NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 18 (01/5/2023 – 07/5/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT ScarCruft triển khai backdoor RokRAT thông qua tệp LNK mở rộng.

- **Cảnh báo:** Phát hiện lỗ hổng mới trong plugin WordPress khiến hơn 2 triệu Website có nguy cơ bị tấn công.

2. Điểm yếu, lỗ hổng

- **413** 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: 330** 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

"Nhóm APT ScarCruft triển khai backdoor RokRAT thông qua tệp LNK mở rộng"

Gần đây, nhóm tấn công APT ScarCruft hay còn được biết đến với tên gọi là APT37 của Triều Tiên đã sử dụng các tệp LNK mở rộng làm phương thức phát tán mã độc RokRAT kể từ tháng 7 năm 2022.

Trong các cuộc tấn công gần đây, RokRAT nhằm mục tiêu chính vào các cá nhân có liên hệ với Triều Tiên, bao gồm các học giả, tiểu thuyết gia, doanh nhân được cho là đang hỗ trợ tài chính cho Triều Tiên. Nhóm này đã sử dụng kỹ thuật tấn công thông qua tệp LNK kích hoạt chuỗi lây nhiễm bằng một cú nhấp chuột đơn giản, trong đó các tệp sử dụng lệnh PowerShell để triển khai RokRAT. Ngoài ra, trong cuộc tấn công được ghi nhận vào tháng 01/2021, nhóm APT ScarCruft đã sử dụng macro trong Word để phát tán mã độc.

Mã độc RokRAT được thiết kế nhằm thực hiện nhiều hành động trái phép như thu thập thông tin chi tiết hệ thống, lọc dữ liệu, chụp ảnh màn hình, đánh cắp thông tin đăng nhập, thực thi lệnh và shellcode đồng thời quản lý tệp/thư mục. Những thông tin trái phép được lưu dưới dạng MP3 sau đó được tải lên các dịch vụ đám mây như Dropbox, OneDrive, pCloud và Yandex Cloud để che giấu thông tin liên quan đến C&C. Mã độc có khả năng nhằm mục tiêu vào macOS (CloudMensis) và Android (RambleOn).

ScarCruft được biết đến như một mối đe dọa đối với nhiều chiến dịch tấn công, đồng thời liên tục được nâng cấp các kỹ thuật tấn công nhằm phát tán mềm độc hại. Để giảm thiểu nguy cơ bị tấn công mạng, các cá nhân, doanh nghiệp nên kiểm tra trước khi truy cập vào bất kỳ đường link nào, thường xuyên sử dụng công cụ quét virus để sớm phát hiện và loại bỏ các phần mềm độc hại trên thiết bị của mình.

Nguồn: https://cyware.com/news/scarcruft-deploys-rokrat-via-lnk-file-04ea8e82

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng mới trong plugin WordPress khiến hơn 2 triệu Website có nguy cơ bị tấn công"

Người dùng plugin Advanced Custom Fields ACF dành cho WordPress được khuyến nghị cập nhật lên phiên bản 6.1.6 sau khi lỗ hổng bảo mật mới trong plugin này được phát hiện.

Lỗ hổng CVE-2023-30777 liên quan đến lỗi Reflected XSS, cho phép đối tượng tấn công thực thi lệnh tùy ý nhằm vào các trang web mục tiêu. Lỗ hổng này được phát hiện vào ngày 02/5/2023 và tại thời điểm đó đã có hơn hai triệu lượt cài đặt, đối với cả phiên bản miễn phí và trả phí.

Lỗ hổng này cho phép các đối tượng tấn công không cần xác thực đánh cắp thông tin nhạy cảm và thực hiện tấn công nâng cao đặc quyền trên trang web WordPress bằng cách lừa người dùng quản trị truy cập vào liên kết URL độc hại. Các cuộc tấn công Reflected XSS xảy ra khi người dùng truy cập vào một liên kết độc hại được gửi qua email. Sau khi truy cập trang web/ liên kết độc hại này, mã độc sẽ được cài cắm và thực thi trên trình duyệt web của người dùng. Reflected XSS thường bắt nguồn từ việc thiếu kiểm tra, sàng lọc dữ liệu do người dùng gửi lên, cho phép đối tượng tấn công sử dụng các chức năng của ứng dụng web và kích hoạt các đoạn mã độc hại.

Lỗ hổng CVE-2023-30777 có thể được kích hoạt trong cài đặt mặc định hoặc cấu hình Advanced Custom Fields.

Ngoài ra, các nhà nghiên cứu bảo mật cho biết còn một lỗ hổng XSS khác trong phần mềm cPanel là CVE-2023-29489 có mức ảnh hưởng Trung bình (điểm CVSS: 6.1). Lỗ hổng này cho phép đối tượng tấn công thực thi mã JavaScript tùy ý mà không cần xác thực. Không chỉ các cổng quản lý của cPanel bị tấn công thông qua lỗ hổng này mà cả những trang web hoạt động trên cổng 80 và cổng 443 cũng có nguy cơ bị tấn công.

Để giảm thiểu nguy cơ bị tấn công mạng các cơ quan, tổ chức nên cập nhật bản vá cho các thiết bị bị ảnh hưởng. Đồng thời kiểm tra kỹ các trang web trước khi thực hiện truy cập.

Nguồn: https://thehackernews.com/2023/05/new-vulnerability-in-popular-wordpress.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 **413** lỗ hổng, trong đó có 46 lỗ hổng mức Cao, 72 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 294 lỗ hổng chưa đánh giá. Trong đó có ít nhất 44 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 02 lỗ hổng trong Microsoft, Nhóm 05 lỗ hổng trong Linux, Nhóm 10 lỗ hổng trong Google, Nhóm 49 lỗ hổng trong Wordpress, Nhóm 12 lỗ hổng trong Gitlab, Nhóm 05 lỗ hổng trong Samsung, Nhóm 18 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-2023-29350, CVE-2023-29354.*
- *Linux: CVE-2023-2235, CVE-2023-2236,…*
- *Google: CVE-2023-2459, CVE-2023-2460,...*
- *Wordpress:CVE-2013-10026,CVE-2014-125100,...*
- *Gitlab: CVE-2023-0155, CVE-2023-0485,...*
- *Samsung: CVE-2023-21484, CVE-2023-21485,...*
- *IBM: CVE-2023-27556, CVE-2023-27557,...*

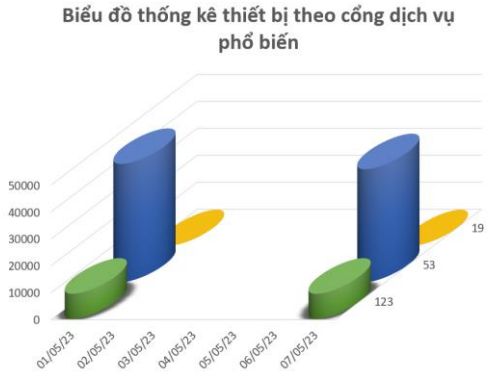
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-29350 CVE-2023-29354	Nhóm 02 lỗ hổng trong Microsoft (Edge) cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực hiện leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-2235 CVE-2023-2236 CVE-2023-2248 …	Nhóm 05 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công gây ra lỗ hổng use-after-free, thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-2459 CVE-2023-2460 CVE-2023-2461 …	Nhóm 10 lỗ hổng trong Google (Chrome) 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
4	Wordpress	CVE-2013-10026 CVE-2014-125100 CVE-2016-15031 …	Nhóm 49 lỗ hổng trong Wordpress cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Gitlab	CVE-2023-0155 CVE-2023-0485 CVE-2023-0756 …	Nhóm 12 lỗ hổng trong Gitlab cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2023-21484 CVE-2023-21485 CVE-2023-21486 …	Nhóm 22 lỗ hổng trong Samsung (Andriod) 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
7	IBM	CVE-2023-27556 CVE-2023-27557 CVE-2022-43871 …	Nhóm 18 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công tiết lộ thông tin đăng nhập, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

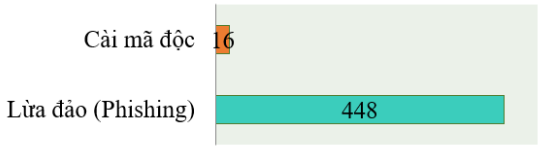
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **51,359** (giảm so với tuần trước **51,953**) 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.

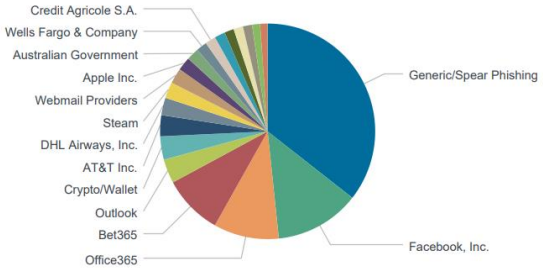


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 464 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 448 trường hợp tấn công lừa đảo (Phishing), 16 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: 12408 IP	xjpakmdcfuqe.ru:261 IP
disorderstatus.ru: 5049 IP	xjpakmdcfuqe.in:295 IP
atomictrivia.ru: 2532 IP	restlesz.su: 271 IP
xjpakmdcfuqe.biz: 379 IP	amnsreiuojy.ru: 736 IP
xjpakmdcfuqe.com: 258 IP	hzmksreiuojy.ru: 34 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **330** 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	itikiab.com	Website giả mạo sàn TMĐT Tiki
2	vp7811.com somnio-evolve.com 888b.biz hdsaison-vn.com thuongmaidientuquocte.com …	Website giả mạo, 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