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: **10**/BC-CATTT

Hà Nội, ngày 06 tháng 03 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 09/2018 (từ ngày 26/02/2018 đến ngày 04/3/2018)

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 09/2018 (từ ngày 26/02/2018 đến ngày 04/3/2018), 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. Cục Quản lý An toàn Hạt nhân Quốc gia, Hoa Kỳ đã cho đăng thông báo mời thầu các doanh nghiệp tham gia ngăn chặn các cuộc tấn công mạng nhằm vào các cơ sở hạt nhân và quá trình vận chuyển vật liệu, thiết bị hạt nhân.

2. Cuối tháng 02/2018, Bộ Tư pháp Hoa Kỳ tuyên bố thành lập bộ phận chuyên trách về an toàn thông tin mạng. Đơn vị này sẽ giúp Bộ Tư pháp Hoa Kỳ chống lại các nguy cơ mất an toàn thông tin mạng và cụ thể hóa việc thực thi pháp luật liên bang hiệu quả hơn.

3. Trong tuần, Cục ATTT ghi nhận có ít nhất 97 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc; lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động .

1. Điểm tin đáng chú ý

1.1. Cục Quản lý An toàn Hạt nhân Quốc gia, Hoa Kỳ đã cho đăng thông báo mời thầu các doanh nghiệp tham gia ngăn chặn các cuộc tấn công mạng

nhằm vào các cơ sở hạt nhân và quá trình vận chuyển vật liệu, thiết bị hạt nhân. Theo một nghiên cứu đang được tiến hành bởi Văn phòng An toàn bức xạ, vận chuyển vật liệu phóng xạ là công việc nguy hiểm, các hệ thống liên lạc được nhúng trong các phương tiện vận chuyển này có thể bị tấn công bởi các cuộc tấn công mạng, dẫn đến hậu quả nghiêm trọng.

Theo thông báo của bên mời thầu thì hợp đồng này có thể được ký kết với cả những doanh nghiệp nhỏ, miễn là các doanh nghiệp đó đáp ứng các tiêu chuẩn nhất định, bao gồm các chứng nhận, giấy phép và kinh nghiệm trong lĩnh vực an toàn thông tin, năng lượng.

Công ty được ký hợp đồng sẽ thực hiện một số trách nhiệm như:

- Hướng dẫn về an toàn thông tin mạng, đào tạo và đánh giá cho Văn phòng An toàn bức xạ;

- Phát triển "kịch bản không gian mạng" tin cậy, bao gồm các thành phần vật lý, cũng như các chiến lược để bảo vệ chống lại các cuộc tấn công mạng tiềm ẩn;

- Tiến hành đánh giá lỗ hổng, điểm yếu và kiểm tra thiết bị để xác định và khắc phục những lỗ hổng, điểm yếu được phát hiện;

- Tham gia làm việc với Nhóm Công tác về Hạt nhân, Nhóm Tương tác an toàn thông tin từ xa và Hội đồng quốc gia điều phối chính sách an ninh hạt nhân với tư cách là chuyên gia;

- Rà soát các chính sách và hướng dẫn cập nhật nhất về an toàn thông tin mạng của Cơ quan Năng lượng nguyên tử Quốc tế và Ủy ban Hạt nhân.

1.2. Cuối tháng 02/2018, Bộ Tư pháp Hoa Kỳ tuyên bố thành lập bộ phận chuyên trách về an toàn thông tin mạng. Đơn vị này sẽ giúp Bộ Tư pháp Hoa Kỳ chống lại các nguy cơ mất an toàn thông tin mạng và cụ thể hóa việc thực thi pháp luật liên bang hiệu quả hơn.

Bộ trưởng Bộ Tư pháp Hoa Kỳ đã yêu cầu bộ phận chuyên trách này ưu tiên nghiên cứu những nỗ lực can thiệp vào cuộc bầu cử; những nỗ lực can thiệp vào cơ sở hạ tầng then chốt; việc sử dụng Internet để truyền bá tư tưởng bạo lực; việc ăn cắp thông tin chính phủ, doanh nghiệp, cá nhân; và việc khai thác lỗ hổng, điểm yếu an toàn thông tin để tấn công các công dân và doanh nghiệp Hoa Kỳ. Bộ phận này sẽ chịu trách nhiệm báo cáo lên Bộ trưởng vào cuối tháng 6 hàng năm.

1.3. Ngày 28/02/2018, trang web lưu trữ mã nguồn của GitHub đã bị tấn công từ chối dịch vụ (DDoS) với quy mô lớn nhất từ trước tới nay với lưu lượng đỉnh đạt 1.35 Tbps tương đương hơn 120 triệu gói tin/giây. Điều đặc biệt của cuộc tấn công này là việc đối tượng tấn công không sử dụng bất kỳ mạng botnet nào, thay vào đó đối tượng tấn công đã lợi dụng các lỗi cấu hình bộ nhớ tạm thời (Memcached) của các máy chủ để khuếch đại tấn công DDoS.

Dạng tấn công DDoS khuếch đại này hoạt động bằng cách sử dụng địa chỉ IP giả mạo địa chỉ IP của nạn nhân để gửi bản tin yêu cầu tới máy chủ mục tiêu trên cổng 11211. Một số byte của bản tin yêu cầu gửi từ đối tượng tấn công đến máy chủ tồn tại điểm yếu sẽ kích hoạt hàng chục nghìn lần phản hồi ngược lại địa chỉ IP nạn nhân.

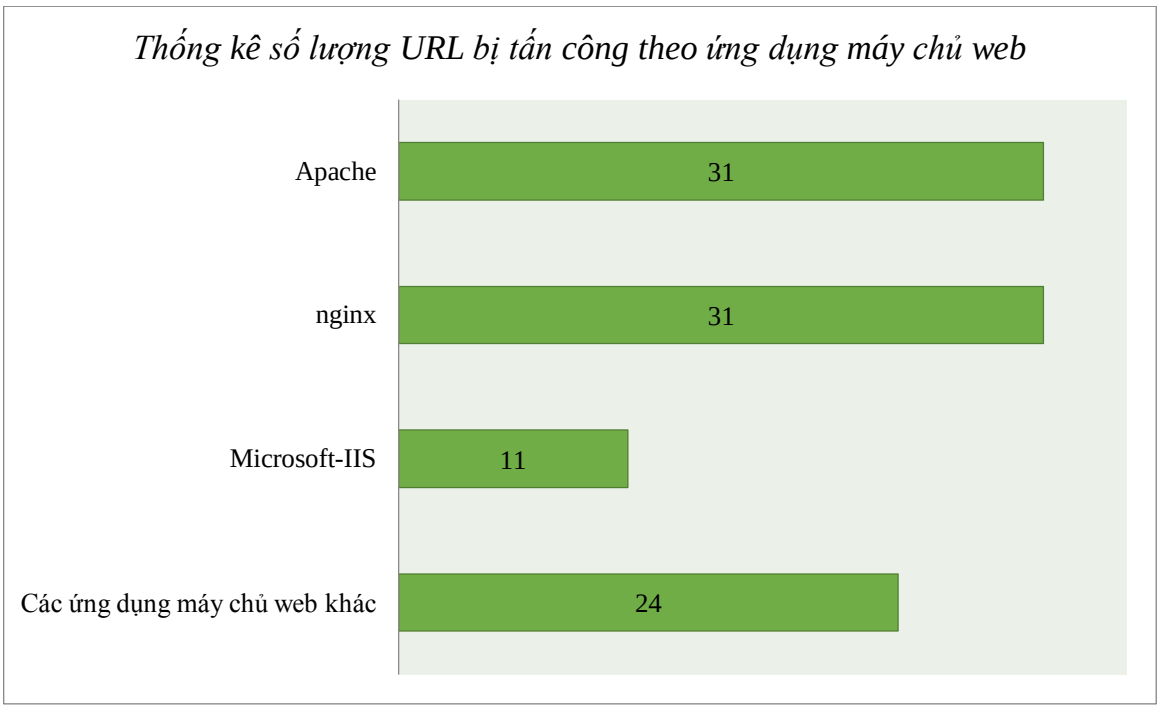
Mặc dù tấn công DDoS khuếch đại không phải là dạng tấn công mới, nhưng trong cuộc tấn công này, đối tượng tấn công đã cải tiến phương thức hướng đến lỗi cấu hình Memcached của hàng nghìn máy chủ, nhiều trong số đó vẫn bị công khai trên Internet và có thể bị khai thác để khởi động các cuộc tấn công DDoS có lưu lượng rất lớn.

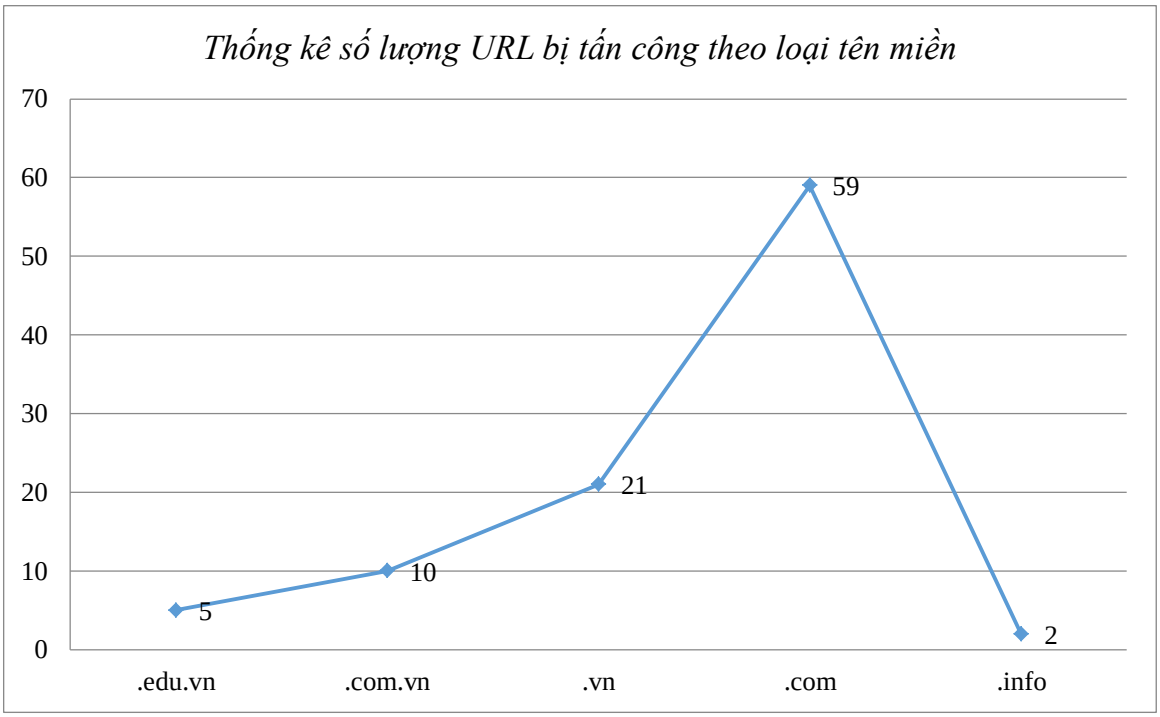
Để phòng ngừa nguy cơ các máy chủ có sử dụng Memcached bị lợi dụng làm công cụ thực hiện các cuộc tấn công DDoS, Cục An toàn thông tin khuyến nghị các quản trị viên tại các cơ quan, tổ chức nên xem xét việc cấu hình tường lửa bảo vệ, chặn hoặc giới hạn tốc độ giao thức UDP trên cổng nguồn 11211 hoặc vô hiệu hóa hỗ trợ giao thức UDP nếu không sử dụng.

2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua, Cục ATTT nhận thấy trên không gian mạng đang tồn tại nhiều trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc (gần đây nhất là cài đặt và phát tán mã độc để đào tiền ảo); lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng .v.v…).

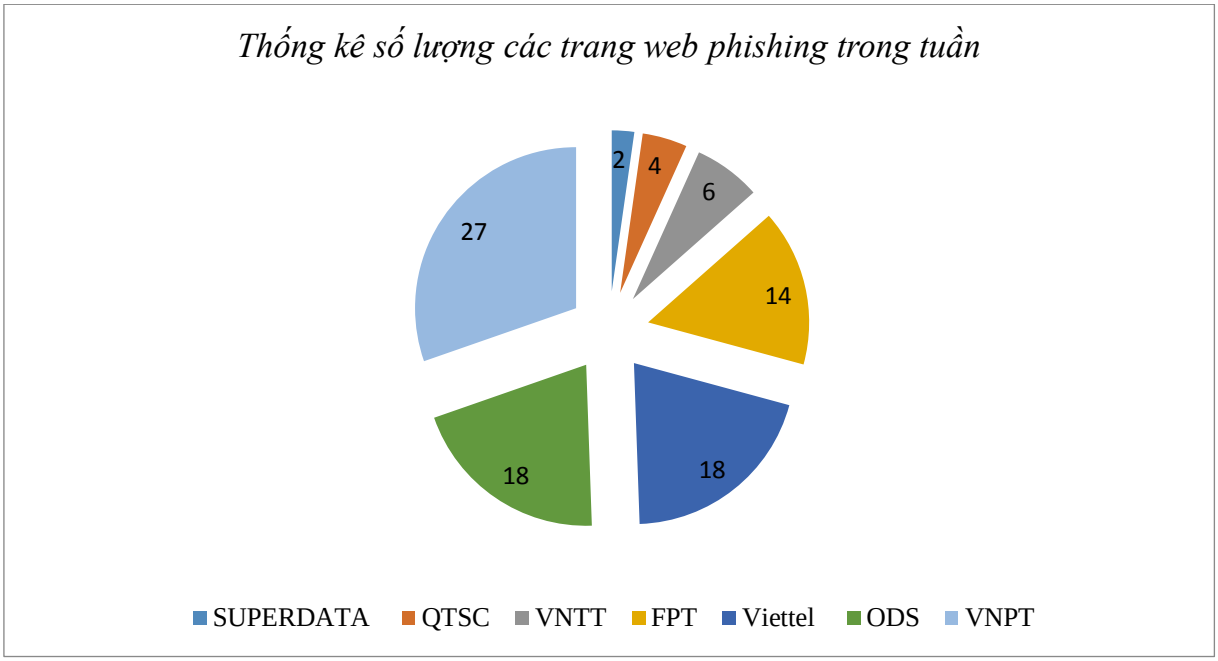
Trong tuần, Cục ATTT ghi nhận có ít nhất 97 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và loại tên miền (.com, .vn, …) cụ thể như sau:



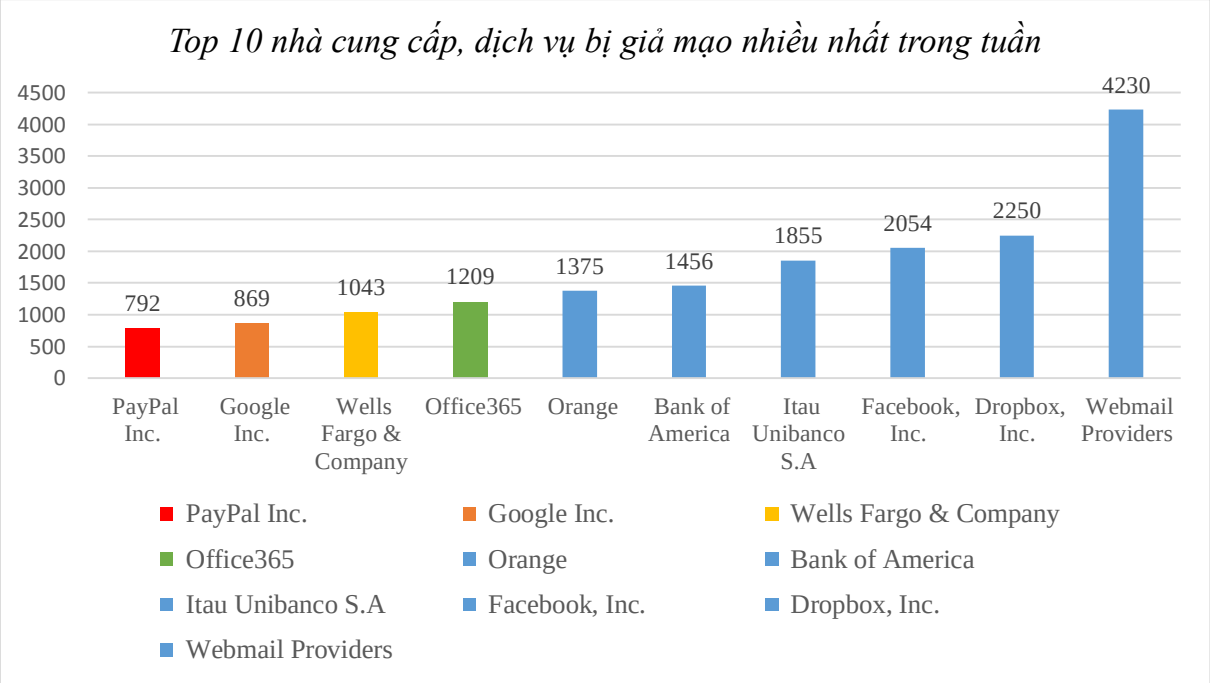


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất 89 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



3.2. 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.

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

4.1. Trong tuần, các tổ chức quốc tế đã phát hiện và công bố ít nhất 292 lỗ hổng trong đó có: 32 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 15 lỗ hổng đã có mã khai thác.

4.2. 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 **01** 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 lỗ hổng trên hệ điều hành Windows Vista, 7, 8 và 8.1; Nhóm 39 lỗ hổng, điểm yếu trên sản phẩm Acrobat Reader .v.v…

4.3. 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	Tenda	CVE-2018-7561	Lỗi tràn bộ đệm trong một số thiết bị Tenda AC9 phiên bản V15.03.05.14_EN cho phép tấn công từ chối dịch vụ từ xa hoặc gây ra các ảnh hưởng khác.	Chưa có thông tin bản vá Đã có mã khai thác
2	Microsoft Windows	CVE-2018-7249 CVE-2018-7250	Nhóm lỗ hổng trên hệ điều hành Windows Vista, 7, 8 và 8.1, cho phép vượt quyền thực thi mã trong kernel hoặc đọc được dữ liệu lưu trên kernel	Đã có xác nhận và thông tin bản vá
3	IBM	CVE-2016-0291 CVE-2016-0295 CVE-2018-1399 CVE-2017-1787 …	Nhóm 12 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (BigFix Platform, Daeja ViewONE, Publishing Engine, Security Guardium Big Data Intelligence …) 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, XSS, SQL Injection,	Đã có xác nhận và thông tin bản vá

			một số lỗ hổng cho phép chèn và thực thi mã lệnh.	
4	Adobe Acrobat Reader	CVE-2018-4902 CVE-2018-4907 CVE-2018-4889 CVE-2018-4895 …	Nhóm 39 lỗ hổng, điểm yếu trên sản phẩm Acrobat Reader cho phép thực hiện tấn công thực thi mã lệnh từ xa, truy cập thông tin trái phép, phá hoại thông tin,…	Đã có xác nhận và thông tin bản vá
5	Drupal	CVE-2017-6926 CVE-2017-6929 CVE-2017-6932 CVE-2017-6928 …	Nhóm 7 lỗ hổng trên nhiều phiên bản Drupal có thể dẫn đến tấn công XSS, phishing hoặc vượt quyền.	Một vài lỗ hổng đã có xác nhận và thông tin bản vá

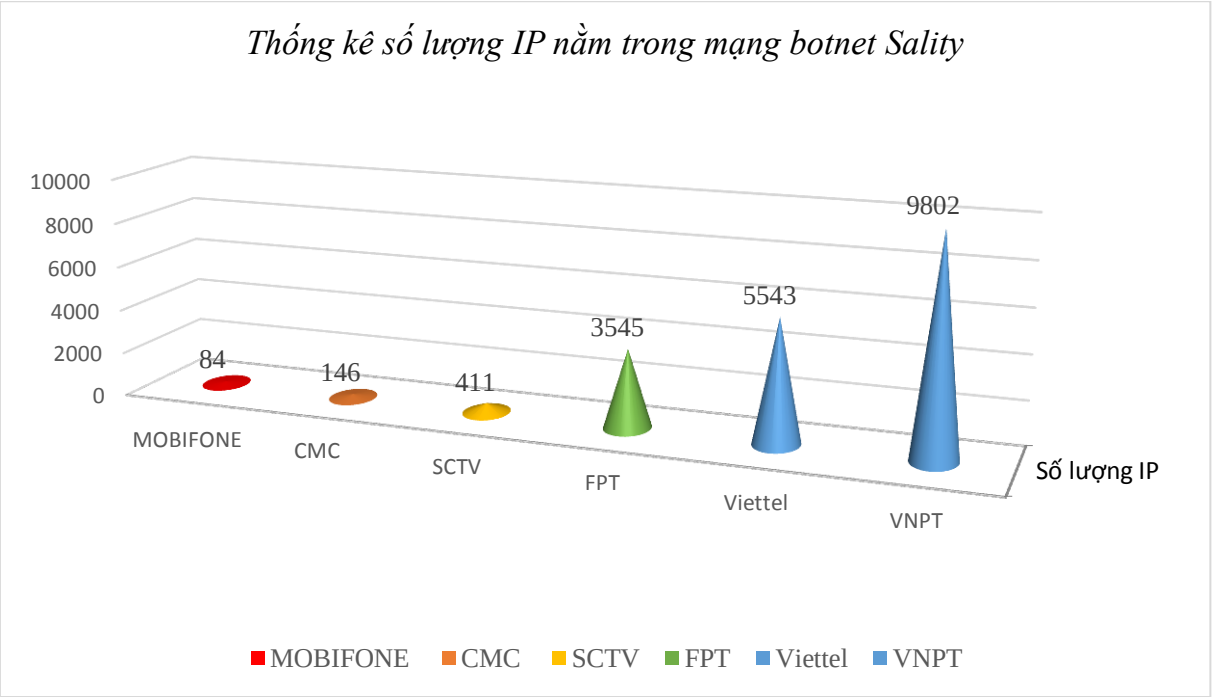
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

5.1. 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.

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



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

TT	Tên miền/IP
1	7r3xtzaao.ru
2	104.244.14.252
3	kukutrustnet777.info
4	mvvyaz09js.ru
5	jwd0ylsp.ru
6	mk.omkol.com
7	g.omlao.com
8	kukutrustnet888.info
9	u.amobisc.com
10	i.onaoy.com

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

Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan, tổ chức, Cục An toàn thông tin khuyến nghị:

- Nhằm tránh việc bị các đối tượng tấn công lợi dụng các trang web để thực hiện các hành vi gây mất an toàn thông tin như đã nêu trong *mục 2*, các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời

phát hiện và cập nhật các điểm yếu, lỗ hổng trên các máy chủ web thuộc cơ quan, tổ chức mình

- 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 3.2* báo cáo này.

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 4.3* 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 5.2* 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;

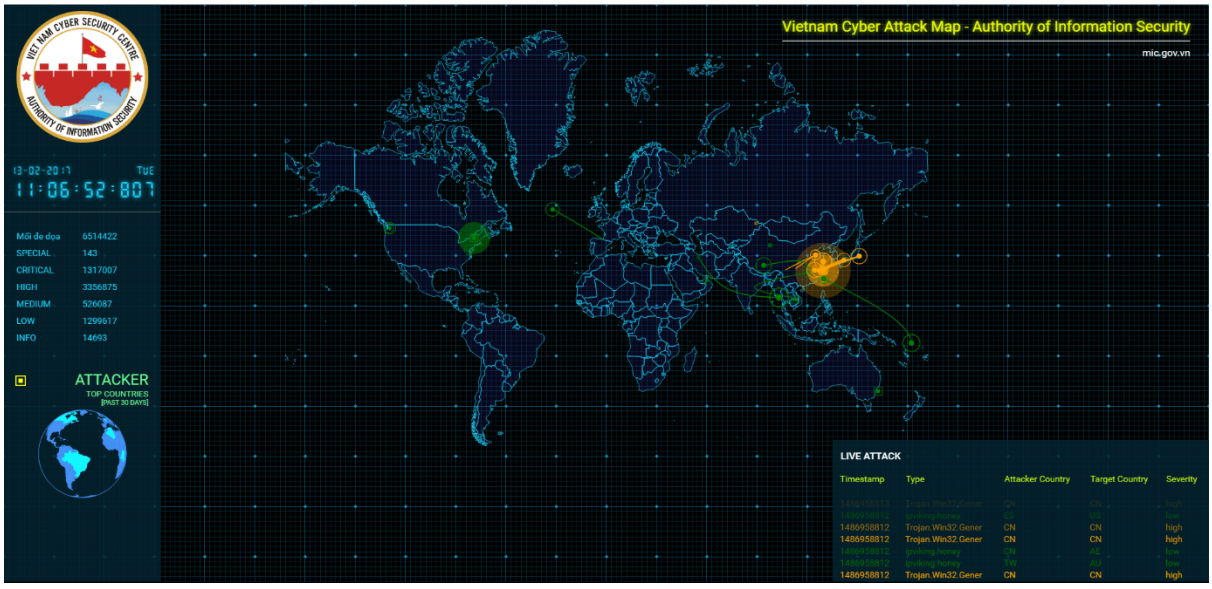
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

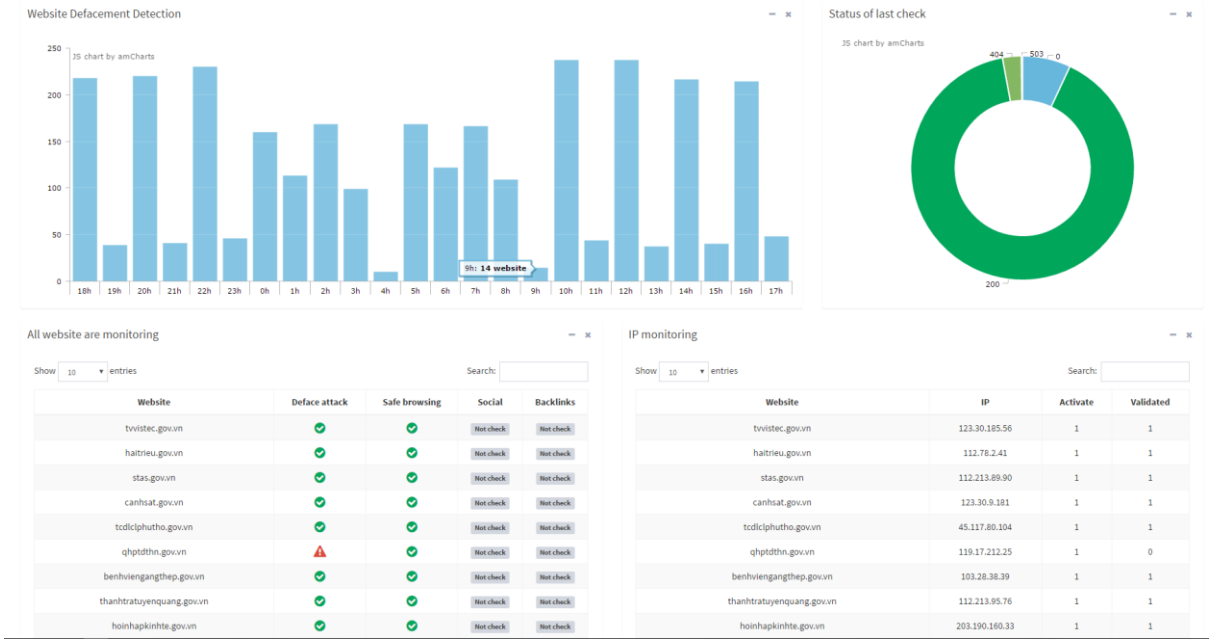
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



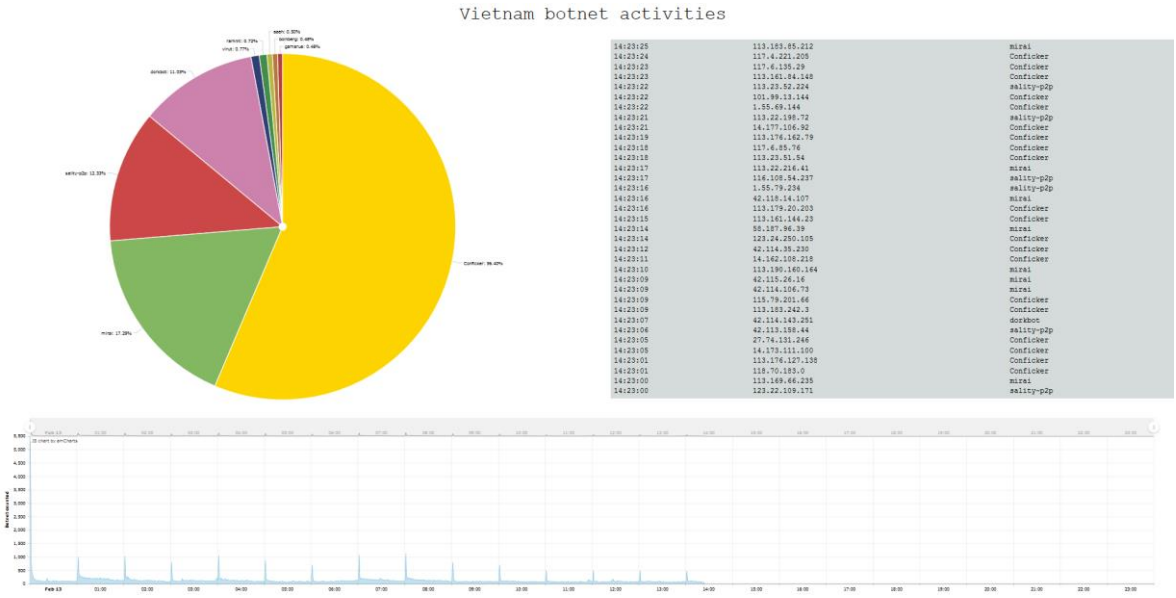
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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