NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 01 (02/01/2023 – 08/01/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Chiến thuật tấn công vượt qua CAPTCHA trên GitHub.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Turla triển khai backdoor mới thông qua cơ sở hạ tầng cũ trước đây.

2. Điểm yếu, lỗ hổng

- **516** 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: 210** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Nhóm tấn công APT Turla triển khai backdoor mới thông qua cơ sở hạ tầng cũ trước đây"

Kể từ khi bắt đầu cuộc xâm lược quân sự của Nga và Ukraine vào tháng 2 năm 2022, các chuyên gia đã phát hiện và liên kết một chuỗi các hoạt động do thám và lừa đảo thông tin xác thực nhằm mục tiêu vào Ukraine là do nhóm Turla đứng sau.

Vào tháng 7 năm 2022, Google cũng công bố rằng Turla đã tạo một ứng dụng Android độc hại để đối tượng tấn công thực hiện các cuộc tấn công từ chối dịch vụ nhằm vào các trang web của Nga.

Gần đây, nhóm APT Turla bị phát hiện đang sử dụng cơ sở hạ tầng tấn công có phần mềm độc hại đã được sử dụng hàng chục năm nhằm mục đích cung cấp các công cụ do thám và backdoor mới. Turla đã lén lút sử dụng các phần mềm độc hại cũ hơn làm cơ chế phân phối phần mềm độc hại, bao gồm cả việc lợi dụng ANDROMEDA lây lan qua các khóa USB bị nhiễm. Phần mềm này là một công cụ để giành quyền truy cập ban đầu vào mục tiêu.

Theo các chuyên gia bảo mật, một thanh USB bị nhiễm virus đã được cắm vào một tổ chức Ukraine vào tháng 12 năm 2021, dẫn đến việc triển khai một phần mềm ANDROMEDA kế thừa trên máy chủ khi khởi chay một liên kết độc hại (.LNK) giả mạo tệp dưới dạng một thư mục trong ổ USB. Sau đó, đối tượng tấn công sử dụng lại một trong những tên miền không hoạt động thuộc cơ sở hạ tầng C&C không còn tồn tại của ANDROMEDA (được đăng kí vào tháng 1 năm 2022) để lập hồ sơ nạn nhân bằng cách sử dụng KOPILUWAK dropper.

Kỹ thuật mới mà Turla sử dụng đã xác nhận rằng quyền sở hữu các miền đã hết hạn được sử dụng phần mềm độc hại được phân phối rộng rãi, có động cơ tài chính và có thể cho phép thực hiện các hoạt động tấn công khác với các mục tiêu khác nhau. Hơn nữa việc sử dụng phần mềm độc hại và cơ sở hạ tầng cũ sẽ giúp đối tượng tấn công tránh bị phát hiện và tăng khả năng tấn công thành công vì thường các chuyên gia và các nhà quản trị viên sẽ bỏ qua và không có biện pháp phòng tránh các phần mềm độc hại cũ.

Nguồn: https://thehackernews.com/2023/01/russian-turla-hackers-hijack-decade-old.html

Tin tức An toàn thông tin

"Cảnh báo: Chiến thuật tấn công vượt qua CAPTCHA trên GitHub"

Nhóm tấn công có tên là Automated Libra đã được quan sát thấy đang sử dụng kỹ thuật tấn công vượt qua xác thực CAPTCHA để tạo tài khoản GitHub độc hại như một phần của chiến dịch freejacking có tên là PURPLEURCHIN. PURPLEURCHIN được phát hiện vào tháng 10 năm 2022, đã tạo tới 30 tài khoản GitHub, 2000 tài khoản Heroku và 900 tài khoản Buddy để mở rộng quy mô hoạt động của mình. Nhóm chủ yếu nhằm mục tiêu vào các nền tảng đám mây cung cấp các bản dùng thử trong thời gian giới hạn để thực hiện các hoạt động khai thác tiền điện tử.

Theo Unit 42, nhóm này đã tạo từ ba đến năm tài khoản GitHub mỗi phút vào thời điểm hoạt động cao nhất vào tháng 11 năm 2022, thiết lập hơn 130.000 tài khoản trên Heroku, Togglebox và GitHub. Ước tính có hơn 22.000 tài khoản GitHub được tạo từ tháng 9 đến tháng 11 năm 2022: ba tài khoản vào tháng 9, 1.652 tài khoản vào tháng 10 và 20.725 tài khoản vào tháng 11.

Mục đích chính của PURPLEURCHIN là khai thác các tài nguyên máy tính được phân bổ cho các tài khoản miễn phí và có phí trên các dịch vụ đám mây để thu lợi nhuận trên quy mô lớn trước khi mất quyền truy cập do không thanh toán phí.

Bên cạnh việc tự động hóa quy trình tạo tài khoản bằng cách tận dụng các công cụ hợp pháp như xdotool và ImageMagick, đối tượng tấn công cũng bị phát hiện khai thác điểm yếu trong CAPTCHA trên GitHub thông qua việc sử dụng lệnh chuyển đổi (convert command) của ImageMagick để chuyển đổi hình ảnh CAPTCHA thành phần bổ sung RGB của chúng, sau đó sử dụng lệnh nhận dạng (identify command) để trích xuất độ lệch của red channel và chọn giá trị nhỏ nhất. Tạo tài khoản thành công, Automated Libra sẽ tiến hành tạo kho lưu trữ GitHub và triển khai các quy trình để có thể khởi chạy tập lệnh Bash và containers để bắt đầu chức năng khai thác tiền điện tử.

Nguồn: https://thehackernews.com/2023/01/hackers-using-captcha-bypass-tactics-in.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 516 lỗ hổng, trong đó có 62 lỗ hổng mức Cao, 20 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 434 lỗ hổng chưa đánh giá. Trong đó có ít nhất 49 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 05 lỗ hổng trong Apache, Nhóm 04 lỗ hổng trong Lenovo, Nhóm 31 lỗ hổng trong Wordpress, Nhóm 03 lỗ hổng trong Nokia, Nhóm 06 lỗ hổng trong Fortinet, Nhóm 11 lỗ hổng trong Google, Nhóm 11 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:

- Apache: CVE-2022-45143, CVE-2022-45787,...

- Lenovo: CVE-2022-4432, CVE-2022-4433,...

- Wordpress: CVE-2022-3241, CVE-2022-4140,...

- Nokia: CVE-2022-2482, CVE-2022-2483,...

- Fortinet: CVE-2022-41336, CVE-2022-42471,...

- Google: CVE-2022-2742, CVE-2022-2743...

- IBM: CVE-2022-42435, CVE-2022-22337,...

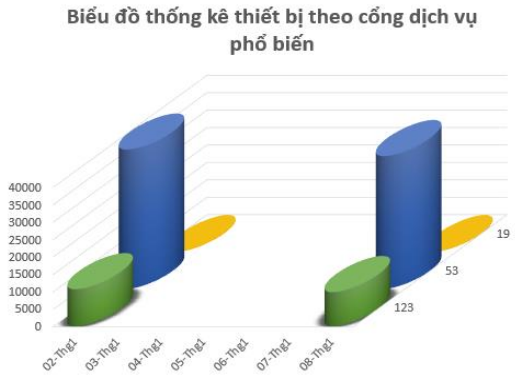
Thông tin điểm yếu, lỗ hổng

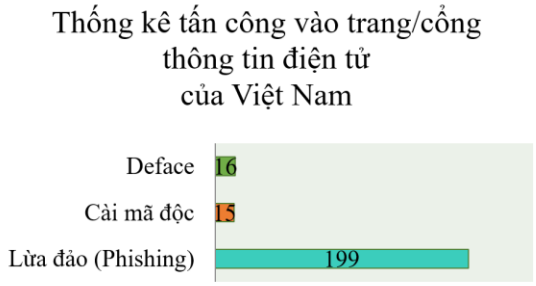
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apache	CVE-2022-45143 CVE-2022-45787 CVE-2021-32824 …	Nhóm 05 lỗ hổng trong Apache (Dubbo, DolphinScheduler,…) cho phép đối tượng tấn công thực thi mã từ xa, truy cập vào dữ liệu nội bộ để thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Lenovo	CVE-2022-4432 CVE-2022-4433 CVE-2022-4434 …	Nhóm 04 lỗ hổng trong Lenovo (ThinkPadX13s BIOS) cho phép đối tượng tấn công với quyền của người dùng cục bộ làm rò rỉ thông tin dữ liệu.	Chưa có thông tin xác nhận và bản vá
3	Wordpress	CVE-2022-3241 CVE-2022-4140 CVE-2022-4142 …	Nhóm 51 lỗ hổng trong Wordpress cho phép đối tượng tấn công với quyền của người dùng cục bộ cài các mã HTML hoặc Javascript độc hại,đọc các tệp tùy ý, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Nokia	CVE-2022-2482 CVE-2022-2483 CVE-2022-2484	Nhóm 03 lỗ hổng trong Nokia (ASIK AirScale) cho phép đối tượng tấn công thực hiện tấn công các chương trình cơ sở, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Fortinet	CVE-2022-41336 CVE-2022-42471 CVE-2022-42475 …	Nhóm 06 lỗ hổng trong Fortinet (FortiManager, FortiOS,…) cho phép đối tượng tấn công thực thi mã hoặc lệnh tùy ý.	Đã có thông tin xác nhận và bản vá
6	Google	CVE-2022-2742 CVE-2022-2743 CVE-2022-3863 …	Nhóm 10 lỗ hổng trong Google (Chrome) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-42435 CVE-2022-22337 CVE-2022-22338 ...	Nhóm 11 lỗ hổng trong IBM (Sterling B2B Integrator, Business Automation Workflow,…) cho phép đối tượng tấn công thu thập thông tin dữ liệu trái phép, cài mã JavaScript tùy ý, truy cập/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

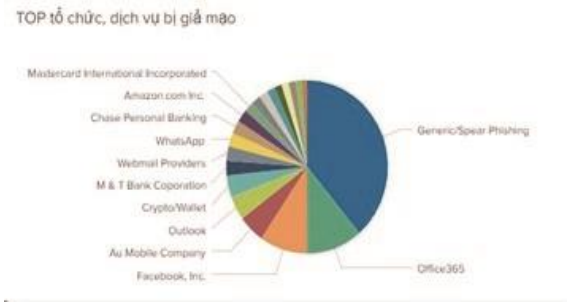
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **45,612** (giảm so với tuần trước **48,843**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 230 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 16 trường hợp tấn công thay đổi giao diện (Deface), 199 trường hợp tấn công lừa đảo (Phishing), 15 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: 27770 IP	xjpakmdcfuqe.ru:644 IP
disorderstatus.ru: 11598 IP	xjpakmdcfuqe.in: 550 IP
atomictrivia.ru: 5704 IP	restlesz.su: 333 IP
xjpakmdcfuqe.biz: 1803 IP	amnsreiuojy.ru: 1301 IP
xjpakmdcfuqe.com: 984 IP	hzmksreiuojy.ru: 104 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 210 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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	momohanoi.me	Giả mạo ví điện tử MoMo

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
ais@mic.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội