Laboratorio 2 : Forensics

Rodrigo Castillo

16 de agosto de 2020

1. 3 reasons that justify to do a Malware Analysis

1.1. Primera razón

La primera razon por la cuál alguien querría analizar un malware es para buscar a sus creadores, pues muchos ataques informáticos son catastróficos para las empresas y por esta razón es bueno buscar a sus culpables

1.2. Segunda razón

Para dimensionar el daño potencial que pueda tener un archivo malicioso en un computador : Muchas veces nosotros descargamos contenido del cuál no sabemos su procedencia, por lo tanto, es bueno poder analizar que acciones está teniendo este contenido en nuestros dispositivos y de esta manera poder hacer un balance para saber si este contenido nos beneficia o nos perjudica.

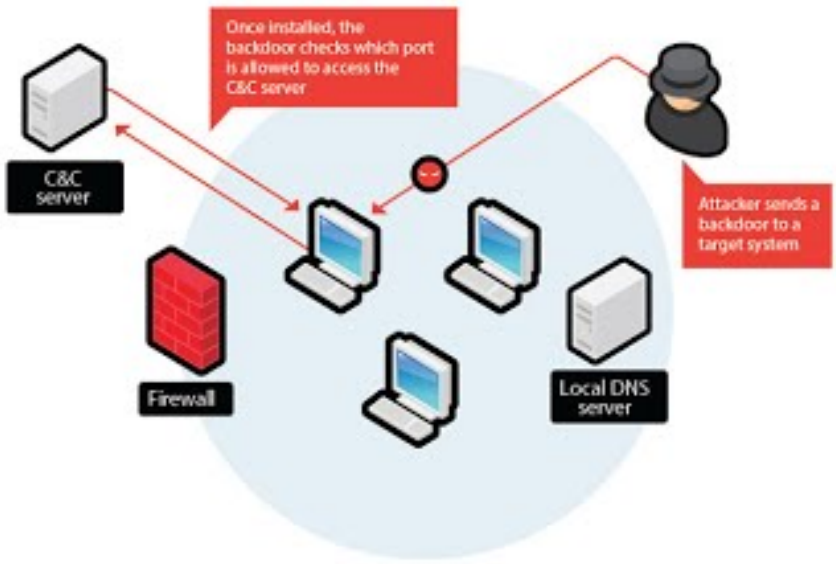
1.3. Tercera razón

Para entender el Malware, entender el malware puede prevenirnos de futuros ataques informáticos en muchas ocaciones, nos puede enseñar como prevenirlo y en un ambiente de seguridad ofensiva , como ejecutarlo.
Además de todo lo anterior, entender el malware puede ser facinante y puede contribuir con otras diciplinas de la informática, con esto, construir herramientas que nos puedan beneifciar en un futuro.

2. Tipos de malware

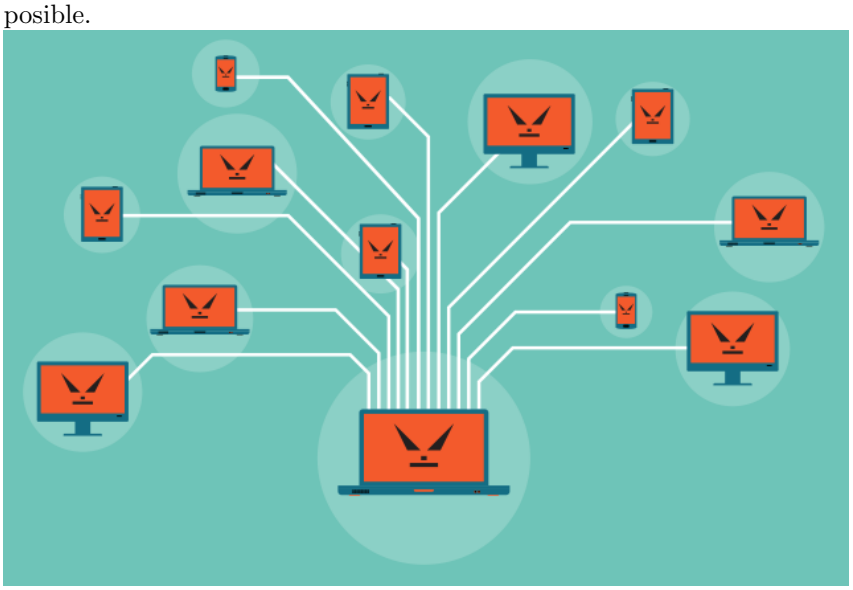
2.1. Backdoor

Un Backdoor(puerta trasera) es un programa o una brecha de seguridad que permite al atacante conectarse al dispositivo cada vez que el lo indique , generalmente se usan generando software vulnerable de exprofeso o instalando scripts que permiten hacer eso.



2.2. Botnet

Una botnet es un programa que permite al atacante obtener el acceso de varias máquinas que no son suyas , esto puede tener varios fines, como hacer ataques DDOS , minar criptomonedas , etc , las botnet siempre intentan adueñarse de la mayor cantidad de máquinas posible.



2.3. Downloader

Los Downloader son programas que descargan e instalan nuevas versiones de programas maliciosos , como troyanos y adware en las computadoras de las víctimas. Estos programas se ejecutan automáticamente cuando se inicia el sistema operativo.

2.4. information stealing malware

hay muchas manifestaciones de malware para robar información, pero se clasifican todos los programas maliciosos que están diseñados para mandar información del interés del atacante sin el consentimiento de la víctima .

2.5. Launcher

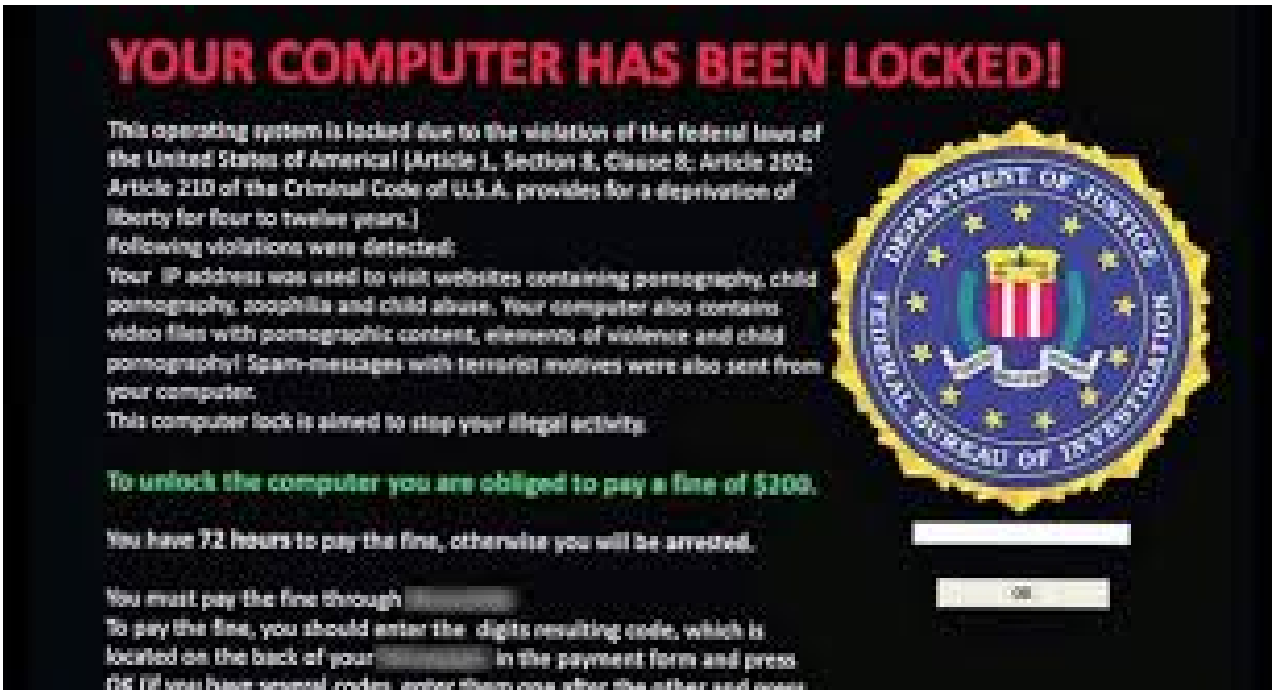
un Launcher es un tipo de malware que ejecuta otro malware.

2.6. Rootkit

Un rootkit es una brecha de seguridad que permite al atacante elevar los privilegios a privilegios no autorizados, pueden ser programas vulnerables del sistema operativo que se ejecutan con permisos de administrador o explotan la funcion setuid, pueden ser implantados por el atacante como estar instalados por el dueño de la maquina. Un ejemplo de un rootkit es la aplicación de Zoom.

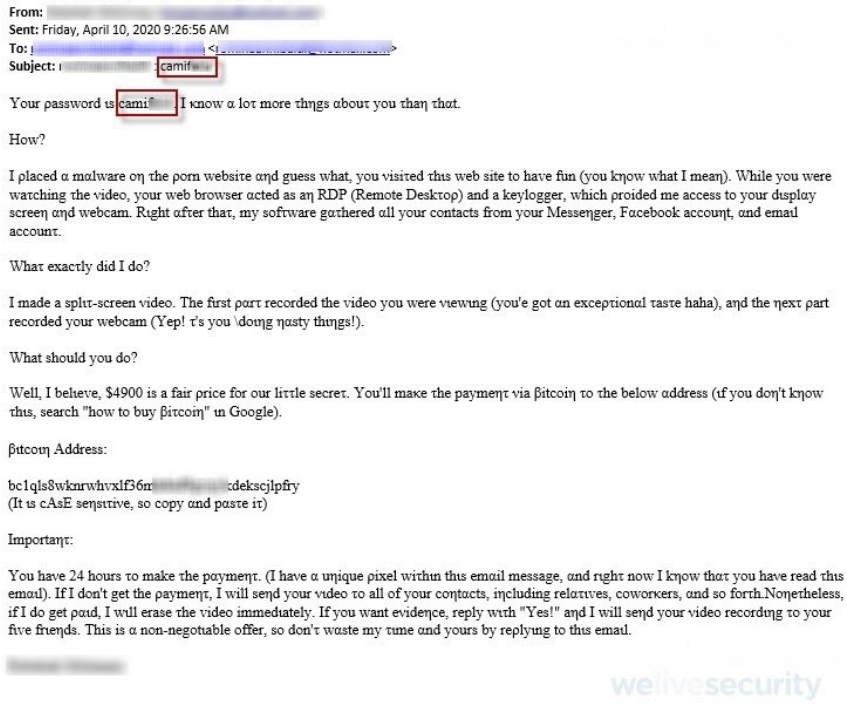
2.7. Scareware

Un Scareware es un programa que simula ser un antivirus o un servicio de seguridad, le advirte al usuario que la seguridad de su equipo esta en riesgo por alguna razon y luego le pide sus credenciales para protegerlo.



2.8. Spam Sending Malware

Un malware de spam es un tipo de malware que infecta a un dispositivo o se roba sus credenciales, y a travéz de esta las usa para mandar publicidad , hay varios ejemplos de este.


From:
Sent: Friday, April 10, 2020 9:26:56 AM
To:
Subject: camif

Your password is camif. I know a lot more things about you than that.

How?

I placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger, which proided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video. The first part recorded the video you were viewing (you'e got an exceptional taste haha), and the next part recorded your webcam (Yep! it's you \doing nasty things!).

What should you do?

Well, I believe, $4900 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy Bitcoin" in Google).

Bitcoin Address:

bc1qls8wknrwhvxlf36m:dekscjlpfry
(It is cAsE sensitive, so copy and paste it)

Importany:

You have 24 hours to make the payment. (I have a unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts, including relatives, coworkers, and so forth.Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your five friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

welivesecurity

2.9. Virus

un virus informático es un programa malicioso que en sus funciones intenta replicarse en otros dispositivos, ya sea por correos, a travez de la red, aplicaciones, etc.

2.10. Worm

un gusano informático es un tipo de virus , un programa malicioso que una vez infecta un dispositivo, intenta propagarse a los dispositivos que se encuentren en su red.

3. Malware analysis techniques

3.1. Basic Static Analisis

3.2. what this analysis inspect

consiste en inspeccionar facciones generales del malware, como su hash(caracterización) o la cantidad de elementos que tiene, no se puede saber mucho de su funcionamiento pero tampoco requiere mucho trabajo pues existen herramientas como virustotal que hacen eso automáticamente.

3.2.1. what is the product of this analysis

se puede identificar el malware

3.3. Basic Dynamic Analysis

3.3.1. What this analysis inspects

consiste en ejecutar un binario malicioso en un entorno controlado llamado sandbox con eso, se puede saber el daño potencial de este binario.

3.3.2. What is the product of this analysis

se puede visualizar el funcionamiento del malware sin necesidad de exponer una máquina real.

3.4. Advanced Static Analysis

3.4.1. What this analysis inspects

Éste analisis mira el código assembly de un binario o el código fuente de un lenguaje interpretado, lo que busca es reconstruir el codigo fuente del programa, con eso es posible entender el funcionamiento de un este. Para esto, se hace uso de una herramienta llamada un dissasembler, que reconstruye el código assembly de un programa sin necesidad de ejecutarlo.

3.4.2. What is the product of this analysis

Haciendo disassembly debidamente se puede entender todo el funcionamiento de un programa sin necesidad de ejecutarlo, sin embargo, hacer disassebly debidamente es un proceso muy complicado que requiere mucha practica , experiencia y dedicación.

3.5. Advanced dynamyc annalysis

3.5.1. What this analysis inspects

Este analisis analiza el funcionamiento del programa paso por paso, haciendo debugging se puede reconstruir el código y tener un panorama bastante amplio del funcionamiento del virus , un debugger es una herramienta con la cual se puede ejecutar el programa paso a paso y analizar cada paso, se pueden poner breakpoints, se pueden modificar los registros del programa, se puede forzar el programa a tomar otros flujos de ejecución...etc .

3.5.2. What is the product of this analysis

se puede entender casi perfectamente la manera en la que el virus fue construído y su funcionamiento .

4. Diferencia entre Host Based Signatures y Antivirus Based Signatures

4.1. Host Based Signatures

Las firmas basadas en host, son firmas que analizan los binarios fijandose en el funcionamiento de estos para decir si son malware o no, si un programa pide muchos permisos, si se conecta a ips poco confiables, es mas probable que sean malware.

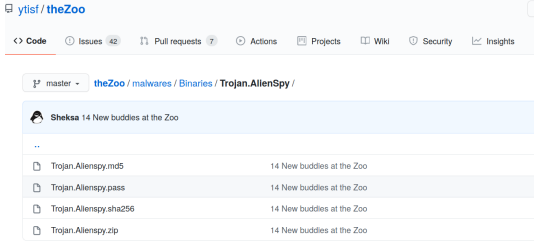
4.2. Antivirus Based Signatures

Las firmas basadas en antivirus son firmas que usan modelos de machine learning para detectar si algo es malware , entrenados con lo que ellas conocen que es malware, sin embargo, estas no son tan eficaces como las firmas basadas en características pues, los atacantes usan distintas técnicas de cifrado de malware con el fin de evitar estos reconocimientos de machine learning.

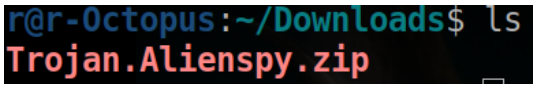
5. Download a file from from Malware Zoo (https://github.com/ytisf/t and upload it to VirusTotal.com. Review the host-based, antivirus, and network-based signatures reported by VirusTotal.com. What is the difference between host-based signatures and antivirus signatures?

5.1. Selección del malware

con propósitos del análisis, me dispuse a buscar un archivo binario de malware el cuál podré inspeccionar, en este curso, elegí el archivo Trojan.Alien_Spy :



el cual contiene un archivo comprimido con su binario.



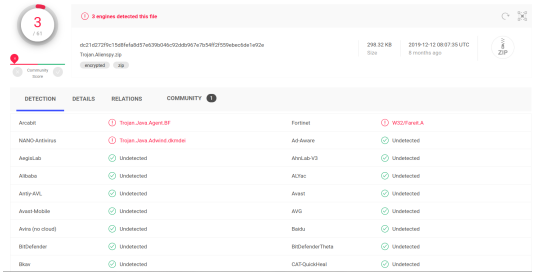
una vez descomprimido el archivo, obtenemos estos archivos .jar que hacen referencia a que este es un malware escrito en java

5.2. Analisis estatico:

Para ejecutar el analisis estático vamos a usar el servicio de virustotal, por lo que subiremos el archivo zip a virustotal.

5.2.1. Analizando el malware como archivo zip con antivirus conocidos(antivirus based signatures)

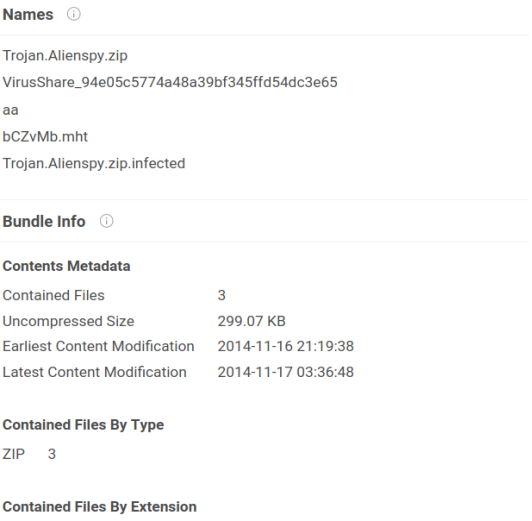
Virustotal es un servicio que usa diferentes servicios para ejecutar el analisis estatico de un malware, sin embargo, solo 3 de 61 de sus servicios detectaron que era un malware.



5.2.2. Analizando el virus como archivo zip con otras propiedades (host based signatures and network based signatures)

propiedades basicas del virus

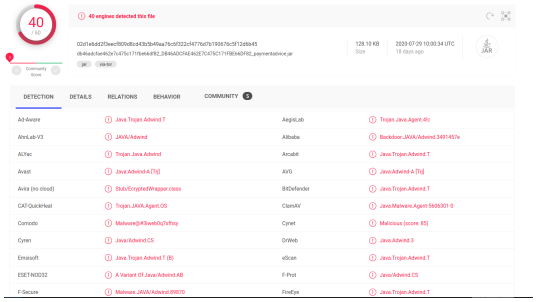
Estas propiedades hacen referencia a los hash del virus, a las carácterísticas del virus que



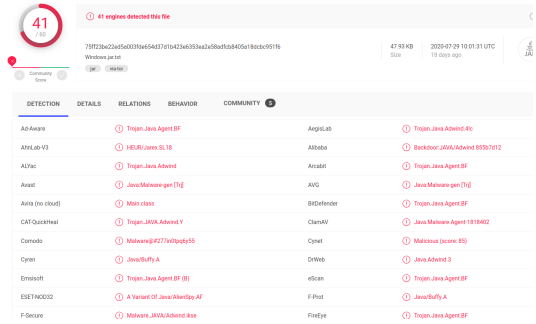
identifican al archivo.
el antivirus analiza los archivos que hay dentro del documento comprimido y retorna que tiene 3 archivos comprimidos con extension .jar, por lo que ahora procederemos a analizar los archivos jar individualmente.

5.2.3. Analizando los archivos jar con antivirus (antivirus based signatures)

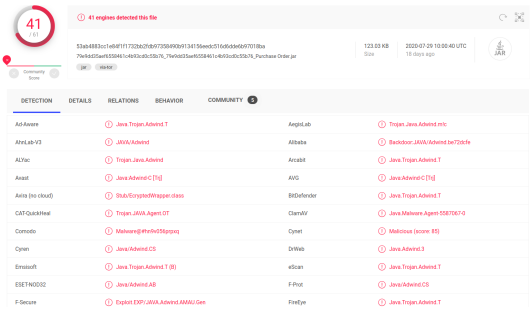
ya ejecutando el analisis con el primer binario en java, podemos ver que 40 de los 61 antivirus detectan que es un troyano:



ejecutando el analisis con el segundo binario 41 de los 60 antivirus lo reconocen



ejecutando el analisis con el tercer binario pasa lo mismo que con el segundo



5.2.4. Analizando los archivos jar según sus caracteristicas individuales

podemos ver los nombres que los diferentes antivirus ya le han asignado a estos archivos :

Names

79e9dd35aef6558461c4b93cd0c55b76_79e9dd35aef6558461c4b93cd0c55b76_Purchase Order.jar
79e9dd35aef6558461c4b93cd0c55b76_Purchase Order.jar
79e9dd35aef6558461c4b93cd0c55b76.jar
Alienspy1.jar
jar.jar
OsxAlienSpy_Purchase Order.jar.vir
MALWARE_JAR (28)
3.jar
79e9dd35aef6558461c4b93cd0c55b76.malware
vti-rescan
LcuSMagrIF.txt
69cad5948c07c50cc971084adff5cdcc
79e9dd35aef6558461c4b93cd0c55b76_Purchase Order.jar.infected
drprov.dll

tambien podemos ver los metadatos de los archivos file, nos muestra la siguiente información :

Bundle Info

Contents Metadata

Contained Files	5
Uncompressed Size	51.49 KB
Earliest Content Modification	2014-10-29 20:44:14
Latest Content Modification	2014-10-29 20:44:20

Contained Files By Type

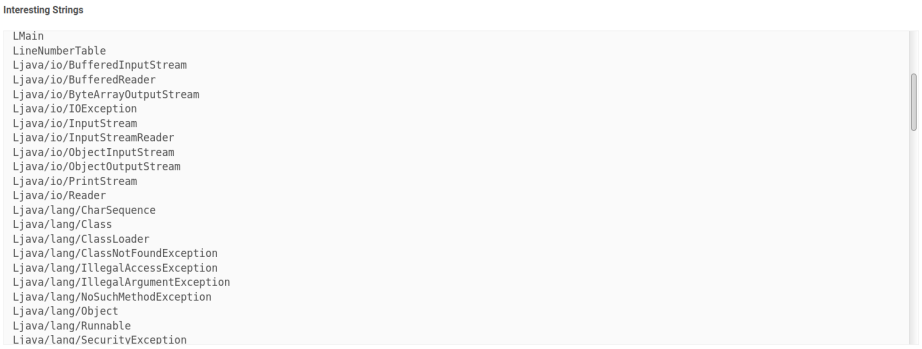
JAVA BYTECODE	2
UNKNOWN	3

Contained Files By Extension

ID	1
MF	2

en los metadatos se puede ver que el archivo fue creado en 29 de diciembre de 2014 , el tamaño del archivo y la cantidad de funciones que contiene , estos datos se pueden ver en el binario de un archivo y son caracteres legibles, sin embargo, existe una herramienta llamada exiftool que los extrae automaticamente.

También podemos ver que paquetes librerias de java está importando el archivo: , la forma de hacer esto localmente es viendo los caracteres legibles del binario mediante la herramienta strings. Esto puede ser de vital imprtancia cuando queramos reversar el codigo del malware en el futuro .



5.2.5. Que otras cosas se pueden saber

la razon principal por que elegí un troyano para hacer este trabajo es porque esta clase de malware tiene que conectarse a un servidor que maneja el atacante, es posible ver los paquetes y mediante estos localizar el servidor atacante, sin embargo , virustotal no hace esto con los binarios tipo java, por lo que hacer esto haria parte del analisis dinamico de maware (pues habria que ejecutarlo o hacerle reversing)y no haria parte de este trabajo :(.