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: **25**/BC-CATTT

Hà Nội, ngày 19 tháng 6 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 24/2018
(từ ngày 11/6/2018 đến ngày 17/6/2018)

BẢNG TỔNG HỢP

1. Cơ quan An toàn mạng và Internet của Hàn Quốc (KISA) công bố hướng dẫn về an toàn thông tin cho ngành y tế và giao thông vận tải tại cuộc họp thường kỳ của Liên minh An toàn IoT Hàn Quốc lần thứ 5.

2. Australia thành lập lực lượng chuyên trách bảo vệ các cuộc bầu cử trước các cuộc tấn công mạng có tên là EITF (Electoral Integrity Task Force). Lực lượng này có trách nhiệm bảo đảm các nhân tố nước ngoài không thể tác động lên kết quả của các cuộc bầu cử tại Australia thông qua tấn công mạng.

3. Nhà nghiên cứu Wojciech Regula từ hãng SecuRing đã công bố một nghiên cứu về nguy cơ mất ATTT từ tính năng "Quick Look" trong macOS giúp người dùng có thể xem trước ảnh, tập tin tài liệu hoặc thư mục mà không cần mở chúng.

1. Điểm tin đáng chú ý

1.1. Cơ quan An toàn mạng và Internet của Hàn Quốc (KISA) công bố hướng dẫn về an toàn thông tin cho ngành y tế và giao thông vận tải tại cuộc họp thường kỳ của Liên minh An toàn IoT Hàn Quốc lần thứ 5. Những hướng dẫn này nằm trong nỗ lực của chính phủ nhằm tăng cường an toàn thông tin cho IoT và xây dựng một môi trường an toàn để vận hành các thiết bị thông minh. Hướng dẫn nhấn mạnh tầm quan trọng của việc hợp tác giữa khu vực công và khu vực tư nhân trong 02 lĩnh vực này.

Bên cạnh việc đặt ra các quy tắc, 02 hướng dẫn cũng phân loại rõ ràng các lĩnh vực trong ngành y tế và giao thông vận tải để có thể quản lý tốt hơn khi mạng các thiết bị IoT không ngừng mở rộng. Hướng dẫn về an toàn thông tin cho y tế thông minh xây dựng một môi trường an toàn cho các nhân viên y tế và

các nhà phát triển thiết bị khi làm việc với các thiết bị y tế thông minh, còn Hướng dẫn về an toàn thông tin cho Giao thông Vận tải thông minh khuyến khích bảo đảm an toàn thông tin nội bộ cho các công ty vận tải và người dùng các sản phẩm và dịch vụ liên quan đến giao thông vận tải thông minh.

1.2. Australia thành lập lực lượng chuyên trách bảo vệ các cuộc bầu cử trước các cuộc tấn công mạng có tên là EITF (Electoral Integrity Task Force). Lực lượng này có trách nhiệm bảo đảm các nhân tố nước ngoài không thể tác động lên kết quả của các cuộc bầu cử tại Australia thông qua tấn công mạng. Thông báo về việc thành lập EITF được đưa ra trước thềm 05 cuộc bầu cử liên bang sẽ tổ chức vào tháng tới.

EITF có sự tham gia của nhiều cơ quan thuộc chính phủ Australia, trong đó bao gồm cả các Bộ như Bộ Tài chính, Bộ Nội vụ … Người phát ngôn lực lượng này cho biết việc thành lập EITF là một biện pháp phòng ngừa cần thiết trong thời đại mà nguy cơ can thiệp và gây tổn hại qua không gian mạng đang ngày một gia tăng.

1.3. Các nhà nghiên cứu ATTT đang cảnh báo về vấn đề bảo mật đã có từ rất lâu với một trong những tính năng của hệ điều hành MacOS của Apple, được thiết kế nhằm thuận tiện cho người dùng nhưng lại có thể gây lộ lọt thông tin của các tập tin được lưu trữ trên ổ đĩa đã được mã hóa bảo vệ bằng mật khẩu.

Cụ thể, mới đây nhà nghiên cứu Wojciech Regula từ hãng SecuRing đã công bố một nghiên cứu về tính năng "Quick Look" trong macOS giúp người dùng có thể xem trước ảnh, tập tin tài liệu hoặc thư mục mà không cần mở chúng. Tính năng Quick Look sẽ tạo ra hình thu nhỏ cho mỗi tập tin/thư mục, mà nhờ đó người dùng có thể nhanh chóng xem xét tập tin trước khi mở. Tuy nhiên các hình thu nhỏ này lại được lưu trữ trong bộ nhớ cache không được mã hóa của máy tính, có thể dễ dàng tìm ra vị trí và không được bảo vệ, dù cho tập tin/thư mục ban đầu thuộc về vùng chứa đã được mã hóa, do đó sẽ làm lộ dữ liệu lưu trữ trên các ổ đĩa đã mã hóa.

Để chứng minh cho nghiên cứu của mình, Regula đã tạo ra 2 bộ nhớ được mã hóa, một bộ nhớ sử dụng phần mềm VeraCrypt và bộ nhớ còn lại sử dụng ổ đĩa Encrypted HFS+/APFS của MacOS, sau đó lưu ảnh trong mỗi bộ nhớ. Như đã giải thích trong bài viết của mình, sau khi chạy lệnh đơn giản trên hệ thống, Regula có thể tìm ra đường dẫn và tập tin lưu trữ cache cho 2 bức ảnh đặt bên ngoài bộ nhớ đã mã hóa. Điều này có nghĩa là tất cả các bức ảnh mà người dùng xem trước sử dụng tính năng Quick Look sẽ lưu trữ một bản thu nhỏ và đường

dẫn của nó trong một thư mục không được mã hóa. Chúng thậm chí sẽ không bị xóa cả khi người dùng xóa tập tin nằm trong bộ nhớ ban đầu.

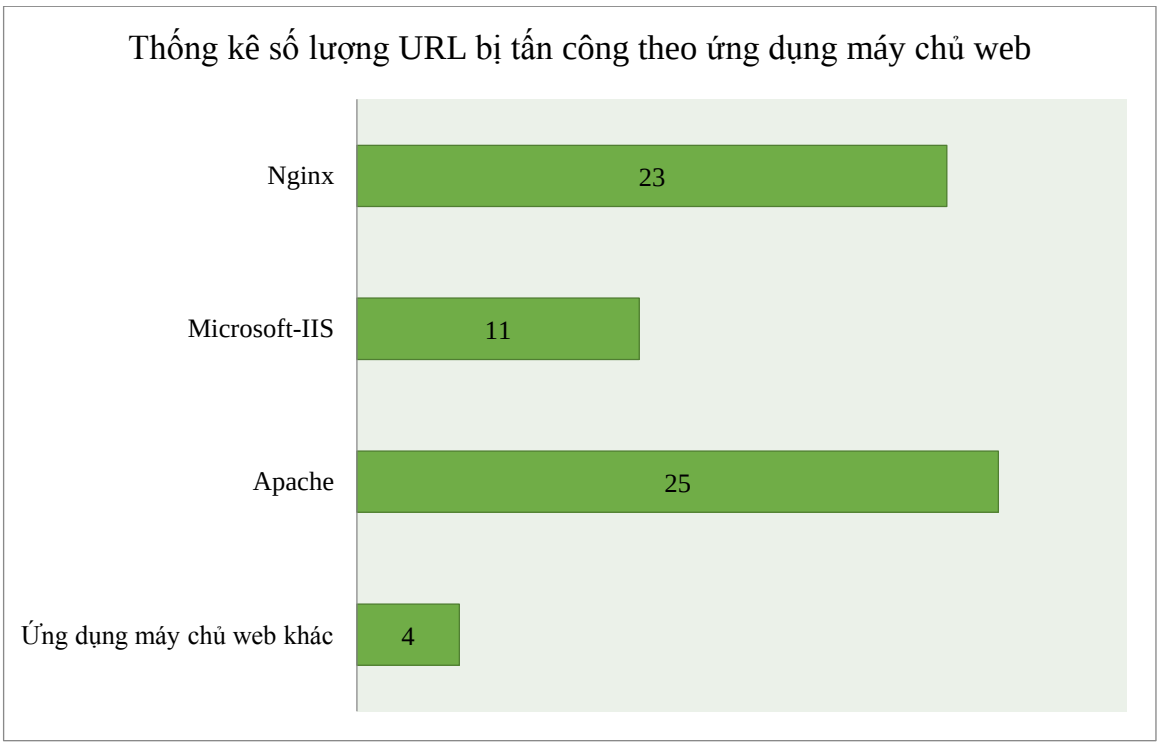
Trong một bài viết khác được công bố sau đó, Patrick Wardle, giám đốc nghiên cứu của Digital Security cũng chia sẻ nghiên cứu tương tự đối với các bộ nhớ AFPS mã hóa được bảo vệ bằng mật khẩu. Hệ điều hành MacOS lưu trữ hình thu nhỏ của tập tin nằm trên bộ nhớ mã hóa dù cho người dùng đã tháo bộ nhớ ra khỏi máy tính. Theo Wardle vấn đề này đã được phát hiện từ ít nhất 8 năm trước, tuy nhiên vẫn còn tồn tại trong phiên bản mới nhất của MacOS hiện nay và ít người dùng MacOS biết đến.

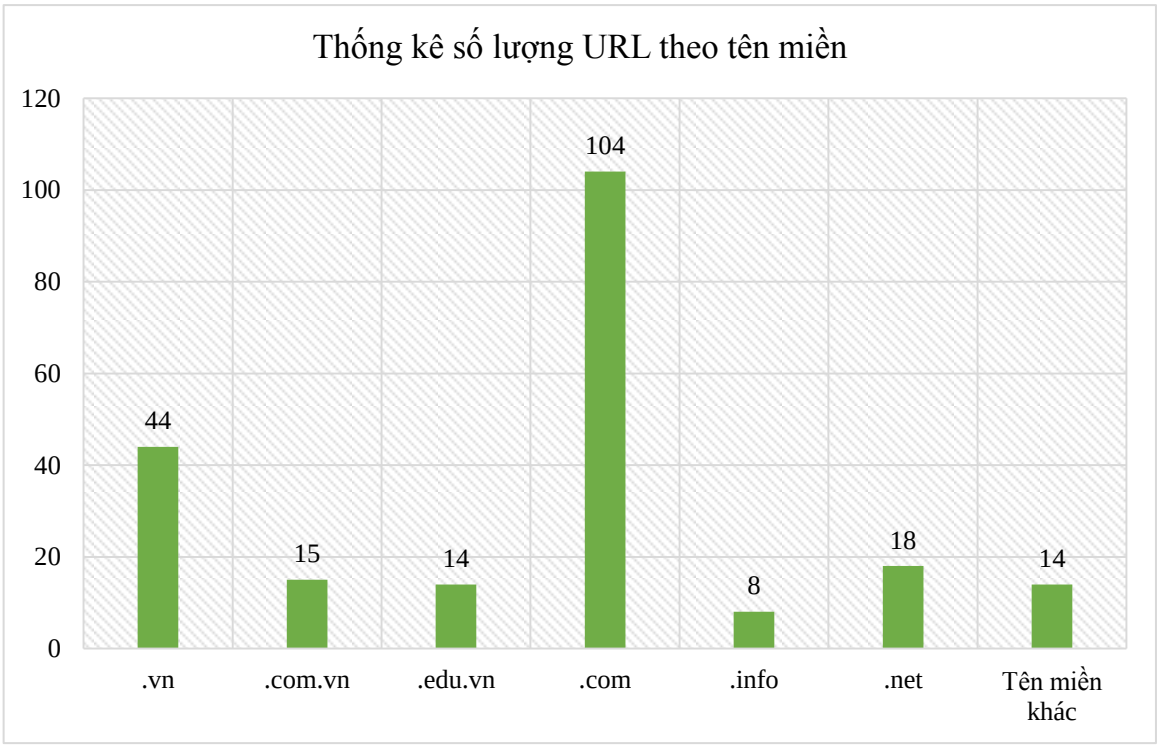
Khuyến nghị dành cho người dùng là nên cân nhắc việc xóa cache QuickLook được tạo ra bởi hệ điều hành sau khi sử dụng nếu thấy việc lưu cache là không cần thiết.

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…).

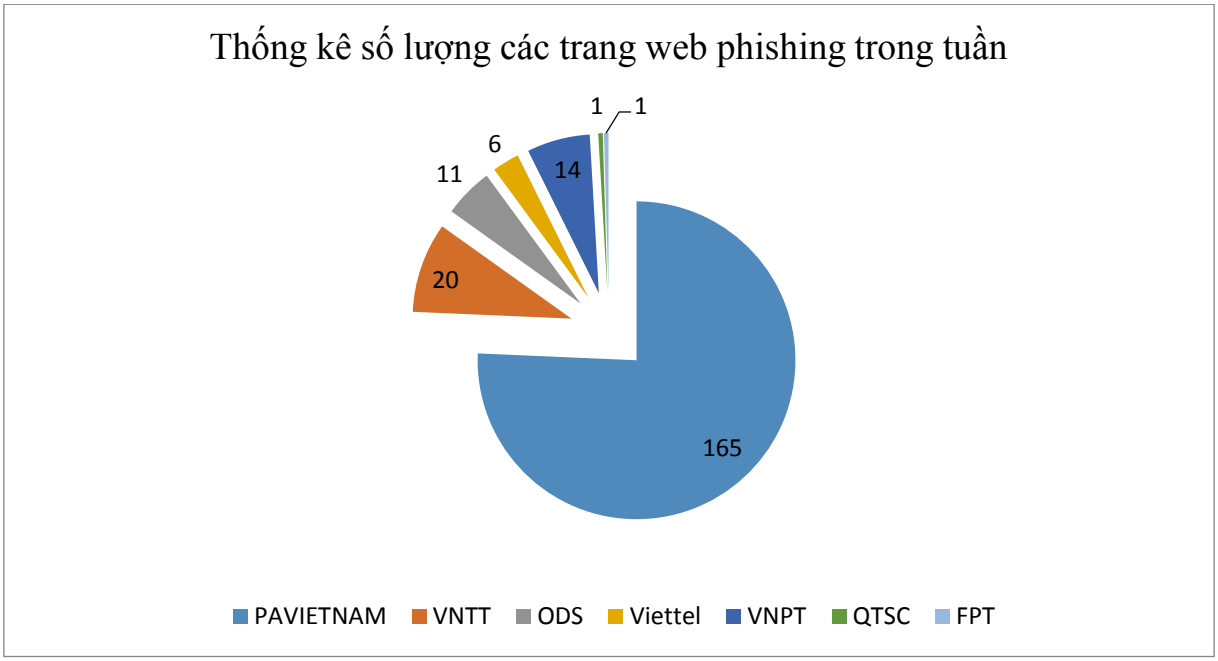
Trong tuần, Cục ATTT ghi nhận có ít nhất 217 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



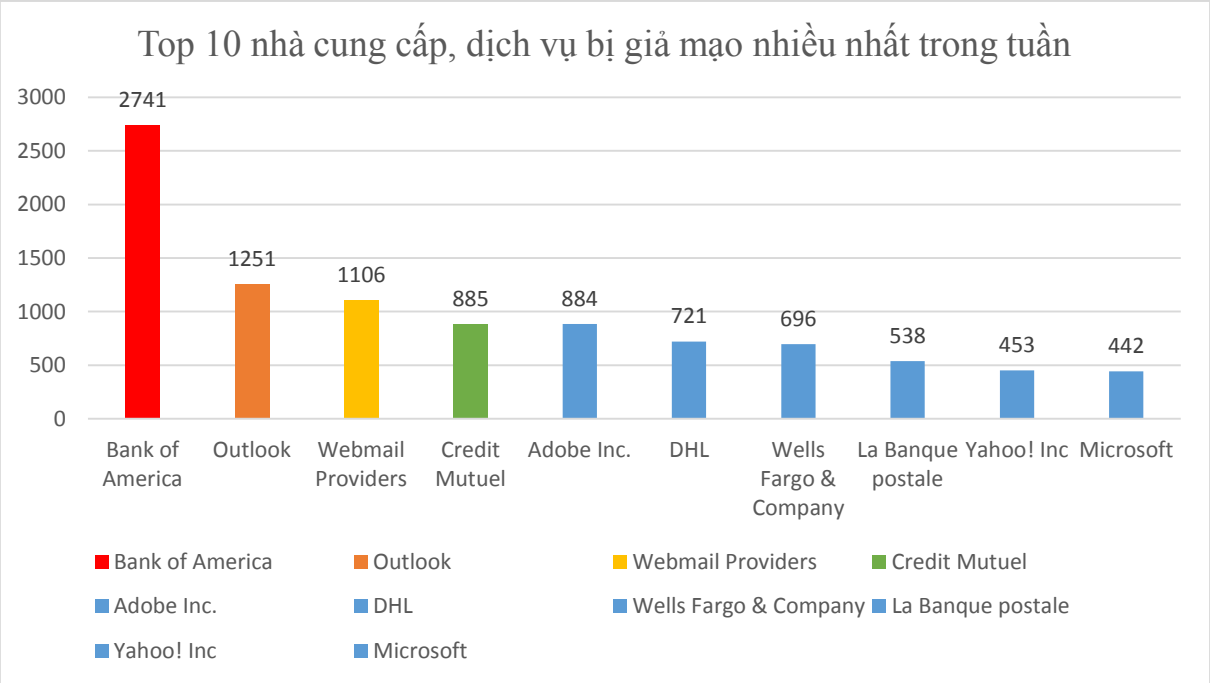


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **218** 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 596 lỗ hổng, trong đó có ít nhất 28 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 31 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 317 lỗ hổng trên các sản phẩm của Mozilla; Nhóm 50 lỗ hổng trên nhiều sản phẩm của Microsoft ..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	Apple	CVE-2018-12418 CVE-2018-4247 CVE-2018-10406 CVE-2018-10405 CVE-2018-10404 …	Nhóm 10 lỗ hổng trên nhiều sản phẩm của Apple (iOS, macOS, Safari) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, đánh cắp thông tin, nhiều lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận
2	Microsoft	CVE-2018-8233 CVE-2018-8251 CVE-2018-0871 CVE-2018-8249 CVE-2018-8244	Nhóm 50 lỗ hổng trên nhiều sản phẩm của Microsoft (Windows, Office, Window Server, Internet Explorer,…) cho phép thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lênh, đánh cắp thông tin nhạy cảm trên hệ thống…	Đã có thông tin xác nhận và bản vá
3	Mozilla	CVE-2018-5118 CVE-2018-5137 CVE-2018-7780 CVE-2018-7759 CVE-2018-7796 …	Nhóm 317 lỗ hổng trên các sản phẩm của Mozilla (Firefox, Firefox ESR, Thunderbird,…) cho phép đối tượng thực hiện tấn công từ chối dịch vụ, XSS, đọc và chỉnh sửa dữ liệu, chèn và thực thi mã lệnh.	Đã có thông tin xác nhận, nhiều lỗ hổng đã có mã khai thác
4	Huawei	CVE-2018-11309 CVE-2018-17172 CVE-2018-17173	3 lỗ hổng trên các thiết bị của Huawei (HG255s-10 V100R001C163B025SP02, LYO-L21, Mate 9) cho phép đối tượng truy cập trái phép vào dữ liệu, chiếm đặc quyền, chèn và thực thi mã lệnh.	Đã có thông tin xác nhận

5	Qualcomm	CVE-2018-12481 CVE-2018-5848 CVE-2018-5851 CVE-2018-18070 CVE-2018-5849 …	Nhóm 24 lỗ hổng trên hệ điều hành Android cho phép đối tượng gây tràn bộ đệm thiết bị hoặc đánh cắp mật khẩu người dùng.	Chưa có thông tin xác nhận và bản vá
6	Joomla!	CVE-2018-12254 CVE-2018-11690	Nhóm 02 lỗ hổng trên hệ quản trị nội dung cho phép đối tượng tấn công thực hiện thực hiện tấn công SQL Injection, tấn công XSS. CVE-208-12254 đã có mã khai thác.	Chưa có thông tin xác nhận và bản vá

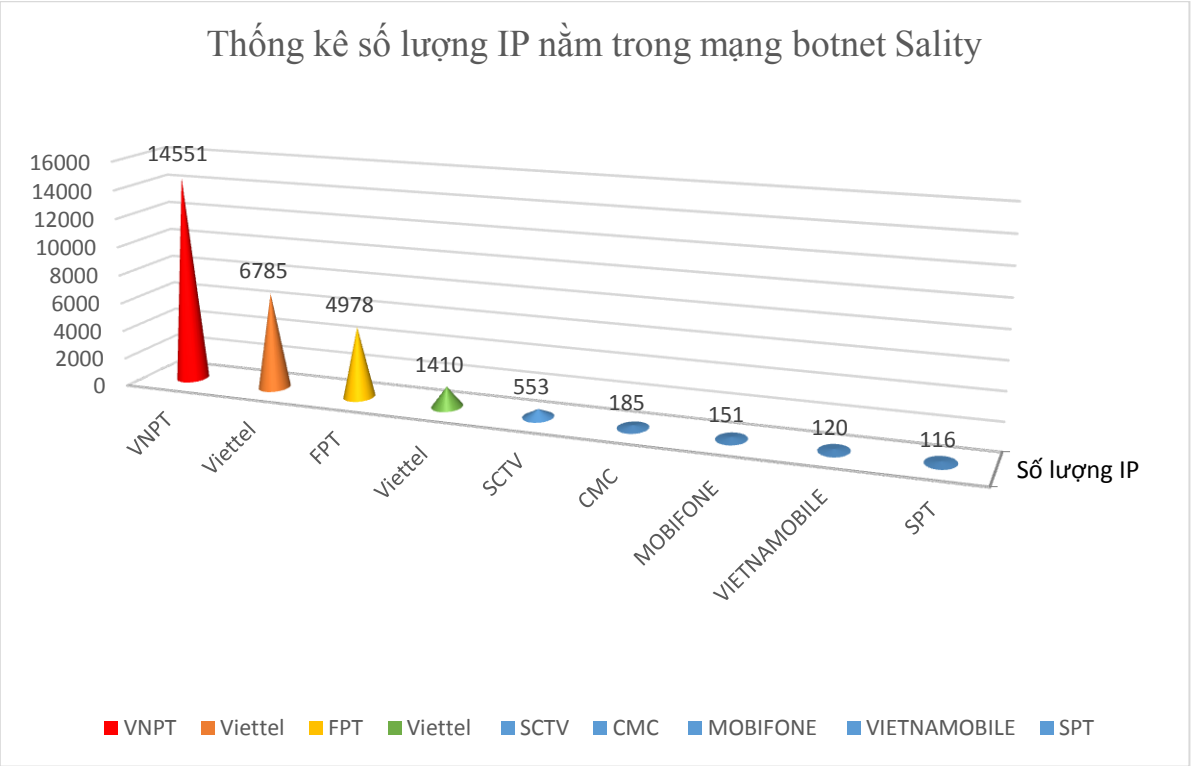
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

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 thống 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	8to8b5hebw.ru
2	kukutrustnet777.info
3	gu2tcqt0v.ru
4	104.244.14.252
5	init.icloud-analysis.com
6	u6p6odiac.ru
7	g.omlao.com
8	kukutrustnet888.info
9	mk.omkol.com
10	u.amobisc.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;

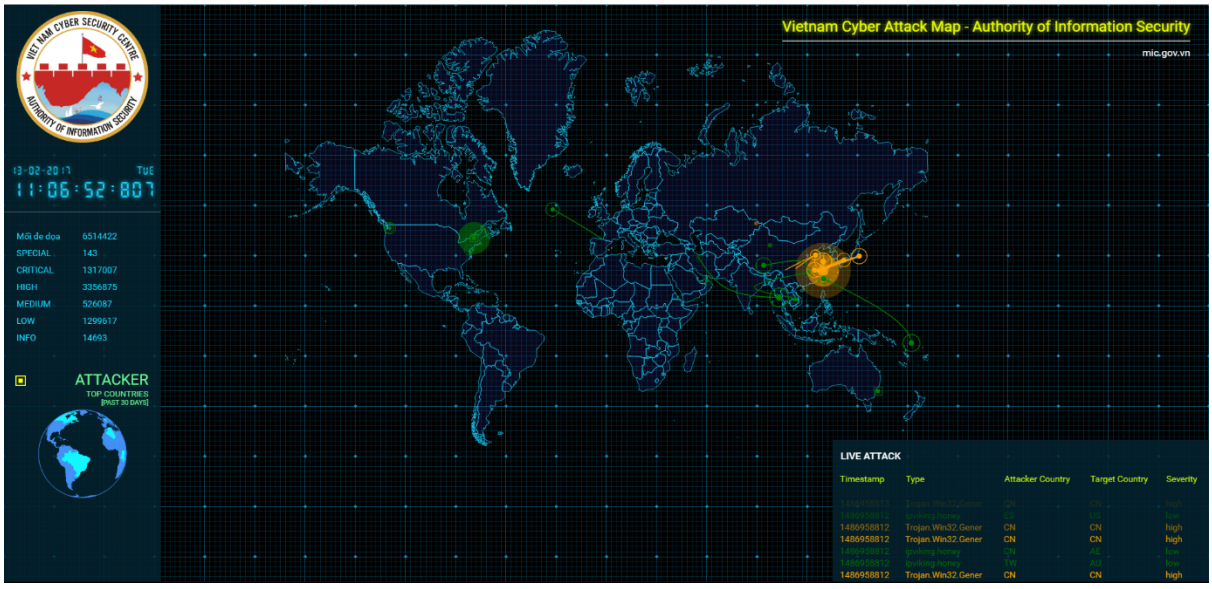
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

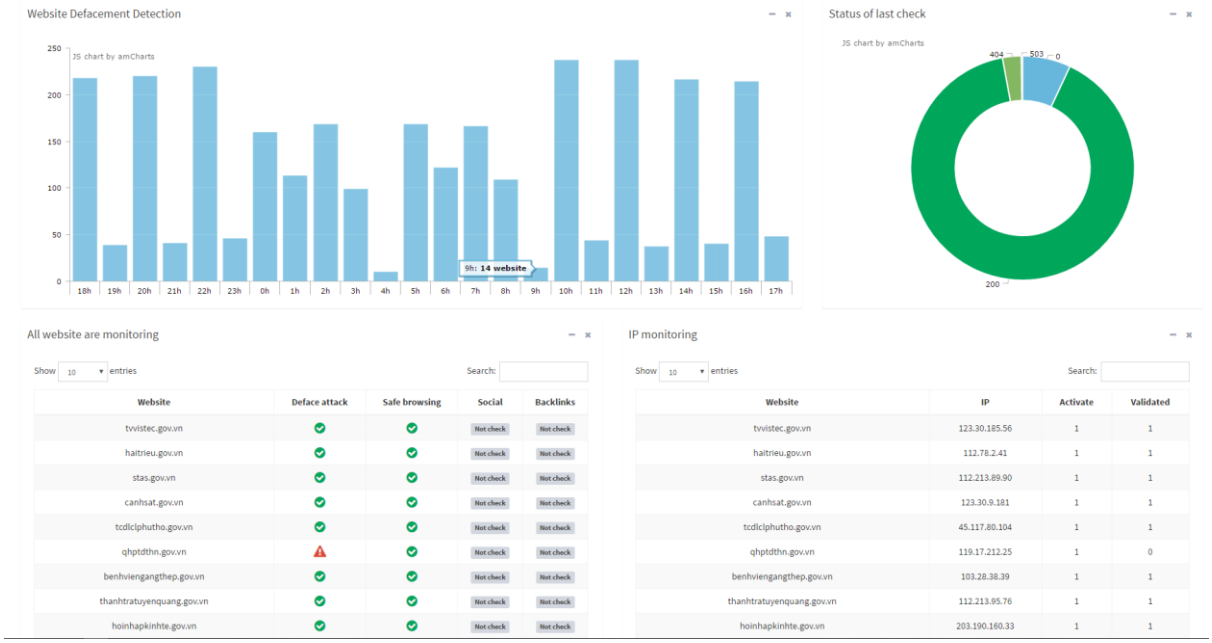
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



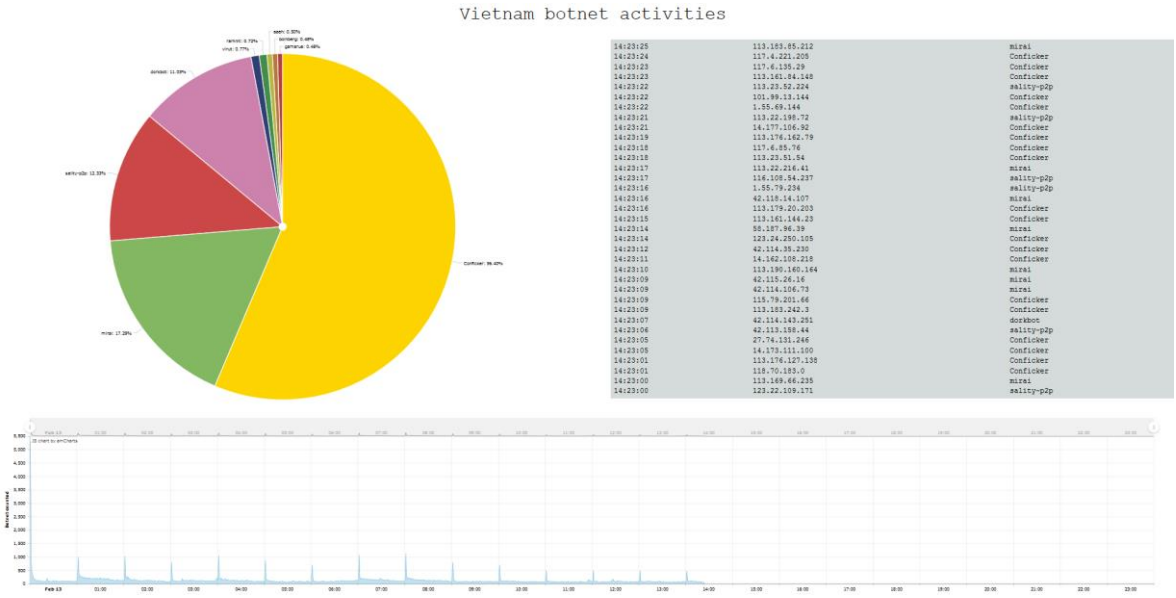
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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