NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 13 (25/03/2024 – 31/03/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT sử dụng thư giả mạo của Không quân để tấn công các tổ chức quốc phòng và năng lượng tại Ấn Độ.

- **Cảnh báo:** Một lỗ hổng trên Linux có thể gây lộ mật khẩu và chiếm quyền truy cập Clipboard.

2. Điểm yếu, lỗ hổng

- **944** 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: 279** 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

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

“Chiến dịch tấn công:Nhóm APT sử dụng thư giả mạo của Không quân để tấn công các tổ chức quốc phòng và năng lượng tại Ấn Độ.”

Một nhóm tấn công APT chưa được xác định đã tấn công vào các tổ chức chính phủ và công ty năng lượng ở Ấn Độ. Nhóm này sử dụng một loại mã độc gọi là HackBrowserData để đánh cắp thông tin. Đáng chú ý, nhóm này còn sử dụng kênh Slack làm máy chủ điều khiển C&C và lưu trữ thông tin bị đánh cắp.

Cụ thể, các đối tượng tấn công đã giả mạo tổ chức “Không quân Ấn Độ” để phát tán email lừa đảo chứa mã độc HackBrowserData. Sau khi mở email này, thiết bị của nạn nhân sẽ bị nhiễm mã độc và dữ liệu của họ sẽ bị đánh cắp. Đối tượng tấn công đã sử dụng kênh Slack làm máy chủ C&C để lưu trữ các thông tin mật, email và dữ liệu cache từ trình duyệt web, tạo ra một cơ sở để thực hiện các hành động xâm nhập và đánh cắp thông tin.

Chiến dịch tấn công này đã được theo dõi từ ngày 07/03/2024 và được đặt tên là Operation NightFlight. Phạm vi của chiến dịch này bao gồm nhiều tổ chức chính phủ tại Ấn Độ, bao gồm các cơ quan truyền thông điện tử, quản trị công nghệ thông tin và quốc phòng. Trong quá trình theo dõi, cơ quan bảo mật đã phát hiện rằng nhóm tấn công đã trích xuất tổng cộng 8.81 GB dữ liệu, trong đó bao gồm tài liệu tài chính, thông tin cá nhân của nhân viên, và nhiều thông tin khác.

Chiến dịch bắt đầu bằng việc gửi email lừa đảo chứa file ISO có tên là "invite.iso", trong đó chứa một file .LNK (Windows shortcut) có khả năng thực thi một tập tin nhị phân ẩn có tên là "scholar.exe". Đồng thời, một file PDF giả mạo thành thư mời sẽ được hiển thị cho người dùng, trong khi mã độc chạy ẩn và thu thập dữ liệu, sau đó chuyển chúng tới kênh Slack với tên là FlightNight.

Theo phân tích, mã độc này là một biến thể của HackBrowserData được trang bị thêm khả năng thu thập các tệp văn bản như Microsoft Office, PDF và các tệp cơ sở dữ liệu SQL, có khả năng giao tiếp thông qua Slack và có thể tránh bị phát hiện bằng các kỹ thuật che giấu. Có khả năng tập tin PDF mồi đã bị đối tượng tấn công đánh cắp từ lần xâm nhập trước đó, và chiến dịch này cũng có một số điểm tương đồng với cách thức hoạt động của chiến dịch GoStealer trước đó.

Theo chuyên gia bảo mật, hai chiến dịch Operation NightFlight và GoStealer là minh chứng cho một cách tấn công đơn giản nhưng hiệu quả, khi kẻ tấn công sử dụng các công cụ mã nguồn mở trong các chiến dịch gián điệp trên không gian mạng. Điều này thể hiện sự nguy hiểm ngày càng gia tăng của các cuộc tấn công trên mạng, khi kẻ tấn công sử dụng các công cụ và nền tảng mã nguồn mở để tiến hành các cuộc tấn công, với rủi ro bị phát hiện và đầu tư ở mức tối thiểu.

Nguồn: https://thehackernews.com/2024/03/hackers-target-indian-defense-and.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Một lỗ hổng trên Linux có thể gây lộ mật khẩu và chiếm quyền truy cập Clipboard."

Các chuyên gia bảo mật đã tiết lộ về một lỗ hổng trong gói util-linux ảnh hưởng đến lệnh "wall". Khi lỗ hổng này bị khai thác, đối tượng tấn công có thể tiết lộ mật khẩu của người dùng và thay đổi nội dung trong bộ nhớ tạm của clipboard trên một số phiên bản Linux.

Lỗ hổng an toàn thông tin có mã CVE-2024-28085, được gọi là WallEscape, xuất phát từ việc không xử lý đúng cách các chuỗi thoát. Khi sử dụng lệnh "wall", nếu không lọc các chuỗi này từ các tham số dòng lệnh, đối tượng tấn công có thể đưa các văn bản tùy ý lên terminal của người dùng khác nếu giá trị mesg được đặt là "y" và của "wall" là "setgid".

Câu lệnh "wall" thường được dùng để gửi tin nhắn đến terminal của tất cả người dùng đang đăng nhập vào máy chủ, giúp người dùng có quyền tạo thông báo cho tất cả mọi người (ví dụ, thông báo về việc tắt hệ thống). Lỗ hổng CVE-2024-28085 lợi dụng việc không lọc các chuỗi thoát từ đối số dòng lệnh, khiến người dùng bị đánh lừa để nhập mật khẩu vào một thông báo sudo giả trên terminal của họ.

Lỗ hổng CVE-2024-28085 có thể bị khai thác khi các điều kiện sau được đáp ứng: tiện ích mesg (quản lý khả năng hiển thị tin nhắn từ người dùng khác) phải được đặt ở giá trị "y" (bật), và câu lệnh "wall" cần phải có quyền setgid.Lỗ hổng CVE-2024-28085 ảnh hưởng đến Ubuntu 22.04 và Debian Bookworm khi các điều kiện này được đáp ứng.

Tuy nhiên, CentOS không bị ảnh hưởng do câu lệnh trên hệ điều hành này không có quyền setgid.

Ngoài ra, trên các hệ thống cho phép thông báo được gửi tới người dùng, kẻ tấn công cũng có thể chỉnh sửa nội dung trong clipboard thông qua chuỗi thoát trên các terminal như Windows Terminal. Đáng chú ý, GNOME Terminal không bị ảnh hưởng bởi lỗ hổng này.

Người dùng được khuyến nghị nhanh chóng cập nhật lên phiên bản 2.40 của util-linux để tránh bị ảnh hưởng bởi lỗ hổng này.

Thông tin về lỗ hổng được tiết lộ sau khi một chuyên gia bảo mật đã phát hiện một lỗ hổng use-after-free trong hệ thống con netfilter trên Linux Kernel, có khả năng bị khai thác để thực hiện tấn công leo thang đặc quyền. Lỗ hổng này có mã CVE-2024-1086 (Điểm CVSS: 7.8) và tồn tại do sự thiếu sót trong quá trình lọc và xử lý dữ liệu đầu vào của netfilter, cho phép kẻ tấn công thực hiện các cuộc tấn công từ chối dịch vụ hoặc thực thi mã từ xa.

Nguồn: https://thehackernews.com/2024/03/new-linux-bug-could-lead-to-user.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 **944** lỗ hổng, trong đó có 284 lỗ hổng mức Cao, 346 lỗ hổng mức Trung bình, 20 lỗ hổng mức Thấp và 294 lỗ hổng chưa đánh giá. Trong đó có ít nhất 102 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 Linux, Nhóm 04 lỗ hổng trong Google, Nhóm 13 lỗ hổng trong Apple, Nhóm 17 lỗ hổng trong Dell, Nhóm 02 lỗ hổng trong Splunk, Nhóm 17 lỗ hổng trong Cisco, Nhóm 06 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-2021-47136, CVE-2021-47137,...

- Google: CVE-2024-2883, CVE-2024-2885,...

- Apple: CVE-2023-42893, CVE-2023-42896,..

- Dell: CVE-2024-25962, CVE-2024-25959,...

- Splunk: CVE-2024-29946, CVE-2024-29945

- Cisco: CVE-2024-20271, CVE-2024-20259,...

- IBM: CVE-2023-47150, CVE-2024-22356,...

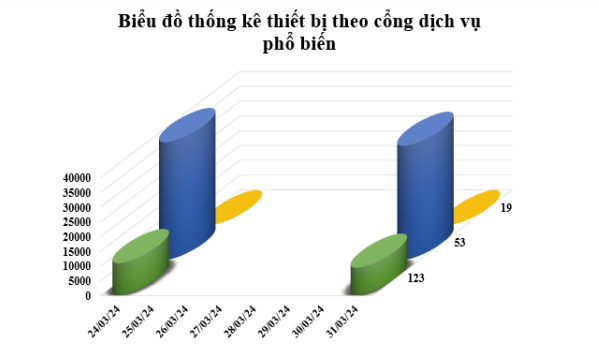
Thông tin điểm yếu, lỗ hổng

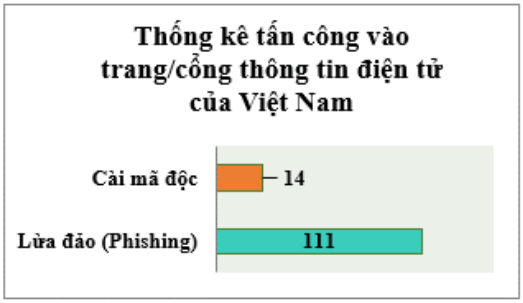
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2021-47136 CVE-2021-47137 CVE-2021-47138 ...	Nhóm 59 lỗ hổng trong Linux cho phép tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Google	CVE-2024-2883 CVE-2024-2885 CVE-2024-2886 ...	Nhóm 04 lỗ hổng trong Google 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	Apple	CVE-2023-42893 CVE-2023-42896 CVE-2023-42936 ...	Nhóm 13 lỗ hổng trong Apple cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
4	Dell	CVE-2024-25962 CVE-2024-25959 CVE-2024-25960 ...	Nhóm 17 lỗ hổng trong Dell cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
5	Splunk	CVE-2024-29946 CVE-2024-29945	Nhóm 02 lỗ hổng trong Splunk cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Cisco	CVE-2024-20271 CVE-2024-20259 CVE-2024-20314 ...	Nhóm 17 lỗ hổng trong Cisco cho 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.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-47150 CVE-2024-22356 CVE-2024-28784 ...	Nhóm 06 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗi XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

Thống 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 **47.913** (giảm so với tuần trước **50.788**) 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.



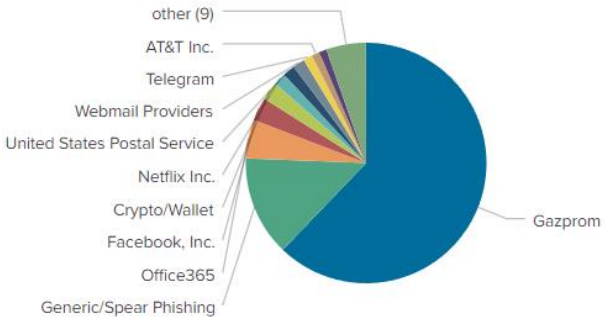


Tấn công Web

Trong tuần, có **125** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 111 trường hợp tấn công lừa đảo (Phishing), 14 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: 2011 IP	hzmksreiuojy.ru: 49 IP
disorderstatus.ru: 954 IP	xjpakmdcfuqe.biz: 26 IP
atomictrivia.ru: 534 IP	xjpakmdcfuqe.com: 21 IP
amnsreiuojy.ru: 112 IP	xjpakmdcfuqe.ru: 13 IP
restlesz.su: 87 IP	xjpakmdcfuqe.in: 11 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **279** 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	vn63251s.com dailyssshopee.com	Website giả mạo sàn TMĐT Shopee
2	khach-hang-ca-nhan-vip5.com nang-hang-ca-nhan-vib-mrk1.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
3	dichvucong.govnx.com dichvucong.vsgov.com	Website giả mạo cổng Dịch vụ công Quốc Gia

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