NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 31 (31/7/2023 – 06/8/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Patchwork sử dụng backdoor Eyeshell nhằm vào các tổ chức tại Trung Quốc.

- **Cảnh báo:** Phát hiện 11 LOLBAS binary được sử dụng cho mục đích gây hại.

2. Điểm yếu, lỗ hổng

- **530** 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: 376** 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: Nhóm tấn công APT Patchwork sử dụng backdoor Eyeshell nhằm vào các tổ chức tại Trung Quốc"

Theo thông tin từ các chuyên gia bảo mật, nhóm APT Patchwork đã bị phát hiện đang thực hiện một chiến dịch tấn công nhằm vào các trường đại học và tổ chức nghiên cứu tại Trung Quốc bằng cách sử dụng backdoor có tên là EyeShell.

Patchwork, hay còn gọi là Operation Hangover hoặc Zinc Emerson, bị nghi ngờ là có liên quan đến Ấn Độ. Nhóm này đã bắt đầu hoạt động từ tháng 12 năm 2015, thường tập trung tấn công vào Pakistan và Trung Quốc bằng các phương thức như Spear-phishing và Watering hole, sử dụng các mã độc tự viết như BADNEWS.

Chiến thuật tấn công được sử dụng bởi Patchwork có những điểm chung với các nhóm tấn công khác tới từ Ấn Độ như SideWinder hay DoNot Team.

Vào tháng 5 năm 2023, công ty Meta đã thông báo về việc khóa 50 tài khoản trên Facebook và Instagram được sử dụng bởi nhóm Patchwork. Các tài khoản này sử dụng một số ứng dụng tin nhắn giả mạo được tải lên Google Play Store để thu thập dữ liệu từ nạn nhân tại Pakistan, Ấn Độ, Bangladesh, Sri Lanka, Tibet và Trung Quốc. Những ứng dụng này thu thập dữ liệu người dùng thông qua các quyền ứng dụng hợp pháp mà người dùng đã cấp phép trên điện thoại cá nhân.

Chuyên gia bảo mật cũng cho biết một số hoạt động của nhóm đã được báo cáo dưới tên ModifiedElephant, một chiến dịch tấn công nhằm vào các nhà hoạt động nhân quyền, luật sư và giảng viên, học viên tại Ấn Độ để tiến hành giám sát dài hạn và cài vào các "chứng cứ buộc tội kỹ thuật số" liên quan tới vụ bạo lực Bhima Koregaon vào năm 2018.

Backdoor EyeShell cùng với BADNEWS là một loại backdoor được viết bằng .NET có khả năng thiết lập kết nối với máy chủ C&C và thực thi các câu lệnh để liệt kê file và thư mục, tải xuống hoặc tải lên các file và thực thi, xóa file trên thiết bị, cũng như chụp lại màn hình.

Mã độc EyeShellcùng với BADNEWS, là một backdoor được viết bằng .NET với khả năng thiết lập kết nối tới máy chủ C&C và thực thi các câu lệnh để liệt kê file, thư mục; tải và đăng lên các file; và thực thi, xóa file trên thiết bị cũng như là chụp lại màn hình.

Những phát hiện này được chỉ ra trong công bố chi tiết của chiến dịch tấn công phishing được thực hiện bởi nhóm tấn công Bitter, nhằm vào ngành hàng không vũ trụ, quân sự, doanh nghiệp lớn, các cơ quan chính phủ và trường đại học tại Bangladesh với mã độc ORPCBackdoor.

Trước đó, nhóm tấn công Patchwork cũng đã bị phát hiện trong việc tấn công vào ngành năng lượng hạt nhân tại Trung Quốc với các công cụ tải mã độc được phát tán qua các file CHM và Microsoft Excel, được thiết kế để duy trì kết nối và thu thập thêm các ứng dụng độc hại.

Nguồn:
https://thehackernews.com/2023/07/patchwork-hackers-target-chinese.html?&webview=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện 11 LOLBAS binary được sử dụng cho mục đích gây hại"

Các chuyên gia bảo mật đã phát hiện một bộ 11 living-off-the-land binaries-and-scripts (LOLBAS) một hình thức tấn công sử dụng binary và script có sẵn trong hệ thống vào các mục đích độc hại có thể bị sử dụng bởi đối tượng tấn công để thực hiện tác vụ hậu khai thác.

Trong 11 LOLBAS được phát hiện gồm có 9 bộ tải LOLBAS và 3 bộ thực thi cho phép đối tượng tấn công tải xuống các dạng mã độc phức tạp hơn và thực thi chúng như một phần của cây tiến trình hợp pháp trong hệ thống.

Cụ thể hơn là các tiến trình: *MsoHtmEd.exe, Mspub.exe, ProtocolHandler.exe, ConfigSecurityPolicy.exe, InstallUtil.exe, Mshta.exe, Presentationhost.exe, Outlook.exe, MSAccess.exe, scp.exe, và sftp.exe*.

Ngoài ra, đối tượng tấn công còn có thể sử dụng các file thực thi từ những phần mềm không phải của Microsoft để đạt được mục tiêu của mình.

Phát hiện được đưa ra sau khi một công ty bảo mật công bố khả năng tồn tại một vector tấn công mới lợi dụng chức năng đồng bộ người dùng chéo (cross-tenant synchronization – CTS) của Microsoft Entra ID (tên cũ - Azure Active Directory) để tiến hành leo thang đặc quyền tới các người dùng khác trong trường hợp một người dùng trên môi trường đám mây của dịch vụ bị xâm nhập. Ngoài ra, đối tượng tấn công còn có thể sử dụng tài khoản bị xâm nhập của người dùng cho việc triển khai cấu hình Cross Tenant Access để duy trì kết nối.

Nguồn: https://thehackernews.com/2023/08/lolbas-in-wild-11-living-off-land.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 **530** lỗ hổng, trong đó có 149 lỗ hổng mức Cao, 140 lỗ hổng mức Trung bình, 04 lỗ hổng mức Thấp và 237 lỗ hổng chưa đánh giá. Trong đó có ít nhất 73 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 16 lỗ hổng trong Apple, Nhóm 06 lỗ hổng trong Linux, Nhóm 60 lỗ hổng trong Google, Nhóm 22 lỗ hổng trong Wordpress, Nhóm 14 lỗ hổng trong Mozilla, 01 lỗ hổng trong TP-LINK, Nhóm 08 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:

- Apple: CVE-2023-34425, CVE-2023-36495,...

- Linux: CVE-2023-4004, CVE-2023-4010,...

- Google: CVE-2022-4920, CVE-2022-4924,...

- Wordpress: CVE-2023-4141, CVE-2023-4142,...

- Mozilla: CVE-2023-4056, CVE-2023-4057,...

- TP-LINK: CVE-2023-31710

- IBM: CVE-2023-35019, CVE-2022-43831,...

Thông tin điểm yếu, lỗ hổng

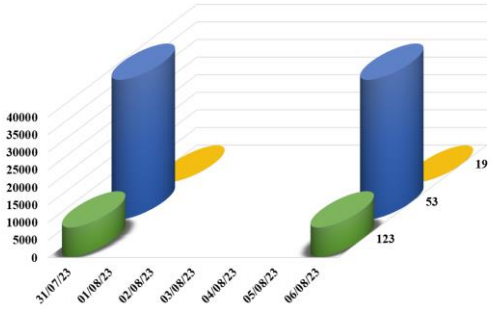
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apple	CVE-2023-34425 CVE-2023-36495 CVE-2023-37285 …	Nhóm 16 lỗ hổng trong Apple cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-4004 CVE-2023-4010 CVE-2023-39346 …	Nhóm 06 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, 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-2022-4920 CVE-2022-4924 CVE-2021-4318 …	Nhóm 60 lỗ hổng trong Google 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
4	Wordpress	CVE-2023-4141 CVE-2023-4142 CVE-2023-4139 …	Nhóm 22 lỗ hổng trong Wordpress cho phép đối tượng tấn công 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	Mozilla	CVE-2023-4056 CVE-2023-4057 CVE-2023-4058	Nhóm 14 lỗ hổng trong Mozilla 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
6	TP-LINK	CVE-2023-31710	01 lỗ hổng trong TP-LINK cho phép đối tượng tấn công thực hiện tấn công Buffer Overflow.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-35019 CVE-2022-43831 CVE-2023-24971 …	Nhóm 08 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

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

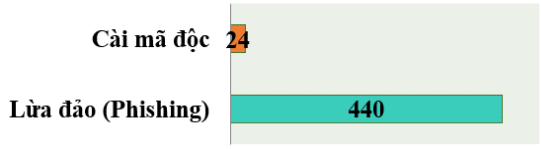
Tấn công DRDoS

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 **51.022**, (tăng so với tuần trước **48.145**) 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

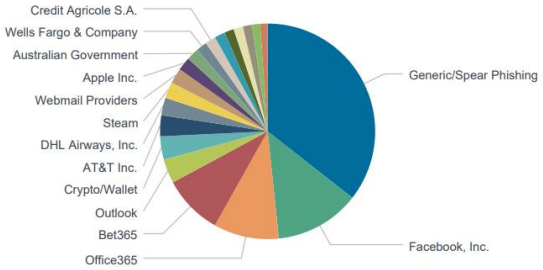


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 464 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 440 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: 11928 IP	xjpakmdcfuqe.ru: 49 IP
disorderstatus.ru: 3129 IP	xjpakmdcfuqe.in: 34 IP
atomictrivia.ru: 1503 IP	restlesz.su: 300 IP
xjpakmdcfuqe.biz: 248 IP	amnsreiuojy.ru: 443 IP
xjpakmdcfuqe.com: 66 IP	hzmksreiuojy.ru: 59 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **376**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	napvidientu.fun shopehltd.com	Website giả Ví điện tử Momo
2	tomo5963.vip	Website giả mạo sàn TMĐT Shopee
3	amg187098.com	Website giả mạo sàn TMĐT Lazada
4	tadcqv.com tadccc.com tadcaz.com	Website giả mạo sàn TMĐT Tiki
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 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