NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 22 (29/5/2023 – 04/6/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Phát hiện nhóm tấn công APT Dark Pink sử dụng TelePowerBot và KamiKakaBot trong các cuộc tấn công gần đây.

- **Cảnh báo:** Chiến dịch Horabot mới đang phát tán mã độc và chiếm quyền kiểm soát tài khoản email.

2. Điểm yếu, lỗ hổng

- **668** 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: 288** 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

"Phát hiện nhóm tấn công APT Dark Pink sử dụng TelePowerBot và KamiKakaBot trong các cuộc tấn công gần đây"

Trong khoảng thời gian từ tháng 02/2022 đến tháng 4/2023, nhóm APT Dark Pink được cho là có liên quan đến 5 cuộc tấn công mạng nhằm vào các tổ chức ở Bỉ, Brunei, Indonesia, Thái Lan và Việt Nam. Các tổ chức bị tấn công bao gồm: tổ chức giáo dục, cơ quan chính phủ, cơ quan quân sự và tổ chức phi lợi nhuận.

Dark Pink (hay còn được biết đến với tên Saaiwc Group) là nhóm APT đến từ châu Á - Thái Bình Dương với các cuộc tấn công nhằm mục tiêu vào các tổ chức ở Đông Á và một vài mục tiêu ở châu Âu.

Nhóm này đã sử dụng các mã độc như TelePowerBot và KamiKakaBot nhằm đánh cắp dữ liệu nhạy cảm từ máy chủ bị xâm nhập. Dark Pink cài cắm các mã độc thông qua Spear Phishing email.

Sau khi bị cài cắm mã độc, các đối tượng tấn công sẽ có quyền truy cập vào mạng của mục tiêu, đồng thời sử dụng cơ chế duy trì nâng cao để tránh bị phát hiện. Chuỗi tấn công của Dark Pink đã cản trở quá trình phân tích của máy chủ đồng thời hỗ trợ KamiKakaBot thực thi các lệnh từ đối tượng tấn công thông qua bot Telegram.

Đặc biệt, trong phiên bản mới này chức năng của mã độc KamiKakaBot được chia thành hai phần riêng biệt: một phần có khả năng điều khiển các thiết bị và phần còn lại nhằm thu thập thông tin quan trọng. Các nhà nghiên cứu đã phát hiện ra một tài khoản GitHub được liên kết với đối tượng tấn công lưu trữ các tập lệnh PowerShell, tệp nén ZIP và mã độc. Các nội dung này được tải lên từ ngày 9/1/2023 đến ngày 11/4/2023.

Ngoài ra, Dark Pink đang lọc các dữ liệu đánh cắp qua http thông qua webhook[.]site và sử dụng Add-ins trong Excel để duy trì TelePowerBot trong máy chủ bị nhiễm mã độc.

Kể từ giữa năm 2021 đến nay, Dark Pink đã thực hiện tổng cộng 13 cuộc tấn công.

Các cá nhân, tổ chức cần thực hiện kiểm tra, rà soát hệ thống và cẩn thận trước mỗi lần nhấp chuột vào các đường liên kết hay tệp đính kèm đáng ngờ trong email.

Nguồn: https://thehackernews.com/2023/05/dark-pink-apt-group-leverages.html?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Chiến dịch Horabot mới đang phát tán mã độc và chiếm quyền kiểm soát tài khoản email"

Một chiến dịch mới liên quan đến botnet Horabot đã nhằm mục tiêu đến những người Tây Ban Nha ở Mỹ Latinh kể từ tháng 11 năm 2020 để lây nhiễm banking trojan (một phần mềm độc hại thường sử dụng để đánh cắp thông tin tài khoản ngân hàng hoặc thông tin tài chính khác) và công cụ spam thư điện tử.

Horabot cho phép đối tượng tấn công kiểm soát hộp thư Outlook của nạn nhân, lọc các địa chỉ email thường liên hệ và gửi email phishing đính kèm các HTML độc hại tới các địa chỉ email trong mailbox. Đồng thời, mã độc này còn chứa banking trojan trên Windows và một công cụ spam nữa nhằm mục đích khai thác các thông tin ngân hàng trực tuyến, các tài khoản email thuộc Gmail, Outlook hay Yahoo! để gửi email spam đến các người dùng.

Theo các nhà nghiên cứu, phần lớn người dùng bị nhiễm mã độc là người dân tại Mexico, một lượng nhỏ tại Uruguay, Brazil, Venezuela, Argentina, Guatemala và Panama. Các đối tượng thực hiện chiến dịch này được cho rằng có liên quan đến Brazil.

Các đối tượng bị chiến dịch này nhắm đến thuộc các lĩnh vực như kế toán, xây dựng và kỹ thuật, nhà phân phối và nhóm đầu tư, ngoài ra, một số lĩnh vực khác trong khu vực cũng có thể bị ảnh hưởng.

Quá trình tấn công bắt đầu bằng các email phishing chứa "mồi nhử" có nội dung liên quan đến thuế nhằm dụ nạn nhân mở các tệp đính kèm HTML mà trong đó có chứa một file RAR. Khi nạn nhân mở tệp đính kèm, script PowerShell sẽ được thực thi và tải xuống một file ZIP chứa các payload từ một máy chủ điều khiển và khởi động lại thiết bị của nạn nhân.

Việc thiết bị bị khởi động lại đóng vai trò như một bệ phóng cho banking trojan và công cụ spam, qua đó cho phép đối tượng tấn công đánh cắp các dữ liệu, ghi lại log của việc gõ phím, chụp ảnh màn hình và phân tán các email phishing khác tới các mối liên hệ của nạn nhân.

Banking trojan này là một Windows DLL 32-bit được viết bằng ngôn ngữ Delphi và có điểm chung với các nhóm mã độc khác của Brazil như Mekotio và Casbaneiro.

Horabot là một chương trình Botnet phishing trên Outlook được viết bằng Powershell với khả năng gửi đi các email phishing tới các địa chỉ email có trong mailbox của nạn nhân để phát tán.

Chiến dịch tấn công diễn ra kể từ năm 2021 nhắm vào hơn 30 tổ chức tài chính của Bồ Đào Nha với các mã độc đánh cắp thông tin.

Việc phát hiện một Banking Trojan Android mới có tên PixBankBot cho phép đối tượng tấn công tận dụng các dịch vụ trợ năng của OS để thực hiện các tác vụ chuyển tiền lừa đảo qua nền tảng thanh toán PIX của Brazil.

PixBankBot là mã độc mới nhắm vào các ngân hàng của Brazil, sở hữu các tính năng tương tự như BrasDex, PixPirate và GoatRat đã được phát hiện trong những tháng vừa qua.

Nguồn: https://thehackernews.com/2023/06/new-botnet-malware-horabot-targets.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 **668** lỗ hổng, trong đó có 144 lỗ hổng mức Cao, 97 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 426 lỗ hổng chưa đánh giá. Trong đó có ít nhất 74 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 19 lỗ hổng trong Microsoft, Nhóm 07 lỗ hổng trong Linux, Nhóm 07 lỗ hổng trong Dell, Nhóm 96 lỗ hổng trong Wordpress, Nhóm 13 lỗ hổng trong Huawei, Nhóm 03 lỗ hổng trong Samsung Galaxy Store, Nhóm 09 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-2022-35744, CVE-2022-35754,...*
- *Linux: CVE-2022-48502, CVE-2023-2598,...*
- *Dell: CVE-2023-24568, CVE-2023-28043,...*
- *Wordpress: CVE-2022-33974, CVE-2022-36345,...*
- *Huawei: CVE-2021-46887, CVE-2022-48478,...*
- *Samsung Galaxy Store: CVE-2023-21516, CVE-2023-21515,...*
- *IBM: CVE-2023-26277, CVE-2023-26278,...*

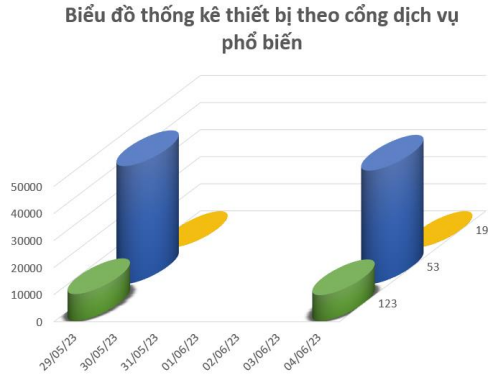
Thông tin điểm yếu, lỗ hổng

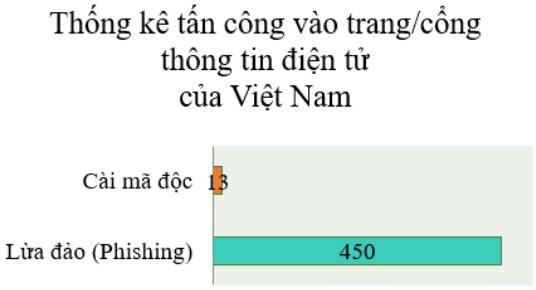
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2022-35744 CVE-2022-35754 CVE-2022-35759 ...	Nhóm 19 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, thực hiện leo thang đặc quyền, tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2022-48502 CVE-2023-2598 CVE-2023-2612 …	Nhóm 07 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	Dell	CVE-2023-24568 CVE-2023-28043 CVE-2023-28066 …	Nhóm 07 lỗ hổng trong Dell cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-33974 CVE-2022-36345 CVE-2022-45372 …	Nhóm 96 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, SQL injection, tiết lộ thông tin nhạy cảm, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Huawei	CVE-2021-46887 CVE-2022-48478 CVE-2022-48479 …	Nhóm 13 lỗ hổng trong Huawei 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	Samsung Galaxy Store	CVE-2023-21516 CVE-2023-21515 CVE-2023-21514 …	Nhóm 03 lỗ hổng trong Samsung Mobile (Galaxy Store) 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
7	IBM	CVE-2023-26277 CVE-2023-26278 CVE-2023-32342 …	Nhóm 09 lỗ hổng trong IBM phép đối tượng tấn công 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

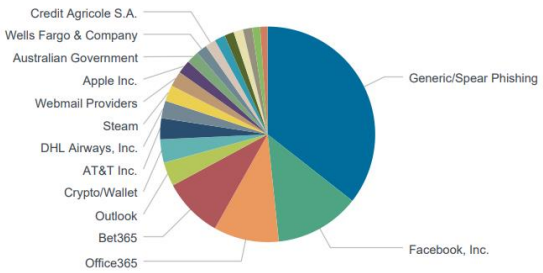
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **52.453,** (tăng so với tuần trước **51.601**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 463 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 450 trường hợp tấn công lừa đảo (Phishing), 13 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: 7613 IP	xjpakmdcfuqe.ru:89 IP
disorderstatus.ru: 3272 IP	xjpakmdcfuqe.in:131 IP
atomictrivia.ru: 1554 IP	restlesz.su: 221 IP
xjpakmdcfuqe.biz: 166 IP	amnsreiuojy.ru: 300 IP
xjpakmdcfuqe.com: 104 IP	hzmksreiuojy.ru: 48 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **288** 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	tadmak.com tadmv.com	Website giả mạo sàn TMĐT Tiki
2	shopaeon.com	Website giả mạo Công ty TNHH Aeon Việt Nam
3	tomo5933.vip	Website giả mạo sàn TMĐT Shopee

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