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: **60**/BC-CATTT

*Hà Nội, ngày 12 tháng 12 năm 2017*

# TÓM TẮT
## Tình hình an toàn thông tin đáng chú ý trong tuần 49/2017 (từ ngày 04/12/2017 đến ngày 10/12/2017)

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 49/2017 (từ ngày 04/12/2017 đến ngày 10/12/2017), 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. Doanh nghiệp công nghệ Trung Quốc đầu tư cho an toàn thông tin nhiều hơn 23,5% so với mức trung bình trên thế giới.

2. Ngày 06/12/2017, Microsoft đã công bố các điểm yếu an toàn thông tin có thể ảnh hưởng đến các sản phẩm bảo đảm an toàn thông tin của Microsoft bao gồm: Windows Defender; Microsoft Security Essentials; Microsoft Forefront Endpoint Protection; Microsoft System Center Endpoint Protection; Windows Intune Endpoint Protection.

3. Trong tuần ghi nhận 05 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. Kết quả khảo sát công bố ngày 07/12/2017 của PwC cho thấy các doanh nghiệp công nghệ Trung Quốc đang chú trọng đặc biệt tới đầu tư cho an toàn thông tin, với mức đầu tư cao hơn 23,5% so với mức trung bình trên thế giới, thuộc nhóm dẫn đầu. Đặc biệt, các doanh nghiệp Trung Quốc chú trọng đầu tư cho lĩnh vực an toàn thông tin với thiết bị IoTs. Song song với việc quan tâm đầu tư, có ngày càng nhiều các doanh nghiệp tuyển dụng giám đốc nhân sự chuyên trách (CISO – Chief Information Security Officer).

1.2. Ngày 06/12/2017, Microsoft đã công bố các điểm yếu an toàn thông tin nghiêm trọng trên các sản phẩm bảo đảm an toàn thông tin của Microsoft bao gồm: Windows Defender; Microsoft Security Essentials; Microsoft Forefront Endpoint Protection; Microsoft System Center Endpoint Protection; Windows Intune Endpoint Protection. Các điểm yếu an toàn thông tin có mã lỗi quốc tế là CVE-2017-11937 và CVE-2017-11940 cho phép chèn và thực thi mã lệnh từ đó đối tượng tấn công có thể tấn công chiếm quyền điều khiển máy tính của nạn nhân. Đến thời điểm thực hiện báo cáo này, Microsoft vẫn chưa đưa ra bản vá cập nhật cho các điểm yếu trên. Cục An toàn thông tin khuyến nghị người dùng cuối và quản trị viên tại các cơ quan, tổ chức liên tục theo dõi, cập nhật tình hình từ Microsoft đối với 2 điểm yếu trên qua các đường dẫn sau:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11937

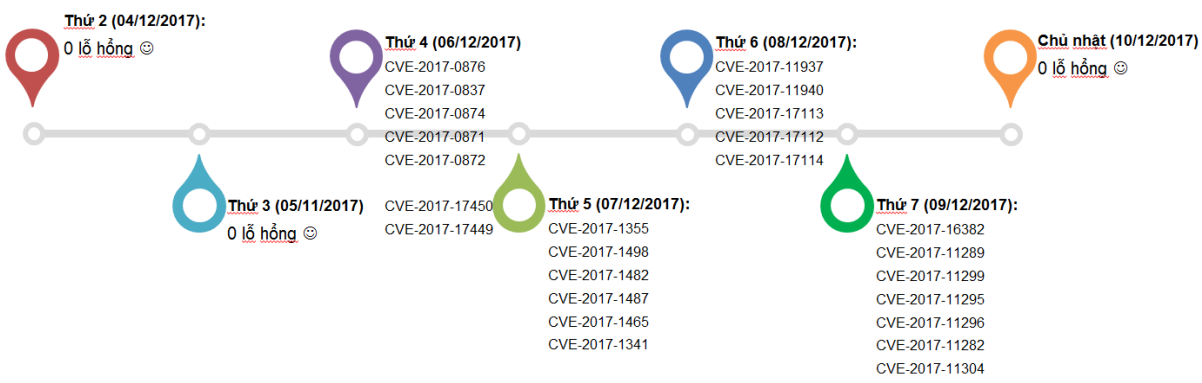
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11940

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

2.1. Trong tuần 49/2017, các tổ chức quốc tế đã phát hiện và công bố ít nhất **313** lỗ hổng, trong đó có **07** lỗ hổng đã có mã khai thác, **37** lỗ hổng cho phép chèn và thực thi mã lệnh.

2.2. 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 **05** 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 30 lỗ hổng hệ điều hành Android; Nhóm 05 lỗ hổng trên các dịch vụ, ứng dụng của hệ điều hành Windows .v.v…

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




*Hình 2: Các lỗ hổng có khả năng ảnh hưởng tới nhiều người dùng tại Việt Nam*

2.3. 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 | Adobe | CVE-2017-16382<br>CVE-2017-11289<br>CVE-2017-11299<br>CVE-2017-11295<br>CVE-2017-11296<br>CVE-2017-11282<br>CVE-2017-11304<br>… | Nhóm 88 lỗ hổng trên các sản phẩm, phần mềm của Adobe (bao gồm Adobe Connect, Adobe Acrobat và Reade, Adobe Digital Editions, Adobe DNG Converter, Adobe Flash Player, Adobe InDesign, Adobe Photoshop, Adobe Shockwave) cho phép thực hiện nhiều hình thức tấn công khác nhau như: lỗ hổng CVE-2017-1639, CVE-2017-16410 trong Adobe Reader và Acrobat cho phép chèn và thực thi mã lệnh, lỗ hổng CVE-2017-11294 trong Adobe Shockwave cũng cho phép thực thi mã lệnh | Đã có mã khai thác.<br>Đã có bản vá |
| 2 | Google - Android | CVE-2017-0876<br>CVE-2017-0837<br>CVE-2017-0874<br>CVE-2017-0871<br>CVE-2017-0872 | Nhóm 30 lỗ hổng hệ điều hành Android cho phép thực hiện nhiều hình thức tấn công khác nhau bao gồm: tấn công leo thang thông qua các trình điều khiển (SCSI, MediaTek, video v4l2…) đặc biệt cho phép chèn và thực thi mã lệnh thông qua libmpeg2, libavc, | Đã có bản vá |

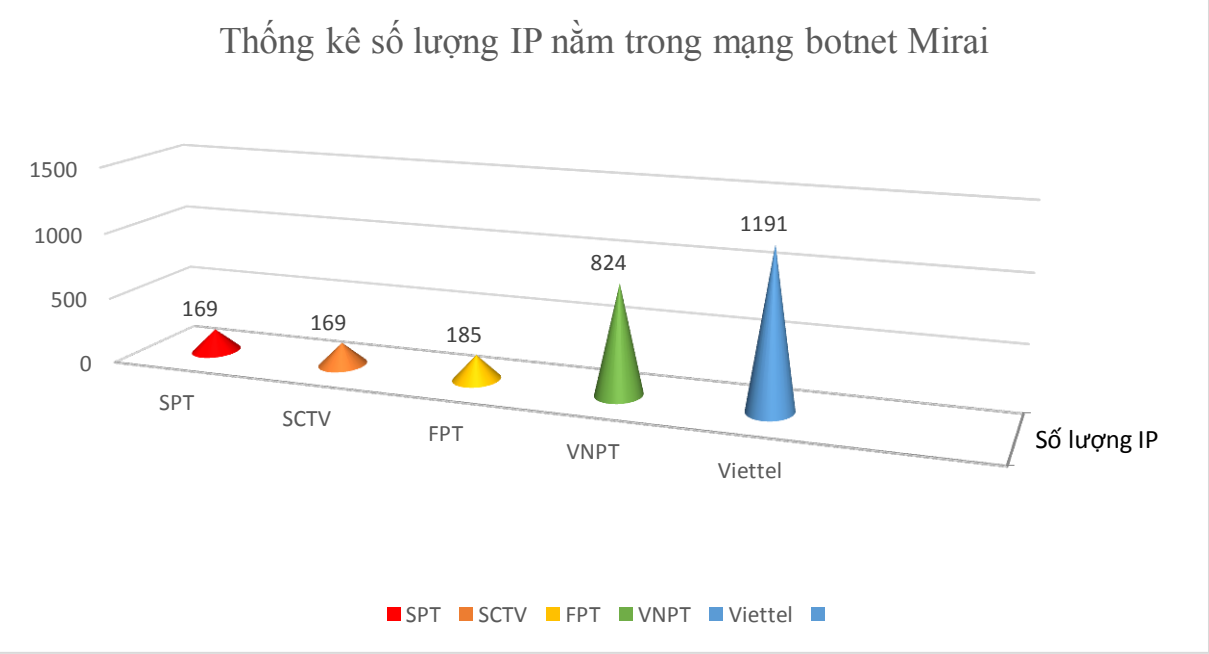
| | | | | |
|---|---|---|---|---|
| | | | libskia (các thành phần để xử lý video) | |
| 3 | IBM | CVE-2017-1355<br>CVE-2017-1498<br>CVE-2017-1482<br>CVE-2017-1487<br>CVE-2017-1465<br>CVE-2017-1341 | Nhóm 15 lỗ hổng trong các giải pháp, sản phẩm của IBM (bao gồm: Atlas eDiscovery Process Management, IBM Connections, Sterling B2B Integrator Standard Edition, Sterling File Gateway, WebSphere, Security Guardium…) cho phép ăn trộm thông tin nhạy cảm, chèn mã lệnh, chuyển hướng người dùng đến các trang độc hại, tấn công SQL Injection... | Đã có bản vá |
| 4 | Linux-Kernel | CVE-2017-17450<br>CVE-2017-17449 | Nhóm các lỗ hổng trong nhân các hệ điều hành Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, tấn công leo thang để chiếm tài khoản cao nhất trên hệ thống. thi mã lệnh.<br>Các lỗ hổng ảnh hưởng tới các phiên bản Samba 4.x và trước 4.7.3 trên tất cả hệ điều hành Linux bao gồm cả Ubuntu, Redhat, Debian, Centos …. | Đã có bản vá |
| 5 | Microsoft | CVE-2017-11937 | Nhóm 05 lỗ hổng trên các dịch vụ, ứng dụng của hệ | Chưa có |

| | | | | |
|---|---|---|---|---|
| | | CVE-2017-11940<br>CVE-2017-17113<br>CVE-2017-17112<br>CVE-2017-17114 | điều hành Windows (bao gồm Microsoft Forefront, MistServer, Microsoft Defender) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau trong đó nguy hiểm nhất là lỗ hổng CVE-2017-11937, CVE-2017-11940 cho phép chèn và thực thi mã lệnh | bản vá |

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

### *3.1 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.




Tại Việt Nam, cũng có số lượng không ít các thiết bị bị nhiễm mã độc Mirai. Dưới đây là một số thông kê về mạng botnet Sality tại Việt Nam trong tuần mà Cục An toàn thông tin đang theo dõi.

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

| TT | Tên miền/IP |
|---|---|
| 1 | anurybadovaqy.biz |
| 2 | christianneunderwood.net |
| 3 | crowdsmell.net |
| 4 | jumpover.net |
| 5 | katherinarichardson.net |
| 6 | lk9x.net |
| 7 | pndbkijqe.com |
| 8 | sundayserve.net |
| 9 | uqikoxomyturo.biz |
| 10 | 1-2-7-8-6-0-3-2-0-0-6-6-8-1-8-6-7-2-5-5-0-4-7-5-8-7-6-5-0-1-5-.0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-33-0-0-0-0-0-0-0-0-0-0-0-0-0.info |

**4. Khuyến nghị đối với các cơ quan, đơn vị**

Theo thống kê số lượng máy tính Việt Nam nằm trong mạng botnet quốc tế là không nhỏ. Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan đơn vị, Cục An toàn thông tin khuyến nghị:

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu trên.

- 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 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, TĐQLGS.

(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;

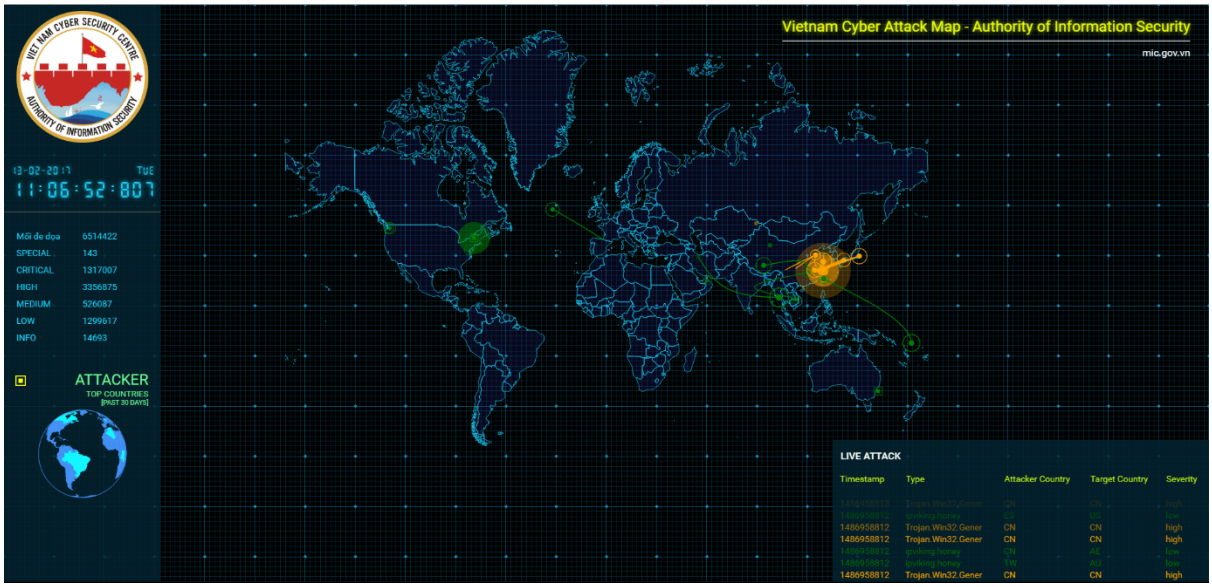
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- Hoạt động theo dõi, phân tích, tổng hợp tình hình an toàn thông tin mạng trên các trang mạng uy tín.

## III. Giới thiệu về Hệ thống theo dõi, xử lý tấn công mạng Internet Việt Nam trực thuộc Cục An toàn thông tin:

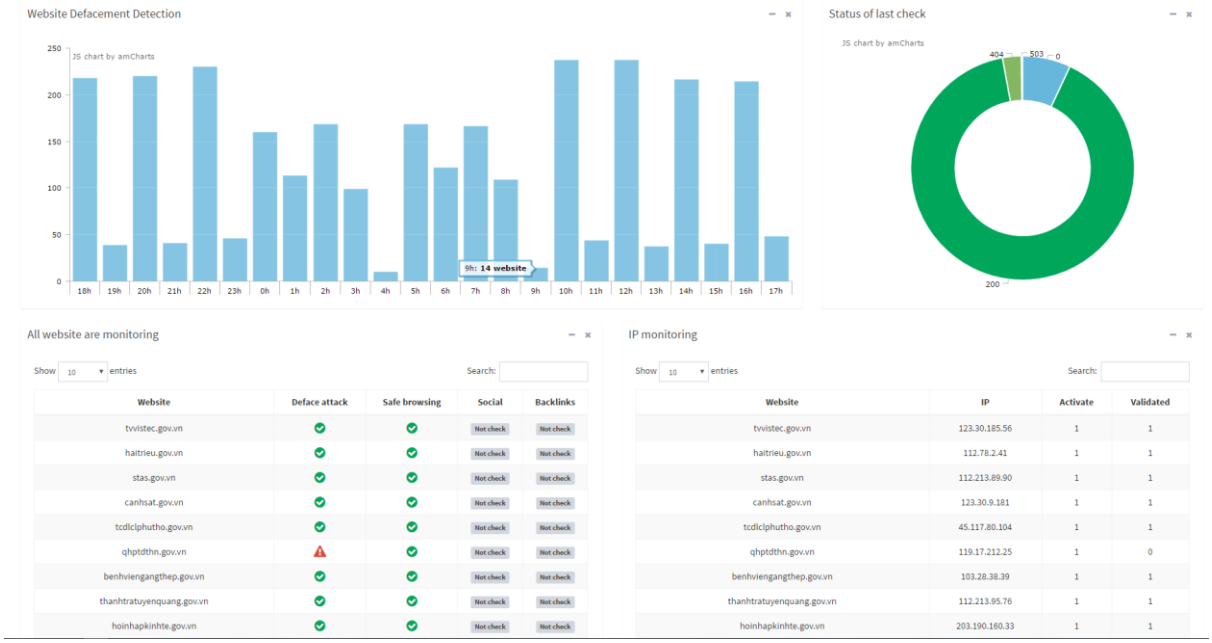
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

### *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**



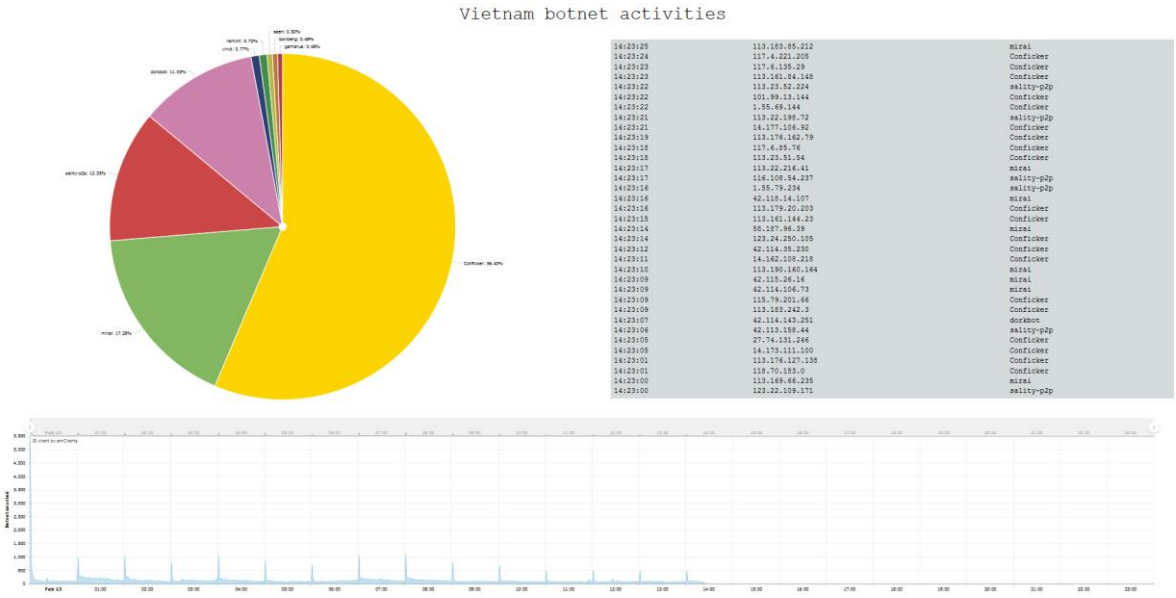

Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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