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

1. Lưu ý sử dụng các nền tảng trò chuyện trực tiếp trong dịch Covid-19

Trong tình hình dịch bệnh Covid-19 căng thẳng, tin tặc có thể chuyển hướng mục tiêu nhắm vào các nền tảng trò chuyện trực tiếp. Người dùng cần cẩn trọng thực hiện các đầy đủ các khuyến nghị để đảm bảo an toàn cho sức khỏe cũng như bảo vệ thông tin cá nhân.

Dịch Covid-19 đã trở thành mối lo ngại hàng đầu trên toàn cầu. Các biện pháp đảm bảo an toàn buộc nhân viên phải tuân thủ khuyến nghị về Covid-19 hay chính sách của chủ lao động, bằng việc bắt đầu làm việc tại nhà nếu có thể.

Làm việc từ xa không phải là biện pháp duy nhất được khuyến nghị, vì hàng ngàn người cũng đã chủ động chọn tự cách ly tại nhà để tránh tiếp xúc với virus. Khi cách ly xã hội trở thành điều thông thường, thì con người ngày càng dựa vào thế giới số để giao tiếp, tương tác, làm việc, mua sắm và cung cấp các hỗ trợ cho nhau.

Nắm bắt được tình trạng này, tội phạm đang cố gắng sử dụng các thủ thuật để tấn công người dùng. Các cuộc tấn công có thể bao gồm: email lừa đảo, website độc hại hay các quảng cáo lừa đảo và tin nhắn giả mạo được gửi trên các nền tảng mạng xã hội và ứng dụng nhắn tin trực tiếp.

Các tác nhân độc hại có thể thực hiện nhiều hành vi xấu nhằm thu lợi bất chính từ người dùng, đặc biệt khi người dùng dựa vào Internet nhiều hơn bao giờ hết. Vì vậy, người dùng cần cẩn trọng khi sử dụng Facebook, Twitter, WeChat hoặc WhatsApp để liên lạc, trao đổi thông tin.

Trong khi Amazon đã loại bỏ hơn 1 triệu sản phẩm quảng cáo giả mạo nội dung liên quan đến cung cấp thông tin về sức khỏe trong việc chống lại dịch Covid-19, thì những kẻ lừa đảo đang lợi dụng các nền tảng mạng xã hội và ứng dụng nhắn tin để quảng cáo các sản phẩm lừa đảo, lan truyền sự hoảng loạn và thông tin sai lệch.

Vào cuối tháng 3/2020, Facebook, Google, Twitter và Reddit cho biết, họ đã cam kết trong việc chống lại thông tin sai lệch và giúp mọi người kết nối một cách an toàn nhất có thể.

Để giải quyết làn sóng tin tức giả mạo và lừa đảo, WhatsApp đã hợp tác với Tổ chức Y tế Thế giới để khai trương trung tâm thông tin về Covid-19, nhằm hỗ trợ giáo dục, doanh nghiệp và người lao động sử dụng ứng dụng trong thời gian này. Nỗ lực chung của các nền tảng trực tuyến trong việc kiểm chứng tin tức giả mạo về Covid-19 được đánh giá cao và rất cần thiết.

Tuy nhiên, tin tức giả mạo và lừa đảo không phải là mối đe dọa duy cần được quan tâm. Theo BitDefender, tội phạm mạng rất có thể sẽ chuyển sang các ứng dụng nhắn tin trực tiếp để gửi tin nhắn có nội dung về Covid-19, lừa người dùng nhấp vào các liên kết giả mạo trông có vẻ hợp pháp.

Khuyến nghị: Nếu người dùng nhận được bất kỳ tin nhắn đáng ngờ nào từ một nguồn không rõ ràng, hãy thực hiện theo các quy tắc đơn giản sau:

- Bỏ qua tin nhắn đó hoàn toàn.

- Không nhấp vào bất kỳ liên kết nào hoặc cung cấp bất kỳ thông tin cá nhân hay thực hiện thanh toán.

- Nếu nhà cung cấp dịch vụ hoặc điện thoại cho phép lọc tin nhắn cá nhân, hãy báo cáo tin nhắn là rác.

- Báo cáo bất kỳ hành vi lạm dụng, quảng cáo rác hoặc lừa đảo cho nhà cung cấp nền tảng.

- Nhận thông tin chính thức từ các nhà cung cấp dịch vụ y tế và chính quyền địa phương.

- Luôn cập nhật các giải pháp bảo mật.

Link tham khảo: http://antoanthongtin.vn/hacker-malware/luu-y-su-dung-cac-nen-tang-tro-chuyen-truc-tiep-trong-dich-covid-19-105954

2. Lộ dữ liệu 41 triệu người dùng Facebook VN

Như VietNamNet đã đưa tin, vào đêm qua, một lượng lớn dữ liệu người dùng Facebook đã bị chia sẻ công khai trên mạng Internet. Theo người đăng tải các dữ liệu này, đăng là thông tin cá nhân của khoảng 41 triệu tài khoản Facebook Việt Nam.

Khi bàn về tính khẩn cấp của sự việc, hiện đang có các luồng ý kiến trái chiều nhau xung quanh vụ việc.

Chia sẻ với Pv. VietNamNet, các chuyên gia của Công ty CP An ninh mạng Việt Nam (VSEC) cho biết, các dữ liệu vừa được chia sẻ là thông tin được thu thập theo kiểu crawler. Đây là kỹ thuật thu thập dữ liệu từ các website trên mạng theo một đường link cho trước.

Theo các chuyên gia, những dữ liệu này là thông tin mà người dùng public, trong đó không bao gồm thông tin riêng tư như mật khẩu. Do đó, người dùng cần nắm bắt đầy đủ thông tin và không nên lo lắng, tránh việc bị lừa đảo bởi những kẻ tống tiền.

Đồng tình với quan điểm này, anh D.Q.V - admin một diễn đàn công nghệ lớn tại Việt Nam cho rằng, dù mới chỉ xem qua, thế nhưng có thể thấy các dữ liệu này thiếu nhiều phần thông tin quan trọng.

Tệp dữ liệu rò ri chỉ bao gồm các trường thông tin cơ bản như họ tên, ngày tháng năm sinh, địa chỉ,... do đó nên không gây ảnh hưởng quá nghiêm trọng tới người dùng.

Tuy vậy, khi trao đổi với Pv. VietNamNet, anh D.Q.V đặt vấn đề về việc các dữ liệu mà hacker này có được có thể nhiều hơn thế. Nói một cách khác, những gì mà tin tặc công bố chỉ là phần nổi của tảng băng chìm.

“Với việc dễ dàng nắm trong tay dữ liệu của 41 triệu user Facebook, hacker rất có thể đang có nhiều thông tin quan trọng khác. Họ chỉ cung cấp những thông tin mà họ nghĩ rằng không còn quan trọng nữa. Tuy nhiên, cũng không loại trừ trường hợp những dữ liệu này được người đăng tải mua từ tay người khác.”, anh D.Q.V chia sẻ.

Bàn về mục đích của người chia sẻ dữ liệu, vị chuyên gia này cho rằng, tuy không chứa các thông tin nhạy cảm, những dữ liệu này đặc biệt phù hợp cho những

ai có nhu cầu làm marketing, quảng cáo online. Do vậy, mục đích tung ra tệp dữ liệu của hacker có thể là một hành động để chào mời nhằm mua bán, trao đổi dữ liệu.

Khuyến nghị: Người dùng cần đặc biệt lưu ý khi đưa các thông tin nhạy cảm lên mạng xã hội để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/lo-41-trieu-du-lieu-nguoi-dung-facebook-vn-co-the-hacker-van-em-hang-628083.html

3. Nhiều app Android trên Google Play lợi dụng Corona để phát tán mã độc

Sự bùng phát của dịch bệnh Corona đang trở thành 'món mồi ngon' cho những kẻ trục lợi. Chúng liên tiếp triển khai hàng loạt các cuộc tấn công mã độc, các chiến dịch lừa đảo; tạo ra các ứng dụng theo dõi độc hại, các trang web lừa đảo.

Các nhà phát triển ứng dụng Android bên thứ ba cũng bắt đầu tận dụng tình hình này, sử dụng các từ khóa liên quan đến Corona để đặt tên ứng dụng, đưa vào mô tả hoặc đặt tên gói tin để chèn mã độc, thực hiện hành vi trộm cắp tài chính hay để được xếp hạng cao hơn trong kết quả tìm kiếm trên Google Store.

"Hầu hết các ứng dụng độc hại có chứa từ ransomware đến mã độc SMS, thậm chí là phần mềm gián điệp được tạo ra với mục đích xóa sạch thông tin cá nhân hay dữ liệu liên quan đến tài chính trên thiết bị nạn nhân", các nhà nghiên cứu cho hay.

Sử dụng các từ khóa liên quan đến virus Corona để được xếp hạng cao trong tìm kiếm trên Game Play Store

Lợi dụng xu hướng tìm kiếm các ứng dụng cung cấp thông tin về Covid-19, tác giả các phần mềm độc hại lén lút chèn thêm adware, trojan ngân hàng (Anubis, Cerberus, Joker) và trình đánh cắp thông tin dưới vỏ bọc của các ứng dụng theo dõi trực tiếp cùng những thông tin xác định triệu trứng của dịch bệnh.

Theo một thống kê từ các chuyên gia an ninh mạng, kể từ ngày 1/1/2020, 579 ứng dụng có chứa các từ khóa liên quan đến virus Corona đã được tìm thấy. Trong số đó, 560 app an toàn, 9 là trojan và 10 là phần mềm độc hại.

Một số ứng dụng như Bubble Shooter Merge và Galaxy Shooter - Falcon Squad thậm chí còn đổi tên và nội dung mô tả bằng cách đưa thêm từ khóa liên quan đến dịch bệnh Corona để được xếp hạng cao hơn trong kết quả tìm kiếm coronavirus trong cửa hàng Google Play.

Thời gian gần đây, một loạt các cuộc tấn công liên quan đến Corona được tiến hành, từ các cuộc tấn công mạng đến tấn công lừa đảo, từ email tống tiền đến các trang web độc hại, lợi dụng chính nỗi sợ về Corona và sự thèm khát thông tin về đại dịch.

• Tấn công Bộ định tuyến - Một vụ tấn công được phát hiện gần đây đã nhắm mục tiêu vào các bộ định tuyến văn phòng nhỏ và gia đình để chuyển hướng người dùng đến các trang web độc hại giả mạo trang thông tin Covid-19, nhưng thực chất là cài đặt mã độc Oski đánh cắp mật khẩu.

• Tấn công Email Scam và Phishing - Các email spam liên quan đến vấn đề sức khỏe chiếm gần 2,5% tổng khối lượng thư rác, cho thấy các vụ lừa đảo qua email liên quan đến đại dịch đã tăng đều đặn chỉ trong tháng 3. Ít nhất 42.578 tên miền "covid"

hoặc "corona" đã được đăng ký mới kể từ đầu tháng, trung bình mỗi ngày có hơn 2.500 tên miền mới được đăng ký trong hai tuần qua.

• Tấn công Spear Phishing - Những kẻ tấn công đang tích cực lợi dụng tên, logo của nhiều công ty và tổ chức trong các chiến dịch tống tiền và lừa đảo, bao gồm Tổ chức Y tế Thế giới (WHO) và Trung tâm Kiểm soát Bệnh Hoa Kỳ (CDC). Chúng gửi các tài liệu RTF nhằm lừa nạn nhân tải trình đánh cắp thông tin, RAT, trình thu thập thông tin xác thực.

• Tấn công Ransomware - Tội phạm mạng đứng sau ransomware Maze đã tấn công vào mạng lưới IT của Viện nghiên cứu Hammersmith (HMR), nơi tiến hành thử nghiệm vắc-xin chống Corona. Chúng công bố thông tin cá nhân của hàng ngàn bệnh nhân sau khi tổ chức này từ chối trả tiền chuộc. Sự việc diễn ra ngay sau khi nhóm tội phạm mạng đưa ra lời hứa công khai không tấn công các tổ chức nghiên cứu y tế trong đại dịch Corona.

• Ứng dụng giả - Các chiến dịch và các ứng dụng lừa đảo tận dụng đại dịch Covid-19 có dấu hiệu gia tăng. Kẻ xấu có nhiều phương thức lừa đảo khác nhau, như giả danh bán thuốc chữa Corona, bán khẩu trang, hoặc kêu gọi đầu tư vào các công ty lừa đảo điều chế vắc xin, hay kêu gọi người dùng quyên góp cho các tổ chức từ thiện giả danh.

• Mã độc ngân hàng và hack thẻ thanh toán – Hacker phát triển trojan ngân hàng Ginp bắt đầu sử dụng thông tin về những người bị nhiễm Corona làm mồi nhử để dụ người dùng Android tại Tây Ban Nha cung cấp dữ liệu thẻ tín dụng.

Khuyến nghị: Người dùng chỉ nên cài đặt ứng dụng từ các nguồn hợp pháp, tìm kiếm thông tin từ các nguồn chính thống và cảnh giác với bất kỳ email nào có tệp đính kèm hoặc liên kết để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/nhieu-app-android-tren-google-play-loi-dung-corona-de-phat-tan-ma-doc.13407/

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	Apache	CVE 2020 1953 CVE 2019 10091 CVE 2019 12416	Nhóm 03 lỗ hổng trên một số thành phần của Apache (DeltaSpike, Commons Confifuration, Geode) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công nghe lén.	Đã có thông tin xác nhận và bản vá.
2	Android	CVE 2019 2058 CVE 2019 2089 CVE 2019 2088 …	Nhóm 08 lỗ hổng trên hệ điều hành Android (Android 10 Andorid ID:A 38390530,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
3	Gitlab	CVE 2020 10074 CVE 2020 10077 CVE 2020 10083 …	Nhóm 20 lỗ hổng trên Gitlab (Gitlab EE 3.0, Gitlab 10.1,…) cho phép đối tượng tấn công thu thập thông tin, tấn công SSRF, tấn công XSS, tấn công DoS, tấn công HTML Injection.	Đã có thông tin xác nhận và bản vá
4	Vmware	CVE 2019 5543 CVE 2020 3947 CVE 2019 19023 …	Nhóm 09 lỗ hổng trên sản phẩm của Vmware (Vmware Horizon Client for Windows,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công DoS, SQL injection, tấn công CSRF.	Đã có thông tin xác nhận và bản vá
5	Wordpress	CVE 2020 10564 CVE 2018 18576 CVE 2020 7916 …	Nhóm 08 lỗ hổng trên phần mềm Wordpress (File Upload plugin,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công XSS.	Đã có thông tin xác nhận và bản vá
6	Cisco	CVE 2020 3266 CVE 2020 3265 CVE 2020 3264 …	Nhóm 05 lỗ hổng trên thiết bị của Cisco (SD WAN Solution,…) cho phép đối tượng tấn công thực thi lệnh tùy	Chưa có thông tin xác nhận và bản vá

			ý với quyền root, tấn công SQL Injection.	
7	Asus	CVE 2018 20333 CVE 2018 20335 CVE 2018 20334	Nhóm 03 lỗ hổng trên các thiết bị của Asus (ASUSWRT 3.0.0.4.284.20308,…) cho phép đối tượng tấn công tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
8	D-link	CVE 2019 12767 CVE 2019 15656 CVE 2019 15655	Nhóm 03 lỗ hổng trên thiết bị D link (D link DAP 1650, DSL 2875AL,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa.	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	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	ydbnsrt.me
6	cp.3b1ffvf2.ru
7	xjpakmdcfuqe.biz
8	xdqzpbcgrvkj.ru
9	40.121.206.97
10	xjpakmdcfuqe.in

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.