BẢN TIN NỘI BỘ

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

1. 3 cách kiểm tra để phòng tránh ứng dụng Android độc hại

Công cụ mới được Google phát triển có tên Google Play Protect có mục đích giúp người dùng Android phòng tránh kịp thời các ứng dụng độc hại đáng ngờ. Công cụ này sẽ kiểm tra thiết bị Android và cảnh báo người dùng nếu phát hiện ra bất kỳ vấn đề nào.

Người dùng nên lưu ý, Play Protect được thiết kế cho cửa hàng ứng dụng Play Store, do đó chỉ có thể quét và phát hiện các ứng dụng độc hại trên đó, nên sẽ không quét các ứng dụng và trang web của bên thứ ba. Do đó, cách bảo vệ thiết bị an toàn nhất chính là chỉ cài đặt ứng dụng từ Google Play.

Dưới đây là 3 cách để kiểm tra một ứng dụng đã được Play Protect xác thực là không có mã độc hay chưa.

Trước khi có thể xem chi tiết của lượt quét gần nhất, người dùng cần kích hoạt dịch vụ này trước đó. Để xem chi tiết của lượt quét gần nhất, người dùng vào Settings (Cài đặt) > Google > Security (Bảo mật) > Google Play Protect. Ở đây, người dùng có thể xem danh sách những ứng dụng được cài đặt gần đây nhất, những ứng dụng gây hại và tùy chọn tắt hay mở dịch vụ này.

Hiện tại, người dùng có thể thấy chứng chỉ kiểm duyệt của Google trên trang của ứng dụng trên Play Store, thể hiện rằng Play Protect đã kiểm duyệt ứng dụng. Đây là cách nhanh nhất để kiểm tra xem ứng dụng có an toàn hay không mà không cần phải cài đặt và chờ Play Protect quét.

Một ứng dụng đã cài đặt có thể là an toàn khi đã qua nhiều lớp kiểm duyệt, tuy nhiên tin tặc có thể xâm nhập và thay đổi hành vi ứng dụng qua các đợt cập nhật, từ đó có thể theo dõi và đánh cắp thông tin người dùng. Mặc dù vậy, Play Protect đã hoàn thiện tính năng quét lại tất cả ứng dụng mà người dùng dự định cập nhật, để xem các phiên bản cập nhật có an toàn hay không. Ngay trên đầu danh sách cập nhật, người dùng có thể thấy thông báo "No problems found", thể hiện rằng bản cập nhật mới của ứng dụng đã được Play Protect quét và không thấy vấn đề gì.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần kiểm tra kỹ càng trước khi sử dụng một phần mềm trên kho ứng dụng Play Store để đảm bảo an toàn thông tin.

Link tham khảo:

http://www.antoanthongtin.vn/Detail.aspx?CatID=afad3c1b-8ab0-41b3-9364-fe76366f1531&NewsID=f1059bf7-716d-44aa-808a-8364d797e05b

2. Quan chức cấp cao của ít nhất 20 nước bị tấn công qua WhatsApp

Theo Reuters, phần lớn nạn nhân của vụ việc là quan chức chính phủ cao cấp và quan chức quân đội của ít nhất 20 quốc gia trên khắp 5 châu lục.

Trường hợp tấn công nhằm vào smartphone của nhân viên chính phủ lần này nghiêm trọng hơn những lần trước đó, và được cho là sẽ gây ra hậu quả lớn về chính trị và ngoại giao.

Trong ngày 29.10, WhatsApp đã đâm đơn kiện NSO Group, công ty chuyên về công nghệ bảo mật với chuyên môn là phát triển công cụ tấn công mạng, công cụ hack để kinh doanh. WhatsApp cáo buộc NSO Group đã phát triển và bán một nền tảng hack, có tác dụng khai thác lỗ hổng trong máy chủ của ứng dụng nhắn tin này, nhằm giúp người mua hack vào điện thoại của ít nhất 1.400 người dùng trong khoảng thời gian từ cuối tháng 4 đến đầu tháng 5.2019.

Tổng số người bị tấn công còn có thể cao hơn. Một nạn nhân, đang là luật sư hoạt động vì nhân quyền ở Anh, đã gửi đến Reuters hình ảnh cho thấy kẻ xấu đã cố ý tấn công vào điện thoại của người này vài lần, vào ngày 1.4.

Không rõ cá nhân hay tổ chức nào đã sử dụng nền tảng trên để nhằm vào quan chức chính phủ. Phía NSO thì thông báo rằng nền tảng hack của họ chỉ được bán độc quyền cho khách hàng dạng chính phủ.

Nguồn tin trong cuộc cho biết một số nạn nhân đang ở Mỹ, Các Tiểu vương quốc Ả Rập Thống nhất, Bahrain, Mexico, Pakistan và Ấn Độ.

Một số công dân Ấn Độ công khai nói họ là nạn nhân trong vài ngày qua; bao gồm những nhà báo, học giả, luật sư...

Trong một tuyên bố khác, NSO chia sẻ rằng "không thể công bố khách hàng là ai hay mô tả cụ thể công dụng của sản phẩm đang kinh doanh". Họ cũng phủ nhận mọi hành vi sai trái, nói sản phẩm của công ty chỉ có mục đích giúp chính phủ các nước truy bắt khủng bố và tội phạm.

Các nhà nghiên cứu an ninh mạng từ lâu đã ngờ vực về tuyên bố trên, phản bác rằng sản phẩm của NSO đã được sử dụng để chống lại một loạt đối tượng, bao gồm cả người biểu tình ở một số quốc gia.

Citizen Lab, một nhóm theo dõi độc lập làm việc với WhatsApp để xác định các mục tiêu bị hack, cho biết ít nhất 100 nạn nhân là người nổi tiếng trong xã hội như nhà báo, người bất đồng chính kiến, chứ không phải là tội phạm.

Trước khi thông báo cho nạn nhân về vụ việc, WhatsApp đã kiểm tra liệu trong số họ có ai đang liên quan đến việc phạm tội hay không, như dính líu đến khủng bố, lạm dụng trẻ em... Nhưng công ty không tìm thấy bất cứ liên kết nào. Giới chức chính phủ có thể gửi yêu cầu cho WhatsApp để tra cứu thông tin như vậy, thông qua một cổng thông tin trực tuyến của công ty.

Những người dùng bị ảnh hưởng đã nhận thông tin cảnh báo vào đầu tuần này. WhatsApp từ chối bình luận về danh tính các khách hàng của NSO Group, vốn được cho là chủ mưu của vụ tấn công.

Link tham khảo:

https://thanhnien.vn/cong-nghe/quan-chuc-cap-cao-cua-it-nhat-20-nuoc-bi-tan-cong-qua-whatsapp-1143945.html

3. Mất trắng tiền trong tài khoản ngân hàng nếu làm theo tin nhắn lạ

Những tin nhắn rác với nội dung quảng cáo sản phẩm, dịch vụ từ lâu đã không còn lạ lẫm với người dùng di động. Đây là một vấn nạn nhức nhối của ngành viễn thông. Dù các cơ quan chức năng đã đưa ra nhiều biện pháp xử lý khác nhau, có một thực tế là tin nhắn rác vẫn đang tràn lan và thậm chí là không ngừng biến tướng.

Theo phản ánh của nhiều người dùng di động, bên cạnh các nội dung quảng cáo, giờ đây tin nhắn rác còn mang trong mình cả những thông tin lừa đảo. Các tin nhắn này có một mô-típ chung là chúng thường mạo danh tổng đài của một nhà cung cấp dịch vụ nhằm đánh lừa người dùng di động.

Chia sẻ với Pv. VietNamNet, anh Minh (Hoàn Kiếm, Hà Nội) cho biết vừa nhận được một tin nhắn giới thiệu chương trình khuyến mại từ ngân hàng Việt Nam Thịnh Vượng (VPBank). Điều đáng nói là tin nhắn này không đến từ đầu số tổng đài mà là từ một số máy lạ.

"Nội dung tin nhắn hướng dẫn tôi truy cập vào một website giả mạo có chứa cụm từ VPBank để nhận thưởng. Khi truy cập vào website này, phần mềm Kaspersky đưa ra cảnh báo đường link có chứa virus. Biết đây là thủ đoạn của bọn lừa đảo nên tôi không làm theo.", anh Minh nói.

Ở thời điểm chiều 31/10, khi Pv. VietNamNet truy cập vào website nói trên, website này đã bị gỡ bỏ bởi nhà quản trị hệ thống. Tuy vậy, đây là một thủ đoạn rất thường thấy của những kẻ lừa đảo.

Thông thường, tội phạm mạng sẽ dùng thủ thuật để gửi đi đồng loạt các tin nhắn cùng một nội dung tới nhiều người dùng khác nhau. Trong một số trường hợp, tùy mục đích mà kẻ xấu còn nhắm vào một đối tượng người dùng cụ thể (ví dụ như những đồng nghiệp cùng trong một cơ quan) để tăng xác suất thành công của phi vụ.

Khi người dùng truy cập vào đường link dẫn đến website giả mạo có trong tin nhắn, hiện ra trước mắt họ sẽ là giao diện giống y hệt của nhà cung cấp dịch vụ thật. Lúc này, nếu người dùng thực hiện thao tác đăng nhập, gõ thông tin tài khoản, mật khẩu, mã OTP,... kẻ xấu sẽ có ngay những thông tin đó để ngay lập tức truy cập vào các tài khoản thật.

Trong trường hợp nhẹ nhàng hơn, website giả mạo sẽ chứa mã độc tự động cài cắm vào máy tính hay điện thoại cá nhân. Từ đây, kẻ xấu có thể xâm nhập thiết bị của bạn, gửi đi các hình ảnh nhạy cảm hay thậm chí là biết được tất cả các nội dung được bạn nhập liệu thông qua bàn phím.

Với trường hợp của anh Minh, vị khách hàng này cảm thấy khó hiểu khi nội dung tin nhắn lừa đảo mình nhận được có chứa họ và tên chuẩn xác của bản thân. "Điều này chứng tỏ số điện thoại và thông tin cá nhân của tôi đã bị kẻ xấu lấy được theo một cách nào đó.", anh Minh bức xúc chia sẻ.

Đây không phải điều gì quá lạ lẫm bởi không ít người từng phản ánh việc nhận được vô số tin nhắn quảng cáo khi chỉ vừa đặt chân tới sân bay. Trước đó, hồi tháng 4/2018, trên một diễn đàn nước ngoài có địa chỉ Raidforums.com, một thành viên

thậm chí đã chia sẻ và rao bán file dữ liệu gồm 163 triệu tài khoản của một doanh nghiệp mạng xã hội trong nước.

Thực tế trên cho thấy tại Việt Nam đang có một lỗ hổng trong việc quản lý và bảo vệ thông tin, dữ liệu cá nhân của người dùng di động. Điều này đến từ nguồn lực dành cho công tác đảm bảo an toàn thông tin, nhận thức của đơn vị vận hành hệ thống cũng như ý thức tự bảo vệ của chính người dùng Internet, mà điều này thì không thể thay đổi trong ngày một ngày hai.

Để không trở thành nạn nhân của những kẻ lừa đảo hay spam tin nhắn, người dùng cần thận trọng trong việc chia sẻ thông tin cá nhân ở bất kỳ đâu. Cách tốt nhất là hạn chế công khai thông tin cá nhân trên các mạng xã hội và chỉ cung cấp chúng cho những công ty hay nhà cung cấp dịch vụ mà mình tin tưởng.

Bên cạnh đó, người dùng cũng nên cảnh giác khi vô tình nhận được các tin nhắn, cuộc gọi lạ. Tránh làm theo hướng dẫn của những thông tin mà mình không biết rõ nguồn gốc.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần đề cao cảnh giác khi nhận được những đường link nghi ngờ, có thể sử dụng trang web https://www.virustotal.com/gui/home/upload để kiểm tra trước khi nhấn vào để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/mat-trang-tien-trong-tai-khoan-ngan-hang-neu-lam-theo-tin-nhan-la-583867.html

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	Linux	CVE-2019-18198	01 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công khai thác bộ nhớ FIB-LOOKUP-NOREF, chèn và thực thi mã lệnh tùy ý, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá.
2	Adobe	CVE-2019-8238 CVE-2019-8088 CVE-2019-8087	Nhóm 15 lỗ hổng trên một số thành phần, sản phẩm của Adobe (Experience Manager Forms, Acrobat and Reader) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh tùy ý. Ảnh hưởng đến nhiều phiên bản Adobe.	Đã có thông tin xác nhận và bản vá
3	WordPress	CVE-2015-9497 CVE-2015-9496 CVE-2015-9531 …	Nhóm 45 lỗ hổng trên nhiều thành phần của WordPress (The Easy Digital Downloads PDF Stamper extension..) cho phép đối tượng tấn công khai thác lỗi XSS	Đã có thông tin xác nhận và bản vá
4	Apache	CVE-2019-10079 CVE-2019-12415	Nhóm 02 lỗ hổng trên Apache (Traffic Server, POI) cho phép đối tượng tấn công thu thập thông tin	Đã có thông tin xác nhận và bản vá
5	D-Link	CVE-2013-4856 CVE-2013-4855 CVE-2013-4857	Nhóm 03 lỗ hổng trên thiết bị D-Link (DIR-865L)cho phép đối tượng tấn công chèn và thực thi mã lệnh qua nhiều thành phần khác nhau	Chưa có thông tin xác nhận và bản vá
6	Google	CVE-2016-5202	Lỗ hổng trên Goole (Google Chrome)cho phép đối tượng tấn công truy cập trái phép thu thập thông tin	Chưa có thông tin xác nhận và bản vá
7	TP-Link	CVE-2019-13653 CVE-2019-13650 CVE-2013-4848	Nhóm 06 lỗ hổng trên thiết bị TP-Link (M7350) cho phép đối tượng tấn công chèn và	Chưa có thông tin xác nhận và

			thực thi mã lệnh từ xa	bản vá
8	Foxit-software	CVE-2019-17141 CVE-2019-17139 CVE-2019-17145	Nhóm 08 lỗ hổng trên phần mềm Foxit-software (PhantomPDF 9.6.0.25114, PhantomPDF 9.5.0.20732…) cho phép đối tượng tấn công thực thi mã lệnh tùy ý , hướng mục tiêu truy cập trang web độc hại.	Chưa 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	l677e13te.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	www.cityofangelsmagazine.com
9	morphed.ru
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.