NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 05 (30/01/2023 – 05/02/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Lỗ hổng bảo mật ảnh hưởng Nghiêm trọng trong sản phẩm Cisco Iox và F5 BIG-IP.

- **Chiến dịch tấn công APT:** Nhóm tấn công mạng APT Trung Quốc sử dụng các công cụ nguồn mở để nhằm mục tiêu vào Đông Á.

2. Điểm yếu, lỗ hổng

- **526** 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: 166** 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 mạng APT Trung Quốc sử dụng các công cụ nguồn mở để nhằm mục tiêu vào Đông Á"

Gần đây, chiến dịch tấn công đã được phát hiện nằm mục tiêu vào các tổ chức ở Đông Á bằng công cụ mã nguồn mở SparkRAT. Đối tượng tấn công sử dụng cơ sở hạ tầng đã bị xâm nhập như cửa hàng bán lẻ sản phẩm dành cho trẻ em, phòng trưng bày nghệ thuật cũng như các trang web trò chơi cờ bạc ở Trung Quốc, Hồng Kông, Singapore và Đài Loan.

Đối tượng tấn công lạm dụng máy chủ web và máy chủ cơ sở dữ liệu MySQL để truy cập lần đầu và sử dụng China Chopper để triển khai webshell thông qua SQL injection, XSS. Kẻ tấn công có thể tấn công leo thang đặc quyền, triển khai phần mềm độc hại và công cụ được lưu trữ tại C&C.

Đối tượng tấn công chủ yếu dựa vào nhiều công cụ nguồn mở như BadPotatom SharpToken, GotoHTTP, ShellCode_Loader và m6699[.]exe. Các công cụ nguồn mở này đã được nhiều nhóm tấn công của Trung Quốc sử dụng trong chiến dịch của họ. Vào cuối tháng 12 năm 2022, Microsoft đã báo cáo về dấu hiệu của những kẻ tấn công sử dụng SparkRAT. Phần mềm độc hại Zegost cũng được sử dụng bởi nhóm FinGhost để nhằm mục tiêu vào một cơ quan chính phủ Trung Quốc vào tháng 9 năm 2022. Đáng chú ý, các nhà nghiên cứu đã tìm thấy một địa chỉ C2 chung giữa các nhóm Zegost và DragonSpark. Webshell của China Chopper đã được sử dụng bởi các nhóm tội phạm mạng và gián điệp Trung Quốc như TG-3390 và Leviathan.

DragonSpark sử dụng phần mềm nguồn mở và phần mềm độc hại dựa trên Golang để tránh bị phát hiện bằng cách làm xáo trộn việc triển khai phần mềm độc hại. Điều này cho thấy rằng các đối tượng tấn công mạng Trung Quốc vẫn đang tích cực mở rộng kho vũ khí và chia sẻ công cụ với nhau.

Nguồn: https://cyware.com/news/chinese-speaking-threat-actors-leveraging-open-source-tools-to-target-east-asia-783532a7

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng bảo mật ảnh hưởng Nghiêm trọng trong sản phẩm Cisco Iox và F5 BIG-IP"

Lỗ hổng bảo mật CVE-2023-22374 trong F5 BIG-IP

F5 đã cảnh báo về lỗ hổng bảo mật có mã CVE-2023-22374 (điểm CVSS: 8.5) ảnh hưởng Nghiêm trọng trong các thiết bị BIG-IP cho phép đối tượng tấn công thực thi mã tùy ý, tấn công từ chối dịch vụ. Lỗ hổng này ảnh hưởng đến các phiên bản BIG-IP sau: 13.1.5, 14.1.4.6-14.1.5, 15.1.5.1-15.1.8, 16.1.2.2-16.1.3 và 17.0.0.

Lỗ hổng tồn tại trong iControl SOAP. Do giao diện iControl SOAP chạy bằng quyền root, nên việc khai thác thành công có thể cho phép đối tượng tấn công kích hoạt thực thi mã từ xa trên thiết bị với quyền root.

F5 đã khắc phục lỗ hổng này trong một hotfix kỹ thuật có sẵn cho các phiên bản BIG-IP được hỗ trợ. Ngoài ra, giải pháp khắc phục thay thế cho lỗ hổng trên là hạn chế quyền truy cập vào iControl SOAP API.

Lỗ hổng bảo mật CVE-2023-20076 trong Cisco IOx

Cisco đã phát hành các bản cập nhật cho lỗ hổng CVE-2023-20076 trong Cisco IOx, cho phép đối tượng tấn công thực thi các lệnh tùy ý với quyền root trên máy chủ. Lỗ hổng này ảnh hưởng đến các thiết bị chạy phần mềm Cisco IOS XE đã bật tính năng Cisco Iox, cũng như 800 Series Industrial ISRs, Catalyst Access Points, CGR1000 Compute Modules, IC3000 Industrial Compute Gateways, IR510 WPAN Industrial Routers.

Khai thác thành công lỗ hổng này, đối tượng tấn công có thể cài đặt và ẩn các backdoor. Mặc dù việc khai thác yêu cầu kẻ tấn công phải được xác thực và có quyền quản trị viên, nhưng điều đáng chú ý là kẻ tấn công có thể tìm nhiều cách khác nhau để leo thang đặc quyền.

Nguồn: https://thehackernews.com/2023/02/new-high-severity-vulnerabilities.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 526 lỗ hổng, trong đó có 17 lỗ hổng mức Cao, 19 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 490 lỗ hổng chưa đánh giá. Trong đó có ít nhất 58 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 Asus, Nhóm 08 lỗ hổng trong Hp, Nhóm 10 lỗ hổng trong Apache, Nhóm 03 lỗ hổng trong Linux, Nhóm 25 lỗ hổng trong Dell, Nhóm 51 lỗ hổng trong Wordpress, Nhóm 06 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:

- *Asus: CVE-2021-37315, CVE-2021-37316,...*
- *Hp: CVE-2021-3808, CVE-2021-3809,...*
- *Apache: CVE-2022-44644, CVE-2022-44645,...*
- *Linux: CVE-2023-0266, CVE-2023-0240,...*
- *Dell: CVE-2022-45100, CVE-2022-45101,...*
- *Wordpress: CVE-2023-0550, CVE-2023-0553,...*
- *IBM: CVE-2022-47983, CVE-2023-23469,...*

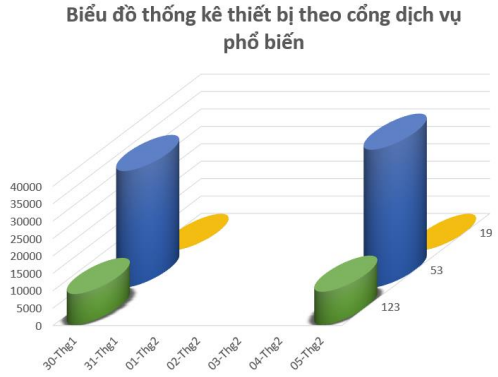
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Asus	CVE-2021-37315 CVE-2021-37316 CVE-2021-37317	Nhóm 03 lỗ hổng trong Asus (ASUS RT-AC68U) cho phép đối tượng tấn công ghi các tệp tùy ý, thu thập thông tin dữ liệu trái phép.	Chưa có thông tin xác nhận và bản vá
2	Hp	CVE-2021-3808 CVE-2021-3809 CVE-2022-27537 …	Nhóm 08 lỗ hổng trong Hp (BIOS) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công từ chối dịch vụ, thực hiện leo thang đặc quyền, làm rỏ rỉ thông tin dữ liệu.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2022-44644 CVE-2022-44645 CVE-2023-24830 …	Nhóm 10 lỗ hổng trong Apache (IoTDB, InLong,…) cho phép đối tượng tấn công , truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
4	Linux	CVE-2023-0266 CVE-2023-0240 CVE-2023-25012	Nhóm 03 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Wordpress	CVE-2023-0550 CVE-2023-0553 CVE-2023-0554 …	Nhóm 51 lỗ hổng trong Wordpress cho phép đối tượng tấn công với quyền của người dùng cục bộ có thể sửa đổi hoặc xóa các bài đăng tùy ý, tạo, cập nhật và xóa mục menu và các chức năng quản lý menu khác, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Dell	CVE-2022-45100 CVE-2022-45101 CVE-2022-45102 …	Nhóm 25 lỗ hổng trong Dell (PowerScale OneFS) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công leo thang đặc quyền, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-47983 CVE-2023-23469 CVE-2023-23477 ...	Nhóm 06 lỗ hổng trong IBM (Automation Decision Services,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

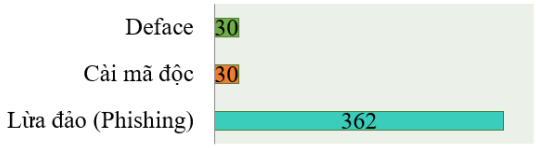
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **47,272** (tăng so với tuần trước **40,895**) 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.

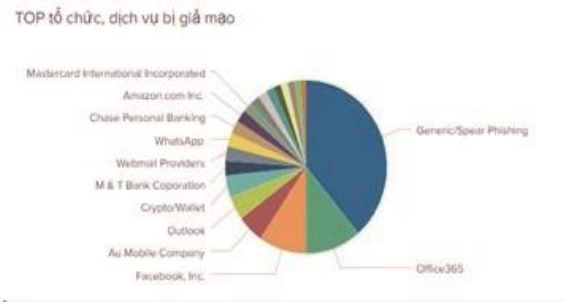


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 422 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 30 trường hợp tấn công thay đổi giao diện (Deface), 362 trường hợp tấn công lừa đảo (Phishing), 30 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: 14445 IP	xjpakmdcfuqe.ru:366 IP
disorderstatus.ru: 6437 IP	xjpakmdcfuqe.in: 353 IP
atomictrivia.ru: 2891 IP	restlesz.su: 282 IP
xjpakmdcfuqe.biz: 576 IP	amnsreiuojy.ru: 597 IP
xjpakmdcfuqe.com: 467 IP	hzmksreiuojy.ru: 49 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 166 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	mmomo.me clmm1.tv	Giả mạo website Ví điện tử Momo
2	mxp00338.com	Giả mạo website sàn TMĐT Lazada
3	Viashopee.com	Giả mạo website sàn TMĐT Shopee
4	cardshinhan.com	Giả mạo website Ngân hàng TNHH MTV Shinhan Việt Nam
5	softwarefpt.com	Giả mạo website Công Ty Cổ Phần Viễn Thông FPT
6	lotte.cm66llks.top	Giả mạo website Lotte
7	evncredit.online	Giả mạo website Tập đoàn Điện lực Việt Nam (EVN)
8	anbinh-finance.club	Giả mạo website Ngân hàng TMCP An Bình
9	hdbankfinance.live	Giả mạo website Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
10	vaymb.org	Giả mạo website Ngân hàng TMCP Quân đội
11	tiki111.com	Giả mạo website sàn TMĐT Tiki
12	tiktokcy1.com vip8591.net v.vl404.cn m.one018.com m.kone365.com vn.btaynguyenfood.com ae888vip.com m.luxurysvip888.com 975.vn h5.tocdovnm.com tindungonline-evn.shop fd2.hmexchangecentre.com …	Trang web 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