NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 10 (06/03/2023 – 12/03/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Tiện ích ChatGPT giả mạo chiếm quyền điều khiển tài khoản Facebook nhằm phát tán những quảng cáo độc hại.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT UNC4540 của Trung Quốc nhằm mục tiêu vào các thiết bị SonicWall SMA.

2. Điểm yếu, lỗ hổng

- **547** 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: 363** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Tiện ích ChatGPT giả mạo chiếm quyền điều khiển tài khoản Facebook nhằm phát tán những quảng cáo độc hại"

Một tiện ích trình duyệt Chrome giả mạo ChatGPT mới được phát hiện có khả năng chiếm quyền điều khiển Facebook và tạo ra các tài khoản quản trị giả mạo, đây là một trong những phương pháp mà đối tượng tấn công sử dụng để phát tán phần mềm độc hại. Nhóm tấn công đã tạo ra một nhóm gồm các bot Facebook và công cụ truyền thông trả phí độc hại nhằm chiếm quyền điều khiển các tài khoản thương mại (business account) nổi tiếng trên Facebook.

Kể từ ngày 03/03/2023 tiện ích mở rộng "Qick access to ChatGPT" đã thu hút hơn 2000 lượt cài đặt mỗi ngày, ngày 09/03/2023 đã bị Google xóa bỏ khỏi Cửa hàng Chrome.

Tiện ích này được quảng bá thông qua các bài đăng do Facebook tài trợ, mặc dù có khả năng kết nối với dịch vụ ChatGPT nhưng nó còn được thiết kế để thu thập cookie và dữ liệu tài khoản Facebook trái phép.

Đối tượng tấn công đã sử dụng hai ứng dụng giả mạo portal và msg_kig để duy trì quyền truy cập cho backdoor và có quyền kiểm soát các tài khoản mục tiêu. Quá trình thêm ứng dụng vào tài khoản Facebook được thực hiện hoàn toàn tự động. Các tài khoản thương mại Facebook bị tấn công sau đó được sử dụng để quảng cáo phần mềm độc hại, giúp mở rộng quy mô nhóm bot Facebook.

Kể từ năm ngoái, sau khi ChatGPT của OpenAI trở nên phổ biến, những kẻ tấn công đã tận dụng sự phổ biến đó để tạo ra các phiên bản giả mạo để đánh lừa người dùng. Tháng 2/2023, một cuộc tấn công social engineering dựa trên trang web giả mạo website chính thức của ChatGPT nhằm điều hướng người dùng đến các trang web độc hại và tải xuống những phần mềm đánh cắp thông tin như: RedLine, Lumma và Aurora.

Ngoài ra, các ứng dụng ChatGPT giả mạo còn được phân phối qua Google Play và các cửa hàng ứng dụng Android để đẩy mã độc SpyNote và thiết bị của người dùng.

Thành công của công cụ AI đã thu hút sự chú ý của những đối tấn công nhằm sử dụng công nghệ này để thực hiện các vụ tấn công tinh vi nhằm vào người dùng Internet. Để tránh trở thành nạn nhân của chiêu trò lừa đảo và các chiến dịch tấn công mạng người dùng nên kiểm tra trước khi truy cập vào bất kỳ đường link nào cũng như chỉ cài đặt ứng dụng từ những nguồn đáng tin cậy, thường xuyên sử dụng công cụ quét virus để sớm phát hiện và loại bỏ các phần mềm độc hại trên thiết bị của mình.

Nguồn: https://thehackernews.com/2023/03/fake-chatgpt-chrome-extension-hijacking.html

Tin tức An toàn thông tin

"Cảnh báo: Nhóm tấn công APT UNC4540 của Trung Quốc nhằm mục tiêu vào các thiết bị SonicWall SMA"

Gần đây, nhóm tấn công APT UNC4540 của Trung Quốc đã nhằm mục tiêu vào 100 thiết bị SonicWall Secure Mobile Access (SMA) thông qua việc phát tán mã độc cho phép đối tượng tấn công đánh cắp thông tin đăng nhập, truy cập và thực hiện các hành động trái phép.

Mã độc này gồm một chuỗi Bash Script và một tập nhị phân ELF được xác định là TinyShell backdoor cho phép đối tượng tấn công có quyền truy cập vào các thiết bị SonicWall.

Mục tiêu của cuộc tấn công nhằm đánh cắp thông tin xác thực từ người dùng đã đăng nhập vào tài khoản và cung cấp quyền truy cập vào thiết bị đã bị xâm nhập.

Ngoài ra, nhóm APT cũng đang phát triển các biến thể mã độc để triển khai trên nhiều loại thiết bị. Chiến dịch tấn công này nhằm vào các thiết bị SMA 100 chưa được vá kể từ năm 2021.

Trong gần hai tháng sau đó, một nhóm tấn công APT khác của Trung Quốc cũng khai thác lỗ hổng đã được cập nhật bản vá trong Fortinet FortiOS SSL-VPN để nhằm mục tiêu vào cơ quan chính phủ ở châu Âu và nhà cung cấp dịch vụ quản lý (MSP) ở châu Phi.

Các đối tượng tấn công đã triển khai nhiều lỗ hổng zero-day và mã độc cho nhiều thiết bị truy cập Internet nhằm xâm nhập toàn bộ hệ thống thông tin của doanh nghiệp. Cơ quan, tổ chức và doanh nghiệp cần thực hiện rà quét, kiểm tra hệ thống để tránh nguy cơ bị tấn công mạng và đưa ra các phương án xử lý kịp thời.

Nguồn: https://thehackernews.com/2023/03/china-linked-hackers-targeting.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 547 lỗ hổng, trong đó có 67 lỗ hổng mức Cao, 108 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 372 lỗ hổng chưa đánh giá. Trong đó có ít nhất 56 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 53 lỗ hổng trong Google, Nhóm 02 lỗ hổng trong Linux, Nhóm 15 lỗ hổng trong Gitlab, Nhóm 45 lỗ hổng trong Wordpress, 01 lỗ hổng trong Dell, Nhóm 16 lỗ hổng trong Fortinet, Nhóm 04 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:

- *Google: CVE-2023-1213, CVE-2023-1214,...*
- *Linux: CVE-2022-3424, CVE-2023-0030.*
- *Gitlab: CVE-2022-3707, CVE-2022-3758,...*
- *Wordpress: CVE-2022-4931, CVE-2022-4932,...*
- *Dell: CVE-2022-46752.*
- *Fortinet: CVE-2022-45861, CVE-2022-41333,...*
- *IBM: CVE-2023-27290, CVE-2023-24975,...*

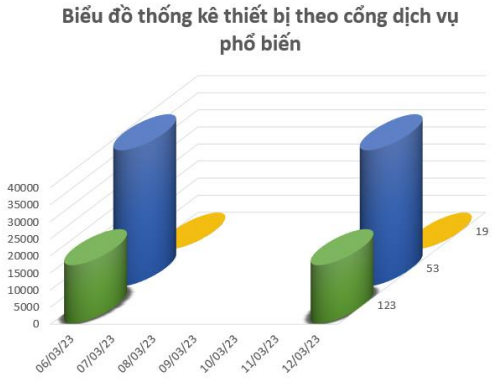
Thông tin điểm yếu, lỗ hổng

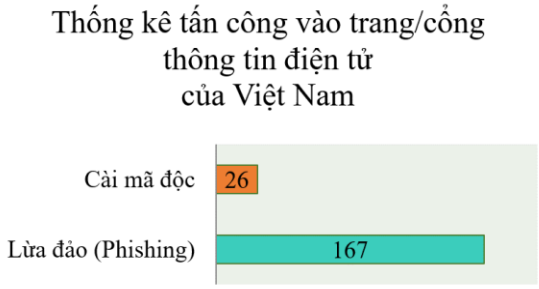
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-1213 CVE-2023-1214 CVE-2023-1215 …	Nhóm 53 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, khai thác lỗi heap thông qua HTML độc hại.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2022-3424 CVE-2023-0030	Nhóm 02 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.	Đã có thông tin xác nhận và bản vá
3	Gitlab	CVE-2022-3707 CVE-2022-3758 CVE-2022-3767 …	Nhóm 15 lỗ hổng trong Gitlab (DAST,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-4931 CVE-2022-4932 CVE-2023-0064 …	Nhóm 45 lỗ hổng trong Wordpress cho phép đối tượng tấn thực hiện với quyền của người dung cục bộ truy cập/thực hiện các hành động trái phép, thực hiện tấn công XSS.	Đã có thông tin xác nhận và bản vá
5	Dell	CVE-2022-46752	01 lỗ hổng trong Dell (BIOS) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
6	Fortinet	CVE-2022-45861 CVE-2022-42476 CVE-2022-41333 …	Nhóm 16 lỗ hổng trong Fortinet (FortiRecorder,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-27290 CVE-2023-24975 CVE-2020-5002 ...	Nhóm 04 lỗ hổng trong IBM (Maximo Application Suite,…) cho phép đối tượng tấn công đánh cắp thông tin dữ liệu, truy cập/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 **51,053** (giảm so với tuần trước **54,042**) 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.



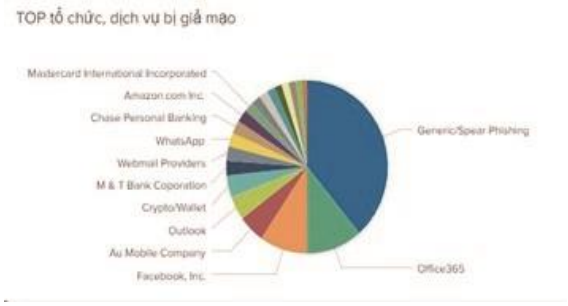


Tấn công Web

Trong tuần, có 193 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 167 trường hợp tấn công lừa đảo (Phishing), 26 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: 21527 IP	xjpakmdcfuqe.ru:491 IP
disorderstatus.ru: 7608 IP	xjpakmdcfuqe.in:489 IP
atomictrivia.ru: 3623 IP	restlesz.su: 364 IP
xjpakmdcfuqe.biz: 825 IP	amnsreiuojy.ru: 1058 IP
xjpakmdcfuqe.com: 535 IP	hzmksreiuojy.ru: 57 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 363 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	tpbank-com.com	Website giả mạo Ngân hàng TMCP Tiên Phong
2	m.tot166.com vay-666.com	Website giả mạo, lừa đảo

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