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: **08**/BC-CATTT

Hà Nội, ngày 22 tháng 02 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 07/2018 (từ ngày 12/02/2018 đến ngày 18/02/2018)

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 07/2018 (từ ngày 12/02/2018 đến ngày 18/02/2018), 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 14/02/2018, Cơ quan năng lượng Hoa Kỳ (DOE) cho biết sẽ thiết lập một đơn vị mới có tên là CESER (Cybersecurity, Energy Security, and Emergency Response). CESER hỗ trợ việc bảo vệ lưới điện quốc gia và các cơ sở hạ tầng quan trọng khác trước các cuộc tấn công mạng và thiên tai.

2. Tại hội thảo an toàn thông tin Munich 2018 diễn ra từ ngày 16/02/2018 đến ngày 18/02/2018, Siemens cùng với một số công ty đa quốc gia khác như IBM, Airbus .v.v… đã đưa ra một bản điều lệ có tên là Trust. Một trong các mục tiêu cơ bản của bản điều lệ Trust là bảo vệ cơ sở hạ tầng quan trọng trên toàn thế giới trước các cuộc tấn công mạng.

3. Trong dịp nghỉ Tết Nguyên đán Mậu Tuất 2018 từ ngày 14/02/2018 và tính đến hết ngày 20/02/2018 (Mùng 05 Tết) có 115.134 địa chỉ IP của Việt Nam tiếp tục nằm trong các mạng bontnet mà Cục An toàn thông tin đang theo dõi (như Mirai, Sality, Ramnit, Cutwail…) con số này giảm đi đáng kể so với số liệu tuần trước tết (234.838), do trong kỳ nghỉ các máy tính ở cơ quan, tổ chức hầu hết đều không hoạt động.

1. Điểm tin đáng chú ý

1.1. Ngày 14/02/2018, Cơ quan năng lượng Hoa Kỳ (DOE) cho biết sẽ thiết lập một đơn vị mới có tên là CESER (Cybersecurity, Energy Security, and Emergency Response). CESER có nhiệm vụ chính là bảo vệ lưới điện quốc gia và các cơ sở hạ tầng quan trọng khác trước các cuộc tấn công mạng và thiên tai. Tổng thống Hoa Kỳ Donald Trump đã công bố đề xuất ngân sách 96 triệu USD cho CESER.

Người đứng đầu Cơ quan năng lượng Hoa Kỳ, Rick Perry tuyên bố an toàn thông tin mạng là một trong số các nhiệm vụ chính của DOE và nhiệm vụ này là thách thức lớn nhất đối với ông.

1.2. Tại hội thảo an toàn thông tin Munich 2018 diễn ra từ ngày 16/02/2018 đến ngày 18/02/2018, Siemens cùng với một số công ty đa quốc gia khác như IBM, Airbus .v.v… đã đưa ra một bản điều lệ có tên là Trust. Một trong các mục tiêu cơ bản của bản điều lệ Trust là bảo vệ cơ sở hạ tầng quan trọng trên toàn thế giới trước các cuộc tấn công mạng.

Bản điều lệ bao gồm 10 nguyên tắc, trong đó có các nguyên tắc như: bảo đảm an toàn thông tin là chức năng mặc định của sản phẩm và dịch vụ; khuyến khích đổi mới các giải pháp an toàn thông tin ...

1.3. Ngày 13/2 Microsoft đã phát hành bản vá bảo mật cho 50 lỗ hổng bảo mật cho các sản phẩm, ứng dụng hầu hết là trên hệ điều hành Windows, Ứng dụng Microsoft Office. Trong số đó có 14 lỗ hổng nghiêm trọng, 34 lỗ hổng ở mức cao, 02 lỗ hổng mức trung bình.

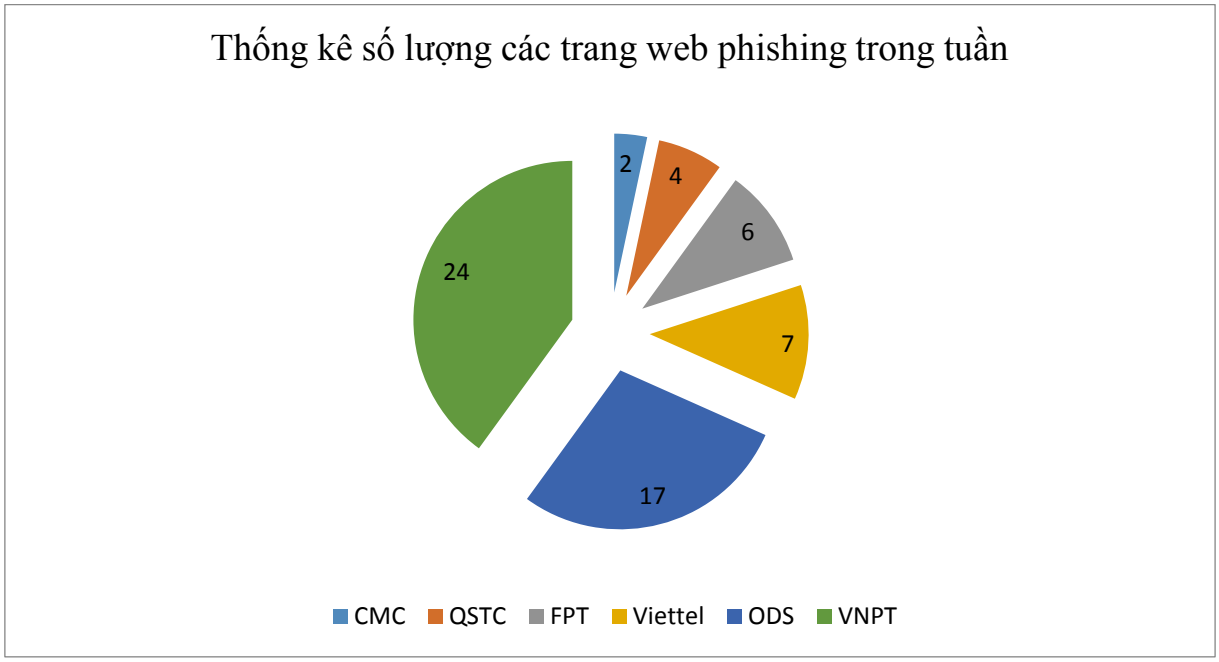
Một trong những lỗ hổng nghiêm trọng là lỗ hổng trên Microsoft Outlook cho phép chèn và thực thi mã lệnh từ xa. Với lỗ hổng này đối tượng tấn công có thể thực hiện tấn công từ xa qua thư điện tử hoặc web.

Trong kịch bản khai thác qua thư điện tử, đối tượng tấn công có thể tạo và gửi một thư điện tử đến người dùng thông qua một tập tin văn bản thông thường (nhưng cho phép đối tượng tấn công chèn mã khai thác lỗ hổng), khi người dùng xem thư điện tử này trong ứng dụng Outlook bị ảnh hưởng, thì mã khai thác sẽ được thực thi, đối tượng tấn công có thể cài mã độc và kiểm soát máy tính, thiết bị người dùng.

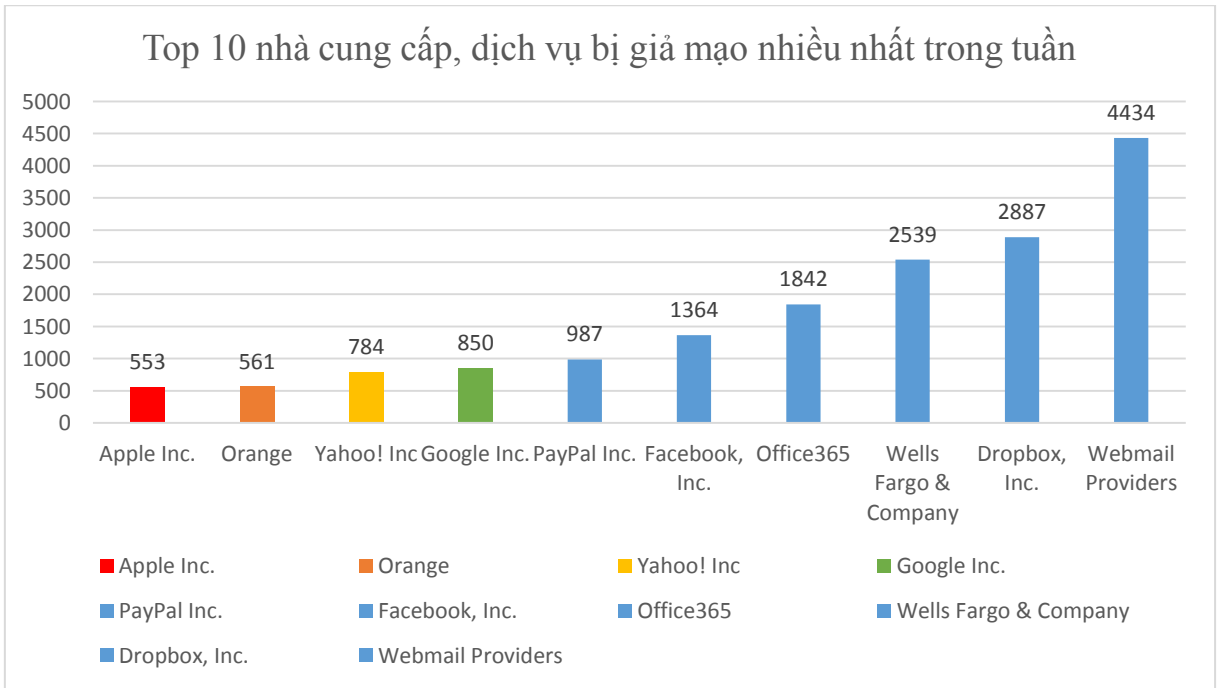
Cục An toàn thông tin khuyến cáo người dùng và quản trị viên tại các cơ quan đơn vị cần chú ý cập nhật ngay bản vá để bảo đảm an toàn thông tin.

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 60 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 .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 542 lỗ hổng trong đó có: 17 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 60 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 20 lỗ hổng trên nhiều thành phần khác nhau của hệ điều hành Android; Nhóm 71 lỗ hổng trên các sản phẩm, hệ điều hành của điện thoại thông minh Huawei .v.v…

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	Google – Android	CVE-2017-13228 CVE-2017-13234 CVE-2017-13230 ...	Nhóm 20 lỗ hổng trên nhiều thành phần khác nhau của hệ điều hành Android cho phép thực hiện các hình thức tấn công gồm: thu thập thông tin nhạy cảm, tấn công từ chối dịch vụ, chèn và thực thi mã lệnh, và tấn công leo thang Các lỗ hổng đã có bản vá, người dùng sử dụng thiết bị di động trên nền tảng Android có thể cập nhật ngay. Lỗ hổng CVE-2017-13236 đã có mã khai thác.	Đã có mã khai thác Đã có thông tin bản vá
2	HP	CVE-2017-5796 CVE-2017-8946 CVE-2017-5827 ..	Nhóm 187 lỗ hổng trên các sản phẩm, thiết bị của Hewlett Packard Enterprise (bao gồm: switch, Aruba AirWave Glass, Cloud Optimizer, Data Protector, ntelligent Management Center…) cho phép thực hiện các hình thức tấn công: CSRF, XSS, SQL Injection, chèn tập tin độc hại, thực thi mã lệnh từ xa, tấn công	Đã có mã khai thác Đã có thông tin bản vá

			leo thang, Nhiều lỗ hổng cho phép thực thi mã lệnh và đã có mã khai thác như CVE-2017-12542, CVE-2017-5817, CVE-2017-5816, CVE-2017-5792	
3	Huawei	CVE-2017-15344 CVE-2017-15343 CVE-2017-17184 CVE-2017-17156 CVE-2017-17283 ...	Nhóm 71 lỗ hổng trên các sản phẩm, hệ điều hành của điện thoại thông minh Huawei cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, vượt qua cơ chế xác thực để thực hiện hành vi trái phép, cài đặt ứng dụng, tập tin độc hại, Ảnh hưởng tới nhiều dòng điện thoại.	Đã có thông tin bản vá
4	IBM	CVE-2018-1383 CVE-2017-1682 CVE-2017-1761 ...	Nhóm 09 lỗ hổng trên các sản phẩm, ứng dụng của IBM (bao gồm IBM Connections, IBM iNotes, Maximo Asset Management, Security Guardium Database Activity Monitor, IBM WebSphere Portal) cho phép thực hiện tấn công: chèn các đoạn mã JavaScript để ăn trộm thông tin xác thực, thực thi tập tin DLL độc hại, chèn và thực thi mã lệnh và tấn công leo thang.	Đã có thông tin bản vá
5	Joomla	CVE-2018-5974 CVE-2018-7180 CVE-2018-7179 CVE-2018-5982 CVE-2018-6373	Nhóm 31 lỗ hổng trên các thành phần, module của Joomla cho phép thực hiện tấn công SQL Injection truy cập vào trái phép vào dữ liệu trên hệ thống Hầu hết các lỗ hổng đã có mã khai thác. Joomla là hệ quản trị nội dung nguồn mở sử dụng phổ biến tại Việt Nam.	Đã có mã khai thác Chưa có thông tin bản vá

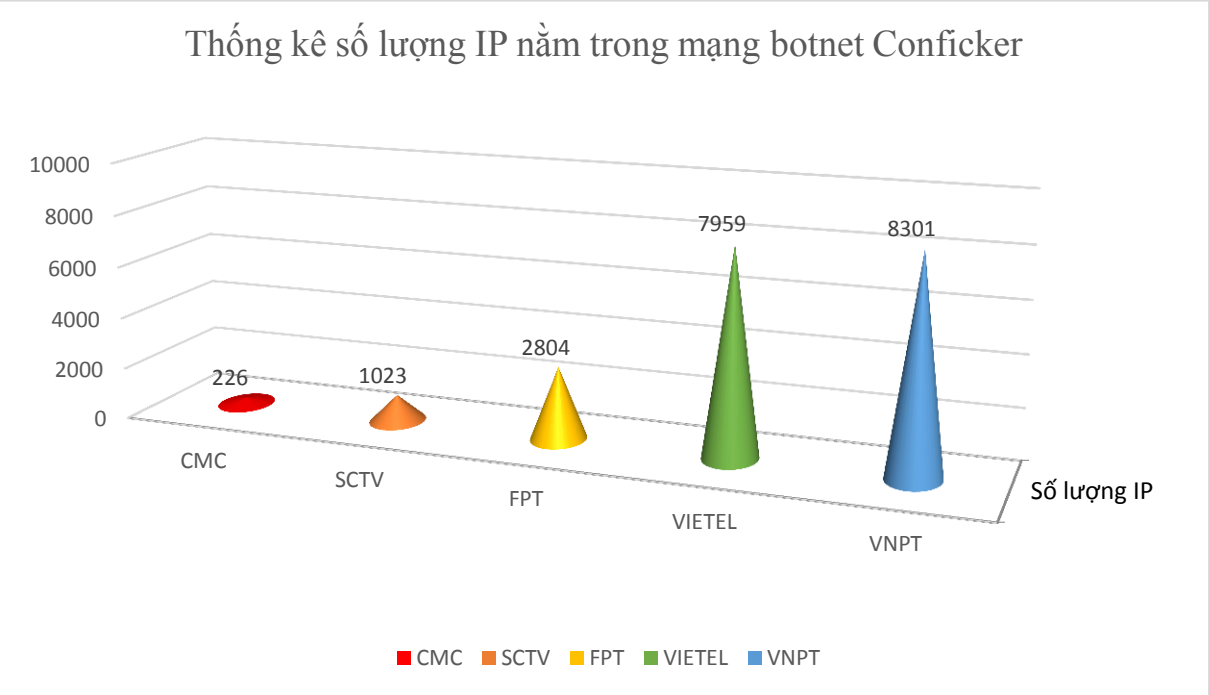
6	Microsoft	CVE-2018-0858 CVE-2018-0763 CVE-2018-0839 CVE-2018-0771 CVE-2018-0856	Nhóm 50 lỗ hổng trên các sản phẩm, ứng dụng (ChakraCore, Microsoft Edge, Internet Explorer, Microsoft Office, Windows) của Microsoft cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau, nhiều lỗ hổng cho phép chèn và thực thi mã lệnh	Đã có thông tin bản vá

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	g.omlao.com
2	u.amobisc.com
3	i.onaoy.com
4	mk.omkol.com
5	jwd0ylsp.ru
6	4yuwi9kbmm.ru
7	kukutrustnet777.info
8	qhcqvdmp.ru
9	104.244.14.252
10	09wb2knotg.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; (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;

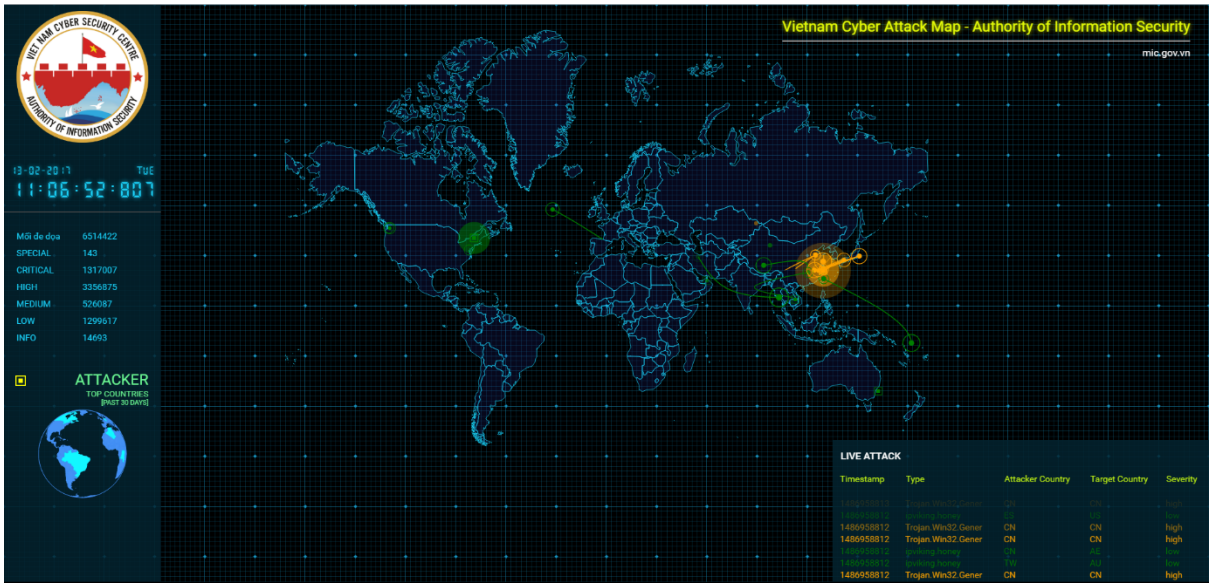
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

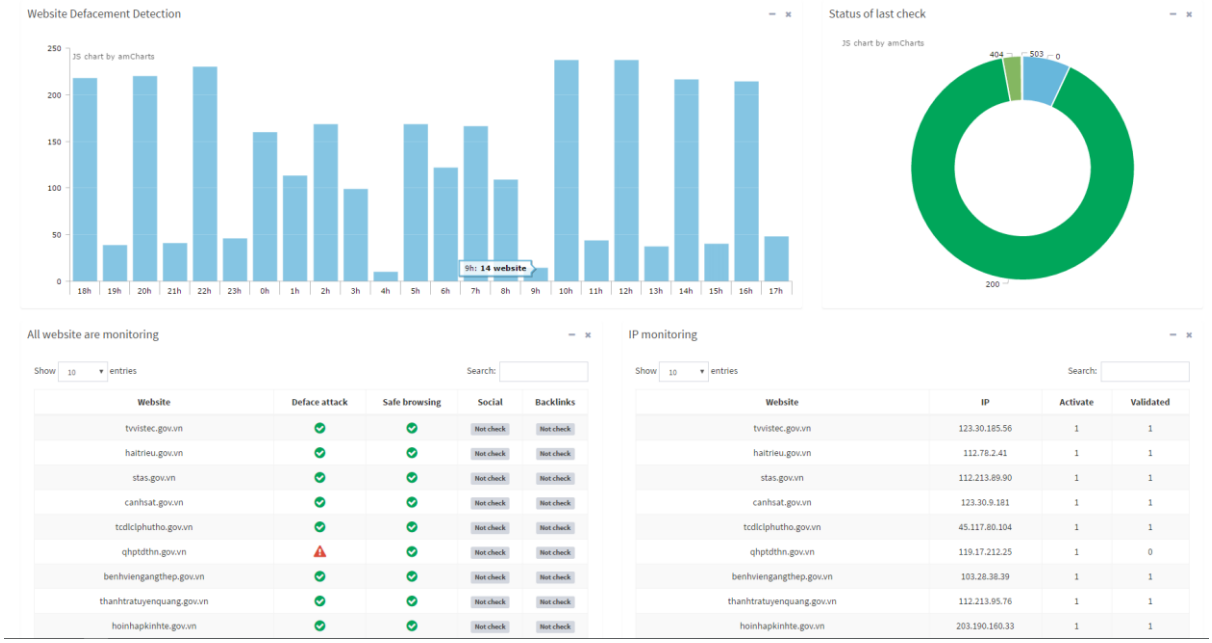
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



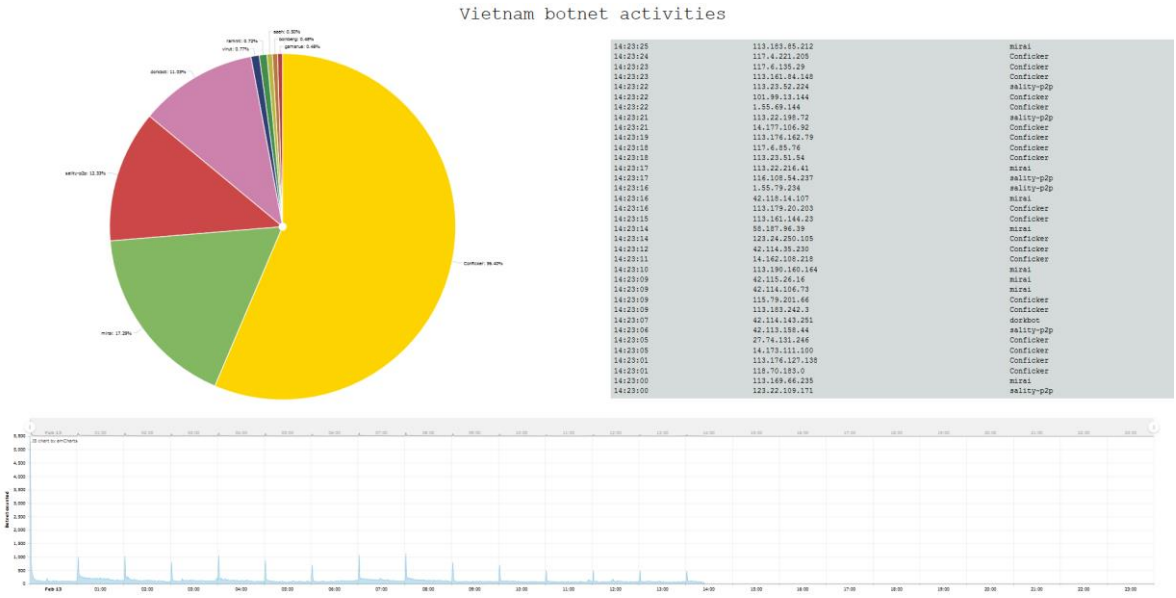
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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