NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 12 (20/03/2023 – 26/03/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Cảnh báo:** Mã độc MacStealer đánh cắp dữ liệu và mật khẩu iCloud Keychain trên hệ điều hành macOS.

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Black Magic nhằm mục tiêu vào Ukraine thông qua CommonMagic và PowerMagic.

2. Điểm yếu, lỗ hổng

- **658** 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: 369** 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

"Mã độc MacStealer đánh cắp dữ liệu và mật khẩu iCloud Keychain trên hệ điều hành macOS"

Mã độc MacStealer sử dụng Telegram làm nền tảng để ra lệnh và kiểm soát C&C nhằm mục tiêu vào các thiết bị dùng hệ điều hành macOS của Apple để đánh cắp thông tin dữ liệu trái phép. MacStealer có khả năng đánh cắp tài liệu, cookie và thông tin đăng nhập của người dùng. Mã độc này ảnh hưởng đến các thiết bị sử dụng phiên bản macOS Catalina trở lên chạy trên CPU M1 và M2.

Đầu tháng 3/2023, MacStealer được công khai trên Internet với giá 100 đô la. Mã độc này hiện vẫn đang trong quá trình hoàn thiện để cập nhập thêm các tính năng như thu thập dữ liệu từ trình duyệt Safari và ứng dụng Ghi chú.

Ở phiên bản hiện tại, MacStealer được thiết kế để trích xuất dữ liệu iCloud Keychain, mật khẩu và thông tin thẻ tín dụng từ các trình duyệt như Google Chrome, Mozilla Firefow và Brave. Ngoài ra, MacStealer có tính năng hỗ trợ thu thập các tệp Microsoft Office, hình ảnh, tài liệu lưu trữ và tập lệnh Python.

MacStealer được phát tán dưới dạng tệp DMG (weed.dmg). Khi được triển khai, mã độc sẽ điều hướng người dùng nhập mật khẩu để truy cập Cài đặt hệ thống nhằm thu thập mật khẩu. Những công cụ đánh cắp thông tin như MacStealer đang gia tăng đáng kể trong vài tháng qua.

Ngoài ra, mã độc khác dựa trên C# có tên HookSpoofer lấy cảm hứng từ StormKitty đi kèm với khả năng keylogging và clipper đồng thời truyền dữ liệu đánh cắp tới bot Telegram. Ducktail, một mã độc đánh cắp cookie của trình duyệt cũng sử dụng bot Telegram để lọc dữ liệu, đã trở lại vào tháng 02/2023 cùng với các chiến thuật cải tiến để tránh bị phát hiện.

Theo các nhà nghiên cứu, những công cụ đánh cắp thông tin này liên quan đến việc thay đổi quá trình lây nhiễm ban đầu từ một kho lưu trữ chứa tệp thực thi độc hại sang một kho lưu trữ chứa tệp LNK để bắt đầu quá trình lây nhiễm.

MacStealer phát tán mã độc qua các kênh khác nhau bao gồm tệp đính kèm email, tải xuống phần mềm Bogus và các cuộc tấn công Social engineering.

Để đề phòng các mối đe dọa, người dùng nên cập nhật hệ điều hành và cài đặt phần mềm bảo mật, đồng thời kiểm tra trước khi nhấp vào các liên kết lạ được đính kèm trong email và không tải xuống tệp từ những nguồn không đáng tin cậy.

Nguồn: https://thehackernews.com/2023/03/new-macstealer-macos-malware-steals.html

Tin tức An toàn thông tin

"Cảnh báo: Nhóm tấn công APT Black Magic nhằm mục tiêu vào Ukraine thông qua CommonMagic và PowerMagic"

Nhóm APT Bad Magic nhằm mục tiêu vào các tổ chức chính phủ, nông nghiệp và giao thông vận tải ở Donetsk, Lugansk, và Crimea.

Chiến dịch tấn công tận dụng các mô hình giả lập cũ được tạo từ tháng 9/2021 cùng một framework độc hại là CommonMagic.

Các nhà nghiên cứu đã phát hiện chiến dịch này bắt đầu vào tháng 10/2022 và vẫn tiếp tục cho đến nay. Nhóm APT Bad Magic sử dụng các tin nhắn lừa đảo trực tuyến chứa đường dẫn URL độc hại để điều hướng người dùng đến một kho lưu trữ các tệp ZIP. Kho lưu trữ này chứa các tệp tài liệu (PDF, XLSX, DOCX) với định dạng LNK mở rộng (ví dụ: .pdf.lnk). Tệp LNK bắt đầu quá trình lây nhiễm và triển khai backdoor có tên là PowerMagic, được viết bằng PowerShell.

Backdoor này được thiết kế để kết nối với máy chủ điều khiển từ xa và thực thi các lệnh tùy ý trên thiết bị mục tiêu. Sau khi thực thi, kết quả của quá trình lây nhiễm được tải lên các dịch vụ đám mây như Dropbox và Microsoft OveDrive, mã OAuth được làm mới sử dụng để xác thực thông tin đăng nhập.

PowerMagic hoạt động như một bước đệm cung cấp nền tảng cho CommonMagic chứa tập hợp nhiều mô-đun được thực thi. Các mô-đun này tương tác với máy chủ C&C, mã hóa và giải mã lưu lượng thông tin C&C thu thập được cũng như thực thi các plugin (ảnh chụp màn hình và USB). Plugin (S[.]exe) thực hiện chụp ảnh màn hình ba giây một lần bằng cách sử dụng GDI API và USB U[.]exe thu thập dữ liệu từ các thiết bị USB được kết nối.

Chiến dịch tấn công này vẫn đang hoạt động và được các nhà nghiên cứu tiếp tục điều tra. Vì vậy, để tránh trường hợp bị tấn công thì các cơ quan, tổ chức cần rà soát hệ thống của mình để có biện pháp ngăn chặn và khắc phục kịp thời.

Nguồn: https://cyware.com/news/black-magic-apt-targets-ukraine-with-commonmagic-and-powermagic-20a39894

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 658 lỗ hổng, trong đó có 144 lỗ hổng mức Cao, 122 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 391 lỗ hổng chưa đánh giá. Trong đó có ít nhất 45 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 145 lỗ hổng trong Google, Nhóm 13 lỗ hổng trong Linux, 01 lỗ hổng trong Microsoft, Nhóm 28 lỗ hổng trong Wordpress, 01 lỗ hổng trong Dell, Nhóm 03 lỗ hổng trong Samsung, Nhóm 11 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-2023-28617, CVE-2023-1529,…*
- *Linux: CVE-2022-4095, CVE-2022-48423,…*
- *Microsoft: CVE-2023-26088.*
- *Wordpress: CVE-2022-44742, CVE-2022-45843,...*
- *Dell: CVE-2021-21548.*
- *Samsung: CVE-2023-26496, CVE-2023-26497,…*
- *IBM: CVE-2023-27874, CVE-2023-27871,…*

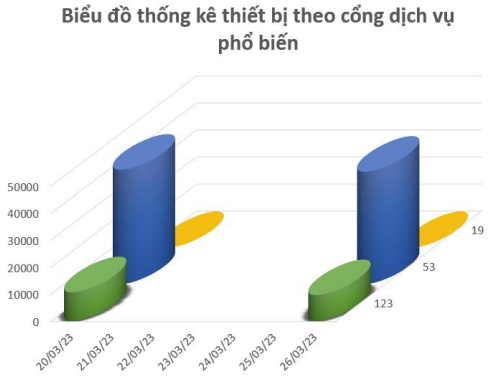
Thông tin điểm yếu, lỗ hổng

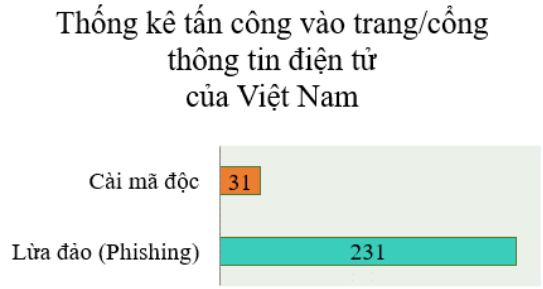
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-28617 CVE-2023-1529 CVE-2023-1528 …	Nhóm 145 lỗ hổng trong Google (Android, Chrome,…) cho phép đối tượng tấn công khai thác lỗi heap thông qua HTML độc hại, thực hiện nâng cao đặc quyền.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2022-4095 CVE-2022-48423 CVE-2022-48424 …	Nhóm 13 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.	Đã có thông tin xác nhận và bản vá
3	Microsoft	CVE-2023-26088	01 lỗ hổng trong phần mềm phòng chống mã độc Malwarebytes cho Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2022-44742 CVE-2022-45843 CVE-2022-47145 …	Nhóm 28 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện với quyền của người dùng cục bộ truy cập/thực hiện các hành động trái phép, thực hiện tấn công XSS.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2021-21548	01 lỗ hổng trong Dell (PowerMax) cho phép đối tượng tấn công thực truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2023-26496 CVE-2023-26497 CVE-2023-26498	Nhóm 03 lỗ hổng trong Samsung 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-2023-27874 CVE-2023-27871 CVE-2023-25684 ...	Nhóm 11 lỗ hổng trong IBM cho phép đối tượng tấn công xem, thêm, sửa đổi hoặc xóa thông tin trong cơ sở 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

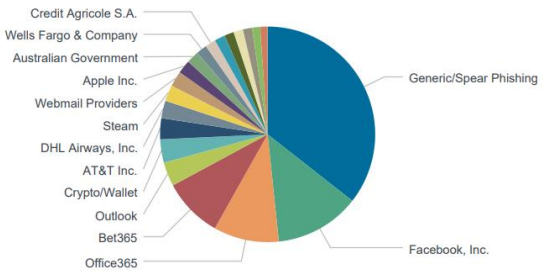
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **49,098** (tăng so với tuần trước **46,563**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 262 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 231 trường hợp tấn công lừa đảo (Phishing), 31 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: 20189 IP	xjpakmdcfuqe.ru:401 IP
disorderstatus.ru: 7407 IP	xjpakmdcfuqe.in:458 IP
atomictrivia.ru: 3599 IP	restlesz.su: 380 IP
xjpakmdcfuqe.biz: 707 IP	amnsreiuojy.ru: 952 IP
xjpakmdcfuqe.com: 439 IP	hzmksreiuojy.ru: 108 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 369 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	vie-tcapital.com	Website giả mạo Ngân hàng TMCP Bản Việt
2	lo.dama582.com	Website giả mạo Western Union
3	shopeemallvn.com	Website giả mạo sàn TMĐT Shopee
4	vietcombank.vn-dll.vip	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
5	vaymbbank.com	Website giả mạo Ngân hàng TMCP Quân đội
6	amazonxk.com	Website giả mạo Amazon
7	fcccredit.com phattai6666.com rik11.fun alibabavn.shop congtykiman.org vincomonevip.net trungtamthuongmaihanoi.com minhchinhmega.com mcredit.vaynhanh-bankcredits.com hackgamemienphi.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