NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 28 (08/07/2024 – 14/07/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT41 bổ sung mã độc DodgeBox và MoonWalk vào kho mã độc của mình trong các chiến dịch tấn công.

- **Cảnh báo:** Palo Alto Networks phát hành bản vá cho lỗi nghiêm trọng trên công cụ di rời Expedition.

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: 1.942** 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 APT41 bổ sung mã độc DodgeBox và MoonWalk vào kho mã độc của mình trong các chiến dịch tấn công"

Nhóm APT41 có nguồn gốc từ Trung Quốc đang bị tình nghi sử dụng phiên bản nâng cấp của mã độc StealthVector để phát tán một backdoor mới có tên MoonWalk. Biến thể mới này, còn được gọi là DUSTPAN hoặc DodgeBox, đã được phát hiện vào tháng 4 năm 2024.

DodgeBox là một loader có nhiệm vụ phát tán backdoor MoonWalk. Cả hai đều sử dụng nhiều kỹ thuật né tránh bị phát hiện và sử dụng Google Drive cho việc giao tiếp C&C.

APT41 bắt đầu hoạt động từ năm 2007 và có nhiều tên gọi khác nhau như Axiom, Blackfly, Brass Typhoon, Bronze Atlas, Earth Baku, HOODOO, Red Kelpie, TA415, Wicked Panda, và Winnti.

Vào tháng 9 năm 2020, Bộ Tư pháp Hoa Kỳ đã truy tố một số thành viên của nhóm với tội danh tổ chức các chiến dịch tấn công nhằm vào hơn 100 tổ chức toàn cầu, bao gồm đánh cắp mã nguồn, chứng chỉ ký mã phần mềm, dữ liệu khách hàng và thông tin kinh doanh có giá trị, cùng với các hoạt động ransomware và crypto-jacking.

Trong những năm gần đây, nhóm APT41 đã bị phát hiện có liên quan đến các vụ xâm nhập vào mạng lưới chính phủ Mỹ từ tháng 5 năm 2021 đến tháng 2 năm 2022, và các cuộc tấn công nhằm vào các tổ chức truyền thông Đài Loan bằng công cụ mã nguồn mở Google Command and Control (GC2).

Mã độc StealthVector lần đầu tiên được ghi nhận do nhóm APT41 sử dụng vào tháng 8 năm 2021, là một shellcode loader viết bằng C/C++ dùng để triển khai Cobalt Strike Beacon và shellcode ScrambleCross (còn gọi là SideWalk). DodgeBox được đánh giá là phiên bản cải tiến của StealthVector, tích hợp nhiều kỹ thuật như stack spoofing, DLL side-loading và DLL hollowing để né tránh bị phát hiện.

Nguồn: https://thehackernews.com/2024/07/chinese-apt41-upgrades-malware-arsenal.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT41 bổ sung mã độc DodgeBox và MoonWalk vào kho mã độc của mình trong các chiến dịch tấn công"

Nhóm APT41 đã sử dụng file thực thi "taskhost.exe" của Sandboxie để sideload DLL độc hại "sbiedll.dll", một DLL loader viết bằng C có nhiệm vụ giải mã và thực thi payload backdoor MoonWalk. Nhóm APT41 được xác định liên quan đến việc sử dụng mã độc DodgeBox dựa trên những điểm tương đồng giữa DodgeBox và StealthVector, cũng như việc sử dụng DLL side-loading – một kỹ thuật phổ biến được các nhóm tấn công Trung Quốc sử dụng để triển khai mã độc như PlugX.

DodgeBox là một loader mã độc mới, sử dụng nhiều kỹ thuật để tránh phát hiện cả tĩnh và động. Mã độc này có khả năng giải mã và tải các thư viện động (DLL) được nhúng vào, thực hiện các kiểm tra để xác định môi trường hoạt động và ràng buộc các điều kiện, đồng thời thực hiện các quy trình để dọn dẹp hệ thống sau khi thực thi. Điều này đặt ra thách thức lớn đối với các biện pháp bảo mật hiện tại. Các mẫu phân tích DodgeBox cũng đã được gửi tới VirusTotal từ Thái Lan và Đài Loan, hai khu vực mang tính chiến lược tại Trung Quốc

Một số IoC được ghi nhận:

0d068b6d0523f069d1ada59c12891c4a
b3067f382d70705d4c8f6977a7d7bee4
d72f202c1d684c9a19f075290a60920f
294cc02db5a122e3a1bc4f07997956da
393065ef9754e3f39b24b2d1051eab61
bcac2cbda36019776d7861f12d9b59c4
f062183da590aba5e911d2392bc29181
4141c4b827ff67c180096ff5f2cc1474
bc85062de0f70afd44bb072b0b71a8cc
72070b165d1f11bd4d009a81bf28a3e5
f0953ed4a679b987a2da955788737602

Nguồn: https://thehackernews.com/2024/07/chinese-apt41-upgrades-malware-arsenal.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Palo Alto Networks phát hành bản vá cho lỗi nghiêm trọng trên công cụ di rời Expedition"

Palo Alto Networks vừa phát hành các bản cập nhật bảo mật để khắc phục 05 lỗ hổng an toàn thông tin, trong đó có một lỗ hổng ở mức nghiêm trọng có thể dẫn đến việc bỏ qua xác thực (bypass).

Lỗ hổng Nghiêm trọng có mã CVE-2024-5910 (Điểm CVSS: 9.3), đây là lỗi bỏ qua xác thực tồn tại trên công cụ di rời Expedition của Palo Alto Networks, có thể dẫn đến việc chiếm quyền quản trị viên. Lỗ hổng này ảnh hưởng đến tất cả các phiên bản của Expedition trước phiên bản 1.2.92 và đã được vá trong phiên bản mới nhất.

Hiện chưa có bằng chứng về việc lỗ hổng này đã bị tấn công trong thực tế, tuy nhiên, người dùng nên cập nhật để bảo vệ hệ thống khỏi các nguy cơ bị tấn công. Trong trường hợp không thể cập nhật ngay, Palo Alto Networks khuyến nghị giới hạn quyền truy cập vào Expedition chỉ cho các người dùng, host và mạng được ủy quyền.

Ngoài ra, Palo Alto Networks cũng đã vá lỗi CVE-2024-3596 (hay BlastRADIUS) trong giao thức RADIUS. Lỗ hổng này cho phép kẻ tấn công thực hiện cuộc tấn công Adversary-in-the-middle (AitM) chen vào kết nối giữa tường lửa PAN-OS của Palo Alto Networks và máy chủ RADIUS để bỏ qua xác thực. Đối tượng tấn công có thể leo thang đặc quyền lên tới mức "superuser" khi máy chủ sử dụng xác thực RADIUS và giao thức CHAP hoặc PAP được kích hoạt.

Cụ thể, các phiên bản PAN-OS sau đây đã bị ảnh hưởng bởi lỗ hổng BlastRADIUS:

- PAN-OS 11.1 (phiên bản cũ hơn 11.1.3, đã được vá từ phiên bản 11.1.3)
- PAN-OS 11.0 (phiên bản cũ hơn 11.0.4-h4, đã được vá từ phiên bản 11.0.4-h4)
- PAN-OS 10.2 (phiên bản cũ hơn 10.2.10, đã được vá từ phiên bản 10.2.10)
- PAN-OS 10.1 (phiên bản cũ hơn 10.1.14, đã được vá từ phiên bản 10.1.14)
- PAN-OS 9.1 (phiên bản cũ hơn 9.1.19, đã được vá từ phiên bản 9.1.19)

Đối với Prisma Access, mọi phiên bản đều bị ảnh hưởng và dự kiến sẽ có bản vá được phát hành vào ngày 30/07. Ngoài ra, lưu ý rằng giao thức CHAP/PAP không nên được sử dụng trừ khi chúng được bảo vệ bởi một lớp tunnel mã hóa, vì hai giao thức này không hỗ trợ Transport Layer Security (TLS).

Nguồn: https://thehackernews.com/2024/07/palo-alto-networks-patches-critical.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 **432** lỗ hổng, trong đó có 133 lỗ hổng mức Cao, 149 lỗ hổng mức Trung bình, 19 lỗ hổng mức Thấp và 131 lỗ hổng chưa đánh giá. Trong đó có ít nhất 81 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 OpenSSH, GeoServer và Microsoft cụ thể là như sau:

- **CVE-2024-6387 (Điểm CVSS: 8.1 – Cao):** Lỗ hổng tồn tại trên máy chủ OpenSSH cho phép đối tượng tấn công khai thác lỗi Race Condition, cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-36401 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên GeoServer cho phép đối tượng tấn công thực thi mã từ xa thông qua việc truyền vào dữ liệu độc hại tới các phiên GeoServer cấu hình mặc định. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2023-24860 (Điểm CVSS: 7.5 – Cao):** Lỗ hổng tồn tại trên Microsoft Defender cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, làm sập dịch vụ bằng cách sử dụng file độc hại. Hiện lỗ hổng chưa 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-2024-6387	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: OpenSSH - 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-2024-6387
2	CVE-2023-24860	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Microsoft Defender. - 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-2023-24860
3	CVE-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: GeoServer - 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-2024-36401
4	CVE-2024-34102	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Adobe Commerce - 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-2024-34102
5	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11. - 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-2024-38112

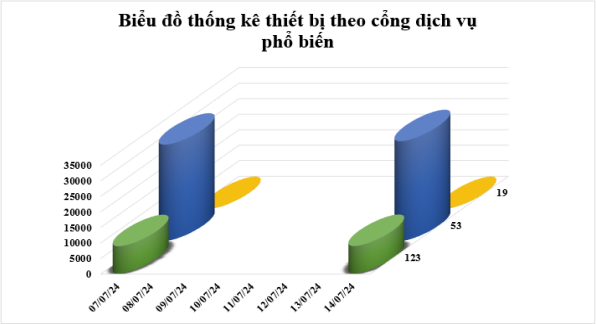
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-35264	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Visual Studio, .NET - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-35264
7	CVE-2024-38080	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 11, Windows Server 2022. - 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-2024-38080
8	CVE-2024-37081	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: VMware vCenter Server. - 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-2024-37081
9	CVE-2024-38021	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Outlook. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-38021
10	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ngôn ngữ lập trình PHP. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý, 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-2024-4577

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 **40.952** (tăng so với tuần trước **39.780**) 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.

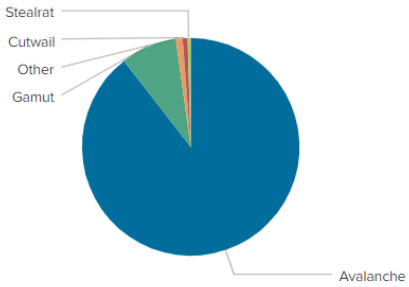


Tấn công Web

Trong tuần, có **64** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 53 trường hợp tấn công lừa đảo (Phishing), 11 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	restless.su
disorderstatus.ru	andall.servicesql.info
atomictrivia.ru	db2017417b23.zapto.org
amnsreiuojy.ru	www.hnmrw.net
restlesz.su	elitiorecfreetoo.cc
xjpakmdcfuqe.biz	www.uyxlemnutwvo.me.uk
hzmksreiuojy.ru	www.uvcbedlkdefg.me.uk
xjpakmdcfuqe.com	sql.onlyslq.lol
xjpakmdcfuqe.ru	ynefefyopqvu.com
xjpakmdcfuqe.in	xkbowvakacehqxkgt.org

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **1.942** 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 các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

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

STT	Website lừa đảo	Ghi chú
1	https://vssid[.]govnn[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://baohiemxahoi[.]vnagov[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
3	https://icchanoi[.]net/	Website giả mạo Công ty Cổ phần Đầu tư Quốc tế ICC Hà Nội
4	https://giiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://mfacebook-com[.]vn/	Website giả mạo Facebook
6	https://www[.]baovietcom[.]vip/	Website giả mạo Ngân hàng TMCP Bảo Việt
7	https://khtechcanhan[.]com/	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
8	https://tcvnhomefic[.]com	Website giả mạo Ngân hàng TMCP Quân đội
9	https://centralmarketing[.]online/	Website giả mạo Ngân hàng Worldbank Việt Nam
10	https://nze98582s[.]com/	Website giả mạo sàn TMĐT Shopee
11	https://vnc75635s[.]com	Website giả mạo sàn TMĐT Shopee
12	https://vnc69977s[.]com	Website giả mạo sàn TMĐT Shopee
13	https://www[.]shopeesop[.]com	Website giả mạo sàn TMĐT Shopee
14	https://www[.]tikifreeship[.]vip/	Website giả mạo sàn TMĐT Tiki
15	https://tdke00[.]com/	Website giả mạo sàn TMĐT Tiki
16	https://tdkt07[.]com	Website giả mạo sàn TMĐT Tiki
17	https://tikijaj2[.]com	Website giả mạo sàn TMĐT Tiki
18	https://tikt88[.]com	Website giả mạo sàn TMĐT Tiki
19	https://businesseventskp[.]top	Website giả mạo sàn TMĐT Tiki
20	https://xacnhanthutuchoantra[.]us/	Website giả mạo Western Union

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