NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 24 (12/6/2023 – 18/6/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Diicot mở rộng chiến dịch bằng tấn công bằng cách sử dụng Cayosin Botnet để chuyển từ Cryptojacking sang tấn công DDoS.

- **Cảnh báo:** Phát hiện lỗ hổng thứ ba trong ứng dụng MOVEit Transfer trong các cuộc tấn công hàng loạt của ransomware Cl0p.

2. Điểm yếu, lỗ hổng

- **687** lỗ hổng được công bố và cập nhật.

- **07** lỗ hổng, nhóm lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Tấn công lừa đảo người dùng Việt Nam: 336** 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://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Diicot mở rộng chiến dịch bằng tấn công bằng cách sử dụng Cayosin Botnet để chuyển từ Cryptojacking sang tấn công DDoS."

Các nhà nghiên cứu bảo mật đã phát hiện một số payload chưa từng được ghi nhận trước đây liên quan đến một đối tượng tấn công tên là Diicot, có nguồn gốc từ Romania, điều này đã dự báo khả năng thực hiện cuộc tấn công từ chối dịch vụ (DDoS).

Diicot (hay còn được biết đến với tên là Mexals) lần đầu được phát hiện vào tháng 7 năm 2021, với khả năng sử dụng công cụ Brute Force SSH dựa trên Go với tên gọi Diicot Brute, nhằm mục đích xâm nhập vào các máy Linux trong một chiến dịch Cryptojacking (một biện pháp tấn công đào tiền ảo trái phép trên máy nạn nhân).

Vào tháng 4 năm nay, các nhà nghiên cứu đã công bố sự trở lại của chiến dịch này và được cho là bắt đầu từ tháng 10 năm 2022, mang lại cho đối tượng tấn công khoản lợi nhuận trái phép trị giá 10.000 USD. Đối tượng tấn công đã sử dụng một chuỗi payload trước khi cài đặt vào công cụ đào tiền ảo Monero. Các khả năng mới bao gồm: việc sử dụng module worm SSH, tăng cường cơ chế báo động, che giấu payload hiệu quả hơn và một module phân tán trong mạng LAN mới.

Nguồn: https://thehackernews.com/2023/06/from-cryptojacking-to-ddos-attacks.html

Phân tích mới nhất cho thấy nhóm tấn công đang triển khai một botnet có sẵn có tên là Cayosin, một nhóm mã độc có các đặc điểm chung với Qbot và Mirai.

Việc phát triển botnet là một biểu hiện cho thấy đối tượng tấn công đã có khả năng thực hiện các cuộc tấn công DDoS. Ngoài ra, đối tượng cũng thực hiện các hành vi khác như Doxxing các nhóm tấn công đối thủ và sự phụ thuộc của những nhóm đó vào Discord để ra lệnh và kiểm soát, đồng thời thực hiện việc đánh cắp dữ liệu.

Đối tượng tấn công đang tận dụng tiện ích Brute Force SSH để tạo điều kiện cho việc cài đặt thêm các mã độc như biến thể của Mirai hoặc công cụ đào tiền ảo. Một số công cụ khác được sử dụng bởi Diicot bao gồm:

- Chrome: Một bộ quét Internet dựa trên Zmap có khả năng ghi lại kết quả của quá trình quét vào file bios.txt.
- Update: Một file thực thi có nhiệm vụ tải và chạy các công cụ như SSH Brute Force và Chrome, nếu chúng chưa tồn tại trong hệ thống của nạn nhân.
- History: Một script shell có nhiệm vụ chạy Update.

Công cụ Brute Force SSH phân tích tệp văn bản được tạo bởi Chrome để xâm nhập vào các địa chỉ IP đã xác định. Nếu thành công, nó sẽ thiết lập kết nối từ xa tới địa chỉ IP đó. Sau đó, một chuỗi lệnh sẽ được thực thi để tạo ra một hồ sơ cho máy bị nhiễm mã độc, sử dụng máy đó để đào tiền ảo hoặc biến nó thành một điểm phân phát mã độc nếu CPU của máy bị nhiễm có ít hơn bốn lõi.

Để ngăn chặn cuộc tấn công này, các cơ quan và tổ chức nên triển khai các quy tắc tường lửa và củng cố hệ thống SSH để hạn chế quyền truy cập SSH và các địa chỉ IP cụ thể.

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng thứ ba trong ứng dụng MOVEit Transfer trong các cuộc tấn công hàng loạt của ransomware Cl0p"

Các nhóm tấn công gần đây đã triển khai chiến dịch tấn công sử dụng ransomware Cl0p để nhằm mục tiêu tấn công vào các công ty sử dụng ứng dụng MOVEit Transfer.

Lỗ hổng bảo mật mới được phát hiện là CVE-2023-35708 (Điểm CVSS: 9.8) với mức độ ảnh hưởng Nghiêm trọng, cho phép đối tượng tấn công nâng cao đặc quyền và truy cập trái phép vào hệ thống, gây ra lỗi SQL injection.

Các công ty đang khuyến nghị khách hàng của mình vô hiệu hóa tất cả truy cập HTTP và HTTPs đối với MOVEit Transfer trên port 80 và port 443, nhằm bảo vệ hệ thống của họ trong khi bản vá đang được cập nhật.

Ngoài ra, lỗ hổng CVE-2023-34362 (Điểm CVSS: 9.8) với mức độ ảnh hưởng Nghiêm trọng cũng đang được ransomware Cl0p khai thác trong các cuộc tấn công nhằm đánh cắp dữ liệu trái phép.

Cl0p đã liệt kê 27 công ty đã bị tấn công bằng cách sử dụng lỗ hổng trong MOVEit Transfer dưới mạng darknet. Các tổ chức có khả năng bị ảnh hưởng lớn hơn nhiều so với con số ban đầu được đề ra trong chiến dịch Fortra Go Anywhere MFT của Cl0p, bao gồm nhiều cơ quan liên bang của Hoa Kỳ như Bộ Năng lượng.

Theo các nhà nghiên cứu, gần 31% trong hơn 1.400 máy chủ sử dụng MOVEit thuộc ngành dịch vụ tài chính, 16% thuộc lĩnh vực chăm sóc sức khỏe, 9% thuộc lĩnh vực công nghệ thông tin và 8% thuộc các lĩnh vực chính phủ và quân sự. Trong số này, có đến 80% máy chủ có trụ sở tại Hoa Kỳ.

Progress phát hành các bản vá khắc phục lỗ hổng trong MOVEit Transfer

Progress Software đã phát hành các bản vá khắc phục lỗ hổng trong MOVEit Transfer, bao gồm các phiên bản 2020.1.10 (12.1.10), 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7) và 2023.0.3 (15.0.3).

Lỗ hổng SQL injection trong ứng dụng MOVEit Transfer cho phép đối tượng tấn công không được xác thực có quyền truy cập trái phép vào cơ sở dữ liệu MOVEit Transfer, đồng thời gửi một payload tự tạo đến điểm cuối (endpoint) của ứng dụng MOVEit Transfer từ đó cho phép đối tượng tấn công chỉnh sửa và tiết lộ nội dung cơ sở dữ liệu của MOVEit.

Để ngăn chặn các cuộc tấn công, người dùng được khuyến cáo cần cập nhật ngay bản vá mới phát hành ngày 09/06/2023.

Nguồn: https://thehackernews.com/2023/06/third-flaw-uncovered-in-moveit-transfer.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 **687** lỗ hổng, trong đó có 130 lỗ hổng mức Cao, 157 lỗ hổng mức Trung bình, 08 lỗ hổng mức Thấp và 392 lỗ hổng chưa đánh giá. Trong đó có ít nhất 78 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam: Nhóm 78 lỗ hổng trong Microsoft, Nhóm 05 lỗ hổng trong Linux, Nhóm 20 lỗ hổng trong Fortinet, Nhóm 40 lỗ hổng trong Wordpress, Nhóm 32 lỗ hổng trong Google, Nhóm 03 lỗ hổng trong Zimbra, Nhóm 08 lỗ hổng trong IBM. Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- *Microsoft: CVE-2023-33131, CVE-2023-32031,...*
- *Linux: CVE-2023-3159, CVE-2023-3161,…*
- Fortinet*: CVE-2022-42478, CVE-2022-43953,...*
- *Wordpress: CVE-2023-2556, CVE-2023-2781,...*
- *Google: CVE-2021-0701, CVE-2021-0945,...*
- *Zimbra: CVE-2023-24030, CVE-2023-24031,...*
- *IBM: CVE-2022-22307, CVE-2022-32752,...*

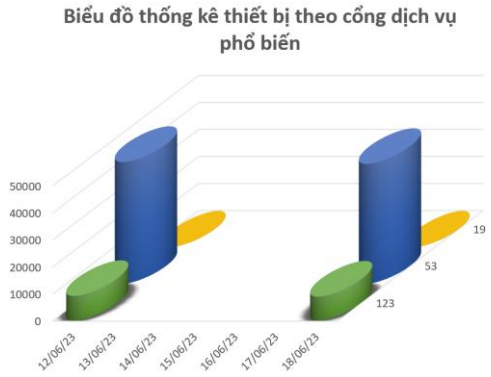
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-32009 CVE-2023-32031 CVE-2023-33131 …	Nhóm 78 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, thực hiện leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-3159 CVE-2023-3161 CVE-2023-3268 …	Nhóm 05 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công làm rò rỉ thông tin dữ liệu, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Fortinet	CVE-2022-42478 CVE-2022-43953 CVE-2023-22639 …	Nhóm 20 lỗ hổng trong Fortinet cho phép đối tượng tấn công không cần xác thực truy cập vào các tệp và thư mục, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-2556 CVE-2023-2557 CVE-2023-2764 …	Nhóm 40 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, SQL injection, tiết lộ thông tin nhạy cảm, tải lên các tệp tùy ý, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Google	CVE-2021-0701 CVE-2021-0945 CVE-2023-21121 …	Nhóm 32 lỗ hổng trong Google (Android,..) cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Zimbra	CVE-2023-24030 CVE-2023-24031 CVE-2023-24032	Nhóm 03 lỗ hổng trong Zimbra cho phép đối tượng tấn công thi mã JavaScript tùy ý dẫn đến lộ lọt thông tin dữ liệu, thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-22307 CVE-2022-32752 CVE-2022-32757 …	Nhóm 08 lỗ hổng trong IBM phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

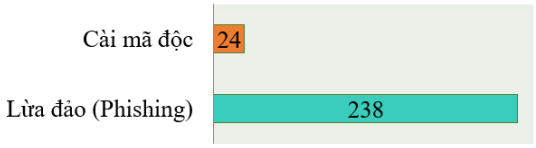
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **53.243,** (giảm so với tuần trước **54.215**) 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.

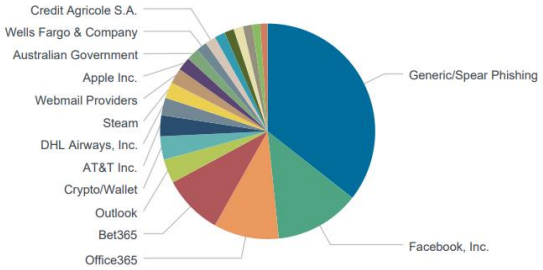


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 262 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 238 trường hợp tấn công lừa đảo (Phishing), 24 trường hợp tấn công cài cắm mã độc.



Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,v.v…Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và tính phí) như các mạng xã hội, Payment, Apple, Paypal,v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để đánh cắp tài khoản.

Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru: 15173 IP	xjpakmdcfuqe.ru:283 IP
disorderstatus.ru: 7138 IP	xjpakmdcfuqe.in:250 IP
atomictrivia.ru: 3511 IP	restlesz.su: 383 IP
xjpakmdcfuqe.biz: 505 IP	amnsreiuojy.ru: 823 IP
xjpakmdcfuqe.com: 333 IP	hzmksreiuojy.ru: 81 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **336** 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 website của ngân hàng, các trang thương mại điện tử…

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

STT	Website lừa đảo	Ghi chú
1	dienmayxanh24h.net	Website giả mạo Điện máy xanh
2	chanlemomo.vin	Website giả mạo ví điện tử Momo
3	amg187208.com	Website giả mạo sàn TMĐT Lazada
4	eeeesss.xyz net.lsipes.com …	Website lừa đảo

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 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, những đơn vị đã có tài khoản trên "Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động" tại địa chỉ https://service.khonggianmang.vn, quản trị viên có thể thêm các sản phẩm đang sử dụng để giám sát và nhận cảnh báo ngay khi có lỗ hổng mới phát sinh.

***

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**, Quý đơn vị cần chú ý quan tâm không truy cập vào các trang web được nêu để tránh nguy cơ bị tấn công lừa đảo, nâng cao nhận thức bản thân và tuyên truyền cho bạn bè, người thân và những người xung quanh tránh việc trở thành nạn nhân của những cuộc tấn công lừa đảo này.

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