NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 41 (07/10/2024 – 13/10/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công Triều Tiên dùng chiêu trò phỏng vấn giả để phát tán mã độc đa nền tảng nhằm vào các lập trình viên.

- **Cảnh báo:** Palo Alto Networks cảnh báo về lỗ hổng chiếm dụng tường lửa đã có mã khai thác trên không gian mạng.

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: 414** 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 tấn công Triều Tiên dùng chiêu trò phỏng vấn giả để phát tán mã độc đa nền tảng nhằm vào các lập trình viên"

Một nhóm tấn công Triều Tiên đã bị phát hiện lợi dụng các nhà phát triển phần mềm đang tìm việc để phát tán các phiên bản mới của mã độc BeaverTail và InvisibleFerret. Nhóm tin tặc này, được theo dõi dưới mã CL-STA-0240, hoạt động trong khuôn khổ chiến dịch Contagious Interview, lần đầu tiên được Palo Alto Networks Unit 42 công bố vào tháng 11 năm 2023.

Theo báo cáo, đối tượng tấn công giả danh nhà tuyển dụng, liên hệ với các lập trình viên qua các nền tảng tìm việc. Sau đó, chúng mời nạn nhân tham gia một cuộc phỏng vấn trực tuyến, trong quá trình đó, chúng dụ dỗ nạn nhân tải và cài đặt mã độc dưới dạng phần mềm cần thiết cho "bài kiểm tra lập trình."

Quá trình tấn công bắt đầu với mã độc BeaverTail, vừa đóng vai trò là công cụ tải mã độc, vừa có khả năng thu thập thông tin trên cả Windows và macOS.

Sau đó, mã độc này còn mở đường cho InvisibleFerret, một backdoor được viết bằng Python để xâm nhập sâu hơn vào hệ thống.

Mặc dù chiến dịch đã bị phát hiện và công khai nhưng nhóm này vẫn tiếp tục hoạt động và thậm chí còn thành công trong việc lừa các lập trình viên thực thi mã độc bằng cách ngụy trang dưới hình thức các bài kiểm tra lập trình.

Theo phân tích của một số chuyên gia bảo mật, các đối tượng tấn công đã sử dụng các ứng dụng hội nghị trực tuyến giả mạo như MiroTalk và FreeConference.com trên cả hai nền tảng Windows và macOS để phát tán mã độc BeaverTail và InvisibleFerret.

Điểm nổi bật trong chiến dịch tấn công lần này là mã độc được phát triển trên nền tảng Qt, giúp nó tương thích với cả Windows và macOS. Phiên bản BeaverTail sử dụng Qt có thể đánh cắp mật khẩu trình duyệt và thu thập dữ liệu từ ví tiền điện tử. Việc ứng dụng Qt không chỉ giúp mã độc qua mặt các hệ thống bảo mật mà còn cho phép đối tượng tấn công mở rộng phạm vi, nhắm đến nhiều nạn nhân hơn mà không cần thay đổi phương thức hoạt động.

Nguồn: https://thehackernews.com/2024/10/n-korean-hackers-use-fake-interviews-to.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm tấn công Triều Tiên dùng chiêu trò phỏng vấn giả để phát tán mã độc đa nền tảng nhằm vào các lập trình viên"

Mã độc BeaverTail không chỉ lấy cắp dữ liệu mà còn tải xuống và cài đặt backdoor InvisibleFerret, gồm hai phần chính:

- Payload chính cho phép đối tượng tấn công điều khiển từ xa, ghi lại hoạt động bàn phím (keylogging), thu thập dữ liệu và tải xuống các công cụ hỗ trợ như AnyDesk.
- Trình đánh cắp dữ liệu trình duyệt chuyên thu thập thông tin đăng nhập và dữ liệu thẻ tín dụng.

Các chuyên gia bảo mật nhận định rằng, các nhóm APT Triều Tiên thường tiến hành tấn công với mục tiêu tài chính. Chiến dịch lần này có thể cũng vì mục đích đó, bởi mã độc BeaverTail được thiết kế để đánh cắp dữ liệu từ 13 loại ví tiền điện tử khác nhau.

Một số IoC được ghi nhận:

95.164.17[.]24	185.235.241[.]208
000b4a77b1905cabdb59d2b576f6da1b2ef55a0258004e4a9e290e9f41fb6923	9abf6b93eafb797a3556bea1fe8a3b7311d2864d5a9a3687fce84bc1ec4a428c
0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132	d801ad1beeab3500c65434da51326d7648a3c54923d794b2411b7b6a2960f31e
36cac29ff3c503c2123514ea903836d5ad81067508a8e16f7947e3e675a08670	de6f9e9e2ce58a604fe22a9d42144191cfc90b4e0048dffcc69d696826ff7170
fd9e8fcc5bda88870b12b47cbb1cc8775ccff285f980c4a2b683463b26e36bf0	0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd
9e3a9dbf10793a27361b3cef4d2c87dbd3662646f4470e5242074df4cb96c6b4	d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6

Nguồn: https://thehackernews.com/2024/10/n-korean-hackers-use-fake-interviews-to.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Palo Alto Networks cảnh báo về lỗ hổng chiếm dụng tường lửa đã có mã khai thác trên không gian mạng"

Palo Alto Networks đã cảnh báo người dùng về các lỗ hổng an toàn thông tin đã có mã khai thác, cho phép các đối tượng tấn công chiếm dụng tường lửa PAN-OS. Những lỗ hổng này có thể bị khai thác để truy cập trái phép vào hệ thống, tiếp cận thông tin nhạy cảm như thông tin xác thực của người dùng, từ đó dẫn tới việc chiếm quyền tài khoản quản trị tường lửa.

Cụ thể, đối tượng tấn công có thể đọc nội dung trong cơ sở dữ liệu Expedition, truy cập các file tùy ý và ghi file tùy ý vào bộ nhớ tạm trên hệ thống Expedition. Điều này giúp đối tượng tấn công thu thập thông tin như tên người dùng, mật khẩu dưới dạng văn bản không mã hóa, cấu hình thiết bị và các khóa API của tường lửa PAN-OS.

Các lỗ hổng được ghi nhận bao gồm:

- CVE-2024-9463 (lỗ hổng Command Injection không cần xác thực)
- CVE-2024-9464 (lỗ hổng Command Injection khi đã được xác thực)
- CVE-2024-9465 (lỗ hổng SQL injection không cần xác thực)
- CVE-2024-9466 (lỗ hổng lưu trữ thông tin xác thực dạng văn bản không mã hóa trong logs)
- CVE-2024-9467 (lỗ hổng Reflected XSS không cần xác thực)

Ngoài ra, một chuyên gia bảo mật đã công bố mã khai thác proof-of-concept, nối chuỗi lỗ hổng CVE-2024-5910 (lỗi reset thông tin quản trị) với lỗ hổng CVE-2024-9464 (Command Injection), cho phép thực thi mã từ xa mà không cần xác thực trên máy chủ Expedition.

Palo Alto Networks cho biết chưa ghi nhận trường hợp nào lỗ hổng này bị khai thác trong thực tế và đã phát hành bản vá cho các phiên bản Expedition 1.2.96 trở lên. Tệp văn bản không mã hóa bị ảnh hưởng bởi lỗ hổng CVE-2024-9466 sẽ được xóa trong quá trình cập nhật.

Người dùng được khuyến nghị thay đổi thông tin xác thực và khóa API trên Expedition cũng như các sản phẩm tường lửa sau khi cập nhật bản vá. Nếu chưa thể cập nhật, cần hạn chế quyền truy cập vào hệ thống mạng có Expedition chỉ dành cho những người dùng có quyền truy cập.

Trước đó, vào tháng 4/2024, Palo Alto Networks đã phát hành bản vá cho lỗ hổng zero-day CVE-2024-3400, lỗ hổng này đã bị nhóm UTA0218 khai thác trên các thiết bị tường lửa PAN-OS.

Nguồn: https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-firewall-hijack-bugs-with-public-exploit/

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 **579** lỗ hổng, trong đó có 198 lỗ hổng mức Cao, 265 lỗ hổng mức Trung bình, 09 lỗ hổng mức Thấp và 107 lỗ hổng chưa đánh giá. Trong đó có ít nhất 117 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 ASUS, GitHub và LiteSpeed Technologies, cụ thể là như sau:

- **CVE-2024-3080 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên router ASUS cho phép đối tượng tấn công khả năng truy cập vào thiết bị dưới tài khoản người dùng bất kì, qua đó thực hiện các hành vi trái phép khác. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2021-4043 (Điểm CVSS: 5.5 – Trung bình):** Lỗ hổng tồn tại trên GitHub cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ sử dụng các gói tin yêu cầu độc hại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-28000 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tại tại trên LiteSpeed Technologies LiteSpeed Cache cho phép đối tượng tấn công 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-2024-3080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: ASUS - 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-2024-3080
2	CVE-2021-4043	- Điểm CVSS: 5.5 (Trung bình) - Ảnh hưởng: GitHub - 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-2021-4043
3	CVE-2024-28000	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache - 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-2024-28000
4	CVE-2024-43572	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022. - 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-2024-43572
5	CVE-2024-43573	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Server 2016, 2019, 2022. - 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-2024-43573

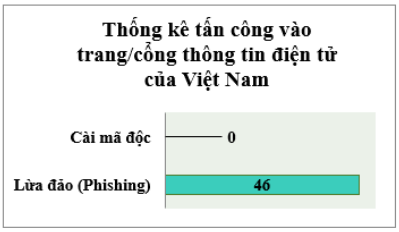
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-43582	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft - 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-2024-43582
7	CVE-2024-9680	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Firefox - 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-2024-9680
8	CVE-2024-43047	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Qualcomm - 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-2024-43047
9	CVE-2024-45519	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Zimbra Collaboration (ZCS) - 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-2024-45519
10	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

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 **36.023** (giảm so với tuần trước **36.892**) 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.

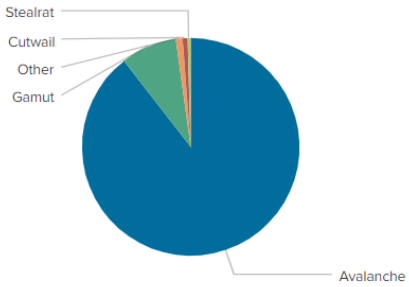


Tấn công Web

Trong tuần, có **46** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 46 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	restless.su
disorderstatus.ru	yk37wagdg.life
amnsreiuojy.ru	api.garageserviceoperation.com
atomictrivia.ru	spaines.pw
hzmksreiuojy.ru	griefcube.cc
xjpakmdcfuqe.biz	butterflyjobs.com
restlesz.su	aurasport.net
xjpakmdcfuqe.in	wrapn.net
xjpakmdcfuqe.ru	rikip.com
xjpakmdcfuqe.com	focusdate.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **414** 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://amazoul[.]xyz	Website giả mạo Amazon
2	soyte[.]cc	Website giả mạo Dịch vụ công quốc gia
3	dichvudienmay-xanh[.]online	Website giả mạo Điện máy xanh
4	https://fasebook[.]com[.]vn	Website giả mạo Facebook
5	giaohangtietkiemvn[.]website	Website giả mạo Giao hàng tiết kiệm
6	thuongmai-dientu[.]com	Website giả mạo sàn TMĐT Lazada
7	acb[.]chamsockhachhang-the-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
8	https://acb[.]chamsockhachhang-uudai-tructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
9	https://acb[.]uudauthekhachhanh-tructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
10	https://acb[.]chamsocthe-uudaikhachhang[.]online	Website giả mạo Ngân hàng TMCP Á Châu
11	acb[.]uudaikhachhang-chamsocthetructuyen[.]com	Website giả mạo Ngân hàng TMCP Á Châu
12	www[.]acb[.]uudaikhachhang-tructuyen-the[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
13	www[.]acb[.]chamsocthe-uudaikhachhang-tructuyen[.]com	Website giả mạo Ngân hàng TMCP Á Châu
14	acb[.]chamsocthe-uudaitructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
15	vpbank[.]uudaikhachhang-chamsocthetructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
16	shinhan[.]chamsocthe-uudaikhachhang[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
17	tiki886[.]vip	Website giả mạo sàn TMĐT Sendo
18	https://www[.]sp7588p[.]com	Website giả mạo sàn TMĐT Shopee
19	https://jetkingncsc[.]online	Website giả mạo Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)
20	vneid[.]vieegovn[.]cc	Website giả mạo VNeID

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