NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 11 (13/03/2023 – 19/03/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Banking Trojan Mispadu thực hiện đánh cắp hơn 90.000 thông tin đăng nhập nhằm vào các nước Mỹ Latinh.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Tick của Trung Quốc phát tán phần mềm độc hại nhằm thực hiện các hành động trái phép.

2. Điểm yếu, lỗ hổng

- **646** 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: 289** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Banking Trojan Mispadu thực hiện đánh cắp hơn 90.000 thông tin đăng nhập nhằm vào các nước Mỹ Latinh"

Banking Trojan có tên là Mispadu (hay còn gọi là URSA) được sử dụng trong nhiều chiến dịch thư rác nhằm mục tiêu vào những quốc gia như Bolivia, Chile, Mexico, Peru và Bồ Đào Nha đánh cắp thông tin đăng nhập và phát tán các phần mềm mã độc khác.

Hoạt động này bắt đầu từ tháng 08/2022 và vẫn tiếp tục diễn ra cho đến tháng 03/2023. Các nhà nghiên cứu cho biết, kể từ tháng 11/2019, Mispadu (URSA) bắt đầu thực hiện hành vi đánh cắp tiền và thông tin đăng nhập, đồng thời hoạt động như một backdoor bằng cách chụp ảnh màn hình và ghi lại các lần nhấn phím.

Các cuộc tấn công thường xâm nhập vào các trang web hợp pháp và tìm kiếm, các phiên bản WordPress có chứ lỗ hổng, sau đó biến chúng thành máy chủ để phát tán, lây nhiễm các loại mã độc.

Mispadu cũng có những điểm tương đồng với các banking trojan khác như Grandoreiro, Javali, và Lampion. Các cuộc tấn công liên quan đến mã độc Delphi sử dụng email thông báo hóa đơn quá hạn giả nhằm điều hướng người dùng mở chúng, từ đó kích hoạt quá trình lây nhiễm mã độc.

Nguồn:
https://thehackernews.com/2023/03/mispadu-banking-trojan-targets-latin.html

Khi người dùng mở tệp đính kèm HTML được gửi kèm qua email spam, việc xác minh tệp đã mở trên máy tính sẽ được thực hiện và chuyển hướng đến máy chủ từ xa để tải xuống phần mềm độc hại trong giai đoạn đầu của chuỗi lây nhiễm. Khi được khởi chạy, tệp RAR hoặc ZIP độc hại sử dụng các chứng chỉ số giả mạo - một là mã độc Mispadu và còn lại là công cụ AutoIT - để giải mã và thực thi trojan bằng cách lạm dụng tiện ích dòng lệnh hợp pháp certutil.

Ngoài ra, Mispadu được trang bị để thu thập danh sách các phần mềm chống vi-rút được cài đặt trên máy chủ bị xâm nhập, thu nhập thông tin đăng nhập từ Google Chrome và Microsoft Outlook, đồng thời tạo điều kiện để tải các phần mềm độc hại bổ sung, bao gồm một dropper Visual Basic Script.

Dropper được thiết kế để tải xuống một công cụ truy cập từ xa cho phép thực thi các lệnh từ máy chủ do đối tượng tấn công kiểm soát và một công cụ tải (loader) được viết bằng Rust, có khả năng thực thi tệp trực tiếp từ bộ nhớ.

Bên cạnh đó, mã độc còn sử dụng các "giao diện vô hình" (overlay screen) độc hại để đánh cắp thông tin đăng nhập liên quan đến tài khoản ngân hàng điện tử và các thông tin nhạy cảm khác.

Phương pháp certutil đã cho phép Mispadu vượt qua sự phát hiện của nhiều phần mềm bảo mật và thu thập hơn 90.000 thông tin xác thực tài khoản ngân hàng từ 17.500 trang web. Để tránh trở thành nạn nhân của các cuộc tấn công mạng, người dùng nên kiểm tra cẩn thận trước khi mở email từ các nguồn lạ, không nhấp vào các liên kết lạ được đính kèm trong email và không tải xuống tệp từ những nguồn không đáng tin cậy, đồng thời bật phần mềm phòng chống mã độc trên thiết bị của mình để kịp thời phát hiện và ngăn chặn các cuộc tấn công.

Tin tức An toàn thông tin

"Cảnh báo: Nhóm tấn công APT Tick của Trung Quốc phát tán phần mềm độc hại nhằm thực hiện các hành động trái phép"

Vừa qua, nhóm tấn công APT Tick của Trung Quốc hay còn được biết đến với những cái tên như Bronze Butler, REDBALDKNIGHT, Stalker Panda, và Stalker Taurus đã nhằm mục tiêu vào một công ty ở Đông Á đang phát triển phần mềm Data-Loss Prevention (DLP). Nhóm tấn công đã xâm nhập các máy chủ của công ty nhằm phân phối phần mềm độc hại để truy cập, thực hiện các hành động trái phép.

Theo các nhà nghiên cứu, nhóm tấn công này đã khai thác lỗ hổng ProxyLogon để xâm nhập vào công ty trong lĩnh vực công nghệ thông tin của Hàn Quốc kể từ đầu năm 2021. Ngoài ra, nhóm cũng có được quyền truy cập vào mạng nội bộ của công ty phát triển phần mềm ở Đông Á. Mục tiêu của nhóm tấn công nhằm vào các công ty phát triển phần mềm DLP, tổ chức chính phủ và quân đội. Sau khi giành được quyền truy cập thông qua backdoor, đối tượng tấn công bắt đầu phát tán phần mềm độc hại trên hệ thống của công ty.

Tháng 04/2021, nhóm tấn công APT Tick đã giả mạo phần mềm Q-Dir để triển khai VBScript backdoor có tên gọi ReVBShell. Vào tháng 6 và tháng 9/2021, phần mềm DLP đã cung cấp các bản cập nhật dưới dạng tệp lưu trữ zip chứa các tệp độc hại. Sau đó, vào tháng 2 và tháng 6/2022, Q-Dir đã bị trojan hóa thành công cụ hỗ trợ từ xa như helpU và ANYSUPPORT.

Nhóm đối tượng tấn công đã duy trì quyền truy cập bằng cách triển khai DLL độc hại để giải mã và đưa payload vào một quy trình được chỉ định. Payload này bao gồm một trình tải xuống có tên ShadowPy và một biến thể của Netbot (còn được gọi là Invader hoặc Kickesgo) hoặc một trình tải xuống có tên mã là Ghostdown.

Nguồn: https://cyware.com/news/china-based-tick-apt-deploys-custom-malware-and-use-other-tools-b4faca0c

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 646 lỗ hổng, trong đó có 227 lỗ hổng mức Cao, 163 lỗ hổng mức Trung bình, 04 lỗ hổng mức Thấp và 252 lỗ hổng chưa đánh giá. Trong đó có ít nhất 56 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 24 lỗ hổng trong Google, Nhóm 02 lỗ hổng trong Linux, Nhóm 74 lỗ hổng trong Microsoft, Nhóm 17 lỗ hổng trong Wordpress, Nhóm 20 lỗ hổng trong Dell, Nhóm 06 lỗ hổng trong Samsung, Nhóm 13 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:

- *Google: CVE-2022-47461, CVE-2023-1214,...*
- *Linux: CVE-2023-28466, CVE-2023-1390.*
- *Microsoft: CVE-2023-24863, CVE-2023-24865,...*
- *Wordpress: CVE-2021-36821, CVE-2022-38063,...*
- *Dell: CVE-2023-24571, CVE-2022-34406...*
- *Samsung: CVE-2023-26072, CVE-2023-26073,...*
- *IBM: CVE-2023-26284, CVE-2022-46773,...*

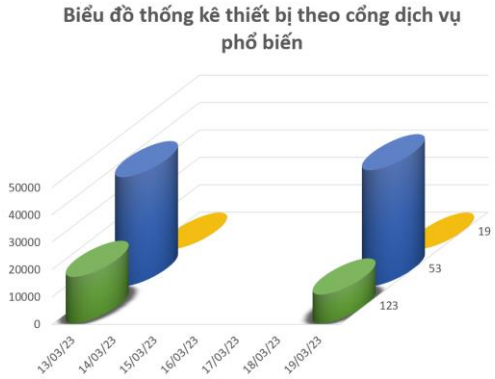
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2022-47461 CVE-2022-47462 CVE-2022-47453 …	Nhóm 24 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công từ chối dịch.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-28466 CVE-2023-1390	Nhóm 02 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Microsoft	CVE-2023-24863 CVE-2023-24865 CVE-2023-24866 …	Nhóm 74 lỗ hổng trong Microsoft cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2021-36821 CVE-2022-38063 CVE-2022-40699 …	Nhóm 17 lỗ hổng trong Wordpress cho phép đối tượng tấn thực hiện với quyền của người dung cục bộ truy cập/thực hiện các hành động trái phép, thực hiện tấn công XSS.	Đã có thông tin xác nhận và bản vá
5	Dell	CVE-2023-24571 CVE-2022-34406 CVE-2022-34407 …	Nhóm 20 lỗ hổng trong Dell (BIOS) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2023-26072 CVE-2023-26073 CVE-2023-26074 …	Nhóm 06 lỗ hổng trong Samsung (FortiRecorder,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2023-26284 CVE-2022-46773 CVE-2022-46774 ...	Nhóm 13 lỗ hổng trong IBM (MQ Certified Container,…) cho phép đối tượng tấn công vượt qua cơ chế bảo mật để đánh cắp thông tin dữ liệu, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

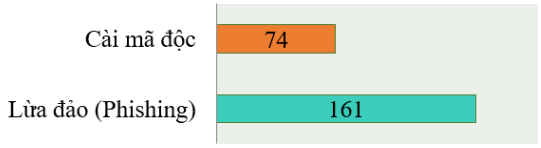
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **46,563** (giảm so với tuần trước **51,053**) 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.

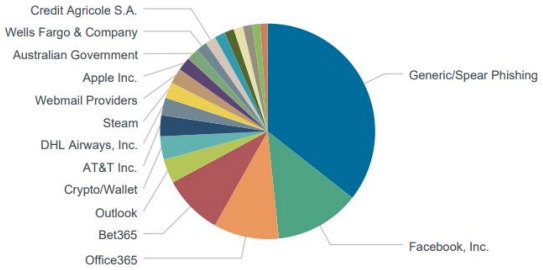


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 235 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 161trường hợp tấn công lừa đảo (Phishing), 74 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: 18267 IP	xjpakmdcfuqe.ru:452 IP
disorderstatus.ru: 7978 IP	xjpakmdcfuqe.in:466 IP
atomictrivia.ru: 3990 IP	restlesz.su: 364 IP
xjpakmdcfuqe.biz: 639 IP	amnsreiuojy.ru: 952 IP
xjpakmdcfuqe.com: 498 IP	hzmksreiuojy.ru: 53 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 289 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	5giay.cc	Website giả mạo Ví điện tử Momo
2	m.tot166.com vay-666.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 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