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

1. Ứng dụng Samsung giả mạo trên Android có 10 triệu lượt tải

Theo SlashGear, ứng dụng mang tên Updates for Samsung này tuyên bố nó sẽ cập nhật phần mềm điện thoại, nhưng thực tế lại chuyển hướng người dùng đến một trang web chứa đầy quảng cáo và gói yêu cầu trả phí thuê bao. Ứng dụng vẫn còn tồn tại trên Google Play Store.

Ngoài việc cung cấp cho người dùng hàng loạt quảng cáo, ứng dụng đang tính phí người dùng để tải xuống các bản cập nhật chương trình cơ sở này, được cung cấp miễn phí thông qua các kênh chính thức. Ứng dụng yêu cầu người dùng cung cấp thông tin thẻ tín dụng của họ thay vì sử dụng đăng ký Google Play.

Báo cáo nói rằng tùy chọn tải xuống miễn phí ứng dụng xấu có giới hạn tốc độ tải xuống chậm dẫn đến thời gian chờ đợi nhiều giờ cho một lần cập nhật. Nạn nhân của ứng dụng báo cáo rằng việc tải xuống của họ thường thất bại, buộc họ phải bắt đầu lại hoặc trả phí vì thất vọng.

Đồng thời, ứng dụng này hướng người dùng đến một dịch vụ tuyên bố mở khóa SIM điện thoại với mức phí 19,99 USD. Một số người dùng đã để lại các đánh giá trên danh sách Google Play Store cho rằng ứng dụng khiến điện thoại của họ không ổn định, dẫn đến việc khởi động lại ngẫu nhiên, bỏ cuộc gọi, quá nóng và các vấn đề khác.

Do xếp hạng trung bình rất cao, mặc dù số lượng đánh giá 1 sao lớn, nhiều khả năng các cá nhân đứng sau ứng dụng này đã sử dụng các đánh giá giả để thêm cảm giác hợp pháp cho sản phẩm lừa đảo của họ. Không rõ có bao nhiêu trong số hơn 10 triệu lượt cài đặt được liệt kê trên trang của ứng dụng là xác thực, nhưng con số có thể rất cao.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng điện thoại Samsung không tải ứng dụng nêu trên và cần kiểm tra kỹ các ứng dụng trước khi tải về điện thoại của mình để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/ung-dung-samsung-gia-mao-tren-android-co-10-trieu-luot-tai-1100568.html

2. Thông tin cấm bán hàng online trên Facebook cá nhân là giả mạo

Đêm 3/7, một sự cố diễn ra với hệ thống của Facebook khiến người dùng Việt Nam và nhiều nơi khác trên thế giới không thể xem ảnh trên mạng xã hội này. Cụ thể, khi đăng các dòng trạng thái mới lên Facebook, hình ảnh không hiện ra trước mắt người xem dù nội dung vẫn hiển thị.

Hiện vẫn chưa rõ nguyên nhân của sự cố nói trên. Tuy nhiên, nhiều khả năng đây là chuỗi phản ứng dây chuyền sau sự cố của Cloudflare, một trong những dịch vụ DNS (phân giải tên miền) trung gian lớn nhất thế giới. Sự cố này khiến nhiều

website và dịch vụ liên quan như Dropbox, BuzzFeed, Discord, Pinterest, Peloton, Feedly, OKCupid, SoundCloud,... không thể truy cập.

Lợi dụng tình hình này, nhiều chủ tài khoản mạng xã hội đã phát tán thông tin về việc Facebook đang có chiến dịch rà quét nhằm chấm dứt hoạt động bán hàng online trên Facebook cá nhân.

Theo thông tin này, các chủ tài khoản đăng bài, up ảnh cá nhân liên tục quá giới hạn cho phép sẽ bị kiểm soát, bài đăng chuyển sang trạng thái "xoay vòng" và không thể mở được nick Facebook.

Nhóm người tung tin giả còn cảnh báo về việc các nick vi phạm sẽ bị Facebook cho "bay màu". Đối tượng phát tán tin giả cũng hướng dẫn người dùng đăng tải dòng chữ "Cmuk" với lời hứa hẹn "hiện lên chữ đỏ sẽ khắc phục được lỗi".

Ngay sau khi xuất hiện, thông tin này đã gây ra tâm lý hoang mang, lo sợ đối với cộng đồng bán hàng online trên Facebook tại Việt Nam. Do Facebook gặp phải sự cố trong thời gian nói trên, điều đó khiến nhiều người dùng càng có niềm tin vào đoạn thông tin giả mạo.

Hiện vẫn chưa rõ mục đích của những kẻ phát tán nội dung giả mạo. Tuy vậy, người dùng mạng xã hội không cần phải hoang mang bởi lỗi load ảnh trên Facebook là sự cố toàn cầu. Facebook cũng chưa đưa ra bất kỳ thông tin nào về việc thắt chặt hoạt động bán hàng trên Facebook cá nhân của người dùng mạng xã hội.

Bên cạnh đó, người dùng Facebook cần hết sức cảnh giác, không nên nghe theo hướng dẫn của kẻ tung tin đồn giả mạo nhằm tránh nguy cơ rò rỉ dữ liệu cá nhân và các rủi ro khác có thể xảy ra.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kiểm tra thông tin trên mạng xã hội trước khi làm theo và chia sẻ, luôn cảnh giác với các thông tin lừa đảo trên mạng.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/thong-tin-cam-ban-hang-online-tren-facebook-ca-nhan-la-gia-mao-547387.html

3. Người dùng cần duy trì chế độ Protected View của Microsoft Office

Chế độ "Xem an toàn" (Protected View) được tích hợp trong phần mềm Microsoft Office từ phiên bản 2010 giúp bảo vệ người dùng khỏi các rủi ro an toàn thông tin như lây nhiễm mã độc hại.

Khi chế độ này được kích hoạt, Office sẽ mở các tệp ở chế độ chỉ đọc, vô hiệu hóa các macro và nội dung ngoài. Thực tế, việc bỏ qua chế độ xem an toàn để soạn thảo tài liệu là khá đơn giản, bởi phần lớn người dùng không thực sự đánh giá đúng lợi ích của chế độ này. Có rất nhiều hướng dẫn tắt hẳn chế độ xem an toàn, tuy nhiên đây là hành động dễ dàng đưa người dùng vào nguy cơ lây nhiễm mã độc.

Một số kịch bản tấn công

Kịch bản thứ nhất

Tại kịch bản này, tin tặc chèn liên kết thay cho hình ảnh vào một văn bản Word được gửi qua thư điện tử. Hành động này có mục đích theo dõi khách hàng nào đã

nhận thư quảng cáo nếu mail client vô hiệu hóa thủ thuật theo dõi thư. URL trỏ tới hình ảnh sẽ có một mã định danh để nhận biết khách hàng nào đọc văn bản quảng cáo. Khi phần mềm Word mở một văn bản ở chế độ xem an toàn, nó sẽ chỉ hiển thị những nội dung chứa trong văn bản đó chứ không tải từ bên ngoài. Điều này có thể khiến cho văn bản không hiển thị đầy đủ, dù hình ảnh lấy từ bên ngoài chỉ là một chấm nhỏ.

Khi người dùng nhấn nút "Enable Editing", tức là đã tin tưởng vào văn bản và bắt đầu tải tất cả các tài nguyên bên ngoài để hiển thị đầy đủ văn bản. Đây chính là lúc cuộc tấn công thành công.

Việc chuẩn bị cho cuộc tấn công theo kịch bản này khá đơn giản. Thay vì chèn một bức ảnh bình thường, kẻ tấn công chỉ cần nhập một địa chỉ liên kết vào File name rồi chọn Link to File thay vì Insert.

Hơn nữa, khi Word truy cập máy chủ của kẻ tấn công để lấy hình ảnh, hắn sẽ biết được cả địa chỉ IP của nạn nhân và chuỗi "user-agent" bao gồm phiên bản của hệ điều hành, Office và Internet Explorer. Những thông tin đó có thể được dùng cho các cuộc tấn công sau này, chứ không chỉ đơn giản là tiết lộ thông tin một khách hàng đã xem quảng cáo.

Kịch bản thứ hai

Kịch bản này cũng thực hiện theo dõi khách hàng, nhưng có thể được thực hiện theo một cách khó nhận biết hơn. Khi kẻ tấn công dùng một mẫu văn bản (Word template) từ xa, người đọc sẽ không phát hiện các dấu hiệu dễ nhận thấy trong văn bản.

Kịch bản thứ ba

Kịch bản này giống như kịch bản thứ nhất là dùng liên kết trỏ tới máy chủ bên ngoài thay cho một hình ảnh bình thường, nhưng lại có thể giúp kẻ tấn công đánh cắp mật khẩu đăng nhập Windows của người đọc. Điểm khác biệt đó là thay vì dùng một địa chỉ HTTP, kẻ tấn công sẽ đổi thành một đường dẫn UNC – kiểu đường dẫn dược dùng trong các thư mục chia sẻ của Windows. Cách sửa thành đường dẫn UNC khá đơn giản: sau khi tạo liên kết trỏ tới máy chủ của mình và lưu văn bản Word, kẻ tấn công chỉ cần thực hiện các bước sau:

- Đổi phần mở rộng từ .docx thành .zip rồi kích đúp vào để mở như một thư mục thông thường.

- Tìm và sao chép tệp document.xml.rels (giả sử tệp Word có tên là "testfile" thì sẽ tìm thấy tệp cần tìm ở đường dẫn "testfile.zip\word_rels\document.xml.rels") ra thư mục khác. Sau đó, sử dụng Notepad để đổi địa chỉ trỏ tới hình ảnh thành dạng đường dẫn UNC và lưu lại.

- Chép đè tệp document.xml.rels vào trong tệp .zip.

- Đổi phần mở rộng tệp .zip thành .docx như ban đầu

Khi người nhận mở văn bản và bỏ qua chế độ xem an toàn, Word sẽ cho rằng hình ảnh còn thiếu nằm trên một máy chủ chia sẻ, cố gắng truy cập nó bằng cách gửi tên người dùng và giá trị băm của mật khẩu để xác thực. Kẻ tấn công dùng công cụ

responder để đóng giả một máy chủ chia sẻ tệp hợp lệ nhằm lấy cắp thông tin đăng nhập của người dùng. Mặc dù, Word sẽ báo lỗi cho người dùng, nhưng giá trị băm của mật khẩu mà người dùng gửi tới có thể được kẻ tấn công giải mã bằng công tụ john-the-ripper hay một công cụ tương tự.

Cách kích hoạt chế độ xem an toàn

Trên đây là 3 kịch bản tấn công đơn giản và dễ thực hiện nhất khi người dùng bỏ kích hoạt chế độ xem an toàn, ngoài ra còn nhiều phương pháp tấn công khác. Người dùng cần giữ chế độ xem an toàn, đồng thời biết cách kiểm tra xem chế độ này đang có được kích hoạt hay không bằng cách: Mở trình soạn thảo Word, Excel hay PowerPoint, chọn File/ Options. Trong cửa sổ Options, chọn mục Trust Center, nhấn nút Trust Center Settings, chọn mục Protected View.

Microsoft Word, PowerPoint và Excel đều có 3 thiết lập chính được kích hoạt mặc định là: Enable Protected View For Files Originating From The Internet (áp dụng cho các tệp từ Internet), Enable Protected View For Files Located In Potentially Unsafe Locations (áp dụng cho các tệp mở từ những thư mục được coi là không an toàn như Temporary Internet Files) và Enable Protected View For Outlook Attachments (áp dụng cho các tệp đính kèm trong thư điện tử mở bằng Microsoft Outlook). Nếu đã bỏ các tùy chọn này, người dùng cần nhanh chóng khôi phục lại trạng thái mặc định.

Riêng Excel có hai thiết lập khác bị bỏ kích hoạt theo mặc định là: Always Open Untrusted Text-Based Files (.csv, .dif and .sylk) In Protected View và Always Open Untrusted Database Files (.dbf) In Protected View.

Tuy nhiên, chế độ xem an toàn có một điểm gây bất tiện cho người dùng, là hiển thị văn bản ở chế độ Read Mode theo mặc định. Ở chế độ này, người dùng không nhìn thấy thanh di chuyển nên khó khăn hơn trong việc xem và sao chép văn bản. Để thấy lại thanh di chuyển trong văn bản, người dùng nhấn nút Esc để quay lại chế độ xem thông thường (vẫn không thể soạn thảo và duy trì trạng thái được bảo vệ). Nếu muốn loại bỏ chế độ Read Mode, mỗi khi mở những tệp có nguy cơ mất an toàn, người dùng chọn File/ Options rồi bỏ dấu chọn ở mục Open e-mail attachments and other uneditable files in reading view.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần kích hoạt tính năng Protected View trong Microsoft Office để đảm bảo an toàn thông tin.

Link tham khảo: http://www.antoanthongtin.vn/Detail.aspx?CatID=751fd4e7-4da5-4f31-85aa-be0240fe4910&NewsID=ad1b30a0-84a3-4d65-90ad-eda5dfef9dd4

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	Cisco	CVE-2019-1619 CVE-2019-1620 CVE-2019-1621 CVE-2019-1622 ...	Nhóm 04 lỗ hổng dựa trên một số sản phẩm của Cisco (Trung tâm dữ liệu Cisco DCNM) cho phép kẻ tấn công truy cập từ xa, chiếm quyền điều khiển, thực thi mã độc, tấn công cục bộ, xác thực các lệnh tùy ý.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2018-1858 CVE-2018-2011 CVE-2018-2013 CVE-2019-4382 …..	Nhóm 37 lỗ hổng dựa trên một số sản phẩm của IBM (API Connect, PureApplication, Security Access Manager) cho phép kẻ tấn công giả mạo yêu cầu thực hiện các hành động độc hại, thực hiện các câu lệnh SQL để xóa và sửa đổi thông tin trong cơ sở dữ liệu, thực hiện giải mã thông tin có độ nhạy cảm cao.	Đã có thông tin xác nhận và bản vá
3	LiveZilla	CVE-2019-12961 CVE-2019-12961 CVE-2019-12939 CVE-2019-12964 ……..	Nhóm 07 lỗ hổng trên máy chủ LiveZilla các phiên bản trước 8.0.1.1 dễ bị tấn công DoS, lỗ hổng trong SQL Injection và dễ bị XSS trong mobile.	Đã có thông tin xác nhận và bản vá.
4	Google	CVE-2017-5028 CVE-2018-16064 CVE-2018-16069 CVE-2018-17460 ……	Nhóm 73 lỗ hổng trên sản phẩm của Google (Chrome) cho phép kẻ tấn công từ xa rò rỉ dữ liệu thông qua trang HTML.	Đã có thông tin xác nhận và bản vá.
5	Mcafee	CVE-2019-3632 CVE-2019-3628 CVE-2019-3629 CVE-2019-3629 …	Nhóm 05 lỗ hổng trên một số sản phẩm của Mcafee (Security Manager (EMS)) cho phép người dùng xác thực quyền nâng cao, truy cập vào một thành phần hệ thống lỗi, thực thi mã tùy ý.	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	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	soplifan.ru
6	4m9k7jh1.ru
7	xjpakmdcfuqe.com
8	somicrososoft.ru
9	www.cityofangelsmagazine.com
10	kodklq.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.