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

Số: 544 /CNTT-KHCN
V/v báo cáo tình hình an toàn, an ninh thông tin tháng 7/2018

Hà Nội, ngày 06 tháng 8 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 7 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, 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 06 tháng 8 năm 2018

BÁO CÁO

TÌNH HÌNH AN TOÀN, AN NINH THÔNG TIN THÁNG 7/2018

(Kèm theo công văn số 544 /CNTT-KHCN ngày 06 /8/2018)

1. Tình hình an toàn thông tin chung

1.1. Bang California, Hoa Kỳ xây dựng Dự luật bảo vệ dữ liệu của người dùng, trong đó mở rộng khái niệm của thông tin cá nhân và cho người tiêu dùng ở California quyền cấm rao bán thông tin cá nhân cho bên thứ ba và lựa chọn ngừng tham gia vào quá trình chia sẻ thông tin nói chung. Dự luật sẽ được áp dụng cho tất cả các doanh nghiệp ở mọi quy mô thực hiện thu thập dữ liệu người dùng.

Luật này khi được áp dụng ở California, các hãng công nghệ nhiều khả năng sẽ phải thay đổi toàn bộ chính sách của họ chiếu theo luật vì việc tạo ra các tiêu chuẩn khác nhau cho mỗi vùng là rất phức tạp. Dự luật có một vài điểm tương tự với Luật Bảo vệ dữ liệu cá nhân của Châu Âu đã có hiệu lực hồi tháng 5/2018. Tuy nhiên, dự luật của California chú trọng trách nhiệm của người dùng trong việc yêu cầu cung cấp thông tin và ngừng chia sẻ dữ liệu, trong khi luật của châu Âu yêu cầu các doanh nghiệp phải chủ động hơn trong việc cung cấp thông tin cho người dùng.

1.2. Văn phòng Chính phủ đã có văn bản truyền đạt ý kiến chỉ đạo của Phó Thủ tướng Vũ Đức Đam về thực hiện Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

Phó Thủ tướng giao Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Giáo dục và Đào tạo nghiên cứu, đề xuất, trình Thủ tướng Chính phủ điều chỉnh mục tiêu của Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020 (Đề án 99) về số lượt cán bộ chuyên trách về an toàn, an ninh thông tin đi đào tạo ngắn hạn ở nước ngoài để phù hợp với tình hình thực tế hiện nay.

Bộ Thông tin và Truyền thông bổ sung nhóm đối tượng "Cán bộ làm về an toàn, an ninh thông tin chịu trách nhiệm quản lý, vận hành, bảo đảm an toàn thông tin cho các hệ thống thông tin phục vụ các cơ quan Đảng, Nhà nước, phát triển chính phủ điện tử và chính quyền điện tử các cấp" và "Giảng viên giảng dạy về an toàn, an ninh thông tin tại các cơ sở đào tạo trọng điểm" tham gia các khóa đào tạo ngắn hạn về an toàn thông tin do Bộ Thông tin và Truyền thông tổ chức hàng năm.

Phó Thủ tướng cũng giao Bộ Thông tin và Truyền thông chủ trì, phối hợp với Hiệp hội an toàn thông tin Việt Nam nghiên cứu, đề xuất cơ chế huy động nguồn lực

xã hội hóa từ các Tập đoàn, Tổng công ty nhà nước, các doanh nghiệp hoạt động trong lĩnh vực an toàn thông tin để triển khai các nhiệm vụ đào tạo, phát triển nguồn nhân lực an toàn, an ninh thông tin tại Việt Nam

1.3. Gần đây các nhà nghiên cứu bảo mật đã phát hiện ra một chiến dịch tấn công mạng bằng mã độc lợi dụng các chứng chỉ số hợp lệ bị đánh cắp từ các công ty công nghệ, để ký số chứng thực cho mã độc, làm cho các mã độc này được coi như các ứng dụng hợp pháp.

Các chứng chỉ số được sử dụng để ký mã hóa các ứng dụng và phần mềm máy tính và chúng được tin cậy bởi máy tính để thực thi các chương trình đó mà không có bất kỳ thông báo cảnh báo nào. Việc đối tượng tấn công đánh cắp và lợi dụng chứng chỉ chữ ký liên kết với nhà cung cấp phần mềm đáng tin cậy để ký chứng thực cho mã độc sẽ làm hạn chế khả năng phát hiện mã độc của các dịch vụ, ứng dụng phòng, chống mã độc trên mạng doanh nghiệp và thiết bị của người dùng.

Các nhà nghiên cứu tại hãng bảo mật ESET đã phát hiện ra 2 họ mã độc được cho là có liên quan đến nhóm gián điệp mạng BlackTech, được ký bằng chứng chỉ số hợp lệ của nhà sản xuất thiết bị mạng D-Link và một công ty bảo mật của Đài Loan có tên là Changing Information Technology.

Mã độc đầu tiên được gọi là Plead, đây là một backdoor kiểm soát từ xa được thiết kế để ăn cắp các file tài liệu và nghe lén người dùng. Mã độc thứ 2 là phần mềm ăn cắp mật khẩu được thiết kế nhằm thu thập mật khẩu của người dùng được lưu trên những ứng dụng phổ biến như Google Chrome, Microsoft Internet Explorer, Microsoft Outlook và Mozilla Firefox.

Ngay sau khi nhận được cảnh báo, D-Link và công ty Changing Information Technology đã thu hồi các chứng chỉ số bị đánh cắp vào đầu tháng này. Tuy nhiên, vì hầu hết các giải pháp phòng, chống mã độc không kiểm tra tính hợp lệ của chứng chỉ số kể cả khi các công ty đã thu hồi chữ ký của chứng chỉ, nhóm BlackTech vẫn đang sử dụng chứng chỉ cũ để ký chứng thực cho các công cụ độc hại.

1.4. Trước thực tế nhiều tổ chức tài chính của nước Anh không có các kế hoạch dự phòng khi bị tấn công mạng, Ngân hàng Trung ương Anh yêu cầu các ngân hàng trong nước chuẩn bị sẵn sàng phương án, kế hoạch dự phòng giảm thiểu rủi ro trước các cuộc tấn công mạng.

Theo đó Ngân hàng Trung ương yêu cầu các tổ chức tài chính, ngân hàng lập một kế hoạch chi tiết cho việc khôi phục các dịch vụ như thanh toán, cho vay và bảo hiểm nếu một cuộc tấn công mạng vào hệ thống của các tổ chức này xảy ra, ngoài ra các tổ chức này cần phải đầu tư phát triển nguồn nhân lực cũng như công nghệ để có thể thực hiện kế hoạch dự phòng này trong thực tế. Ngân hàng Trung ương Anh cũng nhấn mạnh vai trò các quản lý cấp cao của các tổ chức tài chính trong việc nâng cao năng lực phục hồi sau khi bị tấn công.

1.5. Bộ trưởng Bộ Tư pháp, kiêm Bộ trưởng Bộ Điện tử, Công nghệ thông tin Ấn độ ông Ravi Shankar đã làm việc với Bộ trưởng Bộ Tư pháp Anh ông David Gauke để thảo luận về sự hợp tác tiền năng giữa 2 bên về Công nghệ thông tin và các vấn đề pháp lý. Các Bộ trưởng đã ký thỏa thuận hợp tác để thúc đẩy hợp tác hai phía và cung cấp một khuôn khổ để đẩy mạnh hợp tác rộng hơn giữa các chuyên gia pháp luật của hai quốc gia, trong đó có hợp tác về quản lý mạng Internet và ATTT mạng.

Hai Bộ trưởng đã ký một Thỏa thuận hợp tác để thúc đẩy việc hợp tác trong các vấn đề pháp lý, đưa ra một khuôn khổ để đẩy mạnh hợp tác rộng hơn giữa các chuyên gia pháp luật của cả hai quốc gia qua việc trao đổi chuyên môn và huấn luyện, đào tạo; trao đổi thông tin trong vấn đề quốc tế. Thỏa thuận hợp tác cũng đưa ra sự thành lập một Ủy ban Giám sát để hiện thực hóa những trao đổi này.

1.6. Một nhóm 2 nhà nghiên cứu - Vladimir Kiriansky và Carl Waldspurger, đã phát hiện ra 2 lỗ hổng lớp Spectre mới, được gọi là Spectre 1.1 và Spectre 1.2.

Các biến thể của lỗ hổng Spectre mới được tìm ra sau khi các nhà nghiên cứu tại Microsoft và Google công bố một biến thể Spectre 4 ảnh hưởng đến hàng triệu CPUs, bao gồm những sản phẩm từ hãng Apple khoảng một tháng trước đây. Tương tự với tất cả các biến thể của lỗ hổng CPU Meltdown và Spectre trước đây, 2 lỗ hổng mới này lợi dụng kỹ thuật thực thi suy đoán (speculative execution), một tính năng được ứng dụng trên hầu hết tất cả CPU nhằm làm tăng hiệu năng bộ vi xử lý và loại bỏ dữ liệu không cần thiết.

Spectre 1.1 là biến thể phụ của biến thể Spectre 1 ban đầu, gây ra việc tràn bộ nhớ đệm bằng cách tăng lưu trữ suy đoán. Lỗi tràn bộ nhớ đệm trong cache CPU có thể cho phép kẻ tấn công trích xuất dữ liệu từ bộ nhớ CPU bảo mật, bao gồm mật khẩu, khóa mã hóa và các thông tin nhạy cảm khác.

Spectre 1.2 là lỗ hổng phụ thuộc vào kỹ thuật "lazy PTE enforcement", cùng cơ chế khai thác với lỗ hổng Meltdown. Lỗ hổng này có thể cho phép kẻ tấn công vượt qua cờ đọc/ghi PTE, ghi đè lên bộ nhớ dữ liệu read-only, mã siêu dữ liệu và code pointers để tránh giải pháp bảo mật sandbox.

Hãng sản xuất CPU như Intel và ARM đã công khai thừa nhận rằng một số CPU của họ bị ảnh hưởng bởi các lỗi này. Mặc dù chưa có bản vá vào thời điểm hiện tại, tuy nhiên Intel đã đưa ra hướng dẫn kiểm tra và sửa đổi mã nguồn dành cho nhà phát triển nhằm giảm thiểu tác động của lỗ hổng ở cấp độ ứng dụng/phần mềm.

Những lỗ hổng này chủ yếu ảnh hưởng đến hệ điều hành và nền tảng ảo hóa, và có thể cần tiến hành cập nhật phần mềm hoặc vi mã. Các hãng cung cấp phần mềm lớn bao gồm Microsoft, Red Hat và Oracle đã ngay lập tức công bố khuyến cáo rằng họ vẫn đang điều tra nếu như có bất kỳ sản phẩm nào không an toàn với biến thể Spectre mới. Quản trị viên hệ thống cần liên tục theo dõi và cập nhật ứng dụng/phần mềm từ các hãng trên để bảo đảm ATTT cho hệ thống của cơ quan, tổ chức mình.

1.7. Ngày 20/7/2018 trên website của Bộ Y tế (https://www.moh.gov.sg) và một số cơ quan báo chí của Singapore đã thông báo về cuộc tấn công mạng vào hệ thống thông tin của Singhealth (Tập đoàn chăm sóc sức khoẻ lớn nhất của Singapore với 04 bệnh viện, 05 trung tâm chuyên khoa quốc gia và 08 phòng khám đa khoa).

Theo thông tin từ Bộ Y tế, Singapore, thông tin cá nhân của khoảng 1.5 triệu bệnh nhân tại các phòng khám ngoại trú chuyên khoa và phòng khám đa khoa của SingHealth từ 01/5/2015 đến 04/7/2018 đã bị truy cập và sao chép trái phép. Dữ liệu bị lấy bao gồm tên, số nhận dạng cá nhân, địa chỉ, giới tính và ngày sinh … Cơ quan An toàn Thông tin Singapore (CSA) và IhiS (Integrated Health Information Systems, cơ quan vận hành hệ thống CNTT của các tổ chức y tế cộng đồng Singapore) đã khẳng định rằng đây là một cuộc tấn công mạng có chủ đích, có mục tiêu và được lên kế hoạch kỹ lưỡng.

Ngày 04/7/2018, quản trị viên cơ sở dữ liệu của IhiS đã phát hiện các hoạt động bất thường trên cơ sở dữ liệu của SingHealth và đã ngay lập tức tiến hành các biện pháp ngăn chặn hoạt động này. IhiS thực hiện rà soát, kiểm tra để làm rõ bản chất của hoạt động trên, và cùng lúc triển khai thêm các biện pháp đảm bảo an toàn thông tin.

Ngày 10/7/2018, các cuộc kiểm tra, rà soát xác nhận rằng đó là một cuộc tấn công mạng, IhiS thông báo với Bộ Y tế, SingHealth và CSA. Kết quả đã xác nhận dữ liệu bị xâm nhập từ 27/6/2018 tới 4/7/2018. CSA đã xác định rằng, đối tượng tấn công mạng ban đầu đã tiếp cận hệ thống bằng việc xâm nhập vào một máy trạm đầu cuối. Sau đó lấy được thông tin đăng nhập của một tài khoản có đặc quyền cao để truy cập vào cơ sở dữ liệu.

IhiS, với sự hỗ trợ của CSA đã áp dụng thêm các biện pháp để tăng cường bảo đảm ATTT cho hệ thống của SingHealth. Bao gồm: chặn truy cập vào mạng Internet, đặt ra thêm các quy trình điều khiển ở các máy trạm và máy chủ, thiết lập lại các tài khoản người dùng và hệ thông, cài đặt thêm các chương trình giám sát hệ thống. Các biện pháp tương tực cũng đang được triển khai cho các hệ thống công nghệ thông tin trên toàn ngành y tế cộng đồng trước mối de dọa này.

Bộ Y tế, Singapore đã chỉ đạo IhiS thực hiện ngay việc kiểm tra, đánh giá ATTT toàn bộ hệ thống y tế công cộng, với sự hỗ trợ của các chuyên gia ATTT từ các cơ quan chức năng, các tổ chức, doanh nghiệp để nâng cao việc phòng chống, phát hiện và phản ứng trước các nguy cơ tiềm ẩn trên mạng. Nội dung kiểm tra, đánh giá sẽ bao gồm: chính sách an toàn thông tin, quy trình quản lý các nguy cơ tiềm ẩm, quy trình điều khiển hệ thống CNTT, năng lực của nhân viên và tổ chức, các biện pháp phòng, chống tấn công mạng và các biện pháp khắc phục .v.v…

1.8. Vừa qua, Chính phủ Ukraine cho biết đã ngăn chặn thành công cuộc tấn công mạng vào nhà máy hóa chất clo LLC Aulska, cách thành phố Dnepr của tỉnh Dnipropetrovsk. Theo cơ quan chức năng của Ukraine, cuộc tấn công mạng này được

tiến hành bằng mã độc VPNFilter, một loại mã độc nguy hiểm có hoạt động rất tinh vi với nhiều giai đoạn tấn công, có thể đánh cắp thông tin đăng nhập hệ thống và theo dõi các hệ thống điều khiển công nghiệp SCADA, như hệ thống lưới điện và cơ sở hạ tầng công nghiệp.

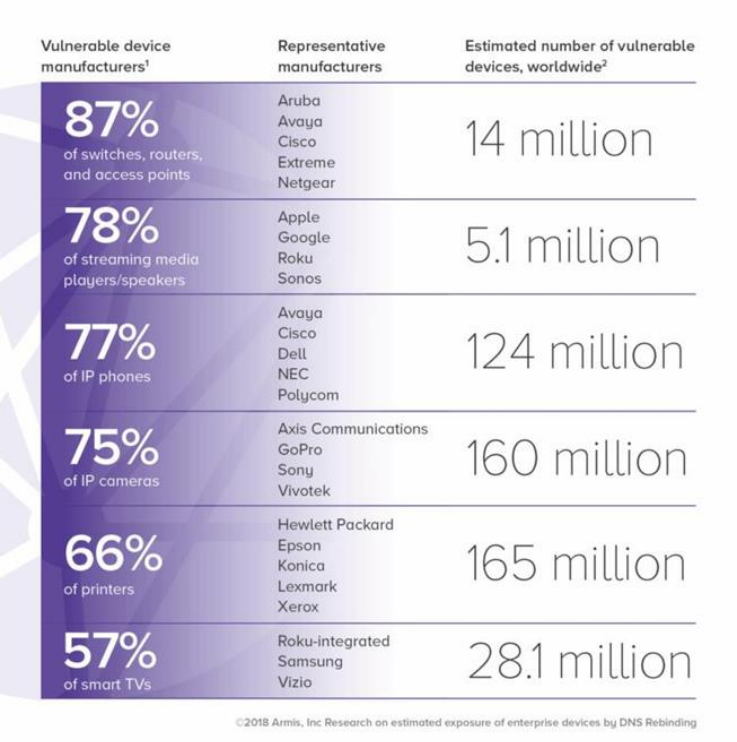
Cuộc tấn công nhằm mục đích phá hoạt quá trình hoạt động ổn định của nhà máy trong việc cung cấp Natri hypoclorit (NaClO, còn gọi là clo lỏng) cho xử lý nước. Cơ quan chức năng của Ukraine cho rằng mã nguồn một số phiên bản của mã độc này có sự tương đồng với các phiên bản của mã độc BlackEnergy, một mã độc liên quan đến những cuộc tấn công vào các trạm phân phối điện của Ukraine. Cơ quan này cũng cho rằng nhóm APT 28 đã tạo ra và phân tán VPNFilter.

1.9. Hàng trăm triệu thiết bị IoT đang tồn tại lỗ hổng và có khả năng bị tấn công bởi phương thức DNS rebinding. Đó là cảnh báo từ nghiên cứu mới nhất của hãng bảo mật Armis, hãng bảo mật đã tìm ra lỗ hổng BlueBorne trong giao thức Bluetooth ảnh hưởng tới 8.2 tỷ thiết bị vào tháng 9/2017. Theo Armis, các doanh nghiệp đang phải chịu rủi ro rất lớn từ phương thức tấn công DNS rebinding bởi số lượng rất lớn thiết bị mạng, điện thoại, máy in, camera IP tại nơi làm việc, thường là mục tiêu của đối tượng tấn công.

DNS rebinding là phương thức tấn công lợi dụng việc trình duyệt hoặc thiết bị của người dùng liên kết với một máy chủ DNS độc hại và sau đó chuyển hướng để thiết bị truy cập các tên miền khác.

DNS rebinding thường được sử dụng để chiếm quyền kiểm soát thiết bị và sử dụng như điểm chuyển tiếp để mở rộng tấn công trong mạng nội bộ. Lỗ hổng do hãng Armis tìm ra lợi dụng một lỗi cũ trong các trình duyệt web cho phép đối tượng tấn công vượt qua tường lửa mạng của nạn nhân và sử dụng trình duyệt web của họ như một proxy để giao tiếp, khai thác trực tiếp điểm yếu các thiết bị khác trong mạng nội bộ. Ví dụ về thiết bị có khả năng bị tấn công là thiết bị hoạt động với giao thức không xác thực như UpnP (Universal Plug and Play) hoặc HTTP, được sử dụng trên máy chủ web. Những giao thức này thường được sử dụng để quản trị bộ định tuyến, máy in, camera IP hoặc cho phép truy cập dễ dàng hơn vào các dịch vụ của thiết bị, khá phổ biến trong môi trường doanh nghiệp.

Theo báo cáo của Armis, IoT và các thiết bị thông minh khác là đối tượng tấn công DNS rebinding là do sự gia tăng về số lượng trong mạng doanh nghiệp và chúng có thể được sử dụng tốt cho hoạt động giám sát và lấy cắp dữ liệu. Sử dụng dữ liệu từ Armis' Device Knowledgebase, bao gồm hồ sơ hành vi của hơn 5 triệu thiết bị, các nhà nghiên cứu đã xác định gần như tất cả thiết bị thông minh đều có khả năng bị tấn công DNS rebinding, với số lượng trên toàn thế giới lên đến gần nửa tỷ (496 triệu thiết bị).



Vulnerable device manufacturers[1]	Representative manufacturers	Estimated number of vulnerable devices, worldwide[2]
87% of switches, routers, and access points	Aruba Avaya Cisco Extreme Netgear	14 million
78% of streaming media players/speakers	Apple Google Roku Sonos	5.1 million
77% of IP phones	Avaya Cisco Dell NEC Polycom	124 million
75% of IP cameras	Axis Communications GoPro Sony Vivotek	160 million
66% of printers	Hewlett Packard Epson Konica Lexmark Xerox	165 million
57% of smart TVs	Roku-integrated Samsung Vizio	28.1 million

Thống kê của hãng Armis

Việc cập nhật bản vá lỗ hổng DNS rebinding cho tất cả thiết bị là một nhiệm vụ với khối lượng rất lớn mà gần như không thể thực hiện được. Khuyến nghị của các chuyên gia ATTT đối với các cơ quan, tổ chức, doanh nghiệp là nên giám sát ATTT mạng dành cho các thiết bị IoT, đây là giải pháp dễ dàng và hiệu quả nhất, thay vì rà soát và kiểm tra các thiết bị mới để thay thế thiết bị cũ. Đây cũng là xu hướng của những cơ quan, tổ chức lớn ngày nay, nhằm ngăn chặn các cuộc tấn công như DNS rebinding và các lỗ hổng, điểm yếu ATTT phát sinh khác.

1.10. Từ ngày 23-25/7, Bảo hiểm Xã hội Việt Nam đã tổ chức Hội nghị An toàn thông tin ngành BHXH toàn quốc.

Tham dự hội nghị có đồng chí Phạm Lương Sơn - Phó Tổng giám đốc BHXH Việt Nam, ông Huỳnh Thanh Điền - Phó Chủ tịch UBND tỉnh Nghệ An cùng đại diện Cục An toàn thông tin - Bộ Thông tin và Truyền thông, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, Cục Chứng thực số và Bảo mật thông tin, Cục Cơ yếu Đảng Chính quyền - Ban Cơ yếu Chính phủ, và đại diện BHXH 63 tỉnh, thành phố trong cả nước.

Các hệ thống thông tin của ngành BHXH có nhiều hệ thống thông tin quan trọng đang được xác định cấp độ 4, cấp độ 5 và cần được đảm bảo an toàn thông tin theo đúng cấp độ quy định tại Luật An toàn thông tin mạng và Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm ATTT theo cấp độ. Các hệ thống thông tin điển hình như: Hệ thống cơ sở dữ liệu về BHYT theo hộ gia đình; Hệ thống giám định BHYT; Hệ thống quản lý thu, sổ thẻ, xét duyệt chính sách .v.v…

Tại Hội nghị, Ông Nguyễn Huy Dũng, Phó Cục trưởng Cục An toàn thông tin - Bộ Thông tin và Truyền thông đã có bài tham luận chia sẻ về những thách thức và kinh nghiệm triển khai công tác phòng, chống tấn công mạng, bảo đảm an toàn thông tin.

Hiện tại, hệ thống thông tin của ngành BHXH đang quản lý trên 20.000 tài khoản công chức, viên chức của gần 1500 đơn vị trong ngành BHXH (tính từ cấp phòng, BHXH huyện trở lên) sử dụng thường xuyên; khoảng 12.000 cơ sở khám chữa bệnh, hơn 500.000 tổ chức, doanh nghiệp sử dụng dịch vụ công.

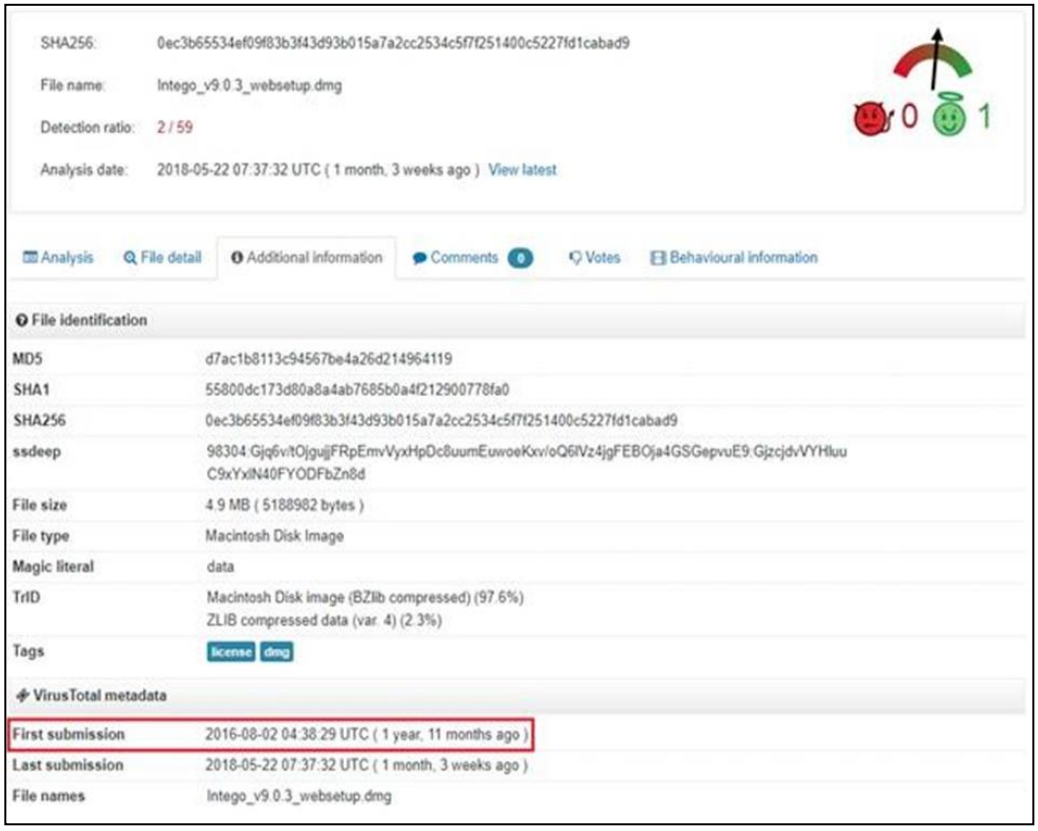
1.11. Ngày 23/7/2018, trong diễn đàn kinh doanh ASEAN CISO tổ chức tại khách sạn Pullman ở Trung tâm Jakarta, Bộ trưởng Bộ Thông tin và Truyền thông Indonesia, ông Rudiantara cho biết an toàn thông tin mạng là một trong những mối quan tâm chính của chính phủ nước này.

Bộ Thông tin và Truyền thông Indonesia nhấn mạnh tầm quan trọng của an toàn Thông tin trong việc ứng dụng Công nghệ Thông tin và Truyên thông (ICT). Bộ Thông tin và Truyền thông Indonesia cho rằng việc phát huy hết lợi ích của ICT có thể đạt được qua bảo đảm an toàn thông tin.

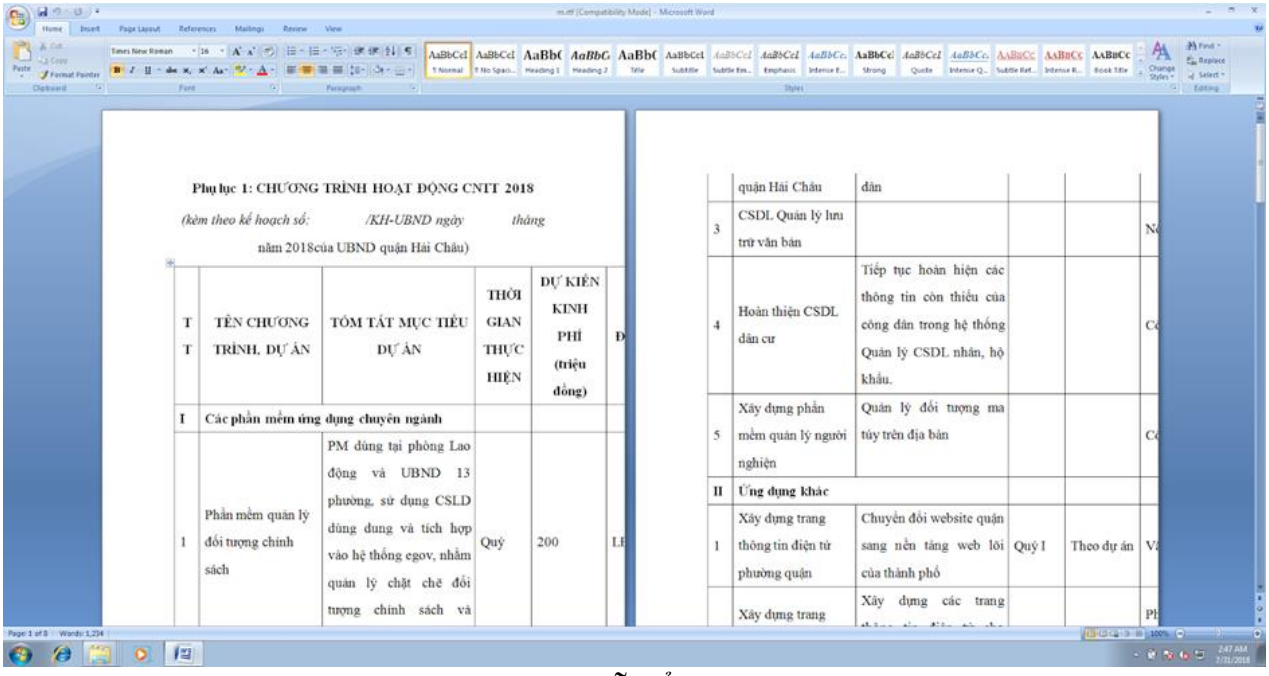
Bộ trưởng Rudiantara cho biết, Bộ Thông tin và Truyền thông Indonesia đang tập trung vào việc xây dựng cơ sở hạ tầng Internet tốc độ cao để kết nối tất cả các khu vực của Indonesia. Dự án Palapa Ring và vệ tinh để cung cấp Internet tốc độ cao là các chương trình để giải quyết vấn đề kết nối với hy vọng tất cả các khu vực của Indonesia sẽ được kết nối vào năm 2019.

Một vấn đề quan trọng đang ảnh hưởng đến các quốc gia ASEAN đó là an toàn thông tin, điều có thể ảnh hưởng đến lợi ích chiến lược và cộng đồng của các quốc gia. Để đảm bảo có thể tận dụng hết tất cả các lợi ích của ICT, việc xử lý các vấn đề an toàn thông tin là vấn đề mấu chốt, nhất là với sự phát triển của Big Data và công nghệ IoT. Theo như báo cáo của Bộ Thông tin và Truyền thông, họ đã chuẩn bị nền tảng nhằm bảo vệ cơ sở hạ tầng thông tin quan trọng cho Indonesia. Khía cạnh An toàn Thông tin bao gồm việc giảm thiểu rủi ro, phản ứng với các cuộc tấn công mạng và khôi phục thông tin.

1.12. Từ năm 2016, mã độc Calisto Trojan đã được tải lên cơ sở dữ liệu của VirusTotal (một công cụ trực tuyến để kiểm tra, phân tích mã độc). Theo các chuyên gia ATTT rất có thể mã độc này đã được tạo ra từ lúc đó. Nhưng phải đến 2 năm sau, vào tháng 5 năm 2018, các giải pháp antivirus mới bắt đầu phát hiện ra hoạt động của nó.



Mã độc Calisto đã được tải lên cơ sở dữ liệu của VirusTotal từ 2016



File .rtf bị khai thác lỗ hổng CVE-2017–11882

Sau các phân tích chuyên môn về tấn công này, chuyên gia Sebdraven đã xác định ra một số các hạ tầng, phương thức sử dụng của đợt tấn công, như sau:

domains:	*RTFs:*	*IP:*
dn.dulichbiendao.org gateway.vietbaotinmoi.com fis.malware-sinkhole.net hn.dulichbiendao.org halong.dulichculao.com news.malware-sinkhole.net cat.toonganuh.com new.sggpnews.com dulichculao.com coco.sodexoa.com. thoitiet.malware-sinkhole.net wouderfulu.impresstravel.ga toonganuh.com coco.sodexoa.com	42162c495e835cdf28670661a53d47d12255d9c791c1c5653673b25fb587ffed 8.t: 2c60d4312e4416745e56048ee35e694a79e1bc77e7e4d0b5811e64c84a72d2d7 PE: f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb15c43de33bbce0bf68(exe) 9f5da7524817736cd85d87dae93fdbe478385baac1c0aa3102b6ad50d7e5e368 (dll)	192.99.181.14 176.223.165.122

Theo đó, chuyên gia này có nhận định tấn công mạng vào các cơ quan nhà nước Việt Nam này từ nhóm 1937cn và sử dụng các phương thức mới, trong đó có nhiều đặc điểm như sử dụng cùng công cụ như Sidewinder.

Tuy nhiên, dưới góc độ phân tích và theo dõi các tấn công có chủ đích và các nhóm tấn công APT vào Việt Nam trong thời gian qua, Trung tâm xử lý tấn công mạng Việt Nam có một số nhận định về tấn công này như sau:

- Đây không phải là tấn công mạng bởi nhóm 1937cn;

- Các hạ tầng (domain C&C) được sử dụng cho tấn công mạng này đã được hệ thống ghi nhận và cảnh báo từ lâu;

- 02 domain toonganuh.com và malware-sinkhole.net chưa đủ các yếu tố kỹ thuật để kết luận có sự liên quan;

- Exploit qua CVE-2017–11882 không phải là kiểu exploit mới và đã có nhiều trong các báo cáo và cảnh báo;

- Phương thức đợt tấn công này ngoài việc sử dụng chung CVE thì không tương đồng với Sidewinder.

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 511 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 992 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 6/2108, các tổ chức quốc tế đã phát hiện và công bố ít nhất 1629 lỗ hổng trong đó có: 156 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 16 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 27 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 111 lỗ hổng trên các phần mềm của Adobe;
- Nhóm 4 lỗ hổng trên nhiều sản phẩm của ZTE;
- Nhóm 58 lỗ hổng trên nhiều phần mềm sử dụng cho Android;
- Nhóm 5 lỗ hổng trên các dòng router của tp-link;
- Nhóm 55 lỗ hổng trên các phần mềm của Adobe;
- Nhóm 52 lỗ hổng trên nhiều sản phẩm của Microsoft;

- Nhóm 37 lỗ hổng trên nhiều dòng sản phẩm của Cisco;

- Nhóm 205 lỗ hổng trên nhiều sản phẩm của Oracle;

.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	D-link	CVE-2018-12103	Lỗ hổng trên dòng router DIR-890L A2 do tính dễ đoán của thuật toán tạo CAPTCHA cho phép đối tượng thực hiện tấn công vét cạn trên hệ thống đăng nhập.	Chưa có thông tin xác nhận và bản vá
2	Dell EMC	CVE-2018-11052 CVE-2018-1249 CVE-2018-1244 CVE-2018-1212 CVE-2018-1243	Nhóm 5 lỗ hổng trên dịch vụ lưu trữ ECS và Trình quản lý Máy chủ từ xa IDRAC của Dell EMC cho phép đối tượng thực hiện đọc và chỉnh sửa tệp lưu trữ, tắt tính năng bảo vệ SSL/TLS, chèn và thực thi mã lệnh. Ngoài ra iDRAC6 còn dễ bị tấn công vét cạn do phiên CGI chỉ sử dụng ID số 96 bit.	Chưa có thông tin xác nhận
3	Huawei	CVE-2018-7944 CVE-2018-17175 CVE-2018-17317 CVE-2018-17316	Nhóm 4 lỗ hổng trên nhiều thiết bị của Huawei (Emily-AL00A, Mate 9 Pro và nhiều dòng thiết bị định tuyến) cho phép đối tượng thực hiện chiếm quyền sử dụng thiết bị, tấn công từ chối dịch vụ, làm tràn bộ đệm và đánh cắp thông tin	Đã có thông tin xác nhận và bản vá

4	Qualcomm	CVE-2018-5907 CVE-2018-5898 CVE-2018-5862 CVE-2018-5853 CVE-2018-5885	Nhóm 58 lỗ hổng trên nhiều phần mềm sử dụng cho Android cho phép đối tượng thực nhiều hình thức tấn công như làm tràn và viết đè bộ đệm, lây nhiễm SQL, chèn và thực thi mã lệnh,…	Đã có thông tin xác nhận và bản vá
5	TP-link	CVE-2018-13134 CVE-2018-12577 CVE-2018-12574 CVE-2018-12576 CVE-2018-12575	Nhóm 5 lỗ hổng trên các dòng router của tp-link (Archer C1200, TL-WR841N) cho phép đối tượng thực hiện nhiều hình thức tấn công XSS, CSRF, clickjacking,…	Chưa có thông tin xác nhận
6	Wordpress	CVE-2018-12426 CVE-2018-13136	Nhóm 02 lỗ hổng trên các tiện ích của Wordpress (WP Live Chat Support Pro trước phiên bản 8.0.0.7 và Ultimate Member trước phiên bản 2.0.18) cho phép đối tượng thực hiện chèn và thực thi mã lệnh, tấn công XSS.	Chưa có thông tin xác nhận
7	Adobe	CVE-2018-4999 CVE-2018-4980 CVE-2018-4985 CVE-2018-5000 CVE-2018-4946 ...	Nhóm 55 lỗ hổng trên các phần mềm của Adobe được sử dụng rất phổ biến ở Việt Nam (Acrobat and Reader, Flash Player, Photoshop CC) cho phép đối tượng thực thi mã lệnh và đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá

8	D-link	CVE-2016-6563	Lỗ hổng trên dịch vụ HNAP ảnh hưởng đến nhiều dòng router của D-link (DIR-823, DIR-822, DIR-818L(W), DIR-895L, DIR-890L, DIR-885L, DIR-880L, DIR-868L, DIR-850L). Xử lý một tin nhắn SOAP độc hại trong quá trình đăng nhập HNAP có thể gây tràn bộ đệm, cho phép đối tượng đánh cắp thông tin đăng nhập và hệ thống. Lỗ hổng đã có mã khai thác.	Chưa có thông tin đăng nhập và bản vá
9	IBM	CVE-2018-1548 CVE-2018-1458 CVE-2018-1487 CVE-2018-1566 CVE-2013-3001 …	Nhóm 29 lỗ hổng trên nhiều sản phẩm của IBM (IBM API Connect, DB2, Infosphere, iNotes, Security Governance and Intelligent Virtual Appliance,...) cho phép đối tượng chèn và thực thi mã lệnh từ xa, đánh cắp thông tin, leo thang đặc quyền.	Đã có thông tin xác nhận và bản vá
10	Intel	CVE-2018-5704 CVE-2018-3652 CVE-2018-3619 CVE-2018-3668 CVE-2018-1667 …	Nhóm 13 lỗ hổng trên nhiều sản phẩm của Intel (Converged Security Manageability Engine Firmware; Nhiều đời chíp xử lý, Processor Diagnostic Tool, Quartus II, Quartus Prime, Quartus Prime Programmer and Tools) cho phép đối tượng thực thi mã lệnh và đánh cắp thông tin.	Đã có thông tin xác nhận

11	Juniper	CVE-2018-0039 CVE-2018-0040 CVE-2018-0027 CVE-2018-0030 CVE-2018-0024 …	Nhóm 16 lỗ hổng trên sản phẩm phần mềm của Juniper (Juniper Network CSO, Junos OS) cho phép đối tượng tấn công từ chối dịch vụ, lợi dụng các thông tin đăng nhập và các khóa, chứng chỉ bảo mật được hardcode, cũng như việc lưu mật khẩu trong các filelog để kiểm soát hệ thống.	Đã có thông tin xác nhận và bản vá
12	Microsoft	CVE-2018-8284 CVE-2018-8321 CVE-2018-8280 CVE-2018-8296 CVE-2018-8323 …	Nhóm 52 lỗ hổng trên nhiều sản phẩm của Microsoft (.Net, Windows, Word, Office, Sharepoint, Chakracore, Edge, Internet Explorer, Skype, Lync, Visual Studio, Powershell) cho phép đối tượng chèn và thực thi mã lệnh, leo thang đặc quyền và từ chối mã lệnh.	Đã có thông tin xác nhận và bản vá
13	VideoLan	CVE-2018-11529	Lỗ hổng trên phần mềm xem video VLC Media Player phiên bản 2.2.x cho phép đối phương chèn và thực thi mã lệnh trên các tệp MKV hoặc tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
14	VMware	CVE-2018-6965 CVE-2018-6966 CVE-2018-6967 CVE-2018-6969	Nhóm 4 lỗ hổng trên các sản phẩm của VMware (ESXi, Workstation, Fusion, VMware Tools) cho phép đối tượng đánh cặp thông tin và crash các máy ảo trên hệ thống.	Đã có thông tin xác nhận và bản vá

15	Xiaomi	CVE-2018-14010 CVE-2018-14060	Nhóm 02 lỗ hổng trên các dòng router của Xiaomi (R3P, R3, R3D) cho phép đối tượng thực hiện chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận và bản vá
16	Adobe	CVE-2018-5028 CVE-2018-5043 CVE-2018-5025 CVE-2018-5037 CVE-2018-5050 …	Nhóm 113 lỗ hổng trên các phần mềm của Adobe được sử dụng rất phổ biến ở Việt Nam (Acrobat and Reader, Connect, Experience Manager, Flash Player) cho phép đối tượng tấn công thực thi mã lệnh và đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá
17	Cisco	CVE-2018-0394 CVE-2018-0368 CVE-2018-0398 CVE-2018-0399 CVE-2018-0370 …	Nhóm 37 lỗ hổng trên nhiều dòng sản phẩm của Cisco (Cloude Service Platform, Digital Network Architecture Center, Finesse, FireSIGHT System Software,…) cho phép đối tượng tấn công chiếm quyền quản trị, chèn và thực thi mã lệnh, tấn công từ chối dịch vụ, tấn công XSS.	Đã có thông tin xác nhận
18	Fortinet	CVE-2017-17541	Lỗ hổng trên các phần mềm FortiManager và FortiAnalyzer (phiên bản 6.0.0 và các phiên bản trước 5.6.4) cho phép đối tượng tấn công thực hiện tấn công XSS.	Đã có thông tin xác nhận và bản vá
19	Foxit	CVE-2018-14442	Lỗ hổng trên Foxit Reader and PhantomPDF trước phiên bản 9.2 cho phép đối tượng chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá

20	Oracle	CVE-2018-2904 CVE-2018-2962 CVE-2018-3004 CVE-2018-3012 CVE-2018-2976 …	Nhóm 205 lỗ hổng trên nhiều sản phẩm của Oracle (Construction and Engineering Suite, Database Server, E-Business Suite, Financial Service Applications, Fussion Middleware, Virtual Box, My SQL,…) cho phép đối tượng tấn công truy cập, chỉnh sửa dữ liệu hệ thống, người dùng; chiếm quyền quản trị, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
21	Wordpress	CVE-2018-14071 CVE-2018-13832	Nhóm 02 lỗ hổng trên các tiện ích của nền tảng Wordpress (Geo Mashup, Techotronic) cho phép đối tượng tấn công thực hiện tấn công XSS, chèn và thực thi mã lệnh từ xa.	Chưa có thông tin xác nhận và bản vá
22	Adobe	CVE-2018-5018 CVE-2018-5024 CVE-2018-12805 CVE-2018-5004 CVE-2018-5007 …	Nhóm 111 lỗ hổng trên các phần mềm của Adobe được sử dụng rất phổ biến ở Việt Nam (Acrobat and Reader, Connect, Experience Manager, Flash Player) cho phép đối tượng tấn công thực thi mã lệnh và đánh cắp thông tin.	Đã có thông tin xác nhận và bản vá
23	Netgear	CVE-2016-5649 CVE-2016-5638	Nhóm 02 lỗ hổng trên các dòng router của Netgear (DGN2200, DGND3700, WNDR4500) cho phép đối tượng tấn công đánh cắp các thông tin nhạy cảm để chiếm quyền quản trị hệ thống.	Chưa có thông tin xác nhận và bản vá

24	Siemens	CVE-2018-11452 CVE-2018-11451	Nhóm 02 lỗ hổng trên nhiều firmware của các sản phẩm của Siemens cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
25	VMware	CVE-2018-6972 CVE-2018-6971	Nhóm 02 lỗ hổng trên các phần mềm của VMware (ESXi, Workstation, Fusion, Horizon View Agents) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ và đánh cắp thông tin đăng nhập.	Đã có thông tin xác nhận và bản vá
26	Wordpress	CVE-2018-14430	Lỗ hổng trong tiện ích Mondula Multi Setp Form (từ phiên bản 1.2.5) của nền tảng Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS.	Chưa có thông tin xác nhận và bản vá
27	ZTE	CVE-2017-10934 CVE-2017-10935 CVE-2017-10936 CVE-2017-10937	Nhóm 04 lỗ hổng trên nhiều sản phẩm của ZTE (ZXIPTV-SNS, ZXIPTV-EPG, ZXIPTV-UCM, ZXR10 1800-2S) cho phép đối tượng thực hiện tấn công lây nhiễm SQL, chèn và thực thi mã lệnh, thay đổi mật khẩu người dùng.	Đã có thông tin 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

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

TT	Tên miền/IP
1	w42f4ctqv4.ru

2	kukutrustnet777.info
3	104.244.14.252
4	g.omlao.com
5	v2k1j0t1.ru
6	mk.omkol.com
7	kukutrustnet888.info
8	init.icloud-analysis.com
9	u.amobisc.com
10	p.omlao.com
11	a6xwktlad.ru
12	b08fyqxb2.ru
13	6r9v0ojq.ru
14	0-0-0-0-0-0-0-0-0-0-0-0-0-0-10-0-0-0-0-0-0-0-0-0-0-0-0.info
15	0-0-0-0-0-0-0-0-0-0-0-0-0-0-5-0-0-0-0-0-0-0-0-0-0-0-0.info
16	zsgnlc8k.ru
17	me4abx32b.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

Ngày 21 tháng 07 năm 2018, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) có Công văn số 234/VNCERT-ĐPƯC gửi Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường về việc theo dõi, ngăn chặn kết nối và xoá các tập tin mã độc tấn công có chủ đích vào ngân hàng và các tổ chức hạ tầng quan trọng quốc gia. Theo công văn, Trung tâm VNCERT đã ghi nhận các hình thức tấn công có chủ đích của tin tặc nhắm vào hệ thống thông tin của một số ngân hàng và hạ tầng quan trọng quốc gia tại Việt Nam vào cuối tháng 7/2018. Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng tấn công và thực hiện các thủ thuật lừa đảo, kết hợp với các biện pháp kỹ thuật cao để qua mặt các hệ thống bảo vệ an toàn thông tin (ATTT) của các ngân hàng và các tổ chức hạ tầng quan trọng nhằm chiếm quyền điều khiển máy tính của người dùng và thông qua đó tấn công các hệ thống máy tính nội bộ chứa thông tin quan trọng khác. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của ngân hàng và các tổ chức hạ tầng quan trọng quốc gia. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT của ngân hàng hoặc các tổ chức hạ tầng quan trọng sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin. Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường đã có công văn số 501/CNTT-KHCN để cảnh báo và hướng dẫn các đơn vị trực thuộc Bộ rà soát và phòng chống mã độc này.

Trên cơ sở Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ, Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường đã có công văn số 437/CNTT-KHCN ngày 15/06/2018 về việc triển khai Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ

nhằm hướng dẫn các đơn vị trực thuộc Bộ thực hiện các nội dung của Chỉ thị. Tuy nhiên đến thời điểm hiện tại, Cục vẫn chưa nhận được báo cáo của một số đơn vị trực thuộc Bộ. Ngày 17/7/2018, Bộ Tài nguyên và Môi trường đã nhận được công văn số 2291/BTTTT-CATTT của Bộ Thông tin và Truyền thông về việc đôn đốc, hướng dẫn thực hiện công tác xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin để thực hiện Nghị quyết số 131/NQ-CP (ngày 6/12/2017) của Chính phủ giao "Các bộ, cơ quan ngang bộ khẩn trương triển khai các nhiệm vụ quy định tại Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ", trong đó đối với các hệ thống thông tin quan trọng được đề xuất là cấp độ 4 và cấp độ 5 cần phải gửi Hồ sơ đề xuất cấp độ về Bộ Thông tin và Truyền thông để thẩm định. Để triển khai có hiệu quả Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ và Công văn số 2291/BTTTT-CATTT ngày 17/7/2018 của Bộ Thông tin và Truyền thông, Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường đề nghị các đơn vị nghiêm túc thực hiện các nội dung của Công văn số 437/CNTT-KHCN (ngày 15/06/2018) và khẩn trương lập danh mục các hệ thông tin gửi về Cục Công nghệ thông tin và Dữ liệu tài nguyên môi trường.

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

3.2.1. Các hình thức tấn công mạng chủ yếu

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. Các hình thức tấn công mạng chủ yếu bao gồm:

- 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, ...).

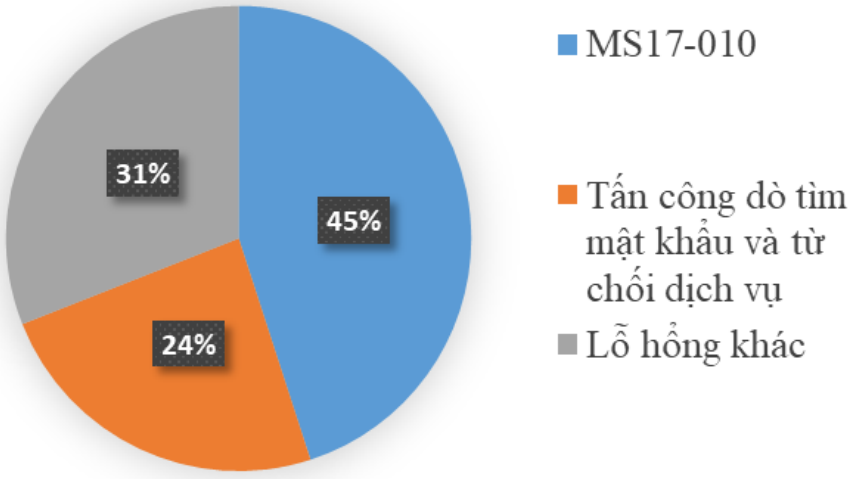
- Nhiều máy tính nội bộ (máy tính của người sử dụng) nhiễm mã độc kết nối tới máy chủ điều khiển - C&C, thực hiện tấn công các máy chủ nội bộ và các IP trên mạng Internet.

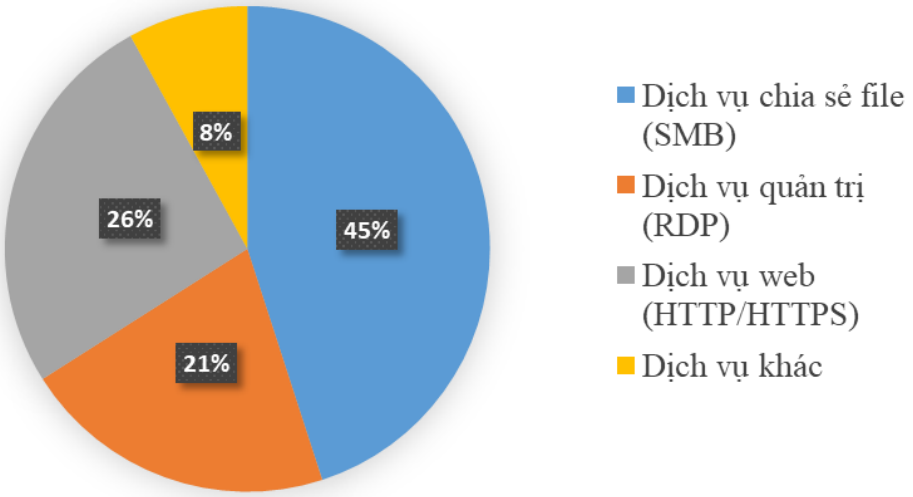
- Hiện tượng người dùng lộ mật khẩu tài khoản, bị hacker lợi dụng để gửi thư rác, thư có nội dung không phù hợp, thư chứa mã độc ra Internet.

- 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.	126,345 Cuộc tấn công; Trong đó tỉ lệ các cuộc tấn công mạng mức độ trung bình và nghiêm trọng là 3%
1. Danh sách các lỗ hổng bị tấn công khai thác nhiều nhất:	
- MS17-010	45 (%)
- 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)	24 (%)
- Lỗ hổng khác	31 (%)
	
2. Danh sách các dịch vụ bị tấn công nhiều nhất	
- Dịch vụ chia sẻ file của windows (cổng 445)	45 (%)
- Dịch vụ quản trị Remote Desktop	21 (%)
- Dịch vụ web (cổng 80, 443)	26 (%)
- Dịch vụ khác	8 (%)

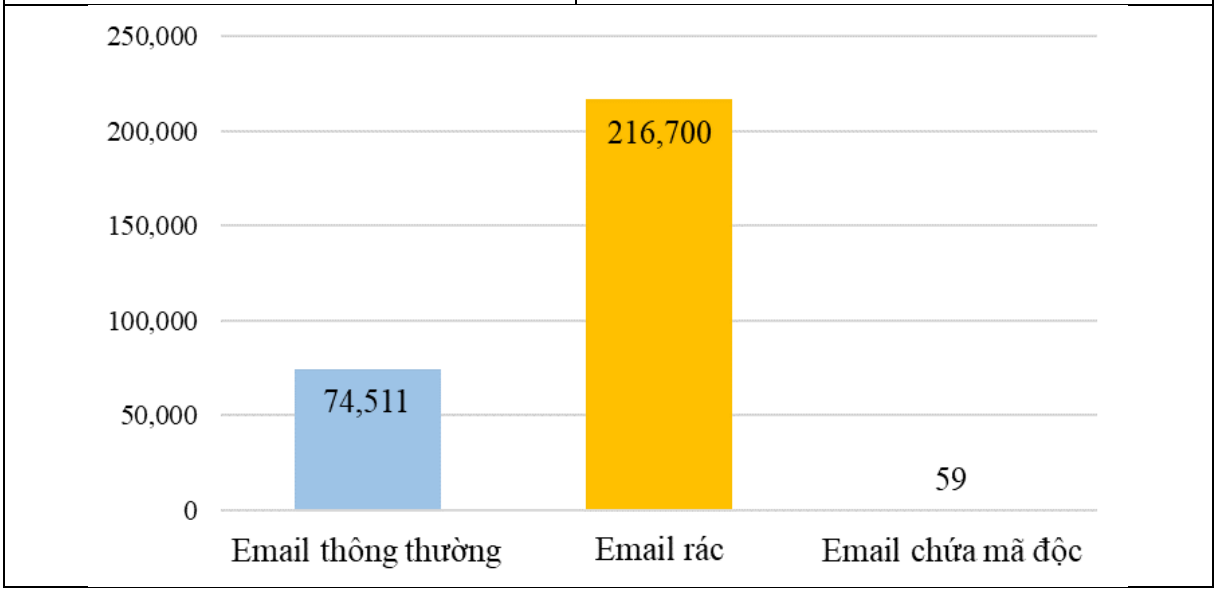


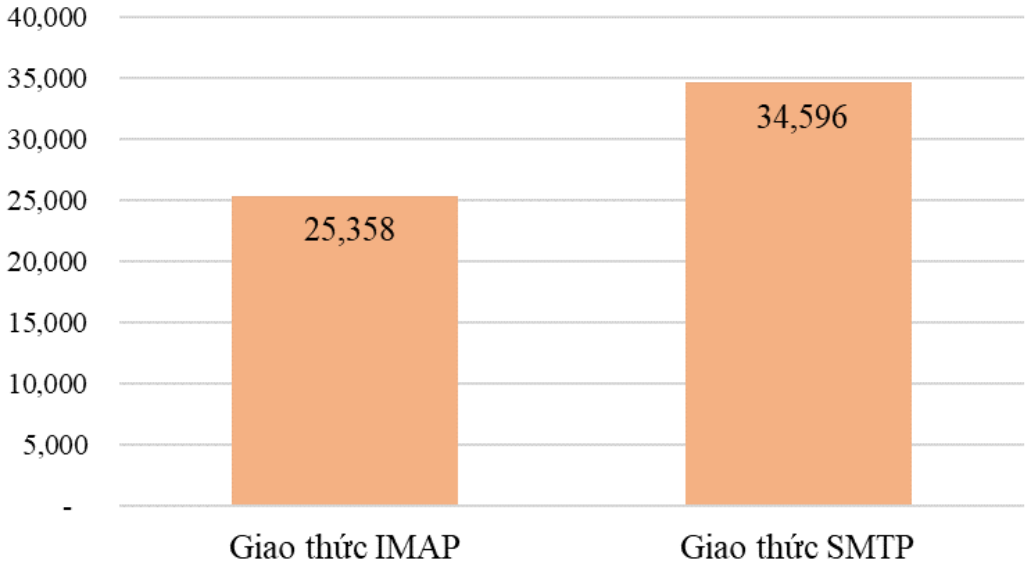
3. Danh sách các loại virus, botnet phát hiện trong hệ thống mạng	
- Loại virus	Andromeda.TC.f Andromeda.TC.gabbaaabb Compromisedsite.cdq Cryptominer-monero.TC.affafaabg Dorkbot.TC.o HEUR:Trojan.Win32.Agent.gen.W.oitgq Malicious Binary.TC.cgami Malicious Binary.TC.chfth Malware.ysxfb MALWARE-URL.hhoiw Phishing.dhsfqk Phishing_website.kdxy REP.TC.fgojw Trojan.Win32.Generic.TC.jwm Wannamine.TC.c website.tqzvev.TC.a XMRig.TC.a
- Mạng botnet	Adware.TC.bw BotnetB.TC.debadabbe BotnetB.TC.debadabbe

	BotnetB.TC.eoe BotnetB.TC.jgv BotnetB.TC.jhk Cnc server.TC.ad Fireball.TC.fdcbaaabbf Fireball.TC.fdcbaaabbf Nitol.TC.m Trojan-Downloader.Win32.Necorapo.A
4. Nhiều máy tính người dùng nhiễm mã độc	
Nhiều máy tính người dùng nhiễm mã độc, kết nối đến các máy chủ điều khiển trên internet (khoảng 49 máy)	Các máy tính nhiễm mã độc 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 6:

Mục	Số liệu thống kê
1. Thống kê chung về gửi nhận mail	
- Tổng lượng email gửi nhận	74,511 (email)
- Tỉ lệ thư rác	74.40 (%) (khoảng 216,700 email)
- Tỉ lệ email chứa mã độc	0.02 (%) (59 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	59,954 (lượt dò tìm mật khẩu)
- Các dịch vụ mail bị tấn công nhiều nhất	IMAP (42.3% số cuộc tấn công) SMTP (57.7% số cuộc tấn công)
- Số lượng tài khoản nghi ngờ mất mật khẩu	2 (tài khoản)
	
3. Tài khoản có dấu hiệu mất mật khẩu. Trong tháng 7, ghi nhận từ hệ thống giám sát 05 tài khoản có dấu hiệu đăng nhập từ IP nước ngoài. Trong đó:	
- 03 trường hợp tài khoản thư điện tử người dùng bị mất mật khẩu; bị hacker lợi dùng để thực hiện gửi thư có nội dung độc hại ra internet. - Các tài khoản trên đều không đổi mật khẩu trong thời gian dài.	Các tài khoản bị mất mật khẩu đã được xử lý kịp thời, không gây ảnh hưởng lớn tới hệ thống thư điện tử.
- 02 tài khoản còn lại đang được nhóm giám sát theo dõi, phối hợp với	Nhiều tài khoản trong số này đã được người dùng đổi mật khẩu, song hiện

đầu mối các đơn vị để xử lý.	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 7/2018 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./.