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: **22**/BC-CATTT

Hà Nội, ngày 29 tháng 5 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 21/2018
(từ ngày 21/5/2018 đến ngày 27/5/2018)

BẢNG TỔNG HỢP

1. Ngày 25/5/2018, Thủ tướng Chính phủ đã ký ban hành Chỉ thị số 14/CT-TTg về việc nâng cao năng lực phòng, chống phần mềm độc hại.

2. Mới đây, Thủ tướng Thái Lan, Ông Prayut Chan-ocha đã chủ trì cuộc họp đầu tiên của Ủy ban Quốc gia về vấn đề An toàn Thông tin. Trong cuộc họp, Thủ tướng Prayut đã đề cập đến việc các nhà chức trách bắt buộc phải đẩy mạnh việc thực thi đạo luật Bảo vệ dữ liệu

3. Hơn 500,000 thiết bị định tuyến (router) và thiết bị lưu trữ (storage) ở nhiều quốc gia trong đó có Việt Nam bị lây nhiễm bởi một loại mã độc botnet mới có tên là VPNFilter.

1. Điểm tin đáng chú ý

1.1. Ngày 25/5/2018, Thủ tướng Chính phủ đã ký ban hành Chỉ thị số 14/CT-TTg về việc nâng cao năng lực phòng, chống phần mềm độc hại. Nội dung Chỉ thị nêu rõ, trong xu hướng của cuộc cách mạng công nghiệp lần thứ tư, sẽ ngày càng có nhiều thiết bị thông minh kết nối mạng. Những thiết bị này khi bị lây nhiễm các loại phần mềm độc hại (gọi tắt là mã độc) sẽ gây mất an toàn thông tin, tiềm ẩn nguy cơ khó lường. Trong năm 2016 và năm 2017, một số cuộc tấn công mạng sử dụng mã độc làm thiệt hại nghiêm trọng cho nhiều cơ quan, tổ chức ở Việt Nam.

Các cơ quan, tổ chức ở Việt Nam đã và đang thực hiện nhiều giải pháp khác nhau trong việc xử lý mã độc. Tuy nhiên, hiệu quả đạt được chưa cao, khả năng chia sẻ thông tin thấp. Thực trạng lây nhiễm mã độc tại Việt Nam hiện nay rất đáng báo động. Đặc biệt, nhiều trường hợp tấn công mã độc mà cơ quan chức năng không phản ứng kịp thời để phát hiện, phân tích và gỡ bỏ.

Thủ tướng Chính phủ đã có những chỉ thị cụ thể đối với các cơ quan, tổ chức thực hiện các biện pháp để nâng cao năng lực phòng, chống phần mềm độc hại, cải thiện mức độ tin cậy của quốc gia trong hoạt động giao dịch điện tử, thúc đẩy phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh của đất nước.

1.2. Mới đây, Thủ tướng Thái Lan, Ông Prayut Chan-ocha đã chủ trì cuộc họp đầu tiên của Ủy ban Quốc gia về vấn đề An toàn Thông tin. Trong cuộc họp, Thủ tướng Prayut đã đề cập đến việc các nhà chức trách bắt buộc phải đẩy mạnh việc thực thi đạo luật Bảo vệ dữ liệu vì điều này sẽ bảo đảm tính riêng tư về dữ liệu của Thái Lan phù hợp với những tiêu chuẩn quốc tế và giải quyết những lo ngại của người dùng internet. Mục tiêu đặt ra là làm cho Thái Lan trở thành một trong 20 quốc gia đứng đầu về tính sẵn sàng trong công tác An toàn Thông tin.

Bốn điểm chính được đưa ra trong cuộc họp là:

(1) Tầm quan trọng của việc có một khuôn khổ chính sách quốc gia để bảo vệ, phòng, chống và giảm thiểu các nguy cơ mất an toàn thông tin.

(2) Xác định cơ sở hạ tầng Thông tin quan trọng trong các lĩnh vực: Viễn thông; An ninh quốc gia và dịch vụ cộng đồng; Giao thông Vận tải; Tài chính và Ngân hàng; Năng lượng và Dịch vụ xã hội; Sức khoẻ cộng đồng. Đưa ra những hướng dẫn và thủ tục vận hành tiêu chuẩn khi xử lý các tình huống khẩn cấp liên quan đến an toàn thôn tin.

(3) Phát triển nhân sự an toàn thông tin.

(4) Thành lập của Cơ quan An toàn Thông tin, cơ quan chịu trách nhiệm phối hợp và phản ứng với các vấn đề an toàn thông tin. Cơ quan này sẽ bảo đảm an toàn thông tin quốc gia Thái Lan tương xứng với các tiêu chuẩn quốc tế.

1.3. Hơn 500,000 thiết bị định tuyến (router) và thiết bị lưu trữ (storage) ở nhiều quốc gia trong đó có Việt Nam bị lây nhiễm bởi một loại mã độc mới có tên là VPNFilter. Theo nghiên cứu từ nhóm Cisco Talos thuộc hãng Cisco, mạng botnet này không tấn công vào lỗi zero-days trên thiết bị mà khai thác dựa trên những lỗ hổng phổ biến, đã được công bố hoặc sử dụng thông tin xác thực mặc định để chiếm quyền điều khiển. Thiết bị home routers và thiết bị lưu trữ có kết nối internet của các hãng Linksys, MikroTik, Netgear và TP-Link là đối tượng có tiềm ẩn nguy cơ bị tấn công cao.

VPNFilter là loại mã độc tinh vi, có nhiều giai đoạn tấn công, có thể đánh cắp thông tin đăng nhập website và theo dõi các hệ thống điều khiển công

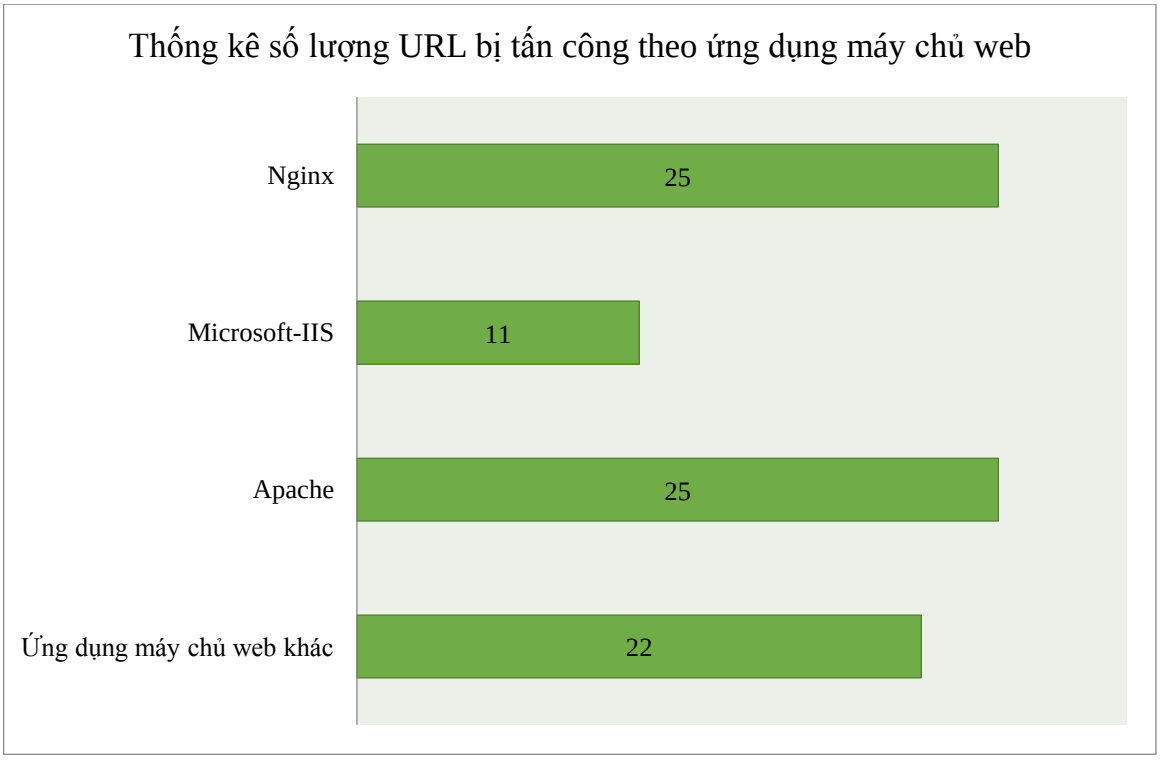
nghiệp SCADA, chẳng hạn như hệ thống lưới điện và cơ sở hạ tầng công nghiệp. Không giống như hầu hết các loại mã độc khác, khi đã lây nhiễm thành công VPNFilter sẽ tiến hành khởi động lại thiết bị, từ đó tạo được kết nối lâu dài và cài đặt mã độc phục vụ cho giai đoạn hai. Đặc trưng của mạng botnet sử dụng mã độc VPNFilter là thư mục có đường dẫn /var/run/vpnfilterw được tạo ra trong quá trình cài đặt.

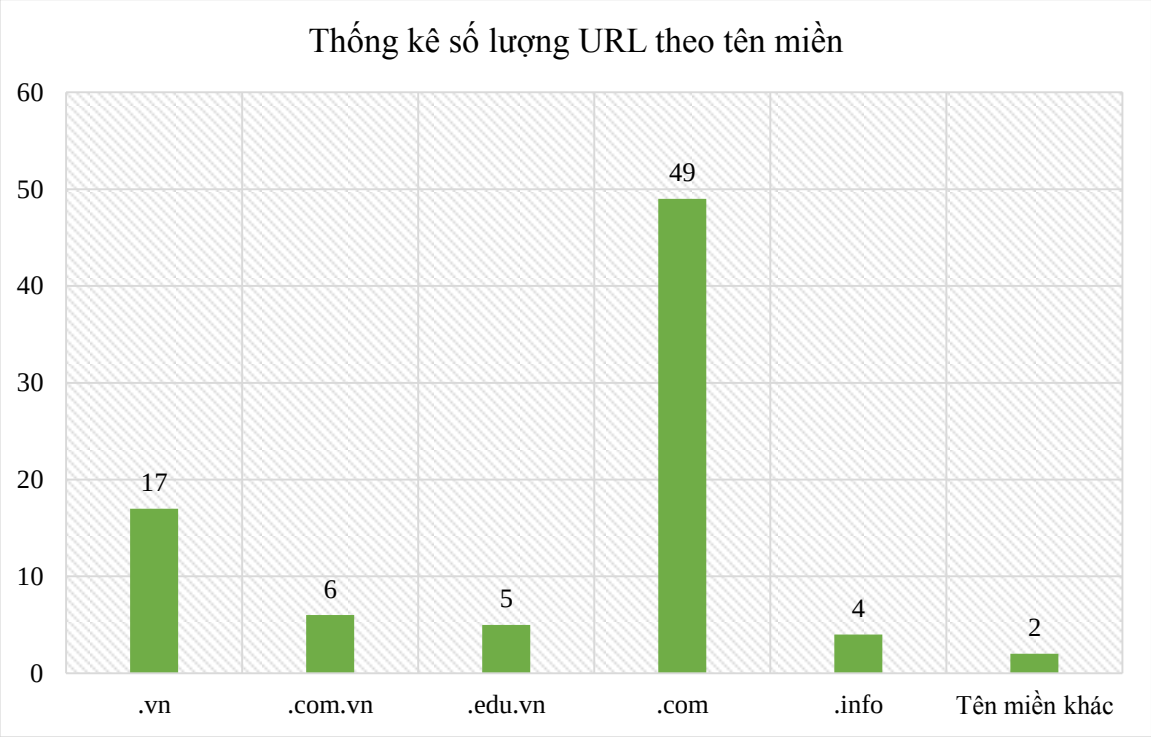
Khuyến nghị từ các chuyên gia ATTT trong trường hợp nghi ngờ thiết bị đã bị lây nhiễm bởi mạng mã độc này, người dùng nên thực hiện cài đặt lại thiết bị về mặc định để xóa mã độc và cập nhật firmware càng sớm càng tốt.

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 Việt Nam (bao gồm cả những trang web sử dụng dịch vụ máy chủ nước ngoài) 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…).

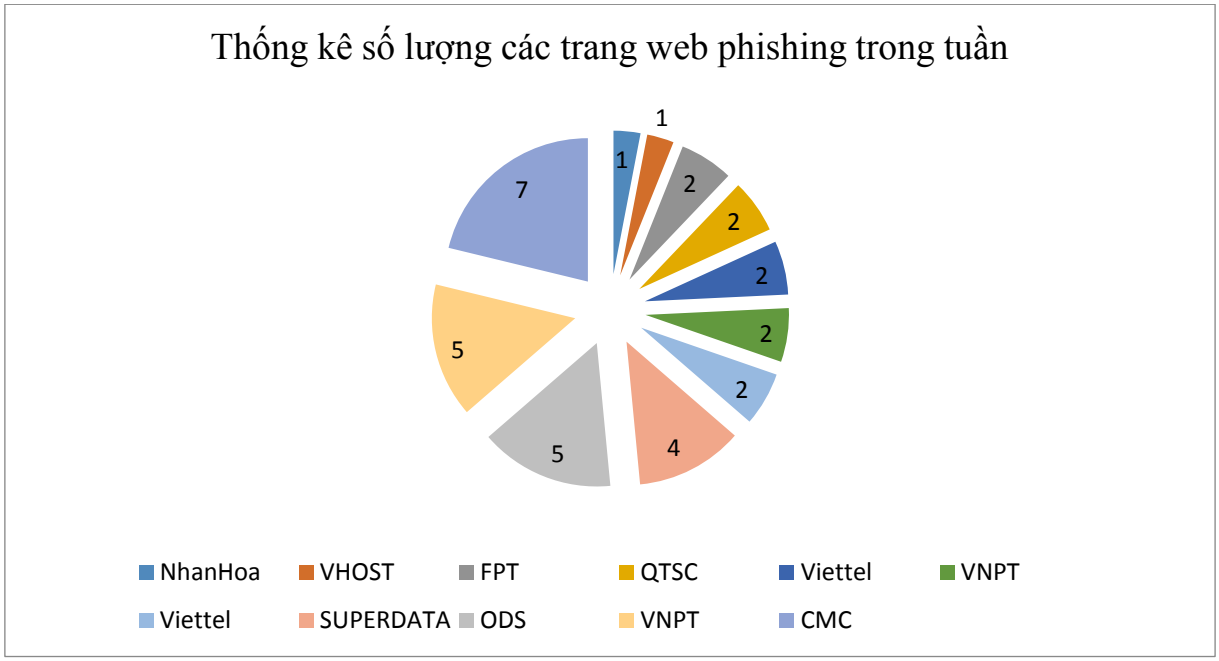
Trong tuần, Cục ATTT ghi nhận có ít nhất 83 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



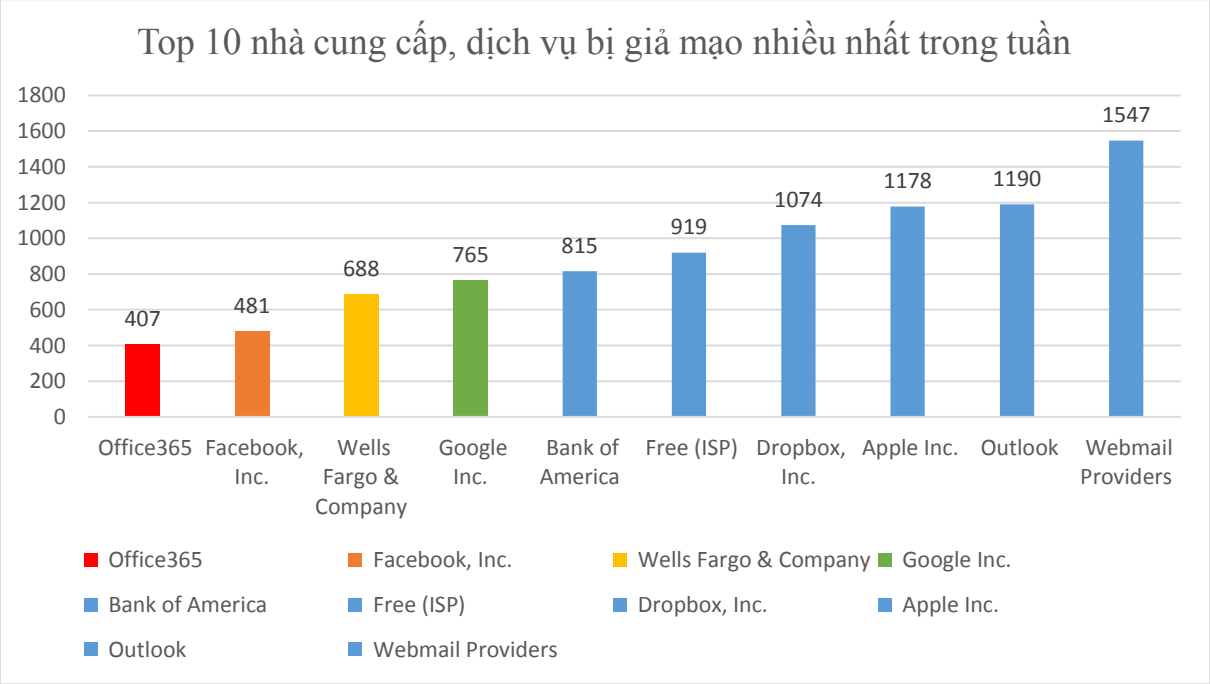


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **33** 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 công bố ít nhất 270 lỗ hổng, trong đó có ít nhất 27 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 13 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 **07** 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 31 lỗ hổng trên nhiều sản phẩm của Adobe; Nhóm 09 lỗ hổng trên một số thành phần Joomla ..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	Adobe	CVE-2018-4918 CVE-2018-4917 CVE-2018-4941 CVE-2018-4938 CVE-2018-4942 …	Nhóm 31 lỗ hổng trên nhiều sản phẩm của Adobe (Acrobat and Reader, Flash player, Cold Fusion,…) cho phép đối tượng tấn công thực hiện chèn và thực thi	Đã có thông tin xác nhận và bản vá, nhiều lỗ hổng đã

			mã lệnh, tấn công leo thang hoặc đánh cắp thông tin.	có mã khai thác
2	Dlink	CVE-2018-8898	Lỗ hổng trên cơ chế xác thực trên dòng thiết bị Router DSL-3782 của Dlink cho phép đối tượng tấn công đọc và thay đổi mật khẩu cũng như cấu hình từ xa khi quản trị viên đăng nhập qua web.	Đã có mã khai thác
3	Foxit	CVE-2018-5679 CVE-2018-5676 CVE-2018-7406 CVE-2018-7407 CVE-2018-5674 …	Nhóm 09 lỗ hổng trên phần mềm đọc file PDF Foxit Reader cho phép đối tượng thực thi mã lệnh khi người dùng mở sử dụng một trang web hoặc tập tin PDF độc hại.	Đã có thông tin xác nhận và bản vá
4	Huawei	CVE-2018-7903 CVE-2018-7904 CVE-2018-7942 CVE-2018-17158 CVE-2018-17315 …	Nhóm 6 lỗ hổng trên một số sản phẩm điện thoại thông minh, thiết bị định tuyến và ứng dụng quản lý iBMC của Huawei cho phép đối tượng tấn công lây nhiễm JSON để thay đổi mật khẩu hệ thống, cũng như đánh cắp thông tin và chiếm quyền quản trị.	Đã có thông tin xác nhận
5	Microsoft	CVE-2018-8176 CVE-2018-8142	Nhóm 02 lỗ hổng trên Microsoft PowerPoint và Windows cho phép đối tượng tấn công thực thi mã lệnh và vượt qua các tính năng bảo mật của Windows để thực hiện những hành vi trái phép trên hệ thống	Đã có thông tin xác nhận
6	VMware	CVE-2018-6962 CVE-2018-6963	02 lỗ hổng trên VMware Fusion (trước phiên bản 10.1.2) và VMware Workstation (trước pheien bản 14.1.2) cho phép đối tượng thực hiện tấn công leo thang đặc quyền và tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
7	Joomla	CVE-2018-6378 CVE-2018-11321	Nhóm 09 lỗ hổng trên một số thành phần (Joomla!	Đã có mã khai thác

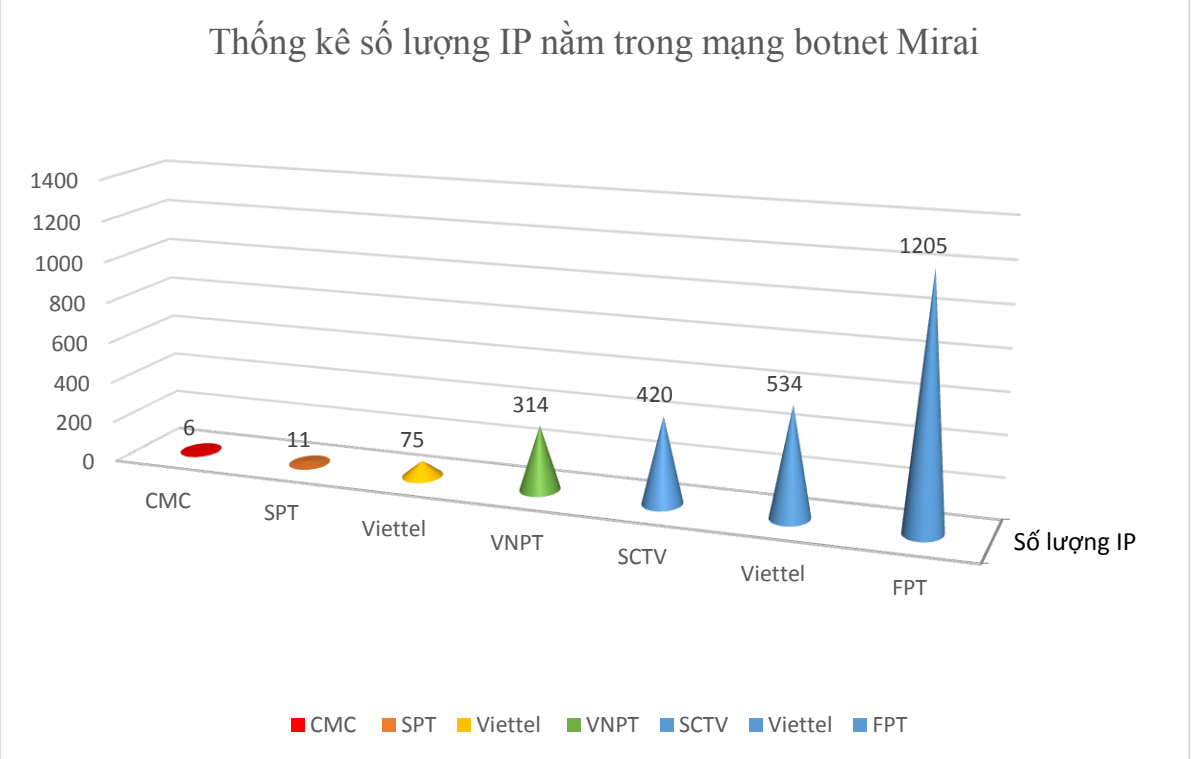
		CVE-2018-11327 CVE-2018-11326 ….	Core,) của phần mềm quản trị nội dung Joomla cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau gồm: tấn công XSS, chèn và thực thi mã lệnh trên hệ thống trong phạm vi quyền của ứng dụng; ăn trộm thông tin xác thực người dùng. Quản trị viên cần cập nhật lên phiên bản mới (3.8.8).	Đã có xác nhận và bản vá.

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

5.1. 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.



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

TT	Tên miền/IP
1	p2xtz27i32.ru
2	104.244.14.252
3	st40pwch.ru
4	ei3rvgfk.ru
5	kukutrustnet777.info
6	b1pzjdesv.ru
7	and31.blllaaaaaazblaaa3.com
8	kukutrustnet888.info
9	ye5cvvufx.ru
10	g.omlao.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;
- Cục KSTTHC, Văn phòng Chính phủ;
- 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;

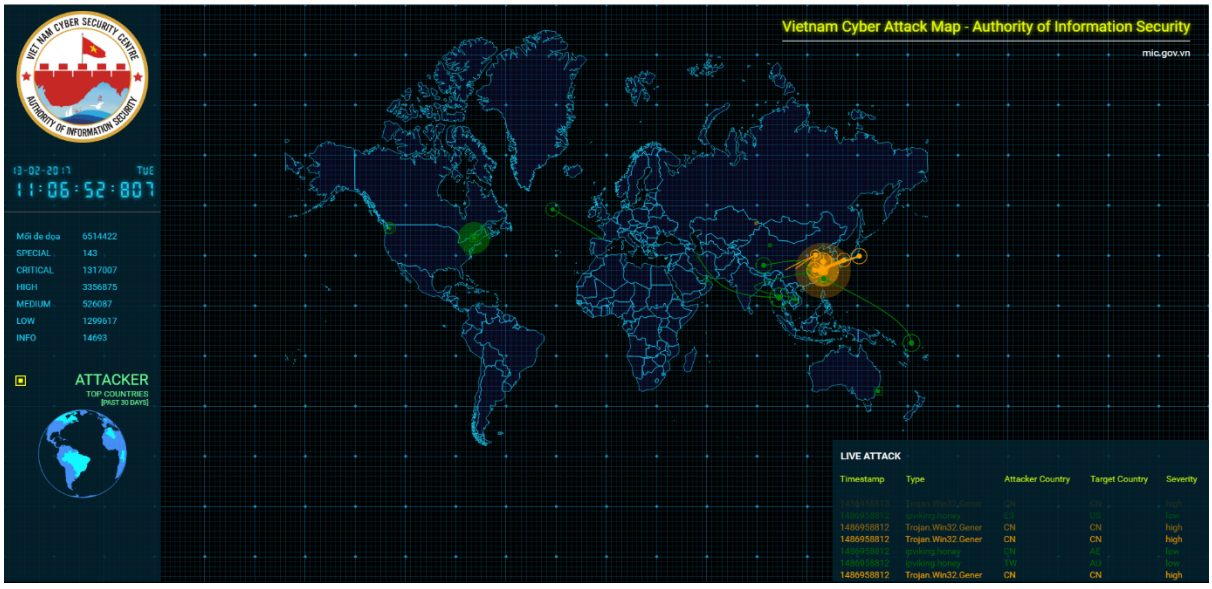
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

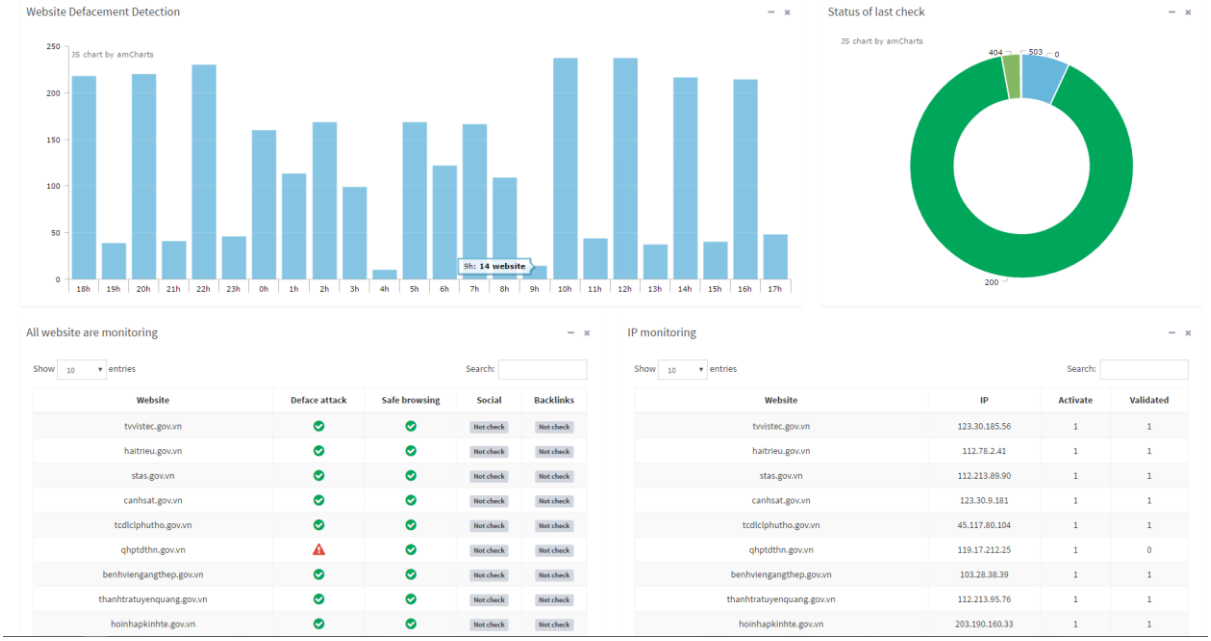
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



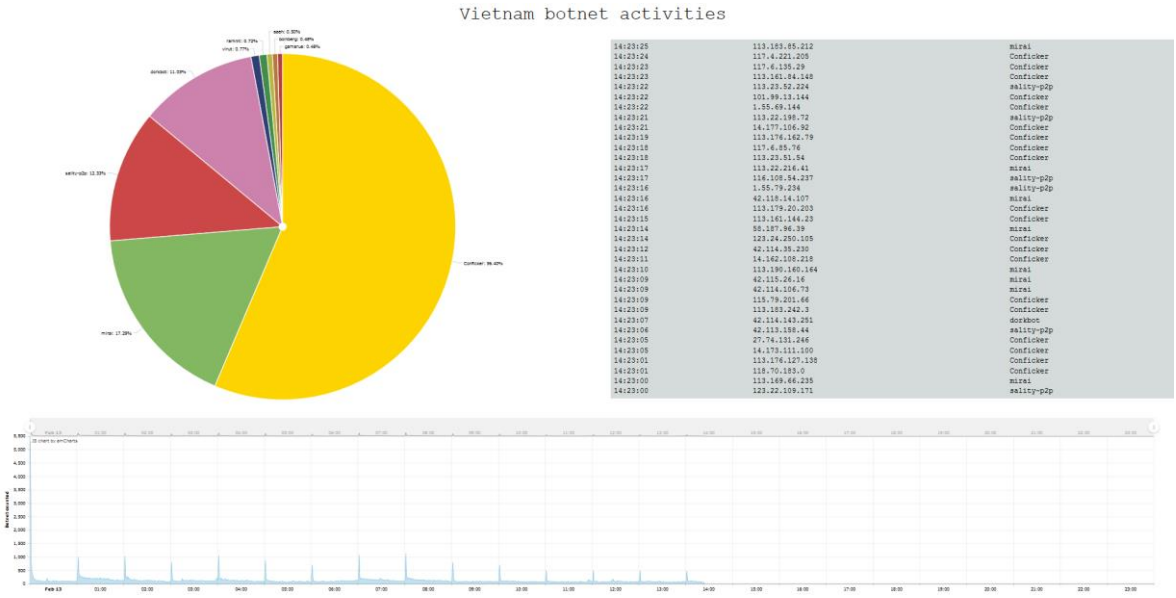
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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