HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

🙦🙤🟇🙦🙤



BÀI TẬP LỚN

**Đề tài** :

**LEARNING NETWORK FORENSICS**

**CHAP 10 – CLOSING THE DEAL SOLVING THE CASE**

***Môn học*** *:* ***Phòng chống và điều tra tội phạm mạng máy tính – Lớp L02***

**Giảng viên hướng dẫn: Lại Minh Tuấn**

**SV thực hiện:**

Nguyễn Thị Huyền– AT12I

NguyễnVăn Luân– AT12I

Nguyễn Thị Xuân – AT12I

*Hà Nội, 25 tháng 11 năm 2019*

Nhận xét của giảng viên ………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**MỤC LỤC**

[**I.** **Xem xét lại phương pháp luận nghiên cứu TAARA** 4](#_Toc25612084)

[**II.** **Xem xét lại các trường hợp** 5](#_Toc25612085)

[**III.** **Trigger of the case** 11](#_Toc25612086)

[**IV.** **Thu thập thông tin và bằng chứng** 12](#_Toc25612087)

[**V.** **Phân tích dữ liệu thu thập - đào sâu** 17](#_Toc25612088)

[**VI.** **Báo cáo các trường hợp** 23](#_Toc25612089)

[**VII.** **Hành động vì tương lai** 24](#_Toc25612090)

[**VIII.** **Tương lai của điều tra mạng** 25](#_Toc25612091)

[**IX.** **Tóm lược** 26](#_Toc25612092)

**LỜI NÓI ĐẦU**

Giống như phương châm của các Thế vận hội Olympic mạng nhanh hơn, cao hơn, mạnh hơn ngày nay nhanh hơn, rộng hơn và lớn hơn. Đối với các mạng tốc độ cao trên diện rộng, việc mang khối lượng dữ liệu lớn hơn đã trở thành một tiêu chuẩn chứ không phải là ngoại lệ. Tất cả các đặc điểm này đi kèm với sự tiếp xúc lớn với một loạt các mối đe dọa lớn đối với dữ liệu được thực hiện bởi các mạng. Bối cảnh mối đe dọa hiện tại đòi hỏi sự hiểu biết ngày càng tăng về dữ liệu trên các mạng của chúng tôi, cách chúng tôi bảo mật dữ liệu và các dấu hiệu nhận biết bị bỏ lại sau một sự cố. Cuốn sách này nhằm mục đích giới thiệu chủ đề pháp y mạng để giúp tiếp tục tìm hiểu cách thức truyền dữ liệu qua mạng cũng như giới thiệu khả năng điều tra các cổ vật pháp y hoặc manh mối để thu thập thêm thông tin liên quan đến vụ việc.

**CHƯƠNG 10. KẾT THÚC THỎA THUẬN – GIẢI QUYẾT VẤN ĐỀ**

Hành trình của chúng tôi, cho đến nay, là một điều thú vị. Khi chúng tôi đi qua đại dương điều tra mạng này, chúng tôi dừng lại ở nhiều điểm dừng và đảo trên đường để tăng cường hiểu biết về môi trường. Những điểm dừng này đã giúp chúng tôi hiểu các công cụ, công nghệ và kỹ thuật khác nhau được yêu cầu để tiến hành điều tra mạng. Chúng tôi đã thấy việc sử dụng điều tra bộ nhớ cho phép chúng tôi tạo ra hình ảnh của nội dung RAM, cách trình thám thính gói cho phép chúng tôi lấy dữ liệu mạng và cũng như cách các máy chủ phát hiện và ngăn chặn xâm nhập khác nhau đóng vai trò bảo vệ mạng. Một phân tích về nhật ký được tạo ra bởi proxy, tường lửa và hệ thống phát hiện và ngăn chặn xâm nhập đã giúp chúng tôi hiểu rõ hơn về mạng, hành vi của họ và các hiện vật điều tra khác nhau để lại cho chúng tôi để tìm bằng chứng về hoạt động độc hại. Chúng tôi cũng đã nghiên cứu về phần mềm độc hại và các loại phần mềm khác nhau và cách phần mềm độc hại ảnh hưởng đến hệ thống của chúng tôi và các bước khác nhau liên quan đến việc điều tra. Khi chuyến du hành xuyên đại dương của chúng ta kết thúc, chúng ta cần phải gắn kết kiến ​​thức của mình lại với nhau để tạo thành một bản đồ về hành trình của chúng ta thông qua điều tra mạng và xem làm thế nào chúng ta có thể sử dụng tất cả kiến ​​thức này để sử dụng tốt theo cách tích hợp.

Trong chương cuối cùng này, chúng tôi sẽ đề cập đến các khía cạnh tốt hơn và cung cấp các chi tiết hoàn thiện để xử lý, xử lý, điều tra và đóng thành công một vụ án điều tra mạng. Bây giờ đã đến lúc tất cả các Network 007 thực hiện hành trình cuối cùng này thông qua mạng của chúng tôi để tìm hiểu trò chơi kết thúc. Đó là những gì thực sự quan trọng!

Chúng tôi sẽ giải quyết trường hợp của chúng tôi theo các bước sau:

* Xem xét lại phương pháp luận nghiên cứu TAARA
* Xem xét lại các trường hợp
* Thu thập thông tin và bằng chứng
* Phân tích dữ liệu thu thập - đào sâu
* Báo cáo các trường hợp
* Hành động vì tương lai
* Tương lai của điều tra mạng

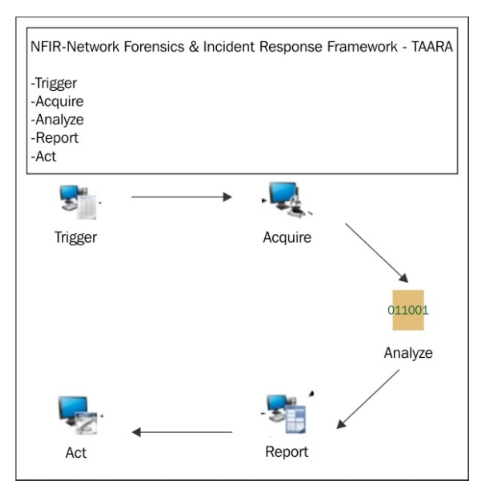
1. **Xem xét lại phương pháp luận nghiên cứu TAARA**

Hãy làm một đánh giá nhanh về pháp lý và phương pháp ứng phó sự cố mạng TAARA.

Như chúng ta đã biết trong Chương 1, Trở thành Mạng 007, TAARA là viết tắt của những điều sau đây:

* **Kích hoạt**: Đây là sự kiện dẫn đến một cuộc điều tra.
* **Tiếp thu**: Đây là quá trình được thiết lập trong chuyển động bởi trình kích hoạt; điều này được xác định trước như là một phần của kế hoạch ứng phó sự cố và liên quan đến việc xác định, thu nhận và thu thập thông tin và bằng chứng liên quan đến vụ việc. Điều này bao gồm nhận thông tin liên quan đến các yếu tố kích hoạt, lý do nghi ngờ sự cố và xác định và thu thập các nguồn bằng chứng cho phân tích tiếp theo.
* **Phân tích**: Tất cả các bằng chứng được thu thập hiện được đối chiếu, tương quan và phân tích. Chuỗi các sự kiện được xác định. Các câu hỏi thích hợp liên quan đến việc sự cố có thực sự xảy ra hay không; nếu nó đã xảy ra, chính xác những gì đã xảy ra, nó đã xảy ra như thế nào, ai có liên quan, mức độ thỏa hiệp là gì, v.v.
* **Báo cáo**: Dựa trên phân tích trước đó, một báo cáo được tạo ra trước các bên liên quan để xác định quá trình hành động tiếp theo.
* **Hành động**: Hành động được đề xuất trong báo cáo thường được thực hiện trong giai đoạn này.

Hình ảnh sau đây cho chúng ta cái nhìn tổng quan về cuộc điều tra mạng phương pháp luận, TAARA:



1. **Xem xét lại các trường hợp**

Một tổ chức đa quốc gia khá lớn đã triển khai Hệ thống quản lý & phân tích dữ liệu cuộc gọi hoặc gọi tắt là CDAM (đây là giải pháp phân tích dữ liệu nhật ký điện thoại.). Là một phần của quy trình thiết lập, nhóm các chuyên gia tư vấn triển khai được yêu cầu nhập và phân tích một khối lượng cuộc gọi rất lớn mà CNTT nội bộ nhận được bàn trợ giúp. Dữ liệu dài hàng năm của nhật ký cuộc gọi từ điện tử toàn tổ chức hiện có hệ thống trao đổi chi nhánh tự động tư nhân (EPABX) đã được hệ thống ăn sâu. Các cuộc gọi được lọc dựa trên hướng cuộc gọi và đích (các cuộc gọi đến bàn trợ giúp CNTT) và được định vị địa lý cũng như phân loại dựa trên bộ phận. Một cái nhìn sơ bộ cho thấy các xu hướng thú vị sau đây:

* Các cuộc gọi từ một số số di động (tương tự như chuỗi do công ty sở hữu ở các khu vực địa lý cụ thể) vào giờ lẻ từ một nhân viên cấp cao Gọi từ bộ phận sản xuất / điều khiển máy tính điều khiển số (CNC) yêu cầu hỗ trợ liên quan đến các vấn đề về hiệu suất của hệ thống của họ do lý do không xác định
* Các cuộc gọi từ nước ngoài nơi tổ chức không có hoạt động Các cuộc gọi từ trụ sở công ty vào giờ hành chính
* Các cuộc gọi liên tục từ một vài người dùng cụ thể cứ sau hai giờ hoặc lâu hơn.

Trong khi hầu hết các cuộc gọi biểu thị chỉ một ngày khác trong cuộc đời của một kỹ thuật viên trợ giúp CNTT, một phân tích chuyên sâu về các cuộc gọi dường như biểu thị rằng có gì đó không ổn.

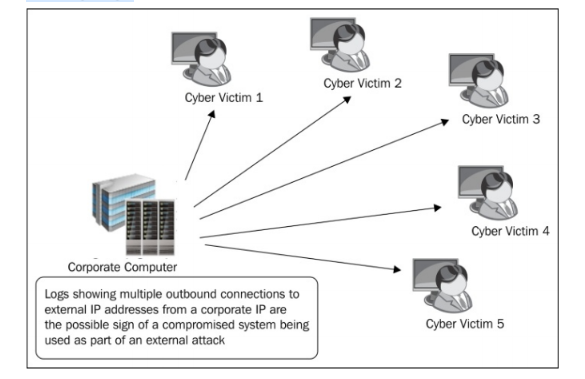
Tất cả các sự cố trước đó đã được kiểm tra chi tiết hơn. Một số được phát hiện liên quan đến yêu cầu thiết lập lại mật khẩu hóa ra là các nỗ lực kỹ thuật xã hội, một số khác liên quan đến nhiễm trùng dai dẳng, cũng như các cuộc tấn công đang diễn ra; bộ phận CNC đã có quyền truy cập USB mở như một yêu cầu chức năng và điều này dẫn đến sự phát triển của phần mềm độc hại và thời gian ngừng hoạt động đắt đỏ.

Khi các mẫu này đã được xác định, việc thực hiện các hành động phòng ngừa trở nên khá dễ dàng bằng cách đặt các số kỹ thuật xã hội bên ngoài và các tiện ích mở rộng yêu cầu đặt lại mật khẩu ngoài giờ làm việc trong danh sách theo dõi điện thoại. Các mẫu điện thoại khác có tương quan với sự cố bảo mật và những sự cố này được xác định là Các chỉ số ban đầu của Thỏa hiệp (IOC). Nói chung, việc giới thiệu CDAM đã bổ sung một khía cạnh hoàn toàn mới cho các cuộc điều tra mạng, cũng như hoạt động như một hệ thống cảnh báo sớm dựa trên phân tích hành vi.

Câu chuyện minh họa làm thế nào các nguồn thông tin khác nhau có thể hoạt động như một yếu tố kích hoạt dẫn đến một cuộc điều tra mạng đầy đủ. Điều này cũng có thể dựa trên các quy tắc được thực hiện trong các thiết bị bảo mật vành đai khác nhau như tường lửa, hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS).

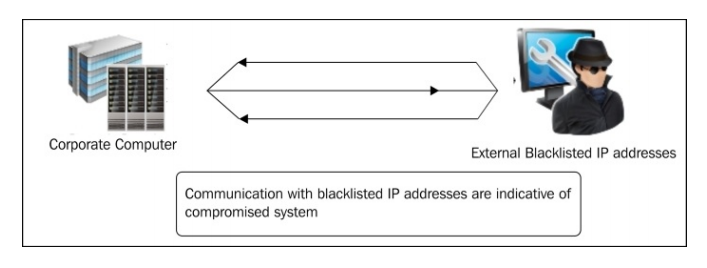
Một số triggers được liệt kê như sau:

* **Nhiều kết nối ra**: Nhiều kết nối ngoài từ một máy chủ nội bộ trong một khoảng thời gian ngắn có thể cho thấy một máy chủ bị xâm nhập đang được sử dụng để tấn công các hệ thống bên ngoài. Một ví dụ cho điều này sẽ là một email máy tính của công ty bị xâm nhập gửi email không mong muốn với nội dung độc hại như được minh họa trong hình ảnh sau đây:



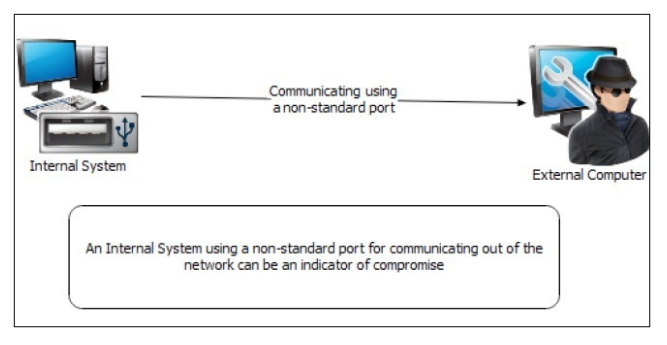
* **Sự kết nối với các địa chỉ IP hoặc URL độc hại được liệt kê**: Khi nền kinh tế phần mềm độc hại bùng nổ, số lượng URL và địa chỉ IP phục vụ phần mềm độc hại đang gia tăng. Bất kỳ máy chủ nội bộ nào liên lạc với một địa chỉ IP hoặc URL độc hại đã biết sẽ là nguyên nhân gây lo ngại nhất định cho bất kỳ quản trị viên hệ thống nào. Để cho phép các tổ chức nhằm chặn truy cập vào các trang web và URL độc hại như vậy, một số tổ chức liên tục duy trì và xuất bản danh sách chặn. Một số trong số này được thể hiện như sau:
* Arbor Networks: https://atlas.arbor.net/
* Clean MX database: http://support.clean-mx.de/clean-mx/viruses
* Malc0de Database: http://malc0de.com/database/
* Malware Domain Blocklist: http://www.malwaredomains.com/wordpress/?
* page\_id=66
* FireHOL IP lists: http://iplists.firehol.org/
* OpenPhish: http://openphish.com/
* Scumware: http://www.scumware.org/
* MalwareURL List: http://www.malwareurl.com/

Giao tiếp giữa các mạng công ty và thế giới bên ngoài được mô tả trong hình ảnh sau:

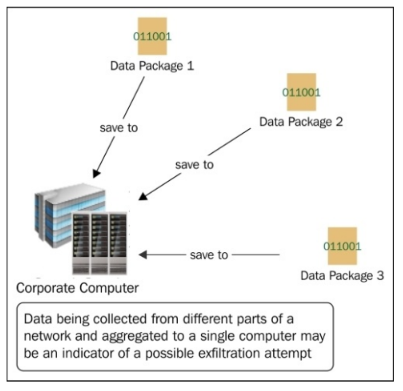


Những thông tin liên lạc có thể được hướng vào trong hoặc ra ngoài. Địa chỉ IP và URL phục vụ phần mềm độc hại phải chịu sự giám sát và hoạt động gỡ xuống liên tục. Do đó, các danh sách này có tính chất động và cần được cập nhật liên tục để đảm bảo tổ chức phòng thủ của tổ chức được cập nhật.

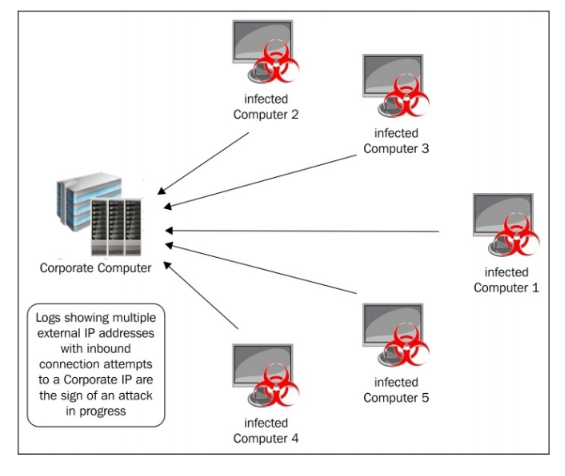
* **Dịch vụ tiêu chuẩn sử dụng cổng không chuẩn**: Giao tiếp với địa chỉ IP bên ngoài bằng cổng không chuẩn là cờ đỏ và có thể là dấu hiệu của hệ thống bị xâm nhập. Ví dụ: FTP là một giao thức thường tương quan với các cổng 20 và 21. Trong trường hợp chúng ta bắt gặp các mục trong nhật ký liên quan đến việc sử dụng FTP trên các cổng được đánh số cao hơn (mà chúng ta không biết), có một điểm mạnh khả năng hệ thống của chúng tôi đã bị xâm phạm như được đưa ra trong hình ảnh sau:



* **Chuyển động dữ liệu bên**: Truyền dữ liệu quá mức đến một hệ thống cụ thể từ toàn doanh nghiệp là một IOC tốt khác. Bất kỳ việc thu thập dữ liệu nào ở một vị trí tối nghĩa của mạng đều có thể báo hiệu việc hết dữ liệu theo kế hoạch sau khi thỏa hiệp. Các dấu hiệu của việc này xảy ra có thể bao gồm việc truyền dữ liệu ngoài giờ vào hệ thống khác với các hoạt động thông thường, sử dụng quá mức tài nguyên mạng, sự hiện diện của dữ liệu ở những nơi không được phép, v.v. Cách thức hoạt động của Công cụ gói nâng cao (APT) bằng cách truy cập vào mạng, xác định các tài sản kỹ thuật số quan tâm, chuyển động bên của các tài sản này, thu thập tài sản kỹ thuật số ở một nơi, xây dựng các phân đoạn lưu trữ có thể quản lý, mã hóa chúng và cuối cùng là xử lý chúng . Cuối cùng, những tài liệu lưu trữ trên mạng Nạn nhân bị xóa để che dấu vết và tăng tính bền bỉ. Exfiltration có thể là một quá trình phức tạp vì nó liên quan đến việc tải lên khối lượng lớn dữ liệu mà không có kiến ​​thức về nạn nhân hoặc phát hiện bởi các phòng thủ vành đai của nạn nhân. Trong trường hợp liên quan đến sự phức tạp bên trong, việc exfiltment có thể xảy ra bằng cách đơn giản như mang dữ liệu ra ngoài ổ cứng ngoài; trong khi trong các trường hợp liên quan đến hành động từ xa, exfiltration có thể đi theo những con đường phức tạp hơn. Các trường hợp dữ liệu được lọc ra đã được ngụy trang thành lưu lượng HTTP hoặc HTTPS bình thường là phổ biến. Kỳ lạ hơn các phương pháp như ngụy trang dữ liệu đã được lọc thành video và tải chúng lên đám mây (lên các trang chia sẻ video) cũng đã được quan sát như thể hiện trong hình ảnh sau:

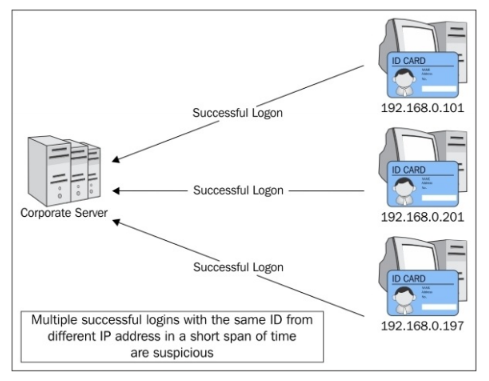


* **Nhiều kết nối gửi đến**: Nhiều kết nối gửi đồng thời gửi yêu cầu đến một tài nguyên mạng cụ thể có thể là dấu hiệu của một cuộc tấn công đang diễn ra. Nếu nhật ký cho thấy số lượng yêu cầu bất thường (chẳng hạn như ping), có khả năng lớn là một nỗ lực đang được thực hiện để áp đảo mạng có sẵn các tài nguyên và một cuộc tấn công từ chối dịch vụ đang được tiến hành, như thể hiện trong hình ảnh sau đây:



* **Nhiều lần đăng nhập**: Nhiều lần đăng nhập từ các vị trí khác nhau vào cùng một tài nguyên hoặc khác nhau cùng một lúc có thể chỉ ra trường hợp thông tin đăng nhập bị xâm phạm. Điều khá phổ biến là những kẻ tấn công khai thác nhanh chóng các thông tin bị xâm phạm để đạt được số dặm tối đa có thể trong thời gian ngắn nhất. Điều này dẫn đến nhiều

cố gắng đăng nhập vào các tài nguyên tổ chức khác nhau để giúp xác định phạm vi truy cập có sẵn. Những thông tin này cũng có thể đã được bán trực tuyến và có thể được sử dụng bởi nhiều người cho các mục đích bất chính khác nhau, như trong hình sau:



Như chúng ta có thể thấy, có một số lượng lớn các hành động đã biết và chưa biết trước đây có thể kích hoạt một cuộc điều tra. Nó thường bắt đầu với việc người dùng phàn nàn về hành vi hệ thống lạ, bao gồm truy cập chậm và có thể tiếp tục theo vòng xoáy đi lên.

Hãy để chúng tôi xem xét trường hợp mà chúng tôi bắt buộc phải điều tra.

1. **Trigger of the case**

Một buổi sáng thứ Hai tốt đẹp, một tổ chức đã bị tấn công bởi nhu cầu tiền chuộc. Một e-mail, được gửi trực tiếp đến CEO, đe dọa sự lộ diện của một khối lượng rất lớn thông tin bí mật của công ty trên mạng trừ khi một khoản tiền lớn được chuyển đến ví Bitcoin được chỉ định. Một số dữ liệu mẫu rất nhạy cảm được đính kèm vào e-mail để cho vay tín nhiệm đối với các mối đe dọa. Hơn nữa, các phương tiện truyền thông gần đây đã đưa chủ đề của các công ty bị tấn công bởi ransomware lên hàng đầu trong sự chú ý của CEO. Giám đốc điều hành đã hoàn toàn run rẩy và không biết gọi ai. Chỉ cần ý tưởng rằng thông tin bí mật có thể xuất hiện trên Web là đủ để gây ra sự đau khổ lớn. Anh ta có thể tưởng tượng sự công khai tiêu cực, giảm giá cổ phiếu, mất niềm tin của khách hàng, sa thải, sự can thiệp của chính phủ và những hậu quả khác sẽ xảy ra sau sự kiện đó.

Sau nhiều lần cân nhắc, ông đã gọi cho CFO, người đã lần lượt gọi CSO và CISO để thảo luận chi tiết về vấn đề này. Rất nhiều suy nghĩ và thảo luận sau đó, nó đã được quyết định tham gia vào một thành viên Nhóm tin cậy khóa đáng tin cậy với các kỹ năng điều tra mạng để xác định nơi rò rỉ xảy ra từ và chứa tiếp xúc như vậy hơn nữa. Thành viên trong nhóm được yêu cầu giữ thông tin cho chính mình và tiến hành điều tra một cách tự tin nhất có thể. Một câu chuyện trang bìa đã được tạo ra để làm cho cuộc điều tra có vẻ giống như một cuộc kiểm toán thông thường. Điều tra viên bị buộc tội với tóm tắt sau:

* Giữ bí mật điều tra; ngay cả câu chuyện trang bìa cũng được truyền đạt trên cơ sở cần biết.
* Thu thập thông tin về vi phạm và xác định mức độ của nó, liệu datanapper có thực sự có tất cả dữ liệu mà họ tuyên bố là có?
* Tìm hiểu làm thế nào vi phạm xảy ra.
* Là người trong cuộc có liên quan?
* Đề nghị kiểm soát để ngăn chặn sự lặp lại của vụ việc.
* Tất cả những điều này đã được thực hiện vào ngày hôm qua (một thực tế đáng buồn của một nhà điều tra mạng lưới Cuộc sống là tất cả các công việc cần phải được thực hiện vào ngày hôm qua).

1. **Thu thập thông tin và bằng chứng**

Giai đoạn được đặt ra, các mục tiêu đã rõ ràng, đã đến lúc chúng ta bắt đầu. Như đã đề cập trong các chương trước, chúng ta cần phải có kế hoạch; bây giờ là lúc kế hoạch đi vào hành động.

Tuy nhiên, trước khi chúng tôi bắt đầu, chúng tôi cần nhấn mạnh vào cách chúng tôi tiếp thu thông tin và bằng chứng. Một cú trượt nhỏ trong cách chúng ta xử lý điều này có thể có sự phân nhánh rộng khắp. Do đó, chúng ta cần tập trung vào cách xử lý giai đoạn này.

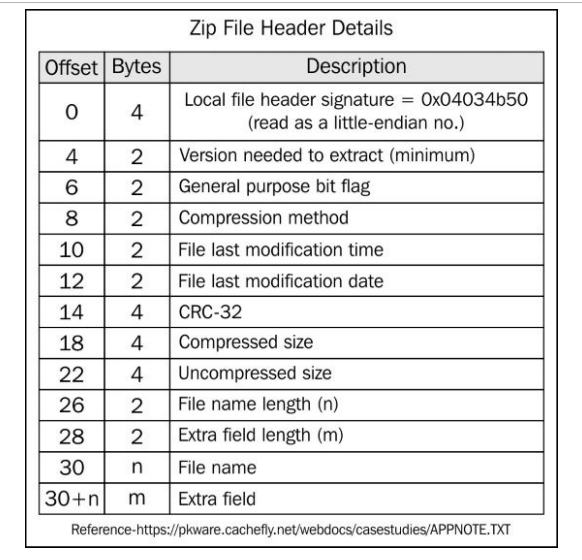
Như bạn đã học trong các chương trước, bằng chứng kỹ thuật số là vô cùng mong manh. Trong thực tế, giống như thuốc, bằng chứng kỹ thuật số đi kèm với ngày hết hạn. Sự vô thường của dữ liệu trong bộ nhớ, tính tuần hoàn của vòng quay nhật ký, lưu trữ dễ bay hơi, suy giảm dữ liệu trên phương tiện truyền thông và phần mềm độc hại góp phần làm mất đáng kể bằng chứng có giá trị trừ khi được thu thập, lưu trữ và xử lý cẩn thận. Tất cả các nhà điều tra cần xem xét các điểm sau:

* Tất cả các hành động được thực hiện phải nằm trong phạm vi của luật pháp
* Tất cả các hành động được thực hiện phải nằm trong nội dung chính sách của công ty
* Cần cố gắng thu thập tất cả các thông tin liên quan đến vụ việc trước khi bắt đầu quá trình thu thập chứng cứ, điều này cho phép hiểu rõ hơn về vụ án và giúp điều tra viên ghi lại các nguồn chứng cứ có thể
* Bản thân quá trình thu thập chứng cứ không nên làm thay đổi chứng cứ theo bất kỳ cách nào
* Tất cả các bằng chứng được thu thập phải là một bản sao được chứng thực của bản gốc
* Lưu trữ an toàn riêng biệt cho các bằng chứng thu thập nên được cung cấp để đảm bảo tính toàn vẹn và chuỗi hành trình sản phẩm
* Cần nhấn mạnh vào việc ghi chép đúng toàn bộ quá trình theo cách có thể đứng lên trước tòa án nếu cần
* Đối với mục đích của phần còn lại của chương, chúng tôi sẽ cho rằng các nhóm điều tra của chúng tôi đã thực hiện tất cả các biện pháp phòng ngừa cần thiết trong khi theo đuổi vụ kiện. Chúng tôi cũng nhấn mạnh rằng tất cả các chính sách và thủ tục được tuân thủ trong khi truy cập dữ liệu bằng chứng.

Phần đầu tiên của giai đoạn mua lại liên quan đến việc thu thập tất cả các thông tin liên quan đến vụ án. Bắt đầu cuộc điều tra bao gồm một nghiên cứu về kích hoạt để xác định quá trình hành động tiếp theo. Trong trường hợp của chúng tôi, e-mail cho CEO là kích hoạt. Do đó, e-mail là bit thông tin đầu tiên được kiểm tra để khởi động cuộc điều tra. Một cuộc thảo luận sơ bộ với nhóm CXO cũng như cái nhìn chi tiết về các tiêu đề email đã đưa ra những sự thật thú vị sau đây:

* ID e-mail trực tiếp CEO CEO không được biết đến bên ngoài tổ chức. Trên thực tế, tất cả các thư được gửi cho CEO thực sự sẽ hạ cánh tại bàn trợ lý của anh ấy và cô ấy sẽ lọc và sau đó chuyển tiếp rất ít thư quan trọng. Do đó, một e-mail trực tiếp từ một hành vi sai trái đòi tiền chuộc đến như một cú sốc. Điều này dường như cho thấy mức độ xâm nhập rất cao vào các hệ thống của công ty và / hoặc sự tham gia của người trong cuộc.
* Email đang được kiểm tra được gửi kèm theo tệp đính kèm có chứa mẫu dữ liệu nhạy cảm. Đây là ở dạng tệp ZIP, có kích thước khoảng 19 MB. Hệ thống e-mail được cấu hình để từ chối tất cả các tệp trên 20 MB. Đây có thể là một sự trùng hợp hoặc hậu quả của sự hiểu biết sâu sắc về hệ thống e-mail của công ty. Đó là công việc điều tra viên để chứng minh hoặc bác bỏ sự trùng hợp.
* Tệp ZIP chứa ba tệp bí mật, mỗi tệp được nhóm CXO giải thích có nguồn gốc từ các hệ thống khác nhau trong tổ chức. Nó cũng được nhấn mạnh rằng kiến ​​thức về sự tồn tại của các tệp này rất hạn chế và chỉ được biết đến với một vài nhân viên đã thực sự làm việc trong dự án. Không ai trong số các nhóm riêng biệt đã nhận thức được sự tồn tại của hai tệp khác, ngoại trừ các thành viên của nhóm lãnh đạo có mặt trong phòng.
* Một cuộc kiểm tra sơ bộ của các tiêu đề e-mail cho thấy rằng thư có nguồn gốc từ thư Tor. Một lần truy cập Web cho thấy dịch vụ này chạy trên mạng Tor được mã hóa và ẩn danh và yêu cầu trình duyệt Tor truy cập. Điều này được sử dụng bởi những người muốn liên lạc qua e-mail theo cách ẩn danh trên Web.
* Các chi tiết khác, chẳng hạn như nội dung email, ngày và giờ, múi giờ, ID tiêu đề, v.v. đã được ghi chú trong e-mail.
* Nội dung email đề cập rằng hacker có hơn 10 GB dữ liệu và sẽ tiết lộ nó trừ khi tiền chuộc được trả.
* Các phiên bản mới nhất của tài liệu được so sánh với nội dung trong tệp ZIP và được xác định rằng các tệp trong ZIP không quá vài ngày. Điều này đã được xác minh chéo bởi ngày và thời gian của các tệp trong ZIP.

Hình ảnh sau đây mô tả tiêu đề của tệp ZIP. Như đã thấy, ngày và thời gian sửa đổi tệp ZIP được lưu trữ trong tiêu đề. Điều này thường mô tả khi tệp ZIP được sửa đổi để thêm hoặc xóa tệp vào kho lưu trữ:



Tất cả các quy trình, hành động được thực hiện và các tệp được kiểm tra đều được ghi lại và băm hợp lệ. Các bản sao được lưu trữ trong một môi trường an toàn. Dựa trên các thông tin thu thập được cho đến nay, nhóm điều tra có thể suy ra một vài thông tin, như sau:

* Kẻ tấn công có cái nhìn sâu sắc về hệ thống phân cấp tổ chức cũng như kiến ​​trúc mạng
* Dữ liệu nhạy cảm đã được thu thập thành công từ các hệ thống cụ thể bởi người hoặc người chưa biết
* Dữ liệu đã được rút khỏi mạng lưới tổ chức gần đây hai ngày trước khi nhận được e-mail
* Kẻ tấn công đã / hiểu biết về kỹ thuật và nhận thức rõ về chu vi bảo mật xung quanh mạng tổ chức.

Do tính chất nhạy cảm về thời gian của bài tập, nó đã được quyết định áp dụng cách tiếp cận nhiều lớp cho quá trình điều tra. Thay vì truy tìm hàng tấn gỗ tròn trong nhiều tháng, người ta đã quyết định rằng giai đoạn đầu tiên chọn lọc nhanh sẽ được bắt đầu, tiếp theo là

thu thập và phân tích đầy đủ các bản ghi để xác định phương thức hoạt động của những kẻ tấn công, hiểu phương pháp vi phạm và đề xuất các biện pháp khắc phục. Là một phần của quy trình thu thập bằng chứng ban đầu, các hành động sau đây đã được thực hiện:

* Các nhật ký trong một tháng qua đã được thu thập, như sau:
* Bức tường lửa
* IPS / IDS
* Máy chủ proxy
* Yêu cầu DNS
* Xác thực tên miền
* Cảnh báo chống vi-rút
* Truy cập file
* Nhật ký máy chủ email
* Thu thập hình ảnh bộ nhớ hệ thống cho bốn hệ thống khác nhau đã được ủy quyền. Điều này bao gồm hệ thống CEO CEO cũng như ba hệ thống khác được xác định là nguồn tiềm năng của các tệp nhạy cảm được gửi đến CEO trong tệp đính kèm e-mail.
* Truyền thông mua lại để tạo hình ảnh đĩa của ba hệ thống với các tệp nhạy cảm đã được cấp phép. Điều này đã được thực hiện trong giờ làm việc để ngăn chặn bất cứ ai được cảnh báo về cuộc điều tra.

Tất cả các thông tin và bằng chứng trước đó đã được thu thập để phân tích thêm, với sự hiểu biết rõ ràng rằng quá trình phân tích dữ liệu thu được trước đó có thể tiết lộ thêm manh mối có thể đưa chúng ta trở lại giai đoạn mua lại nơi chúng ta có thể đi về việc có được dữ liệu và thông tin bổ sung có thể có liên quan đến trường hợp của chúng tôi.

Ví dụ, người ta đã hiểu rằng một nghiên cứu về các bản ghi thu được có thể giúp xác định hệ thống từ nơi diễn ra quá trình exfiltment và việc mua lại bộ nhớ và phương tiện sẽ được yêu cầu để tiếp tục quá trình điều tra. Do đó, chúng ta cần lưu ý rằng đây là một quá trình lặp lại và chúng ta có thể phải quay lại để thu thập thêm dữ liệu dựa trên các sự kiện được phát hiện trong giai đoạn phân tích.

1. **Phân tích dữ liệu thu thập - đào sâu**

Phân tích dữ liệu thu thập được là một quá trình lâu dài và tốn thời gian. Là chuyên gia mạng, chúng tôi cần hướng tới các mục tiêu được xác định cho chúng tôi trong khung thời gian có sẵn. Trong trường hợp cụ thể mà chúng tôi đã thảo luận, tình hình là cực kỳ nghiêm trọng. Nhìn vào khối lượng lớn bằng chứng tiềm năng có sẵn cho chúng tôi, chúng tôi phải thực hiện một cuộc gọi về quy trình xử lý và quyết định những gì chúng tôi muốn tập trung vào đầu tiên.

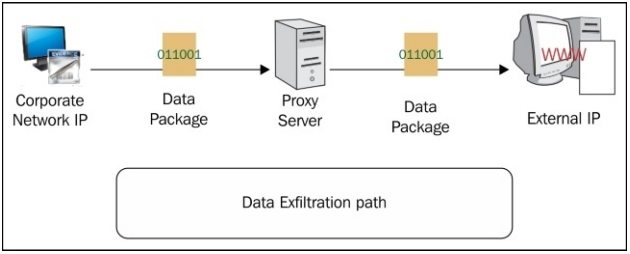
Một đầu vào rất có giá trị mà chúng tôi đã suy luận là dữ liệu đã được hoàn thành chỉ hơn hai ngày trước khi nhận được thư của CEO. Quá trình lọc dữ liệu của bất kỳ tên tội phạm nào thực sự liên quan đến một chuỗi các sự kiện. Các liên kết trong chuỗi hoặc các bước là hiển thị như sau:

* Trinh sát
* Thỏa hiệp
* Thiết lập lệnh và điều khiển
* Nhận dạng, thu thập và tổng hợp dữ liệu
* Lọc dữ liệu

Trong khi mỗi giai đoạn này sẽ để lại một số dấu vết trên các hệ thống nạn nhân, vai trò chính của một điều tra viên sẽ phát huy trong hai giai đoạn cuối.

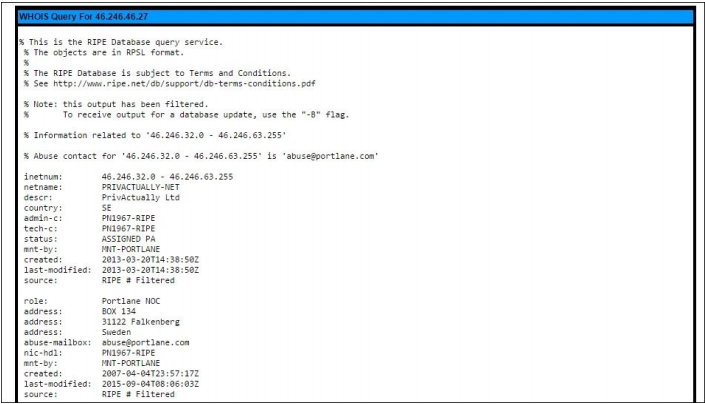
Quay trở lại trường hợp cụ thể của chúng tôi, chúng tôi nhận thức được một sự xuất hiện đã xảy ra. Vì lọc dữ liệu liên quan đến khối lượng lớn dữ liệu rời khỏi mạng, điều quan trọng là phải xác định tất cả các hoạt động mạng bên ngoài liên quan đến điều này trong phạm vi thời gian được chỉ định. Do đó, nhật ký từ máy chủ proxy được kiểm tra trong khoảng thời gian hai ngày để xác định, nếu có thể, việc hoàn thành khoảng 500 MB hoặc nhiều dữ liệu hơn. Con số 500 MB được đưa ra dựa trên nội dung thư mà CEO nhận được, nơi kẻ tấn công đã đe dọa sẽ tiết lộ hơn 500 MB dữ liệu nhạy cảm được cho là của anh ta. Mặc dù không có quy tắc cứng và nhanh nào mà kẻ tấn công sẽ hoàn thành hết 500 MB trong một lần (điều này có thể được chia thành các gói dễ quản lý hơn, được mã hóa và gửi đi cùng một lúc hoặc trong một khoảng thời gian dài), nếu chúng tôi tham khảo trở lại các giai đoạn của một cuộc tấn công tập trung vào lọc dữ liệu, chúng ta sẽ thấy rằng lọc dữ liệu là giai đoạn cuối cùng và cuối cùng. Rất phổ biến trong số những kẻ tấn công tích lũy dữ liệu và sau đó thử và tải lên dữ liệu trong một lần do lo ngại rằng thời điểm dữ liệu được xác định là đã rời khỏi mạng, tất cả các con đường được sử dụng trước đó để lọc dữ liệu tiếp theo sẽ bị tắt và quá trình khắc phục và phục hồi sẽ được bắt đầu. Đây là giai đoạn có nguy cơ phát hiện cao nhất đối với tên tội phạm; một khi khám phá đã được thực hiện, các cơ hội tiếp theo để hoàn thành dữ liệu có thể bị ảnh hưởng nghiêm trọng. Nhật ký máy chủ proxy cung cấp cho điều tra viên một số hiểu biết thú vị. Quan sát đầu tiên được thực hiện là trong khoảng thời gian hai ngày trước email, không có nhiều hoạt động. Đó là điều dễ hiểu do nó là một ngày cuối tuần. Một nghiên cứu về dữ liệu được truyền tải không cho thấy bất kỳ sự lọc lớn nào của một tệp có độ lớn đó. Mặc dù điều này loại trừ việc hết dữ liệu trong một lần chụp, khả năng dữ liệu đã được hoàn thành trong các phân đoạn vẫn còn.

Có một số lưu lượng HTTPS trong nhật ký dường như mang dữ liệu gần 20 MB. Tuy nhiên, điều này được mã hóa và chúng tôi chỉ có thể xem thông tin siêu dữ liệu cơ bản như nguồn, đích và chi tiết cổng. Hình ảnh sau đây biểu thị bằng đồ họa đường dẫn được thực hiện để lọc dữ liệu:



Để bắt đầu, chúng tôi xem xét kỹ các nhật ký liên quan đến lưu lượng truy cập HTTPS bị nghi ngờ.

Kiểm tra các bản ghi cho thấy lưu lượng này được chuyển đến IP 46.246.46.27. Một tra cứu trực tuyến cho thấy địa chỉ IP này thuộc về một tổ chức ở Thụy Điển. Để thực hiện tra cứu trực tuyến này, chúng tôi truy cập bất kỳ trang web nào trên Web cho phép chúng tôi thực hiện tra cứu IP Whois. Tôi sử dụng https://whois.net/. Một truy vấn whois của IP đang được điều tra được hiển thị như sau:



Một nỗ lực để kết nối với nó trong chế độ ẩn danh không mang lại bất kỳ kết quả nào. Nghiên cứu sâu hơn trên Internet cho thấy nhiều danh sách trực tuyến hiển thị IP này như một phần của mạng Tor, như trong hình sau:



Từ góc độ điều tra, đây là một khoảnh khắc eureka. Email đã kích hoạt cuộc điều tra này bắt nguồn từ mạng Tor. Bây giờ chúng tôi đã phát hiện ra các bản ghi cho thấy một số bằng chứng về việc thoát khỏi mạng Tor. Người dùng thông thường thường không truy cập Tor trừ khi họ có lý do quan trọng để ẩn danh.

Bây giờ, khi không biết một đầu của quả bóng dây, điều tra viên tiến hành làm sáng tỏ phần còn lại của câu đố. Dựa trên các biểu đồ kiến trúc mạng tổ chức (được thực hiện trong giai đoạn chuẩn bị trong các chương trước), điều tra viên của chúng tôi xác định địa chỉ IP của tổ chức được liên kết với máy tính được sử dụng làm vị trí dàn dựng cho việc hoàn thành. Điều này hóa ra là một máy tính cũ được sử dụng như một máy chủ in trong tổ chức.

Toàn bộ quá trình điều tra mạng, đội ngũ quản lý cấp cao được giữ thẩm định về sự phát triển và tiến độ.

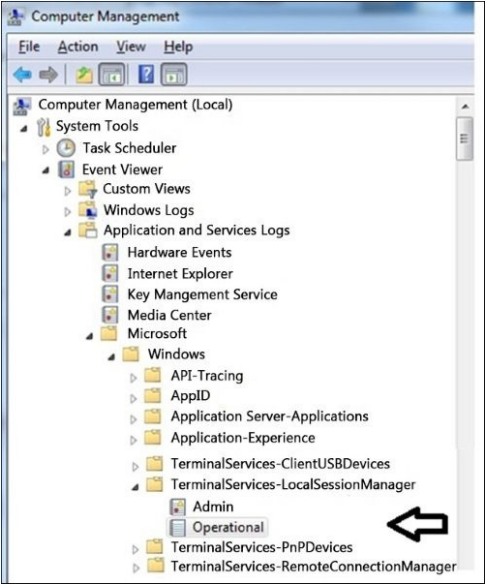
Theo các quy trình thích hợp, một hình ảnh bí mật của cả bộ nhớ và phương tiện của máy chủ in được tạo và lưu giữ.

Dựa trên các quyết định của quản lý cấp cao, quyết định vô hiệu hóa kết nối mạng với máy chủ in trong khi làm cho sự gián đoạn dường như là một phần của sự cố ngừng mạng.

Trong khi đó, một cuộc kiểm tra tốc độ cao về hình ảnh đã được tạo ra trước đó được thực hiện.

Một bản tóm tắt ngắn về những phát hiện có liên quan được liệt kê như sau:

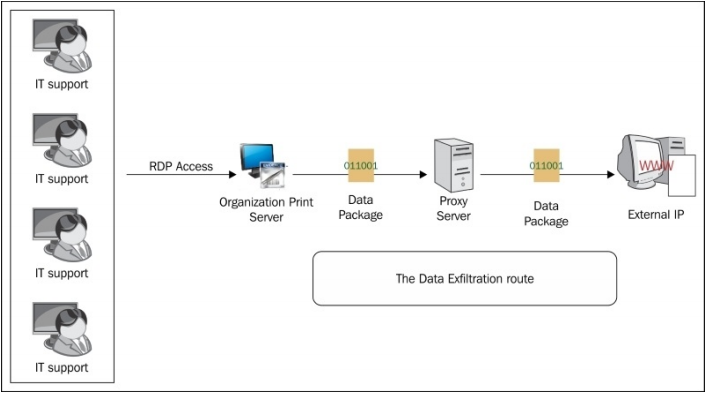
* Máy chủ chạy hệ điều hành Window 7
* Có 2 ổ đĩa logic C và D
* Ổ đĩa D có đường dẫn thư mục là windows\system\print spooler.
* Trong thư mục, có một số lượng lớn các tệp ZIP có tổng dung lượng khoảng 420 MB ở dạng nén.
* Mỗi thư mục nén đều được bảo vệ bằng mật khẩu
* Tuy nhiên, tên tệp của các tệp có trong tệp ZIP có thể được nhìn thấy và chúng tương ứng với các tệp nhạy cảm thu được từ các phần khác nhau của tổ chức.
* Một tệp ZIP không được bảo vệ bằng mật khẩu, đó cũng là tệp ZIP đã được gửi cho CEO qua e-mail.
* Một cuộc kiểm tra về dấu ngày và thời gian trên các tệp này cho thấy rằng kho lưu trữ sớm nhất đã được tạo ra khoảng một tháng trước.
* Nhật ký trên hệ thống được phân tích và được thiết lập rằng máy chủ in được truy cập thường xuyên bằng Windows Remote Desktop Protocol (RDP) trong giai đoạn này. Các nhật ký RDP này có sẵn, theo ảnh chụp màn hình sau:



* Thông tin quản trị mạng đã được sử dụng để truy cập.
* Các máy tính được sử dụng để truy cập là những máy tính thuộc nhóm chung được sử dụng bởi các nhân viên hỗ trợ CNTT trong tổ chức.

Tại thời điểm này, hình ảnh đã trở nên rõ ràng hơn rất nhiều. Bằng chứng thu thập được cho đến nay cũng chỉ ra sự liên quan của người trong cuộc. Một bức tranh về kẻ thù đang xuất hiện từ từ và nhu cầu thận trọng và tốc độ ngày càng tăng.

Một sơ đồ mô tả tuyến đường thoát dữ liệu đã được thực hiện để hiểu rõ hơn về vụ việc. Điều này được thể hiện trong các điều sau đây:



Rõ ràng là một người trong cuộc với đặc quyền quản trị viên thực sự có thể gây ra tác hại đáng kể cho tổ chức và phải được loại bỏ sớm nhất. Tuy nhiên, điều này phải được thực hiện một cách suôn sẻ để người trong cuộc vẫn không biết gì cho đến phút cuối cùng. Một điều khá rõ ràng là, với các đặc quyền của quản trị viên mạng, người trong cuộc có thể giữ bí mật tất cả các cuộc hội thoại email trên máy chủ email, hành động của quản trị viên, cũng như dữ liệu bí mật theo chiều dài và chiều rộng của mạng.

Do đó, cần phải thận trọng và tốc độ!

Một lần nữa, sau khi tham khảo ý kiến nhanh, người ta đã quyết định một lần nữa cho phép truy cập mạng của máy chủ in và thực hiện chụp Wireshark cho tất cả lưu lượng truy cập mạng từ và đến địa chỉ IP đó.

Tuy nhiên, để ngăn chặn dữ liệu được thu thập hiện có bị xóa, người ta đã quyết định rằng các tệp ZIP nằm trên máy chủ in sẽ bị hỏng khi sử dụng trình soạn thảo hex để ngay cả trong trường hợp chúng bị xóa, chúng sẽ bị hỏng và không sử dụng được. Ý tưởng là để có được một chút thời gian và thu thập thêm bằng chứng, trong khi mọi nỗ lực đã được thực hiện để xác định thủ phạm sớm nhất.

Giữ thông tin trước đó là mục tiêu chính, CSO, làm việc song song, đã gọi các hồ sơ truy cập sinh trắc học để xác định những người đã làm việc trong văn phòng được chỉ định vào cuối tuần qua. Hai kỹ sư hỗ trợ CNTT đã được xác định. Ông cũng gọi cho các tập tin nhân sự của họ để kiểm tra hồ sơ theo dõi của họ.

Trong khi đó, Digital 007 của chúng tôi đã tình cờ chụp được những hình ảnh điều tra về bộ nhớ và phương tiện của các hệ thống bị nghi ngờ. Đồng thời, anh nhìn lại các mục nhật ký để xác định những ngày và thời gian khác mà Tor đã được truy cập. Truy cập Tor cũng tương quan với truy cập RDP của máy chủ in. Một dòng thời gian thích hợp của các hoạt động này đã được tạo ra. Điều này đã được chia sẻ với CSO về mối tương quan với hồ sơ tham dự và truy cập.

Kết quả là một trong những kỹ sư hỗ trợ CNTT phù hợp trực tiếp với khe cắm. Với sự rõ ràng thu được, mục tiêu ngay lập tức xác định kẻ tấn công đã đạt được.

Từ các hình ảnh hệ thống được tạo, đã xác định rằng người được hỏi đang lạm dụng vị trí đặc quyền của mình với tư cách là kỹ sư hỗ trợ CNTT bằng cách vô hiệu hóa bảo vệ trên các hệ thống nhạy cảm và triển khai keylogger để thu thập thông tin quan trọng cũng như thông tin đăng nhập của người dùng. Một bộ sưu tập phần mềm độc hại đã được phục hồi cũng như bằng chứng về việc tìm kiếm email ẩn danh miễn phí và các cụm từ tìm kiếm gợi ý khác cho thấy ý định của anh ta.

1. **Báo cáo các trường hợp**

Khi quá trình lặp đi lặp lại của các cuộc điều tra mạng hoàn tất, phần khó khăn thực sự bắt đầu. Đây là thời gian mà tất cả những nỗ lực được đưa vào để duy trì tài liệu tỉ mỉ đã được đền đáp.

Báo cáo một trường hợp rất giống như kể chuyện. Sự khác biệt duy nhất là những câu chuyện có thể là hư cấu hoặc sửa đổi để tạo ra một câu chuyện hay hơn; trong khi đó, một báo cáo điều tra cho phép không có tự do nghệ thuật như vậy. Nó phải được căn cứ kỹ lưỡng trong thực tế. Mỗi tuyên bố nên được hỗ trợ bởi bằng chứng vững chắc. Mọi phỏng đoán nên được hỗ trợ bởi bằng chứng gián tiếp và cần được xác định rõ ràng như vậy.

Một báo cáo trường hợp nên như sau:

* Sạch sẽ
* Ngắn gọn
* Có mục đích

Giữ cho khán giả rằng báo cáo trường hợp là nhằm vào mục đích chính. Các báo cáo rất dài hiếm khi được đọc và các điểm hành động hầu như không được thực hiện, do đó, cấu trúc rất quan trọng.

Hầu hết các báo cáo nên bắt đầu với một bản tóm tắt trường hợp.

Theo đó, báo cáo tối thiểu phải có cấu trúc như sau:

* Giới thiệu
* Thông tin có sẵn và các giả định
* Điều tra
* Kết quả
* Hành động được thực hiện và đề nghị

Các khuyến nghị cần phải được suy nghĩ cẩn thận và nên có một ảnh hưởng cụ thể về khía cạnh điều tra của mạng. Các khuyến nghị nên bao gồm những điều sau đây:

* Việc khắc phục có nên được bắt đầu tại thời điểm hiện tại hay không (điều này có thể ảnh hưởng đến thực tế là nó có thể loại bỏ kẻ tấn công và kết tủa hành động có thể gây tổn hại cho tổ chức).
* Liệu phạm vi của công việc được giao nên được thu hẹp hoặc mở rộng để bao gồm nhiều thiết bị kỹ thuật số hơn. Một danh sách các nguồn bằng chứng bổ sung có thể nên được lập và cung cấp cho ban quản lý.
* Lời khuyên liên quan đến thời gian lưu giữ bằng chứng nên được lấy từ các đội pháp lý. Điều này sẽ tạo thành một phần của các khuyến nghị và lưu trữ an toàn bổ sung nên được sắp xếp cho việc này.
* Nếu các tạo phẩm cụ thể hoặc mới đã được xác định là một phần của cuộc điều tra và chúng có thể được sử dụng như một IOC mới, nên đưa vào đó những IOC để bảo vệ mạng.
* Các khuyến nghị cũng cần bao gồm các hành động mà tổ chức được yêu cầu thực hiện như một phần của việc tuân thủ pháp luật hoặc quy định. Một ví dụ sẽ là việc tìm kiếm nội dung khiêu dâm trẻ em.
* Khác với các điểm trước, có khả năng có một số khuyến nghị cụ thể cho từng trường hợp. Tất cả những điều này nên được hiệu đính và sau đó trình bày cho ban quản lý.

1. **Hành động vì tương lai**

Một khi bất kỳ sự cố đã kết thúc và được thực hiện, nhóm cần tập trung vào các bài học kinh nghiệm. Từ góc độ phản ứng sự cố, trọng tâm là trả lời các câu hỏi như sau:

* Tại sao lại xảy ra chuyện này?
* Chúng ta có thể làm gì để ngăn chặn nó tái xuất hiện?
* Những biện pháp phòng ngừa có thể được đưa vào vị trí nào?
* Làm thế nào để theo dõi và cảnh báo được cải thiện?

Từ góc độ điều tra mạng, các câu hỏi bổ sung sẽ được trả lời bao gồm:

* Những biểu hiện nào tồn tại có thể giúp chúng ta xác định một sự cố như vậy trong tương lai?
* Những bài học kinh nghiệm là gì?
* Làm thế nào chúng ta có thể cải thiện quá trình điều tra?
* Những gì IOC có thể được xác định có thể được chia sẻ với nhóm Ứng phó sự cố để giúp ngăn chặn sự tái diễn của một sự cố như vậy?

Trong khi những kẻ tấn công liên tục phát triển và đổi mới để tiếp tục tìm ra những cách mới hơn để thỏa hiệp các mạng mà không bị phát hiện, các nhà điều tra mạng cũng phải theo kịp. Điều này có nghĩa là liên tục cập nhật bản thân, học hỏi từ các đồng nghiệp,

tham dự hội nghị và các chương trình đào tạo, v.v. Thay vì ở trong một chế độ phản ứng, điều này có ý nghĩa đối với nhà điều tra mạng để theo dõi tương lai.

1. **Tương lai của điều tra mạng**

Trong khi rất khó để dự đoán tương lai, một số xu hướng là hiển nhiên. Hãy để chúng tôi xem xét chúng.

Các tổ chức đang di chuyển đến các mạng băng thông và tốc độ cao hơn. Ngày càng có nhiều dữ liệu truyền qua các mạng và đến và từ nhiều loại thiết bị.

IPv6 ở đây để ở lại! Nó mang theo sự phổ biến của các thiết bị kết nối Internet, ngay từ máy nướng bánh mì, TV, tủ lạnh, máy photocopy và máy pha cà phê cho đến hệ thống báo động và an ninh của bạn. Đây được gọi là Internet of Things hoặc IoT.

Nó không đòi hỏi nhiều ánh mắt pha lê để xác định xu hướng của những thứ sẽ đến trong lĩnh vực điều tra mạng. Khi một số lượng lớn thiết bị được nối mạng, sẽ có vai trò lớn hơn đối với 007 của Network Forensic 007. Chúng tôi sẽ xem xét ngày càng nhiều thiết bị được kết nối, bằng chứng cho thấy chúng lưu trữ, cách chúng hoạt động và cách chúng bị ảnh hưởng bởi các thỏa hiệp khác nhau. Chúng tôi sẽ thu thập, xử lý, bảo quản và phân tích khối lượng lớn dữ liệu.

Phần mềm độc hại đã bắt đầu phát triển và sẽ bắt đầu nhắm mục tiêu các thiết bị kết nối Internet trên quy mô lớn, có thể cung cấp một điểm truy cập dễ dàng vào các mạng tổ chức. Nó đã thắng được rất lâu trước khi chúng ta nghe thấy tin tặc đánh cắp dữ liệu từ một mạng bằng cách đầu tiên xâm phạm máy pha cà phê văn phòng.

Chúng tôi cũng đang thấy một xu hướng ngày càng tăng của dữ liệu di chuyển lên đám mây. Điều tra mạng sẽ cần kiểm tra các địa chỉ IP ảo Hoạt động trên quy mô doanh nghiệp để xác định các hoạt động đóng vai trò là IOC. Cloud forensics sẽ được bổ sung cho điều tra mạng.

Khi kịch bản mối đe dọa thay đổi, các nhà cung cấp bảo mật trên toàn cầu sẽ tăng cường, nâng cấp và đổi mới. Sản phẩm bảo mật mới sẽ được tung ra thị trường. Các nhà điều tra mạng sẽ cần phải học các công nghệ và kỹ thuật mới để theo kịp những gì đang xảy ra.

1. **Tóm lược**

Chương cuối cùng này tổng hợp hành trình của chúng tôi trong việc phát triển sự hiểu biết về điều tra mạng. Trên đường đi, chúng tôi đã thấy vô số nguồn bằng chứng, hiện vật được tạo ra bởi các hoạt động của kẻ tấn công, cũng như các kỹ thuật và quy trình cần thiết để thu thập và phân tích chúng. Bạn đã học được cách kết hợp một báo cáo để trình bày những phát hiện của chúng tôi và cũng hành động theo cách học của bạn từ cuộc điều tra.

Mặc dù cuốn sách này hoạt động như một điểm khởi đầu và giúp xây dựng một nền tảng trong lĩnh vực điều tra mạng, hãy nhớ rằng đó là một thế giới rộng lớn ngoài kia và không có kết thúc nào về kiến thức mà người ta có thể và nên thu thập khi chúng ta mạnh dạn tiến tới.

Cảm ơn vì đã là một phần của hành trình này. Tôi hy vọng rằng nó đã là một điều thú vị và tôi đã thành công trong việc khơi gợi sự quan tâm của bạn trong một lĩnh vực mới rất thú vị.