NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 40 (02/10/2023 – 08/10/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT TA505 sử dụng công cụ Sneaky RMS trong chiến dịch lừa đảo mới nhất.

- **Cảnh báo:** Apple phát hành bản vá bảo mật cho lỗ hổng Zero Day đang bị khai thác trên iOS.

2. Điểm yếu, lỗ hổng

- **583** 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: 338** 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 TA505 sử dụng công cụ Sneaky RMS trong chiến dịch lừa đảo mới nhất"

Nhóm APT TA505 đang triển khai một chiến dịch lừa đảo tinh vi bằng cách sử dụng tệp thực thi Hệ thống quản lý từ xa (RMS) để tấn công người dùng ở các quốc gia mục tiêu, đặc biệt là ở Nga. Tệp thực thi RMS được xem là một công cụ quản lý từ xa uy tín và là một yếu tố then chốt trong các cuộc tấn công của TA505. Đáng chú ý, mã độc này đã phát tán trên nhiều trang web lừa đảo khác nhau, điều này cho thấy rõ sự liên quan giữa nhóm APT TA505 và cộng đồng người Nga.

Bắt đầu hoạt động từ năm 2014, nhóm TA505 trở nên nổi tiếng với những cuộc tấn công ransomware thông qua biến thể Clop. Việc sử dụng công cụ RMS thể hiện tính phức tạp trong chiến thuật tấn công của nhóm này, điều này đã giúp TA505 chiếm được quyền truy cập sớm và thực hiện các chiến dịch tấn công trên phạm vi toàn cầu một cách hiệu quả.

Sự bùng nổ của chiến dịch lừa đảo bằng việc giả mạo các ứng dụng bị chặn

Xu hướng sử dụng các ứng dụng bị chặn để khai thác lỗ hổng bảo mật đang ngày càng trở nên phổ biến, chiến dịch VASTFLUX là minh chứng rõ rệt cho các rủi ro có thể gây ra khi đã ảnh hưởng tới 11 triệu thiết bị thông qua việc giả mạo hơn 1700 ứng dụng từ 120 nhà phát triển.

Hiện tại, các chiến dịch sử dụng kỹ thuật giả mạo ứng dụng bị chặn chủ yếu tập trung tại Nga do những hạn chế về mặt pháp lý.

Kỹ thuật tấn công của nhóm APT TA505

Trong chiến dịch tấn công lừa đảo, nhóm APT TA505 đã sử dụng hàng loạt kỹ thuật tinh vi để đánh lừa người dùng:

Sử dụng công cụ RMS (Remote Management System): TA505 sử dụng một công cụ Quản lý Từ xa (RMS) để triển khai chiến dịch tấn công. Công cụ này cho phép đối tượng tấn công thực hiện các hoạt động từ xa trên máy tính của nạn nhân, như truyền tệp và chia sẻ màn hình.

Phát tán payload độc hại thông qua website lừa đảo: TA505 sử dụng các trang web lừa đảo để phát tán mã độc. Cụ thể, nhóm này sử dụng các tệp thực thi RMS và ẩn mã độc trong các tệp nén tự giải nén (SFX), điều này giúp họ che giấu payload độc hại.

Lợi dụng sự phổ biến của các ứng dụng bị chặn: Chiến dịch của nhóm APT TA505 tận dụng lòng tin của người dùng đối với các ứng dụng bị chặn. Ví dụ, khi người dùng tải xuống một ứng dụng giả mạo giống như ExpressVPN thông qua trang web lừa đảo, họ sẽ thực tải một folder SFX. Khi thực thi, nó sẽ giả mạo thành một trình cài đặt ExpressVPN chính thống, trong khi thực tế đang tải về payload độc hại.

Sử Dụng Khóa Registry và Thư Mục Tạm Thời: File SFX sau đó sẽ chèn dữ liệu vào khóa Registry "HKCUSoftwareWinRAR SFX" và tạo một thư mục trong %TMP% để lưu trữ cả tệp thực thi RMS lẫn trình cài đặt ExpressVPN thật.

Sự trở lại của công cụ RMS trong chiến dịch này được xem như một nỗ lực nhằm tấn công những người thiếu kiến thức về an toàn thông tin. Bằng cách sử dụng các ứng dụng bị chặn tại các quốc gia, nhóm APT TA505 đã linh hoạt và cải thiện các biện pháp để chiến thuật tấn công ngày càng trở nên tinh vi hơn và hiệu quả hơn.

Nguồn: https://thecyberexpress.com/ta505-hacker-rms-tool-phishing-campaign/?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Apple phát hành bản vá bảo mật cho lỗ hổng Zero Day đang bị khai thác trên iOS"

Trong tuần vừa qua, Apple đã phát hành các bản vá bảo mật cho lỗ hổng zero-day trên iOS và iPadOS đang bị khai thác.

Một trong những lỗ hổng đáng chú ý là CVE-2023-42824 nằm ở tầng kernel của hệ thống, cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Mặc dù Apple đã giải quyết vấn đề này trong các bản vá bảo mật mới nhưng thông tin cụ thể về hình thức tấn công và danh tính của các đối tượng này chưa được tiết lộ. Tuy nhiên, để khai thác thành công, khả năng cao là trước đó các đối tượng tấn công đã xâm nhập vào thiết bị.

Ngoài ra, trong bản vá bảo mật này, Apple cũng đã xử lý lỗ hổng CVE-2023-5217 ảnh hưởng tới thành phần WebRTC, trước đây được Google mô tả là một lỗ hổng tràn bộ đệm dựa trên heap, trong định dạng VP8 trên thư viện libvpx.

Bản vá iOS 17.0.3 và iPad 17.0.3 hiện đã có sẵn trên các thiết bị sau:

- iPhone XS trở lên
- iPad Pro 12.9 inch từ thế hệ 2 trở lên, iPad Pro 10.5 inch, iPad Pro 11 inch từ thế hệ 1 trở lên, iPad Air từ thế hệ 3 trở lên, iPad từ thế hệ 6 trở lên và iPad mini từ thế hệ 5 trở lên.

Hiện tại, Apple đã giải quyết tổng cộng 17 lỗ hổng zero-day đã bị khai thác kể từ đầu năm nay.

Bản vá mới được phát hành sau khoảng 2 tuần kể từ khi Cupertino xử lý 3 lỗ hổng (CVE-2023-41991, CVE-2023-41992 và CVE-2023-41993) đã bị một nhà cung cấp phần mềm gián điệp có tên là Cytrox sử dụng để phát tán mã độc Predator tới iPhone của một cựu thành viên quốc hội tại Ai Cập vào đầu năm nay.

Một điểm đáng chú ý là CVE-2023-41992 cũng đề cập đến một khiếm khuyết trong kernel cho phép đối tượng tấn công leo thang đặc quyền. Hiện vẫn chưa rõ rằng hai lỗ hổng này có liên quan đến nhau không, hoặc có thể CVE-2023-42842 là một bản vá bypass cho CVE-2023-41992.

Theo phân tích, các cơ quan bảo mật đã tìm thấy một số điểm tương đồng trong cơ sở hạ tầng và công nghệ phần mềm độc hại của một nhà cung cấp phần mềm có tên là Cytrox (còn gọi là Lycantrox) và một công ty phần mềm khác có tên là Candiru (còn gọi là Karkadann).

Đối với người dùng có nguy cơ bị tấn công bởi lỗ hổng này, cần kích hoạt chế độ Lockdown để giảm thiểu khả năng bị tấn công từ các phần mềm độc hại spyware.

Nguồn: https://thehackernews.com/2023/10/apple-rolls-out-security-patches-for.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 **583** lỗ hổng, trong đó có 233 lỗ hổng mức Cao, 204 lỗ hổng mức Trung bình, 09 lỗ hổng mức Thấp và 137 lỗ hổng chưa đánh giá. Trong đó có ít nhất 59 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 07 lỗ hổng trong Linux, Nhóm 10 lỗ hổng trong Samsung, Nhóm 14 lỗ hổng trong Google, Nhóm 98 lỗ hổng trong Wordpress, Nhóm 14 lỗ hổng trong GitLab, Nhóm 09 lỗ hổng trong Dell, Nhóm 10 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:

- Linux: CVE-2023-44466, CVE-2023-39191,…

- Samsung: CVE-2023-30733, CVE-2023-30692,…

- Google: CVE-2023-32821, CVE-2023-32822,…

- Wordpress: CVE-2015-10124, CVE-2023-25025,…

- GitLab: CVE-2023-5207, CVE-2023-3413,…

- Dell: CVE-2023-32477, CVE-2023-32485,…

- IBM: CVE-2022-22447, CVE-2023-37404,…

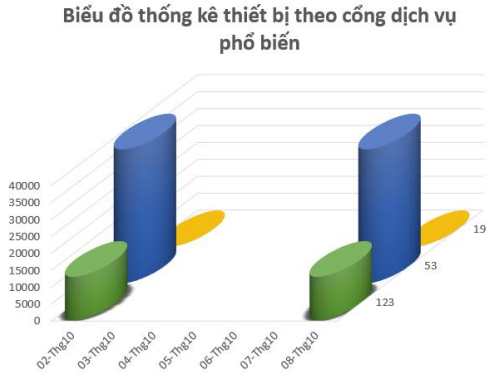
Thông tin điểm yếu, lỗ hổng

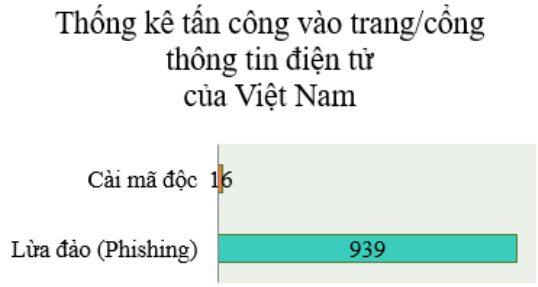
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-44466 CVE-2023-39191 CVE-2023-5345 …	Nhóm 07 lỗ hổng trong Linux cho phép đối tượng tấn công khai thác lỗi Buffer Overflow, thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Samsung	CVE-2023-30733 CVE-2023-30692 CVE-2023-30727 …	Nhóm 10 lỗ hổng trong Samsung cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-32821 CVE-2023-32822 CVE-2023-32823 …	Nhóm 14 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2015-10124 CVE-2023-25025 CVE-2023-25463 …	Nhóm 98 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi CSRF, khai thác lỗi XSS, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
5	GitLab	CVE-2023-5207 CVE-2023-3413 CVE-2023-3917 …	Nhóm 14 lỗ hổng trong GitLab cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Dell	CVE-2023-32477 CVE-2023-32485 CVE-2023-43068 …	Nhóm 09 lỗ hổng trong Dell cho phép đối tượng tấn công thực thi mã từ xa, 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-2022-22447 CVE-2023-37404 CVE-2023-40684 …	Nhóm 10 lỗ hổng trong IBM phép đối tượng tấn công 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

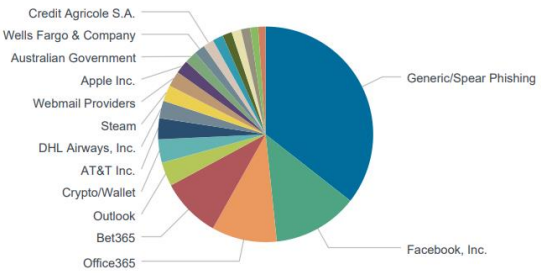
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **52.492**, (tăng so với tuần trước **51.810**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 **955** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 939 trường hợp tấn công lừa đảo (Phishing), 16 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

differentia.ru: 16875 IP	hzmksreiuojy.ru: 277 IP
disorderstatus.ru: 5175 IP	xjpakmdcfuqe.biz: 274 IP
atomictrivia.ru: 2437 IP	xjpakmdcfuqe.com: 104 IP
amnsreiuojy.ru: 922 IP	xjpakmdcfuqe.ru: 78 IP
restlesz.su: 304 IP	xjpakmdcfuqe.in: 69 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **338** 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	kh-cn.tech	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
2	vp-kh-cn-tin-dung.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
3	www.dichvutruyenhinhcab24h.online	Website giả mạo SCTV
4	app.amazon-line.com	Website giả mạo sàn TMĐT Amazon
5	Sendwop.com	Website giả mạo sàn TMĐT Sendo
6	chanlemomo.vet	Website giả mạo Ví điện tử Momo

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