NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 15 (08/04/2024 – 14/04/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT MuddyWater của Iran sử dụng công cụ C&C DarkBeatC2 trong chiến dịch tấn công mới nhất.

- **Cảnh báo:** Palo Alto Networks phát hành bản vá khẩn cấp cho lỗ hổng nghiêm trọng đang bị khai thác trên PAN-OS.

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: 59** 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: Nhóm APT MuddyWater của Iran sử dụng công cụ C&C DarkBeatC2 trong chiến dịch tấn công mới nhất.”

Một nhóm APT liên quan tới chính phủ Iran có tên MuddyWater, đã được biết đến với nhiều biệt danh khác nhau như Boggy Serpens, Mango Sandstorm và TA450. Nhóm MuddyWater đã bắt đầu hoạt động kể từ năm 2017 và thực hiện nhiều chiến dịch sử dụng hình thức tấn công spear-phishing để triển khai giải pháp Giám sát và Quản lý từ xa (Remote Monitoring and Management – RMM) hợp pháp lên các thiết bị mục tiêu.

Gần đây, nhóm MuddyWater đã sử dụng một hạ tầng C&C mới gọi là DarkBeatC2, đây là công cụ mới nhất trong danh sách các công cụ tấn công trước đó của nhóm này như SimpleHarm, MuddyC3, PhonyC2 và MuddyC2Go.

Nhóm MuddyWater khởi động chiến dịch tấn công mới nhất bằng việc gửi đi các email lừa đảo spear-phishing từ tài khoản bị chiếm dụng, trong đó có chứa đường dẫn hoặc file đính kèm độc hại được lưu trữ trên dịch vụ như Egnyte để triển khai phần mềm Atera Agent.

Một trong số các dấu hiệu của đường dẫn độc hại là "kinneretacil.egnyte[.]com", với subdomain "kinneretacil" thuộc "kinneret.ac.il", một viện giáo dục tại Israel từng bị tấn công trong một chiến dịch tấn công chuỗi cung ứng bởi nhóm Lord Nemesis. Lord Nemesis bị nghi ngờ là một chiến dịch giả mạo các nhà hoạt động chính trị nhằm vào Israel, có liên kết với Najee Technology, một nhóm con của Mint Sandstorm - một nhóm APT được cho là có liên quan đến Iran.

Mạng lưới quan hệ của MuddyWater cho thấy khả năng nhóm này sử dụng tài khoản email của Kinneret để phát tán các đường dẫn, qua đó tạo ra vỏ bọc đáng tin cậy để lừa người dùng bấm vào đường dẫn hoặc tập tin đính kèm.

Nguồn: https://thehackernews.com/2024/04/iranian-muddywater-hackers-adopt-new-c2.html

Tin tức An toàn thông tin

"Chiến dịch tấn công: Nhóm APT MuddyWater của Iran sử dụng công cụ C&C DarkBeatC2 trong chiến dịch tấn công mới nhất."

Đáng chú ý, chiến dịch tấn công dựa vào việc sử dụng các địa chỉ IP/domain được kết hợp với tên gọi của DarkBeatC2 để quản lý các thiết bị bị ảnh hưởng. Thông qua lệnh PowerShell, kẻ tấn công có thể thiết lập kết nối với máy chủ C&C sau khi xâm nhập vào thiết bị. Theo điều tra phân tích, nhóm này đã sử dụng chức năng AutodialDLL trong Windows Registry để side-load DLL độc hại và kết nối với máy chủ C&C. Để duy trì kết nối, nhóm tấn công đã lên lịch các tác vụ để thực thi mã PowerShell. Mã này được sử dụng để khai thác khóa registry AutodialDLL, từ đó tải và triển khai DLL độc hại cho framework C&C.

MuddyWater sử dụng một số kỹ thuật khác nhau để thiết lập kết nối với máy chủ C&C. Đầu tiên là việc sử dụng payload giai đoạn đầu được phát tán qua email lừa đảo. Tiếp theo là khai thác DLL side-loading để thực thi các thư viện độc hại. Khi tấn công thành công, các thiết bị bị ảnh hưởng sẽ nhận được một lệnh PowerShell, có chức năng tải thêm hai script PowerShell từ cùng một máy chủ.

Một trong hai script được tạo ra để đọc nội dung từ file "C:\ProgramData\SysInt.log" và gửi thông tin đó đến máy chủ C&C thông qua phương thức HTTP POST. Script còn lại được sử dụng để kiểm tra định kỳ các máy chủ C&C để tải về payload và ghi lại kết quả vào "SysInt.log". Tuy nhiên, bản chất của các payload này vẫn chưa được xác định rõ ràng.

Cần lưu ý rằng framework DarkBeatC2 vẫn sử dụng PowerShell như là phương tiện chính để lây nhiễm, tương tự như các framework C&C trước đó của MuddyWater.

Dưới đây là một số IoC được ghi nhận:

185.236.234[.]161	91.225.218[.]210
185.216.13[.]242	95.164.38[.]68
45.66.249[.]226	45.140.147[.]81
137.74.131[.]19	80.71.157[.]130
164.132.237[.]68	103.35.190[.]203
95.164.61[.]64	95.164.46[.]253
95.164.46[.]54	0

Nguồn: https://thehackernews.com/2024/04/iranian-muddywater-hackers-adopt-new-c2.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Palo Alto Networks phát hành bản vá khẩn cấp cho lỗ hổng nghiêm trọng đang bị khai thác trên PAN-OS."

Palo Alto Networks đã phát hành bản vá cho lỗ hổng nghiêm trọng ảnh hưởng tới PAN-OS hiện đang bị khai thác trên môi trường không gian mạng.

Lỗ hổng CVE-2024-3400 (Điểm CVSS: 10.0) là lỗ hổng an toàn thông tin nghiêm trọng tồn tại trên chức năng GlobalProtect cho phép đối tượng tấn công thực thi mã tùy ý từ xa với quyền root trên thiết bị tường lửa sử dụng PAN-OS.

Bản vá đã được phát hành cho các phiên bản:

PAN-OS 10.2.9-h1

PAN-OS 11.0.4-h1

PAN-OS 11.1.2-h3

Lỗ hổng này chỉ ảnh hưởng đến các thiết bị tường lửa sử dụng PAN-OS 10.2, 11.0 và 11.1, có cấu hình gateway GlobalProtect hoặc cổng GlobalProtect (hoặc cả hai), và với chức năng telemetry được kích hoạt

Thiết bị tường lửa Cloud NGFW không gặp vấn đề này. Chỉ các phiên bản cụ thể của PAN-OS và cấu hình chức năng đặc thù trên tường lửa máy ảo do người dùng triển khai và quản lý trên hệ thống Cloud mới bị ảnh hưởng.

Hiện chưa có thông tin rõ về đối tượng đứng sau việc khai thác lỗ hổng này, tuy nhiên, Unit 42 của Palo Alto Networks đang theo dõi các hoạt động của đối tượng này dưới tên gọi Operation MidnightEclipse.

Volexity, một cơ quan bảo mật khác, đã gán hoạt động của đối tượng vào cụm UTA0218 và thông báo rằng lỗ hổng CVE-2024-3400 đã bị khai thác kể từ ngày 26/03/2024 để phát tán mã độc backdoor Python có tên UPSTYLE tới tường lửa, qua đó cho phép đối tượng thực thi mã từ xa.

Hiện tại, mức độ ảnh hưởng của việc khai thác lỗ hổng vẫn chưa được xác định rõ. Tuy nhiên, đã có dấu hiệu cho thấy đối tượng tấn công đang thăm dò thông tin và mở rộng chiến dịch để nhằm vào các hệ thống khác

Trong báo cáo, UTA0218 đã thực hiện một số hoạt động sau: chạy một phần mềm độc hại để lấy điều khiển từ xa (reverse shells), thu thập thông tin cấu hình của hệ điều hành PAN-OS, xóa các file ghi log, và triển khai công cụ tunneling GOST (GO Simple Tunnel). Ngoài ra, chưa có ghi nhận nào về việc triển khai thêm mã độc hay thực hiện kỹ thuật duy trì kết nối trên hệ thống mạng của người dùng

Nguồn: https://thehackernews.com/2024/04/palo-alto-networks-releases-urgent.htm

Nguy cơ tấn công mạng từ điểm yếu, lỗ hổng

Trong tuần hệ thống kỹ thuật của NCSC 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, nổi bật có 03 lỗ hổng ảnh hưởng tới các sản phẩm của Microsoft, Adobe và Palo Alto Networks, cụ thể như sau:

- CVE-2024-21442 (**Điểm CVSS: 8.1 – Cao**): Lỗ hổng tồn tại trên Internet Shortcut Files cho phép đối tượng tấn công vượt qua biện pháp bảo mật, qua đó thực thi mã tùy ý trên thiết bị người dùng. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm APT như Evilnum, TA428, lockbit,...
- CVE-2024-2070 (**Điểm CVSS: 9.1 – Nghiêm trọng**): Lỗ hổng tồn tại trên Adobe Commerce phiên bản 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 và cũ hơn. Lỗ hổng cho phép đối tượng thực hiện OS Command Injection qua đó thực thi mã tùy ý trên thiết bị người dùng. Hiện lỗ hổng đang bị khai thác trong thực tế.
- CVE-2024-3400 (**Điểm CVSS: 9.1 – Nghiêm trọng**): Lỗ hổng Command Injection tồn tại trên Palo Alto Networks PAN-OS cho phép đối tượng thực thi mã tùy ý với quyền root trên tường lửa sử dụng PAN-OS. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi một số nhóm APT chưa được xác định.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-21412	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2022 - Mô tả: Lỗ hổng cho phép đối tượng vượt qua biện pháp bảo mật - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-21412
2	CVE-2024-20720	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Adobe Commerce - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã tùy ý từ xa. - Lỗ hổng đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-20720
3	CVE-2022-43842	- Điểm CVSS: 8.6 (Cao) - Ảnh hưởng: IBM Aspera Console - Mô tả: Lỗ hổng cho phép đối tượng thực thi SQL Injection - Lỗ hổng đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2022-43842
4	CVE-2024-3400	- Điểm CVSS: 10 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3400
5	CVE-2024-21378	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Outlook - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-21378

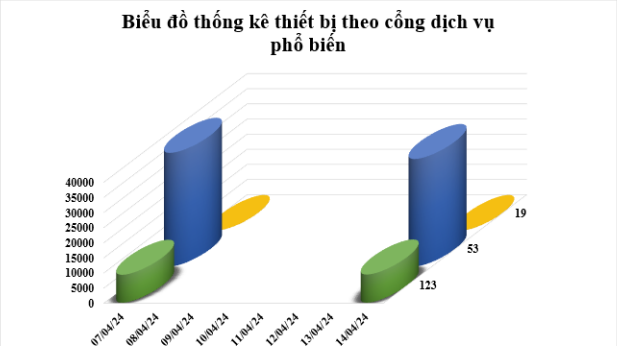
TOP 10 lỗ hổng đáng chú ý trong tuần

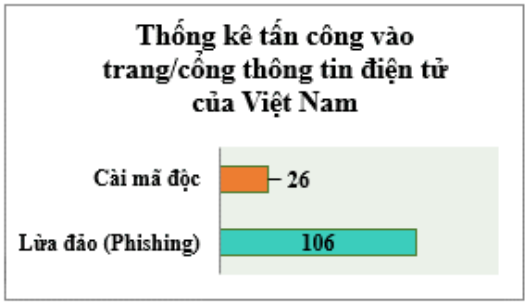
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-1086	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Linux - Mô tả: Lỗ hổng cho phép đối tượng leo thang đặc quyền. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-1086
7	CVE-2024-3273	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: D-Link - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3273
8	CVE-2021-31630	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Open PLC Webserver v3 - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2021-31630
9	CVE-2024-26198	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Exchange Server - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-26198
10	CVE-2024-29988	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: SmartScreen - Mô tả: Lỗ hổng cho phép đối tượng vượt qua biện pháp bảo mật. - Lỗ hổng đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-29988

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 **44.886** (giảm so với tuần trước **46.844**) 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.



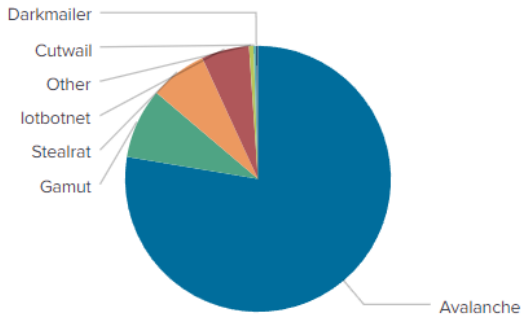


Tấn công Web

Trong tuần, có **132** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 106 trường hợp tấn công lừa đảo (Phishing), 26 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

184.105.192.2	differentia.ru
216.218.185.162	disorderstatus.ru
216.218.135.114	atomictrivia.ru
178.62.201.34	amnsreiuojy.ru
104.131.68.180	restlesz.su
64.71.166.50	hzmksreiuojy.ru
45.77.249.79	xjpakmdcfuqe.biz
184.105.76.250	xjpakmdcfuqe.in
64.71.188.178	xjpakmdcfuqe.ru
restless.su	xjpakmdcfuqe.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **59** 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://www[.]vnambzuon36sc[.]vip/	Website giả mạo sàn TMĐT Amazon
2	https://quaysomediamart2024[.]vip/	Website giả mạo Công ty Cổ phần MediaMart Việt Nam
3	https://mayxanhsupport[.]com/	Website giả mạo Điện máy xanh
4	https://nganhangsaison[.]org/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
5	https://mbfic-plus[.]com	Website giả mạo Ngân hàng TMCP Quân đội
6	https://khachhangvib-canhan[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
7	https://vibbca-nhan[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
8	https://khach-hang-ca-nhan-vip5[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
9	stcard-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	https://tpbank[.]chamsocthekhachang-truc-tuyen[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
11	https://vn68822s[.]com/	Website giả mạo sàn TMĐT Shopee
12	https://sp77888[.]com/	Website giả mạo sàn TMĐT Shopee
13	https://vn63251s[.]com	Website giả mạo sàn TMĐT Shopee
14	https://www[.]dailyssshopee[.]com	Website giả mạo sàn TMĐT Shopee
15	Http://tdkd03[.]com	Website giả mạo sàn TMĐT Tiki
16	https://www[.]tuyendungtiki2024[.]vn/	Website giả mạo sàn TMĐT Tiki
17	https://tdkd00[.]com/	Website giả mạo sàn TMĐT Tiki
18	https://fdsd11[.]com/	Website giả mạo sàn TMĐT Tiki
19	https://nhanvientiki[.]info/	Website giả mạo sàn TMĐT Tiki
20	https://skhf66[.]com/	Website giả mạo sàn TMĐT Tiki

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