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: **15**/BC-CATTT

Hà Nội, ngày 10 tháng 4 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 14/2018
(từ ngày 02/4/2018 đến ngày 08/4/2018)

BẢNG TỔNG HỢP

1. Ngày 04/4/2018, Chính phủ Bulgaria thông qua việc tham gia vào các bản ghi nhớ về tổ chức, chức năng của Trung tâm hợp tác phòng vệ trên Không gian mạng CCDCE (Cooperative Cyber Defence Centre of Excellence).

2. 04 công ty vận hành đường ống dẫn khí đốt của Hoa Kỳ cho biết hệ thống thông tin của các công ty này đã bị gián đoạn trong vài ngày qua, và xác nhận gián đoạn dịch vụ là do một cuộc tấn công mạng.

3. Trong tuần, Cục ATTT ghi nhận có ít nhất 239 đường dẫn (URL) trên các trang web 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 04/4/2018, Chính phủ Bulgaria thông qua việc tham gia vào các bản ghi nhớ về tổ chức, chức năng của Trung tâm hợp tác phòng vệ trên Không gian mạng CCDCE (Cooperative Cyber Defence Centre of Excellence).

CCDCE là một trung tâm bảo vệ an toàn không gian mạng được quốc tế công nhận, tập trung vào nghiên cứu, đào tạo và diễn tập. Tổ chức này có trụ sở tại thủ đô Tallinn của Estonia. Trung tâm này hiện có 18 quốc gia thành viên và 4 nước khác là Bulgaria, Rumani, Na Uy và Thụy Sỹ đang tham gia đàm phán gia nhập. Nhiệm vụ chính của Trung tâm là tăng cường năng lực, hợp tác và trao đổi thông tin giữa các quốc gia thành viên, và các quốc gia đối tác trong lĩnh vực an toàn thông tin mạng. Trước đó, ngày 12/1/2018 Thủ tướng Nhật Bản Shinzo

Abe đã thông báo trong chuyến thăm Estonia của mình quyết định Nhật Bản sẽ sớm tham gia vào CCDCE.

1.2. Ít nhất 04 công ty vận hành đường ống dẫn khí đốt của Hoa Kỳ cho biết hệ thống thông tin của các công ty này đã bị gián đoạn trong vài ngày qua, và xác nhận gián đoạn dịch vụ là do một cuộc tấn công mạng.

Ngày nay, các hệ thống thông tin trong các ngành thuộc lĩnh vực năng lượng như: khí đốt tự nhiên, lưới điện .v.v… ngày càng trở nên phổ biến thì các cuộc tấn công vào các hệ thống này sẽ có ảnh hưởng ngày càng lớn tới cuộc sống của người dân.

1.3. Điểm yếu an toàn thông tin có mã lỗi quốc tế là CVE-2018-9843 ảnh hưởng tới ứng dụng CyberArk Enterprise Password Vault cho phép đối tượng tấn công thực thi mã lệnh từ xa.

CyberArk là một công cụ bảo mật và quản lý mật khẩu, kiểm soát các tài khoản đặc quyền được sử dụng khá phổ biến tại Việt Nam. Lỗ hổng trên được tìm ra bởi nhóm các nhà nghiên cứu bảo mật người Đức RedTeam Pentesting GmbH. Lỗi này là do cách xử lý không an toàn của máy chủ web đối với các hoạt động chuyển đổi (deserialization), có thể cho phép kẻ tấn công thực thi mã trên máy chủ đang xử lý dữ liệu chuyển đổi.

Cụ thể, khi người dùng đăng nhập vào tài khoản, ứng dụng sẽ gửi yêu cầu xác thực đến máy chủ (chứa thông tin xác thực về phiên của người dùng được mã hoá ở định dạng base64). Tuy nhiên, do máy chủ không xác minh tính toàn vẹn của dữ liệu đã chuyển đổi và xử lý thiếu an toàn các hoạt động chuyển đổi nên đối tượng tấn công có thể khai thác mã xác thực để chèn mã độc hại vào yêu cầu xác thực và từ đó có thể thực thi mã lệnh từ xa trên máy chủ web.

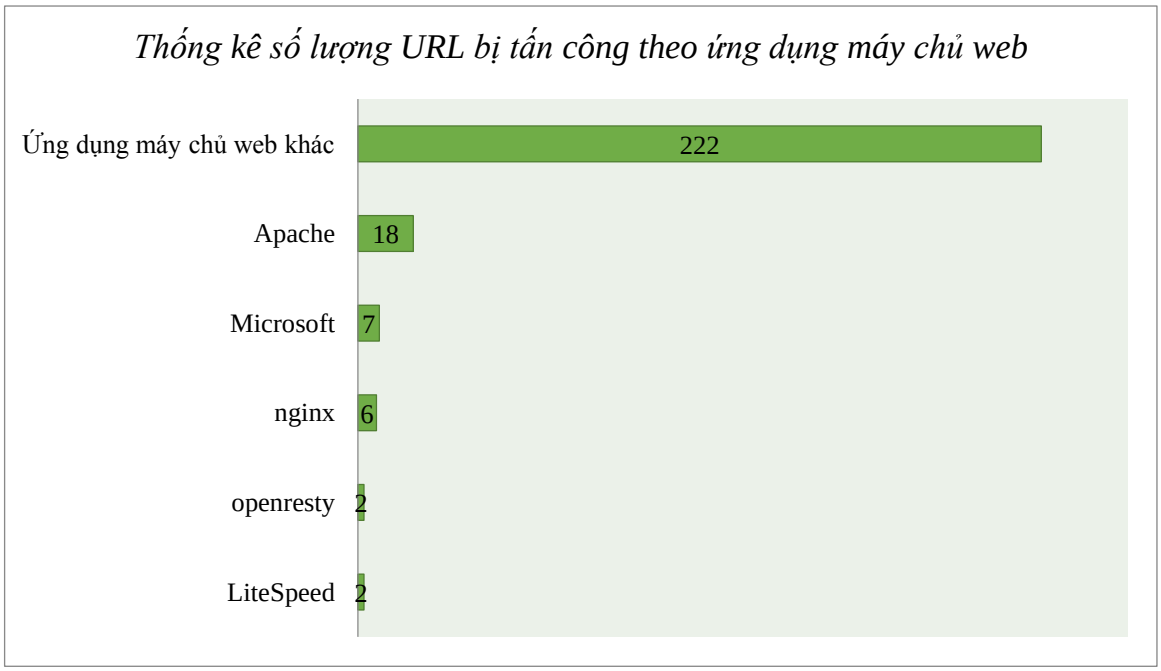
Tổ chức và cá nhân sử dụng giải pháp CyberArk Password Vault Web Access cần nâng cấp phần mềm lên phiên bản 9.9.5, 9.9.10 hoặc 10.2 để giảm thiểu nguy cơ bị tấn công thông qua lỗ hổng này.

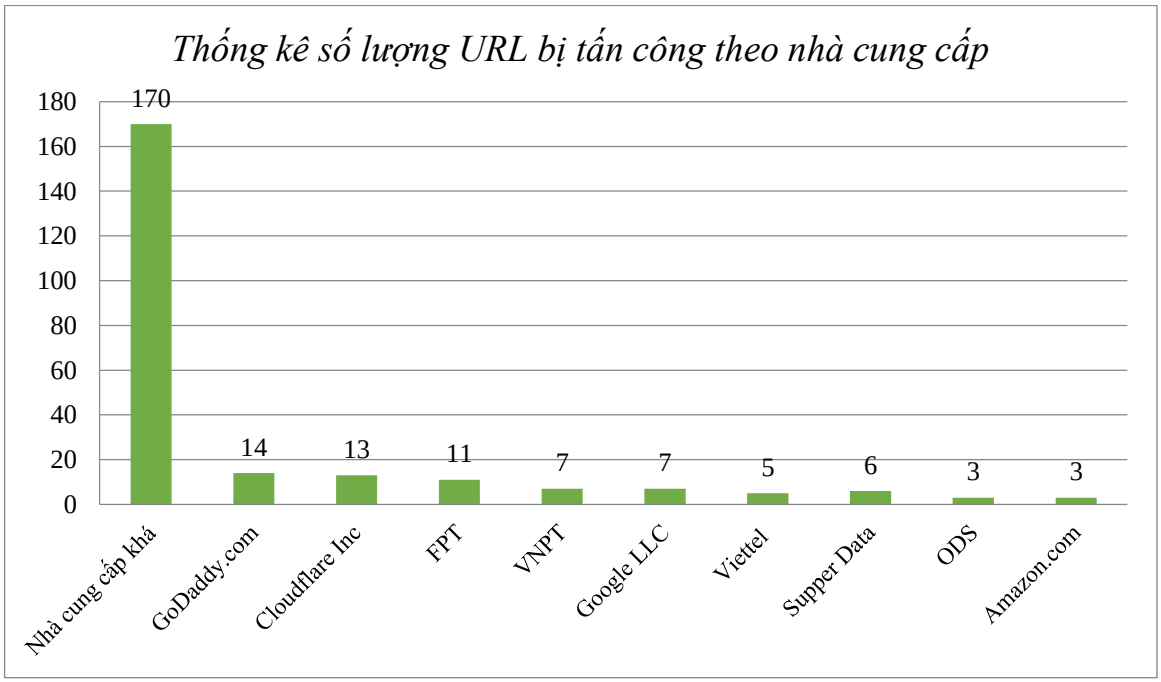
2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

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…).

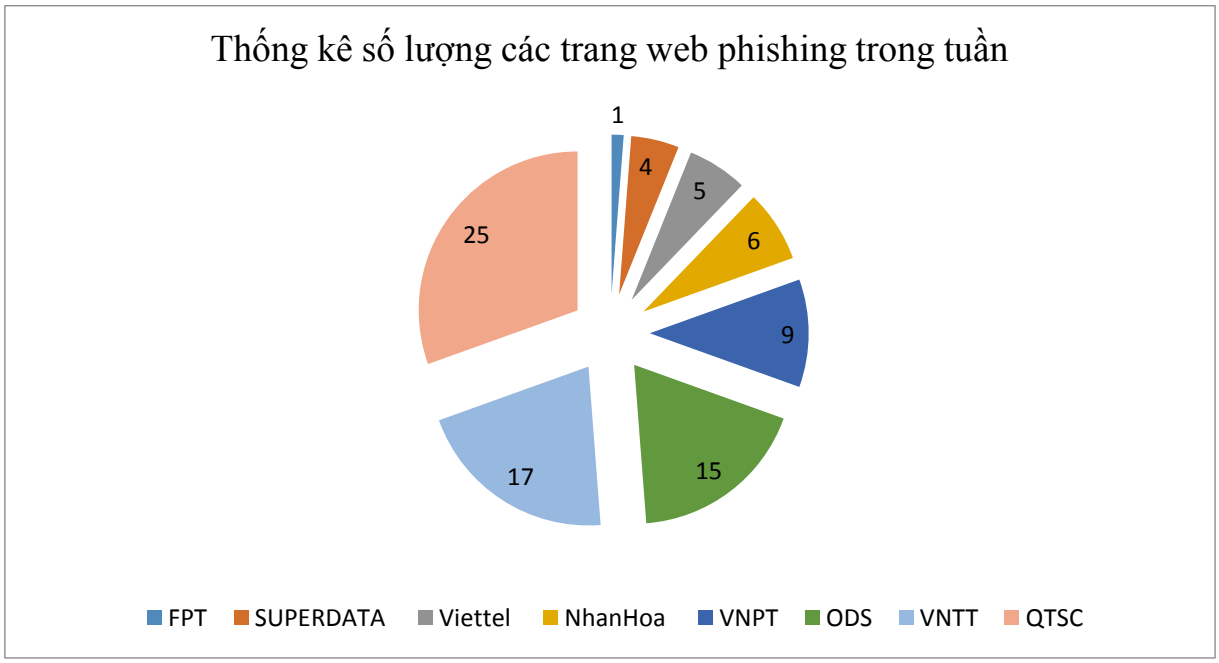
Trong tuần, Cục ATTT ghi nhận có ít nhất 194 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và nhà cung cấp cụ thể như sau:



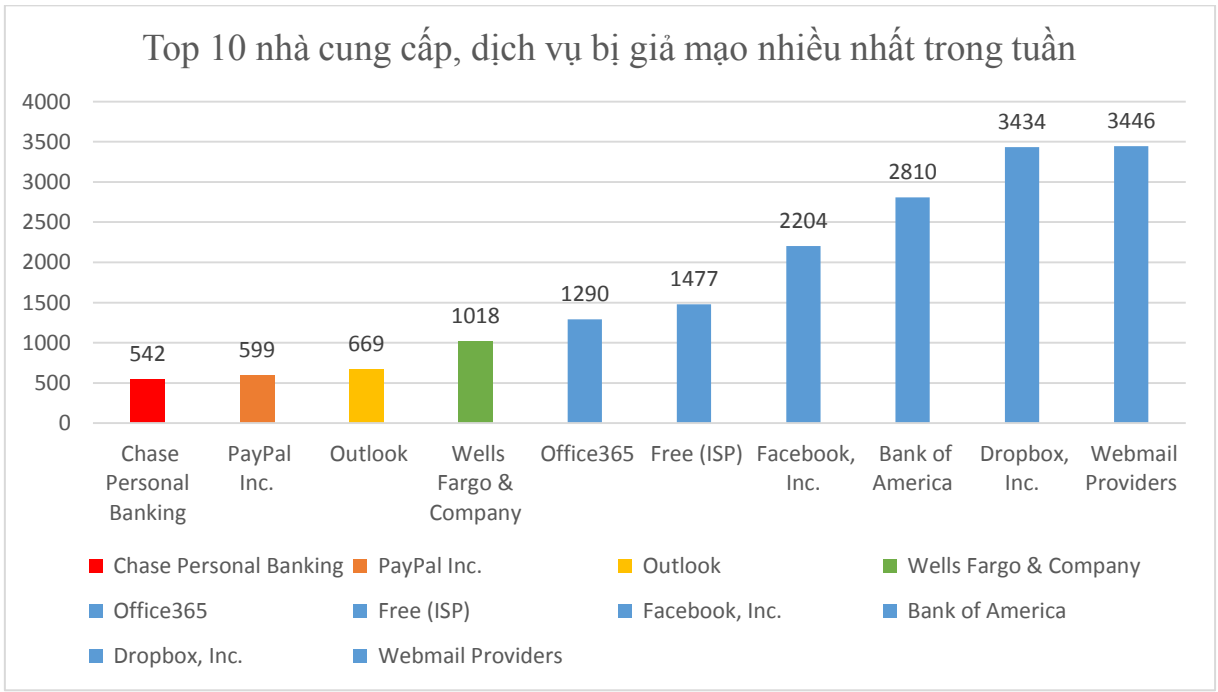


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất 82 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 462 lỗ hổng trong đó có ít nhất 18 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 17 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 120 lỗ hổng bảo mật trên các sản phẩm, dịch vụ của Apple; Nhóm 60 lỗ hổng trên một số thành phần của hệ điều hành nguồn mở Android .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-2017-7065 CVE-2018-4158 CVE-2018-4100 CVE-2017-7002 CVE-2018-4174 ...	Nhóm 120 lỗ hổng bảo mật trên các sản phẩm, dịch vụ của Apple (một số phiên bản hệ điều hành iOS, macOS, tvOS, watchOS, trình duyệt Safari) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau trong đó có nhiều lỗ hổng cho phép chèn và thực thi mã lệnh, một số lỗ hổng đã có mã khai thác gồm CVE-2018-4087, CVE-2017-7004, CVE-2017-7005.	Đã có thông tin bản vá
2	Asus - Router	CVE-2018-9285	Lỗ hổng trên một số dòng thiết bị Router của Asus (bao gồm: ASUS RT-AC66U, RT-AC68U, RT-AC86U, RT-AC88U, RT-AC1900, RT-AC2900, RT-AC3100, ASUS RT-N18U, RT-AC87U, RT-AC3200, RT-AC5300) cho phép đối tượng tấn công thực hiện chèn các lệnh của hệ điều hành từ đó có thể kiểm soát thiết bị và thực hiện nhiều hình	Thông tin bản vá theo dõi và tìm kiếm tại: https://www.asus.com/sg/Networking/RT-AC88U/HelpDesk_

			thức tấn công sâu hơn.	BIOS/
3	Axis - IP camera	CVE-2018-9158 CVE-2018-9156 CVE-2018-9157	Nhóm 03 lỗ hổng trên firmware của một số dòng thiết bị IP camare của Axis (gồm AXIS M1033-W, AXIS P1354) cho phép đối tượng tấn công đưa tập tin độc hại lên thiết bị, lợi dụng thiết bị để thực hiện những cuộc tấn công khác cũng như kiểm soát thiết bị.	Chưa có thông tin xác nhận và bản vá
4	D-link	CVE-2018-5708 CVE-2018-9284 CVE-2018-5708 CVE-2018-8941	Nhóm 03 lỗ hổng trên một số dòng thiết bị của Dlink cho phép đối tượng tấn công chèn và thực thi mã lệnh, và lỗ hổng không mã hóa thông tin xác thực (username, password) cho phép lấy được thông tin quản trị thiết bị dễ dàng.	Đã có mã khai thác, Chưa có thông tin bản vá.
5	Google - Android	CVE-2017-13261 CVE-2017-13288 CVE-2017-13268 CVE-2017-13298 CVE-2017-13259 CVE-2017-13260 ….	Nhóm 60 lỗ hổng trên một số thành phần hệ điều hành nguồn mở Android cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau trong đó có nhiều lỗ hổng cho phép chèn và thực thi mã lệnh và đã có mã khai thác như CVE-2017-13260, CVE-2017-13258.	Một số lỗ hổng đã có mã khai thác Đã có thông tin xác nhận và bản vá.
6	Microsoft	CVE-2018-0986 CVE-2018-1038	02 lỗ hổng trên thành phần Microsoft Forefront, Microsoft Defender và Windows kernel của một số phiên bản hệ điều hành Windows cho phép đối tượng tấn công chèn và thực thi mã lệnh, trong đó lỗ hổng CVE-2018-0986 đã có mã khai thác.	Đã có thông tin xác thực và bản vá.

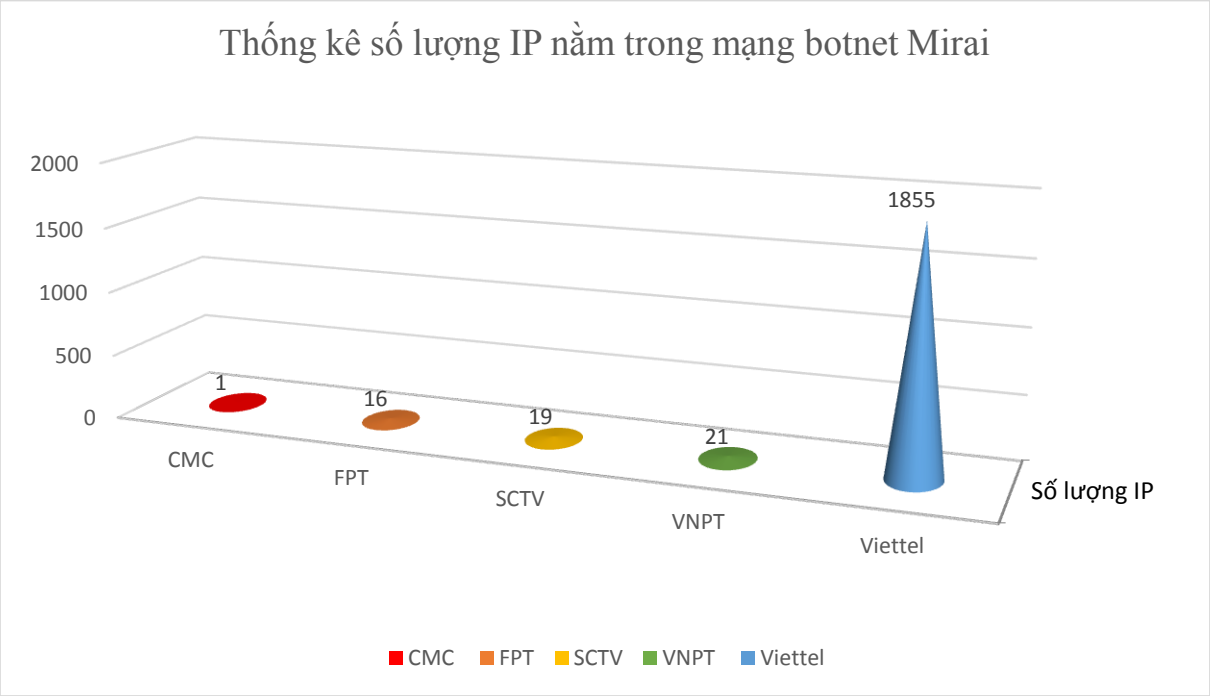
5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

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.



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

TT	Tên miền/IP
1	c84c8098.com
2	jilomet.at
3	2wtzvityfah.com
4	oaksdjhtuenhed.net
5	sonic4us.ru
6	theyunandisavowgove.ru
7	sdffd.com
8	qhcqvdmp.ru
9	kukutrustnet777.info
10	09wb2knotg.ru

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;

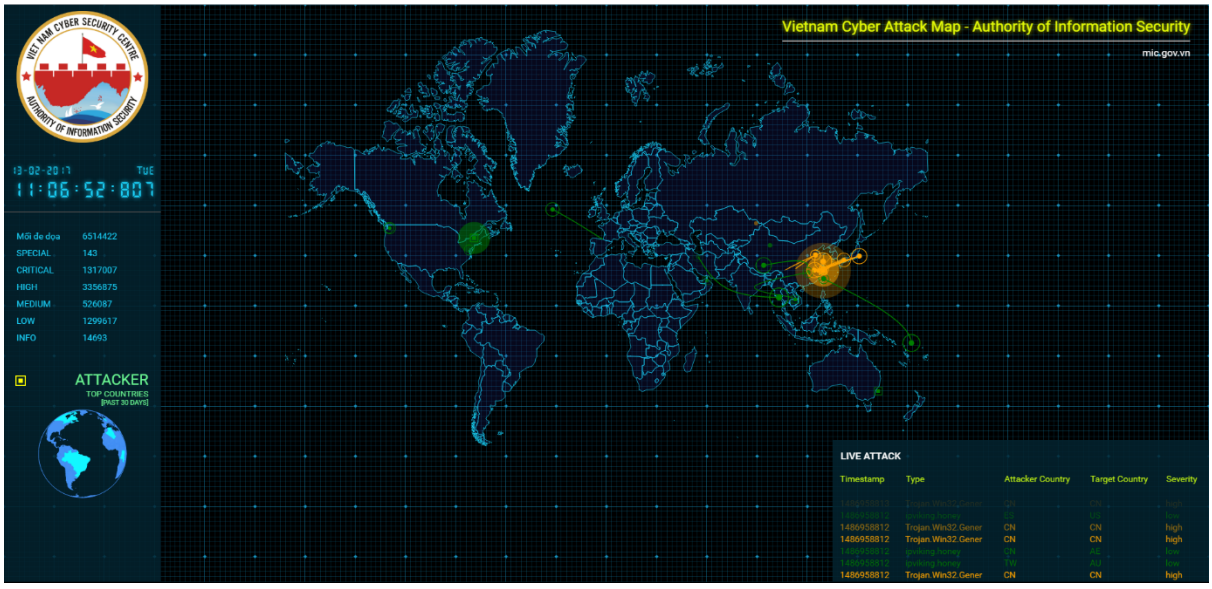
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- 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:

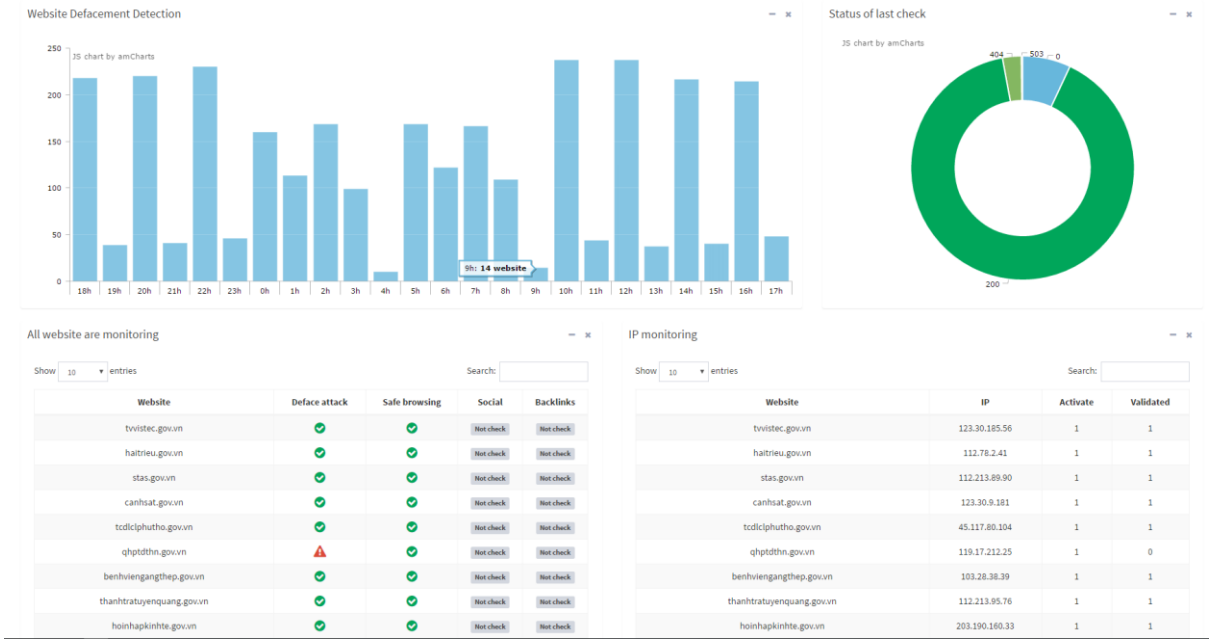
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



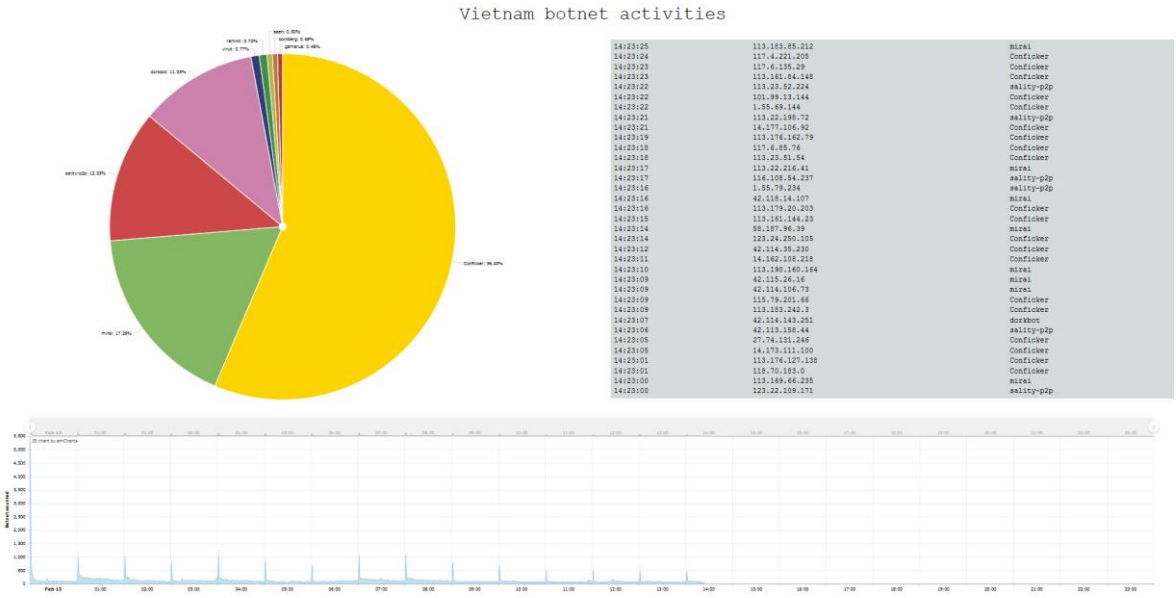
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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