BẢN TIN NỘI BỘ

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

1. Android xuất hiện malware chuyên đánh cắp mã xác thực Google Authenticator

Các nhà nghiên cứu bảo mật đã phát hiện ra một malware chạy trên hệ điều hành Android có khả năng đánh cắp mã xác thực bảo mật từ ứng dụng Google Authenticator. Loại malware này có tên Cerberus.

Trước đây đa số người dùng đều cảm thấy an tâm khi sử dụng phương thức bảo mật xác thực hai lớp 2FA của ứng dụng Google Authenticator. Nhưng sau công bố trên từ ThreatFabric về Cerburus, có thể cần phải xem xét lại về khả năng an toàn tuyệt đối của Google Authenticator.

Cerberus là một trojan chuyên đánh cắp thông tin tài khoản ngân hàng. Nó xuất hiện vào khoảng tháng 6.2019. Với biến thể đầu tiên, chúng chủ yếu tập trung khai thác vào các thông tin nhận diện cá nhân của người dùng như mật khẩu tài khoản ngân hàng.

Sau khi bị chặn đứng bởi các ứng dụng ngăn chặn malware trên Android, vào đầu năm nay các tội phạm mạng đã phát triển Cerberus tiến hành tạo ra một biến thể mới nhằm khắc phục những thiếu sót và có khả năng vượt mặt các ứng dụng bảo mật. Và đáng chú ý Cerberus đã cung cấp các tính năng gần giống với Remote Access Trojans (Trojan truy cập từ xa), khả năng đánh cắp thông tin khóa màn hình của thiết bị (mã PIN hoặc hình vẽ) và cả những mã xác thực 2FA từ ứng dụng Google Authenticator.

Cerberus không hề phá vỡ hoạt động của Google Authenticator mà đi sâu vào bên trong hệ thống tập tin và tải xuống những dữ liệu của nó. Tệ hơn nữa, malware này cũng có thể khởi chạy TeamViewer và thiết lập các kết nối, cung cấp thêm cho tin tặc quyền truy cập từ xa vào thiết bị nạn nhân. Tuy nhiên, các nhà nghiên cứu tin rằng các tác giả của Cerberus vẫn chưa phát hành biến thể chính thức của phần mềm độc hại này và hiện tại nó đang trong giai đoạn thử nghiệm.

Khuyến nghị: Người dùng Andoird cần cẩn trọng khi sử dụng Google Authenticator, cập nhật bản vá mới nhất và tuân thủ các quy định đã ban hành để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/android-xuat-hien-malware-chuyen-danh-cap-ma-xac-thuc-google-authenticator-1189902.html

2. Ứng dụng vẫn là hướng tấn công thiết bị di động phổ biến của tin tặc

Theo Pradeo Labs, tấn công các ứng dụng di động là hướng tấn công chiếm gần 80% các cuộc tấn công nhắm vào thiết bị di động. Theo sau đó là các cuộc tấn công thông qua mạng và hệ điều hành.

Hầu hết, tội phạm mạng sử dụng các ứng dụng để xâm nhập vào thiết bị di động. Các nhà nghiên cứu của Pradeo Labs cho biết, điều này thể hiện qua tỉ lệ 79% các cuộc tấn công nhắm vào thiết bị di động trong năm 2019 và 76% trong đầu năm 2020.

Số liệu này được lấy từ báo cáo "Bối cảnh mối đe dọa thiết bị di động trong doanh nghiệp" năm 2020. Trong đó, chỉ ra 10% trong số 50.000 thiết bị Android chứa mã độc khai thác lỗ hổng zero-day và 3.890 thiết bị chứa mã độc đã biết. Trong khi đó, trong số 50.000 thiết bị iOS, chỉ có 55 thiết bị có chứa mã độc khai thác lỗ hổng zero-day. Các nhà nghiên cứu cảnh báo người dùng về "các ứng dụng gây rò rỉ và xâm nhập" và nhấn mạnh rằng, các ứng dụng di động có thể thực hiện các hành vi không mong muốn do chúng lưu trữ các thư viện bên ngoài (79% ứng dụng di động nhúng thư viện bên thứ ba).

"Các thiết bị Android thường trích xuất nhiều dữ liệu hơn thiết bị iOS. Tuy nhiên, cả hai loại thiết bị đều xử lý các dữ liệu được cấp quyền truy cập một cách quá mức", các nhà nghiên cứu cho biết trong báo cáo. Vì vậy, hai hệ điều hành này đều có thể gây rò rỉ dữ liệu người dùng, danh bạ, dữ liệu vị trí, dữ liệu âm thanh, video.

Theo các nhà nghiên cứu, các cuộc tấn công qua mạng đã tăng 4% trong năm qua. Xu hướng này được thúc đẩy bởi sự gia tăng liên tục của các cuộc tấn công man-in-the-middle trên khắp Bắc Mỹ và Châu Á. Năm 2019, 15.605 thiết bị được kết nối với các điểm truy cập Wifi không an toàn, Hiện nay, đã có tới 19.750 thiết bị như vậy. Tại khu vực Bắc Mỹ và Châu Á, tỷ lệ thiết bị phải đối mặt với tấn công man-in-the-middle lần lượt à 4% và 9,28%.

Bên cạnh đó, các cuộc tấn công nhắm vào hệ điều hành của thiết bị di động đã giảm nhẹ, chiếm 8% các cuộc tấn công. Ngoài ra, có 54% thiết bị Android vẫn sử dụng hệ điều hành cũ, còn iOS là 23%.

Khuyến nghị: Người dùng cần cập nhật phiên bản mới của thiết bị di động, kiểm tra kỹ thông tin trước khi cài đặt những ứng dụng mới để đảm bảo an toàn thông tin.

Link tham khảo: http://antoanthongtin.vn/an-toan-thong-tin/ung-dung-van-la-huong-tan-cong-thiet-bi-di-dong-pho-bien-cua-tin-tac-105856

3. Tin tặc có thể điều khiển các thiết bị tích hợp trợ lý giọng nói qua sóng siêu âm

Một phương thức tấn công mới nhằm vào các thiết bị điều khiển bằng giọng nói vừa được phát hiện. Theo đó, tin tặc có thể truyền sóng siêu âm qua các vật liệu rắn để tương tác và điều khiển thiết bị bằng các lệnh thoại mà nạn nhân không hay biết.

Được gọi là "SurfingAttack", cuộc tấn công sử dụng tính chất độc đáo của truyền âm trong vật liệu rắn - ví dụ như bàn làm việc - để "cho phép tương tác giữa thiết bị điều khiển bằng giọng nói và kẻ tấn công trong khoảng cách xa hơn và không cần trong tầm nhìn".

Với cuộc tấn công này, tin tặc có thể tương tác với thiết bị bằng cách sử dụng trợ lý giọng nói, đánh cắp mã xác thực hai yếu tố gửi qua SMS và thậm chí thực hiện các cuộc gọi lừa đảo, kín đáo kiểm soát thiết bị của nạn nhân.

Nghiên cứu được công bố bởi một nhóm các học giả từ Đại học bang Michigan, Đại học Washington ở St. Louis, Viện Hàn lâm Khoa học Trung Quốc và Đại học

Nebraska-Lincoin, được trình bày tại Hội nghị chuyên đề bảo mật hệ thống phân tán mạng (NDSS) vào ngày 24 tháng 2 tại San Diego.

SurfingAttack hoạt động như thế nào?

Các micro MEMS, tiêu chuẩn trong hầu hết các thiết bị điều khiển bằng trợ lý giọng nói, đều có màng loa, khi chạm vào âm thanh hoặc sóng ánh sáng sẽ dịch thành tín hiệu điện sau đó giải mã thành các lệnh thực tế.

Cuộc tấn công mới khai thác bản chất phi tuyến của các mạch micro MEMS để truyền tín hiệu siêu âm độc hại - sóng âm thanh tần số cao mà tai người không thể nghe được – bằng đầu dò áp điện trị giá 5 đô la gắn trên mặt bàn. Cuộc tấn công có thể được thực hiện từ khoảng cách gần 10 m.

Để che giấu cuộc tấn công, các nhà nghiên cứu đã phát đi một sóng siêu âm chỉnh âm lượng của thiết bị xuống đủ thấp để các phản hồi bằng giọng nói không bị chú ý, trong khi vẫn có thể ghi lại các phản hồi bằng giọng nói từ trợ lý thông qua một thiết bị ghi âm được giấu ở gần thiết bị của nạn nhân bên dưới gầm bàn.

Sau đó, các nhà nghiên cứu không chỉ có thể kích hoạt trợ lý giọng nói (ví dụ: sử dụng "OK Google" hoặc "Hey Siri"), mà còn tạo ra các lệnh tấn công (ví dụ: "đọc tin nhắn của tôi" hoặc "gọi Sam bằng loa ngoài") sử dụng các hệ thống chuyển văn bản thành giọng nói (TTS) - tất cả đều được truyền dưới dạng tín hiệu sóng siêu âm có thể truyền dọc theo bàn để điều khiển thiết bị.

SurfingAttack đã được thử nghiệm thành công với nhiều thiết bị sử dụng trợ lý giọng nói, gồm Google Pixel, Apple iPhone, Samsung Galaxy S9 và Xiaomi Mi 8. Nó cũng hoạt động trên các mặt bàn khác nhau (như kim loại, kính, gỗ) và cấu hình điện thoại khác nhau.

Tuy nhiên, thử nghiệm không thành công với Huawei Mate 9 và Samsung Galaxy Note 10+. Các nhà nghiên cứu cho rằng thất bại là do "cấu trúc và vật liệu của thân điện thoại".

Loa thông minh của Amazon và Google - Amazon Echo và Google Home - không bị ảnh hưởng bởi cuộc tấn công này.

Gia tăng hình thức tấn công dựa trên giọng nói

Mặc dù cho đến nay không có dấu hiệu nào cho thấy cuộc tấn công này đang bị khai thác trong thực tế, đây không phải là lần đầu tiên các cuộc tấn công kiểu này được phát hiện.

Thật vậy, nghiên cứu gần đây cho thấy có thể khai thác tính phi tuyến trong micro để truyền các lệnh không nghe được tới hệ thống qua tín hiệu siêu âm.

Hơn nữa, một nghiên cứu của các nhà nghiên cứu từ Đại học Điện tử Truyền thông ở Tokyo và Đại học Michigan đã phát hiện ra một loạt các cuộc tấn công - được gọi là Light Commands - sử dụng tia laser để tiêm các lệnh không nghe được vào điện thoại thông minh và loa, lén lút khiến chúng mở khóa cửa, mua sắm trên các trang web thương mại điện tử và thậm chí là khởi động xe.

Mặc dù cuộc tấn công này yêu cầu chùm tia laser nằm trong tầm nhìn trực tiếp đến thiết bị mục tiêu đang được đề cập, khả năng lan truyền độc đáo của

SurfingAttack đã loại bỏ yêu cầu này, do đó cho phép kẻ tấn công tiềm năng tương tác từ xa với thiết bị hỗ trợ giọng nói và thực hiện các lệnh trái phép để truy cập thông tin nhạy cảm mà nạn nhân không hay biết.

Phương thức tấn công mới này sẽ yêu cầu các nhà sản xuất thiết bị xây dựng hệ thống an ninh mới và việc bảo vệ các thiết bị khỏi các cuộc tấn công dựa trên giọng nói ngày càng trở thành yêu cầu cho mọi ngôi nhà thông minh.

Link tham khảo: https://whitehat.vn/threads/tin-tac-co-the-dieu-khien-cac-thiet-bi-tich-hop-tro-ly-giong-noi-qua-song-sieu-am.13294/

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	Apple	CVE 2016 4606 CVE 2012 5366	Nhóm 02 lỗ hổng trên thiết bị Apple (Apple Mac OS X,...) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá.
2	Netsweeper	CVE 2014 9613 CVE 2014 9614 CVE 2014 9612 …	Nhóm 09 lỗ hổng trên phần mềm Netsweeper (the web panel,…) cho phép đối tượng tấn công tấn công SQL injection, tấn công XSS.	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE 2020 9043 CVE 2020 9006 CVE 2020 5530 …	Nhóm 07 lỗ hổng trên phần mềm Wordpress (Ninja Form plugin, Portable, Utilities, phpMyAdmin Plugin,…) cho phép đối tượng tấn công tấn công tấn công CSRF, tấn công XSS.	Đã có thông tin xác nhận và bản vá
4	Cisco	CVE 2020 3159 CVE 2015 0749 CVE 2011 2054 …	Nhóm 16 lỗ hổng trên thiết bị Cisco (Cisco Finesse, Cisco Unified Communications Manager,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công XSS, tấn công CSRF.	Đã có thông tin xác nhận và bản vá
5	Gitlab	CVE 2019 15592 CVE 2019 15594 CVE 2020 8795 …	Nhóm 04 lỗ hổng trên phần mềm Gitlab (Gitlab Enterprise Edition,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
6	Adobe	CVE 2020 3765 CVE 2020 8997	Nhóm 02 lỗ hổng trên phần mềm Adobe (Adobe After Effects, Adobe Media Encoder,…) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý.	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	atomictrivia.ru
2	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
3	ydbnsrt.me
4	tttta.sssaaaas.io
5	xdqzpbcgrvkj.ru
6	xjpakmdcfuqe.in
7	amnsreiuojy.ru
8	xjpakmdcfuqe.com
9	xjpakmdcfuqe.biz
10	www.cityofangelsmagazine.com

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.