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: **11**/BC-CATTT

*Hà Nội, ngày 13 tháng 03 năm 2018*

# TÓM TẮT
## Tình hình an toàn thông tin đáng chú ý trong tuần 10/2018
## (từ ngày 05/02/2018 đến ngày 11/3/2018)

**BẢNG TỔNG HỢP**

1. Ngày 07/3/2018, Bộ Công nghiệp kỹ thuật số và Sáng tạo Chính phủ Anh đã phát hành một báo cáo liên quan tới việc bảo đảm an toàn thông tin của người dùng thiết bị IoT (Internet of Things).

2. Bộ Dịch vụ nhân sinh (Department of Human Services - DHS) của Australia đã tăng gấp ba số lượng nhân viên an toàn thông tin mạng trong 12 tháng qua.

3. Trong tuần, Cục ATTT ghi nhận có ít nhất 125 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 như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc; lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động.

### 1. Điểm tin đáng chú ý

1.1. Ngày 07/3/2018, Bộ Công nghiệp kỹ thuật số và Sáng tạo, Chính phủ Anh đã phát hành một báo cáo liên quan tới việc bảo đảm an toàn thông tin của người dùng thiết bị IoT (Internet of Things).

Theo báo cáo, hiện nay, mỗi hộ gia đình ở Anh sở hữu ít nhất 10 thiết bị kết nối internet và dự kiến sẽ tăng lên 15 thiết bị vào năm 2020. Nghĩa là có thể có hơn 420 triệu thiết bị IoT được sử dụng tại Anh vào năm 2020, đồng nghĩa với việc an toàn thông tin của các thiết bị này cần phải được theo dõi và kiểm soát cho phù hợp.

Báo cáo đã đưa ra các đánh giá tổng thể và các khuyến nghị dành cho nhà sản xuất cũng như người dùng cuối, đồng thời đề xuất chính phủ xem xét để áp

đặt các quy tắc bảo đảm an toàn thông tin vào quá trình thiết kế và phát triển các sản phẩm IoT. Chính phủ Anh sẽ tiếp tục nghiên cứu, phát triển các khuyến nghị này, đây là một phần quan trọng trong Chiến lược An toàn thông tin mạng Quốc gia trong 5 năm của Chính phủ Anh, trị giá khoảng 1.9 tỷ Bảng Anh nhằm hướng tới mục tiêu đưa Vương quốc Anh trở thành nơi an toàn trên thế giới để sinh sống và kinh doanh trực tuyến.

Tại Việt Nam, những năm gần đây, các thiết bị IoT cũng đã xuất hiện trên thị trường và được nhiều người sử dụng. Cục An toàn thông tin cung cấp một số khuyến nghị dành cho người dùng về bảo đảm an toàn thông tin thiết bị IoT:

- Tìm hiểu thông tin bảo mật của một sản phẩm trước khi mua;

- Thay đổi mật khẩu và tên người dùng mặc định trong thiết bị;

- Kiểm tra trang web của nhà sản xuất để cập nhật phiên bản phần mềm, firmware (nếu có);

- Nếu có lựa chọn bảo mật định danh hai bước trở lên thì nên sử dụng.

1.2. Bộ Dịch vụ nhân sinh (Department of Human Services - DHS) của Australia đã tăng gấp ba số lượng nhân viên an toàn thông tin mạng trong 12 tháng qua.

Đối mặt với sự thiếu hụt hàng năm khoảng 500 nhân sự về an toàn thông tin mạng tại Australia, DHS đã định hình kế hoạch tuyển dụng của mình bằng cách thuê sinh viên đang theo học tại các trường để làm việc. Và để bổ sung cho kế hoạch này DHS sẽ thuê một số chuyên gia có kinh nghiệm, các chuyên gia này sẽ được phân chia thời gian để vừa làm các công việc được giao và vừa chịu trách nhiệm đào tạo nội bộ, hướng dẫn cho 03 sinh viên. Để cân băng giữa yếu tố kỹ thuật và phi kỹ thuật, nhóm chuyên gia mà DHS tuyển dụng còn bao gồm cả các nhà tâm lý học, luật sư và sinh viên tốt nghiệp các trường đào tạo về chính trị.

Lãnh đạo của DHS hy vọng chiến lược tuyển dụng này sẽ mạng lại hiệu quả trong vòng hai năm tới. Theo dự đoán thì sẽ có một số nhân sự sau khi được đào tạo sẽ rời bỏ tổ chức vì nhu cầu nhân sự trong ngành an toàn thông tin đang rất cao, tuy nhiên DHS tính toán có thể giữ được 1/3 số nhân sự đã qua đào tạo ở lại làm việc.

1.3. Ngày 06/3/2018 Kaspersky đã xác định và công bố thông tin về tấn công APT có tên Slingshot với kỹ thuật tấn công tinh vi. Theo ghi nhận, hoạt động của Slingshot xuất hiện từ năm 2012 và đến thời điểm tháng 2 năm 2018

vẫn hoạt động. Theo giám sát của Kaspersky có trên 100 hệ thống thông tin của các quốc gia khu vực Trung Đông và Châu Phi như: Kenya, Yemen, Libya, Afghanistan, Iraq, Tanzania, Jordan, Mauritius, Somalia, Cộng hòa Dân chủ Congo, Thổ Nhĩ Kỳ, Sudan và Các tiểu vương quốc Ả rập Thống nhất đã bị tấn công.

Để lây nhiễm vào máy tính nạn nhân, bước đầu tiên mã độc sẽ cố gắng thay thế một trong những thư viện liên quan tới việc cấu hình và bảo mật Windows - 'scesrv.dll' với một tập tin độc hại có cùng kích thước. Ngoài ra, nó có tương tác với nhiều thành phần quan trọng trong hệ điều hành Windows như trình nạp Ring 0 (loader), thành phần để nghe lén lưu lượng mạng ở mức nhân, hệ thống tập tin ảo và một số thành phần quan trọng khác.

Các phương thức lây nhiễm của Slingshot hiện vẫn chưa được xác định hết, nhưng có ít nhất một vài trường hợp nhóm tin tặc đã thực hiện thông qua phần mềm quản lý bộ định tuyến WinBox (như Mikrotik) để lây nhiễm vào máy tính nạn nhân.

Đây là một trong những cuộc tấn công APT được bắt đầu từ các thiết bị Router, do vậy nếu trong thời gian tới, không chỉ là các thiết bị Router mà các thiết bị IoT cũng có thể bị lợi dụng. Theo báo cáo của Kapersky thì nạn nhân của các cuộc tấn công mới chỉ tập trung ở khu vực Trung Đông và Châu Phi nhưng không loại trừ khả năng đã ảnh hưởng hoặc trong thời gian tới có thể sẽ ảnh hưởng tới Việt Nam.

Danh sách giá trị băm MD5 của các tập tin có dấu hiệu liên quan đến tấn công sử dụng Slingshot:

| TT | Giá trị băm MD5 của các tập tin có dấu hiệu liên quan đến Slingshot |
|---|---|
| 1 | 42cc382acb5b2b70c78baa77bb7c5f9 |
| 2 | 11ccc2c5811c80f2a796817d9ccbe34b |
| 3 | 142970f7e10e3a49e583b2f557dcbe79 |
| 4 | 64f705e55545a371e0f5e599cfbae5e9 |
| 5 | 6637dbcc6059a1e2e45956d98a3ea590 |
| 6 | 706269c041d94c4501b78c128f1c0e70 |
| 7 | 7fb82333aa08f4bfbbfa515e7e93bad4 |
| 8 | 87a28a99697452a37fc229b3aa3afe97 |

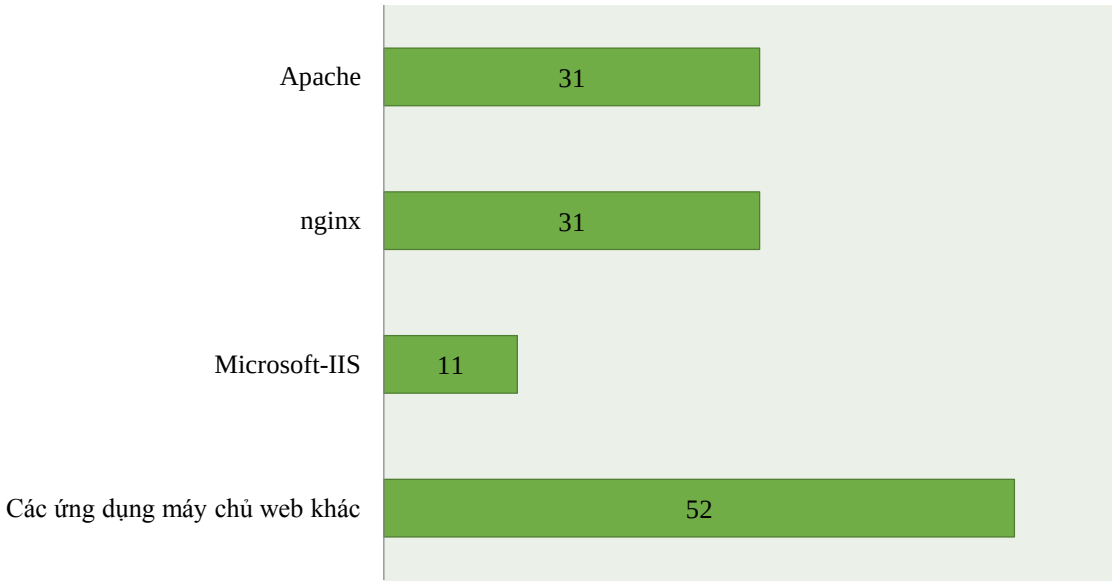
| | |
|---|---|
| 9 | afaff3310d8c094774da6ba856c1a30e |
| 10 | b7a2525e05769540f48733d5673a77fa |
| 11 | c638169aaa777d4f6eae43205a39e274 |
| 12 | db71aed3b9ffbbfa4c49db036520ceeb |
| 13 | f4944c5d47907ce93819aed8c4f76bcc |

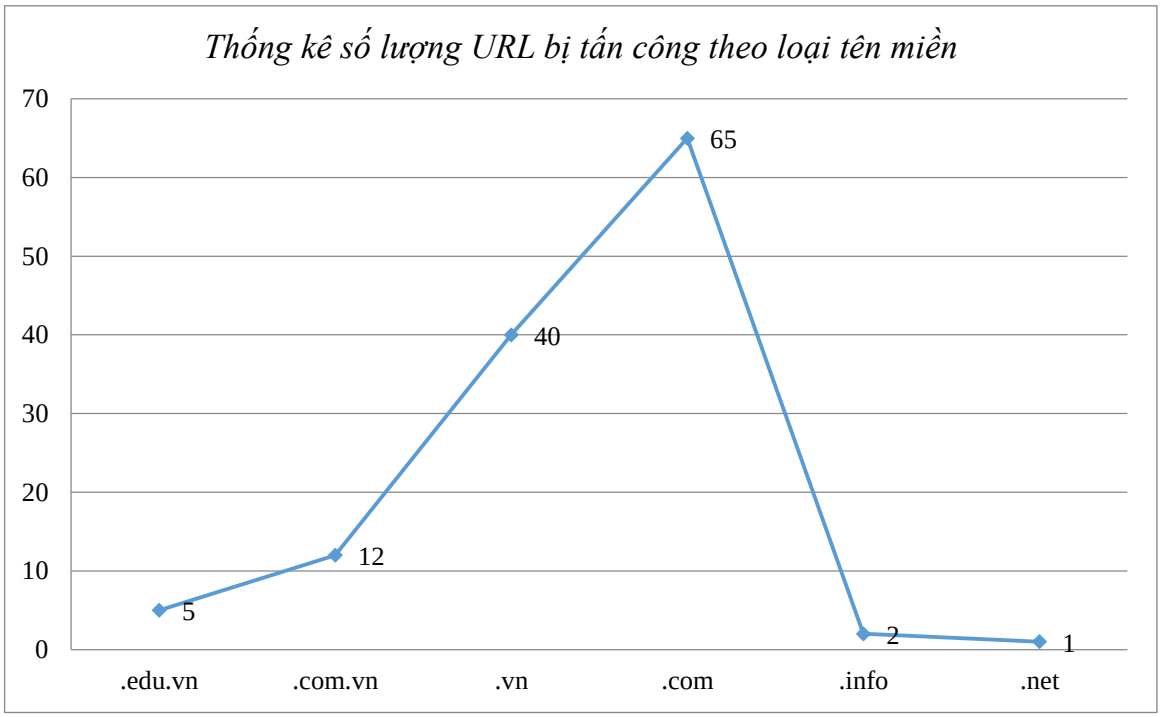
**2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam**

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 tại Việt Nam 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…).

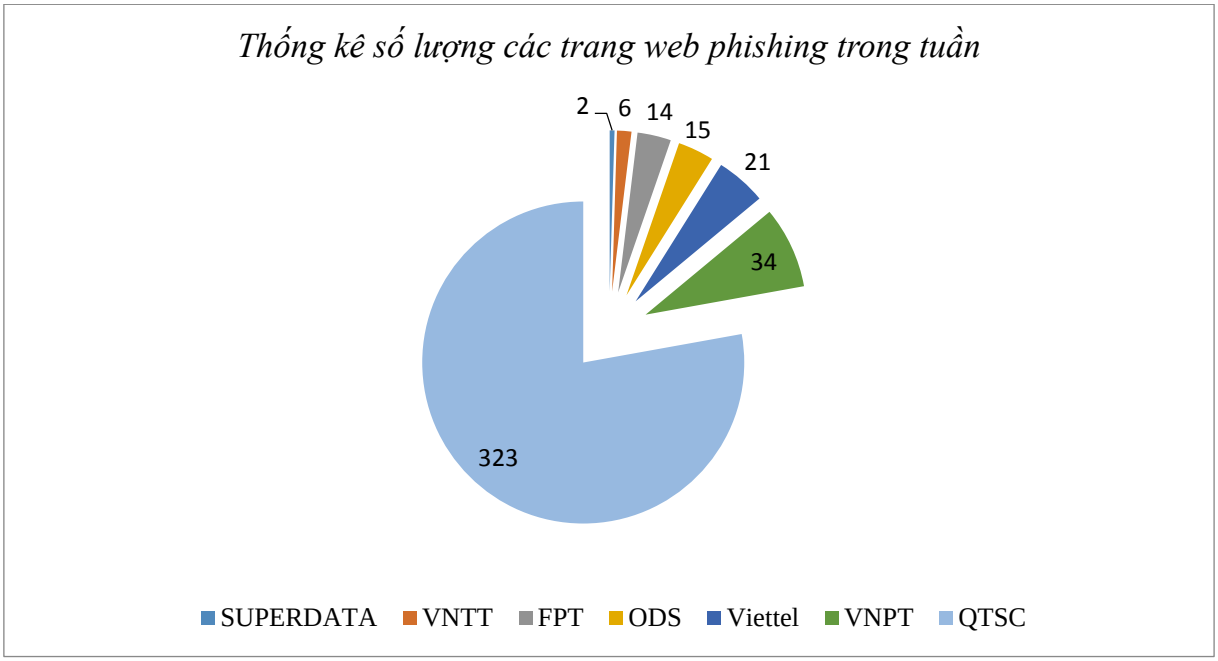
Trong tuần, Cục ATTT ghi nhận có ít nhất 125 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web ( IIS, Apache …) và loại tên miền (.com, .vn, …) cụ thể như sau:

*Thống kê số lượng URL bị tấn công theo ứng dụng máy chủ web*

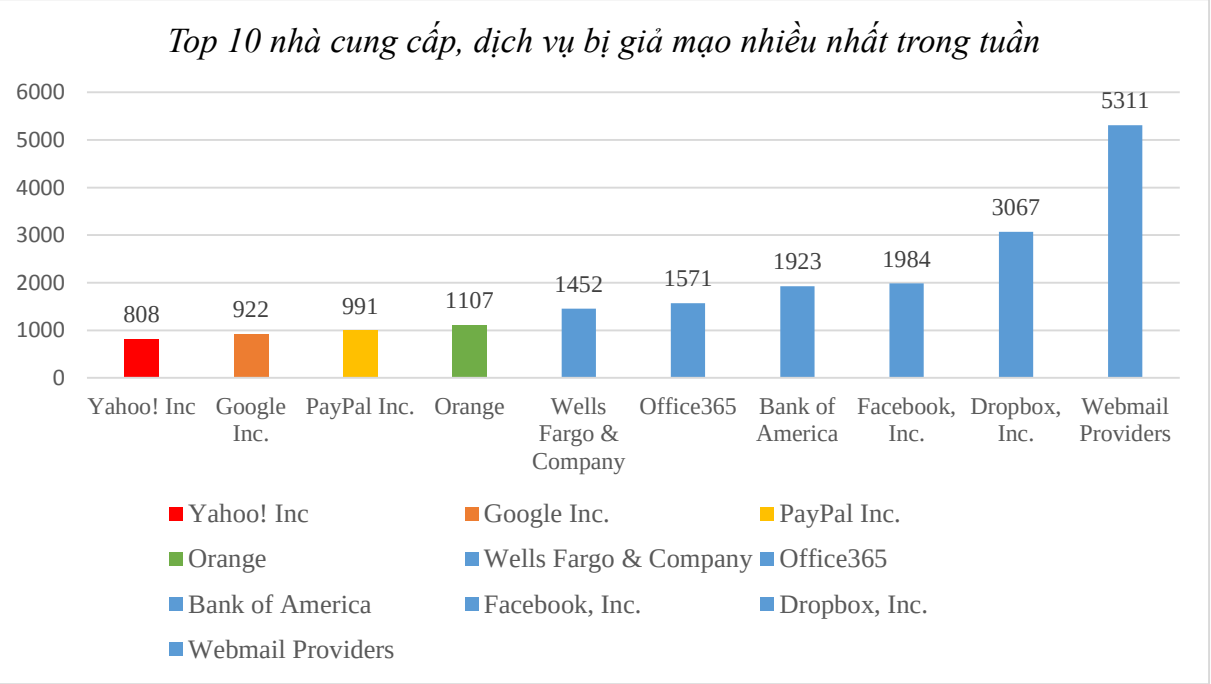





3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất 415 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.




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 phát hiện và công bố ít nhất 317 lỗ hổng trong đó có: 70 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 7 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 **04** nhóm lỗ hổng và **02** lỗ hổng riêng lẻ trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam, như: Nhóm 20 lỗ hổng, điểm yếu trên một số sản phẩm, dịch vụ của Cisco; Nhóm 2 lỗ hổng cross-site scripting trong Wordpress .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-2018-0216<br>CVE-2018-0221<br>CVE-2018-0211<br>CVE-2018-0213<br>… | Nhóm 20 lỗ hổng, điểm yếu trên một số sản phẩm, dịch vụ của Cisco (Data Center Network Manager, | Một vài lỗ hổng đã có xác nhận và thông tin bản |

| | | | | |
|---|---|---|---|---|
| | | | Identity Services Engines, Security Manager, StarOS …) cho phép thực hiện nhiều hình thức tấn công như thu thập thông tin trái phép, chèn các đoạn mã JavaScrip để lấy trộm thông tin xác thực, XSS, SQL Injection, một số lỗ hổng cho phép chèn và thực thi mã lệnh. | vá |
| 2 | Samsung | CVE-2018-6019 | Các phiên bản trước 3.02 của ứng dụng Samsung Display Solution cho Android tồn tại lỗ hổng cho phép tấn công nghe lén nội dung B2B. | Đã xác nhận và có thông tin bản vá |
| 3 | Wordpress | CVE-2018-0546<br>CVE-2018-0547<br>CVE-2018-7204 | Nhóm 2 lỗ hổng cross-site scripting trong Wordpress cho phép tấn công chèn lệnh hoặc mã HTML và lỗi trong plugin Giribaz gây lộ, lọt thông tin cấu hình | Đã xác nhận và có thông tin bản vá |
| 4 | Google Chrome | CVE-2016-5179 | Phiên bản Chrome OS trước 53.0.2785.144 cho phép kẻ tấn công thực thi lệnh khi khởi động | Đã xác nhận và có thông tin bản vá |
| 5 | Huawei | CVE-2017-17322<br>CVE-2017-17328<br>CVE-2017-17227<br>CVE-2017-17150<br>… | Các lỗ hổng điểm yếu trên nhiều sản phẩm, dịch vụ, điện thoại của Huawei cho phép thực hiện các hình thức tấn công như thực thi lệnh từ xa, thu | Đã xác nhận và có thông tin bản vá |

| | | | | |
|---|---|---|---|---|
| | | | thập thông tin trái phép, thiết bị, dịch vụ ngừng hoạt động, … | |
| 6 | D-link | CVE-2018-6529<br>CVE-2018-6527<br>CVE-2018-6528<br>CVE-2018-6530<br>… | Lỗ hổng XSS và chèn lệnh trong một số trang PHP trên một số phiên bản thiết bị router. Các lỗ hổng này cho phép kẻ tấn công truy cập hoặc thực thi trái phép mã trên các thiết bị. | Một số lỗ hổng đã có xác nhận và thông tin bản vá |

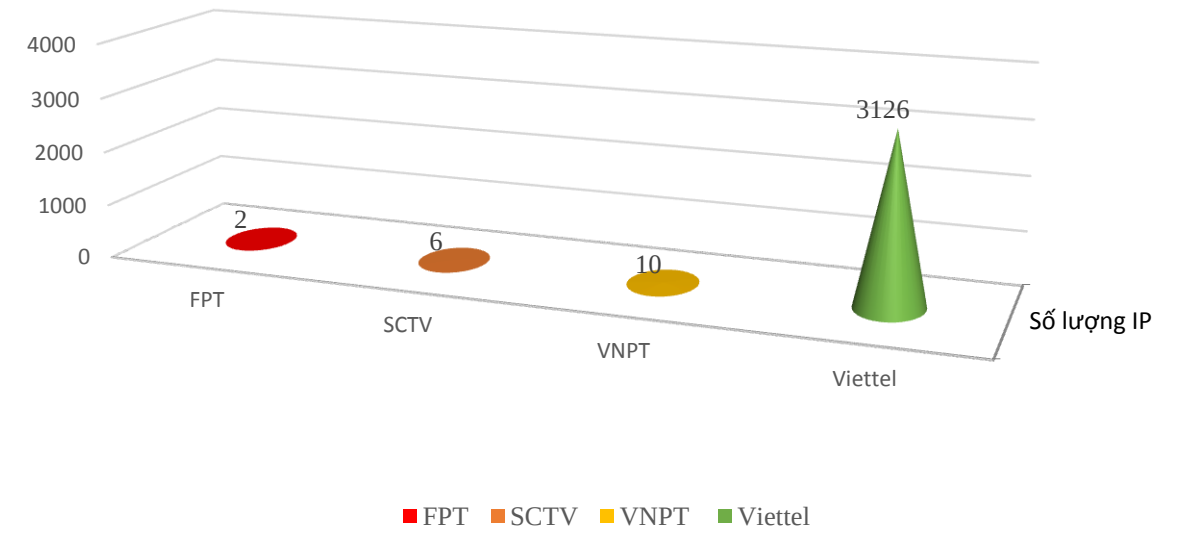
## 5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

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.

*Thống kê số lượng IP 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 | mvvyaz09js.ru |
| 2 | 104.244.14.252 |
| 3 | kukutrustnet777.info |
| 4 | 7r3xtzaao.ru |
| 5 | lbitwuh5.ru |
| 6 | mk.omkol.com |
| 7 | kukutrustnet888.info |
| 8 | g.omlao.com |
| 9 | u.amobisc.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;
- 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;

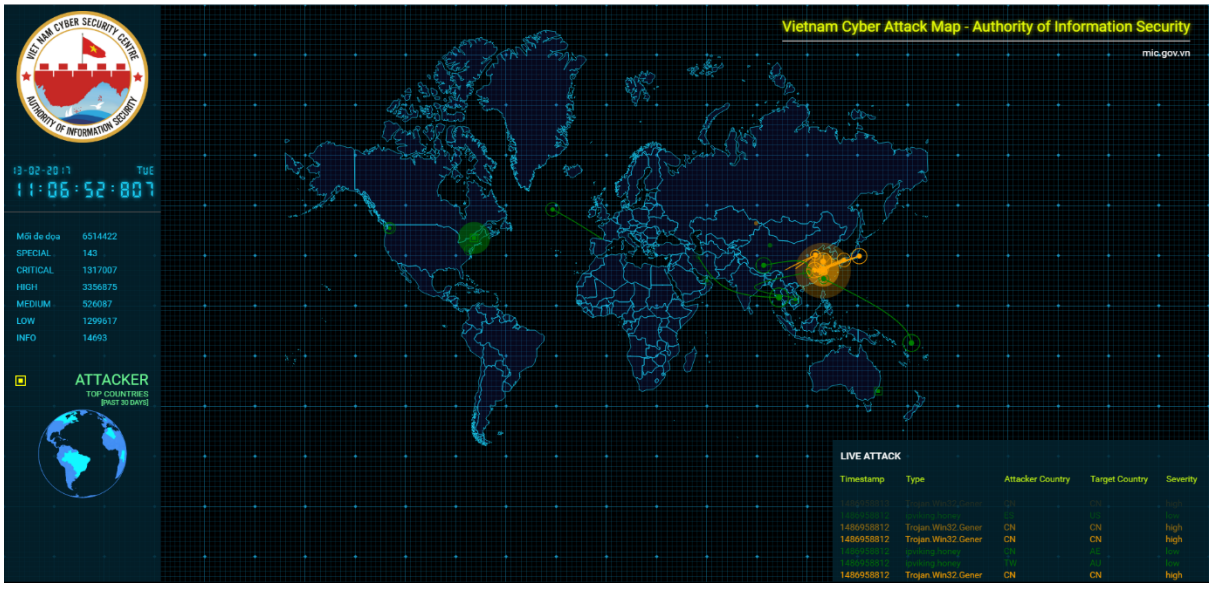
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

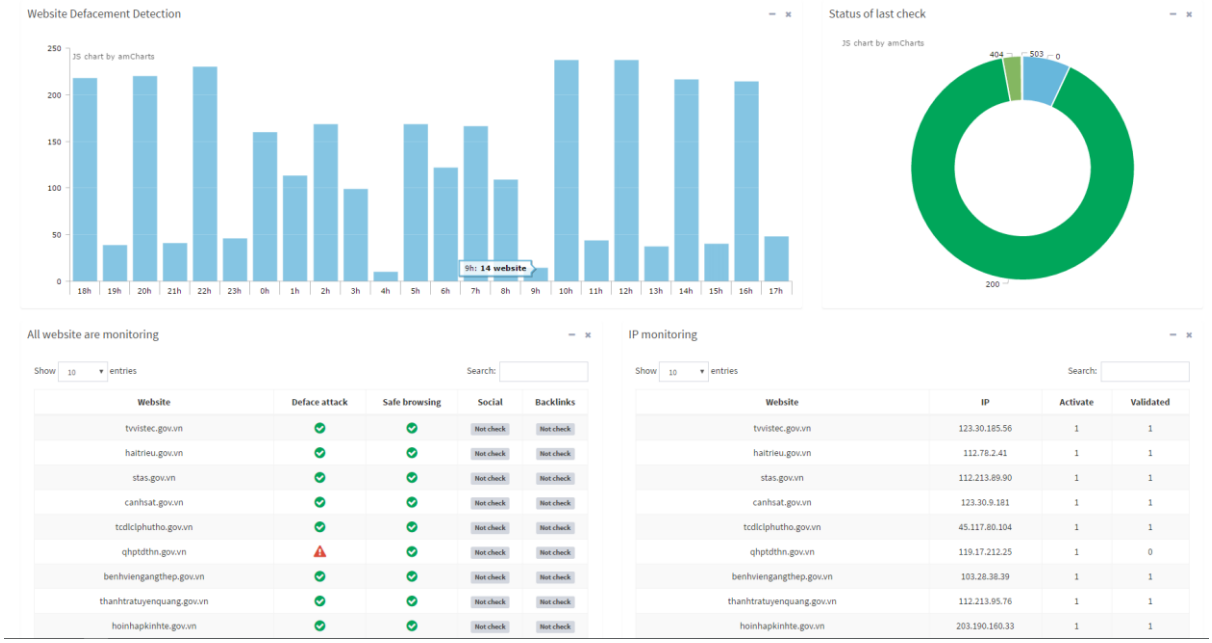
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

### *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***



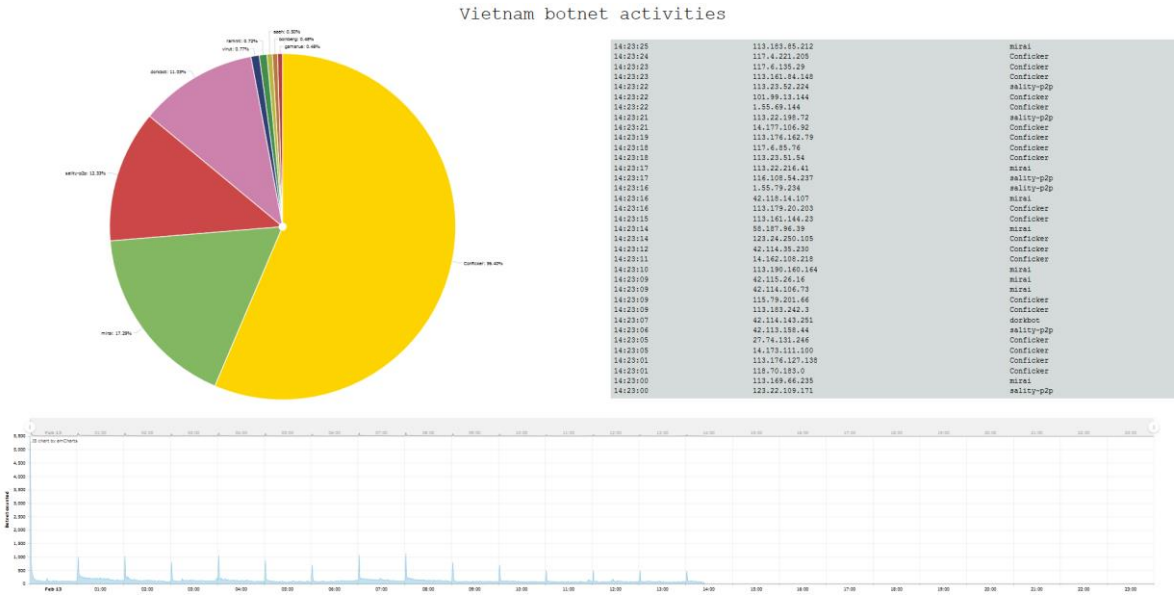

Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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