NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 42 (16/10/2023 – 22/10/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT OilRig thực hiện chiến dịch tấn công kéo dài 8 tháng nhằm vào chính phủ Trung Đông.

- **Cảnh báo:** Hàng ngàn thiết bị nhiễm mã độc Lua Backdoor do lỗ hổng Zero-Day trên Cisco.

2. Điểm yếu, lỗ hổng

- **763** 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: 398** 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

"Chiến dịch tấn công APT: Nhóm APT OilRig thực hiện chiến dịch tấn công kéo dài 8 tháng nhằm vào chính phủ Trung Đông"

Nhóm APT OilRig, còn gọi là APT34 hoặc Crambus, là một tổ chức liên quan đến Iran, đã trở thành một trong những nhóm tấn công mạng và gián điệp đáng chú ý, đặc biệt là tại khu vực Trung Đông và các mục tiêu quốc tế khác.

Gần đây, nhóm APT OilRig đã nhằm mục tiêu vào một cơ quan chính phủ tại khu vực Trung Đông. Đáng chú ý, chiến dịch tấn công đã kéo dài liên tục trong suốt tám tháng, bắt đầu từ tháng 02/2023 đến tháng 09/2023. Mục tiêu chính của cuộc tấn công này là đánh cắp thông tin quan trọng, bao gồm tệp tin và mật khẩu của tổ chức nạn nhân.

Nhóm APT OilRig đã sử dụng một loạt các phương thức tấn công để thực hiện việc đánh cắp tệp tin và mật khẩu, trong đó, phải kể đến việc triển khai một mã độc backdoor PowerShell có tên "PowerExchange." Mã độc PowerExchange lần đầu được phát hiện vào tháng 05/2023 khi nhóm APT OilRig tấn công vào chính phủ Tiểu vương quốc Ả Rập Thống nhất.

Mã độc này cho phép OilRig có thể theo dõi email gửi đến hòm thư bị xâm nhập sau khi sử dụng thông tin cố định để đăng nhập vào Microsoft Exchange Server, qua đó cho phép đối tượng tấn công thực thi payload tùy ý và tải lên/tải xuống các tệp trong thiết bị nhiễm mã độc.

Các email có tiêu đề chứa "@@" bị cài thêm câu lệnh được gửi từ đối tượng tấn công, cho phép thực thi lệnh PowerShell, ghi và đánh cắp tệp tin. Mã độc đã thiết lập một quy tắc Exchange (defaultexchangerules) để lọc các email này và chuyển chúng vào folder Deleted Items.

Bên cạnh PowerExchange, nhóm APT OilRig đã triển khai ba mã độc mới:

- Tokel: backdoor cho phép thực thi lệnh PowerShell tùy ý, tải lên hoặc tải xuống các tệp từ máy chủ đã bị nhiễm.
- Dirps: trojan có khả năng liệt kê các tệp trong một thư mục và thực thi câu lệnh PowerShell.
- Clipog: công cụ đánh cắp thông tin được dùng để thu thập dữ liệu từ bộ nhớ tạm và bàn phím.

Mặc dù phương thức xâm nhập ban đầu chưa được xác định nhưng chuyên gia bảo mật nghi ngờ rằng cuộc tấn công có thể bắt nguồn từ lừa đảo qua email. Theo nhận định từ các chuyên gia, nhóm APT OilRig (APT34 hoặc Crambus) là một tổ chức gián điệp mạng đã tồn tại lâu năm và có kinh nghiệm trong việc thực hiện các chiến dịch tấn công kéo dài, đặc biệt là nhằm vào các mục tiêu có lợi cho Iran. Hoạt động của nhóm này trong vòng 2 năm gần đây đã cho thấy rằng họ tiếp tục đe dọa các tổ chức tại Trung Đông và các vùng khác.

Nguồn: https://thehackernews.com/2023/10/iran-linked-oilrig-targets-middle-east.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Hàng ngàn thiết bị nhiễm mã độc Lua Backdoor do lỗ hổng Zero-Day trên Cisco"

Mới đây, Cisco đã cảnh báo về một lỗ hổng zero-day trong phần mềm IOS XE, đang bị những đối tượng tấn công chưa rõ danh tính khai thác để cài đặt mã độc Lua Backdoor lên hàng nghìn thiết bị.

Lỗ hổng zero-day có mã CVE-2023-20273 (Điểm CVSS: 7.2), cho phép đối tượng tấn công thực hiện leo thang đặc quyền trên chức năng giao diện web. Lỗ hổng này được khai thác đồng thời cùng với lỗ hổng CVE-2023-20198 (Điểm CVSS: 10) trong cùng một chuỗi khai thác.

Ban đầu, đối tượng tấn công khai thác CVE-2023-20198 để truy cập hệ thống và tạo một tài khoản người dùng cục bộ ở quyền cấp thứ 15, điều này cho phép đối tượng đăng nhập vào thiết bị như một người dùng thông thường. Sau đó, các đối tượng này sử dụng CVE-2023-20273 để khai thác một phần của tính năng giao diện web, nhằm nâng cấp quyền từ người dùng cục bộ lên quyền root và ghi mã độc vào hệ thống tệp.

Cisco thông báo rằng bản vá cho cả hai lỗ hổng này đã được hoàn thiện và sẽ phát hành tới người dùng vào ngày 22/10/2023. Nếu không thể cập nhật ngay, người dùng nên tắt chức năng máy chủ HTTP trên thiết bị để đảm bảo an toàn. Trước đây, một lỗ hổng khác với mã CVE-2021-1435 cũng đã bị tấn công để cài đặt backdoor, tuy nhiên, lần này nó không liên quan đến chuỗi tấn công mới.

Khi khai thác thành công cả hai lỗ hổng zero-day này, đối tượng tấn công dễ dàng truy cập vào hệ thống mà không bị hạn chế vào router và switch. Điều này cho phép các đối tượng tấn công theo dõi, can thiệp và định tuyến lưu lượng mạng, đồng thời sử dụng thiết bị như một điểm truy cập ổn định vào mạng lưới. Tất cả xảy ra do sự thiếu sót trong giải pháp bảo mật cho các thiết bị này.

Thông tin được tiết lộ sau khi phát hiện hơn 41,000 thiết bị Cisco sử dụng phần mềm IOS XE bị tấn công bởi hai lỗ hổng zero-day. Tính đến ngày 19/10, số lượng thiết bị bị ảnh hưởng đã giảm còn 36.541. Đáng chú ý, những người chịu tác động chính bởi lỗ hổng này không phải là các tập đoàn lớn, mà là các doanh nghiệp nhỏ và người dùng cá nhân.

Nguồn: https://thehackernews.com/2023/10/cisco-zero-day-exploited-to-implant.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 **763** lỗ hổng, trong đó có 190 lỗ hổng mức Cao, 182 lỗ hổng mức Trung bình, 08 lỗ hổng mức Thấp và 383 lỗ hổng chưa đánh giá. Trong đó có ít nhất 157 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 06 lỗ hổng trong Linux, Nhóm 01 lỗ hổng trong Microsoft, Nhóm 13 lỗ hổng trong Apache, Nhóm 218 lỗ hổng trong Wordpress, Nhóm 14 lỗ hổng trong Fortinet, Nhóm 73 lỗ hổng trong Oracle, Nhóm 38 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:

- Linux: CVE-2023-45871, CVE-2023-40791,...

- Microsoft: CVE-2023-36559

- Apache: CVE-2023-43668, CVE-2023-43667,...

- Wordpress: CVE-2011-10004, CVE-2023-4666,...

- Fortinet: CVE-2023-33303, CVE-2023-41682,...

- Oracle: CVE-2023-22072, CVE-2023-22069,..

- IBM: CVE-2023-45898, CVE-2023-30987,...

Thông tin điểm yếu, lỗ hổng

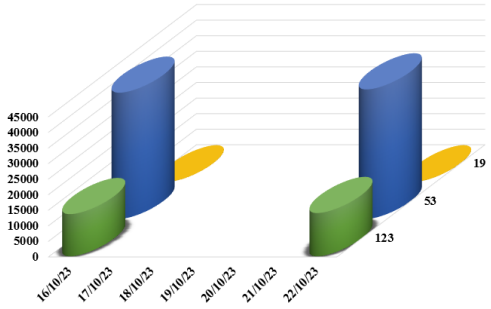
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-45871 CVE-2023-40791 CVE-2023-45898 …	Nhóm 06 lỗ hổng trong Linux cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-36559	Nhóm 01 lỗ hổng trong Microsoft 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
3	Google	CVE-2023-43668 CVE-2023-43667 CVE-2023-39456 …	Nhóm 13 lỗ hổng trong Apache cho phép đối tượng tấn công thực hiện tấn công SQL Injection, khai thác lỗi XSS.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2011-10004 CVE-2023-4666 CVE-2023-45107 …	Nhóm 218 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi CSRF, thực thi mã từ xa, thực hiện tấn công SQL Injection, khai thác lỗi XSS.	Chưa có thông tin xác nhận và bản vá
5	Adobe	CVE-2023-33303 CVE-2023-41682 CVE-2023-41680 …	Nhóm 14 lỗ hổng trong Fortinet cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	Oracle	CVE-2023-22072 CVE-2023-22069 CVE-2023-22089 …	Nhóm 73 lỗ hổng trong Oracle cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2023-45898 CVE-2023-30987 CVE-2023-30991 …	Nhóm 38 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá

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

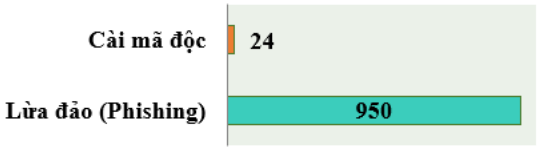
Tấn công DRDoS

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 **55.542**, (tăng so với tuần trước **54.132**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

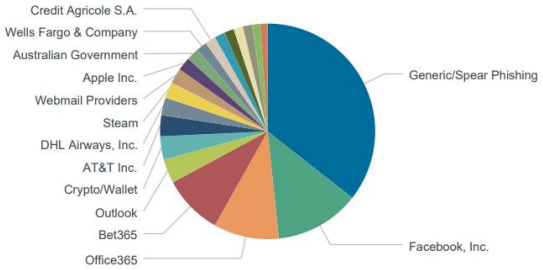


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **947** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 950 trường hợp tấn công lừa đảo (Phishing), 24 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: 15232 IP	hzmksreiuojy.ru: 257 IP
disorderstatus.ru: 7317 IP	xjpakmdcfuqe.biz: 198 IP
atomictrivia.ru: 3455 IP	xjpakmdcfuqe.com: 156 IP
amnsreiuojy.ru: 738 IP	xjpakmdcfuqe.ru: 101 IP
restlesz.su: 289 IP	xjpakmdcfuqe.in: 71 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **398** 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	dienlanhdienmayxanh.com dichvu-dien-mayxanh.com cskh-dienmay-xanh.com mayxanhsg.com	Website giả mạo Điện máy xanh
2	rwrb66.com	Website giả mạo sàn TMĐT Tiki
3	shopetankhv.com	Website giả mạo sàn TMĐT Shopee
4	vietcapital.online	Website giả mạo Ngân hàng TMCP Bản Việt

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 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