HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

🙦🙤🟇🙦🙤

BÀI TẬP LỚN

**Đề tài** :

**LEARNING NETWORK FORENSICS**

**Chapter 9. Investigating Malware – Cyber Weapons of the Internet**

***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 Văn Tài – AT120242

Lê Văn Quang – AT120239

*Hà Nội, Tháng 12 Năm 2019*

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

**MỤC LỤC**

[**MỤC LỤC 1**](#_Toc26538107)

[**DANH MỤC HÌNH ẢNH 2**](#_Toc26538108)

[**Chương 9. Điều tra phần mềm độc hại - Vũ khí kỹ thuật số trên không gian mạng 3**](#_Toc26538109)

[1. Nhận biết phần mềm độc hại 4](#_Toc26538110)

[1.1. Mục tiêu phần mềm độc hại 5](#_Toc26538111)

[1.2. Nguồn gốc phần mềm độc hại 6](#_Toc26538112)

[2. Xu hướng phát triển của phần mềm độc hại 8](#_Toc26538113)

[3. Các loại phần mềm độc hại và tác động của chúng 10](#_Toc26538114)

[3.1. Phần mềm quảng cáo 11](#_Toc26538115)

[3.2. Phần mềm gián điệp 12](#_Toc26538116)

[3.3. Virus 13](#_Toc26538117)

[3.4. Worms 14](#_Toc26538118)

[3.5. Trojans 15](#_Toc26538119)

[3.6. Rootkits 16](#_Toc26538120)

[3.7. Backdoors 17](#_Toc26538121)

[3.8. Keylogger 18](#_Toc26538122)

[3.9. Ransomware 19](#_Toc26538123)

[3.10. Browser hijackers 21](#_Toc26538124)

[3.11. Botnet 22](#_Toc26538125)

[4. Cách thức hoạt động của phần mềm độc hại. 23](#_Toc26538126)

[4.1. Destructive(Phá hoại ) 24](#_Toc26538127)

[4.2. Identity theft(Đánh cắp danh tính ) 25](#_Toc26538128)

[4.3. Espionage(Gián điệp) 26](#_Toc26538129)

[4.4. Financial fraud(Gian lận tài chính ) 27](#_Toc26538130)

[4.5. Theft of data(Đánh cắp dữ liệu) 28](#_Toc26538131)

[4.6. Misuse of resources(Sử dụng sai tài nguyên ) 29](#_Toc26538132)

[5. Phần mềm độc hại tấn công kiến trúc 30](#_Toc26538133)

[6. Indicators of Compromise(Trích xuất các dấu vết tấn công hệ thống) 31](#_Toc26538134)

[7. Performing malware forensics. (Thực hiện điều tra số phần mềm độc hại) 33](#_Toc26538135)

[8. Malware insight – Gameover Zeus Trojan 37](#_Toc26538136)

[9. Tổng kết 39](#_Toc26538137)

**DANH MỤC HÌNH ẢNH**

[Hình 1: Xu hướng phát triển 9](#_Toc26538214)

[Hình 2: Phần mềm quảng cáo 11](#_Toc26538215)

[Hình 3: Phần mềm gián điệp 12](#_Toc26538216)

[Hình 4: Virus 13](#_Toc26538217)

[Hình 5: Sâu máy tính 14](#_Toc26538218)

[Hình 7: Trojans 15](#_Toc26538219)

[Hình 8: Rootkits 16](#_Toc26538220)

[Hình 9: Backdoors 17](#_Toc26538221)

[Hình 10: Keyloggers 18](#_Toc26538222)

[Hình 11: Ransomware 19](#_Toc26538223)

[Hình 12: Browser hijackers 21](#_Toc26538224)

[Hình 13: Botnets 22](#_Toc26538225)

**Chương 9. Điều tra phần mềm độc hại - Vũ khí kỹ thuật số trên không gian mạng**

“Malware Vũ khí kỹ thuật số trên không gian mạng trong thời đại thông tin ”

* Samir Datt -

Cuộc sống thời đại thông tin của chúng ta được thúc đẩy bởi công nghệ. Ngày này qua ngày khác, chúng ta sống với công nghệ từ sáng đến tối. Công nghệ thúc đẩy cuộc sống của chúng ta, chi phối hành vi của chúng ta, quản lý tài chính, cho phép thực hiện công việc của chúng ta, tạo điều kiện cho giao tiếp của chúng ta và thậm chí tăng cường các mối quan hệ của chúng ta. Do đó, không có gì đáng ngạc nhiên khi công nghệ cũng điều khiển những hành vi sai trái của ngày hôm nay. Một ngành công nghiệp hoàn toàn mới đã xuất hiện xung quanh chiến tranh kĩ thuật số . Tội phạm có tổ chức đã đưa đến tội phạm mạng một cách lớn. Ngay cả các nước và các tiểu bang đã tham gia vào cuộc chiến tranh mạng. Ở đâu có tội ác và chiến tranh, vũ khí không thể bỏ lại đằng sau khá xa. Vũ khí hóa Internet là một ngành công nghiệp trị giá hàng tỷ đô la và phần mềm độc hại, như chúng tôi biết điều đó, là vũ khí của sự lựa chọn.

Trong chương này, chúng tôi sẽ hướng tới việc hiểu phần mềm độc hại, các loại khác nhau của nó, các chỉ số khác nhau của sự thỏa hiệp và các phương pháp để điều tra phần mềm độc hại.

Chúng tôi sẽ chia nghiên cứu của chúng tôi thành các chủ đề sau:

* Nhận biết phần mềm độc hại
* Xu hướng phát triển phần mềm độc hại
* Các loại phần mềm độc hại và tác động của chúng
* Cách thức hoạt động của phần mềm độc hại
* Phần mềm độc hại tấn công mô hình kiến trúc
* Trích xuất các dấu vết tấn công hệ thống
* Thực hiện điều tra số phần mềm độc hại

1. **Nhận biết phần mềm độc hại**

Từ ngữ *mal* có nguồn gốc từ tiếng Latin và có nghĩa là tiếng *bad* trong tiếng Anh. Mặt khác, “*ware*” mang ý nghĩa của các sản phẩm trên mạng. Do đó, khi chúng ta kết hợp hai thứ này lại với nhau, chúng ta có được ý thức có sản phẩm xấu hoặc hàng hóa được thực hiện với một mục đích xấu.

Theo ấn phẩm NIST SP800-83, phần mềm độc hại, còn được gọi là mã độc hoặc mã độc phần mềm, có nghĩa là để biểu thị một chương trình được chèn (thường là tình cờ) trong một hệ thống có ý định thỏa hiệp hoặc phá vỡ tính bảo mật, tính toàn vẹn hoặc tính sẵn có của dữ liệu, ứng dụng hoặc hệ điều hành. Trong vài năm qua, phần mềm độc hại đã nổi lên như một thuật ngữ bao gồm tất cả các loại chương trình độc hại, bao gồm virus, sâu, trojan, rootkit, v.v.v

Ngày nay, phần mềm độc hại được coi là mối đe dọa bên ngoài đáng kể nhất đối với máy tính và mạng. Phần mềm độc hại gây thiệt hại đáng kể cho các tổ chức về mức độ phổ biến thiệt hại gây ra, gián đoạn chức năng và các nỗ lực phục hồi lớn cần thiết để lấy lại để bình thường. Phần mềm gián điệp là một danh mục con đáng kể của phần mềm độc hại, tập trung vào vi phạm quyền riêng tư của người dùng.

Phần mềm gián điệp được sử dụng để giám sát hoạt động của người dùng (cả trực tuyến và ngoại tuyến), tập hợp thông tin cá nhân, đặc biệt, liên quan đến các hành động tài chính trực tuyến; và sau đó, gửi nó đến tội phạm cho việc sử dụng sai sau đó.

* 1. **Mục tiêu phần mềm độc hại**

Trong các chương trước, chúng tôi đã hiểu một số công cụ được sử dụng cho điều tra mạng. Chỉ như chúng ta, những kỹ thuật số của thế giới mạng, có những công cụ thương mại, tội phạm và xấu các chàng trai cũng có bộ công cụ riêng mà họ sử dụng để tiếp tục các mục đích bất chính của mình. Những công cụ này được gọi là phần mềm độc hại. Mặc dù, phần mềm độc hại có rất nhiều, bọn tội phạm muốn cài đặt phần mềm độc hại trên các thiết bị kỹ thuật số của nạn nhân để đạt được ít nhất một trong số các mục tiêu sau:

* Để thu thập và đánh cắp thông tin thích hợp (đánh cắp ID, keylogging, v.v.)
* Để cung cấp quyền truy cập từ xa cho kẻ tấn công để cho phép kiểm soát máy tính bị nhiễm / bị xâm nhập và tài nguyên của nó
* Sử dụng máy bị nhiễm làm điểm tổ chức để lây nhiễm / điều tra phần còn lại của mạng
* Để sử dụng máy bị nhiễm để gửi thư rác đến người không mong muốn
* Để thực hiện một cuộc tấn công từ chối dịch vụ (DoS) bằng cách làm ngập mạng hoặc làm chậm xuống kết nối
* Để mã hóa đĩa bị nhiễm và yêu cầu tiền chuộc để giải mã các tệp (ransomware)
* Để không bị phát hiện càng lâu càng tốt (tắt chống vi-rút, v.v.)
* Để chống lại loại bỏ hoặc tăng cường sự kiên trì
  1. **Nguồn gốc phần mềm độc hại**

Mối đe dọa của phần mềm độc hại đang gia tăng bởi những bước nhảy vọt. Trong thực tế, một mục tin tức gần đây từ tạp chí SC Vương quốc Anh ( <http://www.scmagazineuk.com/research-shows-12-new-malware-strains-discovered-every-minute/article/448978/> ) đề cập đến 12 chủng phần mềm độc hại mới được phát hiện mỗi phút.

Làm phần mềm độc hại không còn tồn tại trong vương quốc của những đứa trẻ làm điều đó . Phần mềm độc hại sản xuất, bán và phân phối hiện là một tội phạm có tổ chức nghiêm trọng với thực sự lớn số tiền trên nó. Các báo cáo gần đây về tiền được trích xuất để giải mã tập tin được mã hóa bởi các ransomware bitcoin như CryptoWall và CryptoLocker hiển thị nạn nhân báo cáo thiệt hại lên tới 18 triệu đô la trong khoảng thời gian 14 tháng

( <http://www.coindesk.com/fbi-malware-victims-should-pay-bitcoin-ransoms/> ).

Cũng giống như làm một sản phẩm được sản xuất chuyên nghiệp trong bất kỳ cơ sở sản xuất nào,phần mềm độc hại ngày nay cũng được sản xuất hoặc viết để chính xác thông số kỹ thuật. Điều này được thực hiện bởi lập trình viên tài năng viết khai thác để tận dụng các lỗ hổng trong phần mềm hiện có và phần cứng được sử dụng bởi các mục tiêu hoặc nạn nhân theo kế hoạch. Phần mềm độc hại thực sự là một phần của một thời gian dài chuỗi hoạt động và giúp kích hoạt các mục tiêu của những kẻ tấn công hoặc tội phạm mạng.

Các giai đoạn thông thường trong bài tập này như sau:

**Do thám** : Ở giai đoạn này, kẻ tấn công thực hiện một cuộc thám hiểm sơ bộ để xác định các mục tiêu tiềm năng (nếu sử dụng cách tiếp cận shotgun, kẻ tấn công có thể cố gắng truy cập nhiều, chọn điểm yếu nhất hoặc thực hiện một cách tiếp cận mục tiêu hơn). Quá trình này có thể đượ cthủ công hoặc tự động, tùy thuộc vào mục tiêu của kẻ tấn công.

**Thu thập thông tin** :Ở giai đoạn này, kẻ tấn công sẽ tiến hành lập bản đồ mạng, lấy dấu vân tay và xác định lỗ hổng.

**Thâm nhập mục tiêu** : Đây là giai đoạn thông thường nơi phần mềm độc hại phát huy tác dụng. Đây là khi khai thác các lỗ hổng được xác định trước đó diễn ra. Phần mềm độc hại là thường được giao cho mục tiêu thông qua cơ chế phân phối hoặc mục tiêu được giao cho trang web bị nhiễm cho một ổ nhiễm trùng.

**Leo thang đặc quyền:** Đây là giai đoạn phần mềm độc hại đẩy mạnh trò chơi của nó với mục tiêu đạt được mức đặc quyền tối đa cho hệ thống và mạng.

**Duy trì:** Ở giai đoạn này, phần mềm độc hại tìm ra các phương tiện và cách thức duy trì truy cập liên tục cũng như ngăn chặn bản thân khỏi bị phát hiện hoặc loại bỏ. Cửa hậu bổ sung được xây dựng, mạng được quét để có thể khai thác thêm lỗ hổng, nhiều tài khoản cấp root / cấp quản trị viên được truy cập, các bản nhạc được được bảo hiểm, nhật ký sẽ bị xóa, và bằng chứng của sự thỏa hiệp được loại bỏ.

Rất nhiều trong số các giai đoạn này có xu hướng kính viễn vọng vào nhau. Các tác giả phần mềm độc hại hiện đã chuyển gói các bộ công cụ khai thác phần mềm độc hại mang theo một số phần mềm độc hại khác nhau, mỗi bộ nhắm mục tiêu vào các môi trường khác nhau, khi được kết hợp với nhau, tăng khả năng xác định, thỏa hiệp và thâm nhập các mục tiêu.

1. **Xu hướng phát triển của phần mềm độc hại**

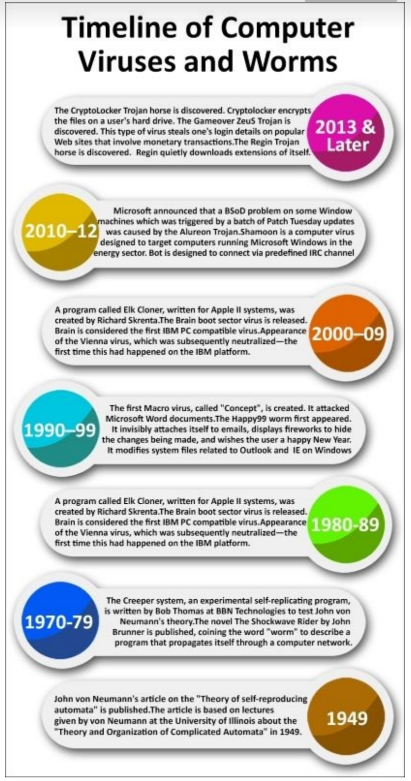
*Phần mềm độc hại có một lịch sử rất thú vị.*

Năm 1949, một nhà khoa học người Mỹ gốc Hungary, John von Neumann, đã viết lý thuyết về tự sinh sản. Năm 1971, lý thuyết này đã hình thành cơ sở của một thí nghiệm về tạo ra chương trình máy tính tự sao chép đầu tiên. Chương trình này được gọi là hệ thống Creeper, nơi nó có được quyền truy cập vào các máy tính mục tiêu thông qua Advanced mạng lưới cơ quan dự án nghiên cứu (ARPANET) và sao chép chính nó với I Laum cây leo, bắt tôi nếu bạn có thể nhắn tin.

Một thông tin thú vị khác về John von Neumann là sau này ông sẽ tiếp tục là một phần của dự án Manhattan và giúp thiết kế bom nguyên tử kết thúc chiến tranh thế giới thứ hai và hướng thế giới theo hướng phi hạt nhân hóa.

Trong khi một cuộc chiến tranh hạt nhân là một cách chắc chắn để hướng tới sự hủy diệt được đảm bảo lẫn nhau (MAD)**,** cuộc chiến không gian mạng của phần mềm độc hại đã leo thang kể từ khi nó bắt đầu. Không có phương tiện của MAD hoặc thậm chí quy kết trong rất nhiều trường hợp, những kẻ tấn công có xu hướng tránh xa với rất nhiều Hoạt động.

Hãy để chúng tôi thấy phần mềm độc hại đã phát triển như thế nào trong nhiều thập kỷ như được trình bày dưới đây hình ảnh, tưởng tượng:



*Hình 1: Xu hướng phát triển*

1. **Các loại phần mềm độc hại và tác động của chúng**

Như chúng ta đã thảo luận trước đó, phần mềm độc hại là một phần mềm độc hại có nhiều loại tên. Một số tên mà nó đã có được trong một khoảng thời gian bao gồm phần mềm lừa đảo, Scarware, Spamware, phần mềm gián điệp, và như vậy.

Phần mềm độc hại là tất cả và nhiều hơn nữa. Hãy để chúng tôi xem xét các loại phần mềm độc hại khác nhau và các loại phần mềm độc hại khác .

* 1. **Phần mềm quảng cáo**

Phần mềm quảng cáo, như tên cho thấy, là phần mềm độc hại được hỗ trợ quảng cáo ảnh hưởng đến máy tính với mục tiêu phục vụ quảng cáo. Adware mang lại lợi nhuận cho nhà phát triển của nó bằng cách tự động hiển thị quảng cáo online trong giao diện người dùng của phần mềm hoặc trên màn hình trong quá trình cài đặt.Phần mềm quảng cáo được thiết kế để tồn tại và có thể không dễ dàng để loại bỏ bằng cách gỡ cài đặt nó. Phần mềm quảng cáo ít nhất có thể gây phiền nhiễu và nó cũng có thể là một phần của mối đe dọa hỗn hợp, như được hiển thị trong hình ảnh sau đây:

*Hình 2: Phần mềm quảng cáo*

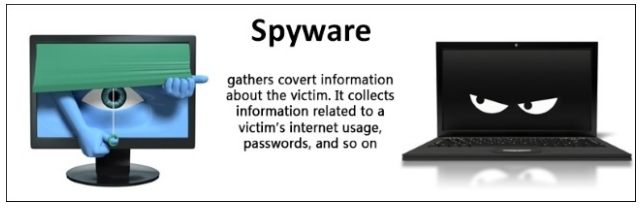
Phần mềm quảng cáo tiếp cận nạn nhân bằng cách tải xuống một phần mềm được cho là hữu ích hoặc truy cập vào trang web được thiết kế để ảnh hưởng đến trình duyệt, hệ điều hành hoặc cả hai.

Kết luận: Để tránh adware, hãy cẩn thận trước khi tải và cài đặt bất cứ phần mềm mới nào, đặc biệt là phần mềm miễn phí. Đọc điều khoản và điều kiện trước khi đồng ý. Tránh các [trang web torrent](https://quantrimang.com/top-22-trang-web-chia-se-torrent-pho-bien-nhat-nam-2017-144874), trang web download phần mềm bất hợp pháp và không bao giờ mở ứng dụng từ một nguồn không xác định, ngay cả khi nó đến với bạn dưới vỏ bọc của một liên hệ email đã biết.

* 1. **Phần mềm gián điệp**

Phần mềm gián điệp là một phần mềm độc hại có mục tiêu thu thập thông tin bí mật về nạn nhân. Phần mềm gián điệp được sử dụng để thu thập thông tin liên quan đến những người sử dụng Internet, e-mail và tài khoản trực tuyến, giao dịch tài chính trực tuyến, thẻ tín dụng ngân hàng, tên người dùng và mật khẩu …. Phần mềm gián điệp ngày càng trở nên phổ biến trong gian lận tài chính.

Phần mềm gián điệp cũng có thể được sử dụng để khen ngợi phần mềm quảng cáo. Điều này được thực hiện bằng cách theo dõi người dùng , Dùng các mẫu duyệt Internet và sau đó phục vụ phần mềm quảng cáo dựa trên các trường hợp thu thập được. Đôi khi phần mềm quảng cáo (và tất cả phần mềm độc hại) có thể làm giả thành một chương trình hữu ích khác như một công cụ chống vi-rút hoặc chống phần mềm độc hại. Các hình ảnh đại diện sau cho chúng ta một tổng quan về phần mềm gián điệp:



*Hình 3: Phần mềm gián điệp*

Kết luận: Mục đích của các cuộc tấn công Spyware tạo ra một mạng lưới nhằm thu thập dữ liệu của càng nhiều nạn nhân càng tốt hoặc dùng để lừa đảo các tài khoản ngân hàng , các hình ảnh video nhằm mục đích tống tiền .

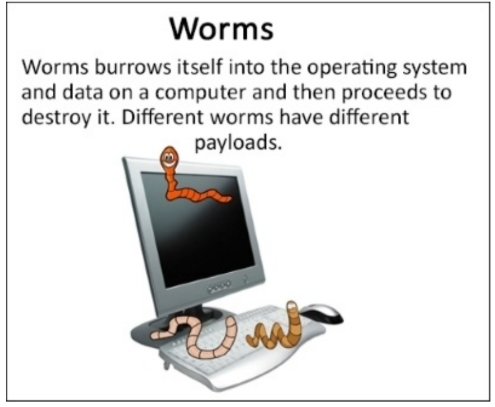
* 1. **Virus**

Virus là một phần mềm độc hại được thiết kế để sao chép chính nó dưới dạng lan truyền cơ chế và nó thường có một trọng tải mà nó cung cấp tại một thời điểm cụ thể hoặc nếu điều kiện nhất định được đáp ứng. Một virus thường tự gắn vào một phần mềm khác và được thực thi mỗi khi phần mềm được chạy, như trong hình sau:

*Hình 4: Virus*

Một vectơ lây nhiễm phổ biến là sao chép phần mềm hoặc tệp giữa nhiều máy tính. Virus thường sửa đổi hoặc làm hỏng các tệp trên máy tính nạn nhân.

* 1. **Worms**

Một con sâu, như tên cho thấy, là một phần mềm độc hại tự đào sâu vào hoạt động hệ thống và dữ liệu trên máy tính và sau đó tiến hành phá hủy nó. Nó có một bản sao sẵn có cơ chế. Mặc dù vi-rút có xu hướng tự gắn vào chương trình khác, nhưng sâu là độc lập ,chương trình tự sao chép và thường lan truyền qua mạng. Sâu thường là nguyên nhân gây ra một số thiệt hại trên mạng ngay cả khi đó chỉ là việc tiêu thụ băng thông và hậu quả của mạng chậm lại. Hình ảnh sau đây cho thấy sâu hoạt động như thế nào trong môi trường kỹ thuật số:

*Hình 5: Sâu máy tính*

Worms khác nhau có tải trọng khác nhau. Tải trọng là những gì một con sâu được thiết kế để làm khác hơn là nhân rộng. Điều này có thể liên quan đến gửi thư hàng loạt, xóa dữ liệu hoặc thậm chí ổ cứng hoặc mã hóa tập tin dựa trên phần mở rộng. Worms lây lan bằng cách tận dụng các lỗ hổng trên mạng. Nếu sâu có

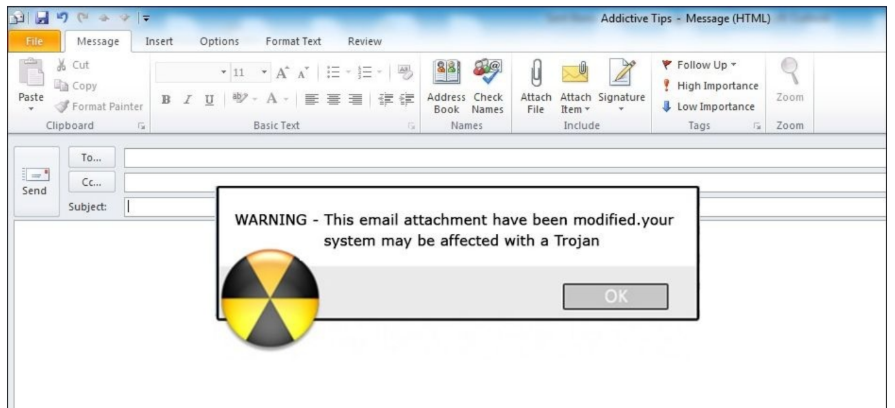
Trong tự nhiên được một thời gian, các bản vá thường có sẵn cho các lỗ hổng mà nó khai thác và nếu áp dụng thành công, sự lây lan của nó có thể bị hạn chế. Tuy nhiên, nếu đó là một con sâu không ngày lợi dụng một lỗ hổng không xác định / chưa được vá, nó có thể gây ra sự tàn phá

mạng.

* 1. **Trojans**

Có một thực tế nổi tiếng là vào thời cổ đại, một con ngựa thành Troy bằng gỗ rỗng, có chứa những người lính, giả mạo như một món quà chia tay từ người Hy Lạp là nguyên nhân dẫn đến sự sụp đổ của thành phố Troy. Trong thời đại ngày nay, phần mềm độc hại giả mạo như một số hữu ích công cụ được biết đến như là một phần mềm độc hại Trojan. Phần mềm độc hại Trojan có thể nguy hiểm vì nó đã được cố ý tải xuống và cài đặt và người dùng có thể xác định hệ thống là một công cụ đáng tin cậy. Điều này có thể dẫn đến sự leo thang ngoài ý muốn của các đặc quyền.

Vectơ lây nhiễm ưa thích cho Trojans là thông qua kỹ thuật xã hội. Ví dụ: nhiễm trùng xảy ra khi người dùng nhấp vào tệp đính kèm của e-mail giả sử nó là một cái gì đó sử dụng hoặc thay thế xuất hiện tại một trang web với mã độc hại. Trojans thường có tải trọng Một chế độ ngày càng phổ biến là mở một cửa hậu và cung cấp truy cập vào một bộ điều khiển. Không dễ để phát hiện các cửa hậu như vậy; tuy nhiên, những điều này dẫn đến tăng lưu lượng truy cập và tải nhiều hơn trên bộ xử lý, hiển thị dưới dạng tính toán phản hồi chậm hơn bình thường, như trong hình sau:

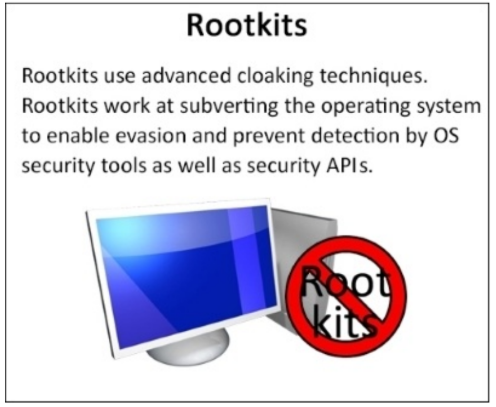
*Hình 7:**Trojan****s***

Đã có một số Trojans cực kỳ tàn phá trong quá khứ và tôi chắc chắn rằng

chúng ta sẽ thấy nhiều hơn trong tương lai. Một số trong những cái đáng chú ý là NetBus, Sub7, Back Orifice, Zeus ...

* 1. **Rootkits**

Tên của phần mềm độc hại thực sự khá mô tả. Như chúng ta đã thấy, mỗi loại phần mềm độc hại có tên từ một số đặc điểm hoạt động của nó. Cùng tương tự dòng, rootkit thực sự là một tập hợp các phần mềm độc hại (bộ công cụ) hoạt động ở gốc (hoặc quản trị viên) cấp. Đây có thể là tự động hoặc yêu cầu một hành vi sai trái để có được root đặc quyền trước khi cài đặt phần mềm. Do tính chất bắt nguồn từ hoạt động của nó, rootkit thường khó phát hiện. Rootkit, sau khi cài đặt, thiết lập quyền kiểm soát hoàn toàn đối với các chức năng quan trọng và có thể ngăn các công cụ phát hiện phần mềm độc hại hoạt động hoặc thậm chí thông tin sai liên quan đến sự hiện diện của phần mềm độc hại. Rootkit có thể được cài đặt trong kernel, khiến chúng khó theo dõi và loại bỏ hơn và có thể cần một bản hoàn chỉnh mới cài đặt lại hệ điều hành. Một số phần mềm đích rootkit, đôi khi, yêu cầu một thay thế phần cứng hoặc ít nhất, thiết bị chuyên dụng để cho phép trả lại để bình thường. Một mô tả hình ảnh của rootkit được hiển thị như sau:



*Hình 8: Rootkits*

Rootkit sử dụng một số kỹ thuật khác nhau để kiểm soát hệ thống. Trong sô phổ biến nhất là khai thác bất kỳ lỗ hổng nào tồn tại trong bất kỳ thành phần nào của hệ thống bị tấn công. Điều này nhanh chóng theo sau sự leo thang đặc quyền. Để ngăn chặn sự phát hiện, rootkit sử dụng các kỹ thuật che giấu tiên tiến. Sau khi cài đặt và có được các đặc quyền cần thiết, rootkit hoạt động trong việc lật đổ hệ điều hành để cho phép trốn tránh và ngăn chặn sự phát hiện của các công cụ bảo mật hệ điều hành cũng như các API bảo mật. Điều này đạt được bằng cách che giấu khả năng hiển thị của các quy trình đang chạy, tiêm mã trong hoạt động hệ thống và sửa đổi trình điều khiển và mô-đun hạt nhân. Rootkit cũng có xu hướng vô hiệu hóa sự kiện đăng nhập để ngăn chặn phát hiện ở giai đoạn sau.

* 1. **Backdoors**

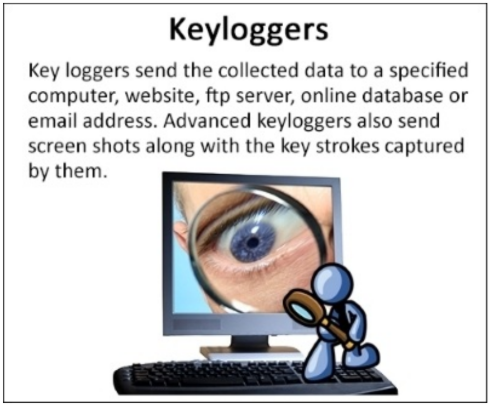
Backdoors là phần mềm độc hại chuyên dụng với mục đích là mở một cửa hậu bị nhiễm hệ thống. Điều này có thể được sử dụng để cho phép các yêu cầu đến từ tin tặc, đánh cắp dữ liệu có giá trị và kiểm soát hoàn toàn hệ thống. Backdoors cũng có thể được sử dụng để gửi virus, SPAM, hoặc quản lý một mạng lưới các bot. Đồ họa sau đây giải thích các cửa hậu trong một tóm lại:



*Hình 9: Backdoors*

* 1. **Keylogger**

Phần mềm độc hại giám sát tổ hợp phím được gọi là keylogger. Họ đăng nhập, lưu trữ và chuyển tiếp mỗi phím được nhấn trên máy tính trên cơ sở định kỳ được xác định trước. Những keylogger này gửi dữ liệu được thu thập đến một máy tính, trang web, máy chủ FTP, cơ sở dữ liệu trực tuyến hoặc e-mail được chỉ định địa chỉ có thể được mã hóa cứng hoặc thậm chí có thể được mã hóa động. Những thói quen này nắm bắt tất cả dữ liệu, bao gồm tên người dùng và mật khẩu. Dữ liệu này thường được ghi lại và được lưu trữ dưới dạng mã hóa. Một số keylogger tiên tiến cũng gửi ảnh chụp màn hình cùng với các nét chính được chụp bởi chúng. Những ảnh chụp màn hình này giúp tương quan các nét chính chụp với bối cảnh nơi chúng đã được thu thập. Một số tổ chức doanh nghiệp sử dụng chúng như một phương tiện giám sát nhân viên. Đồ họa sau đây cho chúng ta một tổng quan về keylogger:

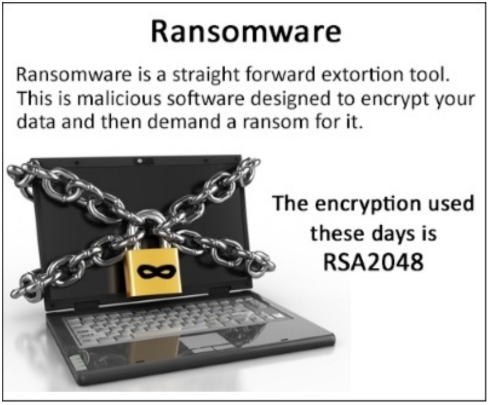
*Hình 10: Keyloggers*

Mặc dù trọng tâm của chúng tôi là phần mềm độc hại và keylogger dựa trên phần mềm, nhưng nó đáng để hiểu rằng keylogger dựa trên phần cứng cũng có sẵn. Đây có thể là USB nhỏ- các thiết bị dựa trên hoặc các đầu nối thông qua đó bàn phím được kết nối. Đây có thể là cả hai loại PS2 hoặc USB.

* 1. **Ransomware**

Ransomware là một công cụ tống tiền đơn giản. Đây là một phần mềm độc hại được thiết kế để mã hóa dữ liệu của bạn và sau đó yêu cầu tiền chuộc cho nó. Mã hóa được sử dụng những ngày này là RSA-2048 và nó đủ mạnh để ngăn người dùng phá vỡ nó trong bất kỳ lý do nào lượng thời gian và điều này buộc họ phải trả tiền chuộc hoặc quên hoàn toàn dữ liệu. Chế độ thanh toán thông qua Bitcoin hoặc các loại tiền kỹ thuật số khác và thanh toán được thực hiện thông qua máy chủ chuyên dụng được lưu trữ trong Deep Web.

Các nhà nghiên cứu bảo mật đã kiểm tra các phiên bản trước đó của Ransomware, chẳng hạn như CryptoLocker và CryptoWall, và đã xác định rằng những thứ này hoạt động bằng cách mã hóa một sao chép tập tin gốc rồi xóa bản gốc. Vì tệp gốc đã bị xóa, nạn nhân thực sự có thể phục hồi các tập tin gốc với sự trợ giúp của phần mềm khôi phục dữ liệu và trong cuộc mặc cả, tránh trả tiền cho những kẻ tống tiền.

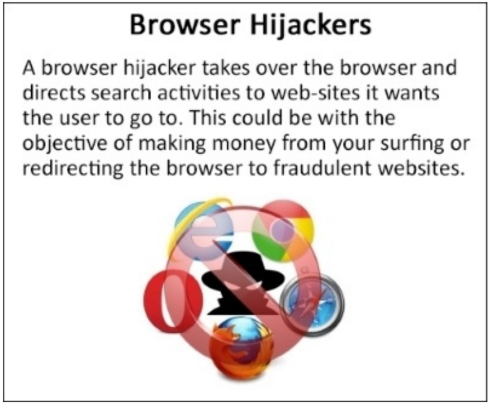
Ngay khi các tác giả phần mềm độc hại nhận ra điều này, họ đã thay đổi cách tiếp cận của họ. Không chỉ làm họ bắt đầu xóa các tập tin bị xóa, họ cũng thêm mối đe dọa làm lộ nội dung của các tập tin được mã hóa ở nơi công cộng. Điều này làm tăng đáng kể tỷ lệ thanh toán của họ và họ được đồn là đã kiếm được hàng chục triệu đô la từ các khoản thanh toán được thực hiện bởi nạn nhân. Đồ họa sau đây cho chúng ta cái nhìn tổng quan về ransomware là gì:

*Hình 11: Ransomware*

Vectơ lây nhiễm thông thường cho ransomware, chẳng hạn như CryptoWall, là bởi các tệp đính kèm e-mail.Email có chủ đề lôi cuốn được gửi, chứa các tệp có phần mở rộng zip như trong thực tế, các tệp đính kèm chứa thực thi bị xâm phạm được ngụy trang dưới dạng tệp PDF. Một số phần mềm độc hại này cũng có thể lây nhiễm các tệp trong chia sẻ mạng, cho phép lây nhiễmlan truyền trên mạng.

* 1. **Browser hijackers**

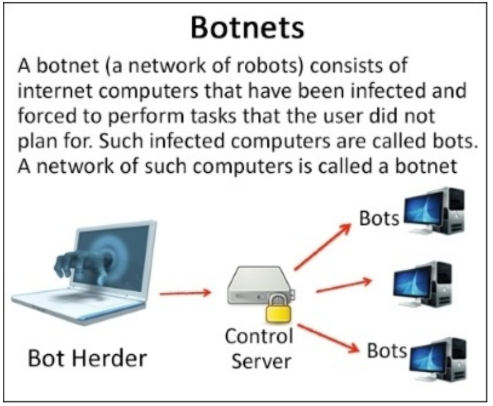
Một biến thể nguy hiểm khác của phần mềm độc hại là không tặc trình duyệt. Một kẻ tấn công trình duyệt mất qua trình duyệt và chỉ đạo các hoạt động tìm kiếm đến các trang web mà nó muốn người dùng truy cập. Điều này có thể với mục tiêu kiếm tiền từ việc lướt web của bạn hoặc chuyển hướng trình duyệt đến các trang web lừa đảo. Điều này có thể là một nguyên nhân của mối quan tâm lớn, đặc biệt, khi sử dụng trình duyệt bị tấn công để thực hiện các giao dịch tài chính trực tuyến. Một hình ảnh mô tả của kẻ tấn công trình duyệt được hiển thị như sau:



*Hình 12: Browser hijackers*

* 1. **Botnet**

Hãy nhớ lại những bộ phim cấp B cũ với một đội quân thây ma sẽ tiếp tục làm đấu thầu tổng thể; botnet theo cùng một hiệu trưởng, như trong hình sau:



*Hình 13: Botnets*

Một mạng botnet (một mạng lưới robot) bao gồm các máy tính Internet đã bị nhiễm và buộc phải thực hiện các nhiệm vụ mà người dùng không có kế hoạch. Các máy tính bị nhiễm như vậy được gọi là bot. Một mạng lưới các máy tính như vậy được gọi là botnet và máy tính điều khiển một số bot như vậy được gọi là bot header. Một nhóm những người chăn nuôi bot có thể báo cáo với một lệnh và trung tâm điều khiển. Chủ sở hữu của một mạng botnet có thể sử dụng mạng của họ theo một số cách. Botnet có thể được sử dụng để tuyên truyền các bệnh nhiễm trùng, gửi thư rác, thực hiện từ chối dịch vụ các cuộc tấn công, và như vậy. Điều khá phổ biến là các botnet được cho thuê hoặc bán hoàn toàn trong cộng đồng ngầm.

1. **Cách thức hoạt động của phần mềm độc hại.**

Theo wikipedia *Payload*là các phần của một loại virus có chứa các mã lệnh cho các mục đích của virus, trong đó có thể bao gồm từ tương đối lành tính (ví dụ, quấy phá nạn nhân, thể hiện bản thân) cho đến rất độc hại (ví dụ, chuyển tiếp thông tin cá nhân cho những người khác, phá hủy hệ thống).

Mỗi phần mềm độc hại đều có một công việc phải làm. Cho dù đó là để làm nghẽn mạng hoặc đánh cắp tiền của bạn, phần mềm độc hại được thiết kế với một mục tiêu. Mục tiêu này là được gọi là payload của nó. Đây là thiệt hại mà phần mềm độc hại gây ra cho hệ thống hoặc mạng của chúng tôi. Từ góc độ phân tích, điều rất quan trọng đối với chúng tôi là hiểu trọng tải của phần mềm độc hại là gì. Điều này giúp chúng tôi xác định phạm vi thiệt hại do phần mềm độc hại gây ra và tìm ra cách ngăn chặn, chống lại hoặc ngăn chặn thiệt hại gây ra.

Các tải trọng này có thể là một trong những điều sau đây:

* Phá hoại
* Trộm cắp danh tính
* Gián điệp
* Gian lận tài chính
* Trộm cắp dữ liệu
* Sử dụng sai tài nguyên
  1. **Destructive(Phá hoại )**

Mặc dù hầu hết các *payload* đều bị phá hủy theo cách này hay cách khác, một số phần mềm độc hại chuyên về thực hiện hoạt động phá hoại tập trung.

Trong một số trường hợp, dữ liệu phá hủy có thể dễ dàng xác định và có thể bao gồm sự cố hệ thống hoặc thiết bị bị nhiễm. Điều này cũng có thể liên quan đến dữ liệu, sửa đổi hoặc xóa các tập tin, thậm chí định dạng phương tiện và phá hủy tất cả nội dung.

Một số phần mềm độc hại được thiết kế để tự phát tán trên mạng. Khác với bản thân góc lan truyền, điều này có thể gây ra sự suy giảm lớn trong hiệu suất của mạng.

Phần mềm độc hại cũng đã được biết là phá hủy phần cứng và làm cho máy tính hoàn toàn không có chức năng. Một kẻ giết máy tính sớm như vậy là virus CIH đã ảnh hưởng đến BIOS trên bo mạch chủ nhất định.

* 1. **Identity theft ( Đánh cắp danh tính )**

Một mục tiêu rất phổ biến của phần mềm độc hại là hành vi trộm cắp danh tính. Phần mềm gián điệp độc hại giám sát tất cả hoạt động với mục đích lấy thông tin liên quan đến danh tính của bạn.

Phần mềm độc hại tập thông trung đánh cắp tin liên quan đến các mục sau:

* Tên người dùng và mật khẩu
* Thông tin thẻ tín dụng và thẻ ghi nợ
* Tài khoản ngân hàng trực tuyến
* Chi tiết về tài khoản e-mail và ngân hàng được liên kết với họ
* Số an sinh xã hội
* Giấy tờ tùy thân khác
* Thông tin sổ địa chỉ bao gồm địa chỉ email
* Thông tin nhận dạng cá nhân khác (PII)
  1. **Espionage(Gián điệp)**

Phần mềm độc hại đã được sử dụng ở vị trí hàng đầu trong hoạt động gián điệp của cả kẻ tốt và kẻ xấu. Nơi tội phạm máy tính đã sử dụng phần mềm độc hại để thu thập thông tin về bạn bè và kẻ thù, bọn tội phạm đã sử dụng thành công phần mềm độc hại cho mục đích thu thập thông tin trên mục tiêu tiềm năng. Phần mềm độc hại cũng đã được sử dụng thành công để tiến hành công nghiệp gián điệp.

Trên thực tế, các phần mềm độc hại như Dino và Regin là biểu hiện cho sự tinh vi của vũ khí không gian mạng đã được phát triển cho mục đích gián điệp. Cấu trúc của những phần mềm độc hại này hiển thị một mức độ tùy biến, cho phép các bộ điều khiển sử dụng họ để giám sát hàng loạt và gián điệp mục tiêu.

Mức độ năng lực kỹ thuật và độ tinh vi mà các vũ khí này thể hiện là chỉ dẫn về các nguồn lực đáng kể dành cho sự phát triển của họ. Chi phí của xây dựng vũ khí không gian mạng ghê gớm như vậy dường như cho thấy sự tham gia của cấp nhà nước diễn viên.

Là một điệp viên kỹ thuật số, nó trở nên rất quan trọng đối với chúng tôi để hiểu, phát hiện và xác định phần mềm gián điệp và hành động của nó.

* 1. **Financial fraud(Gian lận tài chính )**

Một phần phổ biến của sự khôn ngoan điều tra trong ngành điều tra số là theo tiền. Thật không may, đây chính xác là những gì tội phạm mạng thích làm. Một số rất tinh vi phần mềm độc hại được nhắm mục tiêu vào các giao dịch tài chính điện tử cũng như trích tiền với tống tiền điện tử.

Một cách sử dụng khá phổ biến là xác định người trong thương mại quốc tế và giám sát họ tương tác với người mua hoặc nhà cung cấp. Ngay khi hàng hóa được vận chuyển, tội phạm mạng bước vào và trong khi mạo danh người giao hàng, yêu cầu người mua gửi tiền đến tài khoản khác. Khi tiền được chuyển, tiền sẽ được rút nhanh chóng hoặc di chuyển để tiền không thể dễ dàng truy tìm hoặc thu hồi.

Một phần mềm độc hại phổ biến hiện nay chuyên mã hóa dữ liệu trên các hệ thống và sau đó đòi tiền chuộc để giải mã nó. Trong trường hợp tiền chuộc không được trả, bọn tội phạm đe dọa để rò rỉ dữ liệu được giải mã trên Web. Trong khi mọi người có thể chịu đựng được sự mất mát của dữ liệu của họ, họ ít có khả năng chấp nhận ý tưởng có dữ liệu bí mật của họ đột ngột xuất hiện trực tuyến.

* 1. **Theft of data(Đánh cắp dữ liệu)**

Nếu có một điều phổ biến trên không gian mạng , đó là hành vi trộm cắp dữ liệu. Trong hầu hết các trường hợp sử dụng phần mềm độc hại (ngoại trừ một số phần mềm được đề cập trước đó), kiếm tiền từ phần mềm độc hại xảy ra kết hợp với trộm cắp dữ liệu. Một số phần mềm độc hại tập trung vào thông tin người dùng và chi tiết tài chính, một số tập trung vào hình ảnh và video, và những người khác thu hoạch tài liệu và thông tin liên lạc. Trộm cắp bí mật thương mại cũng khá phổ biến.

* 1. **Misuse of resources(Sử dụng sai tài nguyên )**

Hầu hết các phần mềm độc hại có xu hướng tự thiết lập trong một hệ thống bị xâm nhập và sau đó chuyển sang (mis) sử dụng các tài nguyên có sẵn cho hệ thống. Phần mềm độc hại có thể đồng hóa một máy tính là một phần của mạng botnet. Nó có thể được sử dụng để tự động hóa thư rác hoặc thực hiện phân tán sự từ chối của dịch vụ tấn công. Máy tính thỏa hiệp cũng có thể được sử dụng để khai thác tiền điện tử các loại tiền tệ như Bitcoin. Những máy tính như vậy cũng được sử dụng để tấn công, lây nhiễm hoặc tuyển dụng người khác máy tính hoặc thiết bị cho mục đích bất chính tội phạm. Họ cũng đã được biết đến được sử dụng để gián điệp, giám sát và rình rập các mục tiêu.

1. **Phần mềm độc hại tấn công kiến trúc**

Hãy cùng chúng tôi xem xét năm trụ cột (giai đoạn) sau trong kiến ​​trúc của phần mềm độc hại tấn công:

1. Giai đoạn xâm nhập: Đây là điểm mà phần mềm độc hại cố gắng xâm nhập vào hệ thống. Điều này có thể được thực hiện thông qua một ổ đĩa bằng cách tải xuống hoặc nhấp vào một liên kết trong một e-mail, có thể dẫn đến một vụ cướp trình duyệt hướng nạn nhân đến nơi Kẻ tấn công muốn họ đi.

2. Giai đoạn phân chia: Khoảnh khắc nạn nhân kết nối với một trang web độc hại, trang web chỉ đạo nạn nhân liên tục đến Máy chủ phân phối lưu lượng truy cập (TDS). Điều này xác định nạn nhân hệ điều hành và trình duyệt. Một TDS có thể khá phức tạp và có thể lọc ra các yêu cầu kết nối dựa trên loại trình duyệt, HĐH, địa chỉ IP và các loại khác tiêu chí. Ở giai đoạn này, TDS có thể được đặt thành thả hoặc chuyển hướng yêu cầu đến các trang web giải mã từ các địa chỉ IP đã biết của các nhà nghiên cứu bảo mật, công ty chống vi-rút hoặc phần mềm độc hại. Những địa chỉ IP đáp ứng các tiêu chí đặt trước được chuyển sang giai đoạn thứ ba.

3. Giai đoạn khai thác: Ở giai đoạn này, các mục tiêu của kẻ tấn công là để có được quyền truy cập mà không bị phát hiện truy cập máy tính. Dựa trên dữ liệu lượm lặt được về môi trường nạn nhân, bộ công cụ khai thác sẽ xác định lỗ hổng trong trình duyệt hoặc plugin trình duyệt và trực tiếp nạn nhân của một máy chủ đang chạy khai thác cụ thể cần thiết để làm tổn thương máy và có được chỗ đứng trong hệ thống.

4. Giai đoạn lây nhiễm: Đây là giai đoạn dữ liệu độc hại được tải xuống nạn nhân máy tính và hệ thống bị nhiễm.

5. Giai đoạn thực thi: Đây là giai đoạn mà bọn tội phạm có xu hướng lợi dụng hệ thống bị xâm phạm hoặc khai thác. Trong giai đoạn này, phần mềm độc hại có thể gọi về nhà và thiết lập kết nối để lọc dữ liệu nhạy cảm hoặc hoạt động như một phần của mạng botnet. Nó có thể thậm chí mã hóa dữ liệu nạn nhân và cố gắng tống tiền để giải mã nó.

### ****Indicators of Compromise(****Trích xuất các dấu vết tấn công hệ thống****)****

Indicator of Compromise (IoC) chính là những manh mối dữ liệu cho thấy dấu vết của một hành vi xâm nhập trái phép còn lưu lại trên hệ thống. Những dữ liệu này có thể bao gồm các đoạn log, email còn lưu lại, địa chỉ IP sau khi download dữ liệu, hay[giá trị md5](https://quantrimang.com/md5-cua-1-file-la-gi-118565) của các mã độc.

Các manh mối dữ liệu (IOC) vì chúng thường được biết đến là các dấu vết

xác nhận sự hiện diện của phần mềm độc hại. Về cơ bản, từ một mạng lưới điều tra số , đây là những dấu vết (hoặc tàn dư từ một vụ xâm nhập) mà khi được phát hiện trên hệ thống hoặc mạng, cho thấy sự thỏa hiệp với mức độ tin cậy c cụ chuyên dụng như Y ao. Có IOC dành riêng cho phần mềm độc hại và các công YARA ( <http://plusvic.github.io/yara/> ) giúp xác định sự tồn tại của phần mềm độc hại dựa trên các tìm kiếm cho các IOC này.

Thông thường, IOC bao gồm các địa chỉ IP lừa đảo đã biết, chữ ký vi rút, băm MD5 của phần mềm độc hại, URL xấu hoặc tên miền đã biết, v.v.

Để thúc đẩy tiêu chuẩn hóa, một số khung mở có sẵn. Tuy nhiên, không khuôn khổ có thể tuyên bố là tiêu chuẩn thực tế. Hai khung quan trọng nhất là như sau:

* Open IOC: Đây là viết tắt của Open Indicator of Compromise. Khung này là được quảng bá bởi Mandiant và có sẵn tại http://www.openioc.org/. Đây là một đơn giản Khung XML được xây dựng với mục tiêu ghi lại và mô tả sự xâm nhập hiện vật nằm trên một máy chủ hoặc một mạng.
* CybOXTM: Đây là viết tắt của Cyber ​​Observable eXpression. CybOX là một Hoa Kỳ Bộ An ninh Nội địa (DHS) dẫn đầu nỗ lực. CybOX cũng sử dụng XML lược đồ để mô tả các quan sát không gian mạng. CybOX có sẵn tại https://cyboxproject.github.io/.

Các manh mối dữ liệu có thể bao gồm các thành phần sau:

* Email từ một địa chỉ IP cụ thể
* Lưu lượng truy cập mạng đến một địa chỉ IP cụ thể
* Tạo khóa registry
* Xóa tập tin
* HTTP Nhận yêu cầu nhận được
* Tệp được tìm thấy khớp với hàm băm MD5 đã biết
* Dữ liệu được gửi đến một địa chỉ trên ổ cắm
* Một mutex tìm thấy
* Nhật ký dành riêng cho ứng dụng hiển thị thông tin liên lạc trên các cổng cụ thể
* Một giá trị băm MD5 tệp đã biết thay đổi
* Các URL hoặc tên miền xấu được biết đến được phát hiện
* Cấu hình của một dịch vụ đã thay đổi
* Một chủ đề từ xa đã được tạo ra

IOC, một khi được xác định, có thể được sử dụng để cung cấp đầu vào rất hiệu quả cho IDS và IPS và có thể cũng được sử dụng để cấu hình các quy tắc tường lửa. Do đó, bất kỳ hoạt động ứng phó sự cố đó là kế hoạch chắc chắn nên tiến hành vượt quá giai đoạn khắc phục để các IOC có thể xác định và đưa trở lại vào cơ sở hạ tầng phát hiện và phòng ngừa để tránh tổ chức bị tấn công lặp lại.

1. **Performing malware forensics. (**Thực hiện điều tra số phần mềm độc hại**)**

Bây giờ chúng ta đã có các nguyên tắc cơ bản, điều quan trọng là phải hiểu rằng điều tra số và phân tích mã độc. Phân tích phần mềm độc hại liên quan đến việc nắm bắt một mẫu phần mềm độc hại và thực hiện phân tích tĩnh hoặc động trên đó. Đây, mã được biên dịch và mã hóa bị đảo ngược để thử và xác định phần mềm độc hại nào đã được lập trình để làm.

Mặt khác, điều tra phần mềm độc hại cố gắng xác định vị trí và kiểm tra các dấu vết tồn tại trên phương tiện hệ thống, RAM và mạng để giúp trả lời liệu hệ thống có bị xâm nhập, nó đã được thực hiện như thế nào, vectơ lây nhiễm, phần mềm độc hại cụ thể nào đã tham gia, những gì dữ liệu được lọc ra, và như vậy.

Trong phần trước, chúng tôi đã xem xét IOC và cách họ giúp xác định xem hệ thống hoặc mạng đã bị xâm phạm. Trong khi điều này giúp trong trường hợp sự thỏa hiệp đã được gây ra bởi phần mềm độc hại đã biết; cho ngày không hoặc phần mềm độc hại chưa biết hoặc các biến thể của nó, một cuộc điều tra pháp y phần mềm độc hại cần phải được đưa ra.

Dấu hiệu đầu tiên của nhiễm phần mềm độc hại là một loại hành vi bất thường. Các Khoảnh khắc này được báo cáo, một quản trị viên cảnh báo sẽ kiểm tra hệ thống bằng một bản cập nhật chương trình phát hiện phần mềm độc hại như byte hoặc công cụ phần mềm độc hại như YARA IOC. Trong trường hợp hành vi vẫn tồn tại và không có phát hiện tích cực nào xảy ra, nó sẽ trở thành bắt buộc phải thực hiện một cuộc điều tra số chuyên sâu về phần mềm độc hại.

Yếu tố chính cần nhớ khi chúng tôi thực hiện điều tra trên máy bị ảnh hưởng bởi phần mềm độc hại là xem xét và thu thập tất cả các dữ liệu có sẵn để giảm thứ tự biến động. Điều này có nghĩa rằng chúng ta cần xem xét lấy RAM, tất cả các nhật ký mạng có liên quan, cũng như hình ảnh của ổ cứng Hơn nữa, chúng tôi cần giám sát chặt chẽ tất cả lưu lượng truy cập đến và từ bị ảnh hưởng hệ thống.

Chúng ta hãy cùng xem quy trình mà chúng ta cần tuân theo để tiến hành hiệu quả cuộc điều tra:

* Kiểm tra Bản ghi khởi động chính (MBR): Đây thường là khu vực đầu tiên khó khăn ổ đĩa và có kích thước 512 byte. Trong cuộc chiến không ngừng giữa phần mềm độc hại và chống phần mềm độc hại, cuộc đấu tranh là để đảm bảo ai tải lên đầu tiên. Trong trường hợp phần mềm độc hại tạo ra đầu tiên, nó có thể ngăn phần mềm chống phần mềm độc hại phát hiện ra. Đây là nơi MBR đi vào. Bất cứ khi nào máy tính khởi động, đoạn mã đầu tiên được thực thi là mã khởi động trong lĩnh vực này. Nếu phần mềm độc hại quản lý để độc hại sẽ thất bại trong nhiệm vụ của nó và phần mềm độc hại sửa đổi điều này thành lợi ích của nó, chống phần mềm sẽ vẫn tồn tại tất cả thời gian. Trong trường hợp này, sẽ hữu ích nếu chúng ta có một bản sao MBR cơ sở dự kiến.
* ID hệ điều hành: Một khi điều này đã được thực hiện đầy đủ, các xác định, sau đó dễ dàng tải xuống các tệp gói dịch vụ và các bản vá được băm đã biết (từ Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) / Hashkeeper) để kích hoạt điều tra viên để loại bỏ các tập tin tốt được biết đến từ cuộc điều tra. Ngược lại, nó trở nên thực sự dễ dàng để xác định các là các tệp tệp có băm MD5 khác với những gì chúng nên và đây có thể có khả năng bị nhiễm hoặc bị sửa đổi.

Kiểm tra RAM: Nếu chúng ta đã lấy bộ nhớ dễ biến mất như được thảo luận trong phần các chương trước, chúng ta nên tiến hành kiểm tra ảnh RAM hệ thống ở chế độ ngoại tuyến cách thức. Ngoài ra, một phân tích RAM trực tiếp có thể được thực hiện; tuy nhiên, nó nên lưu ý nguy cơ làm tổn hại dữ rằng điều này có liệu dễ biến mất như mọi bit hoạt động mà chúng tôi thực hiện trên một hệ thống tác động đến bộ nhớ dễ tổn thương . Bộ nhớ dễ biến mất thực sự là một lĩnh vực độc lập rộng lớn liên quan đến pháp y kỹ thuật số; tuy nhiên, từ chúng tôi hiểu quan điểm, chúng tôi sẽ xem xét nó một cách đơn giản. Một bài kiểm tra của bộ nhớ dễ biến mất có thể tiết lộ như sau:

* Hiện đang chạy các quy trình (phần mềm độc hại hoạt động trong RAM)
* Các quy trình ẩn
* Quá trình chấm dứt gần đây
* Mở tệp (ví dụ: tệp đang bị phần mềm độc hại truy cập)
* Xử lý sổ đăng ký đang được truy cập
* Kết nối mạng (bộ nhớ dễ bay hơi có thông tin đáng tin cậy hơn một cái có được bằng cách chạy các lệnh, chẳng hạn như netstat có đầu ra có thể có bị phần mềm độc hại xâm nhập)
* Cổng nghe
* Khóa mật khẩu và mật khẩu
* Toàn bộ tập tin
* Đoạn tập tin
* Từ khóa tìm kiếm nội dung không được mã hóa
* Dữ liệu ẩn
* Mã độc hại (phần mềm độc hại không mã)
* Kiểm tra và băm các tệp trên đĩa: Phân tích bộ nhớ dễ bị tổn thương cho chúng ta thấy các tệp nằm trong sử dụng hoặc mở bởi phần mềm độc hại. Điều này dẫn chúng ta đến việc định vị chúng trên đĩa và kiểm tra chúng rất chi tiết Điều này rất hữu ích trong việc xác định nơi chứa phần mềm độc hại thu thập dữ liệu để exfiltration. Các tệp được xác định là đang sử dụng bởi phần mềm độc hại có thể là băm và các tệp đáng ngờ có thể được gửi đến cổng thông tin nhận dạng phần mềm độc hại trực tuyến, chẳng hạn như VirusTotal và các giá trị băm có thể được kiểm tra bằng Phần mềm quốc gia Thư viện tham khảo (NSRL) tại *http://www.hashsets.com/nsrl/search/.*
* Kiểm tra sổ đăng ký: Tìm trong các vị trí tự khởi động, bất kỳ chương trình nào trong nhiều vị trí tự khởi động nên là một nghi phạm. Phần mềm độc hại có xu hướng xác định và đặt chính nó hoặc các biến thể khác nhau của nó ở nhiều vị trí tự khởi động với mục tiêu tăng kiên trì.
* Kiểm tra các chương trình chạy trên hệ thống: Xác định những gì mỗi chương trình làm và yêu cầu các chương trình để thực hiện một nhiệm vụ hợp pháp? Chương trình không xác định cần nhìn vào chi tiết hơn.
* Kiểm tra nhật ký hệ thống: Tìm kiếm những thứ không phù hợp. Xác định đi kết nối.
* Kiểm tra lịch sử duyệt web: Điều này có thể giúp xác định xem người dùng có đã truy cập các trang web bị xâm nhập đã biết cũng như xác định các vị trí mà từ đó một ổ đĩa việc tải xuống đã xảy ra.
* Kiểm tra các tạo phẩm của tệp: Đặc biệt là trong các tệp tải xuống và thư mục tạm thời, điều này có thể giúp xác định điểm vào phần mềm độc hại. Cũng tìm kiếm các tập tin bị xóa; phần mềm độc hại có thể xóa các tập tin mà nó không còn cần chỉ để che dấu vết của nó.
* Xây dựng dòng thời gian: Vẽ tất cả các hoạt động lượm lặt được từ ngày tệp, e-mail, truy cập web, cookie, nhật ký và như vậy để thử và xây dựng một chuỗi các sự kiện. Tập tin xuất hiện trên dòng thời gian của bạn trong khoảng thời gian mà bạn nghi ngờ hệ thống bị xâm phạm chắc chắn đòi hỏi một cái nhìn thứ hai.
* Kiểm tra lại mọi thứ.

Một khi điều này được thực hiện, nó đáng để tải hệ thống bị cáo buộc bị xâm nhập trong ảo môi trường và kiểm tra tất cả các hoạt động được thực hiện bởi nó. Tương tác của nó với mạng và những thay đổi do đó trong hệ thống cơ sở trước đó chắc chắn sẽ là đáng chú ý và một cuộc điều tra số hơn nữa dọc theo các dòng trước đó có thể làđược thực hiện để thu thập thêm thông tin về phần mềm độc hại và các hoạt động của nó. Khi phần mềm độc hại và IOC của nó đã được xác định, các IOC có thể được thêm vào nhiều các thiết bị chu vi để ngăn chặn sự tái phát của phần mềm độc hại trên mạng.

1. **Malware insight – Gameover Zeus Trojan**

Trojan Gameover Zeus là một trong những phần mềm độc hại thành công nhất mọi thời đại. Như Hầu hết các phần mềm độc hại, tất cả đều bắt đầu bằng một email spam vô hại, dẫn đến nhiễm trùng đến lượt nó, dẫn đến việc tiếp quản tài khoản, sau đó là gian lận. Tiền là chuyển ra khỏi tài khoản ngân hàng và để ngăn chặn việc phát hiện kịp thời, ngân hàng hoặc tổ chức tài chính phải chịu một cuộc tấn công từ chối dịch vụ phân tán (DDoS). Điều này cuộc tấn công khiến tất cả các tài nguyên bảo mật của ngân hàng tập trung vào việc giải quyết DDoS và nó cũng cho phép những kẻ tấn công điền vào nhật ký với rất nhiều dữ liệu liên quan đến DDoS điều tra viên có khả năng bỏ lỡ hoặc hoàn toàn mất thông tin liên quan đến tài chính trộm cắp. Trong khi đó, tiền được rút và rửa hiệu quả.

Zeus bắt đầu sự nghiệp với tư cách là một bộ phần mềm độc hại vào năm 2005 và Zeus phiên bản 2 đã được tung ra vào năm 2009. Tuy nhiên, vào năm 2011, mã nguồn Zeus đã được công khai và một số lập trình viên phần mềm đã tiếp tục tinh chỉnh nó thành một số biến thể. Một trong những biến thể đã thêm giao thức ngang hàng (P2P) và Gameover Zeus đã ra đời. Trước đó, có là các máy chủ chỉ huy và kiểm soát tập trung và điều này khiến chúng trở thành mục tiêu của pháp luật các nhà nghiên cứu thực thi và chống phần mềm độc hại.

Các khả năng ngang hàng tinh vi đã thực sự trao quyền cho phần mềm độc hại Zeus, phân cấp cấu trúc chỉ huy và kiểm soát cũng như giúp tạo botnet với các máy tính bị nhiễm nhận biết các đồng nghiệp gần đó, với các cập nhật cấu hình hàng ngày và cập nhật nhị phân hàng tuần thông qua các kênh chỉ huy và kiểm soát. Điều này thiếu một điểm duy nhất thất bại làm cho botnet Gameover Zeus rất kiên cường.

P2P Zeus hoặc Gameover Zeus là phần mềm độc hại nhắm mục tiêu thông tin ngân hàng và có khả năng gây tổn thất tài chính đáng kể. Nó thu hoạch thông tin ngân hàng, lây nhiễm các hệ thống để tham gia botnet, gửi thư rác, cũng được biết là cung cấp phần mềm độc hại khác như CryptoLocker và có thể tham gia vào các cuộc tấn công DDoS. Nó sửa đổi sổ đăng ký và lây nhiễm explorer.exe và các quá trình khác. Khi cư trú trong bộ nhớ, nó sẽ không hoạt động cho đến khi có web trang thuộc về một tổ chức tài chính được truy cập, nơi nó tiêm các trường bổ sung và cửa sổ bật lên để đánh cắp thông tin người dùng.

Các dấu vết do phần mềm độc hại Gameover Zeus để lại bao gồm thông tin trong phần dễ tổn thương bộ nhớ, nhật ký hệ thống, cũng như đăng ký hệ thống.

Một ví dụ về tạo thao tác có thể được tìm thấy trong trường hợp phần mềm độc hại này là một sửa đổi trong khóa đăng ký sau đây gây ra việc vô hiệu hóa tường lửa: *HKLM \ System \ Controlset002 \ Services \ SharedAccess \ Paramameter \ FirewallPolicy \ StandardProfile \ EnableFirewall* Phần mềm độc hại đặt giá trị thành 0, vô hiệu hóa tường lửa và giảm khả năng xảy ra phát hiện.

1. **Tổng kết**

Chương này tập trung vào việc xây dựng sự hiểu biết của chúng ta về phần mềm độc hại, nó là gì, hoạt động như thế nào, loại thiệt hại mà nó có thể gây ra là gì, cũng như cách xác định nó. Bạn tìm hiểu về IOC và hiểu cách xác định các hệ thống bị xâm nhập và Mạng. Bạn cũng đã tìm hiểu về quy trình điều tra phần mềm độc hại và các bước khác nhau mà chúng tôi theo dõi trong cuộc điều tra cùng với sự liên quan của họ.

Tiến về phía trước trong hành trình tìm hiểu về điều tra số , chúng tôi sẽ xem xét làm thế nào để đưa kiến thức của chúng tôi mà chúng tôi đã đạt được để sử dụng tốt và làm việc cùng nhau để giải quyết vụ việc trong chương tiếp theo.