BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: **23**/BC-CATTT

Hà Nội, ngày 05 tháng 6 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 22/2018
(từ ngày 28/5/2018 đến ngày 03/6/2018)

BẢNG TỔNG HỢP

1. Một báo cáo vừa được Bộ An ninh Nội địa và Bộ Thương mại Hoa Kỳ phối hợp nghiên cứu, tổng hợp để báo cáo Tổng thống đã đi sâu phân tích nhiều vấn đề an toàn thông tin. Trong đó bao gồm nhiều nội dung đề cập đến các cuộc tấn công mạng bằng mạng máy tính bị nhiễm mã độc (botnet) đang là một vấn đề toàn cầu.

2. "Dự án Indigo", cho phép thiết lập một kênh chia sẻ thông tin tấn công mạng giữa Trung tâm Phân tích và Chia sẻ Thông tin Dịch vụ Tài chính (FS-ISAC) với cơ quan chức năng về ATTT mạng của Chính phủ Hoa Kỳ. Thông tin được chia sẻ thông qua Trung tâm Phân tích và Phục hồi Hệ thống Tài chính (FSARC).

3. Hãng Avast mới đây đã công bố báo cáo kỹ thuật về một loại mã độc quảng cáo ảnh hưởng tới hàng nghìn người sử dụng thiết bị Android trên thế giới.

1. Điểm tin đáng chú ý

1.1. Một chương trình thí điểm, có tên là "Dự án Indigo", cho phép thiết lập một kênh chia sẻ thông tin tấn công mạng giữa Trung tâm Phân tích và Chia sẻ Thông tin Dịch vụ Tài chính (FS-ISAC) với cơ quan chức năng về ATTT mạng của Chính phủ Hoa Kỳ. Thông tin được chia sẻ thông qua Trung tâm Phân tích và Phục hồi Hệ thống Tài chính (FSARC). Mục đích chính của Dự án Indigo là giúp thông báo cho Chính phủ Hoa kỳ về các cuộc tấn công mang tính quốc gia nhằm vào các ngân hàng. Một số tổ chức tài chính tham gia vào thỏa thuận đồng ý cho FSARC chia sẻ thông tin là: BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street và Wells Fargo.

Theo một thông cáo báo chí của FSARC, tổ chức này có nhiệm vụ chủ động xác định, phân tích, đánh giá và điều phối các hoạt động nhằm giảm thiểu rủi ro cho hệ thống tài chính của Hoa Kỳ từ các nguy cơ mất ATTT mạng thông qua các hoạt động tăng cường hợp tác giữa các cơ quan, tổ chức tham gia, các đối tác trong lĩnh vực tài chính, ngân hàng và chính phủ Hoa Kỳ.

1.2. Bộ An ninh Nội địa và Bộ Thương mại Hoa Kỳ vừa phối hợp nghiên cứu, tổng hợp một báo cáo phân tích sâu nhiều vấn đề an toàn thông tin để và báo cáo lên Tổng thống. Báo cáo bao gồm nhiều nội dung đề cập đến các cuộc tấn công mạng bằng mạng máy tính bị nhiễm mã độc (botnet) đang là một vấn đề toàn cầu, các thiết bị phải được bảo đảm ATTT tốt hơn và người sử dụng cần phải được đào tạo, tuyên truyền tốt hơn về việc làm thế nào để bảo vệ thiết bị của mình. Những cuộc tấn công bằng mã độc không phải là một vấn đề có thể giải quyết được bởi một cá nhân hay tổ chức đơn lẻ.

Báo cáo cũng liệt kê các mục tiêu cần thiết để cải thiện tình hình lây nhiễm mã độc như:

Mục tiêu 1: Xác định một lộ trình rõ ràng hướng đến thị trường công nghệ có khả năng thích nghi, tự cung ứng và bảo đảm an toàn.

Mục tiêu 2: Khuyến khích đổi mới trong cơ sở hạ tầng để có khả năng thích nghi nhanh chóng với các nguy cơ đang biến đổi.

Mục tiêu 3: Khuyến khích đổi mới để ngăn chặn, phát triển và giảm thiểu các cuộc tấn công tự động, phân tán.

Mục tiêu 4: Khuyến khích và hỗ trợ sự phối hợp giữa các cộng đồng ATTT cho cơ sở hạ tầng và công nghệ điều hành trong nước và toàn thế giới.

Mục tiêu 5: Nâng cao nhận thức và đào tạo trên toàn hệ sinh thái.

1.3. Hãng Avast mới đây đã công bố báo cáo kỹ thuật về một loại mã độc quảng cáo ảnh hưởng tới hàng nghìn người sử dụng thiết bị Android trên thế giới. Cụ thể, Avast đã tìm ra nhiều phần mềm quảng cáo được cài đặt sẵn trên một vài phiên bản và thiết bị Android, bao gồm những thiết bị từ nhà sản xuất như ZTE và Archos. Hầu hết các thiết bị này không được Google xác nhận.

Phần mềm quảng cáo mà Avast phân tích có tên là Cosiloon, khi lây nhiễm trên máy người dùng sẽ tạo một lớp hiển thị nội dung quảng cáo chồng lên lớp hiển thị chính của trang web. Mã độc này rất khó bị phát hiện hay bóc gỡ vì nó được cài đặt ở mức firmware. Theo thống kê từ Avast, hiện có ít nhất 18.000 thiết bị phân bố tại hơn 100 quốc gia đã cài đặt phần mềm độc hại này.

Các mẫu mã độc Cosiloon mà Avast thu thập đều có đặc điểm tương tự bất kỳ loại phần mềm quảng cáo khác, phổ biến nhất là:

- com.google.eMediaService
- com.google.eMusic1Service
- com.google.ePlay3Service
- com.google.eVideo2Service

Qua phân tích, các nhà nghiên cứu phát hiện những gói phần mềm độc hại này được tạo ra từ một ứng dụng độc hại (dropper) cài đặt sẵn bởi nhà sản xuất thiết bị với số lượng rất lớn. Phần mềm dropper là một ứng dụng tự động tải và cài đặt ứng dụng độc hại khác. Đặc biệt hơn nữa, những tập tin APK của dropper có ngày phát hành từ 7/3/2013 tới 1/1/2016, cho thấy nó đã được phát triển liên tục.

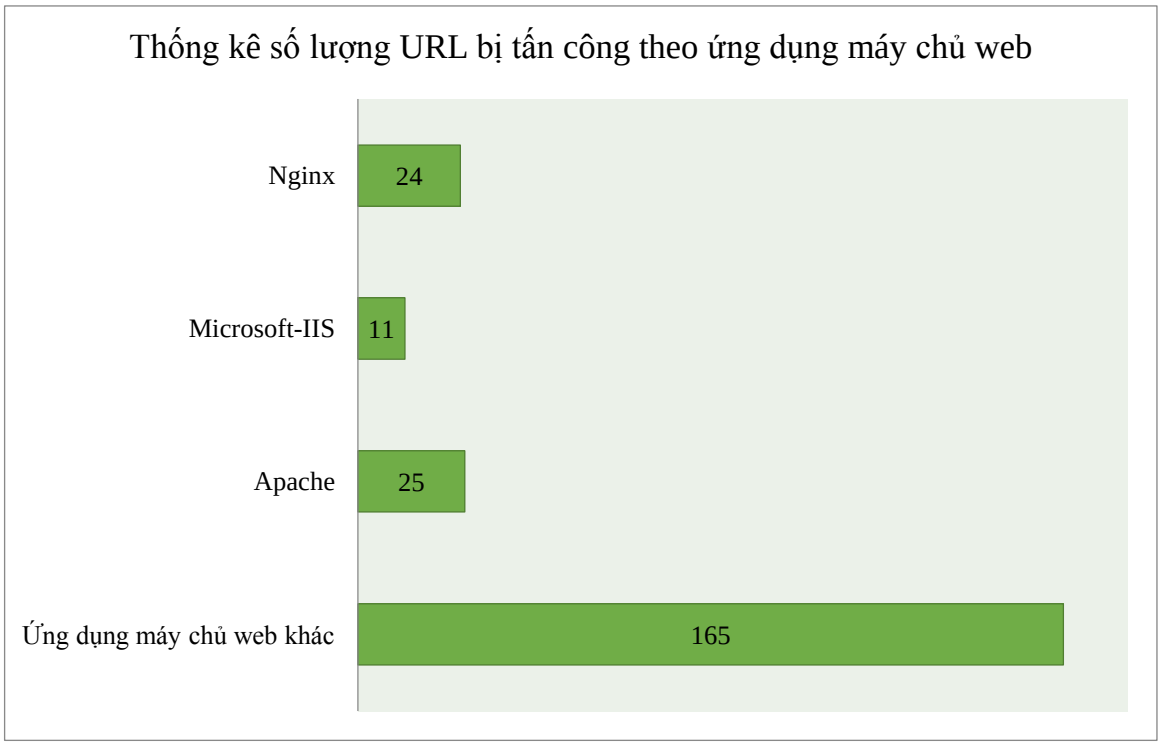
Một vài phần mềm quảng cáo sẽ bị phát hiện và chặn bởi trình antivirus, tuy nhiên phần mềm dropper có thể ngay lập tức cài đặt lại hoặc tải phần mềm khác mà trình antivirus không phát hiện được. Và nếu như dropper không được gỡ bỏ triệt để, đối tượng tấn công luôn có cách để cài đặt bất kỳ phần mềm nào lên thiết bị, bao gồm cả mã độc nguy hiểm như ransomware, spyware, v.v…

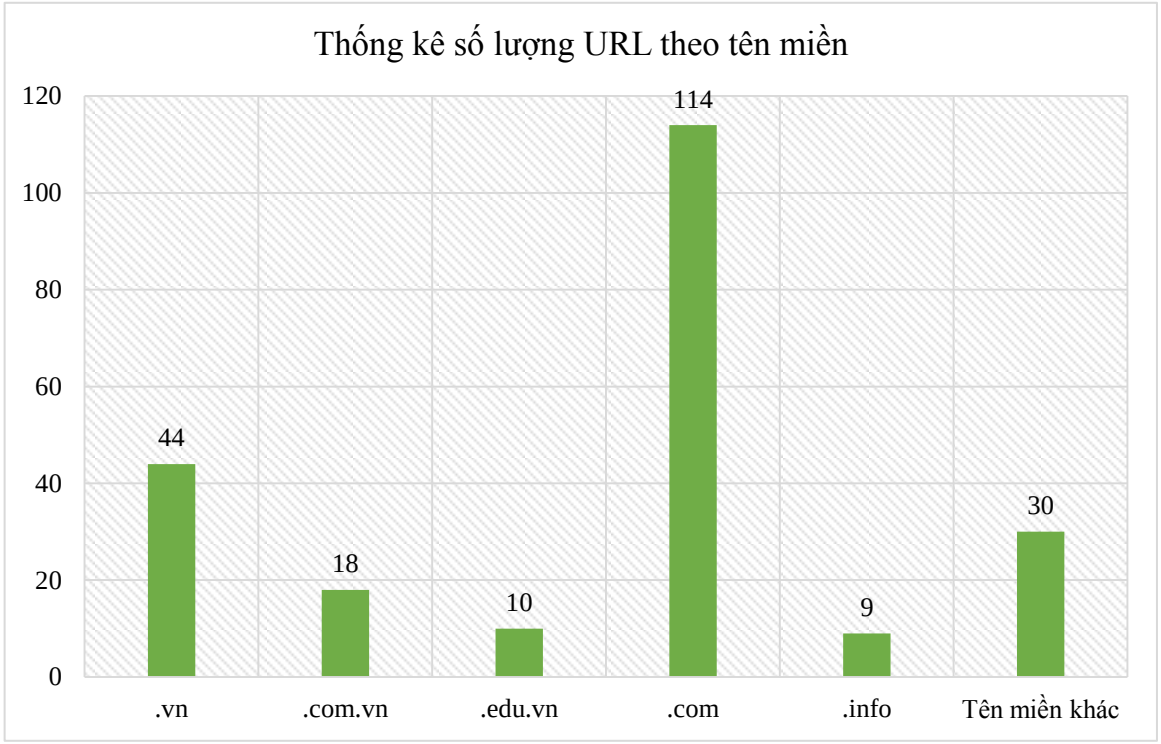
Sau khi nhận được thông tin, hãng công nghệ Google cũng đã đưa ra giải pháp để giảm thiểu khả năng ảnh hưởng của các biến thể mã độc trên một số dòng thiết bị nhất định. Ngoài việc cập nhật Google Play Protect đảm bảo ngăn chặn những ứng dụng này, Google đã liên hệ và cảnh báo với những nhà phát triển firmware để giải quyết vấn đề. Thống kê của Avast cho thấy số lượng thiết bị bị lây nhiễm đã giảm đáng kể sau khi Google Play Protect phát hiện mã độc Cosiloon. Người dùng cũng có thể tìm và vô hiệu hóa mã độc trong tùy chỉnh thiết bị, thường có tên “CrashService”, “ImeMess” hoặc “Terminal” với biểu tượng hệ điều hành Android thông thường.

2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua, Cục ATTT nhận thấy trên không gian mạng đang tồn tại nhiều trang web Việt Nam (bao gồm cả những trang web sử dụng dịch vụ máy chủ nước ngoài) bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc (gần đây nhất là cài đặt và phát tán mã độc để đào tiền ảo); lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng .v.v…).

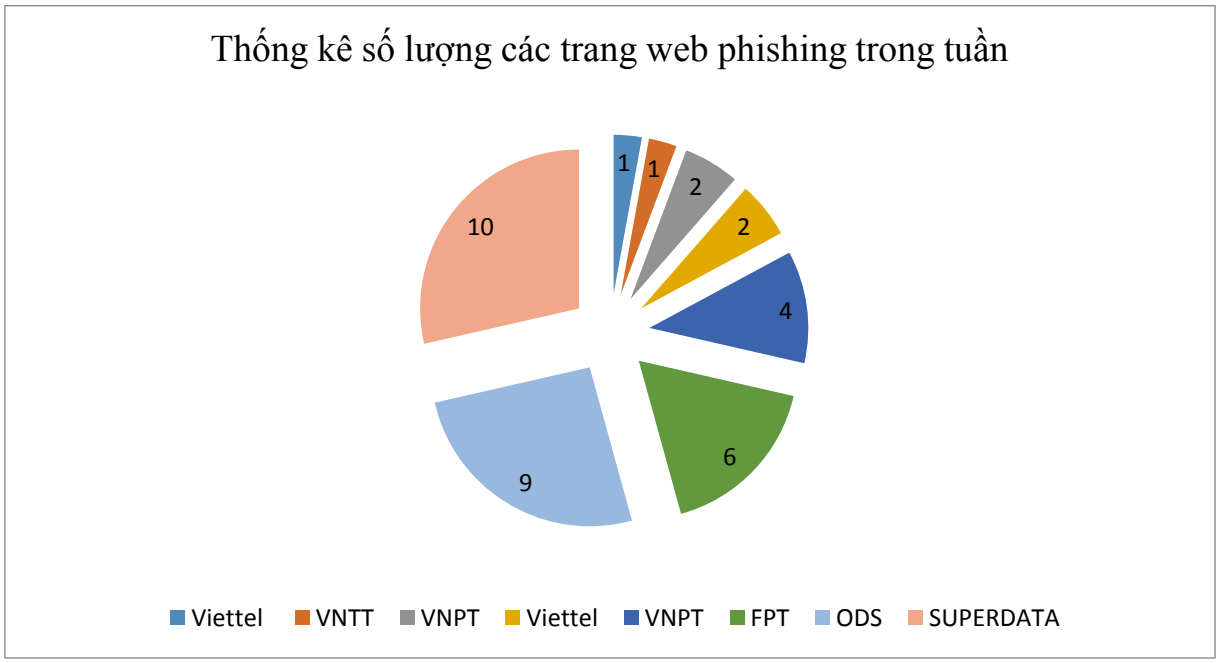
Trong tuần, Cục ATTT ghi nhận có ít nhất **225** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



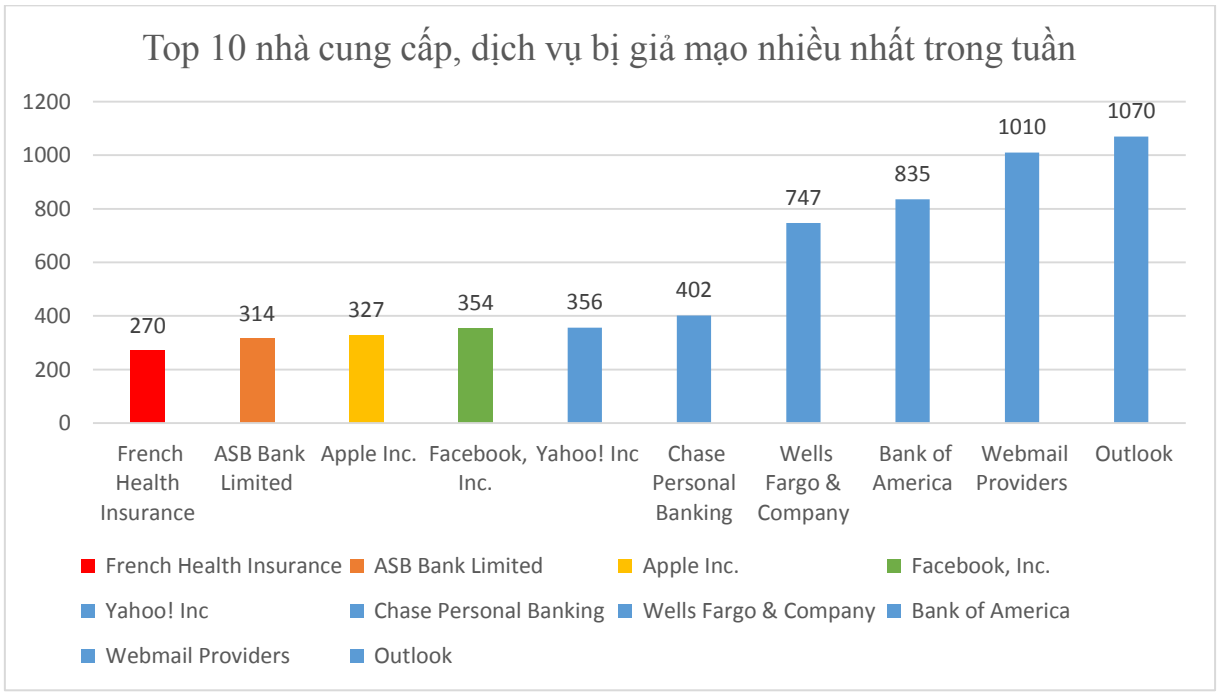


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **35** trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



3.2. Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như Facebook, PayPal, Dropbox .v.v…



Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và có phí) như Facebook, Dropbox .v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

4. Lỗ hổng/điểm yếu an toàn thông tin trong tuần

4.1. Trong tuần, các tổ chức quốc tế đã công bố ít nhất 400 lỗ hổng, trong đó có ít nhất 84 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 18 lỗ hổng đã có mã khai thác.

4.2. Hệ thống kỹ thuật của Cục An toàn thông tin chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có **08** nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam, như: Nhóm 11 lỗ hổng trên nhiều sản phẩm của IBM; Nhóm 5 lỗ hổng trên nhiều sản phẩm máy tính, điện thoại thông minh và máy chủ của Huawei ..v.v.

4.3. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Dell	CVE-2018-1241 CVE-2018-1235 Cve-2018-1242	Nhóm 03 lỗ hổng trên phần mềm bảo vệ dữ liệu EMC RecoverPoint trước phiên bản 5.1.2 và RecoverPoint trên Linux trước phiên bản 5.1.1.3 có thể gây lộ mật khẩu khi lưu trữ mật khẩu dưới dạng rõ trên log của phần mềm, và cho phép đối tượng tấn công thực thi mã lệnh hoặc đọc các tệp RPA.	Chưa có thông tin xác nhận và bản vá
2	Huawei	CVE-2018-7976 CVE-2018-17171 CVE-2018-7949 CVE-2018-7951 CVE-2018-7950	Nhóm 5 lỗ hổng trên nhiều sản phẩm máy tính, điện thoại thông minh và máy chủ của Huawei cho phép đối tượng tấn công thực hiện tấn công XSS, làm treo thiết bị, thậm chí chiếm đặc quyền quản trị hệ thống	Đã có thông tin xác nhận
3	IBM	CVE-2018-1532 CVE-2018-1496 CVE-2018-1450	Nhóm 11 lỗ hổng trên nhiều sản phẩm của IBM cho phép đối tượng thực hiện nhiều phương pháp tấn công để	Đã có thông tin xác nhận và bản vá

		CVE-2018-1495 CVE-2018-1369 …	đánh cắp thông tin quan trọng, ghi đè tệp từ xa, chỉnh sửa dữ liệu bảo mật,...	
4	Tp-link	CVE-2018-11481 CVE-2018-11482	Nhóm 02 lỗ hổng trên một số dòng sản phẩn của Tp-link (IPC TL-IPC223(P)-6, TL-IPC323K-D, TL-IPC325(KP)-*, TL-IPC40A-4) cho phép đối tượng thực hiện chèn và thực thi mã lệnh, trên tập tin /usr/lib/lua/luci/websys.lua có lưu trữ mật khẩu được zMiVw8Kw0oxKXL0	Chưa có thông tin xác nhận và bản vá
5	Vmware	CVE-2018-6963	Lỗ hổng trên Horizon Client cho Linux (phiên bản 4.x trước 4.8.0) của VMware cho phép đối tượng thực hiện tấn công leo thang đặc quyền	Đã có thông tin xác nhận
6	Wordpress	CVE-2018-11366	Nhóm 09 lỗ hổng trên một số tiện ứng của Wordpress (wpForo; MULTIDOTS WooCommerce Quick Reports, Woo Checkout for Digital Goods, Gameplan, Advancce Searh for WooCommerce, Mass Pages/Posts Creator, Add Social Share Messenger Buttons, Whatsapp, Viber; Member Mouse) cho phép đối tượng thực hiện nhiều hình thức tính công như SQL, XSS, CSRF, từ chối dịch vụ, lây nhiễm và thực thi mã JavaScript.	Chưa có thông tin xác nhận và bản vá
7	BMW	CVE-2018-9318 CVE-2018-9322	Lỗ hổng trên Telematics Control Unit và Infotainment - thành phần của hệ thống	Chưa có thông tin xác nhận

		CVE-2018-9313 CVE-2018-9320 CVE-2018-9312 …	điều khiển trên nhiều dòng phương tiện (BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7) của hãng BMW cho phép đối tượng tấn công thực hiện tấn công qua mạng điện thoại di động, bluetooth hay trực tiếp bằng giao diện USB, OBD-II trên xe để khống chế hệ thống điều khiển của xe.	và bản vá

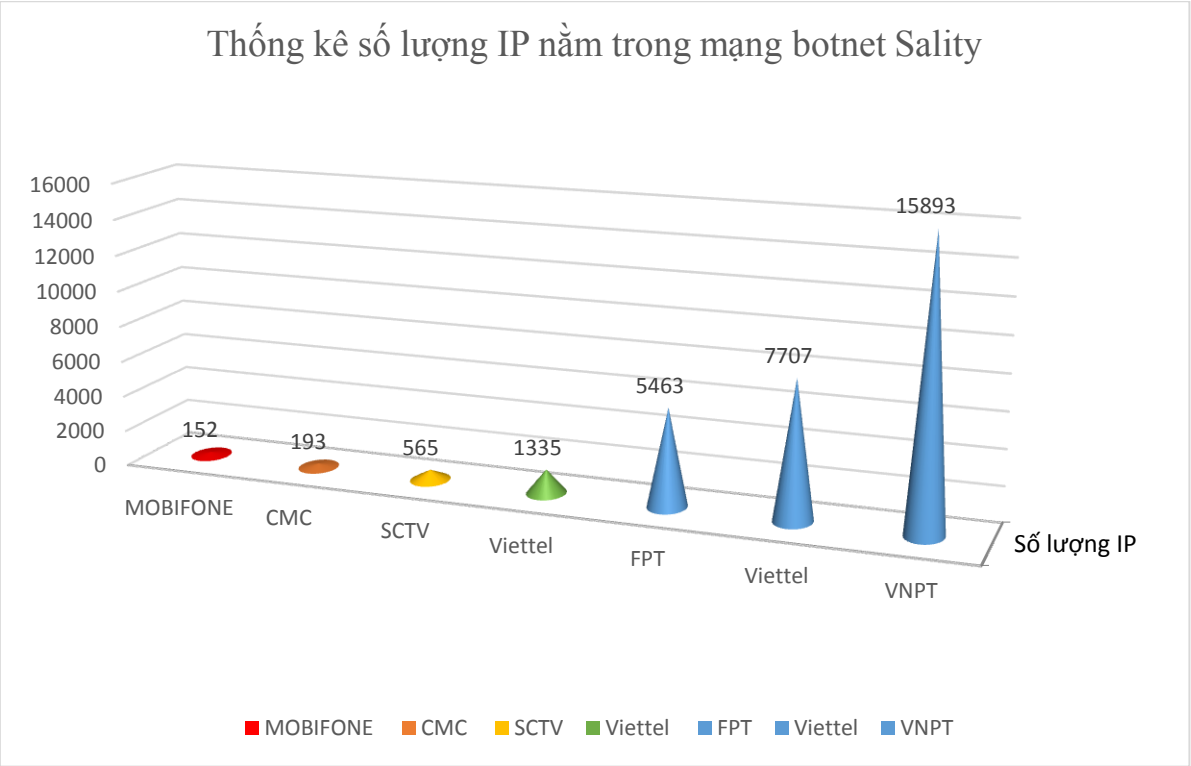
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

5.1. Mạng botnet Sality

Mạng botnet Sality còn gọi là hay KuKu, là tập hợp của nhiều loại vi-rút, trojan cùng hoạt động. Loại mã độc này tấn công vào các máy tính sử dụng hệ điều hành Windows, lần đầu tiên bị phát hiện vào 04/6/2003. Thời điểm đó mã độc Sality được tìm thấy là một mã độc lây nhiễm vào hệ thống qua các đoạn mã chèn vào đầu tập tin host để giúp mở cửa hậu và lấy trộm thông tin bàn phím.

Đến năm 2010 xuất hiện biến thể Sality nguy hiểm hơn và trở thành một trong những dòng mã độc phức tạp và nguy hiểm nhất đối với an toàn của hệ thống. Máy tính bị nhiễm mã độc sẽ trở thành một điểm trong mạng ngang hàng để tiếp tục phát tán mã độc sang các máy tính khác. Mạng botnet Sality chủ yếu để phát tán thư rác, tạo ra các proxy, ăn cắp thông tin cá nhân, lây nhiễm vào các máy chủ web để biến các máy chủ này thành máy chủ điều khiển của mạng botnet để tiếp tục mở rộng mạng botnet.

Theo thông kê về mạng botnet Sality của Cục An toàn thông tin trong tuần có nhiều IP tại Việt Nam vẫn nằm trong mạng botnet Sality.



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

TT	Tên miền/IP
1	dq42b8b5k.ru
2	104.244.14.252
3	p2xtz27i32.ru
4	1952w4ddc.ru
5	kukutrustnet777.info
6	ei3rvgfk.ru
7	and31.blllaaaaaazblaaa3.com
8	init.icloud-analysis.com
9	kukutrustnet888.info
10	www.inform1ongung.info

6. Khuyến nghị đối với các cơ quan, đơn vị

Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan, tổ chức, Cục An toàn thông tin khuyến nghị:

- Nhằm tránh việc bị các đối tượng tấn công lợi dụng các trang web để thực hiện các hành vi gây mất an toàn thông tin như đã nêu trong *mục 2,* các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và cập nhật các điểm yếu, lỗ hổng trên các máy chủ web thuộc cơ quan, tổ chức mình

- Người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản, đặc biệt là các trang web giả mạo các ứng dụng, dịch vụ phổ biến như đã nêu trong *mục 3.2* báo cáo này.

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 4.3* báo cáo này.

- Chủ động kiểm tra, rà soát, bóc gỡ mã độc ra khỏi hệ thống mạng. Cục An toàn sẵn sàng phối hợp với các cơ quan tổ chức tiến hành kiểm tra và bóc gỡ mã độc botnet trên hệ thống của cơ quan đơn vị. Để xác minh các máy tính bị nhiễm mã độc botnet, Quý đơn vị có thể liên hệ với Cục An toàn thông tin theo thông tin bên dưới để phối hợp thực hiện.

- Kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại Cục An toàn thông tin đã chia sẻ, đặc biệt là các tên miền đã nêu trong *mục 5.2* báo cáo này.

Thông tin liên hệ Cục An toàn thông tin, tầng 8, số 115 Trần Duy Hưng, quận Cầu Giấy, TP. Hà Nội; số điện thoại: 024.3943.6684; thư điện tử ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Bộ trưởng và các Thứ trưởng (để b/c);
- Thư ký Lãnh đạo Bộ;
- Đơn vị chuyên trách về CNTT các bộ, ngành;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cục KSTTHC, Văn phòng Chính phủ;
- Vụ Khoa giáo - Văn xã, Văn phòng Chính phủ;
- Trung tâm CNTT, Văn phòng Trung ương Đảng;
- Trung tâm CNTT, Văn phòng Quốc Hội; (email)
- Trung tâm CNTT, Văn phòng Chủ tịch nước;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và Ngân hàng;
- Cơ quan, đơn vị thuộc Bộ;
- Lãnh đạo Cục;
- Lưu: VT, TTTV.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Huy Dũng

PHỤ LỤC

I. Báo cáo được xây dựng dựa trên các nguồn thông tin:

- Hệ thống xử lý tấn công mạng Internet Việt Nam, hệ thống trang thiết bị kỹ thuật phục vụ cho công tác quản lý nhà nước về an toàn thông tin do Cục An toàn thông tin quản lý vận hành;

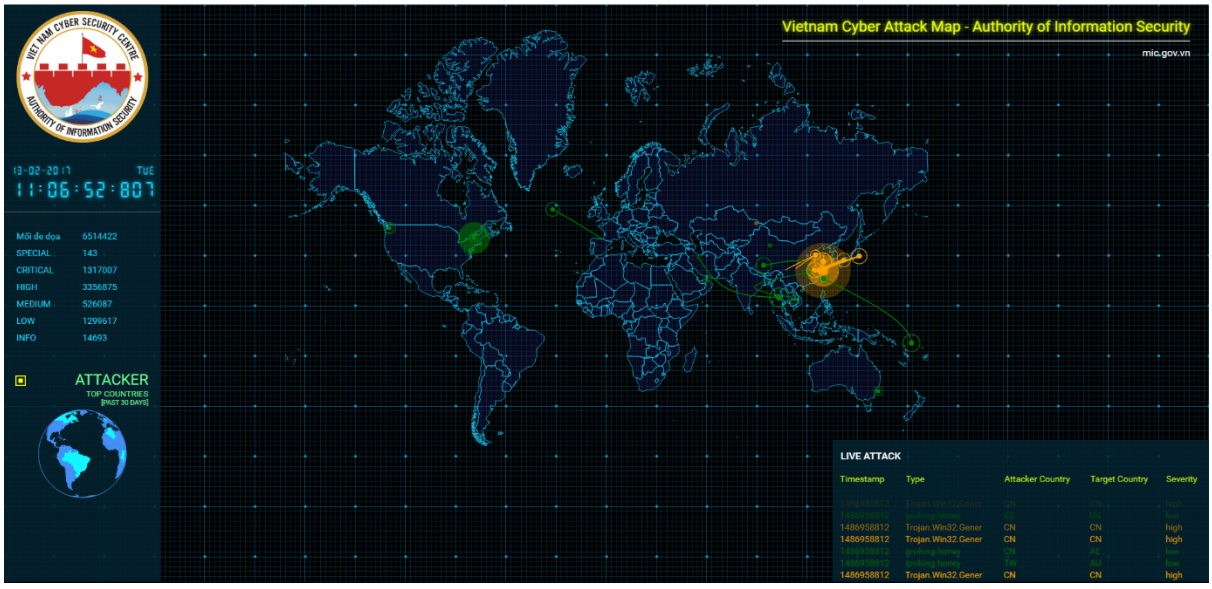
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- Hoạt động theo dõi, phân tích, tổng hợp tình hình an toàn thông tin mạng trên các trang mạng uy tín.

II. Giới thiệu về Hệ thống theo dõi, xử lý tấn công mạng Internet Việt Nam trực thuộc Cục An toàn thông tin:

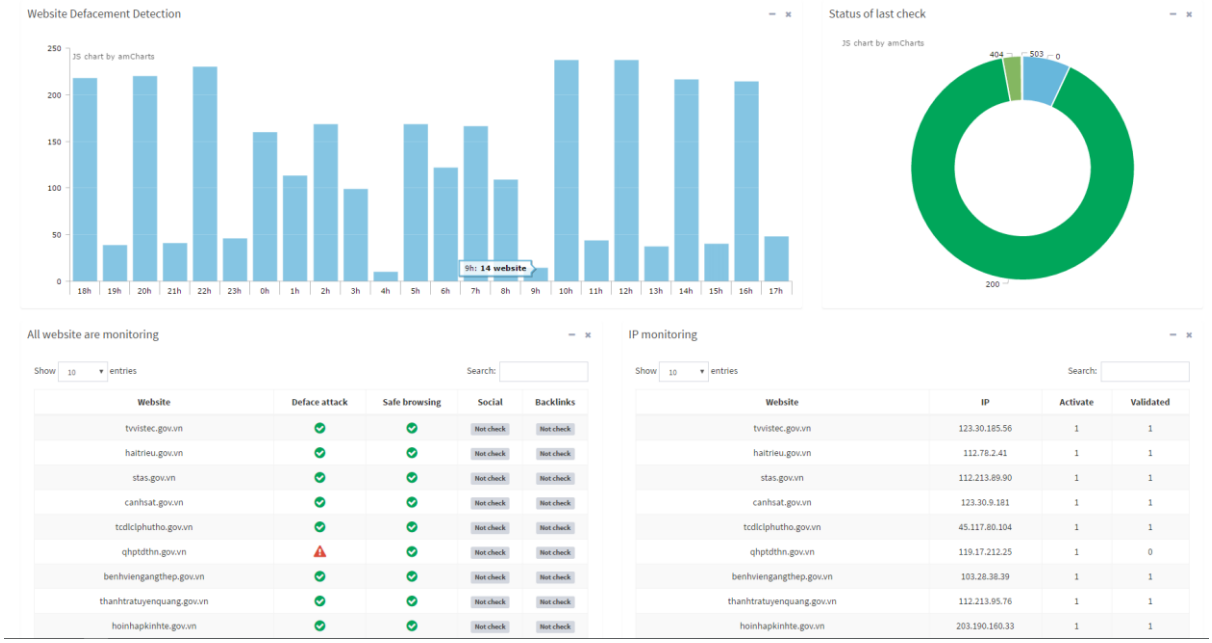
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

1. Hệ thống phân tích, phát hiện tấn công mạng từ xa đa nền tảng



Hệ thống được xây dựng dựa trên các công nghệ AI, thường xuyên dò quét, kiểm tra các mục tiêu dựa trên hệ thống sensor sẵn có của Cục An toàn thông tin và các sensor khác trên toàn thế giới, từ đó, tự động phát hiện, cảnh báo sớm các cuộc tấn công mạng nhắm vào các mục tiêu được cấu hình sẵn, nhanh chóng thông báo cho quản trị viên biết các tình trạng của các cuộc tấn công mạng này.

2. Hệ thống phân tích, dò quét, tự động phát hiện tấn công từ xa các website, cổng thông tin điện tử



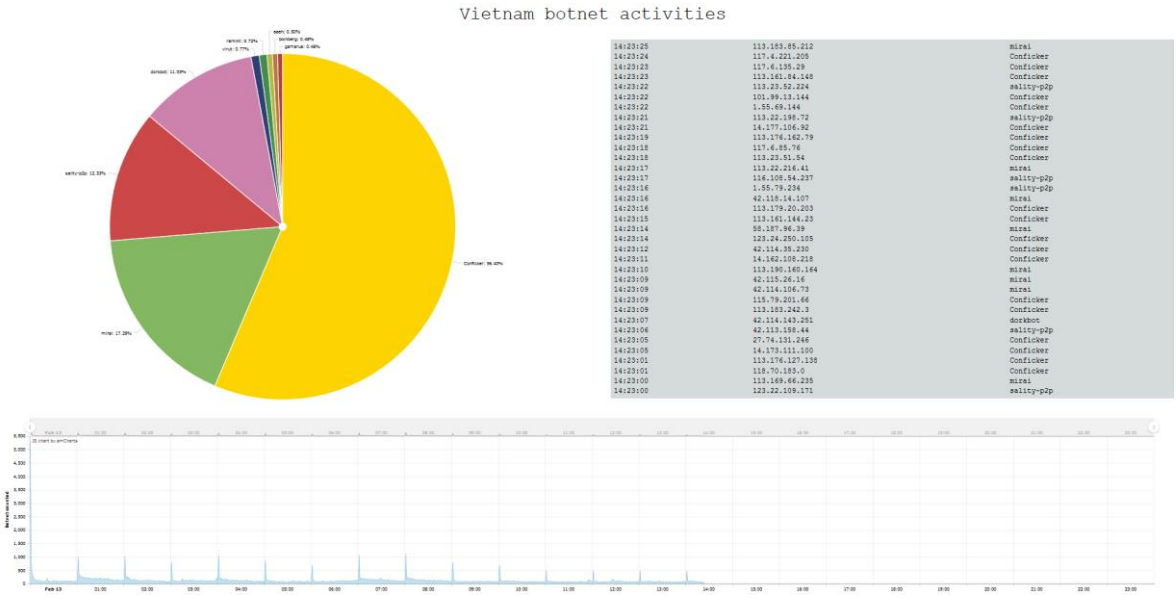
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc trên website…

Cục An toàn thông tin đã xây dựng, phát triển và triển khai Hệ thống phân tích, dò quét, tự động phát hiện tấn công từ xa các website, cổng thông tin điện tử. Hệ thống được thiết kế để hỗ trợ việc theo dõi, giám sát và cảnh báo sớm về mức độ ATTT của các website. Hệ thống thực hiện giám sát từ xa nhưng không can thiệp, không cài đặt phần mềm hay thiết bị vào hạ tầng của các cơ quan chủ quản website đó.

3. Hệ thống theo dõi, phát hiện mã độc, mạng botnet từ xa

Hệ thống theo dõi cập nhật về tình hình mã độc hại được xây dựng và triển khai để hỗ trợ đắc lực trong việc nắm bắt cụ thể và đầy đủ nhất về tình hình lây nhiễm mã độc trong Việt Nam. Từ đó có thông tin để xây dựng kế hoạch và phương án xử lý bóc gỡ các mã độc trên diện rộng.

Với hệ thống này cho phép các cán bộ quản lý, phân tích nắm bắt được chi tiết các dòng mã độc, các mạng botnet đang hoạt động trên không gian mạng Việt Nam.



Bên cạnh đó hệ thống còn giúp các cán bộ phân tích nhanh chóng nắm bắt được xu thế lây lan, phát triển của các họ mã độc, từ đó đề ra các phương án ứng phó kịp thời cho từng thời điểm.

4. Hệ thống giám sát và phòng, chống tấn công mạng

Hệ thống giám sát và phòng, chống tấn công mạng của Cục ATTT được xây dựng trên cơ sở kết hợp giữa giải pháp thương mại và giải pháp nguồn mở, bảo đảm không phụ thuộc vào bất kỳ một hãng hay một công nghệ cụ thể nào trong việc hỗ trợ bảo vệ các hệ thống thông tin.

Cơ quan, tổ chức có thể liên hệ để được tư vấn, hỗ trợ trong công tác bảo đảm ATTT, cụ thể như sau:

- **Đăng ký nhận thông tin cảnh báo chung về ATTT, liên hệ**: Ông Hà Văn Hiệp, số điện thoại: 0968689111, thư điện tử: hvhiep@mic.gov.vn;

- **Đăng ký theo dõi, giám sát trang/cổng thông tin điện tử, liên hệ:** Ông Nguyễn Sơn Tùng, số điện thoại: 0977325416, thư điện tử: nstung@mic.gov.vn;

- **Đăng ký theo dõi, giám sát, xử lý mã độc, lừa đảo qua mạng, liên hệ:** Bà Bùi Thị Huyền, số điện thoại:0932481987; thư điện tử: bt_huyen@mic.gov.vn;

- **Đăng ký hỗ trợ cài đặt cảm biến (sensor) để giám sát, phòng, chống tấn công mạng, liên hệ**: Ông Nguyễn Phú Dũng, số điện thoại: 01676611700, thư điện tử: npdung@mic.gov.vn