NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 47(20/11/2023 – 26/11/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Mustang Panda nhằm vào chính phủ Philippines trong bối cảnh căng thẳng tại Biển Đông.

- **Cảnh báo:** Bot Telekopye trên Telegram được sử dụng bởi các đối tượng tấn công để thực hiện hành vi lừa đảo diện rộng.

2. Điểm yếu, lỗ hổng

- **474** 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: Nhóm APT Mustang Panda nhằm vào chính phủ Philippines trong bối cảnh căng thẳng tại Biển Đông"

Nhóm APT Mustang Panda là một nhóm tấn công mạng có liên quan đến Trung Quốc, được biết đến với các chiến dịch tấn công nhằm vào chính phủ Philippines giữa tình hình căng thẳng của hai quốc gia tại Biển Đông.

Trong tháng 8/2023, nhóm này đã thực hiện ba chiến dịch tấn công mạng, chủ yếu nhằm vào các tổ chức ở Nam Thái Bình Dương. Các chiến dịch tấn công này đã sử dụng một số phần mềm hợp pháp, bao gồm Solid PDF Creator và SmadavProtect (một giải pháp diệt virus có trụ sở tại Indonesia), để tải các tệp độc hại thông qua phương tiện sideloading. Đáng chú ý, nhóm tấn công đã cấu hình malware để giả mạo lưu lượng Microsoft cho các kết nối điều khiển C&C.

Mustang Panda, còn được biết đến với các tên gọi như Bronze President, Camaro Dragon, Earth Preta, RedDelta hay Stately Taurus, là một nhóm APT Trung Quốc đã hoạt động từ năm 2012. Nhóm này chính là thủ phạm của nhiều chiến dịch gián điệp mạng nhằm vào các tổ chức phi chính phủ cũng như các tổ chức chính phủ trên khắp Bắc Mỹ, Châu Âu và Châu Á.

Vào cuối tháng 09/2023, Mustang Panda bị tình nghi là thủ phạm thực hiện chiến dịch tấn công nhằm vào một chính phủ tại Đông Nam Á để phát tán mã độc backdoor TONESHELL. Trong một chiến dịch gần đây, nhóm này đã sử dụng chiến thuật spear-phishing qua email để gửi một tệp ZIP độc hại có chứa DLL giả mạo, được thực thi bởi kỹ thuật DLL side-loading. File DLL này có nhiệm vụ thiết lập kết nối tới máy chủ từ xa.

Đáng chú ý, SmadavProtect đã trở thành một chiến thuật mới được nhóm APT Mustang Panda ưa chuộng để triển khai các mã độc nhằm qua mặt các biện pháp bảo mật. Mustang Panda được đánh giá là một trong những nhóm APT Trung Quốc hoạt động mạnh mẽ, thường xuyên thực hiện các chiến dịch gián điệp mạng nhắm vào các mục tiêu liên quan đến các vấn đề chính trị.

Trong bối cảnh này, nhóm APT Hàn Quốc có tên là Higaisa đang tiến hành tấn công phishing nhằm vào người dùng Trung Quốc thông qua các trang web giả mạo các ứng dụng phổ biến như OpenVPN. Chuyên gia bảo mật cho biết chiến dịch này sử dụng một bộ cài đặt, khi được thực thi sẽ tải về mã độc viết bằng Rust xuống thiết bị rồi thực thi shellcode để chống debug và giải mã. Sau đó, shellcode này thiết lập kết nối mã hóa tới C&C với một trung tâm điều khiển từ xa.

Nguồn: https://thehackernews.com/2023/11/mustang-panda-hackers-targets.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Bot Telekopye trên Telegram được sử dụng bởi các đối tượng tấn công để thực hiện hành vi lừa đảo diện rộng"

Gần đây, một nhóm đối tượng tấn công mạng đã sử dụng bot Telegram độc hại "Telekopye" để triển khai các chiến dịch lừa đảo quy mô lớn bằng cách tạo trang web, email và tin nhắn SMS giả mạo. Nhóm tấn công mạng này có tên là Neanderthals, vận hành một doanh nghiệp lừa đảo núp bóng dưới dạng một công ty hợp pháp, tổ chức theo cấu trúc phân cấp với nhiều thành viên đảm nhận các vai trò khác nhau.

Các thành viên mới của Neanderthals được tuyển dụng thông qua quảng cáo trên diễn đàn ngầm và sau đó mời tham gia vào các kênh Telegram để liên lạc và theo dõi giao dịch. Mục tiêu chính của chiến dịch là thực hiện một trong ba hình thức lừa đảo: người bán, người mua hoặc hoàn tiền.

Trong chiến dịch lừa đảo người bán, Neanderthals giả mạo là người bán và thực hiện các giao dịch với người mua (gọi là Mammoths) cho các sản phẩm không tồn tại. Chiến dịch lừa đảo người mua liên quan đến Neanderthals giả mạo làm người mua để lừa Mammoths cung cấp thông tin tài chính của họ. Trong chiến dịch hoàn tiền, Neanderthals lừa Mammoths lần thứ hai dưới vỏ bọc của việc hoàn tiền giao dịch, sau đó trừ tiền của họ.

Telekopye hoạt động tương tự như Classiscam, một dạng lừa đảo dưới dạng dịch vụ đã thu về cho nhóm đối tượng lừa đảo tổng cộng 64,5 triệu đô kể từ khi bắt đầu hoạt động vào năm 2019.

Neanderthals lựa chọn Mammoths cho chiến dịch lừa đảo người mua dựa trên nhiều yếu tố như giới tính, độ tuổi, kinh nghiệm trên thị trường trực tuyến, đánh giá, số lượng giao dịch hoàn thành và loại hàng hóa họ bán. Họ cũng sử dụng bộ quét web để lựa chọn Mammoth lý tưởng. Trong trường hợp Mammoth muốn thanh toán trực tiếp và giao hàng tận nơi, Neanderthals sẽ đưa ra lý do là mình ở quá xa hoặc phải đi công tác, đồng thời nâng cao mong muốn mua sản phẩm để người bán rơi vào bẫy theo ý của đối tượng.

Neanderthals còn sử dụng VPN, proxy và TOR để giữ danh tính ẩn danh và thực hiện các chiến dịch lừa đảo trong lĩnh vực bất động sản, tạo trang web giả mạo với danh sách chung cư để lừa Mammoths thanh toán phí giữ chỗ. Chiến dịch này kết hợp việc giả mạo người mua, cụ thể hơn, Neanderthals giả làm một người mua tiềm năng hỏi về chung cư và yêu cầu được cung cấp các thông tin bổ sung như ảnh hay hàng xóm của căn này, sau đó các thông tin này sẽ được đối tượng sử dụng để đăng lên website giả mạo dưới hình thức cho thuê với mức giá thấp hơn so với thị trường.

Thông tin về chiến dịch lừa đảo này được công bố sau khi một vụ lừa đảo "qua cầu rút ván" (rug pull) gây thiệt hại gần 1 triệu đô khi người dùng đầu tư vào token giả và sau đó bị đối tượng lừa đảo bán hết số lượng token và rút sạch tiền.

Nguồn: https://thehackernews.com/2023/11/cybercriminals-using-telekopye-telegram.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 **474** lỗ hổng, trong đó có 70 lỗ hổng mức Cao, 39 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 364 lỗ hổng chưa đánh giá. Trong đó có ít nhất 108 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 02 lỗ hổng trong Linux, Nhóm 12 lỗ hổng trong Mozilla, 23 lỗ hổng trong Adobe, Nhóm 154 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong Apache, Nhóm 07 lỗ hổng trong Cisco, 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-2023-5972, CVE-2023-6238

- Mozilla: CVE-2023-6120, CVE-2023-6211,...

- Adobe: CVE-2023-47066, CVE-2023-47067,...

- Wordpress: CVE-2023-4214, CVE-2023-26535,...

- Apache: CVE-2023-48796, CVE-2023-43123,...

- Cisco: CVE-2023-20274, CVE-2023-20208,...

- IBM: CVE-2023-38361, CVE-2023-36777,...

Thông tin điểm yếu, lỗ hổng

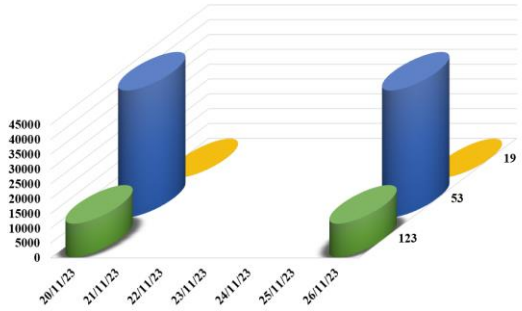
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-5972 CVE-2023-6238	Nhóm 02 lỗ hổng trong Linux cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Mozilla	CVE-2023-6210 CVE-2023-6211 CVE-2023-6213 …	Nhóm 12 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
3	Adobe	CVE-2023-47066 CVE-2023-47067 CVE-2023-47068 …	Nhóm 23 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi XSS, khai thác lỗi SQL Injection, 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
4	Wordpress	CVE-2023-4214 CVE-2023-26535 CVE-2023-47243 …	Nhóm 154 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi CSRF, khai thác lỗi XSS, khai thác lỗi SSRF, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Apache	CVE-2023-48796 CVE-2023-43123 CVE-2023-46302 …	Nhóm 05 lỗ hổng trong Apache 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	Cisco	CVE-2023-20274 CVE-2023-20208 CVE-2023-20272	Nhóm 07 lỗ hổng trong Cisco cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, kha thác lỗi XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-38361 CVE-2022-36777 CVE-2021-39008 …	Nhóm 07 lỗ hổng trong IBM phép đối tượng tấn công khai thác lỗi CSRF, 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

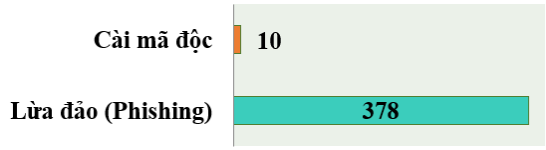
Tấn công DRDoS

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 **53.503**, (giảm so với tuần trước **54.229**) 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

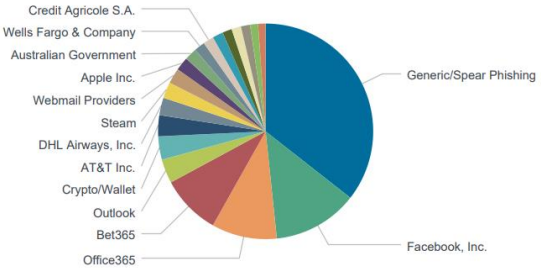


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **388** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 378 trường hợp tấn công lừa đảo (Phishing), 10 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: 10664 IP	hzmksreiuojy.ru: 232 IP
disorderstatus.ru: 5165 IP	xjpakmdcfuqe.biz: 145 IP
atomictrivia.ru: 2506 IP	xjpakmdcfuqe.com: 77 IP
amnsreiuojy.ru: 622 IP	xjpakmdcfuqe.ru: 65 IP
restlesz.su: 333 IP	xjpakmdcfuqe.in: 52 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	tikishop.ws	Website giả mạo sàn TMĐT Tiki
2	hethongbhx.com	Website giả mạo sàn Công ty cổ phần Thương mại Bách Hóa Xanh
3	looklazada.com	Website giả mạo sàn TMĐT Lazada
4	phone.didongvietstore.com	Website giả mạo Di Động Việt
5	dichvucong.tgovn.cc	Website giả mạo Dịch vụ công Quốc Gia
6	ff.memberships-garena.id.vn	Website giả mạo Công Ty Cổ Phần Giải Trí Và Thể Thao Điện Tử Việt Nam

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