NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 47 (18/11/2024 – 24/11/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT "Gelsemium" từ Trung Quốc thực hiện chiến dịch tấn công nhằm vào hệ thống Linux sử dụng mã độc WolfsBane.

- **Cảnh báo:** Apple phát hành bản vá xử lý các lỗ hổng Zero-Day đang bị khai thác trong thực tế.

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: 4.915** 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: Nhóm APT "Gelsemium" từ Trung Quốc thực hiện chiến dịch tấn công nhằm vào hệ thống Linux sử dụng mã độc WolfsBane"

Gần đây, cơ quan bảo mật đã ghi nhận nhóm APT "Gelsemium" sử dụng mã độc backdoor Linux "WolfsBane" trong chiến dịch tấn công nhằm vào Đông Á và Đông Nam Á. Thông tin này được tổng hợp dựa trên các mẫu mã độc tải lên VirusTotal để phân tích từ Đài Loan, Philippines và Singapore kể từ tháng 03/2023.

Mã độc WolfsBane được đánh giá là phiên bản Linux của mã độc Gelsevirine, vốn là mã độc backdoor trên Windows tồn tại từ năm 2014. Ngoài ra, cơ quan bảo mật này cũng đã ghi nhận một mã độc cài cắm "FireWood" có kết nối một bộ công cụ mã độc "Project Wood".

Hiện FireWood đang được nghi là thuộc sở hữu của nhóm Gelsemium, tuy nhiên vẫn tồn tại khả năng mã độc này được chia sẻ giữa nhiều nhóm tấn công từ Trung Quốc khác nhau.

Mục tiêu của mã độc và công cụ này là để thu thập các dữ liệu quan trọng trên hệ thống như thông tin tổng thể về hệ thống, thông tin xác thực của người dùng, file/thư mục quan trọng bị nhằm tới. Ngoài ra, chúng còn được dùng để duy trì kết nối, thực thi mã từ xa một cách bí mật, qua đó cho phép nhóm đối tượng thu thập thông tin và né tránh phát hiện.

Hiện tại, phương thức xâm nhập đầu vào của nhóm đối tượng chưa được làm rõ nhưng có khả năng cao là thông qua việc khai thác lỗ hổng an toàn thông tin trên ứng dụng web để triển khai webshell có mục đích duy trì kết nối từ xa, qua đó phát tán mã độc WolfsBane. Nhóm đối tượng đã được ghi nhận sử dụng công cụ rootkit mã nguồn mở "BEURK" để che giấu hoạt động trên hệ thống Linux và thực thi câu lệnh gửi tới từ máy chủ C&C; mã độc FireWood sử dụng module rookit trên kernel có tên "usbdev.ko" để thực hiện chức năng tương tự.

Việc mã độc WolfsBane và FireWood được sử dụng là lần đầu nhóm Gelsemium sử dụng mã độc nhằm tới hệ thống Linux, báo hiệu cho việc mở rộng phạm vi tấn công của nhóm đối tượng này.

Nguồn: https://thehackernews.com/2024/11/chinese-apt-gelsemium-targets-linux.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT "Gelsemium" từ Trung Quốc thực hiện chiến dịch tấn công nhằm vào hệ thống Linux sử dụng mã độc WolfsBane"

Một số IoC được ghi nhận:

149[.]248[.]14[.]53	210[.]209[.]72[.]180
4vw37z[.]cn	acro[.]ns1[.]name
domain[.]dns04[.]com	info[.]96html[.]com
microsoftservice[.]dns1[.]us	pctftp[.]otzo[.]com
sitesafecdn[.]hopto[.]org	traveltime[.]hopto[.]org
www[.]sitesafecdn[.]dynamic-dns[.]net	www[.]travel[.]dns04[.]com

Nguồn: https://thehackernews.com/2024/11/chinese-apt-gelsemium-targets-linux.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Apple phát hành bản vá xử lý các lỗ hổng Zero-Day đang bị khai thác trong thực tế"

Trong tuần vừa qua, Apple đã phát hành bản vá bảo mật cho iOS, iPadOS, macOS, visionOS và trình duyệt web Safari để xử lý hai lỗ hổng zero-day đang bị khai thác trong thực tế.

Cụ thể, hai lỗ hổng này là:

- CVE-2024-44308 (Điểm CVSS: 8.8): Lỗ hổng trên JavaScriptCore dẫn tới thực thi mã từ xa khi xử lý các nội dung web độc hại.
- CVE-2024-44309 (Điểm CVSS: 6.1): Lỗi quản lý cookie tồn tại trên WebKit cho phép đối tượng tấn công khai thác thực hiện tấn công XSS khi truyền vào nội dung web độc hại.

Được biết, hai lỗ hổng này đã được vá bằng cách cải thiện khâu kiểm tra và quản lý trạng thái. Apple đã không cung cấp nhiều thông tin về bản chất của việc khai thác, nhưng đã cho biết hai lỗ hổng này "có thể đã bị khai thác trong các hệ thống Mac sử dụng Intel".

Theo đánh giá của chuyên gia bảo mật đã phát hiện ra hai lỗ hổng này thì chúng có thể đã bị khai thác trong chiến dịch tấn công sử dụng spywear được hậu thuẫn bởi chính phủ hoặc dưới dạng "đánh thuê".

Hiện bản vá đã được phát hành cho các thiết bị, hệ điều hành sau:

- iOS 18.1.1 và iPadOS 18.1.1 – Cho iPhone XS trở đi, iPad Pro 13-inch, iPad Pro 12.9-inch từ thế hệ 3, iPad Pro 11-inch từ thế hệ 1, iPad Air từ thế hệ 3, iPad từ thế hệ 7 và iPad mini từ thế hệ 5;
- iOS 17.7.2 and iPadOS 17.7.2 - Cho iPhone XS trở đi, iPad Pro 13-inch, iPad Pro 12.9-inch từ thế hệ 2, iPad Pro 10.5-inch, iPad Pro 11-inch từ thế hệ 1, iPad Air từ thế hệ 3, iPad từ thế hệ 6 và iPad mini từ thế hệ 5;
- macOS Sequoia 15.1.1 – Máy Mac sử dụng macOS Sequoia
- visionOS 2.1.1 - Apple Vision Pro
- Safari 18.1.1 – Máy Mac sử dụng macOS Ventura và macOS Sonoma

Tính tới hiện tại, trong năm 2024, Apple đã xử lý 4 lỗ hổng zero-day tồn tại trên phần mềm của hãng, trong đó CVE-2024-27834 đã được thể hiện trong thực tế tại cuộc thi Pwn2Own Vancouver; ba lỗ hổng còn lại đã được vá vào tháng 01/2024 và 03/2024.

Người dùng được khuyến nghị cập nhật thiết bị của mình lên phiên bản mới nhất để giảm thiểu nguy cơ bị ảnh hưởng bởi tấn công.

Nguồn: https://thehackernews.com/2024/11/apple-releases-urgent-updates-to-patch.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 **1.109** lỗ hổng, trong đó có 451 lỗ hổng mức Cao, 428 lỗ hổng mức Trung bình, 53 lỗ hổng mức Thấp và 177 lỗ hổng chưa đánh giá. Trong đó có ít nhất 160 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, Oracle và Apple, cụ thể là như sau:

- **CVE-2024-43451 (Điểm CVSS: 6.5 – Trung bình):** Lỗ hổng tồn tại trên Microsoft Windows 10, Windows 11, Windows Server 2022 cho phép đối tượng tấn công đánh cắp mã băm NTLM từ hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-21287 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng tồn tại trên Oracle Agile PLM Framework thuộc Oracle Supply Chain cho phép đối tượng tấn công với quyền truy cập vào hệ thống mạng qua HTTP khả năng truy cập và thực hiện các hành vi trái phép tới các dữ liệu quan trọng trên hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-44308 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trên Safari, iOS, iPadOS, macOS và visionOS của hãng Apple cho phép đối tượng truyền vào nội dung web độc hại để đạt được khả năng thực thi mã từ xa. 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-2024-21287	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Oracle - 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-2024-21287
2	CVE-2024-43451	- Điểm CVSS: 6.5 (Trung bình) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2022 - 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-2024-43451
3	CVE-2024-44308	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Safari, iOS, iPadOS, macOS và visionOS - 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-2024-44308
4	CVE-2024-9264	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Grafana - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi Command Injection. - 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-2024-9264
5	CVE-2024-48990	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Gói needrestart của Ubuntu - 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-2024-48990

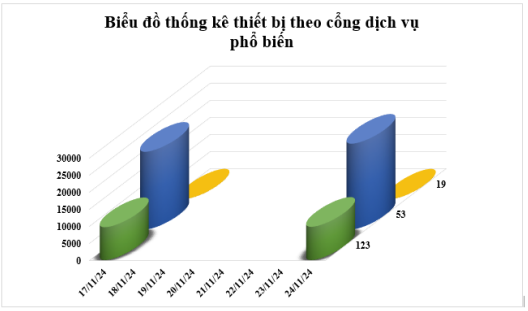
TOP 10 lỗ hổng đáng chú ý trong tuần

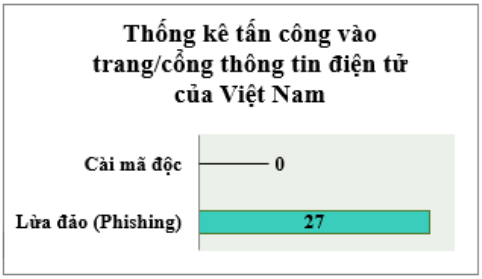
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-0012	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-0012
7	CVE-2024-9474	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng 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
8	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
9	CVE-2024-10924	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Plugin “Really Simple Security” cho WordPress - 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-2024-10924
10	CVE-2024-11003	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Gói needrestart của Ubuntu - 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-2024-11003

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 **34.886** (tăng so với tuần trước **32.424**) 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.



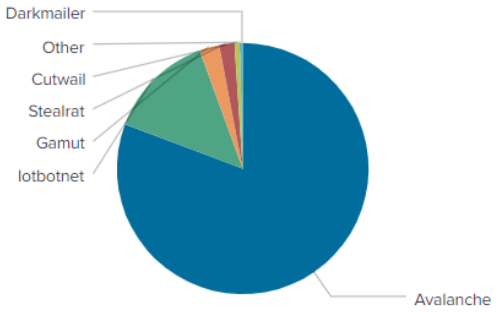


Tấn công Web

Trong tuần, có **27** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 27 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	gjogvvpsf.biz
differentia.ru	morphed.ru
atomictrivia.ru	ygiudewsqhct.in
a.asense.in	hzmksreiuojy.in
sdk.asense.in	a.deltaheavy.ru
statis.multispacesext.net	hzmksreiuojy.ru
ydqlnw.info	xjpakmdcfuqe.biz
thesecond.in	yunalwv.biz
cp.zbum2hkm.ru	b.deltaheavy.ru
amnsreiuojy.ru	yk37wagdg.life

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **4.915** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **292** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **4.623** 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://nhanvienhanghoa[.]com/index/user/index[.]html	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
2	https://chat[.]dichvutonghop[.]vip/index/index/home?visiter_id=&visiter_name=&avatar=&business_id=1&groupid=8&special=32	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://giaohangtietkiem24[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	Giaohangtietkiemm[.]net	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://aeoonmallstore[.]com/	Website giả mạo Công ty TNHH Aeon Việt Nam
6	https://aeoonmallstore[.]com/my	Website giả mạo Công ty TNHH Aeon Việt Nam
7	https://dkvn[.]zvogo[.]com/	Website giả mạo Cục Đăng kiểm Việt Nam
8	bidvnanghanguutien[.]duy2[.]name[.]vn	Website giả mạo Ngân Hàng TMCP Đầu tư và Phát triển Việt Nam
9	hdbank[.]chamsockhachhang-hotro247-capnhatuudai-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
10	hdbank[.]uudaidacbiet-khuyenmaikhachhang-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
11	vib[.]chamsockhachhang-capnhatthethang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	doitac[.]shb-bank[.]com	Website giả mạo Ngân hàng TMCP Sài Gòn – Hà Nội
13	vpbank[.]chamsockhachhang-hotro247-trungtamcapnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
14	vpbank[.]khuyenmaidacbiet-uudaikhachhang-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
15	https://vpbank[.]hotrokhachhang-khuyenmaithethang11[.]com[.]vn/	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
16	https://shinhan[.]chamsockhachhang-hotro247-capnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
17	https://evnspccskh[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
18	evnspccskh[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
19	chinh-phu[.]cc	Website giả mạo Văn phòng Chính phủ
20	https://chinhphu-vn[.]com/	Website giả mạo Văn phòng Chính phủ

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