NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 30 (22/07/2024 – 28/07/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Trung Quốc sử dụng mã độc MgBot và MACMA để tấn công Đài Loan và tổ chức phi chính phủ Mỹ.

- **Cảnh báo:** Lỗ hổng Zero-day trên Telegram cho phép phát tán APK Android độc hại dưới dạng video.

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: 1573** 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 sử dụng mã độc MgBot và MACMA để tấn công Đài Loan và tổ chức phi chính phủ Mỹ"

Các tổ chức tại Đài Loan và một tổ chức phi chính phủ (NGO) của Mỹ đặt tại Trung Quốc đã trở thành mục tiêu của nhóm APT Daggerfly, một nhóm tấn công mạng được Bắc Kinh hậu thuẫn. Nhóm này sử dụng các công cụ mã độc đã được nâng cấp để thực hiện các cuộc tấn công.

Chiến dịch này cho thấy Daggerfly cũng tham gia vào hoạt động gián điệp nội bộ. Trong đó, Daggerfly đã khai thác lỗ hổng CVE-2024-38112 tồn tại trên máy chủ Apache HTTP để phát tán mã độc MgBot. Lỗ hổng này đã được Microsoft khắc phục trong bản vá Patch Tuesday gần nhất, được đánh giá là một lỗ hổng spoofing trong động cơ trình duyệt MSHTML của Internet Explorer.

Daggerfly, còn được biết đến với tên Bronze Highland và Evasive Panda, đã hoạt động từ năm 2012 và từng sử dụng mã độc MgBot trong các chiến dịch thu thập thông tin từ các nhà cung cấp dịch vụ viễn thông tại Châu Phi.

Ngoài mã độc MgBot, Daggerfly còn sử dụng phiên bản cải tiến của mã độc MgBot trên hệ điều hành macOS có tên MACMA. MACMA được phát hiện lần đầu vào tháng 11/2021 bởi nhóm Threat Analysis Group của Google, mã độc này phát tán qua các cuộc tấn công watering hole nhắm vào người dùng tại Hong Kong bằng cách khai thác lỗ hổng trên trình duyệt Safari. Được biết MACMA tái sử dụng mã nguồn từ các nhà phát triển ELF/Android, cho thấy khả năng nó cũng đã nhằm vào điện thoại Android.

Bằng chứng cho thấy mã độc MACMA có liên quan đến nhóm Daggerfly dựa trên sự trùng lặp mã nguồn với MgBot và kết nối đến máy chủ C&C có IP 103.243.212[.]98, đây là IP từng được dropper của mã độc MgBot sử dụng.

Nguồn: https://thehackernews.com/2024/07/chinese-hackers-target-taiwan-and-us.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Trung Quốc sử dụng mã độc MgBot và MACMA để tấn công Đài Loan và tổ chức phi chính phủ Mỹ"

Ngoài hai mã độc trên, Daggerfly còn sử dụng thêm mã độc Nightdoor (hay NetMM và Suzafk), một mã độc gài vào hệ thống sử dụng Google Drive API làm C&C và đã được sử dụng trong các cuộc tấn công watering hole nhằm vào người dùng Tây Tạng kể từ tháng 9 năm 2023.

Thông tin về nhóm Daggerfly và chiến dịch này được công bố ngay sau khi Trung tâm Ứng phó Khẩn cấp Virus Máy tính Quốc gia (CVERC) của Trung Quốc cáo buộc rằng Volt Typhoon, được Five Eyes xác định là nhóm gián điệp mạng của Trung Quốc, thực tế đây là một chiến dịch tin giả do các cơ quan tình báo Mỹ dựng lên nhằm bôi nhọ Trung Quốc.

Một số IoC được ghi nhận:

103.243.212[.]98
103.96.131[.]150
103.96.128[.]44

Nguồn: https://thehackernews.com/2024/07/chinese-hackers-target-taiwan-and-us.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng Zero-day trên Telegram cho phép phát tán APK Android độc hại dưới dạng video"

Một lỗ hổng Zero-day trên Telegram, được gọi là "EvilVideo," đã bị khai thác để gửi các file APK độc hại dưới dạng video đến thiết bị Android. Lỗ hổng này đã được rao bán từ ngày 06/6/2024 bởi một đối tượng có tên là "Ancryno" trên diễn đàn XSS hacking tiếng Nga, và được cho là ảnh hưởng đến các phiên bản Telegram cũ hơn v10.14.4.

Lỗ hổng này được phát hiện sau khi một minh họa PoC được chia sẻ trên kênh Telegram công khai, giúp các chuyên gia bảo mật tại ESET tiếp cận được payload độc hại. Sau khi phân tích, ESET xác nhận lỗ hổng hoạt động như mô tả và đã thông báo cho Telegram vào ngày 26/6 và một lần nữa vào ngày 04/7. Lỗ hổng này đã được vá trong phiên bản v10.14.5 phát hành vào ngày 11/7/2024.

Hiện chưa có thông tin rõ ràng về việc lỗ hổng có bị khai thác trong thực tế hay không, tuy nhiên, các chuyên gia đã phát hiện máy chủ C&C sử dụng bởi payload có địa chỉ "infinityhackscharan.ddns[.]net".

Chi tiết về việc khai thác lỗ hổng Zero-day

Lỗ hổng "EvilVideo" ảnh hưởng đến phiên bản Android của Telegram và cho phép đối tượng tấn công tạo ra các tệp APK độc hại được gửi tới người dùng dưới dạng video. Lỗ hổng này sử dụng API của Telegram để tạo các tin nhắn giả dạng video dài 30 giây.

Với cài đặt mặc định, ứng dụng Telegram trên Android sẽ tự động tải xuống các tệp phương tiện như ảnh và video. Do đó, người dùng chỉ cần mở kênh chứa tin nhắn payload là đã có thể bị nhiễm mã độc ngay lập tức. Nếu tắt tính năng tự động tải xuống, người dùng vẫn có nguy cơ lây nhiễm chỉ bằng một lần click vào video. Khi video giả được mở, Telegram sẽ hiện thông báo yêu cầu chọn trình phát video bên ngoài. Nếu người dùng đồng ý, payload sẽ được thực thi. Tiếp theo, người dùng sẽ được yêu cầu cài đặt một ứng dụng dạng APK thông qua Telegram, ứng dụng này có tên là "xHamster Premium Mod".

Việc khai thác lỗ hổng này yêu cầu người dùng thực hiện nhiều bước để payload độc hại có thể được thực thi trên thiết bị, vì vậy nguy cơ thành công của cuộc tấn công là tương đối thấp.

Nguồn: https://www.bleepingcomputer.com/news/security/telegram-zero-day-allowed-sending-malicious-android-apks-as-videos/

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 **613** lỗ hổng, trong đó có 132 lỗ hổng mức Cao, 234 lỗ hổng mức Trung bình, 18 lỗ hổng mức Thấp và 229 lỗ hổng chưa đánh giá. Trong đó có ít nhất 68 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 Progress, OpenSSH và Rejetto, cụ thể là như sau:

- **CVE-2024-6327 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Progress Telerik Report Server, xảy ra do quy trình giải tuần tự thiếu bảo mật của sản phẩm. Đối tượng tấn công khai thác lỗ hổng có thể thực thi mã từ xa trên hệ thống. Hiện lỗ hổng đang bị khai thác trong thực tế.
- **CVE-2024-6387 (Điểm CVSS: 8.1 – Cao):** Lỗ hổng tồn tại trên máy chủ OpenSSH cho phép đối tượng tấn công khai thác lỗi Race Condition, cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-23692 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Rejetto HTTP File Server, đối tượng tấn công có thể khai thác lỗ hổng bằng cách gửi tới hệ thống các yêu cầu HTTP độc hại, qua đó có thể thực thi mã tùy ý. 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-2024-6327	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Progress Telerik Report Server. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-6327
2	CVE-2024-23692	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Rejetto HTTP File 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-2024-23692
3	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
4	CVE-2024-0044	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Android 12, Android 13 - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-0044
5	CVE-2024-32002	- Điểm CVSS: 9.0 (Nghiêm trọng) - Ảnh hưởng: Git. - 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-2024-32002

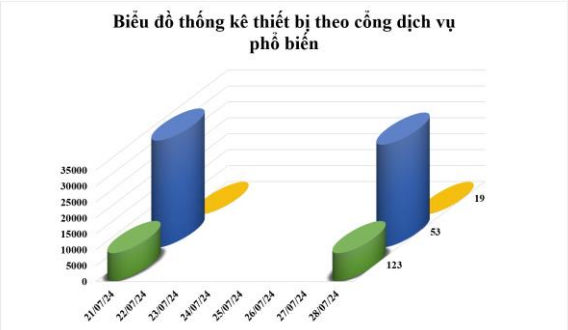
TOP 10 lỗ hổng đáng chú ý trong tuần

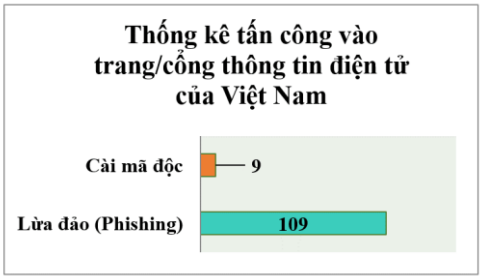
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-21412	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Server 2022. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-21412
7	CVE-2024-41110	- Điểm CVSS: 9.9 (Nghiêm trọng) - Ảnh hưởng: Docker Engine. - 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-2024-41110
8	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 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-2024-38112
9	CVE-2024-34102	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Adobe Commerce - 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-2024-34102
10	CVE-2024-20419	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Cisco Smart Software Manager On-Prem (SSM On-Prem). - 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-2024-20419

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 **41.090** (giảm so với tuần trước **42.408**) 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.



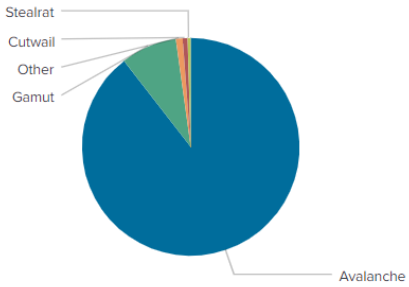


Tấn công Web

Trong tuần, có **118** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 109 trường hợp tấn công lừa đảo (Phishing), 9 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	elitiorecfreetoo.cc
amnsreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	wildrive.com
hzmksreiuojy.ru	upinflinstrix.org
restlesz.su	nnrlerczlj.org
xjpakmdcfuqe.com	maxisurf.net
xjpakmdcfuqe.ru	lsvlkvikynodaywlo.com
xjpakmdcfuqe.in	fe6e4998-6897-11eb-974b-005056834623.captainbicycle.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **1573** 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[.]govnn[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://icchanoi[.]net/	Website giả mạo Công ty Cổ phần Đầu tư Quốc tế ICC Hà Nội
3	https://homecredit[.]hethongvaynhanh247[.]com/	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
4	https://mfacebook-com[.]vn/	Website giả mạo Facebook
5	https://bethivetranh2024[.]weebly[.]com	Website giả mạo Facebook
6	https://www[.]hethongnhanvien[.]com	Website giả mạo sàn TMĐT Lazada
7	https://da1215[.]com	Website giả mạo sàn TMĐT Lazada
8	https://lazadaevent[.]com/	Website giả mạo sàn TMĐT Lazada
9	https://www[.]momoshopvip[.]com	Website giả mạo MoMo
10	https://www[.]baovietcom[.]vip/	Website giả mạo Ngân hàng TMCP Bảo Việt
11	https://vietinbankamc[.]vn	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
12	https://khtechcanhan[.]com/	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
13	https://mcqdvn[.]com	Website giả mạo Ngân hàng TMCP Quân đội
14	https://centralmarketing[.]online/	Website giả mạo Ngân hàng Worldbank Việt Nam
15	https://nze98582s[.]com/	Website giả mạo sàn TMĐT Shopee
16	https://www[.]tikifreeship[.]vip/	Website giả mạo sàn TMĐT Tiki
17	https://tdke00[.]com/	Website giả mạo sàn TMĐT Tiki
18	https://www[.]vntiki[.]vip	Website giả mạo sàn TMĐT Tiki
19	https://tdke02[.]com	Website giả mạo sàn TMĐT Tiki
20	https://xacnhanthutuchoantra[.]us/	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