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

1. FaceApp không phải là ứng dụng của Facebook

Phần mềm làm "thay đổi gương mặt trong ảnh" đang gây bão trên mạng xã hội thuộc về một công ty có trụ sở ở Nga, chứ không phải do Facebook cung cấp như nhiều người đang lầm tưởng. Ngoài việc thu thập dữ liệu ảnh của người dùng, FaceApp hiện chưa có động thái gây ảnh hưởng nào. Tuy vậy, bạn cần cân nhắc kỹ trước khi quyết định tải ứng dụng này về thiết bị của mình.

Theo phân tích, ứng dụng sẽ lấy ảnh từ camera hoặc từ thư viện ảnh, theo sự lựa chọn của người dùng, sau đó tải ảnh lên máy chủ của nhà cung cấp ứng dụng. Ảnh sẽ được phân tích, xử lý và gửi trả về cho người dùng hàng loạt chân dung với các sắc thái già, trẻ khác nhau.

Trên lý thuyết, FaceApp có thể tự xử lý bức ảnh ngay trên thiết bị của người dùng, nhưng vấn đề là nhà cung cấp vẫn lưu những bức ảnh áp dụng hiệu ứng của người dùng lên máy chủ của họ. Việc này dẫn đến nguy cơ, dữ liệu về gương mặt của người dùng có thể bị lộ lọt hoặc bị lợi dụng bất kỳ lúc nào. Bên cạnh đó, việc FaceApp có thể truy cập thư viện ảnh trên thiết bị cũng chứa đựng nguy cơ mọi bức ảnh khác sẽ bị thu thập mà người dùng không biết.

Thực tế, trong lần đầu sử dụng, người dùng sẽ được nhà cung cấp FaceApp thông báo về chính sách quyền riêng tư trong đó bao gồm cả việc, các bức ảnh của người dùng sẽ được lưu lại trên máy chủ của nhà cung cấp. Dẫu vậy, đa phần người dùng không quan tâm đến các cảnh báo này khi sử dụng ứng dụng FaceApp và dễ dàng chấp thuận các chính sách do nhà sản xuất đưa ra.

"Trong thế giới phẳng của Internet và mạng xã hội phát triển như hiện nay, việc cẩn trọng trong sử dụng các ứng dụng phần mềm là điều hết sức cần thiết. Khi một ứng dụng mới được đưa ra, nhà sản xuất luôn khiến nó trở nên hấp dẫn nhất có thể đối với người dùng. Việc tải về hoặc không là quyền của bạn, nhưng hãy cân nhắc kỹ trước khi thực hiện", một Admin của cộng đồng an ninh mạng WhiteHat.vn bình luận.

FaceApp cho biết họ sẵn sàng xóa dữ liệu từ máy chủ của họ nếu có yêu cầu từ người dùng. Có thể gửi yêu cầu thông qua cách sau, vào Cài đặt -> Hỗ trợ -> Báo cáo lỗi với cụm từ "Quyền riêng tư" tại dòng chủ đề.

Hiện ứng dụng này đã có dữ liệu của hơn 150 triệu người dùng trên thế giới chỉ trong thời gian ngắn. Tính riêng trên nền tảng Android, phần mềm này đã có hơn 100 triệu lượt người dùng tải về. FaceApp cũng đang nằm trong số ứng dụng iOS phổ biến nhất ở 121 quốc gia, theo hãng nghiên cứu ứng dụng App Annie.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra nguồn gốc nhà phát hành, đọc kỹ các chính sách của ứng dụng trước khi cài đặt để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/faceapp-khong-phai-la-ung-dung-cua-facebook.12486/

2. Việt Nam bị tấn công mã độc ngoại tuyến cao nhất Đông Nam Á

Theo báo cáo của hãng bảo mật Kaspersky, kết thúc quý 2 vừa qua hãng phát hiện hơn 19 triệu mối đe dọa trực tuyến và hơn 99 triệu mối đe dọa ngoại tuyến tại Việt Nam, giảm đáng kể so với cùng kỳ năm ngoái.

Đây là những phát hiện quan trọng nằm trong Kaspersky Security Bulletin của Kaspersky Security Network (KSN) quý 2/2019.

Theo đó, tấn công thông qua trình duyệt là phương thức mà tội phạm mạng thường sử dụng để phát tán mã độc. Từ tháng 4 đến 6.2019, Kaspersky phát hiện 19.820.196 sự cố, tương ứng với 27,7% người dùng tại Việt Nam bị tấn công bởi các mối đe dọa từ internet. So với cùng thời điểm năm 2018, số lượng các mối đe dọa trực tuyến đã giảm 36,84%, từ 31.382.419 trường hợp.

Khác với tấn công trực tuyến, tấn công ngoại tuyến được thực hiện khi mã độc lây lan qua USB, CD, DVD và các phương thức ngoại tuyến khác. Tại Việt Nam, Kaspersky phát hiện 99.885.492 sự cố, tương ứng với 59,9% người dùng bị tấn công ngoại tuyến. Tuy nhiên, Việt Nam hiện xếp vị trí đầu tiên ở Đông Nam Á và vị trí thứ 30 trên thế giới về các vụ tấn công ngoại tuyến.

Dữ liệu từ KSN cũng cho thấy Singapore là quốc gia có số lượng mối đe dọa trực tuyến và ngoại tuyến thấp nhất khu vực trong quý 2/2019 với số trường hợp nhiễm mã độc trực tuyến và ngoại tuyến lần lượt là 1.300.197 (xếp thứ 143 toàn cầu) và 2.141.642 (xếp thứ 116 toàn cầu).

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra cẩn thận, quét virus khi sử dụng các thiết bị ngoại tuyến như Usb, ổ cứng rời và cả CD, DVD. Cẩn trọng khi bấm vào các liên kết truy cập vào một trang web, đặc biệt là lỗi chính tả hoặc những nội dung bất thường trong link, ngay cả khi đây là trang web được truy cập thường xuyên; Chỉ nhập tên người dùng và mật khẩu qua những kết nối an toàn. Không đăng nhập vào ngân hàng trực tuyến và các dịch vụ tài chính thông qua mạng Wi-Fi công cộng (khi đó có thể tạm thời sử dụng qua Hotspot 3G/4G trên điện thoại di động cho giao dịch ngân hàng, sau khi giao dịch xong quay lại sử dụng Wifi).

Link tham khảo: https://thanhnien.vn/cong-nghe/viet-nam-bi-tan-cong-ma-doc-ngoai-tuyen-cao-nhat-dong-nam-a-1103941.html

3. Lỗ hổng bảo mật iOS 13 cho phép truy cập trái phép mật khẩu

Một lỗi đã được phát hiện trên bản iOS 13 beta mới nhất cung cấp một lỗi truy cập trái phép vào tất cả mật khẩu, email và tên người dùng được lưu trữ bởi tính năng Tự động điền (Autofill).

Hiện tại iOS 13 vẫn đang trong giai đoạn thử nghiệm, do đó lỗi này chỉ ảnh hưởng đến một số lượng hạn chế những người đang chạy bản beta công khai hoặc bản beta dành cho nhà phát triển.

Trên các thiết bị chạy iOS 13 beta, người dùng có quyền truy cập vào tất cả mật khẩu và dữ liệu được lưu trữ trong khóa iCloud (iCloud Keychain) và được sử dụng bởi tính năng Autofill trong iOS. Chỉ cần truy cập Cài đặt > Mật khẩu & Tài khoản và bắt đầu chạm vào tùy chọn Mật khẩu trang web và ứng dụng nhiều lần.

Thao tác này sẽ hủy lời nhắc Face ID/Touch ID trên màn hình sau một vài lần thử và cấp một quyền truy cập vào tất cả mật khẩu và tên người dùng được lưu trữ. Người dùng thậm chí có thể sửa đổi mật khẩu được lưu trữ.

Vì lỗi này đã được công khai chi tiết, Apple có thể sẽ khắc phục sự cố với phiên bản beta tiếp theo của iOS 13 và iPadOS 13.

iOS 13 đi kèm với một số tính năng và cải tiến mới về quyền riêng tư. Mặc dù lỗi này rất nghiêm trọng, nhưng iOS 13 vẫn đang trong giai đoạn phát triển và thử nghiệm beta và các lỗi như vậy chắc chắn sẽ tồn tại.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng iOS nên cập nhật các phiên bản chính thức của hệ điều hành theo bản quyền để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/lo-hong-bao-mat-ios-13-cho-phep-truy-cap-trai-phep-mat-khau-550680.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	Dlink	CVE-2019-13372 CVE-2019-13373 CVE-2019-13375 ...	Nhóm 10 lỗ hổng trên một số sản phẩm, phần mềm của D-link (Central WiFi Manager, DIR-655 C, DIR-818LW) cho phép tấn công thực thi đoạn mã PHP thông qua một số trường, khai thác lỗi SQL Injection, một số lỗ hổng cho phép chèn và thực thi mã lệnh tùy ý.	Đã có thông tin xác nhận. Một số lỗ hổng đã có bản vá.
2	Google - Android	CVE-2019-2106 CVE-2019-2107 CVE-2019-2109 …..	Nhóm 12 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công thực thi mã lệnh từ xa trái phép mà không yêu cầu có quyền thực thi.	Đã có thông tin xác nhận và bản vá
3	Vivotek	CVE-2018-14494 CVE-2018-14495 CVE-2018-14496	Nhóm 03 lỗ hổng mức cao trên firmware của thiết bị Vivotek FD8136 (Thiết bị Camera phổ biến ở Việt Nam) cho phép đối tượng tấn công chèn và thực thi lệnh độc hại từ xa từ đó có thể kiểm soát thiết bị.	Chưa có thông tin xác nhận và bản vá.
4	Fortinet	CVE-2019-13399 CVE-2019-13400 CVE-2019-13401 ……	Nhóm 05 lỗ hổng trên firmware của thiết bị Fortinet Dynacolor FCM-MB40 v1.2.0.0 cho phép đối tượng tấn công lấy được khóa SSL/TLS thiết lập sẵn trên thiết bị từ đó có thể đọc dữ liệu mã hóa, khai thác lỗi CSRF hay lỗi trong quá trình khởi động cho phép duy trì backdoor trên hệ thống.	Chưa có thông tin xác nhận và bản vá.
5	Cisco	CVE-2019-1873 CVE-2019-1932 CVE-2019-1921 …	Nhóm 14 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Security Appliance Software, Firepower Threat Defense,	Đã có thông tin xác nhận và

			Advanced Malware Protection, IOS XR Software, IP Phone 7800...) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lệnh, một số lỗ hổng cho phép đọc và ghi dữ liệu độc hại ở mức dưới của hệ điều hành.	bản vá.
6	EQ-3	CVE-2019-10122 CVE-2019-10119 CVE-2019-10120 ...	Nhóm 04 lỗ hổng trên các thiết bị eQ-3 HomeMatic (CCU2 phiên bản trước 2.41.9 và CCU3 phiên bản rước 3.43.16) - dòng thiết bị của Đức hay sử dụng trong Smarthome cho phép đối tượng tấn công thực thi mã lệnh từ xa, tự động đăng nhập như quyền quản trị	Đã có thông tin xác nhận

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

STT	**Tên miền/IP**
1	differentia.ru
2	disorderstatus.ru
3	atomictrivia.ru
4	soplifan.ru
5	nxzfdsio58.ru
6	xjpakmdcfuqe.com
7	somicrososoft.ru
8	fzhpv0v4i.ru
9	www.cityofangelsmagazine.com
10	awjapmnak.info

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.