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: **19**/BC-CATTT

Hà Nội, ngày 08 tháng 5 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 18/2018
(từ ngày 30/4/2018 đến ngày 06/5/2018)

BẢNG TỔNG HỢP

1. Chính quyền thành phố Dubai đã công bố thông tin về website hỗ trợ công tác bảo đảm an toàn thông tin. Nền tảng trực tuyến này được thiết lập để nhận báo cáo từ các cá nhân, doanh nghiệp và cả các tổ chức thuộc chính quyền.

2. Chính quyền thành phố Luân Đôn đã phát động một chiến dịch có tên là Cyber Griffin với mục tiêu chia sẻ thông tin, tin tức và các khuyến nghị về việc tăng cường khả năng bảo đảm an toàn thông tin cho các doanh nghiệp tại Thành phố.

3. Một nhóm các nhà nghiên cứu bảo mật đã phát hiện ra 08 lỗ hổng mới cùng lớp với lỗ hổng "Spectre" trong CPU của Intel, được gọi là Spectre-NG. Lỗi CPU mới được phát hiện này bắt nguồn từ vấn đề trong thiết kế tương tự lỗi Spectre ban đầu và có cùng kịch bản tấn công, đã được Cục An toàn thông tin cảnh báo trong Công văn số 03/CATTT-TTTV ngày 04/01/2018

1. Điểm tin đáng chú ý

1.1. Chính quyền thành phố Dubai đã công bố thông tin về website hỗ trợ công tác bảo đảm an toàn thông tin. Nền tảng trực tuyến này được thiết lập để nhận báo cáo từ các cá nhân, doanh nghiệp và cả các tổ chức thuộc chính quyền. Website cho phép người dùng Internet gửi thông tin qua 07 bước đơn giản để báo cáo về các vấn đề liên quan đến thư điện tử giả mạo, mạng xã hội, tấn công mạng .v.v…

Chính quyền Dubai nhấn mạnh sự quan tâm của mình trong việc cung cấp các dịch vụ hiện đại phù hợp với định hướng chỉ đạo của UAE và những kế hoạch tương lai trong lĩnh vực dịch vụ thông minh như là một phần của Kế hoạch Dubai 2021.

1.2. Chính quyền thành phố Luân Đôn đã phát động một chiến dịch có tên là Cyber Griffin với mục tiêu chia sẻ thông tin, tin tức và các khuyến nghị về việc tăng cường khả năng bảo đảm an toàn thông tin cho các doanh nghiệp tại Thành phố này.

Theo đó, các doanh nghiệp sẽ nhận được các báo cáo tóm tắt, cập nhật về các nguy cơ mất an toàn thông tin, đồng thời được cung cấp một môi trường để các nhà điều hành, quản lý doanh nghiệp có thể kết nối và chia sẻ kinh nghiệm với nhau. Cyber Griffin cũng cung cấp các bài diễn tập về phản ứng sự cố với 03 trình độ khác nhau, từ cơ bản tới chuyên gia, thực hiện trong thời gian thực (realtime) cùng với quan sát của lãnh đạo doanh nghiệp. Bên cạnh đó, chiến dịch sẽ có các nhóm chuyên gia về an toàn thông tin giúp tư vấn cho thành viên của cộng đồng doanh nghiệp.

1.3. Một nhóm các nhà nghiên cứu bảo mật đã phát hiện ra 08 lỗ hổng mới cùng lớp với lỗ hổng "Spectre" trong CPU của Intel, được gọi là Spectre-NG. Lỗi CPU mới được phát hiện này bắt nguồn từ vấn đề trong thiết kế tương tự lỗi Spectre ban đầu và có cùng kịch bản tấn công, đã được Cục An toàn thông tin cảnh báo trong Công văn số 03/CATTT-TTTV ngày 04/01/2018, tuy nhiên, nó được đánh giá còn nguy hiểm hơn lỗ hổng Spectre ban đầu.

Cụ thể, một trong các lỗi Spectre-NG cho phép kẻ tấn công đơn giản hóa kịch bản tấn công vượt qua ranh giới hệ thống bằng cách khai thác một máy ảo và từ đó tấn công vào hệ thống mục tiêu, ví dụ như các máy ảo nằm trên cùng hệ thống điện toán đám mây (cloud). Ngoài ra, nó cũng có thể sử dụng để tấn công các máy ảo khác nằm trên cùng máy chủ bị khai thác. Mật khẩu và khóa bí mật được sử dụng để truyền dữ liệu an toàn trên hệ thống cloud là mục tiêu tấn công và có rủi ro cao. Thậm chí công nghệ Software Guard Extensions (SGX) của Intel được thiết kế để bảo vệ dữ liệu nhạy cảm trên cloud cũng không an toàn trước kịch bản tấn công Spectre.

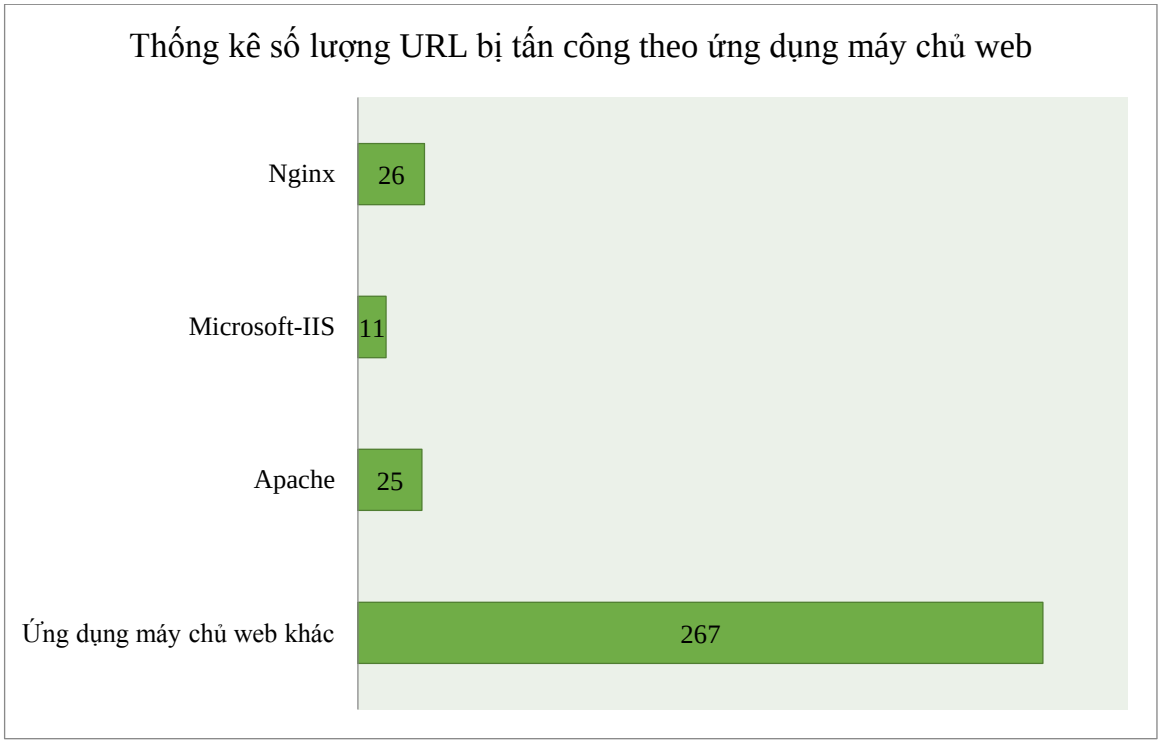
Mặc dù chưa có thông tin xác nhận chính thức, nhưng đã có thông tin hãng sản xuất chip Intel đang lên kế hoạch phát hành 2 bản vá cho các lỗ hổng này, một bản vào tháng 5 và một bản vào tháng 8. Microsoft cũng đang chuẩn bị phát hành bản vá lỗi CPU dành cho Windows trong tháng tới.

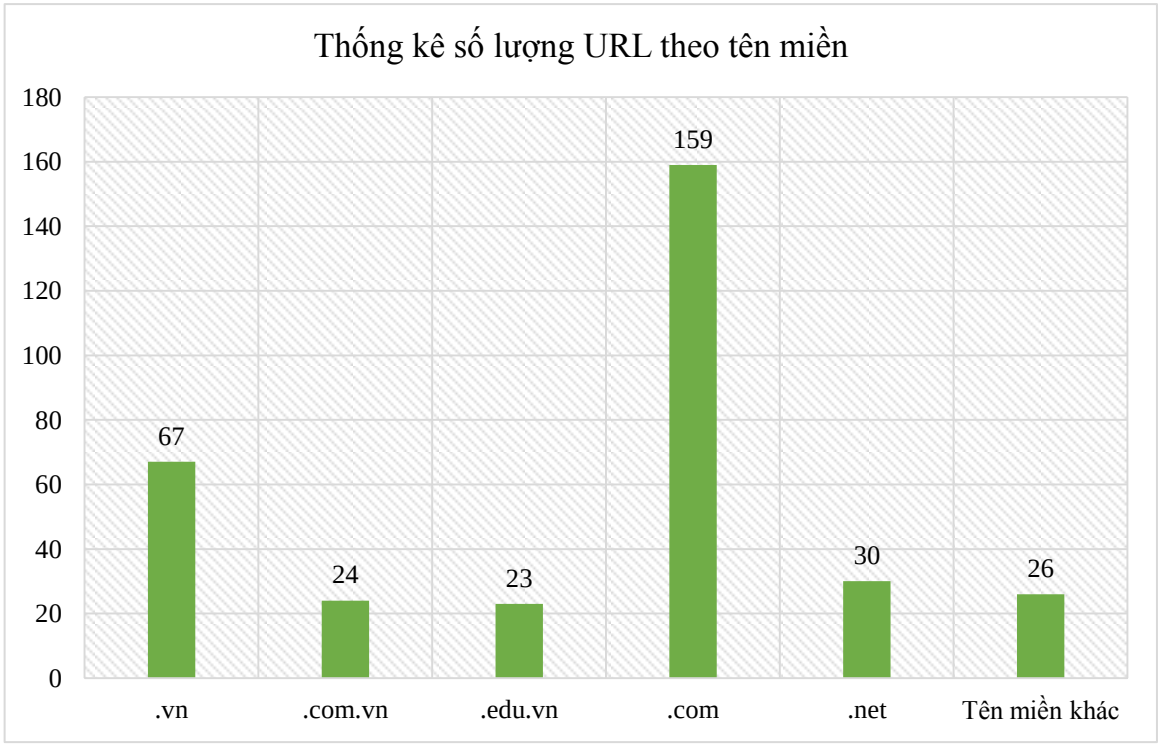
2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

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…).

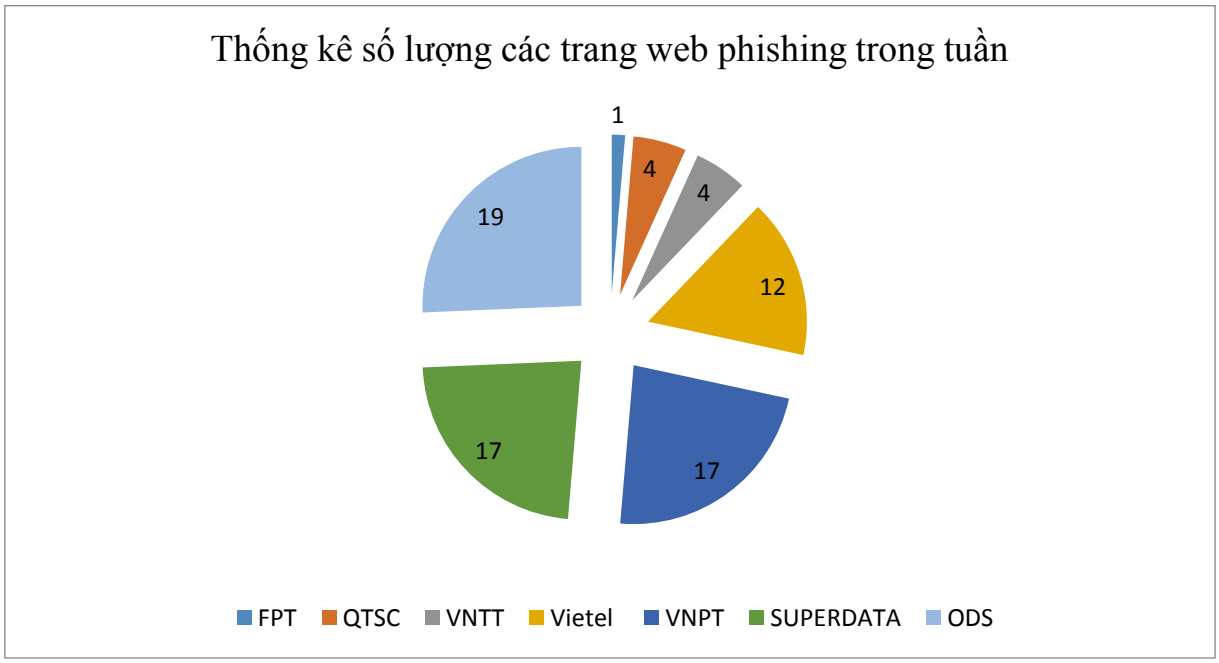
Trong tuần, Cục ATTT ghi nhận có ít nhất 329 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



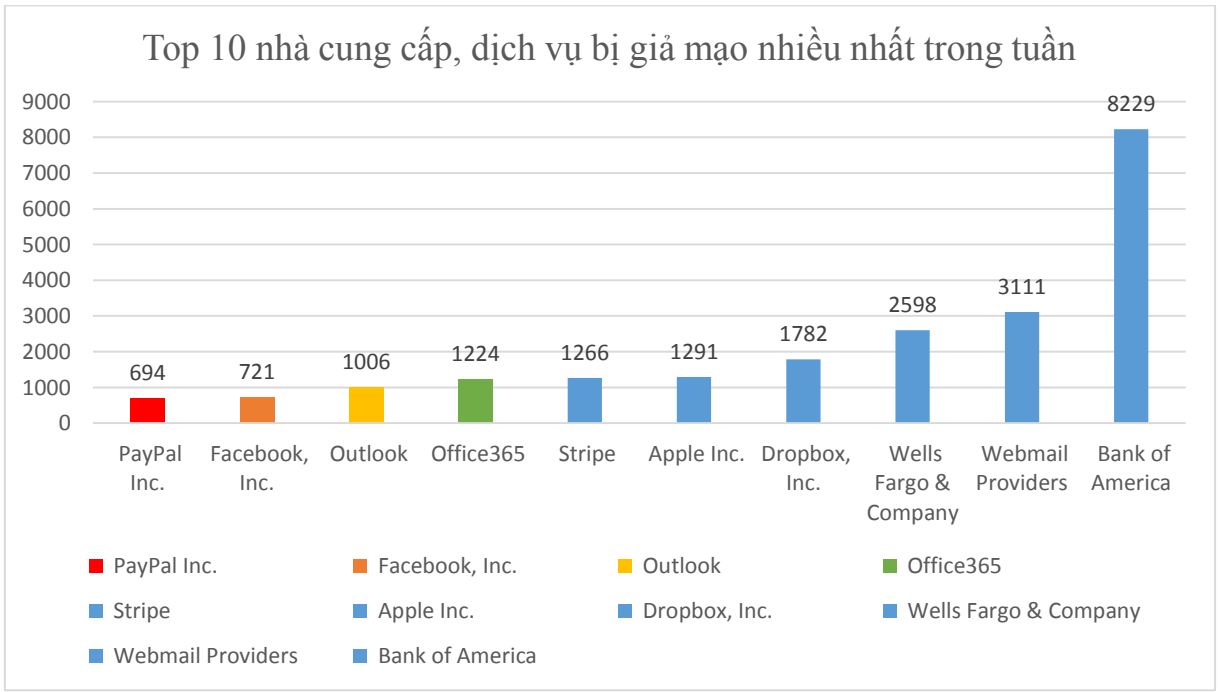


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **74** 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 193 lỗ hổng, trong đó có ít nhất 23 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 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 **05** 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 19 lỗ hổng trên một số sản phẩm, dịch vụ của Cisco; Nhóm 8 lỗ hổng trên các dòng sản phẩm của D-Link..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	Cisco	CVE-2018-0245 CVE-2018-0234 CVE-2018-0249 CVE-2018-0253 CVE-2018-0285 …	Nhóm 19 lỗ hổng trên một số sản phẩm, dịch vụ của Cisco (Wireless LAN Controller, Aironet Access point, Fire Power System Software, Meeting Server, Prime File Upload…) cho phép đối tượng thực hiện nhiều hình thức tấn công như tấn công từ chối dịch vụ, tấn công khai thác các điểm yếu ứng dụng web, đánh cắp thông tin hệ thống, chèn và thực thi mã lệnh, đưa tập tin độc hại, hay chiếm quyền quản trị đối với các thiết bị phát wifi Airnonet Acess Point.	Đã có thông tin xác nhận và bản vá
2	D-link	CVE-2018-10641 CVE-2018-10750 CVE-2017-17020 …	Nhóm 8 lỗ hổng trên các dòng sản phẩm của D-Link cho phép đối tượng thực hiện nhiều hình thức tấn công như: thực thi mã lệnh (trên DCS-5009 và DSL-3782 EU), đánh cắp và thay đổi mật khẩu (trên dòng DIR 601 A1 1.02NA) …	Chưa có thông tin xác nhận và bản vá

3	Dasan GPON	CVE-2018-10561 CVE-2018-10562	02 lỗ hổng trên các thiết bị home router GPON cho phép đối tượng tấn công vượt qua cơ chế xác thực, chèn và thực thi mã lệnh để kiểm soát thiết bị. Việt Nam có ít nhất 152,617 thiết bị đang công khai trên Internet. Nhiều thiết bị home router của các hãng mạng hỗ trợ GPON như Tplink, Netgear, Asus, Linksys, Dlink đều có khả năng bị ảnh hưởng	Đã có mã khai thác Chưa có thông tin bản vá
4	Wordpress	CVE-2018-10752 CVE-2018-10371 CVE-2018-10504	3 lỗ hổng trên các plugin của Wordpress cho phép đối tượng thực hiện tấn công XSS, chèn và thực thi mã HTML/script và lây nhiễm mã độc qua tệp CSV (Web Dorado.) Lỗ hổng CVE-2018-10371 và CVE-2018-10504 đã có mã khai thác.	Đã có mã khai thác Chưa có thông tin xác nhận và bản vá
5	TP-Link	CVE-2018-10168 CVE-2018-10167 CVE-2018-10166 CVE-2018-10165 CVE-2018-10164	Nhóm 05 lỗ hổng trên phần mềm quản lý tập trung (EAP Controller và Omada Controller) các thiết bị qua trình duyệt web của TP-Link cho phép đối tượng thực hiện các lệnh của quản trị viên chỉ với đặc quyền của người dùng bình thường cũng như chèn và thực thi mã lệnh, thực hiện hình thức tấn công trên ứng dụng web như XSS, CSRF.	Đã có bản vá

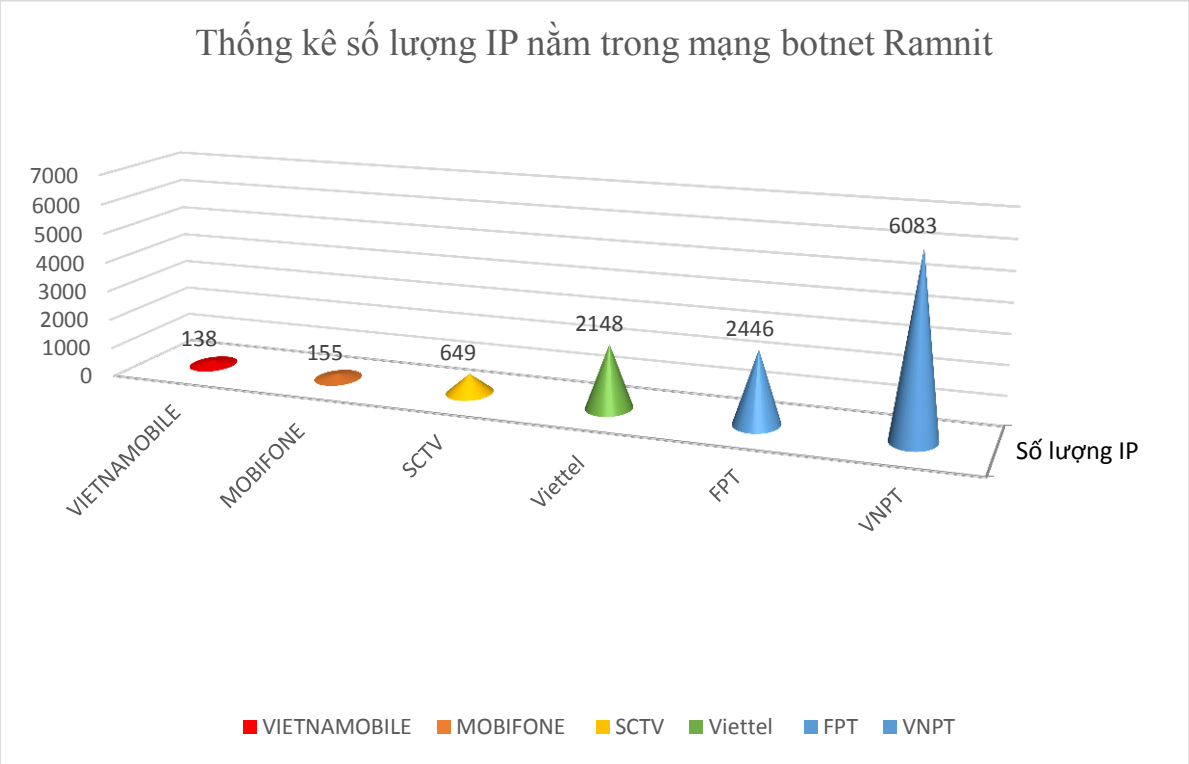
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

5.1. 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.



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

TT	Tên miền/IP
1	3d3bulnt.ru
2	104.244.14.252
3	kukutrustnet777.info
4	qzf163kfd.ru
5	and31.blllaaaaaazblaaa3.com
6	kukutrustnet888.info
7	g.omlao.com
8	u.amobisc.com
9	facialwaxmaxfaxlax3.com
10	init.icloud-analysis.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;

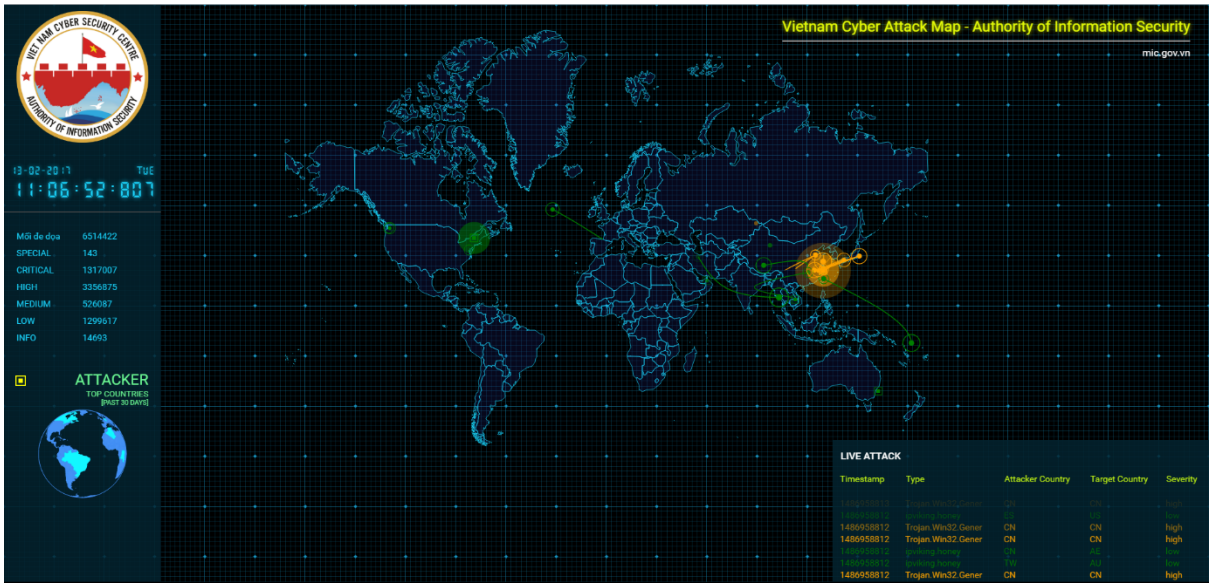
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

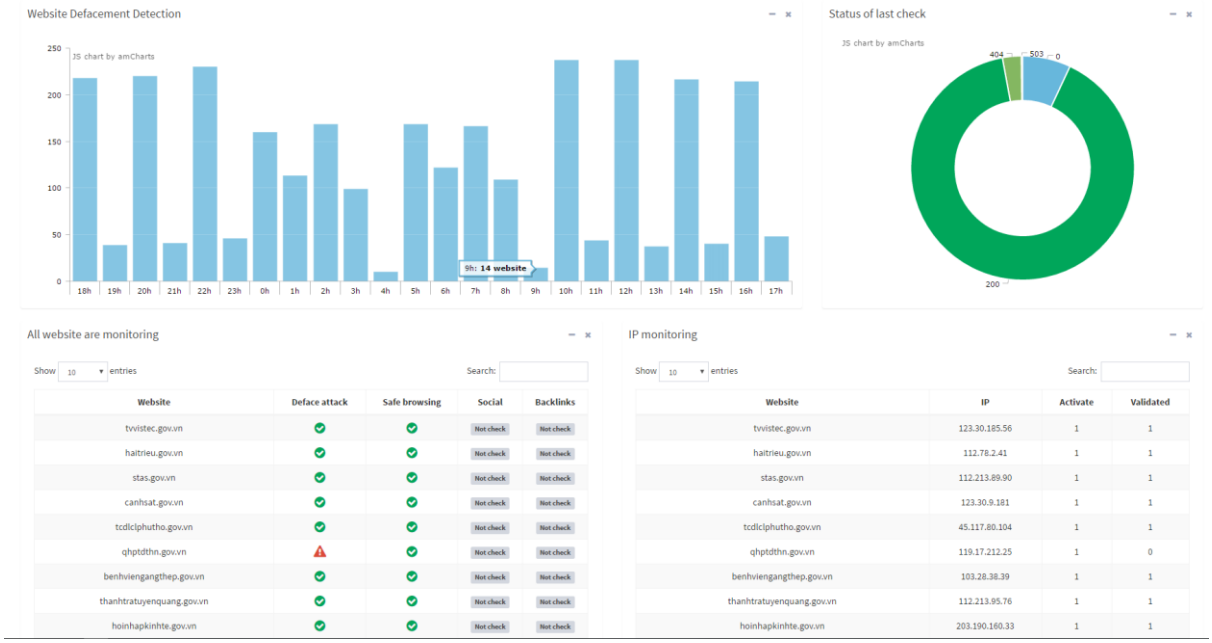
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



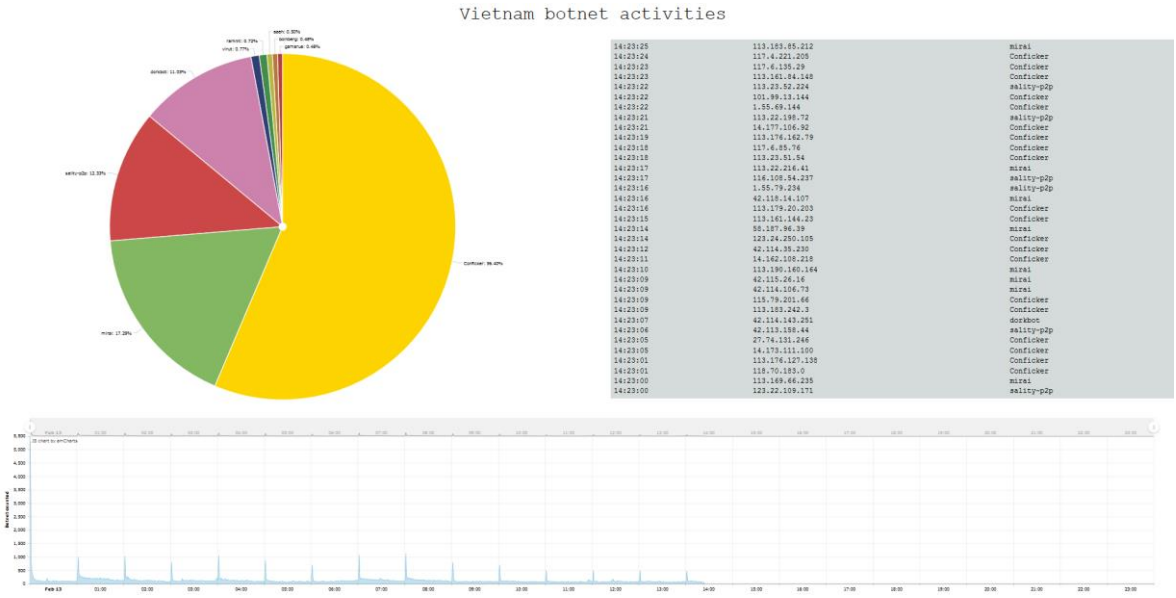
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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