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: **01**/BC-CATTT

Hà Nội, ngày 09 tháng 01 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 01/2018
(từ ngày 01/01/2018 đến ngày 07/01/2018)

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 01/2018 (từ ngày 01/01/2018 đến ngày 07/01/2018), 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 03/01/2018, các chuyên gia về an toàn thông tin của Google công bố một nhóm gồm 03 điểm yếu an toàn thông tin trong các bộ vi xử lý cho phép bất kỳ ứng dụng nào cũng có thể truy cập vào các vùng nhớ để lấy thông tin của hệ thống và thông tin của các các ứng dụng khác (thay vì chỉ được truy cập vào vùng nhớ cấp cho ứng dụng).

2. Người dùng có thể tự kiểm tra lộ, lọt thông tin tài khoản email bằng công cụ do Cục ATTT phát triển tại website: https://khonggianmang.vn/

3. Trong tuần ghi nhận 06 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

1.1. Thời gian qua, thông qua hệ thống của Cục An toàn thông tin (Cục ATTT) và một số kênh thông tin, Cục ATTT đã phát hiện thông tin về việc lộ, lọt 41 GB dữ liệu liên quan đến các tài khoản thư điện tử. Qua các biện pháp kỹ thuật ban đầu, Cục An toàn thông tin đã phát hiện và xác định có rất nhiều thông tin tài khoản thư điện tử của nhiều cơ quan tổ chức tại Việt Nam bao gồm: có 473.770 thông tin tài khoản thư điện tử của Việt Nam trong đó có 1056 tài khoản tên miền .gov.vn; 806 tài khoản của các ngân hàng.

Cục ATTT đã có văn bản cảnh báo cụ thể gửi tới các đơn vị và đã phối hợp với một số đơn vị xử lý đối với các địa chỉ thư điện tử công vụ. Đối với các địa chỉ thư điện tử cá nhân, các đơn vị chuyên trách về CNTT/ATTT các bộ ngành, địa phương có thể hướng dẫn người dùng cuối tự kiểm tra bằng công cụ do Cục ATTT phát triển tại website: https://khonggianmang.vn/ .

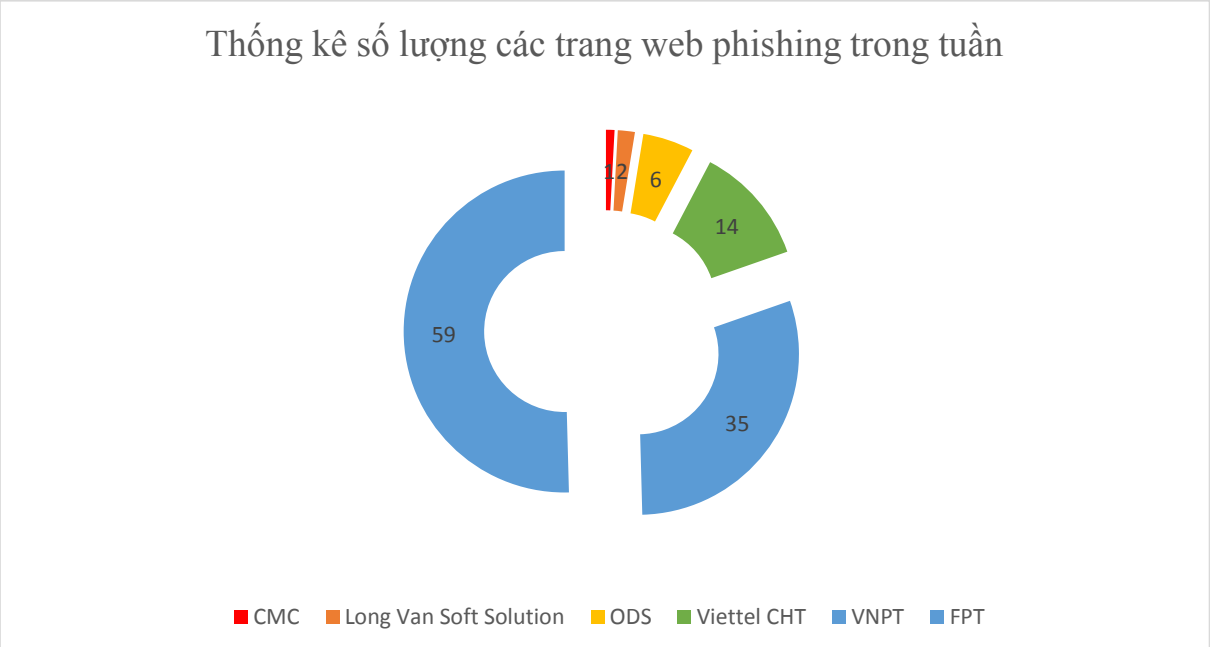
1.2. Ngày 03/01/2018, các chuyên gia về an toàn thông tin của Google công bố một nhóm gồm 03 điểm yếu an toàn thông tin trong các bộ vi xử lý cho phép bất kỳ ứng dụng nào cũng có thể truy cập vào các vùng nhớ để lấy thông tin của hệ thống và thông tin của các các ứng dụng khác (thay vì chỉ được truy cập vào vùng nhớ cấp cho ứng dụng).

Các điểm yếu an toàn thông tin trên có mã lỗi quốc tế là: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754. Các điểm yếu an toàn thông tin này được các chuyên gia đánh giá là nghiêm trọng và có ảnh hưởng tới nhiều thiết bị, bao gồm: máy tính để bàn, máy tính xách tay, máy chủ, điện thoại di động sử dụng các hệ điều hành Linux, Windows, MacOS.

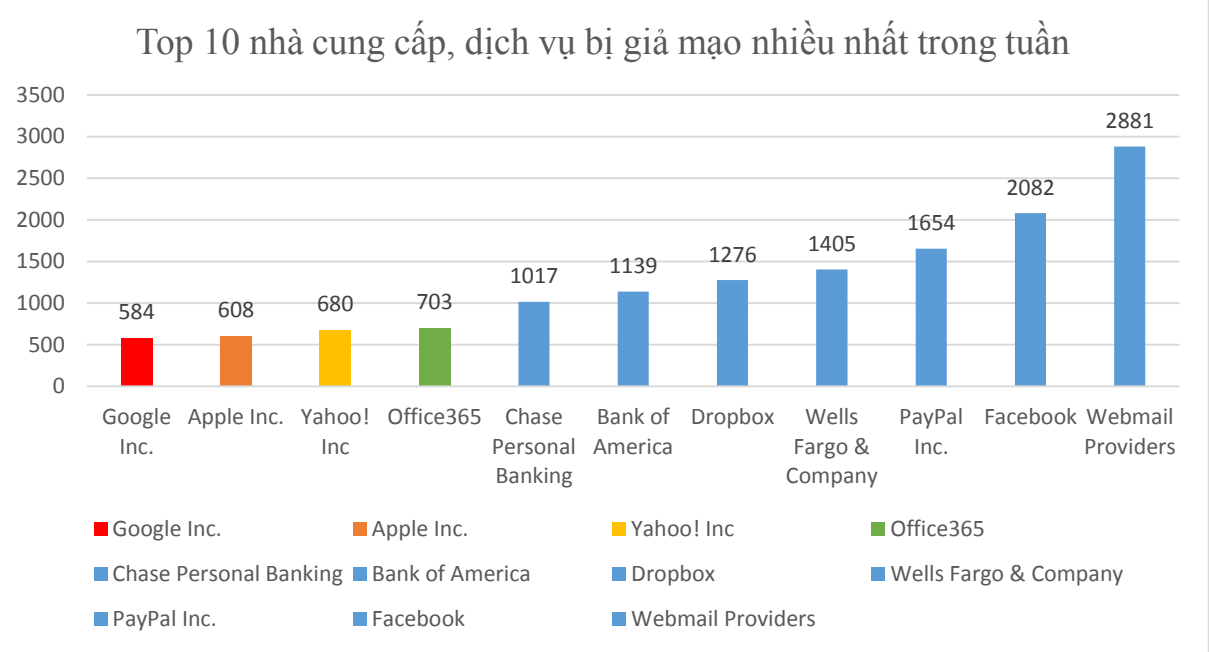
Cục ATTT đã có Công văn số 03/CATTT-TTTV ngày 04/01/2018 gửi các đơn vị chuyên trách về CNTT/ATTT cảnh báo các điểm yếu an toàn thông tin nghiêm trọng nói trên.

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

2.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT nhận thấy tỉ lệ các trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần là không ít.



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



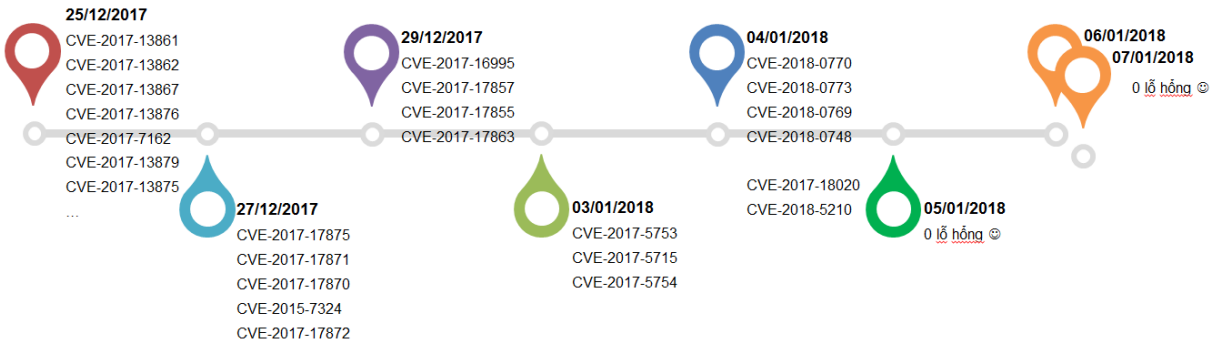
Việt Nam có nhiều người dùng các tài khoản mail server nước ngoài (cả miễn phí và có phí) , Facebook, Gmail, Dropbox .v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

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

3.1. Trong tuần cuối năm 2017 và tuần đầu năm 2018, các tổ chức quốc tế đã phát hiện và công bố ít nhất 470 lỗ hổng bao gồm: 15 lỗ hổng ở mức cao, 34 lỗ hổng ở mức trung bình, 0 lỗ hổng ở mức thấp, 421 lỗ hổng chưa được đánh giá. Trong đó có 39 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 30 lỗ hổng đã có mã khai thác.

3.2. 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 **06** 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 33 lỗ hổng trên các sản phẩm của Apple; Nhóm 03 lỗ hổng trong các bộ vi xử lý; Nhóm 321lỗ hổng trên các ứng dụng sản phẩm, của Microsoft .v.v…

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



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

3.3. 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	Apple	CVE-2017-13861 CVE-2017-13862 CVE-2017-13867 CVE-2017-13876 CVE-2017-7162 CVE-2017-13879 CVE-2017-13875 …	Nhóm 33 lỗ hổng trên các sản phẩm của Apple (bao gồm iOS, tvOS, watchOS, MacOS) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau, trong đó các lỗ hổng cho phép thực thi hầu hết đã có mã khai thác (như lỗ hổng CVE-2017-13875 trên MacOS, CVE-2017-13847 trên iOS, CVE-2017-13876 trên cả MacOS, iOS, tvOS, watchOS).	Đã có mã khai thác
2	Joomla	CVE-2017-17875 CVE-2017-17871 CVE-2017-17870 CVE-2015-7324 CVE-2017-17872	Nhóm 05 lỗ hổng ứng dụng quản trị nội dung Joomla cho phép thực hiện tấn công SQL Injection, XSS Có 03 lỗ hổng có mã khai thác.	Đã có mã khai thác Chưa có thông tin bản vá
3	Linux	CVE-2017-16995 CVE-2017-17857 CVE-2017-17855 CVE-2017-17863	Nhóm 13 lỗ hổng trong nhân Linux cho phép thực hiện nhiều hình thức tấn công khác nhau trong đó có cho phép thực thi mã lệnh và leo thang đặc quyền Ảnh hưởng tới các hệ điều hành sử dụng Linux Kernel với nhiều phiên bản khác	Đã có thông tin bản vá

			nhau: 4.9.x, các phiên bản trước 4.14.8	
4	CPU	CVE-2017-5753 CVE-2017-5715 CVE-2017-5754	Nhóm 03 lỗ hổng an toàn thông tin trong các bộ vi xử lý cho phép bất kỳ ứng dụng nào cũng có thể truy cập vào các vùng nhớ để lấy thông tin của hệ thống và thông tin của các các ứng dụng khác thống. Ảnh hưởng tới hầu hết các bộ vi xử lý hiện đại (Intel, AMD, ARM), trên các thiết bị, bao gồm: máy tính để bàn, máy tính xách tay, máy chủ, điện thoại di động sử dụng các hệ điều hành Linux, Windows, MacOS	Đã có văn bản cảnh báo riêng
5	Microsoft	CVE-2018-0770 CVE-2018-0773 CVE-2018-0769 CVE-2018-0748 …	Nhóm 321ỗ hổng trên các ứng dụng sản phẩm, của Microsoft (Microsoft Edge, Internet Explorer, Windows kernel…) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau. Trong đó có nhiều lỗ hổng cho phép chèn và thực thi mã lệnh, tấn công leo thang Các lỗ hổng này nằm trên ứng dụng, dịch vụ cài sẵn trên hệ điều hành máy trạm (Windows 7, 8, 10) và máy chủ (Windows Server 2012, 2016)	Đã có thông tin bản vá
6	Samsung-Mobile	CVE-2017-18020 CVE-2018-5210	Nhóm 02 lỗ hổng trên điện thoại di động Samsung L(5.x), M(6.x), N(7.x) cho phép đối tượng tấn công chèn và thực thi mã lệnh: Lỗ hổng CVE-2017-18020 cho phép chèn ngay trong Bootloader (phân vùng khởi động của thiết bị)	Đã có thông tin bản vá

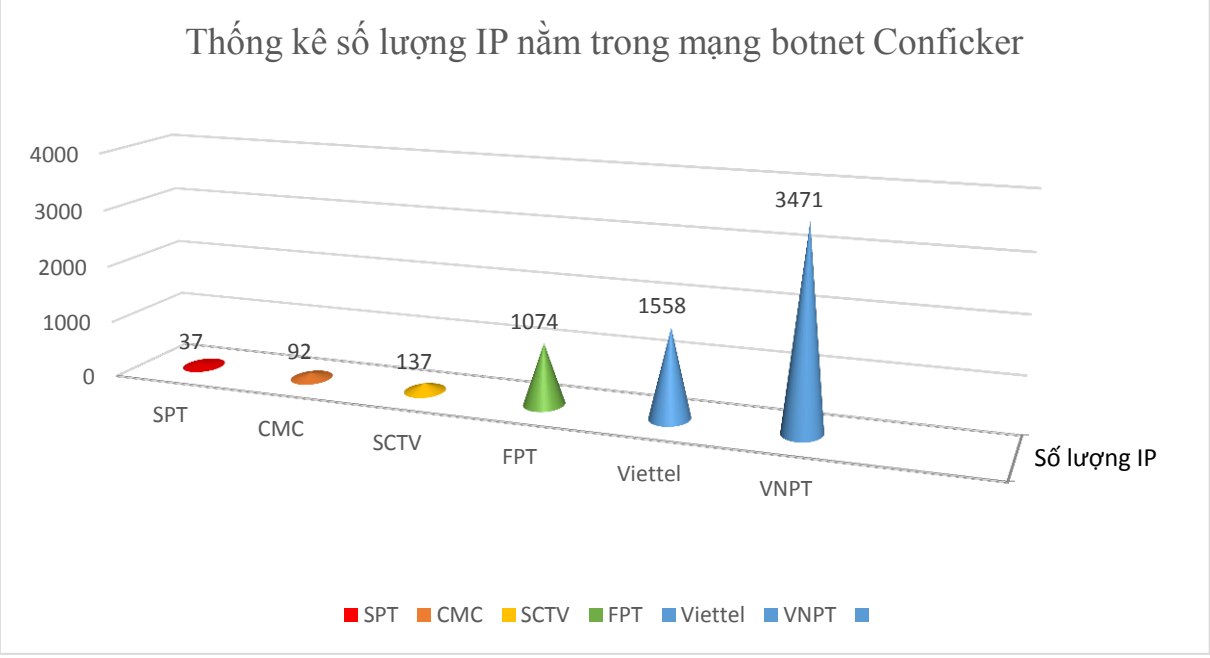
			Lỗ hổng CVE-2018-5210 cho phép thực thi mã lệnh kết hợp với tấn công vét cạn để ăn lấy trộm thông tin xác thực và mở khóa thiết bị.	

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

4.1. Mạng botnet Conficker

Mạng botnet Conficker được phát hiện từ tháng 10/2008. Mã độc này được thiết kế nhằm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống khác. Những máy tính bị lây nhiễm đều không truy cập được các website liên quan đến phần mềm diệt virus hay dịch vụ cập nhật của hệ Windows (Windows Update).

Mặc dù mạng botnet Conficker xuất hiện từ năm 2008, lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật, tuy nhiên tại Việt Nam, số lượng máy tính nằm trong mạng botnet Conficker vẫn còn rất nhiều trong tuần mà Cục An toàn thông tin đang theo dõi.



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

TT	Tên miền/IP
1	granvillemirabelle.net
2	lordsleep.net

3	spamhouseanilingus.ru
4	christabellewhittemore.net
5	grouphtconditionsrights.ru
6	roomshirt.net
7	wg2udkp1oba1.net
8	xxx.103azzxa.com
9	cinrybyetnloora.me
10	episykuj.com

5. 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:

- 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 2.2* báo cáo này.

- 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 *mục 4.2* 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;
- 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

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;

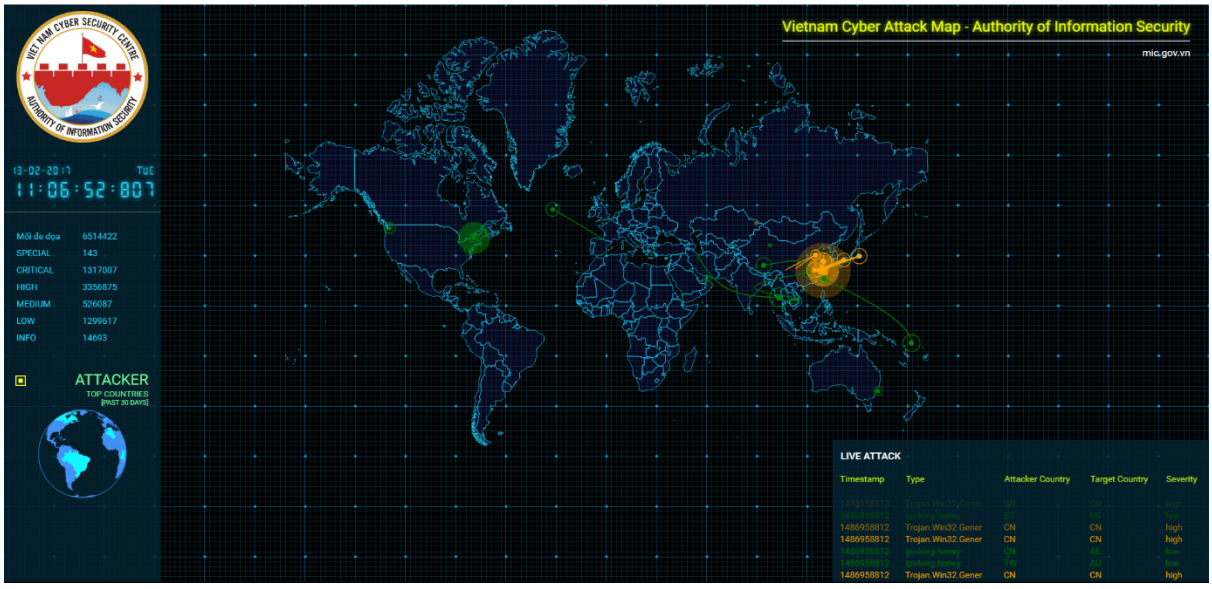
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

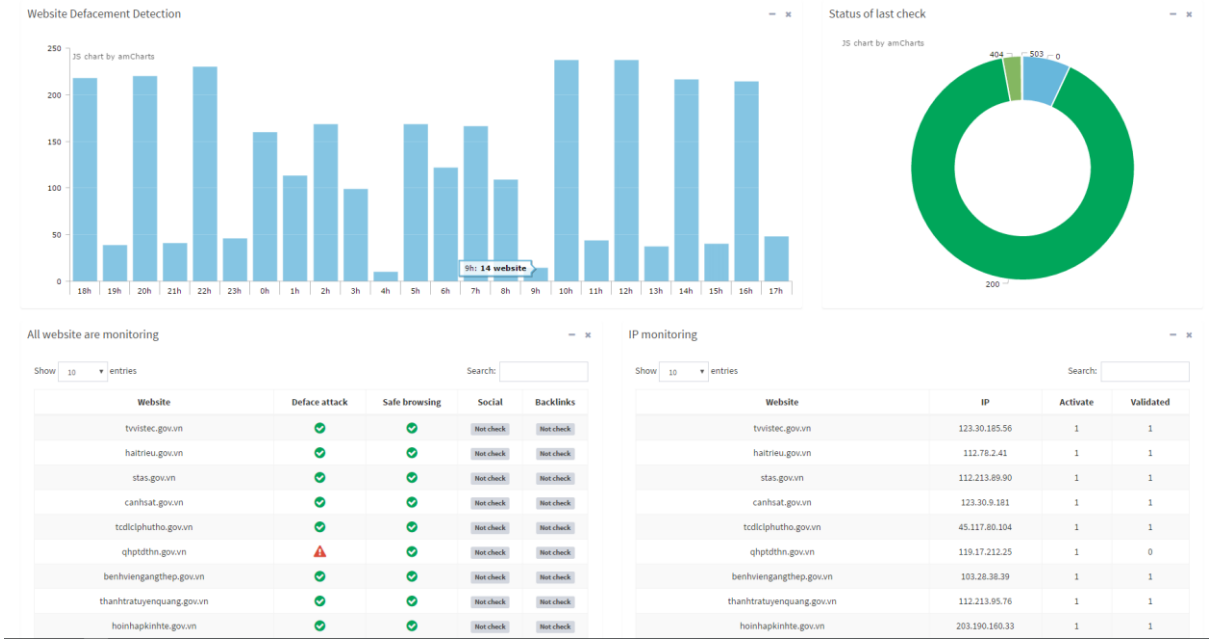
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



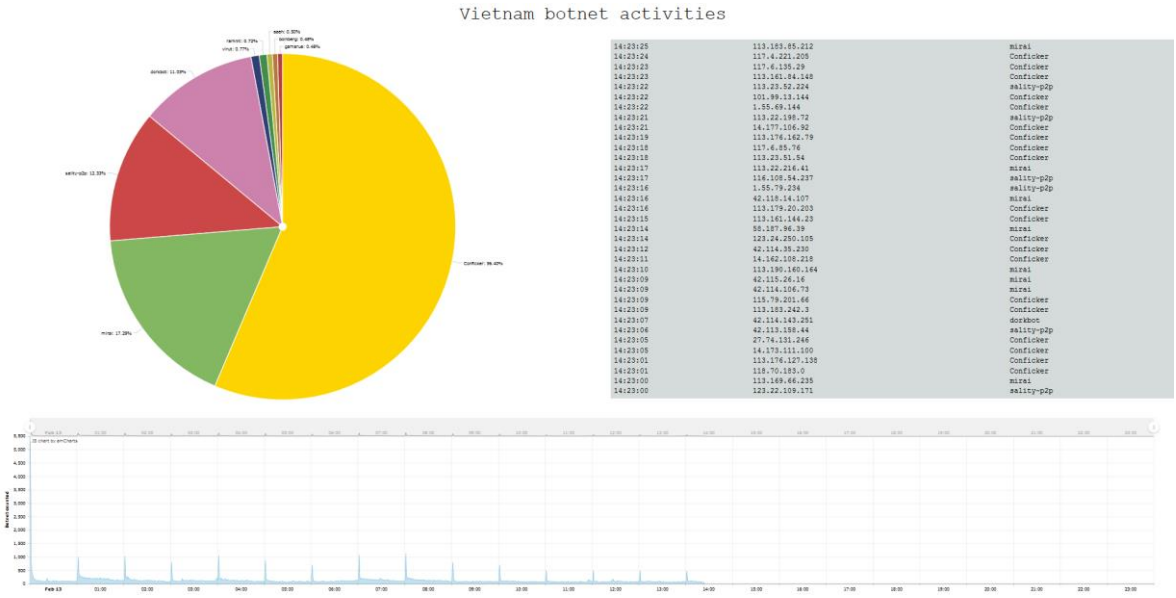
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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