**TÌM HIỂU PHƯƠNG PHÁP TẤN CÔNG APT, XÂY DỰNG THỬ NGHIỆM MÔ HÌNH PHÁT HIỆN TẤN CÔNG APT**

**Lời nói đầu**

**Mục lục**

[LỜI NÓI ĐẦU 2](#_Toc465088951)

[1.Đặc điểm của tấn công APT 3](#_Toc465088952)

[2.Mô hình tấn công APT 5](#_Toc465088953)

[2.1 Các giai đoạn cơ bản của một cuộc tấn công APT 5](#_Toc465088954)

[**(1) Thăm dò mục tiêu, chuẩn bị công cụ:** 6](#_Toc465088955)

[**(2) Phát triển và xâm nhập các nhân tố tấn công:** 7](#_Toc465088956)

[**(3) Bắt đầu khởi tạo cuộc tấn công:** 8](#_Toc465088957)

[**(4) Ra lệnh và điều khiển:** 9](#_Toc465088958)

[**(5) Xâm nhập vào bên trong hệ thống:** 9](#_Toc465088959)

[**(6) Trích xuất, thu nhận dữ liệu:** 9](#_Toc465088960)

[2.2 Tìm hiểu một số cuộc tấn công APT 10](#_Toc465088961)

[2.3 Biện pháp phòng chống tấn công APT 10](#_Toc465088962)

[Tập huấn an ninh mạng 11](#_Toc465088963)

[Công nghệ phòng thủ, bảo vệ hệ thống mạng truyền thống 11](#_Toc465088964)

[Hệ thống phát hiện mã độc nâng cao 11](#_Toc465088965)

[Phát hiện các sự kiện bất thường 12](#_Toc465088966)

[Ngăn chặn việc mất dữ liệu (Data Loss Prevention – DLP) 12](#_Toc465088967)

[Phương pháp sử dụng trí tuệ nhân tạo phòng chống tấn công APT 12](#_Toc465088968)

[3. Hệ thống phòng thủ và ngăn chặn tấn công APT đa tầng 13](#_Toc465088969)

[3.1 Kiến trúc hệ thống 13](#_Toc465088970)

[3.2 Kịch bản ngăn chặn tấn công APT với mô hình đa tầng 16](#_Toc465088971)

[3.3 Một số trường hợp áp dụng cụ thể 18](#_Toc465088972)

# **LỜI NÓI ĐẦU**

Những cuộc tấn công mạng đã và đang xảy ra trong hàng thập kỷ vừa qua, từ Virus máy tính, sâu máy tính cho đến các mã độc, mạng botnets đang là mối đe dọa đến sự an toàn của người dùng khi sử dụng máy tính và sử dụng mạng Internet. Máy tính cá nhân đang dần trở thành một phần không thể thiếu của cuộc sống, đây là nơi lưu trữ nhiều thông tin nhạy cảm như thông tin cá nhân, thông tin thương mại, bí mật quân sự, … .Vì vậy những vấn đề về an ninh, an toàn cho hệ thống máy tính đang là vấn đề cần thiết và cần phải được nghiên cứu quan tâm.

Cùng với sự phát triển không ngừng của mạng Internet, các hình thức tấn công mạng cũng phát triển tinh ngày một tinh vi hơn sử dụng những cách thức tấn công mới nhằm vượt qua sự bảo vệ của Anti-Virus, các hệ thống phát hiện xâm nhập. Trong thời gian gần đây thuật ngữ được nhắc đến nhiều nhất và phổ biến nhất là “Advanced Persistent Threat” (APT) .Tấn công APT là tấn công dai dẳng, có chủ đích, nhằm vào một mục tiêu nhất định đe dọa cao đến người dùng với tính chất khó phát hiện, khó có thể ngăn chặn vì vậy hình thức tấn công này đang là nguy cơ đe dọa cao đến an ninh mạng nói chung và đến người dùng máy tính nói riêng. Xuất phát của các cuộc tấn công APT nhằm vào các mục tiêu quân sự với mục đích thu thập các thông tin bí mật, quan trọng trong quân sự, nhưng ngày nay APT không giới hạn trong một phạm vi hay lĩnh vực nào nó đang là mối đe dọa tới tất cả người dùng máy tính và Internet từ các công ty, tập đoàn, doanh nghiệp tới các tổ chức chính phủ.

Trong khi các mối đe dọa cũng như hậu quả to lớn mà các cuộc tấn công APT để lại thì việc hiểu một cách rõ ràng về bản chất của APT, các phương pháp phòng chông tấn công APT vẫn còn thiếu xót và chưa được nghiên cứu ứng dụng nhiều trong thực tế. Vì vậy, bài nghiên cứu tìm hiểu về phương pháp tấn công APT này trình bày một cách chi tiết và có logic về tấn công APT cũng như các phương pháp cơ bản phòng chống tấn công APT, bao gồm các nội dung chính như sau: (1) Đặc điểm của tấn công APT, (2) Các bước cơ bản của một cuộc tấn công APT, (3) Một số biện pháp phòng chống tấn công APT.

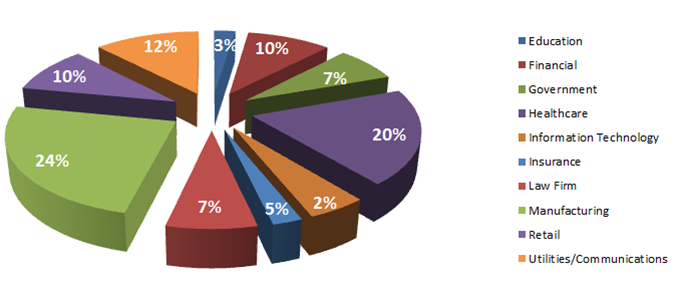
# **1.Đặc điểm của tấn công APT**

APT được nhắc đến rất nhiều đặc biệt trong các hội thảo, nghiên cứu về an ninh mạng trong thời gian gần đây, có rất nhiều định nghĩa được đưa ra nhằm mô tả thế nào là tấn công APT, tuy nhiên cần có một định nghĩa rõ rảng, bao hàm được tính chất, đặc điểm của một cuộc tấn công APT, chúng ta sẽ sử dụng định nghĩa của Viện công nghệ và tiêu chuẩn quốc gia Mỹ (**NIST**).

“Người bị tấn công APT là người sở hữu những tài nguyên quan trọng và có giá trị cho phép các kẻ tấn công thu được chúng bằng nhiều phương pháp khác nhau .Mục đích tấn công bao gồm thiết lập và mở rộng quyền kiểm soát và nắm bắt các thông tin nội bộ trong cấu trúc hạ tầng công nghệ thông tin của mục tiêu tấn công APT.Tấn công APT: (i) Theo đuổi mục tiêu tấn công nhiều lần, lặp đi lặp lại trong một khoảng thời gian dài, (ii) Thích nghi với các nỗ lực bảo vệ nhằm chống tấn công APT, (iii) Duy trì sự tương tác với mục tiêu tấn công”.

Một cuộc chiến dịch tấn công APT được thực hiện khác so với những cuộc tấn công mạng truyền thống, nó bao gồm các đặc trưng cơ bản như sau: (1) Nhằm vào một mục tiêu cụ thể với mục đích rõ ràng, (2) có sự tổ chức và chuẩn bị kỹ lưỡng về mặt con người cũng như những trang thiết bị, tài nguyên cần thiết cho việc tấn công, (3) APT là một chiến dịch tấn công dài hạn, dai dẳng và cố gắng lặp đi lặp lại, (4) Sử dụng công nghệ tấn công bí mật, từng bước kiểm soát hệ thống. Các đặc điểm này được trình bày cụ thể như sau**:**

**Nhằm vào một mục tiêu cụ thể với mục đích rõ ràng:** tấn công APT là việc tấn công hướng đối tượng rất rõ ràng, các mục tiêu tấn công thường được kẻ tấn công xác định cụ thể chi tiết, có quá trình tìm hiểu mục tiêu tấn công công phu, tỉ mỉ và luôn có một mục đích tấn công rõ ràng. Mục tiêu của các cuộc tấn công APT thường là các cơ quan chính phủ, cơ quan lưu trữ, nơi sử dụng, lưu trữ những thông tin quan trọng, có giá trị cao. Theo báo cáo về xu hướng tấn công APT năm 2015 của *FireEye* cho thấy các cuộc tấn công này nhằm vào các ngành có ảnh hưởng và có giá trị cao như: Giáo dục, Tài chính, Chính Phủ, Công Nghệ Thông Tin, Sức khỏe, Bán lẻ, …



Hình 1: Tấn công APT trên các lĩnh vực (FireEye – 2015)

Mục đích của các cuộc tấn công APT thường nhằm vào các thông tin quan trọng của cơ quan, tổ chức và quốc gia, những thông tin có thể tạo lợi thế cho đối thủ tấn công như: thông tin an ninh quốc gia, thông tin thương mại bí mật, các thông tin nội bộ trong các cơ quan, tổ chức, … Trong khi các cuộc tấn công mạng truyền thống hầu hết nhằm thu thập bất hợp pháp các thông tin cá nhân như: thông tin thẻ tín dụng, thông tin thị trường tài chính, trộm cắp tài sản. Mục tiêu này thể hiện sự khác biệt rõ ràng giữa các cuộc tấn công mạng truyền thống với hình thức tấn công mạng APT.

**Được tổ chức và chuẩn bị kỹ lưỡng trước khi tiến hành tấn công:** Hacker tổ chức và sử dụng các hình thức tấn công APT thường là những con người có kỹ năng, có kinh nghiệm cao, thường được tổ chức, huấn luyện bài bản và làm việc có tổ chức theo nhóm kết hợp chặt chẽ giữa các thành viên trong nhóm với nhau. Họ có thể làm việc trong các cơ quan chính phủ, đơn vị quân đội hoặc được thuê bởi chính phủ hoặc các công ty tập đoàn để tấn công nhằm thu được các thông tin cần thiết. Với sự chuẩn bị kỹ lưỡng và kỹ năng cao lợi dụng điểm yếu các lỗ hổng bảo mật *zero-day* và những công cụ cần thiết cho cuộc tấn công APT được diễn ra thành công và thuận lợi.

**Là một chiến dịch tấn công dài hạn và việc theo đuổi mục tiêu dai dẳng:** Một cuộc tấn công APT có đặc điểm thường là các cuộc tấn công trong một thời gian dài với sự lên kế hoạch dài hạn của các kẻ tấn công. Những cuộc tấn công APT có thể nằm trong hệ thống mạng của mục tiêu trong vài tháng hoặc vài năm mà không bị phát hiện. Những nhân tố là mục tiêu của cuộc tấn công APT thường bị các kẻ tấn công cố gắng lặp đi, lặp lại bằng các biện pháp khác nhau nếu như lần tấn công trước bị thất bại, việc này có thể thực hiện bằng các hình thức kỹ nghệ xã hôi. Đây cũng là điểm khác biệt phân biệt giữa các kiểu tấn công truyền thống với các cuộc tấn công APT, trong các cuộc tấn công truyền thống thì kẻ tấn công thường nhằm vào các mục tiêu diện rộng hoặc khi thất bại trong cuộc tấn công, kẻ tấn công thường chuyển sang các mục tiêu khác ít được bảo vệ hơn, ít an toàn hơn.

**Sử dụng công nghệ tấn công dai dẳng, từng bước một nhằm đạt được mục tiêu:** Tấn công APT thường được tổ chức một cách bí mật, thăm dò thực hiện từng chút từng chút một trước khi đạt được mục tiêu.Kẻ tấn công cố gắng làm cho hệ thống nạn nhân không thể phát hiện ra các nhân tố của các cuộc tấn công này. Ví dụ các nhân tố của cuộc tấn công APT có thể sử dụng như: khai thác lỗ hổng zero-day để tránh sự phát hiện của các hệ thống ngăn chặn dựa vào chữ ký số, mặt khác kẻ tấn công cũng có thể sử dụng các kỹ thuật mã hóa, kỹ thuật gây rối (obfuscate) thường khác so với các cuộc tấn công truyền thống thường gây ra các hậu quả mà nạn nhân có thể phát hiện ra ngay sau khi bị tấn công trong *Bảng 1*.

*Bảng 1: Bảng so sánh sự khác nhau giữa tấn công mạng truyền thống và APT*

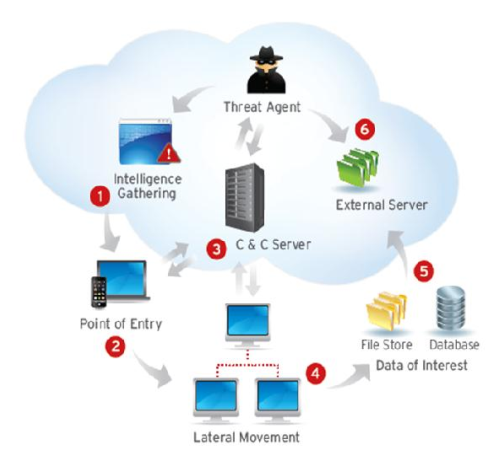
|  |  |  |
| --- | --- | --- |
|  | **Tấn công truyền thống** | **Tấn công APT** |
| Kẻ tấn công | Hầu hết là cá nhân đơn lẻ | Tính tổ chức cao,  chuẩn bị kỹ lưỡng |
| Mục tiêu | Chưa được xác định, hầu hết các hệ hống đơn lẻ | Xác định rõ ràng, chính phủ, tập đoàn tài chính |
| Mục đích | Thu lợi tài chính, thể hiện kỹ năng tấn công | Giành lợi thế cạnh tranh, nắm bắt các chiến lược |
| Phương pháp tiếp cận | Đơn lẻ, ngắn hạn | Dai dẳng, ẩn sâu trong hệ thống, dài hạn |

# **2.Mô hình tấn công APT**

Tấn công APT là một cuộc tấn công có kế hoạch và kịch bản được chuẩn bị một cách tỉ mỉ, kỹ lưỡng. Đặc điểm của cuộc tấn công APT phải trải qua nhiều bước, nhiều giai đoạn khác nhau. Trong mỗi cuộc tấn công APT có thể có những đặc điểm riêng biệt tuy nhiên một cách tổng quan, một cuộc tấn công APT dựa vào mô hình tấn công sáu pha theo trình tự được sử dụng để có thể hiểu những nhân tố, công nghệ trong mỗi pha và đưa ra những biện pháp có thể phòng chống những cuộc tấn công APT một cách tốt nhất.

## **2.1 Các giai đoạn cơ bản của một cuộc tấn công APT**

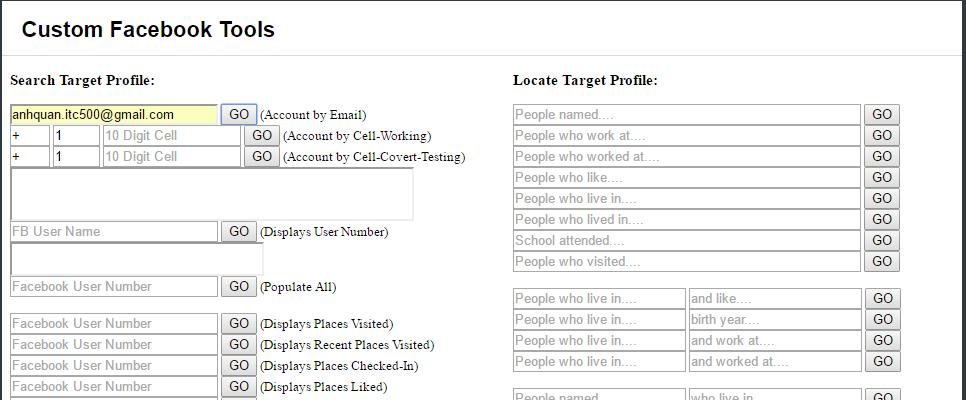
Đặc điểm của cuộc tấn công APT thường dựa vào sáu giai đoạn cơ bản: (1) thăm dò mục tiêu, chuẩn bị công cụ, (2) phát triển các nhân tố tấn công, (3) Bắt đầu khởi tạo cuộc tấn công, (4) Ra lệnh và điều khiển, (5) Xâm nhập bên trong, (6) Trích xuất và thu nhận dữ liệu.



Hình 2: Các giai đoạn cơ bản của một cuộc tấn công APT

**(1) Thăm dò mục tiêu, chuẩn bị công cụ:** Thăm dò mục tiêu cũng được biết đến như là biện pháp thu thập thông tin, đây là một bước chuẩn bị quan trọng mở đầu cho cuộc tấn công. Ở giai đoạn nay, Kẻ tấn công sẽ cố gắng thu thập thông tin về mục tiêu cần tấn công, cả những thông tin công khai và những thông tin bí mật có liên quan đến đối tượng, cơ quan, tổ chức cần tấn công. Kẻ tấn công sẽ cố gắng thu thập nhiều thông tin nhất có thể về môi trường kỹ thuật, những mật khẩu cá nhân, tài liệu quan trọng với mục tiêu cần tấn công. Những thông tin này thường được thu thập và tập hợp bằng những công cụ thông minh mã nguồn mở (Open source Intelligence **OSINT**) và bằng kỹ nghệ xã hội(**Social Engineering**).

**- Công cụ thông minh mã nguồn mở (OSINT).** OSINT là một danh mục thu thập thông tin thông minh từ những nguồn thông tin công khai, sẵn có. Hiện nay, phương pháp này thường được thực hiện bằng việc tổ chức, sắp xếp các thông tin theo danh mục từ các nguồn trên mạng Internet. Nhiều thông tin có thể thu thập được bằng phương pháp OSINT từ các thông tin cá nhân đến thông tin về phần cứng, phần mềm, thông tin cấu hình và của tổ chức là những mục tiêu của kẻ tấn công.



Hình 3: Công cụ OSINT tìm kiếm thông tin người dùng trên mạng xã hồi Facebook

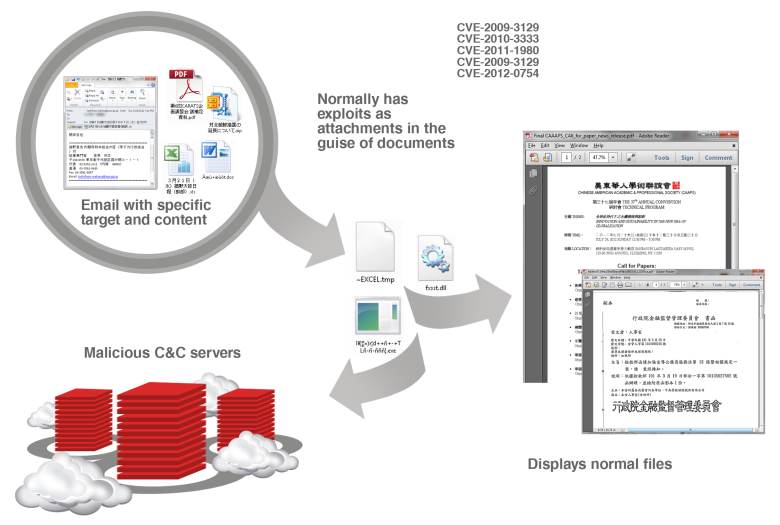
**- Kỹ nghệ xã hội.** Kỹ nghệ xã hội đánh vào tâm lý của con người tập trung vào khai thác, lợi dụng những mục tiêu của người dùng Internet. Trong tấn công mạng, phương pháp kỹ nghệ xã hội thường được sử dụng nhằm thu thập các thông tin quan trọng, nhạy cảm hoặc khiến cho mục tiêu thực hiện các hành động đặc biệt (ví dụ: thực thi mã độc, lây lan virus …)

Bên cạnh việc thu thập các thông tin trên mạng Internet, Kẻ tấn công có thể sử dụng các công cụ khai phá dữ liệu (Data Mining) và Dữ liệu lớn (Big Data) để thu thập các thông tin một cách tự động. Dựa vào việc thu thập các thông tin, bản kế hoạch tấn công APT được xây dựng và chuẩn bị những công cụ cần thiết phục vụ cho việc tấn công. Để đảm bảo cho cuộc tấn công APT thành công, Kẻ tấn công phải xây dựng những công cụ đa dạng cho những tình huống tấn công khác nhau, do đó họ có thể chuyển đổi tình huống tấn công nếu như có thất bại xảy ra một cách nhanh chóng.

**(2) Phát triển và xâm nhập các nhân tố tấn công:** Ở giai đoạn này, kẻ tấn công xâm nhập những nhân tố phục vụ cho việc khai thác tới mục tiêu cần tấn công. Có hai cách chính của công nghệ này: *trực tiếp* xâm nhập, cài đặt *gián tiếp* xâm nhập. Với xâm nhập trực tiếp, Kẻ tấn công gửi những nhân tố tấn công phục vụ sự khai thác của họ tới mục tiêu tấn công bằng nhiều công nghệ tấn công kỹ nghệ xã hội.

Khai thác gián tiếp là cách khai thác một cách bí mật, từng bước, từng bước một. Ở cách tiếp cận này, Kẻ tấn công sẽ thỏa hiệp hoặc lợi dụng điểm yếu, lỗ hổng của bên thứ ba để gián tiếp trở thành nhân tố khai thác mục tiêu tấn công. Bên tin cậy thứ ba có thể là nhà cung cấp và phát triển phần cứng hoặc phần mềm được mục tiêu tấn công sử dụng, hoặc là những website mà mục tiêu tấn công thường xuyên truy cập hoặc tương tác.

- **Spear Phishing**: Tấn công lừa đảo, chiếm đoạt thông tin quan trọng, mật khẩu. Kiểu tấn công này có thể giả mạo địa chỉ email mà mục tiêu tấn công tin tưởng hoặc ít nghi vấn. Bằng việc sử dụng các thông tin trong bước thăm dò thu thập, kẻ tấn công sẽ điều chỉnh nội dung, tiêu đề của bức thư giả mạo, các phần mềm, ứng dụng cần thiết với mục tiêu tấn công sao cho người dùng là mục tiêu tấn công ít thấy nghi ngờ đề đảm bảo khả năng thành công cao. Những người dùng là mục tiêu tấn công dễ tiếp nhận những thông tin này mà không biết đây là các chương trình, văn bản có đính kèm mã độc đã bị kẻ tấn công đính kèm hoặc cũng có thể lừa đảo cho người dùng kích vào các đường link độc hại.



Hình 4: Spear Phishing qua các tin nhắn, email có gắn kèm mã độc

- **Watering Hole Attack**: Tấn công thông qua các Website chứa mã độc. Phương pháp tấn công này được ví tương tự như việc đưa mục tiêu tấn công vào vị trí cần phải có nước như trên xa mạc, đưa người dùng cần thiết phải bị mắc vào những lừa đảo của kẻ tấn công. Kẻ tấn công thường lợi dụng các website của bên thứ ba được người dùng tin cậy và thường xuyên truy cập, tương tác với mục đích cá nhân và cố gắng lây nhiễm vào các website này các mã độc đã được điều chỉnh cho phù hợp với mục tiêu tấn công.

**(3) Bắt đầu khởi tạo cuộc tấn công:** Khởi tạo cuộc tấn công thường diễn ra khi kẻ tấn công nhận được cảnh báo truy cập trái phép (**unauthorized access**) tới mục tiêu tấn công là máy tính/ hệ thống mạng. Trong khi kẻ tấn công có thể thu được sự truy cập tin cậy thông qua kỹ nghệ xã hội và đơn giản sử dụng chúng cho việc truy cập hợp lệ, đặc điểm của giai đoạn này là các mã độc được kích hoạt thực thi để bắt đầu quá trình khai thác lỗ hổng trên hệ thống máy tính nạn nhân.

Trong các cuộc tấn công APT, Kẻ tấn công thường tập trung vào việc khai thác các lỗ hổng trên các ứng dụng và phần mềm như Adobe PDF, Adobe Flash và Microsoft Office, Internet Explore. Quá trình bắt đầu cuộc tấn công là thời điểm then chốt quyết định đến sự thành công của một cuộc tấn công APT. Sự thành công của giai đoạn này có thể tính đến như là việc cài thành công mã độc, **backdoor** từ đây chúng kết nối với hệ thống mạng của máy tính mục tiêu do đó các dữ liệu trao đổi trong hệ thống mạng, các thông tin cá nhân bị các mã độc này thu nhận.

**(4) Ra lệnh và điều khiển:** Sau việc cài đặt **backdoor** thành công, các nhân tố của cuộc tấn công APT sử dụng công nghệ ra lệnh và điều khiển (**Command and Control – C&C**) để điều khiển máy tính nạn nhân, thực hiện việc khai thác hệ thống mạng. Để tránh sự phát hiện, kẻ tấn công tăng cường việc tạo ra các dịch vụ và công cụ công khai.

**-** Social Network Site: Kẻ tấn công đăng ký tài khoản trên nhiều trang mạng xã hội và đặt điều khiển thông tin vào trong các thông điệp post và status

**-** Sử dụng hệ thống mạng Tor: Hệ thống kết nối qua Tor được gọi là những dịch vụ ẩn. Hosting máy chủ **C&C** trên Tor được coi là dịch vụ ẩn làm cho chúng khó bị phát hiện và phân tích hơn.

**-** Công cụ điều khiển truy cập ( **Remote Access Tool - RAT**): Mặc dù phương pháp này thường được sử dụng với mục đích điều khiển hợp pháp, **RAT** cũng thường bị lợi dụng cho cho các cuộc tấn công mạng. Một hệ thống RAT bao gồm: **server** điều khiển từ xa, và **client** được cài đặt trên máy nạn nhân của cuộc tấn công.

**(5) Xâm nhập vào bên trong hệ thống:** Một giao tiếp giữa hệ thống máy nạn nhân với **C&C** server được thành lập, nhân tố tấn công của APT được xâm nhập vào bên trong hệ thống mạng nhằm mục đích mở rộng và tăng cường phạm vi điều khiển hệ thống máy tính nạn nhân, tiến hành khám phá và thu thập những dữ liệu có giá trị. Giai đoạn xâm nhập vào bên trong hệ thống thường thực hiện theo các bước như sau: (1) Biểu diễn các thông tin đã thu thập được trên hệ thống mạng và thu thập bằng các công cụ, phương pháp ở các giai đoạn trên, (2) Đưa ra các thỏa hiệp và những điều kiện với hệ thống nhằm thu thập được những thông tin có giá trị hơn và giành được những đặc quyền điều khiển hệ thống, (3) Định danh và thu thập những thông tin có giá trị như là kế hoạch phát triển, trao đổi bí mật, bí mật quân sự, …

**(6) Trích xuất, thu nhận dữ liệu:** Mục đích cao nhất của một cuộc tấn công APT nhằm thu được những dữ liệu quan trọng, nhạy cảm của mục tiêu tấn công, như vậy bước trích xuất dữ liệu thu được là một bước đặc biệt quan trọng.Thông thường dữ liệu được trao đổi giữa hệ thống mạng với **C&C** sẽ được nén và mã hóa trên đường truyền, trong các cuộc tấn công APT thường sử dụng các giao thức như **SSL/TLS** hoặc sử dụng hệ thống mạng Tor.

## **2.2 Tìm hiểu một số cuộc tấn công APT**

Để hiểu tốt nhất các bước và giai đoạn chuẩn bị của các cuộc tấn công APT từ giai đoạn chuẩn bị đến giai đoạn tiến hành tấn công và thu nhận dữ liệu, chúng ta sẽ tìm hiểu một số cuộc tấn công APT điển hình đã diễn ra: *Operation Aurora, RAS Breach, Operation Ke3chang, Operation SnowMan.*

*Bảng 2: So sánh các một số cuộc tấn công APT theo các giai đoạn*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Giai đoạn** | **Operation**  **Aurora** | **RAS Breach** | **Operation**  **Ke3chang** | **Operation**  **SnowMan** |
| Thời gian | Tháng 06/2009  Tháng12/2009 | Chưa xác định  Tháng 03/2011 | Tháng 05/2010  Tháng 12/2013 | Chưa xác định  Tháng 02/2014 |
| Thăm dò,  chuẩn bị | Email, zero-day, backdoor | Email, zero-day, trojan doc, backdoor, RAT | Email, trojan doc, backdoor, C&C | Điểm yếu trên vfw.org, RAT, backdoor |
| Phát triển,  lây nhiễm | Spear Phishing (link mã độc) | Spear Phishing  (mã độc xls) | Spear Phishing  (mã độc zip) | Watering hole  (vfw.org) |
| Khởi tạo  tấn công | Kích hoạt khi download (CVE-2010-0249) | Lỗ hổng xls  (CVE-2011-0609) | Nạn nhân kích hoạt file chứa mã độc | Khi download  (CVE-2014-0322) |
| Ra lệnh,  điều khiển | C&C server, TCP cổng 443 | Poison Ivy RAT | C&C server,HTTP | ZxShell  Gh0st RAT |
| Xâm nhập  hệ thống | Sử dụng SCM, thu mã nguồn | thu thập ID, khóa bí mật | Thu thập thông tin nội bộ | Chưa xác định |
| Thu nhận  dữ liệu | Upload dữ liệu lên C&C server | Nén, mã hóa bằng RAR, chuyển FTP | Nén, mã hóa bằng RAR | Chưa xác định |

## **2.3 Biện pháp phòng chống tấn công APT**

Đối mặt với tính chất phức tạp và hoạt động một cách bí mật, cẩn thận có kế hoạch của các cuộc tấn công APT sẽ không có một giải pháp đơn lẻ nào có thể phòng chống một cách có hiệu quả. Mà đòi hỏi phải có sự phòng chống kết hợp giữa nhiều yếu tố và biện pháp về hệ thống phần cứng, phần mềm và đặc biệt quan trọng là yếu tố con người. Hiện nay, biện pháp thực thế có thể phòng chống các cuộc tấn công APT hiệu quả là sử dụng mô hình phòng chống đa tầng, chia các phương pháp, biện pháp phòng chống thành các tầng bảo vệ khác nhau. Tuy nhiên chúng ta phải chia các tầng phòng chống này hướng theo mục đích của chúng, ví dụ cần có tầng chuyên dùng để phát hiện, phân tích các mã độc, tầng bảo vệ an toàn ứng dụng người dùng, tầng bảo vệ an toàn hệ thống mạng, … Chúng ta sẽ nghiên cứu, tìm hiểu một số công nghệ phòng chống tấn công APT như sau:

## **Tập huấn an ninh mạng**

Tập huấn và tìm hiểu về các công nghệ, phương pháp thường được sử dụng trong các cuộc tấn công APT (ví dụ: spear-phishing, watering hole attack, …) các tập huấn an ninh mạng cần đưa ra các tình huống tấn công APT, đưa người tập huấn vào các vị trí, vai trò bảo vệ hệ thống máy tính, hệ thống mạng. Bên cạnh việc tập huấn thực tế, cần cung cấp thêm về các tài liệu, nội dung có liên quan đến APT. Theo số liệu thống kê quá nửa các cơ quan tổ chức không đưa ra các tài liệu và tiêu chí so sánh sự khác biệt giữa các cuộc tấn công mạng truyền thống và tấn công APT và hơn 67% các nạn nhân bị tấn công APT thiếu xót việc tập huấn này.

## **Công nghệ phòng thủ, bảo vệ hệ thống mạng truyền thống**

Các công nghệ phòng thủ, bảo vệ hệ thống mạng truyền thống là rất cần thiết vì chúng hạn chế các nguy cơ về an ninh mạng, qua đó góp phần vào việc hạn chế những điểm yếu, lỗ hổng của hệ thống, tạo môi trường mạng an toàn qua đó các cuộc tấn công APT sẽ khó có điều kiện triển khai và hoạt động hơn.

Một số công nghệ phòng chống bảo vệ an ninh mạng có thể kể đến như: phần mềm anti-virus, hệ thống firewall, Host-Based Intrusion Detection System (**HIDS**), Network-based Intrusion Detection System (**NIDS**), Intrusion Prevention System (**IDS**), Security Information and Event Management (**SIEM**), content filtering ,…

Tập huấn về an ninh mạng và các biện pháp phòng chống truyền thống không thể ngăn chặn triệt để và có hiệu quả các cuộc tấn công APT, tuy nhiên chúng được kết hợp cùng chuỗi các biện pháp khác để góp phần ngăn chặn các tấn công APT hiệu quả hơn.

## **Hệ thống phát hiện mã độc nâng cao**

Mã độc là vũ khí đặc biệt quan trọng mở đầu cho các cuộc tấn công. Bởi vì các yếu tố trong cuộc tấn công APT như việc khai thác các lỗ hổng zero-day hoặc các công cụ được sửa đổi để tránh được các công cụ, phương pháp ngăn chặn chuyền thống nên các phương pháp phát hiện mã độc nâng cao có ý nghĩa rất quan trọng góp phần ngăn chặn các cuộc tấn công APT.

*Sandboxing* là một trong những biện pháp phân tích hành vi của mã độc, nó cho phép chúng ta định danh và phát hiện những mẫu mã độc mới. Hiện nay, cùng với sự phát triển của các Sandbox, các mã độc cũng được thiết kế để chống chống lại môi trường Sandbox, môi trường máy ảo (VM). Vì vậy một thách thức quan trọng với phương pháp sử dụng sandbox là phải hoạt động một cách trực tuyến hoặc ngăn chặn được sự phát hiện của các mã độc có chức năng Anti-Sandboxing.

## **Phát hiện các sự kiện bất thường**

Bởi vì các nhân tố hoạt động của cuộc tấn công APT thường hoạt động ngầm, và che giấu đi hành vi hoạt động của chúng do đó các phương pháp truyền thống phát hiện mã độc dựa vào chữ ký số hoặc hàm băm sẽ không phát hiện và phòng chống được chúng. Thay vì việc sử dụng các phương pháp truyền thống mà hầu hết các mã độc ngày nay đều có cơ chế để tự vệ lại các phương pháp này, một cách tiếp cận phòng chống APT hiệu quả là phân tích hành vi của các chương trình và tìm kiếm, phát hiện các hành vi bất thường, có những biểu hiện độc hai. Việc phân tích này được thực hiện dựa trên sự phân tích các gói tin trong mạng, các hoạt động nghi vấn trong hệ thống. Bởi vì các sự kiện, hành vi diễn ra trong hệ thống mạng và hệ thống người dùng thường rất lớn do đó chúng ta cần quan tâm giải quyết vấn đề này dựa vào công nghệ dữ liệu lớn (Big Data)

## **Ngăn chặn việc mất dữ liệu (Data Loss Prevention – DLP)**

Bởi vì các cuộc tấn công APT có mục đích chủ yếu là đánh cắp thông tin dữ liệu có giá trị của mục tiêu tấn công, do đó các biện pháp ngăn chặn việc đánh cắp hoặc mất dữ liệu quan trọng nhạy cảm của hệ thống cần phải được triển khai. Hệ thống ngăn chặn mất dữ liệu được thiết kế để phát hiện và ngăn chặn sự mất mát thông tin bằng cách sử dụng các hệ thống theo dõi, giám sát hoạt động mạng. Có cơ chế chính sách phân quyền, bảo vệ các dữ liệu quan trọng. Đảm bảo tính toàn vẹn, tính bí mật và chống chối bỏ trong quá trình truyền tải cũng như lưu trữ dữ liệu trên hệ thống mạng, hệ thống máy tính của người sử dụng. Áp dụng các phương pháp như mã hóa đường truyền, thực hiện xác thực người dung , …

## **Phương pháp sử dụng trí tuệ nhân tạo phòng chống tấn công APT**

Phương pháp sử dung trí tuệ nhân tạo được biết đến như một chiến lược nhằm thu thập thông tin về địch thủ, và kẻ tấn công và thu thập, thống kê các thông tin có liên quan. Bởi vì APT có đặc điểm là những cuộc tấn công dai dẳng, lặp đi lặp lại trên một mục tiêu tấn công. Chúng ta có thể tạo ra những cơ sở dữ liệu thông minh để tập hợp các dữ liệu và phân chia các lần tấn công theo nhóm, qua đó hiểu về các phương pháp, công nghệ tấn công của đối thủ. Vì vậy chúng ta sẽ có định hướng để đưa ra các biện pháp phòng chống hiệu quả hơn.

*Bảng 3* dưới đây tóm tắt một số công nghệ tấn công APT và các công cụ thường được sử dụng theo các giai đoạn thêm vào đó là đưa ra những biện pháp phòng chống có thể sử dụng

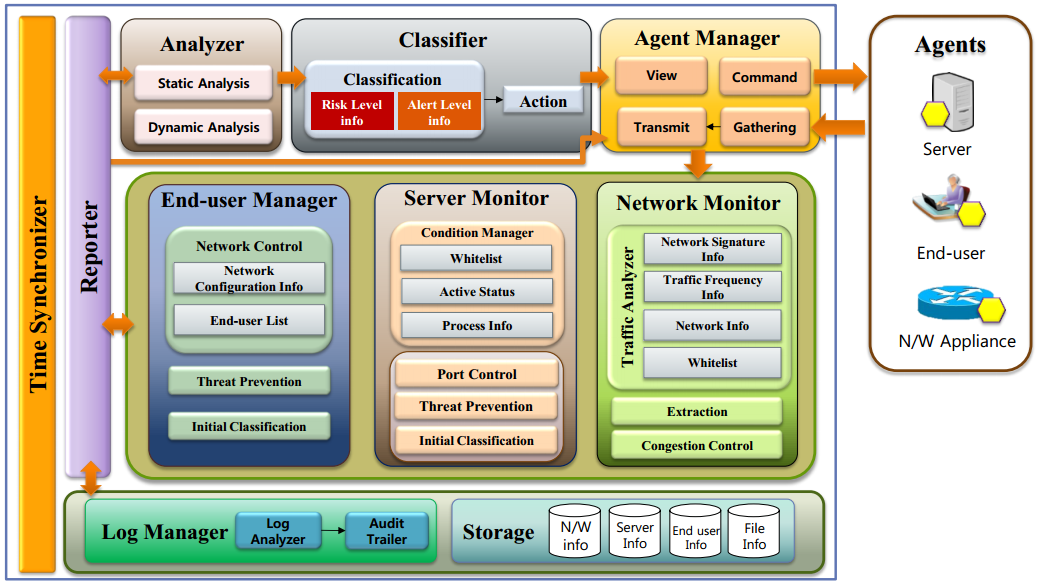
*Bảng 3: Một số kỹ thuật tấn công và cách phòng chống theo giai đoạn của APT*

|  |  |  |
| --- | --- | --- |
| Giai đoạn | Công nghệ/Công cụ | Biện pháp phòng chống |
| Thu thập, chuẩn bị tấn công | OSINT, Kỹ nghệ xã hội  Chuẩn bị Malware | Tập huấn an ninh mạng  Firewall, IDS |
| Phát triển, xâm nhập các nhân tố | Spear phishing  Watering hole attack | Phần mềm lọc nội dung  NIDS, Anti-Virus |
| Khởi tạo  cuộc tấn công | Khai thác zero-day  Triển khai mã điều khiển | HIDS  Chông mã độc nâng cao |
| Ra lệnh  điều khiển | Khai thác tài nguyên  RAT, mã hóa | NIDS, SIEM  Phát hiện sự kiện bất thường |
| Hoạt động trong hệ thống nạn nhân | Leo thang đặc quyền  Thu thập thông tin | Điều khiển truy cập, HIDS  Phát hiện sự kiện bất thường |
| Thu nhận dữ liệu | Nén, mã hóa dữ liệu  Gửi dữ liệu về C&C | Phòng chống mất dữ liệu |

# **3. Hệ thống phòng thủ và ngăn chặn tấn công APT đa tầng**

## **3.1 Kiến trúc hệ thống**

Hệ thống phòng thủ và ngăn chặn tấn công APT đa tầng ngăn chặn sự lây nhiễm của mã độc cho hệ thống mục tiêu bằng cách thu nhận và phân tích thông tin từ thiết bị mạng, hệ thống máy chủ và máy tính người dùng. Hệ thống phòng thủ bao gồm 8 thành phần: Bộ phân loại(*Classifier*), bộ phân tích(*Analyzer*), Tác nhân quản lý (*Agent Management*), Bộ giám sát máy chủ (*Server monitor*), Bộ quản lý người dùng(*End-user Manager*), Bộ giám sát mạng (*Network Monitor*), Quản lý Log và Lưu trữ (*Log manager and Storage*). Kiến trúc của hệ thống như sau:



Hình 5: Kiến trúc hệ thống phát hiện, ngăn chặn tấn công APT đa tầng

+ Module **Time Synronizer** thực hiện các hàm đồng bộ thời gian. Nó cung cấp hệ thống đồng bộ thời gian thực cho các dữ liệu Log bằng việc đồng bộ thời gian với các bộ phận của hệ thống.

+ Module **Reporter** thực hiện việc đảm bảo sự giao tiếp giữa các thành phần. Module này sẽ nhận dữ liệu từ nhiều thành phần khác nhau như: Analyzer, Log Manager, Storage, End-User Manager, Server Monitor và Network Monitor.

+ Bộ phân tích **Analyzer** sẽ thực hiện phân tích các chương trình nghi vấn là mã độc từ phía End-User Manager, Server Monitor và Network Monitor. Thành phần phân tích tĩnh (Static Analysis) bao gồm phân tích theo chữ ký số(signature), giá trị mã băm (hash) của file. Thành phần phân tích động(Dynamic Analysis) bao gồm Sandbox, phân tích hành vi của chương trình, ….Bộ phân tích sẽ phân tích các file tình nghi được chuyển tời từ End-User Manager, Network Monitor và Server Monitor. Nếu như file được chuyển tới chứa mã độc hại, thông tin phân tích của file đó sẽ được gửi đến bộ phân loại (Classifier).

+ Bộ phân loại **Classifier** được chia làm hai phần là Classification Module và Action Module. Ở Classification module có Thông tin gây nguy hại (Risk Level) và thông tin cần cảnh báo (Alert Level). Risk Level có nghĩa là hệ thống đã phát hiện các file phân tích có mã độc. Alert Level là những thông tin cảnh báo tùy thuộc vào các vị trí (server, end-user, network) nơi mà mã độc có thể tồn tại. Classification Module nhận thông tin phân tích từ bộ phân tích Analyzer, phân loại thành Risk Level và Alert Level phụ thuộc vào hành vi mã độc. Action mudule sẽ thực hiện nhiệm vụ chuyển thông tin và đưa ra cảnh báo tới bộ Agent Manager.

+ Bộ **Agent Manager** bao gồm bốn thành phần: View, Command, Gathering và Transmit. Nó quản lý các tác nhân chạy các thiết bị mạng, server và của người dùng từ phía bên ngoài.View module cho phép người quản trị hệ thống kiểm tra trạng thái hiện tại của Hệ thống phòng thủ. Command module nhận từ Action module hoặc từ bộ báo cáo Reporter và gửi tới các tác nhân Agent. Gathering Module thu thập thông tin từ phía Agent. Transmit module gửi các thông tin thu thập được tới các thành phần End-User Manager, Server Monitor và Network Monitor.

+ Bộ quản lý người dùng **End-user Manager** bao gồm các thành phần Network Control, Threat Prevention và Initial Classification. Netwok Control mang thông tin cấu hình mạng và danh sách người dùng. Nếu mã độc được phát hiện bởi người dùng thì thành phần Network Control sẽ hiển thị thông báo người dùng đã bị lây nhiễm mã độc lên hệ thống giám sát mạng. Thành phần Threat Prevention tự động cập nhật những phiên bản mới nhất của các ứng dụng người dùng. Nếu cấu hình hệ thống thay đổi thì các thông tin thay đổi sẽ được gửi đến bộ phân tích Analyzer

+ Bộ **Server Monitor** được cấu thành từ các bộ phận: Condition Manager, Port Control, Threat Prevention và Initial Classification. Thành phần Condition Manager thực hiện chức năng kiểm tra thông tin các tiến trình, trạng thái kích hoạt và Whitelist. Port Control có thể kết nối qua các cổng đến Server. Initial Classification và Threat Prevention dùng để tác động tới những thay đổi từ phía End-User Manager.

+ Bộ **Network Monitor** bao gồm 3 thành phần. Traffic Analyzer kiểm tra và phân tích thông tin đường truyền bao gồm ký số của gói tin trong mạng, tần số các gói tin, thông tin mạng và Whitelist.Thông tin chữ ký số của mạng lưu trữ các thông tin đặc trưng của các luồng độc hại. Thông tin tần số mạng kiểm soát lưu lượng tối đa được trao đổi qua mỗi bộ phận trong hệ thống. Whitelist chứa thông tin về các địa chỉ hợp lệ, trao đổi hợp lệ. Thông tin mạng bao gồm cấu hình mạng và danh sách điều khiển truy cập Access Control List (ACL).

+ Bộ **Log Manager** bao gồm 2 thành phần Audit Trail và Log Analyzer. Với Log Analyzer sẽ ghi nhận và phân tích các thông tin Log, khi có những ghi nhận khác thường được chuyển từ các bộ Server Monitor, End-User Manager và Network Monitor. Thành phần Audit Trail thực hiện chức năng tìm kiếm những người dùng bị nhiễm mã độc và thực hiện phân tích Log của chúng.

+ Bộ **Storage** được dùng để lưu trữ các thông tin về mạng, máy chủ và người dùng từ các bộ Network Monitor, Server Monitor và End-user Manager.Việc lưu trữ này sẽ lưu trữ các thông tin về mã độc phục vụ cho lần phân tích tiếp theo.

## **3.2 Kịch bản ngăn chặn tấn công APT với mô hình đa tầng**

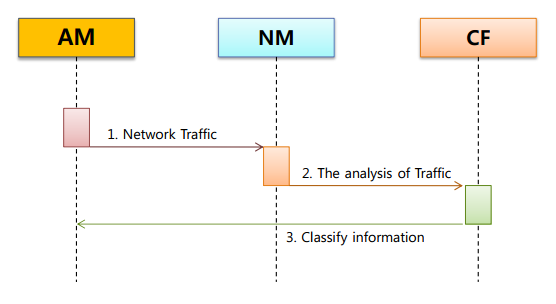
Dựng lên kịch bản ngăn chặn tấn công APT theo các giai đoạn đã nêu ở trên bao gồm 6 giai đoạn chính.

*Bảng 4: Các phương thức tấn công chính theo các giai đoạn trong tấn công APT*

|  |  |  |
| --- | --- | --- |
| Số thứ tự | Giai đoạn | Phương thức tấn công |
| 1 | Thăm dò và chuẩn bị | Quét cổng, mạng,… |
| 2 | Xâm nhập các nhân tố APT | Mã độc, Phishing,… |
| 3 | Khởi tạo tấn công | Backdoor, mã độc |
| 4 | Ra lệnh và điều khiển | C&C, RAT |
| 5 | Hoạt động trong hệ thống nạn nhân | Backdoor, mã độc |
| 6 | Trích xuất thu nhận dữ liệu | Nén, mã hóa dữ liệu |

*Bảng 5: Danh sách từ viết tắt*

|  |  |  |
| --- | --- | --- |
| Từ viết tắt | Từ viết đầy đủ | Ý nghĩa |
| CF | Classifier | Bộ phân loại |
| AM | Agent Manager | Bộ quản lý tác nhân |
| NM | Network Monitor | Bộ giám sát mạng |
| EM | End-user Manager | Bộ quản lý người dùng |
| AZ | Analyzer | Bộ phân tích |



Hình 6: Kịch bản phát hiện tấn công APT tại các giai đoạn 1, 3, 4, 5, 6

*Bước 1: Kịch bản phát hiện tấn công APT tại các giai đoạn (1, 3, 4, 5, 6) – Hình 7*

1. AM -> NM: Gửi thông tin đường truyền mạng

AM thu thập dữ liệu từ các tác nhân mạng và chuyển tới Network Manager

1. NM: Thực hiện phân tích đường truyền mạng

NM phân tích bằng nhiều cách thức như chữ ký mạng, tần số mạng và Whitelist

1. NM -> CF: Gửi thông tin những đường truyền nghi vấn

Khi thành phần Traffic Analysis của NM phát hiện đường truyền nghi vấn, nó sẽ được gửi quan CF

1. CF: Phân loại các đường truyền nghi vấn

Khi CF và AM phát hiện đường truyền có nghi vấn thì hệ thống sẽ được cảnh báo có tấn công APT xảy ra.

*Bước 2: Kịch bản phát hiện tấn công APT tại giai đoạn (3) – Hình 8*

1. AM -> NM: gửi các Email hoặc Web traffic

Email từ mỗi Agent và dữ liệu Network Traffic được chuyển giao từ AM

1. NM -> AZ: gửi các file nghi vấn

NM thực hiện phân tích đường truyền. Khi phát hiện bất kỹ sự kiện bất thường nó sẽ trích xuất file trong đường truyền và chuyển tới bộ AZ

1. AZ: thực hiện phân tích file

Một cách tổng quan, AZ thực hiện phân tích file bằng phân tích tĩnh và động

1. AZ -> CF: gửi file đã được xác định là có mã độc

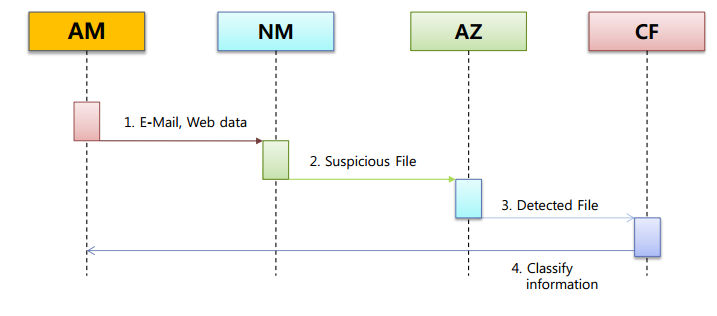
Thông tin file đã xác định có mã độc này sẽ được gửi tới bộ phân loại CF

1. CF: phân loại file

CF: Phân loại file theo mức độ cảnh báo Risk level hoặc Alert level

1. CF -> AM: gửi thông tin

Khi đường truyền và các file trên được phân loại nguy hiểm. Hệ thống sẽ được cảnh báo có tấn công APT



Hình 7: Kịch bản phát hiện tấn công APT tại giai đoạn 2

## **3.3 Một số trường hợp áp dụng cụ thể**

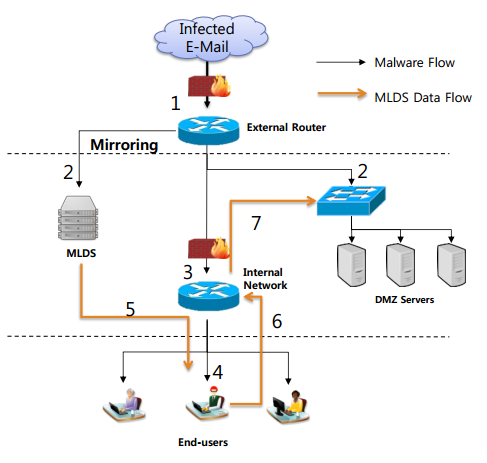
Chúng ta sẽ giả định 2 trường hợp tấn công APT và cách phòng thủ với hệ thống phòng thủ đa tầng:

Trường hợp 1: Thực hiện việc phát hiện và ngăn chặn hình thức Spear Phishing người dùng

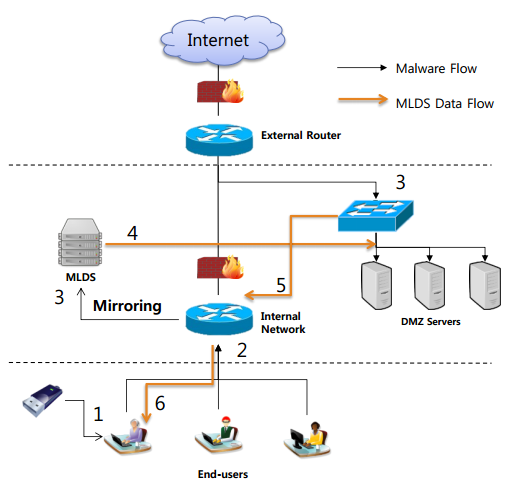
Ở bước ban đầu các email có chứa mã độc xâm nhập vào các router nội bộ. Sau đó mã độc thực hiện công việc tìm kiếm và lây lan các mục tiêu trong hệ thống mạng từ Router nội bộ sang DMZ server và một bản ảnh của mã độc sẽ được chuyển sang hệ thống phòng thủ APT và được phân tích. Trong trường hợp này khi người dùng đọc các email độc hại, các email này sẽ dịch chuyển tới router nội bộ và người dùng. Theo đó, các người dùng sẽ download mã độc được gắn kèm hoặc truy cập vào các link độc hại. Mỗi khi email được lưu hành trong hệt thống mạng, Log file luôn được chuyển tới hệ thống phòng chống APT để tiếp tục phân tích và sẽ truy vết các thiết bị nhiễm mã độc và tiến hành gỡ bỏ các mã độc này

Trường hợp 2: Thực hiện việc phát hiện và ngăn chặn mã độc lây nhiễm từ USB của người dùng

Khi mã độc lây nhiễm qua USB người dùng, mã độc sẽ cố gắng tìm kiếm và lây lan ra các máy người dùng khác trong hệ thống. Khi mã độc tìm thấy DMZ server để lây nhiễm qua đó hệ thống phòng chống APT sẽ phát hiện và thông báo thông tin log về định danh mã độc. Hệ thống sẽ bóc gỡ mã độc trên các thiết bị lây nhiễm.



Hình 8: Ngăn chặn Spear Phishing người dùng



Hình 9: Ngăn chặn lây nhiễm mã độc qua USB người dùng

# **4.Cài đặt thử nghiệm hệ thống chống tấn công APT đa tầng**