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: **06**/BC-CATTT

Hà Nội, ngày 06 tháng 02 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 04/2018 (từ ngày 29/01/2018 đến ngày 04/02/2018)

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 05/2018 (từ ngày 29/01/2018 đến ngày 04/02/2018), 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 28/012018, theo thông tin từ trang mạng www.gov.uk của Chính phủ Anh, các cơ quan, tổ chức là chủ quản hệ thống thông tin quan trọng quốc gia nếu không tuân thủ Chỉ thị của chính phủ về tăng cường bảo đảm an toàn mạng, không có những biện pháp, phương án để tăng cường bảo đảm an toàn thông tin, sẽ phải đối mặt với các mức phạt có thể lên tới 17 triệu bảng Anh.

2. Ngày 29/01/2018, thông tin về lỗ hổng nguy hiểm trên trình duyệt Firefox được công bố. Lỗ hổng có mã lỗi quốc tế là CVE-2018-5124.

3. Trong tuần ghi nhận 03 nhóm lỗ hổng, điểm yếu và 03 lỗ hổng, điểm yếu riêng lẻ được cho là có thể gây ảnh hưởng lớn đến người dùng tại Việt Nam.

1. Điểm tin đáng chú ý

1.1. Ngày 28/01/2018, trước xu hướng tấn công mạng ngày càng tăng, đặc biệt là các cuộc tấn công mạng có tổ chức nhằm vào các dịch vụ và hệ thống thông tin quan trọng của nhiều quốc gia trên thế giới, Chính phủ Anh đã đưa ra thông điệp cảnh báo các cơ quan, tổ chức là chủ quản hệ thống thông tin quan trọng quốc gia nếu không tuân thủ Chỉ thị của chính phủ về tăng cường bảo đảm an toàn mạng, không có những biện pháp, phương án để tăng cường bảo

đảm an toàn thông tin, sẽ phải đối mặt với các mức phạt khác nhau. Các lĩnh vực như năng lượng, giao thông, nước sạch, y tế có mức phạt lên tới 17 triệu bảng Anh.

Tuy nhiên theo ông Ciaran Martin, Giám đốc Trung tâm an toàn thông tin mạng quốc gia Anh thì việc phạt tiền sẽ không áp dụng trong trường hợp các đơn vị vận hành đã thực hiện kiểm tra, đánh giá an toàn thông tin đầy đủ và thực hiện các biện pháp bảo đảm an toàn thông tin thích hợp nhưng vẫn bị tấn công gây thiệt hại.

1.2. Từ ngày 29/01/2018 đến ngày 16/02/2018, học viện SANS (một trong những trường chuyên nghiên cứu và đào tạo chuyên gia về an toàn thông tin trên khắp thế giới) tổ chức đăng ký Chương trình đào tạo trực tuyến về an toàn thông tin cho học sinh phổ thông ở 18 bang và 01 vùng lãnh thổ ở Mỹ.

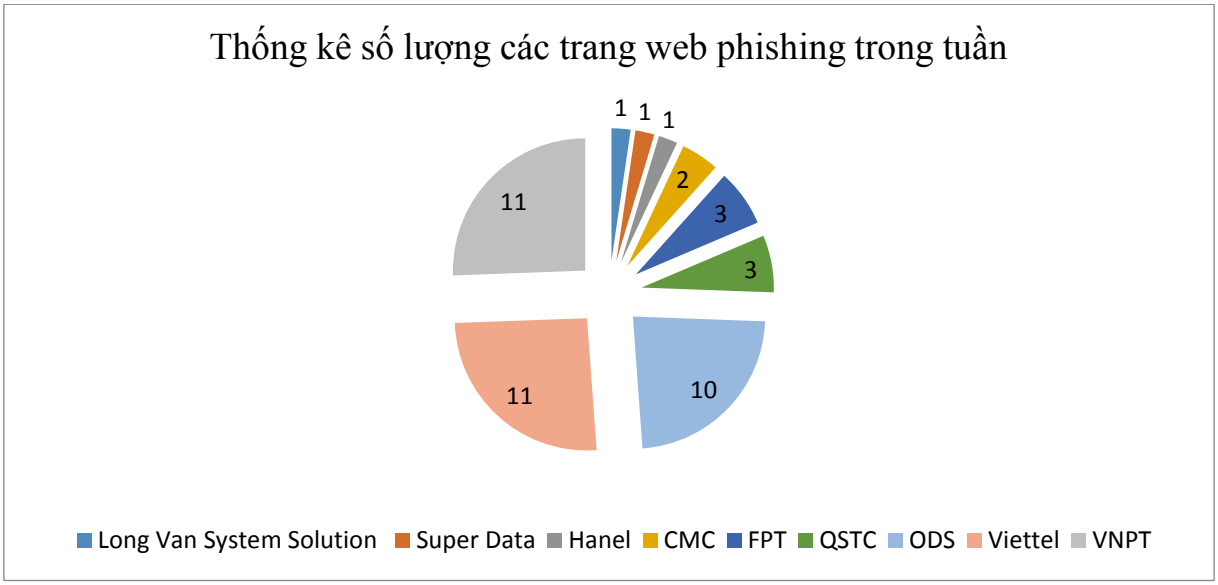
Đặc biệt nhằm thu hút thu hút nữ sinh và cân bằng giới tính trong lĩnh vực an toàn thông tin, SANS sẽ tổ chức những chương trình dành riêng cho nữ sinh như Girls Go CyberStart, Women in Cybersecurity để phát hiện và tìm kiếm những nữ chuyên gia giỏi chưa có cơ hội thể hiện trong lĩnh vực an toàn thông tin.

1.3. Ngày 29/01/2018, thông tin về lỗ hổng nguy hiểm trên các trình duyệt Firefox được công bố. Lỗ hổng có mã lỗi quốc tế là CVE-2018-5124, lỗ hổng này cho phép thực thi mã lệnh trên hầu hết các trình duyệt Firefox phiên bản Firefox 56 (.0, .0.1, .0.2); 57 (.0, .0.1, .0.2, .0.3, .0.4) và 58 (.0) cho phép đối tượng tấn công có thể kết hợp với nhiều kịch bản để cài đặt mã độc vào các máy tính, thiết bị sử dụng trình duyệt này.

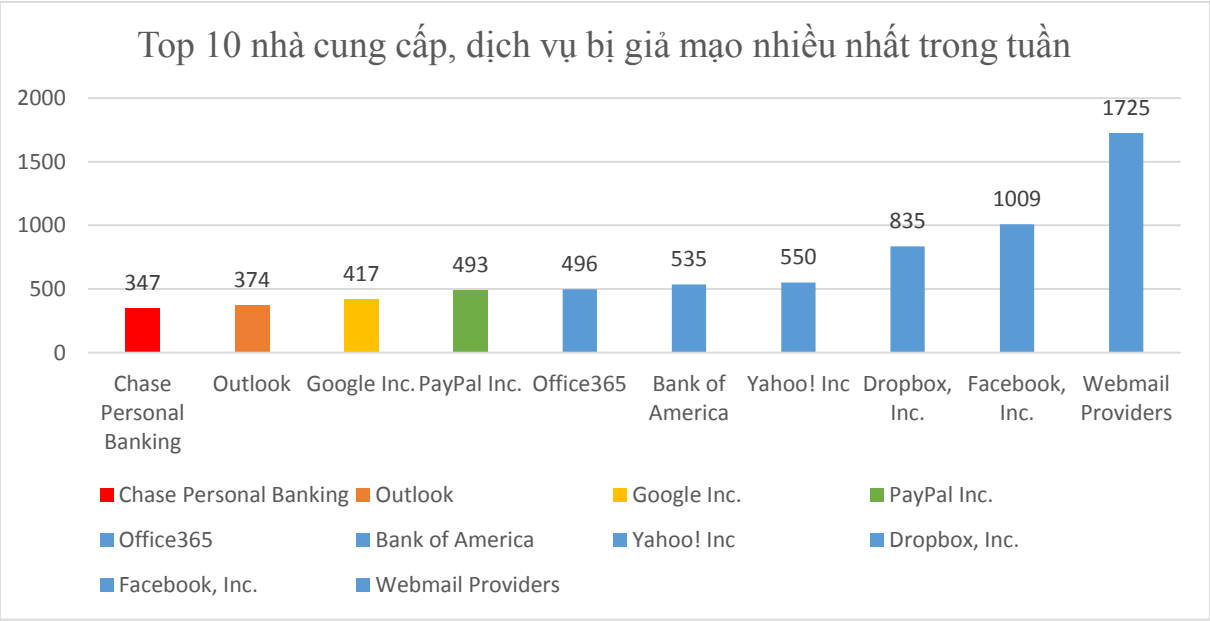
Để bảo đảm an toàn thông tin, Cục An toàn thông tin khuyến nghị người dùng cần cập nhật lên phiên bản Firefox 58.0.1 đã được Firefox phát hành.

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 còn ghi nhận có ít nhất 43 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



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, 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, Outlook .v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

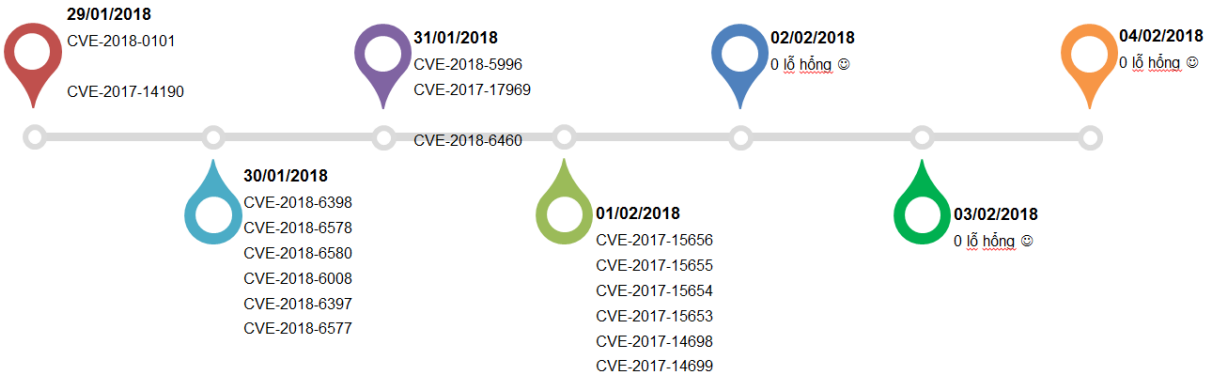
3. Lỗ hổng/điểm yếu an toàn thông tin trong tuần

3.1. Trong tuần, các tổ chức quốc tế đã phát hiện và công bố ít nhất **218** lỗ hổng trong đó có: 19 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 29 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 **03** nhóm lỗ hổng và

03 lỗ hổng riêng lẻ trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam, như: Nhóm 02 lỗ hổng phần mềm nén/giải nén 7-zip; Lỗ hổng trong hệ điều hành của các thiết bị Fortinet; Nhóm 15 lỗ hổng trên nhiều thành phần mở rộng và phần lõi của Joomla .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	7-zip	CVE-2018-5996 CVE-2017-17969	Nhóm 02 lỗ hổng phần mềm nén/giải nén 7-zip cho phép đối tượng tấn công chèn và thực thi mã lệnh và tấn công từ chối dịch vụ. Ảnh hưởng tới 7-Zip phiên bản trước 18.00 và p7zip. Phần mềm 7-zip là phần mềm miễn phí được đánh giá có số lượng người dùng lớn hơn cả winrar.	Đã có thông tin bản vá
2	Asus - asuswrt	CVE-2017-15656 CVE-2017-15655 CVE-2017-15654 CVE-2017-15653 CVE-2017-14698 CVE-2017-14699	Nhóm 06 lỗ hổng trên hệ điều hành thiết bị định tuyến của AsusWRT phiên bản trước 3.0.0.4.384_10007 cho phép đối tượng tấn công có thể thực hiện nhiều hình thức tấn công khác nhau, bao gồm lỗ hổng lưu trữ mật khẩu ở dạng rõ (trên các hệ điều hành phiên bản trước	Đã có thông tin bản vá

			3.0.0.4.380.7743), chèn và thực thi mã lệnh trong các phiên bản trước 3.0.0.4.376.X, vượt qua cơ chế xác thực để thay đổi thông tin tài khoản của người dùng. Tuần 04 đã cảnh báo 2 lỗ hổng có mã khai thác (CVE-2018-6000, CVE-2018-5999)	
3	Cisco	CVE-2018-0101	Lỗ hổng trên Cisco Adaptive Security Appliance cho phép đối tượng tấn công có thể chèn và thực thi mã lệnh, nạp lại cấu hình hệ thống, từ đó kiểm soát thiết bị phục vụ cho nhiều mục tiêu độc hại khác. Ảnh hưởng tới Cisco ASA Software chạy trên các thiết bị : 3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, Cisco Catalyst 6500 Series Switches, Cisco 7600 Series Routers, ASA 1000V Cloud Firewall, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD).	Đã có thông tin bản vá
4	Fortinet	CVE-2017-14190	Lỗ hổng trong hệ điều hành của các thiết bị Fortinet cho phép đối tượng tấn công chèn các đoạn mã HTML để ăn trộm thông tin xác thực và kiểm soát việc hiển trị dữ liệu web đi qua thiết bị và tiếp tục thực hiện nhiều tấn công sâu hơn. . Ảnh hưởng tới FortiOS 5.6.0 -5.6.2 FortiOS 5.4.0 - 5.4.7	Đã có thông tin bản vá

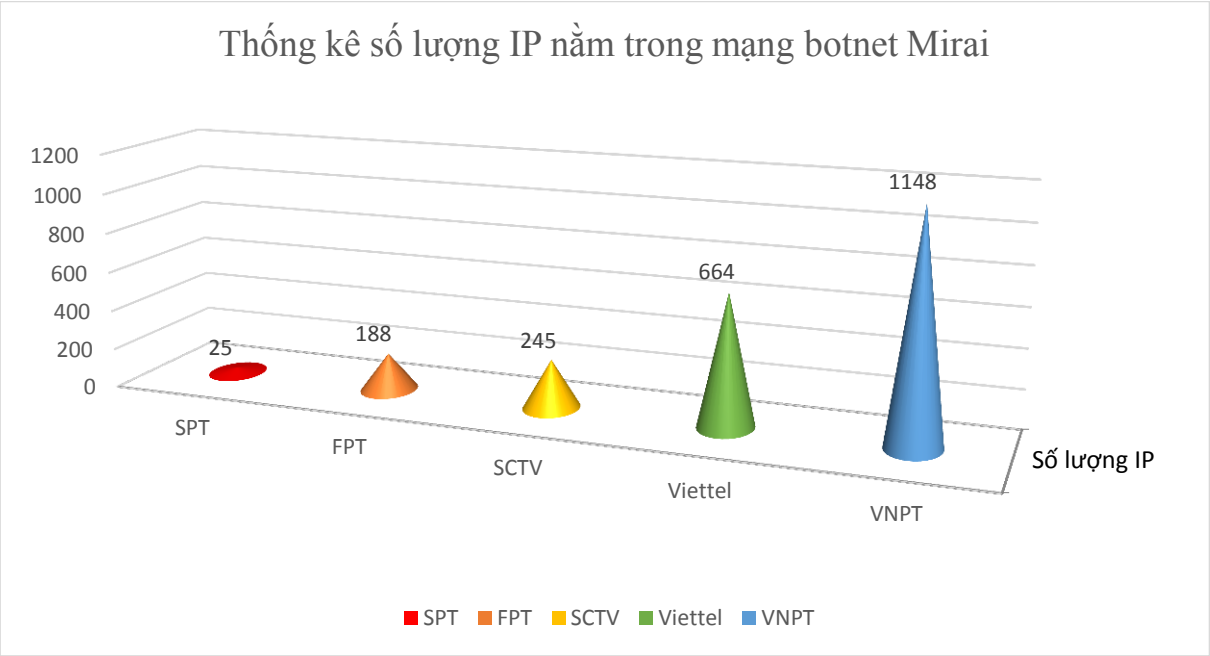
			FortiOS 5.2 và phiên bản trước đó.	
5	hotspot_shield	CVE-2018-6460	Lỗ hổng cho phép thu thập thông tin người dùng (bao gồm thông tin thiết bị, tài khoản người dùng để kết nối VPN) trên phần mềm Hotspot Shield	Chưa có thông tin bản vá
6	joomla	CVE-2018-6398 CVE-2018-6578 CVE-2018-6580 CVE-2018-6008 CVE-2018-6397 CVE-2018-6577	Nhóm 15 lỗ hổng trên nhiều thành phần mở rộng (như Visual Calendar, Support Ticket, SQL Injection exists in the JMS Music, CP Event Calendar…) và phần lõi của hệ quản trị nội dung Joomla cho phép thực hiện nhiều hình thức tấn công khác nhau bao gồm: SQL Injection, CSRF, XSS, file upload, Directory Traversal	Các lỗ hổng đều đã có mã khai thác

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

4.1. Mạng botnet Mirai

Mạng botnet Mirai được phát hiện từ tháng 8/2016. Mã độc này được thiết kế nhằm vào thiết bị IoT chứa lỗ hổng hoặc bảo mật kém vẫn đang sử dụng các mật khẩu mặc định. Khi mã độc Mirai xâm nhập thành công vào một thiết bị IoT, thì thiết bị này tham gia vào mạng botnet Mirai và có thể bị điều khiển để thực hiện các cuộc tấn công mạng, chẳng hạn như tấn công từ chối dịch vụ.

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



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

TT	Tên miền/IP
1	u.amobisc.com
2	i.onaoy.com
3	g.omlao.com
4	p.omlao.com
5	mk.omkol.com
6	qcygky5kvk.ru
7	kukutrustnet777.info
8	qqt31vsu.ru
9	104.244.14.252
10	hs3ftpqzlsr.ru

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

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 tại *mục 3.3* 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 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, TTTV.

(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;

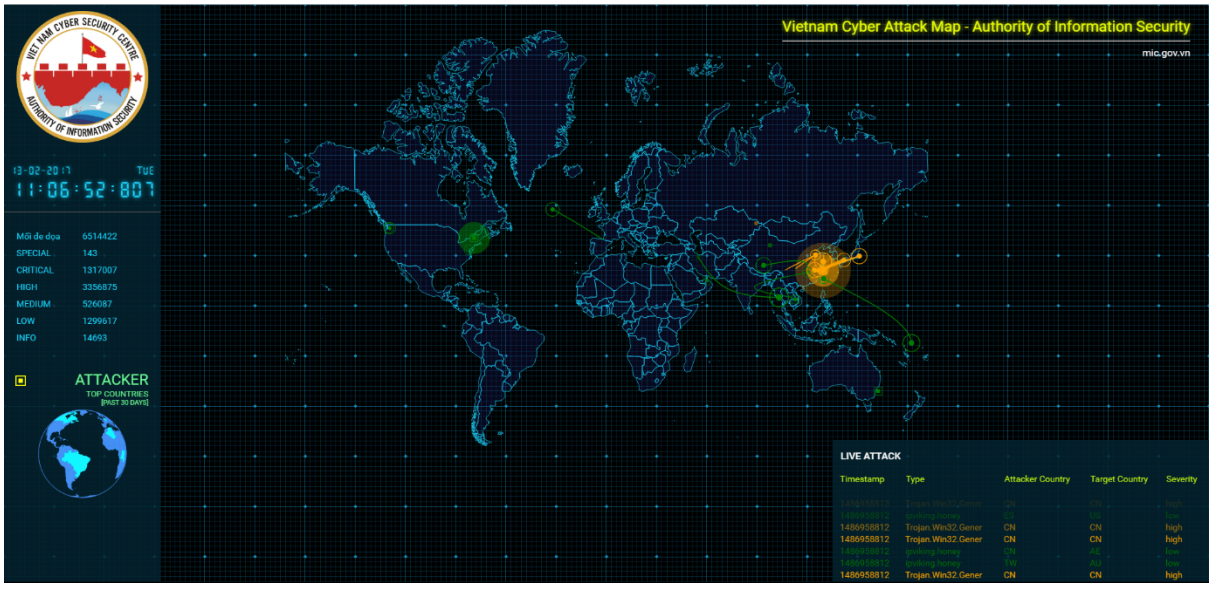
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

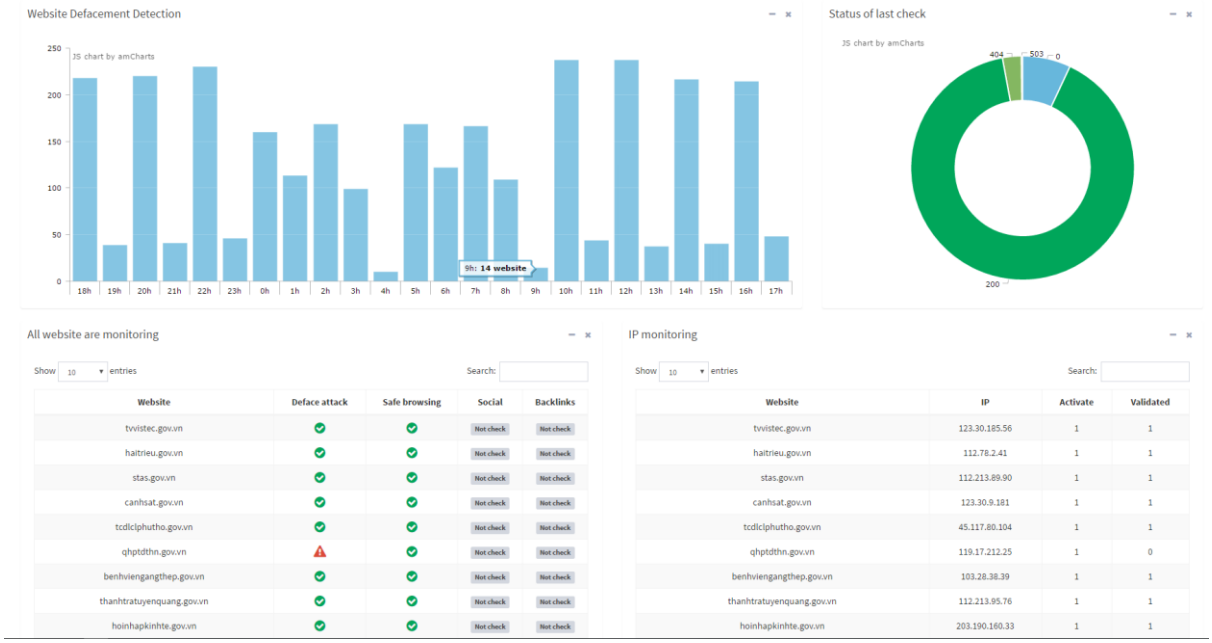
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



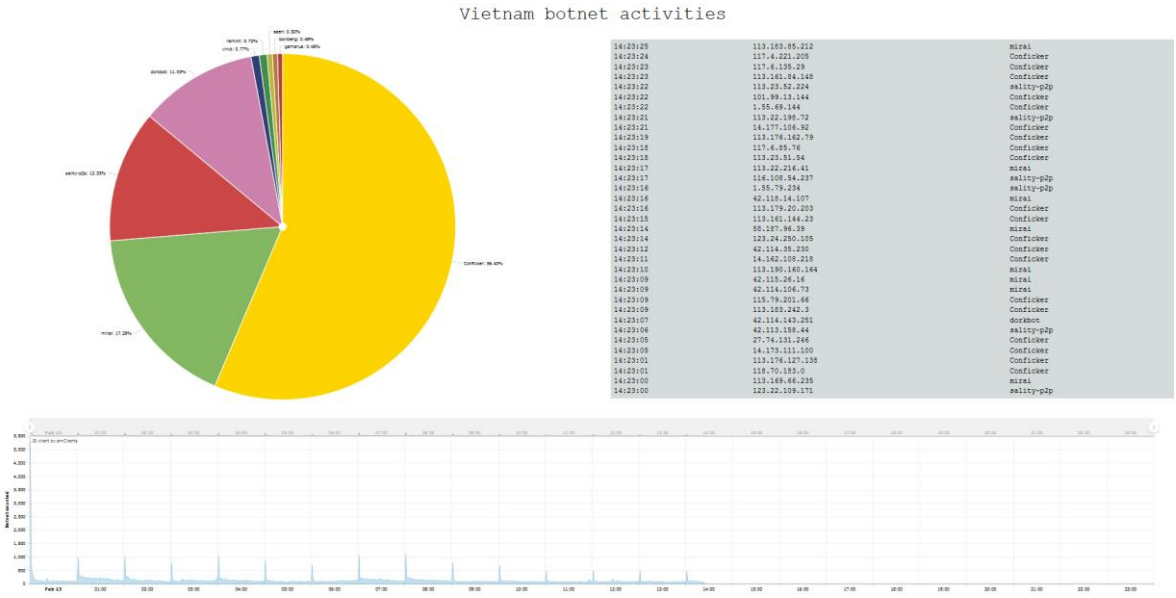
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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