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: **05**/BC-CATTT

Hà Nội, ngày 30 tháng 01 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 04/2018 (từ ngày 22/01/2018 đến ngày 28/01/2018)

Cục An toàn thông tin là cơ quan có chức năng tham mưu, giúp Bộ trưởng Bộ Thông tin và Truyền thông quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin. Qua công tác thu thập, theo dõi, trích xuất, phân tích thông tin trong tuần 04/2018 (từ ngày 22/01/2018 đến ngày 28/01/2018), Cục An toàn thông tin thực hiện tổng hợp tóm tắt về an toàn thông tin diễn ra trong tuần.

Cục An toàn thông tin gửi tóm tắt tình hình để các cơ quan, tổ chức, cá nhân tham khảo và có các biện pháp phòng ngừa hợp lý.

BẢNG TỔNG HỢP

1. Ngày 22/01/2018, theo thông tin từ tờ báo The Telegraph, một số lãnh đạo chính phủ Hà Lan sử dụng điện thoại được thiết kế riêng, nhằm bảo đảm an toàn thông tin trong các chuyến đi công tác nước ngoài.

2. Cảnh báo tấn công lừa đảo lợi dụng thời điểm cuối năm có nhiều chương trình khuyến mại, giảm giá, tặng quà tri ân.

3. Trong tuần ghi nhận 06 nhóm lỗ hổng, điểm yếu được cho là có thể gây ảnh hưởng lớn đến người dùng tại Việt Nam.

1. Điểm tin đáng chú ý

1.1. Ngày 22/01/2018, theo thông tin từ tờ báo The Telegraph, một số lãnh đạo chính phủ Hà Lan sử dụng điện thoại được thiết kế riêng, nhằm bảo đảm an toàn thông tin trong các chuyến đi công tác nước ngoài. Dòng điện thoại này được thiết kế với các thông số kỹ thuật công nghệ thấp để hạn chế việc tấn công mạng vào các điện thoại này. Điện thoại không có kết nối internet, không hỗ trợ cài đặt ứng dụng phổ biến, chỉ hỗ trợ liên lạc bằng thoại, gửi tin nhắn văn bản. Tuy nhiên điện thoại này cũng hỗ trợ truyền dữ liệu hạn chế qua mạng an toàn được thiết lập sẵn.

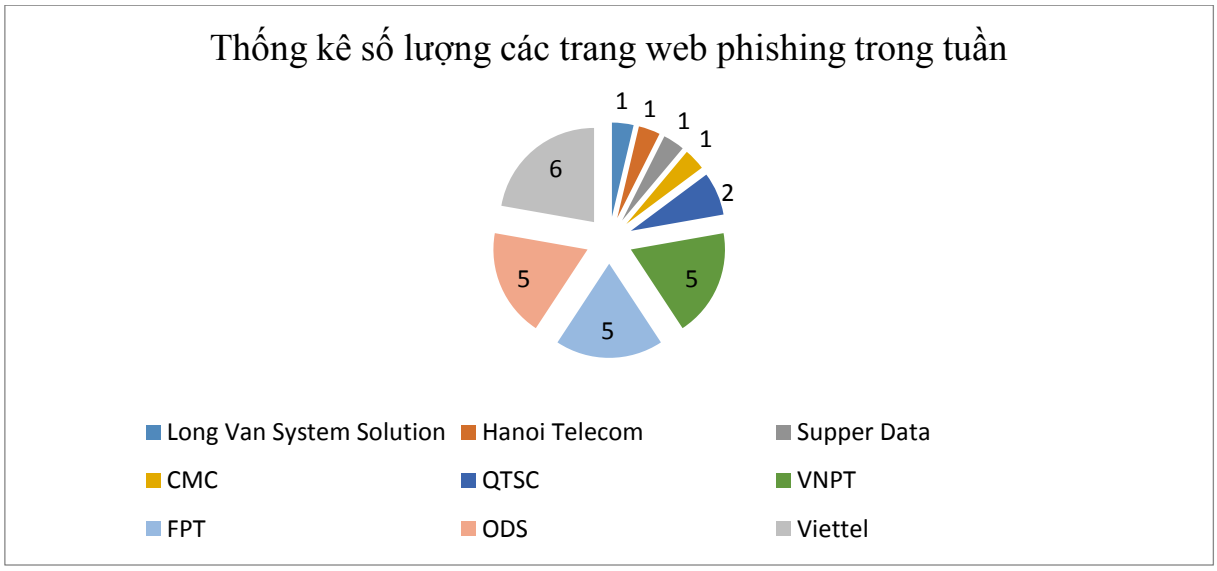
1.2. Ngày 25/01/2018, theo thông tin từ hãng tin Reuters, ba công ty phần mềm lớn là Norton, McAfee và SAP đã chấp nhận cho cơ quan chức năng của Nga kiểm tra mã nguồn các sản phẩm. Để được cung cấp sản phẩm ở thị trường Nga, một số công ty công nghệ đã đồng ý với việc chính phủ Nga dò quét, kiểm tra mã nguồn một số sản phẩm của họ. Chính phủ Nga cho rằng thực hiện kiểm tra mã nguồn để phát hiện ra các điểm yếu an toàn thông tin và khả năng có thể có mã độc cài đặt trong các sản phẩm là cần thiết để phòng, tránh các cuộc tấn công mạng.

1.3. Qua công tác giám sát và theo dõi tình hình, Cục An toàn thông tin đã phát hiện chiến dịch tấn công lừa đảo nhắm vào người sử dụng Internet Việt Nam, đặc biệt là những người dùng mạng xã hội Facebook. Những chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các mạng xã hội, các ngân hàng, các cơ sở dịch vụ lớn, 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 có Công văn số 29/CATTT-TTTV ngày 18/01/2018 gửi các cơ quan, tổ chức cảnh báo về chiến dịch tấn công lừa đảo này.

Đến thời điểm thực hiện báo cáo này, Cục An toàn thông tin đã phát hiện có ít nhất **784** tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên, danh sách các tên miền xin tham khảo tại đường dẫn https://khonggianmang.vn/warn/phishing.txt .

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

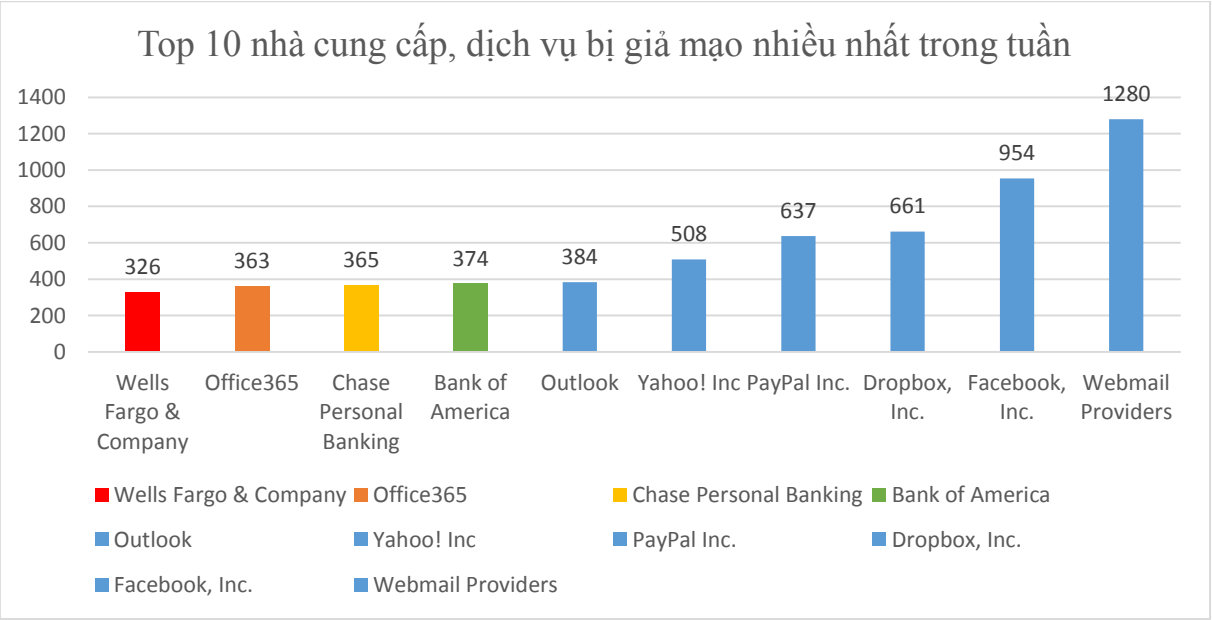
2.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, ngoài 700 tên miền đã đề cập tới ở trên, Cục ATTT còn ghi nhận có ít nhất 27 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



Danh sách các trang mạng, đường dẫn được sử dụng để tấn công lừa đảo, cụ thể như sau:

STT	Đường dẫn
1	http://adgvietnam.com/themes/corporateclean/color/logining.php
2	http://beautyhairvietnam.com.vn/ome/home_2/login.php
3	http://happynest.com.vn/wp-content/themes/unite/oracle/index.html
4	http://hela.vn/mpp/mpp/mpp/date/websc-bank.php
5	http://hoanganhvuaz.com/wp-content/themes/twentyseventeen/assets/css/images/identity.php
6	http://maihienhoangphuc.com/wp-includes/fonts/aa/index2.php?userid=
7	http://nancy.vn/wp-includes/fonts/doc/ProtectedGd/index.php
8	http://nuocuongquan2.com/css/GOOGLENEWW/GOOGLENEWW/GOOGLENEW/realestateseller/doc/work/ec
9	http://pano4you.vn/Alibaba.com/product-inquiry.html
10	http://qlbh.mipec.vn/a4b8b8c4a7/https:/www.netflix.com/login/
11	http://sgdecor.vn/wp-admin/user/bod/cod/114/chines/chines/index.php
12	http://sgdecor.vn/wp-admin/user/YAD/llc/89/chines/chines/index.php?log
13	https://hoanganhvuaz.com/wp-content/themes/twentyseventeen/assets/css/images/identity.php
14	http://sieuthinha.com/upload/embarqmail.com.html
15	http://smarthome.quangcaosangtao.vn/bitm/scheme/admin/earth.html
16	http://smarthome.quangcaosangtao.vn/Chase_Online.html
17	http://tcttruongson.vn/dropbox/5d088a92b61d5f39b6dcef1c8e33b482/
18	http://tcttruongson.vn/dropbox/a63b7bd2f5ae494d164008f085cbb1ca/
19	http://tcttruongson.vn/dropbox/c588da69d76b29f4bf8dc84e51cc9a23/
20	http://vitinhtd.com/amazon.co.uk
21	http://whitestudio.com.vn/wp-content/languages/document/n/home/index2.php
22	http://www.dalatngaynay.com/image/cdevio/index.htm
23	http://www.dalcheenivn.com/wp-admin/user/don/www.Santander.co.uk/myonlineaccounts2.abbeynational.co.uk/log3.php
24	http://www.hela.vn/mpp/mpp/mpp/date/websc-bank.php
25	http://www.hela.vn/mpp/mpp/mpp/date/websc-flowsession.php
26	http://www.ttkgroup.vn/libraries/joomla/plugin/update.html
27	http://xaydunghonngoc.com/wp-includes/js/tinymce/themes/flesh/chines/chines/index.php?login=autopure%40gmial.com

2.2. 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…



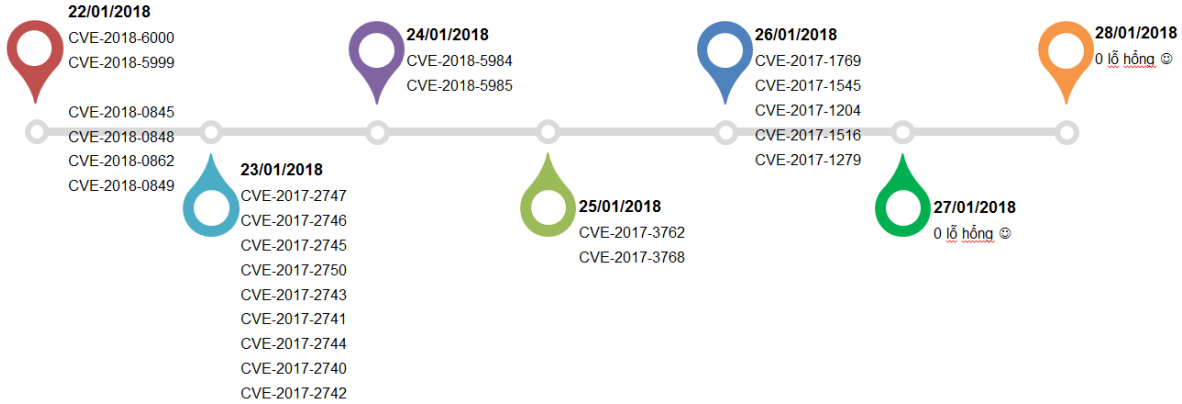
Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và có phí) như Facebook, Dropbox, Outlook .v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

3. Lỗ hổng/điểm yếu an toàn thông tin trong tuần

3.1. Trong tuần, các tổ chức quốc tế đã phát hiện và công bố ít nhất **272** lỗ hổng trong đó có: 48 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 37 lỗ hổng đã có mã khai thác.

3.2. 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 09 lỗ hổng trong sản phẩm, ứng dụng của HP; Nhóm 14 lỗ hổng trong các sản phẩm, giải pháp của IBM; Nhóm 021ỗ hổng trên các gói thành phần mở rộng của Joomla .v.v…

Thời điểm các lỗ hổng, điểm yếu này được công bố theo mốc thời gian (timeline) sau:



Các lỗ hổng có khả năng ảnh hưởng tới nhiều người dùng tại Việt Nam

3.3. 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	AsusWRT	CVE-2018-6000 CVE-2018-5999	Nhóm 02 lỗ hổng trên hệ điều hành thiết bị định tuyến của AsusWRT phiên bản trước 3.0.0.4.384_10007 cho phép đối tượng tấn công vượt qua cơ chế xác thực để thay đổi cấu hình thiết bị (bao gồm cả việc thiết lập mật khẩu tài khoản quản trị, khởi chạy tiến trình SSH cho phép truy cập từ xa)	Đã có mã khai thác Đã có thông tin bản vá
2	HP	CVE-2017-2747 CVE-2017-2746 CVE-2017-2745 CVE-2017-2750 CVE-2017-2743 CVE-2017-2741 CVE-2017-2744 CVE-2017-2740 CVE-2017-2742	Nhóm 09 lỗ hổng trong sản phẩm, ứng dụng của HP (các thiết bị máy in HP,) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau: thu thập thông tin trong hệ thống mạng, tấn công XSS thực hiện các script độc hại trong trình duyệt của người dùng, chèn và thực thi mã lệnh để kiểm soát thiết bị, Lỗ hổng CVE-2017-2741 cho phép chèn và thực thi mã lệnh đồng thời đã có mã khai thác. Nhiều dòng máy in bị ảnh hưởng như: DesignJet T790, T795, T1300, T2300, T920, T930, T1500, T1530, T2500, T2530, NEXUS_01_12_00.11 NEXUS_03_12_00.15… HP Enterprise LaserJet Printers and MFPs, HP OfficeJet Enterprise Color Printers and MFP, HP PageWide Color Printers và MPS Thiết bị máy in có kết nối mạng được sử dụng trong hầu hết các cơ quan, đơn vị nhưng rất ít khi được quan tâm đến vấn đề cập	Đã có thông tin bản vá

			nhật điểm yếu bảo mật.	
3	IBM	CVE-2017-1769 CVE-2017-1545 CVE-2017-1204 CVE-2017-1516 CVE-2017-1279 ….	Nhóm 14 lỗ hổng trong các sản phẩm, giải pháp của IBM (bao gồm:) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau như CSRF, XSS, chèn đường dẫn độc hại (đối với sản phẩm có tích hợp ứng dụng web IBM Business Process Manager, IBM Doors Web Access, IBM Cognos, IBM Integration Bus, IBM Jazz Foundation), lỗ hổng CVE-2017-1204 trong IBM Tealeaf Customer Experienc thiết lập cứng thông tin xác thực cho phép truy cập và hệ thống	2 lỗ hổng đã có mã khai thác. Đã có thông tin bản vá
4	Joomla	CVE-2018-5984 CVE-2018-5985	Nhóm 021lỗ hổng trên các gói thành phần mở rộng của hệ quản trị nội dung mã nguồn mở Joomla (gồm Tumder, LiveCRM SaaS Cloud 1.0) cho phép thực hiện tấn công SQL Injection để truy cập vào dữ liệu nhạy cảm trên hệ thống.	Chưa có thông tin bản vá Đã có mã khai thác
5	Lenovo	CVE-2017-3762 CVE-2017-3768	Nhóm 02 lỗ hổng trong sản phẩm, ứng dụng của Lenovo cho phép thực hiện tấn công khác khau, trong đó lỗ hổng CVE-2017-3762 nằm trong thành phần lưu trữ thông tin xác thực Fingerprint Manager Pro, của máy tính Lenovo (như thông tin đăng nhập và dữ liệu fingerprint…) cho phép bất cứ ai có tiếp xúc vật lý với máy tính đều có thể truy cập vào hệ điều hành một cách dễ dàng. Lỗ hổng bao gồm sử dụng giải thuật mã hóa yếu, thiết lập cứng mật khẩu. Các máy tính thường cài đặt Fingerprint Manager Pro gồm:	Đã có thông tin bản vá

			ThinkPad L560, P40 Yoga, P50s, T440, T440p, T440s, T450, T450s, T460, T540p, T550, T560, W540, W541, W550s, ThinkPad X1 Carbon (Type 20A7, 20A8, Type 20BS, 20BT), X240, X240s, X250, X260, Yoga 14 (20FY), Yoga 460, ThinkCentre M73, M73z, M78, M79, M83, M93, M93p, M93z, ThinkStation.	
6	Microsoft Office	CVE-2018-0845 CVE-2018-0848 CVE-2018-0862 CVE-2018-0849	Nhóm 04 lỗ hổng trong bộ sản phẩm Microsoft Office 2003, 2007, 2010, 2013, 2016 cho phép đối tượng tấn công chèn và thực thi mã lệnh, mã độc từ xa thông qua nhiều kịch bản khai thác khau nhau. Là các lỗ hổng CVE-2018-0805, CVE-2018-0806, CVE-2018-0807 đã được cảnh báo trước đó ngày 9/1/2018.	Đã có thông tin bản vá

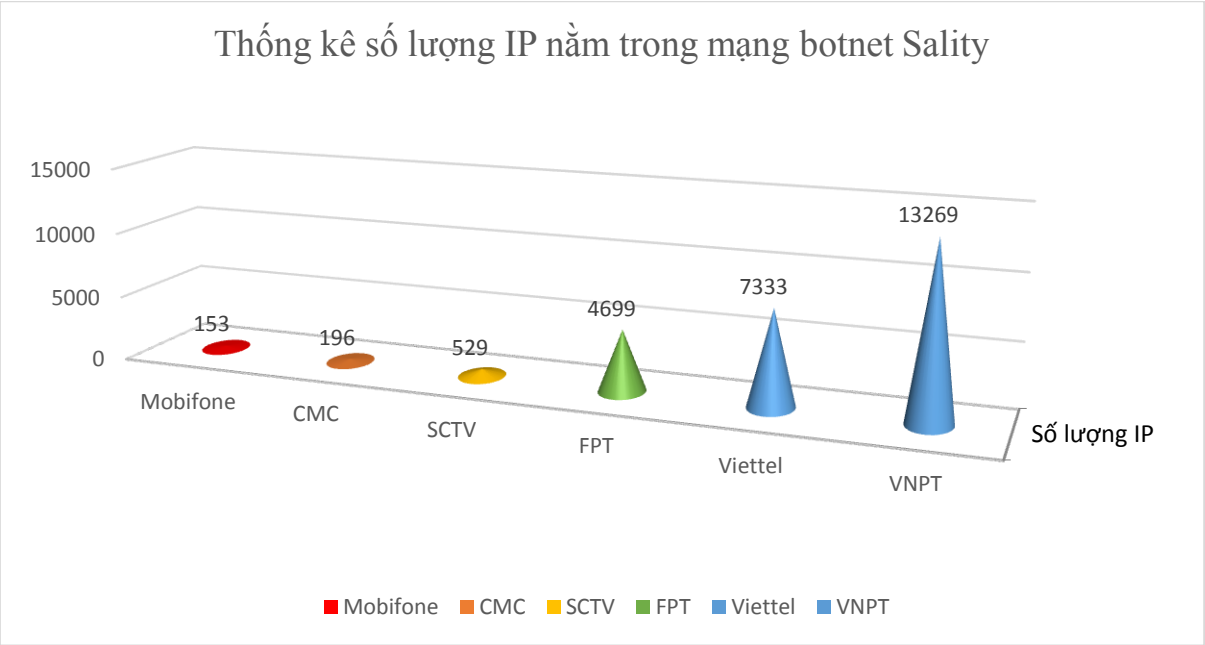
4. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

4.1. 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 thông 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.



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

TT	Tên miền/IP
1	wjobfppuakv.me
2	f3b0c2e2.com
3	ijylapa.com
4	toetomme.ddns.net
5	nugbeokokvil.com
6	ngme.yourwebfind.com
7	sihuxyfn.com
8	8-0-2-4-0-3-2-0-0-0-.0-0-0-0-0-0-0-0-0-0-0-0-0-0-18-0-0-0-0-0-0-0-0-0-0-0-0-0-0.info
9	ruwufsahn.com
10	ywuwegokskgcowec.org

5. Khuyến nghị đối với các cơ quan, đơn vị

Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan đơn vị, Cục An toàn thông tin khuyến nghị:

- 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 2.2* báo cáo này.

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 3.3* 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 4.2* 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;
- 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;

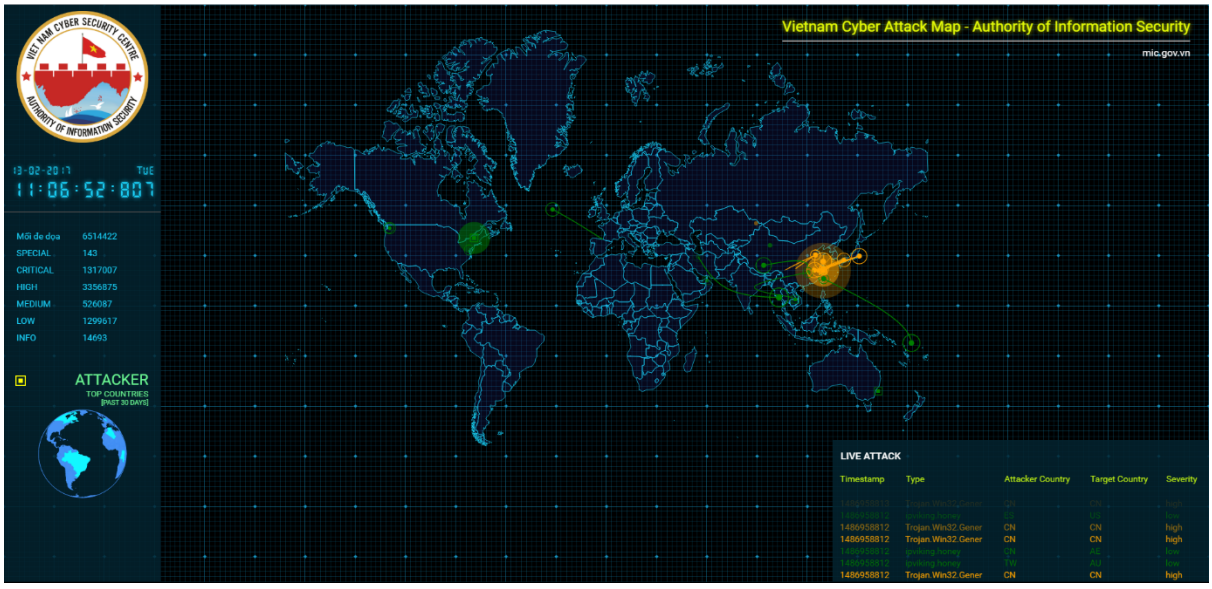
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

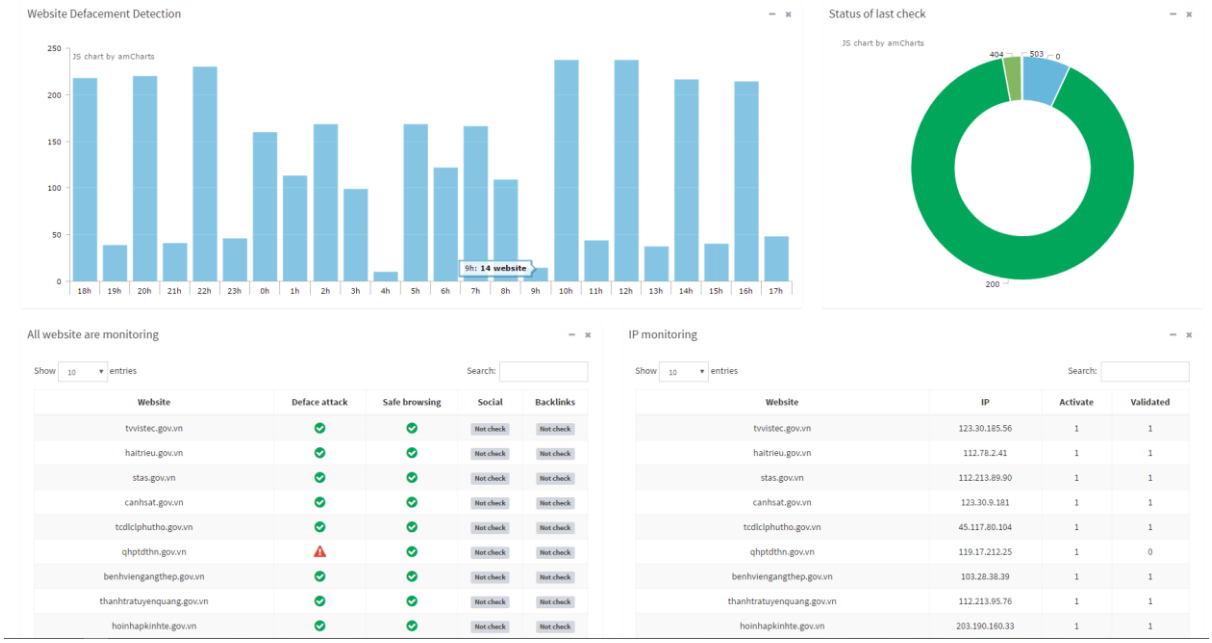
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



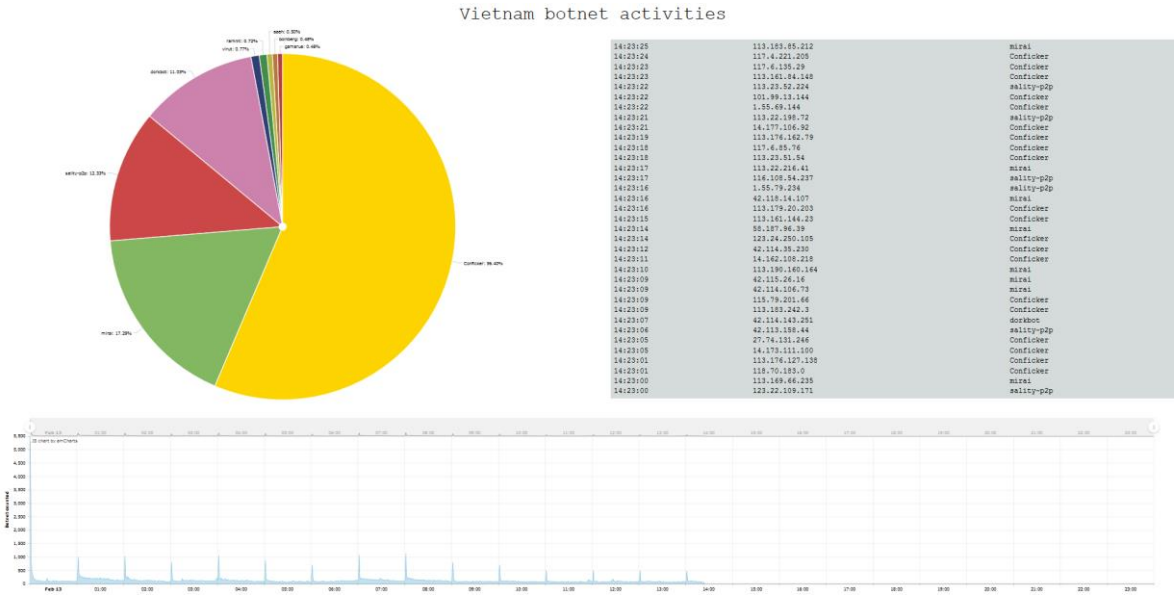
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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