TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 22 (30/5/2022 – 05/6/2022)

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 – ais.@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp.Hà Nội

NỘI DUNG TUẦN

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

TIN CẢNH BÁO

- **Cảnh báo:** Lỗ hổng Zero-day ảnh hưởng Nghiêm trọng trong Atlassian Confluence

- **Chiến dịch tấn công APT:** Chiến dịch tấn công do thám của nhóm APT Turla

ĐIỂM YẾU, LỖ HỔNG

- **438** 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.

SỐ LIỆU, THỐNG KÊ

- Tấn công DRDoS
- Tấn công Web
- Tấn công lừa đảo người dùng Việt Nam

Hot News!

Tài liệu lưu trữ:

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

https://service.khonggianmang.vn

TIN CẢNH BÁO

Cảnh báo: Lỗ hổng Zero-day ảnh hưởng Nghiêm trọng trong Atlassian Confluence ESXi

Ngày 2/6 vừa qua, Atlassian đã công bố thông tin về lỗ hổng bảo mật CVE-2022-26134 ảnh hưởng Nghiêm trọng (điểm CVSS: 9.8) đến các sản phẩm Server và Data Center Confluence, cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này hiện chưa có bản vá và đang bị khai thác trong thực tế.

Tất cả các phiên bản của Server và Data Center Confluence được cho là đều bị ảnh hưởng. Atlassian khuyến nghị cơ quan, tổ chức nên hạn chế để Server và Data Center công khai trên Internet hoặc tắt cả hai cho đến khi có bản vá.

Chuỗi tấn công diễn ra bằng việc khai thác lỗ hổng zero-day – một lỗ hổng command injection, để thực thi mã từ xa và triển khai webshell Behinder trên máy chủ bị xâm phạm. Behinder có khả năng tích hợp các memory webshell và hỗ trợ kết nối với Meterpreter và Cobalt Strike. Nó sẽ bị xóa bỏ khi khởi động lại hệ thống hoặc dịch vụ. Webshell này được dùng để triển khai hai webshell khác, bao gồm China Chopper và một shell cho phép tải tệp tùy ý lên máy mục tiêu.

Khai thác thành công lỗ hổng này, đối tượng tấn công có quyền truy cập vào hệ thống mạng của mục tiêu. Những hệ thống này thường khó có thể điều tra dấu vết tấn công do không có tính năng monitoring/logging. Vì vậy để tránh nguy cơ bị tấn công, các cơ quan, tổ chức sử dụng Confluence cần thực hiện biện pháp khắc phục thay thế trong thời gian chờ có bản vá được công bố. Chi tiết các bước khắc phục tham khảo tại:

https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

Nguồn: https://thehackernews.com/2022/06/hackers-exploiting-unpatched-critical.html?m=1

Chiến dịch tấn công do thám của nhóm APT Turla

Gần đây, các nhà nghiên cứu đã quan sát thấy một chiến dịch do thám của nhóm APT Turla nhằm vào các mục tiêu ở Baltic và Áo, ngoài ra có một tổ chức của NATO.

Mục tiêu đầu tiên của chiến dịch là Trường Cao đẳng Quốc phòng Baltic (hay còn gọi là BALTDEFCOL), một trường cao đẳng quân sự đa quốc gia, đây cũng được xem như một trung tâm nghiên cứu chiến lược được thành lập bởi ba nước Baltic (Estonia, Latvia và Lithuania). Một mục tiêu khác là Phòng Kinh tế Liên bang Áo, đóng vai trò là nhà tư vấn quốc tế về các biện pháp trừng phạt kinh tế và lập pháp.

Đối tượng tấn công sử dụng typosquatting domains để lưu trữ tài liệu Word độc hại được xác định là 'War Bulletin 19.00 CET 27.04[.]docx', tài liệu này được tìm thấy trong thư mục khác nhau của các trang web mục tiêu.

Theo các chuyên gia, nhóm tấn công Turla đang tập trung vào các cuộc tấn công do thám để thu thập thông tin thực hiện các cuộc tấn công lừa đảo trong thời gian tới. Do đó, các cơ quan, tổ chức cần cập nhật thông tin về các cuộc tấn công đang diễn ra và thường xuyên tham gia vào việc chia sẻ thông tin về mối đe dọa.

IoC:

wkoinfo [.] Webredirect [.] Org

baltdefcol [.] Webredirect [.] Org

wko [.] At

baltdefcol [.] Org

Nguồn: https://cyware.com/news/turla-performs-reconnaissance-attacks-137e6645

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 438 lỗ hổng, trong đó có 01 lỗ hổng mức cao, 9 lỗ hổng mức trung bình, 01 lỗ hổng mức thấp và 427 lỗ hổng chưa đánh giá. Trong đó có ít nhất 82 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: 01 lỗ hổng ảnh trong sản phẩm Microsoft, 01 lỗ hổng ảnh trong sản phẩm Apache, 01 lỗ hổng ảnh trong Google, Nhóm 14 lỗ hổng ảnh trong sản phẩm Cisco, 02 lỗ hổng ảnh trong thiết bị D-link, Nhóm 10 lỗ hổng ảnh trong thiết bị Dell, Nhóm 05 lỗ hổng ảnh trong Linux. 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-2022-30190

- Apache: CVE-2022-30973

- Google: CVE-2021-34083

- Cisco: CVE-2022-20670, CVE-2022-20797,...

- D-link: CVE-2022-29778, CVE-2022-30521

- Dell: CVE-2022-29098, CVE-2020-26184,...

- Linux: CVE-2022-1652, CVE-2022-1943,...

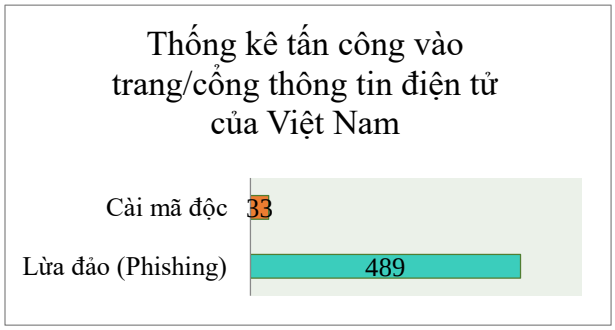
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2022-30190	01 lỗ hổng ảnh trong sản phẩm Microsoft (Microsoft Windows Support Diagnostic Tool (MSDT)) cho phép đối tượng tấn công thực thi mã từ xa	Đã có thông tin xác nhận và bản vá
2	Apache	CVE-2022-30973	01 lỗ hổng ảnh trong sản phẩm Apache (Tika) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2021-34083	01 lỗ hổng ảnh trong Google (Google-it) cho phép đối tượng tấn công thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
4	Cisco	CVE-2022-20670 CVE-2022-20797 CVE-2022-20802 …	Nhóm 14 lỗ hổng ảnh trong sản phẩm Cisco (Common Services Platform Collecto, Enterprise Chat and Email (ECE), Secure Network Analytics,…) cho phép đối tượng tấn công thực hiện tấn công giả mạo XSS, thực thi mã từ xa, mã tùy ý, thu thập thông tin.	Chưa có thông tin xác nhận và bản vá
5	D-link	CVE-2022-29778 CVE-2022-30521	02 lỗ hổng ảnh trong thiết bị D-link (DIR-890L 1.20b01, DIR-890L DIR890LA1_FW107b09.bin) cho phép đối tượng tấn công thực thi mã tùy ý	Chưa có thông tin xác nhận và bản vá
6	Dell	CVE-2022-29098 CVE-2020-26184 CVE-2022-26868 …	Nhóm 10 lỗ hổng ảnh trong thiết bị Dell (PowerScale OneFS, BSAFE Micro Edition Suite, EMC PowerStore,…) cho phép đối tượng tấn công thu thập thông tin,thực thi lệnh/mã tùy ý,tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
7	Linux	CVE-2022-1652 CVE-2022-1943 CVE-2022-1786 …	Nhóm 05 lỗ hổng ảnh trong Linux (Linux kernel, teletype,…) cho phép đối tượng tấn công thực hiện leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công tại 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 **70,286** (giảm so với tuần trước **70,833**) 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.

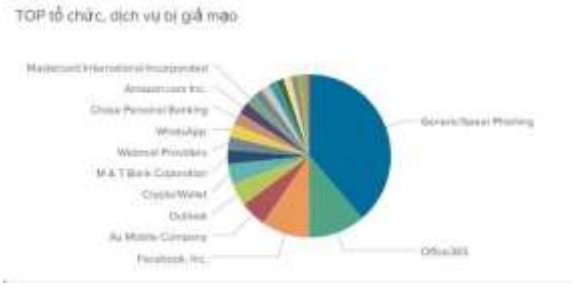


Tấn công Phishing

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, Paypment, 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.

Tấn công Web

Trong tuần, có 522 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 489 trường hợp tấn công lừa đảo (Phishing), 33 trường hợp tấn công cài cắm mã độc.



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

differentia.ru: 19,886 IP	xjpakmdcfuqe.ru: 531 IP
disorderstatus.ru: 10,045 IP	xjpakmdcfuqe.in: 396 IP
atomictrivia.ru: 4,703 IP	restlesz.su: 222 IP
xjpakmdcfuqe.biz: 976 IP	amnsreiuojy.ru: 192 IP
xjpakmdcfuqe.com: 705 IP	hzmksreiuojy.ru: 78 IP

New

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 236 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	https://do005.com https://sd230.com	Giả mạo sàn TMĐT Sendo
2	https://bm1717.com https://shopmall55.com http://shopee298.com https://goshopbackvip.vip	Giả mạo sàn TMĐT Shopee
3	https://lazada8.net https://lazada7788.com	Giả mạo sàn TMĐT Lazada
4	https://trungtamdienmayxanh.net https://dienmayxanhhcm.com https://cskhdienmayxanh.com https://baotrixanhvn.com http://dienmayxanhtantam.com https://cskhdienmayxanhvn.com	Giả mạo website Điện máy xanh
5	https://tikictv9.com https://tiki136.com	Giả mạo sàn TMĐT Tiki

Khuyến nghị đối với các cơ quan, đơn vị

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin cảnh báo** 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 thống thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần **Nguy cơ tấn công mạng từ điểm yếu lỗ hổng**, 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.

***

4. 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.

***

Thông tin liên hệ:

Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 - ais@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội