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

1. An toàn thông tin đối với các dịch vụ tài chính ngân hàng trên mạng viễn thông di động

Các dịch vụ tài chính ngân hàng trên mạng di động như thông báo thay đổi số dư, tra cứu thông tin, lịch sử giao dịch,… đã mang tới rất nhiều tiện ích cho người dùng. Tuy nhiên, các dịch vụ này cũng tồn tại những nguy cơ mất an toàn thông tin do tin tặc khai thác lỗ hổng, từ đó lấy được thông tin tài chính của khách hàng và đánh cắp tiền khỏi tài khoản. Bài viết sẽ trình bày về những nguy cơ mất an toàn thông tin đối với dịch vụ này và đưa ra một số khuyến nghị cho các đơn vị cung cấp dịch vụ tài chính ngân hàng.

Hiện nay, mạng viễn thông di động ngày càng được tích hợp mạnh mẽ với các dịch vụ tài chính ngân hàng, từ việc thông báo thay đổi số dư, đến chủ động tra cứu thông tin về hạn mức tín dụng, lịch sử giao dịch, chuyển tiền, nạp thẻ, thanh toán hóa đơn,… đều có thể được thực hiện bằng SMS/USSD. Với các giao dịch, thủ tục quan trọng hơn, cần bảo vệ nâng cao như kích hoạt tài khoản, đặt lại mật khẩu, chuyển tiền, thì SMS/USSD sẽ được dùng để thực hiện mã xác thực 2 lớp OTP. Đây là các tiện ích mà người dùng đã quen thuộc khi sử dụng các dịch vụ như SMS Banking, Internet Banking, ví điện tử, ví di động, ví tiền ảo, chứng khoán trực tuyến,…

Tuy nhiên khi khảo sát thực tế, nhóm nghiên cứu Viettel đã nhận thấy một số vấn đề như sau:

- Nhiều tổ chức tài chính ngân hàng cho phép khách hàng truy vấn thông tin mà không cần mật khẩu. Điều này có nghĩa là chỉ cần nhắn tin SMS từ thuê bao di động đã được đăng ký trước, thì có thể tra cứu số dư của khách hàng đó và xem được thông tin, sao kê tài khoản.

- Một số dịch vụ SMS Banking không bật tính năng chống tấn công vét cạn (brute-force) giúp tin tặc có thể chuyển tiền thành công khỏi tài khoản người dùng.

- Đa phần mã PIN, mật khẩu của các dịch vụ SMS Banking, ví điện tử ở dạng dễ nhớ, chỉ gồm 6-8 ký tự và nhiều khi chỉ là số. Điều này mang lại sự thuận tiện cho khách hàng nhưng lại là lỗ hổng khiến tin tặc dễ dàng khai thác.

- Các dịch vụ tài chính ngân hàng phần lớn đang phụ thuộc vào khả năng bảo mật của các hạ tầng mạng viễn thông di động bên dưới. Có thể lấy ví dụ, đối với dịch vụ truy vấn thông tin qua SMS banking, việc xác thực hoàn toàn dựa trên khả năng xác thực thuê bao của nhà mạng viễn thông. Mật khẩu và OTP gửi đi qua SMS đa phần là không được mã hóa.

Thực tế là không phải mạng di động nào cũng thực sự an toàn. Gần đây, tại các diễn đàn và hội thảo bảo mật lớn, cũng như trong nội bộ cộng đồng Hiệp hội Hệ thống thông tin di động toàn cầu (Global System for Mobile Communications - GSMA) và Liên minh Viễn thông Quốc tế (International Telecommunication Union - ITU), đã có nhiều cảnh báo về các lỗ hổng ở tầng ứng dụng viễn thông trong mạng báo hiệu giữa các nhà mạng di động trên toàn thế giới. Đây là các lỗ hổng mà tường

lửa truyền thống, hệ thống IDS, IPS cho các hệ thống công nghệ thông tin thông thường và các mạng TCP/IP phổ biến không thể phát hiện và ngăn chặn được.

Khi khai thác được các lỗ hổng này, tin tặc có thể thực hiện được một số hoặc tất cả những tấn công sau và từ đó có thể lấy được thông tin tài chính hoặc đánh cắp tiền khỏi tài khoản, ví điện tử của người dùng:

- Tra cứu thông tin thuê bao: Tin tặc có thể lấy trộm được thông tin về vị trí, tình trạng tắt/mở máy của thuê bao để lựa chọn thời điểm tấn công vào tài khoản tài chính ngân hàng, hoặc làm cơ sở để thực hiện các tấn công lừa đảo phi kỹ thuật. Đây cũng là bước lấy các thông tin khác cần thiết của thuê bao để thực hiện các tấn công leo thang.

- Nghe trộm cuộc gọi hoặc đọc trộm tin nhắn SMS: Sau khi tấn công và thu thập được những thông tin cần thiết, tin tặc có thể lấy được mật khẩu mà người dùng nhắn đi qua SMS hoặc lấy được OTP từ SMS hoặc cuộc gọi xác thực.

- Giả mạo thuê bao: Nếu khai thác lỗ hổng thành công, tin tặc còn có thể giả mạo số điện thoại đã đăng ký dịch vụ tài chính ngân hàng để thực hiện giao dịch với các tổng đài dịch vụ.

Tin tặc có thể khai thác các lỗ hổng để đọc tin nhắn nhằm lấy mật khẩu SMS banking, lấy mã OTP xác thực giao dịch hoặc có thể giả mạo SMS/USSD từ ngân hàng để lừa lấy mật khẩu Internet Banking

Trong một báo cáo mới đây của ITU có tên "Báo cáo kỹ thuật về lỗ hổng mạng báo hiệu SS7 và các biện pháp xử lý cho các giao dịch của các dịch vụ tài chính", khi thực hiện khảo sát tại Châu Âu, chỉ có chưa đến 30% nhà mạng có ý thức về nguy cơ bị tấn công và khoảng 5% nhà mạng đã triển khai giải pháp bảo vệ.

Vào tháng 01/2019, một số khách hàng tại ngân hàng Metro Bank, Anh đã bị đánh cắp tiền khỏi tài khoản. Metro Bank đã xác nhận sự cố và cho biết các tin tặc đã khai thác lỗ hổng trong mạng viễn thông để đánh cắp mã xác thực của các thuê bao gắn với các tài khoản ngân hàng. Trước đó vào tháng 05/2017, các thuê bao của nhà mạng O2-Telefonica tại Đức cũng đã bị tấn công tương tự và bị đánh cắp tiền khỏi tài khoản ngân hàng.

Tại Việt Nam, người dùng có thể tra cứu thông tin thuê bao của một số mạng chỉ với chi phí không đáng kể thông qua một dịch vụ trực tuyến hoàn toàn công khai. Chỉ cần nhập vào số điện thoại và hệ thống sẽ cho biết nhà mạng của thuê bao, số định danh thuê bao di động quốc tế IMSI để tấn công leo thang và tổng đài di động (MSC) đang phục vụ để tấn công leo thang hoặc biết vị trí mức quận huyện, tỉnh thành.

Tuy nhiên, khi nhập vào số thuê bao của nhà mạng Viettel, trang web sẽ không trả lại thông tin nào. Đó là nhờ hệ thống Telecom Anomaly Detection (TAD) mà Viettel đã nghiên cứu phát triển và triển khai vào mạng lưới từ năm 2015 để bảo vệ các thuê bao cũng như đảm bảo an toàn cho các dịch vụ tài chính ngân hàng trên đó. Hệ thống TAD giám sát toàn bộ lưu lượng báo hiệu ra/vào mạng Viettel, từ đó phát hiện và ngăn chặn các tấn công có thể phát sinh. Hiện tại, hàng tháng, hệ thống TAD

đã ngăn chặn hàng trăm nghìn tấn công vào mạng lưới và thuê bao Viettel. Con số này đã giảm đi nhiều so với trước đây do nhiều tin tặc sau khi tấn công không thành công đã từ bỏ mạng Viettel. Năm 2015, khi mới triển khai, hệ thống TAD còn ghi nhận thời gian cao điểm lên đến hơn 50.000 tấn công chỉ trong vòng 1 giờ.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cảnh giác khi nhận được các tin nhắn nghi ngờ, không cung cấp thông tin tài khoản của mình để đảm bảo an toàn thông tin.

Link tham khảo: http://antoanthongtin.vn/hacker-malware/an-toan-thong-tin-doi-voi-cac-dich-vu-tai-chinh-ngan-hang-tren-mang-vien-thong-di-dong-105741

2. Người dùng Windows 10 cần cập nhật phần mềm ngay vì một lỗ hổng nghiêm trọng vừa được phát hiện

NSA kêu gọi mọi người dùng Windows 10 cập nhật phần mềm sau khi phát hiện lỗ hổng nghiêm trọng trong hệ điều hành này. Sau khi phát hiện, NSA đã cảnh báo cho Microsoft. Giám đốc An ninh mạng của NSA, Anne Neuberger, xác nhận cơ quan đã báo cho Microsoft về lỗ hổng.

Microsoft tung ra bản vá vào trưa ngày 14/1 (giờ địa phương) cho Windows 10 cũng như Windows Server 2016 và Windows Server 2019. Công ty chưa tìm thấy bằng chứng nào cho thấy hacker đã khai thác lỗ hổng nhưng hối thúc mọi người dùng Windows 10 cài đặt bản cập nhật.

Lỗ hổng cho phép kẻ tấn công nhằm vào người dùng hệ điều hành Windows 10 chưa vá lỗi với mã độc giả mạo chữ ký số của một nhà cung cấp đáng tin cậy. Nếu người dùng tải file dính mã độc này, hacker sẽ tiếp cận được "thông tin bí mật" lưu trữ trên máy tính.

Theo bà Neuberger, đây là lần đầu tiên NSA tiết lộ lỗ hổng với Microsoft. Còn theo Amit Yoran, Giám đốc sáng lập Đội sẵn sàng ứng cứu máy tính của Bộ An ninh nội địa Mỹ, việc một cơ quan chính phủ chia sẻ phát hiện của mình về lỗ hổng nghiêm trọng với nhà sản xuất là rất hiếm, nếu không muốn nói là chưa có tiền lệ. Nó cho thấy sự thay đổi đáng chú ý từ các hoạt động thông thường và khiến lỗ hổng này cũng rất đáng quan tâm.

Không rõ NSA biết về lỗ hổng bao lâu trước khi báo cáo cho Microsoft. Trong quá khứ, các cơ quan an ninh hàng đầu thường giữ bí mật về các lỗ hổng lớn.

Khuyến nghị: Người dùng cần cập nhật bản vá mới nhất của Windows 10 để đảm bảo an toàn thông tin.

Link tham khảo: https://ictnews.vietnamnet.vn/cntt/bao-mat/khan-nguoi-dung-windows-10-can-cap-nhat-phan-mem-ngay-vi-mot-lo-hong-nghiem-trong-vua-duoc-phat-hien-194155.ict

3. Google thử nghiệm tấn công từ xa iPhone không cần tương tác người dùng

Một lỗ hổng trong phiên bản iOS cũ hơn cho phép kẻ tấn công xâm nhập vào điện thoại iPhone từ xa mà không cần bất kỳ tương tác nào của người dùng.

Lỗ hổng, được phát hiện trong iOS 12.4 và đã được khắc phục trong iOS 12.4.1 vào giữa năm 2019, về cơ bản cho phép kẻ xấu truy cập vào hầu hết mọi thứ trên iPhone, nhà nghiên cứu của Google cho biết.

Điều duy nhất mà hacker cần là Apple ID của người sử dụng để khởi động một cuộc tấn công, vốn chỉ mất vài phút. Sau đó, kẻ tấn công có thể truy cập các tệp, mật khẩu, mã xác thực hai yếu tố, SMS, tin nhắn khác, email và dữ liệu ứng dụng. Tệ hơn nữa, hacker có thể kích hoạt micro và camera để theo dõi người dùng iPhone.

Lỗ hổng, CVE-2019-8641, cho phép tin tặc bỏ qua ASLR (Ngẫu nhiên hóa sơ đồ không gian địa chỉ), sau đó khởi chạy thực thi mã từ xa bên ngoài sandbox mà không cần người dùng phải làm gì.

Nhà nghiên cứu Google giải thích dù lỗ hổng đã được giải quyết, cần phải có các biện pháp giảm thiểu bổ sung để ngăn chặn các vấn đề tương tự.

Mặc dù lỗ hổng cho phép kẻ tấn công hoàn toàn xâm nhập iPhone, chỉ các thiết bị chạy iOS 12.4 bị ảnh hưởng. Vì vậy người dùng được khuyến cáo cập nhật lên phiên bản mới nhất càng sớm càng tốt.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng hệ điều hành iOS cần cập nhật lên phiên bản mới để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/google-thu-nghiem-tan-cong-tu-xa-iphone-khong-can-tuong-tac-nguoi-dung.13153/

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	Wordpress	CVE-2019-20041 CVE-2013-4693 CVE-2019-20141 …	Nhóm 13 lỗ hổng trên một số thành phần của phần mềm Wordpress (Xorbin Digital Flash Clock,...) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá.
2	Apache	CVE-2019-17558	01 lỗ hổng trên phần mềm Apache (Apache Solr 5.0.0, Apache Solr 8.3.1…) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
3	D-link	CVE-2018-7859 CVE-2019-20213 CVE-2019-17621	Nhóm 03 lỗ hổng trên thiết bị D-link (DGS-1510-series, DIR-859,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
4	Gitlab	CVE-2019-19254 CVE-2018-20507 CVE-2018-20488 …	Nhóm 29 lỗ hổng trên một số thành phần của Gitlab (Gitlab Enterprise Edition, Community and Enterprise Edition,...) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
5	Chrome	CVE-2019-5276 CVE-2019-5265 CVE-2019-5266 …	Nhóm 05 lỗ hổng trên hệ điều hành Chrome (trước version 73.0.3683.75) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
6	Linux	CVE-2019-19927 CVE-2019-20095 CVE-2019-20096	Nhóm 03 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
7	HP	CVE-2019-11994 CVE-2019-11993	Nhóm 02 lỗ hổng trên một số sản phẩm của thiết bị HP (HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen	Chưa có thông tin xác nhận và bản vá

			10,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	

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

STT	**Tên miền/IP**
1	mel.cloudcontentsmak.com
2	strikotunrev.top
3	kartop.at
4	localhost.localdomain
5	d3s1.me
6	strikotunrev.top

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.