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: **17**/BC-CATTT

Hà Nội, ngày 23 tháng 4 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 16/2018
(từ ngày 16/4/2018 đến ngày 22/4/2018)

BẢNG TỔNG HỢP

1. Hệ thống Tổng đài số điện thoại khẩn cấp 911 của Hoa Kỳ thường xuyên bị tê liệt do các cuộc tấn công mạng. Dù hệ thống là một phần của cơ sở hạ tầng quan trọng quốc gia nhưng do các kết nối mở rộng và hạ tầng công nghệ lạc hậu khiến chúng trở thành mục tiêu ưa thích của những cuộc tấn công từ chối dịch vụ và mã độc mã hóa tống tiền gây ra sự ngừng trệ và thiệt hại lớn cho chính quyền liên bang.

2. Vương quốc Anh dành 15 triệu bảng để khởi động kế hoạch tăng cường năng lực về an toàn thông tin mạng của Khối Thịnh vượng chung.

3. Trong tuần, Cục ATTT đã phát hiện ít nhất 20 trang lừa đảo thu thập thông tin cá nhân của người dùng với hình thức tương tự như chiến dịch tấn công trước đó (Tết Mậu Tuất 2018), có thể trong dịp nghỉ lễ chiến dịch tấn công này lại bùng phát trở lại.

1. Điểm tin đáng chú ý

1.1. Cuộc tấn công vào hệ thống tổng đài số điện thoại khẩn cấp 911 ở thành phố Baltimore đầu tháng là cuộc tấn công mạng lớn thứ 2 tại Hoa Kỳ chỉ trong vài tuần qua. Trước đó không lâu, thành phố Atlanta đã bị tấn công bởi một cuộc tấn công mã độc mã hóa ransomware làm gián đoạn dịch vụ thu phí, internet không dây của sân bay và tắc nghẽn một số dịch vụ khác của thành phố.

Ông Frank Johnson, giám đốc thông tin của Baltimore cho biết tất cả các cuộc gọi tìm kiếm hỗ trợ khẩn cấp đều không thể chuyển tiếp được đến các điều phối viên điện tử, thay vào đó là các nhân viên hỗ trợ phải sử dụng các hoạt động thủ công để xử lý các cuộc gọi.

Trước đó, tiểu bang Tennesse cũng đã hứng chịu cuộc tấn công tương tự vào hệ thống này vào tháng 6 năm 2016, một trong những cuộc tấn công bằng

mã độc ransomware đầu tiên vào tổng đài điện thoại 911. Tin tặc đã làm tê liệt hệ thống thông báo điện tử của các trạm và yêu cầu $2000 tiền chuộc để mở lại hệ thống. Sau khi từ chối trả tiền, nhân viên của Tennesse đã phải xử lý cuộc gọi bằng giấy và bút trong 3 ngày cho đến khi hệ thống được khôi phục lại.

Theo báo cáo của hãng an toàn thông tin SecuLore Solutions, các tổng đài điện thoại 911 đã bị tấn công trực tiếp và gián tiếp trong 42 trên 198 vụ theo danh sách của SecuLore. Có 24 vụ liên quan đến mã độc ransomware và phần lớn các cuộc tấn công khác là tấn công từ chối dịch vụ, khi mà các trạm trên bị tê liệt bởi một lượng lớn các cuộc gọi giả mạo được tự động hóa.

Một vấn đề khác là hệ thống tổng đài điện thoại 911 hiện tại khá lạc hậu, chưa tương thích với một số công nghệ đang giao tiếp và sử dụng ở xã hội như: tin nhắn, ảnh, video,… Điều này là lý do hệ thống cần phải được nâng cấp chuyển dịch sang thế hệ mới, cho phép người gọi gửi dữ liệu qua các nhà cung cấp dịch vụ viễn thông và internet, trong khi vẫn nhận các cuộc gọi bình thường, đồng thời sử dụng các biện pháp an toàn thông tin hiện đại hơn, bao gồm khả năng phát hiện các dấu hiệu tấn công tức thời, tự động dừng hoạt động khi bị xâm nhập trong khi đồng thời chuyển cuộc gọi đến các trạm khác...

1.2. Vương quốc Anh dành 15 triệu bảng để khởi động kế hoạch tăng cường năng lực về an toàn thông tin mạng của Khối Thịnh vượng chung.

Trong tuần, Thủ tướng Anh đã công bố tài trợ 15 triệu bảng để giúp các nước trong Khối thịnh vượng chung phát triển khả năng bảo đảm an toàn thông tin mạng của họ, đây là một phần trong một cam kết liên chính phủ trên nhiều lĩnh vực để chống lại các hiểm họa trực tuyến, giảm thiểu tội phạm mạng và an ninh quốc gia.

Khối Thịnh vượng chung bao gồm 53 quốc gia thuộc Đế quốc Anh trong quá khứ, đây là một tổ chức đại diện cho gần một phần ba dân số thế giới. Các nhà lãnh đạo dự định sẽ ký "Tuyên bố về bảo đảm an toàn thông tin mạng của Khối Thịnh vượng chung" vào cuộc họp của các nguyên thủ trong tuần này. Đây có thể là một bước tiến quan trọng trong việc đẩy lùi tội phạm mạng trên toàn cầu.

1.3. Qua công tác giám sát và theo dõi tình hình, Cục An toàn thông tin đã phát hiện các chiến dịch tấn công lừa đảo vẫn tiếp tục được đối tượng tấn công thực hiện và nhắm vào người sử dụng Internet Việt Nam, đặc biệt là những người dùng qua mạng xã hội.

Những chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các ngân hàng, các cơ sở dịch vụ lớn, đặc biệt là các chương trình trúng thưởng để

thu thập thông tin cá nhân người sử dụng, các tài khoản mạng xã hội, các tài khoản ngân hàng, thẻ tín dụng .v.v…

Cục An toàn thông tin đã phát hiện có ít nhất 20 tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên. Hầu hết các trang web đều sử dụng tên miền được đăng ký gợi mở đến chương trình trúng thưởng, trao giải như:

- http://trangchutraogiai2018.com
- http://vongquayonline24h.com
- http://vongquayonline2018.com
- http://vongquay79.com
- http://triannam2018.com
- http://tranggiainhat2018.com
- http://vongquay2018.com
- http://trangbaomat123.com
- http://trieuphu52.com
- http://traoqua779.com
- http://sukienqua7979.com
- http://thongtingmail.com
- http://sukienvang247.com
- http://quavn2018.com
- http://tingiaithang4.com
- http://sukienfb339.com
- http://sukien59.com
- http://sukien99.com
- http://quathuonghieu123.com
- http://nhangiaivang2018.com

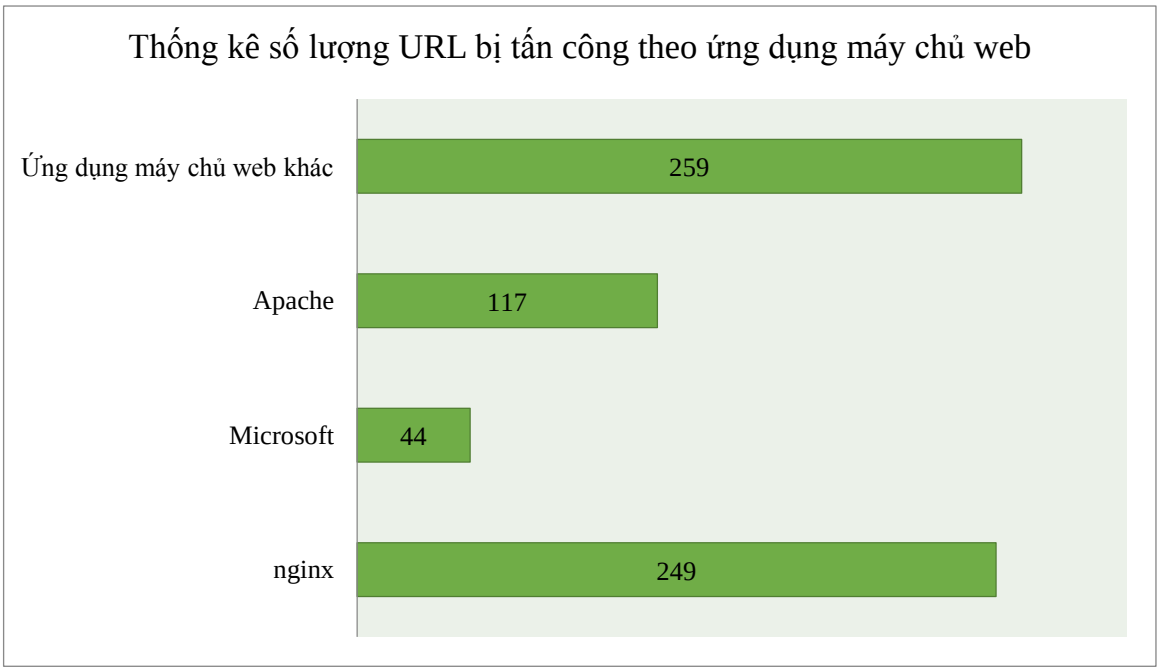
*(Số lượng các trang web lừa đảo rất lớn sẽ được Cục ATTT cập nhật thường xuyên tại **https://khonggianmang.vn/warn/phishing.txt**)*

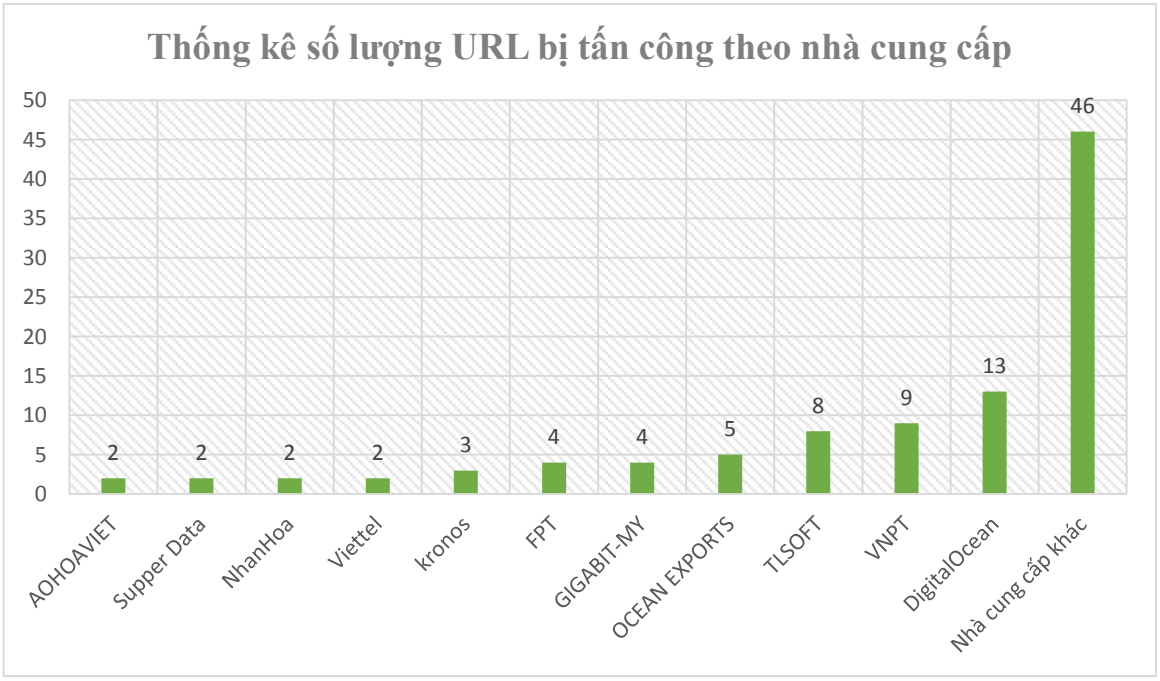
2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

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…).

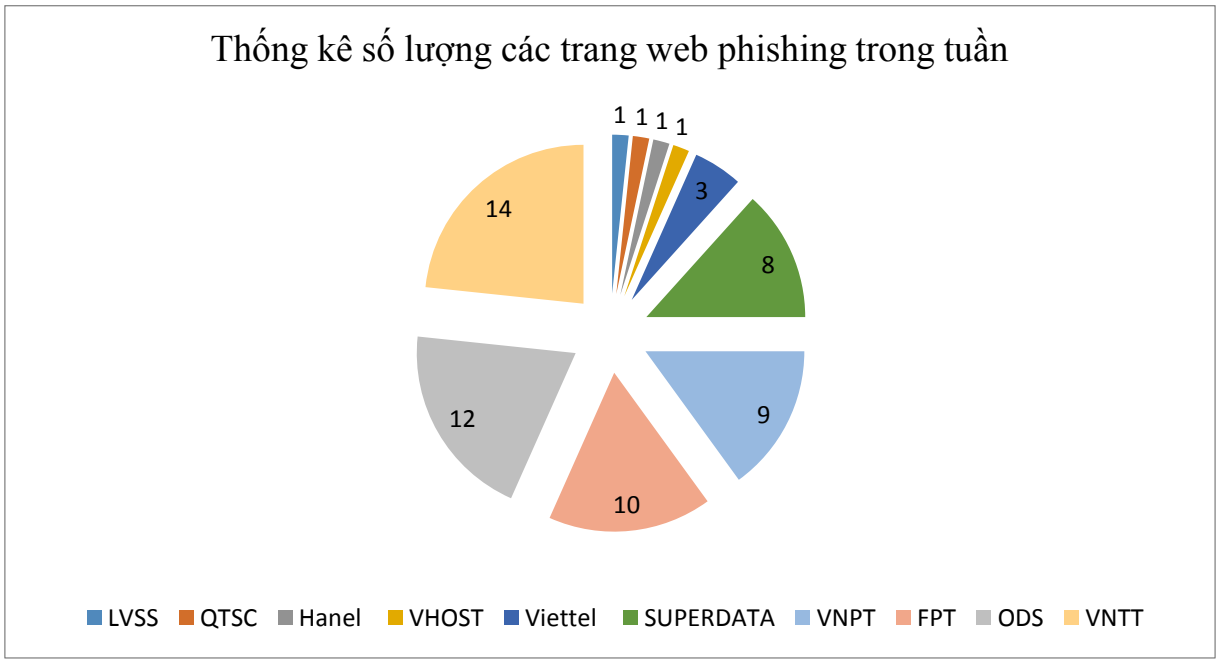
Trong tuần, Cục ATTT ghi nhận có ít nhất 669 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



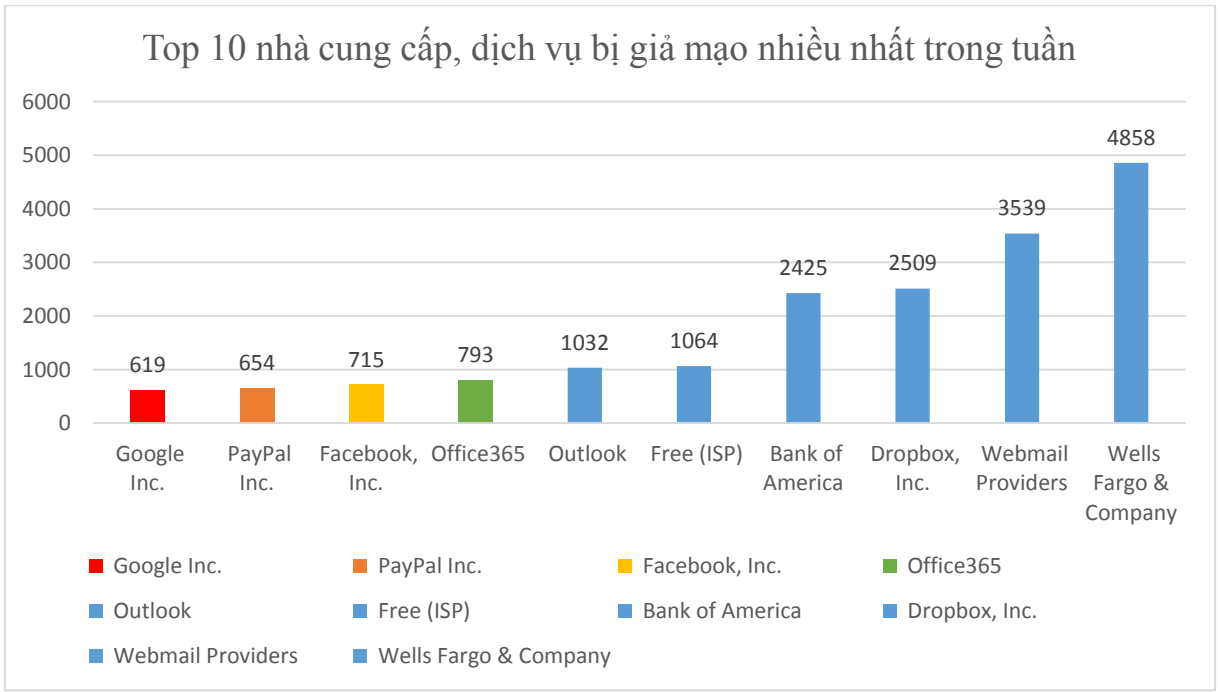


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất 60 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 732 lỗ hổng, trong đó có ít nhất 18 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 10 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 **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 149 lỗ hổng trên các sản phẩm của Oracle; Nhóm 28 lỗ hổng trên một số sản phẩm của Cisco..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	CMS Made Simple	CVE-2018-10081 CVE-2018-1000158	Nhóm 02 lỗ hổng trên phần mềm quản lý mã nguồn mở CMS Made Simple cho phép đối tượng thiếp lập lại mật khẩu admin.	Chưa có thông tin bản vá
2	Asus router	CVE-2018-8826	Lỗ hổng trên một số dòng thiết bị router của Asus (ASUS RT-AC51U, RT-AC58U, RT-AC66U,RT-AC1750,RT-ACRH13, RT-N12 D1, RT-AC52U B1, RT-AC1200, RT-N600, RT-AC55U, RT-AC55UHP,RT-AC86U, RT-AC2900) cho phép đối tượng tấn công chèn và thực thi mã lệnh.	Đã có thông tin bản vá
3	Cisco	CVE-2018-0231 CVE-2018-0240 CVE-2018-0251 ...	Nhóm 28 lỗ hổng trên một số sản phẩm của Cisco (Adaptive Security Apliance, Fire Power Threat Defense, Fire Power System Software,…) cho phép đối tượng thực hiện nhiều hình thức tấn công khác nhau gồm tấn công từ chối dịch vụ, tấn công XSS, ăn trộm	Đã có xác nhận và thông tin bản vá

			thông tin nhạy cảm, gây ảnh hưởng tới lưu lương mạng đi qua thiết bị, vượt qua cơ chế kiểm soát đã cấu hình và chặn các kết nối, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	
4	D-Link	CVE-2018-10110 CVE-2018-010108 CVE-2018-010107 CVE-2018-010106	Nhóm 04 lỗ hổng trên 2 dòng thiết bị của D-Link DIR-615 T1 và DIR-815 REV.B cho phép thực hiện tấn công XSS trên các thiết bị.	Đã có mã khai thác Đã có thông tin xác nhận và bản vá cho DIR-615 T1
5	Foxit PDF Reader	CVE-2018-3843 CVE-2018-3843	Nhóm 02 lỗ hổng trong phần mềm đọc file PDF (phiên bản 9.0.1.1049) cho phép đối tượng tấn công thực hiện chèn và thực thi mã lệnh nếu người dùng mở một file độc hoặc truy cập một trang web độc hại khi sử dụng add-on của Foxit trên các trình web.	Chưa có thông tin xác nhận và bản vá
6	Oracle	CVE-2018-2830 CVE-2018-2837 CVE-2018-2860 CVE-2018-2835 CVE-2018-2808 ….	Nhóm 149 lỗ hổng trên các sản phẩm của Oracle được sử dụng phổ biến ở Việt Nam (Database Server, E-business suite, Java SE, Virtual Box,…) cho phép đối tượng thực hiện nhiều hình thức tấn công khác nhau gồm thu thập thông tin, truy cập và thực hiện hành động trái phép với dữ liệu trên hệ thống	Đã có thông tin xác nhận

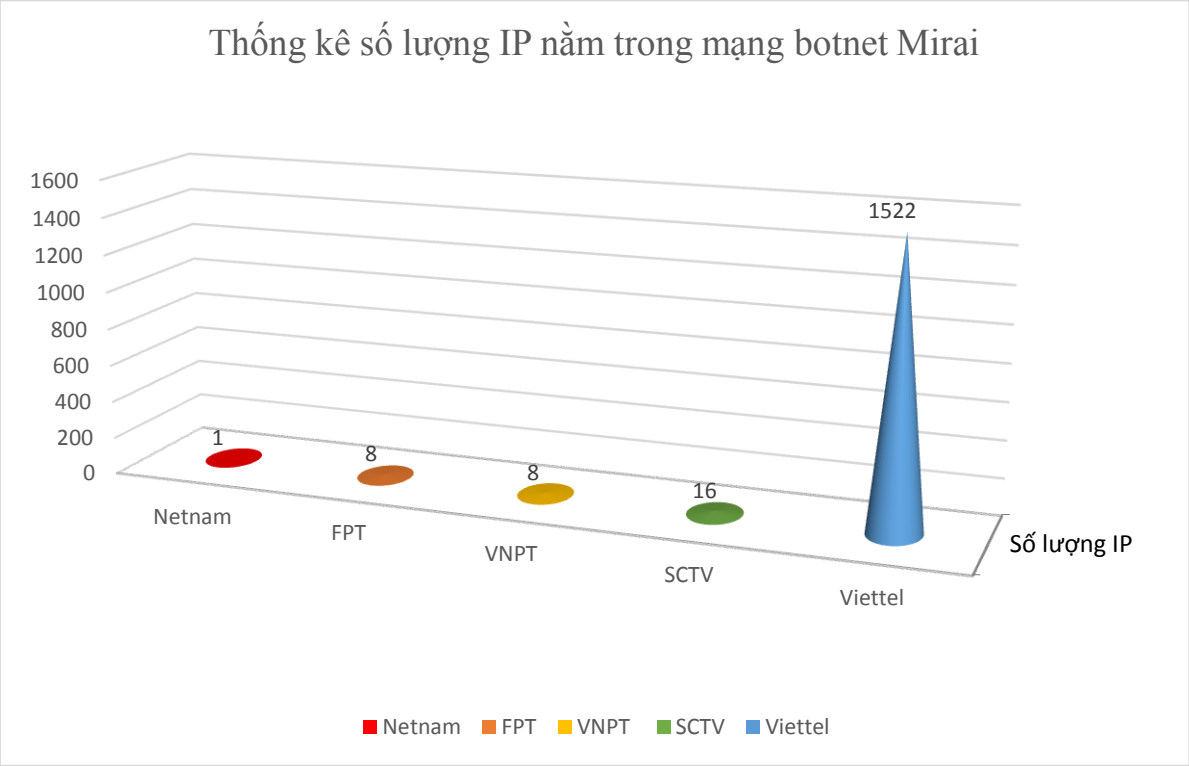
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

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	myxmr.pw
2	c84c8098.com
3	04d92810.com
4	n.hmiblgoja.ru
5	ajkeahkcueafuiaeuf.ru
6	freshwebshop.su
7	tmeansmderivinclusionent.net
8	setsearchg.com
9	pmqzprunfvjdn.net
10	ns1.timedate3.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;

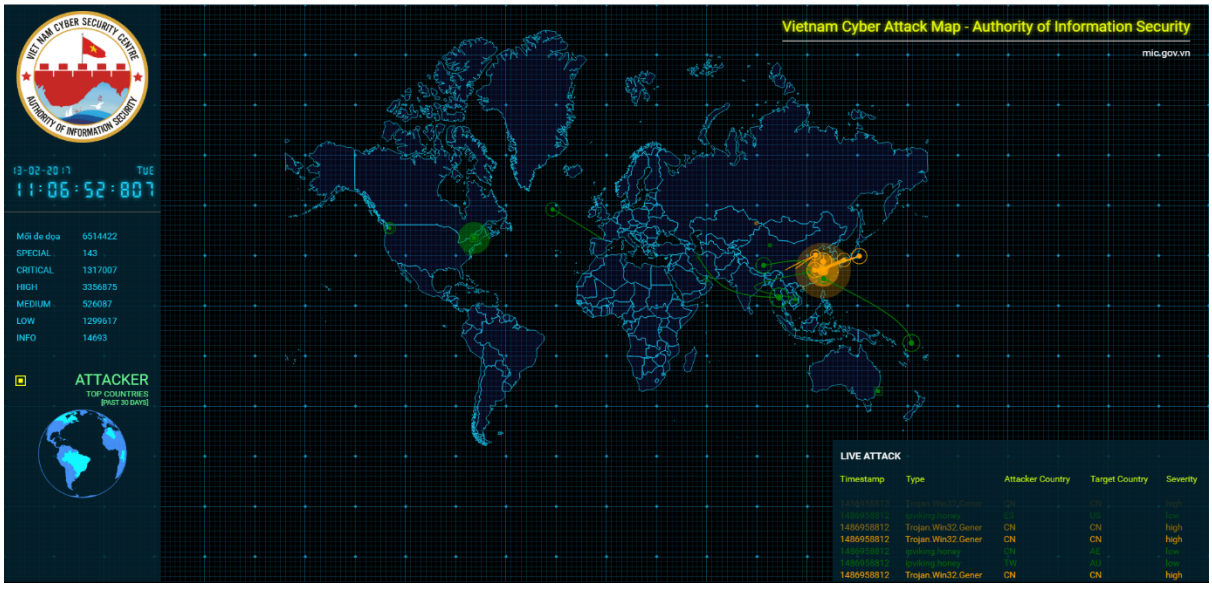
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

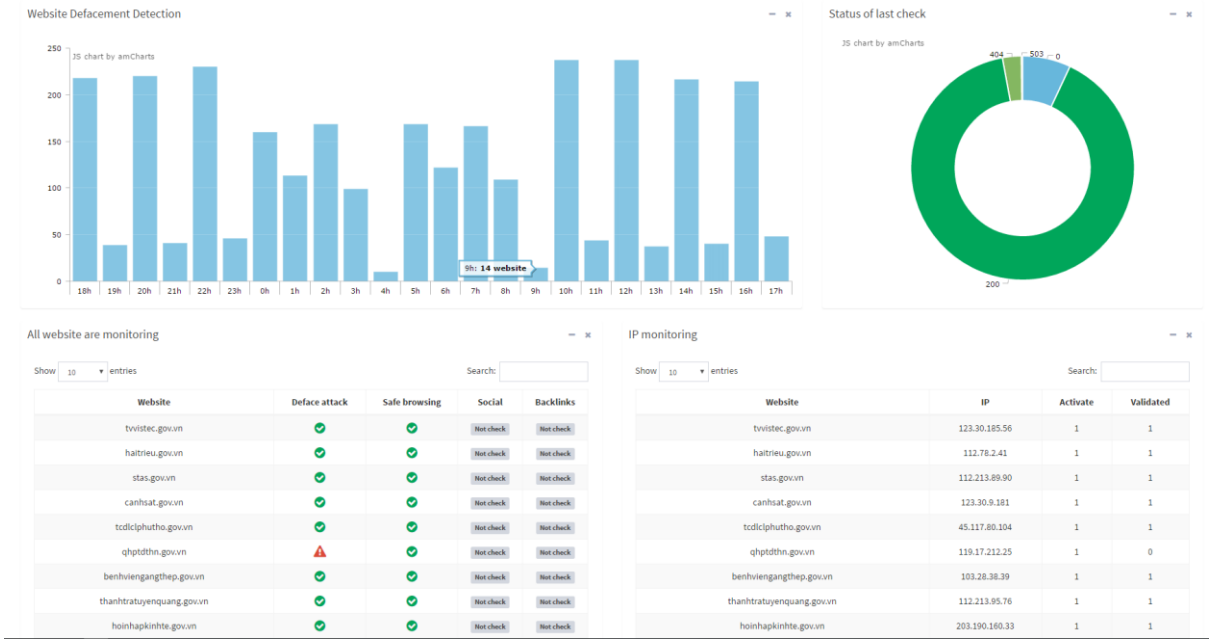
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



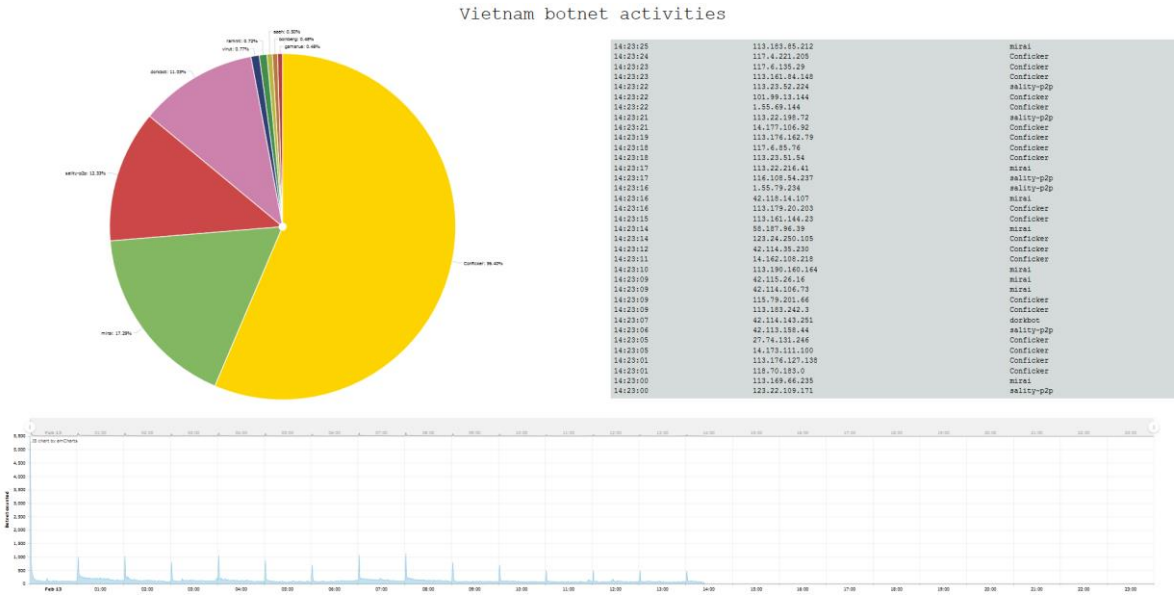
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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