NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 52 (25/12/2023 – 31/12/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công Kimsuky triển khai AppleSeed, Meterpreter và TinyNuke trong chiến dịch tấn công mới nhất.

- **Cảnh báo:** Lần đầu xuất hiện mã độc tấn công iPhone thông qua chức năng ẩn trên phần cứng của Apple.

2. Điểm yếu, lỗ hổng

- **515** 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: 239** 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: Nhóm tấn công Kimsuky triển khai AppleSeed, Meterpreter và TinyNuke trong chiến dịch tấn công mới nhất"

Nhóm APT Kimsuky có liên quan đến Triều Tiên, đã bị phát hiện khi thực hiện một chiến dịch tấn công lừa đảo sử dụng phương thức spear-phishing. Mục tiêu của chiến dịch này là triển khai nhiều loại mã độc như AppleSeed, Meterpreter và TinyNuke để chiếm quyền kiểm soát trên các thiết bị của nạn nhân.

Kimsuky đã hoạt động trong hơn một thập kỷ và nổi tiếng với các chiến dịch tấn công có tầm ảnh hưởng lớn, đặc biệt là tại Hàn Quốc, trước khi mở rộng hoạt động sang nhiều quốc gia khác vào năm 2017. Mới đây, nhóm này đã bị Mỹ trừng phạt do hành động khai thác thông tin chiến lược, ủng hộ lợi ích của Triều Tiên.

Chiến dịch lừa đảo mới của nhóm này sử dụng tấn công spear-phishing thông qua các tệp văn bản có chứa mã độc, khi mở sẽ triển khai nhiều loại mã độc khác nhau xâm nhập thiết bị người dùng. Một trong những loại mã độc đó là AppleSeed (còn gọi là JamBog), là một backdoor trên Windows dưới dạng mã độc DLL đã được sử dụng từ tháng 05/2019. Mã độc này đã được cập nhật phiên bản Android và phát triển thêm một biến thể mới viết bằng ngôn ngữ Golang, được gọi là AlphaSeed.

Mã độc AppleSeed được thiết kế để nhận lệnh từ máy chủ mà đối tượng tấn công kiểm soát, sau đó tải xuống các payload và trích xuất dữ liệu quan trọng như file, nội dung gõ từ bàn phím và ảnh thông qua giao thức HTTP hoặc SMTP. Biến thể AlphaSeed có các chức năng tương tự, nhưng khác biệt ở chỗ sử dụng thư viện chromedp, một thư viện phổ biến trên Golang để tương tác với trình duyệt Google Chrome trong trạng thái không đầu thông qua giao thức DevTools Protocol, để liên lạc với máy chủ C&C.

Có bằng chứng cho thấy Kimsuky đã sử dụng mã độc AlphaSeed trong các chiến dịch tấn công từ tháng 10/2022, và một số chiến dịch sử dụng cả hai biến thể trên cùng một thiết bị, được phân phối thông qua JavaScript dropper. Ngoài ra, trong chiến dịch này, Kimsuky cũng phát tán Meterpreter và các loại mã độc VNC như TightVNC và TinyNuke (hay Nuclear Bot) để chiếm quyền kiểm soát thiết bị bị ảnh hưởng.

Sau khi phát hiện nhiều tài khoản trên LinkedIn và GitHub có thể thuộc sở hữu của nhân viên IT Triều Tiên, thông tin về chiến dịch của nhóm tấn công Kimsuky đã được tiết lộ. Những tài khoản này được sử dụng để ứng tuyển vào các vị trí làm việc từ xa tại Mỹ, chủ yếu để tạo nguồn doanh thu cho quốc gia và hỗ trợ các ưu tiên kinh tế và an ninh của họ. Các cá nhân này tự mô tả với kỹ năng phát triển ứng dụng và có kinh nghiệm trong tiền ảo và giao dịch trên blockchain. Điểm chung giữa các tài khoản là ứng tuyển vào các vị trí công nghệ làm việc từ xa, thường chỉ hoạt động trong khoảng thời gian ngắn trước khi bị vô hiệu hóa.

Trong những năm gần đây, các nhóm tấn công mạng Triều Tiên đã thực hiện hàng loạt cuộc tấn công bằng cách lợi dụng điểm yếu của hệ thống để đánh cắp tiền ảo và thông tin quan trọng của các công ty trong lĩnh vực blockchain. Những đối tượng này rất linh hoạt và khéo léo trong các chiến thuật tấn công để tránh bị trừng phạt từ phía quốc tế và tạo ra thu nhập bất chính từ các cuộc tấn công này.

Nguồn:
https://thehackernews.com/2023/12/kimsuky-hackers-deploying-appleseed.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lần đầu xuất hiện mã độc tấn công iPhone thông qua chức năng ẩn trên phần cứng của Apple"

Các cuộc tấn công bằng mã độc Operation Triangulation nhằm vào các thiết bị Apple iOS đã sử dụng các phương thức khai thác chưa từng được biết đến trước đây, điều này giúp các đối tượng tấn công có thể vượt qua các biện pháp bảo mật phần cứng quan trọng của Apple.

Chiến dịch Operation Triangulation được đặt tên dựa theo kỹ thuật lấy vân tay canvas để vẽ ra một tam giác vàng, nền hồng sử dụng Web Graphics Library (WebGL) lên bộ nhớ của thiết bị. Được cho là bắt đầu hoạt động từ năm 2019 nhưng đến đầu năm 2023 chiến dịch Operation Triangulation mới bị phát hiện khi tấn công vào một cơ quan bảo mật. Đây được mô tả là chuỗi tấn công phức tạp nhất đến thời điểm đó.

Quá trình khai thác trong chiến dịch này sử dụng bốn lỗ hổng zero-day được tập hợp thành một chuỗi để đạt được mức truy cập mới và cài đặt backdoor trên các thiết bị sử dụng iOS phiên bản 16.2 trở về trước, với mục tiêu chính là thu thập thông tin quan trọng. Chuỗi tấn công bắt đầu từ một file độc hại trong iMessage được xử lý tự động, không cần sự tương tác của người dùng, nhằm leo thang đặc quyền và triển khai module spyware. Cụ thể hơn, các lỗ hổng an toàn thông tin sau đã được sử dụng:

- CVE-2023-41990 – Lỗ hổng trên thành phần FontParser cho phép đối tượng tấn công thực thi mã từ xa khi thiết bị xử lý một file font độc hại được gửi trên iMessage (Đã được vá trong iOS 15.7.8 và iOS 16.3)
- CVE-2023-32434 – Lỗ hổng tràn integer trong Kernel cho phép đối tượng tấn công thực thi mã từ xa với quyền kernel khi bị khai thác bởi ứng dụng độc hại (Đã được vá trong các phiên bản iOS 15.7.7, iOS 15.8, iOS 16.5.1)
- CVE-2023-32435 – Lỗ hổng trên bộ nhớ của WebKit cho phép thực thi mã từ xa khi xử lý nội dung web độc hại (Đã được vá trong iOS 15.7.7 và iOS 16.5.1)
- CVE-2023-38606 – Lỗ hổng trên kernel cho phép ứng dụng độc hại điều chỉnh trạng thái của kernel bị ảnh hưởng (Đã được vá trong iOS 16.6). Theo thống kê đã có 26,447 lỗ hổng an toàn thông tin được phát hiện trong năm 2023, nhiều hơn 1500 CVE so với năm ngoái, trong đó có 115 lỗ hổng đã bị khai thác bởi các đối tượng tấn công và các nhóm ransomware.

Đáng chú ý, Apple đã phát hành bản vá cho lỗ hổng CVE-2023-41990 vào tháng 01/2023. Tuy nhiên, thông tin về cách khai thác lỗ hổng chỉ được công bố vào ngày 08/09/2023, cùng ngày Apple phát hành bản vá iOS 16.6.1 để khắc phục hai lỗ hổng CVE-2023-41061 và CVE-2023-41064, đang bị khai thác bởi chiến dịch spyware Pegasus. Trong năm vừa qua, chiến dịch này cũng đã góp phần khiến Apple xử lý lên đến 20 lỗ hổng zero-day.

Trong bốn lỗ hổng được đề cập, CVE-2023-38606 nổi bật với khả năng cho phép tấn công bỏ qua lớp bảo mật phần cứng cho các vùng quan trọng của bộ nhớ kernel. Lỗ hổng này được khai thác bằng cách lợi dụng thanh ghi của memory-mapped I/O (MMIO), một chức năng ẩn trên phần cứng Apple. Lỗ hổng chủ yếu tập trung vào việc khai thác các SoCs Apple A12-A16 Bionic, đặc biệt là các khối MMIO thuộc GPU.

Lỗ hổng CVE-2023-38606 là một liên kết quan trọng trong chuỗi khai thác của chiến dịch Operation Triangulation vì nó cung cấp khả năng kiểm soát hoàn toàn hệ thống bị ảnh hưởng cho đối tượng tấn công.

Thông tin này được tiết lộ ngay sau khi Apple cảnh báo về việc các nhà báo và chính trị gia Ấn Độ bị tấn công trong một chiến dịch spyware vào cuối tháng 10. Sự cố này khiến chính phủ Ấn Độ nghi ngờ về tính xác thực của thông báo này và coi đây như một trường hợp "lỗi thuật toán" trong hệ thống của Apple.

Nguồn: https://thehackernews.com/2023/12/urgent-new-chrome-zero-day.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 **515** lỗ hổng, trong đó có 158 lỗ hổng mức Cao, 153 lỗ hổng mức Trung bình, 31 lỗ hổng mức Thấp và 173 lỗ hổng chưa đánh giá. Trong đó có ít nhất 66 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 01 lỗ hổng trong Microsoft, Nhóm 03 lỗ hổng trong Cloudflare, Nhóm 04 lỗ hổng trong Apache, Nhóm 117 lỗ hổng trong Wordpress, Nhóm 02 lỗ hổng trong Linux, Nhóm 12 lỗ hổng trong Tenda, Nhóm 05 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-2020-17163
- Cloudflare: CVE-2023-7078, CVE-2023-7079,...
- Apache: CVE-2023-492499, CVE-2023-50968,...
-Wordpress: CVE-2023-25054, CVE-2023-51411,...
- Linux: CVE-2023-50254, CVE-2023-50255
- Tenda: CVE-2023-51090, CVE-2023-51091,...
- IBM: CVE-2023-45165, CVE-2023-49880,...

Thông tin điểm yếu, lỗ hổng

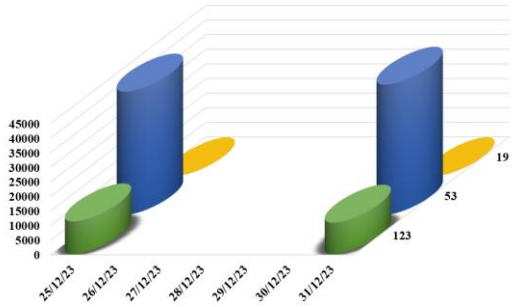
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2020-17163	Nhóm 01 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép	Chưa có thông tin xác nhận và bản vá
2	Cloudflare	CVE-2023-7078 CVE-2023-7079 CVE-2023-7090	Nhóm 03 lỗ hổng trong Cloudflare 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	Apache	CVE-2023-49299 CVE-2023-50968 CVE-2023-51467 …	Nhóm 04 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, khai thác lỗ hổng SSRF, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-25054 CVE-2023-51411 CVE-2023-51419 …	Nhóm 117 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện SQL Injection, khai thác lỗ hổng CSRF, khai thác lỗ hổng XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Linux	CVE-2023-50254 CVE-2023-50255	Nhóm 02 lỗ hổng trong Linux 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	Tenda	CVE-2023-51090 CVE-2023-51091 CVE-2023-51092 …	Nhóm 12 lỗ hổng trong Tenda 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
7	IBM	CVE-2023-45165 CVE-2023-49880 CVE-2023-43064 …	Nhóm 05 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

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

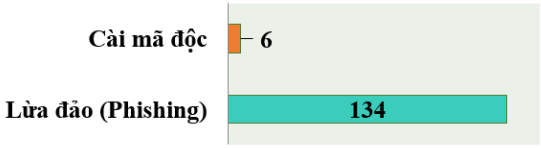
Tấn công DRDoS

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 **55.435**, (giảm so với tuần trước **49.168**) 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

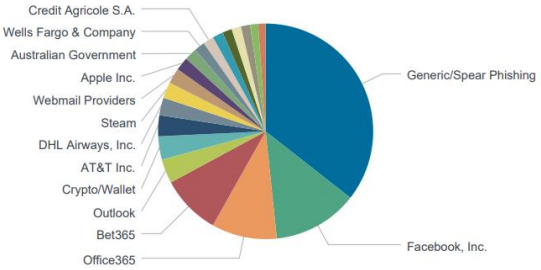


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **140** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 134 trường hợp tấn công lừa đảo (Phishing), 06 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: 10680 IP	hzmksreiuojy.ru: 177 IP
disorderstatus.ru: 5452 IP	xjpakmdcfuqe.biz: 104 IP
atomictrivia.ru: 2543 IP	xjpakmdcfuqe.com: 74 IP
amnsreiuojy.ru: 665 IP	xjpakmdcfuqe.ru: 62 IP
restlesz.su: 273 IP	xjpakmdcfuqe.in: 45 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **239** 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	bit.ly/dang-ky-vietinfinal tienvenhanhvtb.com	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
2	qrsg11.com kjgb11.com	Website giả mạo sàn TMĐT Tiki
3	tb55788.com	Website giả mạo sàn TMĐT Shopee
4	www.e-commercesc.cc	Website giả mạo sàn TMĐT Lazada

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, 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