ chức chính phủ.

Nhóm UNC3886 đã sử dụng các rootkit như Reptile và Medusa để tránh bị phát hiện bởi các biện pháp bảo mật. Medusa được triển khai trên các máy ảo khách bằng bộ cài SEAELF. Khác với Reptile chỉ cung cấp giao diện tương tác với các chức năng rootkit, Medusa có khả năng ghi lại thông tin xác thực của người dùng từ các lần đăng nhập thành công, giúp nhóm này di chuyển dễ dàng trên hệ thống bị xâm nhập.

Ngoài ra, nhóm này còn phát tán mã độc backdoor MOPSLED và RIFLESPINE, sử dụng các dịch vụ GitHub và Google Drive làm kênh chỉ huy và điều khiển (C&C). MOPSLED, có khả năng là biến thể cải tiến của mã độc Crosswalk, là một mã độc module dựa trên shellcode, kết nối qua HTTP để tải xuống các plugin từ máy chủ C&C. Trong khi đó, RIFLESPINE là một công cụ đa nền tảng sử dụng Google Drive để truyền tải tệp và thực thi lệnh.

Các chuyên gia bảo mật cũng cho biết, UNC3886 đã triển khai các client SSH bị cài mã độc để thu thập thông tin xác thực sau khi khai thác CVE-2023-20867, đồng thời sử dụng Medusa để thiết lập các máy chủ SSH tùy chỉnh cho cùng mục đích.

Nguồn: https://thehackernews.com/2024/06/chinese-cyber-espionage-group-exploits.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: UNC3886 khai thác lỗ hổng Zero-Day trên Fortinet và VMware để triển khai chiến dịch gián điệp kéo dài"

Một số chủng mã độc khác được ghi nhận trong chiến dịch tấn công của nhóm này nhằm vào VMware bao gồm:

- Phiên bản trojan của daemon TACACS hợp pháp có chức năng ghi lại thông tin xác thực.
- VIRTUALSHINE, một mã độc backdoor dựa trên socket VMware VMCI, cho phép đối tượng tấn công truy cập vào bash shell.
- VIRTUALPIE, một mã độc backdoor Python có khả năng truyền tải tệp, thực thi mã tùy ý và thực hiện reverse shell.
- VIRTUALSPHERE, một module điều khiển liên quan đến mã độc backdoor dựa trên VMCI.

Các máy ảo đã trở thành mục tiêu hấp dẫn cho các đối tượng tấn công do sử dụng rộng rãi trong các môi trường đám mây. Một máy ảo bị xâm nhập có thể cung cấp cho đối tượng tấn công quyền truy cập không chỉ vào dữ liệu trong instance VM mà còn cả các quyền được gán cho nó.

Các tổ chức được khuyến nghị tuân theo các hướng dẫn bảo mật từ Fortinet và VMware để bảo vệ chống lại các mối đe dọa tiềm ẩn.

Một số IoC ghi nhận được:

8.222.218.20	207.246.64.38	152.32.231.251
8.222.216.144	149.28.122.119	152.32.205.208
8.219.131.77	155.138.161.47	152.32.144.15
8.219.0.112	154.216.2.149	152.32.129.162
8.210.75.218	103.232.86.217	123.58.207.86
8.210.103.134	103.232.86.210	123.58.196.34
47.252.54.82	103.232.86.209	118.193.63.40
47.251.46.35	58.64.204.165	118.193.61.71
47.246.68.13	58.64.204.142	118.193.61.178
47.243.116.155	58.64.204.139	45.77.106.183
47.241.56.157	165.154.7.145	45.32.252.98
165.154.134.40	165.154.135.108	0

Nguồn: https://thehackernews.com/2024/06/chinese-cyber-espionage-group-exploits.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: VMware cập nhật bản vá cho Cloud Foundation, vCenter Server, và vSphere ESXi"

Trong tuần vừa qua, VMware đã phát hành các bản vá nhằm khắc phục các lỗ hổng nghiêm trọng ảnh hưởng đến Cloud Foundation, vCenter Server và vSphere ESXi, có thể bị khai thác bởi đối tượng tấn công để leo thang đặc quyền và thực thi mã từ xa.

Cụ thể, các lỗ hổng bao gồm:

- **CVE-2024-37079 & CVE-2024-37080 (Điểm CVSS: 9.8)** – Các lỗ hổng tràn heap (heap-overflow) trong việc triển khai giao thức DCE/RPC, cho phép đối tượng tấn công với quyền truy cập mạng tới vCenter Server thực thi mã từ xa thông qua các gói tin cụ thể.
- **CVE-2024-37081 (Điểm CVSS: 7.8)** – Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền cục bộ trong VMware vCenter do cấu hình sai sudo, cho phép người dùng cục bộ đã xác thực khai thác để lấy quyền root.

Đây không phải lần đầu VMware phải giải quyết các vấn đề về giao thức DCE/RPC. Trước đó, vào tháng 10/2023, họ đã vá một lỗ hổng bảo mật khác (CVE-2023-34048) cũng có khả năng thực thi mã từ xa.

CVE-2024-37079 và CVE-2024-37080 đã được phát hiện bởi một cơ quan bảo mật tại Trung Quốc. Trong khi đó, CVE-2024-37081 được phát hiện bởi một chuyên gia bảo mật tại Deloitte Romania.

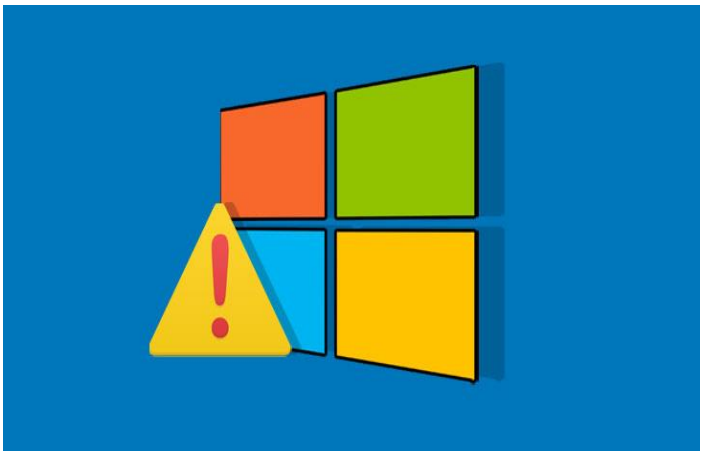
Cả ba lỗ hổng này ảnh hưởng tới vCenter Server phiên bản 7.0 và 8.0, và đã được vá trong các phiên bản 7.0 U3r, 8.0 U1e và 8.0 U2d.

Hiện chưa có báo cáo về việc các lỗ hổng này bị khai thác trong thực tế. Tuy nhiên, người dùng cần nhanh chóng cập nhật bản vá để tránh những rủi ro tiềm ẩn.

Nguồn: https://thehackernews.com/2024/06/vmware-issues-patches-for-cloud.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 **991** lỗ hổng, trong đó có 244 lỗ hổng mức Cao, 448 lỗ hổng mức Trung bình, 28 lỗ hổng mức Thấp và 271 lỗ hổng chưa đánh giá. Trong đó có ít nhất 275 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 Microsoft và ngôn ngữ lập trình PH, cụ thể là như sau:

- **CVE-2024-26169 (Điểm CVSS: 7.8 – Cao):** Lỗ hổng tồn tại trên Microsoft Windows Error Reporting cho phép đối tượng tấn công leo thnag đặc quyền. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-4577 (Điểm CVSS: 9.8 – Nghiêm trọng):** Là lỗ hổng tồn tại trong ngôn ngữ lập trình PHP trên Apache và PHP-CGI của Windows. Lỗ hổng xảy ra do Windows sử dụng hành vi "Best-Fit" để thay thế kí tự trong command line cung cấp tới hàm Win32 API. Đối tượng tấn công có thể khai thác lỗ hổng để truyền các tùy chỉnh độc hại tới binary PHP qua đó biết được mã nguồn, thực thi đoạn mã PHP tùy ý trên máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai thai thác trong thực tế.
- **CVE-2024-30078 (Điểm CVSS: 8.8 – Cao):** Là lỗ hổng tồn tại trên driver Wi-Fi của Microsoft Windows cho phép đối tượng tấn công thực thi mã từ xa sử dụng các gói tin độc hại. Hiện lỗ hổng 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-2024-26169	- 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-2024-26169
2	CVE-2024-30078	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows CSC - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-30078
3	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - 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
4	CVE-2024-26229	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows CSC - 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-2024-26229
5	CVE-2024-29973	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Zyxel - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi các câu lệnh OS từ xa thông qua yêu cầu HTTP POST. - 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-2024-29973

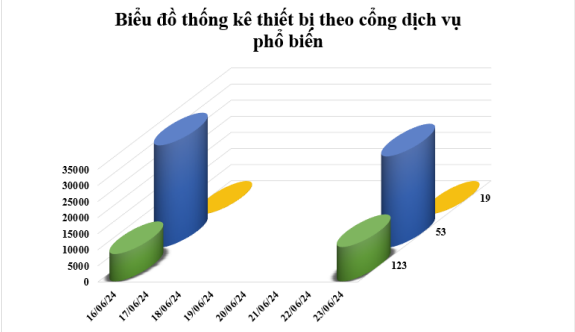
TOP 10 lỗ hổng đáng chú ý trong tuần

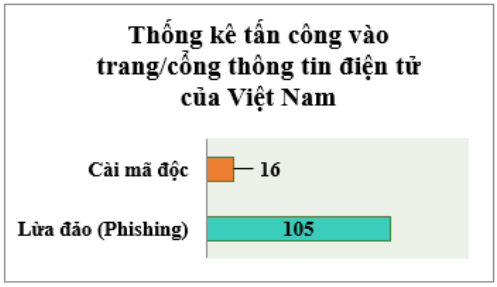
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-3080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: ASUS Router. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3080
7	CVE-2024-3400	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-OS - 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-2024-3400
8	CVE-2024-37079	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: vCenter Server - 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-2024-37079
9	CVE-2024-37080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: vCenter Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-37080
10	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

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 **39.057** (giảm so với tuần trước **40.304**) 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.



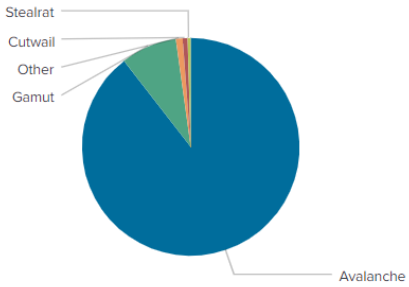


Tấn công Web

Trong tuần, có **121** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 105 trường hợp tấn công lừa đảo (Phishing), 16 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	restless.su
disorderstatus.ru	andall.servicesql.info
atomictrivia.ru	db2017417b23.zapto.org
amnsreiuojy.ru	mcnodes.zapto.org
xjpakmdcfuqe.biz	maxisurf.net
hzmksreiuojy.ru	cicqdaqtrws.info
restlesz.su	ynefefyopqvu.com
xjpakmdcfuqe.com	wioabfwyigasfbksl.org
xjpakmdcfuqe.in	wdxzlv.org
xjpakmdcfuqe.ru	rgbppxtvieoytnoej.org

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **965** 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[.]govvvn[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://vssidgov[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
3	nappthe[.]vn	Website giả mạo Công Ty Cổ Phần Giải Trí Và Thể Thao Điện Tử Việt Nam
4	https://binhchoncuocthivetranhsinhvien2024[.]weebly[.]com	Website giả mạo Facebook
5	https://la5959[.]com	Website giả mạo sàn TMĐT Lazada
6	https://tcbcanhan[.]com	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
7	vib-up-the[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
8	vib-cardnew[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
9	vib-nang-the[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	nang-cap-the-vcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	https://tpbank[.]chamsockhachhang-uudaithe-thang6[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
12	https://sp1776p[.]com	Website giả mạo sàn TMĐT Shopee
13	sp7335p[.]com	Website giả mạo sàn TMĐT Shopee
14	https://vnc63661s[.]com	Website giả mạo sàn TMĐT Shopee
15	https://s2rjtiki[.]com	Website giả mạo sàn TMĐT Tiki
16	https://k2rjtiki[.]com	Website giả mạo sàn TMĐT Tiki
17	https://sh2tiki[.]com	Website giả mạo sàn TMĐT Tiki
18	https://viettlot135p[.]com	Website giả mạo Vietlott
19	https://giaodichquoctes[.]vercel[.]app	Website giả mạo Western Union
20	https://giaodichquoctes[.]com	Website giả mạo Western Union

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