| | |
|---|---|
| BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG<br>**CỤC CÔNG NGHỆ THÔNG TIN VÀ DỮ LIỆU TÀI NGUYÊN MÔI TRƯỜNG** | **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số: 397 /CNTT-KHCN<br>V/v báo cáo tình hình an toàn, an ninh thông tin tháng 05/2018 | *Hà Nội, ngày 04 tháng 6 năm 2018* |

Kính gửi: Các đơn vị trực thuộc Bộ

Thực hiện chức năng quản lý, theo dõi giám sát, bảo đảm an toàn, an ninh thông tin và điều phối ứng cứu sự cố trong Bộ Tài nguyên và Môi trường. Qua công tác thu thập, theo dõi, trích xuất, dò quét, phân tích về an toàn thông tin, trong thời gian tháng 05 năm 2018 Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường gửi báo cáo tóm tắt về tình hình về an toàn, an ninh thông tin để các đơn vị tham khảo và có biện pháp phòng ngừa.

Trân trọng./.

***Nơi nhận*:**
- Như trên;
- Bộ trưởng Trần Hồng Hà (để báo cáo);
- Các Thứ trưởng (để báo cáo);
- Cục trưởng (để báo cáo);
- Lưu: VT, HTTT, KHCN&ATTT, TTCSHT.

**KT. CỤC TRƯỞNG**
**PHÓ CỤC TRƯỞNG**

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN VÀ DỮ LIỆU TÀI NGUYÊN MÔI TRƯỜNG
BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

**Trần Văn Đoài**

| | |
|---|---|
| BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG<br>**CỤC CÔNG NGHỆ THÔNG TIN VÀ DỮ LIỆU TÀI NGUYÊN MÔI TRƯỜNG** | **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |

*Hà Nội, ngày 04 tháng 6 năm 2018*

# BÁO CÁO

## TÌNH HÌNH AN TOÀN, AN NINH THÔNG TIN THÁNG 5/2018

*(Kèm theo công văn số 397 /CNTT-KHCN ngày 04 /6/2018)*

### 1. Tình hình an toàn thông tin chung

1.1. Chính quyền thành phố Dubai đã công bố thông tin về website hỗ trợ công tác bảo đảm an toàn thông tin. Nền tảng trực tuyến này được thiết lập để nhận báo cáo từ các cá nhân, doanh nghiệp và cả các tổ chức thuộc chính quyền. Website cho phép người dùng Internet gửi thông tin qua 07 bước đơn giản để báo cáo về các vấn đề liên quan đến thư điện tử giả mạo, mạng xã hội, tấn công mạng .v.v…

Chính quyền Dubai nhấn mạnh sự quan tâm của mình trong việc cung cấp các dịch vụ hiện đại phù hợp với định hướng chỉ đạo của UAE và những kế hoạch tương lai trong lĩnh vực dịch vụ thông minh như là một phần của Kế hoạch Dubai 2021.

1.2. Chính quyền thành phố Luân Đôn đã phát động một chiến dịch có tên là Cyber Griffin với mục tiêu chia sẻ thông tin, tin tức và các khuyến nghị về việc tăng cường khả năng bảo đảm an toàn thông tin cho các doanh nghiệp tại Thành phố này.

Theo đó, các doanh nghiệp sẽ nhận được các báo cáo tóm tắt, cập nhật về các nguy cơ mất an toàn thông tin, đồng thời được cung cấp một môi trường để các nhà điều hành, quản lý doanh nghiệp có thể kết nối và chia sẻ kinh nghiệm với nhau. Cyber Griffin cũng cung cấp các bài diễn tập về phản ứng sự cố với 03 trình độ khác nhau, từ cơ bản tới chuyên gia, thực hiện trong thời gian thực (realtime) cùng với quan sát của lãnh đạo doanh nghiệp. Bên cạnh đó, chiến dịch sẽ có các nhóm chuyên gia về an toàn thông tin giúp tư vấn cho thành viên của cộng đồng doanh nghiệp.

1.3. Một nhóm các nhà nghiên cứu bảo mật đã phát hiện ra 08 lỗ hổng mới cùng lớp với lỗ hổng “Spectre” trong CPU của Intel, được gọi là Spectre-NG. Lỗi CPU mới được phát hiện này bắt nguồn từ vấn đề trong thiết kế tương tự lỗi Spectre ban đầu và có cùng kịch bản tấn công, đã được Cục An toàn thông tin cảnh báo trong Công văn số 03/CATTT-TTTV ngày 04/01/2018, tuy nhiên, nó được đánh giá còn nguy hiểm hơn lỗ hổng Spectre ban đầu.

Cụ thể, một trong các lỗi Spectre-NG cho phép kẻ tấn công đơn giản hóa kịch bản tấn công vượt qua ranh giới hệ thống bằng cách khai thác một máy ảo và từ đó tấn công vào hệ thống mục tiêu, ví dụ như các máy ảo nằm trên cùng hệ thống điện toán đám mây (cloud). Ngoài ra, nó cũng có thể sử dụng để tấn công các máy ảo khác

nằm trên cùng máy chủ bị khai thác. Mật khẩu và khóa bí mật được sử dụng để truyền dữ liệu an toàn trên hệ thống cloud là mục tiêu tấn công và có rủi ro cao. Thậm chí công nghệ Software Guard Extensions (SGX) của Intel được thiết kế để bảo vệ dữ liệu nhạy cảm trên cloud cũng không an toàn trước kịch bản tấn công Spectre.

1.4. Ngày 9/5/2018, Cục An toàn thông tin - Bộ TT&TT và Bkav đã tổ chức khai mạc chương trình diễn tập An toàn thông tin mạng WhiteHat Drill 05 chủ đề "Điều tra, xử lý và phòng chống mã độc đào tiền ảo qua lỗ hổng phần mềm".

WhiteHat Drill 05 được tổ chức trên hệ thống mới - hệ thống Wargame 2.0 của Diễn đàn WhiteHat.vn, cho phép các đội tham gia có thể gửi (submit) kết quả trực tiếp và xem đánh giá của Ban tổ chức. Whitehat Drill 05 có sự tham gia của 148 đội đến từ các cơ quan quản lý nhà nước, ngân hàng, tập đoàn, doanh nghiệp… trên toàn quốc. Trong đó có: 72 đơn vị cơ quan nhà nước, 13 ngân hàng, 10 đơn vị giáo dục, 34 doanh nghiệp và 19 cá nhân. Các đội tham gia diễn tập được trải nghiệm nhiều tình huống thực tế, qua đó rút kinh nghiệm và có biện pháp chủ động hơn để điều tra, xử lý và phòng chống những loại mã độc đào tiền ảo khai thác các lỗ hổng phần mềm để tấn công vào người sử dụng.

1.5. Quốc hội Australia sẽ tiến hành xây dựng Trung tâm An toàn thông tin trước các lo ngại về những cuộc tấn công mạng vào các hệ thống thông tin của Tòa nhà Quốc hội. Trong công bố ngân sách năm 2018, Chính phủ Australia đã công bố sẽ có một khoản chí phí cho việc thiết lập Trung tâm an toàn thông tin, nằm dưới quyền quản lý của Ban Phục vụ Quốc hội (DPS) "nhằm tăng cường việc bảo đảm an toàn thông tin cho mạng máy tính Quốc hội."

Ban Phục vụ Quốc hội có trách nhiệm bảo đảm an toàn thông tin cho địa chỉ thư điện tử của các Nghị sĩ, Thượng nghị sĩ và nhân viên phục vụ trong Toà nhà Quốc hội, cũng như quản lý các thiết bị như điện thoại di động và máy tính bảng của các Nghị sĩ và Thượng nghị sĩ, và cả dịch vụ Internet trong Tòa nhà Quốc hội.

1.6. 02 lỗ hổng nguy hiểm nằm trong thiết bị định tuyến (Home router) sử dụng công nghệ GPON (được công bố và cảnh báo hồi tháng 4) đã được sử dụng để khai thác kiểm soát các thiết bị bởi ít nhất 05 mạng botnet, bao gồm: Mettle, Muhstik, Mirai, Hajime và Satori.

- Mạng botnet Mettle: Công cụ kiểm soát, điều khiển mã độc và rà quét mạng Internet được lưu trữ trên một máy chủ có địa chỉ tại Việt Nam. Mạng mã độc này sử dụng một môđun tấn công mã nguồn mở có tên là Mettle để lây nhiễm mã độc lên các Home router tồn tại điểm yếu.

- Mạng botnet Muhstik: mạng botnet này mới được phát hiện vào tuần trước, khi đang khai thác lỗ hổng Drupal. Hiện tại mạng botnet này đã được cải tiến để khai thác lỗ hổng GPON, cùng với lỗi trong firmware JBOSS và DD-WRT.

- Mạng botnet Mirai: Mã khai thác GPON cũng đã được tích hợp vào trong một vài biến thể mới của mạng botnet IoT Mirai, mạng botnet này đang được Cục An toàn thông tin theo dõi liên tục và cập nhật số liệu qua cảnh báo tuần.

- Mạng botnet Hajime: Là một mạng botnet khác ít được biết đến, có mục tiêu thường là các thiết bị IoT, cũng đang sử dụng thêm mã khai thác GPON để kiểm soát các thiết bị Home Router.

- Mạng botnet Satori: Mạng botnet đã lây nhiễm hàng trăm nghìn thiết bị trong năm 2017, đã thêm mã khai thác GPON vào trong biến thể mới nhất.

Ngoài ra, mã khai thác chứng minh tính khả thi (PoC) cho các lỗ hổng GPON này được công bố rộng rãi trong cộng đồng, giúp cho những người không có kỹ năng cũng có thể dễ dàng thực hiện kịch bản tấn công.

Trong khi nhà sản xuất cũng như các ISP chưa cung cấp thông tin gì về bản vá hay cập nhật cho lỗ hổng, hàng trăm nghìn thiết bị Home router ở Việt Nam vẫn đang tiềm ẩn rủi ro cao với người dùng. Để tự bảo vệ bản thân, lời khuyên được đưa ra bởi các chuyên gia về an toàn thông tin là người dùng cần thay đổi cấu hình trên các thiết bị có chứa lỗ hổng để ngăn chặn truy cập tới thiết bị từ bên ngoài, hạn chế quyền truy cập vào trang quản trị trong mạng nội bộ, hoặc có thể sử dụng công cụ bảo mật được cung cấp bởi bên thứ 3.

1.7. Nhật Bản thay đổi quy định về quản lý thị trường tiền mã hóa nhằm ngăn chặn các vụ tấn công mạng chiếm đoạt tiền mã hóa. Theo đó, Cục Dịch vụ Tài chính Nhật Bản (FSA) sẽ áp dụng các tiêu chuẩn đánh giá chặt chẽ hơn đối với các sàn giao dịch tiền mã hóa có đăng ký với cơ quan này.

Các sàn giao dịch có đăng ký với chính phủ phải đáp ứng các yêu cầu như: tuân thủ các tiêu chuẩn về hệ thống quản lý, không được lưu trữ tiền tại các máy tính có kết nối với internet, phải đặt nhiều mật khẩu cho các giao dịch; tích cực hợp tác trong việc chống rửa tiền, qua các phương pháp như xác thực danh tính khách hàng trong những giao dịch lớn .v.v… FSA cũng yêu cầu các sàn giao dịch phải có quy định để ngăn nhân viên sử dụng tiền của khách hàng.

1.8. Ngày 15/5/2018, Bộ An ninh nội địa Hoa Kỳ đã đưa ra một chiến lược tóm tắt hướng tiếp cận của cơ quan này trong vấn đề xác định và xử lý các nguy cơ mất an toàn thông tin quốc gia. Chiếc lược này miêu tả hướng tiếp cận cấp Bộ để giải quyết sự biến đổi từng ngày của các mối đe dọa đối với an toàn thông tin, đặc biệt là ATTT của các cơ sở hạ tầng quan trọng.

Chiến lược này nêu ra những mục tiêu và hành động, mức độ ưu tiên để Bộ trưởng Bộ An ninh nội địa Hoa kỳ có thể đảm đương thành công trách nhiệm của mình trong vấn đề ATTT. Mục tiêu của chiến lược này mang lại sự hài hòa và những ưu tiên trong việc thực hiện các kế hoạch, tổ chức, chi tiêu và triển khai hoạt động

trên tất cả các lĩnh vực liên quan đến ATTT của Bộ An ninh nội địa. Chiến lược sẽ tập trung vào việc phối hợp của công tác ATTT trong Bộ để bảo đảm sự đồng nhất.

Chiến lược của Bộ đặt ra 05 hướng tiếp cập để xử lý các nguy cơ gây mất ATTT quốc gia, nhằm bảo đảm ATTT cho các hạ tầng quan trọng của quốc gia, tăng cường sự hiệu quả, đổi mới, tin cận trong công tác phối hợp. 05 hướng tiếp cận, bao gồm:

(1) Xác định rủi ro;

(2) Giảm thiểu điểm yếu, lỗ hổng ATTT;

(3) Giảm thiểu các mối đe dọa;

(4) Phản ứng một cách hiệu quả đối với những sự cố an toàn thông tin;

(5) Tăng cường tính an toàn và độ tin cậy của hệ sinh thái an toàn thông tin bằng các chính sách và hoạt động hỗ trợ.

1.9. Được phát hiện từ năm 2012, Rowhammer là một điểm yếu nghiêm trọng nằm trong chips DRAM thế hệ mới, cho phép đọc hoặc thay đổi nội dung của bộ nhớ RAM bằng cách truy cập liên tục vào một hàng trong bộ nhớ và gây ra sự đảo "bit" của hàng liền kề. Lỗ hổng này không ảnh hưởng đến môđun SDRAM DDR và SDRAM DDR2, nhưng ảnh hưởng đến môđun SDRAM DDR3 và SDRAM DDR4, 2 loại SDRAM phổ biến nhất hiện nay.

Việc khai thác thành công lỗ hổng này có thể dẫn đến việc thực thi lệnh từ xa trên máy tính hoặc máy chủ. Trước đây, đối tượng tấn công phải lừa người dùng truy cập vào một website hoặc cài đặt ứng dụng độc hại để có thể khai thác thành công, tuy nhiên gần đây các nhóm chuyên gia nghiên cứu ATTT độc lập đã công bố 02 phương thức tấn công khác dễ dàng hơn.

Phương thức tấn công đầu tiên gọi là Throwhammer được phát hiện bởi các nhà nghiên cứu đến từ trường đại học Amsterdam và đại học Cyprus. Theo đó, việc đối tượng tấn công gửi các gói tin độc hại qua mạng LAN có thể kích hoạt kiểu tấn công Rowhammer trên hệ thống chạy card mạng Ethernet sử dụng kênh RDMA. Kênh kết nối này khá phổ biến trong giải pháp Clouds và Data Centers.

Phương thức thứ 2 gọi là Nethammer là kiểu tấn công có thể gây ra việc thực thi lệnh trên hệ thống mục tiêu bằng cách ghi lại nhanh bộ nhớ được sử dụng cho xử lý gói tin. Phương thức tấn công Nethammer chỉ có thể thực hiện được nếu có kết nối mạng đủ nhanh giữa đối tượng tấn công và nạn nhân.

Hiện nay vẫn chưa có giải pháp nào thực sự hữu ích để chống lại các kiểu tấn công Rowhammer. Hơn nữa, lỗ hổng Rowhammer khai thác nhằm vào điểm yếu phần cứng máy tính nên không có bản bá phần mềm nào có thể khắc phục hoàn toàn vấn đề. Các nhà nghiên cứu cho rằng rủi ro từ lỗ hổng có thể gây ra những thiệt hại

nghiêm trọng nếu không có sự thay đổi cơ bản trong công nghệ sản xuất bộ nhớ DRAM.

1.10. Ngày 25/5/2018, Thủ tướng Chính phủ đã ký ban hành Chỉ thị số 14/CT-TTg về việc nâng cao năng lực phòng, chống phần mềm độc hại. Nội dung Chỉ thị nêu rõ, trong xu hướng của cuộc cách mạng công nghiệp lần thứ tư, sẽ ngày càng có nhiều thiết bị thông minh kết nối mạng. Những thiết bị này khi bị lây nhiễm các loại phần mềm độc hại (gọi tắt là mã độc) sẽ gây mất an toàn thông tin, tiềm ẩn nguy cơ khó lường. Trong năm 2016 và năm 2017, một số cuộc tấn công mạng sử dụng mã độc làm thiệt hại nghiêm trọng cho nhiều cơ quan, tổ chức ở Việt Nam.

Các cơ quan, tổ chức ở Việt Nam đã và đang thực hiện nhiều giải pháp khác nhau trong việc xử lý mã độc. Tuy nhiên, hiệu quả đạt được chưa cao, khả năng chia sẻ thông tin thấp. Thực trạng lây nhiễm mã độc tại Việt Nam hiện nay rất đáng báo động. Đặc biệt, nhiều trường hợp tấn công mã độc mà cơ quan chức năng không phản ứng kịp thời để phát hiện, phân tích và gỡ bỏ.

Thủ tướng Chính phủ đã có những chỉ thị cụ thể đối với các cơ quan, tổ chức thực hiện các biện pháp để nâng cao năng lực phòng, chống phần mềm độc hại, cải thiện mức độ tin cậy của quốc gia trong hoạt động giao dịch điện tử, thúc đẩy phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh của đất nước

1.11. Mới đây, Thủ tướng Thái Lan, Ông Prayut Chan-ocha đã chủ trì cuộc họp đầu tiên của Ủy ban Quốc gia về vấn đề An toàn Thông tin. Trong cuộc họp, Thủ tướng Prayut đã đề cập đến việc các nhà chức trách bắt buộc phải đẩy mạnh việc thực thi đạo luật Bảo vệ dữ liệu vì điều này sẽ bảo đảm tính riêng tư về dữ liệu của Thái Lan phù hợp với những tiêu chuẩn quốc tế và giải quyết những lo ngại của người dùng internet. Mục tiêu đặt ra là làm cho Thái Lan trở thành một trong 20 quốc gia đứng đầu về tính sẵn sàng trong công tác An toàn Thông tin.

Bốn điểm chính được đưa ra trong cuộc họp là:

(1) Tầm quan trọng của việc có một khuôn khổ chính sách quốc gia để bảo vệ, phòng, chống và giảm thiểu các nguy cơ mất an toàn thông tin;

(2) Xác định cơ sở hạ tầng Thông tin quan trọng trong các lĩnh vực: Viễn thông; An ninh quốc gia và dịch vụ cộng đồng; Giao thông Vận tải; Tài chính và Ngân hàng; Năng lượng và Dịch vụ xã hội; Sức khoẻ cộng đồng. Đưa ra những hướng dẫn và thủ tục vận hành tiêu chuẩn khi xử lý các tình huống khẩn cấp liên quan đến an toàn thôn tin;

(3) Phát triển nhân sự an toàn thông tin;

(4) Thành lập của Cơ quan An toàn Thông tin, cơ quan chịu trách nhiệm phối hợp và phản ứng với các vấn đề an toàn thông tin. Cơ quan này sẽ bảo đảm an toàn thông tin quốc gia Thái Lan tương xứng với các tiêu chuẩn quốc tế.

1.12. Hơn 500,000 thiết bị định tuyến (router) và thiết bị lưu trữ (storage) ở nhiều quốc gia trong đó có Việt Nam bị lây nhiễm bởi một loại mã độc mới có tên là VPNFilter. Theo nghiên cứu từ nhóm Cisco Talos thuộc hãng Cisco, mạng botnet này không tấn công vào lỗi zero-days trên thiết bị mà khai thác dựa trên những lỗ hổng phổ biến, đã được công bố hoặc sử dụng thông tin xác thực mặc định để chiếm quyền điều khiển. Thiết bị home routers và thiết bị lưu trữ có kết nối internet của các hãng Linksys, MikroTik, Netgear và TP-Link là đối tượng có tiềm ẩn nguy cơ bị tấn công cao.

VPNFilter là loại mã độc tinh vi, có nhiều giai đoạn tấn công, có thể đánh cắp thông tin đăng nhập website và theo dõi các hệ thống điều khiển công nghiệp SCADA, chẳng hạn như hệ thống lưới điện và cơ sở hạ tầng công nghiệp. Không giống như hầu hết các loại mã độc khác, khi đã lây nhiễm thành công VPNFilter sẽ tiến hành khởi động lại thiết bị, từ đó tạo được kết nối lâu dài và cài đặt mã độc phục vụ cho giai đoạn hai. Đặc trưng của mạng botnet sử dụng mã độc VPNFilter là thư mục có đường dẫn /var/run/vpnfilterw được tạo ra trong quá trình cài đặt.

Khuyến nghị từ các chuyên gia ATTT trong trường hợp nghi ngờ thiết bị đã bị lây nhiễm bởi mạng mã độc này, người dùng nên thực hiện cài đặt lại thiết bị về mặc định để xóa mã độc và cập nhật firmware càng sớm càng tốt.

## 2. Tình hình an toàn thông tin tại Việt Nam

### *2.1. Tình hình tấn công gây nguy hại trên các trang mạng*

Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua và các thông tin do Cục An toàn thông tin - Bộ Thông tin và Truyền thông cung cấp 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 tháng, Cục ATTT ghi nhận có ít nhất 1067 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.

### *2.2. Tình hình tấn công lừa đảo (Phishing)*

Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục An toàn thông tin - Bộ Thông tin và Truyền thông thông báo đã ghi nhận có ít nhất 309 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong thời gian qua.

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.

***2.3. Lỗ hổng điểm yếu về an toàn thông tin***

Trong tháng 5/2108, các tổ chức quốc tế đã phát hiện và công bố ít nhất 1035 lỗ hổng trong đó có: 116 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 46 lỗ hổng đã có mã khai thác.

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 25 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 19 lỗ hổng trên một số sản phẩm, dịch vụ của Cisco;
- Nhóm 8 lỗ hổng trên các dòng sản phẩm của D-Link;
- Nhóm 85 lỗ hổng trên nhiều sản phẩm, ứng dụng của Microsoft;
- Nhóm 3 lỗ hổng trên một số sản phẩm của Huawei;
- Nhóm 81 lỗ hổng trên nhiều phiên bản Foxit Reader;
- Nhóm 37 lỗ hổng trên nhiều sản phẩm của Adobe;
- Nhóm 09 lỗ hổng trên một số thành phần Joomla;
- v.v.

***2.4. 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-2018-0245<br>CVE-2018-0234<br>CVE-2018-0249<br>CVE-2018-0253<br>CVE-2018-0285<br>… | Nhóm 19 lỗ hổng trên một số sản phẩm, dịch vụ của Cisco (Wireless LAN Controller, Aironet Access point, Fire Power System Software, Meeting Server, Prime File Upload…) cho phép đối tượng thực hiện nhiều hình thức tấn công như tấn công từ chối dịch vụ, tấn công khai thác các điểm yếu ứng dụng web, đánh cắp thông tin hệ thống, chèn và thực thi mã lệnh, đưa tập tin độc hại, hay | Đã có thông tin xác nhận và bản vá. |

| | | | | |
|---|---|---|---|---|
| | | | chiếm quyền quản trị đối với các thiết bị phát wifi Airnonet Acess Point. | |
| 2 | D-link | CVE-2018-10641<br>CVE-2018-10750<br>CVE-2017-17020<br>… | Nhóm 8 lỗ hổng trên các dòng sản phẩm của D-Link cho phép đối tượng thực hiện nhiều hình thức tấn công như: thực thi mã lệnh (trên DCS-5009 và DSL-3782 EU), đánh cắp và thay đổi mật khẩu (trên dòng DIR 601 A1 1.02NA) … | Chưa có thông tin xác nhận và bản vá. |
| 3 | Dasan GPON | CVE-2018-10561<br>CVE-2018-10562 | 02 lỗ hổng trên các thiết bị home router GPON cho phép đối tượng tấn công vượt qua cơ chế xác thực, chèn và thực thi mã lệnh để kiểm soát thiết bị. Việt Nam có ít nhất 152,617 thiết bị đang công khai trên Internet. Nhiều thiết bị home router của các hãng mạng hỗ trợ GPON như Tplink, Netgear, Asus, Linksys, Dlink đều có khả năng bị ảnh hưởng. | Đã có mã khai thác.<br><br>Chưa có thông tin bản vá. |
| 4 | Wordpress | CVE-2018-10752<br>CVE-2018-10371<br>CVE-2018-10504 | 3 lỗ hổng trên các plugin của Wordpress cho phép đối tượng thực hiện tấn công XSS, chèn và thực thi mã HTML/script và lây nhiễm mã độc qua tệp CSV (Web Dorado.) Lỗ hổng CVE-2018-10371 và CVE-2018-10504 đã có mã khai thác. | Đã có mã khai thác.<br><br>Chưa có thông tin xác nhận và bản vá. |
| 5 | TP-Link | CVE-2018-10168<br>CVE-2018-10167<br>CVE-2018-10166<br>CVE-2018-10165<br>CVE-2018-10164 | Nhóm 05 lỗ hổng trên phần mềm quản lý tập trung (EAP Controller và Omada Controller) các thiết bị qua trình duyệt web của TP-Link cho phép đối tượng thực hiện | Đã có bản vá. |

| | | | | |
|---|---|---|---|---|
| | | | các lệnh của quản trị viên chỉ với đặc quyền của người dùng bình thường cũng như chèn và thực thi mã lệnh, thực hiện hình thức tấn công trên ứng dụng web như XSS, CSRF. | |
| 6 | D-link | CVE-2018-10996<br>CVE-2018-10957 | Nhóm 02 lỗ hổng trên 2 dòng router của D- link cho phép đối tượng thực hiện chèn và thực thi mã lệnh, tấn công từ chối dịch vụ (trên dòng DIR-629-B1) và tấn công CSRF (trên dòng DIR 868L). | Chưa có thông tin xác nhận và bản vá. |
| 7 | Google | CVE-2017-6289<br>CVE-2018-6246<br>CVE-2018-6293<br>CVE-2018-6254 | Nhóm 4 lỗ hổng trên một số phần mềm (NVIDIA-TEE, NVIDIA-Widevine-Trustlet, NVIDIA Terga-X1-TZ, NVIDIA-Media-Server) được hệ điều hành Android của Google sử dụng có thể dẫn đến chiếm đặc quyền và thất thoát thông tin. | Đã có thông tin xác nhận và bản vá. |
| 8 | Huawei | CVE-2018-7933<br>CVE-2018-7941<br>CVE-2018-1940 | Nhóm 3 lỗ hổng trên một số sản phẩm của Huawei cho phép đối tượng thực hiện chèn và thực thi mã lệnh (đối với HiRouter-CD02) cũng như bỏ qua yêu cầu xác thực (iBMC V200R002C60 và Mate 10/Mate 10 Pro). | Đã có thông tin xác nhận và bản vá. |
| 9 | Lenovo | CVE-2018-9063 | Lỗ hổng trên MapDrv (C:\Program Files\Lenovo\System Update\mapdrv.exe) của Lenovo System Update trước phiên bản 5.07.0072 cho phép đối tượng thực hiện hành động trái phép bao gồm cả chèn và thực thi mã lệnh. | Đã có thông tin xác nhận và bản vá. |

| | | | | |
|---|---|---|---|---|
| 10 | Microsoft | CVE-2018-0765<br>CVE-2018-1039<br>CVE-2018-8119<br>CVE-2018-8145<br>CVE-2018-8179<br>… | Nhóm 85 lỗ hổng trên nhiều sản phẩm, ứng dụng của Microsoft (.NET, .NET Core, Edge, Word, Excel, Internet Explorer, Chakra, Microsoft Edge, Exchange Server, SharePoint Server,…) cho phép đối tượng chèn và thực thi mã lệnh, tấn công từ chối dịch vụ và đánh cắp thông tin. | Đã có thông tin xác nhận. |
| 11 | Adobe | CVE-2018-10252<br>CVE-2018-11240<br>CVE-2018-4917<br>CVE-2017-11307<br>CVE-2018-4918<br>… | Nhóm 37 lỗ hổng trên nhiều sản phẩm của Adobe (Acrobat and Reader, Flash player, Cold Fusion,…) cho phép đối tượng tấn công thu thập thông tin, nhiều lỗ hổng cho phép chèn và thực thi mã lệnh, đưa tập tin độc hại lên hệ thống, tấn công leo thang và chiếm quyền quản trị. | Đã có thông tin xác nhận và bản vá.<br><br>Nhiều lỗ hổng đã có mã khai thác. |
| 12 | Asus | CVE-2017-5083<br>CVE-2018-5082<br>CVE-2018-5081 | Nhóm 03 lỗ hổng trên firmware của một số dòng các dòng thiết bị định tuyến router ASUS (RT-AC1200HP, RT-AC68U, RT-AC87U) cho phép đối tượng thực hiện chèn và thực thi đoạn mã độc hại để chiếm quyền kiểm soát thiết bị. | Đã có thông tin xác nhận và bản vá. |
| 13 | Cisco | CVE-2018-0268<br>CVE-2018-0222<br>CVE-2018-0271<br>CVE-2018-0323<br>CVE-2018-0279<br>… | Nhóm 17 lỗ hổng trên một số sản phẩm, dịch vụ của Cisco (Digital Network Architecture Center, Interprise NFV Infrastructure Software, Indentity Service Engine,…) cho phép đối tượng không chế thiết bị, chiếm quyền quản trị hoặc thực hiện các hình thức tấn | Đã có thông tin xác nhận và bản vá. |

| | | | | |
|---|---|---|---|---|
| | | | công XSS, XFS, nhiều lỗ hổng cho phép chèn và thực thi mã lệnh. | |
| 14 | D-link | CVE-2018-10967<br>CVE-2018-10968 | Nhóm 3 lỗ hổng trên một số dòng router của D-link (DIR-550A, DIR-604M, DIR-816 A2) cho phép đối tượng thực thi mã lệnh và truy cập trái phép vào thiết bị. | Chưa có thông tin xác nhận và bản vá. |
| 15 | Foxit | CVE-2018-9961<br>CVE-2018-9958<br>CVE-2018-9941<br>CVE-2018-10492<br>CVE-2018-9949<br>… | Nhóm 81 lỗ hổng trên nhiều phiên bản Foxit Reader - phần mềm đọc file pdf được sử dụng phổ biến ở Việt Nam cho phép đối tượng chèn và thực thi mã lệnh nếu người dùng truy cập thông qua trang web hoặc mở một tệp độc hại. | Đã có thông tin xác nhận và bản vá. |
| 16 | Intel | CVE-2018-3661<br>CVE-2018-3611<br>CVE-2018-3634 | Nhóm 03 lỗ hổng trên các một số sản phẩm, dịch vụ của Intel (Configuration Utilities, Graphics Driver, Online Connect Access) cho phép đối tượng thực hiện tấn công từ chối dịch vụ. | Đã có thông tin xác nhận và bản vá. |
| 17 | Qualcomm | CVE-2018-3568<br>CVE-2018-15855<br>CVE-2018-3567<br>CVE-2018-5827 | 4 lỗ hổng trên các hệ Android (Android for MSM, Firefox OS for MSM và QRD Android) sử dụng lõi Linux trước bản vá ngày 5 tháng 4 năm 2018 chép đối tượng làm tràn và ghi đè bộ đệm. | Đã có thông tin xác nhận và bản vá. |
| 18 | Wordpress | | Nhóm 12 lỗ hổng trên một loạt các tiện ích và tính năng của WordPress trước phiên bản 2.0.4 (Open Graph, Ultimate member, Google Map,…) cho phép đối tượng | Đã có thông tin xác nhận và bản vá. |

| | | | | |
|---|---|---|---|---|
| | | | thực hiện chèn và thực thi đoạn mã độc hại. | |
| 19 | Adobe | CVE-2018-4918<br>CVE-2018-4917<br>CVE-2018-4941<br>CVE-2018-4938<br>CVE-2018-4942<br>… | Nhóm 31 lỗ hổng trên nhiều sản phẩm của Adobe (Acrobat and Reader, Flash player, Cold Fusion,…) cho phép đối tượng tấn công thực hiện chèn và thực thi mã lệnh, tấn công leo thang hoặc đánh cắp thông tin. | Đã có thông tin xác nhận và bản vá, nhiều lỗ hổng đã có mã khai thác. |
| 20 | Dlink | CVE-2018-8898 | Lỗ hổng trên cơ chế xác thực trên dòng thiết bị Router DSL-3782 của Dlink cho phép đối tượng tấn công đọc và thay đổi mật khẩu cũng như cấu hình từ xa khi quản trị viên đăng nhập qua web. | Đã có mã khai thác. |
| 21 | Foxit | CVE-2018-5679<br>CVE-2018-5676<br>CVE-2018-7406<br>CVE-2018-7407<br>CVE-2018-5674<br>… | Nhóm 09 lỗ hổng trên phần mềm đọc file PDF Foxit Reader cho phép đối tượng thực thi mã lệnh khi người dùng mở sử dụng một trang web hoặc tập tin PDF độc hại. | Đã có thông tin xác nhận và bản vá. |
| 22 | Huawei | CVE-2018-7903<br>CVE-2018-7904<br>CVE-2018-7942<br>CVE-2018-17158<br>CVE-2018-17315<br>… | Nhóm 6 lỗ hổng trên một số sản phẩm điện thoại thông minh, thiết bị định tuyến và ứng dụng quản lý iBMC của Huawei cho phép đối tượng tấn công lây nhiễm JSON để thay đổi mật khẩu hệ thống, cũng như đánh cắp thông tin và chiếm quyền quản trị. | Đã có thông tin xác nhận. |
| 23 | Microsoft | CVE-2018-8176<br>CVE-2018-8142 | Nhóm 02 lỗ hổng trên Microsoft PowerPoint và Windows cho phép đối tượng tấn công thực thi mã lệnh và vượt qua các tính năng bảo mật của Windows để thực hiện những hành vi trái phép | Đã có thông tin xác nhận. |

| | | | | |
|---|---|---|---|---|
| | | | trên hệ thống. | |
| 24 | VMware | CVE-2018-6962<br>CVE-2018-6963 | 02 lỗ hổng trên VMware Fusion (trước phiên bản 10.1.2) và VMware Workstation (trước phiên bản 14.1.2) cho phép đối tượng thực hiện tấn công leo thang đặc quyền và tấn công từ chối dịch vụ. | Đã có thông tin xác nhận và bản vá. |
| 25 | Joomla | CVE-2018-6378<br>CVE-2018-11321<br>CVE-2018-11327<br>CVE-2018-11326<br>... | Nhóm 09 lỗ hổng trên một số thành phần (Joomla! Core, ) của phần mềm quản trị nội dung Joomla cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau gồm: tấn công XSS, chèn và thực thi mã lệnh trên hệ thống trong phạm vi quyền của ứng dụng; ăn trộm thông tin xác thực người dùng.<br>Quản trị viên cần cập nhật lên phiên bản mới (3.8.8). | Đã có xác nhận và bản vá. |

***2.5. Hoạt động một số mạng botnet, APT, mã độc***

2.5.1 Danh sách các mạng botnet

- Mạng botnet Mirai
- Mạng botnet Sality
- Mạng botnet Conficker
- Mạng botnet Andromeda
- Mạng botnet Ramnit

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

| TT | Tên miền/IP |
|---|---|
| 1 | 3d3bulnt.ru |
| 2 | 104.244.14.252 |
| 3 | kukutrustnet777.info |
| 4 | qzf163kfd.ru |
| 5 | and31.blllaaaaaazblaaa3.com |

| | |
|---|---|
| 6 | kukutrustnet888.info |
| 7 | g.omlao.com |
| 8 | u.amobisc.com |
| 9 | facialwaxmaxfaxlax3.com |
| 10 | init.icloud-analysis.com |
| 11 | ye5cvvufx.ru |
| 12 | z4kzt27u8.ru |
| 13 | st40pwch.ru |
| 14 | b1pzjdesv.ru |
| 15 | eznnxm.info |
| 16 | p.omlao.com |
| 17 | p2xtz27i32.ru |
| 18 | ei3rvgfk.ru |

**3. Tình hình an toàn, an ninh thông tin tại Bộ Tài nguyên và Môi trường**

***3.1. Tình hình triển khai các quy định pháp luật về an toàn thông tin***

Nhận thức được tầm quan trọng của an toàn thông tin đối với các hệ thống thông tin chuyên ngành, Bộ Tài nguyên và Môi trường đã chủ động, tích cực tuyên truyền, phổ biến các văn bản quy phạm pháp luật liên quan đến an toàn, an ninh thông tin trong đó có luật an toàn thông tin mạng năm 2015; các Nghị định, Quyết định của Chính phủ, các công văn hướng dẫn, cảnh báo về an ninh và an toàn thông tin mạng.

Trên cơ sở Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Bộ Tài nguyên và Môi trường đã ban hành Kế hoạch triển khai nhiệm vụ bảo đảm an toàn, an ninh thông tin của Bộ Tài nguyên và Môi trường giai đoạn 2018-2020 (Quyết định số 3313/QĐ-BTNMT ngày 25 tháng 12 năm 2017).

Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường đã chủ trì, phối hợp với Cục An toàn thông tin - Bộ Thông tin và Truyền thông tổ chức khóa đào tạo về bảo đảm an toàn hệ thống thông tin theo cấp độ cho các cán bộ chuyên trách về an toàn thông tin và công nghệ thông tin tại các đơn vị trực thuộc Bộ Tài nguyên và Môi trường vào ngày 01/02/2018.

***3.2. Công tác kiểm tra giám sát, cảnh báo về an toàn thông tin***

Trên cơ sở các trang thiết bị công nghệ được đầu tư từ dự án xây dựng hệ thống An toàn thông tin số tài nguyên và môi trường trên mạng, Cục đã chủ động đầu tư đến đâu đưa vào sử dụng đến đó nhằm bảo vệ, phòng ngừa, ngăn chặn, theo dõi hệ thống mạng của Bộ, các hệ thống dùng chung như: Cổng thông tin điện tử, hệ thống

thư điện tử, hệ thống quản lý văn bản và hồ sơ công việc, hệ thống dịch vụ công, các hệ thống thông tin và Website của các đơn vị.

Trong tháng 5, Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường đã tiến hành rà soát hệ thống mạng và tình hình đảm bảo an toàn thông tin cho một số đơn vị. Kết quả rà soát cho thấy một số vấn đề chung gây ảnh hưởng đến hệ thống mạng và an toàn thông tin như sau:

- Thiết bị người dùng: nhiều máy tính người dùng dùng hệ điều hành không có bản quyền hoặc đã hết vòng đời (dừng phát hành bản vá lỗi từ hãng). Do đó, dẫn đến không thể cập nhật các bản vá lỗi bảo mật, tồn tại nhiều lỗ hổng bảo mật nghiêm trọng như ms17-010.

- Xuất hiện tình trạng rất nhiều máy tính người sử dụng bị nhiễm mã độc ransomware WannaCry, trong đó nhiều máy đã bị mã hóa dữ liệu.

*3.2.1. Các hình thức vi phạm an ninh và tấn công mạng chủ yếu*

- Dò quét mật khẩu các cổng quản trị máy chủ được public ra Internet.

- Dò quét lỗ hổng các dịch vụ - đặc biệt là website (cổng thông tin điện tử bộ, thư điện tử, quản lý hồ sơ công việc, ...).

- Nhiều máy tính nội bộ (máy tính của người sử dụng) nhiễm mã độc kết nối tới máy chủ điều khiển - C&C, thực hiện tấn công các máy chủ nội bộ và các IP trên mạng Internet.

- Hiện tượng người dùng lộ mật khẩu tài khoản, bị hacker lợi dụng để gửi thư rác, thư có nội dung không phù hợp, thư chứa mã độc ra Internet.

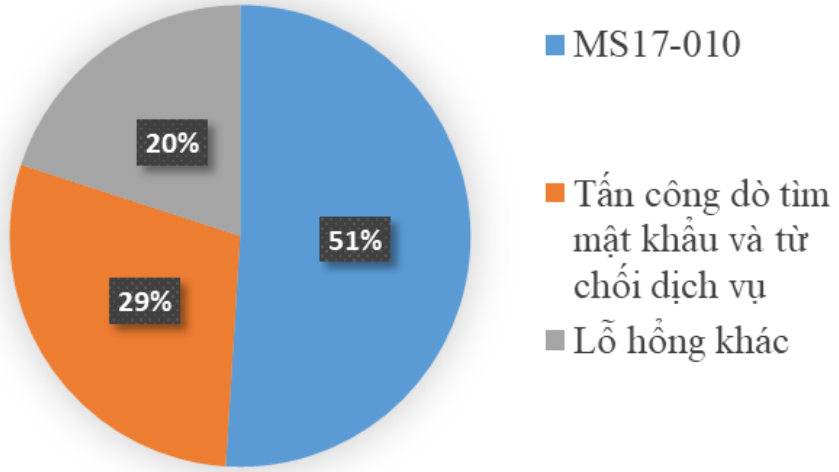
- Thư rác, thư chứa mã độc từ bên ngoài gửi tới dịch vụ thư điện tử Bộ.

*3.2.2. Các số liệu thống kê*

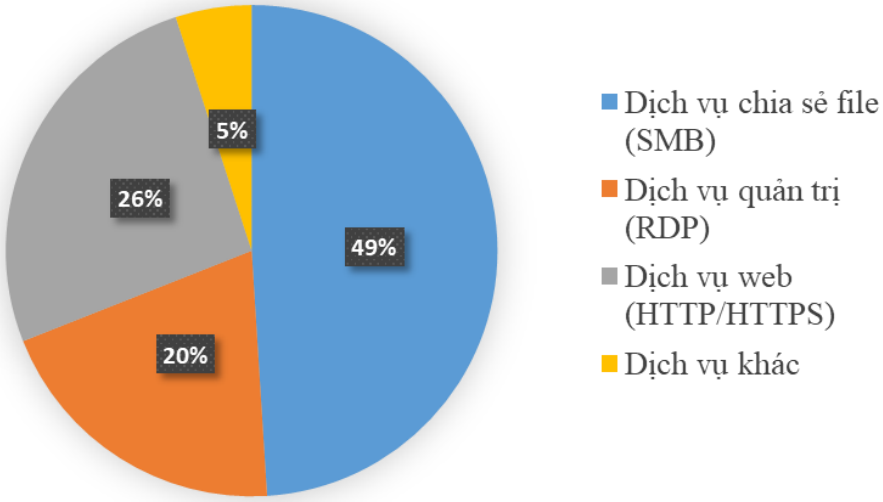
Qua công tác theo dõi từ hệ thống giám sát của Bộ thấy xuất hiện các cuộc tấn công mạng vào hệ thống mạng của Bộ được ghi nhận và ngăn chặn:

| Mục | Tỉ lệ |
|---|---|
| **Tổng số cuộc tấn công mạng được ghi nhận và ngăn chặn thông qua hệ thống bảo mật của Bộ.** | 121,556 Cuộc tấn công; Trong đó tỉ lệ các cuộc tấn công mạng mức độ trung bình và nghiêm trọng là 3.5% |
| **1. Danh sách các lỗ hổng bị tấn công khai thác nhiều nhất** | |
| - MS17-010 | 51 (%) |
| - Tấn công dò tìm mật khẩu và từ chối dịch vụ qua: giao thức quản trị (Remote Desktop, SSH); qua hệ thống thư điện tử (IMAP, POP3, SMTP, OWA) | 29 (%) |

| | |
|---|---|
| - Lỗ hổng khác | 20 (%) |




| **2. Danh sách các dịch vụ bị tấn công nhiều nhất** | |
|---|---|
| - Dịch vụ chia sẻ file của windows (cổng 445) | 49 (%) |
| - Dịch vụ quản trị Remote Desktop | 20 (%) |
| - Dịch vụ web (cổng 80, 443) | 26 (%) |
| - Dịch vụ khác | 5 (%) |

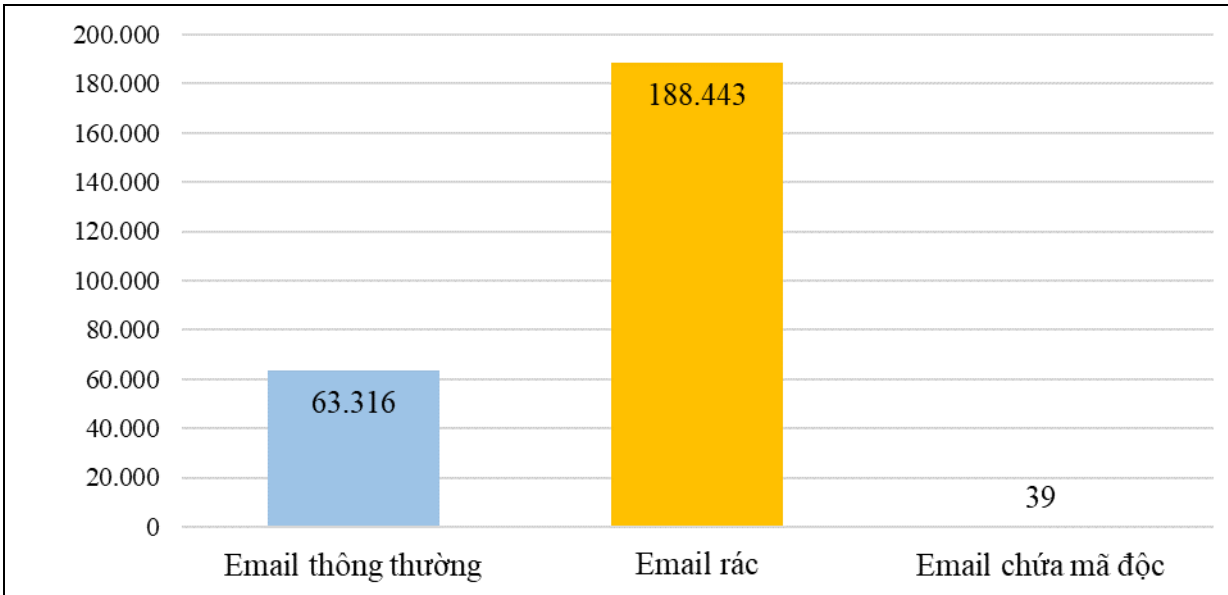



| **3. Danh sách các loại virus, botnet phát hiện trong hệ thống mạng** | |
|---|---|
| - Loại virus | Andromeda.TC.gabbaaabb<br>Andromeda.TC.ijfgeghbh<br>Backdoor.PHP.Peg.gen.TC.bq<br>Compromisedsite.hg<br>Cryptocurrency.c<br>Cryptominer.TC.jfjdjcabf<br>Generic.TC.bxeza<br>Generic.TC.geacfaabg<br>infecting website.ivhuby.a |

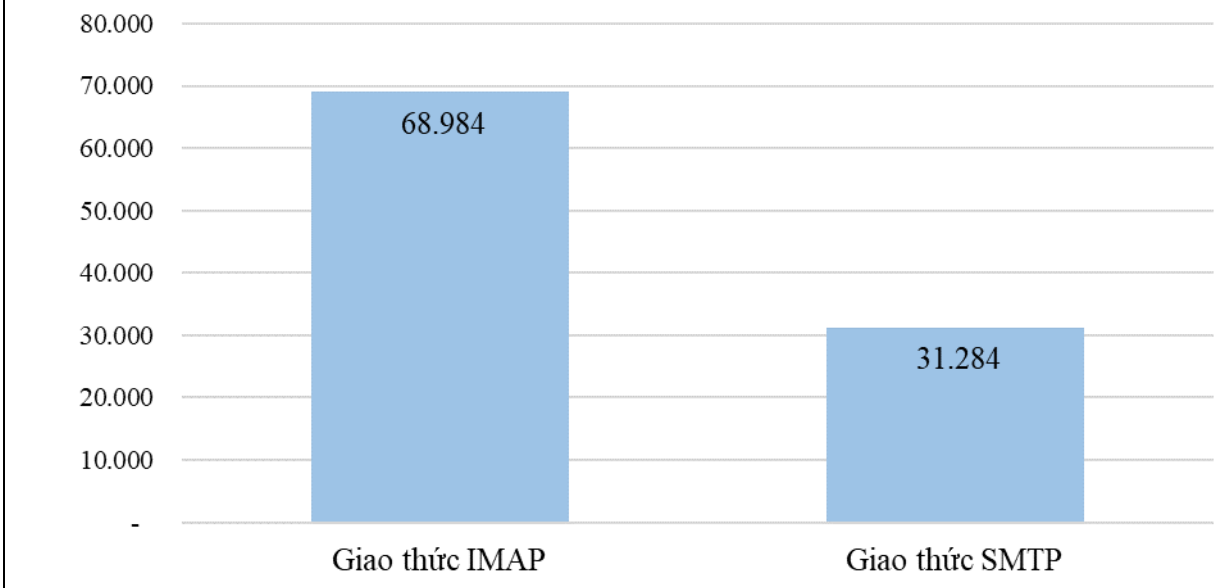
| | |
|---|---|
| | Malware.ysxfb<br>Phishing.dgnxfe<br>Phishing.dhsfqk<br>REP.ibwggn<br>REP.iuijmb<br>REP.TC.ggrb<br>REP.TC.mhmu<br>REP.TC.ohxc<br>Trojan.Win32.Generic.bdepc |
| - Mạng botnet | Andromeda.TC.fabbaaabb<br>BotnetB.TC.eoe<br>Dorkbot.TC.in<br>Nitol.TC.f<br>Operator.cnc server.mkgwhc.a<br>Trojan-Downloader.Win32.Necorapo.A<br>Trojan-Ransom.Win32.WannaCry.A |
| **4. Nhiều máy tính người dùng nhiễm mã độc** | |
| Nhiều máy tính người dùng nhiễm mã độc (khoảng 63 máy) tấn công các máy chủ trong mạng nội bộ. Lỗ hổng chủ yếu bị nhắm đến trong các cuộc tấn công là ms17-010, các lỗ hổng giao thức SMB v1. | Các máy tính nhiễm mã độc thực hiện tấn công đã được ghi nhận để tiến hành xử lý. |

Lượng thư rác và mã độc thông qua hệ thống thư điện tử của Bộ trong tháng 5:

| **Mục** | **Số liệu thống kê** |
|---|---|
| **1. Thống kê chung về gửi nhận mail** | |
| - Tổng lượng email gửi nhận | 251,798 (email) |
| - Tỉ lệ thư rác | 74.84 (%) (khoảng 188,443 email) |
| - Tỉ lệ email chứa mã độc | 0.02 (%) (39 email) |




| **2. Thống kê chung về hành động tấn công nhằm vào hệ thống mail** | |
|---|---|
| - Tổng số cuộc tấn công dò tìm mật khẩu từ nước ngoài vào hệ thống mail | 100,268 (lượt dò tìm mật khẩu) |
| - Các dịch vụ mail bị tấn công nhiều nhất | IMAP (68.8% số cuộc tấn công)<br>SMTP (31.2% số cuộc tấn công) |
| - Số lượng tài khoản nghi ngờ mất mật khẩu | 12 (tài khoản) |




**3. Tài khoản có dấu hiệu mất mật khẩu.**

Trong tháng 5, ghi nhận từ hệ thống giám sát 12 tài khoản có dấu hiệu đăng nhập từ IP nước ngoài. Trong đó:

| | |
|---|---|
| - 02 trường hợp tài khoản thư điện tử người dùng bị mất mật khẩu; bị hacker lợi dùng để thực hiện gửi thư | Các tài khoản bị mất mật khẩu đã được xử lý kịp thời, không gây ảnh hưởng lớn tới hệ thống thư điện tử. |

| | |
|---|---|
| có nội dung độc hại ra internet. | |
| - 01 trường hợp tài khoản thư điện tử người dùng mất mật khẩu; bị hacker lợi dụng phát tán 68 thư có nội dung lừa đảo - yêu cầu người dùng nhập mật khẩu tài khoản. | Thư có nội dung lừa đảo đã được phát hiện kịp thời để cảnh báo người dùng và xóa khỏi hệ thống. |
| - Các tài khoản còn lại đang được nhóm giám sát theo dõi, phối hợp với đầu mối các đơn vị để xử lý. | Rất nhiều tài khoản trong số này đã được người dùng đổi mật khẩu, song hiện tượng đăng nhập từ IP nước ngoài vẫn tiếp diễn. Nhóm giám sát xác định khả năng thiết bị và máy tính của người dùng bị nhiễm mã độc là rất cao. |

**4. 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 Công nghệ thông tin và Dữ liệu tài nguyên môi trường khuyến nghị:

- Người dùng cần phải hết sức cảnh giác với những trang web giả mạo có nguy cơ đánh cắp tài khoản, đặc biệt là các trang web giả mạo các ứng dụng, dịch vụ phổ biến.

- Chủ động rà soát, tăng cường triển khai các giải pháp đảm bảo an toàn thông tin cho các hệ thống thông tin của cơ quan; xây dựng, rà soát các phương án phòng chống tấn công mạng, ứng cứu sự cố và hoạt động dự phòng trong trường hợp hệ thống bị tấn công.

- Cử cán bộ kỹ thuật trực theo dõi, giám sát liên tục hệ thống để kịp thời phát hiện các dấu hiệu bất thường, xử lý kịp thời các vấn đề phát sinh nếu có.

- Chỉ được sử dụng tài khoản công vụ trong công việc, không sử dụng tài khoản công vụ để đăng nhập vào các trang web, mạng xã hội, ...

- Theo dõi, cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng bảo mật.

- Chủ động kiểm tra, rà soát, bóc gỡ mã độc ra khỏi máy tính người dùng, hệ thống mạng.

- 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.

- Tăng cường sử dụng chữ ký số khi gửi thư điện tử có kèm theo mã hóa thư điện tử và dữ liệu kèm theo (hệ thống thư điện tử của Bộ đã được tích hợp chữ ký số để mã hóa nội dung thư gửi).

Trên đây là báo cáo tình hình an toàn, an ninh thông tin tháng 05/2018 của Bộ Tài nguyên và Môi trường, Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường gửi các đơn vị để biết và phối hợp thực hiện./.