NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 43 (21/10/2024 – 27/10/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Phát hiện nhóm APT Lazarus Group khai thác lỗ hổng trên Google Chrome để kiểm soát thiết bị.

- **Cảnh báo:** CISA cảnh báo lỗ hổng nghiêm trọng trên Microsoft SharePoint đang bị khai thác.

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: 207** 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: Phát hiện nhóm APT Lazarus Group khai thác lỗ hổng trên Google Chrome để kiểm soát thiết bị"

Nhóm APT Lazarus Group đến từ Triều Tiên vừa bị phát hiện lợi dụng lỗ hổng zero-day (hiện đã được vá) trong Google Chrome để chiếm quyền kiểm soát thiết bị đang bị lây nhiễm mã độc.

Vào tháng 05/2024, chiến dịch tấn công của nhóm Lazarus Group bị phát hiện nhắm vào máy tính cá nhân của một người dùng tại Nga bằng mã độc Manuscrypt, một dạng mã độc backdoor. Để kích hoạt chuỗi tấn công, người dùng chỉ cần truy cập vào trang web game giả mạo, vốn nhắm đến những ai quan tâm tới lĩnh vực tiền mã hóa. Chiến dịch này được cho là đã bắt đầu sớm nhất từ tháng 02/2024.

Lỗ hổng zero-day mà nhóm Lazarus khai thác là CVE-2024-4947, một lỗi thuộc loại type confusion trên engine V8 JavaScript và WebAssembly của Chrome, đã được Google vá vào giữa tháng 05/2024.

Một điểm đáng chú ý là nhóm này đã sử dụng trò chơi giả mạo với các tên như DeTankWar, DeFiTankWar, DeTankZone hoặc TankWarsZone để phát tán mã độc. Trước đó, chiến thuật đã được sử dụng bởi nhóm Moonstone Sleet, cũng là một nhóm tấn công đến từ Triều Tiên, nhằm dụ dỗ người dùng tải trò chơi thông qua email hoặc tin nhắn giả danh là công ty blockchain hoặc nhà phát triển game cần huy động đầu tư.

Trong phát hiện mới nhất của Kaspersky, chuỗi tấn công này sử dụng hai lỗ hổng:

- Lỗ hổng CVE-2024-4947 cho phép đối tượng tấn công quyền đọc và ghi toàn bộ không gian địa chỉ của tiến trình Chrome thông qua JavaScript;
- Lỗ hổng thứ hai cho phép đối tượng tấn công vượt qua lớp bảo mật sandbox của V8. Nguyên nhân là máy ảo có số register cố định và vùng lưu trữ riêng, nhưng không kiểm tra giới hạn khi truy cập, nên kẻ tấn công có thể truy cập vào bộ nhớ ngoài phạm vi. Google đã vá lỗi này vào tháng 03/2024.

Sau khi khai thác thành công, đối tượng tấn công triển khai một shellcode để thu thập thông tin hệ thống, đánh giá giá trị của thiết bị trước khi quyết định tiến hành các bước hậu khai thác. Tuy nhiên, payload cụ thể được phát tán sau đó hiện vẫn chưa được xác định rõ.

Nguồn: https://thehackernews.com/2024/10/lazarus-group-exploits-google-chrome.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Phát hiện nhóm APT Lazarus Group khai thác lỗ hổng trên Google Chrome để kiểm soát thiết bị"

Nhóm Lazarus còn hoạt động tích cực trên mạng xã hội như X (trước đây là Twitter) và LinkedIn, đồng thời sử dụng các trang web và email nhằm tiếp cận người dùng mục tiêu. Trang web của họ được thiết kế tinh vi để dụ người dùng tải xuống tệp ZIP ("detankzone.zip"), trong đó chứa một trò chơi hoàn chỉnh yêu cầu đăng ký, đồng thời bí mật triển khai một loader tên "YouieLoad". Lazarus còn bị nghi ngờ đã đánh cắp mã nguồn từ trò chơi blockchain DeFiTankLand để tạo ra trò chơi giả mạo này và thực hiện chiến dịch phát tán mã độc.

Một số IoC được ghi nhận:

B2DC7AEC2C6D2FFA28219AC288E4750C	E5DA4AB6366C5690DFD1BB386C7FE0C78F6ED54F
7353AB9670133468081305BD442F7691CF2F2C1136F09D9508400546C417833A	8312E556C4EEC999204368D69BA91BF4
7F28AD5EE9966410B15CA85B7FACB70088A17C5F	59A37D7D2BF4CFFE31407EDD286A811D9600B68FE757829E30DA4394AB65A4CC
detankzone[.]com	ccwaterfall[.]com

Nguồn: https://thehackernews.com/2024/10/lazarus-group-exploits-google-chrome.html

Tin tức An toàn thông tin

"Cảnh báo: CISA cảnh báo lỗ hổng nghiêm trọng trên Microsoft SharePoint đang bị khai thác"

Cơ quan An ninh mạng và cơ sở hạ tầng của Hòa Kỳ (CISA) vừa đưa ra cảnh báo về một lỗ hổng an toàn thông tin mức Cao trên Microsoft SharePoint, lỗ hổng này đã được bổ sung vào danh sách các lỗ hổng bị khai thác (KEV) sau khi có bằng chứng cho thấy nó đang bị khai thác.

Lỗ hổng có mã CVE-2024-38094 (Điểm CVSS: 7.2), là một lỗ hổng giải tuần tự ảnh hưởng đến SharePoint, khi bị khai thác cho phép đối tượng tấn công thực thi mã từ xa. Đặc biệt, khi được xác thực với quyền quản trị viên trang (Site Owner), đối tượng tấn công có thể chèn và thực thi bất kỳ đoạn mã nào trên SharePoint Server.

Microsoft đã phát hành bản vá cho lỗ hổng này trong bản cập nhật Patch Tuesday vào tháng 07/2024. Tuy nhiên, nguy cơ khai thác vẫn cao do các khai thác Proof-of-Concept (PoC) đã có sẵn trên mạng.

Mã PoC này tự động hóa quá trình xác thực trên một trang SharePoint sử dụng NTLM, tạo ra các thư mục và tệp cụ thể, đồng thời gửi payload XML để khai thác lỗ hổng trong API phía client của SharePoint.

Thông tin về lỗ hổng được công bố trong bối cảnh Nhóm Phân tích Đe dọa (TAG) của Google vừa thông báo về một lỗ hổng zero-day (đã được vá) trên CPU của thiết bị di động Samsung. Lỗ hổng này có mã CVE-2024-44068 (Điểm CVSS: 8.1) đã bị khai thác trong một chuỗi tấn công để thực thi mã tùy ý, đã được vá vào ngày 7 tháng 10 năm 2024. Samsung cho biết đây là một lỗi "use-after-free" trong bộ xử lý di động, dẫn đến việc leo thang đặc quyền.

CISA đã đưa ra một đề xuất mới với các yêu cầu bảo mật nhằm ngăn chặn truy cập trái phép vào dữ liệu nhạy cảm của Mỹ. Theo đó, các tổ chức cần khắc phục các lỗ hổng đã khai thác trong vòng 14 ngày, các lỗ hổng Nghiêm trọng không bị khai thác trong 15 ngày, và các lỗ hổng mức Cao không bị khai thác trong 30 ngày. CISA cũng nhấn mạnh sự cần thiết duy trì nhật ký kiểm tra quyền truy cập và phát triển quy trình quản lý danh tính để xác định rõ ai có quyền truy cập vào các tập dữ liệu khác nhau.

Nguồn: https://thehackernews.com/2024/10/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 **775** lỗ hổng, trong đó có 360 lỗ hổng mức Cao, 324 lỗ hổng mức Trung bình, 30 lỗ hổng mức Thấp và 61 lỗ hổng chưa đánh giá. Trong đó có ít nhất 127 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 Microsoft, Roundcube và angular-base64-upload, cụ thể là như sau:

- **CVE-2024-38178 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng tồn tại trên Microsoft Windows 10, Windows 11 là lỗi bộ nhớ trên phần scripting engine. Sau khi khai thác thành công lỗ hổng, đối tượng tấn công có thể thực thi mã tùy ý từ xa trên hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-37383 (Điểm CVSS: 6.1 – Trung bình):** Lỗ hổng tồn tại trên Roundcube Webmail cho phép đối tượng tấn công khai thác lỗi XSS thông qua thành phần SVG animate. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-42640 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên angular-base64-upload cho phép đối tượng tấn công thực thi mã từ xa thông qua việc tải các file tùy ý lên “demo/uploads”. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-38178	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - 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-2024-38178
2	CVE-2024-37383	- Điểm CVSS: 6.1 (Trung bình) - Ảnh hưởng: Roundcube Webmail - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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-2024-38178
3	CVE-2024-42640	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: angular-base64-upload - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, 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-2024-42640
4	CVE-2024-47575	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: FortiManager - 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-2024-47575
5	CVE-2024-46538	- Điểm CVSS: 9.3 (Nghiêm trọng) - Ảnh hưởng: pfsense - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi XSS - 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-2024-46538

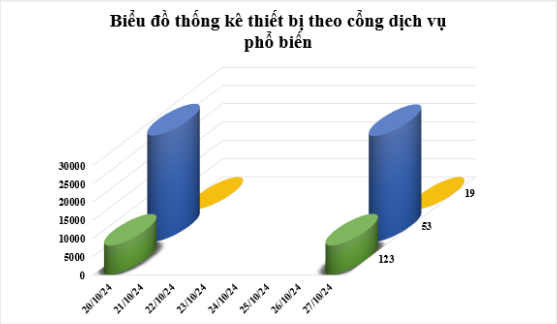
TOP 10 lỗ hổng đáng chú ý trong tuần

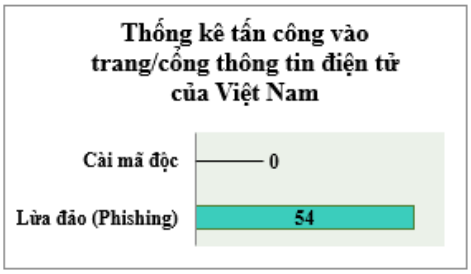
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-20481	- Điểm CVSS: 5.8 (Trung bình) - Ảnh hưởng: Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-20481
7	CVE-2024-23113	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Fortinet FortiOS, FortiProxy, FortiPAM, và FortiSwitchManager - 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-2024-23113
8	CVE-2024-40766	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: SonicWall SonicOS - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - 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-2024-40766
9	CVE-2024-38812	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: VMware vCenter Server - 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-2024-38812
10	CVE-2024-4947	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - 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-2024-4947

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 **36.974** (giảm so với tuần trước **37.102**) 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.



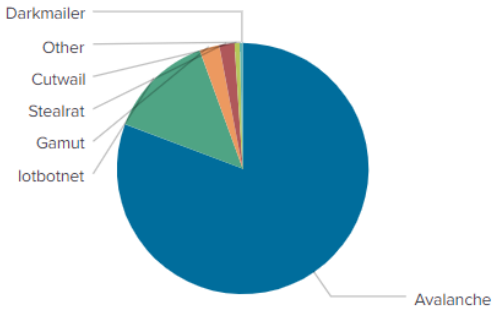


Tấn công Web

Trong tuần, có **54** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 54 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

differentia.ru	xjpakmdcfuqe.ru
disorderstatus.ru	yk37wagdg.life
atomictrivia.ru	restless.su
amnsreiuojy.ru	spaines.pw
hzmksreiuojy.ru	api.garageserviceoperation.com
xjpakmdcfuqe.biz	ctivo.com
restlesz.su	andall.servicesql.info
xjpakmdcfuqe.com	griefcube.cc
08ro35delw.ru	yxjsibeugmmj.com
xjpakmdcfuqe.in	uuyiiuqwownx.pw

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **4624** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **207** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **4417** 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	amazoul[.]site	Website giả mạo sàn TMĐT Amazon
2	amazonl0[.]com	Website giả mạo sàn TMĐT Amazon
3	amazoni2[.]com	Website giả mạo sàn TMĐT Amazon
4	ghtk247[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	www[.]ccty-ghtk[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	dichvugiaohangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
7	dichvucong[.]ccbcavn[.]cc	Website giả mạo Dịch vụ công quốc gia
8	dienlanhdienmayxanhvn[.]com	Website giả mạo Điện máy xanh
9	dienmayxanhcenter[.]vn	Website giả mạo Điện máy xanh
10	thuongmai-dientu[.]com	Website giả mạo sàn TMĐT Lazada
11	momoshopvip[.]com	Website giả mạo MoMo
12	www[.]acb[.]chamsocthe-uudai-tructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
13	acb[.]chamsocthe-uudaitructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
14	acb[.]chamsocthe-uudaikhachhang-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
15	acb[.]chamsockhachhang-uudaithetructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
16	shinhan[.]chamsocthe-uudaikhachhang[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
17	sendo1[.]com	Website giả mạo sàn TMĐT Sendo
18	www[.]evnnpcs[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
19	korshoptiktok[.]com	Website giả mạo Tik tok
20	topcvvn[.]com	Website giả mạo Top CV

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