NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 06 (06/02/2023 – 12/02/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Tin tức:** Google tung ra bản thử nghiệm Privacy Sandbox trên thiết bị Android 13.

- **Chiến dịch tấn công APT:** Nhóm tấn công UAC-0056 bổ sung chức năng đánh cắp thông tin nâng cao trong bộ công cụ của mình.

2. Điểm yếu, lỗ hổng

- **521** 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: 249** 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

"Nhóm tấn công UAC-0056 bổ sung chức năng đánh cắp thông tin nâng cao trong bộ công cụ của mình"

Nhóm tấn công UAC-0056 (hay còn gọi là Nodaria) đã phát động nhiều chiến dịch tấn công Ukraine kể từ khi Nga tiến hành xâm lược quân sự vào nước này. Gần đây, nhóm đã bắt đầu triển khai phần mềm độc hại đánh cắp thông tin mới được đặt tên là Graphiron.

Graphiron được phát triển bằng Go phiên bản 1.18 và có khả năng thu thập nhiều loại thông tin từ máy tính bị lây nhiễm, bao gồm thông tin hệ thống, thông tin đăng nhập, ảnh chụp màn hình và tệp. Phần mềm độc hại này là một phiên bản cải tiến của backdoor tùy chỉnh GraphSteel của nhóm. Nó có các tính năng bổ sung để chạy các lệnh shell và thu thập thông tin hệ thống, tệp,…Hơn nữa, nó giao tiếp với máy chủ C&C bằng cổng 443 và được mã hóa bằng mật mã AES.

Chuỗi lây nhiễm bao gồm hai giai đoạn, Downloader.Graphiron và payload Infostealer.Graphiron. Downloader chịu trách nhiệm truy xuất patload được mã hóa có chứa Infostealer. Graphiron từ một máy chủ từ xa. Còn payload có khả năng thực hiện một số tác vụ, bao gồm truy xuất tên máy chủ, thông tin hệ thống và thông tin người dùng, đồng thời đánh cắp mật khẩu và dữ liệu được lưu trữ từ Firefox, Thunderbird và PuTTY.

UAC-0056 đã nhiều lần triển khai các backdoor tùy chỉnh trong các cuộc tấn công vào Ukraine. Mặc dù nhóm này tương đối ít được biết đến trước cuộc xâm lược Ukraine của Nga, nhưng hoạt động của nhóm này trong năm qua và việc bổ sung các tính năng nâng cao trong Graphiron cho thấy nhóm này đang cập nhật kho vũ khí của mình để khởi động nhiều chiến dịch mạng hơn.

Nguồn: https://cyware.com/news/russian-nodaria-apt-adds-advanced-information-stealing-functionality-63d5fbe6

Tin tức An toàn thông tin

"Google tung ra bản thử nghiệm Privacy Sandbox trên thiết bị Android 13"

Vừa qua, Google công bố đã triển khai tính năng bảo mật Privacy Sandbox trên Android ở phiên bản thử nghiệm cho các thiết bị di động đủ điều kiện đang chạy Android 13. Bản thử nghiệm Privacy Sandbox cung cấp các API mới được thiết kế với nền tảng là quyền riêng tư và không sử dụng số định danh (identifier) để theo dõi hoạt động của người dùng trên các ứng dụng và trang web. Các ứng dụng tham gia thử nghiệm có thể sử dụng các API này để hiển thị cho người dùng quảng cáo có liên quan và đo lường hiệu quả của chúng.

Các thiết bị đã được chọn cho thử nghiệm sẽ có phần Privacy Sandbox trong Cài đặt cho phép người dùng kiểm soát, xem và quản lý các mối quan tâm hàng đầu của họ để hiển thị quảng cáo có liên quan. Theo Google, ban đầu sẽ thiết lập gồm khoảng vài trăm đến vài nghìn chủ đề. Bản thử nghiệm sẽ bắt đầu trên các thiết bị Android 13 và sẽ dần mở rộng trong thời gian tới.

Privacy Sandbox trên Android là câu trả lời của Google đối với tính minh bạch trong việc theo dõi ứng dụng (App Tracking Transparency- ATT), yêu cầu các nhà phát triển ứng dụng phải có được sự đồng ý rõ ràng của người dùng trước khi theo dõi hành vi trực tuyến của họ trên các ứng dụng và trang web thông qua số định danh duy nhất của Apple được giới thiệu trong iOS 14.5 .

Thử nghiệm này là một phần của sáng kiến rộng hơn dành cho các trang web nhằm mục đích bắt đầu loại bỏ dần cookie của bên thứ ba trong trình duyệt web Chrome vào năm 2024.

Hiện tại, các thiết bị Android được chỉ định một mã định danh duy nhất (người dùng có thể đặt lại) cho phép các nhà phát triển ứng dụng có thể sử dụng để theo dõi hành vi trực tuyến. Privacy Sandbox thay thế số định danh bằng một bộ công cụ bảo vệ quyền riêng tư được thiết kế để hạn chế chia sẻ thông tin, đồng thời hỗ trợ quảng cáo được cá nhân hóa.

Nguồn: https://thehackernews.com/2023/01/microsoft-urges-customers-to-secure-on.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 521 lỗ hổng, trong đó có 82 lỗ hổng mức Cao, 57 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 434 lỗ hổng chưa đánh giá. Trong đó có ít nhất 53 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 11 lỗ hổng trong Google, Nhóm 11 lỗ hổng trong Dlink, Nhóm 04 lỗ hổng trong Apache, Nhóm 51 lỗ hổng trong Wordpress, Nhóm 35 lỗ hổng trong Dell, Nhóm 32 lỗ hổng trong Samsung, 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:

- *Google: CVE-2022-32595, CVE-2023-0696,...*
- *Dlink: CVE-2023-24343, CVE-2023-24344,....*
- *Apache: CVE-2022-45786, CVE-2023-22832,...*
- *Wordpress: CVE-2022-27628, CVE-2023-25194,...*
- *Dell: CVE-2022-34364, CVE-2022-34366,...*
- *Samsung: CVE-2022-34376, CVE-2023-21420,...*
- *IBM: CVE-2022-22486, CVE-2023-23477,...*

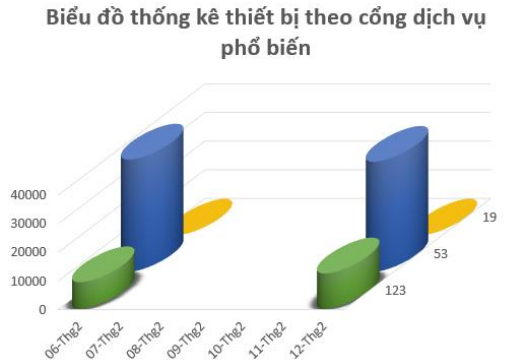
Thông tin điểm yếu, lỗ hổng

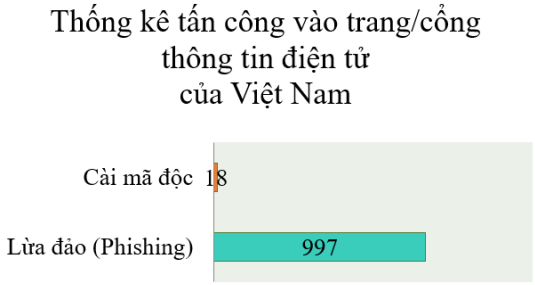
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2022-32595 CVE-2023-0696 CVE-2023-0696 …	Nhóm 11 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Dlink	CVE-2023-24343 CVE-2023-24344 CVE-2023-24345 …	Nhóm 11 lỗ hổng trong Dlink (DIR-605L, …) cho phép đối tượng tấn công truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Apache	CVE-2022-45786 CVE-2023-22832 CVE-2023-25194 …	Nhóm 04 lỗ hổng trong Apache (Kafka Connect, NiFi,…) 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-2022-27628 CVE-2022-2933 CVE-2022-29416 …	Nhóm 51 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2022-34364 CVE-2022-34366 CVE-2022-34376 …	Nhóm 35 lỗ hổng trong Dell (PowerScale OneFS, SupportAssist,…) cho phép đối tượng tấn công có quyền truy cập thông tin cá nhân trái phép, thực thi mã tùy ý, thực hiện nâng cao đặc quyền.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2022-34376 CVE-2023-21420 CVE-2023-21421 …	Nhóm 32 lỗ hổng trong Samsung (WifiSevice, ChnFileShareKit,…) cho phép đối tượng tấn công thực thi mã tùy ý, thu thập thông tin trái phép, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-22486 CVE-2023-23477 CVE-2022-38389 ...	Nhóm 09 lỗ hổng trong IBM (Tivoli Workload Scheduler,…) cho phép đối tượng tấn công thực thi mã từ xa, làm rò rỉ thông tin dữ liệu, truy cập/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

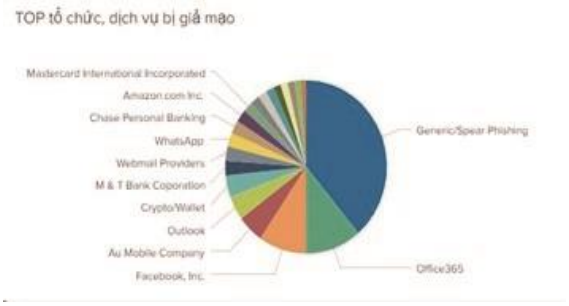
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **48,527** (tăng so với tuần trước **40,895**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 1009 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 0 trường hợp tấn công thay đổi giao diện (Deface), 997 trường hợp tấn công lừa đảo (Phishing), 18 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: 15643 IP	xjpakmdcfuqe.ru:280 IP
disorderstatus.ru: 5014 IP	xjpakmdcfuqe.in: 287 IP
atomictrivia.ru: 2360 IP	restlesz.su: 310 IP
xjpakmdcfuqe.biz: 623 IP	amnsreiuojy.ru: 616 IP
xjpakmdcfuqe.com: 349 IP	hzmksreiuojy.ru: 40 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 249 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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	trangsucluxurydiamond.com vib.mobi vn.btaynguyenfood.com ae888vip.com m.luxurysvip888.com 975.vn h5.tocdovnm.com tindungonline-evn.shop fd2.hmexchangecentre.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 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