NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 05 (29/01/2024 – 04/02/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT28 của Nga tấn công các tổ chức quan trọng bằng phương thức NTLM Relay.

- **Cảnh báo:** CISA cảnh báo về việc lỗ hổng an toàn thông tin trên Apple iOS và macOS bị khai thác.

2. Điểm yếu, lỗ hổng

- **668** 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: 224** 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 APT: Nhóm APT28 của Nga tấn công các tổ chức quan trọng bằng phương thức NTLM Relay"

Nhóm APT28, hay còn được biết đến với nhiều tên gọi khác nhau như Blue Athena, BlueDelta, Fancy Bear, Fighting Ursa, Forest Blizzard (tên cũ Strontium), FROZENLAKE, Iron Twilight, ITG05, Pawn Storm, Sednit, Sofacy và TA422, được cho là một nhóm tấn công mạng có nguồn gốc từ Nga.

Từ tháng 04/2022 đến 11/2023, nhóm APT28 đã sử dụng kỹ thuật NT LAN Manager (NTLM) v2 hash relay để tấn công nhiều tổ chức quan trọng trên toàn cầu, đặc biệt là trong các lĩnh vực như ngoại giao, năng lượng, quốc phòng, vận chuyển, lao động, phúc lợi xã hội, tài chính, tổ chức kế hoạch hóa gia đình và các hội đồng thành phố (UBND Thành phố). Phương thức tấn công của nhóm được đánh giá cao về hiệu suất, đặc biệt khi họ tự động hóa tiến trình brute force để xâm nhập vào hệ thống mạng, có khả năng chiếm dụng hàng ngàn tài khoản email trong quá trình hoạt động.

Từ năm 2009, nhóm APT28 được điều hành bởi một dịch vụ tình báo quân sự tại Nga và đã phát triển lịch sử hoạt động với các chiến dịch spear-phishing, bao gồm việc chứa file đính kèm độc hại hoặc lây nhiễm web một cách chiến lược, nhằm kích hoạt chuỗi lây nhiễm. Vào tháng 04/2018, nhóm APT28 đã khai thác lỗ hổng bảo mật (đã được vá) trên thiết bị mạng của Cisco để thực hiện do thám và triển khai mã độc trên các thiết bị mục tiêu.

Đến tháng 12/2023, nhóm này khai thác thành công lỗ hổng leo thang đặc quyền trên Microsoft Outlook (CVE-2023-23397, Điểm CVSS: 9.8) và lỗ hổng cho phép thực thi mã từ trên WinRAR (CVE-2023-38831, Điểm CVSS: 7.8). APT28 tận dụng các lỗ hổng này để truy cập vào hàm băm NET-NTLMv2 của người dùng và triển khai tấn công NTLM relay, đồng thời chiếm đoạt quyền truy cập trái phép vào hòm thư của các công ty công và tư nhân.

Một cơ quan bảo mật đã xác nhận rằng lỗ hổng CVE-2023-23397 đã được khai thác nhằm vào các tổ chức ở Ukraine vào tháng 04/2022. Nhóm này cũng sử dụng văn bản mồi nhử liên quan đến xung đột Israel-Hamas để triển khai các mã độc như HeadLace, OCEANMAP, MASEPIE và STEELHOOK, trong các cuộc tấn công nhằm vào chính phủ Ukraine và tổ chức Ba Lan.

Điểm đáng chú ý trong các chiến dịch của APT28 là sự đầu tư vào phát triển chiến thuật và tối ưu hóa biện pháp tấn công, sử dụng lớp ẩn danh bao gồm VPN, Tor, địa chỉ IP trung tâm dữ liệu, và thậm chí xâm nhập vào router EdgeOS để quét và dò quét hệ thống. Chiến thuật khác bao gồm gửi tin spear-phishing qua tài khoản email đã bị xâm nhập thông qua Tor hoặc VPN. Ước tính ít nhất 100 router EdgeOS đã bị nhóm xâm nhập trong quá trình này.

Nguồn: https://thehackernews.com/2024/02/russian-apt28-hackers-targeting-high.html

Tin tức An toàn thông tin

"Cảnh báo: CISA cảnh báo về việc lỗ hổng an toàn thông tin trên Apple iOS và macOS bị khai thác"

Cơ quan An ninh Mạng và Cơ sở hạ tầng An toàn thông tin của Hoa Kỳ (CISA) đã bổ sung một lỗ hổng an toàn thông tin ở mức nghiêm trọng ảnh hưởng đến iOS, iPadOS, macOS, tvOS và watchOS vào danh mục "Các lỗ hổng bị khai thác trong thực tế (KEV)" của tổ chức này dựa trên một số bằng chứng về việc lỗ hổng đang bị khai thác gần đây.

Lỗ hổng này có mã CVE-2022-48618 (Điểm CVSS: 7.8) liên quan đến một lỗi trong thành phần kernel. Lỗ hổng cho phép đối tượng tấn công có thể bypass cơ chế bảo mật bộ nhớ để đọc và ghi tùy ý, gọi là Pointer Authentication.

Lỗ hổng này tác động đến các phiên bản iOS cũ hơn 15.7.1. Apple xác nhận rằng vấn đề đã được khắc phục thông qua việc nâng cấp các biện pháp kiểm tra. Tuy nhiên, vẫn chưa rõ liệu lỗ hổng này đã bị khai thác trong các chiến dịch tấn công thực tế hay chưa.

Đáng chú ý, mặc dù bản vá cho lỗ hổng đã được phát hành vào ngày 13/12/2022 với sự ra mắt của iOS 16.2, iPadOS 16.2, macOS Ventura 13.1, tvOS 16.2, và watchOS 9.2 nhưng tới hơn một năm sau (ngày 09/01/2024) thì thông tin này mới được công bố rộng rãi.

Bên cạnh đó, Apple cũng đã giải quyết một lỗ hổng tương tự trong kernel (CVE-2022-32844, Điểm CVSS: 6.3) trên iOS 15.6 và iPadOS 15.6 trong bản vá phát hành vào ngày 20/07/2022. Thông tin này được công bố cùng thời điểm với việc phát hành bản vá mở rộng của Apple cho lỗ hổng an toàn thông tin CVE-2024-23222 (Điểm CVSS: 8.8) tồn tại trên WebKit browser engine để bao gồm cả sản phẩm Apple Vision Pro trên phiên bản visionOS 1.0.2.

Nguồn:https://thehackernews.com/2024/02/cisa-warns-of-active-exploitation-of.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 **668** lỗ hổng, trong đó có 249 lỗ hổng mức Cao, 296 lỗ hổng mức Trung bình, 43 lỗ hổng mức Thấp và 80 lỗ hổng chưa đánh giá. Trong đó có ít nhất 126 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 10 lỗ hổng trong Linux, Nhóm 03 lỗ hổng trong Google, Nhóm 08 lỗ hổng trong Microsoft, Nhóm 45 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong Gitlab, Nhóm 03 lỗ hổng trong Cisco, Nhóm 37 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-2023-6779, CVE-2023-46838,...

- Google: CVE-2024-1059, CVE-2024-1060,...

- Microsoft: CVE-2024-21326, CVE-2024-21385,...

- Wordpress: CVE-2023-6390, CVE-2023-6946,...

- Gitlab: CVE-2024-0402, CVE-2023-6159,...

- Cisco: CVE-2024-20253, CVE-2024-20263,...

- IBM: CVE-2023-38273, CVE-2024-23619,...

Thông tin điểm yếu, lỗ hổng

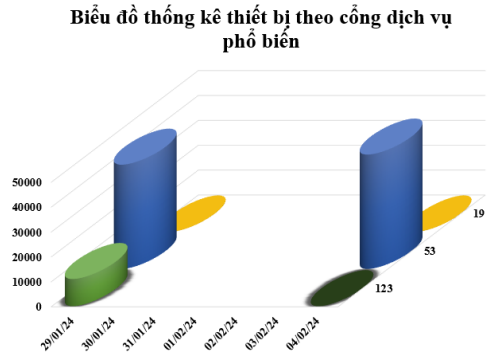
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-6779 CVE-2023-46838 CVE-2023-6200 …	Nhóm 10 lỗ hổng trong Linux cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
2	Google	CVE-2024-1059 CVE-2024-1060 CVE-2024-1077	Nhóm 03 lỗ hổng trong Google 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
3	Microsoft	CVE-2024-21326 CVE-2024-21385 CVE-2024-21399 …	Nhóm 08 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-6390 CVE-2023-6946 CVE-2023-7074 …	Nhóm 45 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗ hổng CSRF, khai thác lỗ hổng XSS.	Chưa có thông tin xác nhận và bản vá
5	Gitlab	CVE-2024-0402 CVE-2023-6159 CVE-2023-5612 …	Nhóm 05 lỗ hổng trong Gitlab cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
6	Cisco	CVE-2024-20253 CVE-2024-20263 CVE-2024-20305	Nhóm 03 lỗ hổng trong Cisco cho phép đối tượng tấn công 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
7	IBM	CVE-2023-38273 CVE-2024-23619 CVE-2024-23621 …	Nhóm 37 lỗ hổng trong IBM 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

NCSC VN
National Cyber Security Center

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

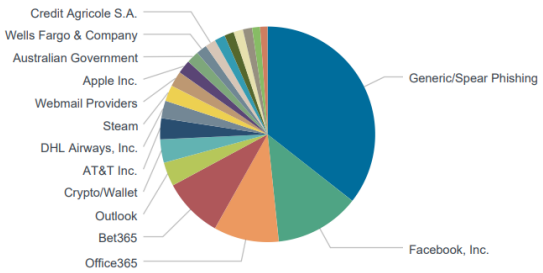
Tấn công DRDoS

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 **56.765**, (tăng so với tuần trước **53.422**) 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 **97** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 88 trường hợp tấn công lừa đảo (Phishing), 09 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: 9513 IP	hzmksreiuojy.ru: 118 IP
disorderstatus.ru: 4647 IP	xjpakmdcfuqe.biz: 189 IP
atomictrivia.ru: 2130 IP	xjpakmdcfuqe.com: 114 IP
amnsreiuojy.ru: 640 IP	xjpakmdcfuqe.ru: 90 IP
restlesz.su: 246 IP	xjpakmdcfuqe.in: 101 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **224** 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	dich-vu-the-cashback-vib.com dich-vu-the-kt3-vib.com vib.tructuyen-chamsockhachang-the.com bio.linkvibthetindung	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
2	vuabem.com trumbem.com	Website giả mạo Ví điện tử Momo
3	ghnn33.com	Website giả mạo sàn TMĐT Tiki
4	vn55779p.com	Website giả mạo sàn TMĐT Shopee
5	mothe.tindung-hd.com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
6	vnsendo.vip	Website giả mạo sàn TMĐT Sendo
7	dichvucong.xgovn.net	Website giả mạo 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 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