HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Thị Hạnh

NGHIÊN CỨU CÁC PHƯƠNG THỨC TẤN CÔNG HỆ THỐNG EMAIL VÀ CÁC GIẢI PHÁP PHÒNG CHỐNG ANTI-SPAM

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2019

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Thị Hạnh

NGHIÊN CỨU CÁC PHƯƠNG THỨC TẤN CÔNG HỆ THỐNG EMAIL VÀ CÁC GIẢI PHÁP PHÒNG CHỐNG ANTI-SPAM

Chuyên ngành : HỆ THỐNG THÔNG TIN
Mã số: 8.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. TRẦN QUANG ANH

HÀ NỘI 2019

LỜI CAM ĐOAN

Tôi xin cam đoan các kết quả nghiên cứu trong luận văn này là sản phẩm của các nhân tôi dưới sự hướng dẫn của thầy giáo PGS.TS Trần Quang Anh. Các số liệu, kết quả được công bố là hoàn toàn trung thực. Những điều được trình bày trong toàn bộ luận văn này là những gì do tôi nghiên cứu hoặc là được tổng hợp từ nhiều nguồn tài liệu khác nhau. Các tài liệu tham khảo có xuất xứ rõ ràng và được trích dẫn đầy đủ, hợp pháp.

Tôi xin hoàn toàn chịu trách nhiệm trước lời cam đoan của mình.

Hà Nội, ngày 20 tháng 11 năm 2019

Người cam đoan

Nguyễn Thị Hạnh

LỜI CẢM ƠN

Đầu tiên, tôi gửi lời cảm ơn chân thành và biết ơn sâu sắc tới thầy giáo PGS.TS Trần Quang Anh – Học viện Bưu chính Viễn thông, người thầy đã luôn tận tình chỉ bảo, giúp đỡ và hướng dẫn tôi trong suốt quá trình nghiên cứu luận văn này.

Tôi xin chân thành cám ơn các thầy, cô giáo trong Khoa Công nghệ thông tin- Học viện Bưu chính Viễn thông đã luôn tận tâm truyền dạy cho tôi những kiến thức bổ ích trong thời gian tôi tham gia học tập và nghiên cứu tại trường.

Tôi cũng xin gửi lời cảm ơn tới Ban lãnh đạo, các anh chị và các bạn trong lớp Hệ thống thông tin đã ủng hộ và khuyến khích tôi trong quá trình nghiên cứu và thực hiện khóa luận này.

Học viên

Nguyễn Thị Hạnh

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC KÍ HIỆU VIẾT TẮT

Viết tắt	Từ hoặc cụm từ
Email	Electronic Mail - Thư điện tử
Spam	Stupid Pointless Annoying- Thư rác
DNS	Domain Name System – Tên miền
RBL	Realtime Blackhole List
MAPS	Multiple Address Processing System
SPF	Sender Policy Framework
XML	eXtensible Markup Language
APT	Advanced Persistent Threat
ESA	Email Security Advanced
DLP	Data Loss Prevention
SNMP	Simple Network Management Protocol
HAT	Host Access Table
RAT	Recipient Access Table
LDAP	Lightweught Directory Access Protocol

MỞ ĐẦU

1. Lý do chọn đề tài

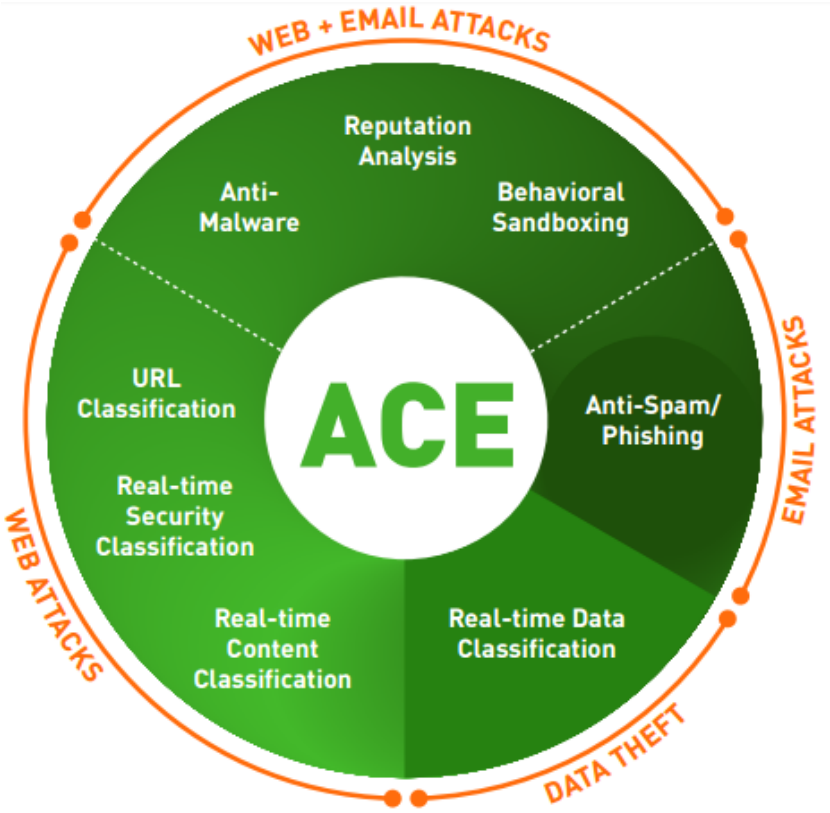
Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của các tổ chức, cá nhân đều được lưu trữ trên hệ thống máy tính và trao đổi với nhau từ mọi vị trí địa lý. Cùng với sự phát triển của tổ chức là những đòi hỏi ngày càng cao của môi trường hoạt động cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua mạng. Việc mất mát, rò rỉ thông tin sẽ có thể ảnh hưởng nghiêm trọng đến tài nguyên thông tin, tài chính, danh tiếng của tổ chức, cá nhân.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của tổ chức. Vì vậy an toàn thông tin là nhiệm vụ quan trọng, nặng nề và khó đoán trước đối với các hệ thống thông tin.

Email là một trong các nguồn chính gây rủi ro về an toàn thông tin. Bên cạnh vấn đề thư rác, virus, có khá nhiều tấn công lừa đảo thực hiện qua Email và Email chính là mục tiêu hàng đầu của các cuộc tấn công có chủ đích (APT). Các rủi ro về mất mát dữ liệu nhạy cảm do tấn công lừa đảo, malware, do người dùng cố ý hoặc vô ý được diễn ra một phần không nhỏ là qua Email. Theo thống kê có:

- 84% các Email là thư rác (spam)
- 89% các Email không mong muốn chứa đường link tới Email độc hại
- 9% rò rỉ dữ liệu nhạy cảm xảy ra qua Email

Do đó, việc phân tích các mối đe doạ theo thời gian thực tại Email Gateway, cung cấp báo cáo nâng cao để đánh giá, điều tra các sự kiện đối với hệ thống Email là rất cần thiết.



Hình 1: Sử dụng ACE phân tích các nguy hại theo thời gian thực

2. Mục đích nghiên cứu:

Trong nhiều năm trước, khi Internet bắt đầu phát triển mạnh mẽ trên khắp thế giới, các Email đã truyền tải thông tin dưới dạng dữ liệu ngày càng phức tạp. Tổng lượng tổ chức, người truy cập và sử dụng Email đã tăng lên nhanh chóng.

Hệ thống Email là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, truyền tải thông tin, là tài sản rất quan trọng nhưng cũng chứa rất nhiều điểm yếu và rủi do. Do Email được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng ngày càng tăng, các loại dịch vụ hoặc thông tin quảng cáo có chứa mã độc mới được thêm vào ngày càng nhiều, điều này làm cho Email không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống Email, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng có thể truy cập thông tin một cách dễ dàng và tin tặc cũng có nhiều mục tiêu tấn công.

Với việc phân tích các phương thức tấn công qua Email, đề tài mà luận văn quan tâm và nghiên cứu sẽ đưa ra cách nhận diện một tấn công từ bên ngoài hoặc bên trong đối với hệ thống Email. Từ đó phân tích các mối nguy hại, các phương thức tấn công và mức độ ảnh hưởng để đưa ra các phương pháp ngăn chặn, phòng chống, khắc phục và bảo vệ hệ thống Email một cách hiệu quả.

- ***Bảo vệ tài nguyên của hệ thống***

Các hệ thống máy tính lưu giữ rất nhiều thông tin cần truyền tải trên mạng và tài nguyên đó phải được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin của các hệ thống nghiên cứu. Đối với rất nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý, sử dụng bởi các chương trình phần mềm. Các tấn công vào hệ thống thông tin có thể được thực hiện qua Email, xuất phát từ những đối thủ của tổ chức hoặc cá nhân. Do đó, các phương pháp để bảo đảm an toàn cho những thông tin này rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng, gây tổn thất lớn đến từng cá nhân và tổ chức.

- ***Bảo đảm tính riêng tư***

Các hệ thống Email lưu giữ, truyền tải rất nhiều thông tin cần được giữ bí mật và chính xác. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,…Những thông tin riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo khi gửi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin của khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin được bí mật, phải thực hiện những quy định để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những Email và đánh cắp các thông tin cá nhân. Do đó bảo vệ Email cũng là một phương pháp để bảo đảm tính riêng tư của cá nhân và tổ chức.

3. Đối tượng và phạm vi nghiên cứu

- Với việc xác định đối tượng nghiên cứu chính là phân tích các phương thức tấn công qua Email và phương pháp phòng chống AntiSpam, đề tài sẽ đưa ra cách nhận diện một tấn công từ bên ngoài hoặc bên trong đối với hệ thống Email, phân tích chi tiết các tấn công Spam Email. Từ đó, làm rõ các mối nguy hại, các phương thức tấn công và mức độ ảnh hưởng để đưa ra các biện pháp ngăn chặn, phòng chống, khắc phục và bảo vệ hệ thống Email một cách hiệu quả.
- Phạm vi nghiên cứu: Để thực hiện nghiên cứu đối với các phương thức tấn công Email và phương pháp phòng chống AntiSpam, luận văn được xây dựng trên cơ sở kế thừa kết quả khảo sát thực tế và các tài liệu tham khảo.

4. Phương pháp nghiên cứu:

Luận văn này dự kiến tổ chức thực hiện nghiên cứu, đề xuất các phương pháp phòng chống tấn công Email và các yếu tố liên quan mật thiết đến việc xây dựng, vận hành hệ thống.

Nghiên cứu thực hiện thông qua phương pháp lý thuyết: các phương thức tấn công hệ thống Email, luồng gửi nhận dữ liệu, các thuật toán mã hóa, các phương pháp lọc gói tin,…

Nghiên cứu bằng phương pháp thực tiễn: từ việc phân tích dữ liệu gửi và nhận, thu thập các mẫu và mô tả cách phòng chống tại Ngân hàng Hàng Hải Việt Nam (MSB).

CHƯƠNG I. GIỚI THIỆU VỀ THƯ ĐIỆN TỬ, THƯ RÁC VÀ CÁC HÌNH THỨC TẤN CÔNG THƯ ĐIỆN TỬ

1.1 Tìm hiểu về thư điện tử (Email) và thư rác (Spam Email)

1.1.1. Tìm hiểu về thư điện tử (Email)

1.1.1.1 Định nghĩa thư điện tử (Email)

Email (là từ ghép viết tắt của Electronic Mail – Thư điện tử) là một dạng tin nhắn/ thông điệp được gửi đi từ một người dùng máy tính đến một hoặc nhiều người nhận qua mạng.

Thông điệp được lưu trữ trong Email có thể tồn tại ở dạng văn bản (text), hình ảnh, âm thanh, video với các hình thức tệp tin đính kèm.

1.1.1.2 Phân loại các loại Email hiện nay

Đối với hệ thống Email hiện nay có 2 loại Email là Email Server và Email miễn phí.

Email server: là giải pháp Email riêng biệt do tổ chức hoặc doanh nghiệp xây dựng hệ thống máy chủ riêng biệt để thực hiện việc quản trị toàn bộ hệ thống mail nội bộ của tổ chức hoặc doanh nghiệp đó. Email server cho phép kiểm soát 1 lượng lớn các Email gửi và nhận của các cá nhân trong đơn vị đảm bảo sự ổn định, liên tục với tốc độ nhanh, an toàn dữ liệu và khả năng khôi phục dữ liệu cao…

Email miễn phí: Sử dụng Email do một nhà cung cấp dịch vụ có sẵn như Gmail, Outlook, iClound Mail, Yahoo! Mail, AOL Mail, Zoho Mail, GMX Email, Yandex Mail, Mail.com, Lycos.com, …

So sánh hai dịch vụ Email Server và Email miễn phí

Tiêu chí so sánh	Email Server	Email Miễn Phí
Phí	Mất phí	Miễn phí
Tính năng	Như nhau (Danh sách liên hệ, lịch, takenote, đọc tin RSS,…)	Như nhau (Danh sách liên hệ, lịch, takenote, đọc tin RSS,…)

Đối tượng khách hàng	Các doanh nghiệp, tập đoàn	Hàng triệu người dùng trên toàn thế giới
Dung lượng	2GB-5GB (Doanh nghiệp chủ yếu gửi mail với thông điệp dạng văn bản	15GB cho tài khoảng Google (bao gồm Google Driver, Google Reader , Mail)
Quyền riêng tư	Khách hàng không bị truy cập mail trái phép, không bị chèn quảng cáo trong mail.	Khách hàng bị truy cập nội dung mail, bị chèn quảng cáo của Google Ads
Tài khoản	Tài khoản có dạng @domain. Không giới hạn số tài khoản. Dung lượng mỗi tài khoản có thể cấu hình tùy thuộc nhu cầu.	Bị giới hạn 10 tài khoản Email đối với khách hàng doanh nghiệp không thể nâng cấp thêm.
Khả năng định vị	Tạo niềm tin vào doanh nghiệp hơn, chuyên nghiệp hơn.	Đại trà nên thiếu cảm giác uy tín.
Đồng bộ hóa	Đồng bộ hóa dễ dàng, truy cập được từ Webmail, PC Outlook, Mobile,…	Đồng bộ danh bạ, truy cập trên điện thoại, PC, Webmail
Ngôn ngữ	Hỗ trợ tiếng Việt, support tại Việt Nam	Hỗ trợ tiếng Việt, Support rất khó nếu khách hàng tại Việt Nam
Tốc độ gửi mail	Tối đa 1 triệu mail/ngày với Email Marketing. 4800 mail/ngày đối với Email Business, tốc độ 2000 mail/phút	Tối đa 2000 mail/ngày, tốc độ chậm
Kiểm soát spam	Hỗ trợ và hướng dẫn khách hàng sử dụng dịch vụ, hạn chế tối đa việc Email gửi rơi vào mục Spam	Không đảm bảo, Email gửi dễ vào mục Spam
Tính thống kê	Hỗ trợ kiểm soát mail spam, mở mail, thống kê danh sách Email,lọc spam.	Không

Nhằm nghiên cứu tổng thể các phương thức tấn công hệ thống Email cũng như chủ động phân tích luồng dữ liệu gửi nhận trong hệ thống, luận văn tập trung nghiên cứu dịch vụ Email Server.

1.1.2. Tìm hiểu về thư rác (Spam Email)

1.1.2.1 Định nghĩa thư rác (Spam Email)

Spam (Stupid Pointless Annoying Messages) là những bức thư phiền toái, vô nghĩa, ngu ngốc.

Spam Email: là việc gửi hàng loạt Email chứa nội dung không liên quan hoặc vô bổ đến nhiều người nhận. Spam Email thường chứa các loại quảng cáo được gửi một cách vô tội vạ từ một địa chỉ không xác định đến nơi nhận là một danh sách rất dài gửi đến các cá nhân hay các nhóm người. Chất lượng của loại thư này thường thấp, đôi khi là một sự lừa đảo để tìm cách thu thập tin tức cá nhân hoặc từ đó xâm nhập vào hệ thống mạng.

Hầu hết các thư rác có bản chất thương mại, không chỉ gây phiền nhiễu mà còn nguy hiểm vì chúng chứa các liên kết dẫn đến các trang web lừa đảo hoặc trang web đang chưa các phần mềm độc hại dưới dạng tệp đính kèm.

Kẻ gửi thư rác thường thu thập địa chỉ Email từ các phòng trò chuyện, trang web, danh sách khách hàng, mạng xã hội và phát tán các virus tới địa chỉ người dùng. Những Email này sẽ được thu thập và đôi khi bán cho những doanh nghiệp kinh doanh hoặc đối thủ cạnh tranh khác.

1.1.2.2 Các đặc điểm thư rác (Spam Email)

Spam Email được gửi đi một cách tự động: Mục đích của những kẻ gửi thư rác (spammer) là có thể phát tán lượng thư rác rất lớn tới người dùng càng nhiều càng tốt. Do vậy, chúng thường xuyên xây dựng phần mềm tự động gửi một lượng lớn thư rác trong một thời gian ngắn.

Spam Email được gửi đến những địa chỉ ngẫu nhiên trên một diện rộng: Địa chỉ Email của người bị nhận thư rác rất ngẫu nhiên và dường như giữa người nhận và người gửi không có mối quan hệ với nhau. Có nhiều phương pháp và thủ

thuật mà những kẻ gửi thư rác áp dụng trong việc dò tìm địa chỉ Email của người dung như:

Dùng chương trình tự động dò tìm địa chỉ Email trên mạng Internet, các trang chủ, Newsgroup, Chat room….

Mua địa chỉ Email từ những công ty đã xây dựng danh sách khác hàng của họ nhưng vì lý do nào đó bán cho đối tác của công ty này để gửi thông tin về dịch vụ hay sản phẩm.

Email chuỗi (Chain letter) từ bạn bè và người thân, yêu cầu gửi thư cho càng nhiều người càng tốt vì lý do ủng hộ hay mời chào thử nghiệm một sản phẩm nào đó, một chương trình giảm giá để người dùng đặc biệt quan tâm nhằm đánh lừa và thu thập thông tin.

Spam Email dùng chương trình đoán tên tự động: Những kẻ gửi Spam Email dùng chương trình này gửi Email liên tục vào một nơi để đoán địa chỉ Email qua những phương pháp như E-pending, Dictionary hay Alphabet

Bên cạnh đó, những kẻ gửi thư rác còn có thể có được địa chỉ Email của người dùng do:

Các nhà cung cấp dịch vụ (ISP) không có chính sách và công nghệ bảo mật, dẫn đến việc các tin tặc (hacker) ăn cắp địa chỉ của khách hàng để buôn bán và gầy phiền nhiễu. Có thể do chính ISP buôn bán địa chỉ Email của khách hàng để kiếm lợi nhuận, các nhân viên ISP đã tiết lộ thông tin về khách hàng cho các đối thủ cạnh tranh chính ISP đó, hoặc cho những công ty muốn quảng cáo cho những khách hàng riêng biệt.

Chính người dùng cung cấp địa chỉ Email của mình qua những lần đăng ký làm thành viên trên các cộng đồng Internet hoặc trên các dịch vụ mà vô tình đã bị đánh cắp thông tin.

Nội dung của Spam Email thường là những nội dung bất hợp pháp, gây phiền hà cho người dùng: Phần lớn nội dung của thư rác là những thông tin mời chào về thương mại hay quảng cáo. Bên cạnh đó, phải kể đến những thư rác có nội dung xấu (như khiêu dâm, chống phá chính trị,…) gây tâm lý lo ngại cho người làm

công nghệ thông tin. Lượng thư rác phát tán virus rất lớn. Trong những thư này thường mang theo virus gây tê liệt hoàn toàn máy tính của người dùng, đánh cắp thông tin cá nhân hoặc làm hỏng dữ liệu trên máy tính.

Địa chỉ của người gửi thư rác thường là những địa chỉ trá hình: Để tránh sự nghi ngờ của người nhận, một số kẻ gửi thư rác thường giả dạng địa chỉ của một người dùng bình thường trong một máy chủ Email nào đó một cách bất hợp pháp hoặc một địa chỉ giả để gửi thư rác.

1.1.2.3 Các kỹ thuật tạo ra một Spam Email

Kỹ thuật che giấu hoặc chuyển hướng nội dung, liên kết: Đó là những kỹ thuật che dấu nội dung cũng như liên kết, có thể với người dùng thì nội dung hay các liên kết của trang web đó là bình thường, nhưng với bộ máy tìm kiếm thì nó lại hiển thị ở một dạng khác hoặc nó chuyển hướng người dùng đến một trang có nội dung hiển thị hoàn toàn khác với trang mà con bọ tìm kiếm nhìn thấy.

Tấn công trang web: Một số trường hợp trang web có thể bị tấn công theo kiểu hiển thị nội dung hoặc các liên kết Spam cho bộ máy tìm kiếm. Trước kia điều này rất nguy hiểm cho website, có thể sẽ bị dính thuật toán một cách oan ức.

Văn bản ẩn hoặc nhồi nhét từ khóa: Những trang web cố tình nhồi nhét từ khóa hoặc chứa các văn bản ẩn, trước kia đây là một trong những lỗ hổng của Google, nhưng đến nay thì lỗ hổng này đã được các thuật toán cập nhật phát hiện và thay thế.

Tên miền trỏ hướng: là các trang web được sử dụng các biện pháp để có thể đứng ở vị trí cao với rất ít nội dung có giá trị, khi mà người dùng click vào tên miền đó nó sẽ chuyển sang một website khác.

Spam thuần túy: Các trang web sử dụng các kỹ thuật Spam có tính công kích ví dụ như những website có nội dung vụn vặt, che giấu, những chuỗi văn bản vô nghĩa được tạo tự động từ các trang web khác.

Cung cấp DNS động và máy chủ lưu trữ gây ra spam: Đó là những trang web được lưu trữ bởi những dịch vụ miễn phí hoặc các nhà cung cấp DNS động chứa một lượng lớn những nội dung spam.

Nội dung nghèo nàn có ít hoặc không có giá trị: Các trang web có chất lượng thấp, nội dung nghèo nàn, có giá trị thấp hoặc không có giá trị cho người dùng hoặc những trang web có chứa nhiều liên kết xấu, kém chất lượng, các trang con giống nhau hàng loạt, nội dung được tạo dựng một cách tự động hoặc sao chép từ các website khác.

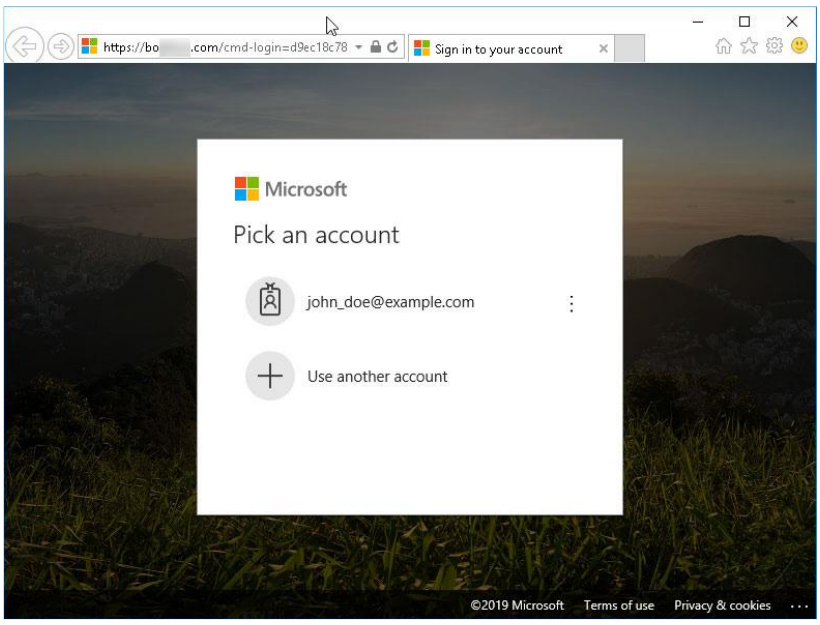
Liên kết bất thường từ trang web: những trang web có sử dụng các liên kết bất thường, những liên kết giả mạo nhằm mục đích thao túng vị trí xếp hạng, pagerank những việc làm này thường được phát sinh từ quá trình mua bán, trao đổi liên kết.

1.2 Các hình thức tấn công Email

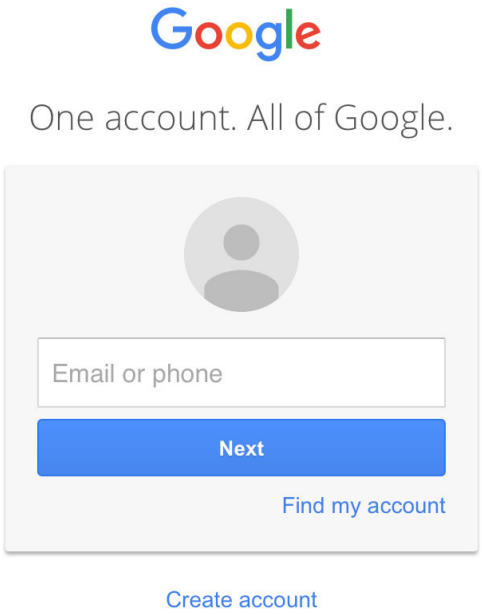
1.2.1 Một số hình thức tấn công Email

Lừa đảo qua tổ chức danh tiếng : Các Email được gửi đến từ Microsoft và đưa ra thông tin về Email của người dùng sẽ bị ngắt kết nối do vi phạm chính sách, yêu cầu xác minh địa chỉ tại địa chỉ liên kết đính kèm. Khi đó người dùng cố gắng đăng nhập và nhận về mail có dạng micros0ftsupport@hotmail.com, nhấp vào liên kết sẽ link đến một trang web giả mạo và yêu cầu đăng nhập thông tin.

Không chỉ Email được gửi từ Microsoft mà các Email khác cũng dễ dàng bị đánh lừa với cách thức tương tự.



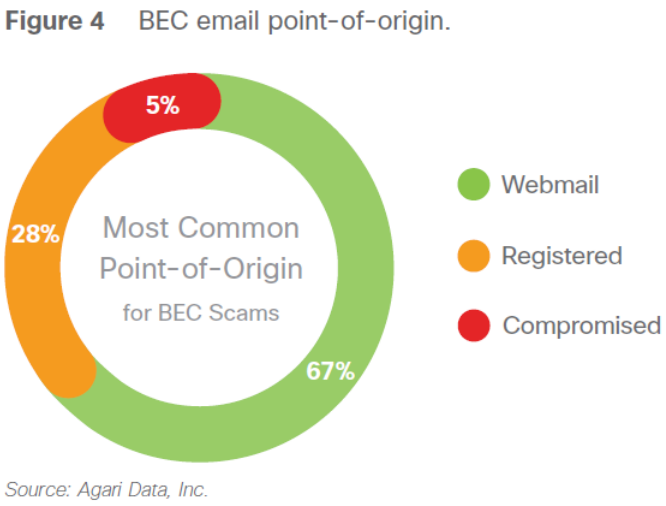
Hình 1.1: Email Outlook dạng lừa đảo



Hình 1.2: Gmail dạng lừa đảo

Hình 1.1 và hình 1.2 là một dạng Email lừa đảo có giao diện giống như các trang web uy tín, tuy nhiên tên website đã bị thay đổi dạng bo.micros0ft.login.com và Gmaiin.com. Khi người dùng không nhận ra sự lừa đảo và nhấp vào liên kết, trang giả mạo sẽ yêu cầu nhập thông tin cá nhân và đánh cắp thông tin đó.

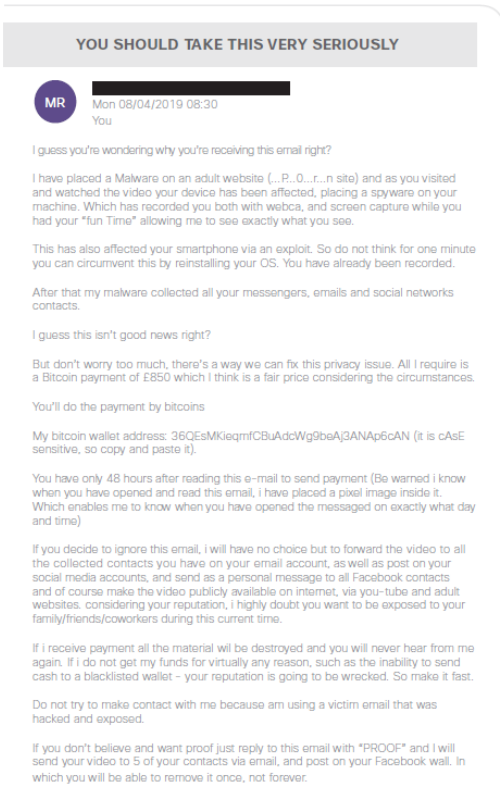
Email thỏa thuận từ doanh nghiệp: Trong thời gian người sử dụng Email đang tham gia đàm phán tài chính. Đột ngột có Email đến hộp thư và hướng dẫn tài khoản thanh toán bị gián đoạn và sẽ gây hậu quả nghiêm trọng đến tổ chức nếu không thực hiện đúng hạn, kèm theo là một hướng dẫn thanh toán. Khi đó kẻ tấn công sẽ tận dụng mạo danh người điều hành và lấy cắp thông tin của người dùng, doanh nghiệp



Hình 1.3: Email lừa đảo thỏa thuận doanh nghiệp

Hình 1.3 cho thấy tỷ lệ Email bị lừa đảo đối với doanh nghiệp theo báo cáo từ tổ chức BEC, trong đó có 67% Email đăng ký, 28% Email đã đăng ký tài khoản, 5% Email thỏa thuận yêu cầu đàm phán tài chính.

Email tống tiền: Một Email được gửi đến với nội dung "YOU SHOULD TAKE THIS VERY SERIOUSLY". Người gửi sẽ yêu cầu một trang web đen mà người nhận đã truy cập, người gửi khẳng định họ đã quay lại video của người nhận và yêu cầu bồi thường, tuy nhiên không trả bằng tiền mặt mà bằng Bitcoin. Đó là một dạng tống tiền kỹ thuật số, kẻ lừa đảo sẽ có thông tin của người dùng và bạn bè người dùng trong danh sách.



YOU SHOULD TAKE THIS VERY SERIOUSLY

MR [redacted]
Mon 08/04/2019 08:30
You

I guess you're wondering why you're receiving this email right?

I have placed a Malware on an adult website (...P...0...r...n site) and as you visited and watched the video your device has been affected, placing a spyware on your machine. Which has recorded you both with webca, and screen capture while you had your "fun Time" allowing me to see exactly what you see.

This has also affected your smartphone via an exploit. So do not think for one minute you can circumvent this by reinstalling your OS. You have already been recorded.

After that my malware collected all your messengers, emails and social networks contacts.

I guess this isn't good news right?

But don't worry too much, there's a way we can fix this privacy issue. All I require is a Bitcoin payment of £850 which I think is a fair price considering the circumstances.

You'll do the payment by bitcoins

My bitcoin wallet address: 36QEsMKieqmfCBuAdcWg9beAj3ANAp6cAN (it is cAsE sensitive, so copy and paste it).

You have only 48 hours after reading this e-mail to send payment (Be warned i know when you have opened and read this email, i have placed a pixel image inside it. Which enables me to know when you have opened the messaged on exactly what day and time)

If you decide to ignore this email, i will have no choice but to forward the video to all the collected contacts you have on your email account, as well as post on your social media accounts, and send as a personal message to all Facebook contacts and of course make the video publicly available on internet, via you-tube and adult websites. considering your reputation, i highly doubt you want to be exposed to your family/friends/coworkers during this current time.

If i receive payment all the material wil be destroyed and you will never hear from me again. If i do not get my funds for virtually any reason, such as the inability to send cash to a blacklisted wallet - your reputation is going to be wrecked. So make it fast.

Do not try to make contact with me because am using a victim email that was hacked and exposed.

If you don't believe and want proof just reply to this email with *PROOF* and I will send your video to 5 of your contacts via email, and post on your Facebook wall. In which you will be able to remove it once, not forever.

Hình 1.4: Dạng Email tống tiền

Email có chứa phần mềm độc hại: Các phần mềm độc hại được đính kèm trực tiếp vào Email nhưng thường được giả mạo để vượt qua Email truyền thống. Thực tế Java và Flash được nén dạng winrar với những nội dung như khuyến mại, mang lại ưu đãi cho người dùng.

Table 1 Malicious attachment types.

Type	Percentage
Office	42.8%
Archive	31.2%
Script	14.1%
PDF	9.9%
Binary	1.77%
Java	0.22%
Flash	0.0003%

Source: Talos Intelligence

Table 2 Top 10 malicious extensions in email.

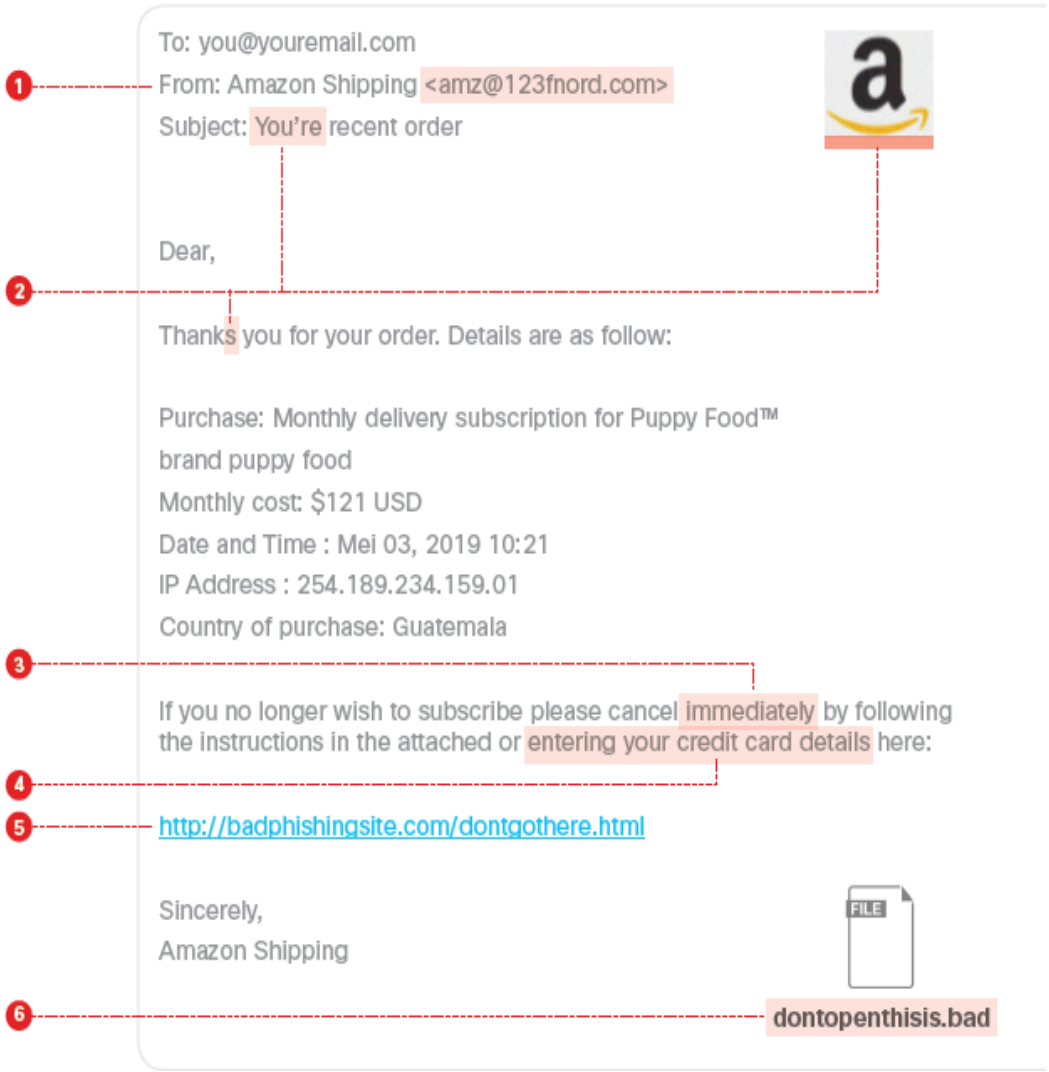
Extension	Percentage
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2%

Source: Talos Intelligence

Hình 1.5: Thống kê Email có đính kèm mã độc

Hình 1.5 cho thấy tỷ lệ các mã độc đính kèm trong các ứng dụng và định dạng, trong đó ứng dụng office các mã độc chiếm 42,8 %, archive chiếm 31,2 %. Các mã độc được mã hóa hoặc gửi đi với các định dạng .doc chiếm 41,8%, .zip chiếm 26,3% và thấp nhất là .xlsx chiếm 0,2%.

1.2.2 Kiến trúc của thư điện tử dạng lừa đảo tấn công



Hình 1.6: Kiến trúc Email lừa đảo

(1) Từ địa chỉ không hợp lệ như : @123fnord.com, @gmaiil, @yahhoo,…

(2) Chứa nhiều lỗi chính tả và ngữ pháp hoặc logo mờ. Địa chỉ được tạo ra không phù hợp hoặc một cách không cẩn thận

(3) Email yêu cầu thực hiện hành động ngay lập tức như click để nhận phần thưởng hoặc khơi gợi trí tò mò

(4) Yêu cầu cung cấp thông tin cá nhân như : họ tên, địa chỉ nhà, số điện thoại, số tài khoản tài chính,…

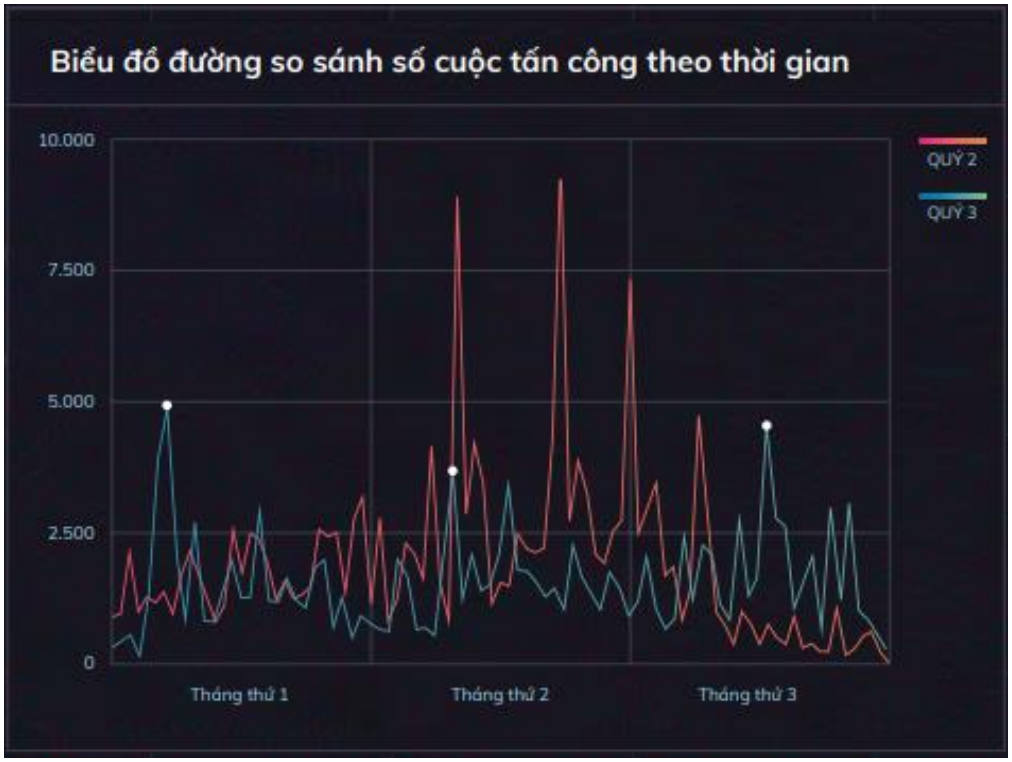
(5) Đính kèm URL bất hợp pháp, có nhiều lừa đảo. URL thường ẩn trong đó là liên kết đến một trang web có chứa mã độc hoặc virus

(6) Loại tệp được định dạng lạ, không thường xuyên nhận được định dạng đó nên cần xem xét và cách ly trước khi thực hiện.

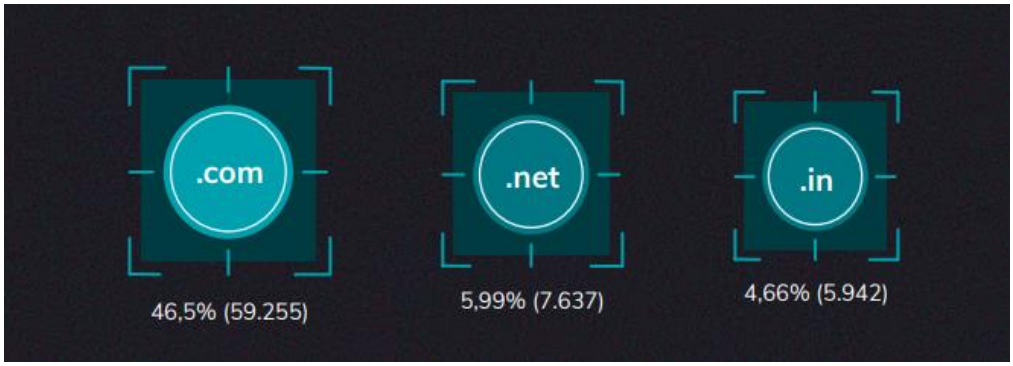
1.3 Hiện trạng về các tấn công Email hiện nay

1.3.1 Tình hình tấn công Email trên thế giới

Trong quý 3 năm 2019 vừa qua, hệ thống CyStack Attack Map đã ghi nhận 127.367 website bị tấn công và chiếm quyền điều khiển. Như vậy, số website này đã giảm 27% so với con số 175.451 website bị tấn công trong quý 2. Cụ thể trong quý 3, số lượng website tháng 7, 8 và 9 lần lượt là 38.385, 44.848 và 44.134, giảm hơn so với mức trung bình 42.483 website/tháng của quý trước. Tuy nhiên, trong các ngày 11/7, 11/8 và 14/9, số website bị hack cũng tăng đột biến, riêng ngày 11/7 số website bị tấn công còn gần chạm mốc năm nghìn

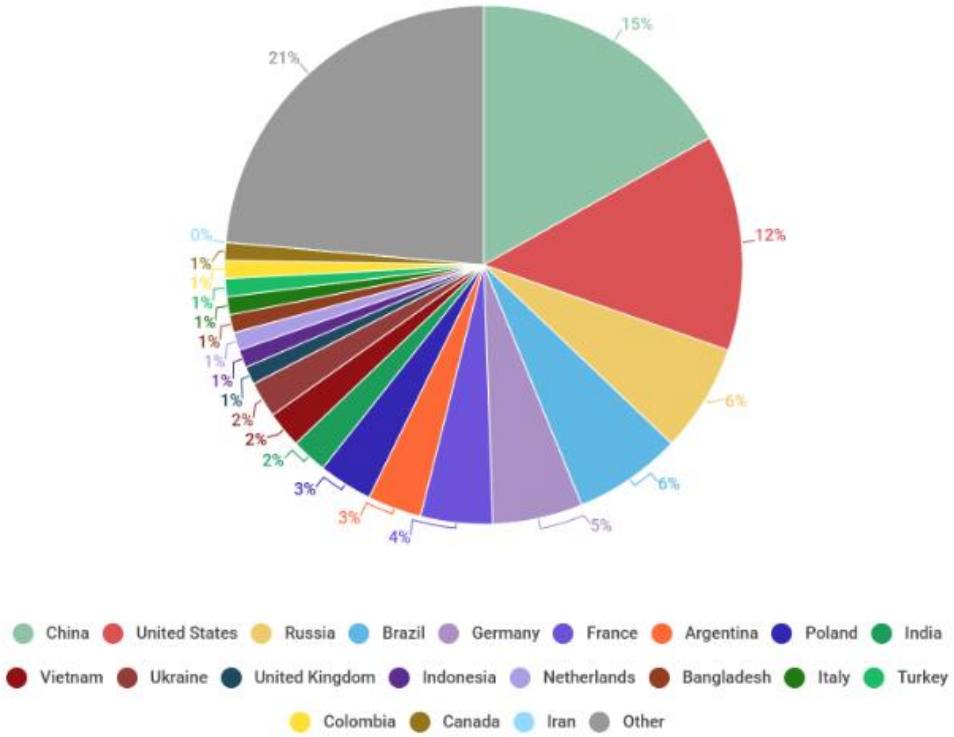


Hình 1.7 :Thống kê tấn công Email quý 3 năm 2018



Hình 1.8: Thống kê theo tên miền quý 3 năm 2018

Căn cứ thống kê tấn công Email quý 3 năm 2018 (hình 1.7) và thống kê theo tên miền quý 3 năm 2018 (hình 1.8) cho thấy tên miền .com phổ biến vẫn là đối tượng được nhắm đến nhiều nhất bởi các hacker, sau đó là tên miền .net với 5,99%. Ngoài ra còn có tên miền đặc trưng của các quốc gia như: .in (Ấn Độ), .ua (Australia), .id (Indonesia), .br(Brazil), .ru (Nga), .vn (Việt Nam), … Đây cũng là điều dễ hiểu bởi vì số lượng tên miền .com phổ biến và cao hơn rất nhiều so với các tên miền còn lại.



Hình 1.9: Tỷ lệ thư rác theo Quốc gia, Q1 2019

Dựa trên tỷ lệ thư ra theo Quốc gia Quý 1 năm 2019 (hình 1.9) trog đó tỷ lệ Spam Email, các quốc gia có nguồn gốc Spam Email hàng đầu là Trung Quốc (15,82%) và Hoa Kỳ (12,64%); Top 3 gồm Đức (5,86%), Nga (6,98%), Brazil (6,95%). Ở vị trí thứ 6 là Pháp (4,26%), Argentina (3,42%), Ba Lan (3,36%) và Ấn Độ (2,58%). Top 10 được làm tròn bởi Việt Nam (2,18%).

1.3.2 Tình hình tấn công Email tại Việt Nam

Năm 2018, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017 *(Kết quả được đưa ra từ chương trình đánh giá an ninh mạng do Bkav thực hiện tháng 12/2018)*.

Trên phạm vi toàn cầu, tội phạm mạng gây thiệt hại lên tới khoảng 600 tỷ USD mỗi năm, tương đương 0,8% GDP toàn cầu. Trong đó, khu vực Đông Á thiệt hại ước tính từ 120 – 200 tỷ USD, tương đương 0,53 – 0,89% GDP khu vực. Mức thiệt

hại 642 triệu USD tương đương 0,26% GDP của Việt Nam tuy chưa phải cao so với khu vực và thế giới, nhưng cũng là kỷ lục đáng báo động.

Hình 1.10: Email có chứa Malware

Theo thống kê, hơn 1,6 triệu lượt máy tính tại Việt Nam bị mất dữ liệu trong năm 2018. Bên cạnh đó, hơn 46% người sử dụng tham gia chương trình đánh giá an ninh mạng của Bkav cũng cho biết, họ đã từng gặp rắc rối liên quan tới mất dữ liệu trong năm qua.

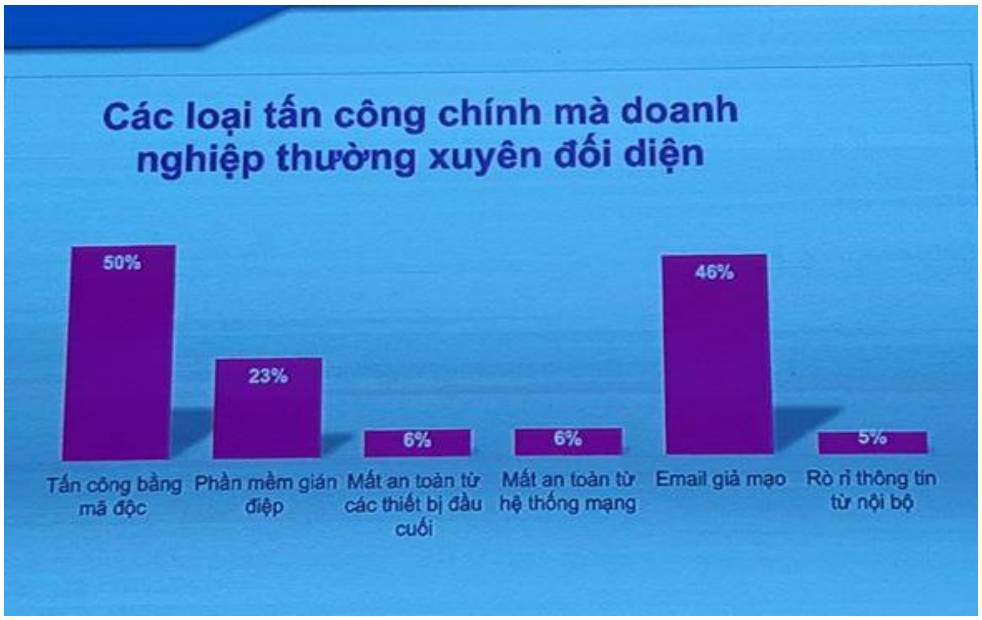
Hình 1.11: Email có chứa Ransomware

Hai dòng mã độc phổ biến tại Việt Nam khiến người dùng bị mất dữ liệu là dòng mã độc mã hóa tống tiền ransomware và dòng virus xóa dữ liệu trên USB. **Các mã độc mã hóa tống tiền lây chủ yếu qua Email**, tuy nhiên có tới 74% người dùng tại Việt Nam vẫn giữ thói quen mở trực tiếp file đính kèm từ Email mà không thực hiện mở trong môi trường cách ly an toàn, điều này rất nguy hiểm. Trong khi đó, do USB là phương tiện trao đổi dữ liệu phổ biến nhất tại Việt Nam nên số máy tính bị

nhiễm mã độc lây qua USB luôn ở mức cao. Thống kê của Bkav cho thấy, có tới 77% USB tại Việt Nam bị nhiễm mã độc ít nhất 1 lần trong năm.

Theo Cục An toàn thông tin (Bộ Thông tin - truyền thông), tính đến tháng 9-2019 đã ghi nhận 3.943 cuộc tấn công vào các hệ thống thông tin tại Việt Nam. 2.015.644 địa chỉ IP của Việt Nam nằm trong các mạng máy tính ma. So với cùng kỳ năm ngoái, tổng số sự cố tấn công tăng 104%.

Khảo sát 30 ngân hàng thương mại và thương mại cổ phần, 16 đơn vị cung cấp dịch vụ tài chính bảo hiểm tại Việt Nam từ tháng 5 - 7-2019 (hình 1.12) cho thấy ngân sách đầu tư an toàn thông tin còn ở mức thấp, chỉ chiếm khoảng 15% trở xuống trong tổng đầu tư về công nghệ thông tin của các đơn vị này.



Hình 1.12: Thống kê các loại tấn công Email vào doanh nghiệp

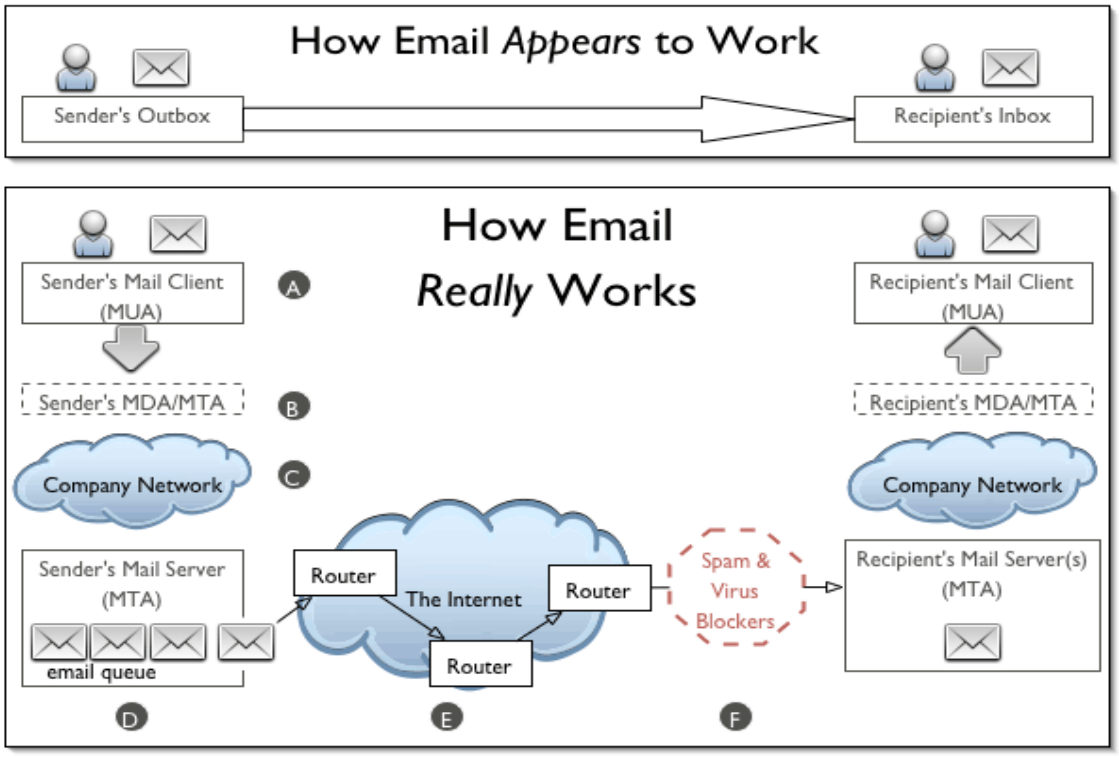
Tội phạm không gian mạng đã lợi dụng sự phổ biến của Email và biến Email thành hướng tấn công vào các doanh nghiệp, thâm nhập các mạng, cướp thiết bị và cướp tiền, dữ liệu nhạy cảm. File đính kèm Email đặc biệt được sử dụng để chèn các phần mềm độc hại vào một tổ chức nhằm tạo ra các cuộc tấn công mạng. Với các nhân viên doanh nghiệp phải làm việc với hàng trăm Email mỗi ngày thì việc trở thành nạn nhân của tấn công qua Email là điều khó tránh. Điều đó khiến các tổ chức, doanh nghiệp trên toàn thế giới luôn quan tâm đến việc chống các mối đe dọa, các cuộc tấn công qua Email. Tuy nhiên, bất chấp các công cụ và công nghệ như mã

hóa Email, sandbox và trí tuệ nhân tạo, tấn công qua Email vẫn rất phổ biến. Từ đó nhận thấy Email vẫn là hướng phổ biến để truyền tập tin độc hại trong nội bộ tổ chức, doanh nghiệp. Để tránh trở thành nạn nhân, các tổ chức cần phải hiểu cách thức hoạt động của các cuộc tấn công qua Email ngày nay và cách ngăn ngừa hoặc giảm thiểu sự cố.

CHƯƠNG II: CÁC PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG THƯ ĐIỆN TỬ

2.1. Các phương pháp phòng chống tấn công đối với Hệ thống Email.

Một hệ thống Email bao gồm những thành phần sau:



Hình 2.1: Những thành phần của hệ thống Email

Theo sơ đồ trên (hình 2.1) hệ thống Email bao gồm các thành phần sau: ứng dụng Mail Client, ứng dụng Mail Server, đường truyền Internet.

Vậy để bảo vệ một hệ thống Email hoàn chỉnh, các thành phần cần xây dựng các phương pháp để bảo vệ các hệ thống trên.

2.1.1 Các phương pháp bảo vệ đối với ứng dụng Mail Client

Bảo vệ ứng dụng Mail Client chính là bảo vệ người dùng tránh được các tấn công lừa đảo từ Email. Để thực hiện được điều đó, người dùng cần thực hiện các phương pháp sau:

Kiểm tra virus và phần mềm độc hại (viruses and malware): Sử dụng một phần mềm diệt virus uy tín; thường xuyên chạy quy trình quét bằng phần mềm diệt

virus đáng tin cậy. Nếu quá trình quét phát hiện bất kỳ chương trình hoặc ứng dụng đáng ngờ nào, hãy xem xét, cách ly và xóa khỏi hệ thống.

Chọn mật khẩu mạnh và không trùng với trang khác: Chọn mật khẩu gồm chữ cái, số và ký tự đặc biệt, ví dụ: Mail@2019$$ .Không nên đặt mật khẩu là ngày sinh hoặc số điện thoại, vì mật khẩu số rất dễ đoán và hacker có thể dò ra một cách dễ dàng. Thay đổi mật khẩu định kỳ vài tháng một lần để đảm bảo tính bảo mật.

Nên có ít nhất khoảng 2 tài khoản Email: Mỗi người nên có ít nhất khoảng 2 tài khoản Gmail:

Một tài khoản công khai, dùng cho các hoạt động trên Internet. Tài khoản này có thể được dùng để gửi Email với bạn bè, người thân, hay đăng ký các dịch vụ như Facebook, các diễn đàn, hoặc các trang mua sắm thông thường, v.v...

Một tài khoản dành cho trao đổi công việc hoặc đăng ký các dịch vụ quan trọng như ngân hàng điện tử và dùng làm tài khoản khôi phục cho tài khoản công khai.

Đăng ký xác minh 2 bước: Xác minh 2 bước là lớp bảo vệ bổ sung cho tài khoản Email. Điều này rất quan trọng nếu người dùng thường sử dụng hoặc đăng nhập Email của mình trên máy tính công cộng …

Chú ý Phishing lừa đảo: Phishing là là cách thức mà các Hacker chuyên nghiệp thường sử dụng nhằm mục đích lấy cắp các thông tin tài khoản như mật khẩu, tài khoản giao dịch trực tuyến... Nếu được một Email yêu cầu nhập thông tin tài khoản, do đó nên tránh xa những Email kiểu này vì có thể là Email lừa đảo nhằm lấy cắp các thông tin như: Số tài khoản ngân hàng; Số CMND; Số thẻ tín dụng; Ngày sinh của người dùng.

Xem xét các link đính kèm Email: Cách nhận biết những Email nguy hiểm chính là những Email đến từ những địa chỉ không xác định hoặc thường là những Email rác. Những Email này thường có nội dung quảng cáo và kèm theo những đường link yêu cầu phải click vào để đăng nhập. Tuy nhiên, Email có thể những đường dẫn này sẽ dẫn đến những Website có chứa mã độc, Virus và các phần mềm

độc hại... Ngoại trừ đó là Email uy tín đến từ các ngân hàng hoặc các dịch vụ đang sử dụng.

Không mở file đính kèm khi không xác định rõ người gửi: Nếu nhận được một Email từ một địa chỉ mà không quen biết chứa các file đính kèm, khi tải xuống những tập tin dạng đó, các mã độc hại sẽ lập tức lan truyền đến máy tính. Đây là những tập tin mà khi click vào sẽ tự động tải về hoặc một số file định dạng EXE nhưng được đặt dưới các định dạng ảnh phổ biến như JPG hay GIF...

Hạn chế kết nối WiFi công cộng: Kết nối WiFi tại các tụ điểm công cộng chẳng hạn như các quán Cafe và truy cập Internet mọi lúc, mọi nơi. Tuy nhiên, nếu chỉ lướt Web bình thường thì không sao nhưng nếu thường xuyên truy cập vào các tài khoản giao dịch trực tuyến thì có thể sẽ bị các phần mềm gián điệp " phát hiện" được các thông tin từ đó làm bàn đạp để tấn công hệ thống Email

2.1.2 Các phương pháp bảo vệ đối với hệ thống ứng dụng Mail Server

Để đảm bảo tính toàn vẹn, an toàn và xác thực đối với hệ thống ứng dụng Mail Server cần đáp ứng các yêu cầu sau:

2.1.2.1 Kiểm tra dữ liệu đầu vào (Input Data Validation)

- Phải xây dựng danh sách các dữ liệu đầu vào không hợp lệ;
- Phải kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, bảo đảm dữ liệu được nhập vào là chính xác và hợp lệ:
    - Phải kiểm tra dữ liệu đầu vào cả phía server và client để loại bỏ các ký tự nằm trong danh sách dữ liệu đầu vào không hợp lệ;
    - Phải kiểm tra tất cả dữ liệu đầu vào bao gồm: HTML form, REST call, HTTP header, cookie, batch file, RSS feed…;
    - Kiểm tra dữ liệu đầu vào: độ dài, kiểu dữ liệu, kiểm tra sự hợp lý của dữ liệu (ví dụ: zip code, post code…)
- Kiểm soát và xử lý dữ liệu đầu vào để chống lại các tấn công sau:
    - *SQL injection:* phải lọc dữ liệu người dùng- sử dụng filter để lọc các lý tự đặc biệt hoặc các từ khóa *(SELECT, UNION*). Ngoài ra kẻ tấn công

thường sử dụng các kỹ tự dưới đây để thực hiện tấn công *SQL injection*, do đó phải kiểm soát chặt chẽ:

- *Null byte (%00);*
- Các ký tự *new line* (%0d, %0a, \r, \n);
- Các ký tự *"dot-dot-slash"* như "…/" hoặc "…\"
- Nếu ứng dụng hỗ trợ UTF-8 (bảng mã Unicode), kiểm tra đầu vào là : "%c0%ae%c0%ae/".

- *LDAP Injection*: loại bỏ hoặc thay đổi các ký tự đặc biệt bằng cách sử dụng các biểu thức chính quy (regex) đã định nghĩa….;
- *OS Command Injection:* loại bỏ các ký tự đặc biệt phía Server: các chuyển hướng, điều kiện *OS command*….;
- *Remote File Inclusion* (RFI) và *Local File Inclusio*n (LFI): thiết lập quyền cho các thư mục hợp lý…..;
- XML *(XPath tampering, XML External Entity, XML Injection);*
- XSS (reflected, *stored, DOM base XSS*, *HTTP Header Injection*): escape các ký tự đặc biệt mà người dùng nhập vào thành các html entity (ví dụ: sử dụng hàm *htmlentities ()* trong PHP)…

- Các kết quả kiểm tra lỗi đầu vào phải được ghi nhật ký;
- Kiểm tra tính hợp lệ của dữ liệu cần được xử lý tự động trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin có chủ ý.

2.1.2.2 Xác thực và quản lý mật khẩu (Authentication and Password Management)

a. Xác thực

- Các thông tin xác thực sử dụng để truy cập hệ thống Email phải được mã hóa và lưu trữ an toàn;
- Phải xác thực người dùng khi có yêu cầu truy cập vào các tài nguyên, ngoại trừ xác tài nguyên công khai;

- Phải xác thực lại người dùng trước khi cho phép thực hiện các hành vi quan trọng (ví dụ: xuất báo cáo, xóa báo cáo…);
- Sử dụng xác thực đa nhân tố khi đăng nhập vào hệ thống (ví dụ: kết hợp xác thực tài khoản/ mật khẩu với OTP….) nhằm tăng cường bảo mật;
- Nếu sử dụng nhân tố xác thực của bên thứ ba, phải có biện pháp rà soát mã độc trước khi sử dụng (ví dụ: Token bên thứ ba cung cấp…);
- Ứng dụng mặc định khóa tài khoản x phút sau y lần đăng nhập sai, người dùng muốn mở khóa tài khoản trở lại cần thông báo cho bộ phận chịu trách nhiệm liên quan. Tham số thời gian cụ thể sẽ được thiết lập phù hợp với yêu cầu sử dụng thực tế của từng ứng dụng;
- Đối với một số ứng dụng mà tài khoản người dùng không thể bị xóa vì lý do toàn vẹn dữ liệu thì ứng dụng phải có tính năng để khóa tài khoản (Disable/ Inactive);
- Các thủ tục xác thực phải mặc định là fail securely, tức là mặc định trả về false nếu có bất kỳ ngoại lệ nào xảy ra trong quá trình xử lý, để đảm bảo kẻ tấn công không thể truy cập được;
- Thời gian phản hồi cho các xác thực thành công hay thất bại là như nhau, để tránh việc kẻ tấn công có thể chèn các palyload theo điều kiện đúng/ sai vào các form đăng nhập và dựa vào thời gian phản hồi của ứng dụng để từ đó có thể suy đoán các thông tin nhảy cảm (ví dụ: tấn công Blind SQL Injection).

b. Mật khẩu

- Mật khẩu truy cập ứng dụng phải đáp ứng yêu cầu chung về độ dài và mức độ phức tạp như sau:
  - Có độ dài tối thiểu 8 ký tự
  - Bao gồm 03 trong 04 loại ký tự: Chữ thường, chữ hoa, số, ký tự đặc biệt;
  - Mật khẩu phải được thay đổi định kỳ theo quy định của tổ chức (vd 90 ngày/ lần);
  - Mật khẩu phải được đổi ngay khi tài khoản sử dụng lần đầu, cấp mới;
- Ứng dụng cần đáp ứng yêu cầu thiết kế, quản lý mật khẩu an toàn:

- Phải có chức năng quản trị, thiết lập độ phức tạp của mật khẩu;
- Phải có công cụ ghi lại được quá trình, trạng thái đăng nhập (như số lần đăng nhập sai, số lần đăng nhập thành công, địa chỉ truy cập ứng dụng…) trong thời gian ít nhất 01 tháng;
- Tạo tài khoản cho người dùng với mật khẩu ngẫu nhiên đáp ứng các yêu cầu về độ phức tạp mật khẩu được nêu;
- Hệ thống có tính năng nhắc người sử dụng đổi mật khẩu sau khi cấp mới lần đầu tiên và trước khi hết hạn, đồng thời kiểm tra độ phức tạp của mật khẩu theo yêu cầu của mật khẩu;
- Chức năng thay đổi mật khẩu bắt buộc phải bao gồm: yêu cầu nhập mật khẩu hiện tại , nhập mật khẩu mới, nhập lại mật khẩu mới;
- Ứng dụng phải có tính năng thông báo đến người dùng khi có bất kỳ yêu cầu reset mật khẩu tài khoản của họ (qua SMS, Email…);
- Nếu sử dụng reset mật khẩu qua Email, thì gửi một liên kết/ mật khẩu tạm tới địa chỉ Email đã đăng kí trước đó. Liên kết / mật khẩu tạm là duy nhất và chỉ có hiệu lực tỏng khoảng thời gian xác định. Tham số thời gian hiệu lực sẽ được thiết lập phù hợp với yêu cầu sử dụng của từng hệ thống ứng dụng;
- Mật khẩu phải được băm với một giá trị Salt ngẫu nhiên, nhằm chống lai các cuộc tấn công dạng Brute-force và Dictionary Attack;
- Vô hiệu hóa chức năng ghi nhớ mật khẩu của trường mật khẩu và tính năng auto fill vào các trường khác của ứng dụng (Ví dụ: thiết lập autofill vào các trường khác của ứng dụng (Ví dụ: thiết lập autocomplete = “off” trong các input tag);
- Thông báo lỗi không được đưa ra chi tiết phần nào của xác thực là không chính xác. Không hiển thị dạng: *“Invalid password/ Mật khẩu không đúng” hoặc “Invalid ID/ Tài khoản không đúng”,* mà phải hiển thị chung như *“Invalid ID or password/ Tài khoản hoặc mật khẩu không đúng”*.

2.1.2.3 Ủy quyền (Authorization)

- Đảm bảo người dùng chỉ được phép truy cập vào các tài nguyên được ủy quyền. Quy tắc này giúp chống lại các tấn côn Spoofing và leo thang đặc quyền;
- Vô hiệu hóa chức năng Directory Browsing;
- Chỉ người dùng có đặc quyền có thể truy cập được vào giao diện quản trị (Admin Panel);
- Không cho phép người dùng (trừ những người dùng có đặc quyền) tác động (sửa, xóa…) đến các dữ liệu của kiểm soát truy cập (người dùng, nhóm người dùng, chính sách….);
- Sử dụng "referer" header với mục đích kiểm tra bổ sung, không sử dụng duy nhất nó để kiểm tra ủy quyền vì có thể bị giả mạo;
- Giới hạn số lượng giao dịch mà mõi người dùng hoặc thiết bị có thể thực hiện trong một khoảng thời gian nhất định;
- Tất cả các truy cập, bất kể thành công hay thất bại đều phải ghi log.

2.1.2.4 Bảo vệ dữ liệu nhạy cảm (Sensitive Data Protection)

- Các dữ liệu nhạy cảm (ví dụ: thông tin định danh, thông tin số điện thoại, địa chỉ,…) không được truyền trong mạng dưới dạng nguyên thủy(Plain Text) không được mã hóa;
- Không lưu trữ các dữ liệu nhạy cảm trên các kho lưu trữ phía client (ví dụ: *HTML5, localStorage, IndexedDB, regular, sessionStorage, cookies hoặc Flash cookies*). Nếu việc lưu thông tin trong các kho lưu trữ trên là cần thiết do yêu cầu đặc thù ứng dụng thì thông tin phải được mã hóa;
- Sử dụng cơ chế *HTTP Expires* cho các ứng dụng nền tảng Web để tránh việc các trang Web bị catching lại dữ liệu nhạy cảm;
- Không sử dụng URL để truyền đi các dữ liệu nhạy cảm. các dữ liệu nhạy cảm phải được gửi đi dưới các thông điệp *HTTP body* hoặc *HTTP header*.

2.1.2.5 Quản lý phiên làm việc (Session Management)

- Session ID phải được tạo ra trên một hệ thống tin cậy, không lưu trữ ở phóa Client trong mô hình Client- server và phải được mã hóa trong quá trình truyền gửi trong hệ thống mạng;
- Session ID phải đủ dài tối thiểu là 1 chuỗi 40 ký tự, ngẫu nhiên và duy nhất cho mỗi phiên;
- Mỗi tài khoản chỉ được phép có một phiên kết nối tại một thời điểm. Đồng thời, mỗi lần xác thực đều phỉa sinh ra một session mới và một session ID mới;
- Khi kết nối HTTP được chuyển sang HTTPS, phải áp dụng một session ID mới. Nên sử dụng HTTPS thay vì điều hướng từ HTTP sang HTTPS;
- Khi mật khẩu được thay đổi, các phiên trước đó phải được chấm dứt;
- Phải tự động ngắn phiên làm việc sau một khoảng thời gian nhất định người dùng không sử dụng. Tham số khoảng thời gian cụ thể sẽ được thiết lập phụ thuộc vào yêu cầu sử dụng thực tế của từng ứng dụng;
- Các trang/ chức năng yêu cầu người dùng xác thực đều phải có chức năng đăng xuất để chấm dứt phiên và các kết nối liên quan;
- Bổ sung Token ngẫu nhiên đối với mỗi phiên để tấn công Cross Site Request Forgery (CSRF);
- Thiết lập tham số “Secure” và “HttpOnly” cho Cookie nhằm chống tấn công XSS.

2.1.2.6 Mã hóa (Cryptographic Practices)

- Mã hóa dữ liệu phải được thực hiện trên hệ thống tin cậy (Ví dụ: trong mô hình Client- Server, thủ tục mã hóa phải được thực hiện ở phía Server);
- Khóa mã hóa phải đáp ứng các yêu cầu sau:
    - Có độ dài tối thiểu 256 bit;
    - Là chuỗi ký tự bao gồm chữ, số, ký tự đặc biệt;

- Một khóa mới phải được khởi tạo cho mỗi phiên, các giá trị ngẫu nhiên phải được tạo ra bằng cách sử dụng bộ sinh số ngẫu nhiên soa cho kẻ tấn công không thể đoạn được giá trị này.

- Tất cả module mã hóa phải mặc định là *fail securely*, tức là sẽ mặc định trả về *false* nếu có một ngoại lệ xảy ra trong quá trình xử lý;
- Sử dụng các thuật toán mã hóa dữ liệu mạng với độ dài lớn (ví dụ: *AES 256, RSA 4096, 3DES*). Không sử dụng các thuật toán mã hóa cũ, không còn an toàn (ví dụ : *DES, RC4, RC5*);
- Sử dụng các hàm băm mật mã mạnh với độ dài khóa lớn (ví dụ: *SHA-256 trở lên, RIPEMD*). Không sử dụng các hàm băm cũ, không còn an toàn (ví dụ: *MD4, MD5, SHA-0, SHA-1*).

2.1.2.7 Kiểm soát và ghi log (Auditing and Logging)

- Log, URL, thông báo lỗi, hướng dẫn khắc phục lỗi không chưa thông tin nhạy cảm như *session ID, API key*, mật khẩu, phiên bản phần mềm….;
- Nhật ký an ninh thông tin (Security Logs) phải bao gồm các thông tin sau:
  - Đăng nhập/ Đăng xuất ứng dụng thành công/ thất bại;
  - Cố gắng đăng nhập ứng dụng ngoài khoảng thời gian làm việc đã được định nghĩa sẵn;
  - Truy cập vào tài nguyên quan trọng; các tệp tin lưu trữ dữ liệu nhạy cảm, thư mục hoặc các tài nguyên khác
  - Các hoạt động tạo, xóa, sửa đổi dữ liệu nhạy cảm;
  - Truy cập trái phép các tập tin, thư mục hoặc các tài nguyên khác;
  - Lỗi của bất kỳ dịch vụ, ứng dụng quan trọng nào.
- Nhật ký hoạt động tài khoản quản trị (User Admin Logs) phải bao gồm các thông tin khởi tạo, xóa, đổi tên, sửa đổi quyền truy cập và thay đổi mức độ mật khẩu cho hồ sơ người dùng (User Profile);
- Nhật ký hoạt động sử dụng để điều tra (Audit log) phải bao gồm tối thiểu các thông tin sau:
  - Transaction ID- Mã giao dịch;

- User ID- Mã người dùng;
- Nội dung các trường dữ liệu trước và sau khi xảy ra sự kiện;
- Hành động xảy ra
- Thời gian xảy ra sự kiện
- Địa chỉ IP

- Hệ thống ghi nhật ký và thông tin nhật ký phải được bảo vệ nhằm chống giả mạo và truy cập trái phép;
- Phải thực hiện sao lưu log để kiểm tra tính toàn vẹn của log. Thiết lập chi cho phép tài khoản có quyền cấu hình ứng dụng được phép xóa log, nhằm bảo vệ log khỏi việc truy cập và chỉnh sửa trái phép;
- Các ký tự *non-printable* (Null, SUB…) và các ký tự *field separators* (,;:*TAB Space) trong log phải được mã hóa để tránh tấn công Log Injection:
- Log phải được lưu trữ ở một phân vùng khác so với phân vùng ứng dụng.

2.1.2.8 Quản lý tập tin và tài nguyên (File and Resource Management)

- Giới hạn các loại tập dữ liệu tải lên, chỉ cho phép tải lên một số loại tên tin xác định và phải scan malware các tệp người dùng tải lên;
- Đảm bảo chỉ có người dùng đã được xác định và cấp quyền mới được upload tập tin;
- Không tải tập tin lên ứng dụng trực tiếp qua các I/O command để tránh các loại tấn công *Path traversal, Local file inclusion, Reflective file download, OS command injection*…;
- Không sử dụng các dữ liệu lấy từ nguồn không tin cậy trong *inclusion, class loader* hoặc *reflection* để ngăn các lỗ hổng *Remote/ Local code execution;*
- Không sử dụng các dữ liệu lấy từ nguồn không tin cậy trong *Cross-domain resource sharing (CORS)* để bảo vệ chống lại tấn công *Arbitrary code execution;*
- Các tập tin và thư mục từ nguồn không đáng tin cậy phải được lưu trữ bên ngoài *Webroot*; thiết lập đặc quyền tối thiểu cho các tập tin và thư mục đó;

- Phải phân cấp tập tin và thư mục, đảm bảo ứng dụng không thể truy cập lên các tài nguyên phía trên, ngăn chặn tấn công *leo thang đặc quyền*;
- Hạn chế các công nghệ, kỹ thuật không còn được hỗ trợ *như plugin NSAPI, Flash, Shokware, Active-X, Silverlinght, NACL, client-side Java applets,..;*
- Kiểm tra bộ đệm để đảm bảo không ghi quá không gian bộ nhớ được phân bổ;
- Khi sử dụng các hàm soa chép như *strncpy(),* kích thước bộ đệm đích phải lớn hơn kích thước bộ đệm nguồn không bị thiếu kí tư *NULL* (ký tự kết thúc string);
- Không sử dụng các hàm chứa lỗ hổng như *printf, stcat, strcpy,..*

2.1.2.9 Cấu hình hệ thống đảm bảo an toàn (Systerm Configuraiton)

- Luôn cập nhật các bản vá cập nhật, bản vá bảo mật. Loại bỏ các file không cần thiết, đặc biệt là test code, các tính năng chỉ dùng trong quá trình phát triển;
- Dữ liệu truyền gửi giữa các thành phần của ứng dụng phải đươc mã hóa, đặc biệt là dữ liệu truyền gửi giữa máy chủ ứng dụng và máy chủ cơ sở dữ liệu hoặc giữa các hệ thống khác nhau. Các dữ liệu này chỉ được gửi nhận bằng tài khoản đã được xác thực, với quyền truy cập tối thiểu phục vụ mục đích gửi nhận dữ liệu;
- Sao lưu file cấu hình nhằm kiểm tra tính toàn vẹn của file. Thiết lập *"read only"* cho file cấu hình và chỉ cho phép tài khoản có đặc quyền truy cập, chỉnh sửa;
- Xác định phương thức truy vấn HTTP mà ứng dụng *(GET, POST…)* và chặn các phương thức không sử dụng *(HEAD, PUT, DELETE…).* Quy tắc này giúp chống lại tấn công *HTTP verb tampering*.

2.1.2.10 An ninh cho các ứng dụng Email trên di động

- Đối với ứng dụng Email trên di động khuyến nghị sử dụng chứng thư số tin cậy;
- Dữ liệu được truyền đi trên đường truyền phải được mã hóa an toàn;

- Ứng dụng không lưu các dữ liệu nhạy cảm lên các tài nguyên chia sẻ như thẻ nhớ, thư mục dùng chung… mà không có cơ chế bảo vệ (ví dụ: không mã hóa);
- Phải kiểm soát các đặc quyền mà ứng dụng Email yêu cầu được cấp phép sử dụng trên thiết bị;
- Các mã code nhạy cảm phải được đặt ở nơi không thể đoán trước trong bộ nhớ (ví dụ: *ASLR*);
- Sử dụng các kỹ thuật/ công nghệ *anti-debug* ngăn chặn việc kẻ tấn công *inject các debugger* vào ứng dụng (ví dụ: làm rối code, mã hóa code…)
- Các dữ liệu nhạy cảm trong bộ nhớ sau một thời gian dài không sử dụng phải được ghi đề *zero*, để tránh tấn công *dump attack.*

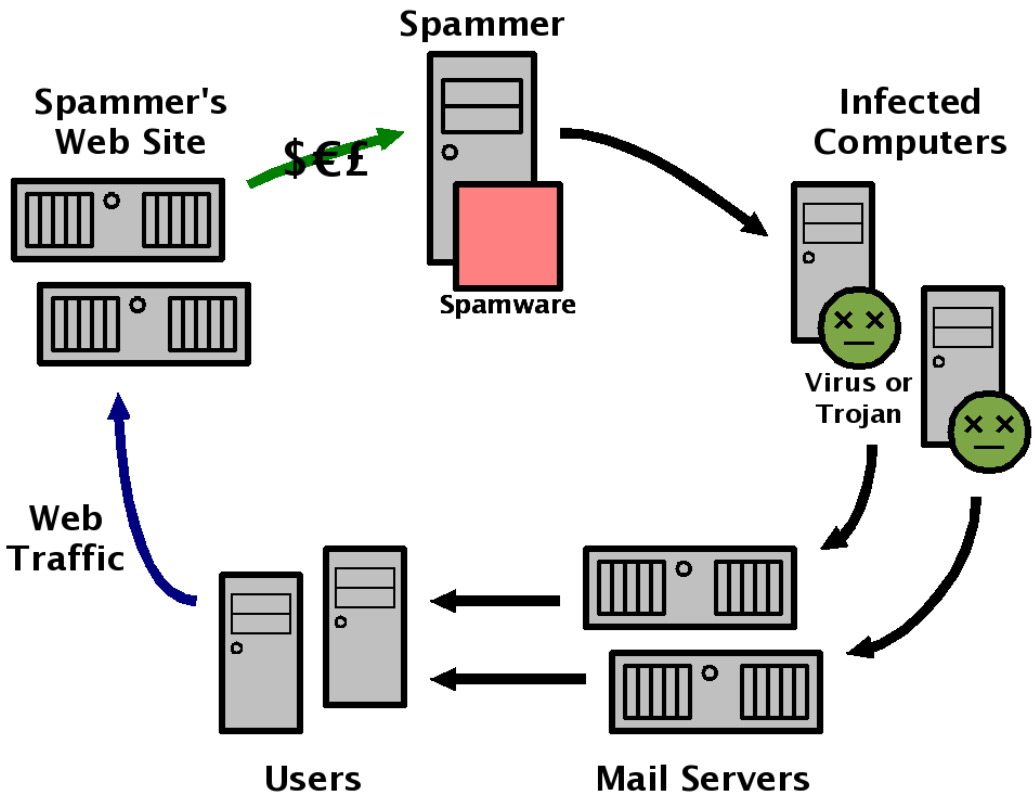
2.1.3 Bảo vệ đường truyền, kết nối (Communication Security)

- Đối với cá ứng dụng Web phải sử dụng chứng thư số. Đối với các ứng dụng khác, khuyến nghị sử dụng chứng thư số tin cậy, ngoài ra dữ liệu được truyền trên đường truyền phải được mã hóa an toàn;
- Sử dụng TLS cho tất cả kết nối để đảm bảo dữ liệu được mã hóa trên đường truyền. Tất cả các lỗi kết nối TLS phải được ghi log để phục vụ cho quá trình điều tra sau này;
- Các kết nối TLS phải được cấu hình đảm bảo an toàn an ninh thông tin: sử dụng bộ giao thức (sử dụng *TLS 1.2*, không sử dụng *SSL2, SSL3*), bộ mật mã mạnh tương ứng (*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 256bit, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256 128bit*….) có khả năng chống lại các tấn công giao thức: *SSLtrip, Heartbleed, Ticketbleed, OpenSSL Padding Oracle (CVE-2016-2107), OpenSSL CCS (CVE-2014-0224),…;*
- Chứng thư số được tạo ra phải đảm bảo an toàn cho các giao dịch trên mạng (cung cấp dịch vụ xác thực, bảo mật, toàn vẹn và chống chối bỏ); được chứng thực với CA tin cậy *(DigiCert Inc, Let's Encrypt*…), thuật toán ký số an toàn, hỗ trợ *HPKP, HSTS, Perfect Forward Secrecy, OCSP stapling*… có khả năng chống lại các tấn công phổ biến: *M1TM, Replay attack, SSLStrip*….;

- Cấu hình ứng dụng sử dụng *HPKP (HTTP public key Pinning)* để chống lại các tấn công M1TM sử dụng chứng thư số giả mạo;
- Cấu hình ứng dụng sử dụng *HSTS* giúp đảm bảo rằng kết nối luôn được thực hiện thống qua HTTPS, chống lại tấn công *downgrade attack* (ví dụ: thiết lập *HSTS* header là Strict-Transport- Security; max-age=6307200; includeSubDomain);
- Thiết lập *OCSP Stapling*; OCSP giúp xác định tính hợp lệ của chứng thư số thời gian thực thay vì phải yêu cầu thông tin từ nhà cung cấp chứng thư.

2.2. Các phương pháp điển hình phòng chống tấn công AntiSpam Email

2.2.1 Cơ chế hoạt động của Spam Email



Hình 2.2: Cơ chế hoạt động của Spam Email

Quá trình thực hiện của một Spammer như sau:

Bước 1: Spammer's web site trả tiền cho các người phán tán Spammer

Bước 2: Spammer gửi spam với các đường dẫn, virus đến các máy tính thông qua đường truyền Internet

Bước 3: Các Email spam được gửi đến Mail Servers của cá nhân hoặc tổ chức.

Bước 4: Các Email Spam được gửi từ Mail Server gửi đến mail của các cá nhân

Bước 5: sau khi các các nhân nhận được Mail Spam để nhập các thông tin cá nhân, khi đó các thông tin sẽ được gửi về Spammer's Website.

2.2.2 Các phương pháp lọc Spam Email

Vấn đề thư rác là vấn đề gây nhức nhối trong xã hội trong những năm gần đây. Nhiều nhà khoa học và nhiều công trình nghiên cứu về phương pháp lọc thư rác đã được đầu tư và tiến hành từ khá lâu.Để đánh giá hiệu quả của một công cụ lọc thư rác người ta thường dựa trên hai độ đo sau:

- False Positive – Tỷ lệ thư thường bị lọc nhầm thành thư rác.
- False Negative – Tỷ lệ thư rác bị lọc nhầm thành thư thường.

Trong hai lỗi trên thì lỗi False Positive là loại lỗi cần tránh nhất, người dùng thường không chấp nhận lỗi này. Các công cụ lọc thư rác thường được tính toán sao cho độ đo False Positives và False Negatives là nhỏ nhất. Tuy nhiên, lỗi False Positives có phần được yêu tiên hơn. Một bộ lọc lý tưởng là sản phẩn có False Positives bằng 0 và False Negatives bằng 0. Điều này dường như là không thể.

Tất cả những công cụ lọc có giá trị ngày nay thường sử dụng một trong số những phương pháp hoặc kết hợp của các phương pháp sau:

2.2.2.1 Phương pháp lọc theo từ khóa

Phương pháp lọc thư rác theo từ khóa là một phương pháp truyền thống trong việc lọc thư rác. Người ta dựa vào những từ hay cụm từ có trong đầu đề của thư (subject) và nội dung của thư để lọc.

Khi một thư mới được gửi tới hòm thư của bạn, bạn phải tạo một bộ lọc mới đơn giản bằng cách chọn một số từ hoặc cụm từ trong nội dung thư. Các từ hay cụm từ này sẽ xác định đó là thư rác hay không. Vì mục đích của tất cả spam cơ bản là giống nhau (bán hoặc quảng cáo một sản phẩm hay một dịch vụ) và nội dung của hầu hết spam đều mang các đặc điểm chung. Những cụm từ, câu chữ như *"Silk ties"* (Cà vạt lụa) hoặc *"Eliminate debt"* (Xoá nợ) xuất hiện thường xuyên trên spam và được coi những cụm từ thường xuyên xuất hiện nhất trong các bức thư

không mong muốn. Các đặc điểm nội dung khác để nhận diện spam như yêu cầu hành động như "*Fin out how, click here*" hoặc thông báo huỷ như *"If you want to be removed from our mailing lists,…"*

Một vài năm gần đây, những kẻ gửi thư rác đã bắt đầu nhận ra rằng thư rác của chúng đã bị chặn bởi bộ lọc theo từ khóa này. Do vậy những kẻ gửi thư rác này đã thay đổi cách viết nội dung của thư rác nhằm làm cho thư rác của chúng có thể "xuyên qua" các bộ lọc. Điều này có thể giải thích tại sao bạn nhận nhiều thư với những từ như *"Vi@gra", "Mort.gage", "L|0|a|n|$"* hay những tranh ảnh được nhúng vào trong thư.

Phương pháp này có một số ưu điểm và nhược điểm sau:

Ưu điểm:

Tính thích nghi: Người dùng có thể dễ dàng biến đổi bộ lọc của mình để nó có thể lọc các kiểu thư rác mà người đó đang phải nhận và điều quan trọng là nó không cản trở (thích nghi) các từ và các cụm từ được sử dụng hàng ngày trong kinh doanh thương mại với bạn bè hay những người thân quen.

Nhược điểm:

Yêu cầu nhiều tiến trình xử lý bằng tay để điều chỉnh và duy trì bộ lọc được hiệu quả. Để có thể đánh lừa các bộ lọc, những kẻ gửi thư rác luôn luôn thay đổi hình thức nội dung của thư rác, do đó những bộ lọc mở rộng phải được tạo ra để chống lại điều đó.

2.2.2.2 Phương pháp lọc Bayesian

Lọc bằng thống kê Bayesian là đánh giá xem những từ ngữ trong một Email lắp được chuyển đến có thường xuyên xuất hiện trên thư rác (spam) hay thư hợp pháp (ham) không. Một cách hiệu quả giúp lọc chính xác là người dùng thông báo cho chương trình lọc bất kỳ thư rác nào mà đã may mắn "thoát" đợt "truy quét" đầu tiên.Lần lọc sau, chắc chắn nó sẽ không thể trốn thoát qua bộ lọc.

Bộ lọc Bayesian phải được học từ những Email được xác định trước là thư tốt hay thư không tốt. Trong suốt quá trình cho bộ lọc học, nội dung của các thư này

được tách các từ tố (token) và lưu vào trong một cơ sở dữ liệu. Dựa vào công thức Bayes,mỗi từ tố được tính cho một giá trị phụ thuộc vào một số tiêu chuẩn sau:

- Mức độ thường xuyên xuất hiện của từ tố đó trong thư rác
- Mức độ thường xuyên xuất hiện của từ tố đó trong thư bình thường
- Số lượng thư rác mà bộ lọc đã được học
- Số lượng thư bình thường bộ lọc đã được học.

Khi phân tích một thư rác đến, nội dung của thư này cũng được tách ra thành các từ tố, tra giá trị ứng với từ tố này có trong cơ sở dữ liệu từ đó tính được xác suất tổng hợp xem thư đó có phải là thư rác không. Giá trị này thường gọi là *"spamicity"*

Ưu điểm:

Yêu cầu sự duy trì ít hơn các bộ lọc khác.

Bộ lọc có thể tự động thích nghi với các hướng thay đổi của thư rác. Bởi vì, bộ lọc Bayesian luôn tiếp tục học từ những thư mới đến, chúng sẽ tự thích nghi dần dần với các hướng thay đổi.

Tự động điều chỉnh phù hợp với hòm thư của những người dùng riêng biệt. Thí dụ, nếu người dùng là nhân viên cho vay lãi thì những thư lặp đi lặp lại yêu cầu cho vay sẽ không bị xác định như là thư rác.

Nhược điểm:

Bộ lọc chỉ lọc tốt đối với những kiểu thư mà chúng đã được học. Để có thể đạt tới khả năng là một bộ lọc tốt, nó cần có thời gian học khá lâu và một lượng dữ liệu thư đủ phong phú. Các thư rác mới phải thường xuyên được cập nhật.

2.2.2.3 Phương pháp lọc SpamAssassin

Phương pháp lọc SpamAssassin bao gồm một tập các chương trình lọc và các luật để xác định và đánh dấu thư rác.

Để xác định một thư mới đến có phải là thư rác hay không, nó dùng đầu đề (header) và nội dung của thư rồi dựa trên tập các luật được xác định trước và những kí hiệu dấu câu đặc biệt (tell-tale), xem thư có vi phạm các luật này không sau đó

tính điểm đối với từng thư.Từ kết quả thu được, xác định được một thư là thư rác hay thư thường.

Ưu điểm:

Tỉ lệ lọc thư rác của phương pháp SpamAssassin rất cao

Nhược điểm:

Phương pháp SpamAssassin tiêu tốn khá nhiều tài nguyên (khối điều khiển trung tâm CPU, bộ nhớ, thời gian xử lý) của máy chủ, đặc biệt khi phải xử lý những Email có dung lượng lớn. Cấu hình để SpamAssassin hoạt động tốt, đồng thời giảm nhẹ sự tiêu tốn tài nguyên cho máy chủ là một vấn đề quan trọng.

2.2.2.4 Phương pháp dùng danh sách trắng/đen

Đây là phương pháp cơ sở của các bộ lọc thư rác. Tuy nhiên, ngày nay người ta ít khi sử dụng nó một cách đơn lập mà được dùng kết hợp với các phương pháp lọc khác như là một phần của hệ thống bộ lọc tích hợp.

Bộ lọc danh sách trắng (*Whitelist filter*) sẽ không chấp nhận những Email từ bất cứ địa chỉ nào nếu không có trong danh sách được chắc chắn là những địa chỉ Email (hoặc địa chỉ IP) tốt.

Bộ lọc danh sách đen (Blacklist filter), ngược lại sẽ cho phép những thư đến từ bất cứ địa chỉ Email (hoặc địa chỉ IP) nào trừ những địa chỉ được liệt kê trong danh sách được biết đến như là địa chỉ Email (hoặc địa chỉ IP) xấu. Danh sách đen có thể được lưu trữ và được quản lý trên những hệ thống địa phương hoặc ánh xạ thông qua mạng Internet.

Ưu điểm:

Danh sách trắng bảo đảm ngăn những Email từ những nguồn không mong muốn.

Với bộ lọc thư rác sử dụng danh sách đen được cập nhật thường xuyên sẽ cho giá trị False Positives bằng 0.

Nhược điểm:

Bộ lọc sử dụng danh sách trắng là cách loại trừ thư rác mạnh mà không có tính mềm mỏng. Bất cứ thư nào tới mà không có địa chỉ trong danh sách này thì đều bị loại thành thư rác, do đó giá trị False Positives thường cao.

Các danh sách này không được tạo tự động mà sẽ do người quản trị thường xuyên cập nhật. Cả Blacklist và Whitelist đều rất khó duy trì và phương pháp này đặc biệt trở lên không hiệu quả đối với những tấn công của những kẻ tấn công cố đưa địa chỉ vào Whitelist và chối bỏ địa chỉ khỏi Blacklist.

Ngày nay, một hình thức ngăn chặn spam mới kế thừa và pháp trển của phương pháp Blacklist được biết đến đó là Realtime Blackhole List (RBL) của Multiple Address Processing System (MAPS). Nó có thể nhận biết các máy chủ có nhiều thư rác do đó nhà cung cấp dịch vụ có thể chặn những máy chủ này và lọc spam trước khi chúng đến hộp thư khách hàng của họ. Hàng ngàn nhà cung cấp dịch vụ dùng cơ sở dữ liệu của RBL đồng thời kết hợp nhiều ứng dụng bảo mật thư điện tử trong máy chủ.

2.2.2.5 Phương pháp lọc thư rác dùng chuỗi hỏi đáp

Đặc trưng của phương pháp này là khả năng tự động gửi thư hồi đáp cho người gửi để yêu cầu một số hành động kiểm tra chắc chắn về việc gửi thư của họ.Chương trình kiểm tra này được đặt tên là *"Turing Test"* do nhà toán học người anh tên là Alan Turing nghĩ ra

Trong một vài năm gần đây xuất hiện của một vài dịch vụ Internet tự động xử lý hàm Challenge/Response này cho người dùng. Chương trình yêu cầu người gửi thư phải vào website của họ và trả lời một số câu hỏi đơn giản để xác minh về Email mà người này đã gửi.Việc này chỉ được yêu cầu trong lần gửi thư đầu tiên. Đáp ứng hàm Challenge/Response này rất đơn giản và không có gì khó khăn khi một người dùng muốn gửi thư cho một người khác nhưng nó không mấy dễ dàng cho những kẻ gửi thư rác muốn phát tán một lượng lớn thư rác đi.

Ưu điểm:

Đối với một số người dùng có lượng thư trao đổi thấp, hệ thống đơn lẻ này có thể chấp nhận được như một phương pháp hoàn hảo để loại trừ hoàn toàn thư rác từ hòm thư của họ.

Nhược điểm:

Người dùng thường cảm thấy không thuận tiện. Những kẻ gửi thư rác có thể viết những chương trình trả lời tự động những chuỗi hỏi đáp trên.

2.2.2.6 Phương pháp lọc dựa vào vị trí của các bộ lọc

Có 3 mô hình chính cho bộ lọc được sắp đặt:

a. Bộ lọc tích hợp với máy trạm Email của người dùng:

Nhiều bộ lọc thư rác được tích hợp với các máy trạm Email chẳng hạn như Outlook hoặc outlool Exprees.

Ưu điểm:

Tối thiểu sự ảnh hưởng đối với những thói quen đọc thư thông thường của người dùng. Thư rác thường bị di chuyển tới một thư mục "Junk Mail". Người dùng có thể xem lại hoặc xóa spam lưu trong thư mục này đi một cách dễ dàng.

Nhược điểm:

Người dùng chỉ có thể sử dụng với máy trạm của Email hiện tại của mình.

Không mềm dẻo: thường đưa cho người dùng giới hạn để chọn những cảnh báo. Thí dụ, khi người dùng đang chạy Microsoft Outlook với một bộ lọc thư rác tích hợp, bất cứ khi nào một thư rác tới, người dùng vẫn bị cảnh bảo một thư mới tới. Người dùng phải vào chương trình Outlook để xác nhận xem thư mới đến đó là thư rác và không phải là một Email quan trọng. Người dùng không thể điều chỉnh để tạo một cảnh báo khác có thể nghe thấy giữa những Email tốt và xấu hoặc chỉ cảnh báo những Email tốt khi những Email được gửi tới hòm thư trước khi chúng hoạt đông chống lại bởi bộ lọc và di chuyển tới một thư mục riêng biệt.

Các bộ lọc hoạt động như là một "proxy" giữa máy chủ Email và máy trạm Email của người dùng

Bộ lọc này chạy bên trong máy của người dùng, định kì thăm dò máy chủ Email, lấy ra những Email của người dùng và nó được lọc trên máy chủ Email trước khi những Email này được gửi tới máy trạm Email bình thường của người dùng và được lọc một lần nữa.

Ưu điểm:

Dễ thay đổi: Các thư trước khi được gửi tới người dùng nó có thể đánh dấu, di chuyển hoặc xóa bởi máy chủ Email trước khi chúng được nhìn thấy bởi máy trạm Email của người dùng.

Bảo mật: chúng tương ứng như một tầng khác ở giữa Internet và máy trạm Email của người dùng. Chúng sẽ không chạy bất cứ một ứng dụng nào hay chạy một tập lệnh nào đó được tìm thấy trong thư.

Nhược điểm:

Sử dụng hiệu quả phương pháp này đòi hỏi tắt chế độ tự động kiểm tra trên máy trạn Email của người dùng vì thế proxy phải thay đổi để làm việc trên máy chủ đầu tiên.

Thông tin tài khoản Email cần được cài đặt trong bộ lọc cũng như trong máy trạm Email của người dùng.

b. Bộ lọc dựa trên máy chủ

Những bộ lọc này thường chỉ được sử dụng trong một nhóm hoặc môi trườnglàm việc kinh doanh hơn là ở trong gia đình. Tất cả Email đến đều thông qua máy chủ trung tâm. Tại máy chủ trung tâm này, Email được lọc bởi bộ lọc dựa trên máy chủ và những người dùng riêng biệt nhận thư của họ trên màn hình nền của máy họ lấy từ máy chủ trung tâm.

Ưu điểm:

Việc quản lý trung tâm của tất cả các luật lọc thư bảo đảm tính an toàn trong mạng.

Những người dùng riêng biệt không phải chịu trách nhiệm cũng như không phải lo lắng đến sự quản lý thư rác, giải phóng họ để họ có thể yên tâm trong công việc với trao đổi thư điện tử.

Nhược điểm:

Thường yêu cầu nhiều tới sự duy trì và cầm có một người quản trị mạng có khả năng và kinh nghiệm để quản lý bộ lọc thư rác này.

Thường tốn nhiều chi phí hơn

2.2.2.7 Phương pháp lọc dựa trên xác nhận danh tính của người gửi

Giả mạo thư điện tử - là việc giả mạo địa chỉ thư điện tử của một công ty hoặc của một người khác để khiến người sử dụng tin tưởng và mở thư - đang là một trong những thử thách lớn nhất mà cộng đồng sử dụng Internet và các kỹ thuật viên chống

thư rác hiện đang phải đối mặt. Nếu không có sự thẩm định quyền, xác nhận và khả năng truy tìm danh tính của người gửi, các hãng cung cấp dịch vụ thư điện tử không bao giờ có thể biết chắc một bức thư là hợp pháp hay bị giả mạo. Do đó việc xác nhận danh tính của người gửi là rất cần thiết. Để xác nhận danh tính của người gửi người ta đưa ra một số giải pháp sau:

a. Phương pháp DomainKeys

Phương pháp DomainKeys có thể giúp phân định rõ thư rác và thư thường bằng cách cung cấp cho các hãng cung cấp dịch vụ thư điện tử một cơ chế xác nhận cả tên miền của mỗi người gửi thư điện tử và sự liêm chính của mỗi bức thư được gửi đi (ví dụ như các thư này không bị thay thế trong khi được truyền qua mạng). Và, sau khi đã xác nhận được tên miền, người ta có thể so sánh tên miền này với tên miền mà người gửi sử dụng trong ô "Người gửi" của bức thư để phát hiện các trường hợp giả mạo. Nếu đây là trường hợp giả mạo, thư đó sẽ bị coi là thư rác hoặc gian lận, và có thể bị loại bỏ mà không ảnh hưởng tới người sử dụng. Nếu đây không phải là thư giả mạo, có nghĩa là tên miền được biết đến và tên miền gửi thư đó có thể được được đưa vào danh sách những tên miền đáng tin cậy và được đưa vào các hệ thống quy định chống thư rác được sử dụng chung giữa các hãng cung cấp dịch vụ và thậm chí đưa ra cho cả người sử dụng.

b. Phương pháp Call-ID

Caller ID là một tiêu chuẩn đặt ra trong quá trình gửi thư. Tiêu chuẩn này đòi hỏi người gửi thư điện tử phải cung cấp địa chỉ IP của máy chủ gửi thư theo dạng XML vào bản ghi DNS trên máy chủ tên miền của họ. Máy chủ nhận thư điện tử và máy khách nhận bức thư đó sẽ kiểm tra địa chỉ gửi thư trong tiêu đề bức thư với địa chỉ đã được công bố để xác nhận máy chủ gửi thư. Các bức thư không khớp với địa chỉ nguồn sẽ bị loại bỏ. DNS là hệ thống diễn dịch các địa chỉ IP số sang các tên miền Internet có thể đọc được.

c. Phương pháp SPF (Sender Policy Framework) - dựa trên cơ cấu chính sách người gửi

Chuẩn SPF cũng yêu cầu người gửi thư điện tử phải sửa đổi DNS để cho biết máy chủ nào có thể gửi thư từ một tên miền Internet nhất định. Tuy nhiên, SPF chỉ kiểm tra sự giả mạo khi bức thư trong quá trình chuyển thư hay còn gọi là ở mức "ngoài phong bì", xác minh địa chỉ "phản hồi" của một bức thư, thường được máy chủ nhận thư gửi trở lại trước khi tiếp nhận phần nội dung thư, sau đó sẽ thông báo tới máy chủ nhận thư để loại bỏ bức thư.

Trong đặc tả kỹ thuật kết hợp hai tiêu chuẩn, các công ty gửi thư điện tử sẽ công bố địa chỉ máy chủ thư điện tử của họ trong bản ghi DNS dưới định dạng Ngôn ngữ đánh dấu mở rộng (XML). Các công ty sẽ có thể kiểm tra sự giả mạo ở mức phong bì (cũng giống như trong đề xuất SPF) và trong phần nội dung thư (theo đề xuất của Microsoft).

Kỹ thuật này sẽ cho phép các công ty sử dụng cách thức của SPF để loại bỏ thư rác trước khi chúng được gửi đi, nếu sự giả mạo bị phát hiện ngay ở mức phong bì. Với những bức thư đòi hỏi sự kiểm tra kỹ hơn trong nội dung thư, thì phương pháp Caller ID sẽ được sử dụng. Đề xuất này cũng sẽ hỗ trợ các tên miền đã có sẵn những bản ghi SPF là văn bản, không theo định dạng XML.

2.2.2.8 Phương pháp lọc thư rác mới dựa trên mạng Xã hội

Các nghiên cứu gần đây đã bắt đầu khai thác thông tin từ mạng xã hội cho việc xác định thư rác bằng cách xây dựng một đồ thị (các đỉnh là địa chỉ Email, cũng được thêm vào giữa 2 node A và B nếu giữa A và B có sự trao đổi thư qua lại). P.O.Boykin và V. Roychowdhury đã sử dụng một số tính chất đặc trưng của mạng xã hội để xây dựng một công cụ lọc thư rác [6].Đầu tiên, người ta phân đồ thị thành các thành phần con rồi tính độ phân cụm cho từng thành phần này. Mỗi thành phần con là một đồ thị mạng xã hội của một node, bao gồm tất cả các node hàng xóm (các node xung quanh có cung liên kết với node này) và những cung liên kết giữa các node hàng xóm này với nhau. Nếu thành phần nào có độ phân cụm thấp thì node tương ứng với thành phần đó là một địa chỉ gửi thư rác. Trong thành phần mạng xã hội của những node gửi thư rác, những node hàng xóm của nó thường là những node rất ngẫu nhiên, không có mối quan hệ (không có sự trao đổi Email qua lại với

nhau) nên độ phân cụm của mạng xã hội của những node này rất thấp. Ngược lại, mạng xã hội ứng với những người dùng bình thường các node hàng xóm của nó có mối liên kết cao với nhau nên có độ phân cụm cao hơn

Dựa vào độ phân cụm, người ta tạo được danh sách đen (Blacklist) gồm địa chỉ Email tương ứng với những node có độ phân cụm rất thấp, danh sách trắng (Whitelist) ứng với node có độ phân cụm cao, số node còn lại sẽ được đưa vào danh sách cần xem xét (Greylist). Phương pháp này có thể phân loại được 53% tổng số Email một cách chính xác là ham hay spam. Nhược điểm của phương pháp là những spammer có thể xây dựng mạng xã hội của chính họ nên khó có thể phát hiện ra

Cho đến nay, một bộ lọc thư rác được xem là hoàn hảo vẫn chưa được tạo ra, và việc tạo ra một bộ lọc thư rác hoàn hảo cho mọi thời đại dường như là thể không thể. Bởi, cuộc chiến không ngừng giữa những tên gửi thư rác và những bộ lọc làm cho siêu bộ lọc thư rác của hôm nay có thể trở thành cái lỗi thời của ngày mai. Bộ lọc thư rác mạnh nhất sẽ là bộ lọc sử dụng kết hợp nhiều bộ lọc khác, hoặc tất cả các thuộc tính đã liệu kê ở trên đây.

CHƯƠNG III: TRIỂN KHAI THỬ NGHIỆM, ĐỀ XUẤT ÁP DỤNG PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG ANTI SPAM EMAIL CHO HỆ THỐNG EMAIL TẠI NGÂN HÀNG HÀNG HẢI VIỆT NAM

3.1. Hiện trạng tấn công Spam Email tại ngân hàng Hàng Hải Việt Nam (MSB)

Ngân hàng MSB là ngân hàng TMCP đầu tiên ra đời (năm 1991) trong thời kỳ kinh tế mở cửa và phát triển của Việt Nam.Với bề dày 28 năm hình thành và phát triển, MSB không ngừng tạo lập nhiều cột mốc mang tính đột phá trong ngành tài chính ngân hàng:

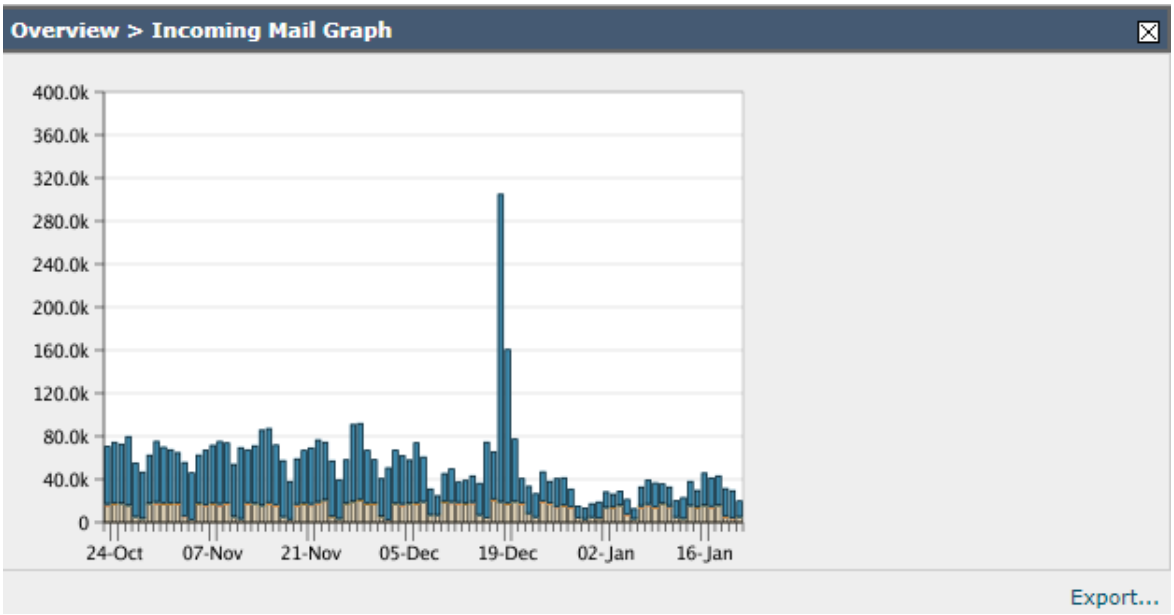
Quy mô khách hàng ngày càng lớn mạnh: với sự đa dạng các sản phẩm dịch vụ tài chính ngân hàng với trên 1,8 triệu khách hàng cá nhân, gần 45.000 khách hàng doanh nghiệp và nhiều đối tác.

Để đảm bảo giải quyết các vấn đề thư rác, virus, các tấn công lừa đảo thực hiện qua Email, và Email chính là mục tiêu hàng đầu của các cuộc tấn công có chủ đích (APT), các giải pháp chống tấn công nhằm xâm nhập hệ thống, khai thác dữ liệu, đánh cắp thông tin và tài chính của khách hàng, ảnh hưởng đến danh tiếng doanh nghiệp. Ngân hàng MSB đã đưa ra phương án chú trọng việc xây dựng một hệ thống an ninh vững chắc, đảm bảo an toàn hệ thống và quyền lợi của mỗi khách hàng.

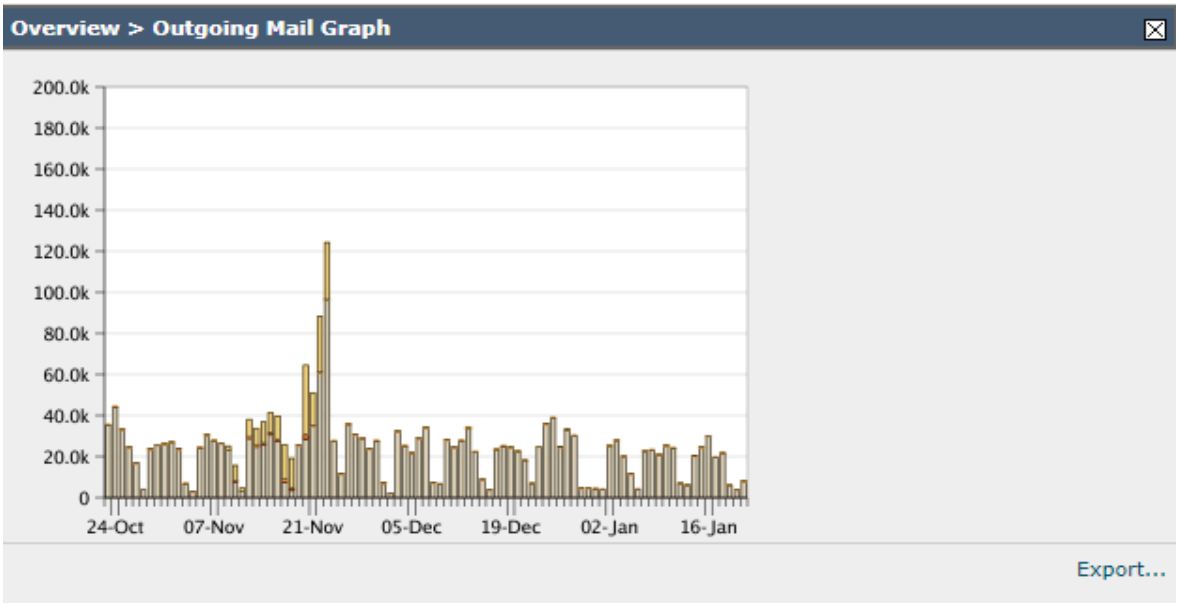
Xây dựng hệ thống Email Security Gateway nhằm đáp ứng khả năng phân tích các mối đe doạ theo thời gian thực tại Email Gateway, cung cấp báo cáo nâng cao để đánh giá, điều tra các sự kiện đối với hệ thống Email, phát hiện và ngăn chặn các mối đe dọa, các tấn công để bảo vệ hệ thống Email tại Ngân hàng Hàng Hải Việt Nam (MSB).

Xây dựng phương án chống tấn công hệ thống Email đáp ứng các yêu cầu như sau:

- Hệ thống Email Security Gateway được thiết kế chạy theo mô hình 2N+1 (1 thiết bị hoạt động tại DC, 1 thiết bị hoạt động tại DR).
- Hệ thống đang đáp ứng cho số lượng: 7.000 người dùng MSB và các tài khoản dịch vụ với các tính năng lọc thư rác, lọc virus, lọc nội dung.
- Hệ thống đang tích hợp với McAfee Network Data Loss Prevention để chặn các Email không được phép gửi ra ngoài; tích hợp với hệ thống Qradar SIEM đẩy các sự kiện an ninh tập trung.
- Hiên trạng lọc Email tại MSB như sau:
  - ➢ Lượng mail lớn nhất: 320.000 Emails/ngày (hình 3.1);
  - ➢ Lượng mail trung bình: 100.000 Emails/ngày.



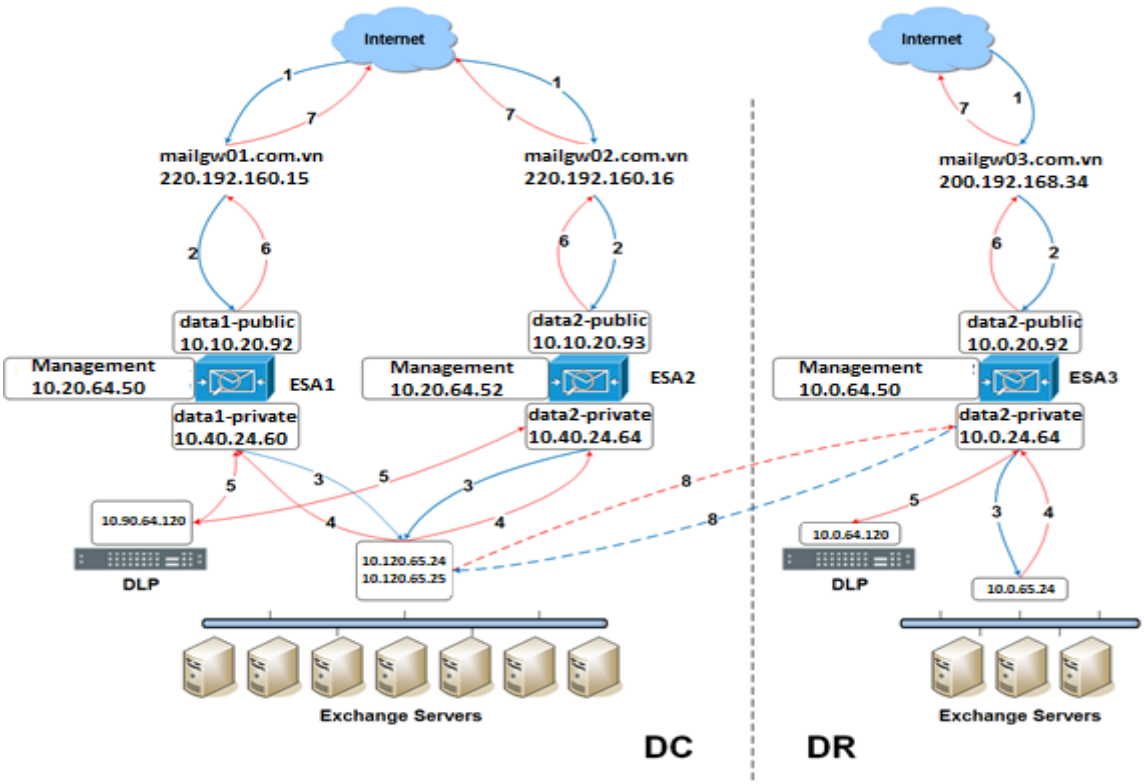
Hình 3.1: Thống kê số lượng Incoming Emails



Hình 3.2: Thống kê số lượng Outgoing Emails

3.2. Phân tích luồng gửi và nhận Email tại ngân hàng Hàng Hải Việt Nam (MSB)

3.2.1 Sơ đồ luồng dữ liệu gửi và nhận Email



Hình 3.3: Sơ đồ luồng dữ liệu gửi và nhận Email tại ngân hàng

(1): Email từ ngoài Internet vào site DC được chia tải qua 2 bản ghi Email1 và Email2, được cấu hình với cùng preference. Theo tiêu chuẩn RFC 5321, server gửi mail sẽ tự động chọn ngẫu nhiên 1 trong 2 địa chỉ public IP ứng với 2 bản ghi MX này để gửi mail. Khi 1 trong 2 địa chỉ IP này gặp sự cố, server gửi mail sẽ thử lại với IP còn lại để tránh gián đoạn luồng mail. Bản ghi của site DR có preference thấp hơn DC, do vậy khi site DC gặp sự cố, toàn bộ luồng mail từ Internet sẽ được chuyển về DR.

(2): Các bản ghi MX trỏ tới IP của public listener trên các thiết bị ESA. Tại đây các thiết bị Cisco Email Security sẽ thực hiện kiểm tra, dò quét từng Email bằng các tính năng Antispam, Antivirus, Outbreak filter, Advanced malware protection, Content filter… để chặn lọc các Email spam, độc hại, vi phạm chính sách.

(3): Các Email an toàn, hợp lệ sẽ được các thiết bị ESA chuyển tiếp tới Exchange server chứa mailbox của người dùng

(4): Email từ người dùng gửi ra ngoài được Exchange server gửi tới private listener của các thiết bị ESA theo cơ chế load balancing của riêng mình.

(5): Các thiết bị ESA chuyển tiếp Email tới thiết bị Network DLP để kiểm tra chính sách DLP. Nếu Email vi phạm, DLP gửi Email thông báo cho người dùng ngược trở lại cho ESA. Nếu Email không vi phạm, DLP gửi trả Email gốc có thêm trường X-Header chứa kết quả kiểm tra lại cho ESA

(6) và (7): Các thiết bị ESA tiếp tục thực hiện các tính năng kiểm soát outbound trước khi chuyển tiếp Email ra ngoài Internet thông qua public IP.

(8): Traffic dự phòng khi cả 2 thiết bị tại DC gặp sự cố

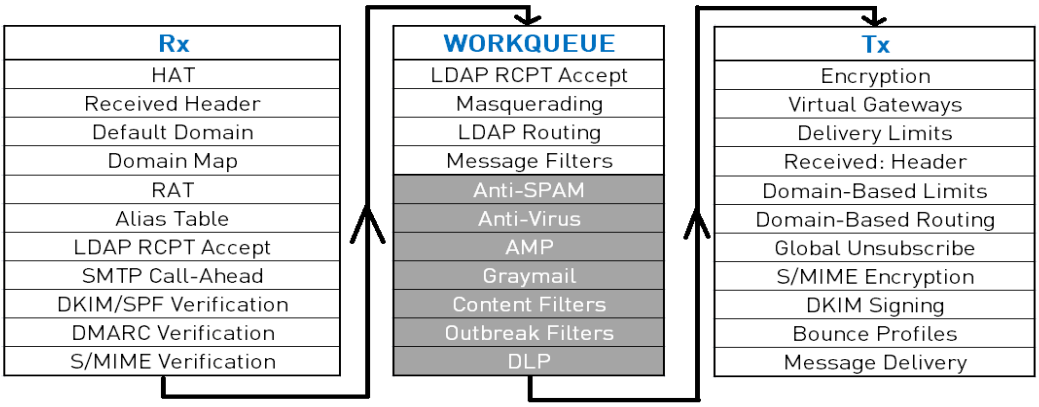
3.2.2 Cơ chế hoạt động đề xuất đối với luồng dữ liệu gửi và nhận Email

Đối với mỗi Email nhận được, ESA thực hiện xử lý theo 3 luồng (3 giai đoạn) tuần tự của một tiến trình được gọi là Email pipeline trên thiết bị, gồm có:

Receipt: thiết bị kiểm tra các thông tin ở mức SMTP connection với host ở đầu gửi mail và thực hiện giới hạn, kiểm soát theo chính sách

Work queue: sau khi trải qua giai đoạn Receipt, thiết bị tiếp tục kiểm soát tập trung vào các thông tin của nội dung bức thư.

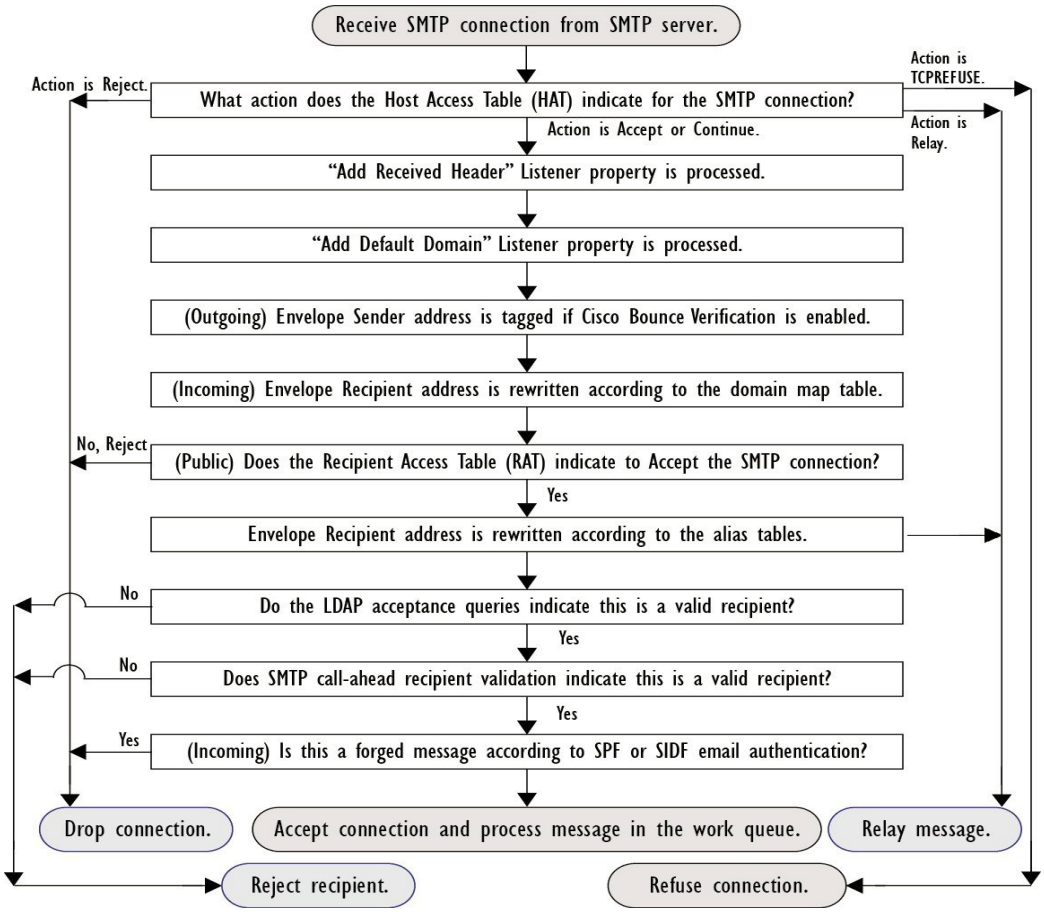
Deliver: sau khi đã vượt qua giai đoạn Work queue, thiết bị chuẩn bị khởi tạo phiên kết nối với host ở đầu nhận mail. Tại bước này thiết bị cũng tiếp tục thực hiện các thao tác thay đổi, kiểm soát Email theo chính sách



Hình 3.4: Trình tự xử lý luồng Email

a. Trình tự xử lý của luồng Receipt

Trình tự xử lý của luồng Receipt được thể hiện tuần tự qua sơ đồ sau:



Hình 3.5: Trình tự xử lý luồng Receipt

(1)Thiết bị nhận kết nối SMTP từ host gửi mail

(2)Thiết bị đối chiếu các thông tin của SMTP connection với bảng HAT

Bảng HAT (Host Access Table): quy định những host nào được kết nối với listener (host nào được phép gửi mail qua thiết bị) - thể hiện qua Sender group, và kết nối đó sẽ được áp dụng những giới hạn nào - thể hiện qua Mail flow policy.

(3)Thiết bị kiểm tra giá trị tuỳ chọn Add Received Header trong cấu hình listener. Tuỳ chọn được bật tại môi trường theo mặc định

Trường Received: có thể được thêm vào bức thư để ghi lại dấu vết về việc bức thư đã đi qua thiết bị. Việc thêm trường này sẽ được thực hiện ở giai đoạn Delivery

(4)Nếu tính năng Add default domain được cấu hình, thiết bị tự động điền domain vào đằng sau địa chỉ người gửi. Tính năng này áp dụng cho một số hệ thống xử lý mail đời cũ, với địa chỉ người gửi không chứa phần domain. Môi trường MSB không sử dụng tính năng này

(5)Đối với mail gửi ra: nếu tính năng Bounce verification được bật, thiết bị thêm tag vào bức thư

Tính năng Bounce verification cho phép ESA thêm 1 tag (là 1 chuỗi ký tự đặc biệt) vào trường Envelope sender (Return-Path header) của Email trước khi gửi ra ngoài. Nếu bức thư bị bounce và trả ngược lại cho ESA, nó sẽ kiểm tra tag này, nếu đúng thì mới cho mail đi qua. Qua đó hệ thống ngăn chặn được những Email giả mạo từ các cuộc tấn công dạng backscatter, bounce attack

Trên thực tế, một số Email client ở đầu nhận có thể hiển thị sai trường From khi tính năng này được bật, do vậy môi trường MSB không sử dụng tính năng này.

(6)Đối với mail gửi vào: nếu tính năng Domain map được sử dụng, thiết bị sẽ sửa lại trường recipient theo bảng domain map. Tính năng này thường dùng trong các trường hợp sáp nhập tổ chức, trong đó các Email gửi tới domain cũ được ánh xạ sang domain mới để phục vụ luồng công việc. Môi trường của MSB không sử dụng tính năng này.

(7)Đối với mail nhận qua public listener, thiết bị đối chiếu thông tin trong SMTP connection với bảng RAT.

Bảng RAT (Recipient Access Table) quy định những local domain mà thiết bị cho phép nhận. Email gửi đến các domain ngoài bảng này sẽ bị reject

(8)Nếu thiết bị có cấu hình alias table, trường Envelope Recipient sẽ được chỉnh lại theo bảng alias.

Bảng alias cho phép ánh xạ các địa chỉ tới một hoặc nhiều người nhận khác nhau. Bảng alias áp dụng cho toàn bộ mail qua cả private và public listener, và thực thi sau khi kiểm tra RAT và trước khi đối chiếu với message filter. Môi trường của MSB không sử dụng tính năng này.

(9)Nếu listener có cấu hình LDAP acceptance query ở bước SMTP connection, thiết bị sẽ đối chiếu người nhận với kết quả trả về từ câu truy vấn tới LDAP server.

LDAP query sẽ thực hiện kiểm tra trường recipient của Email với các user nằm trên LDAP directory. Nếu user không tồn tại, thiết bị có thể delay bounce hoặc drop hẳn Email. LDAP query có thể được áp dụng ở giai đoạn này hoặc giai đoạn work queue.

Tính năng này có thể làm tăng tải cho hệ thống AD do mỗi khi listener nhận được Email, ESA sẽ gửi truy vấn đến AD để kiểm tra. Do vậy môi trường của MSB không sử dụng tính năng này.

(10)Nếu listener bật SMTP call-ahead, thiết bị sẽ kiểm tra trường recipient với call ahead server trước khi xử lý tiếp.

Tính năng SMTP call ahead cho phép thiết bị kiểm tra người nhận có hợp lệ hay không thông qua việc đối chiếu với 1 external server (call ahead server), trước khi nhận kết nối từ server gửi mail. Tính năng này dùng để xác thực người nhận khi không thể dùng LDAP accept hoặc RAT để kiểm chứng. Môi trường của MSB không sử dụng tính năng này.

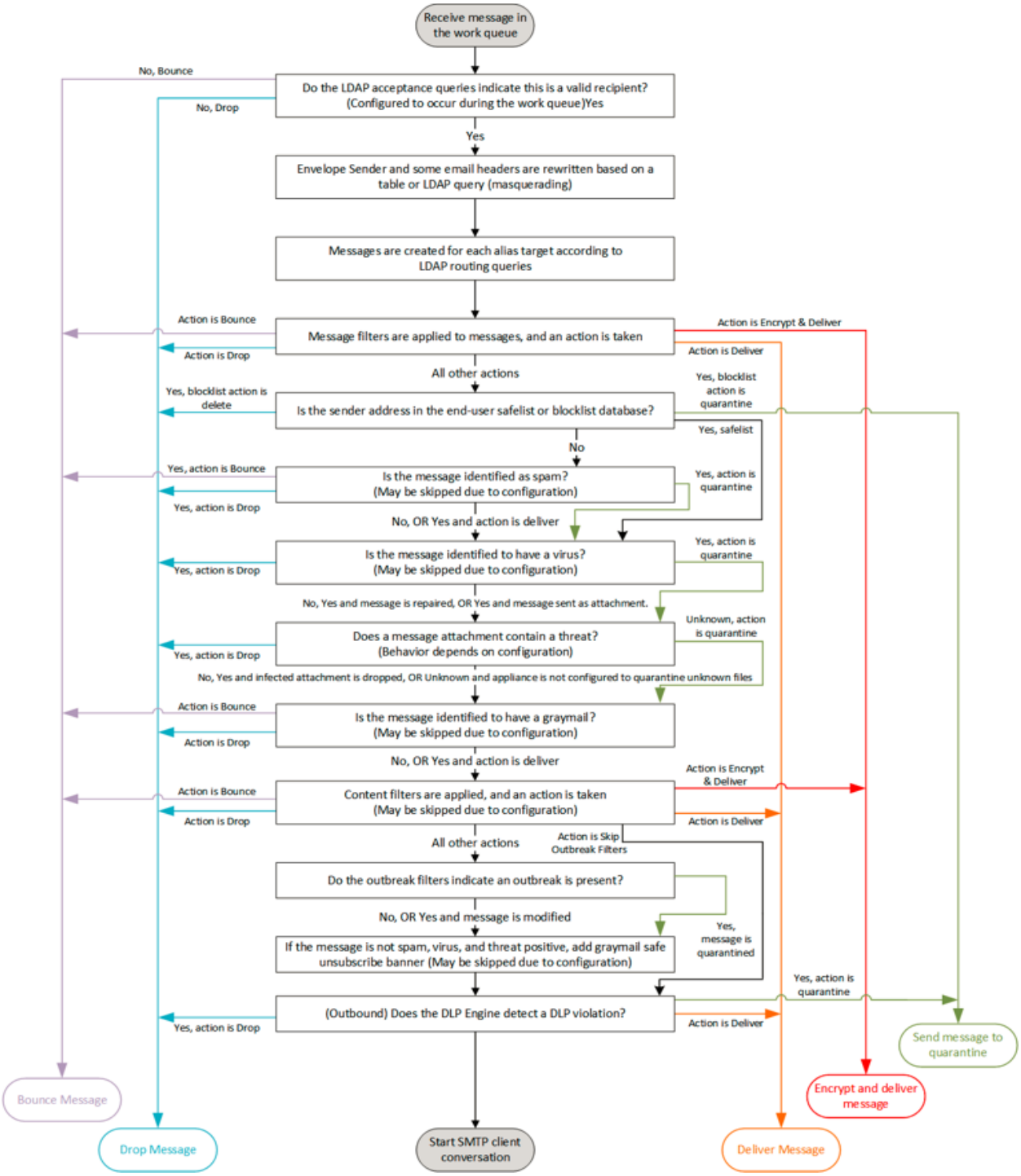
(11)Đối với mail gửi vào, thiết bị kiểm tra bản ghi SPF/SIDF để xác thực nguồn gửi Email.

Tính năng SPF/SIDF checking cho phép thiết bị kiểm tra IP nguồn của server gửi mail có hợp lệ hay không bằng cách đối chiếu nó với kết quả truy vấn từ bản ghi

SPF của domain gửi qua DNS. Nếu IP nguồn có trong danh sách này, nó được coi là hợp lệ, và ngược lại.

b. Trình tự xử lý Work queue

Trình tự xử lý của luồng Work queue được thể hiện tuần tự qua sơ đồ sau:



Hình 3.6: Trình tự xử lý luồng Work queue

(1) Nếu listener có cấu hình LDAP acceptance query ở bước work queue, thiết bị sẽ đối chiếu người nhận với kết quả trả về từ câu truy vấn tới LDAP server. Môi trường của MSB không sử dụng tính năng này

(2) Nếu tính năng masquerading được bật, thiết bị sẽ chỉnh sửa lại trường envelope sender theo cấu hình

Masquerading cho phép ánh xạ trường envelope sender và cả trường To, From, CC theo bảng do người dùng định nghĩa. Việc này có thể thực hiện bằng static table qua CLI hoặc bằng LDAP query. Tính năng này dùng trong trường hợp doanh nghiệp áp dụng virtual domain để host nhiều domain khác nhau cho cùng 1 site; hoặc trong trường hợp doanh nghiệp muốn giấu thông tin về hạ tầng mạng bằng việc cắt bỏ phần subdomain khỏi Email header. Môi trường của MSB không sử dụng tính năng này

(3) Nếu LDAP routing được cấu hình, thiết bị tạo các Email để gửi tới nhiều target khác nhau. Môi trường của MSB không sử dụng tính năng này

(4) Email được xử lý qua các message filter (nếu có)

Message filter cho phép định nghĩa các rule dựa trên các thông tin đầu vào như: nội dung message/attachment, envelope, header, thông tin về network; và áp dụng các hành động với bức thư như drop, bounce, archive, quarantine, BCC hoặc thay đổi nội dung

Các bước tiếp theo thuộc quá trình xử lý của Email Security Manager. Tại đây Email được nhân bản thành từng phiên bản riêng cho từng người nhận (gọi là splinter), và áp dụng các cơ chế dò quét cho từng bản splinter này

(5) Thiết bị đối chiếu sender với safelist, blocklist (nếu có)

Safelist/blocklist là danh sách do người dùng cuối tạo để định nghĩa các sender nào được coi là spam hoặc không spam.

(6) Thiết bị áp dụng bộ lọc spam với bức thư để xác định mức độ spam của nó, và đưa ra hành động tuỳ theo kết quả

(7) Thiết bị áp dụng bộ lọc virus với file đính kèm để phát hiện và vô hiệu hoá (nếu có thể) mã độc bên trong. Sau đó thiết bị đưa ra hành động tuỳ theo kết quả dò quét

(8) Thiết bị kích hoạt tính năng AMP để kiểm tra reputation của file với cloud của Cisco

AMP sử dụng thông tin trên cloud để phát hiện các mối đe doạ dạng zero day bên trong các file đính kèm

(9) Thiết bị phát hiện các bức thư dạng graymail (thư quảng cáo) và tự động unsubscribe khỏi dịch vụ thay cho người dùng cuối. Môi trường của MSB không sử dụng tính năng này

(10) Email được xử lý qua các content filter (nếu có). Việc xử lý này áp dụng cho bức thư đã qua splinter, nghĩa là áp dụng cho từng người gửi và người nhận riêng biệt

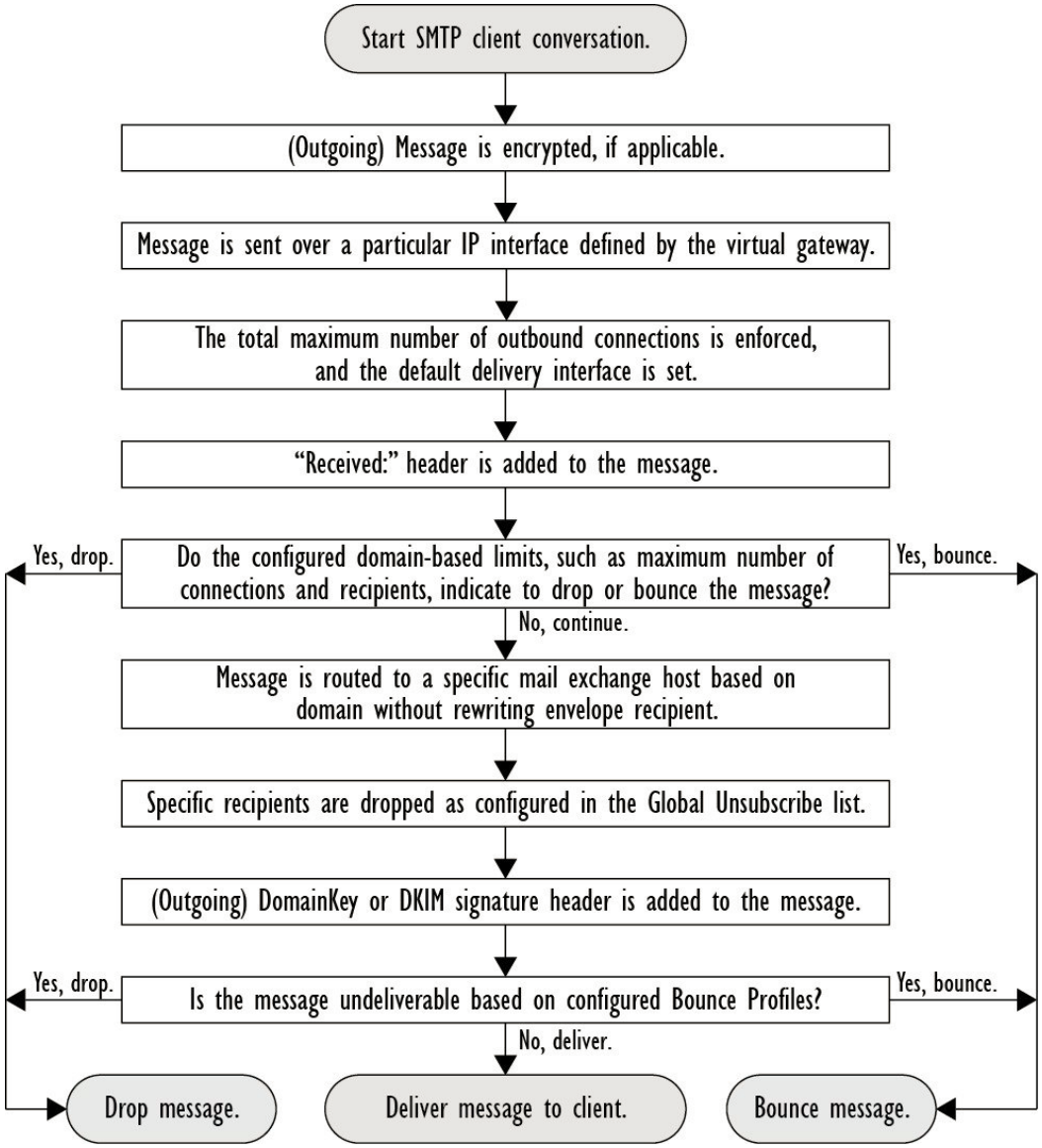
(11) Thiết bị kích hoạt tính năng outbreak filter để phát hiện các zero day hoặc blended threat trong Email

Outbreak filter sử dụng các tập rule update liên tục từ cloud của Cisco để gán cho Email một threat level, dựa trên một bộ các đặc tính của Email mà hãng coi là nguy hiểm. Dựa vào threat level, chính sách có thể quy định hành động áp dụng tương ứng

(12) Thiết bị sử dụng DLP engine để dò quét các vi phạm chính sách DLP. Môi trường của MSB không sử dụng tính năng này

c. Trình tự xử lý của luồng Delivery

Trình tự xử lý của luồng Delivery được thể hiện tuần tự qua sơ đồ sau:



Hình 3.7: Trình tự xử lý của luồng Delivery

(1)Nếu được cấu hình tính năng Encryption, nội dung Email được mã hoá. Môi trường của MSB không sử dụng tính năng này

(2)Nếu Virtual gateway được cấu hình, Email sẽ được gửi đến IP interface xác định theo cấu hình để chuẩn bị gửi ra ngoài. Môi trường của MSB không sử dụng tính năng này

Tính năng Virtual gateway cung cấp khả năng gửi Email tới đầu xa qua nhiều IP khác nhau, với mục đích đảm bảo đầu xa nhận được Email một cách chính xác, tránh các trường hợp chặn do nhầm là spam

(3)Thiết bị giới hạn số lượng connection và chọn default delivery interface theo cấu hình ở câu lệnh deliveryconfig

(4)Cấu hình mặc định là chế độ Auto (thiết bị tự động lựa chọn delivery interface phù hợp) với giới hạn 10000 connection.

(5)Trường Received được thêm vào Email (nếu đã bật ở giai đoạn Receipt trước đó)

(6)Thiết bị giới hạn số lượng kết nối theo cấu hình trong Destination controls

(7)Tính năng Domain-Based Limits cho phép thiết bị kiểm soát số lượng kết nối tới từng domain cụ thể trong 1 khoảng thời gian nhất định

(8)Thiết bị định tuyến Email tới SMTP host dựa trên bảng SMTP routes

(9)Thiết bị đối chiếu danh sách người nhận với Global unsubscribe list và drop hoặc bounce các Email không mong muốn. Môi trường của MSB không sử dụng tính năng này

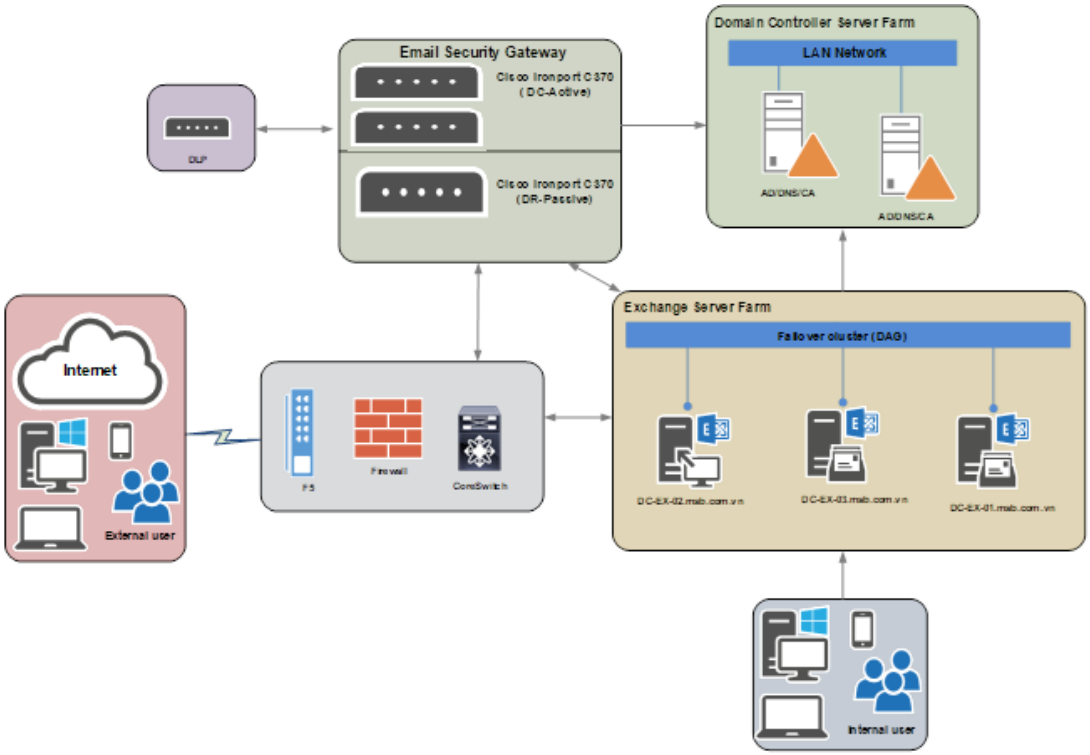
Global unsubscribe cho phép định nghĩa những domain mà hệ thống không bao giờ gửi mail tới, như một giải pháp cuối cùng

(10)Đối với mail gửi ra, nếu bật tính năng DKIM, thiết bị thêm DKIM signature vào Email.

3.2.3 Đề xuất triển khai thực giải pháp

Để phòng chống các tấn công qua hệ thống Email của ngân hàng Hàng Hải Việt Nam, luận văn đề xuất thực hiện các biện pháp phòng chống tấn công đối với hệ thống máy chủ, hệ thống Mail Client, đường truyền Internet. Trong khuôn khổ luận văn này, khi nghiên cứu phòng chống tấn công AntiSpam Email sẽ sử dụng các phương pháp như sau: Phương pháp lọc Spam Email; Phương pháp lọc theo từ khóa; Phương pháp lọc Spam Assasin; Phương pháp dùng danh sách trắng/ đen; Phương pháp lọc dựa vào vị trí của các bộ lọc; Phương pháp lọc dựa trên xác nhận danh tính của người gửi.

Qua quá trình nghiên cứu và tìm hiểu, đề tài đề xuất thực hiện các phương pháp ngăn chặn tại Email Security Gateway với bộ lọc là giải pháp của Cisco Ironport C390 Appliance (đã bao gồm các phương pháp lọc nêu trên) để thực hiện với mô hình kết nối như sau:

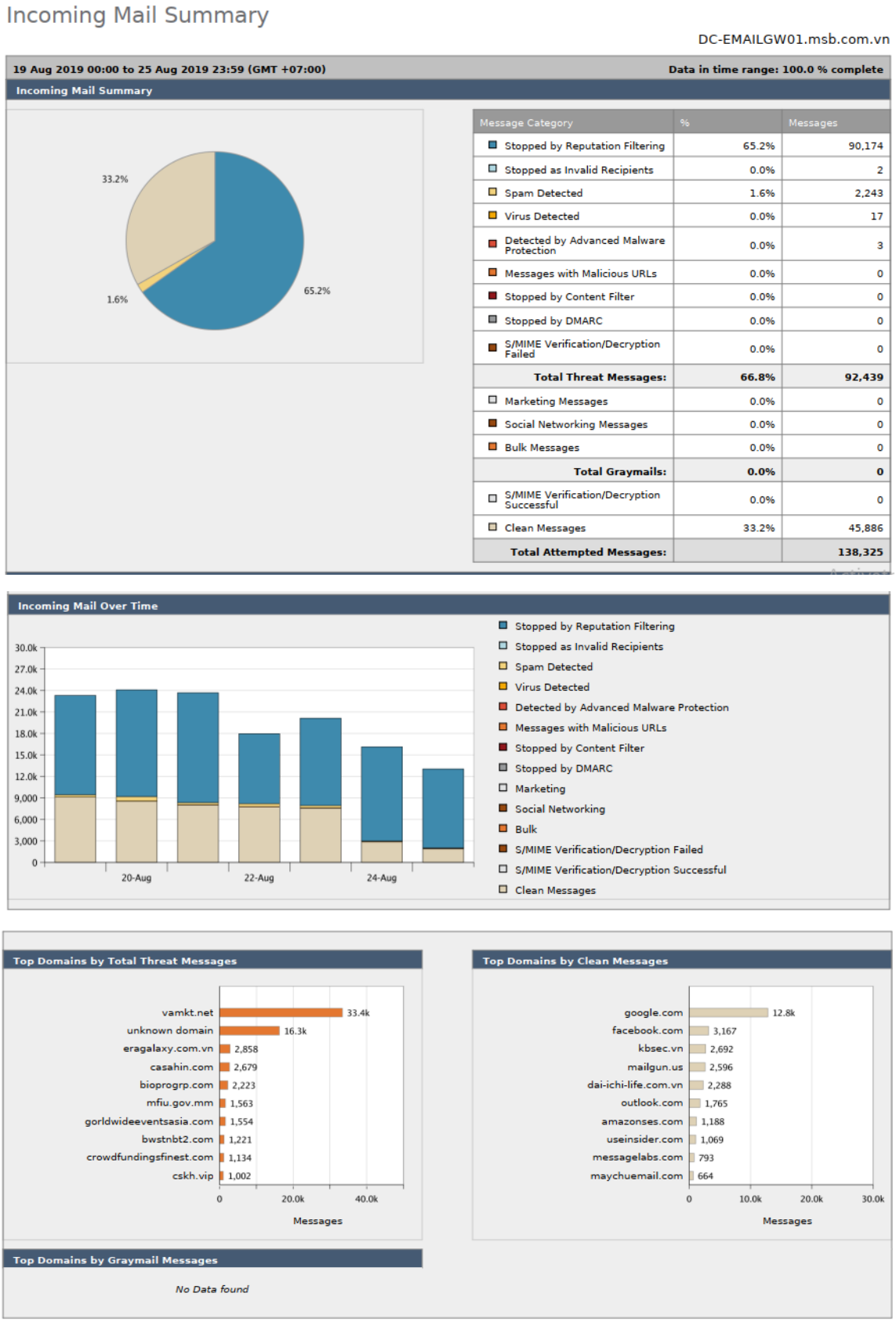


Hình 3.8: Mô hình triển khai giải pháp

Kết quả sau khi thực hiện

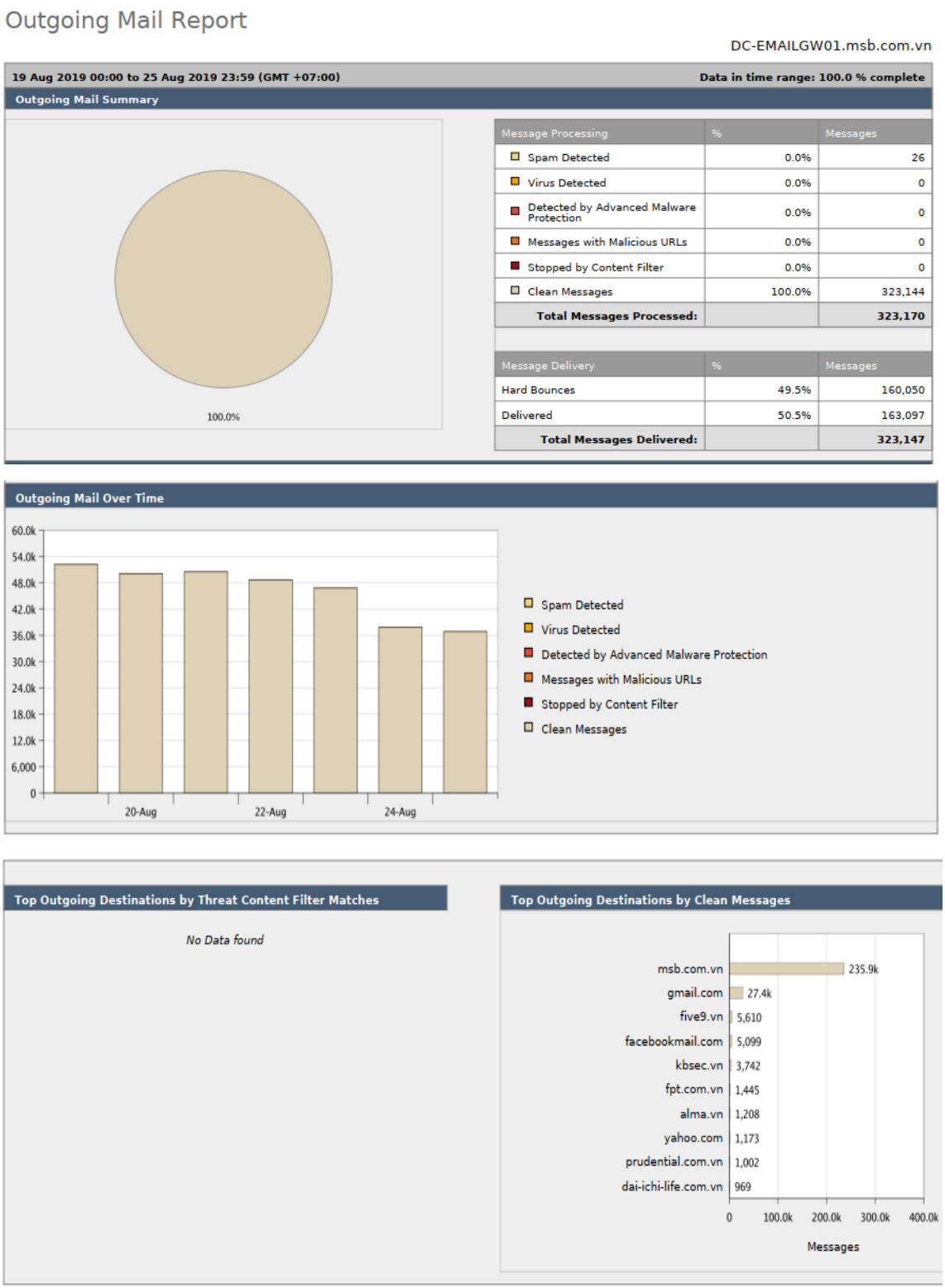
Sau khi thực hiện giải pháp, hệ thống đã ngăn chặn được thư rác, virus, các tấn công lừa đảo thực hiện qua Email, và Email chính là mục tiêu hàng đầu của các cuộc tấn công có chủ đích (APT) với kết quả như sau:

Incoming Mail Summary



Hình 3.9: Kết quả Incoming Mail Summary

Outgoing Mail Report



Hình 3.10: Kết quả Outgoing Mail Summary

KẾT LUẬN

Luận văn đã hệ thống hóa một số vấn đề lý thuyết về thư rác, các hướng tiếp cận trong vấn đề lọc thư rác trước đây đồng thời trình bày một số khái niệm và đặc điểm về quá trình xâm nhập và lừa đảo thông qua thư rác. Đồng thời đề xuất một giải pháp đặc trưng có thể thực hiện phát hiện, ngăn chặn và theo dõi quá trình tấn công an ninh thông tin qua Email.

- Kết quả chính đạt được của luận văn:
  - Tìm hiểu về các tấn công Email
  - Nghiên cứu và phân tích luồng dữ liệu;
  - Phân tích quá trình hoạt động từ đó ngăn chặn được các rủi ro
  - Đề xuất được giải pháp lựa chọn đặc trưng tốt nhất đảm bảo hiệu quả, hiệu suất của hệ thống
  - Tiến hành thực nghiệm và đánh giá, so sánh các kết quả.
- Hướng phát triển tiếp theo của nghiên cứu:

Mở rộng nhiều hướng tiếp cận phân tích mã độc và các phương thức tấn công mới. Thực hiện phân tích dựa trên kinh nghiệm từ đó phối hợp với các giải pháp mới để cập nhật những xu hướng tấn công mới nhất. Đảm bảo an ninh, an toàn cho hệ thống và bảo vệ thông tin của người sử dụng.

DANH MỤC CÁC TÀI LIỆU THAM KHẢO

[1] Cisco Email Security Appliances User Guide, https://www.cisco.com/c/en/us/support/security/Email-security-appliance/products-user-guide-list.html

[2] Email threat report cisco, https://www.cisco.com/c/dam/en/us/products/collateral/security/Email-security/Email-threat-report.pdf

[3] John Aycock, Springer Publishing (2006), *"Computer viruses and Malware (Advances in Information Security)"*. https://pdfs.semanticscholar.org/

[4] IOSR Journal of Engineering (IOSRJEN) *"Comparative and Analysis Study for Malicious Executable by Using Various Classification Algorithms"*. http://iosrjen.org/Papers/vol8_issue7/Version-2/C0807021826.pdf

[5] Threat intelligence analyst, https://www.eccouncil.org/

[6] RFC 5575 – Dissemination of Flow Specification Rules

[7] Báo cáo Spam and Phishing Quý I năm 2019 của Kaspersky Lab, http://kaspersky.nts.com.vn/

[8]https://www.netcraftsmen.com/bgp-flowspec-step-forward-ddos-mitigation/

[9]https://supportforums.cisco.com/t5/service-providers-documents/asr9000-xr-understanding-bgp-flowspec-bgp-fs/ta-p/3139916

[10] https://m.bkav.com.vn/