NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 06 (05/02/2024 – 11/02/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Kimsuky sử dụng mã độc Golang "Troll Stealer" và backdoor "GoBear" trong chiến dịch tấn công nhằm vào Hàn Quốc.

- **Cảnh báo:** Lỗ hổng an toàn thông tin Nghiêm trọng trên Exchange Server (CVE-2024-21410) đang bị khai thác.

2. Điểm yếu, lỗ hổng

- **770** 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: 161** 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

"Nhóm APT Kimsuky sử dụng mã độc Golang "Troll Stealer" và backdoor "GoBear" trong chiến dịch tấn công nhằm vào Hàn Quốc.

Nhóm APT Kimsuky, được cho là có liên quan Triều Tiên, đang sử dụng một mã độc mới viết bằng Golang có tên là Troll Stealer. Mã độc này được thiết kế để đánh cắp SSH, FileZilla, các tệp/thư mục trong ổ C, thông tin trình duyệt, hệ thống, và cả ảnh chụp màn hình từ các hệ thống bị lây nhiễm.

Mã độc Troll Stealer được phát hiện có liên quan đến nhóm Kimsuky do có các đặc điểm giống với các mã độc khác của nhóm như AppleSeed và AlphaSeed. Ngoài ra, nhóm Kimsuky còn được biết đến dưới nhiều tên gọi khác nhau như APT43, ARCHIPELAGO, Black Banshee, Emerald Sleet (trước đây là Thallium), Nickel Kimball, và Velvet Chollima. Nhóm này thường thực hiện các chiến dịch tấn công nhằm vào việc đánh cắp thông tin mật, như trong các vụ tấn công Spear-phishing nhắm vào Hàn Quốc gần đây, trong đó sử dụng các loại mã độc backdoor như AppleSeed và AlphaSeed.

Theo phân tích mới nhất, đã phát hiện rằng nhóm tấn công đã sử dụng một bộ tải giả. Bộ tải này được chạy đồng thời với một bộ cài đặt hợp pháp của chương trình bảo mật và được ký bằng chứng thực của "D2Innovation Co., LTD", cho thấy chứng thực của công ty này đã bị nhóm tấn công đánh cắp. Tên của mã độc được cài đặt sẽ được lấy từ đường dẫn "D:/~/repo/golang/src/root.go/s/troll/agent" được nhúng trong file.

Một tính năng quan trọng của Troll Stealer là khả năng lấy cắp chứng thực GPKI được cấp bởi chính phủ Hàn Quốc từ các hệ thống đã bị mã độc xâm nhập. Điều này cho thấy có khả năng mã độc đã được sử dụng để tấn công vào các tổ chức hành chính công của Hàn Quốc. Vì không có bằng chứng nào về việc nhóm Kimsuky đã đánh cắp thư mục GPKI, nên hành vi vi phạm này có thể là kết quả của một sự thay đổi trong chiến lược hoặc là sản phẩm của một nhóm khác, có mối liên hệ mật thiết với Kimsuky và có truy cập vào mã nguồn của AppleSeed và AlphaSeed.

Cũng có các dấu hiệu cho thấy nhóm APT Kimsuky có thể liên quan đến mã độc backdoor GoBear, mã độc này cũng được ký chứng thực của D2Innovation Co., LTD và thực thi các hướng dẫn từ máy chủ C&C. Mã độc này cũng được ký chứng thực của D2Innovation Co., LTD và thực thi các hướng dẫn từ máy chủ C&C. Chuỗi ký tự trong tên của các hàm mà mã độc thực thi có điểm tương đồng với câu lệnh sử dụng bởi BetaSeed, một mã độc backdoor C++ được sử dụng bởi Kimsuky.

Nguồn: https://thehackernews.com/2024/02/kimsukys-new-golang-stealer-troll-and.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Lỗ hổng an toàn thông tin Nghiêm trọng trên Exchange Server (CVE-2024-21410) đang bị khai thác."

Trong tuần vừa qua, Microsoft đã tiếp tục đối mặt với một lỗ hổng an toàn thông tin Nghiêm trọng trên Exchange Server, được công bố ngay sau khi bản vá Patch Tuesday được phát hành.

Lỗ hổng CVE-2024-21410 (Điểm CVSS: 9.8) là một lỗ hổng nghiêm trọng trong hệ thống, cho phép đối tượng tấn công leo thang đặc quyền trên Exchange Server. Qua đó, đối tượng tấn công có thể nhằm mục tiêu tấn công vào các client NTLM như Outlook, sử dụng lỗ hổng này để xâm nhập và thu thập thông tin đăng nhập. Điều này cho phép kẻ tấn công giả mạo quyền hạn của người dùng mục tiêu và thực hiện các hoạt động độc hại trên máy chủ Exchange Server.

Việc khai thác thành công lỗ hổng này cho phép đối tượng tấn công tái tạo hàm băm Net-NTLMv2 được lấy từ người dùng và chuyển tiếp nó tới các máy chủ Exchange Server bị ảnh hưởng bởi lỗ hổng CVE-2024-21410. Điều này giúp đối tượng tấn công có khả năng xác minh được mình là người đó. Mặc dù chi tiết về cách thức khai thác và danh tính của các kẻ tấn công vẫn chưa được làm rõ, nhưng trước đó, nhóm tấn công APT28 đã sử dụng lỗ hổng tương tự trên Microsoft Outlook để thực hiện tấn công tái tạo NTLM (NTLM relay attack).

Đồng thời, vào tháng 02/2024, Trend Micro đã ghi nhận nhóm APT28 tiếp tục tiến hành các cuộc tấn công này đối với các mục tiêu quan trọng từ tháng 04/2022.

Ngoài ra, lỗ hổng CVE-2024-21410 không chỉ gây ảnh hưởng mà còn có liên kết với hai lỗ hổng khác trên hệ điều hành Windows là CVE-2024-21351 (Điểm CVSS: 7.6) và CVE-2024-21412 (Điểm CVSS: 8.1). Cả hai lỗ hổng này đã được vá trước đó nhưng vẫn bị khai thác trong nhiều chiến dịch tấn công. Một trong số đó, lỗ hổng CVE-2024-21412 cho phép bỏ qua biện pháp bảo mật của Window SmartScreen và đã được sử dụng bởi nhóm APT Water Hydra (hay DarkCasino). Trước đó, nhóm này đã sử dụng một lỗ hổng zero-day trên WinRAR để triển khai trojan DarkMe.

Trong bản vá Patch Tuesday, Microsoft cũng đã xử lý lỗ hổng CVE-2024-21413 gây ảnh hưởng tới phần mềm email Outlook. Lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa bằng cách vô hiệu hóa các biện pháp bảo mật như Protected View.

Nguồn: https://thehackernews.com/2024/02/critical-exchange-server-flaw-cve-2024.html

NCSC VN
National Cyber Security Center

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 **770** lỗ hổng, trong đó có 271 lỗ hổng mức Cao, 326 lỗ hổng mức Trung bình, 25 lỗ hổng mức Thấp và 148 lỗ hổng chưa đánh giá. Trong đó có ít nhất 171 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 14 lỗ hổng trong Linux, Nhóm 14 lỗ hổng trong Google, Nhóm 13 lỗ hổng trong Dell, Nhóm 112 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong VMware, Nhóm 04 lỗ hổng trong Gitlab, Nhóm 53 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-2023-6240, CVE-2023-6356,...

- Google: CVE-2024-20011, CVE-2024-20009,...

- Dell: CVE-2020-29504, CVE-2021-21575,...

- Wordpress: CVE-2021-4436, CVE-2023-6933,...

- VMware: CVE-2024-22237, CVE-2024-22239,...

- Gitlab: CVE-2023-6564, CVE-2023-6736,...

- IBM: CVE-2023-38273, CVE-2023-45191,...

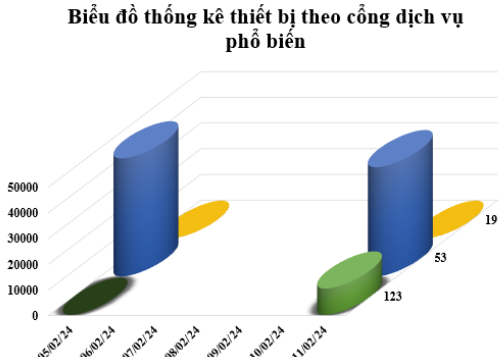
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-6240 CVE-2023-6356 CVE-2023-6535 …	Nhóm 14 lỗ hổng trong Linux 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
2	Google	CVE-2024-20011 CVE-2024-20009 CVE-2024-20007 …	Nhóm 14 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
3	Dell	CVE-2020-29504 CVE-2021-21575 CVE-2022-34381 …	Nhóm 13 lỗ hổng trong Dell 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-2021-4436 CVE-2023-6933 CVE-2023-6989 …	Nhóm 112 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗ hổng SQL Injection, khai thác lỗ hổng XSS, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
5	VMware	CVE-2024-22237 CVE-2024-22239 CVE-2024-22238 …	Nhóm 05 lỗ hổng trong VMware cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Gitlab	CVE-2023-6564 CVE-2023-6736 CVE-2023-6840 …	Nhóm 04 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
7	IBM	CVE-2023-38273 CVE-2023-45191 CVE-2023-32333 …	Nhóm 53 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, 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

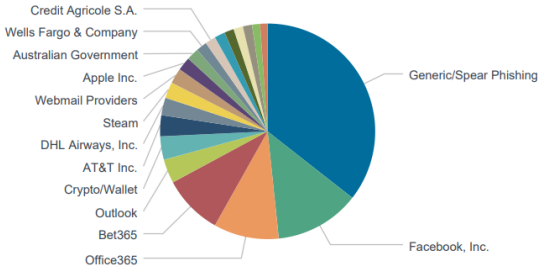
Tấn công DRDoS

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 **52.826** (giảm so với tuần trước **56.765**) 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 **92** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 86 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: 9097 IP	hzmksreiuojy.ru: 130 IP
disorderstatus.ru: 2260 IP	xjpakmdcfuqe.biz: 208 IP
atomictrivia.ru: 966 IP	xjpakmdcfuqe.com: 85 IP
amnsreiuojy.ru: 640 IP	xjpakmdcfuqe.ru: 67 IP
restlesz.su: 445 IP	xjpakmdcfuqe.in: 55 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **161** 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	tindungcanhan.online	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
2	ghnn22.com ghnn11.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