NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 07 (12/02/2024 – 18/02/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Chiến dịch tấn công Zero-day của nhóm Water Hydra là mối đe dọa đối với các nhà giao dịch tài chính.

- **Cảnh báo:** Đối tượng tấn công mạng Trung Quốc sử dụng Deepfake trong chiến dịch tấn công ngân hàng điện tử.

2. Điểm yếu, lỗ hổng

- **796** 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: 195** 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 Zero-day của nhóm Water Hydra là mối đe dọa đối với các nhà giao dịch tài chính."

Đầu năm nay, Cơ quan bảo mật Trend Micro phát hiện một lỗ hổng an toàn thông tin nghiêm trọng có mã CVE-2024-21412 trên hệ thống Microsoft Defender SmartScreen. Lỗ hổng này là một phần trong các cuộc tấn công zero-day phức tạp của nhóm APT WaterHydra (còn được biết đến với biệt danh DarkCasino). Mục tiêu của các cuộc tấn công này là các nhà giao dịch trên thị trường tài chính.

Trend Micro đã cảnh báo về lỗ hổng này để Microsoft có thể vá lỗi kịp thời. Các hoạt động của nhóm WaterHydra đã được theo dõi từ cuối tháng 12/2023 khi nhóm này sử dụng các công cụ, chiến thuật và thủ thuật liên quan đến việc khai thác các đường dẫn tắt trên internet (.URL) và thành phần WebDAV. Trong chiến dịch tấn công, lỗ hổng CVE-2024-21412 đã bị khai thác để bypass Microsoft Defender SmartScreen và triển khai mã độc DarkMe lên các thiết bị của người dùng. Hiện lỗ hổng này đã được khắc phục trong bản vá mới nhất của Microsoft.

Nhóm APT WaterHydra bắt đầu hoạt động kể từ năm 2021 với mục tiêu chính là ngành tài chính. Đáng chú ý, nhóm này đã trước đó đã khai thác thành công lỗ hổng CVE-2023-38831 trên WinRAR, cho thấy trình độ kỹ thuật cao của họ.

Trong chiến dịch này, WaterHydra đã sử dụng các kỹ thuật phức tạp để thao túng người dùng, đặc biệt là thông qua các chiến dịch spear-phishing trên các sàn giao dịch ngoại hối và các diễn đàn giao dịch chứng khoán. WaterHydra đã tận dụng từ khóa "search:protocol" để thay đổi cách Windows Explorer hiển thị và đánh lừa người dùng mở các tập tin đường dẫn tắt Internet độc hại.

Khi tiến hành phân tích chi tiết, đã xác định được rằng nhóm WaterHydra khai thác lỗ hổng CVE-2024-21412 để bypass Microsoft Defender SmarScreen, thông qua việc sử dụng các đường dẫn tắt internet. Qua đó, nhóm này đã vượt qua biện pháp bảo mật và thực thi payload độc hại như mã độc DarkMe. Phương thức hoạt động này của WaterHydra đã khiến mối đe dọa zero-day trong lĩnh vực an ninh mạng trở nên nghiêm trọng hơn.

Nguồn: https://www.infosecurity-magazine.com/news/water-hydras-zero-day-financial/?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Đối tượng tấn công mạng Trung Quốc sử dụng Deepfake trong chiến dịch tấn công ngân hàng điện tử."

GoldFactory là một nhóm tấn công mạng có nguồn gốc từ Trung Quốc và đang tiến hành phát triển hàng loạt các mã độc Trojan ngân hàng rất tinh vi. Trong số đó, lần đầu xuất hiện một mã độc trên iOS được gọi là GoldPickaxe, có khả năng thu thập thông tin cá nhân, dữ liệu nhận diện khuôn mặt và ngăn chặn tin nhắn SMS.

Bên cạnh đó, nhóm GoldFactory cũng đã phát triển một mã độc ngân hàng trên nền tảng Android, bao gồm GoldDigger và phiên bản nâng cấp GoldDiggerPlus, cùng với GoldKefu là một trojan nhúng trong GoldDiggerPlus. Bắt đầu hoạt động từ giữa năm 2023, nhóm GoldFactory chủ yếu triển khai các chiến dịch Social engineering nhằm vào khu vực Châu Á Thái Bình Dương, đặc biệt là Thái Lan và Việt Nam, bằng cách giả mạo các ngân hàng địa phương và tổ chức chính phủ.

Trong các cuộc tấn công, mã độc GoldPickaxe có thể xâm nhập thiết bị người dùng qua các tin nhắn smishing và phishing, bằng cách dẫn dụ người dùng truy cập các liên kết giả mạo trên các ứng dụng tương tự LINE. Ngoài ra, mã độc cũng thường được phân phối qua các ứng dụng giả mạo trên Google Play Store của Android hoặc các trang web giả mạo của doanh nghiệp. Còn trên iOS, mã độc GoldPickaxe thường lây lan qua ứng dụng TestFlight của Apple và yêu cầu người dùng cài đặt cấu hình Quản lý Thiết bị Di Động (Mobile Device Management). Các tổ chức bảo mật tại Thái Lan và trên toàn cầu đều đã cảnh báo chi tiết về mã độc này vào tháng 11/2023.

Mã độc GoldPickaxe được thiết kế để vượt qua biện pháp bảo mật yêu cầu xác thực bằng khuôn mặt tại Thái Lan. Ứng dụng giả mạo chứa mã độc yêu cầu người dùng ghi lại video để xác thực khuôn mặt, sau đó video này được sử dụng để tạo video deepfake qua dịch vụ tráo đổi khuôn mặt AI. Trên cả Android và iOS, mã độc này đều có khả năng thu thập thông tin CCCD và ảnh của người dùng, chặn tin nhắn và làm trung gian cho lưu lượng mạng. Tuy nhiên, biến thể mã độc trên iOS sẽ có ít chức năng hơn do tính đóng của hệ điều hành.

GoldDigger, một biến thể của mã độc GoldPickaxe, có mã nguồn tương tự và không có dấu vết nào nhằm vào thiết bị iOS. Mã độc này đã được phát hiện từ tháng 06/2023 và đang tiếp tục được sử dụng, mở đường cho các phiên bản nâng cấp như GoldDiggerPlus với trojan APK GoldKefu. GoldKefu giả dạng thành ứng dụng nhắn tin phổ biến ở Việt Nam để lừa đảo và thu thập thông tin từ 10 tổ chức tài chính. Điểm đáng chú ý là GoldKefu tích hợp SDK Agora để gọi điện và lừa đảo người dùng với cảnh báo giả về giao dịch lớn trên tài khoản ngân hàng. Cảnh báo này có nội dung gây hoảng loạn cho người dùng vì một lượng tiền lớn đã được giao dịch trên tài khoản ngân hàng.

Để giảm nguy cơ bị tấn công, người dùng nên tránh nhấn vào các liên kết đáng ngờ, không tải ứng dụng từ các trang không tin cậy vì đây là cách thường gặp để lây nhiễm mã độc. Ngoài ra, cần thường xuyên kiểm tra và quản lý các quyền truy cập của ứng dụng trên thiết bị, đặc biệt là những quyền liên quan đến dịch vụ hỗ trợ tiếp cận trên Android.

Nguồn: https://thehackernews.com/2024/02/chinese-hackers-using-deepfakes-in.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 **796** lỗ hổng, trong đó có 303 lỗ hổng mức Cao, 313 lỗ hổng mức Trung bình, 27 lỗ hổng mức Thấp và 153 lỗ hổng chưa đánh giá. Trong đó có ít nhất 161 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 07 lỗ hổng trong Linux, Nhóm 38 lỗ hổng trong Google, Nhóm 72 lỗ hổng trong Microsoft, Nhóm 31 lỗ hổng trong Wordpress, Nhóm 30 lỗ hổng trong Adobe, Nhóm 04 lỗ hổng trong Apache, Nhóm 24 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-2024-1151, CVE-2024-1485,...

- Google: CVE-2023-40122, CVE-2023-21165,...

- Microsoft: CVE-2024-21404, CVE-2024-21386,...

- Wordpress: CVE-2024-0594, CVE-2024-0842,...

- Adobe: CVE-2024-20726, CVE-2024-20727,...

- Apache: CVE-2023-50386, CVE-2023-50291,...

- IBM: CVE-2023-45187, CVE-2023-45191,...

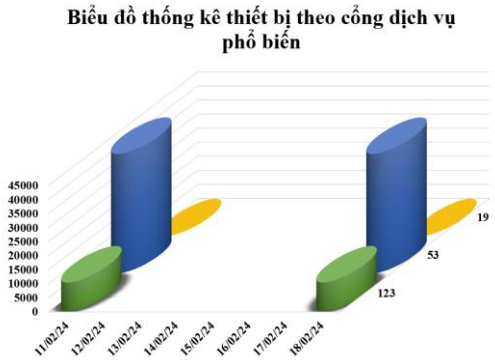
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2024-1151 CVE-2024-1485 CVE-2023-52429 …	Nhóm 07 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-2023-40122 CVE-2023-21165 CVE-2023-40085 …	Nhóm 38 lỗ hổng trong Google cho phép đối tượng tấn công 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
3	Microsoft	CVE-2024-21404 CVE-2024-21386 CVE-2024-21329 …	Nhóm 72 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, thực thi mã từ xa, khai thác lỗ hổng XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2024-0594 CVE-2024-0842 CVE-2024-0610 …	Nhóm 31 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực hiện tấn công SQL Injection, khai thác lỗ hổng XSS, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Adobe	CVE-2024-20726 CVE-2024-20727 CVE-2024-20728 …	Nhóm 30 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗ hổng XSS, 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
6	Apache	CVE-2023-50386 CVE-2023-50291 CVE-2023-50298 …	Nhóm 04 lỗ hổng trong Apache 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
7	IBM	CVE-2023-45187 CVE-2023-45191 CVE-2024-22361 …	Nhóm 24 lỗ hổng trong IBM phép đối tượng tấn công khai thác lỗ hổng XSS, 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** (không thay đổi so với tuần trước **52.826**) 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.

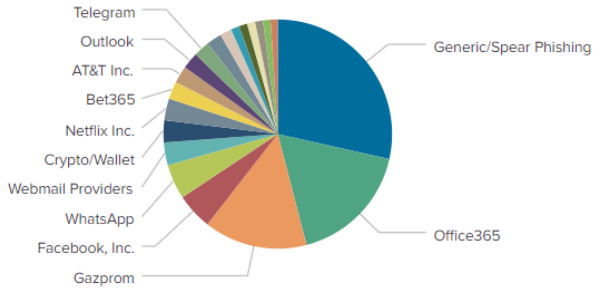


Tấn công Web

Trong tuần, có **95** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 95 trường hợp tấn công lừa đảo (Phishing), không có 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: 5023 IP	hzmksreiuojy.ru: 58 IP
disorderstatus.ru: 2298 IP	xjpakmdcfuqe.biz: 91 IP
atomictrivia.ru: 1060 IP	xjpakmdcfuqe.com: 73 IP
amnsreiuojy.ru: 254 IP	xjpakmdcfuqe.ru: 52 IP
restlesz.su: 121 IP	xjpakmdcfuqe.in: 52 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **195** 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	vinideal-sale.pro	Vingroup
2	spmail88.com	Shopee
3	scb.nanghanmucthenganhangvisa.com/	Ngân hàng Thương mại Cổ phần Sài Gòn

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