NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 36 (04/9/2023 –10/9/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Chuyên gia cảnh báo về vũ khí không gian mạng được sử dụng bởi nhóm Andariel thuộc Lazarus Group.

- **Cảnh báo:** Apple khẩn cấp cập nhật bản vá cho lỗ hổng Zero-Day để tránh lây nhiễm mã độc Pegasus Spyware trên iPhones.

2. Điểm yếu, lỗ hổng

- **670** 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: 385** 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

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Chuyên gia cảnh báo về vũ khí không gian mạng được sử dụng bởi nhóm Andariel thuộc Lazarus Group"

Nhóm APT Andariel, một phần của Lazarus Group, được cho là có liên quan đến Bắc Triều Tiên. Andariel đã triển khai hàng loạt các công cụ mã độc trong chiến dịch tấn công nhằm vào doanh nghiệp và tổ chức tại Hàn Quốc. Đáng chú ý, chiến dịch tấn công này bị phát hiện vào năm 2023 khi sử dụng các công cụ phát tán mã độc bằng ngôn ngữ lập trình Go.

Nhóm Andariel đã hoạt động kể từ năm 2008 và nhằm vào nhiều mục tiêu khác nhau bao gồm các tổ chức tài chính, nhà thầu quốc phòng, cơ quan nhà nước, trường đại học, nhà cung cấp dịch vụ bảo mật và công ty năng lượng. Mục tiêu của nhóm này là thực hiện các hoạt động gián điệp mạng và tạo ra nguồn thu trái phép cho quốc gia.

Nhóm Andariel thường tiến hành tấn công bằng cách sử dụng nhiều phương thức khác nhau, ví dụ như gửi email giả mạo đến mục tiêu cụ thể (spear-phishing), hoặc cài cắm mã độc vào các trang web hoặc nguồn tài liệu mà mục tiêu thường truy cập (watering holes). Ngoài ra, nhóm này cũng tấn công vào các mắt xích của chuỗi cung ứng để từ đó tiến hành các loại tấn công khác.

Andariel đã sử dụng nhiều loại mã độc khác nhau trong các chiến dịch tấn công, bao gồm Gh0st RAT, DTrack, YamaBot, NukeSped, Rifdoor, Phandoor, Andarat, và nhiều phiên bản khác. Ngoài ra, họ đã tận dụng các lỗ hổng bảo mật trong một giải pháp truyền tải file có tên Innorix Agent để cài đặt các mã độc như Volgmer và Andardoor, cùng với một reverse shell viết bằng Golang được gọi là 1th Troy.

Ngoài ra, Andariel đã phát triển một loạt công cụ mới như Black RAT, Goat RAT, AndarLoader, và DurianBeacon. Những công cụ này được triển khai để gia tăng khả năng tấn công của nhóm này bằng cách cung cấp các chức năng như tải xuống tệp, chụp ảnh màn hình và tự động xóa dữ liệu.

Theo chuyên gia bảo mật, nhóm Andariel cùng với các nhóm như Kimsuky và Lazarus là những nhóm tấn công hoạt động tích cực tại Hàn Quốc. Ban đầu, Andariel thường thực hiện các chiến dịch thu thập thông tin về an ninh quốc gia, nhưng hiện tại nhóm này chuyển sang tấn công với mục đích tài chính.

Thông tin này đã được tiết lộ sau khi phát hiện rằng các đối tượng tấn công mạng liên quan đến Triều Tiên triển khai một chiến dịch tấn công mới nhằm vào các kho lưu trữ mã nguồn mở như npm và PyPI bằng cách sử dụng các gói phần mềm độc hại nhằm lây nhiễm mã độc đến các chuỗi cung ứng phần mềm.

Nguồn:
https://thehackernews.com/2023/09/researchers-warn-of-cyber-weapons-used.html?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Apple khẩn cấp cập nhật bản vá cho lỗ hổng Zero-Day để tránh lây nhiễm mã độc Pegasus Spyware trên iPhones"

Trong tuần qua, Apple đã phát hành một bản vá khẩn cấp cho iOS, iPadOS, macOS và watchOS nhằm khắc phục lỗ hổng zero-day đã bị bị các đối tượng tấn công khai thác nhằm lây nhiễm mã độc Pegasus Spyware.

Chi tiết cụ thể về lỗ hổng:

CVE-2023-41061: Đây là một lỗ hổng xác thực trong ứng dụng Wallet của Apple. Lỗ hổng này cho phép đối tượng tấn công thực hiện việc thực thi mã từ xa khi xử lý một tệp tin độc hại. Điều này có nghĩa là, nếu người dùng mở một tệp tin độc hại trong Wallet, đối tượng tấn công có thể thực hiện mã từ xa trên thiết bị của họ.

CVE-2023-41064: Đây là một lỗi Buffer Overflow (tràn bộ đệm) trong bộ phận Image I/O của Apple. Lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa khi xử lý một hình ảnh độc hại. Nếu một người dùng mở một hình ảnh có chứa mã độc, đối tượng tấn công có thể lợi dụng lỗ hổng này để kiểm soát từ xa thiết bị của người dùng.

Apple đã đưa ra bản vá cho các thiết bị và hệ điều hành sau của hãng:

- iOS 16.6.1 và iPadOS 16.6.1 – Dành cho iPhone 8 trở lên, iPad Pro, iPad Air thế hệ 3 trở lên, iPad thế hệ 5 trở lên và iPad mini từ thế hệ 5 trở lên.
- macOS Venture 13.5.2 – Cho các thiết macOS sử dụng macOS Venture
- watchOS 9.6.2 – Dành cho Apple Watch Series 4 trở lên.

Trong một cảnh báo khác, đã ghi nhận rằng cả hai lỗ hổng này đã được sử dụng trong một chuỗi tấn công zero-click (không cần tương tác từ người dùng) trên ứng dụng iMessage, được đặt tên là BLASTPASS, nhằm triển khai phần mềm gián điệp Pegasus trên các iPhone đã được cập nhật lên phiên bản mới nhất của hệ điều hành iOS 16.6.

Chuỗi khai thác này cho phép đối tượng tấn công xâm nhập vào iPhone của người dùng mà không yêu cầu họ phải thực hiện bất kỳ thao tác nào. Quy trình này thực hiện thông qua việc đính kèm một PassKit chứa hình ảnh độc hại được đối tấn công gửi tới người dùng thông qua ứng dụng iMessage.

Hiện tại, các thông tin kỹ thuật chi tiết về lỗ hổng chưa được tiết lộ để tránh việc bị kẻ tấn công lợi dụng. Tuy nhiên, có thông tin cho rằng khi lỗ hổng này bị khai thác, nó có khả năng bỏ qua BlastDoor, một framework sandbox mà Apple sử dụng để ngăn chặn các hình thức tấn công zero-click.

Thông tin về lỗ hổng zero-day này đã dẫn đến việc Trung Quốc đã cấm các công chức nhà nước sử dụng iPhone và các thiết bị của các hãng nước ngoài trong công việc. Đây là một biện pháp nhằm giảm sự phụ thuộc của quốc gia này vào công nghệ nước ngoài, đặc biệt trong bối cảnh căng thẳng của cuộc chiến tranh thương mại với Mỹ.

Nguồn: https://thehackernews.com/2023/09/apple-rushes-to-patch-zero-day-flaws.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 **670** lỗ hổng, trong đó có 206 lỗ hổng mức Cao, 249 lỗ hổng mức Trung bình, 18 lỗ hổng mức Thấp và 197 lỗ hổng chưa đánh giá. Trong đó có ít nhất 141 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 31 lỗ hổng trong Apple, Nhóm 04 lỗ hổng trong Tenda, Nhóm 65 lỗ hổng trong Google, Nhóm 68 lỗ hổng trong Wordpress, Nhóm 38 lỗ hổng trong Adobe, Nhóm 08 lỗ hổng trong Linux, Nhóm 15 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:

- Apple: CVE-2023-29166, CVE-2023-28209,...

- Tenda: CVE-2023-4744, CVE-2021-40546,..

- Google: CVE-2023-4762, CVE-2023-4763,...

- Wordpress: CVE-2023-4634, CVE-2023-4772,...

- Adobe: CVE-2023-36021, CVE-2023-36023,...

- Linux: CVE-2023-3777, CVE-2023-4015,...

- IBM: CVE-2023-35892, CVE-2023-35906,...

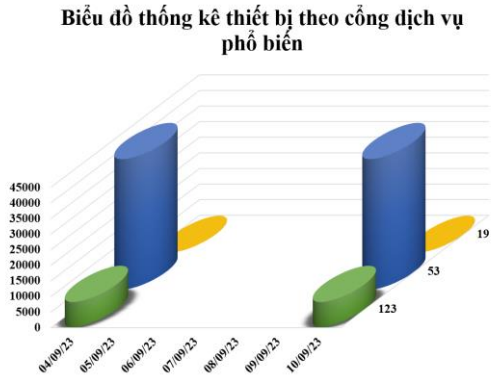
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apple	CVE-2023-29166 CVE-2023-28209 CVE-2023-28210 ...	Nhóm 31 lỗ hổng trong Apple cho phép đối tượng tấn công leo thang đặc quyền, khai thác lỗi Buffer Overflow, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
2	Tenda	CVE-2023-4744 CVE-2021-40546 CVE-2023-40942 ...	Nhóm 04 lỗ hổng trong Tenda cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗi Buffer Overflow.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-4762 CVE-2023-4763 CVE-2023-4761 ...	Nhóm 65 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.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-4634 CVE-2023-4772 CVE-2023-4773 ...	Nhóm 68 lỗ hổng trong Wordpress 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
5	Adobe	CVE-2021-36021 CVE-2021-36023 CVE-2021-36036 ...	Nhóm 38 lỗ hổng trong Adobe 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
6	Linux	CVE-2023-3777 CVE-2023-4015 CVE-2023-4206 ...	Nhóm 08 lỗ hổng trong Linux cho phép đối tượng tấn công 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-2023-35892 CVE-2023-35906 CVE-2022-43903 ...	Nhóm 15 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, 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

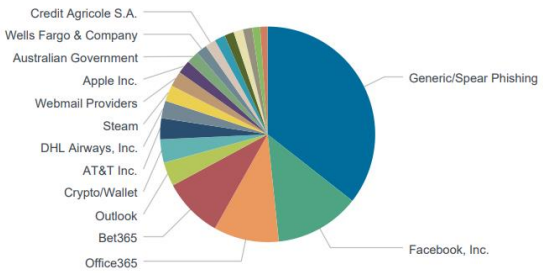
Tấn công DRDoS

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 **46.847**, (giảm so với tuần trước **49.923**) 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 **225** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 218 trường hợp tấn công lừa đảo (Phishing), 07 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: 8170 IP	xjpakmdcfuqe.ru: 42 IP
disorderstatus.ru: 3005 IP	xjpakmdcfuqe.in: 38 IP
atomictrivia.ru: 1510 IP	restlesz.su: 45 IP
xjpakmdcfuqe.biz: 182 IP	amnsreiuojy.ru: 340 IP
xjpakmdcfuqe.com: 71 IP	hzmksreiuojy.ru: 88 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **385** 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	shoopvv.com netwo616.com shopelaie.com vn6932shp.com	Website giả mạo sàn TMĐT Shopee
2	woorivn.online	Website giả mạo Ngân hàng Woori bank Việt Nam
3	tfi1233.com tafccc.com tadcqc.com kfdg22.com kfdg55.com	Website giả mạo sàn TMĐT Tiki

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