NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 16 (17/04/2023 – 23/04/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Lazarus thực hiện các cuộc tấn công chuỗi cung ứng nhằm vào phần mềm 3CX.

- **Cảnh báo:** Cisco và VMware phát hành bản vá khắc phục các lỗ hổng nghiêm trọng.

2. Điểm yếu, lỗ hổng

- **693** 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: 300** 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 APT Lazarus thực hiện các cuộc tấn công chuỗi cung ứng nhằm vào phần mềm 3CX"

Gần đây, nghiên cứu mới nhất cho thấy nhóm tấn công APT Lazarus hay còn được biết đến là UNC4736 của Triều Tiên đang thực hiện các cuộc tấn công chuỗi cung ứng nhằm vào 3CX. Nhóm này đã xâm nhập vào cơ sở hạ tầng quan trọng trong lĩnh vực điện, năng lượng và các doanh nghiệp tham gia giao dịch tài chính thông qua việc cài đặt trojan vào ứng dụng X_TRADER. Những nghiên cứu mới nhất cũng cho thấy việc xâm nhập vào ứng dụng X_TRADER đã gây ảnh hưởng đến nhiều tổ chức khác ngoài phạm vi 3CX.

Các cuộc tấn công diễn ra kể từ tháng 9/2022 đến 11/2022 và vẫn còn tiếp diễn cho đến nay. Nhóm tấn công này đã nhằm mục tiêu vào ứng dụng X_TRADER thông qua việc tải xuống và cài cắm mã độc vào máy tính cá nhân của người dùng tạo điều kiện cho một cuộc tấn công chuỗi cung ứng nhằm vào 3CX.

Nguồn: https://thehackernews.com/2023/04/lazarus-xtrader-hack-impacts-critical.html

APT Lazarus đã sử dụng backdoor VEILEDSIGNAL cho phép đối tượng tấn công truy cập vào máy tính của người dùng và thu thập thông tin đăng nhập trái phép. Sau đó dùng backdoor này nhằm xâm nhập vào hệ thống của phần mềm 3CX, Window và macOS để cài cắm mã độc. Mặc dù X_TRADER đã ngừng hoạt động từ tháng 4/2020 nhưng người dùng vẫn có thể tải xuống ứng dụng này trên các trang web của công ty.

Theo các nghiên cứu, việc triển khai backdoor VEILEDSIGNAL kết hợp với kỹ thuật process-injection có thể được đưa vào trình duyệt web Chrome, Firefox hoặc Edge. Mô-đun này chứa thư viện liên kết động DDL (dynamic-link library) kết nối với trang web của Trading Technologies để ra lệnh và điều khiển C&C. Ngoài ra, cuộc tấn công này còn được liên kết với AppleJeus.

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.

Tin tức An toàn thông tin

"Cảnh báo: Cisco và VMware phát hành bản vá khắc phục các lỗ hổng nghiêm trọng"

Ciso phát hành bản cập nhật khắc phục các lỗ hổng bảo mật

Vừa qua, Cisco đã phát hành bản cập nhật để khắc phục các lỗ hổng bảo mật cho phép đối tượng tấn công thực thi mã tùy ý trên các hệ thống bị ảnh hưởng.

Lỗ hổng bảo mật CVE-2023-20036 có mức ảnh hưởng Nghiêm trọng (điểm CVSS: 9.9) trên hệ thống điều khiển công nghiệp Cisco IND (Industrial Network Director) ảnh hưởng đến giao diện người dùng web (UI), điều này xảy ra do việc thiếu kiểm tra xác thực dữ liệu đầu vào khi tải lên một Device Park. Khai thác thành công lỗ hổng này đối tượng tấn công có thể thực thi các lệnh tùy ý với quyền NT AUTHORITY\SYSTEM trên các thiết bị bị ảnh hưởng.

Lỗ hổng bảo mật CVE-2023-20039 có mức ảnh hưởng Trung bình (điểm CVSS: 5.5) liên quan đến việc phân quyền truy cập file (file permissions) cho phép đối tượng tấn công sử dụng quyền của người dùng cục bộ đã được xác thực, qua đó các đối tượng này có thể thu thập thông tin dữ liệu trái phép.

Lỗ hổng bảo mật CVE-2023-20154 có mức ảnh hưởng Nghiêm trọng (điểm CVSS 9.1) ảnh hưởng đến cơ chế xác thực bên ngoài của nền tảng Modeling Labs cho phép đối tượng tấn công không cần xác thực truy cập vào giao diện web bằng các đặc quyền quản trị.

VMware phát hành bản vá cho Aria Operations for Logs

Ngày 20/04/2023, VMware đã cảnh báo về một lỗ hổng CVE-2023-20864 có mức ảnh hưởng Nghiêm trọng (điểm CVSS: 9.8) và lỗ hổng bảo mật CVE-2023-20865 có mức ảnh hưởng Cao (điểm CVSS: 7.2) ảnh hưởng đến nhiều phiên bản Aria Operations for Logs. Các lỗ hổng này cho phép đối tượng tấn công truy cập mạng vào VMware Aria Operations for Logs để thực thi lệnh tùy ý với quyền root.

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. Tăng cường giám sát và sẵn sàng các phương án xử lý khi phát hiện có dấu hiệu bị cài cắm, khai thác, tấn công mạng.

Nguồn: https://thehackernews.com/2023/04/cisco-and-vmware-release-security.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 **693** lỗ hổng, trong đó có 87 lỗ hổng mức Cao, 118 lỗ hổng mức Trung bình, 09 lỗ hổng mức Thấp và 479 lỗ hổng chưa đánh giá. Trong đó có ít nhất 111 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 44 lỗ hổng trong Google, Nhóm 06 lỗ hổng trong Linux, Nhóm 96 lỗ hổng trong Oracle, Nhóm 27 lỗ hổng trong Wordpress, Nhóm 02 lỗ hổng trong VMware, Nhóm 04 lỗ hổng trong Totolink, 01 lỗ hổng trong Dlink. 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:

- *Google: CVE-2023-21088, CVE-2023-21086,...*
- *Linux: CVE-2023-1998, CVE-2023-28327,...*
- *Oracle: CVE-2023-21948, CVE-2023-21912,...*
- *Wordpress: CVE-2023-0764, CVE-2023-0889,...*
- *Vmware: CVE-2023-20864, CVE-2023-20865.*
- *Totolink: CVE-2023-29798, CVE-2023-29799,...*
- *Dlink: CVE-2022-40946.*

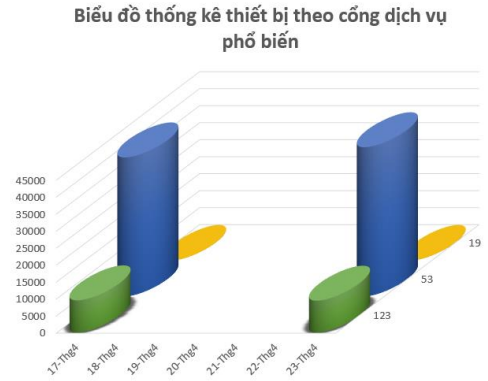
Thông tin điểm yếu, lỗ hổng

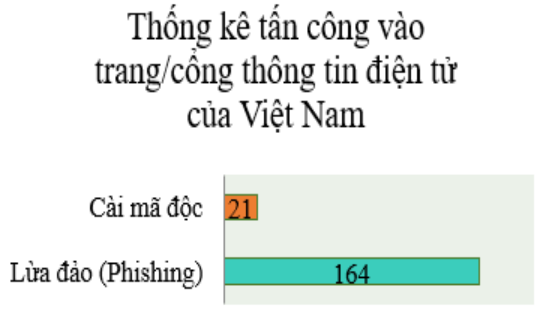
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-21086 CVE-2023-21087 CVE-2023-21088 …	Nhóm 44 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, nâng cao đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1998 CVE-2023-2008 CVE-2023-28327 …	Nhóm 06 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, nâng cao đặc quyền, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
3	Oracle	CVE-2023-21948 CVE-2023-21987 CVE-2023-21912 …	Nhóm 96 lỗ hổng trong Oracle (MySQL Server, WebLogic Server,...) 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
4	Wordpress	CVE-2023-0764 CVE-2023-0765 CVE-2023-0889 …	Nhóm 27 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công CSRF, chiếm quyền quản trị của quản trị viên, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	VMware	CVE-2023-20864 CVE-2023-20865	Nhóm 02 lỗ hổng trong VMware (Aria Operations for Logs) cho phép đối tượng tấn công thực thi các lệnh tùy ý với quyền root.	Chưa có thông tin xác nhận và bản vá
6	Totolink	CVE-2023-29798 CVE-2023-29799 CVE-2023-29800 …	Nhóm 04 lỗ hổng trong Totolink (x18_firmware) 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	Dlink	CVE-2022-40946	01 lỗ hổng trong Dlink phép đối tượng tấn công 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 **53,360** (tăng so với tuần trước **48,574**) 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.



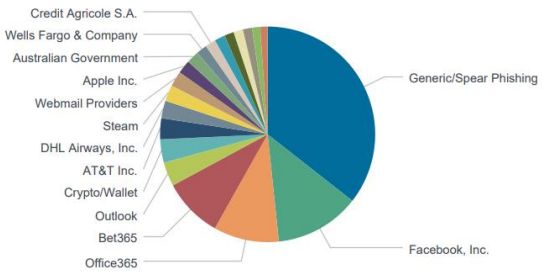


Tấn công Web

Trong tuần, có 185 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 164 trường hợp tấn công lừa đảo (Phishing), 21 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: 14972 IP	xjpakmdcfuqe.ru:378 IP
disorderstatus.ru: 6889 IP	xjpakmdcfuqe.in:381 IP
atomictrivia.ru: 3265 IP	restlesz.su: 341 IP
xjpakmdcfuqe.biz: 477 IP	amnsreiuojy.ru: 844 IP
xjpakmdcfuqe.com: 381 IP	hzmksreiuojy.ru: 57 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **300** 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	faceslitevn.site	Website giả mạo mạng xã hội Facebook
2	pvep.ink	Website giả mạo Tổng công ty cổ phần Dịch vụ kỹ thuật Dầu khí Việt Nam (PTSC)
3	songda5.cc	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