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: **58**/BC-CATTT

Hà Nội, ngày 05 tháng 12 năm 2017

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 48/2017 (từ ngày 27/11/2017 đến ngày 03/12/2017)

Cục An toàn thông tin là cơ quan có chức năng tham mưu, giúp Bộ trưởng Bộ Thông tin và Truyền thông quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin. Qua công tác thu thập, theo dõi, trích xuất, phân tích thông tin trong tuần 48/2017 (từ ngày 27/11/2017 đến ngày 03/12/2017), Cục An toàn thông tin thực hiện tổng hợp tóm tắt về an toàn thông tin diễn ra trong tuần.

Cục An toàn thông tin gửi tóm tắt tình hình để các cơ quan, tổ chức, cá nhân tham khảo và có các biện pháp phòng ngừa hợp lý.

BẢNG TỔNG HỢP

1. Ngày 27/11/2017, Intel đã phát hành công cụ hỗ trợ kiểm tra, phát hiện các lỗ hổng, điểm yếu Intel-SA-00086 trên các dòng vi xử lý của Intel đã được Cục An toàn thông tin đề cập tới trong báo cáo tuần trước (tuần 47).

2. Trong tuần ghi nhận 05 nhóm lỗ hổng, điểm yếu được cho là có thể gây ảnh hưởng lớn đến người dùng tại Việt Nam.

1. Điểm tin đáng chú ý

Trong Báo cáo **tuần 47,** Cục An toàn thông tin đã cảnh báo về các lỗ hổng, điểm yếu an toàn thông tin ảnh hưởng đến các công nghệ lõi CPU của Intel như: Intel Management Engine (ME); Intel Server Platform Server (SPS); Intel Trusted Execution Engine (TXE).

Nhằm khắc phục các điểm yếu trên, ngày 27/11/2017, Intel đã phát hành công cụ hỗ trợ kiểm tra, phát hiện các lỗ hổng, điểm yếu Intel-SA-00086, đồng thời cập nhật thông tin các bản vá cho các dòng vi xử lý bị ảnh hưởng bởi các lỗ hổng, điểm yếu này.

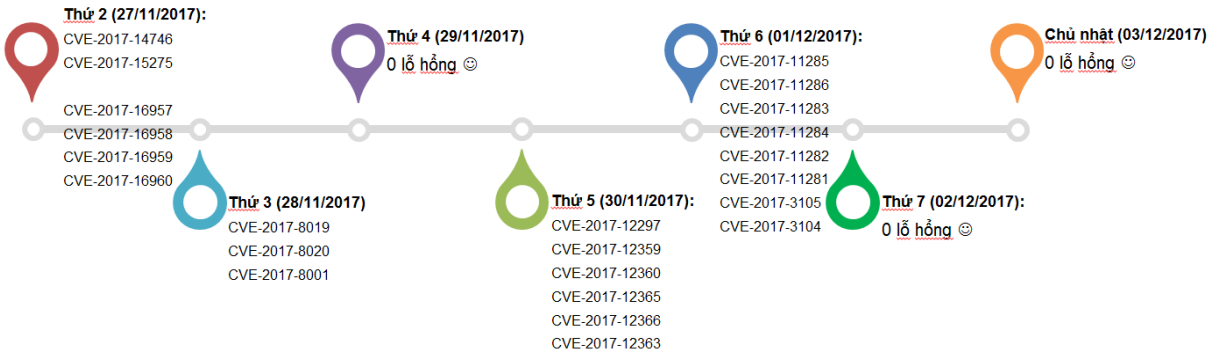
Các cơ quan, tổ chức, đơn vị có thể tham khảo hướng dẫn do Cục An toàn thông tin xây dựng tại *Phụ lục 1 kèm theo* báo cáo này.

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

2.1. Trong tuần 48/2017, các tổ chức quốc tế đã phát hiện và công bố ít nhất **198** lỗ hổng, điểm yếu an toàn thông tin bao gồm: **06** lỗ hổng ở mức trung bình, **192** lỗ hổng chưa được đánh giá. Trong đó có **11** lỗ hổng đã có mã khai thác.

2.2. 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 **05** nhóm lỗ hổng và trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam, như: Nhóm 08 lỗ hổng trên các sản phẩm phần mềm của Adobe (bao gồm Adobe ColdFusion, Adobe Flash Player, Adobe RoboHelp); Nhóm 04 lỗ hổng trên nhiều dòng thiết bị của TP-Link (bao gồm TP-Link TL-WVR, TL-WAR, TL-ER, và TL-R) .v.v…

Thời điểm các lỗ hổng, điểm yếu này được công bố theo mốc thời gian (timeline) sau:



Hình 2: Các lỗ hổng có khả năng ảnh hưởng tới nhiều người dùng tại Việt Nam

2.3. 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	Adobe	CVE-2017-11285 CVE-2017-11286 CVE-2017-11283 CVE-2017-11284 CVE-2017-11282 CVE-2017-11281 CVE-2017-3105 CVE-2017-3104	Nhóm 08 lỗ hổng trên sản phẩm phần mềm của Adobe (bao gồm Adobe ColdFusion, Adobe Flash Player, Adobe RoboHelp) cho phép thực hiện các hình thức tấn công khác nhau, trong đó có 02 lỗ hổng của Adobe Flash Player (CVE-2017-11282, CVE-2017-11281) đã có mã khai thác.	Đã có mã khai thác Đã có bản vá

2	Cisco - webex	CVE-2017-12297 CVE-2017-12359 CVE-2017-12360 CVE-2017-12365 CVE-2017-12366 CVE-2017-12363	Nhóm các lỗ hổng trên Cisco WebEx Meeting cho phép thực hiện nhiều hình thức tấn công khác nhau bao gồm: chuyển hướng người dùng tới trang web độc hại, thực thi mã lệnh trên hệ thống đích, tấn công XSS, truy cập và sửa đổi nội dung các thông điệp thông báo của máy chủ	Đã có bản vá
3	Dell-EMC ScaleIO	CVE-2017-8019 CVE-2017-8020 CVE-2017-8001	Nhóm 03 lỗ hổng trong giải pháp, công nghệ EMC ScaleIO – giải pháp cho phép tạo mạng lưu trữ SAN của Dell cho phép đối tượng tấn công thực thi mã lệnh với quyền root trên hệ thống,	Đã có bản vá
4	Samba	CVE-2017-14746 CVE-2017-15275	Nhóm 02 lỗ hổng trong dịch vụ Samba - dịch vụ chia sẻ file phổ biến trên các hệ điều hành Linux, trong đó lỗ hổng CVE-2017-14746 cho phép đối tượng tấn công thực thi mã lệnh. Các lỗ hổng ảnh hưởng tới các phiên bản Samba 4.x và trước 4.7.3 trên tất cả hệ điều hành Linux bao gồm cả Ubuntu, Redhat, Debian, Centos ….	Đã có bản vá
5	TP-Link	CVE-2017-16957 CVE-2017-16958 CVE-2017-16959 CVE-2017-16960	Nhóm 04 lỗ hổng trên nhiều dòng thiết bị của TP-Link (bao gồm TP-Link TL-WVR, TL-WAR, TL-ER, và TL-R) đều cho phép thực hiện mã lệnh thông qua nhiều hàm, chức năng khác nhau	Đã có bản vá

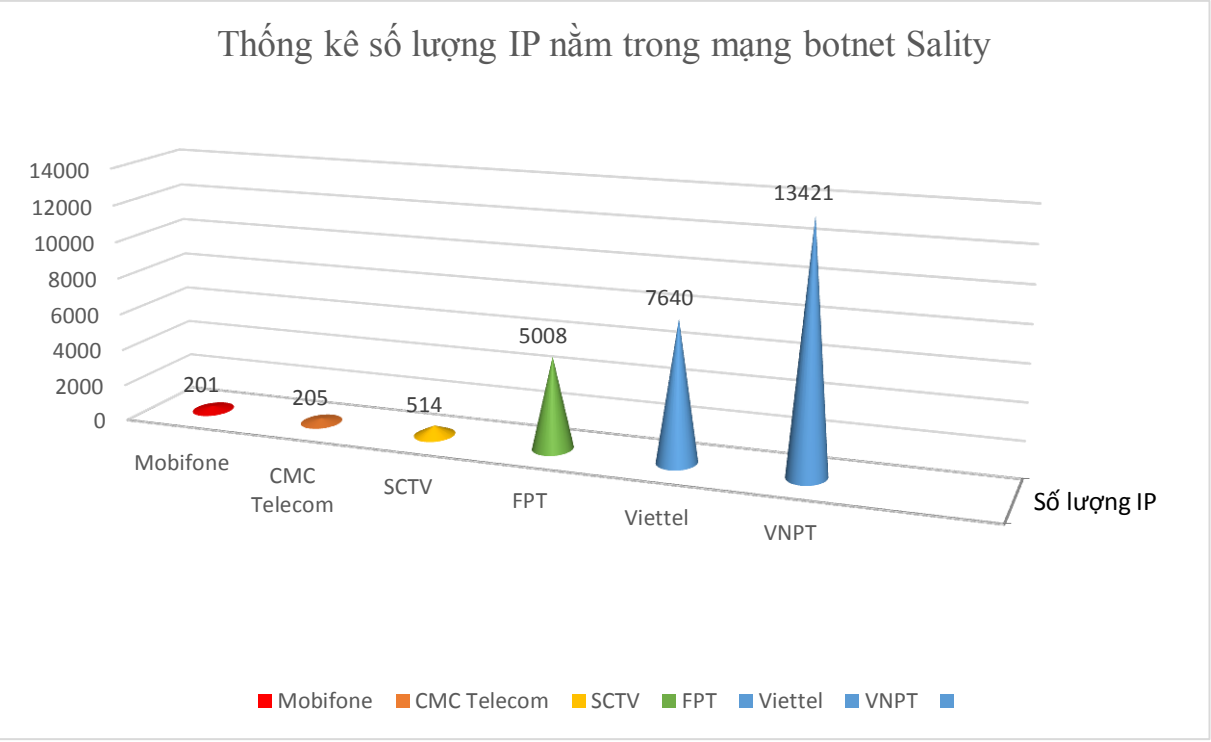
3. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

3.1 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.

Dưới đây là một số thông kê về mạng botnet Sality tại Việt Nam trong tuần mà Cục An toàn thông tin đang theo dõi.



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

TT	Tên miền/IP
1	cx4xzuwesx.com

2	drinkbreak.net
3	monerocash.pw
4	montgomeryamethyst.net
5	nosepudymy.biz
6	owawolyk.biz
7	rodujuhocafy.biz
8	rsymdhk.info
9	ufadaqim.biz
10	www.german-banks.net

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

Theo thống kê số lượng máy tính Việt Nam nằm trong mạng botnet quốc tế là không nhỏ. Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan đơn vị, Cục An toàn thông tin khuyến nghị:

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu trên.

- 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 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;
- Vụ Khoa giáo - Văn xã, Văn phòng Chính phủ;
- Trung tâm CNTT, Văn phòng Trung ương Đảng;
- Trung tâm CNTT, Văn phòng Quốc Hội;
- 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, TĐQLGS.

(email)

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

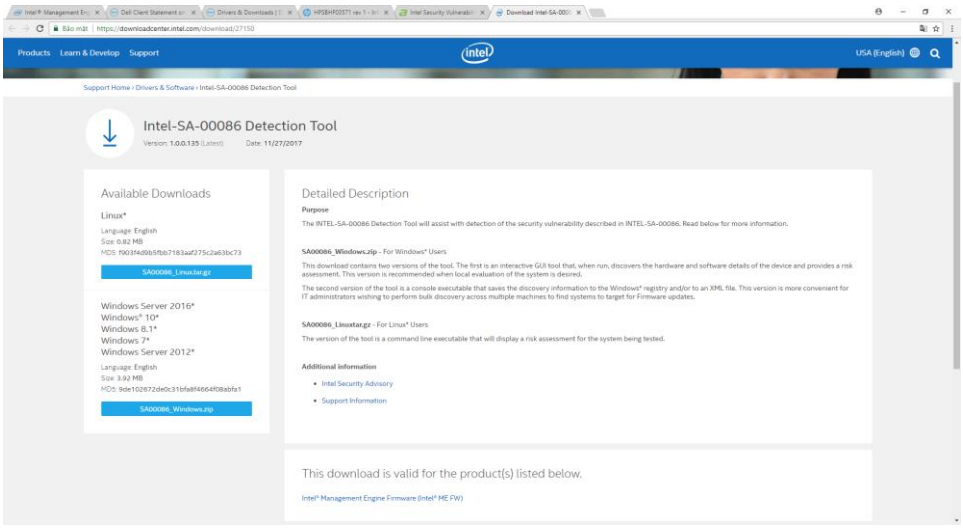
Nguyễn Huy Dũng

PHỤ LỤC 1

Hướng dẫn kiểm tra và cập nhật bản vá Intel-SA-00086

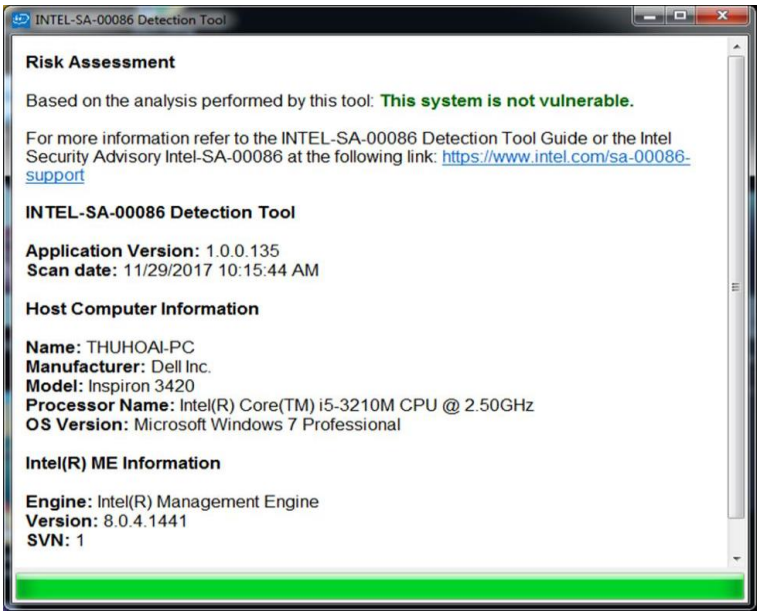
Bước 1: Kiểm tra thiết bị có bị ảnh hưởng hay không bằng cách tải công cụ phát hiện điểm yếu an toàn thông tin Intel-SA-00086 tại đường dẫn:

https://downloadcenter.intel.com/download/27150



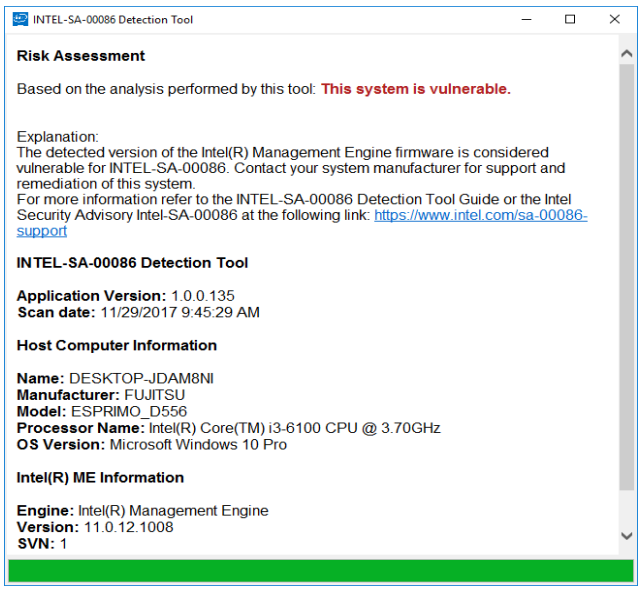
Hình 1: Tải công cụ phát hiện điểm yếu an toàn thông tin Intel-SA-00086

Bước 2: Cài đặt công cụ. Nếu thiết bị không có lỗ hổng thì sẽ có thông báo:



Hình 2: Thông báo không có điểm yếu Intel-SA-00086

Nếu thiết bị có điểm yếu công cụ phát hiện điểm yếu sẽ thông báo:



Hình 3: Thông báo có điểm yếu Intel-SA-00086

Bước 3: Cài đặt bản vá lỗng phù hợp với từng thiết bị tại trang web hỗ trợ của Intel tại đường dẫn: https://www.intel.com/content/www/us/en/support/articles/000025619/software.html

Tham khảo

Một số thông tin về nhà cung cấp thiết bị và bản vá tham khảo tại các đường dẫn bên dưới:

https://www.intel.com/content/www/us/en/support/articles/000025619/software.html

http://www.dell.com/support/article/us/en/19/sln308237/dell-client-statement-on-intel-me-txe-advisory--intel-sa-00086-?lang=en

http://www.dell.com/support/article/us/en/19/qna44242/dell-server-statement-on-intel-me-txe-advisory--intel-sa-00086-?lang=en

http://www.fujitsu.com/global/support/products/software/security/products-f/itsa-00086e.html

PHỤ LỤC 2

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;

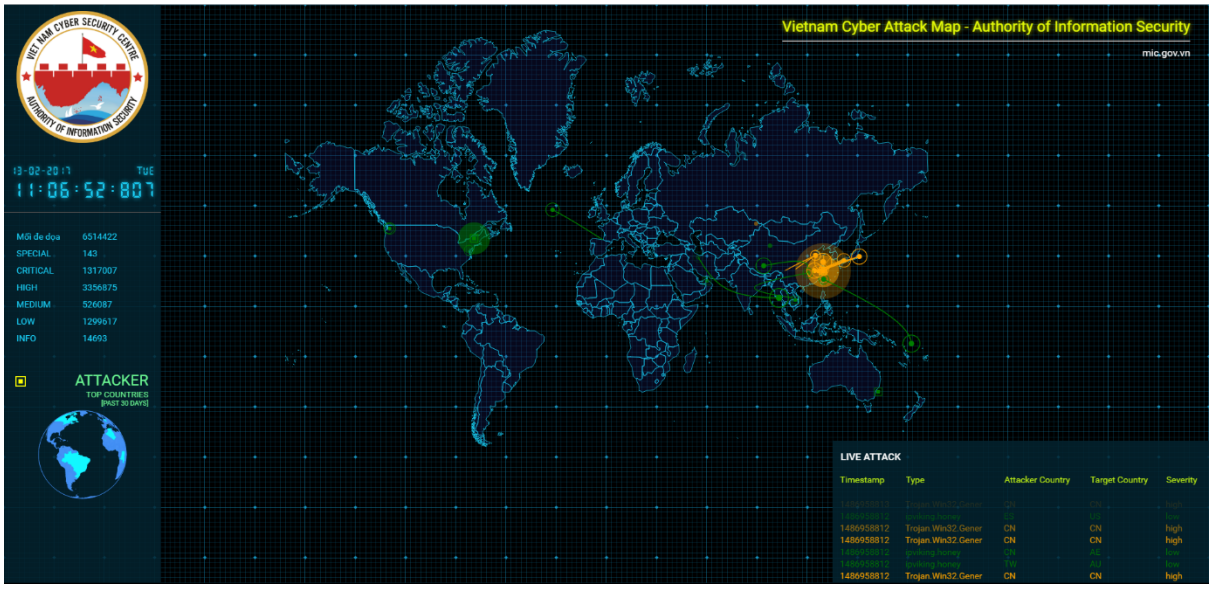
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

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

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

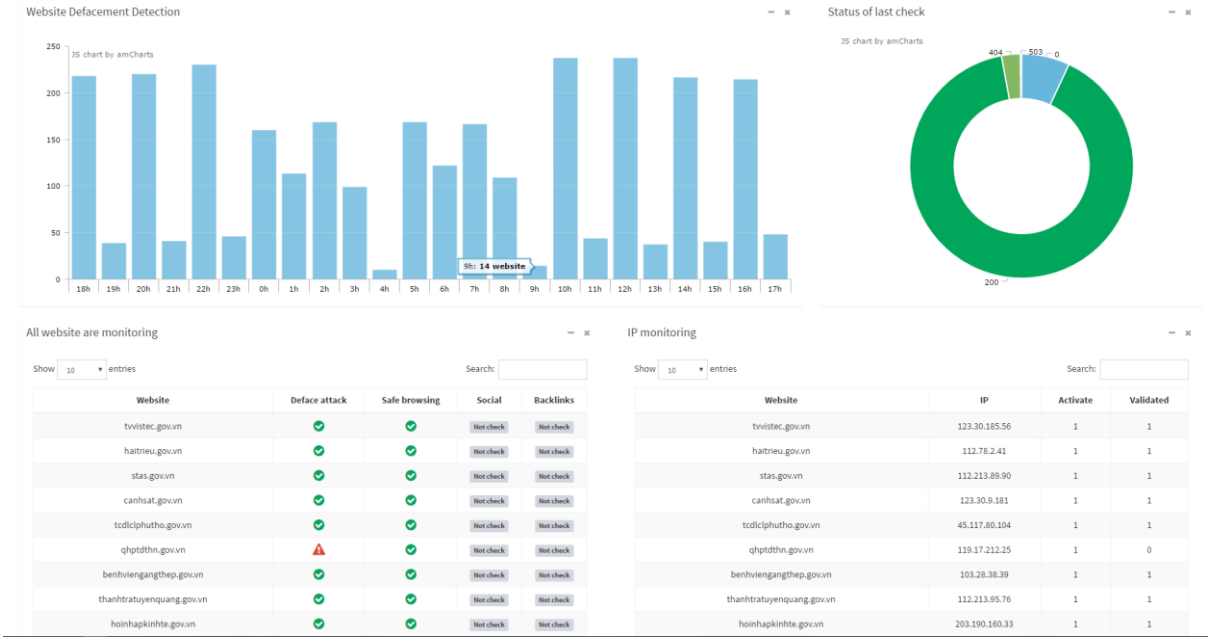
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



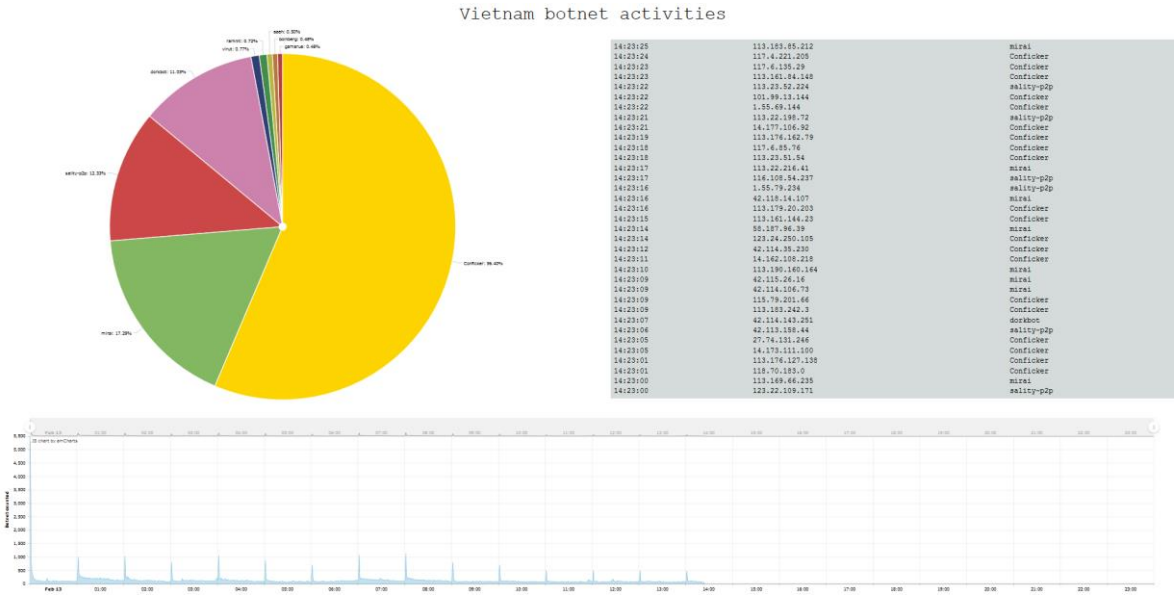
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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