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: **09**/BC-CATTT

Hà Nội, ngày 27 tháng 02 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 08/2018 (từ ngày 19/02/2018 đến ngày 25/02/2018)

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 08/2018 (từ ngày 19/02/2018 đến ngày 25/02/2018), 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 21/2/2018, Ủy ban chứng khoán và giao dịch (SEC), Hoa Kỳ đã thông qua việc phát hành tài liệu hướng dẫn an toàn thông tin mạng cho các công ty đại chúng khi chuẩn bị công bố về các nguy cơ mất an toàn thông tin và các cuộc tấn công mạng vào hệ thống của mình. Tài liệu hướng dẫn cũng thông báo chủ trương của Ủy ban về tầm quan trọng của việc duy trì các chính sách và thủ tục toàn diện liên quan đến an toàn thông tin mạng.

2. Ngày 21/02/2018, Cisco công bố Báo cáo thường niên về an toàn thông tin mạng. Báo cáo dựa trên các số liệu từ các hệ thống của Cisco và thông tin từ việc khảo sát 3600 Lãnh đạo phụ trách an toàn thông tin của các tổ chức.

3. Trong tuần ghi nhận 04 nhóm lỗ hổng và 02 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.

1. Điểm tin đáng chú ý

1.1. Ngày 21/2/2018, Ủy ban chứng khoán và giao dịch (SEC), Hoa Kỳ đã thông qua việc phát hành tài liệu hướng dẫn an toàn thông tin mạng cho các

công ty đại chúng khi chuẩn bị công bố về các nguy cơ mất an toàn thông tin và các cuộc tấn công mạng vào hệ thống của mình. Tài liệu hướng dẫn cũng thông báo chủ trương của Ủy ban về tầm quan trọng của việc duy trì các chính sách và thủ tục toàn diện liên quan đến an toàn thông tin mạng.

Theo Chủ tịch SEC, ông Jay Clayton, quan điểm của Ủy ban về những vấn đề an toàn thông tin mạng sẽ giúp cho việc cung cấp thông tin đầy đủ, rõ ràng hơn cho các nhà đầu tư. Ngày nay, an toàn thông tin mạng rất quan trọng đối với hoạt động của các thị trường tài chính và các công ty, khi họ ngày càng phụ thuộc nhiều vào các công nghệ số trong các hoạt động kinh doanh và liên kết với đối tác, khách hàng. Sự phụ thuộc và tiếp xúc với thế giới số kèm theo đó cũng phải đối mặt với những nguy cơ mất an toàn thông tin mạng.

Tài liệu hướng dẫn cũng nhấn mạnh việc kiểm soát sự chia sẻ thông tin và các quy trình có thể tạo ra cơ chế để xác định tác động của một cuộc tấn công mạng. Đây chính là chìa khoá để các công ty có thể thực hiện bất kỳ yêu cầu công bố thông tin. Các công ty đại chúng phải tập trung vào những vấn đề này và thực hiện tất cả các hành động cần thiết để thông báo cho các nhà đầu tư về các nguy cơ, các cuộc tấn công mạng một cách kịp thời.

1.2. Ngày 21/02/2018, Cisco công bố Báo cáo thường niên về an toàn thông tin mạng. Báo cáo dựa trên các số liệu từ các hệ thống của Cisco và thông tin từ việc khảo sát 3600 Lãnh đạo phụ trách an toàn thông tin của các tổ chức.

Theo Báo cáo, 39% các tổ chức dựa vào các công nghệ tự động hóa như học máy, trí tuệ nhân tạo trong các hoạt động bảo đảm an toàn thông tin. Báo cáo cũng cho biết nhiều tổ chức đang cùng lúc sử dụng các giải pháp, dịch vụ, sản phẩm an toàn thông tin của các hãng khác nhau. Theo số liệu năm 2017 của Báo cáo thì có 25% tổ chức cho biết họ sử dụng công nghệ an toàn thông tin mạng của hơn 10 nhà cung cấp khác nhau, con số này năm 2016 là 18%. Đối với việc cảnh báo an toàn thông tin mạng và phản hồi của các tổ chức, Cisco cho biết chỉ khoảng 56% các cảnh báo thực sự được quan tâm và tiến hành xử lý. Cisco khuyến nghị các tổ chức cần xem xét và thực hiện các thủ tục phản hồi về an toàn thông tin mạng, thường xuyên rà soát và vá các điểm yếu, lỗ hổng đã được công bố, cảnh báo để giảm thiểu nguy cơ gây mất an toàn thông tin.

1.3. Ngày 20/02/2018, hãng bảo mật FireEye đã công bố một báo cáo về một nhóm đối tượng tấn công mạng, được gọi là APT37 (Reaper).

Theo phân tích của FireEye, các hoạt động của nhóm APT37 đang mở rộng phạm vi và ngày càng tinh vi hơn, với bộ công cụ với khả năng phát tán mã độc wiper và các lỗ hổng zero-day. FireEye cho rằng tổ chức Reaper hoạt động dưới

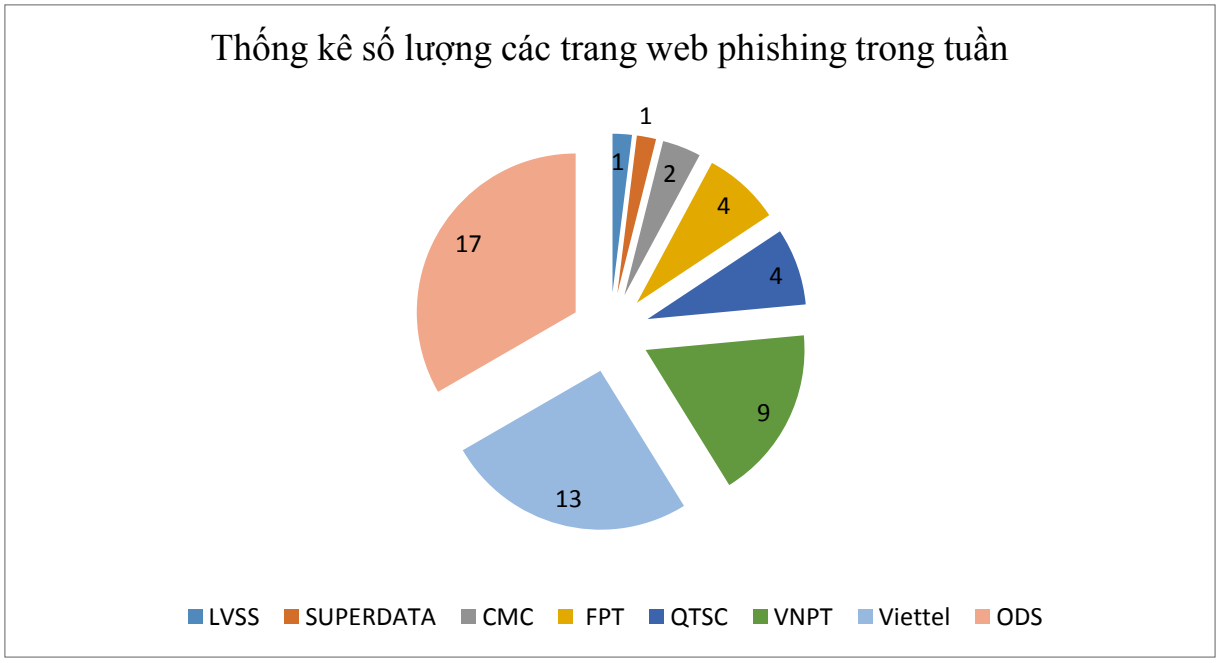
“bóng” của nhóm Lazarus, nhóm đối tượng tấn công mạng được cho là đã thực hiện vụ tấn công hãng Sony Pictures năm 2014 và WannaCry năm 2017. Tuy nhiên, thay vì mục đích phá hoại hay tống tiền như các tổ chức khác, APT37 tập trung vào việc thu thập và đánh cắp thông tin.

Trong báo cáo của FireEye, APT37 đã theo dõi các mục tiêu trong lãnh thổ Hàn Quốc ít nhất từ năm 2012, và gần đây mở rộng hoạt động nhằm vào khu vực Trung Đông, Nhật Bản và các khu vực khác trong đó có Việt Nam. Mục tiêu chính của các hoạt động này là nhằm vào các ngành công nghiệp như năng lượng, hàng không .v.v… Ở Việt Nam, FireEye cho biết, giám đốc của một công ty thương mại và vận tải quốc tế cũng là mục tiêu của nhóm này.

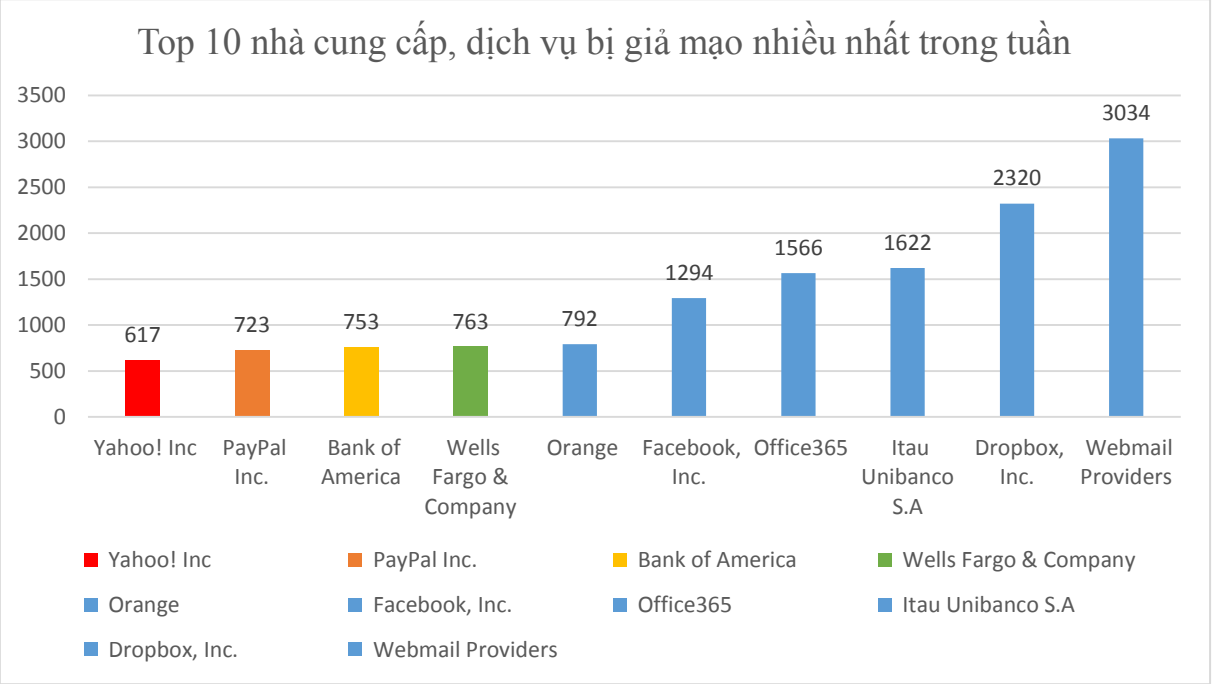
Cục An toàn thông tin đang tiếp tục liên hệ và theo dõi thông tin về nhóm APT37.

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 51 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 287 lỗ hổng trong đó có: 34 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 52 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 **04** nhóm lỗ hổng và **02** 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 14 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco; Nhóm 19 lỗ hổng trên một số sản phẩm, ứng dụng của IBM .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	Cisco	CVE-2018-0145 CVE-2018-0130 CVE-2018-0199	Nhóm 14 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (bao gồm Cisco Data Center Analytics Framework, Elastic Services Controller Software,	Đã có xác nhận và thông tin bản vá

			Jabber Client Framework, UCS Director Software, Integrated Management Controller, Prime Service Catalog, Prime Collaboration Provisioning Tool…) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau: tấn công XSS, CSRF trên các sản phẩm có ứng dụng web, thu thập thông tin trái phép, vượt qua cơ chế xác thực để thực hiện các hành động như một quản trị viên (CVE-2018-0121), nhiều lỗ hổng cho phép chèn và thực thi mã lệnh (như CVE-2018-0124)	
2	D-link	CVE-2018-6936	Lỗ hổng trong sản phẩm Home Router D-Link DIR-600M cho phép thực hiện tấn công XSS từ đó có thể chiếm quyền kiểm soát thiết bị D-Link là một trong những hãng sản xuất thiết bị bộ định tuyến và phát wifi sử dụng khá phổ biến tại Việt Nam, nhưng việc cung cấp các bản vá bảo mật cho các thiết bị của hãng này chưa thực sự được quan tâm do vậy người dùng và quản trị viên khi sử dụng thiết bị này cần phải có những biện pháp riêng nhằm hạn chế tối đa các nguy cơ mất an toàn thông tin.	Chưa có thông tin bản vá
3	Fuji Soft Incorporated	CVE-2018-0519 CVE-2018-0520	Nhóm 02 lỗ hổng trong firmware phiên bản FS010W_00_V1.3.0 và phiên bản trước đó trên sản phẩm Wifi Router cho phép thực hiện một số hình thức tấn công web như CSRF, chèn các đoạn mã HTML để lấy thông tin xác thực	Đã có cảnh báo từ JPCERT Đã có thông tin bản vá
4	Zyxel	CVE-2018-1164	Lỗ hổng trong sản phẩm P-870H-51 DSL Router của Zylxel cho phép truy cập vào	Chưa có thông tin bản vá.

			các chức năng quan trọng trên thiết bị mà không cần xác thực, từ đó có thể chiếm quyền điều khiển thiết bị Zyxel cũng là một trong những thiết bị phổ biến tại Việt Nam nhưng nhiều lỗ hổng trên các thiết bị của hãng này vẫn chưa được vá.	
5	IBM	CVE-2018-1391 CVE-2017-1758 CVE-2018-1392 CVE-2016-0369 CVE-2018-1417 …	Nhóm 19 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (Financial Transaction Manager, IBM Forms Experience Builder, Maximo Anywhere, IBM Notes Diagnostics, IBM Rhapsody DM, BM Security Identity Manager Virtual Appliance) cho phép thực hiện nhiều hình thức tấn công như thu thập thông tin trái phép, chèn các đoạn mã JavaScrip để lấy trộm thông tin xác thực, SQL Injection, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã xác nhận Đã có thông tin bản vá
6	Joomla	CVE-2018-6397 CVE-2018-5981 CVE-2018-7177 CVE-2018-5989 …	Nhóm 41 lỗ hổng trên nhiều thành phần của Joomla cho phép thực hiện các tấn công trên nền web (như SQL Injection) và truy cập trái phép vào các thông tin trên hệ thống. Joomla là một trong những hệ quản trị nội dung được dùng khá phổ biến tại Việt Nam.	Chưa có thông tin bản vá Đã có mã khai thác

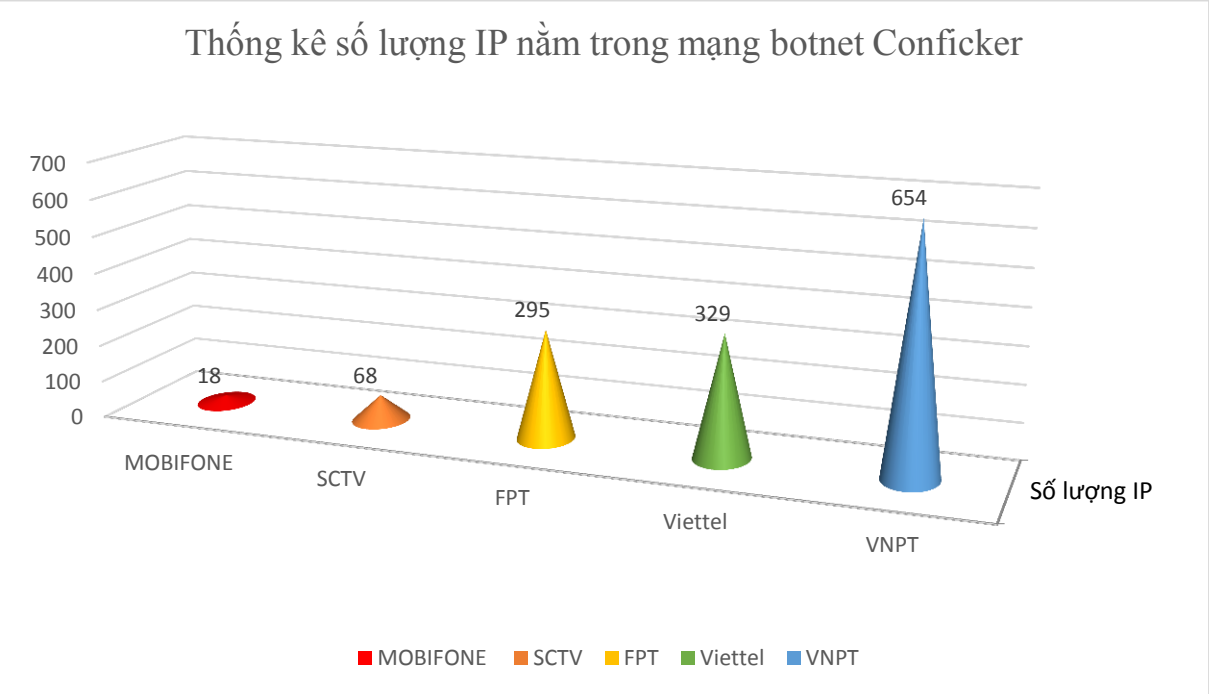
4. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

4.1. Mạng botnet Ramnit

Mạng botnet Ramnit là mạng botnet có mục tiêu tấn công vào ngân hàng và các tổ chức tài chính, phát hiện lần đầu vào năm 2010. Mã độc của mạng botnet này là một sâu máy tính tấn công vào người dùng hệ điều hành Windows. Theo ước tính vào tháng 9 đến tháng 12/2011 mã độc Ramnit đã lây nhiễm vào ít nhất 800.000 máy tính Windows, đến năm 2015 con số này lên đến trên 3 triệu

máy tính. Tháng 12/2015 IBM đã phát hiện ra biến thể mới của Ramnit nhằm vào các ngân hàng ở Canada, Úc, Mỹ và Phần Lan. Năm 2016, mã độc này tiếp tục nhằm vào các ngân hàng ở Anh, Mỹ.

Tại Việt Nam, cũng có một số lượng không ít các thiết bị nằm trong mạng botnet Ramnit. Dưới đây là một số thông kê về về mạng botnet Ramnit tại Việt Nam 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	jwd0ylsp.ru
2	104.244.14.252
3	kukutrustnet777.info
4	7r3xtzaao.ru
5	09wb2knotg.ru
6	mk.omkol.com
7	g.omlao.com
8	u.amobisc.com
9	kukutrustnet888.info
10	i.onaoy.com

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;

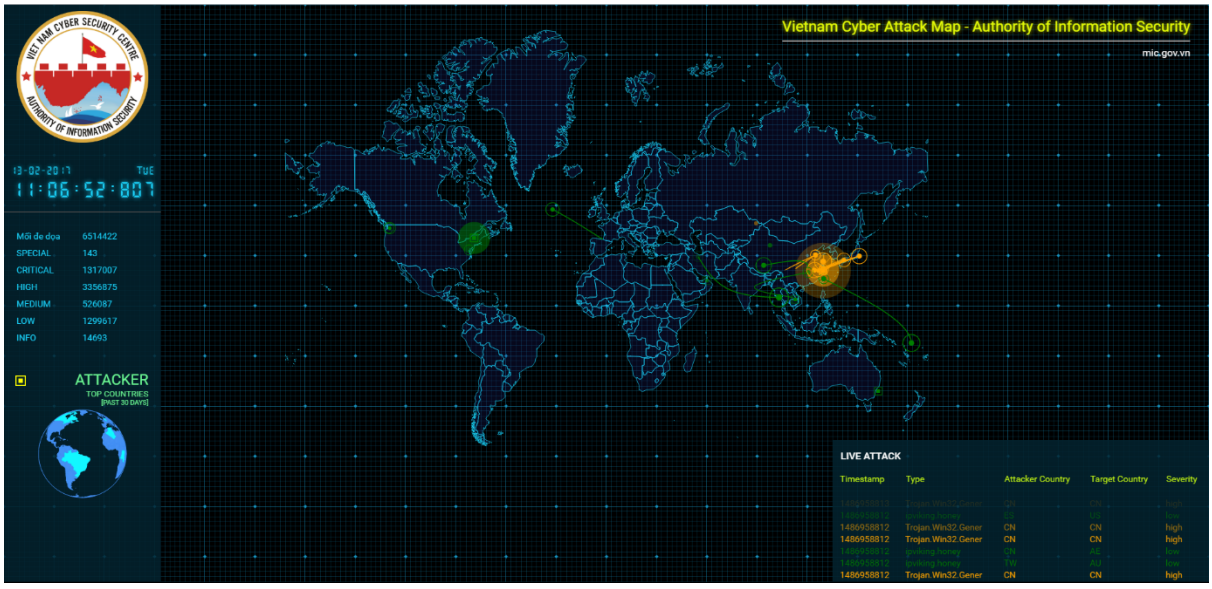
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

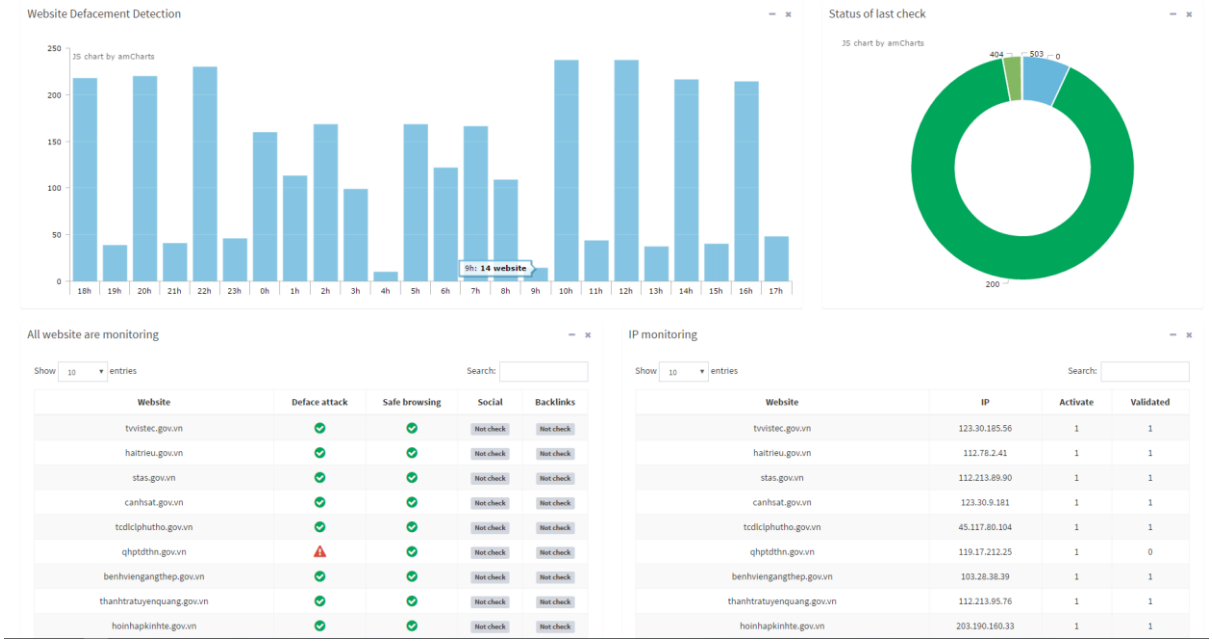
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



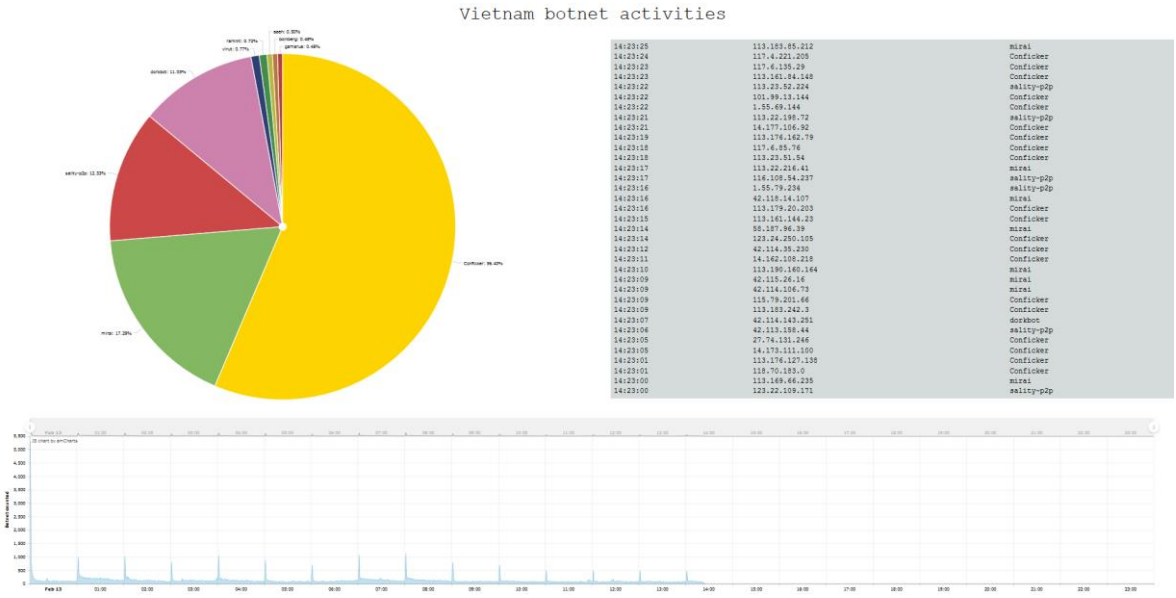
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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