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: **30**/BC-CATTT

Hà Nội, ngày 10 tháng 7 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 27/2018
(từ ngày 02/7/2018 đến ngày 08/7/2018)

BẢNG TỔNG HỢP

1. Bang California, Hoa Kỳ xây dựng Dự luật bảo vệ dữ liệu của người dùng, trong đó mở rộng khái niệm của thông tin cá nhân và cho người tiêu dùng ở California quyền cấm rao bán thông tin cá nhân cho bên thứ ba và lựa chọn ngừng tham gia vào quá trình chia sẻ thông tin nói chung.

2. Văn phòng Chính phủ đã có văn bản truyền đạt ý kiến chỉ đạo của Phó Thủ tướng Vũ Đức Đam về thực hiện Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

3. Các nhà nghiên cứu bảo mật phát hiện ra một chiến dịch tấn công mạng bằng mã độc lợi dụng các chứng chỉ số hợp lệ bị đánh cắp từ các công ty công nghệ, để ký số chứng thực cho mã độc, làm cho các mã độc này được coi như các ứng dụng hợp pháp.

1. Điểm tin đáng chú ý

1.1. Bang California, Hoa Kỳ xây dựng Dự luật bảo vệ dữ liệu của người dùng, trong đó mở rộng khái niệm của thông tin cá nhân và cho người tiêu dùng ở California quyền cấm rao bán thông tin cá nhân cho bên thứ ba và lựa chọn ngừng tham gia vào quá trình chia sẻ thông tin nói chung. Dự luật sẽ được áp dụng cho tất cả các doanh nghiệp ở mọi quy mô thực hiện thu thập dữ liệu người dùng.

Luật này khi được áp dụng ở California, các hãng công nghệ nhiều khả năng sẽ phải thay đổi toàn bộ chính sách của họ chiếu theo luật vì việc tạo ra các tiêu chuẩn khác nhau cho mỗi vùng là rất phức tạp. Dự luật có một vài điểm tương tự với Luật Bảo vệ dữ liệu cá nhân của Châu Âu đã có hiệu lực hồi tháng 5/2018. Tuy nhiên, dự luật của California chú trọng trách nhiệm của người dùng

trong việc yêu cầu cung cấp thông tin và ngừng chia sẻ dữ liệu, trong khi luật của châu Âu yêu cầu các doanh nghiệp phải chủ động hơn trong việc cung cấp thông tin cho người dùng.

1.2. Văn phòng Chính phủ đã có văn bản truyền đạt ý kiến chỉ đạo của Phó Thủ tướng Vũ Đức Đam về thực hiện Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

Phó Thủ tướng giao Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Giáo dục và Đào tạo nghiên cứu, đề xuất, trình Thủ tướng Chính phủ điều chỉnh mục tiêu của Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020 (Đề án 99) về số lượt cán bộ chuyên trách về an toàn, an ninh thông tin đi đào tạo ngắn hạn ở nước ngoài để phù hợp với tình hình thực tế hiện nay.

Bộ Thông tin và Truyền thông bổ sung nhóm đối tượng "Cán bộ làm về an toàn, an ninh thông tin chịu trách nhiệm quản lý, vận hành, bảo đảm an toàn thông tin cho các hệ thống thông tin phục vụ các cơ quan Đảng, Nhà nước, phát triển chính phủ điện tử và chính quyền điện tử các cấp" và "Giảng viên giảng dạy về an toàn, an ninh thông tin tại các cơ sở đào tạo trọng điểm" tham gia các khóa đào tạo ngắn hạn về an toàn thông tin do Bộ Thông tin và Truyền thông tổ chức hàng năm.

Phó Thủ tướng cũng giao Bộ Thông tin và Truyền thông chủ trì, phối hợp với Hiệp hội an toàn thông tin Việt Nam nghiên cứu, đề xuất cơ chế huy động nguồn lực xã hội hóa từ các Tập đoàn, Tổng công ty nhà nước, các doanh nghiệp hoạt động trong lĩnh vực an toàn thông tin để triển khai các nhiệm vụ đào tạo, phát triển nguồn nhân lực an toàn, an ninh thông tin tại Việt Nam

1.3. Gần đây các nhà nghiên cứu bảo mật đã phát hiện ra một chiến dịch tấn công mạng bằng mã độc lợi dụng các chứng chỉ số hợp lệ bị đánh cắp từ các công ty công nghệ, để ký số chứng thực cho mã độc, làm cho các mã độc này được coi như các ứng dụng hợp pháp.

Các chứng chỉ số được sử dụng để ký mã hóa các ứng dụng và phần mềm máy tính và chúng được tin cậy bởi máy tính để thực thi các chương trình đó mà không có bất kỳ thông báo cảnh báo nào. Việc đối tượng tấn công đánh cắp và lợi dụng chứng chỉ chữ ký liên kết với nhà cung cấp phần mềm đáng tin cậy để ký chứng thực cho mã độc sẽ làm hạn chế khả năng phát hiện mã độc của các

dịch vụ, ứng dụng phòng, chống mã độc trên mạng doanh nghiệp và thiết bị của người dùng.

Các nhà nghiên cứu tại hãng bảo mật ESET đã phát hiện ra 2 họ mã độc được cho là có liên quan đến nhóm gián điệp mạng BlackTech, được ký bằng chứng chỉ số hợp lệ của nhà sản xuất thiết bị mạng D-Link và một công ty bảo mật của Đài Loan có tên là Changing Information Technology.

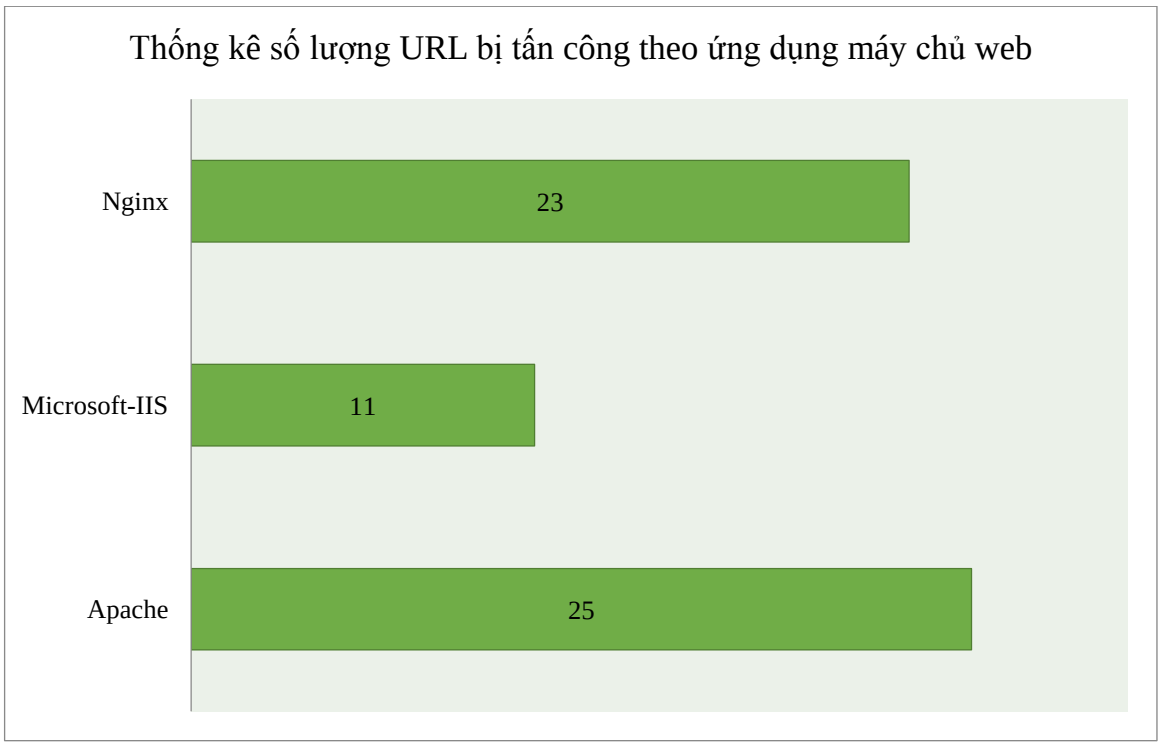
Mã độc đầu tiên được gọi là Plead, đây là một backdoor kiểm soát từ xa được thiết kế để ăn cắp các file tài liệu và nghe lén người dùng. Mã độc thứ 2 là phần mềm ăn cắp mật khẩu được thiết kế nhằm thu thập mật khẩu của người dùng được lưu trên những ứng dụng phổ biến như Google Chrome, Microsoft Internet Explorer, Microsoft Outlook và Mozilla Firefox.

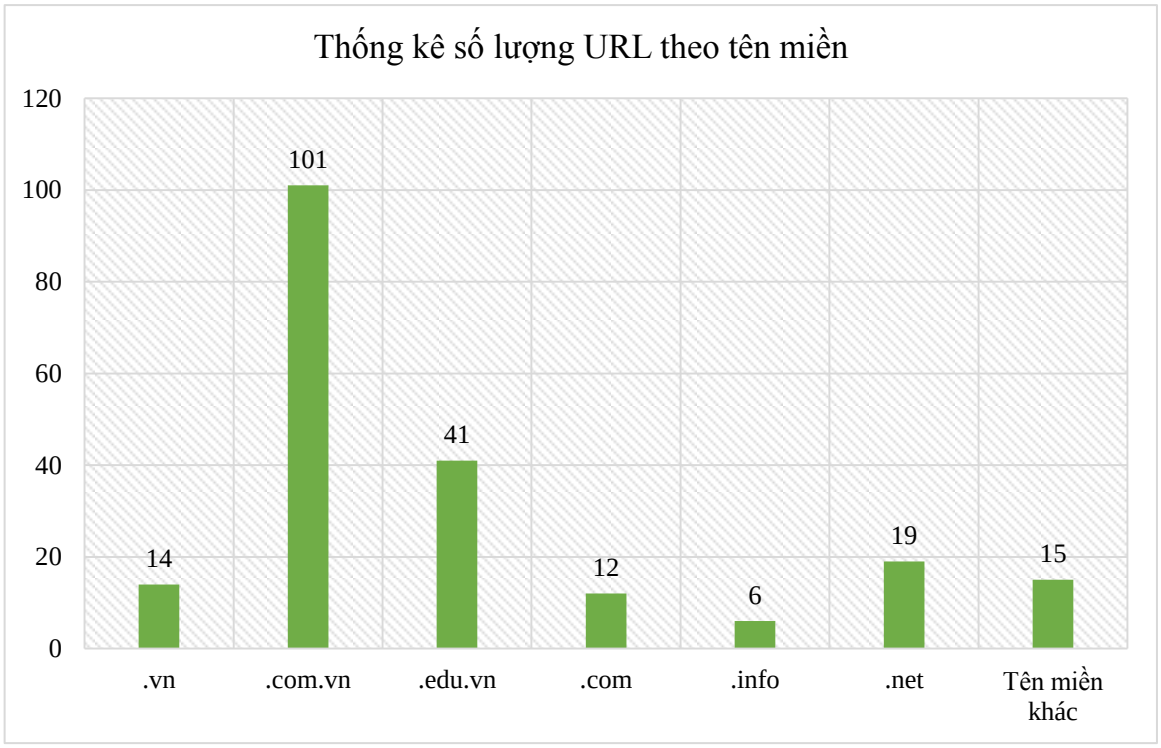
Ngay sau khi nhận được cảnh báo, D-Link và công ty Changing Information Technology đã thu hồi các chứng chỉ số bị đánh cắp vào đầu tháng này. Tuy nhiên, vì hầu hết các giải pháp phòng, chống mã độc không kiểm tra tính hợp lệ của chứng chỉ số kể cả khi các công ty đã thu hồi chữ ký của chứng chỉ, nhóm BlackTech vẫn đang sử dụng chứng chỉ cũ để ký chứng thực cho các công cụ độc hại.

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…).

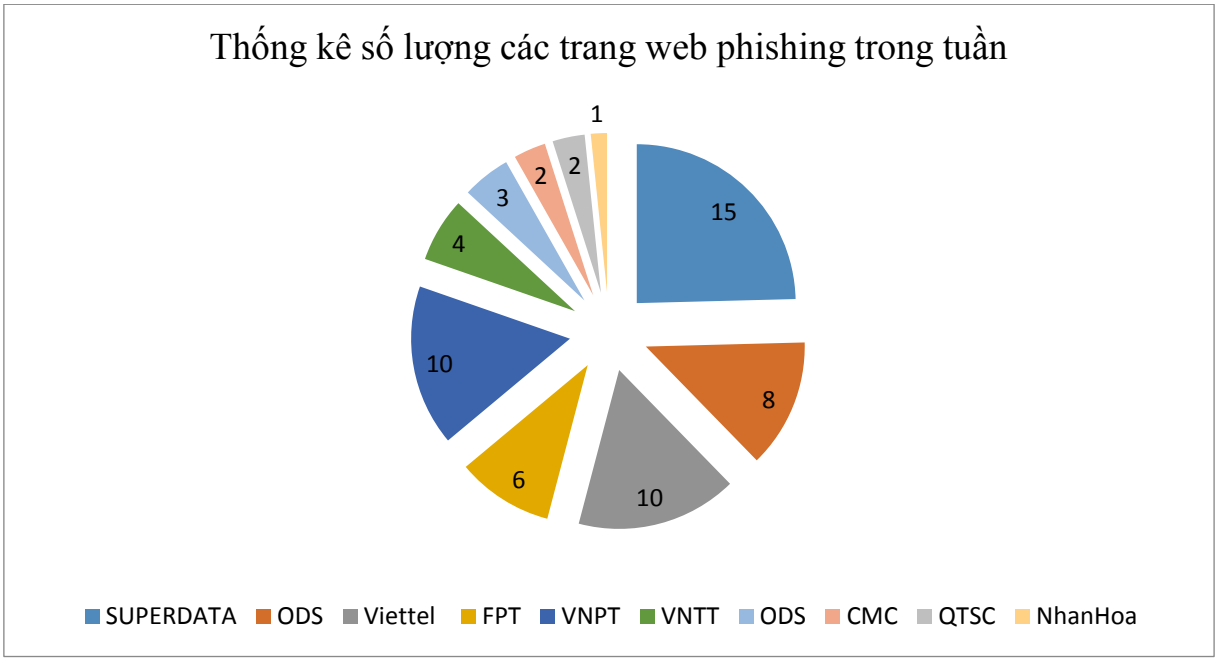
Trong tuần, Cục ATTT ghi nhận có ít nhất **208** đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



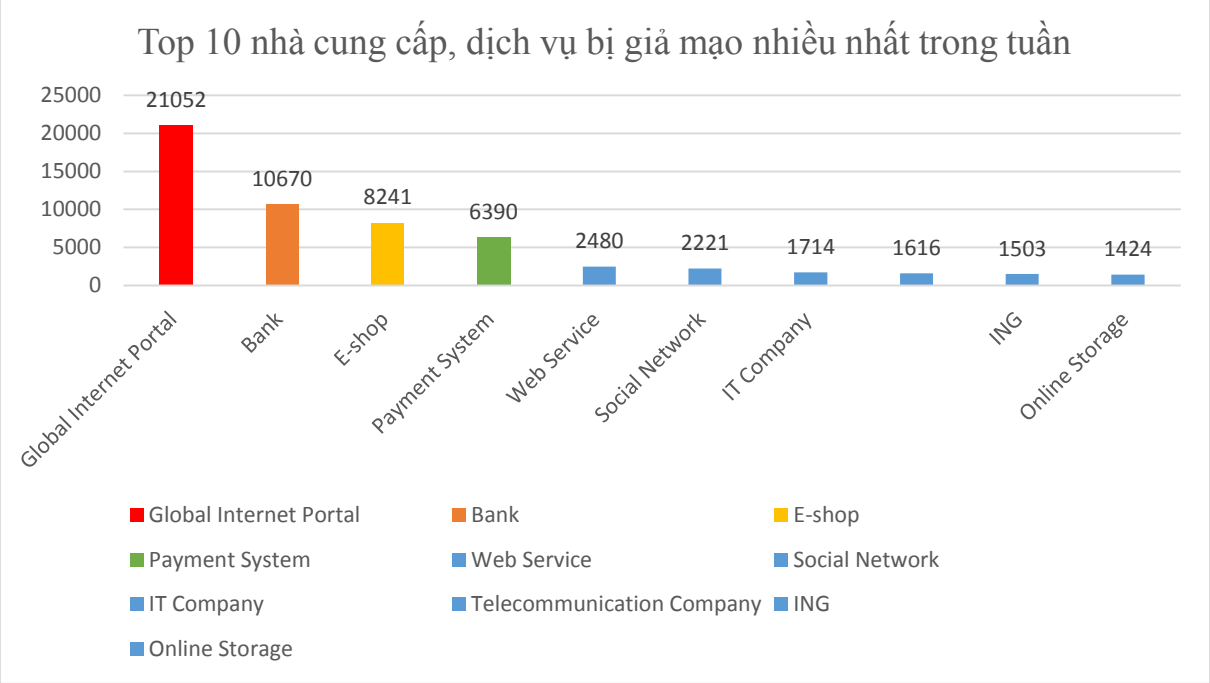


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất **63** 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: Các mạng xã hội, Outlook .v.v…



Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và có phí) như các mạng xã hội, outlook, yahoo .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 439 lỗ hổng, trong đó có ít nhất 7 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh) và 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 58 lỗ hổng trên nhiều phần mềm sử dụng cho Android; Nhóm 5 lỗ hổng trên các dòng router của tp-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	D-link	CVE-2018-12103	Lỗ hổng trên dòng router DIR-890L A2 do tính dễ đoán của thuật toán tạo CAPTCHA cho phép đối tượng thực hiện tấn công vét cạn trên hệ thống đăng nhập.	Chưa có thông tin xác nhận và bản vá
2	Dell EMC	CVE-2018-11052 CVE-2018-1249 CVE-2018-1244 CVE-2018-1212 CVE-2018-1243	Nhóm 5 lỗ hổng trên dịch vụ lưu trữ ECS và Trình quản lý Máy chủ từ xa IDRAC của Dell EMC cho phép đối tượng thực hiện đọc và chỉnh sửa tệp lưu trữ, tắt tính năng bảo vệ SSL/TLS, chèn và thực thi mã lệnh. Ngoài ra iDRAC6 còn dễ bị tấn công vét cạn do phiên CGI chỉ sử dụng ID số 96 bit.	Chưa có thông tin xác nhận
3	Huawei	CVE-2018-7944 CVE-2018-17175 CVE-2018-17317 CVE-2018-17316	Nhóm 4 lỗ hổng trên nhiều thiết bị của Huawei (Emily-AL00A, Mate 9 Pro và nhiều dòng thiết bị định tuyến) cho phép đối tượng thực hiện chiếm quyền sử dụng thiết bị, tấn công từ chối dịch vụ, làm tràn bộ đệm và đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá

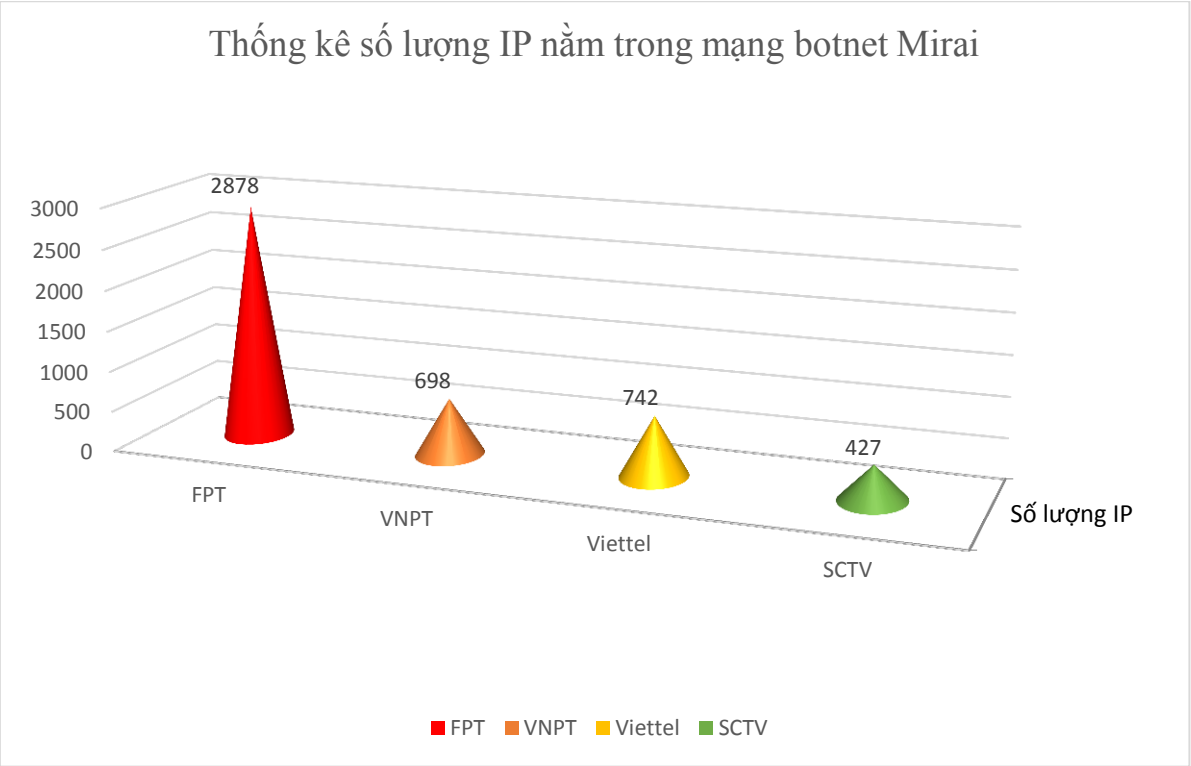
4	Qualcomm	CVE-2018-5907 CVE-2018-5898 CVE-2018-5862 CVE-2018-5853 CVE-2018-5885	Nhóm 58 lỗ hổng trên nhiều phần mềm sử dụng cho Android cho phép đối tượng thực nhiều hình thức tấn công như làm tràn và viết đè bộ đệm, lây nhiễm SQL, chèn và thực thi mã lệnh,…	Đã có thông tin xác nhận và bản vá
5	TP-link	CVE-2018-13134 CVE-2018-12577 CVE-2018-12574 CVE-2018-12576 CVE-2018-12575	Nhóm 5 lỗ hổng trên các dòng router của tp-link (Archer C1200, TL-WR841N) cho phép đối tượng thực hiện nhiều hình thức tấn công XSS, CSRF, clickjacking,…	Chưa có thông tin xác nhận
6	Wordpress	CVE-2018-12426 CVE-2018-13136	Nhóm 02 lỗ hổng trên các tiện ích của Wordpress (WP Live Chat Support Pro trước phiên bản 8.0.0.7 và Ultimate Member trước phiên bản 2.0.18) cho phép đối tượng thực hiện chèn và thực thi mã lệnh, tấn công XSS.	Chưa 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	a6xwktlad.ru
2	kukutrustnet777.info
3	104.244.14.252
4	w42f4ctqv4.ru
5	g.omlao.com
6	kukutrustnet888.info
7	mk.omkol.com
8	init.icloud-analysis.com
9	p.omlao.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;
- 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;

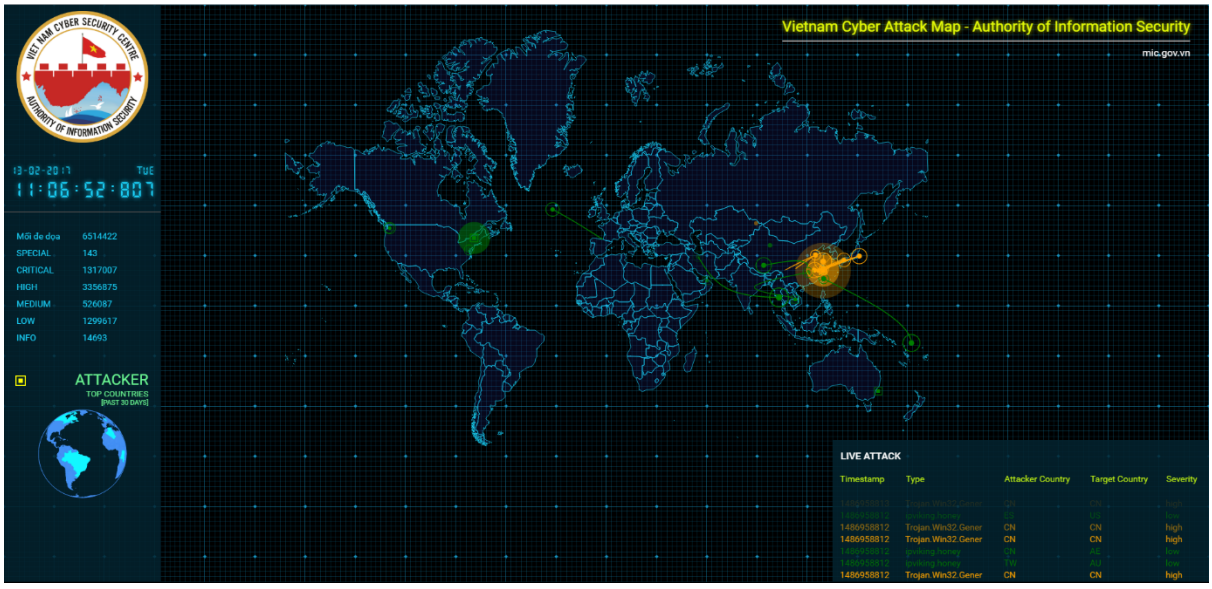
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

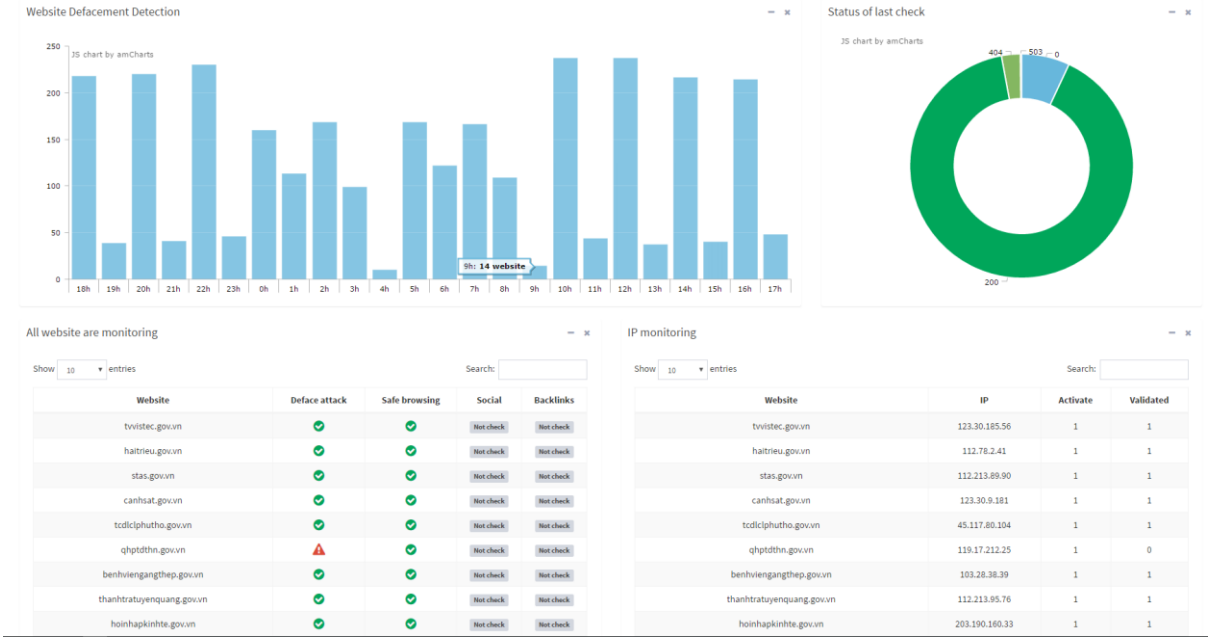
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



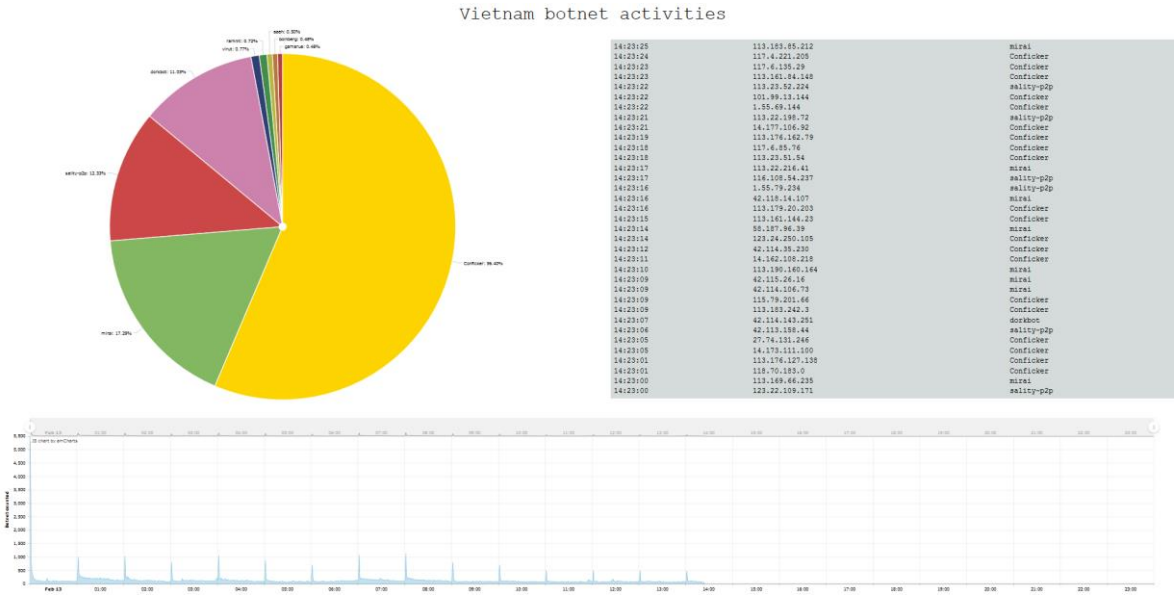
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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