BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

BÀI TẬP LỚN

Môn:

PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH

ĐỀ TÀI: DỊCH CHƯƠNG 2 WINDOWS FORENSICS ANALYSIS

Người hướng dẫn:

Giáo viên: TS. Lại Minh Tuấn

Sinh viên thực hiện:

Lê Trịnh Thanh Hiếu

Nguyễn Ngọc Hải

Đỗ Nhật Minh

Đỗ Hà Thu

Khoa An toàn thông tin – Học viện Kỹ thuật mật mã

Hà Nội, 2019

MỤC LỤC

CHƯƠNG 2: PHẢN HỒI TRỰC TIẾP: PHÂN TÍCH DỮ LIỆU

Chủ để chính trong chương này là phân tích dữ liệu, bao gồm 3 phần chính:

- Tổng quan
- Giải pháp tìm dấu vết nhanh
- Các câu hỏi thường gặp

2.1 GIỚI THIỆU

Bây giờ bạn hãy thu thập một số dữ liệu từ một hệ thống, khi đó sẽ có câu hỏi tại sao "Làm thế nào để tôi "nghe" được những gì nó diễn đạt" hoặc dễ hiểu hơn là "Làm thế nào để tôi biết được dữ liệu mạng cho tôi thông tin gì" Một lần tôi đã thu thập được một số tiến trình đang chạy, làm thế nào để phân loại các tiến trình, nếu có thể, nó có phải là phần mềm độc hại không ? Làm thế nào để tôi biết được có ai đó đã xâm nhập vào hệ thống và đang truy cập hệ thống ? Cuối cùng, bạn có thể sử dụng dữ liệu mà bạn đã thu thập để xây lên một bức tranh tuyệt vời về các cách thức hoạt động trên hệ thống của bạn, đặc biệt là bạn có dễ dàng hình dung và thực hiện việc phân tích.

Mục đích của chương này là để giải quyết các câu hỏi. Bạn đang nhìn thấy cái gì-bạn sẽ tìm được những gì trong gói dữ liệu mà bạn đã thu thập được, phụ thuộc rất nhiều vào vấn đề bạn đang cố gắng giải quyết. Làm thế nào để bạn thông qua các luồng dữ liệu để bạn tìm được những thứ mà bạn đang tìm kiếm? Ở chương này, tôi không nghĩ rằng một lúc nào đó tôi sẽ trả lời các câu hỏi của bạn; Hơn nữa, tôi hy vọng rằng sẽ cung cấp đủ dữ liệu và ví dụ để khi một cái gì đó xảy ra mà tôi tôi không được đảm bảo rằng nó sẽ an toàn. Có lẽ trong thời gian tới bạn sẽ hiểu được điều này khi kết thúc chương này, bạn sẽ hiểu hơn về lý do tại sao bạn thu thập dữ liệu và những gì mà bạn có thể biết về nó.

2.2 PHÂN TÍCH DỮ LIỆU

Một số luồng dữ liệu của thông tin nói cho bạn biết rằng dữ liệu bạn cần lựa chọn ở một hệ thống đang chạy tới khắc phục một sự cố của ứng dụng hoặc đánh giá một sự cố. Hãy xem ở một web chẳng hạn như trang Web Thông tin chứ cứ điện tử (e-Evidence Info) (www.e-evidence.info), ở đây sẽ có thông tin cập nhật hằng tháng với nhiều liên kết mới để thuyết trình, hay trên giấy, và bài viết thảo luận về một loạt các chủ đề, bao gồm các dữ liệu điện động được lựa chọn. Mặc dù nhiều tài nguyên trong

số này đề cập tới việc thu thập dữ liệu, một số được giải quyết về việc lựa chọn dữ liệu và phân tích dữ liệu. Chúng tôi sẽ giải quyết các vấn đề trong chương này.

Khi bắt đầu, bạn cần nhìn vào đầu ra của các công cụ,tới khi dữ liệu được lựa chọn, tới khi nhìn thấy được hình ảnh của dữ liệu có sẵn cho bạn. Khi bạn sử dụng các công cụ chẳng hạn như những vấn đề ở trong chương 1, bạn sẽ bắt đầu với một hình ảnh chụp lại của vấn đề với đầu ra từ một công cụ duy nhất. Với ví dụ, bạn cần nhìn vào một vài bất thường ở trong giao diện Task Manager với giao diện (GUI) hoặc ở đầu ra của **tlist.exe** (chẳng hạn như đường dẫn với một tệp tin hình ảnh bất thường hoặc dòng lệnh). Với một điều tra viên quen thuộc với hệ thống Windows và cái gì là mặc định hoặc "bình thường" các tiến trình được nhìn thấy từ quan điểm này, những chỉ số khá là rõ ràng và có thể nhảy ra ngay lập tức.

Tuy nhiên, một số điều tra viên và một vài người theo dõi hệ thống là không đủ quen thuộc với hệ thống Window để nhận ra các quy trình đang ở trạng thái mặc định hay "bình thường" trong nháy mắt. Đây là các bản đặc biệt đúng khi bạn cho rằng phiên bản Windows (ví dụ : Windows 2000, XP,2003 hoặc Vista) có nhiều việc phải làm với những gì được cho là "bình thường". Với ví dụ, các tiến trình mặc định ở Windows 2000 là khác với trên Windows XP, và đó chỉ là làm sạch, mặc định ở cài đặt, không có ứng dụng nào được bổ sung thêm. Cũng nên xem xét rằng phần cứng là khác nhau cấu hình thường được yêu cầu để cài đặt thêm drivers và các ứng dụng khác.Danh sách của sự biến đổi có thể di chuyển nhưng điểm quan trọng cần ghi nhớ là những gì cấu thành nên sự "bình thường" hay quá trình được hợp pháp có thể phụ thuộc vào nhiều yếu tố khác nhau, vì thế bạn cần một quy trình để kiểm tra dữ liệu có sẵn của bạn và xác định nguồn gốc của vấn đề mà bạn đang điều tra. Đây là việc quan trọng, cần có một quy trình có nghĩ là bạn có các bước mà bạn làm theo, và nếu có gì đó cần được thêm hoặc sửa đổi, bạn có thể làm như vậy một cách dễ dàng. Không có quy trình, làm thế nào để bạn xác định được điều bạn đã làm sai và bạn có thể làm gì để cải thiện nó ? Nếu bạn không biết những gì bạn đã làm, làm thế nào để bạn có thể sửa chữa nó.

Có lẽ đó cách tốt nhất để bắt đầu tìm hiểu sâu hơn về nó. Khi phân tích dữ liệu, nó sẽ giúp bạn có một vài gợi ý của việc bạn đang tìm kiếm cái gì đó. Một vấn đề lớn mà những người quản trị công nghệ thông tin (IT) và người phản hồi phải đối mặt phải khi xảy ra một vấn đề là theo dõi về nguồn gốc cửa dữ liệu mà họ đang có. Một ví dụ là khi có cảnh báo xuất hiện trong việc phát hiện xâm nhập mạng qua hệ thống (NIDS) hoặc một mục lẻ xuất hiện trong phần log tường lửa. Nhiều lần, đó có thể là kết quả của phần mềm độc hại (e.g.,) .Thỉnh thoảng, cảnh báo hay mục nhật ký sẽ chứa thông tin – như cổng và địa chỉ của Internet Protocol (IP), cũng như đích đến đến là địa chỉ IP hay là cổng kết nốt. Nguồn của địa chỉ IP được xác định bởi hệ thống tới luồng lưu

lượng, và như bạn thấy ở trong Chương 1, nếu bạn có cổng nguồn của lưu lượng mạng, bạn có thể sử dụng thông tin đó để xác định ứng dụng đã gửi lưu lượng truy cập và xác định phần mềm độc hại.

CẢNH BÁO

Hãy nhớ rằng để lưu lượng truy cập xuất hiện trên mạng, một số tiến trình – một số điểm đến tạo nên đó. Tuy nhiên, một vài tiến trình là rất ngắn ngủi (ví dụ , một trình tải xuống và cài đặt một số file khác,chẳng hạn như Trojan, và sau đó chấm dứt), và đã cố gắng xác định vị trí của một tiến trình dựa trên lưu lượng ở trong nhật ký của tường lửa trong bốn giờ trước (và không chỉ một lần kể từ đó) có thể chống lại. Nếu lưu lượng truy cập xuất hiện thường xuyên, hãy chắc chắn kiểm tra tất cả các khả năng. Điều này bao gồm cả kiểm tra địa chỉ IP nguồn của lưu lượng để xác định vị trí nào của hệ thống truyền tới nó và thậm chí cái đặt một mạng "sniffer" trực tuyến để bắt được và kiểm tra lưu lượng mạng để xem nó có bị giả mạo hay không.

Một điểm quan trọng khác là người tạo ra phần mềm độc hại thường sẽ cố gắng che dấu sự hiện diện của các ứng dụng trên một hệ thống bằng các sử dụng một tên quen thuộc, hoặc một tên tương tự như là một file bình thường được quản trị viên có thể nhận ra. Nếu điều tra viên tìm kiếm trên web, tìm kiếm sẽ trả về thông tin chỉ ra tệp tin đó là vô hại, hoặc là một tệp hợp pháp được sử dụng bởi hệ điều hành.

CẢNH BÁO

Trong khi đối phó với virus ở trên mạng ở công ty, tôi xác định được một của nguyên nhân là đã được cài đặt ở trên hệ thống cũng như dịch vụ của Windows đã chạy một tệp tin có tên là alg.exe. Tìm kiếm trên thông tin trên tệp nàu, quản trị viên đã xác định được đây là một ứng dụng được hợp pháp được là "Dịch vụ cổng vào tầng ứng dụng". Dịch vụ này xuất hiện trong ở trong việc đăng ký khóa ở CurrentControlSet\Services, ở trong khóa con ALG, và trỏ đến %SystemRoot%\system32\alg.exe dưới dạng tệp hình ảnh. Tuy niên, dịch vụ tôi tìm thấy ở "Dịch vụ cổng vào tầng ứng dụng" với khóa con (first hint : the subkey name is incorrect) và được trỏ đến %SystemRoot%\alg.exe. Cẩn thận khi tìm kiếm tên tệp tin, vì cả người giỏi nhất trong chúng ta cũng có thể mắc lỗi bởi thông tin được trả lại thông qua tìm kiếm như vậy. Tôi đã thấy người phân tích phần mềm độc hại có nhiều kinh nghiệm mắc lỗi khi xác định tệp tin thông qua tên của nó.

Để làm rõ cho tất cả những điều này, hãy xem các ví dụ sau đây.

2.2.1 VÍ DỤ 1

Một kịch bản được nhìn thấy hết lần này đến lần khác là một kịch bản trong đó quản trị viên hay nhân viên hỗ trợ (helpdesk) sẽ là người thông báo về hoạt động bất thường hay đáng ngờ trên hệ thống. Hoạt động bất thườn nó có thể là do phản hồi của người sử dụng hoặc quản trị viên hệ thống tìm thấy một số tệp bất thường trên máy chủ Web, và khi cô ấy đã cố gắng xóa chúng cô ấy đã thông báo rằng chúng không thể bị xóa khi đang sủ dụng một tiến trình khác.

Trong những sự cố như vậy, người phản hồi đầu tiên sẽ phải đối mặt với một hệ thống không thể tắt được để điều tra một cách chi tiết (do thời gian hoặc là do công việc kinh doanh), và một phản ứng nhanh chóng (mặc dù phải kỹ lưỡng) nhưng là rất cần thiết. Thường xuyên, điều này có thể thực hiện thông qua phản hồi trực tiếp, trong đó thông tin liên quan đến trạng thái hiện tại của hệ thống nhanh chóng được thu thập và phân tích với sự hiểu biết rằng phải có đủ thông tin để cung cấp hình ảnh về trạng thái của hệ thống. Với thông tin tìm được được lựa chọn từ một hệ thống đang chạy, mặc dù quá trình thu thập thông tin đó có thể được sao chép, vì một hệ thống đang chạy là luôn luôn ở trạng thái thay đổi.

Bất cứ khi nào một cái gì đó xảy ra trên hệ thống, nó là kết quả của một vài tiến trình đang chạy trên hệ thống. Mặc dù tuyên bố này có vẻ như là "dễ nhận biết nhất cho những người bình thường nhất" (1 tuyên bố mà giáo sư trường đại học từng nói với tôi nhiều lần ở trong lớp học, thường là khi có phương trình vi phân bậc 6), thường

là thực tế bị bỏ qua trong sự áp lực và căng thẳng của công việc để ứng phó với sự cố. Tuy nhiên, sự thật đơn giản là để xảy ra vấn đè nào đó trên hệ thống, một tiến trình hay luồn của dữ liệu phải được tham gia vào hệ thống theo một cách nào đó.

Vì vậy, làm thế nào để một người trả lợi về việc định vị một tiến trình đáng ngờ trên hệ thống ? Câu trả lời là thông qua việc thu thập dữ liệu và phân tích dữ liệu qua hệ thống đang chạy. Và tin tôi đi, tôi đã ở trong một tìn huống mà khách hàng tặng tôi một ổ cứng từ hệ thống (hoặc tệp hình ảnh mà thu thập được từ hệ thống) và hỏi tôi rằng có bao nhiêu tiến trình đang chạy trong hệ thống. Thực tế của vấn đề là hiển thị những gì xảy ra trên hệ thống phải là hệ thống đang chạy, bạn phải có những thông tin bạn thu thập từ hệ thống khi nó đang chạy. Sử dụng các công cụ được thảo luận ở trong chương 1, bạn có thể thu thập thông tin về trạng thái của hệ thống tại 1 thời điểm, chụp lại tại thời điểm đó. Vì thông tin mà bạn thu thập được tồn tại trong bộ nhớ điện động, nên thông tin đó sẽ không còn tồn tại.

Trong kịch bản này, tôi có một hệ thống Windows 2000 đã hoạt động bất thường. Hệ thống này là một máy chủ web mạng nội bộ chạy Internet Information Server (IIS) phiên bảo 5.0, và người dùng đã cố gắng truy cập các trang web trên máy chủ đã báo cáo rằng họ không thể lấy bất kỳ thông tin nào và chỉ thấy trang trống ở trong trình duyệt của họ. Điều này thật là kỳ lạ, có lẽ người sử dụng sẽ thấy thông báo lỗi. Nhưng khi tôi bắt đầu khởi động một phiên bản của Forensic Server (i.e., the Forensic Server Project [FPS] ở chương 1) ở phiên bản của tôi (địa chỉ IP 192.168.1.6) sử dụng dòng lệnh sau :

```
C:\fsp>fspc –c cases –n testcase1 –i "H. Carvey" –v
```

Sau đó, tôi lấy CD về các phản hồi đầu tiên chưa các công cụ và 1 bản copy của First Responder Utility (i.e., fruc.ext, cũng từ chương 1) và tìm kiếm trên hệ thống bị ảnh hưởng. Trong những sự cố như vậy, ban đầu tôi có một cách tiếp cận tối giản nhất; tôi thích giảm thiểu các tác động của mình lên hệ thống (nhớ lại Locard’s Exchange Principle) và tối ưu hóa các nỗ lực của mình và thời gian phản hồi. Cuối cùng, theo thời gian, tôi đã phát triển một tập hợp thông tin trạng thái tối thiểu mà tôi cần trích xuất từ một hệ thống đang chạy để có một cái nhìn toàn diện để tôi xác định được vị trí có hoạt động đáng nghi ngờ.

Tôi cũng đã xác định được có một bộ công cụ mà tôi cần sử dụng để thu thập thông tin (tệp fruc.ini được sử dụng với Công cụ tiện ích sử dụng đầu (FRU: First Responder Utility) ở trong kịch bản này là ở trong thư mục ch2\samples trên phương tiện đi kèm với cuốn sách này). Phần [Commands] của tệp fruc.ini chưa các các thư mục sau :

1=psloggedon.exe::psloggedon.dat
2=netusers.exe -l -h::netusers-lh.dat
3=tlist.exe -c::tlist-c.dat
4=tlist.exe -s::tlist-s.dat
5=tlist.exe -t::tlist-t.dat
6=handle.exe -a -u::handle-au.dat
7=listdlls.exe::listdlls.dat
8=tcpvcon.exe -can::tcpvcon-can.dat
9=autorunsc.exe -l -d -s -t -w::autorunsc-ldstw.dat
10=svc.exe::svc.dat
11=auditpol.exe::auditpol.dat

Một lệnh được chạy theo thứ tự từ trước, và từ danh sách mà bạn có thể nhìn thấy các lệnh thu thập thông tin về người dùng đã đăng nhập (cả cục bộ và từ xa) cũng như lịch sử đăng nhập, vị trí tự khởi động, các tiền trình, các kết nối mạng và các cổng dịch vụ mở, dịch vụ và chính sách kiểm soát trên hệ thống. Nhóm lệnh này sẽ không chỉ cung cấp một cái nhìn toàn diện về trạng thái của hệ thống trong một ảnh chụp trong một thời gian mà thu thập dữ liệu có thể giúp phân tích trực tiếp và có những nỗ lực điều tra tiếp theo.

Tiếp cận với hệ thống Windows 2000 bị ảnh hưởng, tôi đặt CD FRU vào CD-ROM, khởi chạy một dòng lệnh và gõ dòng lệnh sau :

E:\>fruc –s 192.168.1.6 –p 7070 –f fruc.ini –v

CHÚ Ý

Bất cứ khi nào bạn thực hiện phản hồi sự cố trực tiếp, tôi khuyên bạn nên thu thập toàn bộ nội dung của bộ nhớ vật lý (a.k.a. RAM) trước khi thực hiện bất kỳ hoạt động nào khác. Điều này cho phép bạn có được nội dung của RAM ở trạng thái nguyên sơ nhất có thể và trước khi đưa ra các thay đổi bổ sung cho trạng thái hệ thống. Mặc dù điều này vượt ra ngoài phạm vi của chương này, nhưng nó là một sự khác biệt lớn trong Chương 3.

Trong vài giây, dữ liệu điện động mà tôi thu thập được từ hệ thống được trích xuất và lưu trữ trên máy trạm của tôi để phân tích.

Khi quay lại với máy trạm phân tích, tôi thấy rằng, như mọng đợi, thư mục testcase1 chứa 16 tệp. Một trong những lợi ích của FSP là nó tự ghi lại; tệp fruc.ini chứa danh sách các công cụ và dòng lệnh được sử dụng để khởi chạy các công cụ đó khi thu thập dữ liệu điện động. Vì tệp này và bản thân các công cụ có trong CD, chúng không thể được sửa đổi, miễn là tôi duy trì CD đó, tôi sẽ có thông tin bất biến về công cụ nào (phiên bản của từng công cụ, v.v.) Tôi đã chạy trên hệ thống, và các tùy chọn được sử dụng để chạy các công cụ đó. Một trong các tệp trong thư mục testcase1 là tệp case.log, duy trì một danh sách dữ liệu được gửi đến máy chủ bởi FRU và MD5 và SHA-1 các hàm băm cho các tệp mà dữ liệu được lưu. Ngoài ra, tôi thấy tệp case.hash, chứa hàm băm MD5 và SHA-1 của tệp nhật ký sau khi nó được đóng lại.

Thông tin mà tôi quan tâm được chứa trong 14 tệp khác trong thư mục. Một trong những điều đầu tiên tôi thường làm để bắt đầu phân tích là xem liệu có bất kỳ quá trình bất thường nào rời khỏi tôi không. Để làm điều đó, tôi thường sẽ bắt đầu với đầu ra của lệnh tlist, vì điều này sẽ hiển thị dòng lệnh được sử dụng để khởi chạy mỗi quá trình hoạt động (và hiển thị) trên hệ thống. Ví dụ, một trong những quy trình có thể nhìn thấy ngay lập tức là chính quy trình FRUC (do đó thể hiện tầm quan trọng của việc trích xuất bộ nhớ vật lý trước):

1000 FRUC.EXE
Command Line: fruc -s 192.168.1.6 -p 7070 -f fruc.ini –v

Cuộn qua phần còn lại của tập tin, tôi thấy rất nhiều tiến trình của Google bình thường; đó là các tiến trình mà tôi đã từng thấy khi chạy trên hệ thống Windows. Sau đó tôi chạy trên tiến trình cho máy chủ Web IIS mà tôi biết sẽ chạy trên hệ thống này:

736 inetinfo.exe
Command Line: C:\WINNT\system32\inetsrv\inetinfo.exe

Di chuyển xa hơn, tôi chạy qua một tiến trình ngay lập tức hiện ra với tôi là điều bất thường và đáng ngờ:

816 inetinfo.exe
Command Line: inetinfo.exe -L -d -p 80 -e c:\winnt\system32\cmd.exe

Hầu hết các máy chủ Web IIS chỉ có một phiên bản inetinfo.exe đang chạy và hệ thống này có hai phiên bản. Không chỉ vậy, theo “mặc định” phiên bản của inetinfo.exe chạy từ thư mục system32\ inetsrv, giống như chúng ta thấy với ví dụ của inetinfo.exe với mã định danh tiến trình (PID) 736. Tuy nhiên, phiên bản inetinfo.exe với PID 816 dường như đang chạy từ thư mục system32; Ngoài ra, dòng lệnh được sử

dụng để khởi chạy quá trình này trông giống như dòng lệnh được sử dụng để khởi chạy netcat!

Cần thêm thông tin về điều này và lưu ý rằng dòng lệnh cho PID 816 dường như đã ràng buộc quá trình với cổng 80 (sẽ giải thích cho hành vi bất thường được báo cáo bởi người dùng), sau đó tôi mở tệp chứa đầu ra của lệnh chạy thứ tám từ tệp fruc.ini (ví dụ: tcpvcon.exe,exe -can) để xem:

TCP, C:\WINNT\system32\inetsrv\inetinfo.exe,736,,127.0.0.1:443,*.*
TCP, C:\WINNT\system32\inetsrv\inetinfo.exe,736,,127.0.0.1:21,*.*
TCP, C:\WINNT\system32\inetsrv\inetinfo.exe,736,,127.0.0.1:25,*.*
TCP, C:\WINNT\system32\inetsrv\inetinfo.exe,736,,127.0.0.1:1026,*.*
TCP, C:\WINNT\system32\inetsrv\inetinfo.exe,816,,127.0.0.1:80,*.*

Thông thường, tôi sẽ thấy rằng PID 736 bị ràng buộc với cổng 80, nhưng trong trường hợp này, thay vào đó, PID 816 bị ràng buộc với cổng đó.

Như bạn có thể thấy, tôi đã xác định PID 816 là một quy trình đáng ngờ và có vẻ như quy trình này sẽ giải thích cho hoạt động bất thường đã được báo cáo. Kiểm tra đầu ra của các lệnh khác, tôi không thấy bất kỳ dịch vụ bất thường nào đang chạy hoặc bất kỳ sự liên quan nào đến quy trình trong các vị trí tự khởi động. Đầu ra của tiện ích handle.exe cho thấy tiến trình này đang chạy trong tài khoản Administrator, nhưng không có tệp nào được mở. Ngoài ra, đầu ra của lệnh tcpvcon.exe -can cho thấy rằng không có kết nối hiện tại nào với cổng 80 trên hệ thống đó. Tại thời điểm này, tôi đã xác định được vấn đề và bây giờ cần xác định xem phần mềm này có trên hệ thống như thế nào và cuối cùng nó chạy như thế nào bởi một tiến trình.

2.2.2 VÍ DỤ 2

Một kịch bản phổ biến khác được thấy trong môi trường mạng là lưu lượng truy cập bất thường bắt nguồn từ một hệ thống xuất hiện trong hệ thống phát hiện xâm nhập (IDS) hoặc nhật ký tường lửa. Hầu hết thời gian, quản trị viên thấy điều gì đó bất thường hoặc đáng ngờ, chẳng hạn như lưu lượng truy cập rời khỏi mạng không phải là những gì thường thấy. Ví dụ về điều này thường bao gồm IRCbot và nhiễm Worm. Nói chung, IRCbot sẽ lây nhiễm một hệ thống, có lẽ là kết quả của việc người dùng lướt web trang chứa một số mã khai thác lỗ hổng trong trình duyệt Web. Điều đầu tiên điều đó thường xảy ra là một ứng dụng tải xuống ban đầu được gửi trên hệ thống, sau đó tiếp cận với một trang web khác để tải xuống và cài đặt mã IRCbot thực tế Chính nó. Từ đó, IRCbot truy cập một kênh trên máy chủ Internet Relay Chat (IRC) và chờ lệnh từ botmaster.

CẢNH BÁO

IRCbots đã là một vấn đề lớn trong một thời gian dài, khi toàn bộ đội quân bot, hoặc các botnet của người Hồi giáo, đã được phát hiện có liên quan đến một số tội phạm mạng. Trong số ra ngày 19 tháng 2 năm 2006 của Tạp chí Washington Post, Brian Krebs trình bày câu chuyện về botmaster 0x80 cho thế giới. Câu chuyện của ông rõ ràng cho thấy sự dễ dàng với các botnet được phát triển và cách chúng có thể được sử dụng. Chỉ Một vài tháng sau, bài viết Robert Lemos từ SecurityF Focus (www.securityf Focus.com / news / 11390) cảnh báo chúng tôi rằng IRCbots dường như đang di chuyển từ một khách hàng /khung máy chủ thành khung ngang hàng, làm cho chúng khó hơn nhiều để tắt Bạn có thể tìm thấy bài viết tại:

www.washingtonpost.com/wp-dyn/content/post/2006/02/14/AR2006021421401342.html/

Trong trường hợp nhiễm worm, một khi worm nhiễm vào hệ thống, nó sẽ cố gắng tiếp cận và lây nhiễm các hệ thống khác. Worms thường làm điều này bằng cách quét địa chỉ IP, tìm kiếm cùng một lỗ hổng (nhiều worms ngày nay cố gắng sử dụng một số lỗ hổng khác nhau để hệ thống lây nhiễm) mà họ sử dụng để lây nhiễm các máy chủ hiện tại. Một số loài Worm khá độc trong quá trình quét của họ ; Slammer SQL worm (www.cert.org/advisories/CA-2003-04.html) đã phát tán trên Internet vào tháng 1 năm 2003, tạo ra rất nhiều lưu lượng truy cập đến các máy chủ và thậm chí các máy rút tiền ATM trên Internet đã bị tấn công từ chối dịch vụ (DoS).

Việc đề cập đến các cuộc tấn công DoS mang đến một khía cạnh quan trọng khác của kịch bản này. Đôi khi các quản trị viên CNTT được thông báo bởi một bên ngoài rằng họ có thể đã bị nhiễm các hệ thống. Trong những trường hợp như vậy, thường là chủ sở hữu của một hệ thống đang được quét bởi một worm hoặc là trong một cuộc tấn công DoS sẽ thấy địa chỉ IP ban đầu của lưu lượng truy cập trong lưu lượng truy cập, thực hiện một số nghiên cứu liên quan đến chủ sở hữu của địa chỉ IP đó (thường là một phạm vi và không phải là một Địa chỉ IP được gán cho ai đó) và sau đó cố gắng liên hệ với họ. Điều đó đúng, thậm chí vào năm 2009, không có gì lạ khi ai đó gõ cửa nhà bạn để nói với bạn rằng bạn có hệ thống bị nhiễm độc

Bất kể người quản trị được thông báo như thế nào, vấn đề phản hồi vẫn như cũ. Một trong những khó khăn của những vấn đề như vậy là trang bị địa chỉ IP và số cổng (cả hai trong đó được lấy từ các tiêu đề của lưu lượng truy cập mạng bị bắt), sau đó,

quản trị viên phải xác định bản chất của sự cố. Nói chung, các bước để làm điều đó là xác định vị trí thực của hệ thống, và sau đó để thu thập và phân tích thông tin từ hệ thống đó.

Kịch bản này bắt đầu và tiến triển theo cách tương tự như kịch bản trước đó,trong đó tôi khởi chạy FSP trên máy trạm pháp y của mình, đi đến hệ thống đích với CD FRUC của tôi và thu thập dữ liệu dễ bay hơi từ hệ thống.

MẸO

Bạn có thể tìm thấy dữ liệu tôi đã thu thập trong kịch bản này trong các mẫu ch2 \thư mục trên phương tiện đi kèm, trong kho lưu trữ có tên testcase2.zip.

Khi trở lại máy trạm pháp y, tôi mở đầu ra của lệnh tlist.exe –t command (in Cây công việc hiển thị từng quy trình được liệt kê, được thụt vào bên dưới quy trình mẹ của nó)và PID 980 nổi bật như kỳ lạ đối với tôi:

```
System Process (0)
System (8)
   SMSS.EXE (140)
CSRSS.EXE (164)
WINLOGON.EXE (160) NetDDE Agent
  SERVICES.EXE (212)
svchost.exe (404)
spoolsv.exe (428)
svchost.exe (480)
regsvc.exe (532)
mstask.exe (556) SYSTEM AGENT COM WINDOW
snmp.exe (628)
VMwareService.e (684)
WinMgmt.exe (600)
svchost.exe (720)
   wuauclt.exe (1080)
inetinfo.exe (736)
svchost.exe (1192)
 LSASS.EXE (224)
explorer.exe (520) Program Manager
```

VMwareTray.exe (1232)
VMwareUser.exe (1256)
WZQKPICK.EXE (1268) About WinZip Quick Pick
CMD.EXE (812) Command Prompt - svchost 192.168.1.28 80
svchost.exe (980)

Để xem tại sao quá trình này xuất hiện kỳ lạ, điều quan trọng là phải hiểu rằng trên mặc định cài đặt Windows 2000, thường chỉ có hai bản sao của Svchost.exe đang chạy.

MẸO

Bài viết Microsoft Knowledge Base Q250320 của Microsoft (http://support.microsoft.com/? kbid = 250320) cung cấp mô tả về svchost.exe trên Windows 2000, bài viết [http://support.microsoft.com/kb/314056/ EN-US /] cung cấp mô tả về svchost.exe trên Windows XP).Đầu ra ví dụ của tlist –s command không chỉ hiển thị hai bản sao của svchost.exe đang chạy, nhưng cũng tham chiếu khóa Registry liệt kê các nhóm minh họa trong bài viết. Xem thêm bài viết Microsoft Knowledge Base Q263201 (http://support.microsoft.com/?kbid=263201) để biết danh sách các quy trình mặc định tìm thấy trên các hệ thống Windows 2000.

Đầu ra của tlist –t command hiển thị một bản sao bổ sung của svchost.exe và một có vẻ như đang chạy từ cửa sổ nhắc lệnh, thay vì từ services.exe, như với các trường hợp khác của svchost.exe.

Kiểm tra đầu ra của tlist –c command để xem command-line tùy chọn được sử dụng để khởi chạy PID 980, tôi thấy:

980 svchost.exe
Command Line: svchost 192.168.1.28 80

Đầu ra của tcpvcon.exe –can lệnh cho tôi thấy rằng PID 980 đang sử dụng một cổng khách hàng:

TCP,C:\WINNT\system\svchost.exe,980,ESTABLISHED, 192.168.1.22:1103, 192.168.1.28:80

Nó đã được chạy và có *–o* chuyển đổi có sẵn trên hệ thống Windows 2000, đầu ra của netstat.exe –ano lệnh cũng đã cho tôi thấy rằng PID 980 có kết nối mạng đang hoạt động với hệ thống từ xa trên cổng 80:

TCP 192.168.1.22:1103 192.168.1.28:80 ESTABLISHED 980

Tại thời điểm này, dựa trên thông tin tôi có, tôi có thể muốn theo dõi lưu lượng truy cập mạng bằng cách đặt trình thám thính mạng hoặc hệ thống được cài đặt trình thám thính (như Wireshark, được tìm thấy tại www.wireshark.org) trên mạng để bắt đầu lưu lượng truy cập để xem dữ liệu nào đang được truyền giữa hai hệ thống. Từ các dữ liệu dễ bay hơi khác đã được thu thập, PID 980 dường như không có bất kỳ tệp nào được mở (theo đầu ra của công cụ handle.exe) và dường như không có bất kỳ quy trình bổ sung, bất thường nào.

Khi bạn đang xem các quy trình trên một hệ thống, sẽ giúp biết một chút về cách các quá trình được tạo ra trong mối quan hệ với nhau. Ví dụ, như được minh họa trong đầu ra của các tlist –t ra lệnh sớm hơn (lấy từ hệ thống Windows 2000), hầu hết các quy trình hệ thống bắt nguồn từ quá trình có tên là " Hệ thống "(PID 8 trên Windows 2000, PID 4 trên XP), trong khi hầu hết các quy trình người dùng bắt nguồn từ explorer.exe, đó là trình bao hoặc được liệt kê bởi tlist.exe, "Quản lý chương trình". Nói chung (và tôi sử dụng từ này một cách cẩn thận, vì có thể có các trường hợp ngoại lệ), chúng tôi thấy rằng quy trình Hệ thống là quy trình " Cha mẹ" của trực tuyến cho quy trình services.exe, mà lần lượt là quá trình parent , tốt, nhiều dịch vụ. Services.exe là tiến trình cha, ví dụ, đối với các quá trình svchost.exe. Về phía người dùng, một dấu nhắc lệnh (cmd.exe) sẽ xuất hiện dưới dạng một tiến trình con cho tiến trình explorer.exe và bất kỳ lệnh nào chạy từ bên trong dấu nhắc lệnh, chẳng hạn như tlist –t, sẽ xuất hiện dưới dạng một tiến trình con đến cmd.exe.

Vì vậy, làm thế nào là quan trọng để đáp ứng trực tiếp? Hãy xem lại đầu ra từ lệnh *tlist –t* một lần nữa. Bạn sẽ thấy một ví dụ của Svchost.exe (PID 980) đang chạy như một tiến trình con cho cmd.exe, đây là một quá trình con để explorer.exe ... không phải là nơi chúng ta mong đợi để thấy svchost.exe!

Bây giờ, hãy thực hiện một bước xa hơn. Điều gì xảy ra nếu Svchost.exe đang chạy (PID 980) đã được cài đặt như một dịch vụ? Mặc dù chúng tôi sẽ không nhận thấy điều này trong đầu ra của tlist –t, chúng ta sẽ thấy một cái gì đó lẻ trong đầu ra của tlist –c, trong đó cho chúng ta thấy dòng lệnh được sử dụng để khởi chạy mỗi quá trình. Svchost.exe giả mạo rất có thể đã phải có nguồn gốc từ trong một thư mục khác với thư mục system32, nhờ Bảo vệ tệp Windows (WFP). WFP là một cơ chế được sử dụng, bắt đầu với Windows 2000, trong đó một số tệp nhất định của hệ thống (và rất quan trọng khác) được "bảo vệ" , trong đó việc cố gắng sửa đổi các tệp sẽ khiến WFP

“hoạt động lại” và tự động thay thế tệp đã sửa đổi bằng một bản sao mới từ bộ đệm của nó (để lại bằng chứng về hoạt động này trong Nhật ký sự kiện). Windows 2000 có một số vấn đề trong đó WFP có thể dễ dàng bị phá vỡ, nhưng những vấn đề đó đã được khắc phục. Vì vậy, giả sử rằng WFP đã không bị lật đổ theo một cách nào đó, chúng ta sẽ thấy rằng Svchost.exe lừa đảo đang chạy từ một thư mục khác, có thể là Windows \ System hoặc Temp, cảnh báo chúng ta về thủ phạm.

CẢNH BÁO

WFP có thể bị lật đổ trên tất cả các hệ thống Windows, trong một số trường hợp khá dễ dàng. Rõ ràng, một chức năng giao diện chương trình ứng dụng (API) không có giấy tờ có sẵn thông qua sfc_os.dll, được xuất ở thứ 5 và đã được đặt tên là SfcFileException; điều này được thảo luận tại trang Bitsum Technologies (www.bitsum.com/aboutwfp.asp), ngoài các địa điểm khác trên Internet. Tuy nhiên, ngoại lệ đáng chú ý là Microsoft.com. Theocác mô tả về chức năng API này, gọi nó một cách chính xác sẽ vô hiệu hóa WFP trong một phút, đủ thời gian để “ bảo vệ “tập tin được sửa đổi hoặc thay thế. Vì WFP không thăm dò các tệp được bảo vệ, một khi WFP được kích hoạt lại, không có gì để thông báo rằng tệp đã bị thay đổi. Trong các trường hợp thông thường, khi hệ điều hành tạo ra một sự kiện thay đổi tệp, WFP “hoạt động lại”, kiểm tra xem liệu sự kiện thay đổi có xảy ra đối với tệp được bảo vệ hay không, và nếu có, hãy thay thế tệp đó bằng một bản sao tốt được sao chép từ bộ đệm và tạo một bản ghi Nhật ký sự kiện. Với WFP bị vô hiệu hóa trong một phút thông qua API SfcFileException, không có gì để phát hiện hoặc cảnh báo về thực tế rằng tệp đã bị thay đổi. Chúng tôi sẽ thảo luận chi tiết hơn về Chương 5, trong đó tôi cũng sẽ trình bày một công cụ phân tích để cung cấp các chỉ dẫn về loại hoạt động này trong quá trình phân tích sau khi bị vô hiệu

---

2.2.3 VÍ DỤ 3

Microsoft’spsexec.exe (http://technet.microsoft.com/enus/sysinternals/bb897553.aspx) là một công cụ tuyệt vời để chứng minh làm thế nào bạn có thể tìm kiếm các quy trình bất thường hoặc đáng ngờ trên các hệ thống. Nhiều lần, kẻ xâm nhập sẽ có quyền truy cập vào hệ thống thông qua một số có nghĩa và tận dụng sự thật rằng anh ta có các đặc quyền cấp Quản trị viên và nâng các đặc quyền đó lên cấp Hệ thống. Điều này được thực hiện, một phần, để (a) ngăn quản trị viên nhận thấy kẻ xấu đang ở trên hệ thống hoặc có một quy trình đang chạy và (b) ngăn chặn quản trị viên có thể đơn giản ngăn quá trình xấu chạy.

Vì vậy, điều đầu tiên chúng tôi sẽ làm là tải xuống một bản sao của psexec.exe từ trang web Microsoft / Sysiternals, sau đó chạy nó với dòng lệnh sau:

```
C:\tools>psexec –s cmd
```

Tại thời điểm này, chúng tôi vẫn có một dấu nhắc lệnh, nhưng nó chạy với các đặc quyền cấp Hệ thống. Bây giờ, để thêm một số dữ liệu cần quan sát, hãy khởi chạy Solitaire bằng cách nhập **sol** tại dấu nhắc lệnh. Bạn sẽ nhận thấy rằng bạn đã thắng Patrick khi thấy ứng dụng bật lên trên máy tính để bàn của bạn, nhưng bạn sẽ nhận được nhắc nhở trở lại mà không có bất kỳ lỗi nào.

Bây giờ, hãy mở một dấu nhắc lệnh khác và chạy **tlist.exe –t.**Đầu ra sẽ trông tương tự như sau (đầu ra được cắt bớt vì lý do ngắn gọn):

```
D:\tools>tlist -t
System Process (0)
System (4)
  smss.exe (968)
csrss.exe (1032)
  winlogon.exe (1060)
  services.exe (1104)
svchost.exe (1360)
svchost.exe (1704)
 wscntfy.exe (316)
svchost.exe (1968)
svchost.exe (352)
spoolsv.exe (872)
scardsvr.exe (932)
alg.exe (1768)
PSEXESVC.EXE (1560)
  cmd.exe (3664)
    sol.exe (3832)
  lsass.exe (1116)
explorer.exe (372) Program Manager
  DLACTRLW.EXE (780)
  cmd.exe (2748) Command Prompt - tlist -t
tlist.exe (2196)
  cmd.exe (2684) \\WINTERMUTE: cmd
psexec.exe (3448)
```

Lưu ý rằng bên dưới quy trình explorer.exe, bạn thấy các dấu nhắc lệnh đang chạy cho cả tlist.exe và psexec.exe (các quy trình với lần lượt là 2748 và 2684). Tuy nhiên, bạn cũng thấy PSEXESVC.EXE chạy phía trên explorer.exe trong chế độ xem dạng cây liệt kê quy trình. Điều này là do quá trình đang chạy với các đặc quyền cấp Hệ thống. Bên dưới quy trình PSEXESVC.EXE, được thụt lề để chỉ ra rằng đó là một quy trình con của PSEXESVC.EXE, vẫn là một quy trình khác dấu nhắc lệnh (quy trình với PID 3664) và bên dưới quy trình đó là quy trình con Solitaire. Các quy trình chạy dưới dạng dịch vụ (như sol.exe) không chạy trong chế độ tương tác, giống như khi chúng được chạy bình thường bởi người dùng.

Tôi đã sử dụng ví dụ này để minh họa những gì có thể xảy ra khi nguyên tắc đặc quyền tối thiểu được tuân theo khi tạo tài khoản người dùng. Quá thường xuyên, một số loại trình tải xuống có được trên hệ thống người dùng, thông qua người dùng truy cập trang Web độc hại hoặc thông qua một số phương tiện khác, chẳng hạn như tệp đính kèm e-mail. Trình tải xuống sau đó thực hiện nhiệm vụ lấy phần mềm độc hại khác và vì tài khoản người dùng đang chạy trên hệ thống với các đặc quyền của Quản trị viên, phần mềm độc hại sau đó có khả năng thực hiện mọi thứ mà người dùng có thể, như tạo Tác vụ theo lịch hoặc cài đặt dịch vụ Windows. Với các đặc quyền được nâng cấp vượt quá khả năng của tài khoản Quản trị viên, phần mềm độc hại hiện có quyền truy cập hoàn toàn vào tất cả các tài nguyên hệ thống. Ngoài ra, phần mềm độc hại không còn tương tác với máy tính để bàn, điều đó có nghĩa là một số vật phẩm sẽ không còn nữa (xem Chương 4).

2.3 PHÂN TÍCH NHANH

Có lẽ một trong những lý do thường được nhắc tới nhiều nhất về việc không thực hiện phản hồi trực tiếp là không có khả năng xác định nguồn gốc của vấn đề trong rất nhiều dữ liệu đã được thu thập. Nhiều công cụ có sẵn cho việc thu thập dữ liệu có tính dễ bay hơi (và cả không dễ bay hơi) trong quá trình phản hồi trực tiếp sẽ thu thập một lượng lớn dữ liệu, đến mức nó quá nhiều với nhà điều tra. Trong các ví dụ ở chương này, tôi không phải thu thập quá nhiều dữ liệu để xác định nguồn gốc của vấn đề. Các công cụ thu thập dữ liệu mà tôi đã sử dụng trong các trường hợp ví dụ có hai tính chất là: phần mềm độc hại cần ***phải chạy*** để có bất kỳ ảnh hưởng nào đến hệ thống và phần mềm độc hại đó cần ***phải tồn tại*** để có bất kỳ ảnh hưởng nào đến hệ thống (ví dụ: tác giả của phần mềm độc hại muốn phần mềm của họ tồn tại khi khởi động lại và khi người dùng đăng nhập). Chúng tôi cũng sử dụng các tính chất cơ bản này trong phân tích của mình để lọc bỏ dữ liệu có sẵn và xác định nguồn gốc của các

vấn đề. Để thực hiện phân tích nhanh chóng, chúng ta cần tìm đến các kỹ thuật tự động hóa và lọc bớt dữ liệu.

Mặc dù các trường hợp ví dụ trên rất đơn giản và dễ hiểu, nhưng chúng thực sự chỉ ra một vấn đề. Phương pháp được sử dụng để xác định tiến trình đáng ngờ trong từng trường hợp không quá khác biệt so với phương pháp được sử dụng để điều tra bot-russiantopz (www.securityFocus.com/inFocus/1618) vào năm 2002. Thực tế, nó gần giống với phân tích so sánh khác biệt (Differential analysis) (nghĩa là tìm kiếm cho sự khác biệt giữa hai trạng thái). Tuy nhiên, cần lưu ý, đặc biệt nếu bạn đang thực hiện phản hồi trực tiếp (live-response) với tư cách là nhân viên thực thi pháp luật hoặc tư vấn, là trong hầu hết các trường hợp, một trạng thái ban đầu của hệ thống từ trước khi xảy ra sự cố sẽ không có sẵn và bạn phải dựa trên sự hiểu biết về hoạt động của hệ điều hành cơ bản và các ứng dụng. Ví dụ, trong trường hợp ví dụ đầu tiên, chỉ có một trường hợp inetinfo.exe trong thông tin tiến trình và tôi không biết cho dù hệ thống bị nhiễm mã độc có chạy máy chủ Web hay không, tôi có thể tương quan với những gì tôi biết (tiến trình inetinfo.exe đang chạy) với đầu ra của công cụ svc.exe, trong trường hợp này xuất hiện như sau:

736,W3SVC,World Wide Web Publishing Service
,C:\WINNT\system32\inetsrv\inetinfo.exe,Running,Auto,Share Process,#

Mối tương quan này có thể được tự động hóa thông qua việc sử dụng các công cụ có sẵn kịch bản và nếu một dịch vụ hợp pháp (như được hiển thị trước đó) được tìm thấy tương quan với một quy trình hợp pháp (inetinfo.exe với PID 736), chúng tôi đã thực hiện lọc bớt dữ liệu.

LƯU Ý:

"Công cụ svc.exe được sử dụng trong các trường hợp ví dụ thu thập thông tin về các dịch vụ trên hệ thống và hiển thị kết quả ở định dạng giá trị được phân tách bằng dấu phẩy (.csv) để có thể dễ dàng phân tích cú pháp hoặc mở trong Excel để phân tích. Các tiêu đề cột lần lượt là PID, tên dịch vụ, tên hiển thị dịch vụ, đường dẫn đến hình ảnh thực thi, trạng thái dịch vụ, chế độ bắt đầu dịch vụ, có (#) hay không (*) mô tả cho dịch vụ đấy. Nhiều lần, các tác giả phần mềm độc hại sẽ không cung cấp chuỗi mô tả cho dịch vụ của họ; thiếu chuỗi này sẽ là một lý do nghi ngờ để điều tra dịch vụ hơn nữa."

Một nguyên tắc nhỏ mà một nhà điều tra có kiến thức nên ghi nhớ trong khi phân tích dữ liệu dễ bay hơi là sự tồn tại của quy trình inetinfo.exe mà không có sự hiện diện tương ứng của dịch vụ W3SVC, World Wide Web Publishing có thể cho thấy sự hiện diện của phần mềm độc hại hoặc tại ít nhất là một quá trình đáng nghi ngờ."

Tuy nhiên, điều tra viên cũng phải lưu ý rằng quy trình inetinfo.exe cũng hỗ trợ dịch vụ File Transfer Protocol (FTP) và Simple Mail Transfer Protocol (SMTP) cho máy chủ email, dưới đây là minh họa kết quả đầu ra của –s tlist với câu lệnh:

736 inetinfo.exe Svcs: IISADMIN,MSFTPSVC,SMTPSVC,W3SVC

Nói một cách đơn giản, khi một tiến trình inetinfo.exe đang chạy mà không có các dịch vụ tương ứng cũng đang chạy thì rất có thể bạn đang gặp vấn đề đáng nghi ngờ cần kiểm tra. Tất nhiên, việc kiểm tra này cũng có thể được tự động. Ví dụ: nếu đầu ra của các công cụ FRUC được phân tích và nhập vào cơ sở dữ liệu, các câu lệnh SQL có thể được sử dụng để trích xuất và so sánh, đối chiếu các thông tin.

LƯU Ý

"Trong bài thuyết trình tại hội nghị BlackHat DC 2007, Kevin Mandia đã tuyên bố rằng một số sự cố mà công ty của ông đã chịu trách nhiệm trong năm trước đã thể hiện cách thức của các tác giả phần mềm độc hại nhằm duy trì sự tồn tại, tránh bị phát hiện trong phần mềm của họ bằng cách tự cài đặt nó như một dịch vụ Windows. Kinh nghiệm của cá nhân tôi cũng thấy vấn đề này rất đúng. Trên thực tế, trong một số lần tham gia, tôi đã thấy phần mềm độc hại xâm nhập vào hệ thống và tạo ra một dịch vụ mà sau đó, "thực thi" shell (tức là, kết nối dòng lệnh) khỏi hệ thống và tắt cơ

sở hạ tầng mạng sang hệ thống từ xa. Khi "kẻ xấu" kết nối đến điểm cuối khác, sau đó anh ta có quyền Hệ thống, mặc dù chỉ ở mức dòng lệnh, sẽ truy cập trái phép vào hệ thống bị xâm nhập."

Điều này cho thấy rằng với một chút kiến thức và kinh nghiệm, các vấn đề có thể được giải quyết một cách nhanh chóng và kỹ lưỡng, thông qua việc sử dụng tự động hóa và lọc dữ liệu. Tự động hóa rất quan trọng, vì các sự cố thường được đặc trưng bởi biến đổi, tác động bất thường. Tự động hóa cho phép chúng ta đánh mã một tiến trình và có thể theo dõi cùng một tiến trình đó nhiều lần. Nếu chúng ta biết các thành phần và bit của dữ liệu dễ bay hơi sẽ giúp cung cấp cho chúng ta một bức tranh khá đầy đủ về trạng thái của hệ thống, chúng ta có thể nhanh chóng thu thập và so sánh các thông tin, và xác định bản chất và phạm vi của sự cố. Điều này giúp chúng ta có một kết luận nhanh hơn, hành động nhanh chóng, nhưng lại kỹ lưỡng bằng cách sử dụng một số bản ghi tiến trình. Từ đây, dữ liệu dễ bay hơi bổ sung có thể được thu thập, nếu cần thiết. Sử dụng phương pháp tối giản này giúp lọc bớt lượng dữ liệu cần phân tích cú pháp và so sánh, và dẫn đến kết quả thu được tốt hơn. Liên quan đến phân tích và tự động hóa, các "quy tắc của ngón tay cái" được sử dụng bởi một nhà điều tra để xác định các tiến trình đáng ngờ trong dữ liệu dễ bay hơi được thu thập chủ yếu dựa trên kinh nghiệm và sự hiểu biết về các ứng dụng và hệ điều hành cơ bản.

LƯU Ý

"Vài năm trước, một người bạn của tôi đã gửi cho tôi dữ liệu dễ bay hơi mà anh ấy đã thu thập được trong các sự cố khác nhau. Anh ta đã sử dụng một loạt các công cụ và một file batch để thu thập dữ liệu dễ bay hơi, và rất lâu sau khi vụ án được hoàn thành, anh ta sẽ gửi cho tôi các tệp dữ liệu dạng thô, yêu cầu tôi tìm hiểu xem có vấn đề gì. Với việc không thể truy cập trạng thái ban đầu của hệ thống, tôi phải tìm kiếm manh mối trong dữ liệu anh ấy gửi cho tôi. Đây là một cách tuyệt vời để phát triển các kỹ năng và thậm chí một số công cụ phân tích cần thiết."

Một số quy tắc này có thể được đánh mã thành các hàm thủ tục và thậm chí các tập lệnh để làm cho quá trình phân tích và lọc dữ liệu hiệu quả hơn. Một ví dụ cho điều này là tiến trình svchost.exe. Một số tác giả phần mềm độc hại sử dụng trong thực tế thường có một vài bản sao của Svchost.exe đang chạy trên các hệ thống Windows (kinh nghiệm của tôi cho thấy hai bản sao chạy trên Windows 2000, năm trên Windows XP SP2 và bảy trên Windows 2003) và sử dụng tên đó cho phần mềm độc hại. Chúng tôi biết tiến trình svchost.exe hợp pháp và tuân theo một số quy tắc đơn

giản, một trong số đó là tiến trình luôn bắt nguồn từ một image thực thi nằm trong thư mục system32. Do đó, chúng ta có thể viết một tập lệnh Perl sẽ chạy với đầu ra của lệnh tlist -c và gắn cờ ngay lập tức bất kỳ bản sao nào của tiến trình svchost.exe không chạy từ thư mục system32

Đây là một biến thể của phương pháp phân tích sai số (Artificial ignorance), trong đó bạn thực hiện lọc dữ liệu bằng cách loại bỏ mọi thứ bạn biết là không có hại, và những gì còn lại rất có thể là thứ bạn cần xem xét. (Artificial ignorance là một thuật ngữ được đặt ra bởi Marcus Ranum, có thể tìm hiểu tại www.ranum.com.) Tôi đã sử dụng phương pháp này khá hiệu quả trong môi trường công ty, không chỉ trong các hoạt động ứng phó sự cố mà còn trong khi thực hiện quét mạng. cho phần mềm gián điệp và các vấn đề khác. Những gì tôi đã làm là tạo một tập lệnh Perl sẽ tiếp cận với domain controller và nhận được một danh sách tất cả các máy trạm mà nó thấy trên mạng. Sau đó, tôi kết nối với từng máy trạm bằng thông tin đăng nhập của quản trị viên trên tên miền, trích xuất nội dung của key (xem Chương 4 để biết thêm thông tin về Registry key này) từ mỗi hệ thống và lưu thông tin đó vào một tệp trên hệ thống của tôi. Lần đầu tiên tôi chạy tập lệnh này, tôi có khá nhiều trang dữ liệu để sắp xếp. Vì vậy, tôi bắt đầu điều tra một số thứ tôi tìm thấy và xác định rằng đa số trong số chúng là các ứng dụng và trình điều khiển hợp pháp. Do đó, tôi đã tạo một danh sách các mục bản ghi vô hại được biết đến và sau đó khi tôi quét các hệ thống, tôi sẽ kiểm tra thông tin mà tôi đã truy xuất theo danh sách này và chỉ ghi thông tin vào tệp nhật ký của mình nếu nó không có trong danh sách. Theo thứ tự khá ngắn, tôi đã giảm tệp nhật ký của mình xuống còn khoảng nửa trang.

Đây là một cách tiếp cận bạn có thể sử dụng để phân tích nhanh dữ liệu dễ bay hơi mà bạn đã thu thập được. Tuy nhiên, chìa khóa để phân tích nhanh và phản ứng nhanh là giảm lượng dữ liệu bạn thực sự cần điều tra. Điều này có thể có nghĩa là đưa dữ liệu bạn đã thu thập vào một hình thức dễ quản lý hơn hoặc có thể có nghĩa là loại bỏ các thành phần mà bạn biết là vô hại, do đó làm giảm lượng dữ liệu bạn cần thực sự cần để điều tra.

2.4 MỞ RỘNG PHẠM VI ĐIỀU TRA

Điều gì xảy ra khi mọi thứ trở nên phức tạp hơn so với các kịch bản mà chúng ta đã xem xét ở trên? Chúng ta có thể thấy các chuyên gia bảo mật nói trên các phương tiện truyền thông mọi lúc, rằng tội phạm mạng đang ngày càng tinh vi, nguy hiểm hơn (và thực tế đúng là như vậy). Vì vậy, làm thế nào để chúng ta đối phó với các sự cố phức tạp hơn? Rốt cuộc, không phải tất cả các tiến trình liên quan đến một sự cố có thể tồn tại lâu như những tiến trình được ví dụ trong các kịch bản trên của tôi. Chẳng hạn, một trình tải xuống có thể nằm trên một hệ thống thông qua lỗ hổng trình duyệt Web và một khi nó đã tải xuống phần mềm được chỉ định, nó đã hoàn thành mục đích và

không còn hoạt động. Do đó, thông tin về tiến trình đó, bao gồm các kết nối mạng được sử dụng bởi tiến trình, sẽ không còn khả dụng.

Cách đây không lâu, tôi đã xử lý một sự cố liên quan đến một mã thực thi được mã hóa mà không được xác định bởi hơn hai chục công cụ quét chống vi-rút. Chúng tôi cũng gặp khó khăn đáng kể khi giải quyết vấn đề này, vì không có tiến trình nào chạy có cùng tên với tệp bí ẩn trong bất kỳ hệ thống bị ảnh hưởng nào mà chúng tôi đã xem xét, kiểm tra. Phân tích động (xem Chương 6) của phần mềm độc hại cho thấy phần mềm độc hại đã tự chui vào không gian tiến trình Internet Explorer và buộc dừng tiến trình này. Một chút thông tin này cho thấy rằng chúng tôi không thể tìm thấy một tiến trình đang chạy bằng cách sử dụng cùng tên với tệp bí ẩn và tất cả những nỗ lực điều tra của chúng tôi đã đưa chúng tôi trở lại với tiến trình Internet Explorer (iexplore.exe) là thủ phạm. Chúng tôi đã xác nhận phát hiện của mình bằng cách thu thập dữ liệu dễ bay hơi thực tế là trên tất cả các hệ thống mà chúng tôi xem xét không một thiết bị nào có Internet Explorer chạy trên máy tính để bàn. Và ta có thể thấy, tiến trình iexplore.exe, sống và chạy, đưa lưu lượng truy cập ra mạng Internet, nhưng không có cửa sổ trình duyệt nào mở trên máy tính để bàn.

Điều thú vị về sự tham gia đặc biệt này là rất nhiều kỹ thuật tiêm mã độc được sử dụng, hoặc thực tế là tệp thực thi bí ẩn mà chúng tôi tìm thấy dường như không thể nhận dạng được bởi nhiều công cụ chống vi-rút. Thay vào đó, tôi nghĩ khía cạnh thú vị nhất của tất cả những điều này là vấn đề gần như đáng ngạc nhiên với một mã độc Worm có tên là “Setiri”, được giới thiệu bởi một vài nhà nghiên cứu của SensePost (www.sensepost.com/research_conferences.html) tại Hội nghị BlackHat ở Las Vegas năm 2002. Setiri vận hành bằng cách truy cập Internet Explorer dưới dạng máy chủ Component Object Model (COM) và tạo lưu lượng truy cập thông qua Internet Explorer. Thật thú vị, Dave Roth đã viết một tập lệnh Perl (www.roth.Net/perl/scripts) được gọi là IEEvents.pl, với một số sửa đổi nhỏ, sẽ khởi chạy Internet Explorer một cách vô hình (nghĩa là không có cửa sổ hiển thị trên máy tính để bàn) và truy xuất các trang Web.

Vậy vấn đề chính ở đây là gì? Chà, tôi chỉ muốn chỉ ra một số sự cố có thể phức tạp đến mức nào. Nhận được backdoor trên hệ thống thông qua một trình tải xuống, lần đầu tiên được thả vào hệ thống thông qua lỗ hổng trình duyệt Web, đặc biệt tinh vi (lại vô cùng hiệu quả) khi đối mặt với việc mã được đưa vào không gian bộ nhớ xử lý.

Một kỹ thuật khác được sử dụng bởi các tác giả mã độc nhằm mục đích thực thi mã độc của họ (và để giữ cho nó chạy) có thể được tìm thấy trong các vòng lặp phần mềm gián điệp, chẳng hạn như các đối tượng trợ giúp trình duyệt (Browser helper objects-BHOs) (bạn có thể tìm thêm thông tin về BHOs trong Chương 4). Ví dụ: hai BHO được tìm thấy trên một hệ thống là Adobe PDF Reader Link Helper và

DriveLetterAccess helper objects. Bạn có thể tìm thấy những thứ này trong không gian xử lý Internet Explorer bằng cách sử dụng listdlls.exe:

C:\Program Files\Adobe\Acrobat 7.0\ActiveX\AcroIEHelper.dll
C:\WINDOWS\System32\DLA\DLASHX_W.DLL

Hãy nhớ rằng khi phần mềm thay đổi, cập nhật các phiên bản, có thể đường dẫn tệp của chúng trong hệ thống cũng đổi. Ví dụ: với Adobe Reader Phiên bản 8, đường dẫn cho Adobe PDF Reader Link Helper là C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll.

Nếu ai đó xâm nhập hệ thống Windows từ mạng, bạn có thể mong đợi tìm thấy các dấu vết của thông tin đăng nhập (trong nhật ký sự kiện bảo mật (Security Event Log) hoặc trong bản ghi về thời gian đăng nhập cuối cùng cho người dùng đó), mở tệp trên hệ thống và thậm chí xử lý đã được đưa ra bởi người dùng đó. Nếu kẻ tấn công không sử dụng các cơ chế đăng nhập của Microsoft (Remote Desktop, sử dụng lệnh "net use", v.v.) và thay vào đó truy cập hệ thống qua "Back door", bạn có thể thấy các tiến trình đang chạy, xử lý, kết nối mạng...

Với việc hiểu biết bản chất của sự cố, bạn có thể xác định vấn đề hiệu quả hơn về các phản hồi trực tiếp (live-response) để giải quyết vấn đề, không chỉ từ góc độ thu thập dữ liệu mà còn từ góc độ phân tích và so sánh dữ liệu

2.5 CẢM NGHĨ

Sau tất cả, câu hỏi ngay lập tức được đặt ra khi xác nhận vấn đề là : " Chúng ta làm gì bây giờ ? ". Và câu trả lời là : nó phụ thuộc và cơ sở hạ tầng hệ thống của bạn. Chẳng hạn, trong những ví dụ của mục một, bạn nhận thấy những sự cố đang chạy đối với tài khoản admin. Việc mà bạn phải làm bây giờ chính là thiết lập các trường hợp để ứng phó với sự cố để tìm ra và giải quyết vấn đề đối với tài khoản admin, hoặc đối với hệ thống. Cách xử lý chung của mọi người thường trong trường hợp này, là họ không còn tin vào bất cứ điều gì của hệ thống, và cách xử lý duy nhất mà bạn nghĩ có thể chấp nhận là : BẮT ĐẦU LẠI TỪ ĐẦU (sử dụng một hệ điều hành sạch + backup lại dữ liệu từ bản sao lưu).

smss	1024	11	3	21	168	0:00:00.062	8:28:38.109
csrss	1072	13	13	555	1776	0:00:26.203	8:28:36.546

Nghĩ thì đơn giản, nhưng chưa chắc nó đã cách hay để xử lý vấn đề, mà thậm chí nó còn làm rắc rối hơn.

uedit32	940	8	1	88	4888	0:00:03.703	4:07:25.296
cmd	3232	8	1	32	2008	0:00:00.046	3:26:46.640

Thời gian kiểm soát truy cập phương tiện (MAC) trên các tệp được ghi vào ổ cứng có thể được sửa đổi để đánh lừa một điều tra viên, nhưng lượng thời gian một quy trình đã được chạy là khó giả hơn. Với thông tin này, điều tra viên có thể xây dựng một mốc thời gian khi sự cố có thể đã xảy ra và xác định mức độ chung của sự cố (tương tự như cách tiếp cận được sử dụng trong các trường hợp ví dụ trước đó). Mục tiêu là để xác định nguyên nhân gốc rễ của vấn đề, đề đưa ra phương hướng giải quyết và khắc phục. Nếu điều này không được thực hiện, hãy đặt lại một hệ thống được tải sạch trên mạng có thể sẽ dẫn đến việc hệ thống bị xâm phạm trở lại. Nếu hệ thống cần phải được vá, các bản vá có thể được tung ra. Tuy nhiên, nếu nguyên nhân gốc rễ của sự cố là thực sự là một mật khẩu Quản trị viên yếu, không có số lượng bản vá nào sẽ khắc phục vấn đề đó. Các điều tương tự cũng đúng với các lỗ hổng cấu hình ứng dụng, chẳng hạn như được khai thác bởi những " con sâu " mạng.

Bây giờ, hãy xem xét một trường hợp khác : VD : quy trình đáng ngờ được tìm thấy là một dịch vụ, và đầu ra của pslist.exe cho chúng ta thấy rằng quá trình đã được chạy gần giống nhau lượng thời gian như chính hệ thống. Nhưng: vì dường như không có bất kỳ API Windows nào cho phép kẻ tấn công sửa đổi lần LastWrite trên khóa Registry (lần MAC trên tệp có thể dễ dàng sửa đổi thông qua việc sử dụng các API tài liệu công khai), một điều tra viên có thể trích xuất thông tin đó từ một hệ thống trực tiếp và xác định khi nào dịch vụ được cài đặt trên hệ thống. Một điều tra viên am hiểu biết rằng để cài đặt một dịch vụ Windows, người dùng bối cảnh phải là của Quản trị viên, vì vậy hãy kiểm tra thông tin đăng nhập của người dùng và hoạt động của người dùng trên hệ thống có thể dẫn đến nguyên nhân gốc rễ của sự cố. Một lần nữa, điều quan trọng là xác định nguyên nhân gốc rễ của sự cố để tình huống có thể được khắc phục, không chỉ trên hệ thống bị xâm nhập mà còn trên các hệ thống khác.

CẢNH BÁO :

Theo như Microsoft cho biết : "Phân tích cho đến nay cho thấy những kẻ tấn công dường như đã đạt được mục nhập vào hệ thống bằng cách sử dụng mật khẩu quản trị viên yếu hoặc trống. Microsoft không có bằng chứng để đề nghị rằng bất kỳ lỗ hổng bảo mật không xác định trước đây đã được sử dụng trong cuộc tấn công ". Chỉ cần cài đặt lại hệ điều hành, ứng dụng và dữ liệu trên các hệ thống bị ảnh hưởng sẽ dẫn đến sự thỏa hiệp của họ một lần nữa, miễn là các cài đặt cấu hình tương tự đã được sử dụng. Trong môi trường doanh nghiệp, tài khoản Quản trị viên cộng đồng có mật khẩu yếu được sử dụng và một hệ thống được cài đặt lại rất có thể sẽ sử dụng tương tự tên tài khoản và mật khẩu như đã xảy ra trước khi xảy ra sự cố ".

2.6 SỰ PHÒNG NGỪA

Một điều mà bộ phận CNTT có thể làm để giúp công việc ứng phó với các sự cố trở nên dễ dàng hơn (lưu ý rằng những người phản hồi đầu tiên thường là thành viên của nhân viên CNTT) sẽ vượt xa chỉ cần cài đặt hệ điều hành và các ứng dụng và sử dụng hệ thống cứng hướng dẫn và quy trình quản lý cấu hình. Ví dụ: bằng cách giới hạn hoạt động các dịch vụ và quy trình trên máy chủ chỉ những dịch vụ cần thiết cho hoạt động của Bản thân hệ thống, bạn giới hạn bề mặt tấn công của hệ thống. Sau đó, đối với các dịch vụ bạn chạy, cấu hình chúng một cách an toàn nhất có thể. Nếu bạn có máy chủ Web IIS đang chạy, hệ thống đó có thể là một máy chủ Web, nhưng nó cũng là một máy chủ FTP? Nếu bạn không cần máy chủ FTP đang chạy, vô hiệu hóa nó, loại bỏ nó, hoặc don thậm chí cài đặt nó ở nơi đầu tiên. Sau đó, cấu hình máy chủ Web của bạn chỉ sử dụng ánh xạ tập lệnh cần thiết (máy chủ Web IIS với ánh xạ tập lệnh .ida đã bị xóa không dễ bị nhiễm Code Red năm 2001) và thậm chí bạn có thể muốn để cài đặt công cụ UrlScan:

http://technet.microsoft.com/en-us/security/cc242650.aspx

LƯU Ý

Tool UrlScan, có sẵn từ Microsoft, hỗ trợ IIS Phiên bản 6.0 và Blog bảo mật IIS Nazim từ (http://bloss.iis.net/nazim/default.aspx) đề cập rằng UrlScan 3.0 có sẵn cho chúng ta trong việc bảo vệ.

Cách tiếp cận tối giản tương tự này cũng áp dụng cho việc thiết lập người dùng trên một hệ thống. Chỉ những người dùng cần thiết mới có quyền truy cập vào hệ thống. Nếu người dùng không cần truy cập vào hệ thống, để đăng nhập từ bảng điều khiển hoặc truy cập hệ thống từ xa mạng, thì không nên được cập tài khoản. Ví dụ trong một số trường hợp: tài khoản người dùng cũ có mật khẩu yếu bị bỏ lại trên các hệ thống và những kẻ xâm nhập đã có thể truy cập vào hệ thống thông qua các tài khoản đó. Example 1 chẳng hạn, một hệ thống bị xâm nhập đã hiển thị thông tin đăng nhập thông qua tài khoản người dùng trong thời gian đó được biết rằng người được chỉ định tài khoản đó đã ở trên máy bay hơn 33.000 feet Trung Tây Hoa Kỳ. Tuy nhiên, user đó hiếm khi sử dụng tài khoản của mình để truy cập vào hệ thống. Bằng cách giảm bề mặt tấn công của một hệ thống, ta có thể gây khó khăn (thậm chí có thể thực sự khó khăn) để ai đó có quyền truy cập vào hệ thống đó, để thỏa hiệp dữ liệu trên hệ thống hoặc sử dụng hệ thống đó như một bước đệm để từ đó tiến hành các cuộc tấn công tiếp theo. Kẻ tấn công có thể sau đó hoặc tạo ra rất nhiều tiếng ồn trên mạng trên hệ thống, dưới dạng các mục nhật ký và lỗi tin nhắn, làm cho các nỗ lực trở nên rõ

ràng hơn đối với các quản trị viên, hoặc đơn giản là từ bỏ vì Làm tổn hại hệ thống, đó là một chiến thắng dễ dàng. Một cách khác, tôi có thể đối phó với một vài Các tệp nhật ký có giá trị megabyte, hiển thị các lần thử thất bại (như khi sâu Nimda phổ biến; xem www.cert.org/advisories/CA-2001-26.html) hơn là một hệ thống bị xâm phạm nhiều lần do thiếu bất kỳ loại cứng hoặc theo dõi. Ít nhất là nếu một số bước có được thực hiện để hạn chế bề mặt tấn công và mức độ mà hệ thống có thể bị xâm phạm, một điều tra viên sẽ có nhiều dữ liệu hơn để làm việc, trong các tệp nhật ký và các dạng dữ liệu khác.

2.7 TÓM LƯỢC

Khi thu thập dữ liệu điện động có thời gian tồn tại ngắn, bước tiếp theo là phân tích dữ liệu đó và cung cấp một phản ứng hiệu quả và kịp thời. Nhiều lần, các nhà điều tra có thể bị choáng ngợp với khối lượng dữ liệu điện động mà họ cần phải vượt qua, và điều này có thể trở nên áp đảo hơn nếu họ không chắc chắn những gì họ đã tìm kiếm. Bắt đầu với một số ý tưởng về bản chất vấn đề, nhà điều tra có thể bắt đầu giảm lượng dữ liệu bằng cách tìm kiếm và phân tích ra các quy trình tốt được biết đến, các kết nối mạng, người dùng tích cực, v.v. Tự động hóa một số tương quan dữ liệu, tiếp tục giảm tổng lượng dữ liệu, và giảm số lượng sai lầm có thể được thực hiện. Tất cả những điều này sẽ dẫn đến phản ứng kịp thời, chính xác và hiệu quả cho các sự cố.

2.8 GIẢI PHÁP THEO DÕI NHANH

PHÂN TÍCH DỮ LIỆU

- Phản ứng trực tiếp thường được đặc trưng bởi căng thẳng, áp lực và nhầm lẫn. Các nhà điều tra có thể sử dụng các kỹ thuật tự động và giảm dữ liệu để cung cấp đáp ứng hiệu quả.
- Khi dữ liệu đã được thu thập và phân tích, phản hồi cuối cùng về sự cố có thể được dựa trên các yếu tố phi kỹ thuật, chẳng hạn như cơ sở hạ tầng kinh doanh hoặc chính trị của môi trường.
- Thực hiện phân tích nguyên nhân gốc rễ khi gặp sự cố có thể đi một chặng đường dài hướng tới tiết kiệm cả thời gian và tiền bạc.
- Thực hiện một cách tiếp cận tối giản để cấu hình hệ thống thường có thể phục vụ để cản trở hoặc thậm chí ức chế một sự cố hoàn toàn. Ít nhất, làm cho một hệ thống khó khăn hơn. Để thỏa hiệp sẽ tạo ra tiếng ồn Tiếng Việt và thậm chí có thể cảnh báo trong các lần thử.

2.9 CÁC CÂU HỎI THƯỜNG GẶP

Câu hỏi	Sự khác nhau giữa “ quá trình “ và “ dịch vụ “ là gì ?
Đáp	Có rất nhiều điểm khác nhau giữa “ quá trình “ và “ dịch vụ “ , ngoại trừ cách mỗi cái được bắt đầu hoặc khởi chạy, và bối cảnh người dùng thực hiện chạy “ quá trình/ dịch vụ” . Các dịch vụ Windows thực sự là các quá trình và có thể được khởi động tự động khi hệ thống khởi động. Khi một quy trình được bắt đầu như một dịch vụ, nó thường chạy với các đặc quyền cấp Hệ thống, trong khi các quy trình được khởi động tự động thông qua một tổ hợp người dùng Đăng ký sẽ chạy trong bối cảnh của người dùng đó.
Câu hỏi	Tôi nhìn thấy một số lưu lượng không liên tục và bất thường trong nhật ký tường lửa của mình. Lưu lượng truy cập dường như bắt nguồn từ một hệ thống trên mạng của tôi và đi ra một hệ thống khác thường. Khi tôi thấy lưu lượng, tôi vào hệ thống và thu thập dữ liệu dễ bay hơi, nhưng tôi không thấy bất kỳ kết nối mạng nào đang hoạt động, hoặc bất kỳ quy trình hoạt động nào sử dụng cổng nguồn tôi tìm thấy trong lưu lượng. Sau đó tôi thấy giao thông trở lại sáu giờ sau. Tôi có thể làm gì?
Đáp	Trong tệp fruc.ini được sử dụng trong các trường hợp ví dụ trong chương này, tôi đã sử dụng autorunsc.exe từ Microsoft / Sysiternals để thu thập thông tin về các vị trí tự khởi động. Hãy chắc chắn kiểm tra các tác vụ theo lịch trình, cũng như bất kỳ quy trình bất thường nào có thể khởi chạy một quy trình con để tạo lưu lượng truy cập.
Câu hỏi	Tôi có một sự cố mà tôi đã cố gắng điều tra, nhưng dường như tôi có thể tìm thấy bất kỳ dấu hiệu nào của sự cố trên hệ thống ?
Đáp	Đây có vẻ là hành vi khác thường hoặc có thể nghi ngờ trên một hệ thống Windows được tạo ra do chưa quen hệ thống hơn là một sự cố thực tế. Tôi đã thấy người trả lời đặt câu hỏi về sự tồn tại của một số tệp và thư mục nhất định (Prefetch, v.v.) không vì lý do nào khác ngoài việc họ không quen với hệ thống.

	Trong thực tế, tôi nhớ một trường hợp quản trị viên đã xóa tất cả các tệp có phần mở rộng .pf mà anh ta tìm thấy trong thư mục C: \\ Windows \\ Prefetch (Chương 5). Vài ngày sau, nhiều tệp trong số đó đã quay trở lại một cách bí ẩn và anh cảm thấy hệ thống đã bị xâm nhập bởi một Trojan hoặc backdoor.