BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG
CỤC CÔNG NGHỆ THÔNG TIN VÀ DỮ LIỆU TÀI NGUYÊN MÔI TRƯỜNG

Số: 626 /CNTT-KHCN
V/v báo cáo tình hình an toàn, an ninh thông tin tháng 10/2020

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 30 tháng 10 năm 2020

Kính gửi: Các đơn vị trực thuộc Bộ

Thực hiện chức năng nhiệm vụ về bảo đảm an ninh, an toàn và bảo mật thông tin đối với các hệ thống thông tin, cơ sở dữ liệu của Bộ, Ngành tài nguyên và môi trường; Qua công tác thu thập, theo dõi, trích xuất, dò quét, phân tích về an toàn thông tin trong tháng 10 năm 2020, Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường xin gửi báo cáo tóm tắt về tình hình về an toàn, an ninh thông tin đến các đơn vị trực thuộc Bộ (kèm theo công văn).

Các nội dung về tình hình về an toàn, an ninh thông tin được Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường cập nhật trên trang web: http://attt.dinte.gov.vn/.

Kính đề nghị các đơn vị theo dõi để tham khảo và có biện pháp chủ động 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
CỤC CÔNG NGHỆ THÔNG TIN VÀ DỮ LIỆU TÀI NGUYÊN MÔI TRƯỜNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 30 tháng 10 năm 2020

BÁO CÁO

TÌNH HÌNH AN TOÀN, AN NINH THÔNG TIN THÁNG 10/2020

(Kèm theo Công văn số 626 /CNTT-KHCN ngày 30 /10/2020 của Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường)

1. Tình hình an toàn thông tin chung

1.1. Tình hình an toàn thông tin trên thế giới

Trong tháng 10 năm 2020, tình hình an toàn thông tin trên thế giới có các thông tin nổi bật sau:

1.1.1. Lỗ hổng trong chip bảo mật T2 của Apple dễ bị khai thác qua USB-C.

Chip bảo mật T2 của Apple được sử dụng trong các thiết bị Mac của Intel để xử lý khả năng lưu trữ được mã hóa và khởi động an toàn, cũng như 1 số tính năng khác. Chip này dựa trên bộ vi xử lý Apple A10, và điều này cũng là lý do dễ bị tấn công bởi "checkm8" đã được sử dụng để bẻ khóa các thiết bị iOS.

Lỗ hổng cho phép đối tượng tấn công chiếm quyền điều khiển quá trình khởi động của T2 để truy cập vào phần cứng. Sau khi có được quyền truy cập, đối tượng tấn công sẽ chiếm được quyền truy cập root, có thể tạo keylogger và đánh cắp mật khẩu, mã hóa ổ đĩa.

Việc khai thác có thể đạt được mà không cần sự tương tác của người dùng, chỉ cần cắm cáp USB-C độc hại. Đối tượng tấn công tạo ra 1 thiết bị chuyên dụng, đặt chip T2 vào chế độ DFU, chạy khai thác "checkra1n" tải lên trình ghi khóa và thu thập tất cả các khóa. MacOS có thể không bị thay đổi sau khi bẻ khóa, nhưng tất cả các khóa vẫn có thể được đăng nhập trên máy tính xách tay Mac. Điều này là do bàn phím của MacBook được kết nối trực tiếp với T2 và chuyển qua MacOS.

Apple vẫn chưa vá lỗi bảo mật này. Vì mục đích bảo mật, hệ điều hành tùy chỉnh SepOS của T2 được lưu trữ trực tiếp trong SEPROM của chip, nhưng điều này cũng ngăn việc khai thác thông qua bản cập nhật phần mềm. Trong thời gian chờ đợi Apple phát hành bản vá, người dùng có thể ngăn chặn, giảm thiểu rủi ro bị tấn công bằng cách giữ an toàn vật lý cho máy Mac và tránh việc cắm các thiết bị vào cáp USB-C không đáng tin cậy.

1.1.2. Cảnh báo lỗ hổng Instagram.

Các nhà nghiên cứu của Check Point phát hiện ra một lỗ hổng có ảnh hưởng cao (CVE-3030-1895) trên ứng dụng Instagram, cho phép đối tượng tấn công chèn và thực thi mã từ xa và truy cập vào máy ảnh, micrô,…của mục tiêu.

CVE-2020-1895 có điểm CVSS 7,8 (cao), ảnh hưởng đến phiên bản Instagram trước 128.0.0.26.128 trên cả hệ điều hành Android và iOS. Lỗ hổng tồn tại do cách xử lý các thư viện của bên thứ 3, cụ thể là khi sử dụng Mozjpeg (đóng vai trò như 1 bộ giải mã định dạng JPEG cho các hình ảnh được tải lên ứng dụng chia sẻ ảnh) của ứng dụng Instagram.

Đối tượng tấn công chỉ cần gửi hình ảnh độc hại đến thiết bị mục tiêu qua WhatsApp, văn bản, email hoặc bất kỳ dịch vụ nhắn tin nào khác. Người dùng lưu hình ảnh vào điện thoại của họ. Sau này khi mở Instagram, mã sẽ được thực thi và cho phép đối tượng tấn công truy cập và kiểm soát tất cả dữ liệu trên điện thoại có liên kết với Instagram (như máy ảnh của thiết bị, dịch vụ GPS / vị trí, danh bạ và bộ nhớ,…).

Ở cấp độ cơ bản nhất, việc khai thác có thể được sử dụng để làm hỏng ứng dụng Instagram của người dùng, từ chối họ truy cập vào ứng dụng cho đến khi họ xóa nó khỏi thiết bị và cài đặt lại. Nhưng bên cạnh đó, việc khai thác này sẽ không ảnh hưởng trên điện thoại bị vô hiệu hóa quyền đối với Instagram.

1.1.3. Cảnh báo 17 ứng dụng Android bị nhiễm phần mềm độc hại Joker

Cuối tháng 9 vừa qua, Google đã xóa 17 ứng dụng Android bị nhiễm phần mềm đọc hại Joker (Bread) khỏi Play Store. Joker là một trong những mối đe dọa lâu dài và tiên tiến mà Google đã đối phó trong những năm qua. Google đã xóa hơn 1.700 ứng dụng khỏi Play Store kể từ năm 2017.

Phần mềm gián điệp này được thiết kế để đánh cắp tin nhắn SMS, danh sách liên hệ và thông tin thiết bị, đồng thời đăng ký cho người dùng các dịch vụ giao thức ứng dụng không dây WAP. 17 ứng dụng độc hại đã được tải xuống hơn 120.000 lần trước khi bị phát hiện, chúng bao gồm như: Tangram App Lock, Direct Messenger, Private SMS, Desire Translate,…

Theo quy trình, Google đã xóa ứng dụng khỏi Play Store, sử dụng dịch vụ Play Protect để tắt ứng dụng trên các thiết bị bị nhiễm, nhưng người dùng vẫn cần thêm thao tác xóa ứng dụng khỏi thiết bị của mình.

Đối tượng tấn công sao chép chức năng của 1 ứng dụng hợp pháp và tải nó lên Play Store. Ứng dụng này có đầy đủ chức năng, yêu cầu quyền truy cập, nhưng cũng không thực hiện bất kỳ hành động độc hại nào khi nó chạy lần đầu tiên. Vì sự trì hoãn này nên quá trình quét bảo mật của Google không phát hiện ra mã độc hại.

1.1.4. Cảnh báo tấn công APT nhắm vào hệ thống mạng chính phủ, tiểu bang, địa phương, ... có mục đích liên quan đến việc bầu cử.

Gần đây, CISA (Cybersecurity and Infrastructure Security Agency) đã phát hiện các chiến dịch khai thác chuỗi lỗ hổng bảo mật để chiếm quyền truy cập vào hệ thống mạng hoặc các ứng dụng của các nhóm đối tượng tấn công APT, nhằm mục tiêu vào các hệ thống mạng của chính phủ liên bang, tiểu bang, địa phương,…đặc biệt nghi ngờ các nhóm đang nhằm mục tiêu liên quan đến việc bầu cử.

Một số khai thác khai thác lỗ hổng liên quan đến mạng riêng ảo (VPN), lổ hổng trong Netlogon, lỗ hổng MobileIron CVE-2020-15505,… Sau khi có quyền truy cập ban đầu, đối tượng tấn công khai thác lỗ hổng CVE-2020-1472 để truy cập tất cả các dịch vụ nhận dạng Active Directory (AD). Từ đó sử dụng các công cụ điều khiển từ xa như VPN, RDP để truy cập với thông tin đăng nhập thu thập được.

1.2. Tình hình an toàn thông tin tại Việt Nam

Trong tháng 10 năm 2020, tình hình an toàn thông tin tại Việt Nam có các thông tin nổi bật sau:

1.2.1. Website/Cổng thông tin điện tử là kênh cung cấp thông tin hiệu quả tuy nhiên hầu hết chưa được quan tâm đúng mức đến việc bảo đảm an toàn thông tin, rất nhiều trang tồn tại điểm yếu, lỗ hổng bảo mật, đối tượng tấn công có thể khai thác để thực hiện: tấn công thay đổi giao diện, tấn công lừa đảo thu thập thông tin tài khoản, thông tin cá nhân, tấn công cài cắm và phát tán mã độc.

Có 507 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam, trong đó: 6 trường hợp tấn công thay đổi giao diện, 136 trường hợp tấn công lừa đảo (Phishing), 365 trường hợp tấn công cài cắm mã độc.

1.2.2. Nguy cơ phát tán tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ là hình thức tấn công đã có từ lâu và hiện tại vẫn được đối tượng tấn công ưa thích sử dụng để thực hiện các ý đồ xấu. Tấn công từ chối dịch vụ về cơ bản không nguy hiểm nhưng lại gây ảnh hưởng đến hoạt động của hệ thống, gây thiệt hại về kinh tế cho tổ chức bị tấn công.

Tấn công từ chối dịch vụ có thể được thực hiện với nhiều kỹ thuật khác nhau, nhưng trong những năm gần đây phần lớn tin tặc huy động các thiết bị đang mở cổng dịch vụ sử dụng giao thức UDP để thực hiện tấn công. Các thiết bị này có thể bị huy động dễ dàng để thực hiện tấn công DRDoS (tấn công từ chối dịch vụ phản xạ phân tán/Distributed Reflective Denial-of-Service) mà hiệu quả tấn

công lại rất cao. Rất nhiều giao thức tầng ứng dụng đều có điểm yếu/lỗ hổng cho phép thực hiện tấn công này.

Tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tháng, có khoảng có 53.231 thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (cổng 123), DNS (cổng 53), Chargen (19).

1.2.3. Lỗ hổng điểm yếu về an toàn thông tin

Trong tháng 10 năm 2020, các tổ chức quốc tế đã công bố và cập nhật ít nhất 1.492 lỗ hổng, trong đó có 93 lỗ hổng mức cao, 292 lỗ hổng mức trung bình, 75 lỗ hổng mức thấp và 1.032 lỗ hổng chưa đánh giá. Trong đó có ít nhất 116 lỗ hổng cho phép chèn và thực thi mã lệnh. Tại Việt Nam, theo thống kê cho thấy có 29 lỗ hổng/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 86 lỗ hổng trong phần mềm Google, Nhóm 86 lỗ hổng trong phần mềm thiết bị Cisco, Nhóm 23 lỗ hổng trong các sản phẩm của IBM, Nhóm 04 lỗ hổng trong phần mềm Joomla, Nhóm 03 lỗ hổng trong sản phẩm của Lenovo, Nhóm 03 lỗ hổng trong phần mềm Adobe, Nhóm 02 lỗ hổng trong phần mềm Red_hat, Nhóm 16 lỗ hổng trong phần mềm Gitlab, Nhóm 15 lỗ hổng trong các phần mềm Mozilla, Nhóm 09 lỗ hổng trong phần mềm Apache, Nhóm 09 lỗ hổng trong phần mềm Mediawiki, Nhóm 06 lỗ hổng trong phần mềm Foxit, Nhóm 05 lỗ hổng trong các sản phẩm của IBM, Nhóm 05 lỗ hổng trong phần mềm Dpkg, Nhóm 05 lỗ hổng trong phần mềm thiết bị Wavlink, Nhóm 14 lỗ hổng trong phần mềm Gitlab, Nhóm 14 lỗ hổng trong phần mềm thiết bị Cisco, Nhóm 11 lỗ hổng trong phần mềm Google, Nhóm 06 lỗ hổng trong phần mềm Foxit, Nhóm 06 lỗ hổng trong các sản phẩm của IBM, Nhóm 05 lỗ hổng trong phần mềm thiết bị Wavlink, Nhóm 04 lỗ hổng trong phần mềm Redhat,Nhóm 85 lỗ hổng trong các phần mềm của Microsoft, Nhóm 29 lỗ hổng trong thiết bị Netgear, Nhóm 26 lỗ hổng trong các sản phẩm của IBM, Nhóm 25 lỗ hổng trong phần mềm Google, Nhóm 13 lỗ hổng trong phần mềm thiết bị Huawei, Nhóm 08 lỗ hổng trong phần mềm Foxit, Nhóm 05 lỗ hổng trong sản phẩm của Lenovo, v.v…

1.2.4. Thông tin về lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam

Danh sách và thông tin chi tiết các lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam xem tại Phụ lục 1.

1.2.5. Hoạt động một số mạng botnet, APT, mã độc

Danh sách các mạng botnet và danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam xem tại Phụ lục 2.

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

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

Để triển khai Chỉ thị số 14/CT-TTg, Cục Công nghệ thông tin và Dữ liệu tài

Trong tháng 9 năm 2020, Cục Công nghệ thông tin và Dữ liệu Tài nguyên môi trường đã gửi công văn số 528/CNTT-KHCN ngày 08 tháng 9 năm 2020 đến các đơn vị trong Bộ về việc triển khai công tác bảo đảm an toàn thông tin, hướng dẫn các đơn vị lập kế hoạch hồ sơ đề xuất cấp độ cho các hệ thống thông tin đang vận hành, rà soát tổng thể hệ thống thông tin đang vận hành, xây dựng kế hoạch và triển khai đánh giá an toàn thông tin theo mô hình 4 lớp, cử người tham gia Đội ứng cứu khẩn cấp sự cố an toàn thông tin của Bộ Tài nguyên và Môi trường. Hiện nay Cục đang tổng hợp để triển khai thực hiện theo kế hoạch.

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

Qua công tác dò quét hệ thống mạng của Bộ, các hệ thống dùng chung của Bộ và các Cổng thông tin / Trang thông tin điện tử của các đơn vị, đã phát hiện các hình thức tấn công mạng chủ yếu như sau:

- 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, thư có nội dung/liên kết lừa đảo từ bên ngoài gửi tới dịch vụ thư điện tử Bộ.

Thông tin chi tiết thống kê về các cuộc tấn công vào hệ thống mạng của Bộ Tài nguyên và Môi trường xem trong Phụ lục 3.

3. 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 các đơn vị trực thuộc Bộ:

- Truy cập trang web : http://attt.dinte.gov.vn/ để theo dõi hàng tháng các báo cáo, tổng hợp tình hình an toàn thông tin của Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường.

- Thường xuyên cập nhật tin tức từ các báo cáo của đơn vị chuyên trách về an toàn thông tin của Bộ, các cơ quan chuyên trách an toàn thông tin của Bộ thông tin truyền thông và các tin tức từ các chuyên gia bảo mật trên thế giới.

- Chỉ đạo cán bộ/bộ phận chuyên trách về an toàn thông tin cung cấp đầu mối kỹ thuật, đầu mối quản lý để thuận tiện cho việc liên lạc và phối hợp với bộ phận chuyên trách về an toàn thông tin của Bộ xử lý các vấn đề về an toàn thông tin của đơn vị mình.

- Phổ biến đến toàn bộ cán bộ, nhân viên trong đơn vị 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; 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, ...

- 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; 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.

- Phối hợp với Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường trong việc thực hiện các hoạt động xây dựng, thẩm định và phê duyệt hồ sơ đề xuất cấp độ và phương án bảo vệ cho các hệ thống thông tin tại Bộ nhằm triển khai có hiệu quả Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ.

- Để đảm bảo an toàn cho hệ thống thư điện tử cũng như toàn hệ thống mạng, các dịch vụ công công nghệ thông tin của Bộ, đề nghị người sử dụng thư điện tử khi nhận được thư dấu hiệu bất thường cần kiểm tra lại thông tin người gửi (tuyệt đối không nhấn và mở các file đính kèm, các liên kết, cung cấp thông tin tài khoản, mật khẩu,…). Người sử dùng nên đổi mật khẩu thường xuyên và đảm bảo độ khó của mật khẩu theo quy định.

Lưu ý: Tất cả các thông báo về hệ thống thư điện điện tử, các thông báo sửa chữa, nâng cấp các hệ thống CNTT của Bộ được gửi duy nhất từ địa chỉ mail citi@monre.gov.vn. Trong trường hợp nhận được thư điện tử có dấu hiệu bất thường cần thông báo cho đơn vị quản lý vận hành qua số điện thoại: 024 37956868 (số máy lẻ: 1005) và chuyển tiếp thư về địa chỉ mail citi@monre.gov.vn.

Trên đây là báo cáo tình hình an toàn, an ninh thông tin tháng 10/2020 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./.

PHỤ LỤC 1

(Kèm theo Công văn số 626 /CNTT-KHCN ngày 30 tháng 10 năm 2020 của Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường)

DANH SÁCH CÁC LỖ HỔNG TRÊN CÁC SẢN PHẨM/DỊCH VỤ PHỔ BIẾN TẠI VIỆT NAM (CẬP NHẬT THÁNG 10/2020)

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2020-0354 CVE-2020-6551 CVE-2020-6549 …	Nhóm 86 lỗ hổng trong phần mềm Google (Google Android; Google Chrome) cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, leo thang đặc quyền, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Cisco	CVE-2020-3414 CVE-2020-3426 CVE-2029-15992 …	Nhóm 86 lỗ hổng trong phần mềm thiết bị Cisco (Aironet Access Points, Low Power, Wide Area,…) cho phép đối tượng tấn công truy cập trái phép, tấn công từ chối dịch vụ, chèn và thực thi mã tùy ý,tấn công XSS, tấn công CSRF.	Chưa có thông tin xác nhận và bản vá
3	IBM	CVE-2020-4620 CVE-2020-4622 CVE-2020-4616 …	Nhóm 23 lỗ hổng trong các sản phẩm của IBM (Data Risk Manager 2.0.6) cho phép đối tượng tấn công thực thi mã tùy ý, thu thập thông tin, tấn công CSRF, chối dịch vụ, leo thang đặc công XXE Injection, XSS, hijacking.	Đã có thông tin xác nhận và bản vá
4	Joomla	CVE-2020-19447 CVE-2020-19455 CVE-2020-19450 …	Nhóm 04 lỗ hổng trong phần mềm Joomla (Joomla 3.2.63) cho phép đối tượng tấn công thu thập thông tin.	Chưa có thông tin xác nhận và bản vá

5	Lenovo	CVE-2020-8333 CVE-2020-8347 CVE-2020-8348	Nhóm 03 lỗ hổng trong sản phẩm của Lenovo (Desktops, ThinkStation, Enterprise Network Disk) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công XSS.	Đã có thông tin xác nhận và bản vá
6	Adobe	CVE-2020-9745 CVE-2020-9744 CVE-2020-9739	Nhóm 03 lỗ hổng trong sản phẩm của Lenovo (Desktops, Thinkstation, Enterprise Network Disk) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công XSS	Đã có thông tin xác nhận và bản vá
7	Red_hat	CVE-2020-14365 CVE-2020-10687	Nhóm 02 lỗ hổng trong phần mềm Red_hat (Ansible Engine, Undertow) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, thu thập thông tin.	Đã có thông tin xác nhận và bản vá
8	Gitlab	CVE-2020-13296 CVE-2020-13321 CVE-2020-13322 …	Nhóm 16 lỗ hổng trong phần mềm Gitlab (phiên bản Git lab 8, 10, 11, 12, 13) cho phép đối tượng tấn công tấn công từ chối dịch vụ, tấn công stored XSS.	Đã có thông tin xác nhận và bản vá
9	Mozilla	CVE-2020-15673 CVE-2020-15676 CVE-2020-15668 …	Nhóm 15 lỗ hổng trong các phần mềm Mozilla (Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3) cho phép đối tượng tấn công thu thập thông tin, thực thi mã tùy ý, truy cập trái phép, tấn công Open Redirect.	Đã có thông tin xác nhận và bản vá
10	Apache	CVE-2020-11979 CVE-2018-11765 CVE-2020-9487 …	Nhóm 09 lỗ hổng trong phần mềm Apache (Ant, Hadoop, NiFi,…) cho phep đôi tượng tấn công thu thập thông tin, sửa đổi và tải tệp nguồn, tấn công từ chối dịch vụ, tấn	Đã có thông tin xác nhận và bản vá

			công XXE Injection.	
11	Mediawiki	CVE-2020-25869 CVE-2020-25828 CVE-2020-26121 …	Nhóm 09 lỗ hổng trong phần mềm Mediawiki (các phiên bản < 1.31.10, < 1.34.4) cho phép đối tượng tấn công thu thập thông tin, tấn công XSS.	Đã có thông tin xác nhận và bản vá
12	Foxit	CVE-2020-26539 CVE-2020-26537 CVE-2020-26535 …	Nhóm 06 lỗ hổng trong phần mềm Foxit (Foxit Reader, PhantomPDF phiên bản trước 10.1) cho phép đối tượng tấn công thu thập thông tin, thực thi mã từ xa, truy cập trái phép.	Đã có thông tin xác nhận và bản vá
13	IBM	CVE-2020-4531 CVE-2020-4727 CVE-2020-4607 …	Nhóm 05 lỗ hổng trong các sản phẩm của IBM (Business Automation Workflow, InfoSphere Information Server, ...) cho phép đối tượng tấn công thu thập thông tin, tấn công hijacking	Đã có thông tin xác nhận và bản vá
14	Dpdk	CVE-2020-14378 CVE-2020-14376 CVE-2020-14375 …	Nhóm 05 lỗ hổng trong phần mềm dpkg (phiên bản < 18.11.10 và < 19.11.5) cho phép đối tượng tấn công tràn bộ đệm, sửa đổi bộ nhớ, gây mất dữ liệu.	Đã có thông tin xác nhận và bản vá
15	Wavlink	CVE-2020-12125 CVE-2020-12124 CVE-2020-12123 …	Nhóm 05 lỗ hổng trong phần mềm thiết bị Wavlink (wn530h4 router) cho phep đôi tượng tấn công chèn và thực thi lệnh tùy ý, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
16	Gitlab	CVE-2020-13339 CVE-2020-13337 CVE-2020-13338 …	Nhóm 14 lỗ hổng trong phần mềm Gitlab (phiên bản Git lab 7, 11, 12, 13) cho phép đối tượng tấn công truy cập trái phép, chèn và thực thi lệnh tùy ý, tấn công từ chối dịch vụ, tấn công XSS.	Đã có thông tin xác nhận và bản vá

17	Cisco	CVE-2020-3601 CVE-2020-3602 CVE-2020-3568 …	Nhóm 14 lỗ hổng trong phần mềm thiết bị Cisco (Cisco ASR 5000 Series Routers, AsyncOS Software, Expressway Series,…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã tùy ý, tấn công từ chối dịch vụ, tấn công XSS.	Đã có thông tin xác nhận và bản vá
18	Google	CVE-2020-26607 CVE-2020-26604 CVE-2020-26603 …	Nhóm 11 lỗ hổng trong phần mềm Google (Google Android trên các thiết bị SamSung và LG) cho phép đối tượng tấn công truy cập trái phép, tấn công Path Traversal, ngắt kết nối TCP.	Đã có thông tin xác nhận và bản vá
19	Foxit	CVE-2020-26534 CVE-2020-26539 CVE-2020-26537 …	Nhóm 06 lỗ hổng trong phần mềm Foxit (Foxit Reader, PhantomPDF phiên bản trước 10.1) cho phép đối tượng tấn công thu thập thông tin, tấn công thực thi mã từ xa, truy cập trái phép.	Đã có thông tin xác nhận và bản vá
20	IBM	CVE-2020-4493 CVE-2020-4799 CVE-2019-4725 …	Nhóm 06 lỗ hổng trong các sản phẩm của IBM (Security Access Manager Applicance, Maximo Asset Management, Informix spatial, ...) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi lệnh tùy ý, tấn công XSS, tấn công spoofing.	Đã có thông tin xác nhận và bản vá
21	Wavlink	CVE-2020-12125 CVE-2020-12126 CVE-2020-12123 …	Nhóm 05 lỗ hổng trong phần mềm thiết bị Wavlink (WAVLINK WN530H,…) cho phép đối tượng tấn công thực thi lệnh tùy ý, thay đổi cài đặt định tuyến, tấn công từ chối dịch vụ, tấn công CSRF.	Chưa có thông tin xác nhận và bản vá
22	Redhat	CVE-2020-25637 CVE-2020-25644 CVE-2020-25636 …	Nhóm 04 lỗ hổng trong phần mềm Redhat (Libvirt API, WildFly OpenSSL, Ansible) cho phép đối tượng tấn công leo thang quyền, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá

23	Microsoft	CVE-2020-16937 CVE-2020-17003 CVE-2020-16918 …	Nhóm 85 lỗ hổng trong các phần mềm của Microsoft (.NET Framework, Base3D, Dynamics 365,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công XSS, leo thang đặc quyền, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
24	Netgear	CVE-2020-26908 CVE-2020-26909 CVE-2020-26902 …	Nhóm 29 lỗ hổng trong thiết bị Netgear (D6200, D7800, RBK752, …) cho phép đối tượng tấn công thu thập thông tin, tấn công dịch vụ.	Đã có thông tin xác nhận và bản vá
25	IBM	CVE-2020-4302 CVE-2020-4689 CVE-2020-4388 …	Nhóm 26 lỗ hổng trong các sản phẩm của IBM (Cognos Analytics, Security Guardium,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ, tấn công HTML Injection, XSS, CSRF, XXE Injection, Path Traversal.	Đã có thông tin xác nhận và bản vá
26	Google	CVE-2020-0416 CVE-2020-0416 CVE-2020-0420 …	Nhóm 25 lỗ hổng trong phần mềm Google (Google Android 8, 9, 10, 11) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
27	Huawei	CVE-2020-9108 CVE-2020-9107 CVE-2020-9109 …	Nhóm 13 lỗ hổng trong phần mềm thiết bị Huawei (P30 Pro firmware, FusionAccess, HiRouter) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, chèn và thực thi lệnh tùy ý, tấn công tràn bộ đệm, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
28	Foxit	CVE-2020-17415 CVE-2020-17414 CVE-2020-17413 …	Nhóm 08 lỗ hổng trong phần mềm Foxit (Foxit Reader, PhantomPDF) cho phép đối tượng tấn công thu thập thông tin, leo thang quyền, tấn công thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá

29	Lenovo	CVE-2020-8338 CVE-2020-8349 CVE-2020-8345 …	Nhóm 05 lỗ hổng trong sản phẩm của Lenovo (Diagnostics, Cloud Networking Operating System, HardwareScan Plugin, …) cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá

PHỤ LỤC 2

(Kèm theo Công văn số 626/CNTT-KHCN ngày 30 tháng 10 năm 2020 của Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường)

DANH SÁCH CÁC MẠNG BOTNET VÀ IP/TÊN MIỀN ĐỘC HẠI CÓ NHIỀU KẾT NỐI TỪ VIỆT NAM

(THÁNG 10/2020)

1. Danh sách các mạng botnet

2. Wannacry, Conficker, Avalanche, Iotbotnet

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

TT	Tên miền/IP
1	amnsreiuojy.ru
2	atomictrivia.ru
3	cp.hfuabnqx.ru
4	differentia.ru
5	disorderstatus.ru
6	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
7	kvamuvsju.ru
8	qqdqlocstxm.info
9	restless.su
10	rkphklelf.ru
11	xjpakmdcfuqe.biz
12	xjpakmdcfuqe.com
13	xjpakmdcfuqe.in
14	xjpakmdcfuqe.ru
15	ydbnsrt.me

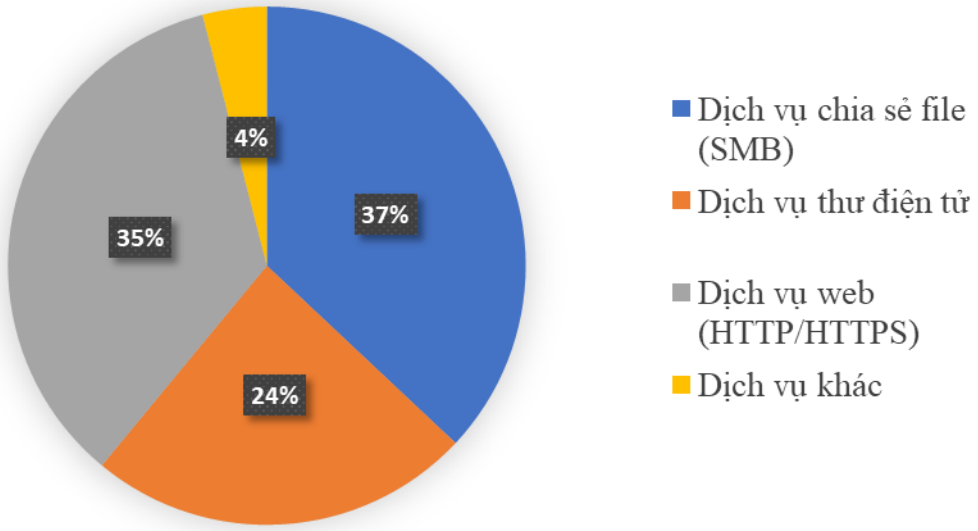
16	zayzyyzmdsdz.info

PHỤ LỤC 3

(Kèm theo Công văn số 626 /CNTT-KHCN ngày 30 tháng 10 năm 2020 của Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường)

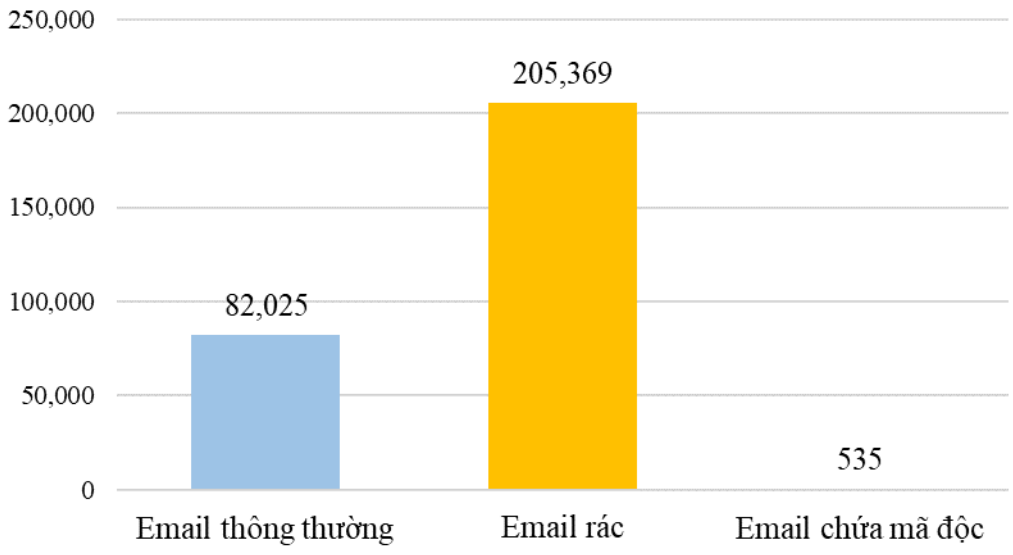
CÁC CUỘC TẤN CÔNG MẠNG VÀO HỆ THỐNG MẠNG CỦA BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

(THÁNG 10/2020)

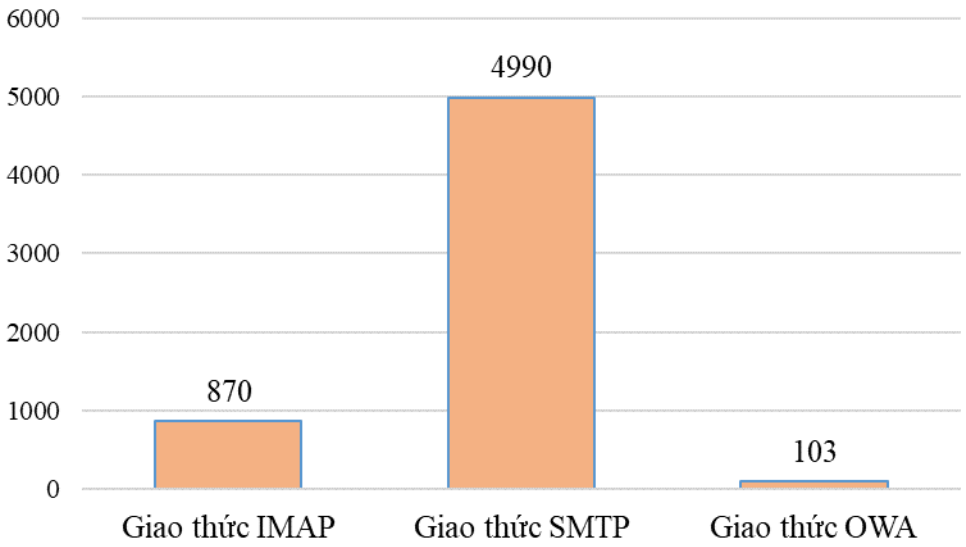
Nội dung	Số liệu thống kê
Tổng số cuộc tấn công mạng được ghi nhận và ngăn chặn:	350,665 trong đó tỉ lệ các cuộc tấn công mạng mức độ trên trung bình là 6%
1. Danh sách các dịch vụ bị tấn công nhiều nhất	
Dịch vụ chia sẻ file của windows (cổng 445)	37 (%)
Dịch vụ thư điện tử	24 (%)
Dịch vụ web (cổng 80, 443)	35 (%)
Dịch vụ khác	4 (%)
	
3. Danh sách các loại virus, botnet phát hiện trong hệ thống mạng	
Loại virus	Adware.TC.gbbgfaeji Andromeda.TC.aaggccbbb Coinhive.TC.be CrossRider.TC.af Cryptominer.TC.gaedjcabf Generic.TC.gtapyt Generic.TC.hhejcv HEUR:Trojan.PowerShell.Generic HEUR:Trojan-PSW.Win64.Generic infecting website.TC.cicq Malicious Binary.TC.jolktn

	MEM:Trojan.Win32.Cobalt.gen phish_report.TC.caot Phishing.RS.TC.xpof Phishing.TC.obsi Phishing_website.TC.aeubjk PUP.Win32.CoreInstaller.TC.bpdu Trojan.Win32.Malware.TC.dflav Trojan-Dropper.VBS.Agent.bp UDS:DangerousObject.Multi.Generic
Mạng botnet	Cnc server Glupteba Iot.tenchier Miniast Sality
4. Tình hình nhiễm mã độc	
Số lượng máy trạm nhiễm mã độc/tham gia mạng botnet	244 máy trạm. Nhóm vận hành hệ thống mạng tiến hành ngăn chặn kết nối mạng, phối hợp với người sử dụng để xử lý

Lượng thư rác và mã độc thông qua hệ thống thư điện tử của Bộ trong tháng 10 năm 2020:

Nội dung	Số liệu thống kê
1. Thống kê chung	
Tổng lượng email gửi nhận	82.025 (email)
Tỉ lệ thư rác	71.3 (%) (khoảng 205.369 email)
Tỉ lệ email chứa mã độc	0,2 (%) (535 email)
	
2. Các 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	184.853 (lượt dò tìm mật khẩu)
Các dịch vụ mail bị tấn công nhiều nhất	IMAP (14,6% số cuộc tấn công) SMTP (83,7% số cuộc tấn công) OWA (1,7% số cuộc tấn công)



4. Email có nội dung lừa đảo gửi tới người dùng Bộ

Trong tháng 10, ghi nhận từ hệ thống giám sát không có tài khoản gửi thư lừa đảo tới người dùng thư điện tử của Bộ