NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 27 (03/7/2023 – 09/07/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Charming Kitten khai thác mã độc NokNok để tấn công người dùng macOS.

- **Cảnh báo:** 1.5 triệu người dùng Google Play có nguy cơ bị tấn công bởi hai phần mềm gián điệp.

2. Điểm yếu, lỗ hổng

- **557** 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: 334** 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 Charming Kitten khai thác mã độc NokNok để tấn công người dùng macOS"

Nhóm tấn công Charming Kitten, còn được biết đến với tên APT42 hay Phosphorus, đã sử dụng mã độc NokNok để tấn công vào hệ điều hành macOS. Chiến dịch này bắt đầu vào tháng 5 và sử dụng phương thức lây nhiễm khác so với trước đây, bằng việc triển khai payload thông qua các file LNK thay vì tài liệu Word như các chiến dịch trước đó.

Nhóm APT Charming Kitten đã tiến hành ít nhất 30 cuộc tấn công tại 14 quốc gia kể từ năm 2015. Các nghiên cứu đã chỉ ra rằng nhóm này có liên quan tới chính phủ Iran, đặc biệt là Quân đội Cách mạng Hồi giáo Iran (IRGC).

Trước đây, nhóm tấn công này đã sử dụng macro trong các tài liệu Word để lây nhiễm, nhưng hiện đã chuyển sang sử dụng các file LNK. Nhóm này mạo danh là chuyên gia hạt nhân Mỹ và tiếp cận mục tiêu bằng cách mời xem bản nháp chính sách đối ngoại.

Tấn công hệ điều hành Windows

Trong cuộc tấn công vào hệ điều hành Windows, sau khi xâm nhập thành công, Charming Kitten gửi cho đối tượng mục tiêu một liên kết độc hại chứa một macro Google Script, đồng thời chuyển hướng đến một địa chỉ Dropbox. Tại đó, một tệp RAR được bảo vệ bằng mật khẩu chứa một dropper mã độc sử dụng mã PowerShell và tệp LNK để triển khai mã độc từ một bên cung cấp dịch vụ lưu trữ đám mây.

Payload cuối cùng là GorjolEcho, một backdoor cơ bản cho phép đối tượng tấn công nhận và thực thi lệnh từ xa. Để tránh bị nghi ngờ, GorjolEcho mở một tệp PDF có nội dung liên quan đến cuộc trò chuyện trước đó giữa nạn nhân và đối tượng tấn công.

Tấn công hệ điều hành macOS

Trong trường hợp nạn nhân sử dụng macOS, nhóm tấn công sẽ nhận ra sau khi lây nhiễm bằng payload Windows không thành công. Nhóm này sẽ gửi một đường dẫn mới tới "library-store[.]camdvr[.]org" để lưu trữ một file ZIP giả dạng ứng dụng RUSI VPN. Khi file script Apple trong ZIP được thực thi, lệnh curl sẽ được kích hoạt để tải xuống payload NokNok và triển khai một backdoor trên thiết bị của nạn nhân.

NokNok tạo ra một hệ định danh hệ thống và sử dụng 4 module bash script để duy trì kết nối, thiết lập liên lạc với máy chủ C&C, đồng thời bắt đầu thu thập dữ liệu từ thiết bị bị nhiễm và gửi về máy chủ này.

Mã độc NokNok thu thập các thông tin hệ thống như: phiên bản hệ điều hành, các trình đang chạy và ứng dụng đã cài đặt. Sau đó, NokNok mã hóa toàn bộ dữ liệu thu thập được dưới dạng base64 rồi gửi về cho đối tượng tấn công.

Các chuyên gia bảo mật cho rằng NokNok có thể chứa nhiều chức năng gián điệp khác trên các module chưa được phát hiện. Sự nghi ngờ này xuất phát từ điểm tương đồng trong mã nguồn của NokNok và GhostEcho, một mã độc đã được phân tích trước đó, có khả năng chụp ảnh, thực thi lệnh và xóa dấu vết lây nhiễm mã độc.

Tóm lại, chiến dịch tấn công này cho thấy nhóm APT Charming Kitten có khả năng thích ứng cao và có khả năng tấn công vào hệ điều hành macOS khi cần thiết. Điều này nhấn mạnh mối đe dọa ngày càng gia tăng của các chiến dịch mã độc phức tạp đối với người dùng macOS.

Nguồn:
https://www.bleepingcomputer.com/news/security/charming-kitten-hackers-use-new-noknok-malware-for-macos/

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: 1.5 triệu người dùng Google Play có nguy cơ bị tấn công bởi hai phần mềm gián điệp"

Trên Cửa hàng Google Play, hai ứng dụng quản lý tệp là File Recovery & Data Recovery (com.spot.music.filedate) với hơn 1 triệu lượt cài đặt và File Manager (com.file.box.master.gkd) với hơn 500.000 lượt cài đặt đã được phát hiện là phần mềm gián điệp (spyware), đe dọa quyền riêng tư và bảo mật của 1.5 triệu người dùng.

Cả hai ứng dụng này đều thuộc cùng một nhà phát triển và có khả năng hoạt động mà không cần sự tương tác từ người dùng. Hai ứng dụng này tham gia vào các hành vi lừa đảo và bí mật đánh cắp dữ liệu quan trọng của người dùng, sau đó gửi chúng đến các máy chủ tại Trung Quốc.

Hai ứng dụng này đều từ cùng một nhà phát hành, có thể chạy mà không cần bất kỳ tương tác nào từ người dùng. Các ứng dụng này tham gia vào các hành vi lừa đảo và bí mật đánh cắp dữ liệu quan trọng của người dùng gửi đến các máy chủ ở Trung Quốc. Các nhà nghiên cứu bảo mật cho biết đã có nhiều thông tin cá nhân bị thu thập trái phép từ hai ứng dụng này, bao gồm:

- Danh sách liên hệ của người dùng lưu trữ trong bộ nhớ trên thiết bị, tài khoản email liên kết và mạng xã hội.
- Hình ảnh, âm thanh và video được quản lý hoặc khôi phục từ bên trong ứng dụng.
- Vị trí người dùng theo thời gian thực.
- Mã quốc gia cho thông tin di động (mobile country code).
- Tên nhà cung cấp mạng.
- Mã mạng của nhà cung cấp SIM.
- Số phiên bản hệ điều hành.
- Thương hiệu và kiểu máy của thiết bị.

Phần mềm gián điệp này sử dụng kỹ thuật ẩn trên thiết bị gây khó khăn cho việc gỡ cài đặt. Đối tượng tấn công đã tăng số lượt tải xuống ứng dụng thông qua việc sử dụng công cụ giả lập hoặc dùng dịch vụ tăng lượt cài đặt nhằm tăng mức độ phổ biến và uy tín cho ứng dụng.

Ứng dụng hiện đã bị xóa khỏi Google Play, tuy nhiên, người dùng nên thận trọng khi tải xuống các ứng dụng đặc biệt là những ứng dụng không có xếp hạng trong khi có lượng tải xuống lớn. Khi cài đặt cũng nên kiểm tra đánh giá của người dùng trước khi cài đặt ứng dụng, chú ý đến các quyền được yêu cầu trong quá trình cài đặt ứng dụng và chỉ tin tưởng vào phần mềm do các nhà phát triển có uy tín cung cấp.

Nguồn: https://thehackernews.com/2023/07/two-spyware-apps-on-google-play-with-15.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 **557** lỗ hổng, trong đó có 46 lỗ hổng mức Cao, 77 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 433 lỗ hổng chưa đánh giá. Trong đó có ít nhất 79 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 04 lỗ hổng trong Microsoft, Nhóm 07 lỗ hổng trong Linux, Nhóm 20 lỗ hổng trong Google, Nhóm 51 lỗ hổng trong Wordpress, Nhóm 30 lỗ hổng trong Huawei, Nhóm 02 lỗ hổng trong Cisco, Nhóm 03 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-2021-31982, CVE-2021-34506,...*
- *Linux: CVE-2023-3117, CVE-2023-2880,...*
- *Google: CVE-2023-20753, CVE-2023-20755,...*
- *Wordpress: CVE-2020-36736, CVE-2020-36737,...*
- *Huawei: CVE-2021-46890, CVE-2021-46891,...*
- *Cisco: CVE-2023-20133, CVE-2023-20180,...*
- *IBM: CVE-2021-39014, CVE-2023-26273,...*

Thông tin điểm yếu, lỗ hổng

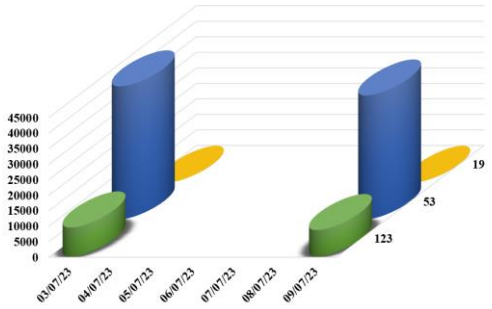
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2021-31982 CVE-2021-34475 CVE-2021-34506 …	Nhóm 04 lỗ hổng trong Microsoft (Edge (Chromium-based)) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, làm rỏ rỉ thông tin dữ liệu, thực hiện tấn công vượt qua cơ chế bảo mật (Bypass).	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-3117 CVE-2023-2880 CVE-2023-1206 …	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.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-20753 CVE-2023-20754 CVE-2023-20755 …	Nhóm 20 lỗ hổng trong Google (Android) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2020-36736 CVE-2020-36737 CVE-2020-36738 …	Nhóm 51 lỗ hổng trong Wordpress 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
5	Huawei	CVE-2021-46890 CVE-2021-46891 CVE-2021-46892 …	Nhóm 30 lỗ hổng trong Huawei (harmonyos,…) cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền, có thể ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính khả dụng của dịch vụ.	Chưa có thông tin xác nhận và bản vá
6	Cisco	CVE-2023-20133 CVE-2023-20180	Nhóm 02 lỗ hổng trong Cisco 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-2021-39014 CVE-2023-30990 CVE-2023-35890	Nhóm 03 lỗ hổng trong IBM phép đối tượng tấn công thực thi JavaScript tùy ý, 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

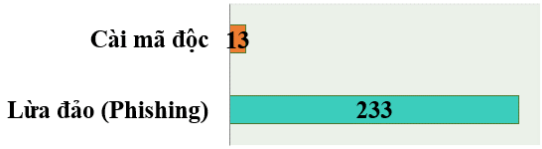
Tấn công DRDoS

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 **48.557,** (giảm so với tuần trước **52.307**) 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

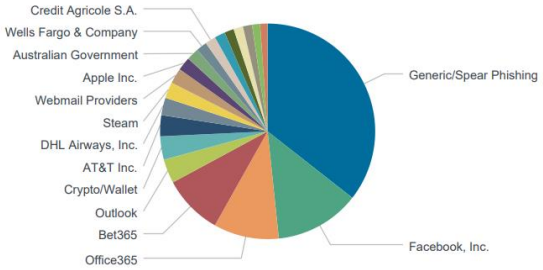


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 246 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 233 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: 10795 IP	xjpakmdcfuqe.ru: 53 IP
disorderstatus.ru: 3344 IP	xjpakmdcfuqe.in: 30 IP
atomictrivia.ru: 1537 IP	restlesz.su: 272 IP
xjpakmdcfuqe.biz: 240 IP	amnsreiuojy.ru: 276 IP
xjpakmdcfuqe.com: 80 IP	hzmksreiuojy.ru: 36 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **334** 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	vn8788.com	Website giả mạo sàn TMĐT Tiki
2	thienshinhan.com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
3	smartphonethongminh.online	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