NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 38 (18/9/2023 – 24/9/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Transparent Tribe sử dụng ứng dụng giả mạo YouTube trên Android để phát tán mã độc CapraRAT.

- **Cảnh báo:** Mã độc SprySOCKS trên Linux - Cuộc tấn công chính phủ của Earth Lusca.

2. Điểm yếu, lỗ hổng

- **425** lỗ hổng được công bố và cập nhật.

- **07** lỗ hổng, nhóm lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Tấn công lừa đảo người dùng Việt Nam: 396** 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://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Transparent Tribe sử dụng ứng dụng giả mạo YouTube trên Android để phát tán mã độc CapraRAT"

Nhóm APT Transparent Tribe bị phát hiện khi sử dụng một ứng dụng giả mạo YouTube trên các thiết bị Android để phát tán mã độc CapraRAT, đây là một phần mềm truy cập từ xa (RAT). Trojan này là một công cụ xâm nhập cho phép đối tượng tấn công kiểm soát phần lớn dữ liệu trên thiết bị Android bị lây nhiễm.

Nhóm Transparent Tribe, còn được biết đến với biệt danh APT36, đã nổi tiếng với các chiến dịch tấn công dưới hình thức xâm nhập vào hệ thống chạy Windows, Linux và Android, nhằm mục đích thu thập thông tin từ người dùng Ấn Độ.

Trong bộ công cụ của họ, CapraRAT đóng một vai trò quan trọng và đã được phát tán dưới dạng các ứng dụng nhắn tin và cuộc gọi giả mạo, hoạt động như một loại trojan với tên gọi MeetsApp và MeetUp. Những ứng dụng này đã được phát tán tới người dùng bằng hình thức tấn công Social engineering.

Hiện tại, các tệp tin APK độc hại mới nhất đã được xác định là giả mạo của ứng dụng YouTube và một trong những ứng dụng đó có liên kết tới kênh "Piya Sharma" trên Youtube.

Các ứng dụng độc hại này đều sử dụng tên giống với các ứng dụng thật, điều này cho thấy rõ đối tượng tấn công đang dùng chiêu trò để đánh lừa người dùng cài đặt chúng. Danh sách ứng dụng được phát hiện bao gồm:

- com.Base.media.service
- com.moves.media.tubes
- com.videos.watchs.share

Sau khi được cài đặt, ứng dụng sẽ gửi được cấp quyền có tính xâm phạm, cho phép mã độc thu thập dữ liệu trên thiết bị và chuyển chúng tới máy chủ do đối tượng tấn công điều khiển. Ngoài ra, CapraRAT cũng có khả năng thực hiện cuộc gọi và ngăn chặn tin nhắn SMS đến.

Theo đánh giá của các chuyên gia bảo mật, Transparent Tribe là một đối tượng tấn công sử dụng các phương thức tấn công giả mạo trong thời gian dài. Nhóm này thường sử dụng các công cụ được thiết kế với mức độ bảo mật thấp nên dễ dàng bị phát hiện. Các chuyên gia cũng khuyến nghị các cá nhân và tổ chức có liên quan đến ngoại giao, quân đội, hoặc các sự kiện xã hội tại Ấn Độ và Pakistan cần thực hiện các biện pháp đánh giá phòng thủ để kịp thời ứng phó với nguy cơ tấn công mạng.

Nguồn:
https://thehackernews.com/2023/09/transparent-tribe-uses-fake-youtube.html

Tin tức An toàn thông tin

"Cảnh báo: Mã độc SprySOCKS trên Linux - Cuộc tấn công chính phủ của Earth Lusca"

Nhóm tấn công mạng Earth Lusca được cho là có liên quan đến Trung Quốc, đã sử dụng một backdoor Linux mới có tên là SprySOCKS để tiến hành các cuộc tấn công cơ quan chính phủ. Nhóm này hoạt động kể từ năm 2021 và lần đầu bị phát hiện vào tháng 01/2022 khi đang thực hiện chiến dịch tấn công nhằm vào các tổ chức công cộng và tư nhân tại châu Á, Úc, châu Âu và Bắc Mỹ.

Earth Lusca thường sử dụng các hình thức "spear-phishing" và "watering hole attacks" để thực hiện các cuộc tấn công gián điệp mạng. Đối tượng tấn công nhắm đến thường là các cơ quan chính phủ trong lĩnh vực ngoại giao, công nghệ và viễn thông, chủ yếu tập trung ở Đông Nam Á, Trung Á và Balkan.

Chiến dịch tấn công bắt đầu bằng việc khai thác các lỗ hổng bảo mật trên các máy chủ công cộng chạy trên các ứng dụng sau:

- Fortinet (CVE-2022-39952 và CVE-2022-40694)
- GitLab (CVE-2021-22205)
- Microsoft Exchange Server (ProxyShell)
- Progress Telerik UI (CVE-2019-18935)
- Zimbra (CVE-2019-9621 và CVE-2019-9670)

Sau đó, nhóm này triển khai các công cụ và phần mềm độc hại, chẳng hạn như Cobalt Strike, để tiến hành các hoạt động xâm nhập và gián điệp mạng. Mục tiêu chính là đánh cắp tài liệu và thông tin đăng nhập tài khoản email. Bên cạnh đó, triển khai các backdoor tiên tiến khác như ShadowPad và phiên bản Linux của Winnti để thực hiện các hoạt động gián điệp dài hạn trên thiết bị lây nhiễm. Điều này đặt ra nghi vấn rằng Earth Lusca có liên quan đến Trung Quốc, bởi vì có sự tương đồng về mục tiêu và phương thức tấn công với một số nhóm tấn công đã bị phát hiện trước đó.

Có ít nhất hai phiên bản của SprySOCKS đã được xác định cho đến nay, cho thấy rằng nhóm này không ngừng cập nhật và nâng cấp mã độc để thêm các tính năng mới. Trong nửa đầu của năm 2023, Earth Lusca đã mở rộng phạm vi hoạt động của họ để tiến hành các cuộc tấn công vào các tổ chức trên toàn cầu.

Trong bối cảnh này, các tổ chức cần phòng thủ bằng cách quản lý phạm vi bị tấn công và tối thiểu hóa các điểm truy cập vào hệ thống để giảm thiểu khả năng xảy ra xâm nhập. Đồng thời, cần phải thường xuyên cập nhật bản vá, công cụ, phần mềm và hệ thống nhằm đảm bảo tính bảo mật, chức năng và hoạt động của đơn vị.

Nguồn: https://thehackernews.com/2023/09/earth-luscas-new-sprysocks-linux.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 **425** lỗ hổng, trong đó có 179 lỗ hổng mức Cao, 99 lỗ hổng mức Trung bình, 05 lỗ hổng mức Thấp và 142 lỗ hổng chưa đánh giá. Trong đó có ít nhất 117 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam: Nhóm 59 lỗ hổng trong Microsoft, Nhóm 14 lỗ hổng trong Mozilla, Nhóm 34 lỗ hổng trong Google, Nhóm 28 lỗ hổng trong Wordpress, Nhóm 21 lỗ hổng trong Adobe, Nhóm 03 lỗ hổng trong Linux, Nhóm 09 lỗ hổng trong IBM. Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- Microsoft: CVE-2023-33136, CVE-2023-36764,...

- Mozilla: CVE-2023-4582, CVE-2023-4584,...

- Google: CVE-2023-35681, CVE-2023-35658,...

- Wordpress: CVE-2023-4153, CVE-2023-4213,...

- Adobe: CVE-2023-38204, CVE-2022-24093,...

- Linux: CVE-2023-4881, CVE-2023-4155,...

- IBM: CVE-2023-33164, CVE-2023-38736,...

Thông tin điểm yếu, lỗ hổng

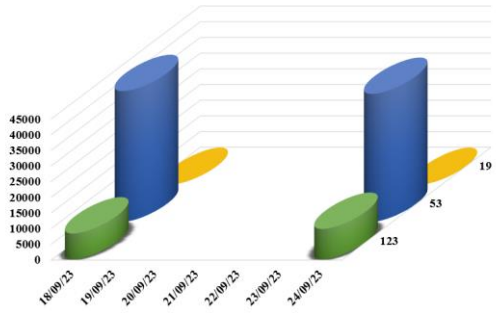
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-33136 CVE-2023-36764 CVE-2023-38146 ...	Nhóm 59 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, khai thác lỗi XSS, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Mozilla	CVE-2023-4582 CVE-2023-4584 CVE-2023-4585 ...	Nhóm 14 lỗ hổng trong Mozilla cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi Buffer Overflow.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-35681 CVE-2023-35658 CVE-2023-35673 ...	Nhóm 34 lỗ hổng trong Google cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-4153 CVE-2023-4213 CVE-2023-4916 ...	Nhóm 28 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi XSS, thực hiện tấn công CSRF.	Chưa có thông tin xác nhận và bản vá
5	Adobe	CVE-2023-38204 CVE-2022-24093 CVE-2022-28831 ...	Nhóm 21 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi XSS, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Linux	CVE-2023-4881 CVE-2023-4155 CVE-2023-4921 ...	Nhóm 03 lỗ hổng trong Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2022-33164 CVE-2023-38736 CVE-2022-22401 ...	Nhóm 09 lỗ hổng trong IBM phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

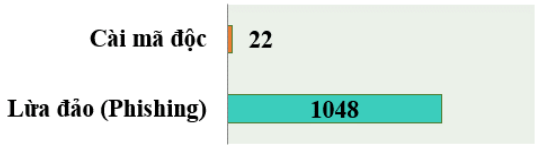
Tấn công DRDoS

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 **50.584**, (tăng so với tuần trước **50.021**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

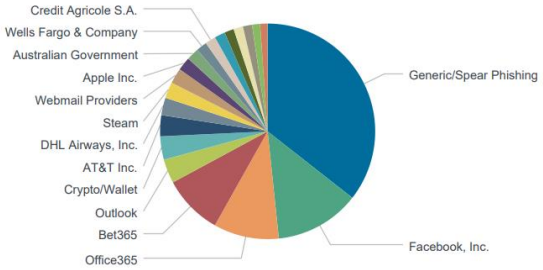


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **1070** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 1048 trường hợp tấn công lừa đảo (Phishing), 22 trường hợp tấn công cài cắm mã độc.



Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,v.v…Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và tính phí) như các mạng xã hội, Payment, Apple, Paypal,v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để đánh cắp tài khoản.

Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

184.105.192.2: 11308 IP	216.218.135.114: 31 IP
216.218.185.162: 131 IP	64.71.166.50: 11 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **396** 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 website của ngân hàng, các trang thương mại điện tử…

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	spohopenm.com	Website giả mạo sàn TMĐT Shopee
2	mbbankmn.com	Website giả mạo Ngân hàng TMCP Quân đội
3	tafcaz.com	Website giả mạo sàn TMĐT Tiki
4	pouy99uo.com	Website giả mạo sàn TMĐT Lazada
5	dienmayxanh.cloud dienmayxanh269.com thegiodidong.com.vn	Website giả mạo Điện máy xanh, Công ty cổ phần Thế Giới Di Động
6	upmiles-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
7	travelokeaaa.vip travelokeaaa.top	Website giả mạo Traveloka
8	vn-vietnam.com	Website giả mạo sàn TMĐT Amazon
9	shbcredit.net	Website giả mạo Ngân hàng Sài Gòn Hà Nội SHB

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 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, những đơn vị đã có tài khoản trên "Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động" tại địa chỉ https://service.khonggianmang.vn, quản trị viên có thể thêm các sản phẩm đang sử dụng để giám sát và nhận cảnh báo ngay khi có lỗ hổng mới phát sinh.

***

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**, Quý đơn vị cần chú ý quan tâm không truy cập vào các trang web được nêu để tránh nguy cơ bị tấn công lừa đảo, nâng cao nhận thức bản thân và tuyên truyền cho bạn bè, người thân và những người xung quanh tránh việc trở thành nạn nhân của những cuộc tấn công lừa đảo này.

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