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

## 1. Google giới thiệu mã hóa Adiantum cho các thiết bị tầm thấp

Google đã chính thức công bố hình thức mã hóa mới, được thiết kế để bảo mật dữ liệu lưu trữ trên điện thoại thông minh tầm thấp và các thiết bị khác không đủ sức mạnh xử lý.

Theo Venture Beat, hầu hết điện thoại Android đều được kích hoạt mã hóa lưu trữ như một tính năng mặc định và trên thực tế, nó là một yêu cầu của các nhà sản xuất điện thoại kể từ phiên bản Android 6.0. Tuy nhiên, đối với các điện thoại có sức mạnh xử lý thấp được yêu cầu để chạy mã hóa trực tiếp trên thiết bị thì tính năng này thường không có sẵn.

Chẳng hạn, Android Go được thiết kế cho các thiết bị có bộ xử lý cấp thấp, điển hình là ở các thị trường đang phát triển, nhưng với nhiều thiết bị này có RAM 1 GB trở xuống, mã hóa lưu trữ bị tắt theo mặc định để cải thiện hiệu suất hoặc hoàn toàn không có. Bộ xử lý ARM Cortex-A7 mà một số mẫu điện thoại cấp thấp sử dụng, thậm chí không hỗ trợ phần cứng cho Tiêu chuẩn mã hóa nâng cao (AES) được Android sử dụng.

Và đây là lúc Adiantum phát huy tác dụng. Adiantum được xây dựng để chạy trên điện thoại và các thiết bị thông minh khác không có phần cứng chuyên dụng để mã hóa dữ liệu được lưu trữ cục bộ một cách hiệu quả. Tuy nhiên, tính năng này không chỉ đơn giản là nhắm mục tiêu vào điện thoại Android giá rẻ hướng đến các thị trường mới nổi mà còn hướng tới mọi thiết bị năng lượng thấp dựa trên nền Linux, từ đồng hồ thông minh đến các thiết bị y tế được kết nối.

Link tham khảo: https://thanhnien.vn/cong-nghe/google-gioi-thieu-ma-hoa-adiantum-cho-cac-thiet-bi-tam-thap-1050173.html

## 2. Apple mạnh tay với các ứng dụng lén chụp màn hình

Ngay sau khi xuất hiện thông tin về việc nhiều ứng dụng trên iPhone đã bí mật ghi lại hình ảnh của màn hình người dùng, vào hôm qua - tức chỉ 1 ngày sau, Apple đã đưa ra thông báo chính thức của mình cho các nhà sản xuất ứng dụng, theo trang TechCrunch.

Theo đó, Apple đã đưa ra thông báo chính thức về vụ việc này, buộc các nhà phát triển ứng dụng phải xóa tính năng này đi, hoặc phải thông báo với người dùng trước khi kích hoạt tính năng đó. Hình phạt mà Apple sẽ áp dụng đối với những nhà phát triển không chịu thực hiện, đó là hãng sẽ gỡ các ứng dụng của họ xuống khỏi kho App Store.

Cũng theo thông báo mới này, Apple đã khẳng định với người dùng rằng, Luật đăng tải ứng dụng của App Store nghiêm cấm các hoạt động này trước khi có sự đồng ý của người dùng. "Bảo vệ người dùng khỏi những nguy hại về vấn đề bảo mật là tôn chỉ của các sản phẩm Apple. Các nhà phát triển phải thông báo với người dùng bằng

hình ảnh, và có sự đồng ý của họ trước khi ghi hình các hoạt động trên màn hình.", thông báo của Apple nhấn mạnh.

Liên quan đến việc này, các công ty như Glassbox đang cung cấp cho các nhà phát triển một dịch vụ mang tên "phát lại phiên sử dụng" (session replaying), giúp cho họ có thể phân tích được tính năng, giao diện người dùng để có thể cập nhật trong các phiên bản phần mềm sau. Nhưng ngược lại, tính năng này cũng có thể ghi lại những thông tin nhạy cảm, và rất có thể rơi vào tay những kẻ xấu.

Theo trang TechCrunch, trách nhiệm lại không nằm trong tay Glassbox mà là ở các nhà phát triển ứng dụng đặt khách sạn, du lịch khi họ không thêm các thông báo với người dùng. Chẳng hạn ứng dụng của hãng Air Canada thậm chí còn không bôi đen một số thông tin nhạy cảm của người dùng trước khi gửi về máy chủ của bên thứ 3 nữa.

Còn theo các nhà chuyên môn, vụ việc này cũng khá giống với vụ Apple gỡ bỏ các ứng dụng nội bộ của Google và Facebook, khi hãng đã rất cứng rắn với việc các nhà phát triển lợi dụng kho ứng dụng App Store của mình. Việc các ứng dụng có sử dụng dịch vụ của Glassbox là không sai, nhưng họ cũng phải có những biện pháp thông báo với người dùng về hoạt động của mình.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng cần xem kỹ các điều khoản yêu cầu khi cài ứng dụng trên iPhone, iPad để đảm bảo an toàn thông tin.

Link tham khảo: http://www.pcworld.com.vn/articles/cong-nghe/an-ninh-mang/2019/02/1262631/apple-manh-tay-voi-cac-ung-dung-len-chup-man-hinh/

### 3. Khoảng 2,2 tỷ tài khoản bị đánh cắp đang bị giới hacker lan truyền

Trang tin BGR vừa cho hay, các hacker đang lan truyền cho nhau bộ sưu tập dữ liệu với khoảng 2,2 tỷ tài khoản hoặc password của người dùng đã bị chúng đánh cắp.

Một báo cáo mới từ các chuyên gia an ninh mạng đã tiết lộ rằng, các "bộ sưu tập" tài khoản người dùng từ 2 - 6 (Collection #2 đến #6) cũng đã xuất hiện trên mạng. Theo đó, có khoảng 2,2 tỷ tài khoản cùng password của người dùng mạng đã bị "phơi bày" cho cả thế giới. Số thông tin khổng lồ này đang được các hacker chuyền tay nhau trên những diễn đàn bằng công cụ torrent, và thậm chí nếu muốn sở hữu chúng, bạn cũng sẽ chẳng mất một xu nào hết, theo BGR.

Ít ngày trước, như Thế giới Vi tính đã đưa, cộng động mạng đã bị rúng động khi một hacker đã chia sẻ lên mạng một bộ sưu tập tên người dùng và tài khoản khổng lồ, bao gồm 773 triệu tài khoản người dùng cùng 21 triệu mã mật khẩu. Tin tặc này đã đặt tên cho nó là "Collection #1" - tức "bộ sưu tập số 1". Giờ đây, chúng ta mới hay rằng nó chỉ là sự khởi đầu, và sau khi tung ra Collection #1, chúng đã tung ra tiếp Collection #2 đến #6, điều đó cho thấy số lượng dữ liệu bị đánh cắp lớn đến nhường nào.

Sau khi nhà nghiên cứu bảo mật của hãng bảo mật Troy Hunt phát hiện ra bộ sưu tập số 1, những chuyên gia khác tại Viện Hasso Plattner Institute ở Potsdam

(Đức) cũng đã lần ra toàn bộ cơ sở dữ liệu đã bị các hacker đánh cắp, và họ đưa ra kết luận rằng" bộ hồ sơ hoàn chỉnh đồ sộ gần gấp 3 lần so với Collection #1, tờ Wired cho biết.

Cụ thể, hầu hết thông tin này đều được hacker trích xuất từ các lần rò rỉ từ trước, bao gồm cả các vụ scandal của Yahoo, LinkedIn và Dropbox. Tuy nhiên, Collection #1 đến #6 cũng chứa rất nhiều dữ liệu chưa từng xuất hiện trên Internet bao giờ.

Các nhà nghiên cứu tại Viện Hasso Plattner Institute đã tìm thấy 750 triệu tài khoản không có trong cơ sở dữ liệu của họ và 611 triệu tài khoản khác từ Collection #2 đến #5 - không trùng lặp với Collection #1. Một số thông tin trong đó được thu thập từ các trang web ẩn, và điều này đồng nghĩa với việc: đây là lần đầu tiên các tổ hợp tên người dùng/mật khẩu này bị phát tán.

Để phát hiện ra chúng, Viện Hasso Plattner Institute đã phát triển ra một công cụ đặc biệt là một trang web, và nó cũng có thể giúp bạn kiểm tra xem dữ liệu của mình đã bị rò rỉ hay chưa. Theo đó, chỉ cần bạn điền email của mình vào website kia của Viện, kết quả sau đó sẽ được gửi cho bạn. Để hạn chế tình trạng bị hacker dò được password, bạn nên đặt mỗi dịch vụ trực tuyến một mật khẩu khác nhau, cũng như sử dụng app quản lý để tạo được những mật khẩu có độ an toàn cao.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng cần luôn đề cao cảnh giác, đổi mật khẩu các ứng dụng theo định kỳ để đảm bảo an toàn thông tin.

Link tham khảo: http://www.pcworld.com.vn/articles/cong-nghe/an-ninh-mang/2019/02/1262623/khoang-2-2-ty-tai-khoan-bi-danh-cap-dang-bi-gioi-hacker-lan-truyen/

## 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 Acrobat | CVE-2018-12830<br>CVE-2018-15987<br>CVE-2018-15991<br>… | Nhóm 88 lỗ hổng trên phần mềm Adobe Acrobat & Readercho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh. Nhiều phiên bản Acrobat bị ảnh hưởng. | Đã có thông tin xác nhận và bản vá |
| 2 | Cisco | CVE-2019-1657<br>CVE-2019-1669<br>CVE-2019-1652<br>..... | Nhóm 26 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Cisco Small Business RV320 & RV325, AMP Threat Grid, Firepower Threat Defense, Identity Services Engine, IoT Field Network Director, Webex Network Recording Player, Webex Meetings Server…) cho phép đối tượng tấn công thực hiện một số hình thức tấn công: thu thập thông tin, vượt qua cơ chế bảo mật để truy cập trái phép vào hệ thống, chèn và thực thi đoạn mã độc hại. CVE-2019-1652 đã có mã khai thác và ảnh hưởng tới nhiều quốc gia trên thế giới | Đã có thông tin xác nhận và bản vá Đã có mã khai thác |
| 3 | Foxit | CVE-2018-17698<br>CVE-2018-17702<br>CVE-2018-17705<br>... | Nhóm 65 lỗ hổng phần mềm Foxit Reader và Foxit PhantomPDF cho phép đối tượng tấn công chèn và thực thi mã lệnh trong phạm vi của triến trình | Đã có thông tin xác nhận và bản vá. |
| 4 | Drupal | CVE-2019-6339 | Nhóm 04 lỗ hổng trên Drupal Core phiên bản 7.x và 8.x.x cho phép đối tượng tấn công đọc và xóa tập tin trên hệ | Đã có thông tin xác nhận và bản vá |

| | | | | |
|---|---|---|---|---|
| | | | thống, sửa đổi dữ liệu trái phép, chèn và thực thi đoạn mã, tập tin độc hại tùy ý. | |
| 5 | Omron CX Supervisor | CVE-2018-19017<br>CVE-2018-19013<br>CVE-2018-19011<br>CVE-2018-19019 | Nhóm 04 lỗ hổng phần mềm CX-Supervisor cho phép đối tượng tấn công chèn lệnh để xóa tập tin trên hệ thống, chèn và thực thi đoạn mã độc hại. Omron CX-Supervisor là phần mềm dùng trong các hệ thống điều khiển công nghiệp dùng để thiết kế và giám sát quy trình hoạt động của thiết bị trong hệ thống | 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 | plpanaifheaighai.com |
| 2 | mokoaehaeihgiaheih.ru |
| 3 | and30.blabladomdom.com |
| 4 | produkktc.com |
| 5 | n.hmiblgoja.ru |
| 6 | ajkeahkcueafuiaeuf.ru |
| 7 | mel.cloudcontentsmak.com |
| 8 | iuefgauiaiduihgs.com |
| 9 | https://kisssweetmilf.com/lbjsmbbeuzsg |
| 10 | dghfhfgjfhjghj6699.net |

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.