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: **64**/BC-CATTT

Hà Nội, ngày 19 tháng 12 năm 2017

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 50/2017 (từ ngày 11/12/2017 đến ngày 17/12/2017)

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 50/2017 (từ ngày 11/12/2017 đến ngày 17/12/2017), 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. Tổng thống Hoa Kỳ, Donald Trump ký lệnh cấm sử dụng các sản phẩm, dịch vụ của hãng Kaspersky Lab trong các cơ quan, tổ chức của Chính phủ liên bang. Trung Quốc sẽ thiết lập một khu công nghiệp an toàn thông tin mạng tầm cỡ thế giới để phát triển ngành công nghiệp an toàn thông tin mạng trị giá 100 tỷ nhân dân tệ (tương đương khoảng 350 nghìn tỷ VNĐ) tại Bắc Kinh vào năm 2020.

2. Ngày 14/12/2017, các chuyên gia về an toàn thông tin cho biết về nguy cơ bị đánh cắp mật khẩu đối với một số máy tính cá nhân sử dụng Hệ điều hành Windows 10 có cài đặt ứng dụng quản lý mật khẩu của bên thứ 3 có tên là "Keeper".

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. Ngày 11/12/2017, Hạ viện Hoa Kỳ thông qua đạo luật nhằm tái thiết lại Cơ quan giám sát và bảo vệ quốc gia (NPPD) thành Cơ quan an toàn thông tin mạng và an toàn cơ sở hạ tầng (CISA). Sự tái thiết này nhằm tạo ra một tổ chức hoạt động độc lập, tập trung và nâng cao các nhiệm vụ để tăng cường sức

mạnh an toàn thông tin và cơ sở hạ tầng quan trọng của Hoa Kỳ. Theo bản dự luật tóm lược, đạo luật quy định CISA sẽ thực hiện tăng cường bảo đảm an toàn thông tin, truyền thông khẩn cấp và bảo vệ cơ sở hạ tầng quan trọng của Hoa Kỳ. Cơ quan được cơ cấu lại này sẽ bao gồm các bộ phận chính là: bộ phận an toàn thông tin mạng, bộ phận an toàn cơ sở hạ tầng và bộ phận truyền thông khẩn cấp.

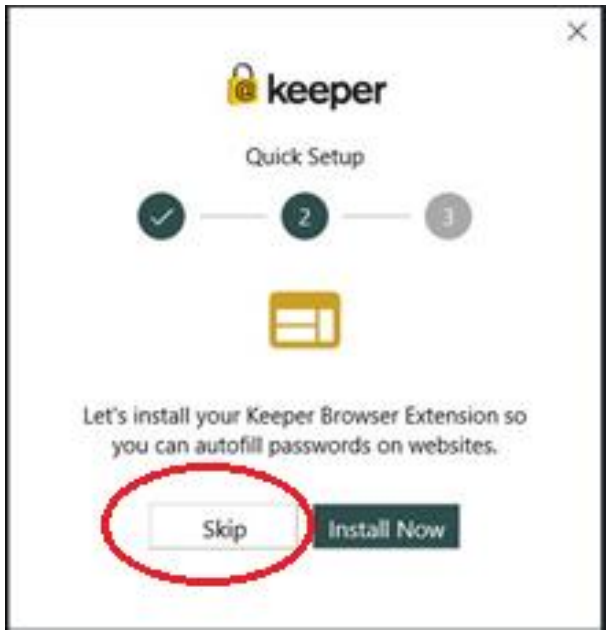
1.2. Ngày 12/12/2017, Tổng thống Hoa Kỳ, Donald Trump đã ký lệnh cấm sử dụng các sản phẩm, dịch vụ của hãng Kaspersky Lab trong các cơ quan, tổ chức của Chính phủ liên bang. Lệnh cấm này được đưa vào trong phần 1634 của Đạo luật NDAA (National Defense Authorization Act) cho năm tài chính 2018 của Hoa Kỳ. Theo đó, bất kỳ sản phẩm phần cứng, phần mềm hoặc dịch vụ được phát triển toàn bộ hoặc một phần bởi Kaspersky Lab đều bị cấm sử dụng trong các cơ quan, tổ chức của Chính phủ hoặc các cơ quan, tổ chức có các hoạt động liên quan tới Chính phủ. Lệnh cấm sẽ có hiệu lực từ ngày 01/10/2018.

1.3. Ngày 13/12/2017, theo thông tin từ Tân Hoa Xã, Trung Quốc sẽ thiết lập một khu công nghiệp an toàn thông tin mạng tầm cỡ thế giới để phát triển ngành công nghiệp an toàn thông tin mạng trị giá 100 tỷ nhân dân tệ (tương đương khoảng 350 nghìn tỷ VNĐ) tại Bắc Kinh vào năm 2020. Khu công nghiệp sẽ được Bộ Công nghiệp và Công nghệ Thông tin (MIIT) kết hợp với chính quyền thành phố Bắc Kinh xây dựng. Hiện tại, khoảng một nửa số doanh nghiệp an toàn thông tin mạng của Trung Quốc có đăng ký tại Bắc Kinh, và sáu trong số đó có doanh thu hàng năm lớn hơn 1 tỷ nhân dân tệ. Năm 2016, quy mô ngành an toàn thông tin mạng của Trung Quốc tăng 21,7% và dự kiến sẽ tăng 32,85% trong năm nay.

1.4. Ngày 14/12/2017, các chuyên gia về an toàn thông tin cho biết về nguy cơ bị đánh cắp mật khẩu đối với một số máy tính cá nhân sử dụng Hệ điều hành Windows 10 có cài đặt ứng dụng quản lý mật khẩu của bên thứ 3 có tên là "Keeper". Chưa rõ thông tin phần mềm này được cài đặt sẵn trên hệ điều hành windows 10 hay không, tuy nhiên, nếu người dùng vô tình cài đặt và sử dụng phần mềm này với các thiết lập mặc định ban đầu của nhà sản xuất, nó sẽ cài đặt thêm một tiện ích mở rộng lên trình duyệt web của người dùng. Tiện ích mở rộng này có chứa điểm yếu an toàn thông tin cho phép kẻ tấn công lấy cắp mật khẩu của người dùng sử dụng để đăng nhập vào các tải khoản qua trình duyệt.

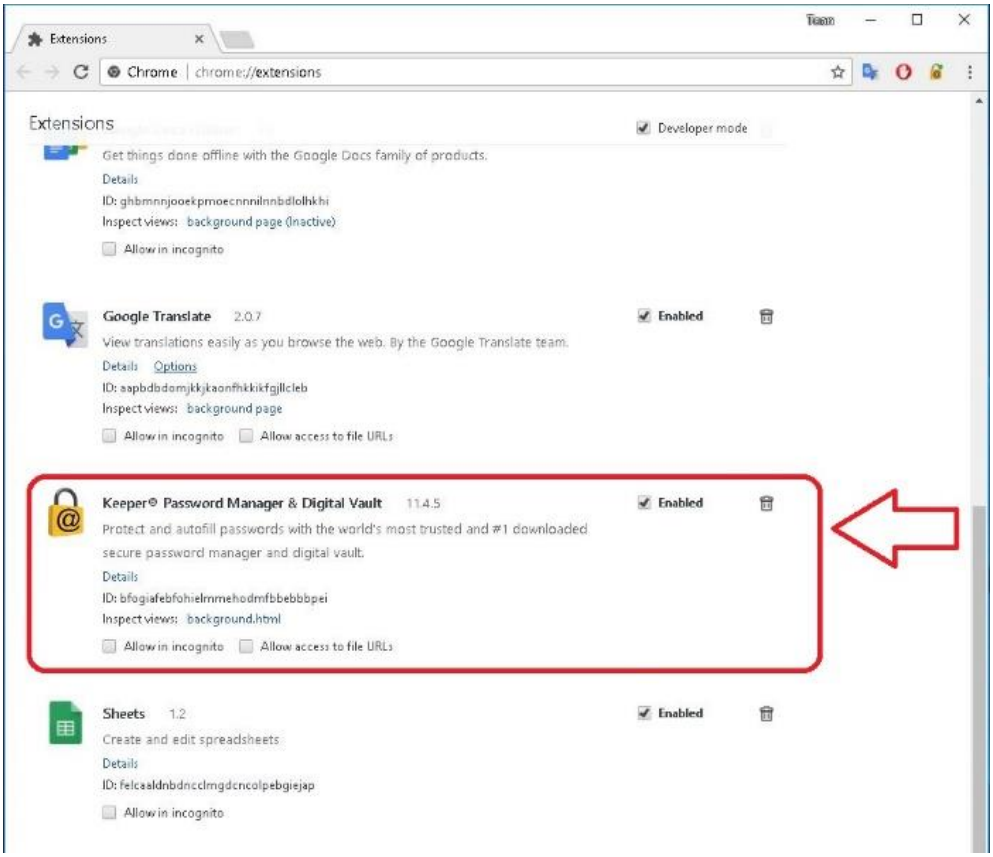
Theo các chuyên gia an toàn thông tin, nếu người dùng vẫn muốn sử dụng ứng dụng quản lý mật khẩu Keeper thì biện pháp trước mắt là lưu ý bỏ qua bước

cài đặt tiện ích mở rộng lên trình duyệt web khi thực hiện các bước cài đặt ứng dụng keeper *(như hình bên dưới)*.



Hình 1: Bỏ qua bước cài đặt tiện ích mở rộng Keeper lên trình duyệt web

Đối với người dùng đã cài đặt và sử dụng ứng dụng keeper, cần tiến hành kiểm tra lại các tiện ích mở rộng của các trình duyệt trên máy tính và tạm thời gỡ bỏ tiện ích mở rộng keeper nếu có.



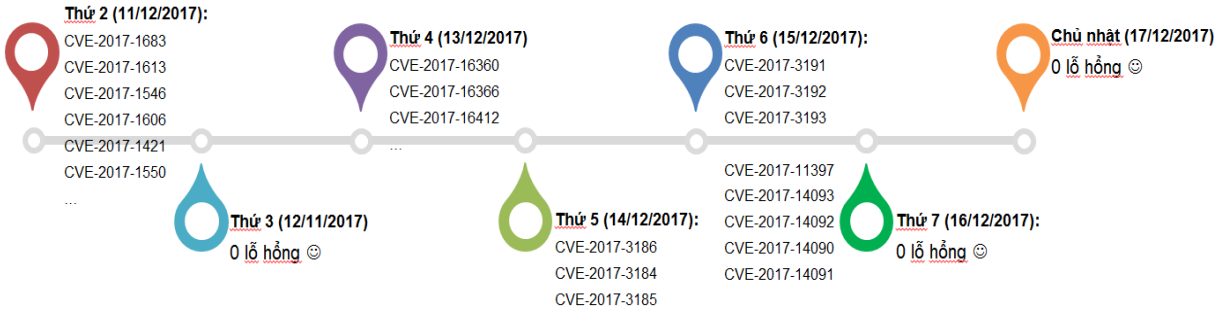
Hình 2: Ví dụ về tiện ích mở rộng Keeper đã được cài đặt lên trình duyệt Chrome

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

2.1. Trong tuần 50/2017, các tổ chức quốc tế đã phát hiện và công bố ít nhất **382** lỗ hổng, điểm yếu an toàn thông tin bao gồm: **59** lỗ hổng, điểm yếu ở mức cao, **18** lỗ hổng, điểm yếu ở mức trung bình, **305** lỗ hổng, điểm yếu chưa được đánh giá. Trong các lỗ hổng, điểm yếu đó có: **04** lỗ hổng đã có mã khai thác và **35** lỗ hổng RCE (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 03 lỗ hổng trong thiết bị D-link cho phép vượt qua cơ chế xác thực và truy cập từ xa vào trang quản trị của thiết bị; Nhóm 15 lỗ hổng trong các sản phẩm, giải pháp của IBM .v.v…

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



Hình 3: 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-2017-16360 CVE-2017-16366 CVE-2017-16412 …	Nhóm các 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	Đã có bản vá. Nhiều lỗ hổng đã cảnh báo trong tuần 49.

			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	
2	Acti-Cameras	CVE-2017-3186 CVE-2017-3184 CVE-2017-3185	Nhóm 03 lỗ hổng trong sản phẩm camera ACTi dòng D, B,I, E sử dụng firmware phiên bản A1D-500-V6.11.31-AC cho phép đối tượng tấn công có thể kiểm soát thiết bị thông qua một số cách: truy cập trực tiếp tới phần cài đặt của thiết bị và khởi tạo lại cấu hình hay sử dụng tài khoản mặc định	Chưa có thông tin bản vá.
3	D-Link	CVE-2017-3191 CVE-2017-3192 CVE-2017-3193	Nhóm 03 lỗ hổng trong thiết bị D-link cho phép vượt qua cơ chế xác thực và truy cập từ xa vào trang quản trị của thiết bị. Lỗ hổng CVE-2017-3191, CVE-2017-3192 ảnh hưởng đến sản phẩm D-Link DIR-130 sử dụng firmware phiên bản 1.23 và DIR-330 sử dụng firmware phiên bản 1.12 Lỗ hổng CVE-2017-3193 ảnh hưởng đến tất cả các sản phẩm bao gồm DIR-850L sử dụng firmware phiên bản 1.14B07 and 2.07.B05	Chưa có thông tin bản vá.

4	IBM	CVE-2017-1683 CVE-2017-1613 CVE-2017-1546 CVE-2017-1606 CVE-2017-1421 CVE-2017-1550 …	Nhóm 15 lỗ hổng trong các sản phẩm, giải pháp của IBM cho phép thực hiện nhiều hình thức tấn công khác nhau bao gồm: truy cập thông tin nhạy cảm, thực hiện tấn công XSS, tấn công Path Traverse, chuyển hướng hướng, SQL Injection, người dùng đã xác thực thay đổi thông tin xác thực của người dùng khác, và nhiều lỗ hổng cho phép thực thi mã lệnh. Các lỗ hổng này nằm trong IBM Connections, IBM DOORS Next Generation, IBM Financial Transaction Manager, IBM iNotes, IBM Jazz Foundation, IBM Maximo Asset Management IBM Sterling File Gateway, IBM WebSphere, IBM Tivoli Monitoring	Đã có thông tin bản vá
5	Trend micro	CVE-2017-11397 CVE-2017-14093 CVE-2017-14092 CVE-2017-14090 CVE-2017-14091	Nhóm 05 lỗ hổng trong một số sản phẩm, giải pháp của TrendMicro (bao gồm: Trend Micro Encryption, ScanMail) cho phép thực hiện một số hình thức tấn công, trong đó lỗ hổng CVE-2017-11397 cho phép đối tượng tấn công có thể chèn và thực thi mã lệnh.	Đã có thông tin bản vá.

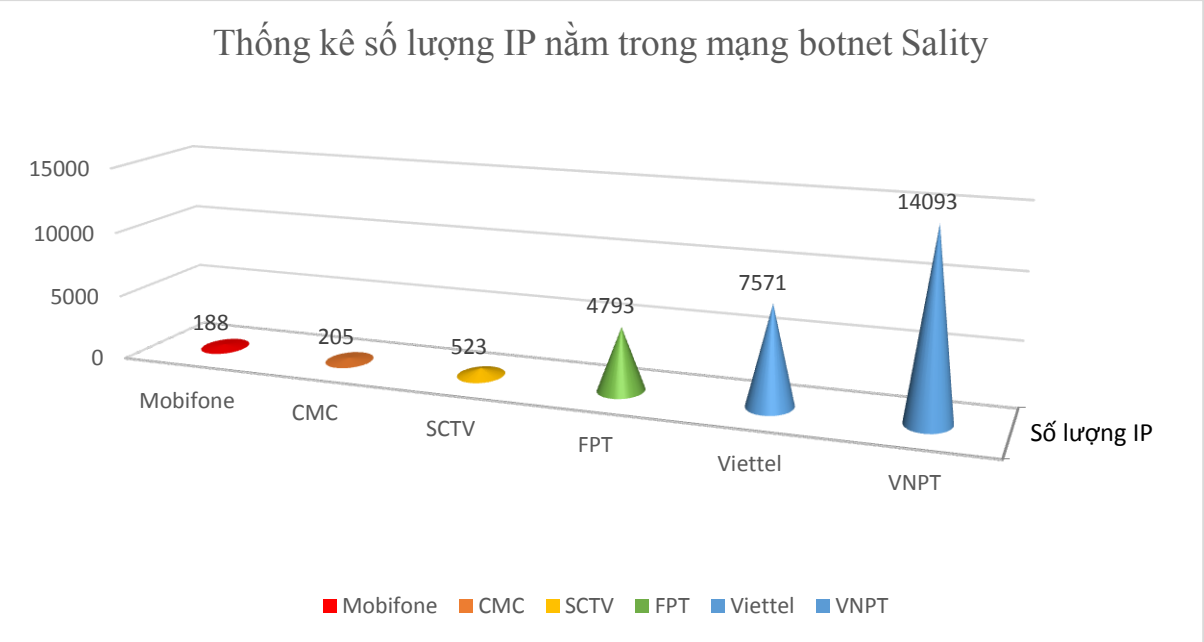
3. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

3.1. 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.



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

TT	Tên miền/IP
1	eluheqizomado.biz
2	f094e9cc.net
3	founefits.at
4	gowasa.com
5	horodityrowoboni.biz
6	sickrain.net
7	withbreak.net

8	app2.winsoft99.com
9	awaptfhcywz.biz
10	glkdfkoeui.org

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;

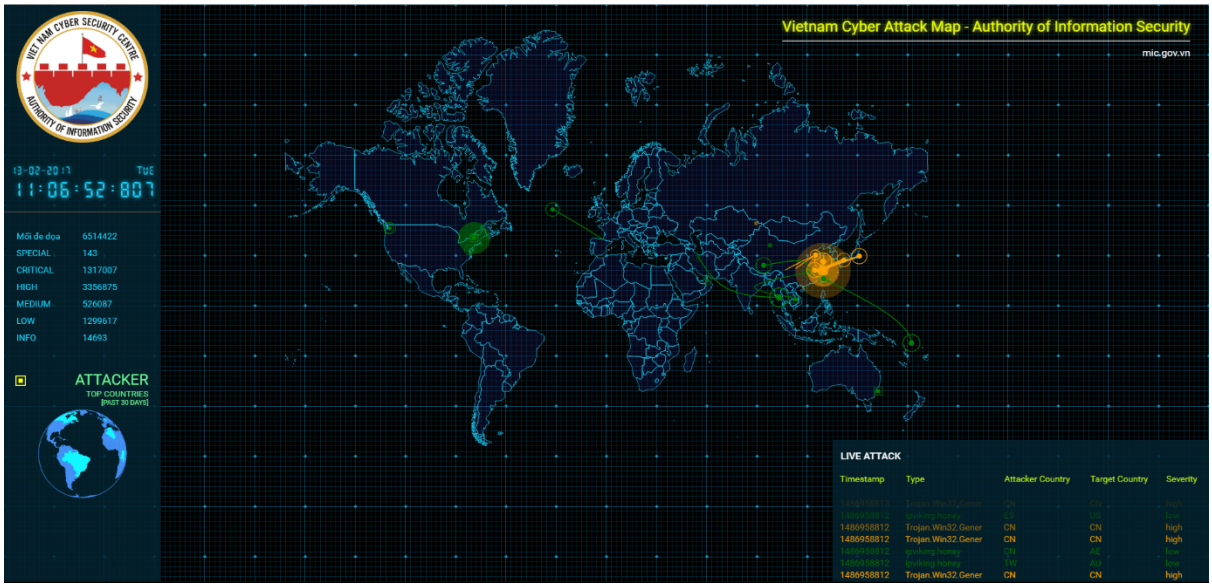
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

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

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

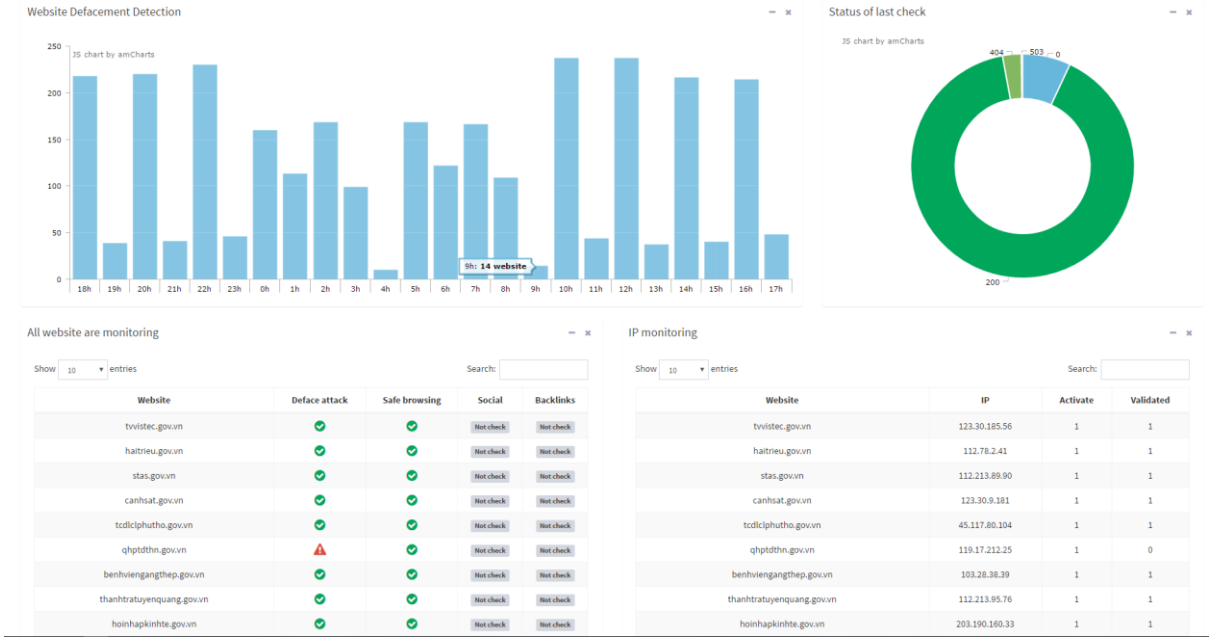
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

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



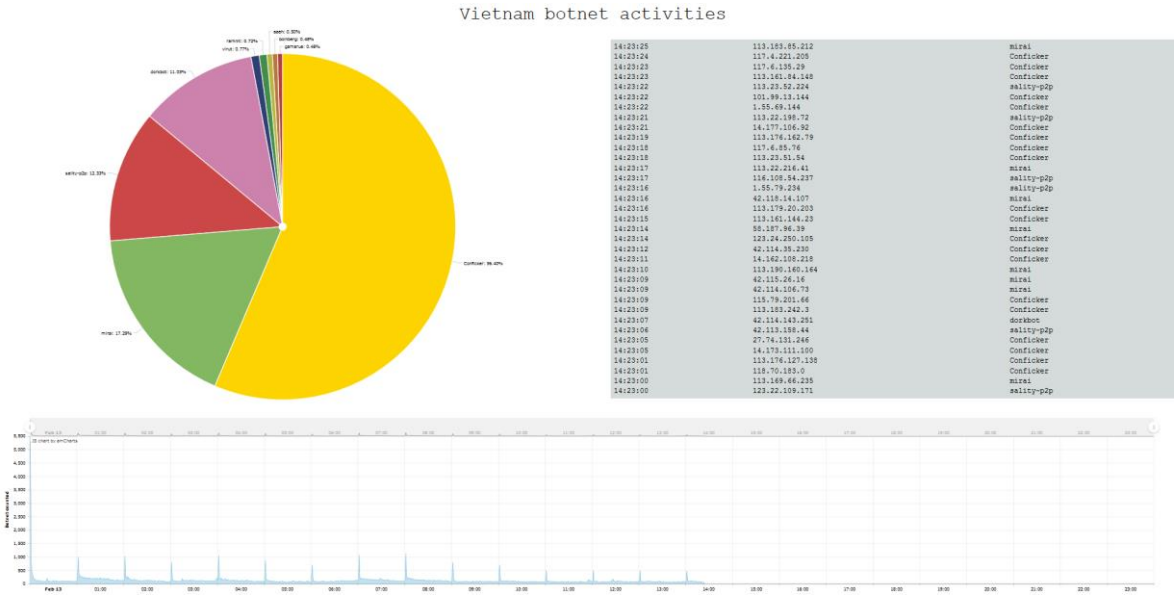
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc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