NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 35 (28/8/2023 –03/9/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Earth Estries triển khai chiến dịch tấn công nhằm vào chính phủ và các công ty công nghệ lớn trên toàn cầu.

- **Cảnh báo:** Đối tượng tấn công mạng Việt Nam sử dụng Malversting nhằm vào tài khoản doanh nghiệp trên Facebook.

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: 378** 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 APT Earth Estries triển khai chiến dịch tấn công nhằm vào chính phủ và các công ty công nghệ lớn trên toàn cầu"

Nhóm APT Earth Estries đang thực hiện một chiến dịch gián điệp mạng nhằm vào chính phủ và các công ty công nghệ lớn tại nhiều quốc gia như: Philippines, Đài Loan, Malaysia, Nam Phi, Đức và Mỹ.

Nhóm Earth Estrie bắt đầu hoạt động kể từ năm 2020 và sử dụng chiến thuật tấn công tương tự với nhóm FamousSparrow. Nhóm FamousSparrow đã bị phát hiện bởi ESET vào năm 2021 khi họ khai thác lỗ hổng ProxyLogon trên Microsoft Exchange Server để xâm nhập vào chính phủ, các ngành dịch vụ khách sạn, kỹ sư và pháp lý.

Đáng chú ý là những điểm tương đồng này cũng đã được phát hiện giữa FamousSparrow và UNC4841, một nhóm tấn công chưa được xác định, hiện đang khai thác lỗ hổng zero-day trong các thiết bị Barracuda Networks Email Security Gateway (ESG).

Theo các chuyên gia bảo mật, nhóm Earth Estries sử dụng Cobalt Strike để tiến hành các tác vụ sau khi xâm nhập thành công vào môi trường hệ thống, sau đó tiến hành triển khai thêm mã độc và mở rộng phạm vi xâm nhập trong hệ thống mạng.

Nhóm tấn công được ghi nhận đang triển khai một số backdoor và công cụ tấn công ba gồm cả bộ đánh cắp dữ liệu trình duyệt và các công cụ quét cổng nhằm nâng cao khả năng thu thập dữ liệu trong chiến dịch. Một trong số công cụ gồm có:

- PlugX;
- Zingdoor: Một mã độc dựa trên Go nhằm thu thập thông tin hệ thống, liệt kê và quản lý các file; thực thi câu lệnh từ xa;
- TrillClient: Một công cụ đánh cắp dữ liệu viết bằng Go và có nhiệm vụ thu thập dữ liệu từ trình duyệt;
- HemiGate: Đây là một backdoor có khả năng lưu trữ dữ liệu được nhập từ bàn phím, chụp màn hình, thực hiện và theo dõi quá trình các tác vụ trên file.

Nhóm tấn công đã xâm nhập vào các máy chủ nội bộ và sử dụng tài khoản hợp lệ trong hệ thống để tiến hành di chuyển trong mạng của mục tiêu, từ đó thực hiện các hành động độc hại một cách lén lút.

Để tránh bị phát hiện, Earth Estries thường xuyên cài đặt lại các backdoor trên các thiết bị đã bị nhiễm mã độc. Đây là một minh chứng cho động cơ gián điệp của Earth Estries. Dựa trên phân tích của các chuyên gia bảo mật, nhóm Earth Estries phụ thuộc phần lớn vào DLL side-loading để tải các công cụ và tránh để lại dấu vết. Nhóm này cũng sử dụng tấn công PowerShell hạ cấp để tránh bị phát hiện bởi cơ chế ghi log của Windows Antimalware Scan Interface (AMSI).

Một điều đáng chú ý khác trong quá trình hoạt động của nhóm tấn công này là việc lợi dụng các dịch vụ công cộng như Github, Gmail, AnonFiles và File.io để trao đổi hoặc truyền câu lệnh và dữ liệu đã bị đánh cắp. Phần lớn máy chủ C&C của nhóm tấn công được đặt tại Mỹ, Ấn Độ, Úc, Canada, Trung Quốc, Nhật Bản, Phần Lan, Nam Phi và Anh.

Nguồn: https://thehackernews.com/2023/08/earth-estries-espionage-campaign.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Đối tượng tấn công mạng Việt Nam sử dụng Malversting nhằm vào tài khoản doanh nghiệp trên Facebook"

Một số đối tượng tấn công mạng tại Việt Nam đang sử dụng quảng cáo trên các nền tảng mạng xã hội như Facebook để phát tán mã độc. Các cuộc tấn công này chủ yếu nhắm vào tài khoản Facebook và Meta Business và đã trở nên phổ biến gần đây, với sự tham gia của các nhóm nổi tiếng như Ducktail và NodeStealer trong việc tấn công cá nhân và doanh nghiệp trên Facebook.

Các đối tượng tấn công đã sử dụng hàng loạt các phương thức truy cập trái phép vào tài khoản của người dùng, trong đó nổi bật nhất là hình thức Social engineering. Người dùng bị tiếp cận thông qua nhiều nền tảng khác nhau như Facebook, LinkedIn, WhatsApp hoặc các cổng công việc cho người làm tự do như Upwork. Ngoài ra, các đối tượng này đã sử dụng "Search Engine Poisoning" để làm tăng khả năng tiếp cận thông qua việc phân phối các phần mềm giả mạo của các ứng dụng CapCut, Notepadd++, OpenAI ChatGPT, Google Bard, và Meta Threads.

Đối tượng tấn công thường lợi dụng dịch vụ rút gọn URL, sử dụng Telegram làm máy chủ C&C và sử dụng các dịch vụ lưu trữ đám mây như Trello, Discord, Dropbox, iCloud, OneDrive và MediaFire để lưu trữ mã độc.

Ví dụ, nhóm tấn công Ducktail sử dụng chiến dịch giả mạo về thương hiệu để tiếp cận cá nhân và doanh nghiệp trên nền tảng Meta Business. Trong cuộc tấn công này, người dùng bị hướng đến những bài đăng giả trên Upwork và Freelancer thông qua quảng cáo trên Facebook hoặc LinkedIn InMail. Những bài đăng này chứa một tệp mô tả công việc có chứa mã độc được lưu trữ trên dịch vụ đám mây. Qua đó, Ducktail đã sử dụng các mã độc này để đánh cắp session cookie từ trình duyệt và chiếm đoạt tài khoản doanh nghiệp Facebook. Những tài khoản này sau đó bị giao bán trên chợ đen với giá dao động từ 15$ tới 340$.

Các cuộc tấn công gần đây đã sử dụng các tệp shortcut và PowerShell để tải và thực thi mã độc. Các đối tượng tấn công cũng đã nâng cấp mã độc để thu thập thông tin cá nhân từ Twitter, TikTok Business và Google Ads, cũng như sử dụng các cookie Facebook bị đánh cắp trước đó để tạo quảng cáo lừa đảo và thực hiện leo thang đặc quyền nhằm phục vụ mục đích khác.

Đối tượng tấn công thường chiếm đoạt tài khoản bằng cách thêm địa chỉ email của mình vào tài khoản nạn nhân, sau đó thay đổi mật khẩu và địa chỉ email để khóa nạn nhân không thể truy cập vào tài khoản của họ. Hơn nữa, phần cuối của payload được ẩn đi bằng cách sử dụng loader để giải mã và thực thi một cách linh hoạt, nhằm tạo ra sự khó khăn trong việc kiểm tra và tránh bị phát hiện.

Ngoài ra, các đối tượng tấn công tại Việt Nam còn sử dụng tên người dùng có lượt theo dõi cao trên LinkedIn để tiếp cận mục tiêu và mở rộng phạm vi tiếp cận. Ducktail là một trong những đối tượng tấn công tại Việt Nam sử dụng các công cụ và chiến thuật chung để thực hiện các cuộc tấn công lừa đảo. Ngoài ra, còn có một phiên bản giả mạo của Ducktail được gọi là Duckport, cũng thực hiện đánh cắp dữ liệu và chiếm đoạt tài khoản trên Meta Business. Điều này cho thấy mối quan hệ giữa các đối tượng tấn công và việc chia sẻ công cụ và chiến thuật giữa các nhóm đe dọa hoặc hệ sinh thái tội phạm mạng Việt Nam đang phục vụ dịch vụ xã hội như Facebook.

Có hai nhóm tấn công mạng có liên quan đến Việt Nam là Ducktail và Duckport, đã sử dụng các công cụ và chiến thuật tương tự để thực hiện các cuộc tấn công lừa đảo trên nền tảng Meta Business và Facebook. Tuy Duckport bắt chước cách thức tấn công của Ducktail nhưng cũng sử dụng một số tính năng mới như mở rộng khả năng đánh cắp dữ liệu, chiếm đoạt tài khoản, có thể chụp ảnh hoặc sử dụng dịch vụ ghi chép note online trong chuỗi C&C, qua đó thay thế Telegram làm phương thức chuyển câu lệnh tới thiết bị nạn nhân.

Các chuyên gia bảo mật cho rằng sự trùng hợp giữa các yếu tố liên quan đến Việt Nam, cấu trúc hạ tầng và mục tiêu lựa chọn có thể là dấu hiệu cho thấy sự hợp tác giữa các nhóm tấn công hoặc hình thành một hệ sinh thái tội phạm mạng tại Việt Nam, tương tự như một mô hình dịch vụ tổng tiền xoay quanh các nền tảng mạng xã hội như Facebook.

Nguồn: https://thehackernews.com/2023/09/vietnamese-cybercriminals-targeting.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 180 lỗ hổng mức Cao, 217 lỗ hổng mức Trung bình, 06 lỗ hổng mức Thấp và 127 lỗ hổng chưa đánh giá. Trong đó có ít nhất 107 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 01 lỗ hổng trong Microsoft, Nhóm 31 lỗ hổng trong Tenda, Nhóm 04 lỗ hổng trong Google, Nhóm 109 lỗ hổng trong Wordpress, Nhóm 08 lỗ hổng trong Splunk, Nhóm 12 lỗ hổng trong Gitlab, Nhóm 17 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:

- Microsoft: CVE-2023-3674.

- Tenda: CVE-2023-40799, CVE-2023-40837,...

- Google: CVE-2019-13690, CVE-2022-4452,...

- Wordpress: CVE-2023-3162, CVE-2023-4596,...

- Splunk: CVE-2023-40595, CVE-2023-40596,..

- Gitlab: CVE-2023-3915, CVE-2023-3205,..

- IBM: CVE-2023-26270, CVE-2022-43907,...

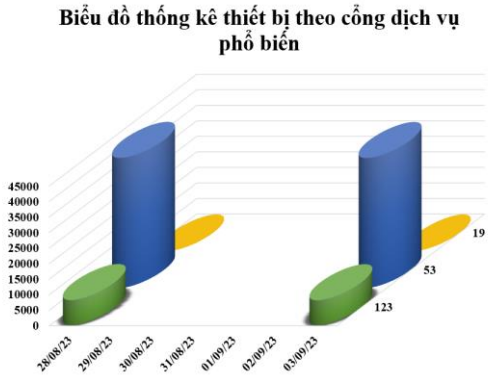
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-36741	Nhóm 01 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
2	Tenda	CVE-2023-40799 CVE-2023-40837 CVE-2023-40838 ...	Nhóm 31 lỗ hổng trong Tenda cho phép đối tượng tấn công thực hiện lỗi Buffer Overflow, thực thi mã từ xa, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2019-13690 CVE-2022-4452 CVE-2023-4572 ...	Nhóm 04 lỗ hổng trong Google 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
4	Wordpress	CVE-2023-3162 CVE-2023-4596 CVE-2023-2229 ...	Nhóm 109 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã từ xa, tấn công CSRF, khai thác lỗi XSS.	Đã có thông tin xác nhận và bản vá
5	Splunk	CVE-2023-40595 CVE-2023-40596 CVE-2023-40597 ...	Nhóm 08 lỗ hổng trong Splunk cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, khai thác lỗi XSS.	Chưa có thông tin xác nhận và bản vá
6	Gitlab	CVE-2023-3915 CVE-2023-3205 CVE-2023-3210 ...	Nhóm 12 lỗ hổng trong Gitlab cho phép đối tượng tấn công thực hiện leo thang đặc quyền, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-26270 CVE-2022-43907 CVE-2023-22877 ...	Nhóm 17 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công SQL Injection, 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 **49.923**, (giảm so với tuần trước **50.012**) 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.

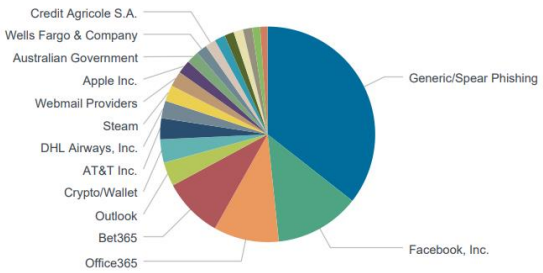


Tấn công Web

Trong tuần, có **139** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 133 trường hợp tấn công lừa đảo (Phishing), 06 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: 8856 IP	xjpakmdcfuqe.ru: 66 IP
disorderstatus.ru: 3322 IP	xjpakmdcfuqe.in: 65 IP
atomictrivia.ru: 1548 IP	restlesz.su: 267 IP
xjpakmdcfuqe.biz: 136 IP	amnsreiuojy.ru: 386 IP
xjpakmdcfuqe.com: 94 IP	hzmksreiuojy.ru: 29 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **378** 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	shoopency.com vn6315shp.com	Website giả mạo sàn TMĐT Shopee
2	vpbank.appvest.vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
3	dmxprovip.com	Website giả mạo Điện máy xanh

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