NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 32 (07/8/2023 – 13/8/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Khám phá cuộc khủng hoảng gián điệp mạng kéo dài nhiều năm tại các Đại sứ quán nước ngoài ở Belarus.

- **Cảnh báo:** Các trung tâm dữ liệu có nguy cơ bị tấn công bởi nhiều lỗ hổng bảo mật trong các sản phẩm của CyberPower và Dataprobe.

2. Điểm yếu, lỗ hổng

- **871** 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: 365** 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

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Khám phá cuộc khủng hoảng gián điệp mạng kéo dài nhiều năm tại các Đại sứ quán nước ngoài ở Belarus"

Nhóm tấn công APT MoustachedBouncer hoạt động tại Belarus kể từ năm 2014, đã thực hiện cuộc tấn công nhằm vào các Đại sứ quán nước ngoài. Theo các chuyên gia bảo mật, MoustachedBouncer đã có thể thực hiện các cuộc tấn công adversary-in-the-middle (AitM) (tấn công đánh cắp thông tin) ở cấp ISP để xâm nhập vào nhiều mục tiêu trong phạm vi của Belarus.

Nhóm này được cho là có liên quan đến lợi ích của Belarus và có khả năng sử dụng hệ thống nghe lén hợp pháp như SORM để thực hiện các cuộc tấn công AitM, đồng thời triển khai các công cụ khác như NightClub và Disco. Hiện tại, vector lây nhiễm của NightClub chưa được làm rõ còn Disco lây nhiễm qua tấn công AitM.

Cả 2 framework mã độc Windows trên đều hỗ trợ các plugin gián điệp bổ sung bao gồm chức năng chụp ảnh màn hình, ghi âm, và đánh cắp tập tin. Mẫu cũ nhất của NightClub được phát hiện vào ngày 19/11/2014, khi được tải lên VirusTotal từ Ukraine.

Từ tháng 06/2017, có ít nhất 04 quốc gia có đại sứ quán được ghi nhận bị ảnh hưởng bởi chiến dịch tấn công của MoustachedBouncer. Nhóm này được cho là hợp tác cùng nhóm APT Winter Vivern (hay còn gọi là TA471/UAC-0114), đây là nhóm đã từng tấn công vào các quan chức chính phủ tại châu Âu và Hoa Kỳ.

Nhóm MoustachedBouncer tấn công mục tiêu bằng cách điều chỉnh truy cập Internet của nạn nhân ở cấp ISP để khiến Windows tin rằng thiết bị hiện đang nằm sau một Captive Portal. Đối với các dải IP bị tấn công, lưu lượng mạng bị sửa đổi tại tầng ISP và URL bị điều hướng tới một Window Update URL giả mạo.

Nhóm MoustachedBouncer tấn công bằng cách khiến nạn nhân truy cập vào trang web giả mạo, thúc đẩy cài đặt bảo mật qua một chương trình "Windows Update" tải xuống máy tính và cài đặt một nhiệm vụ tải xuống các plugin, mở rộng chức năng của Disco, bao gồm chụp ảnh màn hình, thực thi lệnh PowerShell, và cài đặt reverse proxy.

Điểm đáng chú ý của plugin là việc sử dụng giao thức Server Message Block (SMB) để thu thập và gửi dữ liệu về máy chủ điều khiển (C&C), không thể truy cập qua Internet, tạo tính bền bỉ cho hạ tầng tấn công.

Ngoài ra, trong chiến dịch tấn công vào tháng 01/2020 sử dụng dropper C# là SharpDisco để triển khai 02 plugin thông qua reverse shell, mục tiêu là liệt kê các ổ đĩa kết nối và trích xuất file.

NightClub framework còn sử dụng dropper để khởi động thành phần điều phối thu thập và gửi đi các tập tin mục tiêu bằng giao thức SMTP. Các phiên bản sau của NightClub, phát hiện vào năm 2017 và năm 2020, sử dụng keylogger, thu âm, chụp ảnh màn hình và cổng sau backdoor sử dụng DNS-tunneling.

Các nhà nghiên cứu bảo mật tin rằng NightClub được sử dụng trong trường hợp không thể chặn lưu lượng ở cấp ISP, như khi sử dụng VPN mã hóa đầu cuối để định tuyến lưu lượng mạng định tuyến ra ngoài Belarus.

Nguồn:
https://thehackernews.com/2023/08/researchers-uncover-decade-long-cyber.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Các trung tâm dữ liệu có nguy cơ bị tấn công bởi nhiều lỗ hổng bảo mật trong các sản phẩm của CyberPower và Dataprobe"

Nhiều lỗ hổng bảo mật ảnh hưởng tới phần mềm quản lý cơ sở hạ tầng trung tâm dữ liệu (DCIM) PowerPanel Enterprise của CyberPower và sản phẩm đơn vị phân phối điện (PDU) iBoot của Dataprobe. Hai nền tảng quản lý dữ liệu tập trung này có thể bị đối tượng tấn công khai thác để chiếm đoạt quyền truy cập trái phép, qua đó gây ra thiệt hại nghiêm trọng tới môi trường hệ thống.

Có tổng cộng 9 lỗ hổng đã được xác định, từ CVE-2023-3259 tới CVE-2023-3267, mức độ ảnh hưởng từ Trung bình đến Nghiêm trọng với điểm CVSS từ 6.7 tới 9.8. Các lỗ hổng này cho phép đối tượng tấn công tắt nguồn toàn bộ trung tâm dữ liệu và xâm nhập vào hệ thống để đánh cắp dữ liệu hoặc thực hiện các cuộc tấn công quy mô lớn.

Ngoài ra, chuyên gia bảo mật còn cảnh báo rằng cả hai sản phẩm trên còn bị ảnh hưởng bởi cuộc tấn công chèn mã từ xa, được tận dụng để cài một backdoor hoặc điểm truy cập tới mạng lưới của các thiết bị kết nối với trung tâm dữ liệu và hệ thống doanh nghiệp.

Phát hiện về lỗ hổng được công bố tại hội thảo DEF CON diễn ra vào ngày 12/8. Danh sách của lỗ hổng cũng đã được đề cập tới ở phiên bản 2.6.8 của phần mềm PowerPanel Enterprise và phiên bản 1.44.08042023 của phần mềm iBoot PDU.

Danh sách cụ thể của các lỗ hổng gồm có:

Dataprobe iBoot PDU:

- CVE-2023-3259 (Điểm CVSS: 9.8) – Cho phép đối tượng tấn công thực hiện tấn công Bypass.
- CVE-2023-3260 (Điểm CVSS: 7.2) – Cho phép đối tượng tấn công chèn mã vào OS dẫn tới thực thi mã từ xa.
- CVE-2023-3261 (Điểm CVSS: 7.5) – Cho phép đối tượng tấn công gây ra lỗi buffer overflow dẫn tới tấn công từ chối dịch vụ DoS.
- CVE -2023-3262 (Điểm CVSS: 6.7) – Lỗ hổng hard-coded credential
- CVE-2023-3263 (Điểm CVSS: 7.5) – Cho phép đối tượng tấn công thực hiện tấn công BypassCyberPower PowerPanel Enterprise:
- CVE-2023-3264 (Điểm CVSS 6.7) – Lỗ hổng hard-coded credential CVE-2023-3265 (Điểm CVSS 7.2) – cho phép đối tượng tấn công thực hiện tấn công Bypass
- CVE-2023-3266 (Điểm CVSS 7.5) – Cho phép đối tượng tấn công thực hiện tấn công Bypass
- CVE-2023-3267 (Điểm CVSS 7.5) – Cho phép đối tượng tấn công chèn mã vào OS dẫn tới thực thi mã từ xa.

Khai thác thành công các lỗ hổng này có thể ảnh hưởng trực tiếp tới việc triển khai hạ tầng quan trọng dựa vào trung tâm dữ liệu. Đối tượng tấn công có thể tắt hệ thống chỉ với một lần nhấn nút, tiến hành tấn công ransomware, DDoS hoặc wiper trên diện rộng cũng như thực hiện các tác vụ gián điệp mạng.

Nguồn: https://thehackernews.com/2023/08/multiple-flaws-in-cyberpower-and.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 **871** lỗ hổng, trong đó có 304 lỗ hổng mức Cao, 215 lỗ hổng mức Trung bình, 03 lỗ hổng mức Thấp và 349 lỗ hổng chưa đánh giá. Trong đó có ít nhất 130 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 74 lỗ hổng trong Microsoft, Nhóm 04 lỗ hổng trong Linux, Nhóm 38 lỗ hổng trong Google, Nhóm 77 lỗ hổng trong Wordpress, Nhóm 15 lỗ hổng trong Zoom, Nhóm 51 lỗ hổng trong Apache, Nhóm 03 lỗ hổng trong Cisco. 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-2023-21709, CVE-2023-35385,...

- Linux: CVE-2023-4128, CVE-2023-4147,...

- Google: CVE-2023-33913, CVE-2023-20783,...

- Wordpress: CVE-2023-3452, CVE-2023-2843,...

- Zoom: CVE-2023-36534, CVE-2023-39216,...

- Apache: CVE-2023-39508, CVE-2023-37581,...

- Cisco: CVE-2020-26064, CVE-2020-26065,...

Thông tin điểm yếu, lỗ hổng

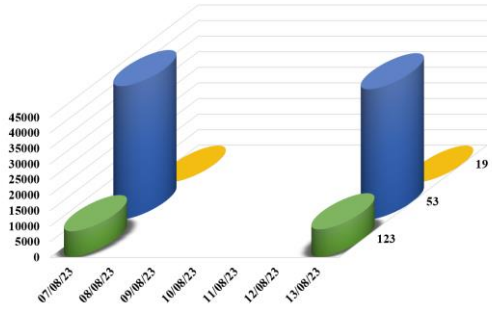
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-21709 CVE-2023-35385 CVE-2023-36903 …	Nhóm 74 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, thực hiện lỗi Spoofing, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-4128 CVE-2023-4147 CVE-2023-4194 ….	Nhóm 04 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-33913 CVE-2023-20783 CVE-2023-20784 …	Nhóm 38 lỗ hổng trong Google cho phép đối tượng tấn công thực hiện leo thang đặc quyền, 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
4	Wordpress	CVE-2023-3452 CVE-2023-2843 CVE-2023-4140 …	Nhóm 77 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công chèn SQL, tấn công CSRF, thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Zoom	CVE-2023-36534 CVE-2023-39216 CVE-2023-36541 …	Nhóm 15 lỗ hổng trong Zoom cho phép đối tượng tấn công thực hiện leo thang đặc quyền, 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
6	Apache	CVE-2023-39508 CVE-2023-37581 CVE-2022-47185 …	Nhóm 05 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
7	Cisco	CVE-2020-26064 CVE-2020-26065 CVE-2020-26082	Nhóm 03 lỗ hổng trong Cisco phép đối tượng tấn công thực thi mã tùy ý, 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

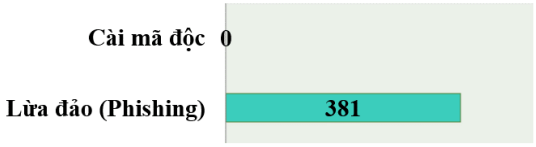
Tấn công DRDoS

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 **50.652**, (giảm so với tuần trước **51.022**) 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

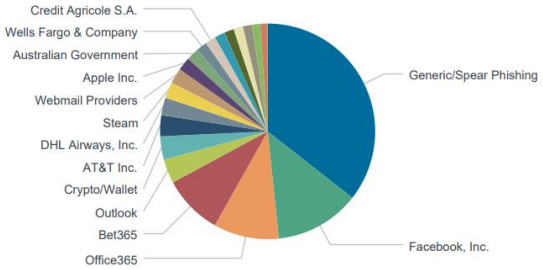


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 381 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 381 trường hợp tấn công lừa đảo (Phishing), 0 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: 7422 IP	xjpakmdcfuqe.ru: 18 IP
disorderstatus.ru: 1569 IP	xjpakmdcfuqe.in: 21 IP
atomictrivia.ru: 745 IP	restlesz.su: 185 IP
xjpakmdcfuqe.biz: 124 IP	amnsreiuojy.ru: 217 IP
xjpakmdcfuqe.com: 27 IP	hzmksreiuojy.ru: 39 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **365** 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	Ymx33.com	Website giả mạo Amazon
2	shopelpie.com bb9998.com h5.50db8hsdoq.shop	Website giả mạo sàn TMĐT Shopee
3	eulo99.com fhef11.com eulo11.com	Website giả mạo sàn TMĐT Tiki
4	nouespaipenedes.com	Website giả mạo MXH Facebook
5	dichvucongbaohiemxahoi.com dangkyhosotructuyen2023.com handico.vaytienmat-nhanh24h.com m.vnsc-finhay.com …	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