

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. TRẦN ĐỨC SỰ, ThS. PHẠM MINH THUẬN

GIÁO TRÌNH
PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH

HÀ NỘI, 2013

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. TRẦN ĐỨC SỰ, ThS. PHẠM MINH THUẦN

GIÁO TRÌNH
PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH

HÀ NỘI, 2013

MỤC LỤC

Mục lục	i
Danh mục từ viết tắt.....	iv
Danh mục hình vẽ.....	v
Lời nói đầu	vii
Chương 1 Tội phạm máy tính	1
1.1 Khái niệm tội phạm máy tính.....	1
1.2 Lịch sử tội phạm máy tính	4
1.2.1 Tội phạm máy tính những năm 1990	11
1.2.2 Tội phạm máy tính của thế kỷ 21	16
1.2.3 Tội phạm máy tính trong thời điểm hiện tại.....	20
1.3 Các nguy hại xảy đến từ tội phạm máy tính	22
1.3.1 Nguy hại đối với cá nhân	22
1.3.2 Nguy hại đối với tổ chức	29
1.4 Các dạng tội phạm máy tính	31
1.4.1 Đánh cắp định danh.....	31
1.4.1.1 Giả mạo	32
1.4.1.2 Tấn công hoặc sử dụng phần mềm gián điệp	33
1.4.1.3 Truy cập trái phép dữ liệu.....	35
1.4.1.4 Dựa vào thông tin rác.....	36
1.4.2 Rình rập, quấy rối.....	37
1.4.3 Truy cập bất hợp pháp tới hệ thống máy tính và các dữ liệu nhạy cảm	39
1.4.4 Lừa đảo trực tuyến.....	39
1.4.4.1 Lừa đảo đầu tư	40
1.4.4.2 Lừa đảo giao dịch trực tuyến	41
1.4.4.3 Lừa đảo nhận/ chuyển tiền.....	42
1.4.4.4 Vi phạm bản quyền dữ liệu.....	42
1.4.5 Phát tán tin rác, mã độc hại	42
Chương 2 Một số hành vi của tội phạm máy tính.....	44
2.1 Trộm cắp thông tin	44
2.1.1 Giả mạo	44

2.1.2	Sử dụng phần mềm gián điệp.....	46
2.2	Phát tán mã độc hại	49
2.3	Lừa đảo.....	50
2.3.1	Lừa đảo thông qua giao dịch	51
2.3.2	Lừa đảo thông qua lôi kéo đầu tư kinh doanh bất hợp pháp.....	54
2.4	Tấn công trái phép.....	55
2.4.1	Tấn công thăm dò	55
2.4.2	Tấn công hệ thống và các thiết bị mạng.....	61
2.4.3	Tấn công cơ sở dữ liệu và ứng dụng Web.....	63
Chương 3 Các phương pháp điều tra tội phạm máy tính		65
3.1	Cơ sở pháp lý khi điều tra tội phạm máy tính.....	65
3.2	Các bước thực hiện điều tra	66
3.2.1	Quan sát, bảo vệ hiện trường vụ án.....	66
3.2.2	Ghi và lập tài liệu về hiện trường.....	67
3.2.3	Bảo quản chứng cứ.....	70
3.2.4	Tiến hành điều tra.....	72
3.2.5	Lập tài liệu báo cáo	72
3.3	Thu thập và phân tích chứng cứ từ các linh kiện phần cứng	72
3.4	Thu thập và phân tích chứng cứ từ mạng.....	74
3.4.1	Phân tích gói tin.....	75
3.4.2	Phân tích thống kê lưu lượng	76
3.5	Thu thập và phân tích chứng cứ từ hệ thống.....	77
3.5.1	Từ trình duyệt, nhật ký trò chuyện.....	77
3.5.1.1	Tìm kiếm bằng chứng trong các trình duyệt.....	77
3.5.1.2	Tìm kiếm chứng cứ trong nhật ký trò chuyện	80
3.5.2	Từ các file log hệ thống.....	80
3.5.2.1	Windows Log.....	80
3.5.2.2	Linux log.....	82
3.5.3	Phục hồi các dữ liệu đã bị xóa.....	84
3.5.3.1	Phục hồi tập tin từ hệ điều hành Windows	85
3.5.3.2	Phục hồi tập tin từ hệ điều hành Unix/ Linux.....	88
3.5.4	Vị trí quan trọng cần kiểm tra	90

3.5.4.1	Trong Windows	90
3.5.4.2	Trong Linux	91
3.5.5	Các tiện ích hệ điều hành	91
3.6	Thu thập và phân tích chứng cứ từ nguồn khác	94
3.6.1	Truy tìm địa chỉ IP.....	94
3.6.2	Chứng cứ từ Email	98
3.6.3	Chứng cứ từ các thiết bị mạng	101
3.6.4	Chứng cứ từ điện thoại di động.....	103
3.6.5	Chứng cứ từ tường lửa	104
3.6.6	Chứng cứ từ hệ thống phát hiện xâm nhập	106
Chương 4 Phòng chống tội phạm máy tính		110
4.1	Sử dụng kỹ thuật, công nghệ.....	110
4.1.1	Tường lửa	110
4.1.2	Hệ thống IDS/IPS	112
4.1.3	Ngăn chặn mã độc hại	114
4.1.4	Mã hóa.....	117
4.1.5	Các kỹ thuật, công nghệ khác.....	117
4.2	Sử dụng quy định, luật pháp	118
4.3	Nâng cao nhận thức người sử dụng	120
4.4	Các biện pháp khác	123
Tài liệu tham khảo.....		125
Phụ lục		126

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Chú giải tiếng Anh	Chú giải tiếng Việt
IT	Information Technology	Công nghệ thông tin
FBI	Federal Bureau of Investigation	Cục Điều tra Liên bang
ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
DDoS	Distributed Denial of Service	Từ chối dịch vụ phân tán
DNS	Domain Name System	Hệ thống tên miền
SMTP	Simple Mail Transfer Protocol	Giao thức truyền tải email đơn giản
FTC	Federal Trade Commission	Ủy ban Thương mại Liên bang
CNTT		Công nghệ thông tin
IP	Internet Protocol	Giao thức Internet
SQL	Structured Query Language	Ngôn ngữ truy vấn có cấu trúc
ID	Identification	Định danh
IOCE	International Organization on Computer Evidence	Tổ chức quốc tế về Bằng chứng máy tính
ECPA	Electronic Communications Privacy Act	Đạo luật Bảo mật truyền thông điện tử
SOP	Standard Operating Procedure	Quy trình hoạt động chuẩn

DANH MỤC HÌNH VẼ

Hình 1.1. Lừa đảo trực tuyến qua Email	32
Hình 2.1. Cài đặt phần mềm gián điệp qua email	47
Hình 2.1. Quét cổng sử dụng FreePortScanner.....	59
Hình 2.2. Phân tích mạng với công cụ Baseline Security Analyzer	60
Hình 2.3. Kết quả thu được từ công cụ Baseline Security Analyzer	61
Hình 3.1. Tài liệu về hình ảnh.....	68
Hình 3.2. Tài liệu các chuỗi hành trình.....	70
Hình 3.3. Công cụ Wireshark.....	76
Hình 3.4. Lịch sử trình duyệt Internet Explorer.....	78
Hình 3.5. Lịch sử trình duyệt Mozilla Firefox	79
Hình 3.6. Thanh địa chỉ của trình duyệt.....	79
Hình 3.7. Cửa sổ Event Viewer.....	81
Hình 3.8. Recycle Bin	85
Hình 3.9. UndeletePlus.....	86
Hình 3.10. Lựa chọn ổ đĩa Disk Digger.	87
Hình 3.11. Tìm kiếm trên DiskDigger	87
Hình 3.12. Tìm kiếm tập tin trên DiskDigger	88
Hình 3.13. Tiện ích Netstat	92
Hình 3.14. Lệnh fc.....	92
Hình 3.15. Tiện ích Recover	93
Hình 3.16. Tiện ích ps	93
Hình 3.17. Lệnh Tracert	95
Hình 3.18. Tìm kiếm với Whois	96
Hình 3.19. Tìm kiếm giải pháp mạng với Whois.....	96
Hình 3.20. Tìm kiếm với Visual Route.....	97
Hình 3.21. Tìm tiêu đề Yahoo! E-mail	98
Hình 3.22. Xem thông tin đầy đủ tiêu đề Yahoo! E-mail full	98
Hình 3.23. eMailTrackerPro trong Outlook.....	99
Hình 3.24. eMailTrackerPro trace.....	99
Hình 3.25. Mở một file .pst	100
Hình 3.26. Xem e-mail	100

Hình 3.27. Ghi dữ liệu với Hyper Terminal.....	102
Hình 3.28. Nhật ký tường lửa CheckPoint.....	105
Hình 3.29. Phân tích nhật ký tường lửa	105
Hình 3.30. Nhật ký thu được từ Snort.....	107
Hình 4.1. Mô hình phòng chống mã độc hại.....	114

LỜI NÓI ĐẦU

Ngày nay công nghệ thông tin và Internet đang chiếm một vị trí quan trọng trong mọi lĩnh vực của đời sống xã hội. Sự bùng nổ của khoa học công nghệ nói chung và công nghệ thông tin nói riêng đã đem lại rất nhiều lợi ích cho con người, rút ngắn khoảng cách giao tiếp, tiết kiệm thời gian, chi phí và công sức. Tuy nhiên song song cùng với những thành tựu to lớn đó thì những rắc rối mà nó đem lại cũng không nhỏ. Môi trường Internet dần dần trở thành môi trường cho các cuộc chiến tranh không gian số, nơi mà các hacker thực hiện các cuộc tấn công nhằm đánh cắp tài khoản người dùng, truy cập bất hợp pháp, lừa đảo trực tuyến, gây nên những hậu quả vô cùng nghiêm trọng. Chính vì thế, vấn đề an toàn bảo mật thông tin, phát hiện và phòng chống tội phạm mạng đang được các cơ quan, tổ chức và chính phủ ưu tiên hàng đầu.

Giáo trình “Phòng chống và điều tra tội phạm máy tính” được xây dựng nhằm mục đích cung cấp các khái niệm, kiến thức cơ bản về tội phạm máy tính và các phương pháp, kỹ năng phục vụ trong việc phân tích, điều tra và phòng chống tội phạm máy tính.

Nội dung giáo trình gồm 4 chương, trong đó:

Chương 1: Tội phạm máy tính

Chương này cung cấp các khái niệm tổng quan về tội phạm máy tính, lịch sử tội phạm máy tính, các nguy hại xảy đến đối với tội phạm máy tính và các dạng tội phạm máy tính điển hình.

Chương 2: Một số hành vi của tội phạm máy tính

Chương này cung cấp các kiến thức về những hành vi của tội phạm máy tính như: trộm cắp thông tin, phát tán mã độc, lừa đảo, tấn công trái phép. Từ đó học viên có thể hiểu và nắm được các hành vi của tội phạm máy tính thường sử dụng hiện nay.

Chương 3: Các phương pháp điều tra tội phạm máy tính

Chương này cung cấp các kiến thức và kỹ năng để điều tra tội phạm máy tính từ cơ sở pháp lý cho tới quy trình thực hiện và cụ thể các vấn đề cần thực hiện khi tiến hành điều tra tội phạm máy tính.

Chương 4: Phòng chống tội phạm máy tính

Chương này cung cấp các kiến thức nhằm phục vụ mục đích phòng chống tội phạm máy tính như: sử dụng kỹ thuật, công nghệ, pháp luật, nâng cao nhận thức người dùng,

Giáo trình này được viết lần đầu tiên và trong thời gian ngắn, do đó chắc chắn sẽ còn nhiều khiếm khuyết về nội dung cũng như phương pháp thể hiện. Chúng tôi rất mong nhận được những ý kiến đóng góp của các đồng nghiệp và các bạn đọc, sinh viên để giáo trình tiếp tục hoàn thiện.

Hà nội, tháng 10 năm 2013

Nhóm biên soạn

Chương 1

TỘI PHẠM MÁY TÍNH

1.1 KHÁI NIỆM TỘI PHẠM MÁY TÍNH

Trước khi nói về khái niệm tội phạm máy tính, ta cần phân biệt “Tội phạm công nghệ cao” và “Tội phạm máy tính”.

Từ điển Bách khoa Công an nhân dân Việt Nam nêu khái niệm tội phạm công nghệ cao là: “Loại tội phạm sử dụng những thành tựu mới của khoa học – kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện để thực hiện hành vi phạm tội một cách cố ý hoặc vô ý, gây nguy hiểm cho xã hội. Chủ thể của loại tội phạm này thường là những người có trình độ học vấn, chuyên môn cao, có thủ đoạn rất tinh vi, khó phát hiện. Hậu quả do loại tội phạm này gây ra không chỉ là thiệt hại lớn về mặt kinh tế, xã hội mà nó còn xâm hại lớn tới an ninh quốc gia.”

Theo tổ chức Cảnh sát hình sự quốc tế INTERPOL thì khái niệm tội phạm công nghệ cao là “Loại tội phạm sử dụng, lạm dụng những thiết bị kỹ thuật, dây chuyền công nghệ có trình độ công nghệ cao như một công cụ, phương tiện để thực hiện hành vi phạm tội...”. Trong các dạng của tội phạm công nghệ cao có 2 dạng chính, đó là tội phạm máy tính (computer crime) và tội phạm công nghệ thông tin- điều khiển học (cyber crime). Việc xác định hành vi phạm tội, mức độ phạm tội và mức hình phạt ở các nước trên thế giới có sự khác nhau tùy thuộc vào hệ thống pháp luật mà nước đó đang áp dụng.

Theo Bộ tư pháp Mỹ thì khái niệm tội phạm công nghệ cao là “bất cứ hành vi vi phạm pháp luật hình sự nào có liên quan đến việc sử dụng các hiểu biết về công nghệ máy tính trong việc phạm tội”.

Theo các chuyên gia về tội phạm học ở Việt Nam thì khái niệm tội phạm máy tính công nghệ cao được sử dụng với nội hàm gồm hai nhóm tội phạm:

Nhóm thứ nhất: Tội phạm công nghệ cao là các tội phạm mà khách thể của tội phạm xâm hại đến hoạt động bình thường của máy tính và mạng máy tính được quy định tại các Điều 224, 225, 226 Bộ luật Hình sự nước Cộng hòa XHCN Việt Nam năm 1999.

Nhóm thứ hai: Tội phạm sử dụng công nghệ cao gồm các tội phạm truyền thống được quy định trong Bộ luật Hình sự nước cộng hòa XHCN Việt Nam 1999, khi thực hiện hành vi phạm tội, người phạm tội sử dụng các công cụ làm công cụ, phương tiện thực hiện hành vi phạm tội.

Như vậy, có thể thấy mọi “Tội phạm máy tính” đều là “Tội phạm sử dụng công nghệ cao”. Dựa trên các quan điểm trên và dựa trên bộ luật hình sự năm 1999 sửa đổi năm 2009, ta có khái niệm về tội phạm máy tính như sau:

“Tội phạm máy tính là hành vi vi phạm pháp luật hình sự do người có năng lực trách nhiệm hình sự sử dụng máy tính để thực hiện hành vi phạm tội, lưu trữ thông tin phạm tội hoặc xâm phạm đến hoạt động bình thường và an toàn của máy tính, hệ thống mạng máy tính”.

Các loại tội phạm máy tính công nghệ cao chủ yếu là: đánh cắp tiền trong tài khoản ngân hàng, lừa đảo trong thanh toán, đánh cắp dữ liệu trái phép, phát tán virus... Có thể nói công nghệ thông tin có vai trò, mức độ nhất định trong việc thực hiện, che giấu và gây ra những hậu quả nguy hiểm cho xã hội. Nhìn một cách tổng thể đối với loại tội phạm công nghệ cao, chúng ta thấy công nghệ thông tin (máy tính và mạng máy tính) đóng một số vai trò quan trọng trong quá trình phạm tội. Dưới góc độ như là khách thể, hiểu theo nghĩa thông thường máy tính và các thiết bị có liên quan là một loại tài sản có giá trị, do vậy nó trở thành đối tượng của các tội phạm về xâm phạm quyền sở hữu như trộm, cướp hay phá hoại tài sản. Hiểu theo một góc độ phức tạp hơn, máy tính với vai trò khách thể còn được thể hiện trong việc tội phạm cố tình phá hoại hay ăn cắp chúng nhằm xóa bỏ hoặc lấy cắp các thông tin mà nó chứa đựng. Dưới góc độ là công cụ phạm tội, máy tính và mạng máy tính với những khả năng ưu việt ngày càng được các loại tội phạm khác nhau sử dụng

để thực hiện các hình thức phạm tội truyền thống như đánh bạc, tội lừa đảo... hoặc sử dụng máy tính làm trung gian chuyển tiền bất hợp pháp phục vụ cho các mục đích phi pháp khác.

Tiếp cận trên phạm vi rộng, thì việc phân loại thế nào là tội phạm công nghệ cao cần dựa trên vai trò của công nghệ thông tin. Theo quan điểm này thì tội phạm máy tính công nghệ cao gồm những tội phạm có sự liên quan của máy tính với ba vai trò sau: sử dụng máy tính, mạng máy tính làm mục đích của tội phạm; làm công cụ phạm tội; là vật trung gian để cất giấu, lưu trữ, phát tán những tư tưởng đối lập, tuyên truyền thông tin đồn nhảm thất thiệt, tuyên truyền văn hóa phẩm độc hại, đồi trụy...

Tiếp cận trên phạm vi hẹp, có nhà nghiên cứu cho rằng tội phạm máy tính công nghệ cao chỉ là tội phạm thực hiện và gây hậu quả trên môi trường ảo, thế giới ảo do thành tựu của khoa học công nghệ thông tin mang lại và nó hoàn toàn khác với các loại tội phạm truyền thống trước kia. Bộ luật hình sự năm 1999 đã tiếp cận quan điểm này. Tuy nhiên, Bộ luật Hình sự 1999 chỉ mới đề cập đến 3 tội danh có liên quan đến máy tính (Điều 224, 225, 226 BLHS năm 1999). Trên thế giới hiện nay đã xuất hiện thêm nhiều hành vi khác được coi là tội phạm máy tính công nghệ cao hiểu theo nghĩa hẹp như: tội đột nhập với mật khẩu ăn cắp; sao chép bất hợp pháp các chương trình phần mềm; tội đe dọa tấn công hệ thống máy tính... Phương pháp tiếp cận theo phạm vi hẹp này tuy có ưu điểm là định rõ được tội danh cần xử lý nhưng lại có nhược điểm là rất dễ bỏ sót tội phạm, nhất là trong bối cảnh công nghệ thông tin đang phát triển mạnh mẽ trong thời gian qua. Một ví dụ điển hình là hiện nay trên thế giới cũng như ngay tại Việt Nam đang tranh cãi về việc có coi hành vi trộm cắp, lừa đảo tài sản mà người chơi (các game thủ) có được khi chơi trò chơi trực tuyến hay không (trò chơi Võ lâm truyền kỳ ở Việt Nam là một điển hình, game thủ có thể sở hữu những chiếc áo giáp, kiếm... nếu đánh thắng đối thủ trong trò chơi). Nếu nhìn dưới góc độ thế nào là tài sản theo quy định pháp luật hiện hành thì các “tài sản ảo” này hoàn toàn không có giá trị vì nó thực chất không phải là tài sản thực mà chỉ là sản phẩm được tạo ra trong thế giới ảo do những người xây dựng trò chơi trực tuyến nghĩ ra và xây dựng lên thông qua phần mềm máy tính. Tuy nhiên, nếu xét dưới góc độ các tài sản này do game thủ đã bỏ ra nhiều công sức để tạo lập

được, cùng với tính chất có thể “chiếm hữu, sử dụng và định đoạt” và đặc biệt tài sản này có thể quy đổi sang giá trị thực (có thể bán lại cho người chơi khác với giá tiền rất cao) thì chúng lại thực sự cần được coi là một tài sản thực và cần được pháp luật bảo vệ trước các hành vi lừa đảo, trộm cắp như đối với các tài sản hữu hình khác.

1.2 LỊCH SỬ TỘI PHẠM MÁY TÍNH

Để có thể hiểu rõ hơn về tội phạm máy tính, chúng ta cần đi tìm hiểu về lịch sử tội phạm máy tính. Bởi lẽ khi biết được lịch sử thì từ đó chúng ta mới có một cái nhìn toàn diện về những gì xảy ra trong quá khứ và cho tới hiện tại đang tiếp diễn như thế nào. Trong phần này, chúng ta sẽ xem lại lịch sử phát triển của tội phạm máy tính. Chúng ta sẽ xem xét sự phát triển của tội phạm máy tính trong vài thập kỷ qua và có một cái nhìn tổng quan về tội phạm máy tính trong thời điểm hiện tại.

Tội phạm máy tính đầu tiên **xuất hiện từ các năm 1960 và 1970**. Phần lớn các sự cố thực sự chỉ là **trò đùa chơi trên hệ thống máy tính tại các trường đại học của sinh viên ham học hỏi**. Sự cố xảy ra với ít thiệt hại, thực sự là có vài luật lệ chống lại hoạt động này, vì vậy có nghĩa là họ không phải tội phạm. Toàn bộ **mục đích của hacker trong thời kỳ đó chỉ đơn giản là để hiểu một hệ thống**.

Lý do chính có ít tội phạm máy tính trong giai đoạn này là do có **ít sự tiếp cận rộng rãi với máy tính và mạng**. Trong thời kỳ tiền sử của tội phạm máy tính, không có quyền truy cập rộng rãi vào mạng, không có Internet, và không có luật liên quan đến hoạt động máy tính. Trong thực tế, **những người có thể truy cập vào máy tính và mạng thường là các giáo sư, sinh viên và nhà nghiên cứu**.

Khi Internet phát triển và truyền thông trực tuyến trở nên phổ biến hơn, tội phạm máy tính cũng phổ biến hơn. Trước đây, có một vài phương thức chuyển dữ liệu từ điểm A đến điểm B. Bài báo đầu tiên về chuyển mạch gói là của Leonard Kleinrock tại MIT vào năm 1961. Bây giờ, điều này có vẻ là một chủ đề khá phức tạp đối với cuốn sách về tội phạm máy tính. Tuy nhiên, tội phạm máy tính thường xuyên liên quan đến việc theo dõi các gói tin gốc của chúng. Cho dù đó là một truy tìm một email sử dụng trong spam lừa đảo, theo

dõi một ai đó đã đột nhập vào một máy chủ ngân hàng, hoặc chứng minh nguồn gốc của hành vi quấy rối email, khả năng theo dõi các gói tin là chìa khóa để điều tra tội phạm máy tính. Trong các chương sau, khi chúng ta thảo luận về kỹ thuật điều tra, chúng ta sẽ thấy rõ hơn về vấn đề này. Bây giờ, điều quan trọng là nhận ra sự quan trọng của chuyển mạch gói cho tất cả các thông tin liên lạc Internet. Một gói về cơ bản là một đơn vị dữ liệu. Các gói tin sẽ có một tiêu đề xác định điểm nguồn, điểm đến và những loại gói tin như là email, trang web... Khi các kỹ thuật chuyển mạch gói được thiết lập, mạng lưới rộng khắp là bước logic tiếp theo. Ngày nay, Internet phổ biến, hiếm thấy một doanh nghiệp mà không có trang web hoặc một cá nhân không có một tài khoản email. Tuy nhiên, đây là một hiện tượng tương đối mới. Chúng ta hãy dành một thời gian ngắn nhìn lại lịch sử của Internet và làm thế nào mà nó đã phát triển với mạng truyền thông toàn cầu lớn như ngày nay.

Internet thực sự đã bắt đầu như là một dự án nghiên cứu được gọi là ARPANET (ARPA là Advanced Research Projects Agency, một phần của Bộ Quốc Phòng Mỹ). **Năm 1969**, mạng lưới chỉ bao gồm **bốn node: Đại học Utah, Đại học California tại San Barbana, Đại học California tại Los Angeles, và Đại học Stanford**. Mười hai năm sau, vào **năm 1981**, mạng đã tăng lên đến **213 node**, số lượng không đáng kể so với hàng triệu người dùng Internet chúng ta có ngày hôm nay. Và thời đó, 213 node chỉ đơn giản là các **viện nghiên cứu, trường đại học và cơ quan chính phủ**. Trong những ngày đầu, tội phạm máy tính khá hiếm. Không có Internet để sử dụng, và ARPANet mới sinh ra chỉ có thể truy cập vào một nhóm người dùng nhỏ, tất cả những người tham gia vào nghiên cứu. **Năm 1979, CompuServe đã trở thành dịch vụ email thương mại đầu tiên**. Nhưng thậm chí sau đó, thư điện tử không được sử dụng rộng rãi và không ai nghĩ rằng có thể sử dụng nó cho các mục đích phạm tội.

Tuy nhiên, sự ra đời của các tài khoản email thương mại cũng là một đánh dấu quan trọng trong lịch sử tội phạm máy tính. Sẽ không cường điệu khi nói rằng việc tiếp cận email phổ biến là động lực đằng sau sự tăng trưởng của Internet. Trong khi xâm nhập vào mạng máy tính là cực kỳ hiếm hoi trong khoảng thời gian này, nhưng chúng ta không thể không nói về **xâm nhập vào hệ thống điện thoại**. Sự kiện đầu tiên của một hệ thống điện thoại bị tấn công

là trong đầu những năm 1970. John Draper, một cựu kỹ sư của Không quân Mỹ, sử dụng một chiếc còi đồ chơi tặng kèm trong hộp ngũ cốc Cap'n Crunch để hack vào đường dây điện thoại và thoải mái thực hiện các cuộc gọi “miễn phí”.. Draper vô tình nhận ra rằng chiếc còi tạo ra một âm thanh có tần số giống hệt tần số tín hiệu cuộc gọi trên đường dây điện thoại. Nhờ đó mà ông ta đã có thể điều khiển cuộc gọi tiếp tục được diễn ra mà người nghe vẫn tưởng rằng là cuộc gọi đã kết thúc rồi.

Năm 1972, Draper bị phát hiện khi **hãng điện thoại “nhìn thấy sự bất thường” trong hóa đơn tiền điện thoại** của ông. Sau đó Draper bị kết án 2 tháng tù giam. Trường hợp này khá thú vị bởi nó làm nổi bật lên tình trạng tội phạm liên quan đến máy tính trước cả Internet. Vụ tấn công của Draper đã sinh ra một thuật ngữ “*Phreaking*”. Nghĩa của thuật ngữ này trong xã hội của chúng ta ngày nay là “**tấn công vào các hệ thống viễn thông**”. John Draper là một trong những hacker nổi tiếng, và từ đó đã trở thành một nhà tư vấn bảo mật máy tính.

Trường hợp của ông John Draper cũng cho thấy bản chất thực của hacker. **Để hack một hệ thống, cần phải hiểu một cách toàn diện về hệ thống đó.** Ông Draper đã có thể làm ảnh hưởng đến hệ thống thoại vì kiến thức bao quát về hệ thống thoại. Ngày nay, người ta thường có thể tìm thấy các tiện ích trên Internet để có thể thực hiện hacking. Nhưng **để thực sự hack được một hệ thống đòi hỏi một chiều sâu và bề rộng về kiến thức.**

Trong thời kỳ đầu của hacking, không phải là không phổ biến những người đã bị kết án về tội phạm máy tính để sau này trở thành một nhà tư vấn bảo mật máy tính. Lý do là người này biết rõ làm thế nào để thỏa hiệp hệ thống và hỗ trợ như thế nào trong việc đảm bảo hệ thống.

Lừa đảo thoại đã trở nên khá phổ biến. Khét tiếng là vụ **Abbie Hoffman xây dựng hệ thống lừa đảo thoại John Draper**. Hoffman đưa ra kỹ thuật của Draper và đưa ra những lỗ hổng của hệ thống. **Hoffman bắt đầu một bản tin cho thấy người ta làm thế nào để thỏa hiệp hệ thống thoại và thực hiện cuộc gọi đường dài miễn phí.** Ông cảm thấy rằng thực hiện cuộc gọi đường dài không mất phí không phải trộm cắp và tội phạm. Ông tuyên bố rằng việc đang được sử dụng không phải là một tài nguyên bị đánh cắp,

nhưng nguồn tài nguyên công cộng không giới hạn bất cứ ai truy cập. Ông muốn đảm bảo các kỹ thuật để truy cập vào tài nguyên phổ biến rộng rãi.

Song song với các tội phạm về điện thoại, thời điểm này tội phạm liên quan đến máy tính cũng phát triển và bắt đầu được chú ý. Chúng ta sẽ xem một số ví dụ sau đây:

1970 – Tại đại học Wisconsin, một quả bom được kích nổ, làm chết một người và làm bị thương hơn ba người. Vụ nổ cũng phá hủy 16 triệu đô la dữ liệu máy tính được lưu trữ trên trang web.

1970 – Tại đại học New York, một nhóm sinh viên nơi nổ bom trên một máy tính ủy ban năng lượng nguyên tử. Sự cố này đã được kết nối với một nỗ lực để giải phóng một Black Panther bị cầm tù.

1973 – Tại Melbourne, Úc, những người biểu tình chống lại sự tham gia của Hoa Kỳ tại Việt Nam đã bắn vào hệ thống máy tính của một công ty của Mỹ bằng một khẩu súng hai nòng.

1978 – Tại căn cứ không quân Vandenberg ở California, một người biểu tình đã phá hủy một máy tính IBM mà không sử dụng nhiều công cụ khác nhau giống như một cuộc biểu tình chống lại hệ thống dẫn đường cho vệ tinh NAVSTAR. Những người biểu tình đã lo ngại rằng hệ thống định vị được thiết kế để cung cấp cho Hoa Kỳ một cơ hội đầu tiên của cuộc đình công.

Một số nguồn tin xem xét tất cả các ví dụ về tội phạm máy tính. Tuy nhiên, trong mỗi trường hợp, nó là phần cứng máy tính đã bị hư hỏng, dữ liệu không phải là mục tiêu cụ thể, cũng không phải là một máy tính được sử dụng để thực hiện hành vi phạm tội.

Năm 1981 là một năm bản lề trong lịch sử tội phạm máy tính. Năm đó, lan Murphy đã bị bắt vì hắn và ba kẻ đồng lõa đột nhập vào hệ thống AT & T thay đổi thời gian bên trong hệ thống. Sự thay đổi này có vẻ tầm thường, nhưng nó đã có tác động đáng kể. Murphy có một điểm khác biệt là người đầu tiên bị kết án như là một tội phạm máy tính. Và hắn bị kết án 1000 giờ lao động công ích cùng 30 tháng quản chế. Mục tiêu cuối cùng của hắn ta là làm gián đoạn hoạt động bình thường của hệ thống điện thoại. Thông thường, các hacker có tay nghề cao sẽ sử dụng kỹ thuật đơn giản, dựa trên sự hiểu biết chi tiết về hệ thống máy tính đang hoạt động. Trong trường hợp này, **thủ phạm**

đã nhận ra vai trò quan trọng trong hệ thống thời gian phát. Ví dụ này cho thấy hacker thực sự đòi hỏi một kiến thức toàn diện về hệ thống đích. Sẽ thành công hơn để bắt tội phạm máy tính nếu có sự thành thạo về phần cứng và phần mềm máy tính.

1981 không chỉ là năm bắt giữ được tội phạm máy tính đầu tiên, nó cũng là năm đánh dấu lịch sử của virus máy tính. Các virus đầu tiên được biết đến rộng rãi trong tự nhiên như là **Apple I, II, và III**, được khám phá đầu tiên vào năm 1981. Những loại **virus nhắm vào hệ điều hành Apple II và lan rộng ra các hệ thống trường đại học Texas A&M** thông qua trò chơi máy tính vi phạm bản quyền. **Vụ việc này thực sự thú vị bởi nó thực sự liên quan đến 2 loại tội phạm:** Tội đầu tiên là việc phát hành thực tế của các virus máy tính, thứ hai là thực tế nhiều nạn nhân của virus đã trở thành nạn nhân thông qua các hoạt động phạm tội của mình, hành vi trộm cắp dữ liệu thông qua vi phạm bản quyền phần mềm. Thực tế cho đến **ngày nay vẫn còn các phần mềm vi phạm bản quyền, tải nhạc bất hợp pháp, và các trang web bất hợp pháp là những điểm nóng để tìm virus và phần mềm gián điệp.** Điều này chắc chắn không có nghĩa ám chỉ rằng mọi người bị một loại virus tham gia vào hoạt động phạm tội của mình. Nhưng cũng giống như tội phạm truyền thống, khi ai thường lui tới khu vực nhiều tội phạm, cũng có khả năng trở thành nạn nhân của tội phạm.

Các virus Apple cũng rất quan trọng vì chúng minh họa một điểm liên quan đến sản phẩm của Apple và các mục tiêu của người viết ra những virus này. Nhiều người ủng hộ của Apple thực tế là virus là khá hiếm trong giới máy tính Macintosh. Đó là sự thật hôm nay kể từ khi PCs chiếm 90% máy tính. Điều đó không đúng trong những ngày đầu, tuy nhiên, khi Apple thống trị thị trường máy tính để bàn thì Microsoft và Windows chưa bao giờ được nghe nói tới. Điều này cũng sẽ cung cấp cho bạn một số kiến thức về tư duy của người viết virus, mà tương tự như là kẻ phá hoại và tác giả graffiti. Có một mong muốn ảnh hưởng đến số lượng lớn nhất người dùng, vì vậy người viết virus có xu hướng viết virus của họ ảnh hưởng đến số lượng người dùng lớn nhất có thể. Bất kỳ nền tảng mà có một thị phần nhỏ thường có ít khả năng là mục tiêu của những người viết virus.

Năm 1983, ARPANet chuyển sang sử dụng giao thức TCP/IP để liên lạc. Tiêu chuẩn hóa này đã mở đường cho những gì sẽ trở thành Internet mà chúng ta biết đến ngày hôm nay. Nếu không có một giao thức chuẩn cho truyền thông, mạng lưới toàn cầu lan rộng sẽ không thể tồn tại. Những năm 1980 cũng đánh dấu sự ra đời nhanh chóng của Internet. Trong thập kỷ này, Internet lần đầu tiên tiếp cận với một số lượng lớn người sử dụng. Nếu không có truy cập Internet rộng rãi thì tất nhiên tội phạm máy tính sẽ không xuất hiện. Trong suốt thập niên 1980, các thông báo đã được bổ sung vào mạng Internet, bao gồm cả các trang web quốc tế như các phòng thử nghiệm CERN ở Châu Âu.

Vào năm 1987, đã có khoảng 10.000 máy chủ kết nối tới Internet. Nhưng **bước ngoặt thực sự trong việc sử dụng Internet một cách rộng rãi đi kèm với phát minh ra World Wide Web (WWW, hay Web) bởi Tim Berners-Lee vào năm 1991.** Berners-Lee là người phát minh ra các trang web. Nhiều người đã nhầm lẫn Internet với các trang web, nhưng trong khi Internet bao gồm truyền tải file, thư điện tử, và nhiều hoạt động khác, World Wide Web đề cập cụ thể đến các trang web mà ta có thể xem. Con đường mới này của truyền thông đã trở thành tâm điểm của lưu lượng truy cập Internet. Khả năng để mọi người đi đến một địa chỉ web cụ thể và truy cập thông tin hình ảnh bởi Internet đều được ưa thích và có thể tiếp cận với công chúng. Với web, cũng giống như thương mại điện tử đóng vai trò xúc tác trong sự nghiệp phát triển của Internet. **Nhiều người cho rằng nếu không có các trang web, mạng Internet sẽ không bao giờ phát triển.** Internet đã phát triển, vì vậy tội phạm liên quan đến Internet cũng phát triển theo.

Trong năm 1983, chúng ta đến với một trong những vụ bắt giữ hacker đầu tiên. Trong trường hợp này, một nhóm thanh thiếu niên, tự xưng là 414s tham chiếu đến mã vùng (Milwaukee), đã bị bắt bởi FBI và bị buộc tội đột nhập vào hệ thống máy tính. **Một trong những hệ thống mà họ đã đột nhập vào được là trung tâm Sloan Kettering Cancer và phòng thí nghiệm the Los Alamos National.** Một trong những bị cáo đã được miễn trừ truy tố để đổi lấy việc hợp tác với chính quyền, và những người khác nhận 5 năm quản chế. Trường hợp này thú vị bởi nhiều lý do. Trước hết, nó là một trong những vụ bắt giữ hacker đầu tiên. Trong thời kỳ đầu, các luật liên quan đến tội phạm

máy tính còn hạn chế, và thắng thắn thì các cơ quan thực thi pháp luật cũng thiếu chuyên môn để điều tra tội phạm máy tính. Đã có ít sự cố hacking mà ngay cả người trong cộng đồng IT cũng không nhận thức được đầy đủ về những nguy hiểm tiềm năng này. Cuối cùng, bản án đưa ra là tương đối nhẹ. Những cá nhân này đã đột nhập vào hệ thống máy tính và gây ra lượng thiệt hại lớn cho dữ liệu, nhưng hệ thống công lý hình sự lại xử lý trường hợp này như một trò đùa vô hại của tuổi trẻ.

Trường hợp này cũng gây chú ý cho các nhà điều tra. Lưu ý rằng các hacker để lại manh mối về danh tính của họ trong tên nhóm, trong trường hợp này đó là mã vùng của chúng. Với hacker mới vào nghề, chúng có thể khoe khoang trên các diễn đàn và phòng chat. Địa điểm như vậy có thể cung cấp cho điều tra viên những chứng cứ có giá trị.

Năm 1984 có thể coi là năm công khai của cộng đồng hacker. Đây là năm 2600 tạp chí hacking được xuất bản lần đầu. Các tạp chí vẫn được xuất bản định kỳ hàng quý và có rất nhiều thông tin hữu ích. 2600 tạp chí gồm nhiều bài báo về ý thức thể hệ và haking. **Nó không phải là hướng dẫn để hack mà cung cấp cái nhìn sâu sắc có giá trị về cộng đồng hacker.** Các ấn phẩm của tạp chí này đưa ra sự tồn tại và công khai hoạt động của cộng đồng hacker đã thành công. Chắc chắn sẽ là một ý tưởng tốt cho điều tra viên về tội phạm máy tính.

Năm 1986, một người đàn ông 17 tuổi tên là Herbert Zinn đã bị buộc tội tấn công vào hệ thống máy tính AT&T. Ông Zinn sau đó nhận tội. Điều làm cho tội phạm này gây được sự chú ý là sự kiện này đã diễn ra sau khi thông qua gian lận máy tính và Luật lạm dụng năm 1986. Ông Zinn, hoạt động với tên "Shadow Hawk", làm việc trong phòng của mình trong ngôi nhà của cha mẹ và lấy cắp hơn 50 chương trình máy tính. Cuối cùng ông đã bị kết án 9 tháng tù giam. Rõ ràng, án 9 tháng tù là khá nhẹ bởi ông không chỉ hack hệ thống mà còn thực sự ăn cắp dữ liệu.

Chúng ta cùng đến với một trường hợp thú vị năm 1988. Đại học Cornell, nghiên cứu sinh Robert Morris đã đưa ra một sâu lây lan sang hơn 6000 máy tính, làm tắc nghẽn mạng. Mục đích của sâu mạng là để khai thác lỗ hổng bảo mật/ lỗ hổng trong hệ điều hành Unix. Và sự lây lan của nó, gây ra thiệt hại hơn 100 triệu USD. Mặc dù theo pháp luật thì án này lên đến 5

năm tù giam và quản chế 250.000\$ tiền phạt, tuy nhiên Morris đã nhận 3 năm tù giam và 400 giờ phục vụ cộng đồng, 10.000\$ tiền phạt. Tại thời điểm này, cộng đồng pháp lý vẫn không xem tội phạm máy tính như là một vấn đề hình sự nghiêm trọng.

1989 là một năm đáng chú ý về tội phạm máy tính. Đây là năm đầu tiên công nhận rộng rãi hoạt động gián điệp không gian mạng. 5 người từ miền tây nước Đức đã bị bắt giữ do đã hack hệ thống mạng của chính phủ và ăn cắp dữ liệu và các chương trình của các trường đại học. Ba trong số năm tên đó đã bán các dữ liệu và phần mềm cho chính phủ Liên Xô. Sự cố hoạt động gián điệp này lần đầu tiên được biết đến công khai. Đây là điều hợp lý để giả định rằng việc sử dụng hệ thống máy tính cho mục đích gián điệp có trước năm 1989, và còn tiếp diễn đến ngày hôm nay.

Cũng trong năm 1989, **Kevin Mitnick, một cái tên đã trở thành gần như đồng nghĩa với hacking**, bị kết tội ăn cắp phần mềm từ tháng 12 và ăn cắp mã số đường dài từ MCI. Hắn bị kết án 1 năm tù và không được sử dụng máy tính hoặc kết hợp với các hacker khác. Có lẽ Kevin Mitnick là hacker được biết đến nhiều nhất. Cuộc sống và những khai thác của ông đã truyền cảm hứng cho một cuốn sách và các nhân vật điện ảnh. Ngày nay, Mitnick là một tác giả và là cố vấn an ninh.

1.2.1 Tội phạm máy tính những năm 1990

Nếu những năm 1980 là thập kỷ tăng trưởng của tội phạm máy tính, thì những năm 1990 là thập kỷ của quá trình chuyển đổi cho tội phạm máy tính. Những năm 1990 đánh dấu một sự thay đổi thực sự của tội phạm máy tính. Sự thay đổi đầu tiên là mức độ phổ biến của kỹ thuật hacking, điều này làm cho tội phạm máy tính phổ biến hơn. Ngoài ra, công chúng đã bắt đầu nhận thức được các khái niệm hacker, virus, và tội phạm máy tính. Thậm chí còn có phim hư cấu Hackers (1995) dường như để tôn vinh cộng đồng hacker. Sự phổ biến này của hacking, kết hợp với việc truy cập dễ dàng vào Internet khiến nhiều người trẻ tuổi có kỹ năng cơ bản quan tâm đến hack máy tính. Đồng thời, pháp luật bắt đầu xem xét tội phạm máy tính một cách nghiêm túc hơn.

Trong năm 1990, cơ quan mật vụ đưa ra “Operation Sundevil” với mục đích bắt hacker. Trong khi hoạt động này liên quan đến thực thi pháp luật địa phương cùng với 150 nhân viên mật vụ, các cuộc tấn công trong 15 tiểu bang, và thu giữ một lượng lớn thiết bị máy tính, đỉnh điểm là ba vụ bắt giữ. Sẽ mất thời gian cho các cán bộ thực thi pháp luật truyền thống học hỏi để điều tra đúng và đấu tranh chống tội phạm máy tính.

Năm 1991, Mark Abene, tên trên mạng được biết đến là “Phiber Optik”, đã bị bắt và buộc tội theo luật New York với tội giả mạo và xâm nhập vào máy tính. Các điều tra hình sự chủ yếu dựa trên các bằng chứng thu thập được khi nghe trộm các cuộc đàm thoại giữa các thành viên của một nhóm hacker gọi là Masters of Deception. Khía cạnh đáng chú ý là việc sử dụng dây nghe lén để ghi lại các cuộc hội thoại và truyền dữ liệu của máy tính hacker. Trong khi Mark Abene đang ở tuổi vị thành niên và vẫn bị bắt giữ, đã bị truy tố và lĩnh án 1 năm tù.

Năm 1989, Kevin Poulsen bị bắt với tội danh đột nhập trái phép máy tính và máy chủ điện thoại. Tuy nhiên, ngay trước khi bị đưa ra xét xử, Poulsen đã trốn thoát và thực hiện một vụ tấn công được cho là nổi tiếng nhất trong suốt “cuộc đời hacker”. Đài phát thanh KIIS-FM Los Angeles đã tổ chức một cuộc thi với giải thưởng là một chiếc xe ô tô thể thao giá trị Porsche 944-S2 cho người thứ 102 gọi điện đến đài. Poulsen đã tìm cách chiếm quyền điều khiển hệ thống chuyển mạch (switchboard line), chặn mọi cuộc gọi đến và nghiễm nhiên trở thành người giành giải thưởng nói trên. Năm 1991, Poulsen mới bị bắt tại một siêu thị ở Los Angeles.

Năm 1994, một cậu bé 16 tuổi ở Anh đã sử dụng tên “Data Stream” đã đột nhập vào nhiều hệ thống nhạy cảm, bao gồm Griffith Air Force Base, NASA, và viện nghiên cứu Nguyên tử Hàn Quốc. Tội phạm này đã được điều tra bởi Scotland Yard, cuối cùng đã bị phát hiện và bị bắt giữ. Trường hợp này khá thú vị bởi tính nhạy cảm của hệ thống mà cậu ta đột nhập vào. Nó cũng nhấn mạnh nhu cầu hợp tác quốc tế trong điều tra tội phạm máy tính. Trong trường hợp này, thủ phạm ở Châu Âu và đột nhập vào hệ thống ở Bắc Mỹ và Châu Á. Trường hợp này cho thấy thực thi pháp luật chống lại tội phạm máy tính cần có sự hợp tác giữa các cơ quan không chỉ nhà nước, địa phương, bang và liên bang, mà trên cả quy mô quốc tế.

1994 cũng là năm mà Kevin Mitnick bị nghi là đã đột nhập vào hệ thống máy tính tại Trung tâm siêu máy tính San Diego. Máy tính mà được điều hành bởi chuyên gia bảo mật Tsutomu Shimomura. Shimomura hỗ trợ FBI trong việc điều tra vào năm 1995, Mitnick bị bắt. Mitnick cuối cùng đã nhận tội hành vi này cùng với một loạt các hành vi phạm tội khác. **Trường hợp này cũng khá thú vị bởi nó liên quan đến một chuyên gia máy tính dân sự hỗ trợ cán bộ thực thi pháp luật trong việc điều tra một tội phạm máy tính.** Rõ ràng, nhiều cơ quan thực thi pháp luật quá tải với các trường hợp và thiếu nhân sự. Đôi khi việc sử dụng một nhà tư vấn bên ngoài có thể là một lợi ích lớn. Nó thậm chí còn tốt hơn nếu tình nguyện viên là các chuyên gia bên ngoài. Tuy nhiên, các cán bộ thực thi pháp luật phải cẩn thận sàng lọc các chuyên gia bên ngoài như vậy. Một cuộc điều tra lý lịch tiêu chuẩn sẽ là điều tối thiểu. Ngoài ra các cơ quan bảo vệ pháp luật cần phải có một ý tưởng rõ ràng rằng tại sao chuyên gia này tình nguyện.

Năm 1995, đánh dấu bằng việc bắt giữ Vladimir Levin, tốt nghiệp Đại học St Petersburg Tekh-nologichesky. Levin đã dẫn đầu vòng cáo buộc một nhóm tổ chức của hacker Nga. Nhóm này có ý định bỏ trộm với khoảng 10 triệu USD từ Citibank. Levin đã bị bắt bởi Interpol tại sân bay Heathrow vào năm 1995. Cuối cùng, hắn bị dẫn độ sang Mỹ, bị kết án 3 năm tù giam và phải trả Citibank 240,015\$. Trường hợp này khá quan trọng bởi nó đã chứng minh rõ ràng cả hai nhu cầu hợp tác quốc tế và hiệu quả cho biết sự hợp tác có thể đạt được không. Nếu không có sự hợp tác quốc tế, thủ phạm sẽ không bao giờ bị bắt. **Trường hợp này cũng khá thú vị bởi nó liên quan đến một máy tính được dựa trên một băng đảng có tổ chức.**

Năm 1995 cũng là năm mà FBI tạo ra Innocent Images National Initiative (IINI). Mục tiêu của việc này là để điều tra và truy tố nhóm pedophiles trực tuyến. Tại thời điểm đó, hầu hết công chúng vẫn không nhận thức được mối nguy hiểm nghiêm trọng đối với trẻ em trên Internet, nhưng pedophiles đã phát hiện ra rằng Internet là một cách phát tán khiêu dâm trẻ em. Năm sau đó, với sự ra đời của các mạng xã hội, phòng chat, và nhiều trẻ em có tài khoản email của mình, pedophiles sẽ leo thang để rình rập trẻ em trực tuyến.

Năm 1996, một hacker máy tính liên kết với một nhóm supremacist trắng tạm thời vô hiệu hóa một Massachusetts ISP và phá hỏng một phần hệ thống lưu trữ hồ sơ của ISP. ISP đã cố gắng ngăn chặn hacker từ việc gửi đi thông điệp phân biệt chủng tộc trên toàn thế giới dưới tên của ISP. Các hacker đã ký tắt với các mối đe dọa: *"Bạn chưa thấy chủ nghĩa khủng bố điện tử thực sự. Đây là một lời hứa"*. Đặc biệt tấn công này gây ra ít thiệt hại. Tuy nhiên, điều này rõ ràng là một sự cố của một cuộc tấn công dựa trên tư tưởng, và về mặt kỹ thuật mạng. Chúng ta đã thấy vào đầu những năm 1970 những người ủng hộ triệt để cho một nguyên nhân cụ thể sử dụng thiệt hại cho thiết bị máy tính làm quan điểm của họ. Vào những năm 1990, chúng ta đã bắt đầu thấy defacing trang web như một phương tiện ngày càng phát triển để truyền bá thông điệp của họ. Đến thế kỷ 21, Website defacements đã gần như trở nên phổ biến.

Những năm 1990 cũng mang lại nhiều ví dụ về chủ nghĩa khủng bố không gian mạng. Trong năm 1998, quân du kích Tamil tràn ngập đại sứ quán Sri Lanka với 800 email mỗi ngày trong vòng 2 tuần. Các tin nhắn: *"Chúng tôi là Internet Black Tigers và chúng tôi đang làm điều này để làm gián đoạn thông tin liên lạc của bạn"*. Cơ quan tình báo coi đó là cuộc tấn công đầu tiên được biết đến bởi những kẻ khủng bố chống lại hệ thống máy tính của một quốc gia. Rõ ràng, người ta có thể tranh luận về cuộc tấn công khủng bố mạng đầu tiên, sự cố này chắc chắn có tất cả các yêu cầu. Đầu tiên, đó là một cuộc tấn công không gian mạng, không chỉ đơn thuần là cuộc tấn công vật lý truyền thống được hỗ trợ bởi các nguồn tài nguyên máy tính. Thứ hai, nó rõ ràng thực hiện cho mục đích chính trị. Cuối cùng, nó là một phần của một cuộc xung đột diễn ra.

Những năm 1990 tiếp tục với sự phát triển của khủng bố mạng. Trong cuộc xung đột Kosovo năm 1999, máy tính của NATO đã bị ngập lụt với bom email và cũng là mục tiêu của tấn công từ chối dịch vụ của hacker phản đối các vụ đánh bom của NATO. Ngoài ra, các doanh nghiệp, các tổ chức công cộng, và các trường đại học nhận được virus đầy email từ một loạt quốc gia Đông Âu. Sau khi đại sứ quán Trung Quốc đã vô tình bị đánh bom ở Belgrade, hacker Trung Quốc đăng tải những thông điệp đó như: *"Chúng tôi*

sẽ không ngừng tấn công cho đến khi chiến tranh dừng lại" trên trang web của chính phủ Mỹ.

Giữa những năm 1990 đã thấy một xu hướng mới. Các nhóm tổ chức tội phạm truyền thống, chẳng hạn như mafia New York, bắt đầu thấy không gian mạng là một lĩnh vực mới chúng có thể tấn công. Đến năm 1996, gia đình mafia New York đã tham gia vào chương trình ‘pump và dump’, sử dụng Internet để giúp thổi phồng và bán cổ phiếu. Vào giữa những năm 1990, Sovereign Equity Management Corp, một công ty có trụ sở tại Boca Raton, Florida, đã được sử dụng như là một phương tiện để ‘pump và dump’. Các chi tiết về công ty và quá trình này đã được trình bày chi tiết trong năm 1996 bởi Business Week¹. Các yếu tố cần thiết là: Công ty là mặt trận để lấy tiền của nhà đầu tư ban đầu, đặt nó vào cổ phiếu hiệu suất thấp, thổi phồng một cách giả tạo các mã cổ phiếu, sau đó bán cổ phiếu.

Vào những năm 1990, đặc biệt là năm 1996 và 1997, thế giới đã nhận thức một mối đe dọa mạng mới: lừa đảo. Vụ việc đầu tiên được biết đến của lừa đảo đó là liên quan đến các tài khoản trực tuyến Mỹ, và đã phần nào khác với chúng ta nghĩ là lừa đảo ngày nay. Ban đầu, AOL đã không kiểm tra số thẻ tín dụng khi bạn lần đầu tiên tạo một tài khoản. Điều này cho phép các hacker tạo ra các tài khoản giả sử dụng một máy phát thẻ tín dụng. Trong năm 1996, các tài khoản này được gọi là ‘phish’, và 1997 chúng đã thực sự được giao dịch trực tuyến bởi hacker.

Các phương tiện lừa đảo sớm nhất được thực hiện vào tháng 3 năm 1997. Đó là một trích dẫn từ giám đốc điều hành AOL, lừa đảo được gọi là ‘phishing’. Các tài liệu tham khảo về lừa đảo trên các phương tiện truyền thông đã xuất bản năm 1997 bởi Ed Stansel, trong báo cáo của Liên bang Florida Times. Lừa đảo ở đây là cố gắng có được thông tin cá nhân, dữ liệu, đặc biệt là tài chính hoặc mật khẩu từ mục tiêu vụ lừa đảo. Trong bài viết này, khoảng 13 năm sau vụ việc năm 1997, nó không phải là phổ biến khi một người nhận được nhiều email lừa đảo mỗi ngày. Internet đã trang bị đầy đủ thông tin cho cá nhân tạo điều kiện cho tội phạm thu thập và trộm cắp danh tính.

Năm 1997, giải pháp đăng ký tên miền Internet đã bị hack bởi một đối thủ kinh doanh. Eugene Kashpureff, chủ sở hữu của AlterNic, cuối cùng cũng

đã nhận tội trong vụ này. Vụ này cũng khá thú vị bởi hai lý do: thứ nhất, nó gây ra sự tàn phá nặng nề trên Internet, thứ hai đây là một trường hợp rõ ràng của chủ nghĩa khủng bố kinh tế giữa các doanh nghiệp. Một công ty sử dụng việc hacking để phá vỡ các hoạt động kinh doanh của đối thủ. Điều này thể hiện rằng chiến tranh của các công ty đang diễn ra trên Internet.

Năm 1997 cũng ra đời các công cụ thực hiện điều tra tội phạm máy tính. Các công cụ như vậy đã tồn tại từ trước năm 1997, nhưng đó là lúc chúng được sử dụng trên diện rộng. Năm đó có tiện ích gọi là AOLHell đã được phát hành. Đó là một ứng dụng miễn phí cho phép hầu như bất cứ ai cũng có thể khởi động các cuộc tấn công trên America Online (AOL). Trong nhiều ngày, phòng chat room AOL đã bị tắc nghẽn bởi thư rác, và các hộp thư điện tử của người sử dụng AOL đã bị quá tải bởi thư rác. Kể từ năm đó, nhiều công cụ khác đã được phát tán trên Internet. Ngày nay để tìm tiện ích bẻ mật khẩu, thực hiện tấn công từ chối dịch vụ, hay hacking một mạng là một vấn đề bình thường.

1999 là năm của virus Melissa. Lập trình viên David Smith tạo ra sâu này, từ đó đã gây thiệt hại 500 triệu USD. Smith đã bị kết án và nhận được 5 năm tù giam. Trường hợp này là quan trọng trong lịch sử tội phạm máy tính vì nhiều lý do, đầu tiên là các thiệt hại gây ra bởi virus Melissa và thứ hai là án hấn nhận được. Điều này cho thấy tòa án đã bắt đầu coi tội phạm máy tính nghiêm túc hơn và đưa ra án phù hợp hơn với tội phạm.

1.2.2 Tội phạm máy tính của thế kỷ 21

Những năm đầu của thế kỷ 21 tội phạm máy tính nhắm vào thế giới mạng một cách đáng kể. Internet đã trở thành một điểm nóng của hoạt động tội phạm có tổ chức, và các nhóm tội phạm đang sử dụng không gian mạng trong mọi cách có thể hình dung được. Bây giờ thậm chí chúng ta còn thấy những nhóm hacker có tổ chức sử dụng kỹ năng của họ để cung cấp dịch vụ như đánh cắp danh tính, rửa tiền, hỗ trợ tội phạm dựa trên máy tính, ...

Vào tháng 6, 2002, nhà chức trách Nga bắt giữ một người đàn ông bị cáo buộc nhà gián điệp không gian mạng cho CIA. Họ cáo buộc hấn hack hệ thống Do-mestic Security Service (FSB) của Nga và bí mật thu thập, sau đó chuyển cho CIA. Trong khi có khả năng hoạt động gián điệp trên máy tính đã

diễn ra lâu trước năm 2002, đây là một trong các trường hợp công bố công khai đầu tiên của nó.

Vào tháng 1 năm 2003, sâu Slammer đã làm lây nhiễm hàng trăm ngàn máy tính trong vòng chưa đầy ba tiếng đồng hồ. Virus này gây ra vấn đề nghiêm trọng. Nó tàn phá dữ liệu các doanh nghiệp trên thế giới, làm gián đoạn các máy rút tiền và thậm chí trì hoãn cả các chuyến bay. Virus này nằm trên một máy nhất định, sau quét mạng cho bất kỳ máy tính nào chạy Microsoft SQL Server Desktop Engine. Sau đó, nó sẽ sử dụng một lỗ hổng trong ứng dụng để làm lây nhiễm các máy tính mục tiêu. Nó sẽ liên tục quét tất cả các máy tính kết nối với máy bị nhiễm. Virus này thú vị trong lịch sử bởi ba lý do, đầu tiên là tốc độ mà nó lây lan, và lý do thứ hai là thiệt hại mà nó gây ra. Lý do thứ ba là ảnh hưởng của virus là để bắt đầu một tấn công từ chối dịch vụ tấn công trên bất kỳ mạng nào mà nó đã được cài đặt trên đó. Virus này có mục đích khác là thực hiện tấn công từ chối dịch vụ từ bên trong mạng.

Một virus quan trọng năm 2003 là virus SoBig. Virus này đặc biệt nguy hiểm. Nó sử dụng một cách tiếp cận đa phương thức để lây lan. Điều này có nghĩa là nó được sử dụng nhiều hơn một cơ chế để phát tán và lây nhiễm sang máy mới, không giống như các phương pháp đơn thức. Một trong nhiều phương pháp lan rộng chỉ đơn giản là sao chép chính nó vào bất kỳ ổ đĩa chia sẻ trên mạng và sau đó email gửi chính nó đến tất cả mọi người trong sổ địa chỉ của các máy tính bị lây nhiễm. Phương pháp đa phương thức truyền bá cho thấy lập trình tinh vi đã được sử dụng rõ ràng trong việc tạo ra virus này.

Năm 2003 cũng đã mang đến cho chúng ta virus Bagle và Mimail. Loại virus này lây lan qua email, mặc dù phương pháp cụ thể của chúng là khác nhau. Ví dụ, virus Mimail đã có thể trích xuất địa chỉ email không chỉ từ sổ địa chỉ của các máy tính bị lây nhiễm, nhưng cũng từ bất kỳ tài liệu trên ổ cứng máy tính bị lây nhiễm. Điều này cho phép nó lây lan xa hơn và nhanh hơn. Virus Bagle cũng quét các ổ đĩa cứng bị nhiễm tìm kiếm các địa chỉ email. Trong khi không gây hại như Slammer hay Sobig nhưng thực tế chúng ta có thể dễ dàng tìm thấy 4 virus lớn chỉ trong năm 2003 minh họa cho quan điểm rằng vào đầu thế kỷ 21, virus đã trở thành một tâm điểm trên Internet.

2003 là một năm bùng nổ về tội phạm máy tính. Ngoài một số đợt bùng phát virus lớn, những kẻ lừa đảo đã bắt đầu một chiến thuật mới. Thay vì gửi email dẫn nạn nhân của họ vào các trang web ngân hàng giả mạo, các liên kết email sẽ thay vì đưa người dùng đến trang web ngân hàng thật, nhưng thêm một cửa sổ pop – up ở phía trước của nó mà đã đăng nhập giả mạo của kẻ lừa đảo màn hình. Chiến thuật này sẽ thể hiện một sự leo thang trong cả sự tinh tế kỹ thuật và sự sáng tạo của kẻ lừa đảo.

2003 mang đến cho chúng ta một chương thú vị trong lịch sử tội phạm máy tính. Đây là năm Microsoft đã bắt đầu công bố tiền thưởng trong việc nắm bắt hacker, người viết virus, và các tội phạm máy tính khác. Cho đến nay, không có dấu hiệu cho thấy việc này thành công, nhưng đó là một cách hay để chống lại tội phạm máy tính.

Năm 2004, công chúng đã ý thức được kẻ thù trực tuyến. Trong khi nhiều người trong lĩnh vực thực thi pháp luật đã nhận thức được vấn đề, và FBI đã có một lực lượng đặc nhiệm tại chỗ từ năm 1995, nhiều người trong công chúng đã không nhận ra mối đe dọa mới này. Chương trình “*The Dateline NBC to Catch a Predator*” đầu tiên phát sóng vào năm 2004. Một số lượng lớn tranh cãi xung quanh chương trình này, và một số đã cáo buộc nhà sản xuất của nó có xung đột lợi ích thậm chí là một cái bẫy. Nhưng sự thật vẫn là, chương trình đã làm cho các bậc cha mẹ trên toàn nước Mỹ và thế giới nhận rõ sự nguy hiểm rất thực tế của pedophiles trên Internet. Chương trình được tiếp tục cho đến năm 2007, và qua ba năm nó đã cho công chúng thấy chính xác thì kẻ thù trực tuyến đã hoạt động và làm thế nào thu hút trẻ em. Vì lý do đó, chương trình này kiếm được vị trí của nó trong lịch sử tội phạm máy tính.

Năm 2005, hacker đã cố gắng chuyển 420 triệu USD từ một ngân hàng ở London. Đây có thể là vụ cướp điện tử lớn nhất trong lịch sử. Điều gì làm cho trường hợp này thú vị nhất đó là cảnh sát đã có thể ngăn chặn hành vi này. Thủ phạm đã quản lý để có được keylogger trên máy tính của nhân viên ngân hàng, và do đó đã đạt được tên người dùng và mật khẩu, cho phép chúng truy cập vào hệ thống ngân hàng. Keylogger là một chương trình nằm trên một máy tính và chỉ đơn giản là ghi lại hình ảnh quan trọng. Dữ liệu sau đó có thể được lấy trực tiếp từ thủ phạm hoặc các keylogger có thể được cấu hình để

tự động gửi dữ liệu đến một số địa chỉ IP được xác định trước. Trong một chương trình điển hình, thủ phạm sẽ cài keylogger trong một số phần mềm khác, như là tạo ra một con Trojan.

Trojan là phần mềm xuất hiện với mục đích hữu ích nhưng thực sự cung cấp một số nguy hiểm. Khi người dùng tải về những gì họ tin là hữu ích, keylogger cũng được gửi. Tội phạm này đã lập một địa chỉ IP để gửi dữ liệu đến. Thông thường, đây là một máy chủ không an toàn thuộc một bên thứ ba không nghi ngờ rằng bị hack và giúp mục đích này. Sau đó, khi dữ liệu vào máy chủ, người chịu trách nhiệm việc tạo ra các keylogger có thể quét các thông tin hữu ích. Phần mềm gián điệp là một vấn đề ngày càng phát triển trên Internet. Nó đang trở thành một trong những mối đe dọa nghiêm trọng nhất đối với an ninh máy tính.

2008 là năm nổi tiếng với Lori Drew, người mẹ đã thành lập một trang MySpace giả để chế nhạo đối thủ của con gái tuổi teen của mình. Các công tố viên liên bang đã cố gắng truy tố bà Drew dưới hình thức gian lận máy tính liên bang và lạm dụng quy chế.

Năm 2009, Brian Hurt sử dụng Craigslist để tìm một cô gái mại dâm đến nơi cư trú của mình. Sau đó ông bán cô gái ấy. Trường hợp này được đưa ra ánh sáng những nguy hiểm của quảng cáo trên Craigslist. Nhiều quảng cáo trên đó thực sự là một phần của một số chương trình gian lận, và dịch vụ 'khiêu dâm'. Nhưng mối liên hệ giữa trang quảng cáo Craigslist và giết người mang lại sự giám sát trang web.

Trong năm 2009, một hacker có tên là Israel Ehd Tenenbaum bị tình nghi là ăn cắp khoảng 10 triệu USD từ các ngân hàng ở Mỹ. Phần gây sốc của trường hợp này là Tenenbaum đã bị bắt ở Canada vì tội ăn cắp 1,5 triệu USD năm 2008. Trường hợp này cho thấy cộng đồng pháp lý vẫn đối phó chưa hiệu quả với tội phạm máy tính.

2009 cũng là năm quan trọng trong lịch sử tội phạm máy tính do sự nhận tội và kết án tiếp theo của Albert Gonzales. Gonzales ở Miami, Florida, đã bị buộc tội ăn cắp số thẻ tín dụng từ một mảng rộng của các nhà bán lẻ bao gồm Office Max, cơ quan thể thao, thi trường Boston, và Barnes và Noble. Gonzales đã nhận tổng cộng 19 tội bao gồm âm mưu, gian lận máy tính, đường dây lừa đảo, gian lận thiết bị truy cập, và nghiêm trọng hơn là đánh cắp

định danh. Hắn cũng nhận tội tại New York với âm mưu gian lận để đột nhập vào Dave và Busters. Cuối cùng Gonzales phải đối mặt với 25 năm tù giam. Điều làm cho vụ này thú vị là hai sự kiện. Đầu tiên là án mà hắn ta nhận được. Đây là một điều khác xa với hình phạt nhỏ của tòa án trong những năm 1980. Thứ hai đó là Gonzales tiếp tục cuộc sống xa hoa, chi tiêu hơn 2,8 triệu USD tiền đánh cắp được. Trường hợp này cho thấy một điều rất rõ ràng đó là tội phạm máy tính rất nguy hiểm, và tòa án đang xét nó khá nghiêm túc trong thế kỷ 21.

1.2.3 Tội phạm máy tính trong thời điểm hiện tại

Trong những năm gần đây, vấn đề tội phạm mạng vẫn liên tục được nhắc đến. Tại Anh, thủ tướng Anh D. Cameron đã siết chặt luật cấm phim ảnh đồi trụy trên mạng Internet, đồng thời yêu cầu các nhà cung cấp công cụ tra cứu trên mạng như Google, Yahoo và Bing ngăn chặn các hình ảnh khiêu dâm trẻ em. Tuy nhiên theo Ủy ban Nội vụ của Quốc hội Anh, nỗ lực này cũng không giải quyết được nhiều vấn đề bởi vì các tội phạm Internet, từ giả dạng, đánh cắp dữ liệu đến truyền bá các hình ảnh trái phép cũng như các tài liệu cực đoan trên mạng vẫn tràn lan tại Anh. Ngoài ra, trong một buổi điều trần mở hiếm hoi của Ủy ban Tình báo Thượng viện, Giám đốc Cục Điều tra liên bang Mỹ FBI lúc đó R. Mueller đã phải thốt lên rằng: “Ngăn chặn khủng bố vẫn là ưu tiên số một. Nhưng trong thời gian tới, mối đe dọa trên không gian mạng sẽ là nỗi lo hàng đầu cho đất nước”. Cục Chiến lược an ninh quốc gia của Anh thì xếp hạng các mối đe dọa đến từ Internet ngang hàng với chủ nghĩa khủng bố, và cũng gây nguy hiểm không kém đối với hệ thống cơ sở hạ tầng quốc gia.

Theo kết quả nghiên cứu của Tập đoàn an ninh McAfee và Trung tâm Nghiên cứu Chiến lược Quốc tế (CSIS), nạn tội phạm mạng đang gây tổn thất cho nền kinh tế toàn cầu từ 100-500 tỷ USD mỗi năm. Nghiên cứu cho biết tổn thất do loại tội phạm này gây ra bao gồm thiệt hại do tài sản trí tuệ và các thông tin mật bị đánh cắp; niềm tin của người sử dụng Internet suy giảm; chi phí cho công tác phục hồi, bảo hiểm và an ninh mạng gia tăng cũng như uy tín của các doanh nghiệp bị tổn hại. Chưa dừng ở đó, Giám đốc Cục tình báo Anh (MI 5) còn cảnh báo viễn cảnh các tổ chức khủng bố sẽ áp dụng loại phương

thức tấn công mạng trong tương lai. Theo ông, hậu quả của những vụ việc tương tự sẽ ngày càng lớn hơn, do mạng Internet hiện đã gắn kết với gần như mọi khía cạnh cuộc sống, từ văn phòng, công sở đến xe hơi, hệ thống quản lý giao thông cho đến máy rút tiền mặt ATM...

Tại Việt Nam, theo báo cáo của cục Phòng chống tội phạm sử dụng công nghệ cao (C50), cũng như báo cáo của Hiệp hội An toàn thông tin (VNISA), ngày nay, tình hình an ninh mạng tiếp tục diễn tiến phức tạp với mức độ tăng. Các loại hình tấn công phổ biến của hacker là phát tán virus, phần mềm gián điệp thông qua thư rác (spam mail), diễn đàn, mạng xã hội... Ngoài ra, các loại virus do thám còn được nhúng trong các phần mềm ứng dụng thường dùng.

Các trang web, hệ thống mạng của doanh nghiệp còn bị tấn công DDOS gây tắc nghẽn đường truyền. Hacker sử dụng mạng máy tính botnet truy cập liên tục, lặp đi lặp lại vào một địa chỉ trang web định trước. Ở cuộc tấn công vào báo điện tử Vietnamnet, lượng truy cập vào lúc cao điểm lên đến một triệu kết nối.

Hacker còn sử dụng loại virus “siêu đa hình” nhằm qua mặt các phần mềm phòng chống virus trên máy tính. Một số vụ tấn công còn sử dụng phần mềm tạo địa chỉ giả mạo trên Internet, giả mạo Email, che giấu địa chỉ trên mạng...

Hacker truy cập vào các trang web mua bán trực tuyến nhằm đánh cắp thông tin về tài khoản thẻ tín dụng. Hoặc lây nhiễm các loại keylogger (virus ghi ký tự bàn phím) hoặc spyware (virus do thám) để lấy thông tin thẻ tín dụng. Thông qua các thẻ tín dụng lấy được, hacker sử dụng mua sắm trên các trang web mua bán trực tuyến. Hacker cũng tìm cách “rửa tiền” từ các tài khoản thẻ ngân hàng bằng cách mua bán lòng vòng trên mạng. Đã có trường hợp sử dụng thẻ cào nạp tiền điện thoại lừa đảo được để rao bán mã thẻ với giá rẻ.

Trong một số chuyên án, hacker còn dùng đến công cụ tạo Proxy có tên gọi TOR để che giấu địa chỉ IP. Khi sử dụng TOR, hacker có thể chuyển đổi liên tục máy chủ Proxy kết nối Internet. Ví dụ: Khi dùng mạng lưới Proxy này, các nhóm hacker sẽ cứ tuần tự 10 phút/lần thay đổi kết nối Internet từ nhiều quốc gia khác nhau.

Một số tội phạm còn dùng Skimming (ăn trộm mật khẩu ATM) gài chip vào đầu đọc thẻ (trên máy ATM) để ghi trộm mã số thẻ ATM. Thông qua thiết bị đọc mã số và camera quay lên thao tác gõ mật khẩu, hacker có thể tạo thẻ ATM giả mạo để rút tiền. Bọn tội phạm còn có thể “rửa tiền” bằng cách nạp tiền thông qua các hệ thống thanh toán trực tuyến với dạng “tiền điện tử” như Liberty Reserve, e-Gold, WebMoney... Sau đó, số “tiền điện tử” này có thể được rút ra để sử dụng như tiền hợp pháp.

C50 cũng dự báo các nhóm tội phạm công nghệ cao sẽ chuyển dần hướng tấn công sang điện thoại di động. Các loại điện thoại thông minh hiện nay lưu trữ nhiều thông tin cá nhân nhưng lại dễ bị virus thâm nhập và đánh cắp.

Trong thời gian tới, có thể các nhóm hacker sẽ khai thác ứng dụng Điện toán đám mây để tấn công vào các lỗ hổng bảo mật trên máy chủ, đánh cắp thông tin trên các trang web dịch vụ trực tuyến...

1.3 CÁC NGUY HẠI XẢY ĐẾN TỪ TỘI PHẠM MÁY TÍNH

1.3.1 Nguy hại đối với cá nhân

Cá nhân thường là những đối tượng chính của hacker để thực hiện các hành vi lợi dụng, lừa đảo và chiếm đoạt tài sản thông qua mạng. Mặc dù Internet đã phát triển từ lâu song kiến thức để bảo vệ an toàn cho Internet vẫn chưa thực sự được mọi người chú ý đặc biệt là với những người không làm việc trong lĩnh vực an toàn thông tin. Chính vì thế hàng năm, những vụ tấn công tới tài khoản cá nhân, lừa đảo trực tuyến vẫn không ngừng gia tăng và luôn là mối lo ngại của toàn thế giới.

Có thể kể ra ở đây không ít ví dụ. Trong một sự kiện tại Francisco vào năm 2012, ông R. Mueller đã tiết lộ suýt nữa mình trở thành nạn nhân của một vụ lừa đảo trực tuyến. Kẻ lừa đảo đã gửi cho ông một email giả mạo y hệt nội dung từ một ngân hàng mà ông có tài khoản. Chỉ cần thêm vài cú click chuột, người quyền lực nhất FBI sẽ sập bẫy và kéo theo đó là hàng loạt các vấn đề nảy sinh. Ngoài ra mới đây, trên Facebook xuất hiện nhiều trang mạo danh chuyên mục “*Tám lòng Nhân ái*”, mạo danh phóng viên để kêu gọi sự ủng hộ của mọi người đối với các hoàn cảnh nhân ái, nhưng nếu được mọi người ủng hộ thì số tiền trên sẽ bị kẻ mạo danh chiếm dụng hoàn toàn.

Các vụ lừa đảo trên mạng không chỉ đơn giản như vậy. Có nhiều cuộc lừa đảo mang tính siêu hạng, tầm cỡ thế giới khiến người bị lừa hoàn toàn không biết mình đã bị lừa và bị sập bẫy một cách dễ dàng. Chúng ta sẽ thử xem một ví dụ dưới đây:

Thả câu:

Xin chào,

Tên em là Benny Dider. Em là một cô gái độc thân. Em rất ấn tượng khi xem hồ sơ tìm bạn của anh và mong muốn được làm bạn với anh. Nếu có thể, xin anh trả lời cho em qua hộp thư riêng bennydider@yahoo.com .

Cảm ơn và mong hồi âm.

Benny

Lá thư trên đây được gửi đến hộp thư của một doanh nhân còn độc thân và có mở một hồ sơ trên website www.docthan.com . Sau nhiều lần im lặng vì người gửi là một cô gái nước ngoài, anh đành trả lời với một lời lẽ rất nhã nhặn. Chỉ chờ có thế, cô gái tên Benny đã tấn công một cách rất khéo léo, đưa anh ta vào một quan hệ trao đổi thư từ không thể từ chối.

Anh mến,

Em cảm ơn thư hồi âm của anh. Một ngày qua anh sống thế nào?

Em đã lại vừa qua một ngày kinh khủng ở Dakar. Như em đã nói trong thư trước, em tên là Benny Dider, ở Bờ Biển Ngà Tây Phi. Hiện tại em sống trong một trại tị nạn ở Dakar mà nguyên nhân là do cuộc nội chiến đang diễn ra ở đất nước của em.

Bố dượng em là Tiến sĩ Remi Dider, vốn là cố vấn riêng của nguyên thủ cũ của Bờ Biển Ngà trước khi phiên quân đột nhập vào nhà em, giết chết ông cùng với mẹ em. Em may mắn trốn thoát và chạy loạn sang Senegal, và ở đây, em được đưa vào một trại tị nạn.

Em mong được biết thêm về anh. Những gì anh thích, những gì anh ghét, những gì anh đang làm.

Em gửi kèm đây bức ảnh của em.

Chờ thư anh,

Benny

Và với lá thư trên đây, giữa những mối quan hệ làm quen khác nhau, Benny đã hiển nhiên trở thành mối quan hệ đáng quan tâm hàng đầu, với một

hoàn cảnh đầy đau thương và cần được chia sẻ. Ít nhất, nếu không phải để cầu tình, thì cũng để xoa dịu một cô gái đã và đang trải qua một cuộc sống đầy chấn động và bất công.

Gài bẫy:

Anh yêu,

Một ngày qua anh sống thế nào?

Em tin rằng, mọi thứ đối với anh đều tốt đẹp. Còn với em, anh biết, trong trại tị nạn này mỗi ngày thật kinh khủng, y như trong nhà tù. Em hy vọng, nhờ Chúa, em sẽ sớm được ra khỏi trại. Em không còn người thân nào khác bên ngoài, vì họ đều chạy loạn hết rồi. Người thân thiết duy nhất của em hiện tại là mục sư Chris Henshaw, thuộc tổ chức Nhà thờ Nguồn sống Thiên Chúa, trong trại. Ông ấy rất tử tế với em kể từ khi em đến đây, nhưng em không sống với ông ấy, mà trong khu tị nạn dành cho nữ (ở đây có khu tị nạn dành riêng cho nam và nữ).

Nếu được, anh có thể gọi ông ấy số 00-221-444-5321, rồi nhờ ông ấy gọi em để nói chuyện. Là một người tị nạn, em không có quyền hay được ưu đãi gì khác, dù có tiền hay gì cũng vậy, vì đây là luật của đất nước này.

Em mong muốn được trở lại trường đại học, vì em mới học năm thứ nhất ở đó trước khi gia đình em bị giết. Hãy nghe em nói, trước khi chết, bố dựng em có gửi một số tiền, nghe đâu là 7,5 triệu USD, ở một ngân hàng ở châu Âu, mà tên em được ghi là người thụ hưởng kế tiếp. Em có giữ thông tin tài khoản cùng với giấy chứng tử của ông, nhưng em không thể tin tưởng ai được ngoài mục sư Chris Henshaw, vì ông ấy đối với em như là cha mình. Trong trại, nếu thông tin lộ ra, thì em sẽ mất cả mạng lẫn tiền.

Em nhờ anh xem có thể chuyển số tiền đó sang tài khoản của anh, rồi rút một số gửi sang cho em lo giấy tờ ra trại cùng vé máy bay sang gặp anh.

Hãy nhớ rằng em nhờ anh vì lòng tin tưởng em đặt vào nơi anh. Em yêu anh vì anh là một người trung thực, hiểu biết, chăm chỉ và có lòng nhân ái. Anh yêu, em sẽ đến với anh, khi đó chúng ta sẽ nói chuyện chung sống nhé.

Hãy nghĩ về em,

Benny,

Đến đây, cái bẫy đã được giương ra với đầy cám dỗ: một số tiền quá lớn, cộng thêm một câu chuyện mang đầy màu sắc nhân đạo. Câu chuyện về

một mục sư, cộng thêm một số điện thoại cố định đã cho bức mail một hoàn cảnh có vẻ xác thực. Như thế, mọi con mồi, dù có nghi ngờ gì đi nữa, vẫn chỉ nhìn thấy miếng thịt mà chưa móc câu: Nếu cô ta định lừa mình, thì lừa ở chỗ nào? Vì mình đang là người đắc lợi kia mà. Thế là con mồi dần tiếp thêm một bước, và nhận được những lời dễ thương như sau:

Anh yêu,

Một ngày nữa của anh thế nào? Em nghĩ là tốt đẹp, phải không?

Em đọc lại những bức mail của anh và nhận thức rõ rằng anh là người đàn ông mà em luôn tìm kiếm. Em muốn có một người sẽ đối xử với em một cách yêu thương và hiểu biết vì em đang trải qua một quãng thời gian nhiều chấn động.

Cảm ơn ý định giúp đỡ của anh, cũng như cảm ơn thái độ cao cả của anh trong chuyện tiền bạc, nhưng có thể nói trong cuộc sống đầy khó khăn và nguy hiểm hiện tại của em, toàn bộ hy vọng của em đang đặt vào anh.

Em đã báo cho ngân hàng STANDARD LIFE BANK OF SCOTLAND về ý định rút tiền và điều duy nhất mà họ yêu cầu là tìm kiếm một đối tác thứ ba thay mặt em rút tiền. Vì thế, em muốn anh sớm tiếp xúc với ngân hàng để hỏi rõ thủ tục chuyển tiền.

STANDARD LIFE BANK OF SCOTLAND

Email :(customerservices@standard-lifebank.com)

Tên của nhân viên chuyển tiền là David Newlands

Telephone +44-704_010-9889.

Fax +44-703-192-4802

Anh nhớ cho họ biết rõ, anh là đối tác của em và muốn giúp em rút số tiền 7,5 triệu USD trong tài khoản của Tiến sĩ Remi Dider mà em là người thụ hưởng kế tiếp.

Đến đây, chỉ cần tiếp xúc với địa chỉ email ở trên, thì nạn nhân ngay sau đó bị cuốn vào một ma trận được tạo bởi ba người: nhân viên ngân hàng, mục sư và nhân vật chính yếu trong chuyện móc tiền là một luật sư, với vai trò được khéo léo giới thiệu qua bức mail sau:

Kính thưa Ngài,

Về việc Ngài yêu cầu giải ngân tài khoản của Tiến sĩ Remi Dider (7,5 triệu USD) mà người thụ hưởng kế tiếp là Cô Benny Dider hiện ở Dakar,

Senagal, chúng tôi đã ghi nhận và chuyển yêu cầu đến bộ phận chuyển tiền. Tuy nhiên, Ngài được yêu cầu chứng minh cái chết của Tiến sĩ Remy Dider, đồng thời phải chứng thực được rằng Ngài là người được cô Benny Dider uỷ nhiệm trước khi chúng tôi có thể thực hiện việc giải ngân. Các loại giấy tờ cụ thể như sau:

Ngài phải trình một giấy uỷ quyền do Cô Benny Dider ký được xác nhận bởi một luật sư bản địa Senegal.

Ngài phải trình một bản sao chứng tử của Tiến sĩ Remy Dider.

Ngài phải trình một bản khai thông tin tài khoản của Tiến sĩ Remy Dider.

Kính chào Ngài,

David Newlands

Tel: 00 44 704 010 9889

Sập bẫy:

Ngay trong bức mail kế tiếp, thì bẫy được sập xuống với vai trò chủ đạo của một luật sư được giới thiệu liền sau đó. Thông thường, nạn nhân được yêu cầu chi trả một số tiền từ vài ngàn đến vài chục ngàn USD cho những việc như: xác nhận giấy uỷ quyền, mua chuộc các quan chức Senegal, hay một loạt các trò bịp khác. Thế nhưng nạn nhân, luôn luôn bị kẹp giữa lòng nhân đạo cộng với lòng tham và những đòi hỏi tiền bạc này, sẽ rất khó từ chối. Thông thường, các nạn nhân cũng chỉ trả ít nhất vài ngàn USD cho những đòi hỏi ban đầu và chỉ tỉnh lại khi thấy những yêu cầu chi phí ngày càng lớn.

Với những cách gài bẫy khôn ngoan như vậy, lừa đảo trực tuyến đã trở thành một vấn nạn trên không gian ảo. Một website đã được lập ra, <http://www.joewein.de/sw/419-penpal.htm#missclara> để cảnh báo những người dùng mạng về những trò bịp này. Trên website này, mọi người có thể dễ dàng nhận ra một loạt những ví dụ tương tự nhau, với những khuôn mẫu chỉ thay đổi chút ít cho phù hợp với từng trường hợp.

Lừa tình mới chỉ là một trong nhiều trò bịp được sử dụng trên không gian ảo. Ngoài trò này, còn một loạt các trò bịp khác:

- + Cá độ trên mạng: Thắng một giải xổ số ảo trên mạng, nhưng để nhận giải, người nhận phải trả trước một khoản chi phí.

- + Tài khoản không có người thừa kế: Một người ngoại quốc có tài khoản tại một ngân hàng ở châu Phi hay châu Á chết mà không có người thừa kế. Nạn nhân được yêu cầu tham gia với vai trò bà con giả, nhưng trước hết phải trả những khoản phí hồi lộ.
- + Hợp đồng chính phủ chưa được thanh lý: Thông thường, là một hợp đồng với chính phủ một nước châu Phi chưa được thanh lý, nghiệm thu và giải ngân. Chúng ta được hứa hẹn một phần hợp đồng, nhưng phải trả tiền hồi lộ trước.
- + Doanh nhân bị ám sát: Trước khi chết tìm kiếm sự giúp đỡ để có thể giải ngân một tài sản kénch xù cho người thừa kế. Chúng ta được hứa hẹn một phần của tài sản, nhưng phải trả một khoản phí cho một công ty bảo hiểm.
- + Không chỉ giới hạn với những trò bịp trên, những kẻ lừa đảo trên mạng ngày càng viết ra những kịch bản mới, tinh vi hơn nhằm đánh vào lòng tham: tham tình, tham tiền, tham danh của cộng đồng những người dùng mạng.

Ngoài các đối tượng là những người lớn tuổi, sử dụng máy tính thường xuyên thì những tội phạm mạng còn nhắm đến các đối tượng là trẻ nhỏ. Chính vì thế, vấn đề bảo vệ trẻ em khi cho trẻ tiếp cận sớm với máy vi tính là một trong các vấn đề luôn làm đau đầu các bậc cha mẹ. “*Làm cách nào giúp các con tôi online an toàn?*” hay “*Tôi có thể làm gì để bảo vệ con cái khi cho con sử dụng máy vi tính?*” là các câu hỏi thường được các phụ huynh đặt ra. Để nói rõ hơn về vấn đề này, chúng ta thử theo dõi một câu chuyện như sau:

Ellie sống tại Liên Hiệp Vương Quốc Anh. Khi cô mười bốn tuổi, cô đã dành nhiều thời gian trên máy điện toán. Ellie và bạn bè của cô đã sử dụng mạng xã hội website MySpace. Trên địa chỉ này, người ta có thể tạo những trang tiểu sử tóm tắt cá nhân. Những trang này trình bày những sở thích của họ. Bạn bè có thể gửi những tin nhắn cho nhau.

Ellie thích dùng trang MySpace của mình. Cô đã có nhiều bạn bè ghé thăm trang của cô. Một ngày nọ, một người mà Ellie chưa hề nhận biết đã yêu

cầu được làm bạn với cô. Ellie đã thấy lời đề nghị này trên trang MySpace của cô. Người này xác nhận là một phụ nữ hai mươi sáu tuổi. Ellie đã chấp nhận lời yêu cầu làm bạn ấy.

Ellie không biết nhiều về người này. Thực ra, người bạn mới này của cô thực tế là một người đàn ông năm mươi lăm tuổi tên là Ian. Ian đã theo dõi trang MySpace của Ellie rất kỹ. Ông ta đã đọc những lời bình mà Ellie đã thể hiện. Ông ta đã đọc những gì mà Ellie và bạn bè của cô nói chuyện với nhau. Chẳng mấy chốc ông đã biết nhiều thông tin về Ellie. Thậm chí ông ta còn biết cả những gì, những sự kiện mà Ellie và bạn bè của cô dự định thực hiện. Rồi một ngày, Ian thậm chí đã theo Ellie trên đường đến trường. Trên chuyến đi này, Ian đã cố gắng nói chuyện với Ellie và bạn bè của cô. Họ đã nghi ngờ một điều gì đó không đúng đắn. Họ chẳng biết gì về người đàn ông này! Dùng điện thoại di động của mình, cô đã chụp hình người đàn ông này. Cô đã giao tấm hình này cho cảnh sát. Cảnh sát đã tìm kiếm nhà của hắn. Ở đó, cảnh sát đã thấy nhiều hình ảnh tình dục trẻ em. Ian là một người lợi dụng tình dục trên internet.

Như vậy là suýt chút nữa, Ellie đã là nạn nhân tiếp theo của Ian, và cô có thể bị lợi dụng tình dục chỉ đơn giản sử dụng MySpace trên Internet.

Hiện nay, những câu chuyện “tiếng sét ái tình” trên mạng ảo dẫn tới mất tiền, mất của thật ngoài đời vẫn còn xảy ra rất nhiều và chủ yếu là do các em tò mò, thiếu hiểu biết. Không chỉ dừng lại ở đó, trên mạng còn có những nguy hiểm khác mà cha mẹ thường khó có thể kiểm soát khi trẻ em truy cập vào Internet đó là hành vi dụ dỗ trẻ tiếp xúc với nội dung khiêu dâm, bạo lực, các quảng cáo lừa đảo nhằm ăn cắp thông tin và vô số loại vi rút nham nhảm trên các trang web không chính thống. Khi trẻ em chơi game flash trực tuyến trên mạng, rất có khả năng chúng sẽ nhấn vào một nút “Tải về” có hình ảnh sống động và âm thanh hấp dẫn. Và việc đây có thể sẽ dẫn đến máy tính sẽ bị nhiễm các loại vi rút, những phần mềm độc hại và người dùng bị ăn cắp thông tin ngay khi đang sử dụng máy tính tại nhà riêng của mình.

Tóm lại, với phương thức ngày càng tinh vi và phức tạp, các tội phạm mạng có thể dễ dàng thực hiện lừa đảo tới các cá nhân – những người thường xuyên sử dụng Internet và các trẻ nhỏ để đánh cắp tài khoản, tiền của, lợi dụng tình dục, phát tán các nội dung khiêu dâm trên mạng.

1.3.2 Nguy hại đối với tổ chức

Không chỉ nguy hại đối với cá nhân, các tổ chức cũng thường xuyên phải đối mặt với các nguy hại từ tội phạm máy tính. Khoảng 1h35 ngày 5-6-2013, diễn đàn HVA ở địa chỉ <http://www.hvaonline.net> bị sự cố trên đĩa cứng. Đồng thời, diễn đàn bị một lượng DDoS (tấn công từ chối dịch vụ) rất lớn ập vào, làm bão hòa hoàn toàn đường truyền đến máy chủ HVA. Đến đêm 12-6, HVA lại tiếp tục phải chịu một đợt tấn công DDoS nữa với cường độ rất lớn. Nhà cung cấp dịch vụ tự động ngăn cản toàn bộ các truy cập đến HVA. HVA cho biết, phần lớn các địa chỉ tấn công đều có nguồn từ nước ngoài nhưng một số máy tính ma (botnet) có cả địa chỉ của Việt Nam. Điều đó chứng tỏ không ít máy tính tại Việt Nam bị nhiễm virus và đã thành zombies (chương trình bí mật không chế một máy tính kết nối internet, sau đó dùng máy tính này để tấn công) cho mạng máy tính ma tại nước ngoài.

Tối 9-6-2013, Báo điện tử Petro Times của Tập đoàn Dầu khí Việt Nam đã phải hứng chịu 2 cuộc tấn công liên tiếp từ hacker. Cùng với đó, nhiều trang web của các bộ, ngành của Việt Nam cũng bị hacker tấn công. Trao đổi với báo chí, ông Nguyễn Minh Đức - Giám đốc Bộ phận an ninh mạng của Công ty Bkav cho hay, từ đầu tháng 6 đến nay, có 249 website của Việt Nam bị tội phạm mạng tấn công, phần lớn với phương thức thay đổi giao diện và từ chối dịch vụ. Hacker sẽ để lại các thông điệp bằng tiếng Anh hoặc tiếng Trung. Con số website bị tấn công trong 15 ngày đầu tháng này đã nhiều gấp 2,5 lần so với những tháng trước (khoảng 100 website bị tấn công mỗi tháng). Đáng chú ý, trong số website nạn nhân của hacker này có đến hơn 50 website có tên miền gov.vn, của các cơ quan Nhà nước.

Ngoài ra, tại Trung Quốc, cộng đồng mạng thực sự bức xúc vì sự chậm trễ trong hệ thống website của họ. Tất cả các truy cập vào website với đuôi .cn trong suốt tháng 8-2013 cũng như nhấn refresh liên tục nhưng rất khó khăn. Theo Trung tâm Thông tin mạng Internet của Trung Quốc, xảy ra hiện tượng này là do toàn bộ hệ thống miền mở rộng và các trang blog phổ biến như Sina và Weibo của Trung Quốc đã bị tấn công từ chối dịch vụ. Đây là cuộc tấn công lớn nhất của loại hình này từ trước đến nay tại quốc gia có đến 1 tỷ dân này. Hiện tại vẫn chưa rõ liệu có phải các vụ tấn công nhằm vào các sự kiện

chính trị ở Trung Quốc là khởi đầu cho cuộc đàn áp những ý kiến bất đồng trên Internet hay không. Đáng lưu ý là cuộc tấn công này diễn ra đúng vào thời gian chính phủ khép lại phiên tòa xử ông trùm chính trị Bạc Hy Lai khiến cho cộng đồng mạng Trung Quốc không thể không hoài nghi. Trên mạng lan tràn những ý kiến trái chiều về sự kiện tấn công này. Một cư dân Weibo nói: “Lẽ nào cứ vào những “ngày hội” là Internet của Trung Quốc lại bị tê liệt?”

Một ví dụ khác về tấn công mạng mà người ta gọi là “tấn công mạng lớn nhất lịch sử, làm internet toàn cầu lâm nguy”. Đây là cuộc tấn công xảy ra từ vụ tranh cãi giữa một tổ chức chống thư rác và một công ty lưu trữ web Hà Lan và đã leo thang thành tấn công mạng lớn nhất trong lịch sử internet, gây ra hiện tượng nghẽn mạng trên toàn cầu. Vụ tranh cãi bắt đầu khi nhóm chống nội dung rác Spamhaus đưa công ty Hà Lan Cyberbunker vào danh sách đen, vốn được các nhà cung cấp dịch vụ email sử dụng nhằm loại bỏ nạn spam (Cyberbunker có đại bản doanh đặt tại một boongke cũ của NATO, cung cấp dịch vụ lưu trữ cho mọi website ngoại trừ “khiêu dâm trẻ em và bất cứ thứ gì liên quan đến khủng bố”). Spamhaus tố cáo Cyberbunker, vốn hợp tác với các băng đảng tội phạm Đông Âu và Nga, đứng sau cuộc tấn công nhằm trả đũa việc bị đưa vào danh sách đen. Trong vụ tấn công này, hệ thống phân giải tên miền (DNS) của Spamhaus, đã bị nhắm đến. Vụ tấn công được lưu ý trước hết bởi CloudFlare, một hãng bảo mật internet tại thung lũng Silicon (Mỹ) vốn cố gắng chống đỡ cuộc tấn công trước khi chính họ trở thành mục tiêu. Giám đốc điều hành của CloudFlare Matthew Prince nói với tờ *New York Times*: “*Những thứ này có bản chất giống bom hạt nhân. Việc gây ra quá nhiều thiệt hại là rất dễ dàng*”. Ông Steve Linfood, Giám đốc điều hành của Spamhaus, nói với BBC rằng quy mô của cuộc tấn công là “*chưa từng thấy*”. Cuộc tấn công này huy động từ hệ thống máy tính trên khắp thế giới, với lưu lượng trung bình lên đến 300 Gb/s, lớn gấp nhiều lần kích thước trung bình của những tấn công DDoS trước đây. Các chuyên gia bảo mật xem đây là cuộc tấn công mạng lớn nhất từ trước đến nay trong lịch sử. Ít nhất 5 lực lượng “cảnh sát Internet” cấp quốc gia đã được huy động để điều tra cuộc tấn công này.

Trên đây mới chỉ là một vài ví dụ trong hàng tỉ các vụ tấn công mỗi năm tới các cơ quan tổ chức cũng như chính phủ các quốc gia. Các tấn công này chủ yếu nhằm tới mục đích làm nghẽn hệ thống mạng dẫn tới hệ thống

không được hoạt động bình thường, gây ra các thiệt hại về danh tiếng cũng như tiền của cho tổ chức và cao hơn nữa là các tấn công nhằm vào mục đích chính trị, để đánh cắp các tài nguyên mật của quốc gia. Chính vì thế, việc bảo vệ an toàn an ninh cho hệ thống mạng là vô cùng cần thiết.

1.4 CÁC DẠNG TỘI PHẠM MÁY TÍNH

1.4.1 Đánh cắp định danh

Đánh cắp định danh là quá trình thu thập thông tin cá nhân để thủ phạm giả danh người khác. Điều này thường được thực hiện để có được thẻ tín dụng của nạn nhân, để lại cho nạn nhân những khoản nợ mà không hề hay biết. Mỹ xác định hành vi trộm cắp danh tính như sau: “Tội phạm trộm cắp và lừa đảo danh tính là thuật ngữ dùng để chỉ các loại tội phạm ăn cắp, gian lận, lừa dối và sử dụng trái phép dữ liệu cá nhân của người khác” .

Sử dụng dữ liệu cá nhân của người khác để thực hiện bất kỳ loại hành vi gian lận hoặc lừa dối là đánh cắp định danh. Tội phạm loại này thường thực hiện vì lợi ích kinh tế hay động cơ tài chính . Tội phạm cũng có thể sử dụng dữ liệu cá nhân để mạo danh người khác, hủy hoại danh tiếng ... Ví dụ thủ phạm có thể đặt mua tài liệu khiêu dâm sử dụng danh tính người khác. Tuy nhiên hầu hết các sự cố đánh cắp định danh liên quan đến động cơ kinh tế. Ủy ban thương mại liên bang thống kê rằng trong năm 2005, 8,3 triệu người Mỹ là nạn nhân của tội phạm trộm cắp định danh. Đa số các sự cố nhận dạng hành vi trộm cắp là về vấn đề tài chính, với 3,2 triệu vụ liên quan đến lạm dụng tài khoản tín dụng và 1.800.000 liên quan đến sử dụng thông tin của nạn nhân để mở tài khoản mới. Thiệt hại lên đến hàng tỷ đô la mỗi năm do hành vi trộm cắp định danh. Rõ ràng đây là một vấn đề rất quan trọng .

Trộm cắp định danh làm mất danh tiếng nạn nhân thường là một vấn đề dân sự, không phải tội phạm. Đánh cắp định danh không có động cơ kinh tế là một lỗi nhỏ do đó thường xử lý thông qua tố tụng dân sự chứ không phải là truy tố hình sự. Điều quan trọng là phải xem xét các phương tiện mà hành vi trộm cắp định danh sử dụng. Đầu tiên và hầu hết các bước quan trọng để phạm tội là đạt được quyền truy cập vào dữ liệu cá nhân để có thể trộm danh tính. Có bốn cách có thể truy cập vào thông tin cá nhân:

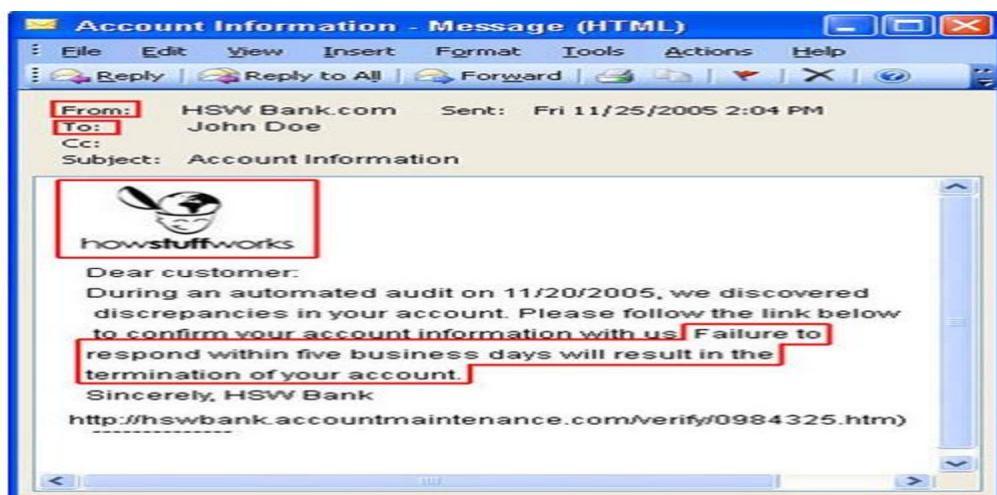
- Giả mạo.

- Tấn công hoặc sử dụng phần mềm gián điệp.
- Truy cập trái phép dữ liệu.
- Dựa vào thông tin rác.

1.4.1.1 Giả mạo

Giả mạo là quá trình ăn cắp những dữ liệu cá nhân từ các nạn nhân mục tiêu. Hành vi này thường được thực hiện thông qua e-mail. Thủ phạm có thể thiết lập một trang web ảo được thiết kế giống như trang web của một tổ chức tài chính hợp pháp (ngân hàng, thẻ tín dụng vv..). Sau đó thủ phạm sẽ gửi email cho càng nhiều người càng tốt, thông báo rằng tài khoản của họ cần xác minh và cung cấp cho họ một liên kết họ có thể bấm vào đăng nhập và xác minh tài khoản của họ. Khi ai đó nhấn vào liên kết, họ được đưa đến trang web giả mạo, nạn nhân nhập thông tin đăng nhập của mình để xác minh tài khoản, cung cấp cho thủ phạm với tên đăng nhập và mật khẩu. Sau đó thủ phạm có thể giả mạo đăng nhập vào tài khoản thực của nạn nhân và ăn cắp tiền.

Thủ thuật này ngày càng trở nên phổ biến. Email như **hình 1.1** là một ví dụ khá điển hình của lừa đảo trực tuyến. Không như những email bình thường, đây là lá thư yêu cầu nạn nhân reply ngay lập tức, nếu không, tài khoản của sẽ bị khóa. Nếu nạn nhân ấn nút reply, không những dữ liệu cá nhân bị đánh cắp, tay trộm còn có thể thông qua đó phát tán virus và tiếp tục lây nhiễm sang những người dùng khác. Tệ hại hơn thế, nạn nhân ấy có thể đang vô thức tham gia vào quá trình rửa tiền giúp những tay tin tặc này.



Hình 1.1. Lừa đảo trực tuyến qua Email

Và cách thường gặp và cũng đơn giản nhất đó là sử dụng các phần mềm tạo email cho phép người dùng điền thông tin vào 2 phần “From” và “Reply-to”. Những phần mềm này rất tiện dụng với những người sử dụng nhiều địa chỉ email, nhưng mặt khác nó giúp cho công việc của bọn lừa đảo dễ dàng hơn. Chỉ cần điền thông tin (trông có vẻ đáng tin cậy) vào mục “From”, ta đã có thể tạo ra một message trông hoàn toàn hợp pháp.

Một số máy chủ email cho phép các máy tính được phép kết nối trực tiếp đến cổng giao thức chuyển mail đơn giản (SMTP) mà không cần sử dụng password. Điều này cho phép tay lừa đảo có thể trực tiếp kết nối tới server và thông qua đó gửi tin nhắn đến hàng loạt cá nhân.

Tội phạm giả mạo có thể khó điều tra với một số lý do. Đầu tiên, nạn nhân thường không biết bị mắc lừa cho đến lâu sau khi nó đã xảy ra. Thứ hai là chúng sử dụng ngay và có kỹ năng ẩn dấu vết. Chúng chỉ tiến hành hoạt động lừa đảo chỉ trong một thời gian hạn chế sau đó dừng lại. Có nghĩa là khi bị tiến hành điều tra hoạt động lừa đảo có sự sẵn sàng dừng lại một thời gian. Thứ ba là các trang web giả mạo thường được thiết lập trên máy chủ công cộng, đôi khi là trên một máy chủ thứ ba bất đắc dĩ. Sau đó, các trang web thường được tháo dỡ ngay sau khi thủ phạm đã có đủ lượng dữ liệu cá nhân. Những yếu tố này có nghĩa là loại tội phạm này phải điều tra càng sớm càng tốt ngay sau khi xảy ra.

1.4.1.2 Tấn công hoặc sử dụng phần mềm gián điệp

Với một số chuyên gia bảo mật, có thể kì lạ khi phân loại tội phạm sử dụng tấn công và phần mềm gián điệp với nhau, nhưng khi nói đến việc đánh cắp định danh, thì cả tấn công lẫn sử dụng phần mềm gián điệp đều có cùng một mục tiêu: Đạt quyền truy cập vào hệ thống máy tính để có được dữ liệu cần thiết.

➤ **Tấn công:** Là một hoặc một chuỗi các hành động cố gắng vượt qua sự an toàn của hệ thống để truy cập vào dữ liệu không có chủ quyền. Có nhiều cách để thực hiện tấn công, bao gồm cả việc tìm kiếm một số lỗ hổng trong hệ điều hành khai thác, tấn công từ xa hợp pháp để truy cập được vào hệ thống mục tiêu, liên quan đến hầu hết các kiến thức cơ bản của mạng và hoạt động của hệ thống. Bất cứ phương pháp nào được sử dụng, nếu hệ thống mục tiêu

có dữ liệu cá nhân mà thủ phạm muốn, chúng có thể nhận được toàn bộ dữ liệu từ hệ thống máy tính. Khi nói đến tấn công, có một thuật ngữ mà người ta thường nhắc đến, đó là Hacker.

Thuật ngữ hacker được sử dụng trên hầu hết các phương tiện truyền thông biểu thị kẻ xâm nhập bất hợp pháp vào hệ thống. Trong hai thập kỷ qua, những thuật ngữ đã trở nên phổ biến đó là Hacker mũ trắng, Hacker mũ đen và Hacker mũ xám.

- + Hacker mũ trắng là những người sử dụng các kỹ năng của mình để bảo vệ hệ thống. Hacker mũ trắng chỉ thực hiện xâm nhập vào hệ thống khi được cho phép bởi người quản trị hệ thống. Đó thường là thực hiện các thử nghiệm nhằm tìm ra các điểm yếu trên hệ thống để người quản trị có thể vá các điểm yếu trước khi bị kẻ xấu lợi dụng tấn công.
- + Trái ngược với hacker mũ trắng là hacker mũ đen. Hacker mũ đen tiến hành các hoạt động bất hợp pháp, gắn liền với tội phạm máy tính. Thuật ngữ này đồng nghĩa với cracker. Thông thường khi các phương tiện truyền thông thảo luận về hacking, họ đề cập đến hacker mũ đen.
- + Hacker mũ xám là thuật ngữ để chỉ về các hacker vừa mang tính chất hacker mũ trắng vừa mang tính chất hacker mũ đen. Họ có thể vi phạm pháp luật, nhưng thường là không có mục đích xấu.

Ví dụ một người tiến hành kiểm tra thâm nhập cho các công ty là một hacker mũ trắng. Hacker mũ xám là hacker đứng giữa, mặc dù thường xuyên bên ngoài pháp luật. Một hacker mũ xám có thể cố gắng tìm ra điểm yếu trong hệ thống mà không cần sự cho phép của chủ sở hữu hệ thống, nhưng là tìm vị trí chứ không phải là khai thác chúng, các hacker mũ xám sẽ thông báo cho chủ sở hữu của hệ thống. Không dễ dàng để hiểu được hacking. Mặc dù nhiều phim cho thấy có thể truy cập vào hệ thống bảo mật cao trong vài phút, điều này hẳn là không đúng sự thật. Hacking giống như một vụ trộm cần có mục tiêu, kỹ năng và thời gian để xâm nhập. Và cũng như các vụ trộm, xâm nhập vào hệ thống an toàn đòi hỏi phải có kỹ năng và kiến thức chuyên sâu. Một hacker có tay nghề cần hiểu biết rõ về hệ điều hành mạng và các biện pháp an ninh. Hacker giỏi rất hiếm.

➤ **Phần mềm gián điệp:** Phần mềm gián điệp cũng có mục tiêu thu thập dữ liệu cá nhân từ máy tính mục tiêu. Không giống như hacking tuy nhiên mục tiêu duy nhất của phần mềm gián điệp là để có được dữ liệu. Nó thường liên quan đến một số phần mềm được tải về của máy tính mục tiêu. Phần mềm có thể ghi lại tên, mật khẩu người dùng, các tổ hợp phím, các trang web truy cập hoặc các dữ liệu khác. Thậm chí có những sản phẩm phần mềm gián điệp có thể chụp ảnh màn hình định kỳ, ghi lại mọi hoạt động trên màn hình. Trong một số trường hợp, điều này có thể được thực hiện bằng các phần mềm gián điệp theo định kỳ hoặc tải dữ liệu đến một địa chỉ Internet cụ thể, từ đó thủ phạm có thể truy cập bất hợp pháp đến dữ liệu. Nếu thủ phạm đặc biệt có tay nghề, địa chỉ này sẽ là một máy chủ bên thứ ba hoàn toàn không liên quan đến tội phạm. Phần mềm gián điệp rất phổ biến vì 2 lý do. Đầu tiên, nó khá dễ dàng có được. Đó là bởi vì nhiều sản phẩm với mục đích hợp pháp có thể sử dụng như phần mềm gián điệp. Ví dụ sản phẩm được thiết kế để giám sát truy cập web cho trẻ em, năng suất lao động, hoặc cho mục đích hợp pháp khác cũng có thể được sử dụng như phần mềm gián điệp. Thứ hai thật là dễ dàng để cung cấp. Thường thì phần mềm gián điệp được gửi qua một con Trojan có nghĩa là phần mềm có mục đích hữu ích mà còn cung cấp một số tin nguy hiểm. Ví dụ khi tải về một trò chơi miễn phí hoặc mã chứng khoán từ Internet, người dùng cũng vô tình tải về phần mềm gián điệp.

Cả tấn công và phần mềm gián điệp có thể dễ dàng điều tra hơn là tội phạm giả mạo. Vì phần mềm gián điệp để lại dấu vết rõ ràng, dữ liệu thu được phải truyền đi một nơi nào đó. Vấn đề thực sự với cả phần mềm gián điệp và tấn công đó là mức độ kỹ năng của thủ phạm.

1.4.1.3 Truy cập trái phép dữ liệu

Truy cập trái phép dữ liệu là hành vi truy cập đến dữ liệu mà không được phép. Hành vi phổ biến là khi một người có quyền hợp pháp một số nguồn dữ liệu cụ thể hoặc là để truy cập dữ liệu không được phép hoặc sử dụng các dữ liệu một cách khác hơn so với cách họ được ủy quyền. Một ví dụ là nhân viên bệnh viện truy cập hồ sơ bệnh nhân sử dụng các dữ liệu để ăn cắp thông tin của bệnh nhân. Hoặc một người không có quyền truy cập vào tất

cả những hồ sơ ấy. Ví dụ này sẽ là một hacker đột nhập vào hệ thống để ăn cắp dữ liệu.

Phương pháp phổ biến nhất của loại tội phạm này là đăng nhập với tài khoản của người khác. Điều đó cho phép thủ phạm có thể truy cập đến các tài nguyên hoặc dữ liệu mà người có mật khẩu đã được truy cập và sử dụng bởi nhiều người đặt mật khẩu yếu, tệ hơn là viết mật khẩu của họ ra bàn cho dễ nhớ hoặc chia sẻ mật khẩu với người khác. Ví dụ, một người quản lý bị bệnh nhưng cần kiểm tra xem khách hàng có gửi email hay không nên đã gọi cho trợ lý đăng nhập email của mình. Như vậy, trợ lý có thể sử dụng tài khoản đó hoặc tiết lộ cho người khác (vô tình hay cố ý), có nghĩa là bây giờ có một cơ hội lớn cho những người khác sử dụng đăng nhập vào mà người quản lý truy cập dữ liệu không cho phép. Có nhiều lý do đằng sau những truy cập trái phép này. Có thể là tò mò đơn giản, muốn biết những gì không biết như lương hay thông tin cá nhân của các nhân viên khác. Tuy nhiên cũng có những lý do nghiêm trọng hơn như: đánh cắp danh tính, lấy danh sách khách hàng trước khi rời khỏi công ty với mục đích ăn cắp khách hàng hay bán nghiên cứu nhạy cảm của công ty cho một đối thủ cạnh tranh,... Đây là lý do tại sao kiểm soát truy cập trái phép dữ liệu phải được thực hiện nghiêm túc bởi các chuyên gia an ninh mạng và pháp luật.

1.4.1.4 Dựa vào thông tin rác

Các cá nhân cũng như tổ chức thường xuyên loại bỏ dữ liệu cũ cũng là một cách tiếp cận cho bọn tội phạm. Có thể là bất cứ dữ liệu nào từ các hóa đơn cũ ném vào thùng rác để loại bỏ các sao lưu. Từ đó thủ phạm có thể có được các phương tiện truyền dữ liệu (giấy, đĩa mềm, ổ đĩa...) từ thùng rác và sau đó lấy dữ liệu cá nhân. Trong năm 2004, một cơ quan tuyển dụng quân đội Mỹ ở khu vực Dallas đã tìm thấy hồ sơ bị loại bỏ của một tân binh mới trong thùng rác. May mắn là các dữ liệu được phát hiện bởi một phóng viên mà không phải một tên trộm danh tính. Từ góc độ Pháp luật, điều tra loại tội phạm này cũng khó khăn. Xác định nguồn gốc của dữ liệu khi bị bỏ đi là đơn giản, nhưng việc xác định thủ phạm thực tế có thể rất khó khăn.

1.4.2 Rình rập, quấy rối

Tội phạm loại này là tương đối mới và ngày càng phát triển. Hành vi của tội phạm này đó là bạo lực, trong đó có tấn công tình dục và giết người. Hầu hết các quốc gia đã từ lâu thông qua nhiều luật chống rình rập, những hành vi này gần đây đã mở rộng trên không gian mạng. Thủ phạm sử dụng Internet để sách nhiễu, đe dọa người khác. Hoặc như Bộ tư pháp Mỹ đưa ra:

“ Không có định nghĩa cụ thể về tội phạm rình rập trên mạng, đó có thể là việc sử dụng internet, thư điện tử, hoặc các thiết bị thông tin liên lạc điện tử khác để theo dõi người khác. Tội phạm rình rập nhìn chung là hành vi quấy rối hoặc đe dọa một cá nhân ví dụ như theo dõi một người, xuất hiện ở nhà của một người hoặc địa điểm kinh doanh, thực hiện cuộc gọi quấy rối, để lại lời nhắn bằng văn bản hoặc là phá hoại tài sản. Hầu hết các luật liên quan đến tội phạm rình rập là mối đe dọa đối với nạn nhân, gia đình nạn nhân. Trong một số hành vi liên quan đến hành vi gây phiền nhiễu hay đe dọa có thể là rình rập bất hợp pháp, hành vi như vậy có thể là mở màn cho bạo lực và cản trở trị nghiệm túc. ”

Điều đó có nghĩa là nếu một người sử dụng Internet theo dõi nhằm mục đích quấy rối, đe dọa người khác thì đó là tội phạm rình rập trên mạng. Một ví dụ điển hình về rình rập trên mạng là việc gửi email đe dọa. Nhưng định nghĩa về quấy rối, đe dọa hiện nay rất mơ hồ. Rõ ràng, nếu một người gửi email cho một người đe dọa giết người và cung cấp hình ảnh của người nhận để chứng minh rằng người gửi quen thuộc với sự xuất hiện của mục tiêu, đó chính là rình rập trên mạng. Cũng có những email có một đe dọa mơ hồ, chẳng hạn như “ Mày sẽ nhận được những gì xứng đáng” liệu có phải là rình rập? Đây không phải là một câu hỏi dễ trả lời, và không có câu trả lời duy nhất cho tất cả tình huống. Thế nào là đe dọa, quấy rối khác nhau rất nhiều từ thẩm quyền, nhưng hướng dẫn chung là nếu các email (hoặc tin nhắn) nội dung bất thường sẽ được coi là đe dọa trong lời nói bình thường, sau đó sẽ có thể được coi là mối đe dọa nếu được gửi bằng điện tử. Vậy để tìm ra mối đe dọa thì điều quan trọng là tìm ra bốn yếu tố sau:

➤ **Độ tin cậy:** Điều này dễ dàng xác định. Đối với mỗi đe dọa cho là đáng tin cậy, phải có dấu hiệu hợp lý rằng nó có thể được thực hiện. Ví dụ một phụ nữ ở Nebraska đang thảo luận trên Internet và nhận được mối đe dọa

chung từ một người dùng sống tại Bangkok trong một quá trình tranh luận. Trong tình huống này, người gửi rất có thể không biết nơi sống của người nhận. Trên thực tế có người sử dụng tên ảo trên Internet, người gửi có thể thậm chí không biết tên, giới tính, tuổi tác của người nhận thực tế. Có nghĩa là mối đe dọa này có độ tin cậy thấp. Tuy nhiên nếu người phụ nữ ở Nebraska nhận được mối đe dọa từ người sử dụng tại Bangkok đi kèm với thông tin cá nhân như địa chỉ, nơi làm việc, hoặc một bức ảnh đó là mối đe dọa tin cậy.

➤ **Tần suất:** Đưa ra nhận xét thiếu khôn ngoan trên Internet, một lời nhận xét thù địch chỉ là phản ứng gay gắt, quá nhanh trên Internet. Loại hình này đã bình luận trong một phòng chat hoặc trên một thông báo. Thường xuyên quấy rầy ý kiến và đe dọa theo thời gian, dần dần xây dựng để chỉ nơi họ sẽ hành động. Trong khi đó chắc chắn có thể là trường hợp mối đe dọa điều tra đảm bảo duy nhất, như một quy luật chung, các mối đe dọa cô lập là mối quan tâm ít hơn một mô hình của quấy rối và đe dọa.

➤ **Đặc trưng:** Đề cập đến thủ phạm liên quan đến bản chất của các mối đe dọa, các mục tiêu của các mối đe dọa, và các phương tiện thực hiện các mối đe dọa. Tất nhiên, nó rất quan trọng với cán bộ thực thi pháp luật để nhận ra rằng mối đe dọa thực tế đôi khi có thể mơ hồ. Nói cách khác, mối đe dọa thực sự sẽ không luôn luôn cụ thể. Nhưng mối đe dọa thường có thật. Ví dụ một người nào đó nhận được một email nói rằng “*Mày phải trả giá cho điều đó*” ít quan tâm hơn một email có chứa một mối đe dọa cụ thể của bạo lực, chẳng hạn như “*Tao sẽ chờ mày sau khi làm việc và bắn vào đầu mày*” cùng với một bức ảnh để lại nơi làm việc của người nhận. (Hình ảnh này cũng làm cho nó rất đáng tin cậy). Mối đe dọa này rất cụ thể và cần được quan tâm hơn trong khi thực thi pháp luật.

➤ **Cường độ:** Vấn đề này đề cập đến những giai điệu chung của truyền thông, bản chất của ngôn ngữ và cường độ của các mối đe dọa. Mối đe dọa bạo lực phải luôn được thực hiện nghiêm túc thực thi pháp luật. Thông thường, khi một người nào đó chỉ đơn giản là thông báo hoặc phản ứng thái độ có thể lập báo cáo coi là đe dọa, nhưng trong trường hợp này hầu hết mọi người lập báo cáo cường độ thấp, chẳng hạn như đe dọa để đánh bại một người nào đó. Các mối đe dọa như này ít quan tâm hơn đó là mối đe dọa chia cắt một ai đó. Điều này là do bình thường những người bất bạo động, có thể mất bình tĩnh.

Nhưng bình thường, những người bất bạo động không thường mất bình tĩnh và muốn cắt một người nào đó thành miếng bằng cưa máy. Bất cứ lúc nào có mối đe dọa lớn lên đến mức độ vượt quá những gì một người bình thường có thể nói, ngay cả trong một tình huống thù địch, các mối đe dọa sẽ trở thành mối quan tâm lớn hơn.

Hiện nay thì tất cả bốn tiêu chí trên cần phải xem xét để xác định một mối đe dọa là khả thi. Cán bộ thực thi pháp luật phải luôn dựa vào tình huống và phải luôn luôn nghi vấn về phía cảnh báo.

1.4.3 Truy cập bất hợp pháp tới hệ thống máy tính và các dữ liệu nhạy cảm

Truy cập trái phép vào hệ thống máy tính hoặc dữ liệu có thể được cho là mục đích khác hơn so với tội phạm đánh cắp định danh. Ví dụ, thủ phạm có thể muốn ăn cắp dữ liệu bí mật của công ty, tài liệu tài chính nhạy cảm hoặc các dữ liệu khác. Thông tin này có thể được sử dụng để thu hút khách hàng từ đối thủ cạnh tranh, phát hành để làm hỏng cổ phiếu của công ty, hoặc sử dụng để tống tiền. Trong mọi trường hợp, các yếu tố phổ biến là thủ phạm hoặc là không được cho phép truy cập dữ liệu hoặc không được phép sử dụng dữ liệu vậy mà cố tình sử dụng nó. Các phương pháp tương tự như bất kể mục đích của các truy cập trái phép. Nó có thể được thực hiện thông qua hacking hoặc phần mềm gián điệp, các nhân viên truy cập dữ liệu hoặc thông qua phương tiện truyền thông dữ liệu bị loại bỏ. Đặc biệt, hành vi trộm cắp dữ liệu là một vấn đề quan trọng, lý do chính là khó khăn để ngăn chặn nhân viên được phép truy cập đến dữ liệu. Đôi khi cũng rất khó để phân biệt giữa các truy cập trái phép và được phép.

1.4.4 Lừa đảo trực tuyến

Tội phạm lừa đảo khá phổ biến. Một trong số các hành vi lừa đảo trực tuyến trên Internet bao gồm:

- Lừa đảo đầu tư.
- Lừa đảo giao dịch.
- Nhận/ lừa đảo tiền đặt hàng.
- Vi phạm bản quyền dữ liệu.

1.4.4.1 Lừa đảo đầu tư

Là phần tư vấn, môi giới đầu tư không hợp pháp, đây không phải là một trào lưu mới mà cũng không hẳn là một hoạt động phạm tội. Thậm chí một số môi giới chứng khoán hợp pháp chứng tỏ sự sinh tồn của họ đơn giản chỉ là kêu gọi mọi người đầu tư vào một cổ phiếu cụ thể. Mặc dù thực tế điều này đôi khi được sử dụng bởi các nhà môi giới chứng khoán hợp pháp, nhưng đây lại là một phương pháp khá phổ biến với những tội phạm lừa đảo. Khái niệm này thường được gọi là “*bơm và rút tiền*”: Tội phạm mua một số lượng đáng kể cổ phiếu có giá trị thấp. Sau đó, chúng sử dụng những chiêu để làm tăng nhu cầu đối với cổ phiếu và từ đó giá cổ phiếu được đẩy lên. Chúng cũng có thể đưa ra những lời khuyên giả, cho thấy các công ty để đảm bảo một hợp đồng lớn của chính phủ hoặc một bằng sáng chế, hoặc để phát hành một sản phẩm đột phá mới. Khi các cổ phiếu đã được đẩy lên mức cao, thủ phạm sẽ bán cổ phiếu khi đó các công ty sản xuất không được lợi, giá cổ phiếu sau đó trở về mức ban đầu của nó và có khi còn thấp hơn. Đây mới chỉ là một ví dụ về lừa đảo đầu tư.

Máy tính và Internet không làm thay đổi quá trình cơ bản của các chương trình lừa đảo, chúng chỉ làm cho tội phạm dễ dàng thâm nhập hơn. Chìa khóa của lừa đảo kiểu này đó là thay vì kêu gọi thông qua điện thoại, chúng gửi một bức thư điện tử hấp dẫn đến càng nhiều người càng tốt. Tất nhiên, thủ phạm nhận ra rằng hầu hết mọi người sẽ không đáp trả những email hấp dẫn ấy, nhưng nếu 1/10% làm theo, thủ phạm gửi lên đến một triệu email, vẫn có thể đẩy lên một số tiền đáng kể. Đây là một lý do tại sao thư rác lại là một vấn đề: phần lớn các thư rác nhận được thực sự là một phần của một số hành vi lừa đảo.

Có rất nhiều biến thể lừa đảo trên mạng. Một ví dụ phổ biến là gửi cho các nạn nhân một email dường như là từ một người nổi tiếng ở nước ngoài. Người đó cần sự giúp đỡ của người nhận trong việc chuyển giao một khoản tiền lớn từ đất nước của mình tới một ngân hàng ở Hoa Kỳ. Trong một số tình huống, người gửi yêu cầu thông tin tài khoản ngân hàng của người nhận để chuyển tiền vào tài khoản đó. Tất nhiên cuối cùng là chuyển tiền ra khỏi tài khoản của nạn nhân. Một cách tiếp cận phổ biến hơn là nói các nạn nhân phải

nhận một khoản phí nhỏ để xử lý chuyển giao. Thủ phạm thu phí và không bao giờ thấy xuất hiện nữa.

Những tội phạm loại này cũng khó khăn để điều tra. Phải truy tìm lại email nhưng đôi khi chúng lại không hữu ích. Các email thường được gửi từ những tài khoản vô danh mà khó có thể theo dõi được. Để theo dõi thì phải kiểm tra các tài liệu thực tế và kiểm tra đường truyền tới một địa chỉ mail thực tế. Thông thường, địa chỉ này là một hộp buro điện, không phải là văn phòng hoặc một nơi cư trú nào đó.

1.4.4.2 Lừa đảo giao dịch trực tuyến

Hiện nay giao dịch đấu giá trực tuyến khá phổ biến. Người dùng hợp pháp có thể khó khăn xác định một mức giá tốt, hoặc loại bỏ các mặt hàng không còn nhu cầu. Cũng như nhiều địa điểm kinh doanh hợp pháp, tuy nhiên, bọn tội phạm nỗ lực thao tác lừa đảo để ăn cắp từ các nạn nhân. Ủy ban thương mại Liên bang Mỹ (FTC) liệt kê bốn phạm trù sau của lừa đảo giao dịch trực tuyến:

- Không giao hàng hóa.
- Giao hàng có giá trị thấp hơn so với quảng cáo.
- Cung cấp hàng hóa không đúng thời hạn.
- Không tiết lộ các thông tin liên quan về một sản phẩm hoặc các điều khoản của người bán.

Đầu tiên là không giao hàng hóa. Đây là một hành động rõ ràng. Nạn nhân gửi tiền và người bán không giao hàng. Loại tội phạm này dễ dàng điều tra, truy tố. Loại thứ hai, giao hàng có giá trị thấp hơn, có nhiều khó khăn hơn để điều tra và truy tố loại này. Người bán luôn có thể nói người mua hiểu lầm về thông báo đấu giá được diễn đạt một cách mơ hồ. Hai loại cuối thì thường không có bị cáo để thực thi pháp luật và trong nhiều trường hợp cũng không cấu thành tội để điều tra. Nếu không cung cấp kịp thời vật chứng thì rõ ràng không phải là một tội phạm, nhưng trong hoàn cảnh khác có thể đặt vấn đề là một vụ kiện dân sự. Việc không tiết lộ những thông tin liên quan tương tự như là giao cái gì đó nhỏ hơn giá trị và có thể khó điều tra hoặc truy tố.

1.4.4.3 Lừa đảo nhận/ chuyển tiền

Một loạt các trò gian lận trên Internet có liên quan đến việc trao đổi một lệnh chuyển tiền giả hoặc ký séc tiền thật. Các chương trình gian lận khá phổ biến trên các trang web Craigslist. Nạn nhân có một số mặt hàng bán trên Craigslist chẳng hạn như một chiếc đồng hồ đẹp. Tội phạm liên lạc với nạn nhân và đồng ý mua hàng. Tuy nhiên, thủ phạm tuyên bố sống bên ngoài khu vực và phải có một người đến nhận hàng. Sau đó đến lấy hàng và ký séc giả mạo không có giá trị gì.

1.4.4.4 Vi phạm bản quyền dữ liệu

Vi phạm bản quyền là các hành vi trộm cắp tài sản trí tuệ. Trong nhiều năm qua, vấn đề vi phạm bản quyền liên tục được nhắc đến. Có thể đó là bản quyền phần mềm, bài hát, đoạn phim,... được trao đổi, mua bán mà chưa có sự đồng ý từ tác giả. Và dù cho người đó có được người sở hữu cho sử dụng thì đưa nó cho bạn bè, hoặc bán nó vẫn là hành vi phạm tội. Thông thường thì các trường hợp đó là vấn đề dân sự. Vụ kiện sẽ ngăn chặn cả thủ phạm và giải quyết thiệt hại bằng tiền một cách đáng kể. Mặc dù hầu hết mọi người đã quen thuộc với các khái niệm phần mềm lậu và tải nhạc bất hợp pháp, có một nhóm vi phạm bản quyền dữ liệu có liên quan đến hành vi trộm cắp danh tính. Trong một số trường hợp, cá nhân ăn cắp danh tính, không sử dụng mà mang bán chúng. Người mua có thể là người nước ngoài bất hợp pháp muốn tài liệu hướng dẫn về việc làm hoặc một kẻ chạy trốn muốn có một danh tính khác. Ngày nay có cả một thị trường chợ đen ngày càng phổ biến về dữ liệu bị đánh cắp.

1.4.5 Phát tán tin rác, mã độc hại

Một dạng tội phạm nữa rất phổ biến hiện nay là tội phạm chuyên thực hiện các hành vi phát tán tin rác, mã độc hại. Phát tán tin rác là hành vi gửi các tin nhắn hoặc các email chứa nội dung quảng cáo, marketing và được gửi một cách vô tội vạ gây phiền toái cho người nhận. Đôi khi, nó dẫn dụ người nhẹ dạ, tìm cách đọc số thẻ tín dụng và các tin tức cá nhân của họ. Theo thống kê từ hãng bảo mật Kaspersky Lab tháng 6-2013, tỉ lệ thư rác chiếm trung bình đến 71,1% lượng thư điện tử toàn cầu. Trong đó hơn một nửa số thư rác có nguồn gốc từ Trung Quốc (23,9%) và Mỹ (17,2%) - hai quốc gia hàng đầu

về phát tán thư rác. Việt Nam xếp vị trí thứ sáu với tỉ lệ phần trăm thư rác chiếm khoảng 3,3%.

Viết mã độc - Phát tán mã độc là một trong những hình thức tấn công mới trên mạng. Kẻ tấn công sử dụng các chương trình mã độc để lây nhiễm vào các hệ thống, phần mềm nhằm mục đích phá hoại hệ thống hoặc đánh cắp các thông tin trái phép. Để thực hiện phát tán mã độc, kẻ tấn công thường gửi một email có chứa mã độc tới nạn nhân hoặc đính kèm trong một phần mềm phổ dụng; người dùng chỉ cần kích hoạt chương trình là mã độc sẽ tự động lây nhiễm vào hệ thống. Như vậy, kẻ tấn công có thể theo dõi toàn bộ hoạt động trên hệ thống bị lây nhiễm hoặc sử dụng hệ thống bị lây nhiễm như một công cụ thực hiện tấn công tới các đối tượng khác.

Chương 2

MỘT SỐ HÀNH VI CỦA TỘI PHẠM MÁY TÍNH

2.1 TRỘM CẤP THÔNG TIN

Một trong những hành vi thường thấy của tội phạm máy tính là trộm cắp thông tin. Mục tiêu của hành động này là đánh cắp các thông tin về một cá nhân và thực hiện giả mạo người đó để có được thẻ tín dụng, truy cập vào các tài khoản ngân hàng, thực hiện các giao dịch bất hợp pháp qua mạng. Tuy nhiên, cũng có những trường hợp không nhằm vào mục đích tài chính mà họ trộm cắp thông tin để phục vụ cho một cuộc tấn công, hay đơn giản chỉ là muốn tìm hiểu về đối tượng.

Các hành vi trộm cắp thông tin ngày nay rất phổ biến trên Internet bởi có rất nhiều thông tin cá nhân có sẵn trên các mạng xã hội. Thủ phạm sẽ tìm kiếm một loạt thông tin thực sự có thể tiếp cận tới các tài sản tài chính. Thủ phạm có thể truy cập trực tiếp vào tài khoản ngân hàng, hoặc đủ thông tin mà người đó có thể mở tài khoản tín dụng với tên nạn nhân. Có nghĩa là loại tội phạm này muốn tên đăng nhập, mật khẩu của nạn nhân trong các trang web tài chính hoặc đủ dữ liệu cá nhân để thủ phạm có thể có được thẻ tín dụng.

Có hai cách mà thủ phạm hay sử dụng để trộm cắp thông tin, đó là :

- + Giả mạo.
- + Sử dụng phần mềm gián điệp.

2.1.1 Giả mạo

Chỉ đơn giản là quá trình gửi email cho hàng loạt, trong đó các email có mục đích từ một số nguồn hợp pháp và lôi kéo người nhận cung cấp thông tin cá nhân hoặc nhấn vào một liên kết trong email đến một trang web cung cấp

thông tin cá nhân. Kịch bản phổ biến nhất hiện nay là các email từ một ngân hàng hoặc thẻ tín dụng và thông báo cho nạn nhân một số vấn đề về tài khoản của họ, sau đó sẽ yêu cầu nạn nhân nhấp chuột vào một liên kết để đăng nhập vào tài khoản. Liên kết sẽ đưa nạn nhân đến một trang web khác giống như là một tổ chức tài chính hợp pháp. Khi đó nếu thực hiện đăng nhập vào, nạn nhân sẽ bị đánh cắp tên đăng nhập và mật khẩu.

Bước đầu tiên với hành vi này là tội phạm phải thiết lập một máy chủ để lưu trữ các trang web lừa đảo mà không thể truy cập trở lại. Có hai cách thực hiện: một là sử dụng thẻ Visa trả trước để mua web lưu trữ trên một dịch vụ lưu trữ thường được sử dụng, tốt nhất là sử dụng nước ngoài; hai là thủ phạm tấn công bất kỳ máy chủ nào có độ bảo mật kém, sau đó thủ phạm có thể sử dụng máy chủ để lưu trữ các trang web lừa đảo của mình. Thông thường các tội phạm sẽ sử dụng phương pháp thứ hai. Điều đó lý giải tại sao nhận thức về an ninh mạng là rất quan trọng với tất cả những người tham gia mạng máy tính. Khi một máy tính đang được sử dụng cho một cuộc tấn công và bị tấn công như trường hợp trên, máy tính được gọi là một zombie. Việc sử dụng các zombie trong lừa đảo để phát tán nội dung khiêu dâm trẻ em, hoặc để tung ra các cuộc tấn công từ chối dịch vụ đã trở thành khá phổ biến.

Bước tiếp theo là cạnh tranh với trang web của một số tổ chức tài chính. Điều này có thể được thực hiện bằng cách truy cập các trang web hợp pháp cho các tổ chức tài chính và sao chép càng nhiều đồ họa và bố trí càng tốt. Trong nhiều trường hợp, chỉ cần nhấp chuột vào hình ảnh trên bất kỳ trang web và lưu nó. Hay cũng có thể là click chuột vào trang và xem mã nguồn thực tế cho trang đó. Điều này là vấn đề đơn giản để có thể sao chép một trang web và sau đó sử dụng các đồ họa, bố cục đánh cắp tạo một trang web mô phỏng trang web tài chính càng giống mục tiêu càng tốt. Một phần quan trọng đó là làm thế nào để lấy cắp được thông tin đăng nhập của người dùng. Thông tin của nạn nhân có thể được lưu trữ trong một tập tin, cơ sở dữ liệu, hoặc bất kỳ phương tiện mà thủ phạm mong muốn. Kẻ trộm danh tính xảo quyệt hơn cũng sẽ thu thập các địa chỉ IP và email từ người ghé thăm trang web của chúng. Khi người dùng đã đăng nhập vào trang web của tổ chức giả mạo, các trang web lừa đảo sẽ hiển thị một tin nhắn hoặc cảm ơn

người dùng đã xác nhận đăng nhập của họ hoặc thông báo rằng thông tin tài khoản là hiện không có sẵn và xin vui lòng thử lại .

Bây giờ điều duy nhất còn lại đó là thủ phạm lấy cắp thông tin. Điều này thực sự đơn giản chỉ cần đăng nhập vào máy chủ và sao chép thông tin. Thủ phạm khéo léo hơn sẽ làm điều này từ một địa điểm truy cập như một quán cafe có Internet, chắc chắn có nhiều trường hợp thủ phạm không đăng nhập vào máy chủ tại nhà riêng của chúng. Các trang web không có thật cũng có thể được lập trình để gửi thông tin định kỳ đã thu thập được. Quá trình này xảy ra khá thường xuyên.

2.1.2 Sử dụng phần mềm gián điệp

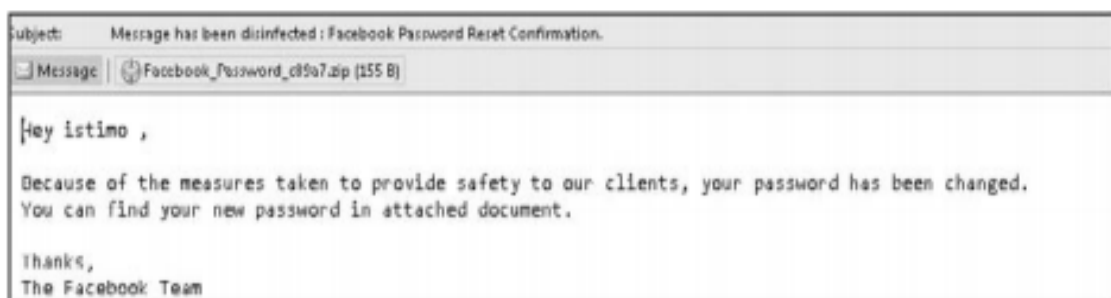
Một phương pháp khác để trộm cắp thông tin cá nhân là cài phần mềm gián điệp vào máy tính của mục tiêu và thu thập thông tin trực tiếp từ bàn phím, màn hình hoặc các hoạt động xảy ra trên máy tính nạn nhân. Dạng phần mềm gián điệp phổ biến là keylogger. Keylogger chuyên ghi lại các thao tác trên bàn phím vào một tập tin nhật ký để người cài đặt nó xem. Nó là loại phần mềm gián điệp có thể chụp lại màn hình định kỳ chính xác những gì có trên màn hình và lưu chúng vào một tập tin. Dữ liệu được lưu trữ tạm thời trên máy tính của nạn nhân, sau đó thủ phạm phải lấy được những dữ liệu đó ra. Có một số cách để thực hiện việc này. Một là sẽ có phần mềm gián điệp gửi định kỳ dữ liệu đó đến một địa chỉ email hoặc một địa chỉ IP được xác định trước. Cách khác đó là kẻ tấn công truy cập vào máy tính mục tiêu và đăng nhập vào để lấy dữ liệu. Trường hợp này, kẻ tấn công có thể đã từng đột nhập vào máy tính và cài đặt phần mềm gián điệp, sau đó có thể trở lại để thu thập dữ liệu.

Đôi khi, phần mềm gián điệp cũng có thể được sử dụng trong các tấn công leo thang đặc quyền. Leo thang đặc quyền là hành vi cố gắng để có thể có được những tài khoản người dùng đăng nhập và thúc đẩy khả năng tiếp cận. Ví như thủ phạm có thể đăng nhập vào một máy trạm windows 7 như một tài khoản khách. Bây giờ, tài khoản khách có quyền truy cập rất hạn chế. Tuy nhiên nếu thủ phạm tải phần mềm gián điệp về máy tính, sau đó người dùng đăng nhập vào, các phần mềm gián điệp sẽ ghi lại hoạt động bao gồm tên người dùng và mật khẩu. Nếu một trong những người dùng có đặc quyền

cao hơn ví như một người hỗ trợ công nghệ với các đặc quyền quản trị viên đăng nhập vào để khắc phục một số vấn đề, sau đó thủ phạm có được thông tin đăng nhập của người đó và có thể truy cập vào máy tính với những quyền rộng hơn.

Cài phần mềm gián điệp vào các máy mục tiêu: Các chương trình phần mềm gián điệp có thể theo dõi tất cả các hoạt động trên máy tính và thu thập thông tin được lấy ra qua một số phương pháp khác nhau. Làm thế nào mà phần mềm gián điệp được cài vào một hệ thống máy tính mục tiêu như vậy? Và làm thế nào để một thủ phạm có thể xâm nhập vào máy tính hoặc hệ thống để tải về dữ liệu thu được. Đó có thể là các thủ phạm xâm nhập vào hệ thống máy tính và tải phần mềm gián điệp về. Tuy nhiên phương pháp này cần rất nhiều thời gian và đòi hỏi trình độ kỹ thuật cao. Cách tốt nhất để cài được phần mềm gián điệp vào máy tính mục tiêu là sử dụng Trojan. Trojan là một chương trình xuất hiện để sử dụng một cách vô hại nhưng trong thực tế được ẩn trong đó là các công cụ có hại như virus, worm, hoặc phần mềm gián điệp khác.

Cũng có thể là khi truy cập một trang web nhất định, phần mềm gián điệp sẽ được tự động tải về. Tất nhiên, nạn nhân sẽ không biết mình đã bị cài đặt phần mềm gián điệp và bị kẻ tấn công kiểm soát. Các tội phạm cũng có thể thực hiện cài đặt phần mềm gián điệp lên máy nạn nhân một cách đơn giản thông qua việc gửi một email đính kèm phần mềm đến nạn nhân và nhắc nhở nạn nhân mở file đính kèm. Nếu người dùng làm theo sẽ tự động cài đặt một tiện ích phần mềm gián điệp trên máy tính. Hình 2.3 cho thấy một email của loại hình này.



Hình 2.1. Cài đặt phần mềm gián điệp qua email

Trong cả hai trường hợp, mục đích là tạo một email có một thông điệp hấp dẫn khuyến khích người nhận mở email lên và do đó cài đặt phần mềm trên máy tính của họ.

Phần mềm gián điệp hợp pháp: Có một số phần mềm gián điệp được sử dụng hoàn toàn hợp pháp. Pháp luật cho phép sử dụng theo dõi lao động của mình để quản lý năng suất, giám sát nhân viên của các công ty. Hiện nay nhiều công ty đã theo dõi cả điện thoại, email, hoặc lưu lượng truy cập web. Bởi các máy tính, mạng và hệ thống điện thoại là tài sản của công ty, tổ chức phân cho người lao động. Trong một số trường hợp như vậy giám sát được coi là một phần cần thiết của an ninh mạng. Qua giám sát các công ty có thể đảm bảo được nhân viên không vô tình tải về một số loại virus, gửi đi bí mật của công ty, hoặc tham gia vào bất kỳ cuộc xâm nhập riêng tư nào. Hay nó cũng hoàn toàn là hợp pháp cho phụ huynh theo dõi hoạt động của con em chưa thành niên của họ. Điều này có thể bảo vệ trẻ em từ kẻ thù trực tuyến. Tuy nhiên với một số nhân viên của công ty có thể gây ra một số phản ứng tiêu cực. Đặc biệt là cha mẹ phải cân nhắc những rủi ro với con cái của họ bởi đó là hành vi vi phạm lòng tin. Lợi dụng các phần mềm hợp pháp này, các tội phạm có thể thực hiện trộm cắp thông tin của nạn nhân mà nạn nhân khó có thể phát hiện được.

Thu thập phần mềm spyware: Do những tiện ích này có mục đích pháp lý, một số công ty đã tạo ra và ứng dụng tích cực phần mềm gián điệp trên thị trường. Chúng ta có thể có được nhiều sản phẩm phần mềm gián điệp miễn phí, hoặc với chi phí rất thấp trên Internet. Có thể kiểm tra các trang web khai thác truy cập như <http://www.cexx.org> cho một danh sách dài các sản phẩm phần mềm gián điệp nổi tiếng có sẵn trên Internet cũng như thông tin về các phương pháp có thể sử dụng để loại bỏ chúng. Trang web phần mềm gián điệp <http://www.spywareguide.com> liệt kê các phần mềm gián điệp có thể giám sát hoạt động máy tính của ai đó. Một ứng dụng keylogger nổi tiếng Absolute Key Logger, Tiny keyLlogger và TypeO. Hầu hết đều có thể được tải miễn phí hoặc với giá rẻ. Một số danh sách các sản phẩm phần mềm gián điệp thương mại được đưa ra ở đây:

- + SpectorSoft (<http://www.spectorsoft.com>)
- + Watcher web (<http://www.webwatchernow.com>)

- + Kid safe gaurdian (<http://www.kidsafeguardian.com>)
- + Soft Activity (<http://www.softactivity.com>)
- + Imonitor soft (<http://www.imonitorsoft.com>)

2.2 PHÁT TÁN MÃ ĐỘC HẠI

Hiện nay mã độc hại đang tràn lan trên mạng, và có thể lây nhiễm vào máy tính bất cứ lúc nào. Để thực hiện phát tán mã độc hại, tội phạm có thể sử dụng các phương thức như sau:

- + Gửi các email có đính kèm mã độc
- + Chèn mã độc vào các website hợp pháp
- + Cài đặt trong các chương trình phần mềm

Email là con đường lây lan mã độc chủ yếu và phổ biến nhất hiện nay. Các tội phạm chỉ cần ngồi tại 1 máy tính, tiến hành thu thập các địa chỉ email và gửi email giả mạo kèm theo file mã độc để lừa người nhận mở các file này. Các email có chứa mã độc được gửi đi gửi thường có nội dung khá “hấp dẫn”, với các tiêu đề như:

- + “Reset your Twitter password” [Thiết lập lại mật khẩu Twitter]
- + “Reset your Facebook password” [Thiết lập lại mật khẩu Facebook]
- + “Outlook Setup Notification” [Thông báo về việc cài đặt Outlook]
- + ...

Và các file đính kèm thường là:

- + news.html
- + open.html
- + index.html
- + ecard.html
- + facebook_newpass.html
- + ..

Khi mở những file .html này, người dùng sẽ bị chuyển hướng truy cập tới các website chứa mã độc khai thác lỗi của Adobe, Java và Internet Explore nhằm tải mã độc xuống máy người dùng. Vì thế, việc mở các file

đính kèm .html có thể coi là sự chấp nhận ghé thăm các website độc hại mà hacker dựng lên.

Phương pháp này dễ thành công, bởi lẽ từ trước đến nay người sử dụng vẫn cảnh giác với các email có đuôi file đính kèm là exe, .zip, .pif vì các định dạng này đã được cảnh báo nhiều về việc bị hacker lợi dụng. Trong khi đó, đối với file đính kèm là .html hầu hết mọi người vẫn cho là an toàn. Hơn nữa, kiểu phát tán này có khả năng qua mặt được các phần mềm diệt virus tích hợp trong các mail server. Bởi vì bản thân file .html đính kèm không chứa mã độc hay mã khai thác lỗi, mà chỉ chứa đường link tới một website của hacker. Do đó, file này rất khó bị phần mềm diệt virus phát hiện.

Ngoài cách gửi email có đính kèm mã độc tới nạn nhân, các tội phạm cũng thường tấn công lên các website hợp pháp và chèn mã độc vào trong website. Người sử dụng khi thực hiện truy cập lên website và vô tình chạy các chương trình Active X, JAVA applets hoặc VBScript... có chứa mã độc thì sẽ bị lây nhiễm mã độc vào máy tính mà không hề hay biết. Bởi lẽ từ trước đến nay, hầu hết mọi người đều nghĩ rằng chỉ có các website tai tiếng như các trang web khiêu dâm, cài đặt phần mềm lậu và các trang web có nội dung tương tự mới có chứa mã độc. Tuy nhiên trên thực tế, các trang web bình thường, hợp pháp lại tồn tại nguy cơ chứa mã độc gấp 10 lần so với các trang web tai tiếng.

Một cách phát tán mã độc nữa là cài đặt mã độc vào trong các chương trình phần mềm. Khi người dùng chạy chương trình có chứa mã độc, song song với chương trình chạy là các mã độc cũng bắt đầu hoạt động và lây nhiễm vào máy tính của họ. Quá trình lây lan của mã độc có thể diễn ra một cách "âm thầm", nạn nhân sẽ khó có thể nhận ra máy tính của mình đã bị nhiễm mã độc bởi vì chương trình bị lây nhiễm vẫn chạy bình thường.

2.3 LỪA ĐẢO

Thông thường trong đời sống chúng ta đã nghe nhiều đến tội phạm lừa đảo. Đây là các hành vi lợi dụng lòng tin, lợi dụng sự thiếu hiểu biết của một số người để chiếm đoạt tài sản của họ. Trong lĩnh vực công nghệ thông tin cũng có dạng tội phạm này, và các hành vi của chúng tinh vi hơn nhiều so với lừa đảo ngoài đời thường.

2.3.1 Lừa đảo thông qua giao dịch

Giao dịch trực tuyến là một lĩnh vực mở ra nhiều cơ hội cho bọn tội phạm. Trước khi có sự ra đời của Internet và mua bán trực tuyến, để thực hiện mua hàng người ta phải thỏa thuận giá cả trực tiếp hoặc qua điện thoại và nếu hai bên đã thỏa thuận được thì người mua sẽ phải trả bằng tiền mặt rồi nhận hàng. Nhưng từ khi có mua bán trực tuyến, để mua hàng, chúng ta chỉ cần lựa chọn các mặt hàng cần mua với giá niêm yết sẵn trên mạng và thực hiện các giao dịch trực tuyến, sau đó vật phẩm sẽ được gửi đến cho chúng ta. Ví dụ như eBay có thể là một cách tuyệt vời để tìm kiếm hàng hóa với giá cả tốt. Tuy nhiên, bất kỳ trang web giao dịch nào cũng có thể chứa đầy nguy hiểm, và liệu sản phẩm nhận được qua giao dịch trực tuyến có thực sự tốt? Dưới đây là những rủi ro đồng thời cũng là các hành vi của giao dịch trực tuyến:

- + Không giao hàng hóa.
- + Giao hàng có giá trị thấp hơn so với quảng cáo.
- + Không tiết lộ các thông tin liên quan về sản phẩm hoặc các điều khoản của người bán

Không giao hàng hóa là ví dụ rõ ràng nhất của loại lừa đảo này. Rất đơn giản đó là sau khi nạn nhân đã trả tiền cho một số sản phẩm mà thủ phạm không gửi hàng hóa và giữ tiền của nạn nhân. Nếu thủ phạm đã lên kế hoạch tốt, toàn bộ quá trình sẽ được thực hiện với một nhận dạng giả mạo và một dịch vụ e-mail ẩn danh. Sau đó thủ phạm sẽ biến mất cùng với số tiền lừa đảo được.

Một dạng tội phạm của loại hình này là lừa đảo giao dịch cùng với hành vi trộm cắp danh tính. Quá trình này đầu tiên là ăn cắp định danh của một số người, sau đó thiết lập các cuộc đấu giá bằng cách sử dụng danh tính bị đánh cắp. Trong phương pháp này, thủ phạm có thể tự bảo vệ mình khi bị điều tra. Nếu một cuộc gian lận xảy ra, bên thứ ba bất đắc dĩ sẽ bị theo dõi chứ không phải thủ phạm.

Loại thứ hai là lừa đảo cung cấp một sản phẩm có giá trị thấp hơn so với một trong những quảng cáo có thể là một vùng xám cho thực thi pháp luật. Ví dụ, giả sử người bán quảng cáo lần đầu tiên ấn bản cuốn tiểu thuyết Stephen King nhưng khi ship thì lại là một phiên bản kém chất lượng. Điều

này có thể là lừa đảo có chủ ý, hoặc có thể chỉ đơn giản là một sai lầm vô ý. Vì vậy rất khó xác định đó là một sai lầm hay một trường hợp lừa đảo. Vấn đề này là gửi một vật phẩm có giá trị thấp hơn có liên quan chặt chẽ đến vấn đề không thông báo tất cả các thông tin có liên quan về các mặt hàng. Ví dụ, một cuốn sách có thể là một bản in đích thực đầu tiên và có được chữ ký tác giả, nhưng khi giao hàng đó lại là một cuốn không có gì cả. Giao dịch trực tuyến đã làm cho tội phạm dễ dàng thâm nhập.

Ủy ban thương mại (FTC) đã liệt kê ba khu vực gian lận giao dịch hiện nay đang phổ biến trên Internet. Từ trang web của FTC.

- **Cò mồi:** Là khi lừa đảo giá vào của các mặt hàng của người bán để đẩy giá lên. Cò mồi giao dịch đã trở thành phổ biến nhất của ba loại gian lận giao dịch niêm yết bởi FTC. Một trong những lý do đó là nó rất dễ dàng thực hiện. Chiến thuật rất đơn giản: Nếu muốn bán một món hàng trên một trang web giao dịch trực tuyến nhưng muốn đảm bảo một mức giá cao, khi đó cò mồi giao dịch có thể được sử dụng. Thủ phạm thiết lập nhiều tài khoản người mua giả và sử dụng để chào giá. Bằng cách này, chúng giả tạo thổi phồng giá lên và tạo ra ảo giác rằng nhu cầu cao. Điều này có thể làm tăng đáng kể giá trị của mặt hàng. Hiện nay sự việc như thế này không có khả năng đến sự chú ý của pháp luật. Trong các trường hợp đó nạn nhân không hề biết có gian lận xảy ra. Từ đó cách duy nhất để xác nhận cò mồi giao dịch là xác định danh tính của tất cả các khách hàng. Tất nhiên, có thể có âm mưu giao dịch với nhau tạo ra, trong trường hợp đó sẽ có thủ phạm cò mồi khác với người bán. Một âm mưu như vậy sẽ được thực hiện liên tục và liên quan đến nhiều cuộc giao dịch trong một khoảng thời gian. Trong trường hợp này, quá trình điều tra sẽ yêu cầu khai thác một số dữ liệu. Chúng ta có thể thấy rằng người bán thường chào giá trên các mặt hàng tương tự nhưng không nhận được phiếu mua hàng. Điều này vẫn là sự xác thực gián tiếp. Để xác định được một âm mưu lừa gạt, chúng ta phải thấy được các cá nhân đã có kết nối với nhau. Một bằng chứng là tình huống trong đó những tên cò mồi giành chiến thắng trong một cuộc giao dịch nhưng không bao giờ trả tiền cho nó và người bán không phàn nàn với các

trang web giao dịch. Đây sẽ là một dấu hiệu rõ ràng chúng đã thông đồng với nhau và cò mồi giao dịch vô tình giành được sản phẩm.

➤ **Chào giá:** Khi mà người mua giả nộp hồ sơ dự thầu rất cao để ngăn cản các nhà thầu khác cạnh tranh. Sau đó rút lại hồ sơ dự thầu cao ấy, và chúng có thể nhận được các món hàng với mức giá thấp hơn. Chào giá hiếm khi có sự chú ý của thực thi pháp luật, đó là một vấn đề cho các trang web giao dịch. Cuối cùng thì nó chỉ đơn giản là một trường hợp nhà thầu muốn xua đuổi hồ sơ dự thầu cạnh tranh. Điều có hại cho các nạn nhân đó là họ không giành phần thắng trong mục họ đã đấu thầu. Sự việc xảy ra ở đây là một người làm cho giá thầu thấp hơn và sau đó kẻ đồng lõa sẽ sử dụng một hồ sơ dự thầu cao hơn khuyến khích những khách hàng khác. Nhưng khi cuộc đấu giá kết thúc và giá thầu cao thuộc về khách hàng tiếp theo. Điều này chắc chắn là gian lận và hiện nay khá phổ biến trên các trang web giao dịch đấu giá, do đó chắc chắn nó là một loại tội phạm máy tính. Tuy nhiên rất khó để điều tra loại tội phạm này. Đầu tiên nó thường không bị phát hiện trừ khi là nạn nhân nhiều lần. Thứ hai đó là khó khăn để chứng minh rằng có sự thông đồng giữa các nhà trung thầu và nhà thầu cao. Nó chỉ bị phát hiện nếu 2 thủ phạm lừa đảo cùng nhau nhiều lần. Cuối cùng hơi khó khăn để truy tố loại tội phạm này vì những món hàng đã không bị đánh cắp, nó đã được trả tiền cho những thiệt hại chỉ đơn giản là người bán bị bán mức giá thấp hơn.

➤ **Bòn rút:** Khi thủ phạm thu hút các khách hàng ra khỏi trang web giao dịch hợp pháp bằng cách cung cấp cùng một mặt hàng với giá thấp hơn, với mục đích lừa người tiêu dùng gửi tiền mà không có bất kỳ điều kiện gì. Thay vào đó khách hàng sẽ mất đi bảo hiểm, các hình thức thông tin phản hồi hoặc bảo lãnh. Ngày nay loại tội phạm này khá phổ biến. Thủ phạm đặt một mục chính đáng trên một trang web giao dịch. Nhưng sau đó, trong các quảng cáo cho mặt hàng đó, chúng cung cấp các liên kết đến các trang web không phải là một phần của trang giao dịch. Người mua không cẩn thận click vào sẽ thấy mình trên một trang web lừa đảo thay thế. Tuy nhiên điều này có thể chỉ đơn giản là một cách để làm tăng lượng truy cập tới trang web khác và không có hành vi gian lận

hay lừa đảo. Đây là tình huống nằm ngoài phạm vi hoạt động thực thi pháp luật. Tất cả các chương trình giao dịch chia sẻ mục tiêu lật đổ quá trình giao dịch bất hợp pháp và công bằng. Quá trình giao dịch đấu giá bình thường là : mọi người đều có cơ hội như nhau để có được những sản phẩm nếu như trả giá cao hơn người mua hàng khác. Người mua sẽ tự định giá sản phẩm mà họ cảm nhận được giá trị của sản phẩm với mình. Giao dịch đấu giá là phương tiện khá tuyệt vời cho thương mại. Tuy nhiên điều đáng lo ngại vẫn là thái độ đạo đức của người tham gia.

2.3.2 Lừa đảo thông qua lời kéo đầu tư kinh doanh bất hợp pháp

Lời kéo đầu tư kinh doanh bất hợp pháp đã trở thành một vấn đề khá phổ biến. Thậm chí với một số nhà môi giới lớn một phần thu nhập đáng kể của họ là do kêu gọi, thuyết phục mọi người đầu tư vào một cổ phiếu nào đó. Hiện nay hầu hết người đọc có thể quen với việc mời gọi cung cấp đầu tư tràn ngập thông qua hộp thư của họ hàng ngày. Một số các thông báo qua email lôi kéo bạn tham gia trực tiếp với một kế hoạch đầu tư cụ thể trong khi các email đó là cung cấp miễn phí các thông tin từ các nhà đầu tư. Trong khi các bản tin trực tuyến hợp pháp có thể giúp nhà đầu tư thu thập các thông tin có giá trị, nhưng một số bản tin trực tuyến cũng có thể là lừa đảo.

– **Lừa đảo đầu tư:** Lừa đảo đầu tư có rất nhiều dạng. Một trong những các phổ biến đó là việc gửi một email cho thấy bạn có thể có một số tiền khá lớn với một số vốn đầu tư tối thiểu. Có lẽ đề án gian lận nổi tiếng nhất là của người Nigeria. Trong đó kịch bản cụ thể đó là có một email được gửi đến một số địa chỉ email khác ngẫu nhiên, mục đích là gửi lời đề nghị đến một khối lượng lớn các email này dù chỉ có một số ít email reply lại nhưng vẫn có một số đáng kể các mục tiêu cho thủ phạm. Mỗi email chứa một thông điệp dường như là từ thân nhân của một số vị bác sỹ hay quan chức chính phủ người Nigeria đã chết. Do đó tăng khả năng lôi kéo của thủ phạm. Đó là một phần kế hoạch tin cậy chung của gian lận đầu tư. Thủ phạm đầu tiên phải đạt được sự tin cậy của các nạn nhân. Đây là lý do tại sao các e-mail luôn tuyên bố là trong mối quan hệ với một số thành viên nổi bật của cộng đồng chẳng hạn như một bác sỹ.

Những phác thảo chung của kế hoạch rất giống nhau. Một người có một khoản tiền mà anh ta muốn chuyển khỏi đất nước của mình, vì lý do an ninh, anh ta không thể sử dụng được các kênh thông thường, anh ta muốn sử dụng tài khoản ngân hàng của bạn để làm quỹ tạm thời. Nếu bạn cho phép anh ta truy cập vào tài khoản của bạn, bạn sẽ nhận được một khoản phí rất lớn. Nếu nạn nhân không đồng ý với sự sắp xếp này, họ sẽ nhận được một loạt tài liệu thuyết phục điều đó là hợp pháp. Nạn nhân sau đó sẽ được yêu cầu ứng trước một số tiền để chi trả cho các loại thuế và lệ phí. Nếu nạn nhân thực sự gửi tiền, thủ phạm đã thành công.

Kế hoạch này cũng như nhiều hành vi gian lận, phụ thuộc vào lòng tham của nạn nhân. Và những trường hợp này có thể là vô cùng khó khăn để điều tra vì chúng thường gây ra từ các tài khoản e-mail ẩn danh hay thuê hộp thư hoặc cũng có thể là được tiến hành ở nước ngoài.

– **Tư vấn đầu tư:** Một số công ty có thuê người viết bản tin trực tuyến để giới thiệu cổ phiếu của họ. Trong khi hoạt động này là không hợp pháp, pháp luật chứng khoán liên bang Mỹ xác định các bản tin được tiết lộ như vậy đó là bất hợp pháp. Thông tin nhận được có thể là hoàn toàn sai lệch bởi đó là một quảng cáo được trả tiền. Cạm bẫy này được coi là một trong những cái bẫy nổi tiếng nhất của tư vấn đầu tư trực tuyến.

Thủ phạm có thể nhờ những bản tin trực tuyến để lừa đảo, chúng chọn một cổ phiếu hầu như vô giá trị, sau đó mua một số lượng lớn cổ phiếu đó và sử dụng một loạt các kỹ xảo thổi phồng giá cổ phiếu. Bằng cách sử dụng gọi điện nhưng hiện nay thì phổ biến là spam email cố gắng thuyết phục mọi người mua cổ phiếu. Chúng cũng có thể tạo lên những tin đồn giả mạo trên Internet tuyên bố các công ty ấy có một số bước đột phá hoặc một số hợp đồng lớn. Tất cả những kỹ thuật khác nhau ấy có cùng mục tiêu : thổi phồng giá cổ phiếu vượt quá giá trị mà thực tế nó có được.

2.4 TẤN CÔNG TRÁI PHÉP

2.4.1 Tấn công thăm dò

Về cơ bản thì hacker cũng giống như một tên trộm, trước tiên là xác định phải làm gì trước khi cố gắng đột nhập vào hệ thống mục tiêu. Trong thuật ngữ máy tính thì điều này được gọi là tấn công thăm dò. Thủ phạm phải

dành thời gian tìm hiểu về hệ thống muốn đột nhập. Một tên trộm thường tìm hiểu về hệ thống báo động, an ninh, giờ hoạt động để tìm kiếm được lỗ hổng để có thể đột nhập vào. Và điều này cũng đúng với các hacker. Một hacker phải học tất cả để tìm ra lỗ hổng của hệ thống mục tiêu.

Để minh họa cho một quá trình tấn công thăm dò, chúng ta tưởng tượng qua ví dụ sau. Giả sử bạn là một thủ phạm có ý định đột nhập vào mạng được sử dụng tại hội trường thành phố (bao gồm cả cảnh sát) cho một thành phố của Metropolis. Trước tiên cần phải tìm hiểu về hệ thống trước khi hack hệ thống. Điều này sẽ giúp hiểu chính xác cách mà tin tức hoạt động trên thực tế.

Bước đầu tiên sẽ là: Tìm kiếm các trang web của thành phố, các đài tin tức địa phương. Mục đích của việc tìm kiếm là tìm thấy bất kỳ thông tin nào liên quan đến cơ sở hạ tầng kỹ thuật và nhân viên của thành phố. Ví như một thiết bị, phần mềm mà thành phố đã mua. Hay một bài báo thảo luận về việc thành phố đã chuyển sang Windows Server 2008, hay bài báo nói thành phố đã trao một hợp đồng mạng tới một nhà cung cấp nhất định. Phải tìm kiếm cả thông tin về nhân viên CNTT. Và sử dụng thông tin này bởi một trong ba cách sau:

- Khi biết được phần cứng và hệ điều hành mà thành phố đang sử dụng, ta có thể tập trung nghiên cứu về lỗ hổng được biết đến trong hệ thống đó. Ví như “tìm kiếm được lỗ hổng được biết đến trong các bộ định tuyến” của mô hình nào đó, hoặc có thể tìm thấy các bài báo hay trang web cụ thể chi tiết lỗ hổng được biết đến trong mô hình định tuyến. Sau đó có thể sử dụng thông tin này để có kế hoạch tấn công cuối cùng.

- Khi biết được tên nhân viên kỹ thuật, ta có thể tìm kiếm được các bản tin được biết đến rộng rãi cho bất kỳ câu hỏi mà những người này đã yêu cầu. Ví dụ nếu tên người quản trị mạng là John Doe, chúng ta sẽ tìm kiếm câu hỏi mà người này đã đăng trên mạng ví như làm thế nào để cấu hình đúng một loại tường lửa, chắc chắn rằng người này không phải có kỹ thuật cao trong phần này. Điều này mang lại cho ta một mục tiêu có giá trị để tấn công.

- Cuối cùng ta có thể tìm kiếm thông tin qua các trang mạng xã hội. Ví dụ như biết tên người quản lý CNTT là Jane Smith, ta có thể tìm kiếm các trang mạng xã hội như MySpace và Facebook để có được thông tin chi tiết về bà Smith. Sau đó ta có thể qua sở cảnh sát và giả là một người hỗ trợ công

nghe làm việc mới cho bà Smith. Ta sẽ thông báo về tên của bà ấy và một sự kiện thực tế về bà ấy (ví dụ như có lẽ rằng chỉ có con gái bà mới dành được một hội chợ khoa học nhà nước). Điều này sẽ là thông tin đáng tin cậy cho người tiếp nhận. Sau đó ta nói rằng cần cập nhật máy tính của bà ấy nhưng đã bị mất mật khẩu và yêu cầu người tiếp nhận cung cấp. Bây giờ tùy thuộc vào khả năng của hacker, có thể đặt một số phần mềm gián điệp (ví dụ như keylogger) vào hệ thống để có thể thu thập được tin tức, ta sẽ hoàn toàn sở hữu được hệ thống mạng mà không cần phải thực hiện bất cứ kỹ thuật gì đặc biệt.

Tiếp theo, ta cần thu thập thông tin về hệ thống mục tiêu. Thường có được dễ dàng nhất khi xâm nhập thông qua một trang web, sau đây là các bước cụ thể mà ta cần phải làm:

1. Ta sẽ sử dụng một công cụ mạng như Whols hoặc một giao diện web tốt ví như <http://cqcounter.com/whois> để theo dõi các tên miền trang web của thành phố và tất cả các cơ quan liên quan (Cảnh sát, vệ sinh môi trường...) cũng như email(máy chủ email). Ta có thể nhận được thông tin này từ các địa chỉ email trên trang web của thành phố và sẽ nhận được:

- a. Địa chỉ IP của máy chủ web và máy chủ email.
- b. Địa chỉ vật lý sẽ biết nếu thành phố tổ chức email riêng của mình và máy chủ web hoặc sử dụng một công ty lưu trữ. Ta sẽ cần những địa chỉ IP dù chỉ là trong một chút.

2. Bước tiếp theo là chạy tên miền web thông qua một công cụ như Netcarf.com. Điều này sẽ cho ta thông tin chi tiết về máy chủ Web, chẳng hạn như hệ điều hành mà nó đang chạy và trong bao lâu thì nó được khởi động lại.

3. Bằng cách sử dụng địa chỉ IP đã tìm được ta có thể tìm thấy rất nhiều cổng quét miễn phí trên Internet. Một cổng quét cho ta thấy những gì các cổng được mở tại địa chỉ IP và cổng nào đang được mở trên tường lửa giữa ta và địa chỉ IP. Đây là thông tin rất có giá trị. Ví dụ nếu cổng 110 được mở, sau đó máy chấp nhận lưu lượng truy cập POP3 và có thể là một máy chủ email. Nếu cổng 137,138 và 139 được mở, Sau đó địa chỉ IP này chấp nhận NetBIOS, mà làm cho nó một máy chủ Windows. Điều đó có nghĩa ta có thể

tìm được lỗ hổng được biết đến trong Windows. Bảng dưới đây mô tả các cổng thường được sử dụng:

Số cổng	Mô tả
15/TCP,UDP	Giao thức NETSTAT
19/TCP,UDP	Giao thức CHARGEN (Character Generator)
20/TCP	FTP—dữ liệu
21/TCP	FTP—kiểm soát
22/TCP,UDP	Secure Shell (SSH) – sử dụng cho đăng nhập an toàn, trao đổi (scp, sftp) và cổng chuyển tiếp
23/TCP,UDP	Giao thức Telnet – kết nối văn bản không mã hóa
25/TCP,UDP	Simple Mail Transfer Protocol (SMTP)—được sử dụng cho định tuyến email giữa các máy chủ mail.
43/TCP	Giao thức WHOIS
49/TCP,UDP	Giao thức TACACS Login Host
53/TCP,UDP	Domain Name System (DNS)
57/TCP	Giao thức MTP (Mail Transfer Protocol)
69/UDP	Trivial File Transfer Protocol (TFTP)
79/TCP	Giao thức Finger
80/TCP	Hypertext Transfer Protocol (HTTP)
88/TCP	Kerberos—Hệ thống xác thực
107/TCP	Giao thức dịch vụ TELNET ở xa
110/TCP	Post Office Protocol 3 (POP3)
115/TCP	Simple File Transfer Protocol (SFTP)
118/TCP,UDP	Dịch vụ SQL (Structured Query Language)
119/TCP	Network News Transfer Protocol (NNTP)
123/UDP	Network Time Protocol (NTP)
137/TCP,UDP	Dịch vụ NetBIOS Name
138/TCP,UDP	Dịch vụ NetBIOS Datagram

139/TCP,UDP	Dịch vụ NetBIOS Session
143/TCP,UDP	Internet Message Access Protocol (IMAP)— sử dụng cho việc nhận, tổ chức và đồng bộ thông điệp email.
161/TCP,UDP	Simple Network Management Protocol (SNMP)
179/TCP	BGP (Border Gateway Protocol)
194/TCP	IRC (Internet Relay Chat)
445/TCP	Microsoft-DS Active Directory, Windows shares
445/UDP	Microsoft-DS SMB file sharing

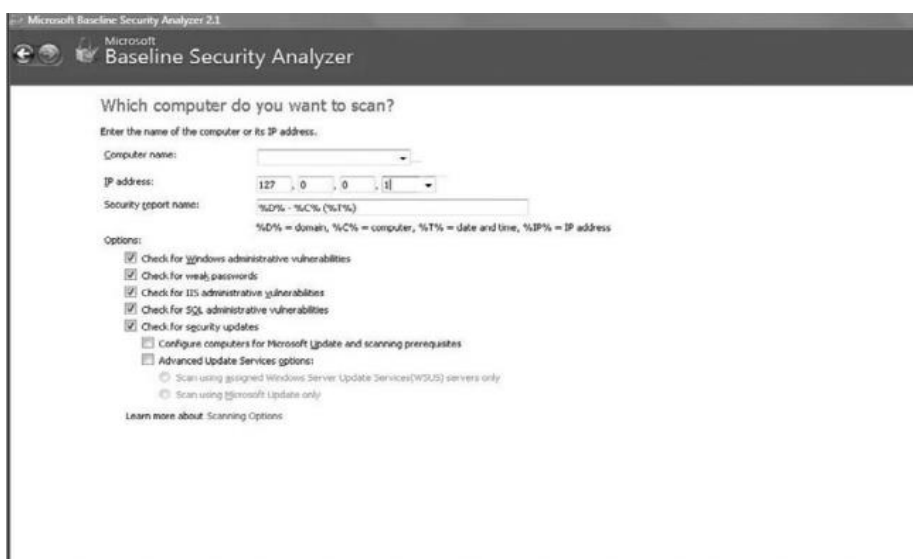
Hình 2.1 cho thấy kết quả của một công cụ quét cổng miễn phí. Như đã thấy, tương đối dễ dàng xác định cổng nào đang mở và cổng nào được đóng lại:



Hình 2.1. Quét cổng sử dụng FreePortScanner

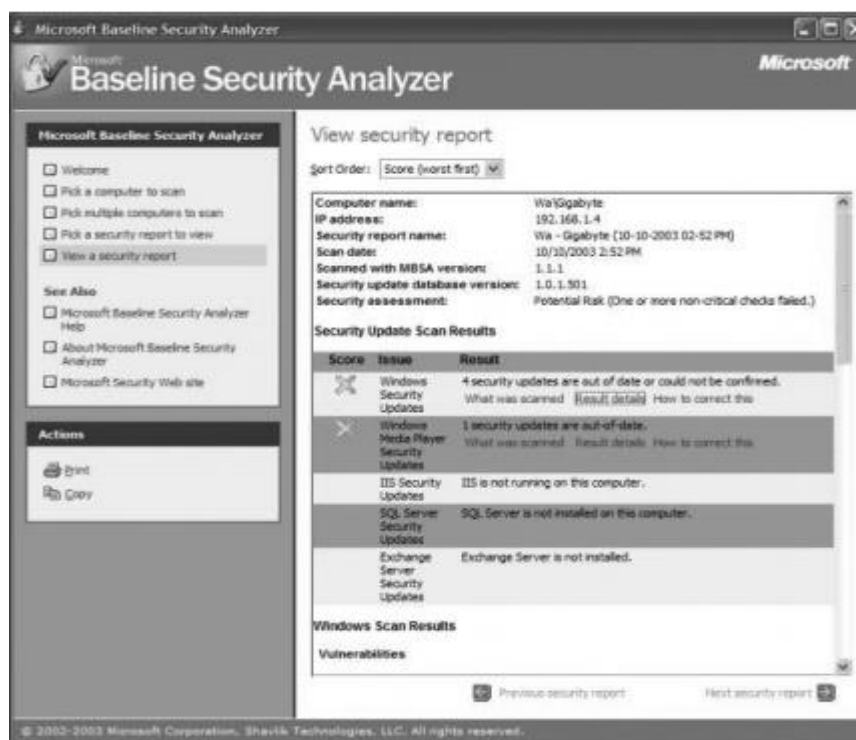
4. Bây giờ ta có thể sử dụng trang web www.archive.org để xem trang web của thành phố. Điều này có thể cung cấp cho ta thông tin có giá trị như thay đổi nhân sự có thể đã xảy ra hoặc thông báo về những thay đổi trong cơ sở hạ tầng CNTT.

5. Tiếp theo, ta sử dụng một công cụ phân tích mạng như Microsoft Baseline Security Analyzer, tải về miễn phí từ trang web. Công cụ này là miễn phí và được thiết kế để giúp các nhà quản trị mạng đánh giá hệ thống của họ. Công cụ này khá là dễ sử dụng vì vậy ta cần xem xét nó. Màn hình đầu tiên cho phép chọn quét một hay nhiều máy. Sau đó, chúng ta nhập địa chỉ IP của máy muốn quét. Trong ví dụ này, chúng ta sẽ sử dụng một địa chỉ IP của một máy tính trên mạng lưới phòng thí nghiệm. Ta có thể nhìn thấy đầu ra của công cụ này. Như chúng ta thấy, nó rất dễ sử dụng và nó có thể cung cấp khá nhiều thông tin. Trong khi các thông tin này được thiết kế cho các quản trị viên mạng để giám sát sự an toàn của mạng lưới hệ thống của họ, nó cũng là một công cụ có giá trị cho một hacker.



Hình 2.2. Phân tích mạng với công cụ Baseline Security Analyzer

6. Cuối cùng sau tất cả các bước ta có được rất nhiều thông tin liên quan đến mạng đích. Đây là cách mà các hacker thực sự cần khi bắt đầu. Các biện pháp đối phó rõ ràng là hệ thống phát hiện xâm nhập các quản trị viên mạng lưới cảnh báo khi hoạt động như quét cổng đang xảy ra. Cũng nên khá cẩn thận với những thông tin được cung cấp tới công chúng.



Hình 2.3. Kết quả thu được từ công cụ Baseline Security Analyzer

Đây chỉ là một trong những công cụ và kỹ thuật một hacker có thể sử dụng để tìm hiểu tất cả các lỗ hổng của mạng mục tiêu trước khi cố gắng tấn công chúng. Một hacker chuyên nghiệp sẽ dành nhiều thời gian để tìm hiểu một hệ thống mục tiêu trước khi xâm nhập nó.

2.4.2 Tấn công hệ thống và các thiết bị mạng

Hệ thống và thiết bị mạng được coi như là các thành phần xương sống trong một hệ thống mạng. Tấn công được vào hệ thống cùng các thiết bị mạng thì gần như kẻ tấn công đã có thể chiếm được toàn bộ mạng, và đánh cắp được các dữ liệu quan trọng bên trong. Một cách rõ ràng đó là muốn vào một hệ thống và các thiết bị mạng thì phải crack được mật khẩu của người dùng hợp pháp hoặc lợi dụng các lỗ hổng; sau đó tạo tài khoản và đăng nhập như người dùng bình thường. Về cơ bản có hai cách rất phổ biến để crack một mật khẩu.

- + Tấn công Brute- Force: xảy ra khi các công cụ phần mềm đang sử dụng chỉ đơn giản là mã hóa của chữ cái, số, và biểu tượng có thể crack mật khẩu. Nó sẽ xuất hiện trong nhật ký máy chủ như một số lần đăng nhập thất bại trong một khoảng thời gian ngắn.

- + Tấn công Dictionary: có thể là cách nhanh nhất để crack mật khẩu. Một tập tin dictionary sẽ cho một tập tin văn bản đơn giản chứa mật khẩu thường được sử dụng. Nó cũng có thể là mật khẩu cụ thể liên quan đến mục tiêu. Ví dụ, nếu mật khẩu muốn crack là một fan hâm mộ Pittsburgh Steelers rất lớn, ta có thể tải một tập tin văn bản với một số điều liên quan đến Steelers. Sau đó tập tin này sẽ được nạp vào một ứng dụng crack (như L0phtCrack, Brutus,...) và chạy với tài khoản người dùng đặt bởi các ứng dụng. Bởi vì phần lớn mật khẩu thường đơn giản. Cũng như một cuộc tấn công Brute-force điều này thường sẽ xuất hiện trong nhật ký máy chủ như một số lần đăng nhập thất bại trong một khoảng thời gian ngắn.

Chắc chắn sẽ có những phương pháp khác để phá mật khẩu, nhưng hiện nay hai cách trên vẫn phổ biến nhất. Chúng cũng rất dễ dàng để sử dụng. Người ta có thể thực hiện tìm kiếm trên Web về cách phá mật khẩu và tìm thấy rất nhiều công cụ miễn phí sẽ giúp được hacker.

Chúng ta cùng xem xét một phương pháp hack mật khẩu Windows phổ biến trong cộng đồng hacker. Phương pháp này đơn giản với thủ phạm quen thuộc với cách làm việc của Windows. Trong Windows, mật khẩu được lưu trữ trong một hàm băm định dạng trên ổ đĩa cứng. Nếu đơn giản có thể cài đặt một brute-force trên tập tin băm, người ta sẽ dần dần có được tên người dùng và mật khẩu. Tuy nhiên hầu hết các máy dùng Windows có một tính năng khóa mật khẩu khi đăng nhập thất bại thường là ba lần. Khóa mật khẩu là một tính năng của hệ điều hành Windows. Để phá vỡ được phần đó của hệ điều hành, cần sử dụng một đĩa CD khởi động Linux, khởi động máy tính với Linux sau đó cài đặt các cracker mật khẩu để làm việc trên các tập tin băm mật khẩu. Thậm chí có một công cụ có thể nhận được trên Internet gọi là OphCrack có thể khởi động Linux và crack mật khẩu. Đơn giản chỉ cần ghi OphCrack vào một đĩa CD, đặt nó vào bất kỳ máy Windows và khởi động lại từ đĩa CD. Đây chỉ là một ví dụ về cách có thể crack mật khẩu Windows.

Bên cạnh việc crack mật khẩu, lợi dụng các lỗ hổng tồn tại trên hệ thống và các thiết bị mạng cũng thường được hacker sử dụng. Hầu hết các hệ điều hành khi phát hành đều có một vài lỗi và sau một thời gian mới có các bản vá sửa chữa. Trong khoảng thời gian đó, nếu hacker tìm ra trước khi hệ

thống được vá thì hoàn toàn có thể xâm nhập và thực hiện các hành vi trái phép bên trong. Trên các thiết bị mạng cũng như vậy. Gần như mỗi thiết bị đều có những lỗ hổng cho phép kẻ tấn công có thể khai thác. Những lỗ hổng này xuất phát từ lỗi cấu hình do người quản trị, hoặc các lỗ hổng từ phía nhà sản xuất. Trên thực tế đã có rất nhiều các tấn công như vậy xảy đến gây nên những hậu quả ảnh hưởng nghiêm trọng tới toàn bộ hệ thống mạng.

2.4.3 Tấn công cơ sở dữ liệu và ứng dụng Web

Một trang web có thể công khai truy cập, và chúng có thể nhận được nhiều lượng truy cập. Điều này khiến chúng trở thành mục tiêu cho kẻ tấn công và địa điểm hợp lý cho những xâm nhập bắt đầu. Có rất nhiều cách để thử nghiệm và tấn công qua website, sau đây ta sẽ xem xét các cách thường được sử dụng nhất.

– **SQL injection** : SQL là viết tắt của Structured Query Language. Là ngôn ngữ được sử dụng bởi tất cả các cơ sở dữ liệu quan hệ. Một trang web mục tiêu giao tiếp với bất kỳ cơ sở dữ liệu qua SQL. Hacker chuyên nghiệp sử dụng thực tế này và khai thác nó để truy cập vào hệ thống. SQL Injection là một quá trình mà hacker nhập mã SQL trực tiếp vào một form web như mục đăng nhập hoặc một thanh địa chỉ trong trình duyệt. Mục đích là để bẫy các trang web vào trình mã SQL truy cập vào cơ sở dữ liệu thực hiện mã. Để làm được việc này các hacker phải có một hiểu biết sâu về SQL. Đây là một tấn công hiệu quả, và nó cũng khá nghiêm trọng. Xét ví dụ. Các hacker muốn đăng nhập vào một trang web. Nếu một trang web được thiết kế có nhiều lỗ hổng, hacker có thể sử dụng một tính năng của SQL để buộc các trang web để cho hacker có thể đăng nhập, đây là một câu lệnh đơn giản thường thấy trên màn hình đăng nhập để xác minh đăng nhập :

```
SELECT * FROM USERS WHERE USERNAME = 'usernameentered'
AND PASSWORD = 'passwordentered'
```

Usernameentered; passwordentered là user và pass người dùng cần đăng nhập. Vì vậy nếu trong box mật khẩu hacker có 'pass or 1 =1' thì câu lệnh SQL sẽ trở thành

```
SELECT * FROM USERS WHERE USERNAME = 'usernameentered'
AND PASSWORD = 'passwordentered' or 1 = 1.
```

Nói cách khác, “đi đến một tài khoản người dùng và đăng nhập nếu có một tài khoản phù hợp tên và mật khẩu nhập vào là $or\ 1 = 1$ ”. Có nhiều cuộc tấn công SQL injection, chỉ cần sử dụng công cụ tìm kiếm để tìm “sql injection” sẽ hiện ra rất nhiều thông tin. Và tất nhiên có nhiều cách để mã một trang web khiến nó ngừng hoạt động. Nhiều lập trình viên không sử dụng những phương thức này bởi có quá nhiều thông tin đăng nhập. Đây chỉ là ví dụ về cách một hacker có thể khai thác một hệ thống. Các duy nhất để theo dõi đó là xem lại thông tin đăng nhập. Tuy nhiên các trang web dễ bị tấn công thường không thực hiện theo dõi thường xuyên, vì vậy có thể coi như một người sử dụng đăng nhập hợp pháp.

– **Tấn công XSS :** Là kỹ thuật phổ biến mà hacker thường sử dụng tấn công các trang web. Kiểu tấn công này khó khăn hơn SQL injection và ngày càng phổ biến. Nhiều trang web nổi tiếng đã từng là nạn nhân của tấn công XSS bao gồm cả Google, MySpace và thậm chí cả Microsoft. Tấn công bằng cách nhúng mã JavaScript vào hyperlinks của một trang web. Điều này cho phép kẻ xâm nhập quyền kiểm soát các thông tin cá nhân, trang web quảng cáo,... Một tình huống xấu nhất đó là một hacker truy cập được vào thông tin tài khoản và có quyền tham gia trên toàn bộ trang web.

– **Chiếm quyền điều khiển :** Việc cướp quyền là hành động của việc kiểm soát của một phiên người dùng sau khi có thành công hay tạo ra xác thực ID. Kiểu tấn công này đòi hỏi một mức độ tương đối cao về kỹ năng và do đó hiếm gặp hơn. Việc cướp quyền liên quan đến một kẻ tấn công . Khi một phiên giao dịch là một thông tin hợp lệ được thiết lập giữa máy khách và máy chủ. Khi đăng nhập vào mạng LAN, bạn đã thiết lập một phiên làm việc. Có ba kỹ thuật chính để chiếm quyền điều khiển :

- + Brute force : Kẻ tấn công cố gắng thử nhiều ID cho đến khi thành công.
- + Calculate : Trong nhiều trường hợp, ID được tạo ra không ngẫu nhiên và có thể đã được tính toán.
- + Steal : Sử dụng các kỹ thuật khác nhau, kẻ tấn công có thể trộm được các ID.

Chương 3

CÁC PHƯƠNG PHÁP ĐIỀU TRA TỘI PHẠM MÁY TÍNH

Từ các chương trước chúng ta đã thấy có rất nhiều dạng tội phạm cũng như hành vi phạm tội. Mỗi dạng tội phạm tương ứng với các hành vi khác nhau và không dễ để có thể tìm ra chúng. Khi thực hiện điều tra, người điều tra cần tuân thủ theo các bước và theo quy định của pháp luật. Bỏ qua bất cứ bước nào sẽ có thể gây ra vấn đề nghiêm trọng khi tiến hành xét xử tại tòa. Trong chương này, chúng ta sẽ đi tìm hiểu cụ thể về các phương pháp điều tra để có thể xác định chính xác các hành vi tội phạm làm bằng chứng cho việc thực thi pháp luật.

3.1 CƠ SỞ PHÁP LÝ KHI ĐIỀU TRA TỘI PHẠM MÁY TÍNH

Điều tra tội phạm máy tính cũng giống như điều tra hình sự. Trước khi thực hiện điều tra, cần có những cơ sở pháp lý để phân định rõ quyền hạn, trách nhiệm của cơ quan điều tra. Tùy từng nước mà có những quy định riêng. Ở Việt Nam, những cơ sở này được quy định trong "*Chương IX- Những quy định chung về điều tra*" của Bộ Luật Tố tụng hình sự nước Cộng hòa XHCN Việt Nam.

Các quy định từ điều 110 đến 125 chỉ rõ phạm vi thẩm quyền điều tra, quyền hạn của cơ quan công an cũng như viện kiểm soát và các trách nhiệm khi thực hiện điều tra, thời gian điều tra cùng các điều khoản về giữ bí mật trong quá trình điều tra. Cuối cùng là biên bản điều tra.

Quyền cá nhân là một trong những vấn đề còn nhiều yếu tố chưa được quyết định bởi tòa án. Điều luật Bảo mật điện tử của Mỹ đưa ra những hạn chế về khả năng thực thi pháp luật cụ thể trong việc chặn bắt và tiếp cận chứng cứ, sự phân biệt giữa thông tin được lưu trữ (như email) và thông tin

truyền thông liên lạc (như VOIP). Sau này, khía cạnh quyền riêng tư được đưa ra xem xét kỹ lưỡng hơn nhưng vẫn còn nhiều yếu tố khó bảo đảm. ECPA cũng ảnh hưởng đến việc điều tra các công ty qua máy tính hay các liên lạc giữa những nhân viên với nhau, đây là một khía cạnh vẫn còn đang được tranh luận để quyết định việc giám sát của công ty trong quá trình điều tra.

Điều 5 của Công ước Châu Âu về nhân quyền khẳng định những hạn chế riêng tư tương tự như ECPA và giới hạn việc xử lý cũng như chia sẻ dữ liệu cá nhân của cả hai trong EU với các nước bên ngoài. Khả năng thực thi pháp luật của Vương quốc Anh được luật hóa trong Luật Quyền hạn điều tra.

3.2 CÁC BƯỚC THỰC HIỆN ĐIỀU TRA

Mỗi một vụ án khác nhau sẽ có những cách điều tra khác nhau, nhưng dù có điều tra theo cách nào, thì các nguyên tắc (các bước) thực hiện điều tra vẫn phải được tuân theo. Có 5 bước cần thực hiện là:

1. Quan sát, bảo vệ hiện trường vụ án.
2. Ghi và lập tài liệu về hiện trường
3. Bảo quản chứng cứ
4. Tiến hành điều tra
5. Lập báo cáo điều tra

3.2.1 Quan sát, bảo vệ hiện trường vụ án

Với một số tội phạm truyền thống, chẳng hạn như một vụ cướp hoặc giết người, phạm vi thường được đánh dấu bởi băng cảnh sát hoặc hàng rào cảnh sát. Nó xác định khu vực cần bảo đảm. Bảo vệ hiện trường vụ án gồm một số bước. Trước hết phải loại bỏ cá nhân không cần thiết tại hiện trường. Quy tắc rất đơn giản: Nếu ai đó không hoàn toàn ở đó, họ không phải là các nhân viên thực thi pháp luật. Người không cần thiết tại hiện trường chỉ làm cho chứng cứ bị tổn hại. Tiếp theo rất quan trọng đó là đánh dấu khu vực này, cô lập hiện trường vụ án, và ngăn không cho người xâm nhập vào hiện trường. Mỗi người trong hiện trường có thể để lại chứng cứ như tóc, sợi quần áo, hoặc các chất gây ô nhiễm khác. Chỉ cho phép nhân viên cần thiết vào hiện trường, họ chịu trách nhiệm về những gì họ làm và đưa ra tài liệu cần thiết bổ sung vào biên bản ban đầu. Cũng sẽ có nhân viên cảnh sát giữ nhật ký của những người đi vào, ra khỏi hiện trường. Các bản ghi là rất quan trọng.

Bởi các luật sư có thể bào chữa rằng trong hiện trường có những người không cần thiết và chứng cứ không được xem trọng.

Quá trình này tương tự với tội phạm máy tính. Trước hết cần phải đảm bảo hiện trường vụ án. Rõ ràng, việc đảm bảo tội phạm máy tính có thể khác nhau với việc đảm bảo hiện trường một tội phạm truyền thống. Hiện trường vụ án thường là các máy tính thực tế, các bộ định tuyến, và các máy chủ có liên quan đến tội phạm. Để bảo đảm chứng cứ phải tắt chúng đi, ngăn chặn người dùng truy cập vào chúng. Nếu có một máy tính đang bị nghi ngờ là công cụ của tội phạm thì nó phải được bảo đảm.

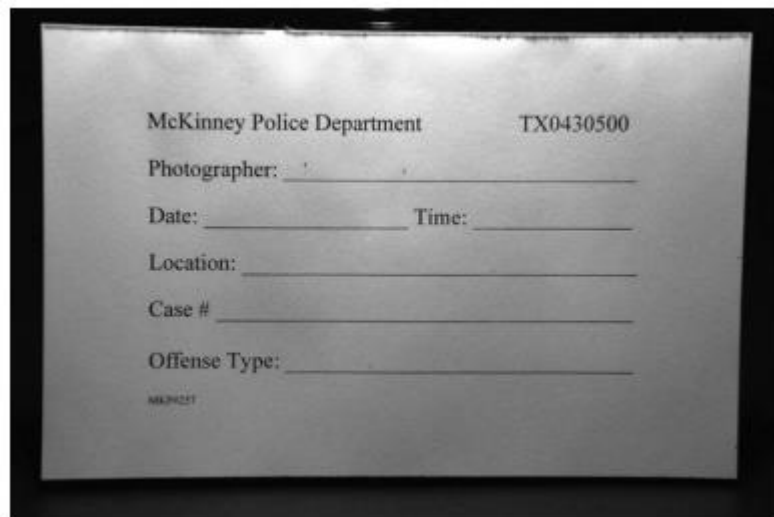
Xác định khu vực của tội phạm máy tính khác với tội phạm truyền thống. Các máy khác nhau có thể bị cô lập về mặt địa lý, nhưng quan trọng là được bảo đảm và cô lập để kiểm tra. Sau đó cần hạn chế số lượng người đã được tiếp cận với hiện trường vụ án và tất cả các tài liệu tương tác với hiện trường vụ án. Trong nhiều trường hợp, các hệ thống liên quan cần thiết cho hoạt động của nạn nhân cần tiếp tục được theo dõi. Ví dụ nếu máy chủ cơ sở dữ liệu của công ty đã bị hack và dữ liệu bị đánh cắp, họ sẽ vẫn cần máy chủ để tiếp tục hoạt động kinh doanh. Phương pháp tiếp cận sau đó là sử dụng những máy chủ đã thoát tạm thời, sao chép ổ đĩa cứng cho máy chủ và sau đó đặt các ổ đĩa bản sao trở lại vào dịch vụ, do đó việc giữ ổ đĩa gốc đảm bảo được làm bằng chứng.

3.2.2 Ghi và lập tài liệu về hiện trường

Không được chạm vào bất cứ gì cho đến khi bắt đầu thu thập bằng chứng. Một khi đã đi qua và quan sát hiện trường, bây giờ là lúc ghi lại những gì đã quan sát được. Quay phim toàn bộ hiện trường là điều không bắt buộc trong tài liệu chứng cứ. Nếu chọn quay video hiện trường vụ án thì nó phải là cái nhìn 360 độ của căn phòng. Video giống như cái nhìn thứ hai của hiện trường, và nó cũng hữu ích cho hội đồng bồi thẩm xem lại những gì đã thấy trong quá trình điều tra. Các điều tra viên phải luôn nêu ở đầu video người đã làm đoạn băng và chắc chắn thời gian là chính xác. Trong đoạn video, nếu có gì đó nổi bật thì phải có nhận xét về nó, có thể là cách thức kết nối được gắn vào máy tính hoặc các thiết bị khác hoặc có thể là mô tả của căn phòng. Trong mọi trường hợp, một băng video cho phép bất cứ ai kể cả bồi thẩm xem. Do

vậy cần cẩn thận những gì nói trong video, phải là một người chuyên nghiệp. Một bình luận tiêu cực hay tệ hơn có thể gây ra nghi ngờ về kỹ năng của bạn. Luật sư bào chữa sẽ nhận ra và đặt câu hỏi về tính công bằng và kỹ thuật điều tra. Sau đó phải giải thích tại sao những nhận xét đã được thực hiện cho các luật sư bào chữa và bên thẩm phán. Đây có thể là một cách mà luật sư bào chữa có thể sử dụng để chống lại quá trình điều tra.

Sau khi làm video, chụp ảnh lại các cảnh điều tra. Các quy tắc tương tự áp dụng trong chụp ảnh hiện trường như là quay video: trình bày chi tiết. Máy ảnh có hiện thị ngày, thời gian, đảm bảo được thiết lập đúng. Sau khi có được video và hình ảnh, cần tìm hiểu về chúng (hình 3.1). Với hình ảnh kỹ thuật số hoặc film 35mm, sử dụng một tài liệu để ghi lại hình ảnh.



Hình 3.1. Tài liệu về hình ảnh

Một số bộ phận vẫn còn sử dụng film 35mm, do đó cần ghi lại cuộn film để được xử lý. Vài năm trước đây, đã có rất nhiều tranh cãi về bằng chứng hình ảnh kỹ thuật số được chấp nhận tại tòa án. Bởi các bức ảnh kỹ thuật số có thể được thay đổi. Trong cuốn sách được viết bởi Steven Staggs: *Crime Scene and Evidence Photographer's Guide* là một hướng dẫn rất tốt trong quá trình điều tra tội phạm công nghệ cao. Trong cuốn sách, Staggs cung cấp một số yêu cầu chính để có được các bức ảnh bằng chứng :

- Xây dựng SOP (quy trình hoạt động tiêu chuẩn).
- Bảo vệ các hình ảnh kỹ thuật số ban đầu. Điều này rất quan trọng. Có thể nâng cao chất lượng hình ảnh để xem một số chi tiết, nhưng nên

thực hiện với một bản sao, không bao giờ để mất tập tin ban đầu. Tập tin gốc không bao giờ được chỉnh sửa hay xóa.

- Bảo tồn ảnh ở định dạng ban đầu.

Ghi lại tất cả hạng mục của bằng chứng có thể mất thời gian, nhưng nó rất quan trọng. Chi tiết quá trình đó phụ thuộc vào từng trường hợp tội phạm máy tính cụ thể. Các tài liệu thu thập bằng chứng rất quan trọng nhưng tốt nhất là ghi chính xác là đã thu thập các bằng chứng ngoài tài liệu bằng chứng chính nó. Sẽ không được làm gì trên máy tính, router hoặc thiết bị khác. Bất kỳ hành động nào cũng có thể làm thay đổi dữ liệu và làm bằng chứng thu được vô hiệu lực.

Các dây cáp gắn vào máy tính có thể cần phải tô màu chúng để tránh nhầm lẫn. Sau khi có được các dây cáp đúng màu sắc đúng mã, bắt đầu ghi lại các thiết bị gắn vào đó. Khi tài liệu hoàn tất, sau đó có thể bắt đầu ngắt kết nối các thiết bị với nhau.

Ở đây đưa ra một tài liệu nghĩa là phải nhận ra một notepad và thẻ bằng chứng. Các phần khác nhau của bằng chứng phải được ghi lại và cả vị trí mà nó đã được lấy ra. Notepad sẽ giúp ta theo dõi điều này. Mỗi mục nắm bắt cũng nên có một thẻ bằng chứng. Thẻ sẽ ghi ngày, giờ, địa điểm, hành vi phạm tội, mặt hàng bị tịch thu, số lượng dịch vụ, nhân viên, người nhận hàng.

Trên mặt sau thẻ là nơi mà tài liệu đã xử lý bằng chứng và chuỗi hành trình (xem hình 3.2). Chuỗi hành trình là rất quan trọng. Vậy chuỗi hành trình là gì ? Theo viện SANS Institute-Score: “ nó là một thuật ngữ pháp lý mô tả các bộ sưu tập, vận chuyển và lưu trữ bằng chứng để ngăn chặn mất mát, thiệt hại vật chất, hoặc tiêu hủy”.

Hình 3.2. Tài liệu các chuỗi hành trình

Nếu không có đủ chuỗi tạm giữ tài liệu, luật sư bào chữa sẽ cố gắng làm cho nó xuất hiện với những nghi ngờ tính toàn vẹn của tập chứng cứ này. Toàn bộ mục tiêu của luật sư là phải đặt nghi ngờ trong thẩm phán về độ tin cậy của các bằng chứng. Quá trình này phải nhất quán trong mỗi hiện trường vụ án mà bạn có tài liệu.

Sau đây sẽ xét một ví dụ về một chuỗi hành trình. Nếu là một thám tử thu thập các thiết bị điện tử tại hiện trường vụ án. Có tất cả các thiết bị đánh dấu chúng, và chúng vẫn đang nằm trong chu vi bên trong hiện trường vụ án. Khi đưa chúng lên chiếc xe để bảo vệ chúng, viên sĩ quan được di chuyển vào và ra khỏi hiện trường vụ án ghi nhận những gì đang làm. Bây giờ giả sử thám tử khác đang giúp và anh ta cũng đang đăng nhập vào ra với các thiết bị điện tử. Sau đó, tạo bổ sung về những việc đã làm ở hiện trường vụ án, giả sử bổ đề cập đến các thám tử khác. Sau đó điền vào thẻ bằng chứng về chuỗi hành trình mà không có sự góp mặt của các thám tử khác ấy. Khi luật sư bào chữa các bản ghi hoặc bản sao của thẻ bằng chứng không thấy đề cập đến những thám tử khác, sẽ gây ra nghi vấn cho quá trình thực hiện điều tra. Nếu một chi tiết nhỏ bị bỏ qua, thì những chi tiết lớn sẽ không được đề cập đến trong bổ sung hoặc hiển thị trên thẻ bằng chứng.

3.2.3 Bảo quản chứng cứ

Bảo quản chứng cứ cũng là một vấn đề rất quan trọng trong quá trình điều tra. Một khi hoàn tất tài liệu trên tất cả bằng chứng, cần đặt từng hạng

mục thu được vào túi chứng cứ cho thấy đã đánh dấu đúng. Cần đeo găng tay chống tĩnh trong khi thu thập và đưa vào túi bằng chứng. Một số vật chứng có thể được đặt trong túi giấy và luật sư có thể phản biện rằng không dùng túi chống tĩnh thì vật chứng có thể bị thay đổi hoặc hư hỏng. Điều này áp dụng đặc biệt cho các thiết bị đã đề cập trước như máy ảnh kỹ thuật số, điện thoại di động... Mỗi vật chứng đóng gói sẽ có một thẻ bằng chứng với nó. Túi cũng sẽ lưu ý trên đó các thông tin phù hợp với các thẻ bằng chứng. Điều này sẽ giúp theo dõi từng vật chứng. Một khi đã được bọc lại thì phải giữ bằng chứng tại hiện trường cho đến khi đã sẵn sàng mang nó đến khu vực an toàn của bộ phận điều tra. Không để nhân viên, điều tra viên khác đặt bằng chứng trong xe của họ, họ có thể không nhận thức được các yếu tố có thể gây thiệt hại cho thiết bị và sẽ không thể giữ được quyền kiểm soát vật chứng. Chuỗi hành trình là rất quan trọng.

Bước tiếp theo là đóng gói các bằng chứng và vận chuyển chúng đến khu vực bảo đảm cho bộ phận điều tra. Dùng tủ khóa để bảo vệ các bằng chứng. Nếu lượng bằng chứng lớn cần đến một phòng để bảo vệ. Thư ký sẽ lấy các bằng chứng và đăng nhập đúng cách vào khu vực lưu trữ. Thẻ bằng chứng sẽ hiển thị các chuỗi hành trình của chứng cứ. Và bằng chứng phải được bảo vệ an toàn, lưu ý về nơi đặt chúng. Ví dụ không đặt máy tính bên cạnh loa hộp lớn bởi các máy tính có thể bị ảnh hưởng bởi các nam châm trong loa. Nếu dữ liệu bị thay đổi bằng bất kỳ cách nào, nó có thể không được chấp nhận tại tòa án.

Thủ tục pháp lý là tuyệt đối quan trọng. Thất bại trong bảo vệ hiện trường và duy trì chuỗi bằng chứng có thể làm hỏng một cuộc điều tra. Bước đầu tiên là phải đảm bảo hiện trường vụ án hoàn toàn an toàn. Sau đó, phải đảm bảo được rằng các bằng chứng được thu thập theo đúng thủ tục pháp y. Với trường hợp này với một điều tra viên có tay nghề cao, họ sẽ làm như sau: Bước đầu tiên là để đảm bảo cho các máy chủ đó. Nếu ai đó đã xâm nhập vào máy chủ, cần phải đảm bảo máy chủ đó. Vì vậy, các quản trị mạng đã offline máy chủ, sao chép ổ cứng tới một nơi mới, đặt các bản sao phục vụ, giữ ổ cứng ban đầu cho bằng chứng. Toàn bộ quá trình phải được ghi lại. Ràng tài liệu hướng dẫn chi tiết ai đã tham gia và quá trình. Sau đó ổ đĩa cứng sẽ được phân tích bất kỳ dữ liệu bản ghi hoặc nguồn khác có thể được kiểm tra bằng

chứng. Bằng chứng sau đó sẽ được ghi lại. Ví dụ, có thể ghi nhận rằng bản ghi truy cập cho thấy máy chủ được truy cập từ địa chỉ IP nhất định tại một thời điểm nhất định. Bước tiếp theo là triệu tập các nhà cung cấp dịch vụ Internet nghi ngờ, do đó có thể lần lại địa chỉ IP mà kết nối đến máy chủ và xác định xem kết nối đã thực sự đến từ thủ phạm. Cuối cùng, đảm bảo quyền truy cập vào máy tính thủ phạm và xử lý nó giống như cách đã làm với máy chủ, cẩn thận ghi lại từng bước.

3.2.4 Tiến hành điều tra

Sau khi đã thực hiện tất cả các công việc về giám định, tạo bản sao và lưu trữ chứng cứ; bây giờ sẽ bắt tay vào tiến hành điều tra. Tùy từng tính chất, tầm quan trọng cũng như hành vi của vụ án mà phạm vi điều tra diễn ra trên các vị trí khác nhau. Các mặt có thể thực hiện điều tra gồm:

- Thu thập và phân tích chứng cứ từ các linh kiện phần cứng
- Thu thập và phân tích chứng cứ từ hệ thống
- Thu thập và phân tích chứng cứ từ email, điện thoại, thiết bị mạng, ...

Chi tiết về các mặt điều tra sẽ được trình bày cụ thể trong phần sau. Kết quả của quá trình điều tra là tìm ra các bằng chứng phạm tội và các hành vi phạm tội, để từ đó có thể quy trách nhiệm trước tòa án.

3.2.5 Lập tài liệu báo cáo

Bước cuối cùng trong quy trình điều tra tội phạm máy tính là lập báo cáo về quá trình điều tra. Báo cáo này mô tả toàn bộ các bước tiến hành điều tra từ lúc bắt đầu cho đến khi kết thúc, và cũng là hồ sơ lưu trữ cho các công tác xử lý về sau.

3.3 THU THẬP VÀ PHÂN TÍCH CHỨNG CỨ TỪ CÁC LINH KIỆN PHẦN CỨNG

Công nghiệp sản xuất các loại thiết bị điện tử có bộ nhớ kỹ thuật số và chip điều khiển đang ngày càng phát triển. Hầu hết các thiết bị gia đình, phương tiện giao thông, thiết bị sản xuất đều đã được số hóa, tích hợp loại đơn giản là microprocessor với memory chip và phần mềm nhúng như TV,

điện thoại, tủ lạnh, máy in, máy fax... loại phức tạp là cả một hệ thống máy tính như ở ô tô, máy bay, tàu thuyền, máy công cụ với hệ thống CAD/CAM... Những thiết bị này đều có thể lưu trữ dữ liệu điện tử. Để thu được chứng cứ điện tử, trước tiên phải thu được các thiết bị có bộ nhớ kỹ thuật số đã được sử dụng làm phương tiện gây án như: máy tính, máy điện thoại di động, máy GPS, máy in... và xác định những thiết bị này có được sử dụng trong quá trình chuẩn bị gây án, thực hiện hành vi phạm tội, lưu chứng cứ phạm tội, truy cập vào website bị tấn công... Trên cơ sở đó quyết định cần tìm và thu giữ máy tính hoặc các thiết bị có bộ nhớ kỹ thuật số nào, ở đâu.

Công tác tìm và thu giữ các thiết bị lưu trữ chứng cứ từ các linh kiện phần cứng cần quan tâm đến các nguồn như: ổ cứng, bộ nhớ, điện thoại di động, USB, đĩa VCD, DVD, thiết bị không dây bluetooth, wifi... Để thực hiện thu thập chứng cứ, chúng ta cần làm như sau:

- Đối với máy tính:

- + Nếu máy tính đang bật: chụp ảnh màn hình, ngưng kết nối mọi nguồn điện, tắt máy tính đột ngột (không tắt theo trình tự)
- + Nếu máy tính đang tắt: không được bật lên
- + Nếu máy tính xách tay đang hoạt động: cần tháo pin ra để tắt máy, ngăn sự cố khởi động bất ngờ
- + Đánh số, chụp ảnh, vẽ sơ đồ, lập biên bản hiện trạng tang vật ở hiện trường
- + Đóng gói, vận chuyển máy tính và các loại thiết bị kỹ thuật số khác tránh xa nam châm và các tác nhân gây nguy hiểm
- + Thu tất cả cáp nối, thiết bị ngoại vi, bàn phím và màn hình
- + Thu tài liệu hướng dẫn và ghi chép (có thể có mật khẩu)
- + Đối với máy chủ: nếu đang chạy, copy dữ liệu từ ổ cứng máy chủ sang ổ cứng lưu trữ bằng cách: rút ổ cứng hoặc sử dụng USB cài phần mềm EnCase, kết nối ổ cứng ngoài vào bằng máy chủ rồi chạy EnCase

- Đối với smart phone, máy tính bảng:

- + Nếu thiết bị ở chế độ “OFF”, không bật “ON”, nếu ở chế độ “ON” cần tiến hành các bước: Chụp ảnh màn hình/hiển thị, ngắt tất cả nguồn điện rút ở phía sau thiết bị.
 - + Thu hướng dẫn sử dụng, dây nguồn, các thiết bị ngoại vi
 - + Giữ thiết bị tránh xa nam châm, máy truyền tín hiệu radio và các môi trường nóng, lạnh, ẩm...
- Đối với thiết bị media: thường có bộ nhớ trong và bộ nhớ ngoài, được sử dụng để lưu dữ liệu, như ổ cứng di động HDD, SSD, thẻ nhớ, chip các loại, đĩa CD, VCD, DVD... Đối với các thiết bị này cần thu và chuyển cho chuyên gia phục hồi dữ liệu điện tử.

Công tác phục hồi chứng cứ điện tử phải sử dụng các thiết bị và phần mềm chuyên dụng, để đảm bảo các nguyên tắc xác lập chứng cứ điện tử, không làm ảnh hưởng đến tính nguyên trạng của chứng cứ và phải được những chuyên gia đã qua đào tạo thực hiện. Bản chất của quá trình phục hồi chứng cứ điện tử là phục hồi, tìm, thu thập, phân tích, nghiên cứu giá trị chứng cứ của dữ liệu và báo cáo kết quả về nội dung và tình trạng của chứng cứ để chuyển hóa thành chứng cứ và được công nhận là chứng cứ pháp lý trước tòa. Việc phục hồi dữ liệu được tiến hành trên bản sao, nên không làm tổn hại đến dữ liệu gốc.

3.4 THU THẬP VÀ PHÂN TÍCH CHỨNG CỨ TỪ MẠNG

Chứng cứ từ mạng rất quan trọng trong điều tra tội phạm. Phần lớn những kẻ tấn công đều lợi dụng môi trường mạng để thực hiện tấn công. Việc thu thập và phân tích thông tin đi qua mạng có thể giúp phát hiện ra các hành vi của kẻ tấn công và cũng có thể khắc phục sự cố mạng.

Hầu hết các kỹ thuật điều tra mạng là giám sát thụ động, chủ yếu dựa trên lưu lượng mạng, hiệu năng CPU hoặc quá trình nhập/ xuất (Input/Output) với sự can thiệp của con người. Trong đa số các trường hợp, dấu hiệu của cuộc tấn công mới được phát hiện thủ công hoặc trong một số trường hợp nó không bị phát hiện cho đến khi vụ việc được báo cáo. Trọng tâm của lĩnh vực pháp y mạng là để tự động hóa quá trình phát hiện tất cả các cuộc tấn công và thêm vào đó ngăn chặn các thiệt hại do vi phạm an ninh. Ý tưởng chính của điều tra mạng là xác định tất cả các vi phạm an ninh có thể xảy ra và xây dựng

các dấu hiệu vào cơ chế phát hiện và ngăn chặn để hạn chế những mất mát về sau.

Có 2 phương pháp để thu thập và phân tích chứng cứ từ mạng là:

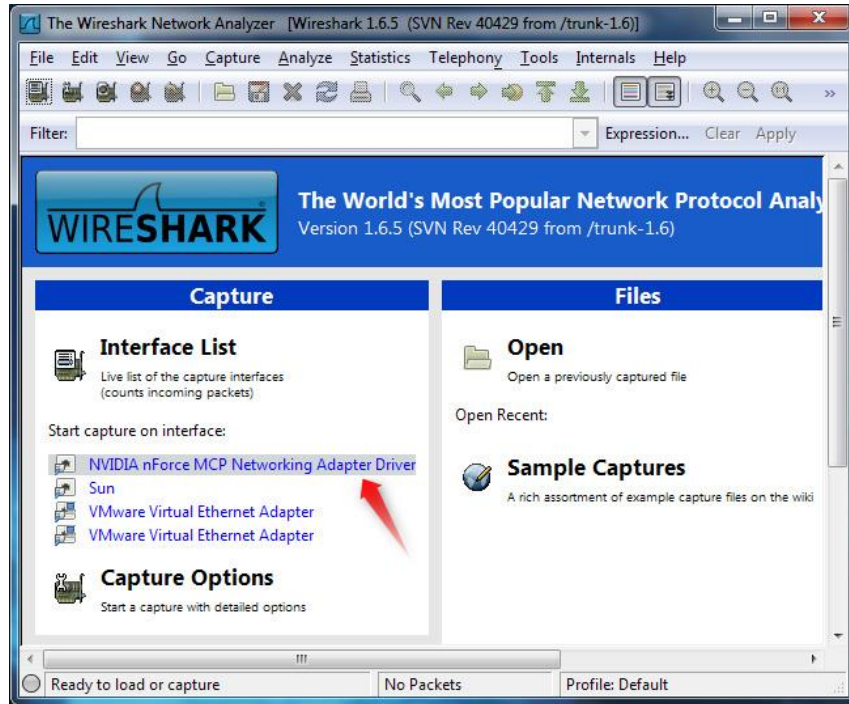
- Phân tích gói tin
- Phân tích thống kê lưu lượng mạng

3.4.1 Phân tích gói tin

Phân tích gói tin thông thường được quy vào việc nghe các gói tin và phân tích giao thức, mô tả quá trình bắt và phiên dịch các dữ liệu sống như là các luồng đang lưu chuyển trong mạng với mục tiêu hiểu rõ hơn điều gì đang diễn ra trên mạng. Phân tích gói tin thường được thực hiện bởi một packet sniffer, một công cụ được sử dụng để bắt dữ liệu thô đang lưu chuyển trên đường dây. Phân tích gói tin có thể giúp chúng ta hiểu cấu tạo mạng, ai đang ở trên mạng, xác định ai hoặc cái gì đang sử dụng băng thông, chỉ ra những thời điểm mà việc sử dụng mạng đạt cao điểm, chỉ ra các khả năng tấn công và các hành vi phá hoại, và tìm ra các ứng dụng không được bảo mật.

Để thực hiện việc bắt các gói tin trên mạng, ta phải chỉ ra những vị trí tương ứng để đặt “máy nghe” vào hệ thống đường truyền của mạng. Quá trình này đơn giản là đặt “máy nghe” vào đúng vị trí vật lý nào trong một mạng máy tính. Việc nghe các gói tin không đơn giản chỉ là cắm một máy xách tay vào mạng và bắt gói. Thực tế, nhiều khi việc đặt máy nghe vào mạng khó hơn việc phân tích các gói tin. Thách thức của việc này là ở chỗ là có một số lượng lớn các thiết bị mạng phần cứng được sử dụng để kết nối các thiết bị với nhau. Lý do là vì 3 loại thiết bị chính (hub, switch, router) có nguyên lý hoạt động rất khác nhau. Và điều này đòi hỏi ta phải nắm rõ được cấu trúc vật lý của mạng mà ta đang phân tích.

Có rất nhiều công cụ hỗ trợ phân tích gói tin, phổ biến nhất trong số đó là Wireshark. Đây là công cụ có khả năng theo dõi, giám sát các gói tin theo thời gian thực, hiển thị chính xác báo cáo cho người dùng qua giao diện khá đơn giản và thân thiện.



Hình 3.3. Công cụ Wireshark

3.4.2 Phân tích thống kê lưu lượng

Ngoài phân tích gói tin, việc phân tích thống kê lưu lượng cũng cần thiết để điều tra tội phạm máy tính. Có thể các tội phạm mạng thực hiện tấn công lên băng thông mạng (tấn công từ chối dịch vụ), hoặc lợi dụng một điểm để chặn bắt các thông tin từ các máy trong hệ thống (tấn công ARP). Như vậy, khi thực hiện phân tích thống kê lưu lượng mạng có thể dễ dàng phát hiện ra kẻ tấn công.

Thông lượng của một mạng có thể được đo bằng các công cụ có sẵn trên các nền tảng khác nhau. Lý do để đo thông lượng trong mạng là mọi người thường quan tâm đến dữ liệu tối đa trong mỗi giây của một liên kết thông tin liên lạc hay một truy cập mạng. Một phương pháp điển hình thực hiện việc đo đạc này là chuyển một tập tin lớn từ một hệ thống sang một hệ thống khác và đo thời gian cần thiết để hoàn tất việc chuyển giao hay sao chép tập tin. Thông lượng sau đó được tính bằng cách chia kích thước tập tin theo thời gian để có được kết quả theo megabit, kilobit hay bit trên mỗi giây. Tuy nhiên, kết quả của một lần tính như vậy sẽ dẫn đến việc thông lượng trên thực tế ít hơn thông lượng dữ liệu tối đa trên lý thuyết, làm người ta tin rằng liên kết thông tin liên lạc của họ là không chính xác. Trên thực tế, có rất nhiều các

chi phí chiếm trong thông lượng ngoài các chi phí truyền tải, bao gồm cả độ trễ, kích thước cửa sổ và hạn chế của hệ thống, có nghĩa là các kết quả không phản ánh được thông lượng tối đa đạt được.

Phần mềm kiểm tra băng thông được sử dụng để xác định băng thông tối đa của một mạng hoặc kết nối internet. Nó thường được thực hiện bằng cách cố gắng tải về hoặc tải lên số dữ liệu tối đa trong thời gian ngắn nhất. Vì lý do này, kiểm tra băng thông có thể trì hoãn tốc độ truyền của mạng và gây ra chi phí dữ liệu tăng cao.

Một phương pháp chính xác hơn là sử dụng phần mềm chuyên dụng như Netcps, JDSU QT600, Spirent Test Center, IxChariot, Iperf, Ttcp, netperf hay bwping để đo thông lượng tối đa cho một truy cập mạng.

3.5 THU THẬP VÀ PHÂN TÍCH CHỨNG CỨ TỪ HỆ THỐNG

Hệ điều hành là nơi chứa nhiều điểm yếu mà kẻ tấn công có thể lợi dụng để tấn công chiếm quyền điều khiển hệ thống. Tuy nhiên trong hệ điều hành và các ứng dụng cài đặt trên đó luôn được ghi lại nhật ký. Do vậy thực hiện thu thập và phân tích chứng cứ từ hệ thống là công việc rất quan trọng cho điều tra tội phạm máy tính.

3.5.1 Từ trình duyệt, nhật ký trò chuyện.

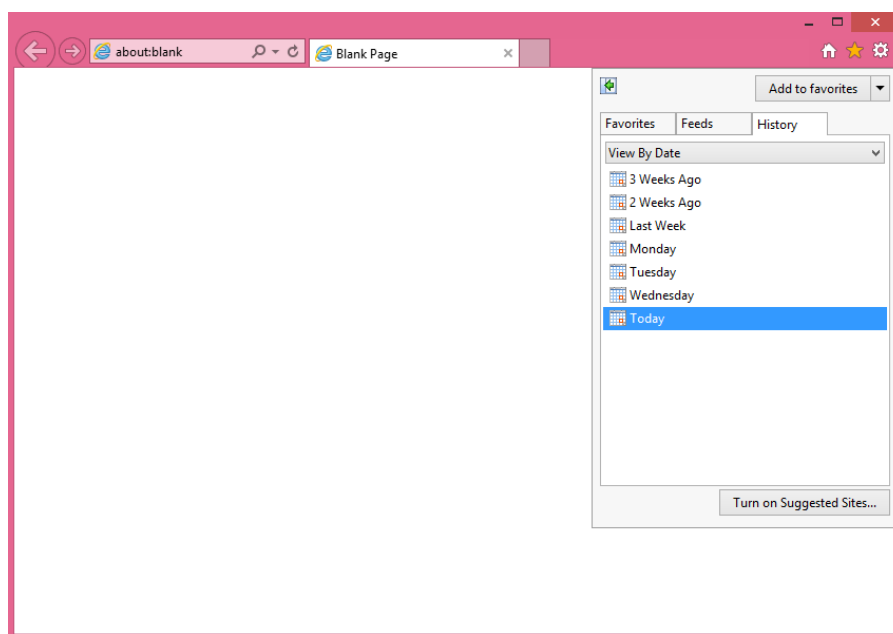
Có thể tìm kiếm chứng cứ trong trình duyệt, nhật ký trò chuyện, và các ứng dụng khác. Bất kỳ ứng dụng nào có thể sử dụng để giao tiếp trên Internet có khả năng chứa các chứng cứ. Trình duyệt web, email khách hàng, và các bản ghi trò chuyện là một số nơi có thể tìm kiếm chứng cứ. Trong phần này sẽ xem xét cụ thể các trình duyệt và nhật ký chat logs.

3.5.1.1 Tìm kiếm bằng chứng trong các trình duyệt

Tùy thuộc vào từng loại tội phạm máy tính, có thể tìm thấy chứng cứ trong trình duyệt. Rõ ràng, với tội phạm khiêu dâm trẻ em, trình duyệt có thể chứa bằng chứng trực tiếp của tội phạm. Trong hầu hết các trường hợp thì nó có thể cung cấp chứng cứ gián tiếp liên quan đến tội phạm máy tính. Ví dụ, nếu một người bị tình nghi là đã crack mật khẩu và xâm nhập vào máy chủ, ăn cắp dữ liệu tài chính, có thể tìm thấy chứng cứ gián tiếp thông qua trình duyệt của người đó. Có thể tìm thấy gần đây người đó đã tìm kiếm phương pháp

crack mật khẩu và có thể tải về một số tiện ích crack mật khẩu. Điều đó chắc chắn là bằng chứng gián tiếp, giúp thúc đẩy quá trình điều tra. Biết được những chứng cứ từ công cụ tìm kiếm cho ta cái nhìn sâu sắc về phương pháp mà tội phạm sử dụng đồng thời cho phép ta xây dựng lại chính xác hơn những gì đã xảy ra. Trong một cuộc điều tra hình sự, thậm chí một số thông tin không buộc tội trực tiếp có thể hữu ích trong việc tìm hiểu các tội phạm. Vậy nên, cần xem xét làm thế nào để có thể nhận được thông tin từ trình duyệt. Cần xem xét các trình duyệt khác nhau.

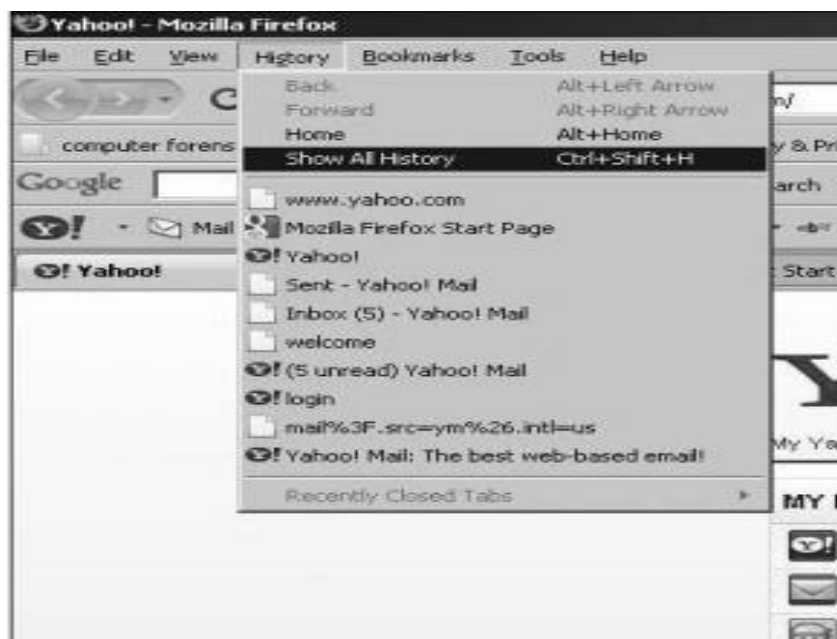
Khi sử dụng Internet Explorer, có thể xem toàn bộ lịch sử duyệt web của người dùng như trong hình 3.3. Rõ ràng nhiều tội phạm máy tính có đủ hiểu biết để xóa toàn bộ lịch sử duyệt web của chúng. Nhưng chỉ mất rất ít thời gian để kiểm tra lịch sử ấy và có thể nó mang lại kết quả. Có thể xem lịch sử trong trình duyệt bất kỳ. Hình 3.4 cho thấy lịch sử qua trình duyệt Mozilla Firefox. Hầu hết các trình duyệt có một tùy chọn cho phép ta xem lịch sử duyệt web, nhưng cũng có một tùy chọn xóa lịch sử đó. Đây là lý do tại sao khía cạnh cụ thể này thường không mang lại kết quả, nhưng nó vẫn còn giá trị để tìm hiểu được.



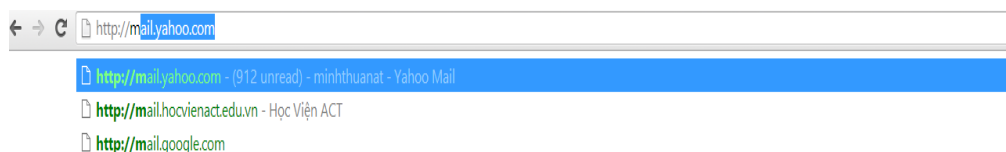
Hình 3.4. Lịch sử trình duyệt Internet Explorer.

Một cách khác đó là kiểm tra địa chỉ. Một số người không nhận ra rằng đây là một phần được tách ra khỏi lịch sử. Thanh địa chỉ ghi lại những địa chỉ web mà tội phạm gõ vào. Thanh địa chỉ có thể đặc biệt buộc tội trong trường

hợp điều tra tội phạm khiêu dâm trẻ em. Thủ phạm có thể cho rằng “chúng vô tình” xem qua khiêu dâm trẻ em là một lỗi tìm kiếm một chủ đề vô thưởng vô phạt. Tuy nhiên, rất khó để sử dụng lý do đó một khi đã trực tiếp gõ địa chỉ web chính xác vào thanh địa chỉ. Ví dụ về thanh địa chỉ như hình 3.5.



Hình 3.5. Lịch sử trình duyệt Mozilla Firefox



Hình 3.6. Thanh địa chỉ của trình duyệt

Một mục nữa hay quên xóa đó là phần hiển thị. Hầu hết các trình duyệt sẽ lưu lại những thuật ngữ tìm kiếm đã nhập trước đó để có thể dễ dàng tiến hành tra cứu một lần nữa nếu cần. Nếu gõ một vài từ khóa vào thanh tìm kiếm của bất kỳ một công cụ tìm kiếm nào, có thể thấy tính năng tự động của nó. Nếu nghi ngờ một người nào đó sử dụng máy tính này để crack mật khẩu thì chỉ cần gõ từ “crack mật khẩu” vào công cụ tìm kiếm.

Không có một kỹ thuật nào rõ ràng, chỉ có thể dùng cách này nếu có nghi ngờ tội phạm. Nó chỉ mất ít thời gian để kiểm tra và có thể mang lại những thông tin quan trọng. Một vấn đề khác là nhận thức được rằng nhiều người thường sử dụng nhiều trình duyệt khác nhau. Một tên tội phạm chuyên

nghiệp có thể không dùng biểu tượng của trình duyệt trên màn hình máy tính vậy nên cần tìm kiếm tất cả các trình duyệt trên máy tính.

3.5.1.2 Tìm kiếm chứng cứ trong nhật ký trò chuyện

Chat room là chương trình thường được sử dụng để liên lạc. Đôi khi nó cũng được sử dụng để trao đổi thông tin, thúc đẩy hoạt động của tội phạm thông qua các cuộc thảo luận trên phòng chat. Buôn bán hàng hóa bị đánh cắp, mại dâm,... tất cả những tội phạm ấy có thể sử dụng phòng chat là nơi giao tiếp, bàn bạc.

Hầu hết các phần mềm chat đều giữ ít nhất một bản ghi tạm thời của cuộc hội thoại. Điều này đúng với MSN Messenger, Yahoo! Messenger, và nhiều phần mềm khác. Đường dẫn chính xác để xem các bản ghi tùy thuộc vào từng phần mềm. Tuy nhiên trên menu thả xuống ta sẽ thấy một tùy chọn để xem lại các bản ghi ấy và có một tùy chọn là lưu lại. Nên kiểm tra phần mềm chat để xem nhật ký chat đã lưu giữ những cuộc trò chuyện. Điều này có thể cung cấp manh mối có giá trị.

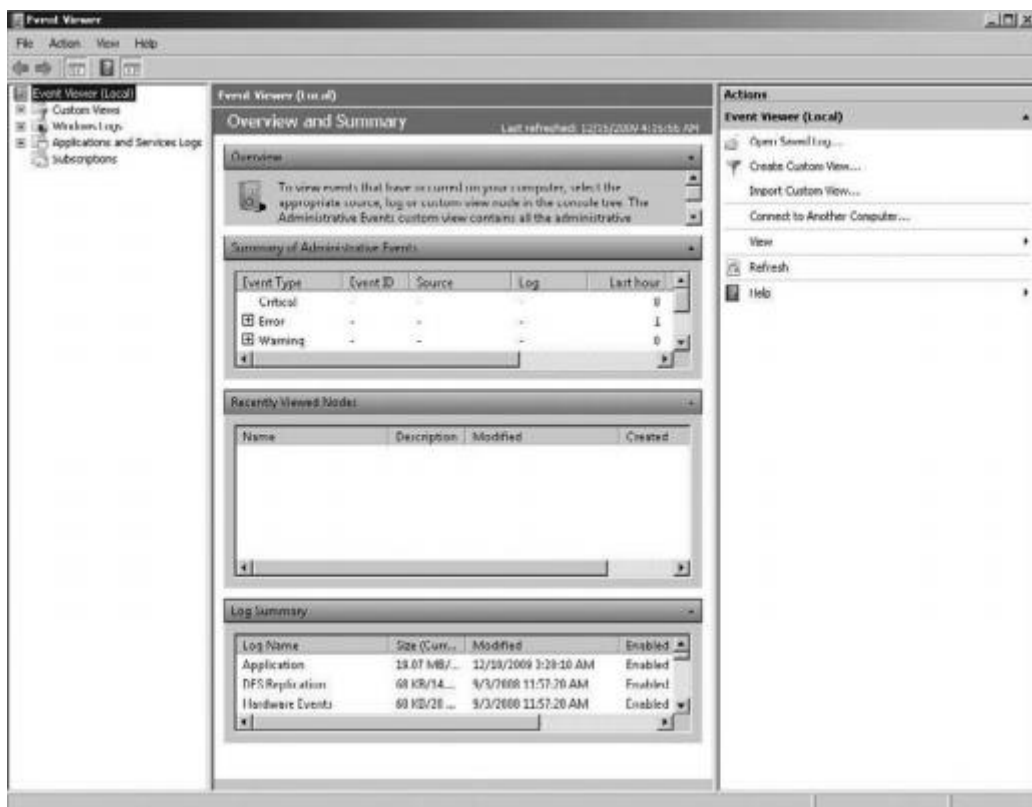
3.5.2 Từ các file log hệ thống

Mỗi hệ thống điều duy trì ghi log có thể cung cấp các thông tin. Điều quan trọng là có thể tìm kiếm các bản ghi bằng chứng ấy. Bản ghi log hệ thống thường chỉ ra đăng nhập thất bại hay thành công, cũng như bất kỳ cảnh báo mà hệ điều hành đưa ra. Sự khác nhau của các phiên bản Windows Server cũng ghi lại mỗi lần khởi động trong nhật ký. Vì vậy khi điều tra, chúng ta có thể nhìn vào bản ghi log trong một vài hệ điều hành để tìm ra những thông tin hữu ích.

3.5.2.1 Windows Log

Với Windows XP/Vista/7. Trong tất cả các phiên bản của Windows, ta có thể tìm thấy các bản ghi log bằng cách nhấp vào nút Start ở góc dưới bên trái của màn hình, sau đó nhấp vào Control Panel. Sau đó click vào Administrator Tools và Event Viewer. Ta thấy Event Viewer thể hiện trong hình 3.6. Bây giờ từ màn hình này ta có thể xem bản ghi log và các sự kiện. Nếu xem xét một phiên bản của Windows trước XP, một số log sau có thể không có mặt :

- **Bản ghi log ứng dụng** : ghi lại nhiều sự kiện đăng nhập bởi các ứng dụng. Nhiều ứng dụng sẽ ghi lại lỗi của chúng ở đây trong bản ghi log ứng dụng. Điều này có thể hữu ích đặc biệt là nếu đăng nhập trên một máy chủ mà có cơ sở dữ liệu.
- **Bản ghi log bảo mật** : Điều quan trọng nhất có thể tìm thấy trong bản ghi log bảo mật là lần đăng nhập thành công và lỗi. Bản ghi này cũng ghi lại các sự kiện liên quan đến sử dụng tài nguyên, như tạo, mở, hoặc xóa các tập tin hoặc đối tượng khác. Các quản trị viên có thể xác định những sự kiện được ghi lại trong bản ghi log bảo mật. Một số hacker/cracker tắt bản ghi log bảo mật để hoạt động của chúng không được ghi lại.
- **Bản ghi log Setup** : chứa các sự kiện liên quan đến cài đặt ứng dụng. Nơi này sẽ hiển thị các ứng dụng mới được cài đặt trên máy. Rõ ràng, hầu hết các virus và phần mềm gián điệp sẽ không ghi tới bản ghi log ứng dụng. Tuy nhiên, bản ghi này có thể cho biết các ứng dụng mới đã được cài đặt mà có thể là một lỗ hổng bảo mật hoặc là trojan.



Hình 3.7. Cửa sổ Event Viewer

- **Bản ghi log hệ thống:** Có chứa các sự kiện đăng nhập bởi các thành phần hệ thống Windows. Điều này bao gồm các sự kiện như lỗi driver.
- **Bản ghi sự kiện chuyển tiếp:** Được sử dụng để lưu trữ các sự kiện thu thập được từ máy tính từ xa. Nhật ký này rất quan trọng trong một môi trường mạng. Tuy nhiên, các hệ thống khác nhau phải được cấu hình để có được bản ghi này.
- **Bản ghi các ứng dụng và dịch vụ:** Là một loại bản ghi mới của bản ghi log sự kiện. Những sự kiện này lưu trữ các bản ghi từ một ứng dụng hoặc thành phần chứ không phải là sự kiện có tác động lên toàn hệ thống. Điều này có tiết lộ các vấn đề với một ứng dụng cụ thể hoặc thành phần Windows.

Hai bản ghi log quan trọng là bảo mật và đăng nhập hệ thống. Các hạng mục quan trọng nhất trong bản ghi log bảo mật là bản ghi của tất cả các đăng nhập hoặc đăng xuất dù là thành công hay không thành công. Đây là dấu hiệu đầu tiên của một nỗ lực xâm nhập vào máy chủ. Nếu thấy rất nhiều lần đăng nhập thất bại, hoặc nếu thấy thông tin đăng nhập tài khoản vào các giờ lẻ, mà có thể là một dấu hiệu cho thấy hoạt động bất hợp pháp đang diễn ra. Đây là một trong những điều đơn giản nhất để kiểm tra, vì vậy chắc chắn không nên bỏ qua phần này.

3.5.2.2 *Linux log*

Hệ điều hành Linux cũng ghi lại nhật ký hoạt động. Tất cả các bản ghi log hệ thống điều hành có thể tìm được trong mục /var/log subdirectory. Có một số bản ghi log có thể tìm thấy trong thư mục này. Một vài trong số này không có mặt trong tất cả các bản của Linux, vậy cần tìm trong thư mục đó và xem các bản ghi log có mặt:

- /var/log/faillog: tập tin đăng nhập này có chứa thông tin đăng nhập người dùng không thành công. Điều này có thể rất quan trọng khi theo dõi cracker.
- /var/log/kern.log: tập tin đăng nhập này được sử dụng cho tất cả các tin nhắn từ nhân của hệ điều hành. Điều này không có khả năng thích hợp với hầu hết các máy tính của tội phạm.

- /var/log/lpr.log: đây là nhật ký log máy in có thể cung cấp một bản ghi bất kỳ được in ra từ máy này. Điều này có thể hữu ích cho doanh nghiệp cạnh tranh.
- /var/log/mail.*: đây là nhật ký máy chủ email và có thể hữu ích trong việc điều tra tội phạm máy tính. Email có thể là một phần cần thiết của bất kỳ tội phạm máy tính nào .
- /var/log/mysql.*: bản ghi log này liên quan đến hồ sơ máy chủ cơ sở dữ liệu MySQL .
- /var/log/apache2/*: nếu máy tính này đang chạy máy chủ web Apache, sau đó bản ghi log sẽ hiển thị các hoạt động liên quan. Điều này hữu ích khi theo dõi hacker.
- /var/log/lighttpd/*: nếu máy này đang chạy máy chủ web Lighttpd, sau đó bản ghi log sẽ hiển thị các hoạt động liên quan. Điều này có thể hữu ích khi theo dõi hacker cố gắng hack máy chủ web.
- /var/log/apport.log: Đây là hồ sơ ứng dụng bị treo. Đôi khi, nó cho thấy sự hiện diện của virus hoặc phần mềm gián điệp.
- /var/log/user.log: Chứa bản ghi hoạt động của người dùng và có thể rất quan trọng với một cuộc điều tra hình sự.

Có một số phương pháp để xem các bản ghi, trong đó có một số lệnh ai cũng có thể vào và xem các bản ghi trong hệ thống linux. Ví dụ nếu muốn xem nhật ký ghi log máy in, làm như sau :

- # tail -f/var/log/lbr.log
- # less/var/log/lbr.log
- # more -f/var/log/lbr.log
- # vi/var/log/lbr.log

Tuy nhiên, bằng cách sử dụng lệnh dmesg trong Linux có thể xem các bản ghi từ vỏ. : dmesg | lpr

Nhưng một số bản ghi log chỉ có quyền root mới được xem. Nếu sử dụng giao diện người dùng đồ họa Gnome, nó đi kèm với một tiện ích có tên là System Log Viewer. Tiện ích này là một đồ họa, xem trình đơn điều khiển có thể sử dụng xem tất cả các bản ghi log của hệ thống. Hệ thống Log Viewer đi kèm với xây dựng các chức năng như lịch, màn hình đăng nhập và hiển thị

số liệu thống kê. Đây là một công cụ rất hữu ích cho việc kiểm tra các bản ghi hệ thống Linux.

Có những kỹ thuật có thể được sử dụng xóa bản ghi log hoàn toàn hoặc chọn xóa mục tùy chọn. Cũng có những hacker có thể chuyển bản ghi log ra trong khi đang hoạt động và sau đó tiếp tục. Nhưng không phải tất cả tội phạm máy tính đều thành thạo các kỹ thuật này, vì vậy nên kiểm tra các bản ghi log các sự kiện. Tuy nhiên, không có bằng chứng trong tất cả các bản ghi log có thể đảm bảo rằng vi phạm an ninh đang xảy ra.

Để biết được những kỹ thuật này, sau đây là mô tả ngắn gọn một vài kỹ thuật:

- Xóa bản ghi log: Bất kỳ người sử dụng với quyền quản trị đơn giản có thể quét sạch một bản ghi log. Tuy nhiên, điều này rõ ràng khi bạn nhìn thấy một bản ghi sự kiện rỗng.
- Sử dụng auditpol.exe. Đây là một tiện ích quản trị tồn tại trong hệ thống Windows. Nó sẽ không hiển thị trên máy tính để bàn hoặc trong các chương trình, cần phải biết và tìm nó. Sử dụng auditpol \ipaddress / vô hiệu hóa lần lượt các bản ghi log. Sau đó khi tội phạm thoát ra, chúng sẽ sử dụng auditpol \ipaddress / cho phép quay trở lại.
- Có một tiện ích trên Web có thể giúp kẻ tấn công trong quá trình này. Ví dụ, WinZapper cho phép loại bỏ chọn lọc một số bản ghi log trong Windows.

Đây là một vài ví dụ về kỹ thuật mà tin tặc có thể sử dụng. Cho rằng bản ghi log dễ bị xóa, có thể tự hỏi tại sao phải kiểm tra chúng. Nhưng trên thực tế, hầu hết các tội phạm máy tính không phải là hacker có tay nghề cao. Hầu hết tội phạm máy tính không có khả năng che giấu tất cả dấu vết của chúng.

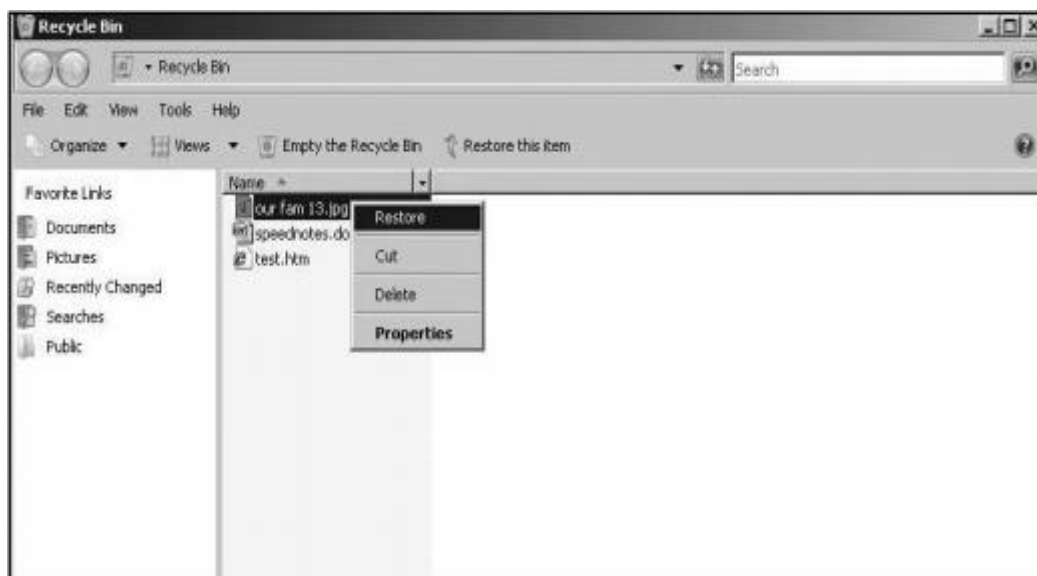
3.5.3 Phục hồi các dữ liệu đã bị xóa

Với bất kỳ loại tội phạm nào, hủy chứng cứ là một mối quan tâm cho các thủ phạm. Thông thường, chúng sẽ xóa các tập tin có thể bị buộc tội. Xem các tập tin khiêu dâm trẻ em, phần mềm gián điệp, hoặc tài liệu, thủ phạm có thể xóa các tập tin quan trọng. Nhưng nó có thể phục hồi lại được. Tập tin được lưu trữ trên một ổ đĩa, và hệ điều hành giữ một bản ghi của tất

cả các tập tin trên ổ đĩa cứng của máy. Tùy thuộc vào hệ điều hành máy tính đang chạy, mà ta có thể lấy lại các tập tin bị xóa.

3.5.3.1 Phục hồi tập tin từ hệ điều hành Windows

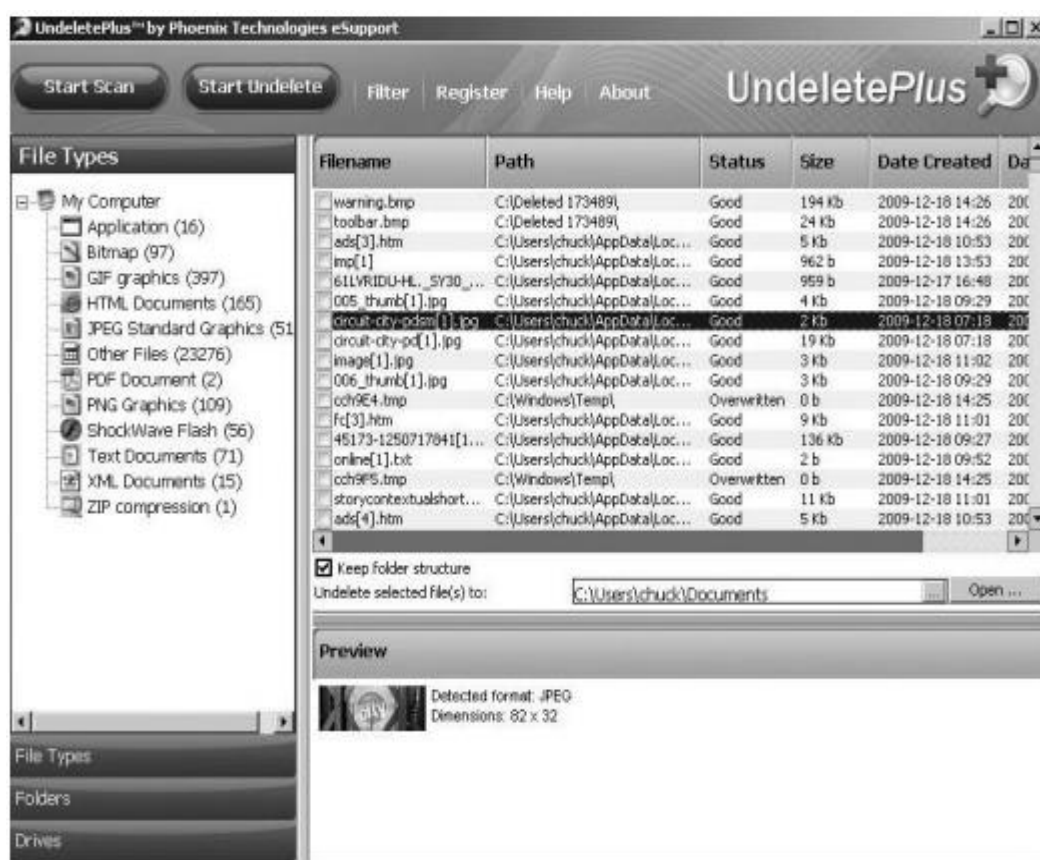
Trong hệ điều hành Windows, các tập tin được lưu trữ tại một bảng gọi là File Allocation Table (FAT). Đó là các file hệ thống được dùng trong Windows 3.1 và Windows 95/98. Từ Windows 2000 trở đi, Microsoft đã sử dụng NTFS cho hệ thống tập tin, tuy nhiên NTFS vẫn giữ vai trò một file table. Khi một tập tin bị xóa, đầu tiên nó bị chuyển qua thùng rác, với điều tra viên phải luôn kiểm tra thùng rác đầu tiên, những dữ liệu bị xóa ở đây có thể khôi phục lại đơn giản như hình 3.7. Nếu thùng rác đã bị làm trống, thì tất cả cũng chưa bị mất. Cách mà Windows làm việc khi bạn xóa một tập tin, đó là nó được chuyển đến một vị trí mới – thùng rác. Khi thùng rác rỗng, các tập tin bị xóa đơn giản chỉ bị loại bỏ từ bảng phân bổ nhưng nó vẫn còn trên ổ đĩa cứng. Nhiều nhà cung cấp như McAfee đã tạo ra một tiện ích mà khi mất một tập tin, không chỉ xóa nó, loại bỏ nó trong thùng rác nhưng sau ghi đè lên không gian tập tin với dữ liệu ngẫu nhiên, sau đó xóa các dữ liệu ngẫu nhiên. Quá trình này lặp đi lặp lại nhiều lần để đảm bảo rằng các tập tin ban đầu đã thực sự được xóa. Quá trình này thường được gọi như là băm nhỏ.



Hình 3.8. Recycle Bin

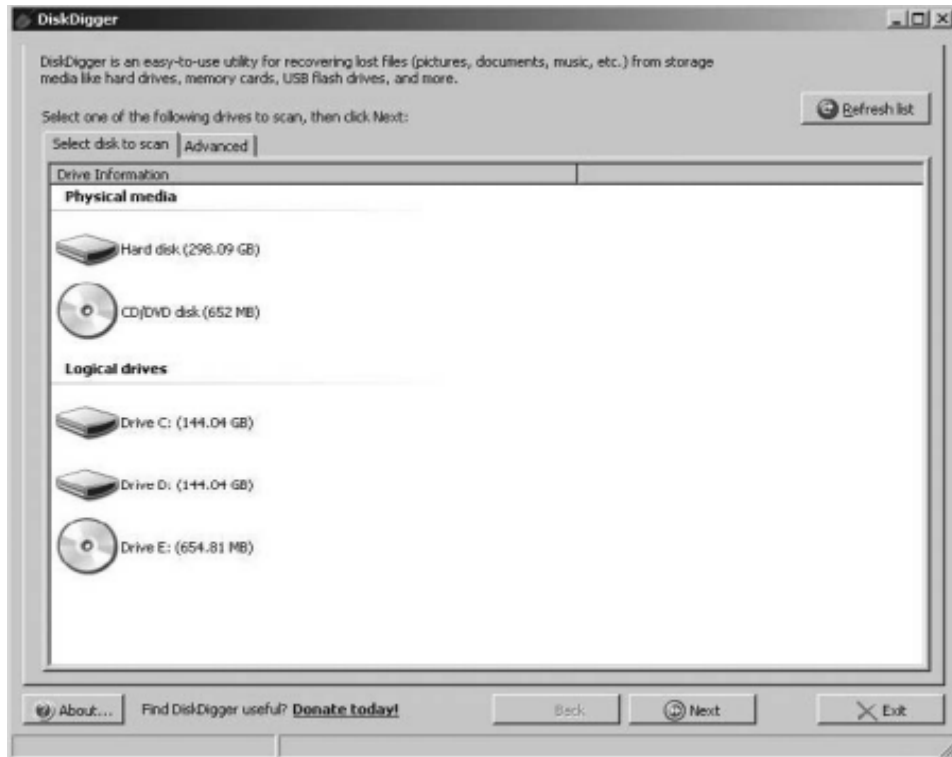
Vẫn có thể phục hồi các tập tin, nhưng cần một số loại tiện ích phục hồi. Có một số tiện ích có sẵn trên Internet. Chúng có chi phí thấp và thậm chí còn cho tải miễn phí. Sau đây sẽ xem xét một vài tiện ích như vậy :

- UndeletePlus : có sẵn tại <http://www.undelete-plus.com> với giá 29,95\$. Điều làm cho công cụ này xứng đáng được đề cập đến đó là nó rất dễ sử dụng. Chỉ cần chọn ổ đĩa và nhấn vào nút Scan, nó sẽ liệt kê các tập tin đã bị xóa (xem hình 3.8)

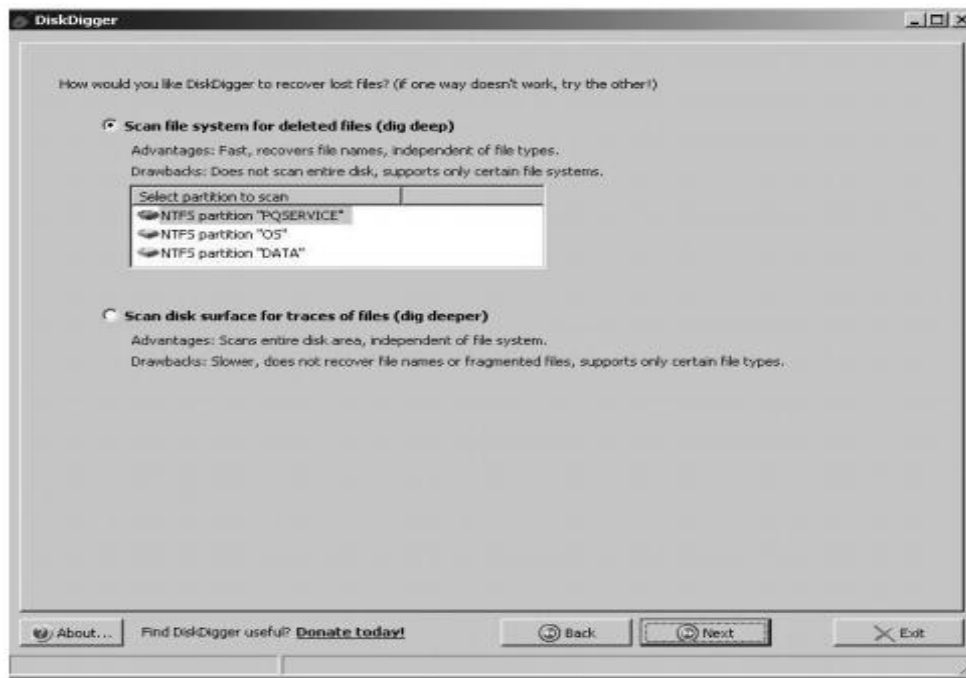


Hình 3.9. UndeletePlus

- DiskDigger: Sản phẩm này có tại <http://dmitrybrant.com/diskdigger> và nó là phần mềm miễn phí. Tiện ích này có một giao diện wizard mà người dùng có thể truy cập. Màn hình ban đầu thể hiện trong hình 3.9, yêu cầu người dùng mà ổ đĩa họ muốn quét. Sau đó người dùng được yêu cầu những gì cần tìm kiếm. Nó có thể thực hiện tìm nhanh và ít kỹ lưỡng hoặc tìm kiếm sâu và chậm hơn, như hình 3.10. Cuối cùng người dùng có thể chọn tìm kiếm các tập tin nhất định. Điều này rất hữu ích nếu biết những gì đang tìm kiếm. Thể hiện như hình 3.11.



Hình 3.10. Lựa chọn ổ đĩa Disk Digger.

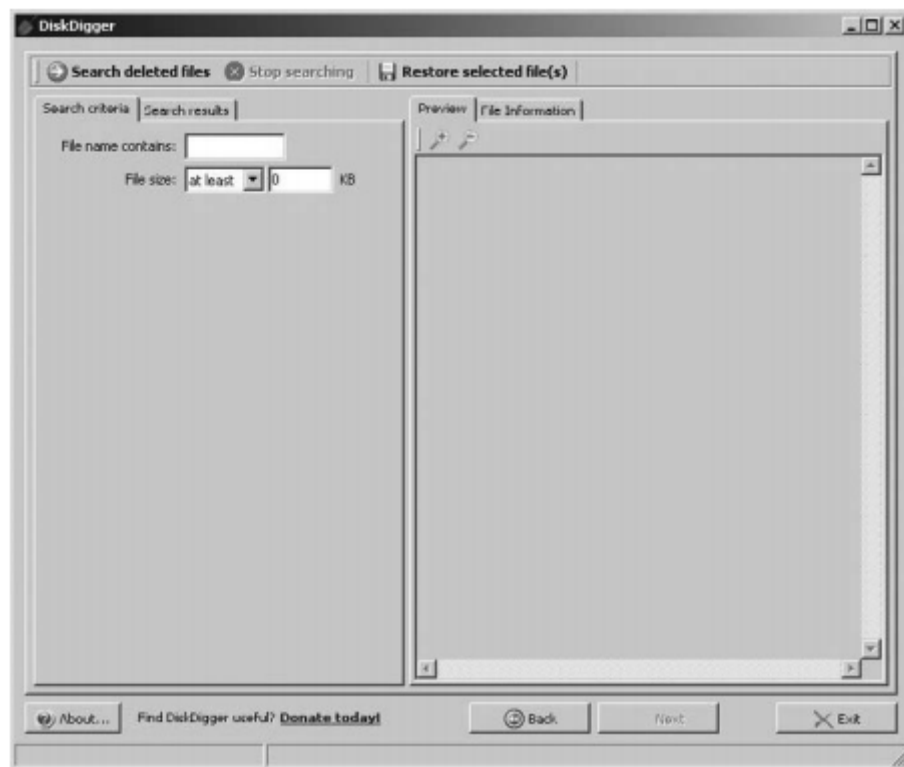


Hình 3.11. Tìm kiếm trên DiskDigger

Có rất nhiều tiện ích có sẵn khác. Chỉ đơn giản là tìm kiếm bằng Yahoo hay Google sẽ mang lại rất nhiều. Nhưng điều quan trọng đó là nhận ra rằng hiệu quả của những công cụ này phụ thuộc vào nhiều yếu tố. Thời gian khi tập tin bị xóa là một yếu tố. Một tập tin đã được xóa

rất lâu thì nhiều khả năng nó là một tập tin đã bị ghi đè. Một vấn đề khác nữa đó là tần số mà các ổ đĩa cứng là phân mảnh/ tối ưu hóa. Mỗi khi nó được chống phân mảnh, có một cơ hội ghi đè lên tập tin bị xóa. Nhưng nó luôn là một ý tưởng tốt để cố gắng khôi phục các file bị xóa.

Cũng có một số phương pháp thủ công cho việc khôi phục các tập tin bị xóa trong Windows. Để khôi phục lại một tập tin, cần đổi lại tên tập tin. Cũng cần phải sửa chữa các chuỗi (danh sách thư mục, FAT, clusters). Điều này có thể được thực hiện thủ công bằng cách sử dụng một chương trình như DiskDigger.



Hình 3.12. Tìm kiếm tập tin trên DiskDigger

3.3.3.2. Phục hồi tập tin từ hệ điều hành Unix/ Linux

Khi sử dụng hệ điều hành Unix hoặc một hệ thống điều hành liên quan chẳng hạn như Linux hoặc BSD một tập tin bị xóa thì liên kết truy cập bị giảm đi. Ngay khi liên kết truy cập là 0, các tập tin là “unlinks”, và bị loại bỏ. Vì Linux là hệ điều hành đa người dùng, đa nhiệm, người sử dụng hoặc các quá trình khác có thể ghi đè lên xóa không gian tập tin trên ổ đĩa. Vì vậy trước tiên cần phải cài hệ điều hành xuống chế độ người dùng đơn. Một tập tin có thể bị xóa bằng cách sử dụng công cụ debugfs: đầu tiên thay đổi thời gian xóa

là 0, tiếp theo tăng số liên kết lên 1. Sau đó chạy e2fsck sẽ cho phép đi tới các liên kết bị bỏ và tìm thấy thư mục bị mất. Có nhiều phương pháp cho phép khôi phục lại tập tin đã bị xóa. Đây là một quá trình theo từng bước :

- Đầu tiên, sử dụng lệnh `shell#wallOutput` để cho người dùng biết hệ thống đang chuyển sang chế độ người dùng đơn. Điều này sẽ cung cấp kết quả như sau : `System is going down to please save your work. Press CTRL+D to send message.`
- Khi đã chuyển sang chế độ đơn người dùng, có một số phương pháp có thể sử dụng. Sau đây là phương pháp Unix/ Linux thay vì sử dụng lệnh `grep`. Cú pháp như sau :

```
grep -b 'search-text' /dev/partition > file.txt
```

Hoặc cũng có thể sử dụng cú pháp sau :

```
grep -a -B[size before] -A[size after] 'text' /dev/[your_partition] > file.txt
```

Những cờ sử dụng được quy định như sau :

- i : Bỏ qua trường hợp khác biệt trong cả PATTERN và các tập tin đầu vào (tức là phù hợp với cả chữ hoa và chữ thường)
- a : Quá trình một tập tin nhị phân như là văn bản.
- B : In số dòng / kích thước phần đầu của văn bản trước khi nối các dòng.
- A : In số dòng/ kích thước phần sau của văn bản sau khi nối các dòng.

Ví dụ, để phục hồi một tập tin văn bản bắt đầu với `nixCraft` trên `/dev/sda1`, có thể sử dụng lệnh sau :

```
# grep -i -a -B10 -A100 nixCraft' /dev/sda1 > file.txt
```

- Tiếp theo xem `file.txt`. Phương pháp này chỉ hữu ích khi file đã xóa là file văn bản. Cũng giống như hệ điều hành Windows, có những tiện ích có thể sử dụng để phục hồi các file Unix. Nó thường tốt hơn là sử dụng một tiện ích cố gắng phục hồi tập tin. Sau đây là một vài tiện ích :

- Midnight

Commander:

<http://www.datarecoverypros.com/recover-linux-midnightcommander.html>.

- Disk Doctors : <http://www.diskdoctors.net>; Sản phẩm này cũng đi kèm các phiên bản cho Windows và Macintosh.

Dù phục hồi các file bị xóa bằng tay hay sử dụng một tiện ích để thực hiện thì vấn đề cũng vẫn giống nhau. Như đã nói không có gì đảm bảo rằng tập tin đã xóa không bị ghi đè. Và một tên tội phạm máy tính hiểu biết sẽ sử dụng các công cụ xóa của McAfee hay đơn giản là trình phân mảnh Windows để phục hồi file bị xóa khó khăn hơn. Nhưng đây vẫn luôn là ý tưởng tốt để kiểm tra.

3.5.4 Vị trí quan trọng cần kiểm tra

Trong bất kỳ hệ điều hành nào, có những thư mục quan trọng sẽ có những thông tin giá trị cho điều tra viên. Thông tin có thể bao gồm các tập tin, hình ảnh, các tập tin cookies. Chúng nằm ở vị trí khác nhau với mỗi hệ điều hành, vì vậy cần xem xét từng hệ thống riêng biệt :

3.5.4.1 Trong Windows

Khi cài đặt Windows, trình cài đặt có thể chọn vị trí bất kỳ. Tuy nhiên trên hầu hết các máy, có thể tìm thấy vị trí mặc định. Ví dụ C:\thư mục người dùng, chỉ truy cập được nếu người dùng có quyền quản trị.

- C:\Program Files. Đây là nơi hầu hết các chương trình được cài đặt. Là nơi tốt để tìm các phần mềm gián điệp, công cụ hack, và phần mềm khác có thể liên quan đến tội phạm máy tính.
- C:\Windows. Đây là nơi mà các hệ điều hành được lưu trữ. Kiểm tra các thư mục tạm thời có thể mang lại những bằng chứng hữu ích. Cũng là một ý hay để tìm kiếm bất cứ file mới trong thư mục này, vì chúng có thể là dấu hiệu của phần mềm gián điệp hay virus.
- C:\Windows\System32. Thư mục này chứa các file hệ thống quan trọng DLLs. Nếu thấy có bổ sung mới có nghĩa là phần mềm mới được cài đặt. Phần mềm mới có thể bao gồm các chương trình chat, phần mềm gián điệp hoặc virus.
- C:\Users\username\Documents. Đây là vị trí mặc định của các tài liệu, và là một nơi tốt để kiểm tra. Khi đăng nhập vào Windows và vào C:\Users \username\Documents – thư mục cho người sử dụng hiện đang đăng nhập.

- C:\Users\username\Pictures. Đây là nơi lưu trữ hình ảnh mặc định của Windows, cũng như tài liệu là thư mục tài liệu mặc định.
- C:\Users\username\Favorites. Đây là nơi Internet Explorer lưu trữ thư mục yêu thích của mỗi người dùng. Là nơi có thể tìm ra những trang web mà tội phạm có thể đánh dấu.
- C:\Users\username\Desktop. Cho thấy màn hình máy tính người dùng.
- C:\Users\username\Downloads. Thư mục này quan trọng. Đây là vị trí mặc định cho bất kỳ chương trình tải về từ Internet.

3.5.4.2 Trong Linux

Cũng giống như Windows, Linux có một số thư mục quan trọng cần xem xét và phải đăng nhập như người dùng với quyền quản trị để xem. Trong Linux, thực sự trong tất cả các hệ thống Unix, tài khoản quản trị là root.

- /home. Thư mục này là thư mục của mỗi người dùng. Nó tương tự như C:\Users trong Windows.
- /root. Đây là thư mục cho người quản trị có quyền root. Hacker luôn muốn hack được tài khoản root trên bất kỳ hệ thống Unix.
- /var. Thư mục này có chứa các mục quản trị như các bản ghi, cần kiểm tra thư mục này triệt để.
- /temp. Nơi đây chứa các tập tin tạm thời.
- /etc. Chứa các tập tin cấu hình. Khi điều tra sự xâm nhập, thường thì thủ phạm thay đổi file cấu hình. Vì vậy so sánh các tập tin cấu hình trên máy tính bị nghi ngờ với các phiên bản sao lưu có thể rất hữu ích.

3.5.5 Các tiện ích hệ điều hành

Trong mỗi hệ điều hành các tiện ích có thể giúp đỡ điều tra viên.

Tiện ích đầu tiên cần xem xét đó là netstat. Tiện ích này hoạt động trong Linux hoặc Windows. Nó viết tắt bởi “network status”, và cho biết bất kỳ kết nối trực tiếp nào trên máy. Nếu ai đang truy cập vào máy tính hoặc nếu máy tính đang truy cập vào một số tài nguyên từ xa, nó sẽ hiển thị trong netstat. Có thể thấy netstat trong hình 3.12

```

C:\WINDOWS\system32\cmd.exe - netstat
Proto Local Address      Foreign Address    State
C:\Documents and Settings\Administrator>netstat
Active Connections
Proto Local Address      Foreign Address    State
TCP    COMPANY-8884706:1100 65.55.21.250:http  ESTABLISHED
TCP    COMPANY-8884706:1101 65.54.77.76:http   ESTABLISHED
TCP    COMPANY-8884706:1102 65.55.17.25:http   ESTABLISHED
TCP    COMPANY-8884706:1103 205.128.92.126:http ESTABLISHED
TCP    COMPANY-8884706:1104 199.93.62.126:http  ESTABLISHED
TCP    COMPANY-8884706:1105 199.93.62.126:http  ESTABLISHED
TCP    COMPANY-8884706:1106 8.12.213.126:http   ESTABLISHED
TCP    COMPANY-8884706:1107 8.12.213.126:http   ESTABLISHED
TCP    COMPANY-8884706:1108 *.112.207.net:http  ESTABLISHED
TCP    COMPANY-8884706:kpoe 65.54.77.92:http    ESTABLISHED
TCP    COMPANY-8884706:1110 24.143.192.27:http  ESTABLISHED
TCP    COMPANY-8884706:1111 cds99.sjc9.msecn.net:http CLOSE_WAIT
TCP    COMPANY-8884706:1112 cds215.sjc9.msecn.net:http ESTABLISHED
TCP    COMPANY-8884706:1113 cds215.sjc9.msecn.net:http ESTABLISHED
TCP    COMPANY-8884706:1114 65.55.15.243:http   ESTABLISHED
TCP    COMPANY-8884706:1115 65.55.15.122:http   ESTABLISHED
TCP    COMPANY-8884706:1116 65.55.239.188:http  ESTABLISHED

```

Hình 3.13. Tiện ích Netstat

Chạy lệnh Start, Run và gõ cmd nếu là hệ điều hành Windows XP, hoặc chọn start, gõ cmd vào hộp tìm kiếm nếu là hệ điều hành Windows Vista hay Windows 7. Lệnh có thể chạy từ dòng lệnh là fc, viết tắt của tập tin so sánh. Ví dụ nếu có một tập tin cấu hình mà biết là bị thay đổi và có một bản sao trước đó, có thể sử dụng fc để so sánh, sẽ xuất hiện sự khác biệt. Ví dụ như hình 3.13 so sánh 2 tập tin văn bản. Tương tự như vậy với lệnh CMP trong Linux.

```

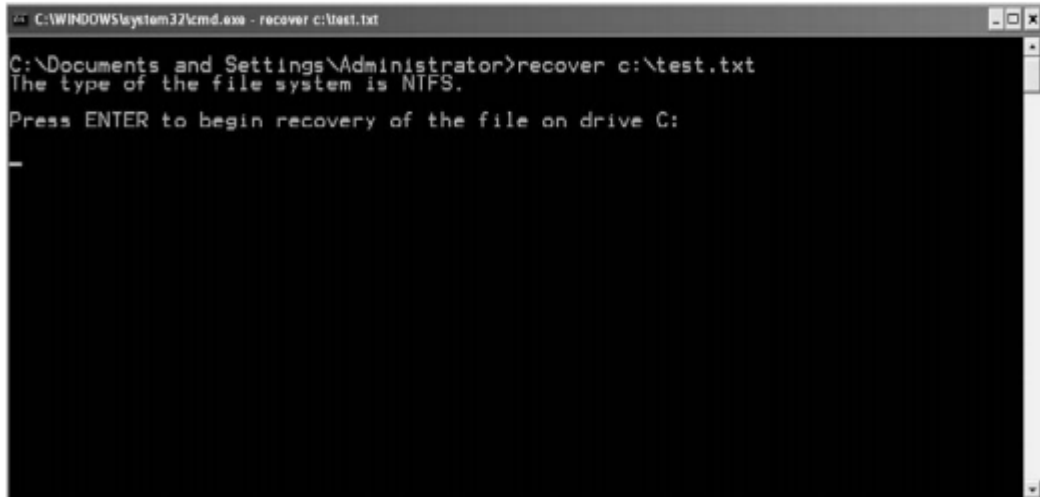
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>fc test1.txt test2.txt
Comparing files test1.txt and TEST2.TXT
***** test1.txt
these are the same
this line is the altered line
***** TEST2.TXT
these are the same
this line is the original line
*****
C:\Documents and Settings\Administrator>

```

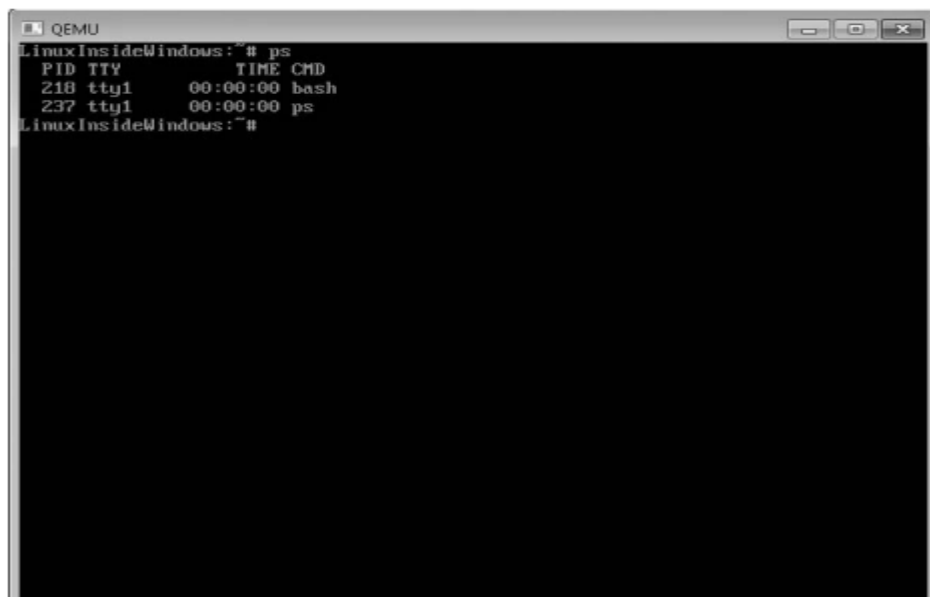
Hình 3.14. Lệnh fc

Một lệnh hữu ích trong điều tra đó là phục hồi. Lệnh này phục hồi những phần có thể đọc được của một tập tin bị xóa. Ví như hình 3.14. Có một

tiện ích tương tự trong Linux là ddrescue. Một lệnh hữu ích có trong Linux mà Windows không có đó là ps. Điều này cung cấp cho ta một danh sách tất cả các tiến trình đang chạy. Nếu có virus hoặc phần mềm gián điệp đang chạy ở chế độ nền, sẽ thấy trong danh sách tiến trình. Lệnh ps được thể hiện trong hình 3.15



Hình 3.15. Tiện ích Recover



Hình 3.16. Tiện ích ps

Đây chỉ là một số tiện ích có thể hữu ích trong điều tra tìm chứng cứ.

Hệ điều hành có thể là một kho tàng các thông tin và bằng chứng. Các bản ghi hệ thống, trình duyệt, và cả những tập tin đã bị xóa có thể cung cấp những thông tin có giá trị. Điều quan trọng là các điều tra viên phải quét tất cả

các bằng chứng có thể có sẵn trong đó. Tuy nhiên cần lưu ý rằng phải chứng minh từng bước trong quá trình này. Nếu sử dụng một số tiện ích để phục hồi các file bị xóa, cần chứng minh những tiện ích đã sử dụng và lưu lại chính xác các bước đã thực hiện.

3.6 THU THẬP VÀ PHÂN TÍCH CHỨNG CỨ TỪ NGUỒN KHÁC

Trong các phần trước, chúng ta đã xem xét cách thu thập chứng cứ từ các nguồn khác nhau bao gồm cả ổ đĩa cứng và hệ điều hành, kỹ thuật để thu thập chứng cứ từ trình duyệt của máy tính thậm chí cả những tiện ích có sẵn trong hệ điều hành để tìm ra bằng chứng. Tuy nhiên, bằng chứng đang tìm kiếm có thể chưa được tìm ra. Cần xét thêm cả những chứng cứ có thể có được từ máy chủ email trong một địa điểm từ xa, hay theo dõi máy tính của thủ phạm. Đó có thể là thiết bị định tuyến, và các thiết bị khác có thể tìm ra chứng cứ. Điều quan trọng là kỹ năng điều tra bao gồm khả năng thu thập chứng cứ từ các nguồn khác nhau. Trong phần này sẽ tìm hiểu thêm bổ sung vào kỹ thuật tìm kiếm chứng cứ từ các nguồn khác.

3.6.1 Truy tìm địa chỉ IP

Đôi khi có những dữ liệu cần theo dõi nguồn của nó. Ví dụ nếu nạn nhân nhận được email đe dọa hoặc muốn tìm ra nguồn của một cuộc đột nhập an ninh. Hay cũng có thể trong trường hợp theo dõi hình ảnh, địa điểm cụ thể về trẻ em khiêu dâm. Trong phần này chúng ta sẽ xem xét theo dõi địa chỉ IP như thế nào.

Xét về mặt tổng thể IP là viết tắt của Internet protocol. Một địa chỉ IP là địa chỉ xác định số node trên mạng. Một node bất kỳ thiết bị kết nối mạng. Một node có thể là máy tính cá nhân, máy chủ, router hoặc một thiết bị nối mạng như máy in. Địa chỉ IP bao gồm bốn số từ 0 đến 255. Ví dụ 192.168.1.1. Địa chỉ IP xác định duy nhất một node. Địa chỉ IP có thể thay thế bởi địa chỉ dùng tên miền (DNS) ví dụ như <http://www.google.com>. Những địa chỉ này được gọi là một URL. Máy tính chỉ có thể hiểu được các địa chỉ IP, còn chúng ta dùng địa chỉ URL để ghi nhớ dễ dàng hơn. Khi bất kỳ liên lạc được thiết lập, có một địa chỉ IP đích và một địa chỉ IP nguồn. Bây giờ nếu như đang điều tra thông tin liên lạc đến từ một nguồn mà bị nghi là của tội phạm, thì bước đầu tiên là theo dõi địa chỉ IP nguồn của nó. Đầu tiên nếu

trong Windows vào Start, gõ cmd và bắt đầu tìm kiếm địa chỉ muốn theo dõi. Nếu sử dụng Linux, gõ tracer, sau đó là địa chỉ IP hoặc URL muốn theo dõi. Ví dụ hình 3.16

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\chuck>tracert www.ChuckEasttom.com

Tracing route to sbs-p6p.asbs.yahoodns.net [98.136.92.77]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    192.168.1.1
  1  *         *         *         Request timed out.
  2  17 ms    30 ms    17 ms    24.164.211.145
  3  16 ms    19 ms    17 ms    24.164.209.116
  4  19 ms    11 ms    8 ms     gig5-0-0.dl1atxchn-rtr5.tx.rr.com [70.125.217.10]
  5  35 ms    25 ms    22 ms    gig2-0-2.hstntxl3-rtr1.texas.rr.com [72.179.205.145]
  6  23 ms    22 ms    15 ms    xe-9-1-0.bar1.Houston1.Level3.net [4.79.88.25]
  7  32 ms    19 ms    21 ms    ae-0-11.bar2.Houston1.Level3.net [4.69.137.134]
  8  35 ms    35 ms    37 ms    ae-7-7.ebr1.Atlanta2.Level3.net [4.69.137.142]
  9  32 ms    35 ms    48 ms    ae-73-70.ebr3.Atlanta2.Level3.net [4.69.138.201]
 10  50 ms    51 ms    53 ms    ae-2.ebr1.Washington1.Level3.net [4.69.132.86]
 11  56 ms    53 ms    56 ms    ae-61-61.csw1.Washington1.Level3.net [4.69.134.1]
 12  48 ms    47 ms    45 ms    ae-11-69.car1.Washington1.Level3.net [4.68.17.3]
 13  55 ms    56 ms    57 ms    4.79.228.2
 14  59 ms    65 ms    65 ms    xe-7-0-0.mar2.ac2.yahoo.com [216.115.108.129]
 15  56 ms    60 ms    63 ms    te-9-1.bas-b1.ac4.yahoo.com [76.13.0.207]
 16  71 ms    65 ms    62 ms    p6p2.geo.ac4.yahoo.com [98.136.92.77]

Trace complete.

C:\Users\chuck>

```

Hình 3.17. Lệnh Tracert

Điều này hiển thị tất cả các bước truyền trực tiếp từ máy điều tra và máy thủ phạm. Đã có địa chỉ IP đích ta có thể tìm hiểu thông tin về nó sử dụng cơ sở dữ liệu như Whois. Một số trang web cung cấp giao diện người dùng thân thiện với một cơ sở dữ liệu có chứa thông tin về những người đã đăng ký một trang web hay lĩnh vực nào đó. Ví dụ :

- + <http://www.whois.net>
- + <http://www.networksolutions.com/whois/index.jsp>
- + <http://www.who.is>
- + <http://www.internic.net/whois.html>.
- + <http://cqcouneter.com/whois/>

Cũng có thể nhập một URL vào các trang web này. Ví dụ trang <http://cqcouneter.com/whois/> có thể cho ta thấy <http://www.chuckeasttom.com>. Hình 3.17 ta thấy tên miền được đăng ký vào ngày 24/7/2011; người đang lưu trữ trang web (Yahoo!) và các thông tin khác.

CHUCKEASTTOM.COM - Domain Information	
Domain	CHUCKEASTTOM.COM [Site Info Traceroute RBL/DNSBL lookup]
Registrar	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Registrar URL	http://www.melbourneit.com
Whois server	whois.melbourneit.com
Created	24-Jul-2001
Updated	16-Aug-2009
Expires	24-Jul-2011
Time Left	569 days 20 hours 56 minutes
Status	ok
DNS servers	NS8.SAN.YAHOO.COM 66.218.71.205 NS9.SAN.YAHOO.COM 66.196.84.168

Hình 3.18. Tìm kiếm với Whois

Các trang OtherWhoisWeb có thể cung cấp chi tiết hơn. Ví dụ khi chạy URL <http://www.chuckeasttom.com> thông qua công cụ Network Solutions's Whois (<http://www.networksolutions.com/whois/index.jsp>) có thể thấy thông tin bổ sung như hình 3.18. Đó là tên liên hệ, địa chỉ, số điện thoại. Điều này là thông tin vô giá đối với cả tin tặc và điều tra viên. Nếu tội phạm đang tiến hành từ một máy chủ, thông tin này có thể giúp điều tra viên xác định được vị trí của chúng.

```

Domain Name..... chuckeasttom.com
Creation Date..... 2001-07-24
Registration Date.... 2001-07-24
Expiry Date..... 2011-07-24
Organisation Name.... Chuck Easttom
Organisation Address. 1845 W. Walntu Unit C
Organisation Address.
Organisation Address. Garland
Organisation Address. 75042
Organisation Address. TX
Organisation Address. UNITED STATES

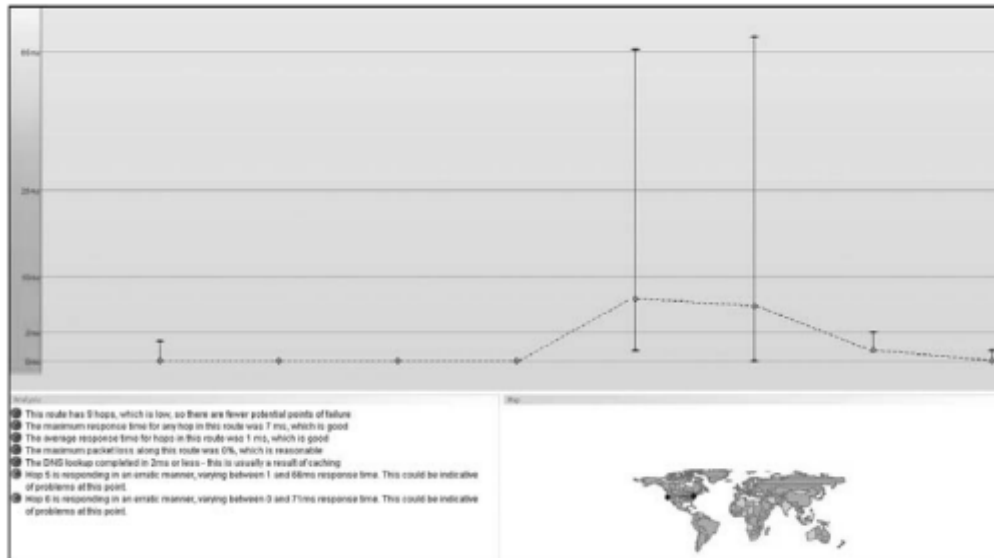
Admin Name..... Chuck Easttom
Admin Address..... 1845 W. Walntu Unit C
Admin Address.....
Admin Address..... Garland
Admin Address..... 75042
Admin Address..... TX
Admin Address..... UNITED STATES
Admin Email..... admin@chuckeasttom.com
Admin Phone..... 972-494-1747

```

Hình 3.19. Tìm kiếm giải pháp mạng với Whois

Truy tìm trở lại một địa chỉ IP là khá dễ dàng và có được nhiều thông tin. Tuy nhiên, có những công cụ khá rẻ mà ta có thể có được nhiều thông tin hơn. Một trong số đó là Visual Route (<http://www.VisualRoute.com>). Đây là một chương trình khá rẻ theo dõi địa chỉ IP và URL. Trong hình 3.19 là

những thông tin chi tiết mà Visual Route cung cấp mỗi bước nhảy từ vị trí nguồn đến đích. Visual Route cũng cung cấp thông tin rõ ràng như là nơi traffic mạng đang diễn ra.



Hình 3.20. Tìm kiếm với Visual Route

Bất kỳ phương pháp có thể giúp tìm hiểu thông tin về các địa chỉ IP nguồn. Điều quan trọng cần lưu ý đó là đó có thể là các gói tin gửi đến là giả mạo, có nghĩa là thay đổi để làm cho địa chỉ IP nguồn khác đi. Tuy nhiên trong nhiều trường hợp sẽ thấy IP nguồn thực sự. Bởi số lượng các hacker có tay nghề cao là rất nhỏ.

Quan tâm nhiều hơn so với vấn đề giả mạo IP đó là email ẩn danh. Có một số trang web mà sẽ cho phép gửi email và đặt nguồn địa chỉ email bất kỳ. Với loại này, vẫn có thể theo dõi địa chỉ IP của máy chủ email, nhưng hơi khó khăn. Các dịch vụ thường không lưu giữ bất cứ hồ sơ nào của khách truy cập vào trang web của họ, và có khả năng họ sẽ không có hồ sơ về người thực sự gửi email. Một số trang như sau :

- + <http://www.anonymizer.com/>
- + <http://anonymize.net/>
- + <http://www.publicproxyservers.com/>
- + <http://www.ultimate-anonymity.com/>
- + <http://www.mutemail.com/>

3.6.2 Chứng cứ từ Email

Có hai cách có thể giúp thu chứng cứ từ email. Đầu tiên là theo dõi nguồn gốc của một email được nhận. Thứ hai là thu thập email từ máy chủ email.

Đầu tiên ta xem xét việc theo dõi nguồn gốc email. Điều này có thể là một nhiệm vụ quan trọng và phổ biến trong các cuộc điều tra tội phạm máy tính. Khi giao dịch với tội phạm rình rập trên mạng, virus, hoặc khiêu dâm trẻ em, thường sẽ có email liên quan đến tội phạm và truy tìm chúng là một phần rất quan trọng trong quá trình điều tra. Nơi đầu tiên để tìm kiếm đó là tiêu đề các email. Tất cả các email có thông tin tiêu đề. Nếu đang sử dụng giao diện Yahoo! Email's Web, ví dụ trong các email cá nhân ở góc dưới bên phải có tùy chọn có nhãn tiêu đề (hình 3.21). Khi nhấn chuột vào đó, email sẽ hiển thị thông tin tiêu đề đầy đủ như hình 3.22. Có nhiều thông tin hữu ích trong đó. IP có nguồn gốc rất quan trọng, nó cho biết địa chỉ IP mà email đến từ đâu. Rất có thể đó là địa chỉ IP của máy chủ email của người đang sử dụng, máy tính cá nhân của họ. Có thể sử dụng tìm kiếm Whois như đã nói ở trên để theo dõi địa chỉ IP này.



Hình 3.21. Tìm tiêu đề Yahoo! E-mail



Hình 3.22. Xem thông tin đầy đủ tiêu đề Yahoo! E-mail full

Visual Route đã đề cập đến cũng là một sản phẩm gọi là eMailTrackerPro, cung cấp chức năng tương tự cho email. Sản phẩm gắn vào Outlook, như hình 3.23. Khi có bất kỳ email nào nổi bật, có thể nhấn vào nút eMailTrackerPro và truy xuất sẽ được thực hiện như hình 3.24.



Hình 3.23. eMailTrackerPro trong Outlook

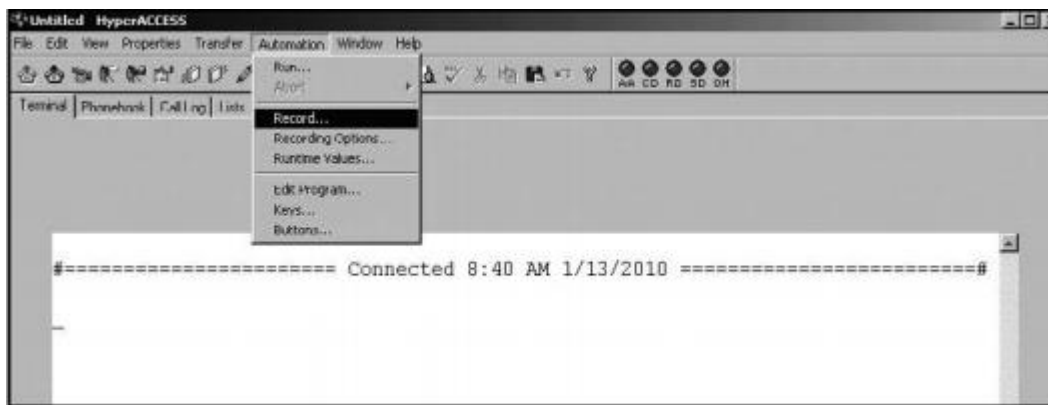


Hình 3.24. eMailTrackerPro trace

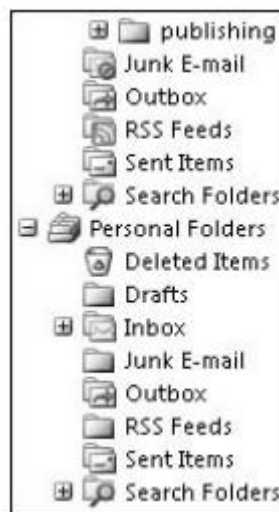
Như đã thấy, có thể theo dõi một địa chỉ IP, các công cụ như eMailTrackerpro đã làm cho quá trình truy tìm dễ dàng hơn và cung cấp những dữ liệu phong phú về địa chỉ email đang được theo dõi. Trong khi theo dõi email liên quan đến tội phạm hoặc tranh chấp dân sự, thì cách này không phải luôn luôn hiệu quả. Không mất nhiều khó khăn để thiết lập một Hotmail vô danh, Google hay tài khoản email Yahoo!. Tài khoản này rất khó theo dõi. Bây giờ nếu như có thể theo dõi các IP có nguồn gốc, sau đó yêu cầu nhà cung cấp cho biết cụ thể máy tính/ địa chỉ IP được sử dụng để gửi email.

Một điều rất quan trọng đó là không chỉ đơn giản dựa trên email thấy trong các mail client. Hầu hết các ứng dụng email cho phép người sử dụng lưu email vào một file. Thường là lưu lại email cũ. Tuy nhiên nó hoàn toàn có thể có email mà không thấy được. Ví như email trong Outlook được lưu trữ trong

tập tin có phần mở rộng .pst. Nếu tìm thấy file này trên máy, có thể mở bằng cách File>Open>Outlook Data file như hình 3.25. Và cuối cùng các file trong Outlook sẽ hiển thị như hình 3.26. Một thiết lập hoàn toàn mới của thư mục cá nhân có thể kiểm tra. Điều quan trọng là để tìm kiếm ổ đĩa cứng cho bất kỳ tập tin .pst và kiểm tra chúng. Một tên tội phạm thông minh có thể giữ một tập tin .pst riêng biệt mà chúng sử dụng hợp pháp. Ví dụ xem trong Outlook khi tìm kiếm một email khách hàng mà tìm thấy trong máy của kẻ tình nghi. Hầu hết ứng dụng email bao gồm cả Outlook và Eudora cho phép sao lưu email vào một file, cũng như khả năng mở và đọc các file trong máy khách.



Hình 3.25. Mở một file .pst



Hình 3.26. Xem e-mail

Cũng có thể thu thập chứng cứ từ máy chủ email. Một người có thể xóa email từ máy tính của họ nhưng trong nhiều trường hợp những email bị xóa ấy vẫn lưu trữ trên máy chủ email của cả bên gửi và bên nhận. Nhưng phải nhận thức được thời gian tính chất nhạy cảm của chứng cứ. Hầu hết các công

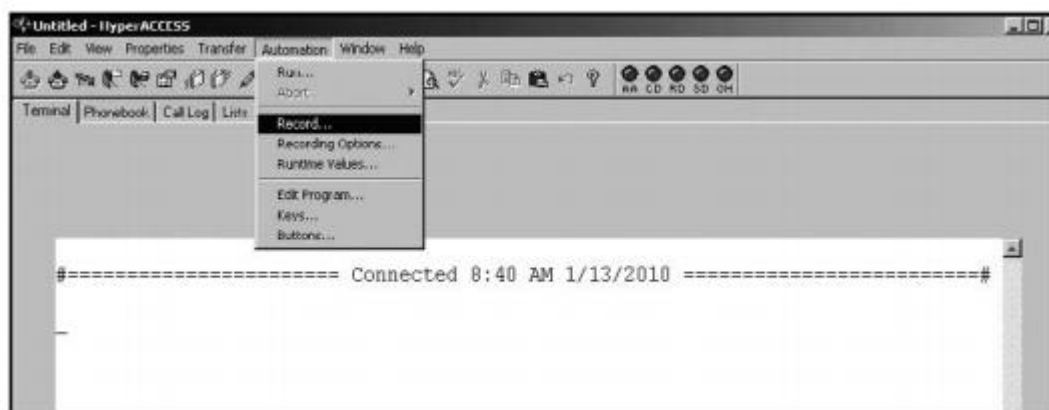
ty có chính sách xóa định kỳ thư điện tử trên máy chủ. Nếu không làm vậy thì ổ cứng email server sẽ bị đầy cứng.

Có được email từ máy chủ thì phải liên quan đến bên thứ ba, như là một nhà cung cấp dịch vụ Internet. Không thể đơn giản có được tất cả email vì hầu hết các email không liên quan đến vụ điều tra. Nó không chỉ là vi phạm quyền riêng tư cá nhân mà còn là một khối lượng công việc khá lớn cho điều tra viên.

3.6.3 Chứng cứ từ các thiết bị mạng

Tại một số thời điểm, tất cả các thông tin Internet đi qua các router, trong trường hợp tấn công lên mạng của một tổ chức, cuộc tấn công phải qua router của công ty. Vì vậy cần xem xét kiểm tra router để tìm chứng cứ. Hiện nay router Cisco là phổ biến nhất. Vấn đề đầu tiên cần xem xét đó là phân biệt giữa dữ liệu ổn định và dữ liệu không ổn định. Dữ liệu không ổn định là dữ liệu không được lưu trữ vĩnh viễn và sẽ bị mất đi khi tắt các nguồn điện từ các thiết bị. Trong các router Cisco, non-volatile RAM (NVRAM) là nơi lưu trữ của các bộ định tuyến. Tuy nhiên hiện nay dữ liệu không ổn định được lưu trữ trong bộ nhớ truy cập ngẫu nhiên (RAM).

Để lấy dữ liệu từ RAM và NVRAM, trước tiên phải thiết lập kết nối với router. Phương pháp tốt nhất là chỉ cần kết nối một cáp để một trong những đầu nối RJ-45 cắm trên router. Nếu không kết nối được trực tiếp, ta có thể truy cập từ xa đến các bộ định tuyến. Nếu truy cập từ xa đến các bộ định tuyến chắc chắn rằng bạn nên sử dụng SSH (Secure Shell); nó đã được mã hóa. Trong trường hợp này ta chỉ cần đăng nhập toàn bộ phiên với Hyper terminal. Hyper terminal là một công cụ phổ biến cho điều khiển từ xa kết nối với hệ thống và có sẵn cho nhiều hệ điều hành bao gồm cả Windows 7. Có thể có Hyper terminal tại: <http://www.hilgraeve.com/>. Có một phiên bản thử nghiệm có sẵn. Hyper terminal cho phép ta sử dụng SSH để bảo đảm kết nối. Khi sử dụng Hyper terminal, ta có thể chọn ghi lại bằng cách chọn ghi tự động như hình 3.27.



Hình 3.27. Ghi dữ liệu với Hyper Terminal

Router của Cisco có nhiều chế độ, chẳng hạn như đăng nhập nhanh, cho phép thiết lập ban đầu, cấu hình và giao diện. Hai chế độ chính đó là chế độ người dùng và cho phép chế độ đặc quyền. Để truy cập vào chế độ đặc quyền, mật khẩu phải được biết đến bởi nhà phân tích. Cần lưu ý rằng một cách khác mà hacker cố gắng xâm nhập vào một hệ thống đó là cố gắng truy cập từ xa đăng nhập vào router/ gateway sử dụng một công cụ như Hyper Terminal. Nó luôn là cách tốt nhất để cấu hình bộ định tuyến để yêu cầu một mật khẩu, và nếu nó khả thi chỉ cho phép kết nối trực tiếp, không kết nối từ xa.

Khi kết nối với các bộ định tuyến, muốn ghi lại thời gian. Ghi thời gian sẽ là bước quan trọng sau khi tham khảo dữ liệu trong một vụ điều tra. Có thể sử dụng tiện ích dòng lệnh chương trình đồng hồ để hiển thị đồng hồ và thời gian. Có lệnh router khác nhập vào dòng lệnh có thể sẽ giúp :

- Lệnh show version: Cung cấp thông tin phần cứng, phần mềm của router. Nó sẽ hiển thị các nền tảng, phiên bản hệ điều hành, tập tin ảnh hệ thống, bất kỳ giao diện, số lượng RAM router có và bao nhiêu mạng, giao diện có.
- Lệnh show running-config : Cấu hình đang thực hiện.
- Lệnh show startup-config : Cấu hình khởi động của hệ thống. Sự khác nhau của 2 lệnh trên có thể là dấu hiệu của một hacker đã cố tình thay đổi hệ thống.
- Các lệnh show ip route: Hiển thị bảng định tuyến. Là thao tác mà tin tặc có thể thâm nhập vào.

Đây chỉ là một vài lệnh router quan trọng có thể cung cấp cho ta những thông tin giá trị. Nếu router không phải của hãng Cisco, sẽ có sự khác biệt. Điều này cho thấy nếu muốn trở thành một nhà điều tra tội phạm máy tính đòi hỏi kỹ năng khá rộng. Cần phải thành thạo các hệ điều hành, mạng lưới hoạt động và các bộ định tuyến. Vì vậy cần học hỏi mở rộng kỹ năng. Nếu như nó thuộc ngoài chuyên môn thì cần thiết phải gặp chuyên gia tư vấn để hỗ trợ.

3.6.4 Chứng cứ từ điện thoại di động

Điều tra thiết bị di động là một nhánh của khoa học điều tra số liên quan đến việc thu hồi bằng chứng kỹ thuật số hoặc dữ liệu từ các thiết bị di động. Thiết bị di động ở đây không chỉ đề cập đến điện thoại di động mà còn là bất kỳ thiết bị kỹ thuật số nào có bộ nhớ trong và khả năng giao tiếp, bao gồm các thiết bị PDA, GPS và máy tính bảng.

Việc sử dụng điện thoại với mục đích phạm tội đã phát triển rộng rãi trong những năm gần đây, nhưng các nghiên cứu điều tra về thiết bị di động là một lĩnh vực tương đối mới, có niên đại từ những năm 2000. Sự gia tăng các loại hình điện thoại di động trên thị trường (đặc biệt là điện thoại thông minh) đòi hỏi nhu cầu giám định các thiết bị này mà không thể đáp ứng bằng các kỹ thuật điều tra máy tính hiện tại.

Chứng cứ từ các thiết bị di động rất hữu ích trong việc xác nhận vị trí của tội phạm thông qua hệ thống định vị GPS, cũng như việc khôi phục các tin nhắn trao đổi của tội phạm, khi chúng sử dụng thiết bị di động để liên lạc với nhau, ngày nay khi công nghệ thông tin phát triển, thì việc điều tra thiết bị di động đang trở nên cần thiết và cần đội ngũ có chuyên môn cao, trong điều tra tội phạm công nghệ cao.

Hiện nay điện thoại rất phổ biến và không ngạc nhiên khi điện thoại di động có thể đóng vai trò giúp tội phạm máy tính. Thậm chí có một số tội phạm thực hiện hành vi chủ yếu thông qua điện thoại di động. Ví dụ như gửi hình ảnh khiêu dâm qua điện thoại di động. Một số loại dữ liệu có thể được lấy ra làm bằng chứng liên quan đến điện thoại di động bao gồm :

- + Hình ảnh.
- + Video.
- + Tin nhắn văn bản hoặc tin SMS.

- + Thời gian gọi, cuộc gọi đã nhận, cuộc gọi nhỡ và thời gian cuộc gọi.
- + Tên danh bạ và các số điện thoại.

Rõ ràng hình ảnh, video hay tin nhắn có thể chứa chứng cứ phạm tội.

Có một vài quy tắc, luật chung cần lưu ý khi điều tra :

- Luôn ghi lại nơi sản xuất, model, và bất kỳ chi tiết nào về tình trạng điện thoại.
- Chụp lại hình ảnh ban đầu của điện thoại.
- Xem xét thẻ sim của điện thoại.

3.6.5 Chứng cứ từ tường lửa

Bất kỳ cuộc tấn công có nguồn gốc từ bên ngoài mạng đều phải đi qua tường lửa. Thông thường, để qua được tường lửa cần phải quét cổng và lắng nghe sau đó thực hiện hành vi vi phạm. Hầu hết tường lửa có cơ chế ghi nhật ký tất cả các thông tin nó kiểm tra. Vì vậy bằng cách kiểm tra ghi nhận của tường lửa là sẽ có thể có được bằng chứng có giá trị.

Tường lửa thường phân làm ba nhóm chính: các vấn đề về hệ thống quan trọng, hành động quản trị và các kết nối mạng. Các vấn đề hệ thống quan trọng bao gồm các lỗi phần cứng. Hành động quản trị bao gồm việc thêm người dùng, cho phép thay đổi, và những công việc liên quan. Nhật ký kết nối mạng là các nhật ký ghi lại kết nối thành công hay thất bại.

Mỗi loại nhật ký sẽ cung cấp một thông tin giá trị. Rõ ràng, việc cố gắng kết nối là bước đầu tiên của cuộc tấn công và trong thực tế là một phần của cuộc tấn công. Hành động của quản trị cũng có thể là một phần của tấn công, một kẻ xâm nhập có thể thực hiện công việc của quản trị để tạo ra một cửa hậu (backdoor) mà chúng thuê hệ thống để có thể truy cập vào tài nguyên trên mạng. Và tất nhiên một số lỗi của một thiết bị có thể là do tội phạm máy tính gây ra. Tất cả các phần này phải được điều tra trong tường lửa. Hình dưới đây là một ví dụ của nhật ký tường lửa checkpoint ghi lại các truy cập vào hệ thống

```
"Date","Time","Action","FW.Name","Direction","Source","Destination","Bytes","Rules","Protocol"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.67.8.235","dst=139.203.160.214","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=210.22.4.200","dst=139.203.133.42","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=200.211.147.23","dst=139.203.18.177","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.184.77.8","dst=139.203.141.128","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=61.129.122.129","dst=139.203.250.160","bytes=64","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=61.142.57.208","dst=139.203.67.133","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=206.247.102.9","dst=139.203.111.23","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=211.75.239.157","dst=139.203.152.208","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=209.165.171.246","dst=139.203.73.178","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:02","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=64.70.1.57","dst=139.203.241.128","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:03","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=61.138.33.102","dst=139.203.13.45","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:03","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.142.143.60","dst=139.203.131.222","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:03","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.184.155.183","dst=139.203.143.53","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:03","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.44.116.240","dst=139.203.241.7","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:03","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=61.141.206.1","dst=139.203.43.222","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:03","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.111.50.220","dst=139.203.31.197","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:04","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=194.244.77.147","dst=139.203.212.209","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:04","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.139.67.57","dst=139.203.219.68","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:04","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=139.142.136.156","dst=139.203.111.30","bytes=48","rule=29","proto=tcp/http"
"datetime=26Aug2013","20:26:04","action=drop","fw_name=NFL-cp.NFL.gov","dir=inbound","src=64.171.190.52","dst=139.203.15.41","bytes=48","rule=29","proto=tcp/http"
```

Hình 3.28. Nhật ký tường lửa CheckPoint

Chứng cứ này sẽ rất hữu ích trong việc phân tích điều tra mạng. Từ nhật ký ghi lại được ta sử dụng công cụ Texpipe pro xuất ra định dạng sau để dễ quan sát

08/26/2013	20:26:02	drop	NFL-cp.NFL.gov	inbound	61.142.57.208	139.203.67.133	48	29	HTTP
08/26/2013	20:26:02	drop	NFL-cp.NFL.gov	inbound	206.247.102.9	139.203.111.23	48	29	HTTP
08/26/2013	20:26:02	drop	NFL-cp.NFL.gov	inbound	211.75.239.157	139.203.152.208	48	29	HTTP
08/26/2013	20:26:02	drop	NFL-cp.NFL.gov	inbound	209.165.171.246	139.203.73.178	48	29	HTTP
08/26/2013	20:26:02	drop	NFL-cp.NFL.gov	inbound	64.70.1.57	139.203.241.128	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	61.138.33.102	139.203.13.45	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.142.143.60	139.203.131.222	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.184.155.183	139.203.143.53	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.7	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.7	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.8	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.9	48	29	HTTP
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.10	48	29	HTTP
08/26/2013	20:26:03	accept	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.11	48	29	TELNET
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.7	48	29	TELNET
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.7	48	29	TELNET
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.8	48	29	TELNET
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.9	48	29	TELNET
08/26/2013	20:26:03	drop	NFL-cp.NFL.gov	inbound	139.44.116.240	139.203.241.10	48	29	TELNET

Hình 3.29. Phân tích nhật ký tường lửa

Từ hình trên ta có thể xác định được gói tin nào được cho phép, gói tin nào bị drop, và cũng như địa chỉ ip xuất phát của gói tin đó... Chi tiết về việc phân tích hệ thống tường lửa sẽ được trình bày rõ hơn ở phần sau.

Ở trên chúng ta cũng mới chỉ xét đến việc hệ thống tường lửa ghi lại nhật ký các truy cập đi qua nó, nhưng khi phân tích điều tra một hệ thống tường lửa, chúng ta không chỉ căn cứ vào mỗi nhật ký ứng dụng, chúng ta cần

xem xét xem hệ thống tường lửa liệu đã bị thỏa hiệp bởi kẻ tấn công hay chưa, nếu như hệ thống tường lửa đã bị thỏa hiệp thì hướng điều tra chúng ta cũng phải cố gắng xác định phương thức mà kẻ tấn công đã sử dụng để thỏa hiệp đó, việc này có thể thực hiện bằng cách ghi lại bộ nhớ RAM, xem xét lại các ứng dụng, giao thức đang được sử dụng cũng như cấu hình của hệ thống. Từ đó quan sát và điều tra xác định nguyên nhân bị thỏa hiệp.

3.6.6 Chứng cứ từ hệ thống phát hiện xâm nhập

Hệ thống phát hiện xâm nhập là điểm kiểm soát truy cập, làm nhiệm vụ phát hiện các tấn công tới hệ thống dựa trên việc phân tích hành vi hoặc dựa trên các mẫu có sẵn. Ví dụ, một hệ thống phát hiện xâm nhập sẽ lưu ý một người nào đó đang tiến hành dò quét gói tin trên mạng và cảnh báo cho người quản trị. Tất nhiên, không phải tất cả các mạng sử dụng một hệ thống phát hiện xâm nhập, nhưng nếu mạng đang điều tra có thì sau đó phải kiểm tra các bản ghi của hệ thống. Cũng giống như tường lửa, hệ thống phát hiện xâm nhập có những bản ghi ghi lại bất kỳ sự kiện nào xảy ra. Hành vi vi phạm an ninh mạng sẽ để lại những dấu hiệu trong các bản ghi của hệ thống phát hiện xâm nhập.

Ta có thể nhận được thông tin từ email khách hàng, thiết bị định tuyến, điện thoại di động, và bất kỳ thiết bị có thể lưu trữ dữ liệu. Các nguồn thông tin này có thể là một kho tàng bằng chứng. Tuy nhiên cần chú ý rằng phải lưu lại, chứng minh được từng bước trong quá trình điều tra. Nếu sử dụng phần mềm hay tiện ích để phục hồi các file bị xóa thì phải chứng minh được những gì mà phần mềm hay tiện ích đó đã sử dụng. Ngoài ra, không nên bỏ sót bất kỳ thông tin nào, nên xem các bộ định tuyến và điện thoại di động bởi chúng cũng có thể là những chứng cứ rất quan trọng. Bất kỳ thiết bị thủ phạm có thể sử dụng để truyền dữ liệu, hoặc nạn nhân có thể kết nối với, đều có khả năng là chứng cứ quan trọng. Dưới đây là ví dụ về chứng cứ thu được từ Snort:

```

Sep 1 10:38:36 10.10.10.1 615: *Sep 1 17:36:34.307: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 616: *Sep 1 17:36:34.531: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 617: *Sep 1 17:36:34.531: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 618: *Sep 1 17:36:34.783: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 619: *Sep 1 17:36:34.783: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 620: *Sep 1 17:36:35.087: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 621: *Sep 1 17:36:35.087: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:36 10.10.10.1 622: *Sep 1 17:36:35.495: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:37 10.10.10.1 623: *Sep 1 17:36:35.495: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:37 10.10.10.1 624: *Sep 1 17:36:36.111: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:37 10.10.10.1 625: *Sep 1 17:36:36.111: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:39 10.10.10.1 626: *Sep 1 17:36:37.047: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:39 10.10.10.1 627: *Sep 1 17:36:37.047: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:41 10.10.10.1 628: *Sep 1 17:36:38.719: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:41 10.10.10.1 629: *Sep 1 17:36:38.719: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:59633 -> 10.10.10.10:80]
Sep 1 10:38:49 10.10.10.1 630: *Sep 1 17:36:46.715: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:52032 -> 10.10.10.10:80]
Sep 1 10:38:50 10.10.10.1 631: *Sep 1 17:36:48.199: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:54000 -> 10.10.10.10:80]
Sep 1 10:38:58 10.10.10.1 632: *Sep 1 17:36:55.827: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:63596 -> 10.10.10.10:4444]
Sep 1 10:38:58 10.10.10.1 633: *Sep 1 17:36:55.827: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:49486 -> 10.10.10.10:80]
Sep 1 10:38:58 10.10.10.1 634: *Sep 1 17:36:55.831: $IPS-4-SIGNATURE: Sig:5123 Subsig:2 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:49486 -> 10.10.10.10:80]
Sep 1 10:38:59 10.10.10.1 635: *Sep 1 17:36:56.831: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:59499 -> 10.10.10.10:4444]
Sep 1 10:38:59 10.10.10.1 636: *Sep 1 17:36:56.883: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:56017 -> 10.10.10.10:4444]
Sep 1 10:39:29 10.10.10.1 647: *Sep 1 17:37:28.027: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:60915 -> 10.10.10.10:80]
Sep 1 10:39:29 10.10.10.1 648: *Sep 1 17:37:28.031: $IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:29 10.10.10.1 649: *Sep 1 17:37:28.035: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:29 10.10.10.1 650: *Sep 1 17:37:28.259: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:30 10.10.10.1 651: *Sep 1 17:37:28.511: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:30 10.10.10.1 652: *Sep 1 17:37:28.511: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:30 10.10.10.1 653: *Sep 1 17:37:28.815: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:30 10.10.10.1 654: *Sep 1 17:37:28.815: $IPS-4-SIGNATURE: Sig:5769 Subsig:0 Sev:4 Malformed HTTP Request [192.168.100.11:54068 -> 10.10.10.10:80]
Sep 1 10:39:30 10.10.10.1 655: *Sep 1 17:37:29.223: $IPS-4-SIGNATURE: Sig:5123 Subsig:0 Sev:5 WWW IIS Internet Printing Overflow [192.168.100.11:54068 -> 10.10.10.10:80]

```

Hình 3.30. Nhật ký thu được từ Snort

Hệ thống phát hiện xâm nhập, phát hiện dựa vào dấu hiệu, hoặc là sự lạm dụng, những hành vi bất thường đang diễn ra trên hệ thống, ở hình trên chúng ta thấy nhật ký snort ghi lại tấn công “www iis internet printing overflow”. Snort phát hiện ra tấn công dựa vào dấu hiệu của kỹ thuật tấn công này, trong điều tra mạng việc phân tích nhật ký rất quan trọng, những chứng cứ đặc biệt từ hệ thống phát hiện xâm nhập giúp chúng ta có cái nhìn tổng quan hơn về những mối đe dọa từ các cuộc tấn công đã và có thể đang diễn ra trên hệ thống của mình.

Hệ thống phát hiện xâm nhập cũng giống như hệ thống tường lửa, chúng ta cũng cần xem xét nó đã bị thỏa hiệp hay chưa, chứ không chỉ chú tâm vào ứng dụng mà nó được sử dụng để có cái nhìn bao quát hơn khi điều tra.

BÀI TẬP

1. Thu thập và phân tích chứng cứ từ các file nhật ký

Mục tiêu:

Hiểu về phương pháp, quy trình thu thập thông tin từ các file nhật ký và phân tích để điều tra tội phạm máy tính.

Nội dung thực hiện:

- + Thu thập và phân tích thông tin từ nhật ký hệ điều hành Windows
- + Thu thập và phân tích thông tin từ nhật ký hệ điều hành Linux
- + Thu thập và phân tích thông tin từ nhật ký WebServer

2. Thu thập và phân tích gói tin qua mạng

Mục tiêu:

Hiểu về cách thức thu thập các gói tin qua mạng và có thể phân tích để tìm ra dấu hiệu tấn công, kẻ tấn công.

Nội dung thực hiện:

- + Cài đặt công cụ phân tích gói tin Wireshark
- + Sử dụng Wireshark thu thập và phân tích gói tin qua mạng
- + Thực hiện thu thập và phân tích gói tin về một số kiểu tấn công điển hình.

3. Thu thập và phân tích nhật ký từ hệ thống tập tin

Mục tiêu:

Hiểu về phương pháp, quy trình thực hiện thu thập và phân tích chứng cứ từ hệ thống tập tin FAT và NTFS để điều tra dữ liệu trên các tập tin và điều tra tội phạm máy tính.

Nội dung thực hiện:

- + Thu thập dữ liệu từ hệ thống tập tin FAT
- + Thu thập dữ liệu từ hệ thống tập tin NTFS
- + Tìm kiếm và phân tích từ các dữ liệu đã thu thập để điều tra tính toàn vẹn của dữ liệu và các dấu hiệu xâm nhập.

4. Thu thập và phân tích nhật ký từ hệ thống tường lửa

Mục tiêu:

Hiểu về phương pháp, quy trình thực hiện thu thập và phân tích chứng cứ từ tường lửa để thực hiện điều tra tội phạm máy tính

Nội dung thực hiện:

- + Thu thập và phân tích nhật ký từ tường lửa CheckPoint
- + Thu thập và phân tích nhật ký từ tường lửa Cisco

5. Thu thập và phân tích nhật ký từ hệ thống IDS/IPS

Mục tiêu:

Hiểu về phương pháp, quy trình thực hiện thu thập và phân tích chứng cứ từ hệ thống IDS/IPS để thực hiện điều tra tội phạm máy tính

Nội dung thực hiện:

- + Thu thập và phân tích nhật ký từ Snort IDS
- + Thu thập và phân tích nhật ký từ Cisco IPS

Chương 4

PHÒNG CHỐNG TỘI PHẠM MÁY TÍNH

Tội phạm máy tính gây cho chúng ta những lo ngại về sự mất an toàn của hệ thống. Với sự phát triển như hiện nay, tội phạm máy tính chỉ cần sử dụng một số công cụ và kỹ thuật đơn giản cũng hoàn toàn có thể thực hiện tấn công và vi phạm an ninh của hệ thống. Do vậy, để bảo vệ an toàn cho hệ thống, một mặt chúng ta cần tăng cường các biện pháp an ninh; mặt khác cần phải kiện toàn về luật pháp và giáo dục để nâng cao ý thức người sử dụng để giúp cho việc ngăn chặn tội phạm máy tính. Trong chương này chúng ta sẽ đề cập tới một số biện pháp kỹ thuật, công nghệ và các biện pháp khác nhằm chống lại tội phạm máy tính và nâng cao độ an toàn của hệ thống.

4.1 SỬ DỤNG KỸ THUẬT, CÔNG NGHỆ

Có rất nhiều các giải pháp về kỹ thuật có thể áp dụng để phòng chống tội phạm máy tính. Các giải pháp phổ biến hiện nay là sử dụng tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập, phòng chống mã độc hại, sử dụng các biện pháp mã hóa, Dưới đây chúng ta sẽ tìm hiểu cụ thể về các giải pháp này.

4.1.1 Tường lửa

Tường lửa là một cơ chế để ngăn cách bảo vệ mạng tin cậy (trusted network) khỏi các mạng không tin cậy (untrusted network). Tường lửa như một trạm kiểm soát ở các điểm nối giữa các vùng, làm nhiệm vụ kiểm tra và quyết định luồng dữ liệu mạng có được đi qua hay không .

Tường lửa thường là trạm kiểm soát đầu tiên tiếp nhận luồng dữ liệu từ Internet để thực hiện xác định cho phép hay không cho phép một gói tin được

đi vào hoặc đi ra. Giống như một nhân viên an ninh, đứng ở cửa tòa nhà, xác định cho phép hay không việc đi vào và đi ra tòa nhà đó. Nhờ đó, tường lửa giúp hạn chế khá nhiều các thông tin không được phép đi vào hệ thống mạng, gây ảnh hưởng tới hệ thống và ngăn chặn được nhiều các tấn công xâm nhập hệ thống, đặc biệt là tấn công từ chối dịch vụ.

Một tường lửa có thể hoạt động trên nhiều lớp khác nhau của mạng, từ lớp cao nhất là lớp ứng dụng cho đến lớp datalink (địa chỉ MAC). Phần lớn các tường lửa hoạt động trên lớp mạng và lớp giao vận. Chúng kiểm tra gói tin TCP/IP, sau đó ra quyết định dựa trên các thông tin trong gói tin đó như địa chỉ nguồn, địa chỉ đích, cổng nguồn, cổng đích hoặc tổ hợp của hai hay nhiều thông tin trên. Các tường lửa hoạt động trên lớp ứng dụng có thể kiểm soát theo nội dung, theo các từ khoá hoặc kiểm tra virus. Các tường lửa có nhiều loại khác nhau (hoạt động trên lớp mạng, lớp ứng dụng,...) nhưng chúng đều có chung đặc điểm trong nguyên tắc hoạt động: Tóm bắt dữ liệu, kiểm tra rồi quyết định cho đi qua, thay đổi thông tin (chỉnh sửa lại thông tin header,...) hay cấm. Một số tường lửa phức tạp hơn còn có khả năng yêu cầu xác thực (dưới dạng tên và mật khẩu hoặc theo dạng xác thực thẻ) trước khi cho phép truy cập. Tính năng này tương đối quan trọng vì việc kiểm soát theo địa chỉ IP trong nhiều trường hợp không đủ chặt chẽ. Người dùng dễ dàng đổi địa chỉ IP máy sang địa chỉ IP “tin cậy” và có đầy đủ các quyền truy cập của IP “tin cậy” này.

Tường lửa được chia làm 2 loại: tường lửa cứng và tường lửa mềm. Tường lửa cứng là loại tường lửa đi kèm theo một thiết bị phần cứng, thường được đặt tại ranh giới các vùng mạng để kiểm soát các thông tin đi qua mạng, hay còn gọi là tường lửa mạng. Tường lửa mềm là một chương trình phần mềm, được cài đặt trên một hệ thống phần cứng. Tường lửa cá nhân là một trong các loại tường lửa mềm.

Xét về công nghệ, thông thường hiện nay tường lửa được chia làm 3 công nghệ chính:

- + Tường lửa lọc gói tin (Packet filter Firewall)
- + Tường lửa ứng dụng (Application level Gateway hay Proxy server)
- + Tường lửa kiểm soát trạng thái (Stateful Inspection Firewall)

Tường lửa hoạt động dựa trên việc kiểm tra các gói tin thông qua bảng tập luật. Các luật được kiểm tra theo thứ tự từ trên xuống. Khi một gói tin phù hợp với một luật trong bảng tập luật, gói tin sẽ được xử lý theo các hành động được quy định: đi qua hoặc bị chặn lại tại tường lửa. Nếu trong bảng tập luật có các luật trùng nhau khi xử lý cùng một gói tin, thì luật ở trên sẽ được áp dụng và các luật phía dưới sẽ bị bỏ qua. Thông thường luật mặc định cuối cùng của tường lửa là từ chối tất cả các gói tin đi qua.

Tường lửa là trạm kiểm soát đầu tiên, do vậy cũng là nơi hứng chịu nhiều các nguy hại đến từ những kẻ tấn công có ý định xâm nhập vào hệ thống. Chính vì thế, để có thể kiểm soát tốt các kết nối vào ra, và tránh được các tấn công ảnh hưởng đến tường lửa thì việc đầu tiên là cần bảo vệ an toàn cho chính tường lửa. Các nguy hại không chỉ xảy đến từ bên ngoài mạng, mà chính những kết nối từ bên trong vùng được bảo vệ cũng có thể ảnh hưởng tới tường lửa. Giám sát các kết nối từ bên trong cũng như bên ngoài là hết sức cần thiết giúp bảo vệ tường lửa một cách chặt chẽ nhất. Ngoài ra, tường lửa được cấu hình đúng cũng lưu lại các hoạt động trong mạng. Những bản ghi này có thể là bằng chứng có giá trị trong việc truy tố những người tấn công bất hợp pháp vào hệ thống của chúng ta.

4.1.2 Hệ thống IDS/IPS

Giải pháp thứ 2 để phòng chống tội phạm máy tính chính là hệ thống phát hiện và ngăn chặn xâm nhập IDS/IPS.

Phát hiện xâm nhập (Intrusion Detection) là quá trình giám sát các sự kiện xảy ra trong một hệ thống máy tính hoặc mạng và phân tích chúng để tìm ra các dấu hiệu của những rắc rối tiềm ẩn. Các dấu hiệu này được định nghĩa là sự vi phạm hoặc cố tình vượt qua các chính sách an ninh của máy tính, mạng. Các dấu hiệu xâm nhập có thể bị gây ra bởi nhiều nguyên nhân như sâu mạng, phần mềm gián điệp, kẻ tấn công đang cố gắng chiếm đoạt quyền truy cập hợp pháp vào máy tính từ Internet, người sử dụng hợp lệ có các hành vi vượt qua các đặc quyền truy cập được định trước hoặc lạm dụng đặc quyền của họ.

Phòng chống xâm nhập (Intrusion Prevention) là hành vi của hệ thống tự động ngăn chặn các xâm nhập trái phép, có khả năng gây hại cho hệ thống.

Một hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) là phần mềm hoặc thiết bị chuyên dụng làm nhiệm vụ tự động thực hiện các hành động phát hiện xâm nhập.

Một hệ thống ngăn chặn xâm nhập (Intrusion Prevention System - IPS) là phần mềm hoặc một thiết bị chuyên dụng có khả năng phát hiện xâm nhập và có thể ngăn chặn các nguy cơ gây mất an ninh.

Các dấu hiệu của hành vi xâm nhập trái phép được định nghĩa là việc thực hiện các hành động bất hợp pháp hoặc vượt qua những cơ chế bảo mật của máy tính hay của mạng. Các vụ xâm nhập có thể là do kẻ tấn công truy cập vào hệ thống từ Internet, do những người dùng hợp pháp của hệ thống muốn đạt được sự truy cập vào các đặc quyền mà họ không được phép, và do những người dùng hợp pháp lạm dụng đặc quyền của họ. Các hệ thống phát hiện xâm nhập là các sản phẩm phần cứng hoặc phần mềm trợ giúp quá trình giám sát và phân tích xâm nhập.

Nhiệm vụ chính của các hệ thống phát hiện và ngăn chặn xâm nhập là phòng chống cho một hệ thống máy tính bằng cách phát hiện các dấu hiệu tấn công và có thể đẩy lùi nó. Việc phát hiện các tấn công phụ thuộc vào số lượng và kiểu hành động thích hợp. Để ngăn chặn xâm nhập tốt cần phải kết hợp tốt giữa “bả và bẫy” được trang bị cho việc nghiên cứu các mối đe dọa. Việc làm lệch hướng sự tập trung của kẻ xâm nhập vào tài nguyên được bảo vệ là một nhiệm vụ quan trọng khác. Cả hệ thống thực và hệ thống bẫy cần phải được kiểm tra một cách liên tục. Dữ liệu được tạo ra bằng các hệ thống phát hiện xâm nhập được kiểm tra một cách cẩn thận (đây là nhiệm vụ chính cho mỗi IDS) để phát hiện các dấu hiệu tấn công.

Hệ thống phát hiện xâm nhập là những chương trình hay thiết bị thực hiện việc tìm kiếm dấu hiệu của một xâm nhập bất hợp pháp. Ví dụ, một IDS/IPS có thể nhận thấy rằng một máy quét cổng đang xảy ra hoặc cho rằng ai đó đang cố gắng để đăng nhập vào với việc sử dụng tấn công SQL Injection. Hệ thống phát hiện xâm nhập sau đó có thể cảnh báo người quản trị về các hành vi truy cập vi phạm an ninh hệ thống và lưu lại chi tiết của các sự kiện như địa chỉ IP nguồn. Điều này có thể không chỉ cho phép chúng ta ngăn chặn các cuộc tấn công, mà còn cung cấp bằng chứng để truy tố sau.

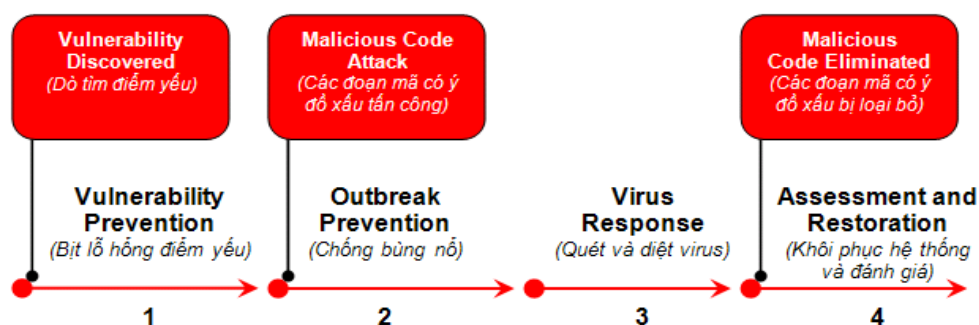
Có rất nhiều loại hệ thống phát hiện và ngăn chặn xâm nhập khác nhau, mỗi hệ thống có mức độ khác nhau về hiệu quả. Tuy nhiên không thể phủ nhận việc trang bị hệ thống IDS/IPS sẽ giúp tăng cường, cải thiện an ninh và chống được đáng kể các tấn công không đáng có ảnh hưởng tới hệ thống mạng. Ngoài ra, các bản ghi của một IDS/IPS, giống như các bản ghi tường lửa, có thể cung cấp bằng chứng có giá trị trong việc điều tra và truy tố bất kỳ tội phạm máy tính nào.

4.1.3 Ngăn chặn mã độc hại

Internet là nơi vô cùng hữu ích cho mọi người truy xuất thông tin, hoặc thực hiện các giao dịch điện tử giữa các vùng cách xa nhau về địa lý. Tuy nhiên Internet lại là nơi mà các tội phạm và tin tặc trực tuyến luôn rình rập để gây rắc rối, đánh cắp các thông tin nhạy cảm của chúng ta. Một cách mà các tội phạm thường sử dụng đó là lây nhiễm và phát tán phần mềm độc hại. Chính vì thế, một giải pháp nữa cần được áp dụng để phòng chống tội phạm máy tính là ngăn chặn mã độc hại, ngăn chặn các nguy cơ lây lan của mã độc.

Mã độc hại được định nghĩa là “một chương trình được chèn một cách bí mật vào hệ thống với mục đích làm tổn hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống”. Định nghĩa này sẽ bao hàm rất nhiều thể loại mà chúng ta vẫn quen gọi chung là virus máy tính ở Việt nam như: worm, trojan, spy-ware, ... thậm chí là virus hoặc các bộ công cụ để tấn công hệ thống mà các hacker thường sử dụng như: backdoor, rootkit, key-logger, ...

Để thực hiện ngăn chặn mã độc hại, cần phải thực hiện theo 4 giai đoạn như sau:



Hình 4.1. Mô hình phòng chống mã độc hại

- + Giai đoạn 1: Là giai đoạn phòng vệ trên các lỗ hổng, điểm yếu của hệ thống mà virus cũng như các đoạn mã chương trình có ý đồ xấu có thể lợi dụng để tấn công vào hệ thống.
- + Giai đoạn 2: Là giai đoạn phòng và chống virus bùng nổ trong hệ thống
- + Giai đoạn 3: Là giai đoạn quét và diệt virus đã lây nhiễm trong hệ thống
- + Giai đoạn 4: Là giai đoạn khôi phục sửa chữa những phần hệ thống đã bị virus làm hỏng. Khôi phục lại cho hệ thống hoạt động trở lại bình thường. Và đánh giá về mức độ thiệt hại cũng như đánh giá rút ra kinh nghiệm về việc phòng chống virus vừa qua

Muốn bịt được lỗ hổng, điểm yếu của hệ thống thì cần phải có công cụ để kiểm soát, tìm xem trong hệ thống có những lỗ hổng điểm yếu nào đang tồn tại, phân loại các lỗ hổng điểm yếu nào là rất nguy hiểm có nguy cơ bị lợi dụng tấn công rất cao, loại nào bình thường, loại nào nguy cơ thấp. Cần phải có hệ thống cập nhật tập trung các miếng vá của Microsoft. Ngoài ra cần có công cụ để kiểm tra duy trì việc thực hiện các công việc trên, nói rộng ra là cần có công cụ để giám sát việc thực hiện việc thực hiện chính sách phòng chống mã độc hại.

Các mã độc hại thế hệ mới có tốc độ lây lan rất nhanh chỉ cần không đầy một giờ đồng hồ đã có thể lây lan, tràn ngập (hay còn gọi là bùng nổ) trong 1 mạng LAN, gây nghẽn, tê liệt hệ thống mạng và máy tính. Mã độc hại vẫn có thể gây bùng nổ với xác suất rất cao nếu hệ thống mạng đã có trang bị hệ thống phòng chống mã độc hại nhưng không có công cụ để phòng chống virus bùng nổ. Vì các sản phẩm phòng chống mã độc hại thông thường đều nhận dạng và diệt theo mẫu (được hãng cung cấp sản phẩm phát hành, và các khách hàng phải cập nhật cho hệ thống của mình) nhưng thời gian để các hãng cung cấp sản phẩm tìm ra và phát hành được mẫu mã độc hại thường không kịp để ngăn chặn virus bùng nổ. Vì thế hệ thống phòng chống mã độc hại cần được trang bị các công cụ nhằm ngăn chặn bùng nổ nhằm triển khai đồng loạt các chính sách chống bùng nổ xuống từng end-points.

Tiếp theo, hệ thống cần được trang bị các giải pháp đồng bộ nhằm ngăn chặn tất cả các con đường lây nhiễm và phát tán mã độc hại:

- +Để ngăn chặn các tấn công ở lớp mạng (network service worm), cần có thiết bị chuyên dụng có khả năng dò quét, phát hiện và ngăn chặn các tấn công.
- +Cần có giải pháp bảo vệ tại cổng kết nối internet nhằm ngăn chặn mã độc hại ngay tại gateway(kiểm soát các giao thức kết nối internet như: HTTP, HTTPS, SMTP, POP3)
- +Cần có giải pháp ngăn chặn mã độc hại phát tán qua email
- +Giải pháp ngăn chặn mã độc hại trên các end-point

Cuối cùng, giải pháp bảo vệ end-points cần có chức năng có khả năng làm sạch các rác do worm, trojan, spyware để lại trong hệ thống, giúp khôi phục sửa chữa các file hệ thống và registry của hệ thống đã bị virus làm hỏng.

Để thực hiện được 4 giai đoạn phòng chống mã độc hại như trên, ngoài các sản phẩm thì còn có một phần không thể thiếu và giữ vai trò rất quan trọng trong giải pháp phòng chống mã độc toàn diện đó là các dịch vụ hỗ trợ kỹ thuật. Các dịch vụ hỗ trợ kỹ thuật sẽ cung cấp cho khách hàng các kinh nghiệm, kỹ thuật của các chuyên gia phòng chống mã độc hại. Giúp cho khách hàng các thông tin nhanh, chính xác để đối phó với các mã độc hại nguy hiểm. Giúp khách hàng kiểm tra đánh giá tình trạng hoạt động của hệ thống phòng chống mã độc hại, đồng thời có các tư vấn hỗ trợ kỹ thuật để nâng cao hiệu quả hoạt động của hệ thống phòng chống mã độc hại, cũng như tư vấn về kế hoạch mở rộng, nâng cấp cho hệ thống phòng chống mã độc hại. Các chuyên gia cũng hỗ trợ kỹ thuật trong việc xử lý các sự cố khi vận hành hệ thống phòng chống mã độc hại giúp nâng cao tính sẵn sàng của hệ thống phòng chống mã độc hại và góp phần nâng cao tính sẵn sàng của hệ thống chung.

Ngoài ra giải pháp bảo mật cùng với chính sách bảo mật chung cho cả hệ thống cũng ảnh hưởng đến hiệu quả của hệ thống phòng chống mã độc hại. Cần phải kết hợp với các giải pháp bảo mật mạng khác để nâng cao tính an toàn cho hệ thống như FireWall (để kiểm soát truy nhập), xác thực mạnh (để chống việc giả mạo, mạo danh), Hệ thống phát hiện/phòng chống xâm nhập,... Vì chương trình, hệ thống diệt mã độc hại không thể đảm nhận được chức năng của các giải pháp khác mà kỹ thuật tấn công của mã độc hại ngày nay lại là sự kết hợp pha tạp rất nhiều kỹ thuật tấn công với nhau.

4.1.4 Mã hóa

Một phương pháp nữa giúp phòng chống tội phạm máy tính là mã hóa. Mã hoá nhằm đảm bảo tính trong suốt của thông tin và ngăn chặn những kẻ tấn công bất hợp pháp xem, sửa đổi dữ liệu; bởi vì một khi thông tin đã được mã hoá và gửi đi thì kẻ xấu rất khó hoặc không thể giải mã được

Có 2 phương pháp mã hóa được sử dụng hiện nay là mã hóa đối xứng và mã hóa bất đối xứng. Hai loại mã hóa này khác nhau ở số lượng khóa. Mã hóa đối xứng sử dụng cùng một khóa để mã hóa/giải mã. Trong khi đó, mã hóa bất đối xứng sử dụng hai khóa khác nhau để mã hóa và giải mã thông tin. Mỗi hệ thống mã hóa có ưu nhược điểm riêng. Mã hóa đối xứng xử lý nhanh nhưng độ an toàn không cao. Mã hóa bất đối xứng xử lý chậm hơn, nhưng độ an toàn và tính thuận tiện trong quản lý khóa cao. Trong các ứng dụng mã hóa hiện tại, người ta thường kết hợp các ưu điểm của cả hai loại mã hóa này.

Mã hóa có vai trò rất quan trọng, đặc biệt là trong giao dịch điện tử. Nó giúp đảm bảo bí mật, toàn vẹn của thông tin, khi thông tin đó được truyền trên mạng. Mã hóa cũng là nền tảng của kỹ thuật chữ ký điện tử, hệ thống PKI...

Với những ưu điểm của mã hóa đem lại sẽ giúp cho chúng ta giảm thiểu nguy cơ do tội phạm máy tính đem lại.

4.1.5 Các kỹ thuật, công nghệ khác

Ngoài các kỹ thuật, công nghệ đã nói ở trên; còn rất nhiều các giải pháp kỹ thuật khác cần được áp dụng để phòng chống tội phạm máy tính như:

- + Sử dụng các giải pháp xác thực mạnh
- + Sử dụng mạng riêng ảo
- + Dò quét, đánh giá điểm yếu
- + Chống tấn công mạng không dây
- +

Tùy vào mục đích cũng như yêu cầu của hệ thống mà lựa chọn các giải pháp kỹ thuật phù hợp. Dĩ nhiên càng sử dụng nhiều giải pháp thì thông tin càng được bảo mật, song đi đôi với đó là chi phí trả cho việc bảo mật cũng tăng cao. Ngoài ra, hiệu năng cũng trái ngược với tốc độ. Càng sử dụng nhiều giải pháp bảo mật, có nghĩa là một gói tin muốn đi vào được hệ thống bên trong sẽ qua nhiều khâu kiểm tra; như vậy sẽ làm chậm băng thông của hệ

thống. Chính vì thế cần cân đối các yếu tố để vừa có thể đảm bảo an toàn cho thông tin, tránh sự xâm nhập từ các tội phạm máy tính, trong khi đó vẫn đảm bảo được nhu cầu chi phí và đảm bảo hiệu suất hoạt động của toàn bộ hệ thống mạng.

4.2 SỬ DỤNG QUY ĐỊNH, LUẬT PHÁP

Song song với các giải pháp kỹ thuật, công nghệ là các quy định, luật pháp liên quan tới các hành vi tội phạm máy tính. Điều này một phần để răn đe, khiến cho các tội phạm mạng phải suy xét cẩn thận trước khi thực hiện hành vi phạm tội, đồng thời cũng là cơ sở cho việc xử phạt khi có tranh chấp hình sự xảy ra.

Đối với các cơ quan, tổ chức cần xây dựng các quy định cho riêng tổ chức mình để hướng dẫn và buộc các nhân viên tuân thủ. Trong phạm vi cả nước, cần áp dụng các quy định, thành văn bản và có các chế tài xử phạt tương ứng với từng hành vi phạm tội. Ở Việt Nam đã có các điều khoản được quy định trong Bộ luật Hình sự song trên thực tế vẫn còn nhiều bất cập. Ngoài tội phạm đã được quy định trong Bộ luật Hình sự, với thủ đoạn dùng máy tính được sử dụng như một công cụ để gây án, để lưu giữ thông tin tội phạm, như: lừa đảo chiếm đoạt tài sản, trộm cắp tài sản, rửa tiền, buôn bán ma túy, tuyên truyền văn hóa phẩm đồi trụy... thì hiện nay đã xuất hiện tội phạm với mục tiêu tấn công là cơ sở dữ liệu của máy tính, hoặc mạng máy tính, trong đó những hành vi chủ yếu là: Tạo ra, lan truyền, phát tán các chương trình virus, đột nhập trái phép cơ sở dữ liệu máy tính, trộm cắp dữ liệu, thông tin (đặc biệt là cơ sở dữ liệu quốc gia, an ninh, quốc phòng), tấn công từ chối dịch vụ (DDOS-Botnet), sử dụng trái phép dữ liệu, đưa thông tin trái phép lên mạng... Trong khi đó, theo quy định của Bộ luật Hình sự hiện hành, mới chỉ có 3 điều luật điều chỉnh những hành vi vi phạm trong lĩnh vực tội phạm công nghệ cao: Điều 224: Tội tạo ra và lan truyền, phát tán các chương trình virus tin học. Điều 225: Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử. Điều 226: Tội sử dụng trái phép thông tin trên mạng và trong máy vi tính.

Trong xu hướng toàn cầu hóa nền kinh tế thế giới, tội phạm công nghệ cao cũng mang tính toàn cầu. Những loại tội phạm công nghệ cao xuất hiện

trên thế giới cũng xảy ra ở Việt Nam và gây nguy hại cho nền kinh tế, chính trị và xã hội như ở các nước khác. Do vậy, tất cả những hành vi gây nguy hiểm cho xã hội cần phải bị xử lý bằng luật hình với các chế tài nghiêm khắc, đủ để trấn áp, răn đe và phòng ngừa như kinh nghiệm ở các nước trên thế giới. Muốn vậy, Việt Nam cần bổ sung những điều luật về phòng chống tội phạm công nghệ cao vào Bộ luật Hình sự.

Trên thế giới, trong lĩnh vực tội phạm mạng, điều đầu tiên một Nhà nước phải làm là ban hành trong nước một văn bản luật hiệu quả, có nội dung hài hoà với luật của các nước khác nhằm tạo điều kiện thuận lợi cho việc hợp tác. Công ước của Hội đồng Châu Âu ngày 23 tháng 11 năm 2001 về tội phạm mạng nhằm giải quyết vấn đề này. Công ước này vượt ra xa khỏi biên giới Châu Âu vì đã được mở cho tất cả các nước trên thế giới

Công ước này giúp các nước có một cách tiếp cận thống nhất về tội phạm mạng, tạo điều kiện thuận lợi cho việc thu thập chứng cứ điện tử và điều tra các hành vi phạm tội sử dụng máy tính, không chỉ các tội riêng trong lĩnh vực mạng Internet mà còn cả các tội phạm “truyền thống” được thực hiện với sự hỗ trợ của máy tính (hợp pháp hoá tiền và tài sản do phạm tội mà có, khủng bố và các tội phạm khác). Công ước giúp thống nhất quy định pháp luật của các nước thành viên. Các nước thành viên được mời tham dự vào mọi công việc của Ủy ban tư vấn, cơ quan phụ trách việc nghiên cứu soạn thảo các nghị định thư hoặc phụ lục bổ sung cho Công ước trong tương lai.

Một quốc gia để gia nhập Công ước, trước hết phải cải thiện hệ thống pháp luật của mình cho phù hợp với Công ước trước khi phê chuẩn. Vào thời điểm phê chuẩn, pháp luật của nước đó đã phải phù hợp với Công ước. Vì vậy, cần phải bắt đầu công việc sửa đổi pháp luật từ trước. Sau khi đã hoàn thành công việc này, nước muốn gia nhập phải gửi văn bản xin gia nhập cho Ban thư ký của Hội đồng Châu Âu. Tiếp đó, các nước thành viên Công ước sẽ tiến hành tham vấn. Ba tháng sau khi tham vấn, Hội đồng Châu Âu sẽ mời nước ứng cử viên gia nhập Công ước. Khi đó, nước ứng cử viên có quyền tự do lựa chọn phương thức gia nhập (ngày, tháng...).

Ngay cả trường hợp không gia nhập Công ước, thì Công ước vẫn có thể được dùng như luật mẫu để cải thiện pháp luật trong nước. Có thể phân tích từng điều của Công ước và so sánh chúng với quy định pháp luật của mình.

Nhiều nước đã yêu cầu Hội đồng Châu Âu phân tích thực trạng của mình. Đến nay, Hội đồng Châu Âu đã có báo cáo đánh giá cho khoảng 40 nước, trong đó có báo cáo rất chi tiết về Việt Nam, Campuchia, Lào và Thái Lan. Riêng trường hợp Rumania lại rất thú vị, vì nước này đã thông qua một văn bản luật hầu như sao chép y nguyên nội dung của Công ước.

Năm 2007, Thái Lan cũng đã thông qua một đạo luật khá đầy đủ về vấn đề tội phạm mạng. Việt Nam đã thông qua hai điều luật mới bổ sung cho Bộ luật hình sự và sẽ có hiệu lực trong tháng 1 năm 2010, về tội truy cập bất hợp pháp, gian lận trên hệ thống máy tính. Việt Nam còn phải bổ sung thêm nhiều điều nữa trong thời gian tới, đặc biệt khi sửa đổi bộ luật tố tụng hình sự, Việt Nam cần đưa ra các quy định trên cơ sở tham khảo Công ước. Hội đồng Châu Âu có thể hỗ trợ các nước trong quá trình dự thảo : nếu ban soạn thảo đã được thành lập thì có thể tiến hành hợp tác trong quá trình nghiên cứu, soạn thảo và đóng góp ý kiến vào các dự thảo. Ngoài ra, còn có thể tổ chức các lớp tập huấn cho thành viên của ban này. Trong tháng 3 năm 2010, Hội đồng Châu Âu sẽ tổ chức một cuộc hội nghị tại Strasbourg về hợp tác đấu tranh chống tội phạm mạng. Các nước trong khu vực Châu Á Thái Bình Dương cũng có thể sẽ được mời tham gia.

Tuy nhiên, cũng phải lưu ý rằng trong mọi trường hợp, đấu tranh chống tội phạm mạng không phải là cơ để vi phạm các quyền cơ bản của cá nhân. Cần phải tìm ra một điểm cân bằng giữa vấn đề đảm bảo an ninh và các quyền cơ bản của công dân cũng như quyền đối với đời tư. Để làm được điều đó, cần phải giải quyết vấn đề tội phạm mạng và bảo vệ dữ liệu cá nhân cùng nhau chứ không tách rời nhau xét dưới góc độ pháp luật.

4.3 NÂNG CAO NHẬN THỨC NGƯỜI SỬ DỤNG

Nâng cao nhận thức người sử dụng là một vấn đề rất cần thiết để bảo vệ an toàn cho chính người sử dụng cũng như giúp phòng chống tội phạm máy tính. Trong một cơ quan, doanh nghiệp, số lượng người sử dụng máy vi tính có kết nối Internet để làm việc gần như là 100%; tuy nhiên số lượng người có kiến thức về an toàn thông tin, tuân thủ đúng các quy định về đảm bảo an toàn thông tin lại chiếm một phần rất nhỏ. Theo một khảo sát về an toàn thông tin tại một Ngân hàng Việt Nam, số lượng người hiểu biết về an toàn thông tin

chỉ chiếm khoảng 20% trên tổng số. Từ vấn đề như thế, việc nâng cao nhận thức người sử dụng là nhu cầu thiết yếu với bất kỳ cơ quan, tổ chức nào.

Nâng cao nhận thức cần phải được thực hiện đồng bộ, từ trên xuống dưới và theo nhiều khía cạnh khác nhau. Dưới đây là một số vấn đề cần thiết trong việc nâng cao nhận thức về an toàn cho người dùng khi sử dụng máy tính:

Cần thường xuyên cập nhật hệ điều hành và phần mềm

Hệ điều hành và phần mềm ứng dụng thường tồn tại các lỗ hổng mà kẻ tấn công có thể lợi dụng để khai thác nhằm chiếm quyền điều khiển hệ thống hoặc đánh cắp các thông tin nhạy cảm. Microsoft và Apple thường phát hành các bản cập nhật cho hệ điều hành của họ và người sử dụng nên cài đặt các bản cập nhật này khi chúng có sẵn cho máy tính Windows và Mac. Những bản cập nhật này thường bao gồm bản sửa lỗi có thể cải thiện tính bảo mật của hệ thống. Do vậy cần khuyến cáo người dùng thường xuyên thực hiện cập nhật lên các phiên bản mới nhất để vá các lỗ hổng, nâng cao tính an toàn khi sử dụng hệ thống.

Người dùng Windows có thể cài đặt bản cập nhật bằng cách sử dụng tính năng được gọi là “Cập nhật Windows”, trong khi người dùng Mac có thể cài đặt bản cập nhật bằng cách sử dụng tính năng được gọi là “Cập nhật phần mềm”. Nếu không quen với các tính năng này, người sử dụng có thể lên các trang web của Microsoft và Apple để biết thêm thông tin về cách cài đặt các bản cập nhật hệ thống trên máy tính.

Sử dụng tài khoản không phải là quản trị viên bất cứ khi nào có thể

Hầu hết hệ điều hành đều cho phép người dùng tạo nhiều tài khoản trên máy tính của mình, do đó, những người dùng khác nhau có thể có cài đặt khác nhau. Những tài khoản người dùng này cũng có thể được thiết lập để có cài đặt bảo mật khác nhau.

Ví dụ: tài khoản “quản trị” thường có khả năng cài đặt phần mềm mới, trong khi tài khoản “có giới hạn” hoặc “chuẩn” thường không có khả năng làm như vậy. Để sử dụng các công việc bình thường, có thể không cần phải cài đặt phần mềm mới, vì vậy chỉ nên sử dụng tài khoản người dùng “có giới hạn” hoặc “chuẩn” bất kỳ khi nào có thể. Làm điều này có thể giúp ngăn phần

mềm độc hại cài đặt trên máy tính và thực hiện các thay đổi cho toàn bộ hệ thống.

Sử dụng mật khẩu đủ mạnh để đặt cho các tài khoản

Mật khẩu sử dụng cho các tài khoản quyền “quản trị” cũng như tài khoản bình thường, người sử dụng nên đặt mật khẩu đủ mạnh để tránh bị kẻ tấn công dò quét ra mật khẩu hòng đánh cắp tài khoản.

Mật khẩu đủ mạnh là mật khẩu bao gồm các yếu tố như sau:

- + Độ dài ít nhất là 8 ký tự
- + Bao gồm cả chữ thường, chữ hoa, số và ký tự đặc biệt
- + Thường xuyên thay đổi
- + Không bao giờ được đặt mật khẩu trùng với username
- + Không sử dụng các từ dễ đoán để dùng cho mật khẩu (tên người thân, tên cơ quan, biển số xe)
- + Không sử dụng các chuỗi liên tục (abcde, qwert, 12345,) để làm mật khẩu

Cần xem xét cẩn thận trước khi nhấp vào các liên kết hoặc tải xuống bất cứ cái gì

Khi có một liên kết lạ từ một người không quen biết gửi tới, người dùng cần cẩn thận trước khi nhấp vào liên kết bởi vì những liên kết thường trở tới một website chứa mã độc hại nhằm lây nhiễm vào máy tính người sử dụng để đánh cắp các thông tin về tài khoản hoặc thông tin nhạy cảm khác.

Trong nhiều trường hợp khi duyệt web, có thể một trang web đột nhiên hiện ra với nội dung hấp dẫn. Lúc đó người dùng cũng cần cẩn thận bởi thường những website như thế cũng chứa các mã độc và khi người dùng click vào đồng nghĩa với tải các chương trình độc hại về máy tính của mình.

Cần kiểm tra trước khi mở tệp đính kèm email hoặc hình ảnh

Nếu có một người nào đó gửi email đáng ngờ có chứa tệp tin đính kèm hoặc hình ảnh, người sử dụng cũng cần cẩn thận trước khi mở tệp đính kèm. Mặc dù đôi khi, những email đó có thể chỉ là spam, nhưng những lần khác, những email đó có thể bí mật chứa phần mềm độc hại gây hại cho máy tính.

Không tin tưởng cửa sổ bật lên yêu cầu tải xuống phần mềm

Khi lướt web, người sử dụng có thể gặp các trang web hiển thị cửa sổ bật lên làm cho người dùng tin rằng máy tính của đã bị nhiễm và yêu cầu tải

xuống một số phần mềm để tự bảo vệ mình. Đây cũng là một trong những trò lừa đảo. Bởi vì chỉ cần click vào đó là người dùng đã có thể bị nhiễm virus vào máy tính. Do đó cần đóng cửa sổ bật lên và không nhấp chuột vào bên trong cửa sổ.

Cẩn thận khi chia sẻ file trên web

Một số trang web và ứng dụng cho phép người dùng dễ dàng chia sẻ các file với người dùng khác. Tuy nhiên nhiều trang web và ứng dụng trong số này lại không có nhiều các chương trình bảo vệ chống lại mã độc hại. Do đó rất có thể khi chia sẻ file trên các server này, các file sẽ ngẫu nhiên bị nhiễm mã độc và nếu người dùng khác tải file xuống, chạy chương trình thì sẽ bị nhiễm mã độc vào máy tính. Các phần mềm độc hại thường có thể được ngụy trang dưới dạng phim, album, trò chơi hoặc chương trình phổ biến.

Sử dụng phần mềm diệt vi rút

Nếu cần phải tải xuống mục gì đó, người dùng nên sử dụng chương trình diệt vi rút để quét phần mềm độc hại cho bản tải xuống đó trước khi mở. Phần mềm diệt vi rút cũng quét các phần mềm độc hại cho toàn bộ máy tính của người dùng.

Ngoài ra, người sử dụng cần thường xuyên quét máy tính của mình để sớm phát hiện phần mềm độc hại và ngăn chặn phần mềm độc hại đó phát tán.

4.4 CÁC BIỆN PHÁP KHÁC

Ngoài các biện pháp như trên, để phòng chống tội phạm máy tính chúng ta cũng có thể sử dụng kết hợp thêm nhiều các biện pháp khác. Các biện pháp này có thể là đảm bảo an ninh vật lý: như khóa cửa cẩn thận, có hệ thống camera giám sát 24/24, tách biệt hẳn các máy tính có chứa dữ liệu quan trọng khỏi mạng Internet, hoặc các biện pháp công nghệ như: sử dụng các thiết bị nhiễu sóng để tránh kẻ tấn công nghe lén thông tin từ bên ngoài, sử dụng lồng Faraday để chống tấn công thu bức xạ màn hình, ...

Công nghệ ngày một phát triển, tội phạm mạng ngày một gia tăng và tinh vi hơn song quan trọng nhất vẫn là ý thức của người sử dụng. Để đảm bảo một hệ thống an toàn, kẻ tấn công khó có thể lợi dụng tấn công đánh cắp dữ liệu thì bản thân từng người sử dụng cần ý thức được các hành động của mình khi tham gia vào cộng đồng mạng. Dĩ nhiên các biện pháp về kỹ thuật,

công nghệ là không thể thiếu để kiểm soát và ngăn chặn các tấn công. Đồng thời, quy định, luật pháp cũng cần được áp dụng thì mới có thể răn đe, ngăn ngừa các hành vi đánh cắp thông tin qua mạng.

TÀI LIỆU THAM KHẢO

1. Tài liệu từ sách

- [1] Chuck Easttom and Det.Jeff Taylor, *Computer Crime Investigation and the Law*, Cengage Learning PTR, (Năm 2011).
- [2] Cory Altheide & Harlan Carvey, *Digital Forensics with Open Source Tools*, Syngress, (Năm 2011).
- [3] Michael Kunz & Patrick Wilson, *Computer Crime and Computer Fraud*, University of Maryland, Department of Criminology and Criminal Justice Fall, (Năm 2004).
- [4] Thomas A.Johnson, *Forensic Computer Crime Investigation*, Academic Press, (Năm 2005).
- [5] EC-Council, *Computer Forensics: Investigation Procedures and Response*, Cengage Learning, (Năm 2009).
- [6] Eoghan Casey BS MA, *Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet*, Academic Press, (Năm 2001).
- [7] Christine Hess Orthmann and Kären M. Hess, *Criminal Investigation*, Cengage Learning, (Năm 2012).

2. Tài liệu từ Internet

- [8] Website: <http://www.toiphammaytinh.com/>
- [9] Bộ luật hình sự Việt Nam – Bộ tư pháp
<http://www.moj.gov.vn>
- [10] Bộ luật tố tụng dân sự Việt Nam
<http://www.boluatdansu.com>

PHỤ LỤC

Phụ lục 1: LUẬT VỀ TỘI PHẠM MÁY TÍNH Ở VIỆT NAM

Tại Việt Nam, các luật về tội phạm máy tính được quy định trong Bộ luật hình sự Việt Nam năm 1999 và được sửa đổi bổ sung năm 2009.

Dưới đây là các điều khoản liên quan tới tội phạm máy tính trong Bộ luật hình sự Việt Nam số 15/1999/QH10:

Điều 125. Tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín của người khác

1. Người nào chiếm đoạt thư, điện báo, telex, fax hoặc các văn bản khác được truyền đưa bằng phương tiện viễn thông và máy tính hoặc có hành vi trái pháp luật xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín của người khác đã bị xử lý kỷ luật hoặc xử phạt hành chính về hành vi này mà còn vi phạm, thì bị phạt cảnh cáo, phạt tiền từ một triệu đồng đến năm triệu đồng hoặc phạt cải tạo không giam giữ đến một năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt cải tạo không giam giữ từ một năm đến hai năm hoặc phạt tù từ ba tháng đến hai năm:

- a) Có tổ chức;*
- b) Lợi dụng chức vụ, quyền hạn;*
- c) Phạm tội nhiều lần;*
- d) Gây hậu quả nghiêm trọng;*
- đ) Tái phạm.*

3. Người phạm tội còn có thể bị phạt tiền từ hai triệu đồng đến hai mươi triệu đồng, cấm đảm nhiệm chức vụ nhất định từ một năm đến năm năm.

Điều 224. Tội tạo ra và lan truyền, phát tán các chương trình vi - rút tin học

1. Người nào tạo ra và cố ý lan truyền, phát tán các chương trình vi-rút qua mạng máy tính hoặc bằng các phương thức khác gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại các dữ liệu của máy tính hoặc đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm, thì bị phạt tiền từ năm triệu đồng đến một trăm triệu đồng hoặc phạt tù từ sáu tháng đến ba năm.

2. Phạm tội gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng, thì bị phạt tù từ hai năm đến bảy năm.

3. Người phạm tội còn có thể bị phạt tiền từ năm triệu đồng đến năm mươi triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Điều 225. Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử

1. Người nào được sử dụng mạng máy tính mà vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại các dữ liệu của máy tính hoặc đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm, thì bị phạt tiền từ năm triệu đồng đến một trăm triệu đồng, cải tạo không giam giữ đến ba năm hoặc phạt tù từ một năm đến ba năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ hai năm đến năm năm:

a) Có tổ chức;

b) Gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

3. Người phạm tội còn có thể bị phạt tiền từ năm triệu đồng đến năm mươi triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Điều 226. Tội sử dụng trái phép thông tin trên mạng và trong máy tính

1. Người nào sử dụng trái phép thông tin trên mạng và trong máy tính, cũng như đưa vào mạng máy tính những thông tin trái với quy định của pháp luật gây hậu quả nghiêm trọng, đã bị xử lý kỷ luật, xử phạt hành chính mà còn vi phạm, thì bị phạt tiền từ năm triệu đồng đến năm mươi triệu đồng, cải tạo không giam giữ đến ba năm hoặc bị phạt tù từ sáu tháng đến ba năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ hai năm đến năm năm:

a) Có tổ chức;

b) Gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

3. Người phạm tội còn có thể bị phạt tiền từ ba triệu đồng đến ba mươi triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Năm 2009, các điều luật 244, 225, 226 trong Bộ luật Hình sự Việt Nam năm 1999 được sửa đổi bổ sung. Bộ luật sửa đổi bổ sung này có số 37/2009/QH12 được thông qua ngày 19 tháng 6 năm 2009 và bắt đầu có hiệu lực vào ngày 1 tháng 1 năm 2010. Các điều khoản về tội phạm máy tính trong Bộ luật Hình sự Việt Nam được quy định tại điều 224, 224, 226, 226a, 226b.

Dưới đây là các điều khoản liên quan tới tội phạm máy tính trong Bộ luật hình sự Việt Nam số 37/2009/QH12:

Điều 224. Tội phát tán vi rút, chương trình tin học có tính năng gây hại cho hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số

1. Người nào cố ý phát tán vi rút, chương trình tin học có tính năng gây hại cho mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số gây hậu quả nghiêm trọng, thì bị phạt tiền từ hai mươi triệu đồng đến hai trăm triệu đồng hoặc phạt tù từ một năm đến năm năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ ba năm đến bảy năm:

- a) Có tổ chức;*
- b) Gây hậu quả rất nghiêm trọng;*
- c) Tái phạm nguy hiểm.*

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ năm năm đến mười hai năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ an ninh, quốc phòng;

b) Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông;

c) Gây hậu quả đặc biệt nghiêm trọng.

4. Người phạm tội còn có thể bị phạt tiền từ năm triệu đồng đến năm mươi triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Điều 225. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số

1. Người nào thực hiện một trong các hành vi sau đây gây hậu quả nghiêm trọng nếu không thuộc trường hợp quy định tại Điều 224 và Điều

226a của Bộ luật này, thì bị phạt tiền từ hai mươi triệu đồng đến hai trăm triệu đồng hoặc phạt tù từ một năm đến năm năm:

- a) Tự ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu thiết bị số;
- b) Ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số;
- c) Hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ ba năm đến bảy năm:

- a) Có tổ chức;
- b) Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông, mạng Internet;
- c) Gây hậu quả rất nghiêm trọng;

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ năm năm đến mười hai năm:

- a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ an ninh, quốc phòng;
- b) Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông;
- c) Gây hậu quả đặc biệt nghiêm trọng.

4. Người phạm tội còn có thể bị phạt tiền từ năm triệu đồng đến năm mươi triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Điều 226. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, mạng Internet

1. Người nào thực hiện một trong các hành vi sau đây xâm phạm lợi ích của cơ quan, tổ chức, cá nhân, xâm phạm trật tự, an toàn xã hội gây hậu quả nghiêm trọng, thì bị phạt tiền từ mười triệu đồng đến một trăm triệu đồng, cải tạo không giam giữ đến ba năm hoặc bị phạt tù từ sáu tháng đến ba năm:

- a) Đưa lên mạng máy tính, mạng viễn thông, mạng Internet những thông tin trái với quy định của pháp luật, nếu không thuộc trường hợp quy định tại Điều 88 và Điều 253 của Bộ luật này;

b) Mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa những thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân khác trên mạng máy tính, mạng viễn thông, mạng Internet mà không được phép của chủ sở hữu thông tin đó;

c) Hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông, mạng Internet.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ hai năm đến bảy năm:

a) Có tổ chức;

b) Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông, mạng Internet;

c) Thu lợi bất chính từ một trăm triệu đồng trở lên;

d) Gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

3. Người phạm tội còn có thể bị phạt tiền từ hai mươi triệu đồng đến hai trăm triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Điều 226a. Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác

1. Người nào cố ý vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của thiết bị số; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ, thì bị phạt tiền từ hai mươi triệu đồng đến hai trăm triệu đồng hoặc phạt tù từ một năm đến năm năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ ba năm đến bảy năm:

a) Có tổ chức;

b) Lợi dụng chức vụ, quyền hạn;

c) Thu lợi bất chính lớn;

d) Gây hậu quả nghiêm trọng;

đ) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ năm năm đến mười hai năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ an ninh, quốc phòng;

b) Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông;

c) Thu lợi bất chính rất lớn hoặc đặc biệt lớn;

d) Gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

4. Người phạm tội còn có thể bị phạt tiền từ năm triệu đồng đến năm mươi triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Điều 226b. Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản

1. Người nào sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện một trong những hành vi sau đây, thì bị phạt tiền từ mười triệu đồng đến một trăm triệu đồng hoặc phạt tù từ một năm đến năm năm:

a) Sử dụng thông tin về tài khoản, thẻ ngân hàng của cơ quan, tổ chức, cá nhân để chiếm đoạt hoặc làm giả thẻ ngân hàng nhằm chiếm đoạt tài sản của chủ thẻ hoặc thanh toán hàng hóa, dịch vụ;

b) Truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản;

c) Lừa đảo trong thương mại điện tử, kinh doanh tiền tệ, huy động vốn tín dụng, mua bán và thanh toán cổ phiếu qua mạng nhằm chiếm đoạt tài sản của cơ quan, tổ chức, cá nhân;

d) Hành vi khác nhằm chiếm đoạt tài sản của cơ quan, tổ chức, cá nhân.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ ba năm đến bảy năm:

a) Có tổ chức;

b) Phạm tội nhiều lần;

c) Có tính chất chuyên nghiệp;

d) Chiếm đoạt tài sản có giá trị từ năm mươi triệu đồng đến dưới hai trăm triệu đồng;

đ) Gây hậu quả nghiêm trọng;

e) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ bảy năm đến mười lăm năm:

a) Chiếm đoạt tài sản có giá trị từ hai trăm triệu đồng đến dưới năm trăm triệu đồng;

b) Gây hậu quả rất nghiêm trọng.

4. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ mười hai năm đến hai mươi năm hoặc tù chung thân:

a) Chiếm đoạt tài sản có giá trị từ năm trăm triệu đồng trở lên;

b) Gây hậu quả đặc biệt nghiêm trọng.

5. Người phạm tội còn có thể bị phạt tiền từ năm triệu đồng đến một trăm triệu đồng, tịch thu một phần hoặc toàn bộ tài sản, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ một năm đến năm năm.

Phụ lục 2: MỘT SỐ VỤ ĐIỂN HÌNH VỀ TỘI PHẠM MẠNG Ở VIỆT NAM

1. Tấn công vào cơ sở dữ liệu lấy cắp thông tin và thay đổi nội dung

1.1. Vụ Bùi Minh Trí tấn công website mot.gov.vn

Ngày 27-11-2006, website mot.gov.vn đã bị đột nhập và ảnh Bộ trưởng Nguyễn Thiện Nhân đã bị thay bằng ảnh của 1 thanh niên cởi trần. Qua điều tra đã phát hiện 1 số dấu vết do thủ phạm để lại trên mạng: Vào cuối tháng 6-2006, Trí đã tấn công website VNMedia và lấy được toàn bộ các thông tin về DataBase của các website nằm cùng server, trong đó có website của báo Nhân dân điện tử: www.nhandan.org.vn và của website www.dangcongsan.vn Trí đã khoe lên diễn đàn với bài viết “How I hacked home.vnn.vn” . Đây là 1 số trích lại bài viết của Bùi Minh Trí khoe trên diễn đàn HVA như sau:

How I hacked

Home.vnn.vn:

Found 17 websites with the IP 203.162.0.12

- | | |
|--------------------|--------------------------|
| 1. 203.162.0.12 | 2. Cpv.org.vn |
| 3. Dangcongsan.vn | 4. Dienhoa.vnn.vn |
| 5. Hanoi.vnn.vn | 6. Hanoitelecom.vnn.vn |
| 7. Home.vnn.vn | 8. Hssv.vnn.vn |
| 9. Info.vdc.com.vn | 10. Khoahoc.vnn.vn |
| 11. Nhandan.org.vn | 12. Support.vnn.vn |
| 13. Tintuc.vnn.vn | 14. Tuyensinh.vdc.com.vn |
| 15. Vdc.com.vn | 16. Wap.vnn.vn |
| | 17. Xaydungdang.org.vn |

Bằng lỗi viewsource trên dienhoa.vnn.vn, GY đã gom được hầu hết thông tin về DB acc+pass của các site trên server 203.163.0.12 và của vnmedia.vn cùng 1 số site khác.

Đối tượng tấn công và tạo ra 1 tài khoản tên là GuanYu và đăng nhập vào máy chủ qua Remote Desktop vào lúc 15:59 ngày 27/11/2006 từ địa chỉ IP 125.234.59.209

Thông tin về địa chỉ IP đã đột nhập vào server Bộ GDDT là:

Tên: Võ Thị Kim Phụng

Địa chỉ: 45A Phạm Thái Bường, Phường 4, thị xã Vĩnh Long

Điện thoại : 070 83378..

Đây là địa chỉ nhà riêng của Bùi Minh Trí

Thông tin về đối tượng tấn công website:

Về nick GuanYu: Trước đó đã thực hiện một số vụ tấn công và máy chủ VDC cũng do nick này thực hiện:

Trong vụ VNMEDIA bị hack ngày 03/09/2006, trên website có nhúng 1 bài hát trỏ đến tên miền <http://www.xprofiles.net>. Xem thôn tin về người quản lý tên miền thì thấy, đó là Bùi Minh Trí, địa chỉ Vĩnh Long. Hiện nay, thôn tin về domain này đã thay đổi nhưng vẫn để tên: Bùi Minh Trí

Thôn tin về GuanYu-Bùi Minh Trí đã được lưu lại trên 1 số forum từ đó. Đến khi vụ website của Bộ GDDT bị tấn công, nick GuanYu một lần nữa xuất hiện và lần này đã để lại dấu vết và tìm được địa chỉ nhà riêng. Những chứng cứ trên cho thấy. Bùi Minh Trí đã nhiều lần tấn công các website, cài virus, lấy cắp dữ liệu, phá hoại dữ liệu, thể hiện là 1 hacker mũ đen, vi phạm pháp luật.

1.2. Vụ tấn công vào website của Sở kế hoạch đầu tư TP HCM

Vào ngày 05/05/2006 một chuyên viên của Sở KHĐT đã gặp một người tên là Hoàng Anh, giám đốc công ty TNHH phần mềm ý tưởng Việt. Người này cho biết đang nắm giữ cơ sở dữ liệu về quản lý doanh nghiệp của Sở trên internet, đồng thời đưa ra các thôn tin chi tiết về cấu trúc kỹ thuật của cơ sở dữ liệu mà Sở KHĐT đang đặt tại công ty VDC. Sở KHĐT TP HCM đã kiểm tra lại thôn tin trên và thấy các thôn tin này hoàn toàn phù hợp với tổ chức kỹ thuật tại VDC. Đến ngày 10/07/2006, Sở KHĐT nhận được thôn tin của nhiều doanh nghiệp cho biết không truy cập được vào hồ sơ đã được đăng ký trên mạng của Sở. Sở KHĐT kiểm tra và phát hiện có 38 hồ sơ đã bị thay đổi so với nội dung ban đầu, nội dung những thay đổi này là :ngày đăng ký, mật khẩu truy cập, địa chỉ IP đã thực hiện những thay đổi này là: 221.121.34.198 đã thực hiện thay đổi 22 hồ sơ, địa chỉ này là của Công ty TNHH Quốc tế Hoàng Anh thuê đường truyền của Công ty SPT. Đồng thời các doanh nghiệp bị thay đổi hồ sơ cũng thôn báo Công ty TNHH Quốc tế Hoàng Anh đã gửi thư qua đường bưu điện đến người đại diện của các doanh nghiệp này để đề nghị thực hiện dịch vụ làm hồ sơ với giá khoảng 1,2 triệu đồng một hồ sơ, trong thời hạn từ 7 đến 10 ngày. Qua xác minh cho thấy: Cơ sở dữ liệu của Sở KHĐT chứa các thôn tin về hồ sơ đăng ký kinh doanh của các doanh nghiệp. Các thôn tin này không được công bố trên trang web của sở và cũng không được cung cấp cho bất kỳ cá nhân hay cơ quan nào. Cơ sở dữ liệu này đã bị kẻ gian truy cập trái phép, sửa đổi và sao chép toàn bộ dữ liệu. Đối tượng đã thực hiện việc truy cập, sửa đổi và sao chép trái phép cơ sở dữ liệu của Sở KHĐT TP HCM nhằm mục đích kéo dài thời gian giải quyết hồ sơ của Sở và gây khó

khẩn cho các doanh nghiệp đăng ký kinh doanh qua mạng. Từ đó liên hệ với doanh nghiệp để đề nghị sử dụng dịch vụ làm hồ sơ với giá khoảng 1,2 triệu. Việc làm trên của các đối tượng đã vi phạm các quy định về quản lý và sử dụng mạng internet, phá hủy các thông tin trên mạng của Sở KHĐT nhằm mục đích kiếm tiền. Gây ảnh hưởng nghiêm trọng đến quá trình giải quyết hồ sơ của Sở KHĐT TP HCM và việc đăng ký kinh doanh của các doanh nghiệp. Kết quả xác minh các địa chỉ IP nói trên và những “dấu vết” thủ phạm đã để lại trên internet đã phát hiện Giám đốc Công ty TNHH Quốc tế Hoàng Anh đã tấn công cơ sở dữ liệu của Sở KHĐT TP HCM để làm dịch vụ đăng ký cho các doanh nghiệp.

1.3. Vụ việc tấn công vào hệ thống mạng Công ty VMS(Mobifone) lấy cắp dữ liệu

Vào khoảng đầu tháng 4/2006 Nguyễn Văn N., đã vào mạng internet và tiến hành dò tìm tên đăng nhập và mật khẩu để đăng nhập vào mạng VNP(mạng LAN nội bộ) của công ty VMS. Sau đó N vào website của VMS ftp:\\203.160.109.249 để tải phần mềm đấu nối thuê bao điện thoại di động và cài vào máy tính cá nhân ở nhà riêng. Sau khi đã vào được hệ thống, có được phần mềm đấu nối thuê bao, N tiến hành việc đấu nối thuê bao điện thoại di động đầu số đẹp 090. N có thể sử dụng được phần mềm đấu nối thuê bao này là do phần mềm này có 1 User tên truy cập mặc định với mật khẩu đơn giản và N có thể dò tìm được. Theo N khai: N có được User truy cập này bằng cách truy cập trái phép vào cơ sở dữ liệu của Trung tâm 3 mạng nội bộ VMS. Sau đó vào kho dữ liệu số đẹp, tiến hành xóa những số đẹp trong danh sách kho số đẹp và tiến hành chuyển sang kho số bình thường, được phép đấu nối để tiến hành tự đấu nối vào các phôi sim có được và sử dụng. N khai đã tiến hành đấu nối bất hợp pháp để lấy trộm các thuê bao là: 0905522222; 0905588888; 0905599999; 0905688888; 0906559999. Đây là những số nằm trong kho danh sách số đẹp, khi đấu nối phải có phiếu đấu nối để kiểm soát. N đã sử dụng phôi sim có được khi làm ở cửa hàng Toàn Thịnh, khách hàng chuyển từ dịch vụ trả trước sang dịch vụ trả sau thì những sim còn lại của dịch vụ trả trước sẽ là sim hủy, sim này sẽ trở thành phôi sim nếu sử dụng lại). Ngoài ra, N còn khai, trước đó vào khoảng tháng 10/2005 cũng bằng cách thức trên, N tiến hành đấu nối bất hợp pháp sim số 0902000000 và đến cửa hàng Mobifone ở Hà Đông để tiến hành đăng ký thuê bao này từ trả trước sang trả sau. Như vậy, N đã có hành vi truy cập trái phép, tấn công vào hệ thống mạng, cơ sở dữ liệu của VMS. Khi tiến hành rà quét tên truy cập và mật

khẩu không đúng 03 lần, hệ thống sẽ tự động khóa tài khoản đó lại, gây ra treo máy, muốn cho máy hoạt động trở lại, phải khởi động lại, gây ảnh hưởng đến hoạt động của hệ thống mạng, các đại lý không thể kết nối đến hoạt động kinh doanh. Trong quá trình truy cập trái phép vào hệ thống mạng N đã trộm cắp và đầu nối bất hợp pháp 05 số điện thoại đẹp với giá trị lớn, có biểu hiện để bán thu lợi.

2. Tấn công từ chối dịch vụ DDoS-BotNet:

2.1. Vụ tấn công cơ sở dữ liệu của công ty Nhân Hòa

Đầu tháng 5/2006 trang web của 1 số khách hàng thuê máy chủ tại công ty Nhân Hòa đã bị tấn công từ chối dịch vụ (tấn công DDOS) .Các trang web này gồm: www.nhatquangcomputer.com.vn, và kimduc.com. Các trang web này đều bị tấn công từ chối dịch vụ theo kiểu xFlash. Trang web: www.nhatquangcomputer.com.vn của công ty TNHH Thương mại và Công nghệ Nhật Quang, thuê máy chủ tại công ty Nhân Hòa. Phân tích nhật ký máy chủ cho thấy địa chỉ chứa flash tấn công trang web này là: tungtuyengroup.50webs.com/nhatquang/nhatquang.swf. Trang web này không chứa nội dung mà chỉ chứa 1 đoạn mã để khi truy cập máy tính của người sử dụng sẽ tải về và chạy 1 flash được đặt tên là nhatquang.swf, đoạn flash này khi chạy sẽ liên tục tạo các truy cập tới địa chỉ: www.nhatquangcomputer.com.vn Qua tìm kiếm và phân tích cho thấy trang web: tungtuyengroup.50webs.com trước đây đã từng chứa các nội dung giống hệt trang web tungtuyen.com Trang tungtuyen.com là của công ty TNHH Tùng Tuyền, có Giám đốc là Trần Thanh Tùng. Tên miền tungtuyen.com được đăng ký bởi Công ty TNHH Hạ Long. Như vậy việc trang web: www.nhatquangcomputer.com.vn bị tấn công từ chối dịch vụ có liên quan trực tiếp tới chủ sở hữu hoặc người viết trang web: tungtuyen.com. Trang: kimduc.com là của Công ty Thành Nam mobile, thuê máy chủ tại công ty Nhân Hòa. Qua file nhật ký máy chủ cho thấy địa chỉ chứa flash tấn công trang: kimduc.com là: yeuviet.info/maoi/index.html, người đăng ký tên miền này là Vũ Tiến Mạnh.

Ngoài trang web này, Vũ Tiến Mạnh còn có 1 số trang web như: www.nguoiyeuxua.cc, <http://vumanh.be>, <http://yeunhac.org>. Trang <http://vumanh.be> chứa liên kết đến các trang <http://www.vumanh.be/home> và <http://yeunhac.org>, còn trang www.nguoiyeuxua.cc sẽ tự động chuyển người truy cập đến trang <http://hlnyx.t35.com>. Như vậy Vũ Tiến Mạnh có 3 trang web có chứa nội dung là: <http://hlnyx.t35.com> , <http://www.vumanh.be/home>,

<http://yeunhac.org>. Những trang web này có cấu trúc và nội dung tương đối giống nhau, chủ yếu là âm nhạc và giải trí. Người sử dụng có thể truy cập những địa chỉ này và nghe nhạc miễn phí, vì vậy số lượng người truy cập là tương đối lớn. Phân tích cấu trúc của những trang web này cho thấy, tất cả đều chứa 1 đoạn mã để khi người sử dụng truy cập máy tính của họ. Sẽ tự động truy cập vào địa chỉ <http://yeuviet.info/maoi/index.html>, tải về và chạy 1 file flash mà người dùng không hề biết. File flash này sẽ tạo những truy cập hướng tới địa chỉ mà chủ nhân của nó đã định trước những địa chỉ tấn công này nằm trong nội dung của các file văn bản có tên là 1.txt, 2.txt, 3.txt, 4.txt, attack.txt và được đặt trên cùng máy chủ với file flash, đường dẫn đến những file này là: <http://yeuviet.info/maoi/>. Qua nội dung những file văn bản này cho thấy, mục tiêu tấn công không chỉ là trang web <http://kimduc.com> mà còn có 1 số địa chỉ khác như <http://www.mianlien.net/~kennyvan/HoangVu5.0/>. Như vậy người trực tiếp liên quan đến việc tấn công từ chối dịch vụ trang web <http://kimduc.com> là Vũ Tiến Mạnh. Mạnh sinh ngày 02/06/1986, địa chỉ tổ 23 phường Quán Triều, TP Thái Nguyên - Thái Nguyên.

2.2. Vụ tấn công website raovat.net và vietco.com

Đây là 2 website của công ty Việt Cơ bị Nguyễn Thành Công tấn công DDOS do có hình thức cá nhân với người quản lý website của công ty Việt Cơ: Công đã đặt 1 mã script có tên là netinfor lên trang web bongdem.net . Khi người sử dụng truy cập vào web này sẽ bị lây đoạn mã script đó và máy sẽ tự động đăng nhập vào website là mục tiêu tấn công với tốc độ theo yêu cầu (có thể từ 1-10 lần/giây) Với tốc độ như vậy website bị tấn công sẽ lâm vào tình trạng ngập lụt đường truyền, không ai có thể truy cập vào được, nếu quá tải lâu sẽ gây sập hệ thống. Công ty đã đặt lệnh tấn công 2 website raovat.net và vietco.com của công ty Việt Cơ trong 1 thời gian dài gây ảnh hưởng rất lớn đến hoạt động của Công ty. Cơ quan điều tra đã tìm được đoạn mã script này đang lưu trong thư mục C:\makeboot\netinfor ở máy tính cá nhân của Công. Ngoài ra vào khoảng tháng 12/2004, có 1 vài lần Trục thuê Công tấn công DDOS 1 số website về thẻ tín dụng. Trục đã trả cho Công hơn 10 triệu đồng vào tài khoản Vietcombank của Công.