NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 52 (23/12/2024 – 29/12/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Ghi nhận chiến dịch tấn công gây ảnh hưởng tới 16 tiện ích mở rộng trên Chrome dẫn tới lộ lọt dữ liệu.

- **Cảnh báo:** Apache đưa ra cảnh báo về các lỗ hổng an toàn thông tin nghiêm trọng trên MINA, HugeGraph, Traffic Control.

2. Điểm yếu, lỗ hổng

- TOP **10** lỗ hổng đáng chú ý trong tuần.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 7.083** 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

"Chiến dịch tấn công APT: Ghi nhận chiến dịch tấn công gây ảnh hưởng tới 16 tiện ích mở rộng trên Chrome dẫn tới lộ lọt dữ liệu"

Gần đây, các chuyên gia bảo mật đã ghi nhận một chiến dịch tấn công nhằm vào các tiện ích mở rộng trên trình duyệt Google Chrome, dẫn tới việc ít nhất 16 tiện ích đã bị ảnh hưởng và khiến dữ liệu của hơn 600.000 người dùng bị lộ lọt, đánh cắp.

Chiến dịch này tấn công nhằm vào các nhà phát hành tiện ích trình duyệt trên Chrome Web Store thông qua hình thức phishing và sử dụng quyền truy cập đạt được từ họ để chèn mã độc vào các tiện ích. Mục tiêu là để đánh cắp cookie và token truy cập của người dùng.

Cụ thể, tiện ích bị ảnh hưởng đầu tiên được ghi nhận thuộc sở hữu của hãng bảo mật Cyberhaven, khi một nhân viên của hãng bị lừa và làm mất quyền truy cập vào tay đối tượng tấn công, cho phép đối tượng phát hành phiên bản độc hại của tiện ích vào ngày 24/12. Phiên bản độc hại của tiện ích có khả năng kết nối tới máy chủ C&C, tải file cấu hình và trích xuất dữ liệu người dùng.

Email phishing được đối tượng sử dụng được cho là tới từ "Google Chrome Web Store Developer Support" có mục đích tạo ra vấn đề cấp bách giả tạo cho người nhận bằng cách nói rằng tiện ích của hãng này đang đứng trước nguy cơ bị gỡ bỏ khỏi Web Store do vi phạm chính sách. Trong email, đối tượng cũng giục người dùng bấm vào đường dẫn độc hại để chấp nhận chính sách mới, khi bấm vào sẽ được điều hướng tới một trang có chức năng cấp quyền tới một ứng dụng Oauth độc hại có tên "Privacy Policy Extension".

Sau đó, đối tượng tấn công sẽ đạt được quyền truy cập cần thiết để có thể tải lên tiện ích độc hại tới Chrome Web Store.

Một số tiện ích mở rộng khác bị ảnh hưởng gồm có: AI Assistant - ChatGPT and Gemini for Chrome; Bard AI Chat Extension; GPT 4 Summary with OpenAI; Search Copilot AI Assistant for Chrome; TinaMInd AI Assistant; Wayin AI; VPNCity; Internxt VPN; Vindoz Flex Video Recorder; VidHelper Video Downloader; Bookmark Favicon Changer; Castorus; Uvoice; Reader Mode; Parrot Talks; Primus; Tackker - online keylogger tool; AI Shop Buddy; Sort by

Nguồn: https://thehackernews.com/2024/12/16-chrome-extensions-hacked-exposing.html

"Chiến dịch tấn công APT: Ghi nhận chiến dịch tấn công gây ảnh hưởng tới 16 tiện ích mở rộng trên Chrome dẫn tới lộ lọt dữ liệu"

Oldest; Rewards Search Automator; ChatGPT Assistant - Smart Search; Keyboard History Recorder; Email Hunter; Visual Effects for Google Meet; Earny - Up to 20% Cash Back.

Với việc nhiều tiện ích mở rộng bị ảnh hưởng đã chứng minh được quy mô của chiến dịch tấn công này là rất lớn. Theo ý kiến từ một chuyên gia bảo mật, có khả năng chiến dịch này đã diễn ra kể từ ngày 05/04/2023 hoặc thậm chí là cũ hơn khi một domain C&C được sử dụng có ngày đăng ký từ năm 2021.

Các tiện ích mở rộng một khi bị ảnh hưởng sẽ có phương thức thực hiện hành vi độc hại theo hướng riêng, đối với ghi nhận của hãng Cyberhaven, tiện ích độc hại này nhằm vào dữ liệu danh tính, token truy cập của tài khoản Facebook, cụ thể hơn là tài khoản của Facebook Ads.

Hiện các chuyên gia bảo mật vẫn đang tiếp tục quá trình rà quét nhằm phát hiện thêm các tiện ích mở rộng bị ảnh hưởng, tuy nhiên tính phức tạp và phạm vi của chiến dịch này là một lời cảnh báo cho các nhà phát triển để họ cải thiện khả năng bảo mật của tiện ích do mình phát hành.

Ngoài ra, tại thời điểm hiện tại vẫn chưa phát hiện được nhóm đối tượng tấn công đằng sau chiến dịch này là ai.

Một số IoC được ghi nhận:

cyberhavenext[.]pro	api.cyberhaven[.]pro
149.28.124[.]84	149.248.2[.]160

Nguồn: https://thehackernews.com/2024/12/16-chrome-extensions-hacked-exposing.html

Tin tức An toàn thông tin

"Cảnh báo: Apache đưa ra cảnh báo về các lỗ hổng an toàn thông tin nghiêm trọng trên MINA, HugeGraph, Traffic Control"

Gần đây, hãng Apache Software Foundation đã phát hành bản vá nhằm sửa ba lỗ hổng ảnh hưởng tới giải pháp MINA, HugeGraph-Server và Traffic Control.

Một trong các lỗ hổng được vá là CVE-2024-52046 (Điểm CVSS: 10.0) gây ảnh hưởng tới giải pháp MINA, cụ thể là trên hàm "ObjectSerializationDecoder" gây ra bởi việc giải tuần tự Java không được bảo mật, qua đó cho phép đối tượng tấn công thực thi mã từ xa. Hãng Apache cũng cho biết, lỗ hổng này chỉ có thể bị khai thác nếu phương thức "IoBuffer#getObject()" được sử dụng kết hợp với một số lớp cụ thể. Ngoài việc cập nhật bản vá, người dùng còn cần phải thiết lập việc từ chối tất cả các lớp, trừ các lớp được ghi trong danh sách cho phép đưa ra bởi Apache.

Lỗ hổng thứ hai có mã CVE-2024-43441, là lỗi cho phép đối tượng tấn coogn bỏ qua biện pháp bảo mật xác thực tồn tại trên HugeGraph-Server. Xảy ra do logic xác thực không được xử lý đúng cách.

Lỗ hổng thứ ba được vá là CVE-2024-43587 tồn tại trên Software Foundation và là lỗi SQL Injection xảy ra do thiếu sót trong không làm sạch dữ liệu đưa vào trên câu truy vấn SQL, từ đó cho phép đối tượng tấn công thực thi lệnh SQL tùy ý thông qua yêu cầu PUT.

Các quản trị viên hệ thống được Apache khuyến nghị nên cập nhật bản vá sớm nhất có thể để tránh rủi ro bị ảnh hưởng bởi tấn công của các nhóm đối tượng khai thác các lỗ hổng này.

Nguồn: https://www.bleepingcomputer.com/news/security/apache-warns-of-critical-flaws-in-mina-hugegraph-traffic-control/

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 **589** lỗ hổng, trong đó có 79 lỗ hổng mức Cao, 124 lỗ hổng mức Trung bình, 32 lỗ hổng mức Thấp và 354 lỗ hổng chưa đánh giá. Trong đó có ít nhất 43 lỗ hổng cho phép chèn và thực thi mã lệnh.

Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm trọng cao hoặc đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của Acclaim, Palo Alto Networks và Apache, cụ thể là như sau:

- **CVE-2024-56338 (Điểm CVSS: Chưa xác định):** Lỗ hổng tồn tại trên Apache Tomcat là lỗi Time-of-check Time-of-use (TOCTOU) Race Condition xảy ra khi người dùng cố truy cập vào một file đang được chỉnh sửa bởi một tiến trình khác. Đối tượng tấn công sau khi khai thác thành công có thể thực thi mã từ xa. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2021-44207 (Điểm CVSS: 8.1 – Cao):** Lỗ hổng tồn tại trên Acclaim USAHERDS xảy ra do thông tin xác thực trên giải pháp được sử dụng một cách cố định và định sẵn từ trước. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế
- **CVE-2024-9474 (Điểm CVSS: 7.2 – Cao):** Lỗ hổng tồn tại trên Palo Alto Networks PAN-OS cho phép đối tượng tấn công với quyền quản trị viên có thể truy cập vào giao diện web và thực hiện các hành vi trái phép trên tường lửa với đặc quyền root, từ đó dẫn tới việc leo thang đặc quyền. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-56337	- Điểm CVSS: Chưa xác định - Ảnh hưởng: Apache Tomcat - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-56337
2	CVE-2021-44207	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Acclaim USAHERDS - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2021-44207
3	CVE-2024-9474	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-9474
4	CVE-2024-3393	- Điểm CVSS: 8.7 (Cao) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-3393
5	CVE-2024-40896	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: libxml2 - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-40896

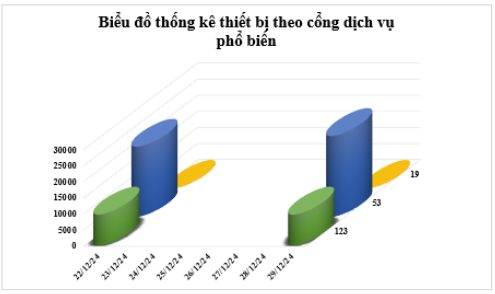
TOP 10 lỗ hổng đáng chú ý trong tuần

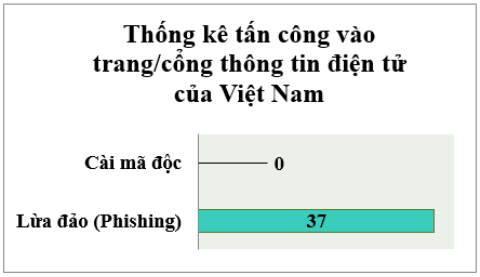
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-45387	- Điểm CVSS: 9.9 (Nghiêm trọng) - Ảnh hưởng: Apache Traffic Control - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi SQL Injection - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-45387
7	CVE-2024-50379	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Apache Tomcat - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-50379
8	CVE-2024-12856	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: Route Four-Faith mẫu F3x24 và F3x36 - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-12856
9	CVE-2024-21182	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Oracle WebLogic Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-21182
10	CVE-2024-53961	- Điểm CVSS: 7.4 (Cao) - Ảnh hưởng: ColdFusion - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-53961

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 **34.860** (tăng so với tuần trước **31.516**) 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.



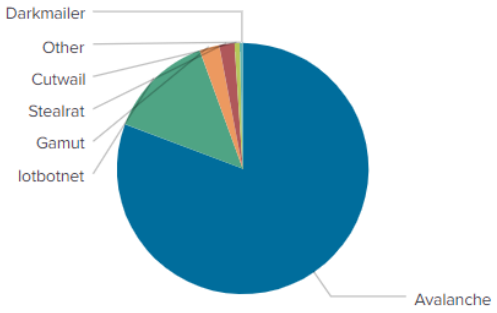


Tấn công Web

Trong tuần, có **37** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 37 trường hợp tấn công lừa đảo (Phishing), 0 trường hợp tấn công cài cắm mã độc.

Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.



Địa chỉ được sử dụng trong các mạng botnet

disorderstatus.ru	ygiudewsqhct.in
differentia.ru	xjpakmdcfuqe.biz
atomictrivia.ru	japqhs.info
morphed.ru	amnsreiuojy.ru
a.asense.in	devicesta.ru
thesecond.in	c.deltaheavy.ru
sdk.asense.in	b.deltaheavy.ru
hzmksreiuojy.in	gjogvvpsf.biz
statis.multispacesext.net	xjpakmdcfuqe.com
a.deltaheavy.ru	xjpakmdcfuqe.in

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **7.083** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **174** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **6.909** trường hợp phản ánh cuộc gọi, tin nhắn lừa đảo thông qua tổng đài 156/5656

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	https://amazonl5[.]vip	Website giả mạo sàn TMĐT Amazon
2	http://amazonl5[.]vip/#/pages/order/order-detail?id=89190	Website giả mạo sàn TMĐT Amazon
3	Aeonmail[.]shop	Website giả mạo Công ty TNHH Aeon Việt Nam
4	cucanninhmang24h[.]com	Website giả mạo Cục An ninh mạng, Bộ Công an
5	https://dienmay-xanh24h[.]online/?gad_source=1&gclid=CjwKCAiAmrS7BhBJEiwAei59izlOa1dbyUoVni_pjS4IFzvHXSt7Ob7yY4gCVP_wKgNIsytPvdwI5xoCTuoQAvD_BwE	Website giả mạo Điện máy xanh
6	https://kythuatdmayxanh[.]com/sua-bep-tu-bep-hong-ngoai-dien-may-xanh/?zarsrc=30&utm_source=zalo&utm_medium=zalo&utm_campaign=zalo	Website giả mạo Điện máy xanh
7	giaohangnhanh88[.]com	Website giả mạo Giao hàng nhanh
8	https://kbthuhoivontreo[.]com/	Website giả mạo Kho bạc Nhà nước
9	https:/kbthuhoivontreo[.]com/	Website giả mạo Kho bạc Nhà nước
10	https://vietnam-mensual[.]com	Website giả mạo Netflix
11	https://nzu23516s[.]com/	Website giả mạo sàn TMĐT Shopee
12	https://www[.]tbaovn-cms[.]top	Website giả mạo sàn TMĐT Taobao
13	https://marketing-oder[.]com/	Website giả mạo sàn TMĐT Taobao
14	https://tbaovn-cms[.]top/	Website giả mạo sàn TMĐT Taobao
15	https://khaosat[.]me/survey/tap-doan-buu-chinh-vien-thong-viet-nam-02e9140	Website giả mạo Tập đoàn Bưu chính Viễn thông Việt Nam
16	www[.]evnspcs[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
17	https://tiktok-svip85[.]com/r?code=NXMHDY	Website giả mạo TikTok
18	https://travelokaintern[.]vn/	Website giả mạo Traveloka
19	https://chinhphu[.]kbshkdt[.]org/	Website giả mạo Văn phòng Chính phủ
20	https://www[.]vingroupcompany991[.]com/	Website giả mạo Vingroup

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, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

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**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

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