BẢN TIN NỘI BỘ
CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Ứng dụng mạo danh "Bộ Công an" kiểm soát thông tin người dùng điện thoại

Một ứng dụng mạo danh "Bộ Công an" vừa bị phát hiện. Khi nạn nhân cài ứng dụng mạo danh "Bộ Công an" vào điện thoại, tất cả tin nhắn, mã OTP chuyển tiền của chủ nhân điện thoại đều bị đối tượng lừa đảo kiểm soát.

Nguồn tin từ Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Công an TP Hà Nội cho biết, cơ quan công an vừa phát hiện một ứng dụng giả danh "Bộ Công an" có hình đại diện là huy hiệu Bộ Công an để lừa đảo chiếm đoạt tài sản.

Vụ việc được phát hiện khi cơ quan công an nhận được trình báo của một số nạn nhân bị lừa đảo tiền, có người bị đánh cắp hàng trăm triệu đồng sau khi cài đặt ứng dụng mạo danh vào điện thoại.

Nạn nhân khi cài ứng dụng mạo danh này vào điện thoại thì đối tượng lừa đảo có quyền nhận, đọc, gửi và xem tin nhắn văn bản SMS của điện thoại của nạn nhân, đối tượng lừa đảo có thể đọc được tin nhắn OTP của ngân hàng và từ đó thực hiện các giao dịch chuyển tiền như chủ tài khoản ngân hàng. Khi truy cập, ứng dụng sẽ hiển thị "Hệ thống bảo vệ Bộ Công an" với các mục chọn nhưng đều báo lỗi. Một số nạn nhân đã bị đánh cắp tiền trong tài khoản sau khi cài ứng dụng này.

Gần đây, các ngân hàng liên tục đưa ra cảnh báo với khách hàng về các thủ đoạn phổ biến đang được tội phạm sử dụng là giả danh ngân hàng, gọi điện, nhắn tin từ số điện thoại lạ thông báo khách hàng đã trúng thưởng lớn, sau đó gửi đường dẫn tới các website giả mạo ngân hàng và yêu cầu họ hoàn tất thủ tục nhận thưởng bằng cách cung cấp các thông tin bảo mật của tài khoản, bao gồm: Số CMND, điện thoại, địa chỉ email, mật khẩu đăng nhập, mã OTP, SmartOTP, số thẻ..

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng không cài ứng dụng lạ, cần kiểm tra kỹ thông tin trước khi cài đặt một ứng dụng mới để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/ung-dung-mao-danh-%E2%80%9Cbo-cong-an%E2%80%9D-kiem-soat-thong-tin-nguoi-dung-dien-thoai.12624/

2. Mã độc tống tiền trên Android lây lan qua SMS và Reddit

Mới đây, các nhà nghiên cứu của Công ty An ninh mạng ESET (có trụ sở chính tại Slovakia) đã cảnh báo về một mã độc tống tiền nguy hiểm trên hệ điều hành Android, lây lan qua các liên kết độc hại trong tin nhắn SMS và các bài đăng trên diễn đàn Reddit.

Lukas Stefanko, nhà nghiên cứu mã độc của công ty ESET cho biết, mã độc tống tiền trên Android này có tên Android/Filecoder.C, bắt đầu hoạt động chậm nhất kể từ ngày 12/7/2019. Mã độc được phát tán qua các bài đăng trên diễn đàn Reddit và một diễn đàn dành riêng cho các nhà phát triển Android có tên "XDA Developer".

Nó có thể lây lan rộng hơn bằng tin nhắn SMS chứa các liên kết độc hại và sử dụng danh sách liên lạc của nạn nhân.

Vì phạm vi mục tiêu mã độc này đang nhắm đến chưa rộng rãi và còn tồn tại sơ hở khi thực hiện tấn công, nên mức độ tác động của mã độc tống tiền mới này vẫn còn hạn chế. Tuy nhiên, nếu tin tặc bắt đầu nhắm vào các nhóm người dùng rộng hơn, thì mã độc tống tiền này có thể trở thành mối đe dọa nghiêm trọng.

Tin tặc sẽ gửi các tin nhắn tới danh sách liên lạc của nạn nhân có nội dung thông báo rằng ảnh của họ đã được tìm thấy trong một ứng dụng. Khi người dùng truy cập ứng dụng, mã độc này sẽ mã hóa hầu hết các tệp tin và đòi tiền chuộc.

Hầu hết các diễn đàn và các bài đăng độc hại trên Reddit có nội dung liên quan đến chủ đề nhạy cảm hay công nghệ. Các liên kết cũng có thể được rút gọn, hoặc sử dụng mã QR để trỏ đến mã độc.

Để tối đa phạm vi tiếp cận, mã độc tống tiền được thiết kế có tới 42 phiên bản ngôn ngữ khác nhau của mẫu tin nhắn. Trước khi gửi, mã độc sẽ lựa chọn phiên bản ngôn ngữ phù hợp với cài đặt ngôn ngữ trên thiết bị nạn nhân và sử dụng tên chính xác của nạn nhân.

Mã độc chứa thông tin về địa chỉ của máy chủ C&C và địa chỉ Bitcoin được mã hóa cứng (hardcode) trong mã nguồn. Tuy nhiên, tin tặc có thể thay đổi những địa chỉ này bất cứ lúc nào bằng cách sử dụng dịch vụ Pastebin miễn phí. Nếu người dùng xóa ứng dụng có chứa mã độc tống tiền thì các tệp tin sẽ không thể giải mã được.

Theo ESET, dù mã độc tống tiền thông báo rằng dữ liệu bị ảnh hưởng sẽ biến mất sau 72 giờ, nhưng trong mã nguồn của mã độc không cho thấy điều này. Khoản tiền chuộc là tương đối nhỏ, khoảng 94-188 USD. ESET cũng kêu gọi người dùng Android chỉ nên tải xuống các ứng dụng từ cửa hàng Google Play chính thức, luôn cập nhật phiên bản mới nhất của hệ điều hành, chú ý đến quyền mà các ứng dụng yêu cầu và tải phần mềm diệt virus cho các thiết bị di động.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android chỉ tải xuống các ứng dụng từ cửa hàng Google Play chính thức, luôn cập nhật phiên bản mới nhất của hệ điều hành, chú ý đến quyền mà các ứng dụng yêu cầu để đảm bảo an toàn thông tin.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=c74b5c11-1141-471b-95c8-a05fe6e7d3a6&NewsID=605273e6-79b4-43fd-a626-827453e0bd2f

3. Phát hiện mã độc trong ứng dụng Android CamScanner với hơn 100 triệu người dùng

Kẻ tấn công có thể từ xa chiếm quyền điều khiển thiết bị Android của bạn và đánh cắp dữ liệu được lưu trữ trên thiết bị nếu bạn đang sử dụng CamScanner phiên bản miễn phí, một ứng dụng tạo PDF trên điện thoại rất phổ biến với hơn 100 triệu lượt tải xuống trên Google Play Store.

Để an toàn, bạn chỉ cần gỡ ứng dụng CamScanner khỏi thiết bị Android, vì Google đã gỡ bỏ ứng dụng này khỏi Play Store chính thức.

Gần đây các nhà nghiên cứu tìm thấy mô-đun Trojan Droppper ẩn trong ứng dụng CamScanner có thể cho phép kẻ tấn công từ xa bí mật tải xuống và cài đặt chương trình độc hại trên thiết bị Android của người dùng mà họ không biết.

Mô-đun độc hại không thực sự nằm trong mã của chính ứng dụng CamScanner cho Android; thay vào đó, nó là một phần của thư viện quảng cáo bên thứ 3 gần đây đã được giới thiệu trong ứng dụng tạo PDF.

Vấn đề được đưa ra ánh sáng sau khi nhiều người dùng CamScanner phát hiện ra hành vi đáng ngờ và đăng các đánh giá tiêu cực trên Google Play Store.

Phân tích mô-đun Trojan Dropper độc hại cho thấy có thành phần tương tự trong một số ứng dụng được cài đặt sẵn trên điện thoại Trung Quốc.

Các nhà nghiên cứu của Kaspersky đã báo cáo phát hiện của mình cho Google, sau đó Google đã nhanh chóng gỡ bỏ ứng dụng CamScanner khỏi Play Store và cho biết thêm "có vẻ như các nhà phát triển ứng dụng đã loại bỏ mã độc với bản cập nhật CamScanner mới nhất".

Vì phiên bản trả tiền của ứng dụng CamScanner không bao gồm thư viện quảng cáo của bên thứ 3 và do đó không bị ảnh hưởng bởi mô-đun độc hại nên vẫn có sẵn trên Google Play Store.

Mặc dù trong vài năm trở lại đây Google đã tăng cường nỗ lực loại bỏ các ứng dụng có khả năng gây hại khỏi Play Store và thêm các biện pháp kiểm tra phần mềm độc hại nghiêm ngặt hơn cho các ứng dụng mới, các ứng dụng lừa đảo vẫn tồn tại và nhắm mục tiêu đến hàng triệu người dùng.

Do đó, người dùng nên luôn cài sẵn phần mềm diệt virus trên thiết bị Android để có thể phát hiện và ngăn chặn các hoạt động độc hại trước khi chúng có thể lây nhiễm vào thiết bị của bạn.

Ngoài ra, luôn luôn xem xét các đánh giá ứng dụng do những người dùng khác để lại và cũng xác minh các quyền của ứng dụng trước khi cài đặt bất kỳ ứng dụng và chỉ cấp các quyền đó có liên quan cho mục đích của ứng dụng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần gỡ bỏ ứng dụng CamScanner để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/phat-hien-ma-doc-trong-ung-dung-android-camscanner-voi-hon-100-trieu-nguoi-dung.12626/

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Adobe	CVE-2019-7965 CVE-2019-8003 CVE-2019-8009 ...	Nhóm 79 lỗ hổng trên một số phiên bản của Adobe Acrobat and Reader, Creative Cloud Desktop Application cho phép đối tượng tấn công thực thi mã lệnh tùy ý	Đã có thông tin xác nhận và bản vá.
2	Google Android	CVE-2019-2126 CVE-2019-2127 CVE-2019-2128 …..	Nhóm 16 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công chèn và thực thi mã lệnh Một số lỗ hổng có điểm CVSS 9.3 Ảnh hưởng tới các phiên bản: Android-7.0, 7.1.1, 7.1.2, 8.0 8.1, 9.	Đã có thông tin xác nhận và bản vá.
3	IBM	CVE-2019-4294 CVE-2019-4481 CVE-2019-4483	Nhóm 31 lỗ hổng trên một số sản phẩm của IMB (API Connect, Intelligent Operations Cente DataPower Gateway, Contract Management, Informix Dynamic Server Enterprise Edition…) cho phép đối tượng tấn công thu thập thông tin, khai thác lỗi SQL Injection để tương tác trái phép với cơ sở dữ liệu back-end, lỗi XSS, Path Traversal, tấn công leo thang. Một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá
4	Atlassian Jira	CVE-2019-11585 CVE-2019-11588 CVE-2019-11586 …	Nhóm 10 lỗ hổng trên Jira cho phép đối tượng tấn công khai thác lỗi XSS, CSRF, thu thập thông tin tài khoản người dùng, chuyển hướng người dùng đến trang web độc hại.	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-1883 CVE-2019-1907 CVE-2019-1900 …	Nhóm 27 lỗ hổng trên một số sản phẩm của Cisco (NFVIS, Firepower Threat Defense, HyperFlex Software,Integrated	Đã có thông tin xác nhận và bản vá

			Management Controller...) cho phép đối tượng tấn công thu thập thông tin, tấn công nghe lén, chèn và thực thi mã lệnh, tấn công leo thang.	
6	Dlink	CVE-2019-15526 CVE-2019-15527 CVE-2019-15528 ...	Nhóm 05 lỗ hổng trên một số firmware sản phẩm của D-Link DIR-823G cho phép đối tượng tấn công chèn và thực thi mã lệnh để kiểm soát thiết bị.	Đã có thông tin xác nhận và bản vá
7	Lenovo	CVE-2019-6178 CVE-2019-6159 CVE-2019-6177 ...	Nhóm 05 lỗ hổng trên một số sản phẩm, ứng dụng của Lenovo (Lenovo Solution Center, ThinkPad) cho phép đối tượng tấn công thu thập thông tin, khai thác lỗi XSS, tấn công leo thang.	Đã có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	soplifan.ru
5	xdqzpbcgrvkj.ru
6	xjpakmdcfuqe.com
7	kn0ugjov.ru
8	ixhtiv.info
9	www.cityofangelsmagazine.com
10	somicrososoft.ru

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.