NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 44 (30/10/2023 – 05/11/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm Muddy Water của Iran thực hiện chiến dịch tấn công Spear-phishing nhằm vào Israel.

- **Cảnh báo:** Tài khoản Facebook Business có thể bị đánh cắp bởi mã độc NodeStealer.

2. Điểm yếu, lỗ hổng

- **720** 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: 358** 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 Muddy Water của Iran thực hiện chiến dịch tấn công Spear-phishing nhằm vào Israel"

Nhóm APT Muddy Water từ Iran đã được gán với một chiến dịch tấn công Spear-phishing nhằm vào hai đối tượng người Israel để triển khai một công cụ quản trị hợp pháp từ xa đến từ N-able có tên gọi Advanced Monitoring Agent.

Chi tiết của chiến dịch được ghi nhận là có sự cập nhật về TTPs đã được tìm thấy trong hoạt động trước đó của nhóm MuddyWater, sử dụng chuỗi tấn công tương tự để phát tán các công cụ truy cập từ xa khác như ScreenConnect, RemoteUtilites, Syncro và SimpleHelp.

Tuy đây là lần đầu ghi nhận việc sử dụng phần mềm giám sát từ xa của N-able bởi MuddyWater, phát hiện từ chuyên gia cũng chỉ ra thực tế rằng phương thức hoạt động gần như không thay đổi này vẫn mang lại thành công cho các chiến dịch do nhóm đối tượng thực hiện.

MuddyWater là một nhóm gián điệp không gian mạng hoạt động từ năm 2017 và được hậu thuẫn bởi chính phủ Iran, giống với OilRig, Lyceum, Agrius hay Scarred Manticore.

Các chuỗi tấn công trước đó của nhóm sử dụng hình thức gửi đi email Spear-phishing chứa đường dẫn trực tiếp hoặc đính kèm file HTML, PDF và RTF có chứa đường dẫn tới các trang lưu trữ của nhiều nền tảng khác nhau, tất cả với mục đích phát tán một trong các công cụ quản trị từ xa.

Chiến thuật và công cụ mới nhất được sử dụng là biểu tượng cho sự tiếp diễn, hoặc là một sự tiến hóa của nhóm Mango Sandstorm và Static Kitten. Điểm khác biệt trong chiến dịch này là việc sử dụng dịch vụ chia sẻ file Storyblok để bắt đầu vector lây nhiễm đa giai đoạn.

Cụ thể hơn, trong đường dẫn có chứa các file ẩn, một file LNK khởi động quá trình lây nhiễm, và một file thực thi được thiết kế để bỏ ẩn file văn bản mồi nhử trong lúc thực thi công cụ Advanced Monitoring Agent. Sau khi người dùng bị lây nhiễm bởi mã độc, MuddyWater sẽ kết nối tới thiết bị sử dụng công cụ quản trị hợp pháp nhằm tìm kiếm thông tin của người dùng.

File văn bản mồi nhử này là một bản ghi chép chính thức từ Ủy ban Dịch vụ Dân sự Israel, có thể được tải trên trang web chính thức của tổ chức.

Ngoài ra, một dấu hiệu nữa cho thấy khả năng phát triển nhanh chóng nhóm MuddyWater là việc đang tận dụng một framework C&C mới có tên gọi MuddyC2Go, phiên bản kế nhiệm của MuddyC3 và PhonyC2.

Nguồn: https://thehackernews.com/2023/11/irans-muddywater-targets-israel-in-new.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Tài khoản Facebook Business có thể bị đánh cắp bởi mã độc NodeStealer"

Một loại mã độc mới đang gây sóng gió trên Facebook, khi nó có thể lấy cắp thông tin đăng nhập và cookies của người dùng trên trình duyệt. Mã độc này được phát tán qua các quảng cáo có hình ảnh gợi cảm, do các tài khoản Facebook doanh nghiệp bị chiếm quyền kiểm soát.

Mã độc này có tên là NodeStealer, được viết bằng .NET và JavaScript. NodeStealer được cài cắm trong một file .exe có tên "Photo Album" để đánh lừa người dùng tải xuống và nghĩ rằng đây là một bộ sưu tập ảnh gợi cảm. Khi người dùng tải về và mở file này, một file khác sẽ được cài đặt ngầm để thực hiện việc đánh cắp dữ liệu.

NodeStealer được Meta phát hiện lần đầu vào tháng 05/2023, khi nó chỉ là một đoạn mã JavaScript nhỏ. Sau đó, nhóm tấn công đã nâng cấp mã độc và sử dụng biến thể Python trong các cuộc tấn công mới.

Mã độc này là một ví dụ về sự phát triển của hệ sinh thái tấn công mạng tại Việt Nam. Các đối tượng tấn công mạng tại Việt Nam thường sử dụng các phương thức tương tự nhau và chủ yếu dùng Facebook làm kênh để lan truyền mã độc.

Hiện nay, các chiến dịch tấn công mới nhất vẫn phát tán mã độc bằng cách sử dụng các quảng cáo độc hại trên Facebook để chiếm quyền truy cập vào tài khoản của người dùng. Những quảng cáo này được đăng từ các tài khoản Facebook bị đánh cắp trước đó, sử dụng công cụ Ads Manager của Meta. Nạn nhân chủ yếu là nam giới có độ tuổi từ 18 tới 65 ở Châu Âu, Châu Phi và vùng Caribe, đặc biệt là những người trên 45 tuổi.

Các đối tượng tấn công dùng file thực thi giả làm album ảnh để lây nhiễm mã độc cho người dùng Facebook. Sau đó, đối tượng tấn công dùng các cookie bị đánh cắp để vượt qua xác thực hai bước và đổi mật khẩu, khiến người dùng không thể đăng nhập lại vào tài khoản của mình.

Chiến dịch này được phát hiện trong bối cảnh có nhiều vụ lừa đảo khác nhau nhằm vào người chơi Roblox và người giao dịch bất động sản tại Trung Đông. Các đối tượng tấn công thường thu thập thông tin đăng nhập và tiền tệ trong trò chơi của người chơi Roblox bằng cách dùng các đường dẫn lừa đảo. Hơn 3.500 domain giả mạo đã bị phát hiện trong những chiến dịch lừa đảo trực tuyến này, chủ yếu là để thu thập thông tin về người giao dịch bất động sản tại Trung Đông và bán trên diễn đàn đen.

Nguồn: https://thehackernews.com/2023/11/nodestealer-malware-hijacking-facebook.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 **720** lỗ hổng, trong đó có 77 lỗ hổng mức Cao, 67 lỗ hổng mức Trung bình, 10 lỗ hổng mức Thấp và 566 lỗ hổng chưa đánh giá. Trong đó có ít nhất 102 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 03 lỗ hổng trong Microsoft, Nhóm 32 lỗ hổng trong Cisco, Nhóm 101 lỗ hổng trong Wordpress, Nhóm 10 lỗ hổng trong Nvidia, Nhóm 137 lỗ hổng trong Google, Nhóm 07 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-2023-1192, CVE-2023-1476,...

- Microsoft: CVE-2023-36022, CVE-2023-36029,...

- Cisco: CVE-2023-20042, CVE-2023-20086,...

- Wordpress: CVE-2023-5821, CVE-2023-46153,...

- Nvidia: CVE-2023-31016, CVE-2023-31017,...

- Google: CVE-2023-21356, CVE-2023-21361,...

- IBM: CVE-2023-35896, CVE-2023-40685,...

Thông tin điểm yếu, lỗ hổng

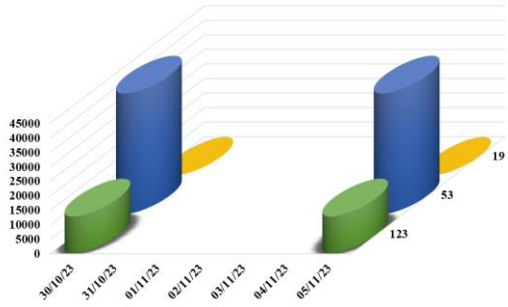
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-1192 CVE-2023-1476 CVE-2023-3397 …	Nhóm 06 lỗ hổng trong Linux cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, thực thi mã từ.	Chưa có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-36022 CVE-2023-36029 CVE-2023-36034	Nhóm 03 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Cisco	CVE-2023-20042 CVE-2023-20086 CVE-2023-20095 …	Nhóm 32 lỗ hổng trong Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thắc lỗi XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-5821 CVE-2023-46153 CVE-2023-46194 …	Nhóm 101 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi XSS, khai thác lỗi CSRF, thực hiện SQL Injection, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
5	Nvidia	CVE-2023-31016 CVE-2023-31017 CVE-2023-31019 …	Nhóm 10 lỗ hổng trong Nvidia cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, 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
6	Google	CVE-2023-21356 CVE-2023-21361 CVE-2023-40129 …	Nhóm 137 lỗ hổng trong Google cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2023-35896 CVE-2023-40685 CVE-2023-46176 …	Nhóm 07 lỗ hổng trong IBM phép đối tượng tấn công khai thác lỗi SSRF, leo thang đặc quyền, 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

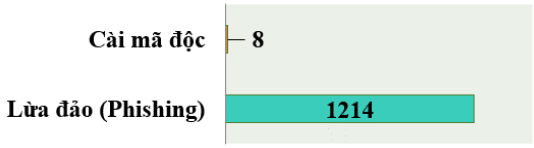
Tấn công DRDoS

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 **55.896**, (tăng so với tuần trước **54.241**) 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

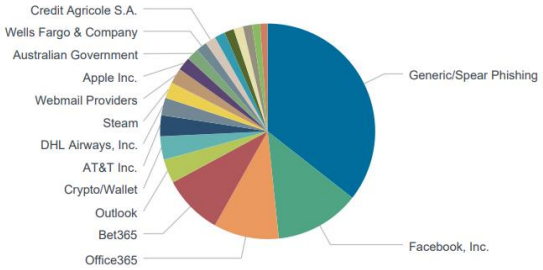


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **1222** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 1214 trường hợp tấn công lừa đảo (Phishing), 08 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: 17341 IP	hzmksreiuojy.ru: 251 IP
disorderstatus.ru: 4610 IP	xjpakmdcfuqe.biz: 279 IP
atomictrivia.ru: 2213 IP	xjpakmdcfuqe.com: 98 IP
amnsreiuojy.ru: 887 IP	xjpakmdcfuqe.ru: 53 IP
restlesz.su: 305 IP	xjpakmdcfuqe.in: 28 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **358** 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	tah2a.com tiki5688.shop kdsf11.com	Website giả mạo sàn TMĐT Tiki
2	vn55866shp.com spohopenm.org vn66733shop.com shopee.vntheme.com	Website giả mạo sàn TMĐT Shopee
3	lottefinancev.cc	Website giả mạo LOTTE
4	travelokaaaa.com	Website giả mạo Traveloka
5	vib-tindung.click	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
6	suppliersbhx.com	Website giả mạo Công ty cổ phần Thương mại Bách Hóa 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 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