|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  Description: Logo HvKTMM |
| **PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH**  **ĐỀ TÀI: DỊCH TÀI LIỆU WINDOWS FORENSICS ANALYSIS CHAPTER 8**  *Lớp:* **L02 - AT12** |
| *Giảng viên:* **Lại Minh Tuấn**  *Sinh viên thực hiện:*   1. Phạm Ngọc Sơn 2. Nguyễn Đình Hiếu |
| Hà Nội, 2019 |

**MỤC LỤC**

[GIỚI THIỆU 1](#_Toc25850683)

[I. Nghiên cứu trường hợp 2](#_Toc25850684)

[1.1. Nguồn của tài liệu 2](#_Toc25850685)

[1.2. Xâm nhập 3](#_Toc25850686)

[1.3. DFRWS 2008 Forensic Rodeo 6](#_Toc25850687)

[1.4. Nghiên cứu trường hợp 4: Sao chép các tập tin 6](#_Toc25850688)

[1.5. Thông tin mạng 9](#_Toc25850689)

[1.6. SQL Injection 10](#_Toc25850690)

[1.7. Ứng dụng đã làm điều đó 12](#_Toc25850691)

[II. Getting Started 16](#_Toc25850692)

[III. Documentation 18](#_Toc25850693)

[IV. Goals 21](#_Toc25850694)

[V. Checklists 22](#_Toc25850695)

[VI. Now What? 24](#_Toc25850696)

[VII. Extending Timeline Analysis 25](#_Toc25850697)

[VIII. Summary 27](#_Toc25850698)

[IX. Solutions Fast Track 27](#_Toc25850699)

**NHẬN XÉT CỦA GIẢNG VIÊN**

# 

# GIỚI THIỆU

Trong suốt cuốn sách cho đến nay, chúng tôi đã bao gồm rất nhiều thông tin kỹ thuật, nhưng trong mỗi trường hợp, thông tin đó rất cụ thể đối với một khu vực cụ thể của bộ nhớ Windows, the Registry, files, v.v. Tuy nhiên, hầu hết các phản ứng sự cố mà người phản hồi bắt buộc phải thực hiện hoặc phân tích pháp y máy tính mà người kiểm tra sẽ phải làm, liên quan đến nhiều hơn một trong những lĩnh vực này. Ví dụ: lưu lượng truy cập mạng đáng ngờ hoặc một quy trình đáng ngờ có thể dẫn đến một tệp trên hệ thống, điều này sẽ dẫn đến cơ chế lưu giữ lâu dài cho phần mềm độc hại, có thể là khóa Đăng ký. Hiểu mối quan hệ giữa các thành phần khác nhau này và có thể hiểu và nhận ra sự cần thiết phải đi từ cái này sang cái khác rất có thể có nghĩa là sự khác biệt giữa hiểu cách xảy ra sự cố và không hiểu làm thế nào nó xảy ra.

Kiểm tra pháp y không nên chỉ dựa vào phân tích hệ thống tệp, đặc biệt khi nhà phân tích đang kiểm tra hình ảnh thu được từ hệ thống Windows. Đơn giản là có quá nhiều thông tin có sẵn từ Cơ quan đăng ký, cũng như từ trong các tệp khác như Nhật ký sự kiện Windows, để một nhà phân tích chỉ dựa vào các quy trình và kỹ thuật kiểm tra cơ bản nhất.

Trong chương này, tôi trình bày các tình huống và các kỳ thi trước đây, hãy để chúng tôi gọi chúng là trường hợp nghiên cứu. đã sử dụng một số kỹ thuật được trình bày cho đến nay trong cuốn sách để đạt được mục tiêu của họ. Trong mỗi trường hợp, tôi sẽ cố gắng hoàn thiện về mặt kỹ thuật như tình huống cho phép, hiểu rằng nhiều chi tiết cụ thể cần phải được vệ sinh hoặc bỏ qua. Trong một số trường hợp nghiên cứu, thông tin có thể được rút ra từ một số sự cố hoặc kiểm tra, nhưng điểm chung vẫn giống nhau để chứng minh làm thế nào thông tin từ các chương khác nhau trong cuốn sách này có thể dẫn đến và tương quan với thông tin khác để xây dựng như một hình ảnh càng tốt của một sự cố.

# Nghiên cứu trường hợp

## Vết của tài liệu

Tôi đã nhận được một bài kiểm tra liên quan đến nhiều ổ đĩa cứng, mỗi ổ đĩa có một người dùng chính và được cài đặt hệ điều hành Windows XP SP2. Bối cảnh của sự cố chỉ đơn giản là hoạt động gian lận đã xảy ra đối với các tài khoản được duy trì bởi tổ chức khách hàng, và cuộc điều tra của họ về vấn đề này đã khiến họ nghi ngờ rằng sự gian lận này có thể là hành động của môt nhân viên.

Bước đầu tiên là cố gắng xác định những gì tôi đang tìm kiếm. Để làm điều đó, tôi đã liên lạc với khách hàng và xem qua các chi tiết điều tra của riêng họ về hoạt động liên quan. Và có vẻ như vấn đề từ quan điểm của họ tập trung vào chính các tài khoản và đặc biệt là các số được sử dụng để theo dõi các tài khoản. Nhận thông tin về các số tài khoản này khiến tôi khá nhanh chóng nhận ra rằng việc cố gắng tìm kiếm bất kỳ số nào khớp với cấu trúc của số tài khoản (sử dụng biểu thức chính quy Perl) sẽ rất khó khăn và có thể dẫn đến nhiều kết quả sai. Tôi cần một số cách để giảm lượng dữ liệu tôi sẽ phải xem lại.

Khách hàng đồng ý gửi cho tôi danh sách các số tài khoản mà họ đã xác định đã bị ảnh hưởng bởi gian lận. Sử dụng những con số đó làm danh sách từ khóa, tôi đã tìm kiếm trên mỗi hình ảnh thu được và tìm thấy lượt truy cập chỉ trong một hình ảnh, với hồ sơ người dùng cho một người dùng cụ thể. Trên thực tế, các lượt truy cập tìm kiếm được tập trung chủ yếu trong một tệp, theo một bài viết tôi đặt trong Cơ sở Kiến thức Microsoft, đã xuất hiện trong thư mục được Outlook sử dụng để lưu trữ các tệp được mở từ tệp đính kèm e-mail. Bước tiếp theo của tôi tại thời điểm đó là trích xuất một bản sao của tệp đó (một bảng tính) từ hình ảnh để phân tích. Mở bảng tính trên hệ thống phân tích của tôi, tôi có thể thấy nội dung nhưng tôi không biết nó đại diện cho cái gì, ngoài nó chứa thông tin tài khoản và đưa ra các lượt truy cập tôi nhận được từ tìm kiếm, các tài khoản tương quan với các hoạt động đáng ngờ đã được cam kết.

Vì tôi đã trích xuất các tệp hive Registry từ vị trí của chúng trong ảnh (xem Chương 4), tôi đã phân tích thông tin từ khóa Đăng ký Recent Recentocs của người dùng, cũng như khóa liệt kê bảng tính Excel mà người dùng đã mở. Tôi tìm thấy một tham chiếu tên tệp đến bảng tính từ thư mục lưu trữ tạm thời của Outlook (tệp Outlook.pst của người dùng không nằm trên hệ thống) cũng như các bảng tính khác, một trong số đó dường như được đặt trên máy chủ tệp, có thể trong thư mục tài liệu của người dùng (nhiều tổ chức có nhân viên của họ lưu trữ tài liệu trên một máy chủ tệp để họ có thể là một phần của quy trình sao lưu thông thường). Tôi đã có thể định vị các bảng tính khác dường như được tham chiếu và nằm trên hệ thống người dùng, và không có kết quả nào trong tìm kiếm của tôi được tìm thấy trong không gian chưa phân bổ, chỉ ra rằng các tệp chứa cụm từ tìm kiếm đã bị xóa gần đây.

Bước tiếp theo của tôi là trích xuất siêu dữ liệu từ bảng tính Excel. Các tài liệu Microsoft Office (tài liệu Word, bảng tính Excel và thậm chí các bản trình bày PowerPoint) sử dụng một bộ lưu trữ hỗn hợp, cấu trúc tập tin trong hệ thống tập tin trong hệ thống tập tin, lưu trữ dữ liệu. Như vậy, rất nhiều siêu dữ liệu có thể được (và được) lưu trữ trong cấu trúc tài liệu và có thể được trích xuất để phân tích và sử dụng. Sử dụng tập lệnh oledmp.pl Perl được tìm thấy trên phương tiện đi kèm với cuốn sách này, tôi có thể trích xuất siêu dữ liệu và thấy rằng người dùng trong câu hỏi đã mở, chỉnh sửa và in bảng tính. Các trường siêu dữ liệu trong bảng tính bao gồm ngày và giờ hiển thị khi các hành động này diễn ra và những ngày và thời gian này cũng tương quan với tem thời gian của hệ thống tệp và Đăng ký.

Khi tôi đã kéo tất cả các thông tin này lại với nhau thành một dòng thời gian dễ hiểu, tôi đã cung cấp nó trong một báo cáo cho khách hàng. Giống như nhiều nhà phân tích, tôi không thường thấy tầm quan trọng của việc tham gia vào quá trình báo cáo cuối cùng của tôi và đây là một ví dụ khác về tình huống đó. Tuy nhiên, cuộc kiểm tra này đã minh họa cách nhiều kỹ thuật phân tích có thể được sử dụng để thực sự đi sâu và có được nhiều thông tin về một sự cố. Trong trường hợp này, một tìm kiếm từ khóa cung cấp rất nhiều giảm dữ liệu và dẫn đến một tài liệu cụ thể, có vị trí trong hệ thống tệp tiết lộ nguồn tài liệu có khả năng (tệp đính kèm e-mail Outlook). Sau đó, phân tích Registry minh họa rằng người dùng đã truy cập tài liệu, cũng như các tài liệu khác có tiêu đề tương tự, ngoài thực tế là có ít nhất một trong số các tài liệu đó được đặt trên một máy chủ tệp. Cuối cùng, phân tích siêu dữ liệu được trích xuất từ tài liệu cho thấy rằng bất kỳ ai có quyền truy cập vào tài khoản người dùng đều đã sửa đổi và in tệp và đưa ra ngày của các hành động này. Điều này cung cấp rất nhiều thông tin cho khách hàng để hỗ trợ họ xác định nguồn gốc của hoạt động lừa đảo.

## Xâm nhập

Nghiên cứu trường hợp này liên quan đến sự xâm nhập vào cơ sở hạ tầng của công ty, mà sự nguy hại này đến từ hệ thống nhà của nhân viên. Loại sự cố này có lẽ phổ biến hơn người ta nghĩ. Các hệ thống người dùng gia đình, ngoài các hệ thống được sử dụng bởi người dùng thông thường (sinh viên sử dụng máy tính xách tay, hệ thống máy tính để bàn của nhân viên và máy tính xách tay, v.v.), thường rất dễ bị xâm phạm vì chúng được coi là mục tiêu dễ dàng; có rất nhiều người trong số họ ở ngoài đó (tức là, một môi trường giàu mục tiêu của người Hồi giáo) và phần lớn họ bị quản lý kém. Nhiều người dùng gia đình không nhận ra dữ liệu nào có giá trị thực sự trên hệ thống của họ. Người dùng gia đình làm ngân hàng trực tuyến và khai thuế mỗi năm từ các hệ thống máy tính đó. Các game thủ truy cập các trò chơi trực tuyến, và tin hay không, thực sự có một nền kinh tế để bán các nhân vật chơi game trực tuyến. Vì vậy, bên cạnh không gian ổ cứng, RAM và sức mạnh xử lý được thêm vào mạng botnet, các hệ thống máy tính gia đình có thể cung cấp khá nhiều kho báu cho kẻ đột nhập.

Điều đó đang được nói, trong trường hợp này, một kẻ xâm nhập đã truy cập vào hệ thống nhà của nhân viên và cài đặt một bộ ghi bàn phím (điều này sau đó đã được xác nhận thông qua phân tích riêng về hệ thống nhà của nhân viên). Từ đó, kẻ xâm nhập phát hiện ra rằng nhân viên đã đăng nhập vào cơ sở hạ tầng của công ty thông qua Windows Remote Desktop Client và vì anh ta đã bắt được các phím bấm của nhân viên, anh ta đã nhập tên người dùng và mật khẩu. Từ thời điểm đó, việc anh ta kích hoạt Remote Desktop Client của mình, khởi chạy nó theo đúng địa chỉ IP và cung cấp thông tin xác thực mới được phát hiện của anh ấy và anh ấy ở trên mạng công ty, xuất hiện với mọi mục đích và mục đích làm nhân viên

Hóa ra kẻ xâm nhập rất dễ theo dõi. Bằng cách truy cập cơ sở hạ tầng thông qua Remote Desktop Client, kẻ xâm nhập có quyền truy cập Shell-level (Shell là một môi trường trong đó chúng ta có thể chạy các lệnh, các chương trình và Shell script), nghĩa là hành động của anh ta khiến anh ta tương tác với trình Windows Explorer giống như một người dùng bình thường ngồi trên máy tính để bàn. Do đó, nhiều hành động của Kẻ xâm nhập đã được ghi lại thông qua Cơ quan đăng ký. Ngoài ra, kẻ xâm nhập có mức độ truy cập khá cao do thực tế là các thông tin bị đánh cắp là dành cho người dùng quản lý tài khoản người dùng. Mặc dù vậy, kẻ xâm nhập đã kích hoạt tài khoản quản trị viên tên miền không hoạt động, một tài khoản đã được thiết lập nhưng đơn giản là không bao giờ được sử dụng. Điều này có nghĩa là mỗi lần kẻ xâm nhập truy cập vào một hệ thống khác trong cơ sở hạ tầng của công ty, một hồ sơ cho tài khoản quản trị viên tên miền đã được tạo trên hệ thống đó. Điều này làm cho các hoạt động của kẻ xâm nhập trên khắp cơ sở hạ tầng khá dễ theo dõi, ít nhất là ban đầu (tức là, chúng tôi không muốn phạm sai lầm khi cho rằng đây là tất cả những gì kẻ xâm nhập đã làm).

Phối hợp chặt chẽ với nhân viên CNTT tại chỗ, chúng tôi đã tạo ra một tập lệnh sẽ tìm kiếm tất cả các hệ thống trong miền để tìm chỉ dẫn về hồ sơ người dùng đang đề cập. Trước tiên chúng tôi xác định các hệ thống mà hồ sơ tồn tại, cho chúng tôi một số lượng ban đầu các hệ thống mà kẻ xâm nhập đã truy cập. Sau khi có được từng cái, chúng tôi bắt đầu quá trình phát triển dòng thời gian hoạt động, sử dụng ngày tạo của thư mục hồ sơ làm chỉ báo về lần đầu tiên kẻ xâm nhập truy cập vào từng hệ thống và thời gian sửa đổi cuối cùng của tệp hive NTUSER.DAT Registry một dấu hiệu cho thấy khi kẻ xâm nhập lần cuối truy cập hệ thống. Những cửa sổ thời gian này sau đó đã được xác nhận khi chúng tôi kiểm tra nội dung của các phím UserAssist.

Khi chúng tôi đã lập bản đồ hành trình của kẻ xâm nhập qua mạng, bước tiếp theo là xác định kẻ xâm nhập đã làm gì hoặc cố gắng làm gì trên mỗi hệ thống. Một lần nữa, thực tế là kẻ xâm nhập đã truy cập vào từng hệ thống thông qua Windows Explorer đã cung cấp cho chúng tôi rất nhiều thông tin rất có giá trị. Khách hàng đặc biệt này đã dành rất nhiều thời gian và công sức để lập bản đồ dữ liệu nhạy cảm trong cơ sở hạ tầng của họ và có một danh sách nơi dữ liệu nhạy cảm này (như được định nghĩa bởi luật thông báo của tiểu bang như SB-1386 của California, cũng như Ngành Thẻ thanh toán Visa [PCI] Tiêu chuẩn bảo mật dữ liệu) đã tồn tại. Một lần nữa chuyển sang phân tích Registry, chúng tôi tập trung vào hồ sơ người dùng Tệp NTUSER.DAT, kiểm tra khóa RecentDocs, cũng như danh sách các tài liệu được truy cập gần đây như bảng tính Excel và tài liệu MSWord và bất kỳ dấu hiệu nào khác mà chúng tôi có thể tìm thấy. Chúng tôi có thể tập trung nỗ lực của mình bằng cách kiểm tra các khóa RecentDocs để xem loại tệp nào đã được truy cập (ví dụ: .xls, .doc, .jpg, v.v.) và sau đó kiểm tra danh sách (MRU) được sử dụng gần đây nhất cho các ứng dụng thường được sử dụng để truy cập vào các tập tin. Thật thú vị, không có nhiều tệp đã được truy cập, có lẽ một phần là do những gì chúng tôi tìm thấy trong khóa Đăng ký ACMru. Có vẻ như kẻ xâm nhập đã tiến hành tìm kiếm bằng cách nhấp vào Bắt đầu | Tìm kiếm | Đối với Tệp và Thư mục và đã cố gắng xác định các tệp có từ khóa nhất định. Điều này có thể đã không được nhân viên chú ý vì một số hệ thống được đặt trong trung tâm dữ liệu, nhưng thông tin mà kẻ xâm nhập đang tìm kiếm sử dụng từ khóa là một thứ gì đó mà tổ chức thực sự duy trì. Tuy nhiên, rõ ràng từ các chỉ dẫn trên một vài hệ thống mà kẻ xâm nhập đã tìm kiếm và tìm thấy một bảng tính có chứa mật khẩu, và các bước thích hợp đã được thực hiện để giải quyết thông tin bị xâm phạm này.

Một lần nữa, nhiều nguồn dữ liệu đã được sử dụng theo phản hồi và kiểm tra này. Nhật ký VPN đã được sử dụng để xác nhận quyền truy cập và xác định địa chỉ IP của kẻ xâm nhập, và sau đó phân tích thời gian của hệ thống tệp và MAC được sử dụng để xác nhận các chuyển động của kẻ xâm nhập trên toàn mạng. Cuối cùng, phân tích Registry đã cung cấp một bức tranh rõ ràng về các hành động của kẻ xâm nhập, bao gồm các tìm kiếm và truy cập tệp. Phân tích cuối cùng này được chứng minh là cực kỳ có giá trị trong việc xác định liệu kẻ xâm nhập có truy cập dữ liệu nhạy cảm hay không; phân tích đăng ký kỹ lưỡng cung cấp cho chúng tôi một lập luận mạnh mẽ rằng kẻ xâm nhập đã không truy cập các tệp đã được xác định trước đó để chứa dữ liệu nhạy cảm.

## DFRWS 2008 Forensic Rodeo

Vào tháng 8 năm 2008, Cory Altheide và tôi đã tham dự hội nghị DFRWS 2008. Chúng tôi đã có một thời gian tuyệt vời ở đó, và vào tối thứ ba, Cory đã tham gia vào Forensic Rodeo. Tôi không muốn tham gia nhiều nhưng tôi muốn quan sát, đứng sau theo dõi và xem cách họ tiếp cận nhiệm vụ. Ngồi trong văn phòng của mình, tôi thường tự mình thực hiện phân tích một số loại, vì thế tôi thường xuyên không có cơ hội quan sát như vậy, để không chỉ tham gia với người khác về công việc chúng tôi làm và những gánh nặng chúng tôi chia sẻ mà còn thực sự thấy được cách họ hành động. Nhìn lại, thật buồn cười khi nghe bản thân mình nói "…Hãy hành động", bởi vì sự thật được nói ra, có rất nhiều hành động trong phân tích pháp y cũng như khi xem tóc mọc. Tuy nhiên, nhìn chung, đây là một trải nghiệm rất mới mẻ giúp tôi giác ngộ, với lợi ích bổ sung là cho phép người khác thử sức mình với những thứ này. Đúng vậy, kịch bản pháp y và các tập tin pháp y có thể được tìm thấy tại www.dfrws.org/2008/rodeo.shtml.

Thử thách Forensic Rodeo liên quan đến kết xuất bộ nhớ (xem Chương 3) và hình ảnh thu được từ ổ ngón tay cái. Mục tiêu của thử thách là phân tích hai mẩu dữ liệu và trả lời một số câu hỏi được cung cấp bởi các trọng tài, Eoghan Casey và Dan Kalil. Tiến sĩ Michael Cohen đã giành chiến thắng trong cuộc đua, được đánh giá là đã hoàn thành nhiều câu hỏi được cung cấp hơn bất kỳ ai khác. Tôi không muốn cung cấp bất kỳ lời khuyên hoặc thông tin bên trong nào liên quan đến dữ liệu rodeo, nhưng tôi sẽ nói rằng theo đuổi rodeo liên quan đến phân tích bộ nhớ và ghi dữ liệu (lần này không có phân tích Registry!).

## Nghiên cứu trường hợp 4: Sao chép các tập tin

Một câu hỏi tôi thấy (và được hỏi) rất thường xuyên là liệu có thể xác định các tệp đã được sao chép vào một ổ USB hoặc thiết bị lưu trữ bên ngoài không. Tôi thấy câu hỏi này nhiều lần trong danh sách công khai, và khi tôi tham dự Hội nghị Pháp y SANS đầu tiên vào tháng 10 năm 2008, tôi đã được hỏi câu hỏi này từ hai người tham dự cũng như từ một trong những thành viên trong nhóm của tôi, người đang trả lời câu hỏi cho khách hàng. Cho đến ngày nay, các ổ USB phổ biến như thế nào, cũng như các phương tiện lưu trữ di động khác như máy ảnh kỹ thuật số, iPod, v.v., đây là một mối quan tâm rất thực tế đối với nhiều tổ chức liên quan đến việc lọc dữ liệu (ví dụ như đánh cắp dữ liệu như sở hữu trí tuệ, v.v.). Thật không may, quá thường xuyên nó là một mối quan tâm sau khi sự việc đã xảy ra chứ không phải là một cái gì đó được giải quyết (phòng tránh) một cách chủ động.

Như chúng ta đã thấy trong Chương 4 và 5, các thiết bị lưu trữ di động USB có thể được theo dõi trên các hệ thống. Sử dụng các kỹ thuật phân tích từ cả hai chương, chúng ta có thể xác định không chỉ khi thiết bị được cắm lần đầu tiên vào hệ thống mà cả khi thiết bị được ngắt kết nối lần cuối khỏi hệ thống. Đây có thể là thông tin rất hữu ích khi ánh xạ kết nối các thiết bị lưu trữ di động với một hệ thống hoặc trên một số hệ thống. Điều này cũng cho chúng ta một cái gì đó để bắt đầu một timeline.

Bây giờ, một trong những vấn đề liên quan đến câu hỏi ban đầu là hầu hết các hệ điều hành hiện đại (và tôi nói là hầu hết các đơn giản vì tôi đã thấy tất cả) không kiểm tra hoặc ghi nhật ký các hoạt động sao chép hoặc di chuyển trong hệ thống tệp. Tuy nhiên, nhiều người dường như nghĩ rằng vì phân tích pháp y có thể phục hồi các tệp đã bị xóa, nên các loại phép thuật khác cũng có thể được thực hiện cũng như ma thuật, chẳng hạn như xác định ai đã sao chép tệp từ vị trí này sang vị trí khác và khi họ thực hiện việc này. Trái ngược với các chương trình truyền hình nổi tiếng như CSI, điều này chỉ đơn giản là không phù hợp với hầu hết các trường hợp. Nếu nhà phân tích có cả hai phần của phương tiện truyền thông, thì nguồn và ổ đĩa đích hoặc ổ đĩa cho bản sao chép thì họ có thể xác định bằng cách phân tích các tệp trên cả hai phần của phương tiện (và dấu thời gian của họ) nguồn và đó là đích đến. Tuy nhiên, trong hầu hết các trường hợp, nhà phân tích không có cả hai phương tiện truyền thông.

Chỉ có một phần phương tiện để kiểm tra có thể không cho phép nhà phân tích xác định dứt điểm các tệp được sao chép từ phương tiện đó, nhưng nhà phân tích có thể xác định các chỉ dẫn của các tệp có thể được sao chép vào phương tiện, sử dụng thông tin được cung cấp trong Microsoft Knowledge Bài viết cơ bản 299648, có tiêu đề là Mô tả về mô tả ngày và thời gian của NTFS cho các tệp và thư mục tên (http://support.microsoft.com/?kbid=299648). Bài viết Cơ sở Kiến thức này cung cấp một mô tả rõ ràng về thời gian tập tin bị ảnh hưởng bởi việc sao chép hoặc di chuyển từ phương tiện này sang phương tiện khác. Ví dụ: nếu một tệp được sao chép từ phân vùng FAT (hầu hết các ổ USB được định dạng theo hệ thống tệp FAT theo mặc định) sang phân vùng NTFS, ngày sửa đổi cuối cùng của tệp vẫn không thay đổi, nhưng ngày tạo tệp được cập nhật đến thời điểm hiện tại trên hệ thống. Điều tương tự cũng đúng nếu tệp được sao chép từ thư mục NTFS sang thư mục con NTFS. Tuy nhiên, nếu tệp được di chuyển (chứ không phải sao chép), ngày tạo tệp của tập tin được cập nhật thành ngày của tệp ở vị trí ban đầu. Theo bài báo, trong tất cả các ví dụ, ngày và giờ sửa đổi của tệp không thay đổi trừ khi thuộc tính của tệp đã thay đổi. Ngày và giờ đã tạo của tệp thay đổi tùy thuộc vào việc tệp được sao chép hoặc di chuyển.

Tuy nhiên, như một lời cảnh báo, bài viết Cơ sở Kiến thức (Knowledge Base) không mô tả phương pháp được sử dụng để di chuyển tệp. Ví dụ, hãy xem xét các dòng lệnh sau đây Di chuyển các lệnh Lệnh, trong đó một tệp được sao chép từ thiết bị lưu trữ di động có định dạng FAT (E: \) sang thư mục NTFS:

C:\test>dir /tc E:\Dec03\_0004.jpg

Volume in drive E has no label.

Volume Serial Number is 18DA-DF72

Directory of E:\

12/03/2008 09:59 PM 7,250 Dec03\_0004.jpg

1 File(s) 7,250 bytes 0 Dir(s) 72,757,248 bytes free

C:\test>move E:\Dec03\_0004.jpg

C:\test>dir /tc Dec03\_0004.jpg

Volume in drive C has no label.

Volume Serial Number is B83C-BC0A

Directory of C:\test

12/05/2008 09:36 AM 7,250 Dec03\_0004.jpg

1 File(s) 7,250 bytes 0 Dir(s) 11,019,108,352 bytes free

Như bạn có thể thấy trong ví dụ này, ngày tạo của tệp không giữ nguyên sau khi thao tác di chuyển diễn ra, trái với những gì được nêu trong bài viết Cơ sở tri thức (Knowledge Base) Microsoft 299648. Điều này minh họa rõ ràng sự cần thiết phải kiểm tra và kiểm tra công cụ và kỹ thuật.

Điều này chỉ ra một số yếu tố quan trọng liên quan đến phân tích của chúng tôi, trong đó đầu tiên là nếu người dùng sao chép một tệp và sau đó sửa đổi tệp theo cách nào đó, chúng tôi đã mất thông tin có thể chỉ ra một tệp được sao chép từ vị trí này sang vị trí khác; cụ thể, một tệp có ngày sửa đổi cũ hơn ngày tạo có thể chỉ ra rằng tệp đã được sao chép. Hãy xem xét câu nói đó trong một khoảnh khắc. Nên một tập tin phải được tạo trước và sau đó, tại một thời điểm nào đó sau khi nó được tạo, sửa đổi? Theo mặc định, MS Word sẽ tự động lưu một bản sao của tệp bạn đang chỉnh sửa khoảng 10 phút một lần, do đó, sau 10 phút đầu tiên, bạn sẽ có ngày tạo cũ hơn 10 phút so với ngày sửa đổi (tất nhiên là trong trường hợp lý tưởng ). Một yếu tố khác cần xem xét là chỉ với một phần phương tiện để phân tích, bạn có thể không xác định được một cách dứt khoát các tệp đã được di chuyển từ vị trí này sang vị trí khác chỉ vì thời gian tệp được cập nhật so với thời gian ban đầu tệp (giả sử tùy chọn menu Cắt & Dán được sử dụng thay vì lệnh di chuyển tại CLI).

Cuối cùng, mặc dù thời gian tệp được liên kết với hệ thống tệp bị ảnh hưởng bởi thao tác sao chép hoặc di chuyển, thời gian được nhúng trong nội dung của tệp (chẳng hạn như nội dung OLE trong một số phiên bản của tài liệu MS Office, như được thảo luận trong Chương 5) vì siêu dữ liệu sẽ không được sửa đổi và do đó có thể được sử dụng trong một số mô-đun phân tích. Tùy thuộc vào loại tài liệu và mức độ siêu dữ liệu được duy trì trong tài liệu, bạn có thể xác định rõ ràng rằng tài liệu có nguồn gốc từ một vị trí khác bên cạnh phương tiện được phân tích.

Phân tích một hình ảnh thu được trong một nỗ lực để xác định các tệp có thể đã được sao chép vào hệ thống có thể liên quan đến phân tích Registry cũng như phân tích thời gian của hệ thống tệp và MAC. Trong một số trường hợp, tùy thuộc vào loại tài liệu được sao chép, phân tích siêu dữ liệu tệp có thể làm sáng tỏ tình huống.

## Thông tin mạng

Đôi khi trong các hoạt động phát hiện hoặc phản hồi sự cố, khi nhân viên vận hành mạng có thể truy cập vào nhật ký tường lửa từ bộ lọc đi ra, hoặc để lưu lượng truy cập mạng hiển thị lưu lượng truy cập (và có thể là dữ liệu) rời khỏi cơ sở hạ tầng bên trong. Bất kể nguồn nào (nhật ký hoặc lưu lượng truy cập), ai đó sẽ có quyền truy cập vào dữ liệu hiển thị rõ ràng địa chỉ IP nguồn của lưu lượng (vì nó bắt nguồn từ bên trong cơ sở hạ tầng mạng), có thể được bắt nguồn từ một hệ thống hoạt động trên mạng nội bộ , thông qua việc truy tìm hệ thống thông qua địa chỉ IP tĩnh, không thay đổi hoặc thông qua nhật ký DHCP. Một thông tin khác, cổng nguồn của lưu lượng truy cập (một phần của tiêu đề TCP hoặc UDP), sẽ giúp bạn gắn lưu lượng truy cập bên ngoài đó vào một quy trình đang chạy trên hệ thống.

Trước khi tiếp tục với mô tả này, một thực tế quan trọng cần được chỉ ra và hiểu: Không có gì xảy ra trên hệ thống máy tính mà không có quá trình thực thi. Chính xác hơn, các luồng là lượng tử thực thi trên các hệ thống Windows, nhưng thực tế là để lưu lượng được tạo từ một hệ thống, phải có một số mã thực thi trên hệ thống để tạo ra bất kỳ lưu lượng mạng nào. Trong trường hợp đó, một phản ứng tức thì đối với việc phát hiện ra các chi tiết lưu lượng mạng (ví dụ: địa chỉ IP nguồn và cổng) sẽ tự cho mình một thuật ngữ Tôi nghe Aaron Walters sử dụng khoảng cách tạm thời của Em. y, thuật ngữ này đề cập đến việc trả lời ngay lập tức và tương đối gần với thời điểm phát hiện sự cố, trái với thời gian chờ đợi hoặc thậm chí vài ngày để phản hồi. Bằng cách quan sát sự gần gũi tạm thời đối với sự cố, người phản hồi sẽ có nhiều khả năng thu thập dữ liệu tươi hơn (và có lẽ đầy đủ hơn); đầu ra của netstat.exe (hoặc các kết nối mạng hiển thị trong kết xuất bộ nhớ) vẫn có thể hiển thị các dấu hiệu của kết nối đầu ra đó và chuyển phản hồi đến quá trình mà lưu lượng truy cập bắt nguồn. Ví dụ, trên hệ thống thử nghiệm của tôi, dòng lệnh netstat hèano trả về mục sau đây, một đoạn trích về đầu ra của lệnh:

TCP 192.168.1.5:8352 98.136.112.141:80 ESTABLISHED 3536

Đoạn trích này về đầu ra của lệnh netstat minh họa địa chỉ IP nguồn và cổng được sử dụng bởi quy trình với mã số 3536, trong trường hợp này là firefox.exe. Thông tin tương tự này sẽ được hiển thị rõ ràng trong một lưu lượng truy cập mạng (như được mô tả trước đây) hoặc có thể hiển thị trong nhật ký tường lửa hoặc nhật ký được duy trì bởi các thiết bị mạng khác. Biết cách chuyển đổi suôn sẻ từ thu thập và phân tích dữ liệu dựa trên máy chủ có thể giảm đáng kể thời gian cần thiết để xác định và ứng phó với sự cố. Trong tình huống như vậy, nhật ký thiết bị có thể tương quan với lưu lượng truy cập mạng và dữ liệu dựa trên máy chủ (nghĩa là kết xuất bộ nhớ) để xác định khối lượng và loại dữ liệu rời khỏi mạng.

## SQL Injection

Trong nửa cuối năm 2007, một số cuộc tấn công SQL Injection đã xảy ra và khi nhiều tuần và tháng trôi qua, chúng dường như tăng không chỉ về tần suất mà cả về độ tinh vi. SQL Injection là một kỹ thuật tận dụng điểm yếu trong lớp ứng dụng giữa máy chủ Web và hệ thống cơ sở dữ liệu. Kẻ xâm nhập sẽ gửi các câu truy vấn đặc biệt được tạo thủ công đến máy chủ Web, các truy vấn đó sẽ vào cơ sở dữ liệu mà không có xác nhận đầu vào của người dùng, không kiểm tra giới hạn, v.v. Đổi lại, cơ sở dữ liệu sẽ xử lý các lệnh đó cho kẻ xâm nhập (xem Chương 5).

Vào đầu mùa xuân năm 2008, đã có rất nhiều sự chú ý của truyền thông đối với một kiểu tấn công SQL Injection, trong đó phần mềm tự động đưa các liên kết được chế tạo đặc biệt vào JavaScript, cơ sở dữ liệu và các liên kết đó sẽ được xử lý bởi trình duyệt Web của người dùng, khi cơ sở dữ liệu cung cấp các liên kết đó trở lại máy chủ Web dưới dạng nội dung Web động. Kiểu tấn công này nhận được sự chú ý của truyền thông vì nó rất dễ thấy, trong khi các cuộc tấn công không được nói đến công khai là những cuộc tấn công mà kẻ xâm nhập đã sử dụng SQL Injection để vào sâu trong cơ sở hạ tầng của mục tiêu và trong nhiều trường hợp, vẫn nằm trên mạng với các đặc quyền cực kỳ cao trong một khoảng thời gian đáng kể.

Cơ sở của cuộc tấn công SQL Injection lợi dụng thiết kế cơ sở hạ tầng âm thanh trong đó máy chủ Web được công bố rộng rãi bố trí trong “khu phi quân sự” hoặc DMZ phần của cơ sở hạ tầng, và cơ sở dữ liệu nằm trên cơ sở hạ tầng nội bộ. Các lệnh của kẻ xâm nhập sẽ được máy chủ Web nhận và chuyển đến máy chủ cơ sở dữ liệu, hoàn toàn bỏ qua tường lửa (vì giao tiếp giữa Web và máy chủ cơ sở dữ liệu là một yêu cầu nghiệp vụ). Từ góc độ phản ứng sự cố, các lệnh của Kẻ xâm nhập có thể thấy rõ trong nhật ký máy chủ Web ở định dạng ASCII, ban đầu không có mã hóa đặc biệt. Trích xuất nhật ký, một người phản hồi có thể thấy rõ liên hệ ban đầu, kiểm tra lỗ hổng, trinh sát vào mạng (các lệnh do kẻ xâm nhập như ipconfig / all và net view), và thậm chí phân nhánh ra các hệ thống khác. Lúc nào đó, kẻ xâm nhập sẽ tạo được chỗ đứng trên các hệ thống mà họ (kẻ xâm nhập) có quyền truy cập bằng cách tải phần mềm xuống các hệ thống đó. Ban đầu, điều này sẽ được thực hiện thông qua việc sử dụng máy khách TFTP bằng giao thức UDP để tải tệp xuống hệ thống. Sau đó, việc tạo và thực thi các tập lệnh FTP (nghĩa là tạo ra các tập lệnh bằng cách sử dụng lệnh “echo” và sau đó khởi động chúng bằng ftp -s: filename) để tải phần mềm xuống nền tảng. Có vẻ như trong một số trường hợp, các tài liệu lưu trữ được tải xuống là các tệp thực thi tự giải nén vì nhật ký máy chủ Web cho thấy kẻ xâm nhập khởi chạy tệp download.exe và sau đó kiểm tra (thông qua thư mục) các tệp kết quả hoặc chỉ đơn giản là chạy các lệnh.

Trong quá trình xử lý sự cố, một số mẫu đã được thu thập các tệp thực thi được tải xuống hệ thống. Lúc đầu, các mẫu này không được phát hiện bởi các máy quét chống vi-rút hoặc được xác định khi gửi đến các trang web như VirusTotal.com. Khi mùa đông trôi qua, các hoạt động ứng phó sự cố tiếp tục bao gồm các cuộc tấn công SQL Injection đang gia tăng độ tinh vi. Trong một vài tháng ngắn ngủi, các thuật ngữ tìm kiếm được sử dụng để xác định các cuộc tấn công SQL Injection trong nhật ký máy chủ Web là vô ích vì những kẻ tấn công đã sử dụng các kỹ thuật mới để mã hóa (mã hóa thập lục phân hoặc, trong một số trường hợp, mã hóa ký tự) các lệnh của chúng. Do đó, các tiêu chí tìm kiếm cần được cập nhật để phát hiện các cuộc tấn công. Một phương pháp để làm điều này là xác định trang đang được yêu cầu và sau đó tìm kiếm các yêu cầu dài bất thường đang được gửi đến trang đó. Việc thêm các từ khóa mới được phát hiện vào tiêu chí tìm kiếm đã giúp thu hẹp các kết quả dương tính giả và các tập lệnh Perl tùy chỉnh đã giúp giải mã nhanh các truy vấn thành định dạng có thể đọc được. Một kỹ thuật khác mà kẻ tấn công sử dụng để lấy mã thực thi trên hệ thống là chia một tệp thực thi thành các đoạn 512 byte và gửi từng đoạn trong một chuỗi được đánh số vào các trường cơ sở dữ liệu (hãy nhớ, thông qua SQL Injection, kẻ tấn công đang thực thi các lệnh trên cơ sở dữ liệu ở cùng cấp đặc quyền với cơ sở dữ liệu, mà đối với MS SQL Server thường là Hệ thống), sau đó tập hợp lại và thực thi mã trong hệ thống tệp của máy chủ cơ sở dữ liệu. Trong các trường hợp sử dụng kỹ thuật này, chúng tôi có thể trích xuất và lắp lại mã thực thi từ nhật ký máy chủ Web và sau đó xác thực rằng chúng tôi có tệp thực thi được định dạng chính xác bằng cách phân tích tiêu đề PE (xem Chương 6). Nếu chúng tôi có các tệp thực thi có tên tương tự trong kho lưu trữ của chúng tôi từ các cuộc tấn công SQL Injection trước đó, chúng tôi đã sử dụng ssdeep.exe của Jesse Kornblum (http://ssdeep.sourceforge.net/) để thực hiện so sánh băm mờ và, trong hầu hết các trường hợp, xác định rằng các tệp là 98 phần trăm hoặc 99 phần trăm tương tự. Phân tích tiêu đề PE để chia tệp thực thi thành các phần cho phép chúng tôi xác định các phần đã thay đổi (thông qua so sánh băm MD5) từ các phiên bản trước của tệp.

Khi phản ứng với các cuộc tấn công SQL Injection, các kỹ thuật theo dõi kẻ tấn công trong cơ sở hạ tầng bao gồm phân tích Registry vì kẻ tấn công có thể tương tác với trình Windows Explorer của các hệ thống bị xâm nhập. Trong một số trường hợp, tài khoản quản trị tập thể (hoặc chung) đã bị xâm phạm (nghĩa là mật khẩu dễ đoán), nhưng trong hầu hết các trường hợp, kẻ tấn công sẽ tạo tài khoản người dùng cấp quản trị viên tên miền (trong một số trường hợp, sự tồn tại của tài khoản đã bị chứng thực bởi Sự kiện Các mục nhật ký hiển thị việc tạo tài khoản) và sau đó sử dụng các tài khoản đó để truy cập các hệ thống khác trong cơ sở hạ tầng. Phân tích hệ thống tệp minh họa việc tạo hồ sơ người dùng trên các hệ thống và đưa ra mốc thời gian ban đầu cho việc sử dụng các tài khoản đó, trong khi phân tích Registry cung cấp chỉ dẫn về hoạt động của kẻ tấn công trên các hệ thống đó, cũng như việc sử dụng các cơ chế kiên trì được sử dụng bởi kẻ tấn công phần mềm độc hại được thêm vào hệ thống bị xâm nhập. Do máy chủ Web không bị xâm phạm trong cuộc tấn công SQL Injection, nên nhật ký máy chủ Web đã cung cấp một bức tranh rõ ràng về các hoạt động ban đầu của kẻ tấn công (trong một số trường hợp, các tàu thăm dò trinh sát đã đạt được vài tuần hoặc vài tháng) để truy cập vào cơ sở hạ tầng. Phân tích tệp hoặc phần mềm độc hại cung cấp các dấu hiệu cho thấy các công cụ tương tự (nâng cao hơn) đang được sử dụng theo thời gian.

## Ứng dụng đã làm điều đó

Cách đây không lâu, tôi đã thực hiện một số phản ứng sự cố có thể phải làm với một số hoạt động độc hại. Như một trường hợp thường xuyên là một nhà tư vấn doanh nghiệp, cuộc gọi ban đầu của tôi liên quan đến sự cố đến từ khách hàng và một yếu tố phổ biến trong số hầu hết các khách hàng của tôi là họ không có kinh nghiệm ứng phó sự cố. Trong trường hợp này, vấn đề liên quan đến việc tra cứu tên miền lặp đi lặp lại đối với các tên miền nghi ngờ của Hồi giáo, nghi ngờ theo nghĩa là có ít nhất một trong các tên miền xuất hiện ở Trung Quốc. Khách hàng đã lấy tên miền và nhận thấy rằng nó có liên quan đến lỗ hổng ứng dụng được xác định vào mùa xuân năm 2008. Với điều đó, và một số ít khác, họ đã gọi cho chúng tôi.

Khi đến nơi, tôi thấy rằng một hệ thống cụ thể đã được xác định là điểm khởi đầu của ít nhất một số lưu lượng DNS đáng ngờ. Hệ thống này rõ ràng đã được cấu hình với một địa chỉ IP tĩnh (trái ngược với việc sử dụng DHCP), do đó khách hàng có thể dễ dàng theo dõi và lấy được từ nhân viên của họ. Thật không may, các bước duy nhất được thực hiện là tắt hệ thống và xóa nó khỏi mạng; không phải nội dung của bộ nhớ vật lý hay dữ liệu dễ bay hơi khác được thu thập từ hệ thống trước khi tắt nó. Một sơ xuất đã xảy ra là khi nhân viên được thông báo rằng có lưu lượng đáng ngờ bắt nguồn từ hệ thống của anh ta và hệ thống sẽ phải được kiểm tra, anh ta đã tuyên bố rằng anh ta sẽ xóa một cách an toàn từ hệ thống. Tại thời điểm này, các mục tiêu kiểm tra của tôi có hai mặt: (1) xác định xem trên thực tế, nhân viên có cài đặt và sử dụng tiện ích xóa an toàn hay không và (2) xác định nguồn gốc của việc tra cứu DNS đáng ngờ.

Bước đầu tiên của tôi là có được một hình ảnh của ổ cứng máy tính để bàn của nhân viên. Trong khi điều này đang diễn ra, tôi đã cố gắng thu thập thông tin về bất kỳ nhật ký nào có thể có sẵn từ mạng. Tôi đã được thông báo rằng một báo cáo quản lý minh họa việc tra cứu DNS thường xuyên nhất đã cảnh báo họ về tình huống này và có một số nhật ký từ một thiết bị phát hiện botnet minh họa một số tra cứu DNS; tuy nhiên, sự vắng mặt đáng chú ý là bất kỳ tham chiếu nào đến tên miền Trung Quốc vốn là mối quan tâm hàng đầu của khách hàng trong suốt cuộc gọi để được giúp đỡ. Tôi nhận thấy rằng các bản ghi mạng đã hiển thị tra cứu DNS theo thứ tự bảng chữ cái, cùng với dấu thời gian.

Khi việc thu thập hình ảnh ổ cứng đã hoàn tất và được xác minh, và tôi đã đảm bảo rằng tất cả các tài liệu của mình đều được sắp xếp theo thứ tự, tôi mở ghi chú trường hợp của mình, gắn hình ảnh thu được dưới dạng hệ thống tệp chỉ đọc trên máy tính xách tay phân tích của tôi và bắt đầu quét với một ứng dụng quét chống vi-rút. Là một phần trong quá trình giảm dữ liệu của tôi và cố gắng xác định vị trí mô tả vô định của một thứ gì đó đáng nghi ngờ, tôi đã quét hình ảnh được gắn với một số ứng dụng chống vi-rút, bao gồm cả kính hiển vi được nhắm mục tiêu để tìm phần mềm độc hại cụ thể. Quá trình quét của tôi đã phát hiện ra một số tệp có thể là phần mềm độc hại hoặc phần còn lại của phần mềm độc hại, nhưng siêu dữ liệu tệp (thời gian MAC) và nội dung dường như cho thấy đây là những thông tin sai. Bước tiếp theo của tôi là kiểm tra nhật ký từ hệ thống, bao gồm nhật ký ứng dụng chống vi-rút đã cài đặt và nhật ký Công cụ loại bỏ phần mềm độc hại MS (mrt.log, như đã thảo luận trong Chương 5). Không chỉ ra bất cứ điều gì có vẻ liên quan đến vấn đề trong tay.

Sau đó tôi chuyển sang phân tích Nhật ký sự kiện Windows. Tất cả ba Nhật ký sự kiện từ hệ thống đều có kích thước 512 kilobyte và Nhật ký sự kiện bảo mật không chứa hồ sơ (tôi đã tìm thấy qua phân tích tệp trung tâm đăng ký bảo mật mà kiểm toán chưa được kích hoạt). Nhật ký sự kiện ứng dụng đã tiết lộ một số bản ghi sự kiện do ứng dụng chống vi-rút tạo ra, nhưng quan trọng nhất, Nhật ký sự kiện hệ thống cho thấy hệ thống đã được khởi động lại nhiều lần trong hai tuần qua. Trong mỗi trường hợp, sau bản ghi sự kiện đã tuyên bố rằng dịch vụ Nhật ký sự kiện đã bắt đầu, có một bản ghi khác nói rằng một ứng dụng chống phần mềm cụ thể đã bắt đầu. Tôi đã ghi chú về điều này và tạo ra một bản đồ minh họa thời gian bắt đầu hệ thống gần đúng dựa trên các bản ghi sự kiện này. Tôi đã có thể tương quan thời gian bắt đầu hệ thống với một số nhật ký thiết bị botnet mà khách hàng đã cung cấp; ba nhật ký hoàn chỉnh nhất (chúng thực sự được trích xuất từ nhật ký thiết bị, minh họa hoạt động chỉ liên quan đến hệ thống được đề cập) cho thấy việc tra cứu DNS bắt đầu trong tương quan gần như trực tiếp với hệ thống khởi động. Trên thực tế, mục nhập đầu tiên trong mỗi bản ghi tương quan rất chặt chẽ với thời gian ứng dụng chống phần mềm độc hại bắt đầu. Tuy nhiên, một lần nữa, nhật ký thiết bị botnet không có tham chiếu đến miền Trung Quốc đáng ngờ.

Sau đó, tôi đã thực hiện một tìm kiếm trên toàn bộ hình ảnh cho tên miền Trung Quốc đáng ngờ, tạo ra một mạng lưới rộng rãi và hoàn toàn mong đợi để xem kết quả duy nhất trong tệp trang. Tuy nhiên, thật ngạc nhiên, tôi đã tìm thấy một số tài liệu tham khảo về tên miền (cũng như các tài liệu khác) trong một số tệp hive của Registry (đáng chú ý nhất là tệp NTUSER.DAT cho tất cả người dùng, cũng như những người được tìm thấy trong Hệ thống Windows XP Khôi phục điểm), cũng như trong tệp máy chủ (tầm quan trọng của tệp máy chủ liên quan đến độ phân giải tên được thảo luận tại http: // support. Microsoft.com/kb/172218). Kiểm tra tệp máy chủ cho thấy rằng một công cụ chống phần mềm độc hại đã được cài đặt trên hệ thống đã thêm một số mục vào tệp (nhận xét trong tệp máy chủ cho biết rằng các mục được thêm bởi ứng dụng), chuyển hướng tất cả chúng vào localhost (ví dụ: 127.0.0.1), hiệu quả của Blackholing, những nỗ lực để kết nối với các miền này. Việc kiểm tra các tệp hive của Registry cho thấy vào cùng một ngày (dựa trên khóa LastWrite), tất cả các tên miền giống nhau, theo cùng một thứ tự, cũng đã được thêm vào các khóa Registry, buộc các tên miền vào Internet Explorer (IE) Khu vực bị hạn chế. Nhóm Điều này đặt hiệu quả các hạn chế đối với những gì người dùng có thể thực hiện thông qua Internet Explorer, nếu họ có thể kết nối với máy chủ trong các miền đó.

Tại thời điểm này, tôi đã tương đối chắc chắn rằng, dựa trên tất cả thông tin tôi có được cũng như một số tìm kiếm trên Internet, hoạt động đáng ngờ không phải là kết quả của phần mềm độc hại (vi rút, sâu hoặc phần mềm gián điệp) trên hệ thống mà là sự tương tác của hai ứng dụng antispyware; nghĩa là, một người đã sửa đổi Sổ đăng ký và tệp máy chủ để bảo vệ hệ thống và các truy vấn DNS được thực hiện khác cho mỗi tên miền được tìm thấy được liệt kê trong tệp máy chủ. Một bài đăng trên một diễn đàn Internet chỉ ra rằng đây có thể là trường hợp và tôi đã làm việc với khách hàng để thực hiện kiểm tra trực tiếp hệ thống trên mạng để xác minh thông tin này. Chúng tôi đã khởi động hệ thống, vô hiệu hóa các dịch vụ ứng dụng chống phần mềm độc hại và khởi động lại, kích hoạt lại các dịch vụ và khởi động lại, thậm chí sửa đổi tệp máy chủ để chứa các mục cụ thể và khởi động lại. Mỗi lần, chúng tôi thấy lưu lượng DNS trên mạng (thông qua trình thám thính trên một hệ thống riêng trên cùng một mạng con), như chúng tôi mong đợi; trong trường hợp khởi động lại hệ thống với các dịch vụ ứng dụng chống phần mềm độc hại bị vô hiệu hóa, chúng tôi không thấy có truy vấn tên miền DNS nào cả.

Cuối cùng, cả phân tích Registry cũng như phân tích nội dung của thư mục Prefetch đều cung cấp bất kỳ dấu hiệu nào cho thấy nhân viên đã cài đặt tiện ích xóa tệp an toàn trên hệ thống, chứ đừng nói đến việc chạy một phương tiện từ phương tiện lưu độn g.

Sử dụng một phương pháp điều tra toàn diện và tương quan nhiều nguồn dữ liệu, chứng thực cho phép chúng tôi xác định nguồn gốc của hoạt động đáng ngờ và có khả năng độc hại. Trong phản hồi ban đầu, khách hàng chỉ thu thập được một lượng dữ liệu hạn chế và sau đó dựa trên giả định về hoạt động độc hại không gì khác hơn là tìm kiếm Google cho một tên miền. Việc thiếu dữ liệu thích hợp (ví dụ, chụp toàn bộ mạng, dữ liệu nhật ký mạng toàn diện hơn, bộ nhớ vật lý hoặc một phần dữ liệu dễ bay hơi từ hệ thống nghi ngờ, v.v.) dẫn đến việc kiểm tra mất nhiều thời gian hơn, do đó dẫn đến chi phí cao hơn khách hàng. Cuối cùng, thử nghiệm trực tiếp hệ thống, đã khởi động trên mạng, cho phép chúng tôi xác nhận rằng hoạt động đó là kết quả của một ứng dụng hợp pháp (thực tế là hai tương tác) và các truy vấn tên miền DNS không được theo sau bởi các nỗ lực kết nối với máy chủ trong các miền đó thông qua UDP hoặc TCP.

# Getting Started

Một câu hỏi tôi thấy trong các diễn đàn công cộng khá thường xuyên là, Làm thế nào để bạn bắt đầu kiểm tra? Đưa ra một tập hợp các dữ liệu hình ảnh trong bộ dữ liệu thu được từ nhiều hệ thống, chụp gói, tập tin nhật ký, v.v., trên đó, nơi một người kiểm tra bắt đầu bài kiểm tra của mình? Làm thế nào để bạn bắt đầu?

Câu trả lời hấp dẫn, viên đạn bạc (ý nói là cách để giải quyết vấn đề hoặc chấm dứt được thắc mắc) mà tôi đã học được trong sáu tháng huấn luyện tại Trường cơ bản ở Quantico, Virginia (nơi tất cả các sĩ quan hải quân được đào tạo ban đầu), là, “it depends”. tốt bởi vì đó là sự thật. Hãy để nói rằng bạn có một hình ảnh thu được từ một hệ thống duy nhất. Hệ điều hành đang chạy hoặc có sẵn tại thời điểm hình ảnh được thu thập là gì? Nền tảng là gì? Nó đã được ghi nhận? Bạn có thể hỏi tại sao điều này lại quan trọng, nhưng hãy xem các công cụ của bạn và xem công cụ nào có khả năng xử lý hệ thống tập tin nào. Là hình ảnh của một hệ thống Linux? Nếu vậy, hệ thống tệp trong hình ảnh ext2, ext3 hoặc ReiserFS?

Được rồi, được rồi, tôi biết rằng đây là một cuốn sách về phân tích pháp y của Windows. Nhưng tôi hy vọng bạn nhìn thấy quan điểm của tôi. Khi bắt đầu kiểm tra, có một số điều mà người kiểm tra có thể cần phải tính đến. Một trong những điều của người Viking là hệ thống tệp: Bạn có công cụ phù hợp để mở và xem lại hình ảnh thu được không? Tuy nhiên, quan trọng hơn, người kiểm tra phải xem xét mục tiêu của mình: Cô ấy hy vọng đạt được gì từ việc kiểm tra? Những gì cần phải đạt được thông qua việc kiểm tra các dữ liệu có sẵn? Hãy xem tôi dễ dàng quay lại xung quanh để đến với nó như thế nào?

Bước quan trọng nhất để bắt đầu một cuộc kiểm tra là hiểu các mục tiêu của kỳ kiểm tra đó. Bất kể môi trường mà bạn tham gia, bất kỳ sự kiểm tra nào cũng sẽ có lý do hoặc mục đích. Nếu bạn thực thi pháp luật, bạn đang tìm kiếm cái gì? Bạn đang cố gắng xác định thông tin về một đứa trẻ mất tích hoặc xác định xem chủ sở hữu hệ thống có buôn bán hình ảnh bất hợp pháp không? Nếu bạn là chuyên gia tư vấn, trước khi bắt đầu kiểm tra, bạn đã gặp khách hàng và thảo luận kỹ lưỡng về những gì họ hy vọng đạt được hoặc đạt được thông qua kiểm tra của bạn. Ngay cả khi bạn phản ứng lại sự cố, khi di chuyển ứng phó với sự cố, bạn cần hiểu những gì bạn phải đạt được sau hành động của mình trước khi thực hiện chúng. Nếu bạn đang phản ứng với việc nhiễm phần mềm độc hại, bạn có đang cố xác định các phần mềm độc hại và có thể lấy một bản sao của mã phần mềm độc hại để cung cấp cho nhà cung cấp phần mềm chống vi-rút của bạn không? Bạn đang phản ứng với việc chấm dứt lưu lượng truy cập bất thường tại một hệ thống trên cơ sở hạ tầng nội bộ của bạn? Các mục tiêu kiểm tra hoặc phản ứng của bạn thúc đẩy hành động của bạn.

* **Tool & Trap: Các mục tiêu của ứng phó sự cố**

Là một người phản ứng sự cố, một trong những điều mà tôi đã nhận thấy là trên thực tế, nhiều lần, thông tin phản hồi ban đầu của những người phản hồi đầu tiên tại chỗ có thể khiến tổ chức gặp rủi ro lớn hơn chính sự cố.

Bây giờ, tôi nhận ra rằng bạn có thể đọc và đọc lại câu cuối cùng đó và cố gắng hiểu ý nghĩa của nó. Rốt cuộc, điều đó không chính xác trực quan, phải không? Vâng, những gì tôi đã thấy là trong nhiều trường hợp, những người phản hồi đầu tiên là nhân viên CNTT, và các hoạt động và quy trình trả lời của họ rất tập trung vào CNTT. Rất thường xuyên, các nhân viên CNTT được giao nhiệm vụ (bởi quản lý cấp cao) với việc giữ cho các hệ thống máy chủ e-mail, truy cập Internet, v.v., trên mạng và hoạt động như nhiệm vụ chính của họ. Vì vậy, nếu phần mềm độc hại được phát hiện trên một hệ thống, các mục tiêu của nhân viên CNTT là loại bỏ nó và đưa hệ thống bị ảnh hưởng trở lại hoạt động nhanh nhất có thể. Điều này có thể có nghĩa là làm sạch hệ thống bằng cách xóa phần mềm độc hại hoặc xóa tất cả dữ liệu khỏi hệ thống và cài đặt lại mọi thứ (hệ điều hành, dữ liệu, v.v.) khỏi phương tiện sạch hoặc sao lưu hoặc có thể có nghĩa là thay thế h ếu tố quan trọng nhất đóng vai trò trong tất cả những điều này đến từ các cơ quan quản lý. Tiểu bang California bắt đầu với SB-1386, một luật yêu cầu thông báo cho bất kỳ cư dân California nào nếu thông tin nhận dạng cá nhân của họ (được xác định kỹ lưỡng và được ghi lại trong văn bản luật) bị lộ do vi phạm hoặc xâm nhập. Theo văn bản này, một số tiểu bang khác có luật tương tự, và một luật liên bang có thể đang trên đường. Thêm vào đó là các tiêu chuẩn tuân thủ Visa PCI, cũng như HIPAA, SEC và các cơ quan quản lý khác, và bạn đã có khá nhiều kích thích bên ngoài để có kế hoạch phản hồi tốt, vững chắc. Trong nhiều trường hợp, các cơ quan quản lý yêu cầu một kế hoạch phản ứng phải được ghi lại và xem xét để tuân thủ. Mặt trái của đồng tiền, chi phí của việc không có kế hoạch phản hồi tốt, vững chắc đó có thể bao gồm tiền phạt cũng như cả chi phí cứng và mềm của thông báo và phơi bày công khai về việc vi phạm và lộ dữ liệu nhạy cảm toàn hệ thống.

Cách tốt nhất để giải thích làm thế nào hai mẩu thông tin này khớp với nhau là với một ví dụ. Một công ty bị tấn công bởi phần mềm độc hại thông qua trình duyệt tạo ra và dành thời gian để dọn dẹp khoảng hai chục hệ thống bị nhiễm. Trong quá trình trả lời, họ tìm thấy một số dấu hiệu cho thấy phần mềm độc hại có thể bao gồm thành phần logger gõ phím hoặc thành phần mạng, mặc dù không có gì chắc chắn được xác định (hãy nhớ rằng, các hệ thống đã được làm sạch, không có phân tích nguyên nhân gốc nào được thực hiện hoặc ghi lại) . Khi tư vấn pháp lý của công ty nghe về điều này, sau khi tất cả các hệ thống đã được dọn sạch và đưa trở lại dịch vụ, câu hỏi sau đó trở thành, trên hệ thống có bất kỳ dữ liệu nhạy cảm nào bị nhiễm nào bị lộ không? Làm thế nào để nhân viên CNTT trả lời câu hỏi đó? Rốt cuộc, mục tiêu của họ là làm sạch các hệ thống và đưa chúng trở lại hoạt động để duy trì hoạt động kinh doanh. Không có dữ liệu nào được thu thập để xác định xem có bất kỳ dữ liệu nhạy cảm nào không, thông tin nhận dạng cá nhân của anh ấy như tên, địa chỉ và số An sinh xã hội hoặc các dữ liệu khác như số thẻ tín dụng đã có trên các hệ thống đó hoặc đã bị xâm phạm do phần mềm độc hại nhiễm trùng.

Trường hợp vấn đề rủi ro xảy ra là một số cơ quan quản lý tuyên bố rằng nếu bạn không thể xác định chắc chắn rằng dữ liệu không bị lộ theo bất kỳ cách nào, thì bạn phải thông báo trên toàn bộ phạm vi của dữ liệu được bật hoặc có thể truy cập được bằng cách đó hệ thống. Nói một cách đơn giản, nếu bạn không thể chứng minh rằng dữ liệu nhạy cảm không bị lộ, thì bạn phải thông báo cho mọi người rằng dữ liệu của họ có thể đã bị lộ. Điều này cho thấy rõ rằng phản ứng sự cố không còn là một quy trình CNTT: Đây là một quy trình kinh doanh tổng thể liên quan đến tư vấn pháp lý, nguồn nhân lực, quan hệ công chúng và truyền thông, và thậm chí cả quản lý điều hành.

# Documentation

Chìa khóa cho bất kỳ sự kiểm tra hoặc phân tích nào mà bạn thực hiện sẽ là tài liệu của bạn. Tài liệu phải được lưu giữ theo cách mà cho phép bạn hoặc người khác xem (kiểm tra) lại tài liệu vào một ngày nào đó (ví dụ: sáu tháng, một năm hoặc lâu hơn) và hiểu hoặc thậm chí xác minh kết quả kiểm tra. Điều này có nghĩa là tài liệu của bạn phải rõ ràng và súc tích, và nó phải đủ chi tiết để thể hiện rõ ràng về những gì bạn đã làm, những gì bạn tìm thấy và cách bạn diễn giải những phát hiện của bạn.

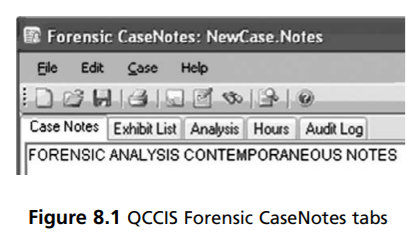
Tài liệu có thể được lưu giữ trong bất kỳ phương tiện nào có sẵn. Không cần phải định vị hoặc mua một ứng dụng đặc biệt lưu tài liệu của bạn ở định dạng độc quyền. Trên thực tế, có lẽ bạn không muốn làm điều này vì bạn có thể không sử dụng ứng dụng này trong một năm hoặc ai đó cần xem lại tài liệu của bạn có thể không có ứng dụng đó. Một cái gì đó đơn giản như một tài liệu văn bản sẽ đủ, nhưng nếu có quyền truy cập vào định dạng có khả năng mở được trong một trình xử lý văn bản như Microsoft Word có thể được mong muốn hơn. Ví dụ: với trình xử lý văn bản, bạn có thể nhúng các liên kết và hình ảnh vào tài liệu, bao gồm những thứ như sơ đồ pin-out ổ cứng, chụp màn hình và thậm chí liên kết đến hướng dẫn tháo gỡ máy tính xách tay (rất hữu ích khi được cung cấp máy tính xách tay mà bạn cần tháo rời để có quyền truy cập vào ổ cứng). Ngoài ra, nhiều định dạng tài liệu của trình xử lý văn bản (nghĩa là MS Word và Adobe PDF) có thể được xem và truy cập từ một số nền tảng, vì vậy định dạng này có phần phổ biến. Ngay cả trên các hệ thống Linux (và Windows), OpenOffice (www.openoffice.org/) cung cấp quyền truy cập vào các tài liệu định dạng MS Word và có sẵn miễn phí. Một điều rất hữu ích khác cần ghi nhớ về định dạng tài liệu của bạn là định dạng báo cáo của bạn. Sử dụng cùng một trình xử lý cho cả hai cho phép bạn giữ các ghi chú trường hợp của mình và sau đó, khi bạn đã sẵn sàng, hãy cắt và dán các mục trực tiếp vào báo cáo của bạn. Rốt cuộc, khi báo cáo, bạn có thể không cần mức độ chi tiết được tìm thấy trong ghi chú trường hợp của bạn, nhưng thông tin đó có thể dễ dàng được chuyển đến báo cáo của bạn và được sửa đổi một cách thích hợp.

Vì vậy, những gì bạn nên ghi lại? Là một nhà tư vấn, một trong những mục tôi cần theo dõi là giờ sẽ được lập hóa đơn cho khách hàng, cho công việc được thực hiện trong một kỳ thi. Trong một số trường hợp, tôi có thể là nhà phân tích cao cấp về một cam kết và sẽ theo dõi không chỉ giờ của các nhà phân tích khác mà còn cả các nhiệm vụ được cung cấp cho họ và phản hồi, phát hiện và đầu vào của họ. Điều này có thể cực kỳ đơn giản, sử dụng định dạng bảng, đồng thời rất hiệu quả và dễ hiểu. Ghi lại thông tin này trong ghi chú trường hợp của tôi, cùng với phân tích của tôi, cho phép tôi hiển thị thời gian đã sử dụng nên tôi cần phải chứng minh thông tin này vào một ngày sau đó. Đồng thời, thông tin tương tự được nhập vào ứng dụng thanh toán trực tiếp từ trường hợp của tôi ghi chú, không nên có sự khác biệt giữa hai thông tin. Điều này cho phép tôi giảm thiểu sai lầm, đặc biệt trong lĩnh vực kiểm tra cực kỳ quan trọng này.

Một mục khác mà tôi có xu hướng theo dõi trong tài liệu của mình là những dữ liệu mà tôi có quyền truy cập để kiểm tra và cũng là phương tiện truyền thông cho dữ liệu này trên, đó là, ổ cứng ngoài USB, ổ cứng trong, CD hoặc DVD, v.v. . Tôi theo dõi thông tin này theo một số sê-ri mục Mặt hàng để tôi có thể dễ dàng tham khảo lại mục phù hợp trong suốt quá trình kiểm tra.

Một công cụ hữu ích để theo dõi các ghi chú trường hợp của tôi là ứng dụng Forensic CaseNotes từ QCC Information Security ([www.qccis.com/?section=casenotes](http://www.qccis.com/?section=casenotes)).

Hình 8.1 minh họa các tab tôi đã thiết lập để nắm bắt tất cả các thông tin được thảo luận trước đó.



Bất kể ứng dụng nào mà bạn chọn để duy trì ghi chú trường hợp của bạn thì chúng đều nên có thể truy cập và súc tích, và chúng phải minh họa rõ ràng cho các hoạt động và kết quả phân tích của bạn, đến mức mà các hoạt động đó có thể được xác minh và xác nhận, nếu cần.

* **Tools & Traps: Hỗ trợ phân tích của bạn**

Một điều tôi muốn đưa vào ghi chú trường hợp của tôi trong khi kiểm tra là bất kỳ tài liệu nào hỗ trợ cho lý luận của tôi. Có những lúc tôi có thể thêm ghi chú dựa trên việc kiểm tra một lý thuyết, nhưng tôi cũng có một nền tảng học thuật, và một trong những điều tôi học được khi viết luận văn thạc sĩ của tôi là tôi phải hỗ trợ những gì tôi đã nói trong luận án. Đó là một vấn đề đơn giản để đưa ra tuyên bố vì bạn biết điều gì đó, nhưng bao gồm các tuyên bố tương tự được thực hiện bởi những người khác làm tăng thêm độ tin cậy cho phân tích của bạn. Một nguồn tuyệt vời cho loại tài liệu hỗ trợ này khi phân tích các hệ thống Windows là Cơ sở tri thức Microsoft. Nhiều lần tìm kiếm chính Cơ sở tri thức Microsoft, hoặc thậm chí Google, sẽ cung cấp cho bạn các liên kết đến thông tin có giá trị có thể trả lời câu hỏi của bạn và hỗ trợ phân tích của bạn. Trong các trường hợp khác, bạn có thể truy cập các bài viết của Cơ sở tri thức Microsoft bằng cách của một trang web khác, chẳng hạn như Eventid.net.

Một trong những bài viết trong Cơ sở Kiến thức mà tôi sử dụng khá thường xuyên cho mục đích này là http: // support.microsoft.com/?kbid=299648, có tiêu đề là Mô tả về tem ngày và giờ của Ntfs cho các tệp và thư mục. thời gian bị ảnh hưởng bởi các hoạt động sao chép và di chuyển giữa và trong các hệ thống tệp (cụ thể là FAT và NTFS). Các bài viết khác của Cơ sở Kiến thức mô tả Mã trạng thái máy chủ Web (IIS) của MS Internet Information Server trong nhật ký máy chủ Web, cách các tệp được lưu trữ trong Thùng rác trên Windows XP và 2003, v.v. Có một số bài viết trong Cơ sở Kiến thức có thể cung cấp hỗ trợ và độ tin cậy cho phân tích của bạn và có thể dễ dàng được tham khảo trong các ghi chú trường hợp cũng như các báo cáo của bạn.

# Goals

Cách đây rất lâu, tôi đã thảo luận về một cuộc kiểm tra được thực hiện bởi một nhà phân tích khác từ một tổ chức khác với một thành viên của nhân viên an ninh trong công ty chúng tôi. Nhà phân tích tư vấn đã định vị SubSeven Trojan được cài đặt trong hình ảnh thu được, là một phần của các dịch vụ được ký hợp đồng (tức là, để xác định xem phần mềm độc hại có được cài đặt trên hệ thống không); tuy nhiên, như đồng nghiệp của tôi đã chỉ ra, chuyên gia tư vấn không xác định phân vùng DOS ẩn. Tại sao? Bởi vì đó không phải là mục tiêu của việc kiểm tra. Khi tôi nói chuyện với chuyên gia tư vấn, cô ấy nói rằng cô ấy thực sự đã chú ý đến phân vùng ẩn khi chuẩn bị kiểm tra hình ảnh, và cô ấy thậm chí còn ghi chú nó trong ghi chú kiểm tra của mình. Tuy nhiên, đó không phải là một trong những câu hỏi cần được trả lời liên quan đến hợp đồng, không phù hợp với kỳ kiểm tra, và do đó không được trình bày trong báo cáo cuối cùng.

Điều này rất quan trọng đối với tất cả các giám khảo cần nhớ, bất kể bạn là nhà tư vấn hay làm việc cho cơ quan thực thi pháp luật. Có thể rơi vào một tinh huống khó khăn là không bao giờ kết thúc (Nguyên văn là “rabbit hole : lỗ thỏ” ý là luôn có thể xảy ra tinh huống khó khăn, phức tạp), tìm kiếm hoạt động đáng ngờ của Hồi giáo và không bao giờ thực sự kết thúc, nếu bạn không có (và tuân thủ) các mục tiêu được xác định rõ ràng cho bài kiểm tra của bạn.

Biết những gì bạn nên hoặc cần phải tìm kiếm cũng cung cấp cho bạn một điểm khởi đầu thuận lợi trong phân tích của bạn. Vấn đề là nhiễm một phần mềm độc hại, hoặc một sự xâm nhập? Là mục tiêu của việc kiểm tra để xác định gian lận hoặc vi phạm chính sách sử dụng được chấp nhận bởi người dùng? Hiểu những gì bạn nên tìm kiếm giúp xác định nơi bắt đầu tìm kiếm.

Một người bạn của tôi đã từng nói với tôi về một báo cáo mà anh ấy đã xem xét về sự cố phần mềm độc hại. Sau khi thu thập dữ liệu và hoàn thành kiểm tra, Người kiểm tra đã viết một báo cáo, bao gồm một luận án kỹ lưỡng về khả năng của phần mềm độc hại đã diễn ra trong khoảng hai chục trang. Cuối báo cáo, bạn tôi nói rằng anh ta phải hỏi người kiểm tra xem phần mềm độc hại này có thực sự được tìm thấy trong hệ thống thu được không? Rốt cuộc, câu hỏi mà khách hàng trả cho họ để trả lời, và trong một báo cáo kéo dài gần ba chục trang, không có tuyên bố rõ ràng nào về việc phần mềm độc hại có được tìm thấy trong hình ảnh thu được hay không.

Phân tích pháp y kỹ thuật số có thể là một đề xuất đắt tiền, và các mục tiêu cần phải được xác định rõ ràng tại điểm bắt đầu. Một nhà phân tích có thể dành nhiều thời gian để kiểm tra một hình ảnh thu được cho hoạt động độc hại và một nhóm người trả lời có thể dành nhiều thời gian hơn để xem qua vô số hệ thống trong cơ sở hạ tầng nếu hướng dẫn duy nhất của họ là tìm thấy tất cả những thứ xấu. Mục tiêu được xác định rõ ràng giúp tập trung vào phương pháp phân tích, hướng dẫn xây dựng kế hoạch phản hồi hoặc phân tích, cũng như xác định điểm cuối của kỳ thi. Mục tiêu phân tích cần được phát triển, hiểu và ghi chép rõ ràng.

# Checklists

Một cách tuyệt vời để bắt đầu với phân tích là với danh sách kiểm tra. Danh sách kiểm tra phác thảo những điều chúng ta cần làm và một danh sách kiểm tra tốt thường sẽ chứa nhiều mục hơn chúng ta cần, vì nó được dự định là toàn diện, và yêu cầu chúng ta chứng minh và xác thực, thông qua quy trình suy nghĩ hợp lý, lý do của chúng ta bỏ qua các mục trong danh sách kiểm tra, hoặc không thực hiện các bước nhất định.

Một ví dụ về danh sách kiểm tra sẽ là ghi lại thông tin về từng hình ảnh mà bạn đang phân tích. Ví dụ: bạn có thể muốn ghi lại tên hệ thống, thời gian tắt máy cuối cùng và các thông tin cơ bản khác được trích xuất từ hình ảnh có thể phù hợp với bài kiểm tra của bạn. Một số cài đặt, chẳng hạn như việc cập nhật lần truy cập gần nhất đã bị vô hiệu hóa hay nếu hệ thống được đặt để bỏ qua Thùng rác khi tệp bị xóa hoặc nếu tệp trang được đặt thành bị xóa khi tắt máy, có thể có tác động đáng kể đến phần còn lại phân tích của bạn.

Một ví dụ khác về danh sách kiểm tra có thể bao gồm các bước bạn sẽ thực hiện nếu phần mềm độc hại bị nghi ngờ có trên hệ thống. Điều này có thể đơn giản như gắn hình ảnh với SmartMount và quét hệ thống tệp bằng một ứng dụng chống vi-rút duy nhất hoặc có thể toàn diện hơn, bao gồm một số ứng dụng chống vi-rút và phần mềm chống phần mềm (với các phiên bản của chúng được ghi lại) cũng như một số bước khác ( xem Chương 5) bao gồm để càng kỹ càng tốt. Điều này cũng có thể bao gồm khởi động hình ảnh với LiveView và thực hiện quét tìm rootkit. Nói chung, khi tôi thực hiện quét chống vi-rút hình ảnh thu được, điều đầu tiên tôi làm là nhìn vào bên trong hình ảnh để xác định xem đã có sản phẩm chống vi-rút được cài đặt chưa, và nếu vậy, nhà cung cấp và phiên bản ứng dụng. Từ đó, tôi có thể xem lại nhật ký ứng dụng để xem liệu phần mềm độc hại có thể được phát hiện hay không và nếu có, ứng dụng đã thực hiện những hành động nào (cách ly, cố gắng cách ly nhưng không thành công, v.v.). Ngoài ra, tôi thường kiểm tra Nhật ký sự kiện để xác định xem có bất kỳ thông báo nào được đăng ở đó không, chẳng hạn như phần mềm độc hại được phát hiện hoặc ứng dụng chống vi-rút bị dừng bất thường (một chiến thuật được chứng minh bằng tài liệu của một số phần mềm độc hại). Ngoài ra, còn có tệp mrt.log (xem Chương 5), sẽ cung cấp cho tôi một số chỉ dẫn về các cơ chế bảo vệ được đặt trên hệ thống trong Cập nhật Windows.

Tuy nhiên, ngắn gọn hoặc mở rộng danh sách kiểm tra, nó nên bao gồm đủ tài liệu để cho phép một nhà phân tích khác sao chép và xác minh các bước của bạn, nếu cần.

Danh sách kiểm tra không nhằm mục đích từng bước, cách kiểm tra hộp thực hiện phân tích. Danh sách kiểm tra nên được coi là bắt đầu một kỳ thi, một cách để đảm bảo rằng các nhiệm vụ cụ thể được hoàn thành (hoặc ít nhất là được ghi lại về lý do tại sao họ đã hoàn thành), thay vì được coi là toàn bộ bài kiểm tra. Danh sách kiểm tra nào cho phép bạn làm là đảm bảo rằng bạn đã bao quát tất cả hoặc hầu hết các cơ sở của mình và cho phép bạn sao chép các bước cần được sao chép qua mỗi lần kiểm tra mà không phải lo lắng về việc quên một bước. Giống như các ứng dụng và tiện ích phân tích của bạn, danh sách kiểm tra là công cụ mà bạn có thể sử dụng để lợi thế của mình. Danh sách kiểm tra là một quá trình và bằng cách có một quy trình, bạn cũng có thứ gì đó bạn có thể cải thiện (ngược lại, nếu bạn không nhớ những gì bạn đã làm trong lần kiểm tra trước, bạn có thể cải thiện như thế nào?).

Một danh sách kiểm tra mẫu có tiêu đề Phân tích sự cố Checklist.doc có thể được tìm thấy trên phương tiện đi kèm với cuốn sách này. Danh sách kiểm tra mẫu chỉ đơn giản là một tài liệu Word có chứa một số trường giống nhau được xác định bởi các tab hiển thị trong Hình 8.1. Danh sách kiểm tra cung cấp một số trường cơ bản để xác định sự cố và người kiểm tra, cũng như ngày bắt đầu và ngày kết thúc phân tích xảy ra. Ngoài ra còn có các bảng để xác định các mục cần phân tích (hình ảnh thu được, lưu lượng truy cập mạng, tệp nhật ký, v.v.), cũng như các hộp kiểm xác định một số mục tiêu cơ bản và các bước phân tích có thể được sử dụng. Phần này có thể bao gồm các mục là một phần của quy trình xử lý tiêu chuẩn của tổ chức của bạn, chẳng hạn như nhận dạng hệ điều hành hình ảnh thu được, bất kỳ tài khoản người dùng nào trên hệ thống, trích xuất dữ liệu từ Cơ quan đăng ký, quét phần mềm độc hại, v.v. Mặc dù bản thân danh sách kiểm tra chỉ có một trang, nhưng các trang bổ sung có thể được thêm vào khi người kiểm tra tiến hành phân tích và kết quả có thể được ghi trực tiếp vào danh sách kiểm tra. Một lần nữa, danh sách kiểm tra này chỉ phục vụ như một mẫu và một ví dụ, và có thể được mở rộng hoặc sửa đổi để đáp ứng nhu cầu cụ thể của bạn.

* **Tools & Traps: Which Version of Windows?**

Thông thường khi làm việc với phản hồi sự cố trực tiếp hoặc thậm chí kiểm tra hình ảnh thu được, tôi sẽ muốn biết phiên bản Windows nào tôi đang làm việc. Từ những gì tôi thấy trên các diễn đàn công cộng, thường thì đây không phải là mối quan tâm của người trả lời hoặc người kiểm tra, nhưng đã tiến hành hoặc hỗ trợ một số lượng lớn các phản hồi trực tiếp và tham gia phân tích pháp y, điều mà một số người coi là sắc thái tinh tế giữa các phiên bản Windows thực sự có thể là sự khác biệt khá đáng kể. Từ Chương 3, chúng ta biết rằng các cấu trúc nhân chính (nghĩa là cấu trúc EProcess và EThread) được tìm thấy trong bộ nhớ không chỉ thay đổi giữa các phiên bản Windows mà còn có thể thay đổi giữa các gói dịch vụ trong cùng một phiên bản! Từ góc độ phân tích pháp y, có những tạo tác có sẵn trên một số phiên bản Windows không có sẵn trên các phiên bản khác; một ví dụ đáng chú ý là Điểm khôi phục hệ thống được tìm thấy trên Windows XP nhưng không có trên Windows 2000 hoặc Windows 2003.

Có lẽ phương pháp nổi tiếng nhất để xác định phiên bản hệ điều hành (HĐH) nào của Windows mà bạn đang làm việc là kiểm tra nội dung của một số khóa Registry. Trong khóa Microsoft \ Windows NT \ CurrentVersion trong tổ hợp Phần mềm, bạn sẽ tìm thấy các giá trị như CSDVersion, BuildLab và ProductID có thể được sử dụng để xác định phiên bản Windows. Bài viết Cơ sở tri thức của Microsoft 189249 (http://support.microsoft.com/kb/189249) cung cấp thông tin để xác định phiên bản cho hệ thống trực tiếp và nó cũng cung cấp chỉ dẫn về cách thực hiện tương tự trong khi kiểm tra.

Một cách khác để xác định phiên bản HĐH là định vị tệp ntoskrnl.exe trong thư mục system32 và phân tích thông tin phiên bản tệp từ tệp thực thi đó. Điều này cũng sẽ hoạt động với các tệp như cmd.exe và winver.exe (lưu ý rằng trên hệ thống trực tiếp, chạy winver.exe tại dấu nhắc lệnh sẽ mở hộp thoại Giới thiệu về Windows hiển thị một số thông tin cơ bản về HĐH, bao gồm cả phiên bản và dung lượng bộ nhớ vật lý).

Cuối cùng, nếu bạn đang làm việc với một phiên bản Windows XP và cần xác định xem đó là phiên bản Home hay Professional, hãy tìm prodspec.ini trong thư mục system32 và tìm kiếm (bạn có thể phải cuộn xuống) the “[Product Specification]” entry. On my system, I see “Product=Windows XP Professional”.

Khi nói đến nó, việc biết phiên bản Windows mà bạn đang kiểm tra có thể hướng dẫn bạn về những đồ tạo tác cần tìm, nơi để tìm và cả những thứ không nên có. Tất cả những điều này có thể có một tác động đáng kể đến những phát hiện của bạn.

# Now What?

Bây giờ bạn đã có tài liệu bắt đầu của mình, bạn đã hiểu mục tiêu của mình và bạn có một danh sách kiểm tra, thì sao? Chuyện gì xảy ra tiếp theo? Vâng, đây là nơi bạn bắt đầu phân tích thực tế của bạn. Giả sử bạn đang phân tích hình ảnh thu được từ hệ thống Windows và sau khi ghi lại tài liệu mua lại, hệ điều hành và bất kỳ tài khoản người dùng nào trên hệ thống, bạn có một số hoạt động phân tích khác mà bạn cần thực hiện như một phần của trường hợp tiêu chuẩn của mình xử lý, chẳng hạn như tìm kiếm từ khóa và quét phần mềm độc hại. Nếu danh sách từ khóa tương đối ngắn, hãy đưa vào danh sách từ khóa trực tiếp trong tài liệu phân tích của bạn và chạy tìm kiếm. Hoặc, xác định lý do tại sao tìm kiếm không được chạy, nếu bạn chọn không làm như vậy. Tương tự, xác định ứng dụng (hoặc ứng dụng) được sử dụng trong quá trình quét phần mềm độc hại của bạn hoặc nêu rõ lý do tại sao quá trình quét không được tiến hành.

Tìm kiếm danh sách kiểm tra phân tích pháp y kỹ thuật số của Google, Google xác định một loạt các phương pháp tiếp cận được sử dụng cho các danh sách này. Một số bao gồm phân tích chữ ký tệp, nhận dạng hình ảnh đồ họa (bao gồm cả phim và hình ảnh tĩnh), phân tích hoạt động của trình duyệt Web, phân tích cú pháp của Recycl Bin và các phím tắt Windows (.lnk), v.v. Tất cả những điều này có thể quan trọng đối với bài kiểm tra của bạn hoặc đơn giản là một phần trong quy trình xử lý tình huống tiêu chuẩn của tổ chức của bạn. Dù bằng cách nào, các hoạt động phân tích của bạn nên được ghi chép lại một cách kỹ lưỡng và chính xác, đặc biệt là nếu bạn đang đi ra khỏi kịch bản, và theo đuổi một dòng phân tích nằm ngoài định mức (một số người có thể gọi đây là một linh cảm vụng trộm). Ghi lại những linh cảm của bạn sẽ mở rộng kiến thức cũng như khả năng quay trở lại vào một ngày sau đó và xem những gì bạn đã làm để bạn có thể sao chép các hoạt động đó khi cần thiết.

# Extending Timeline Analysis

Như đã thảo luận trong Chương 5, thông tin dòng thời gian mà nhà phân tích thu được do sử dụng fls và mactime.pl được phân lập thành chỉ các tệp và thư mục trong hình ảnh thu được và không xem xét các sự kiện hoặc tạo tác khác trong hình ảnh thu được cũng chứa thông tin đóng dấu thời gian. Một phần để giải quyết vấn đề này, Michael Cloppert đã viết một công cụ có tên ex-Tip, có sẵn trên Sourceforge (http://sourceforge.net/projects/ex-tip/). Ngoài ra, bài viết về Michael phát triển và sử dụng Ex-Tip có sẵn từ Sans

(https://www2.sans.org/reading\_room/whitepapers/forensics/32767.php). Ex-Tip lấy các nguồn dữ liệu được đóng dấu thời gian bổ sung, chẳng hạn như các khóa Registry và nội dung của nhật ký quét ứng dụng chống vi-rút, xem xét, phân tích và chuẩn hóa chúng thành định dạng thời gian chung (thời gian Unix) và trình bày chúng theo một cách khác , mặc dù định dạng dựa trên văn bản.

Các công cụ và tiện ích như RegRipper (được thảo luận ở Chương 4) có thể cung cấp chức năng bổ sung để trích xuất các giá trị được đóng dấu thời gian từ các tệp hive của Registry. Trong khi mô-đun được cung cấp với Ex-Tip trích xuất tất cả các khóa và thời gian LastWrite của chúng từ tệp hive, RegRipper sử dụng phương pháp phẫu thuật nhiều hơn và chỉ có thể cung cấp các khóa quan tâm, cung cấp một mô-đun giảm dữ liệu (để không áp đảo nhà phân tích với các điểm dữ liệu), cũng như cung cấp ngữ cảnh cho dữ liệu được truy xuất. Ví dụ, như được thảo luận trong Chương 4, khóa RecentDocs và các khóa con của nó đều chứa danh sách MRU và tệp được truy cập gần đây nhất được xác định tương đối dễ dàng trong giá trị MRUList (hoặc MRUListEx). Do đó, các plugin RegRipper có thể cung cấp không chỉ thời gian LastWrite từ khóa mà còn cả tên của tệp được truy cập gần đây nhất. Hơn nữa, các giá trị Sổ đăng ký, chẳng hạn như các giá trị trong khóa UserAssist chứa dữ liệu được đóng dấu thời gian và có thể được trích xuất bằng plugin thích hợp và sau đó được tích hợp vào tệp cơ thể theo định dạng thích hợp.

Các tệp khác cũng có thể được phân tích cú pháp cho dữ liệu được đóng dấu thời gian. Ví dụ, như được thảo luận trong Chương 5, Nhật ký sự kiện Windows chứa dấu thời gian khi mỗi bản ghi sự kiện được tạo và viết. Các tệp Rp.log từ bên trong Điểm khôi phục hệ thống Windows XP chứa thông tin về không chỉ khi điểm khôi phục được tạo mà còn cả lý do (điểm kiểm tra hệ thống, cài đặt trình điều khiển, v.v.) để tạo điểm khôi phục. Thông tin này thêm ngữ cảnh vào dữ liệu có sẵn và sau đó có thể tương quan với thông tin có được từ đầu ra của fls.exe. Ngoài ra còn có các tệp nhật ký chống vi-rút và một số tệp khác có sẵn chứa thông tin có thể (và có lẽ nên) được đưa vào phân tích dòng thời gian. Một nguồn thông tin bổ sung có thể bao gồm các sự kiện được nhập thủ công, chẳng hạn như tạo các tệp kết xuất sự cố, v.v.

Như đã thảo luận trong bài báo của Michael, một số phương tiện tồn tại để phân tích dữ liệu được đóng dấu thời gian có sẵn (một khi dữ liệu đó đã trải qua một số hình thức chuẩn hóa thành định dạng dữ liệu chung, giảm dữ liệu, v.v.) và trình bày dữ liệu đó theo định dạng trực quan dễ hiểu . Ví dụ: Zeitline (http://projects.cerias.purdue.edu/forensics/timeline.php) và EasyTimeline (http://en.wikipedia.org/wiki/Wikipedia: EASTimeline) là hai tùy chọn như vậy. Zeitline dựa trên Java Swing và dường như nó chưa được cập nhật hoặc thấy bất kỳ hoạt động quan trọng nào kể từ năm 2006. EasyTimeline trình bày một cách tiếp cận đồ họa để biểu diễn dữ liệu được đóng dấu thời gian. Một công cụ khác có tiềm năng lớn là Timile Simile, ban đầu có sẵn từ MIT và hiện có sẵn dưới dạng tiện ích Google (http://code.google.com.vn/p/similewidgets/). Dòng thời gian Simile cung cấp khả năng không chỉ đại diện cho cả hai điểm (một sự kiện xảy ra tại một thời điểm duy nhất, chẳng hạn như ngày truy cập cuối cùng của tệp) và thời lượng (một sự kiện xảy ra trong một khoảng thời gian, chẳng hạn như quét vi-rút) mà còn để trình bày dữ liệu theo thời gian trên các dải liền kề, riêng biệt để thông tin có thể tách biệt rõ ràng nhưng được xem tương quan với dữ liệu khác.

Một khía cạnh của việc sử dụng định dạng đầu ra dựa trên văn bản hoặc một trong các định dạng đầu ra dựa trên đồ họa được đề cập trước đây có thể bao gồm thay đổi cách các nhà phân tích xác định các sự kiện, chẳng hạn như đầu ra của tiện ích fls.exe.

# Summary

Hầu hết các nhà phân tích sẽ thấy rằng họ sẽ không sử dụng một khu vực duy nhất của hình ảnh thu được, chẳng hạn như hệ thống tệp, để ghép các bài kiểm tra của họ và các trường hợp của họ. Họ sẽ kết thúc bằng cách sử dụng dữ liệu từ Cơ quan đăng ký, các tệp được tìm thấy trong hệ thống tệp và thậm chí cả bộ nhớ và gói chụp mạng để xây dựng một bức tranh hoàn chỉnh về các trường hợp của họ. Rốt cuộc, tại sao lại đưa ra kết luận của bạn về một phần dữ liệu khi bạn có thể niêm phong mọi thứ bằng nhiều mẩu dữ liệu để hỗ trợ cho phát hiện của bạn? Bất kể bạn sử dụng bao nhiêu dữ liệu, tuy nhiên, chìa khóa cho mọi thứ sẽ là tài liệu của bạn.

# Solutions Fast Track

• **Case Studies**

Các nghiên cứu trường hợp luôn là một cách tuyệt vời để minh họa cách các bit thông tin và kỹ thuật phân tích dường như khác nhau có thể được kết hợp thành một khung gắn kết để có được cái nhìn sâu sắc hơn về phân tích. Nhiều người thích xem những gì người khác đã làm, và trong nhiều trường hợp, điều này sẽ khiến độc giả cân nhắc những gì họ đã xem, thử các kỹ thuật của riêng họ và thậm chí mở rộng kỹ thuật.

• **Getting Started**

Các mục chính cần ghi nhớ trong suốt quá trình phân tích của bạn là bám sát mục tiêu phân tích của bạn (không theo dõi hoặc mất tập trung có thể dễ dàng trì hoãn hoặc trì hoãn phân tích của bạn) và ghi lại chính xác và hoàn toàn phân tích của bạn.

• **Extending Timeline Analysis**

Đại diện cho dữ liệu có sẵn trong một định dạng timeline có thể là một công cụ cực kỳ mạnh mẽ cho một nhà phân tích.

Nhiều nguồn dữ liệu bên trong một hình ảnh thu được có thể chứa thông tin theo thời gian có giá trị, trong đó có các nội dung của các file log, các khóa Registry và các giá trị, và các nội dung của Recycle Bin.