NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 23 (05/6/2023 – 11/6/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công mạng Triều Tiên giả danh các công ty đầu tư vốn mạo hiểm tại Nhật Bản, Việt Nam và Mỹ.

- **Cảnh báo:** Phát hiện backdoor mới có tên SPECTRALVIPER nhằm mục tiêu tấn công vào các công ty lớn tại Việt Nam.

2. Điểm yếu, lỗ hổng

- **729** 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: 344** 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 tấn công mạng Triều Tiên giả danh các công ty đầu tư vốn mạo hiểm tại Nhật Bản, Việt Nam và Mỹ"

Theo một nghiên cứu mới đây, đã phát hiện một nhóm tấn công mạng có liên quan đến Triều Tiên đang tiến hành một chiến dịch giả danh các tổ chức tài chính và công ty đầu tư vốn mạo hiểm tại Mỹ, Việt Nam và Nhật Bản.

Một nhóm chuyên gia bảo mật đã đưa ra nghi vấn rằng chiến dịch tấn công này có liên quan đến APT38. Đây là một nhóm tấn công được cho là hoạt động dưới sự hỗ trợ của chính phủ Triều Tiên và đã thực hiện nhiều chiến dịch tấn công nhằm vào các công ty tiền ảo và tổ chức khác.

Trước đó, nhóm tấn công này đã thực hiện nhiều chiến dịch khác với mục tiêu liên quan đến tài chính, xâm nhập vào các sàn giao dịch tiền ảo, ngân hàng thương mại và hệ thống thương mại điện tử.

Mục tiêu của những chiến dịch này là củng cố nỗ lực của chính quyền Triều Tiên trong việc thực hiện các lệnh trừng phạt. Điểm nổi bật của chiến dịch này là việc giả mạo các công ty đầu tư vốn mạo hiểm. Trước đó, APT38 đã từng tấn công Hiệp hội Viễn thông tài chính liên ngân hàng toàn cầu - SWIFT và một sàn giao dịch tiền ảo.

Trong tháng 03/2022, đã xác định được sử dụng 18 máy chủ độc hại bởi nhóm tấn công, cho phép đối tượng tấn công phát tán mã độc và giả danh thành dịch vụ cloud, sàn giao dịch tiền ảo và các công ty đầu tư tư nhân để đánh lừa người dùng mở các nội dung độc hại hoặc cung cấp thông tin cá nhân của họ cho nhóm tấn công.

Mục tiêu của những cuộc tấn công vào các công ty và ngân hàng đầu tư là tiết lộ thông tin bí mật của đối tượng và người dùng, tạo ra những hành động pháp lý và gây rối cho các thỏa thuận và đàm phán kinh doanh còn đang diễn ra hoặc để tiết lộ thông tin có hại cho chiến lược đầu tư.

Trong một chiến dịch tấn công mạng diễn ra từ giữa tháng 1 đến tháng 3 năm 2023, nhóm chuyên gia đã phát hiện thêm 3 địa chỉ IP liên quan đến nhóm tấn công này. Các địa chỉ IP này đã lưu trữ 21 tên miền liên quan đến các thuật ngữ thường được sử dụng bởi phần mềm văn bản như "doc-share" và "autoprotect", và một số tên miền khác chứa nội dung của các công ty tài chính tại Nhật Bản, Việt Nam và Mỹ.

Để giảm thiểu nguy cơ bị tấn công mạng, các cơ quan và tổ chức cần tăng cường kiểm tra và quét hệ thống, cũng như sẵn sàng áp dụng các biện pháp xử lý khi phát hiện dấu hiệu của một cuộc tấn công mạng.

Nguồn: https://therecord.media/north-korean-hacking-group-spoofs-venture-capital-firms-finance-japan-vietnam?&web_view=true

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện backdoor mới có tên SPECTRALVIPER nhằm mục tiêu tấn công vào các công ty lớn tại Việt Nam"

Hiện nay, các công ty lớn tại Việt Nam đang trở thành mục tiêu của một chiến dịch tấn công mạng nhằm triển khai backdoor mới có tên SPECTRALVIPER. Đây là một loại backdoor chưa được biết đến trước đây, với mã nguồn bị xáo trộn và được thiết kế để hoạt động trên hệ điều hành Windows x64. SPECTRALVIPER có khả năng tải và lây nhiễm các tệp thực thi (Portable Executable - PE), cho phép thực thi mã độc thông qua các chu trình hợp lệ, tải lên và tải xuống các tệp tin, thao túng tệp tin và thư mục, đồng thời mạo danh người dùng.

Các cuộc tấn công này được biết đến với tên gọi REF2754, có sự tương đồng với nhóm tấn công APT32 của Việt Nam (còn được gọi là Canvas Cyclone, Bismuth, Cobalt Kitty và OceanLotus).

Theo các nhà nghiên cứu, trong một đợt tấn công gần đây, tiện ích SysInternals ProcDump đã được khai thác để tải tệp DLL kiểu unsigned (không được ký số) có chứa DONUTLOADER, tệp này được cấu hình để tải SPECTRALVIPER và các mã độc khác như P8LOADER hoặc POWERSEAL.

SPECTRALVIPER được thiết kế để kết nối với một máy chủ được kiểm soát bởi kẻ tấn công và chờ lệnh. Đồng thời, SPECTRALVIPER sử dụng các phương pháp che giấu như Control Flow Flattening để tránh bị phát hiện.

Mã độc P8LOADER được viết bằng ngôn ngữ C++, có khả năng khởi chạy payload tùy ý từ một tệp hoặc từ bộ nhớ. Mã độc POWERSEAL được thiết kế để chạy các lệnh hoặc tệp lệnh PowerShell được cung cấp bởi kẻ tấn công.

Có thông tin cho rằng hình thức tấn công của nhóm APT REF2754 có nhiều điểm tương đồng so với nhóm tấn công APT REF4322, nhóm này được biết đến chủ yếu tấn công vào các tổ chức tại Việt Nam để triển khai một công cụ sau khai thác được gọi là PHOREAL (còn được gọi là Rizzo).

Các cá nhân và tổ chức cần cập nhật bản vá hệ điều hành Windows và bật chế độ tự động cập nhật. Đồng thời, triển khai các giải pháp giám sát an toàn thông tin mạng như cài đặt phần mềm diệt virus AV, cài đặt và cấu hình tường lửa trên thiết bị, tạo bản sao lưu cho các dữ liệu quan trọng, thực hiện kiểm tra và rà soát để phát hiện kịp thời dấu hiệu bất thường của các cuộc tấn công nhằm ứng cứu, xử lý kịp thời.Bên cạnh đó, chiến dịch mã độc này là dấu hiệu cho sự quay trở lại của các đối tượng tấn công với động cơ tài chính. Để giảm thiểu nguy cơ bị tấn công mạng các cơ quan, tổ chức cần thường xuyên cập nhập bản vá, đồng thời tăng cường lớp bảo mật cho mạng nội bộ và kiểm tra trước khi truy cập vào bất kỳ trang web nào.

Nguồn: https://thehackernews.com/2023/06/new-spectralviper-backdoor-targeting.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 **729** lỗ hổng, trong đó có 103 lỗ hổng mức Cao, 143 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 482 lỗ hổng chưa đánh giá. Trong đó có ít nhất 106 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 03 lỗ hổng trong Microsoft, Nhóm 04 lỗ hổng trong Linux, Nhóm 67 lỗ hổng trong Mozilla, Nhóm 229 lỗ hổng trong Wordpress, Nhóm 41 lỗ hổng trong Google, Nhóm 14 lỗ hổng trong Gitlab, Nhóm 12 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-2023-29344, CVE-2023-29345,...*
- *Linux: CVE-2023-0635, CVE-2023-0636,...*
- *Mozilla: CVE-2023-23605, CVE-2023-23606,...*
- *Wordpress: CVE-2015-10111, CVE-2023-2781,...*
- *Google: CVE-2023-30863, CVE-2022-48478,...*
- *Gitlab: CVE-2023-2001, CVE-2023-2015,...*
- *IBM: CVE-2023-23480, CVE-2023-23481,...*

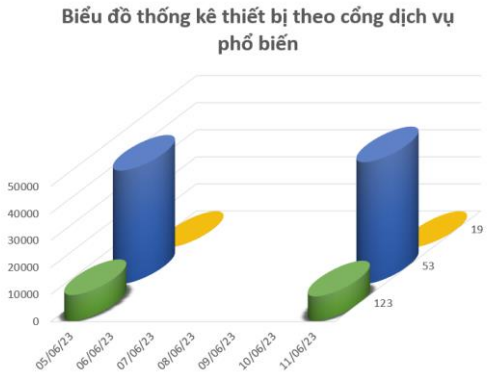
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-33143 CVE-2023-29344 CVE-2023-29345	Nhóm 03 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, thực hiện leo thang đặc quyền, lỗ hổng Bypass.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-0635 CVE-2023-0636 CVE-2023-3141 …	Nhóm 04 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	Mozilla	CVE-2023-23605 CVE-2023-23606 CVE-2023-25729 …	Nhóm 67 lỗ hổng trong Mozilla cho phép đối tượng tấn công làm lộ lọt thông tin đăng nhập, thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2015-10111 CVE-2023-2781 CVE-2022-45372 …	Nhóm 229 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-2023-30863 CVE-2023-30864 CVE-2023-30865 …	Nhóm 41 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	Gitlab	CVE-2023-2001 CVE-2023-2013 CVE-2023-2015 …	Nhóm 14 lỗ hổng trong Gitlab 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-2023-23480 CVE-2023-23481 CVE-2023-23482 …	Nhóm 12 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

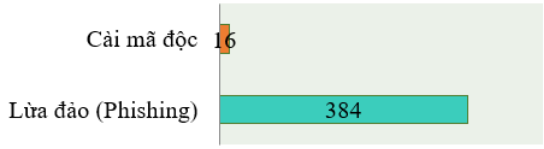
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **54.215,** (tăng so với tuần trước **52.453)** 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.

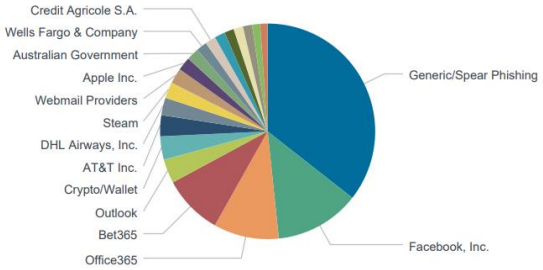


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 400 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 384 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: 8349 IP	xjpakmdcfuqe.ru:113 IP
disorderstatus.ru: 3351 IP	xjpakmdcfuqe.in:102 IP
atomictrivia.ru: 1601 IP	restlesz.su: 282 IP
xjpakmdcfuqe.biz: 256 IP	amnsreiuojy.ru: 531 IP
xjpakmdcfuqe.com: 139 IP	hzmksreiuojy.ru: 40 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **344** 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	gplxgovn.vn	Website giả mạo Tổng cục Đường bộ Việt Nam
2	daef33.com adef66.com adef22.com tiki11.top adef77.com sadm26.com	Website giả mạo sàn TMĐT Tiki
3	amg133180.com share.ttchanging.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