Universitat Oberta de Catalunya

uoc.edu

IMPLEMENTACIÓN DE ANTIVIRUS SOBRE DISPOSITIVOS IOT

Yesith Alexander Álvarez Matta
Seguridad de las Tecnologías de la Información y de las comunicaciones
Seguridad en la Internet de las cosas

Carlos Hernández Ganan
Helena Rifà Pous
02/06/2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*IMPLEMENTACIÓN DE ANTIVIRUS SOBRE DISPOSITIVOS IOT*
Nombre del autor:	*Yesith Alexander Álvarez Matta*
Nombre del consultor/a:	*Carlos Hernández Ganan*
Nombre del PRA:	*Helena Rifà Pous*
Fecha de entrega (mm/aaaa):	06/2020
Titulación::	*Plan de estudios del estudiante*
Área del Trabajo Final:	*Máster universitario en* Seguridad de las Tecnologías de la Información y de las comunicaciones
Idioma del trabajo:	*Español*
Palabras clave	*IoT, Antivirus, Aseguramiento*

Resumen del Trabajo:

Durante la última década hemos evidenciado un aumento exponencial en la cantidad de dispositivos IoT que han sido vendidos en todo el mundo, desde asistentes virtuales, electrodomésticos inteligentes, automóviles, hasta sistemas complejos industriales, esto ha traído un incremento sustancial en el malware, ya que las malas prácticas por parte de los fabricantes y la falta de seguimiento de los usuarios finales, han convertido estos dispositivos en un foco creciente de infecciones para las botnets, creando así un negocio muy lucrativo que permite reclutar dispositivos sin ningún consentimiento, con el fin de realizar ataques de denegación de servicio distribuido a demanda u otorgado una capacidad de computo gigantesca al reunir miles de estos dispositivos para el minado de criptomonedas de forma ilegal. Es aquí que nace la idea de implementar un antivirus, un proceso de hardening y todo un conjunto de medidas que permitan controlar y proteger estos dispositivos de los peligros de internet y que a día de hoy ya se encuentran en nuestras casas.

Abstract (in English, 250 words or less):

Over the last decade we have seen an exponential increase in the number of IoT devices that have been sold worldwide, from virtual assistants, smart appliances, cars, to complex industrial systems, this has brought a substantial increase in malware, since Malpractice by manufacturers and lack of monitoring by end users have made these devices a growing focus of infection for botnets, thus creating a very lucrative business that allows devices to be recruited without any consent, in order to Undertake distributed denial-of-service attacks or grant gigantic computing power by gathering thousands of these cryptocurrency mining devices illegally. It is here that the idea of implementing an antivirus, a hardening process and a whole set of measures that allow to control and protect these devices from the dangers of the internet and that today are already in our homes is born.

A Dios, mis padres y mis hermanos quienes me han enseñado y cuidado durante cada etapa de mi vida.

A mis profesores y amigos quienes han sido un apoyo, una guía y una fuente de conocimiento.

Índice

Lista de Imágenes

1. Introducción

1.1 Contexto y justificación del Trabajo

La sociedad, es un grupo o conjunto de personas, pueblos o naciones que conviven bajo normas comunes [1], estas reglas se definen de acuerdo a las necesidades de los individuos y permiten la cooperación para lograr un beneficio mutuo. Nuestra sociedad, una civilización cada vez más enlazada, globalizada y conectada mantiene un proceso de evolución constante, caracterizándose por usar de manera intensiva las tecnologías de la información y la comunicación facilitando la creación, distribución, almacenamiento y manipulación de la información que dichos actores producen y consumen.

Este tipo de tecnologías que se utilizan de manera exponencial han traído consigo un fenómeno conocido como el IoT o el Internet de las cosas, por su nombre en inglés The internet of Things, el cual se puede describir como una red de dispositivos físicos que llevan sensores integrados, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos del mismo tipo. Estos dispositivos pueden abarcar desde objetos domésticos o de uso cotidiano hasta sofisticadas herramientas de tipo industrial [2], convirtiéndose en tecnologías innovadoras que se adecuan o se adaptan de manera más eficiente a cada uno de los ambientes donde se implementan.

Dentro de los dispositivos cotidianos más populares se encuentran las cámaras, los automóviles y asistentes virtuales, seguidos por los electrodomésticos tales como: televisores, neveras, cafeteras, entre otros; tomando cada vez más fuerza y haciendo que nos acostumbremos a una nueva realidad donde todos nuestros dispositivos se encuentran interconectados [3].

Ahora bien, con la creciente demanda por hardware, software y redes especializadas, los dispositivos IoT se han convertido a en una nueva amenaza, debido a que los ciberdelincuentes se han enfocado en este tipo de tecnologías, convirtiéndolos en un foco de infecciones informáticas de todo tipo. Sin embargo, cabe aclarar que el malware que los afecta opera de forma diferente al tradicional, debido a que estas plataformas no tienen la misma potencia de cómputo y no cuentan con los mismos cuidados tanto por parte del fabricante como del usuario final [4]. Por esta razón, es indispensable la implementación de medidas, controles y estándares que permitan mitigar la mayor cantidad de riesgos a los que se exponen, con el fin de proteger la salud de los dispositivos, evitar fugas de información, accesos no deseados y finalmente perdidas económicas para las empresas y la población en general.

1.2 Objetivos del Trabajo

- Investigar cómo funcionan los antivirus y sus diferentes modelos de protección sobre un dispositivo IoT.

- Investigar el comportamiento de los tres virus más comunes sobre un dispositivo IoT.

- Investigar cómo implementar un antivirus sobre un dispositivo IoT.

- Investigar las posibilidades que ofrecen los sistemas de antivirus para un dispositivo IoT.

1.2.1 Objetivos de Implantación

- Instalar y configurar un sistema Sandbox para realizar pruebas sobre un dispositivo IoT.
- Instalar y configurar un antivirus sobre un dispositivito IoT.
- Instalar y configurar un dispositivo IoT de forma asegurada.
- Puesta en marcha del producto final y realización de pruebas técnicas sobre el dispositivo.

1.2.2 Objetivos de Entrega

- Desarrollar las entregas parciales y entregarlas dentro del tiempo establecido.
- Crear La Memoria Final del trabajo realizado y entregarla dentro del tiempo establecido.
- Crear Video de Presentación y entregarlo dentro del tiempo establecido.

1.3 Enfoque y método seguido

La metodología que se seguirá durante el desarrollo del TFM de la UOC consta de 3 fases muy bien definidas que se evidencian a continuación:

Investigación: La investigación, es una actividad orientada a la obtención de nuevos conocimientos para su posterior aplicación con el fin de dar solución a un problema o interrogante, para esta fase se evaluarán los siguientes aspectos teniendo en cuenta el estado actual de las investigaciones publicadas enfocadas a las siguientes temáticas:

- Investigación del comportamiento de los virus más recientes sobre los dispositivos IoT.
- Investigación del funcionamiento de los antivirus actuales y sus diferentes modelos de trabajo sobre los dispositivos IoT.

Desarrollo: Una vez culminada la fase de investigación, se realizará la recolección de datos obtenidos sobre el comportamiento de los virus estudiados y el funcionamiento de los antivirus frente a estas amenazas, con el fin de realizar un análisis y determinar las principales causas de las infecciones.

- La evaluación de los diferentes antivirus se pone en marcha la ejecución de un malware en un ambiente Sandbox, se prueban las marcas más comunes disponibles y se evalúa el comportamiento de malware en el dispositivo IoT evaluado, adicionalmente se realizará una prueba de integridad sobre el dispositivo con el fin de comprobar su estado.

Resolución: Una vez identificados el comportamiento, y las principales causas de infección sobre el malware estudiado, se procederá a realizar la construcción de los entregables que se enumeran a continuación:

- Guía de aseguramiento del dispositivo IoT evaluado.
- Desarrollo de un script en python que permita evaluar los archivos del sistema operativo del dispositivo IoT con respecto a las firmas recolectadas durante la fase de investigación.
- La instalación de un sistema antivirus de manera adecuada sobre el dispositivo IoT.

1.4 Planificación del Trabajo

La planificación del proyecto consta de 5 fases, las cuales se evidencia su estado actual en la siguiente imagen:

	Actividades	Duración	Inicio	Fin
0	**Implementación de antivirus sobe IoT**	**116 días**	20/02/2020	15/06/2020
1	**Planeación**	**13 días**	20/02/2020	03/03/2020
1.1	Establecer el Problema	3 días	20/02/2020	22/02/2020
1.2	Definición de Objetivos	3 días	23/02/2020	25/02/2020
1.3	Definición de metodología	2 días	26/02/2020	27/02/2020
1.4	Definición de Tareas	3 días	28/02/2020	01/03/2020
1.5	Creación estado del Arte	1 día	02/03/2020	02/03/2020
1.6	**Entrega 1(Plan de Trabajo)**	1 día	03/03/2020	03/03/2020
2	**Investigación**	**27 días**	04/03/2020	31/03/2020
2.1	Investigación sobre Malware sobre IoT	5 días	04/03/2020	08/03/2020
2.2	Investigación sobre BotNets IoT	5 días	09/03/2020	13/03/2020
2.3	Investigación sobre Hacking IoT	5 días	14/03/2020	18/03/2020
2.4	Investigación sobre Antivirus	5 días	19/03/2020	23/03/2020
2.5	Recopilación de información	6 días	24/03/2020	29/03/2020
2.6	**Entrega 2**	1 día	31/03/2020	31/03/2020
3	**Implementación**	**27 días**	01/04/2020	28/04/2020
3.1	Instalación y configuración de SandBox	3 días	01/04/2020	03/04/2020
3.2	Pruebas de detección de Virus sobre SandBox	4 días	04/04/2020	07/04/2020
3.3	Monitoreo de actividad Maliciosa	3 días	08/04/2020	10/04/2020
3.4	Adquisición y Configuración de dispositivo IOT	3 días	11/04/2020	13/04/2020
3.5	Pruebas de detección de Acceso	3 días	14/04/2020	16/04/2020
3.6	Pruebas de detección de Virus sobre IOT	3 días	17/04/2020	19/04/2020
3.7	Aseguramiento de Dispositivo	3 días	20/04/2020	22/04/2020
3.8	Recopilación de información	4 días	23/04/2020	27/04/2020
3.9	**Entrega 3**	1 día	28/04/2020	28/04/2020
4	**Presentación**	**51 días**	29/04/2020	19/06/2020
4.1	Creación de Memoria Final	34 días	29/04/2020	02/06/2020
4.2	**Entrega 4 (Memoria Final)**	1 día	02/06/2020	02/06/2020
4.3	Creación de Vídeo	6 días	03/06/2020	09/06/2020
4.4	**Entrega 5 (Vídeo de Presentación)**	1 día	09/06/2020	09/06/2020
4.5	Preparación sustentación	5 días	10/06/2020	14/06/2020
5	**Defensa TFM**	**5 días**	**15/06/2020**	**19/06/2020**

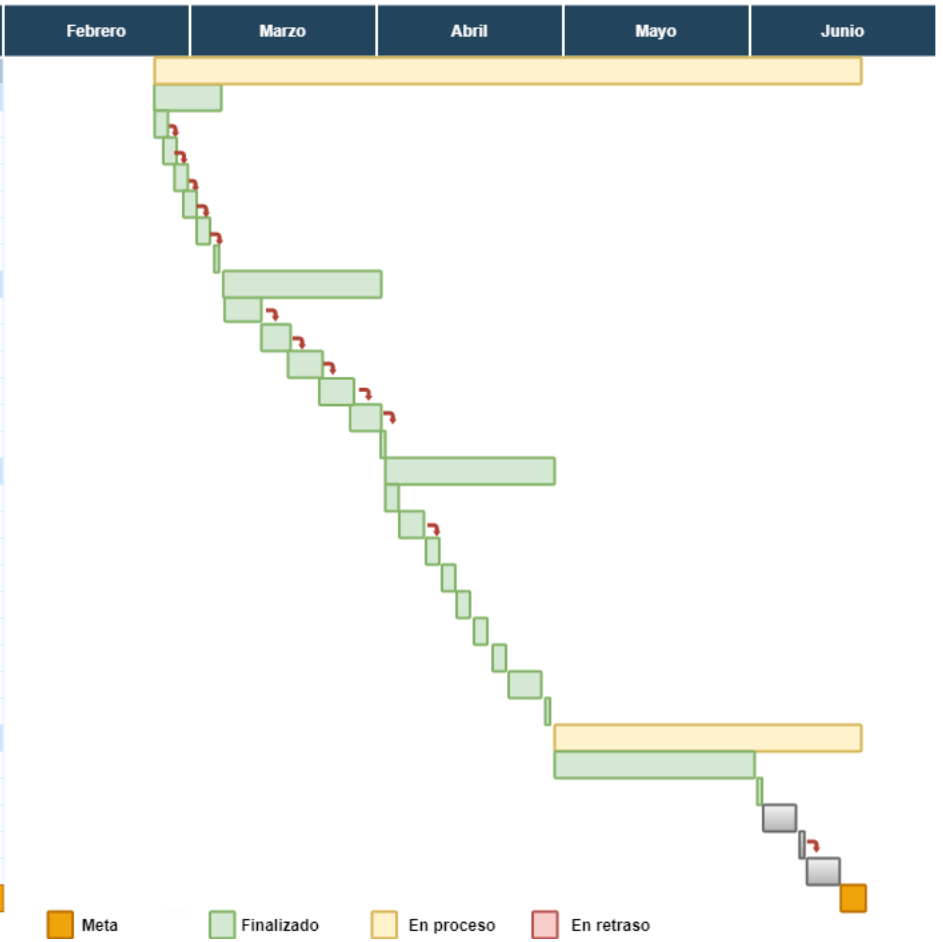

Imagen 1. Planificación del proyecto.

1.5 Breve sumario de productos obtenidos

En la finalización del proyecto se han obtenido dos productos:

- Una guía completa de aseguramiento para dispositivos IoT que utilicen sistema operativo Raspbian(Basado en Linux Debian).
- Un Script en Python para dispositivos IoT con sistemas operativos basados en Linux Debian.

1.6 Breve descripción de los otros capítulos de la memoria

- En la primera fase encontramos la investigación del malware, las botnets, los antivirus, la virtualización anidada y los ambientes sandbox enfocados a dispositivos IoT.
- En la segunda fase encontramos las pruebas de los antivirus Open Source en el dispositivo IoT.
- En la tercera fase se realiza el desarrollo del Script en Python que funciona como antivirus Ligero estático con las últimas firmas de botnets investigadas.
- En la cuarta fase se realiza la documentación de la correcta configuración del dispositivo IoT elegido, las conclusiones y el trabajo futuro.

2. Estado del Arte

De acuerdo a las referencias consultadas hasta la fecha y una fase antes del proceso de investigación se establece el estado del arte como una compilación de investigaciones donde se evidencian las malas prácticas y configuraciones de manera deficiente a la hora de implementar un dispositivo del tipo IoT [5]**,** trayendo un número importante de alarmas que evidencian el crecimiento de malware como virus, troyanos y *botnets* enfocadas específicamente sobre este tipo de dispositivos, los cuales se conectan directa o indirectamente a internet [6]. Por lo tanto se infiere que esta situación puede traer un número considerable de riesgos que se pueden materializar sobre las empresas y los hogares que disponen de estos dispositivos. Así pues es necesario evaluar el uso de antivirus y estándares de aseguramiento sobre este tipo de dispositivos ilustrando la manera más adecuada para su implementación que minimice riesgos y ponga barreras a los peligros que se encuentran expuestos a día de hoy [7].

3. Malware Sobre IoT

La palabra Malware viene de la abreviatura del inglés “malicious software” es decir corresponde a todo tipo de software malicioso incluyendo todas las formas conocidas como troyanos, ransomware, virus y gusanos [8] cuya finalidad es hacer daño, ya sea con la denegación de un servicio informático, destrucción de datos, robo de información, secuestro de recursos o la propia propagación de la infección entre otras, con el propósito de generar ganancias, espionaje, robo de secretos o sabotaje [9].
Actualmente se destacan cinco categorías de Malware muy reconocidas las cuales se enumeran a continuación:

- **Adware:** Recopila la mayor cantidad de información sobre los hábitos de navegación de un usuario con el propósito de envía anuncios emergentes al usuario.
- **Spyware:** Al igual que el Adware recopila información pero de manera mucho más intrusiva llegando a validar historiales de navegación, contenido de archivos para poder detectar clientes o informes financieros y recopilación de contraseñas, tokens y números de cuenta.
- **Ransomware:** Una vez descargado y ejecutado en el equipo victima procede a encriptar la mayor cantidad de archivos con el fin de ofrecer una calve a la víctima si se realiza un pago a cambio, es decir se convierte en un secuestro de datos con la posibilidad de un rescate.
- **Cryptomining:** Realiza el secuestro de un dispositivo con el único propósito de utilizar sus recursos computacionales para minado de criptomonedas.

- **Fileless:** Este tiene diferentes propósitos, pero su principal característica es que se ejecuta directamente en memoria evitando la dependencia archivos para su ejecución [9].

En efecto, todo este abanico de posibilidades ha hecho que más ciberdelincientes se adhieran a estas tecnologías para sacar el mayor provecho posible, generando una ola cada vez mayor de ataques, variantes y estrategias con el pasar de los años, por ejemplo el último estudio realizado por el CIS (Center of internet Security) evidencia que hasta Noviembre de 2019 el malware más utilizado es Zeus, seguido por Dridex, Nanocor y Coinminer utilizados específicamente como troyanos bancarios o mineros de criptomonedas [10]:

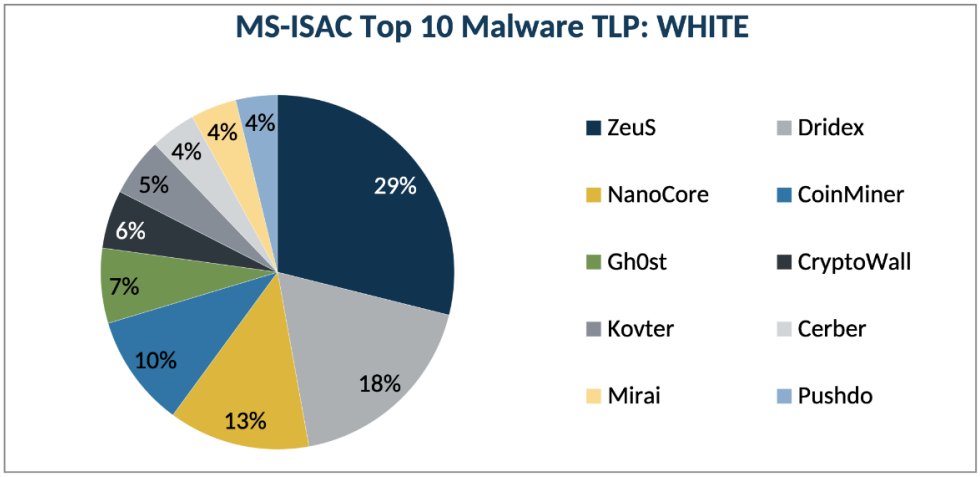

Imagen 2. Top 10 Malware.

Ahora bien, los dispositivos IoT se están convirtiendo cada vez más en un factor en la toma de decisiones por parte del consumidor, es decir a medida que más dispositivos electrónicos y dispositivos personales se ofrecen al mercado más dependencia y exigencia por parte del usuario final, haciendo que los fabricantes incluyan este tipo de tecnologías sobre la mayor cantidad de dispositivos posibles, lo que convierte en una tarea enorme por parte de los fabricantes para hallar la manera de proteger sus productos [11].

Sin embargo, lo que se evidencia es totalmente diferente ya que de acuerdo al estudio realizado por la Unidad 45 de Palo Alto Networks de un total de 1.2 millones de dispositivos analizados se revela que el 98% no utilizan ningún tipo de cifrado para sus conexiones, el 72% no tiene una correcta segmentación lo que facilita la propagación del malware y el 51% permite obtener datos sensibles de los usuarios de la herramienta, lo que se considera altamente preocupante [12].

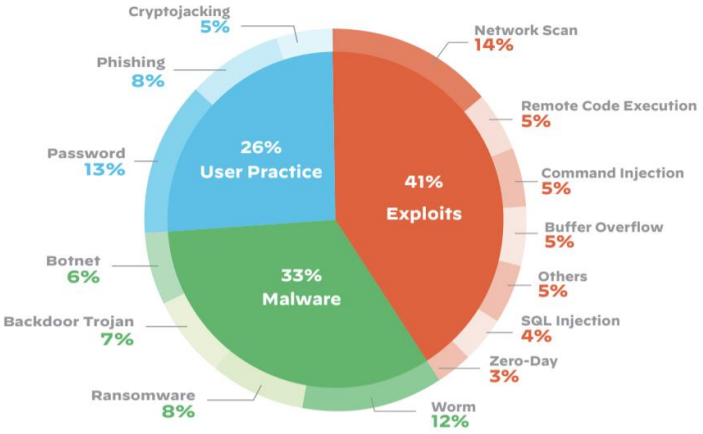

Imagen 3. Principales amenazas sobre dispositivos IOT.

Adicionalmente como parte del estudio se descubrió que el 57% de los dispositivos analizados son vulnerables a ataques de criticidad alta o media, el 41% son explotables por parte de un atacante y el 26% se debe a malas prácticas de configuración, sin mencionar el cambio de motivación por parte de los atacantes ya que la tendencia se enfoca en desplegar botnets con diferentes propósitos los cuales se encuentran en el siguiente capítulo [12].

4. Botnets Sobre IoT

Una botnet es una red de equipos informáticos conformados por computadores, tabletas, celulares o cualquier tipo de dispositivo con salida a internet que han sido infectados con malware, este software malicioso permite controlar de forma remota estos equipos, obligándolos a realizar actos para los cuales nos están diseñados como minar criptomonedas, enviar Spam, propagar virus o realizar ataques de denegación de servicio (DoS) a un objetivo en particular, claramente sin el conocimiento o el consentimiento de los propietarios de dichos equipos [13]. Normalmente a estos dispositivos infectados se les conoce como “bots” o “zombies” y se dice que no existe un número mínimo de equipos para crear una red de este tipo [14].

En el mundo se dieron a conocer este tipo de programas maliciosos a partir del año 2000 cuando un adolescente de Canadá lanzó una serie de ataques de negación de servicio contra páginas web muy populares como Yahoo, ETrade, Dell, eBay, Amazon, entre otros durante varios días, sobrecargando los servidores donde se encontraban los sitios web hasta que colapsaron, generando pérdidas millonarias para estas empresas [14].

Sin embargo en la actualidad este tipo de redes maliciosas se enfocan principalmente sobre dispositivos IoT como Smartphones, SmarTV, Routers, Rasberrys, etc., ya que este tipo de tecnologías por lo general carecen de actualizaciones, parchados y controles, sin contar con su

alto crecimiento por parte de las empresas en todo el mundo, convirtiéndolos en blancos mucho más fáciles, jugosos y llamativos para las botnets de los ciberdelincuentes [15].

Así pues, con el alto crecimiento de ataques sobre este tipo de dispositivos se puede evidenciar la tendencia, es decir el propósito por el cual los ciberdelincuentes utilizan este tipo de mecanismos para su beneficio, siendo el minado de criptomonedas la opción con mayor remuneración, seguido por el malware bancario [16], como se evidencia en la siguiente imagen:

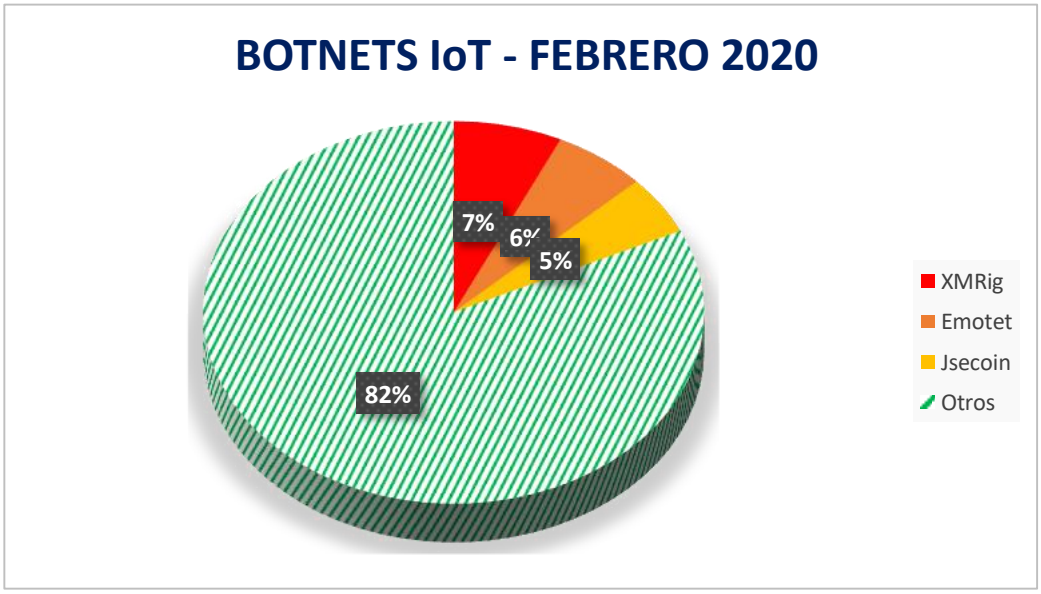

Imagen 4. Porcentaje mundial de Botnets.

Donde la botnet de nomrbe XMRig ocupa el primer lugar con 7% del total de las organizaciones a nivel mundial, seguido por Emotet y Jsecoin, impactando al 6% y al 5% respectivamente [16].

A continuación se relacionas las botnets más impactantes a nivel mundial:

N°	Nombre	Descripción
1	XMRig	XMRig es un software que utiliza la CPU para minar criptomonedas Monero, es de código abierto y se identificó por primera vez en Mayo de 2017.
2	Emotet	Emotet es un conocido troyano, avanzado, autopropagante y modular. Inicialmente solía ser un troyano bancario, pero recientemente se ha utilizado como distribuidor de otro malware o campañas maliciosas. Utiliza múltiples métodos para mantener la persistencia y técnicas de evasión para evitar la detección. Además,

		se puede propagar a través de correos electrónicos de phishing que contienen archivos adjuntos o enlaces maliciosos.
3	Jsecoin	Jsecoin es un minero de criptomonedas basado en la web, diseñado para realizar minería en línea de la criptomoneda Monero cuando un usuario visita una página web en particular. El JavaScript implantado utiliza una gran cantidad de recursos computacionales de las máquinas del usuario final para extraer monedas, lo que afecta el rendimiento del sistema.
4	Trickbot	Trickbot es un troyano bancario dominante que se actualiza constantemente con nuevas capacidades, características y vectores de distribución. Esto permite que Trickbot sea un malware flexible y personalizable que se puede distribuir como parte de campañas multipropósito.
5	Lokibot	Lokibot es un ladrón de información distribuido principalmente por correos electrónicos de phishing y se utiliza para robar diversos datos, como credenciales de correo electrónico, así como contraseñas para billeteras CryptoCoin y servidores FTP.
6	Agent Tesla	Agent Tesla es un RAT avanzado que funciona como un keylogger y un ladrón de contraseñas. AgentTesla es capaz de monitorear y recopilar la entrada del teclado de la víctima, el portapapeles del sistema, tomar capturas de pantalla y filtrar credenciales pertenecientes a una variedad de software instalado en la máquina de la víctima (incluidos Google Chrome, Mozilla Firefox y el cliente de correo electrónico Microsoft Outlook).
7	Ramnit	Ramnit es un troyano bancario que roba credenciales bancarias, contraseñas FTP, cookies de sesión y datos personales.
8	Formbook	Formbook es un InfoStealer que recopila credenciales de varios navegadores web, recopila capturas de pantalla, monitorea y registra pulsaciones de teclas, y puede descargar y ejecutar archivos de acuerdo con sus órdenes de C&C.

9	Vidar	Vidar es un infostealer dirigido a los sistemas operativos Windows. Está diseñado para robar contraseñas, datos de tarjetas de crédito y otra información confidencial de varios navegadores web y billeteras digitales
10	Glupteba	Glupteba es un backdoor que gradualmente se convirtió en botnet. Para 2019, incluía un mecanismo de actualización de direcciones C&C a través de listas públicas de BitCoin, una capacidad integral de robo de navegador y un explorador de enrutadores.
11	QSnatch	QSnatch un malware descubierto a finales de 2019 que se especializa en dispositivos NAS de la firma taiwanés QNAP, este permite modificar tareas y scripts programados así como evitar actualizaciones de firmware sobrescribiendo las URL del origen de la actualización e impide que se ejecute la aplicación nativa QNAP “MalwareRemover” y su principal función es extraer y robar nombres de usuario y contraseñas de todos los usuarios del dispositivo.

Tabla 1. Top 10 Botnets IoT.

5. Comportamiento de Virus IoT Más Recientes

5.1 Dark_Nexus IoT Botnet

De acuerdo a las últimas investigaciones realizadas por diferentes empresas de antivirus se ha descubierto una nueva botnet con características nuevas y capacidades nunca antes vistas, superando a la mayoría de botnets y malware especializados en dispositivos IoT, esta red de dispositivos controlados se le conoce como "dark_nexus" debido a una serie de caracteres que se evidencian en su banner principal de ataque "dark_NeXus_Qbot / 4.0", así como una fuerte influencia por la botnet “Qbot” la cual se enfocaba en atacar servicios de banca en línea desde hace 10 años.

Durante este estudio se evidenciaron Payloads para al menos 12 tipos diferentes de arquitecturas de CPU haciendo una entrega dinámica de acuerdo a la configuración de la víctima [17]:

ARQUITECTURA	DESCRIPCIÓN
arm	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
arm5	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
arm6	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
arm7	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
mpsl	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
mips	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
i586	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically, linked, stripped
x86	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
spc	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
m68k	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
ppc	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (GNU/Linux), statically linked, stripped
arc	Se desconoce aún.
sh4	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
rce	Se desconoce aún.

Tabla 2. Arquitecturas compiladas para

Su funcionalidad es muy parecida al Qbot y a Mirai ya que intenta ocultarse cambiando su nombre a "/ bin / busybox" e intenta bifurcarse varias veces en el host de la víctima pero asegurando que una sola instancia del programa se ejecute en el dispositivo, esto lo hace normalmente mediante el puerto 7630 enviando un registro con su propio protocolo al servidor “Command and Control”, el cual es un servidor u ordenador de comando y control que se utiliza para recibir comandos e instrucciones y recuperar datos de forma remota, evitando el rastreo y la detección a los ciberdelincuentes [18]. Este registro se realiza con un mensaje el cual contiene en sus parámetros el vector de infección, la arquitectura de la CPU y los puertos utilizados por los módulos, dichos módulos conocidos como scanner, killer y proxy se ejecutan en procesos separados mientras que el proceso principal se enfoca en la comunicación con el servidor “Command and Control”, esperando una señal para realizar alguna acción por parte del atacante como por ejemplo un ataque tipo DDOS mediante los protocolos UDP, TCP o HTTP.

Ahora bien para su propagación "dark_nexus" utiliza dos módulos, uno síncrono y el otro asíncrono, ambos módulos utilizan fuerza bruta mediante el protocolo Telnet y una vez descubiertas las credenciales de la nueva víctima este informa al servidor “Command and Control” empezando nuevamente el ciclo de inflexión, a continuación se relacionan las credenciales más utilizadas por el malware [17]:

("admin","zhone")
("root","cxlinux")
("root","ahetzip8")
("root","dreambox")
("admin","QwestM0dem")
("e8telnet","e8telnet")
("admin","adminHW")
("root","hdipc%No")
("root","ipc71a")
("hacktheworld1337","hacktheworld1337")
("root","hipc3518")
("telnetadmin","hacktheworld1337")
("root","059AnkJ")
("admin","samsung")
("root","tiesseadm")
("root","linuxshell")
("root","xc3511")
("root","1234")
("root","ipcam_rt5350")
("root","iDirect")
("root","twe8ehome")
("root","xmhdipc")
("root","cat1029")
("root","IPCam@sw")
("root","hslwificam")
("root","fxjvt1805")
("root","taZz@23495859")
("telecomadmin","admintelecom")
("default","1")
("default","default")
("default","OxhlwSG8")
("default","S2fGqNFs")
("root","vizxv")
("telnetadmin","telnetadmin")
("user","user"_
("root","svgodie")
("root","colorkey")
("root","solokey")
("root","telecomadmin")
("root","zlxx.")
("daemon","daemon")
("support","support")
("admin","4321")
("root","5up")
("root","7ujMko0vizxv")
("root","7ujMko0admin")
("root","admin")
("adm","")
("guest","guest")
("root","tsgoingon")

Imagen 5. Credenciales más utilizadas para ataques de fuerza bruta.

5.2 Kaiji IoT Botnet

A finales de abril de 2020, investigadores de intezer.com identificaron una nueva botnet de origen totalmente chino, la cual está dirigida 100% a dispositivos IoT y se propaga a través de fuerza bruta mediante el protocolo SSH, una vez más y como de costumbre para las nuevas botnets que se despliegan a día de hoy, esta reutiliza el código de la famosa Mirai pero implementa nuevas funcionalidades hechas desde cero en lenguaje Golang [19].

De acuerdo a los investigadores se le nombro Kaiji por el nombre de una de las funciones encontradas en su código, además de su principal característica que es exigir acceso de “root” al momento de la infección ya que requiere estos privilegios para realizar ataques de tipo DDOS.
En su fase de infección, una vez obtenidas las credenciales de SSH realiza la creación del directorio “/usr/bin/lib” y se instala con el nombre de “netstat”, “ls”,”ps” o algún nombre de herramienta del sistema operativo Linux para evitar ser detectado, así como la creación de una copia en el directorio “/tmp/seeintlog” para su persistencia, seguido de esto procede a ejecutar las funciones “doLink”,“doTask” y “Rotkit” las cuales en muchos casos están cifradas u ofuscadas en Base64.

La función “doLink” contiene los nombres de los servidores donde se registra el malware, la función “doTask” permite recibir comando externos para ejecutar ataques DDOS, instrucciones de fuerza bruta, eliminarse o ejecutar algún comando en la Shell y por último la función “Rotkit” permite realizar conexiones a los host conocidos mediante claves SSH RSA o a IPs que se encuentren en el historial del dispositivo.

Para esta investigación es importante destacar que esta botnet fue escrita prácticamente desde cero, aunque con la inspiración de Mirai, lo que resulta muy interesante debido a que normalmente este tipo de malware se adquiere en foros sobre la deep web o proyectos de código abierto publicados, sin embargo no es más que una vulgar operación de DDOS [20].

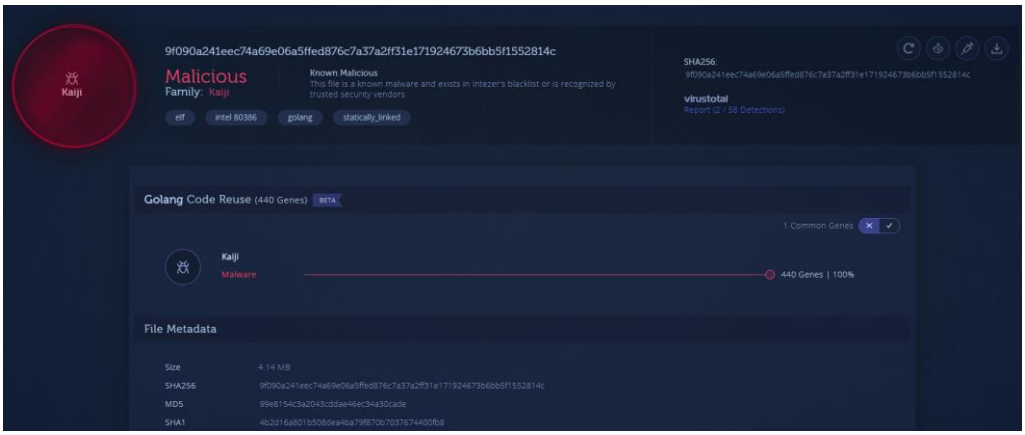

Imagen 6. Evaluación de virus realizado con analyze.intezer [21].

6. Análisis de Malware a Nivel Mundial.

El análisis de malware es una tarea ardua y compleja la cual busca comprender, identificar y determinar cuáles son las acciones que un código malicioso realiza, con el propósito de comprender las amenazas a las cuales se está expuesto al conectar un dispositivo a internet, esto se hace valiéndose de metodologías, técnicas y herramientas específicas para esta labor ya que cada día se implementan nuevas estrategias para evitar su detección, valiéndose de técnicas de ocultamiento como el cifrado, el ofuscamiento o el enmascaramiento con el único propósito de perdurar el mayor tiempo posible y generar una rentabilidad a los ciberdelincuentes [22].

De acuerdo los últimos estudios realizados podemos identificar que a 31 de mayo de 2020 existe un crecimiento exponencial del malware que se despliega para dispositivos IoT siendo India, China y Vietnam los países con mayor número de dispositivos infectados como se evidencia en la siguiente tabla el top 10 de países infectados [23]:

Top	País	Número de Bots
1	India	1.721.728
2	China	1.375.309
3	Vietnam	963.978
4	Irán (República Islámica de)	759.781
5	Brasil	544.590
6	Tailandia	479.365
7	Estados Unidos de América	335.126
8	Indonesia	325.942
9	Argelia	299.280
10	Federación Rusa	250.322

Tabla 3. Top 10 dispositivos infectados a nivel mundial.

A continuación se presenta esta información en un mapa de calor geográfico:

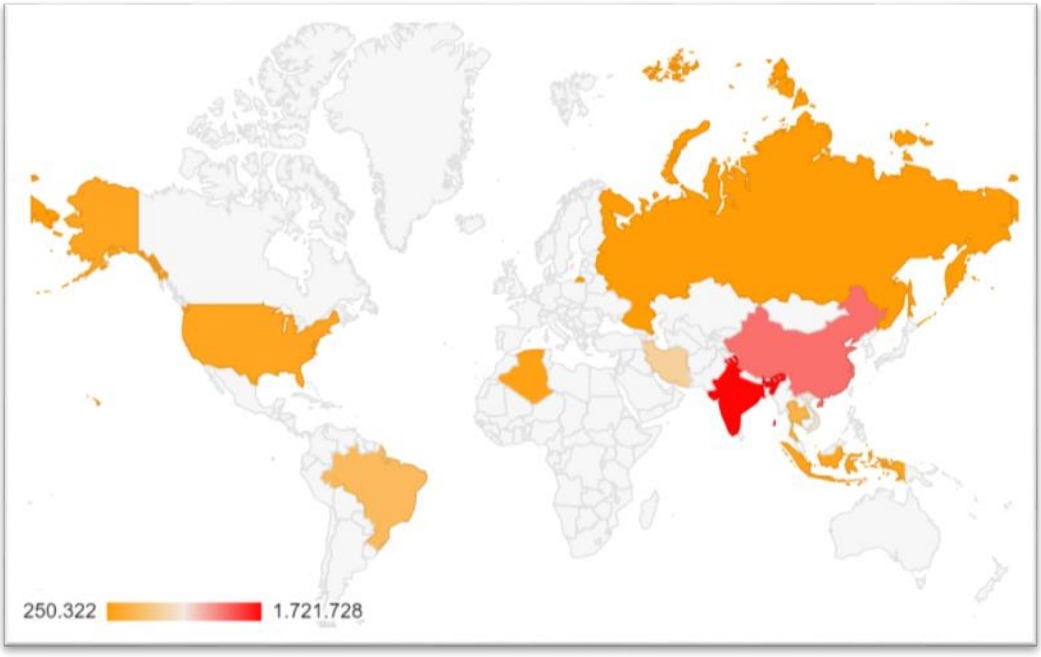

Imagen 7. Mapa de calor de países con dispositivos infectados a nivel mundial.

Asimismo, de acuerdo al último análisis de malware reportado por Kaspersky, para el primer cuartil de 2020 se evidencia una distribución a nivel mundial, donde el 18.9% del origen de los ataques evaluados corresponden a de fuerza bruta mediante el protocolo SSH y un 81,1% para el protocolo Telnet respectivamente [24]. A continuación se relaciona en las tablas el top 10 de fuentes de ataques mediante el Protocolo Telnet y SSH:

Top	País	% de origen
1	China	13,04%
2	Egipto	11,65%
3	Brasil	11,33%
4	Vietnam	7,38%
5	Taiwán	6,18%
6	Rusia	4,38%
7	Corrí	3,96%
8	India	3,14%
9	Turquía	3,00%
10	Estados Unidos	2,57%

Tabla 4. Top 10 origen de ataques mediante el protocolo Telnet.

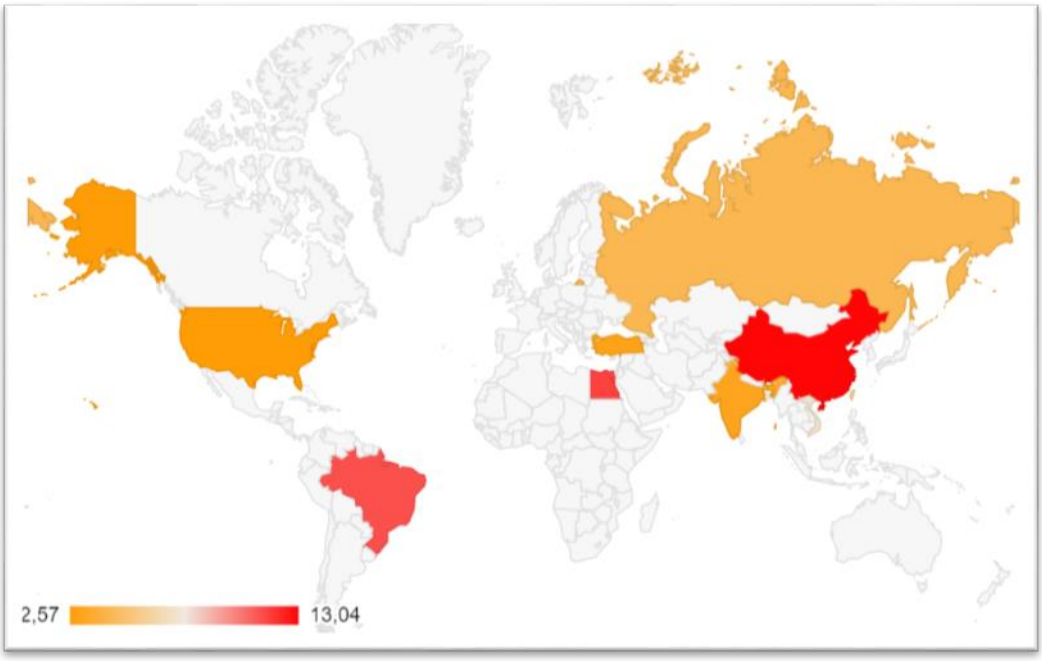

Imagen 8. Mapa de calor de origen de ataques mediante el protocolo Telnet.

Top	País	% de rigen
1	China	14,87%
2	Vietnam	11,58%
3	Estados Unidos	7,03%
4	Egipto	6,82%
5	Brasil	5,79%
6	Rusia	4,66%
7	India	4,16%
8	Alemania	3,64%
9	Tailandia	3,44%
10	Francia	2,83%

Tabla 5. Top 10 origen de ataques mediante el protocolo SSH.

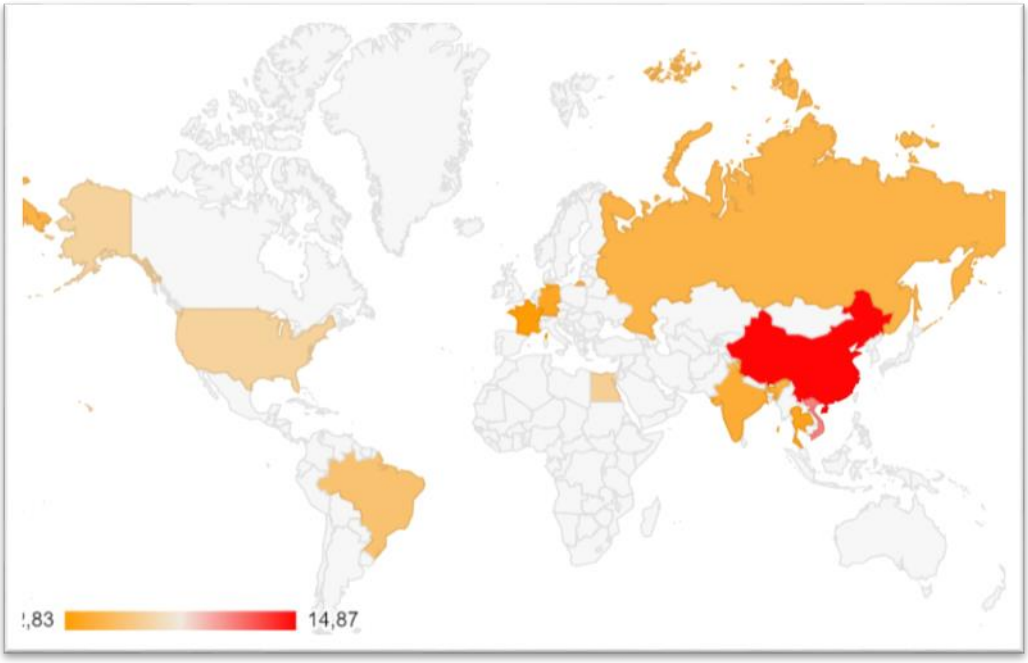

Imagen 9. Mapa de calor de origen de ataques mediante el protocolo SSH

Como se puede evidenciar en las anteriores imágenes, el origen de los ataques corresponde principalmente a China, Vietnam, Egipto y Estados Unidos donde respectivamente son los países que más dispositivos IoT que se encuentran desplegados

7. Antivirus Sobre IoT

Un antivirus es un software altamente especializado en detectar, corregir y destruir amenazas como virus, malware, ransomware, spyware entre otros [25], su principal función consiste en buscar patrones sobre una gran biblioteca de malware conocido que cumpla una serie de características o variantes para identificarlos. Hoy en día muchos antivirus detectan comportamientos, fragmentos de código y procesos en ejecución sospechosos que permitan identificar posibles amenazas no solo por un historial, sino por su conducta [26].

A continuación se relacionan las principales marcas de antivirus y sus características según el portal PC Magazine:

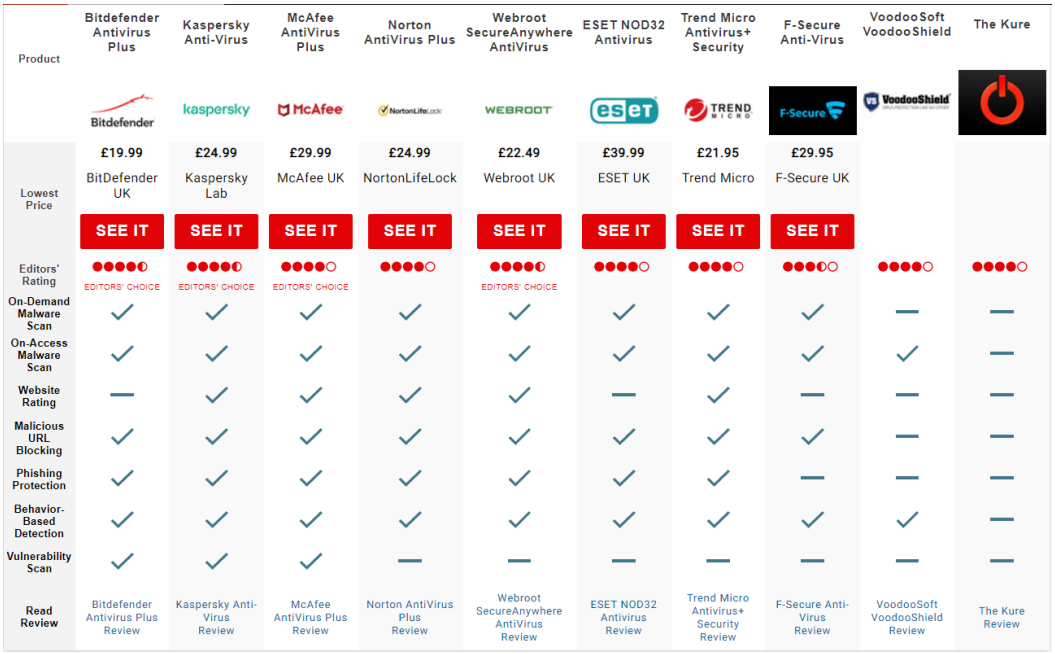

Imagen 10. Benchmark Antivirus.

Como se puede apreciar en la imagen anterior, las herramientas que cuenta con mayor número de servicios son Kaspersky, McAfee y BitDefender quienes soportan escaneos por demanda, protección contra phishing, escaneo de vulnerabilidades y detección de comportamiento respectivamente, por un precio que oscila entre las £20 a las £30 libras esterlinas [27].

Sin embargo, haciendo un sesgo netamente sobre los dispositivos IoT encontramos que empresas como BitDefender, Kaspersky, Symantec y F-Secure Sense proveen herramientas especializadas para este tipo de dispositivos [28] como se evidencian a continuación:

Imagen	Empresa	Nombre	Descripción
 **Imagen 11. Bitdefender BOX**	Bitdefender	Bitdefender BOX 2	Esta es una solución de seguridad de Internet que incorpora hardware, software y nube también. Asegura teléfonos inteligentes, televisores inteligentes y todos los demás electrodomésticos o dispositivos que están conectados a Internet [29] [28].
 **Imagen 12. Symantec Embedded Security**	Symantec	Symantec Embedded Security	Es un sistema que protege los sistemas operativos integrados como Linux, QNX y Windows Embedded OS, ademas de proveeer protección a todo tipo de dispositivos como smartphones, SmartTV, tables entre otros [28].
 **Imagen 13. Norton Core**	Symantec	Norton Core	Es un router inalámbrico más seguro, que ofrece protección y rendimiento, este ayuda a defender una red LAN WIFI contra malware, virus, ciberdelincuentes y otras amenazas cibernéticas [30].
 **Imagen 14. SENSE security Router**	F-Secure	SENSE security Router	Es un Router Wi-Fi que funciona como un dispositivo de seguridad para proteger simultáneamente cualquier número de dispositivos conectados a su red local [31].

Tabla 6. Soluciones Antivirus IOT.

8. Virtualización Anidada

La virtualización es el proceso de crear una representación física basada en software, es decir utilizar un software en lugar de un hardware de propósito, mediante un proceso de conversión de físico a virtual, esto se efectúa principalmente sobre servidores, appliance, redes, dispositivos de almacenamiento, entre otros y se considera a día de hoy como la forma más eficaz para reducir costos de infraestructura TI sobre una empresa.

8.1 Ventajas de la virtualización

Normalmente la virtualización permite mejorar la agilidad, flexibilidad y escalabilidad de una infraestructura empresarial o doméstica, así como reducción de costos de manera importante. Unas de las principales ventajas de la virtualización consiste en mejorar las cargas de trabajo de los servidores, el aumento del rendimiento y mejoras en la disponibilidad de los recursos, así como la automatización de diferentes tipos de procesos como el mantenimiento, mejorando significativamente la gestión de la empresa frente a su infraestructura TI, adicionalmente se consideran las siguientes ventajas y características [32]:

- Reducción de la inversión en capital y los costos operativos.
- Reducción o eliminación de tiempos de inactividad.
- Aumento de productividad, eficiencia, la agilidad por parte del departamento de TI de una empresa.
- Distribución más rápida de las aplicaciones y recursos.
- Mejora de la continuidad del negocio y de la capacidad de recuperación ante desastres.
- Gestión simplificada del centro de datos.

8.2 Virtualización Anidada

La virtualización anidada es una característica de la virtualización que permite ejecutar una máquina virtual dentro de otra máquina virtual [33], esto se debe a que los hipervisores, que son los programas de administración encargados de asignar recursos, realizan una asignación de manera especial para que estos puedan funcionar de manera correcta [34]. Con el propósito de optimizar aún más los recursos que se tienen.

9. Ambientes Sandbox

Un ambiente Sandbox es un tipo de entorno de prueba de software que permite la ejecución aislada del software para su evaluación, monitoreo o pruebas de manera independiente, su propósito es salvaguardar la integridad de un sistema embebiendo la ejecución de programas sobre una capa se software [35], esto se realiza frecuentemente sobre entornos virtuales con el fin de ejecutar todo sobre memoria y poder regresar a estados de configuración anteriores de un sistema operativo de forma rápida mediante la utilización de snapshots o instantáneas.

Para la realización de este proyecto se configuraron diferentes tipos de Sandbox con el fin de evidenciar el comportamiento de los códigos maliciosos que se desean evaluar, para el siguiente caso se realizó un proceso de virtualización anidada donde se virtualizan los sistemas operativos Android y Raspbian, sobre un hipervisor VMware Workstation 15, sobre un sistema operativo Windows 10 virtualizado, a su vez sobre otro hipervisor de VMware Workstation 15, que se encuentra instalado en un Windows 10, sobre una maquina física con el fin de crear el mayor aislamiento posible como se evidencia en la siguiente imagen:

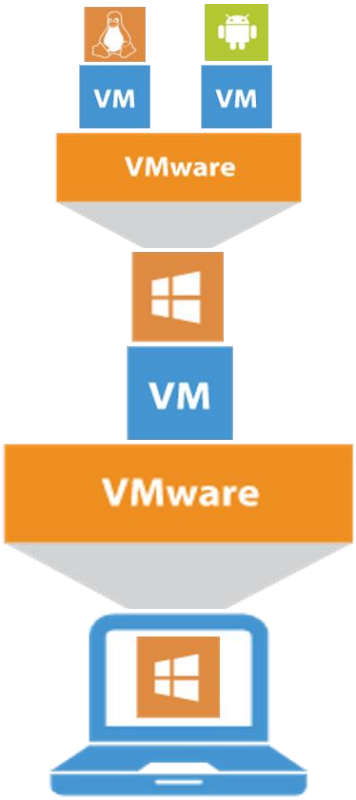

Imagen 15. Sandbox sobre virtualización anidada

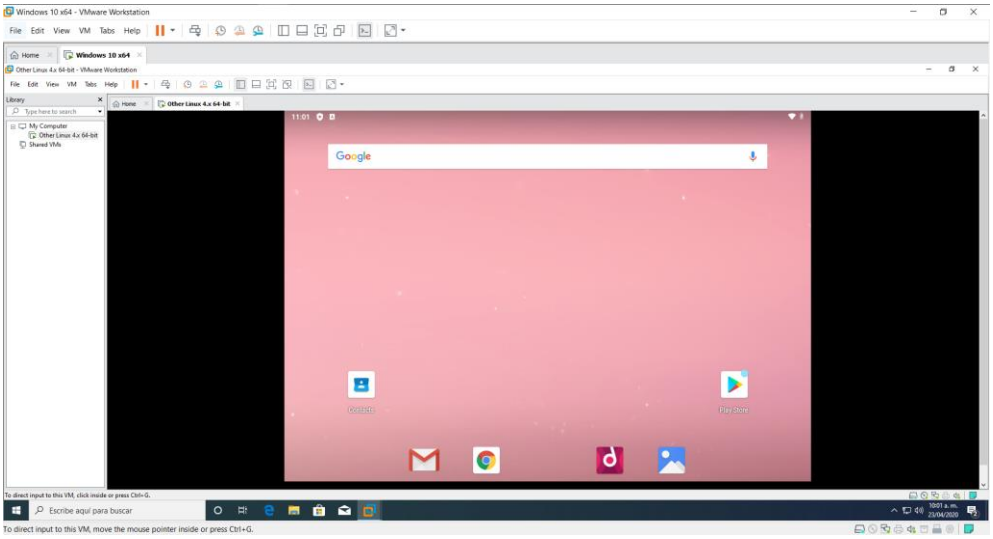

Imagen 16. Virtualización anidada para S.O. Android.

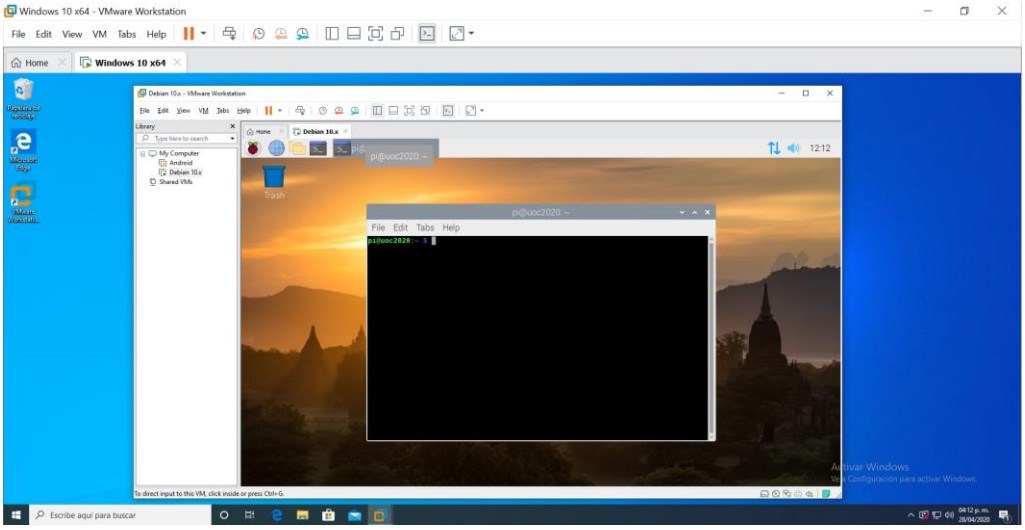

Imagen 17. Virtualización anidada para S.O. Raspbian.

10. Instalación de Antivirus Sobre el Dispositivo

10.1 Clamav Antivirus

Clam AntiVirus es software de antivirus de código abierto para Linux, el cual proporciona una serie de utilidades que incluyen un daemon multiproceso flexible y escalable, un escáner de línea de comandos y una herramienta avanzada para actualizaciones automáticas de bases de datos, sus principales características son [36]:

- Está diseñado para escanear archivos rápidamente.
- Realiza escaneos en tiempo real (solo Linux).
- Detecta más de 1 millón de virus, gusanos y troyanos, incluidos los virus de macro de Microsoft Office, malware móvil y otras amenazas.
- Las bases de datos de firmas, aseguran que solo ejecuta definiciones de firmas confiables.
- Escanea dentro de archivos comprimidos.
- Protege contra las bombas lógicas y de archivos.

10.2 Instalación de Clamav

La instalación de ClamAv se puede realizar de dos maneras mediante el instalador descargado de la página oficial o mediante el gestionador de paquetes APT:

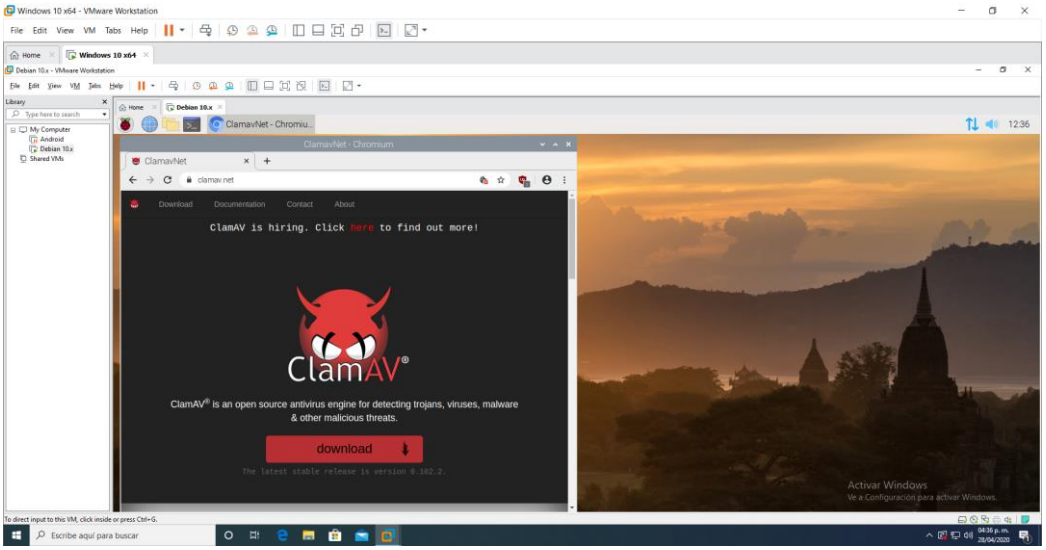

Imagen 18. Búsqueda de antivirus ClamAV.

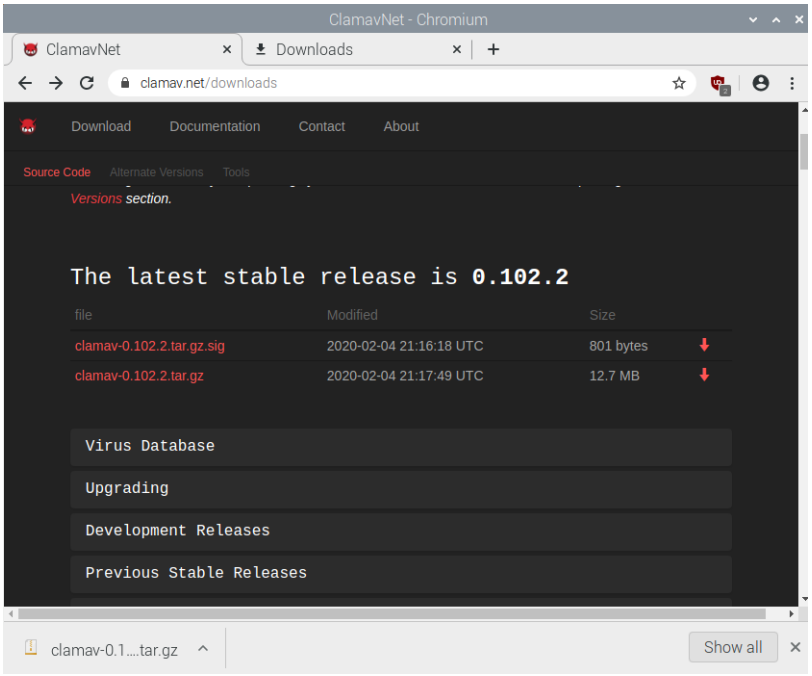

Imagen 19. Descarga del antivirus ClamAV.

Sin embargo para agilizar y optimizar la instalación realizamos la instalación con el comando apt-get el cual realiza esta tarea de manera mucho más sencilla:

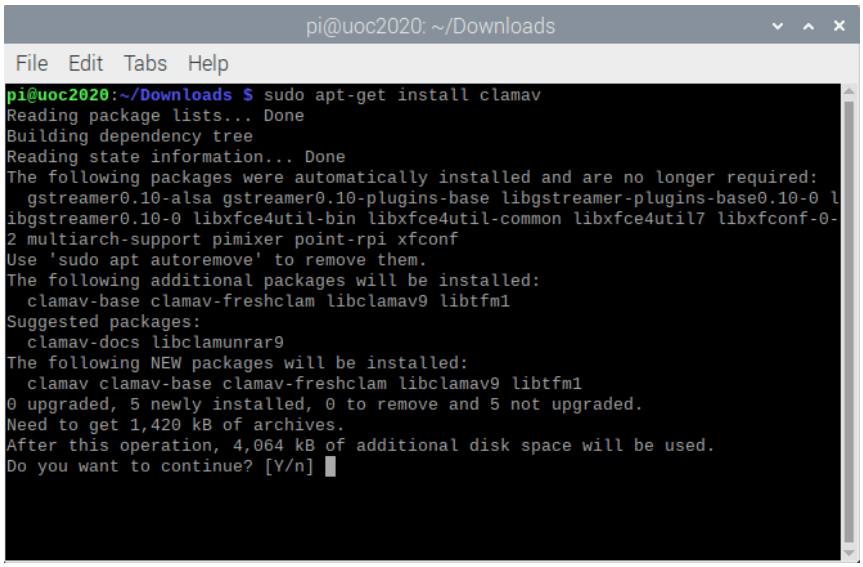

Imagen 20. Instalación de ClamAV.

Y por último se procede a realizar un escaneo sobre la raíz del sistema operativo:

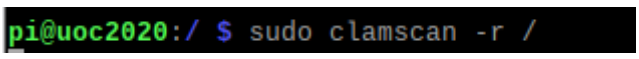

Imagen 21. Ejecución de escaneo sobre todo el dispositivo.

10.3 Comodo Antivirus

Comodo Free es un poderoso Antivirus que viene equipado con impresionantes funciones de seguridad, lo que según sus creadores lo convierten en el mejor software antivirus gratuito en la industria de seguridad de TI. Este software ayuda a proteger un dispositivo contra virus, troyanos, gusanos, spyware, backdoors, rootkits, adware y malware en general a continuación se relacionan las principales características del producto [37]:

- Enfoque de rechazo: Evita que todos los archivos ingresen al sistema de manera predeterminada hasta que se demuestren que son inofensivos.
- Contención: Permite contener o restringir los archivos y ejecutables en un entorno aislado, hasta que demuestren ser inofensivos, sin afectar la seguridad del dispositivo.
- HIPS: Capacidad para monitorear exhaustivamente el dispositivo y evitar la entrada de ataques maliciosos.

10.4 Instalación de Comodo

La instalación de Comodo antivirus se realiza descargando el instalador del sitio oficial según la versión del sistema operativo:

Imagen 22. Descarga Antivirus Comodo

Se ubica el instalador y se realiza la ejecución de este con el comando dpkg –i, con permisos de root como se evidencia a continuación:

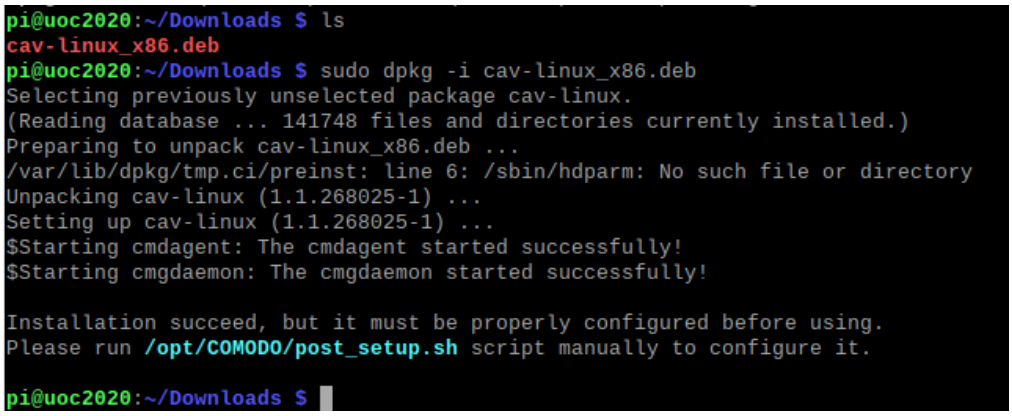

Imagen 23. Instalación de antivirus Comodo.

De acuerdo a la indicación se realiza la configuración del software:

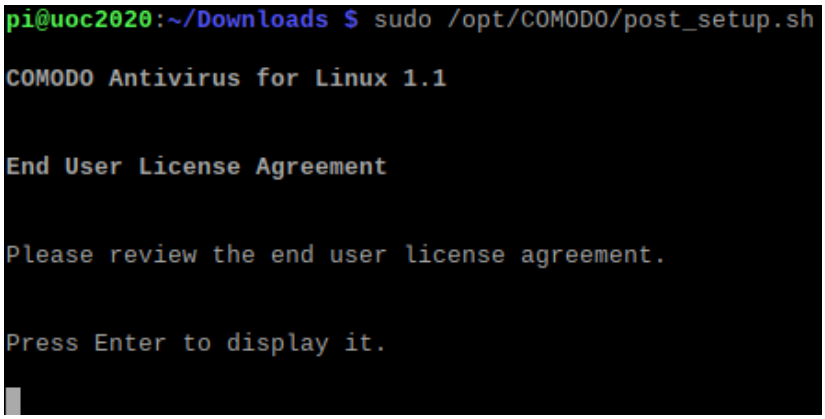

Imagen 24. Configuración de Comodo Software.

Ahora se realiza la presentación de los acuerdos de licencia del software que se está utilizando y se procede aceptar los términos después de la lectura:

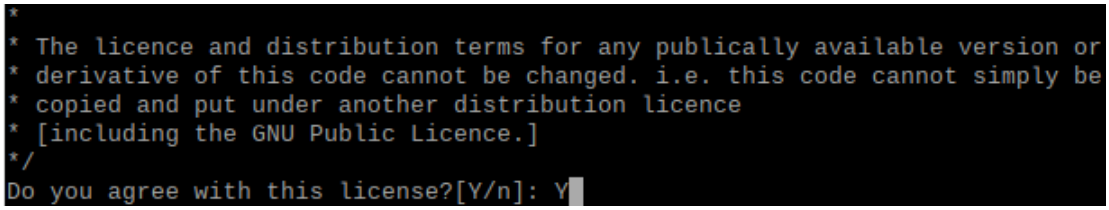

Imagen 25. Aceptación de términos del Antivirus.

Seguido de esto se procede a configurar el idioma de preferencia:

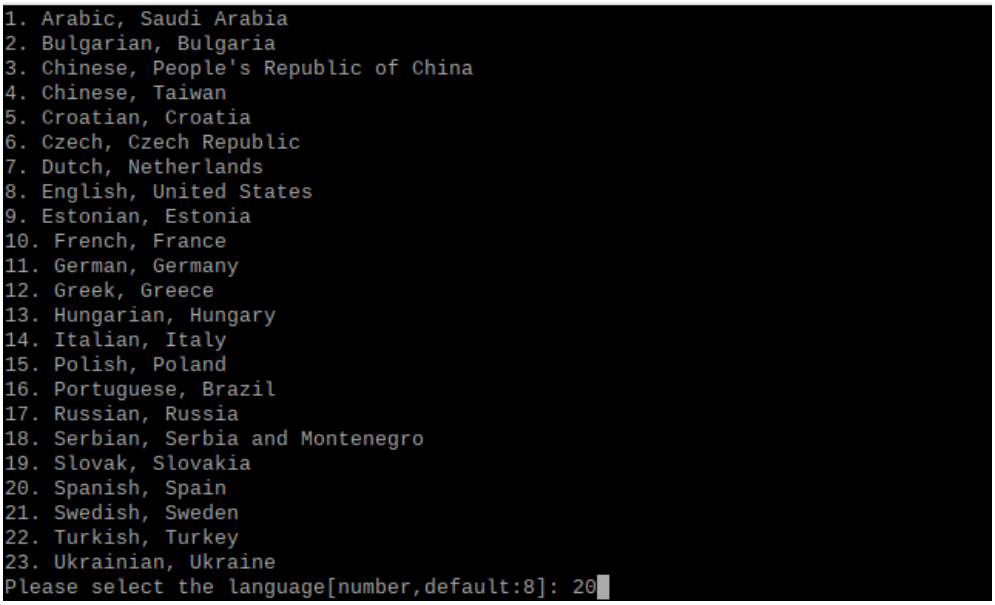

Imagen 26. Configuraciones de idioma.

Y se finaliza el proceso de instalación del antivirus sobre el dispositivo IoT con la siguiente imagen:

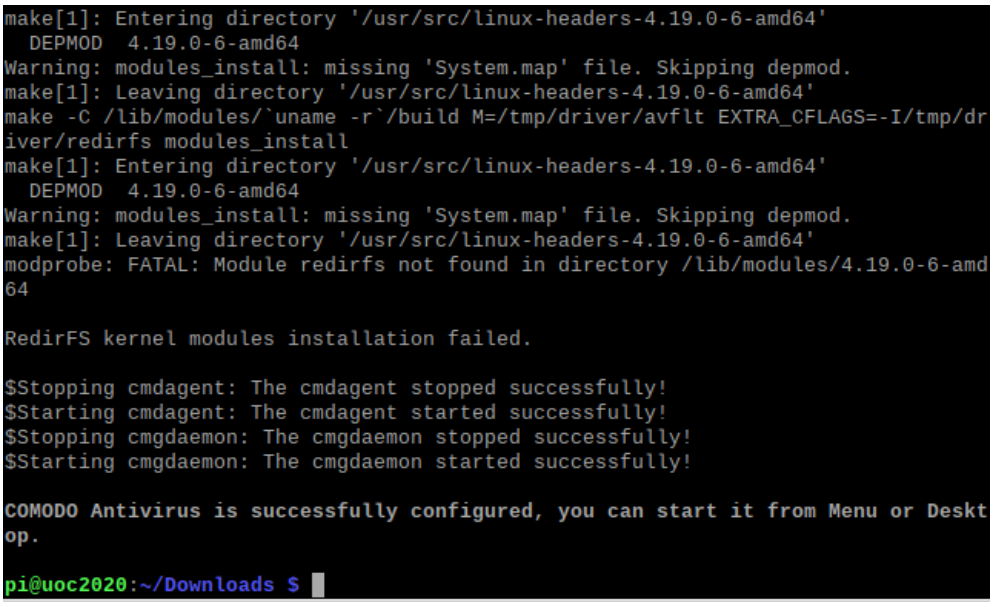

Imagen 27. Finalización de la instalación.

Una vez finalizado el proceso de instalación se procede a ejecutar el programa para realizar las pruebas pertinentes:

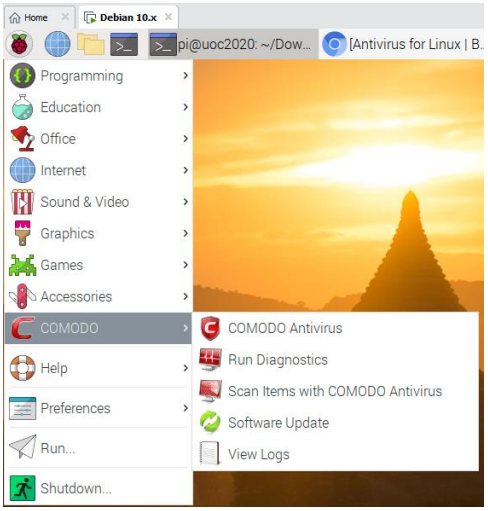

Imagen 28. Ejecución de antivirus Comodo.

Seguido de esto se abre la consola del software y se procede a configurar el escaneo que se desea y la actualización de la base de datos:

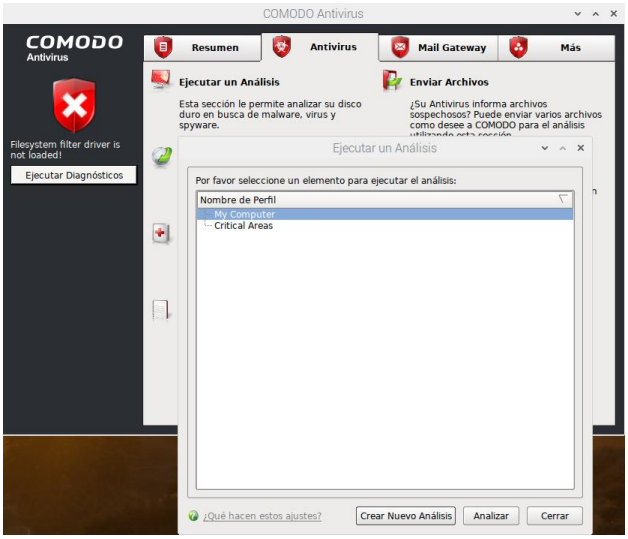

Imagen 29. Configuración de Escaneo.

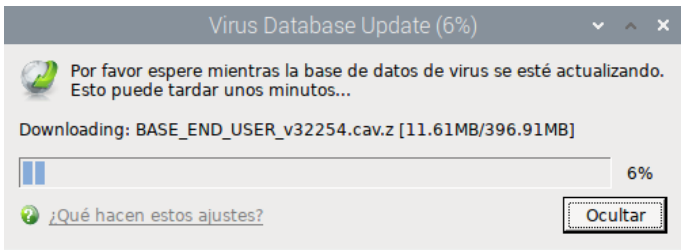

Imagen 30. Actualización de Base de Datos.

11. Creación de Antivirus Lite en Python

Continuando con el proceso de investigación y con el único propósito de mejorar los tiempos de escaneo frente a las amenazas más recurrentes sobre dispositivos IoT, se realiza la creación de un Script en Python que permita realizar el trabajo de un antivirus pero de forma más ligera debido a que los dispositivos IoT por lo general cuentan con un procesamiento limitado y ajustado a su propósito de despliegue, el cual se demuestra un fragmento en la siguiente imagen:

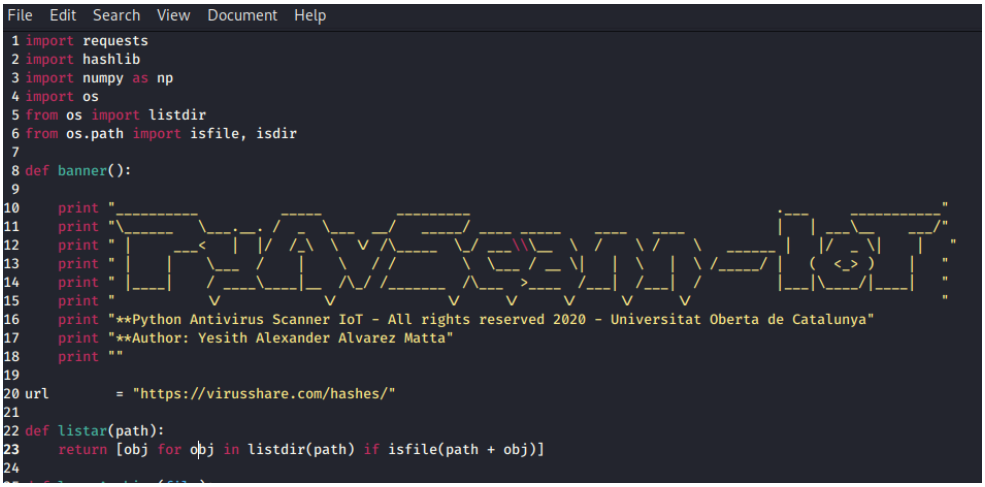

Imagen 31. Ejemplo de código creado.

Imagen 32. Ejemplo de firmas obtenidas.

Para la obtención de firmas se realiza la búsqueda y se identifica el portal web virusshare.com el cual tiene más de 34.000 registros de firmas de virus en hash md5, la cual nos es de mucha utilidad para la prueba de concepto [38].

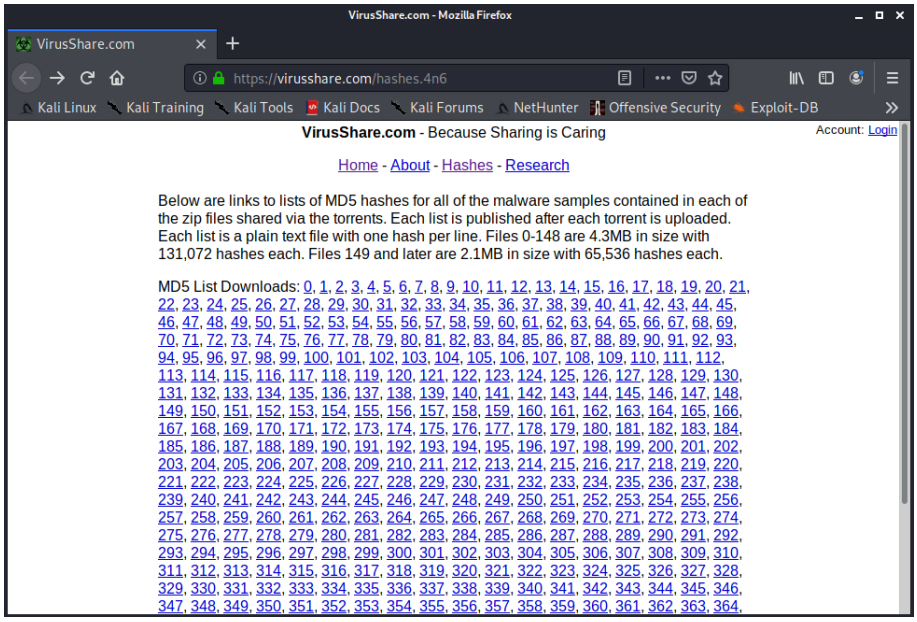

Imagen 33. Hashes disponibles.

11.1 Instalación de PyAvScan-IoT

La instalación de este antivirus se realiza descargando el código del repositorio creado en github [39], como se evidencia a continuación:

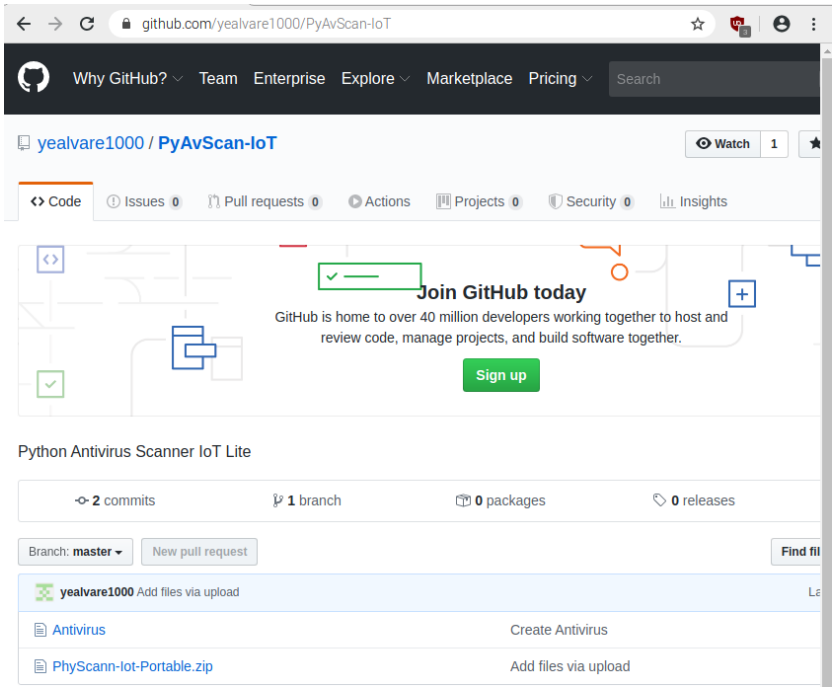

Imagen 34. Repositorio de código.

Luego se procede a realizar la descompresión sobre la ruta deseada con el comando unzip como se evidencia en la siguiente imagen:

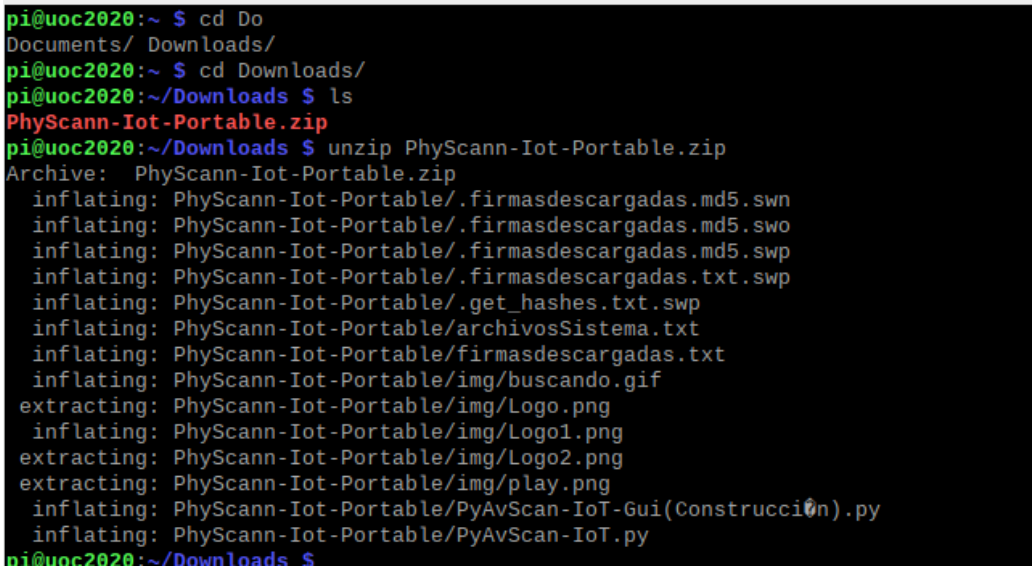

Imagen 35. Descompresión de Archivos.

Y por último para su ejecución se realiza con los permisos de sudo, con el fin de evitar problemas de lectura al momento de comparar las firmas:

Imagen 36. Ejecución de PyAvScan-IoT.

Como se evidencia en la siguiente imagen el antivirus realizara una comparación de firmas sobre cada uno de los archivos del sistema operativo con el fin de detectar algún archivo malicioso

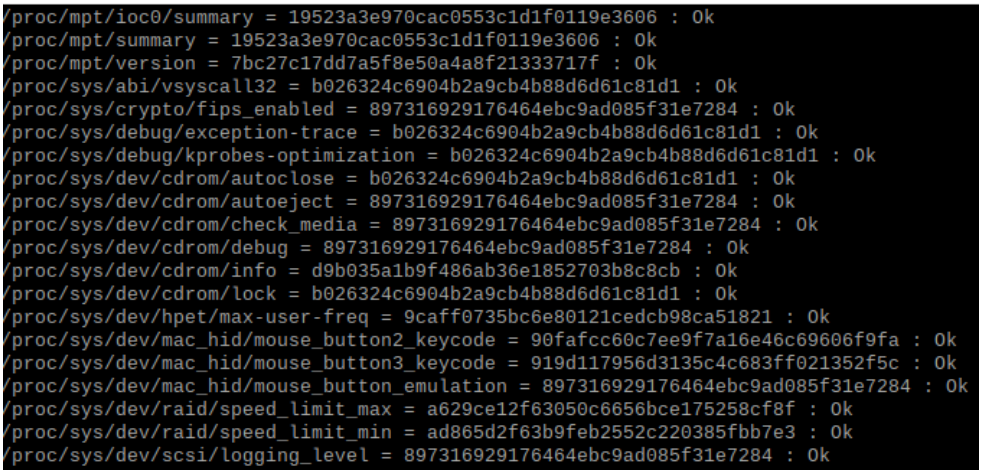

Imagen 37. Detección de firmas con PyAVScan-IoT.

12. Análisis Estático, Pruebas de Escaneo y Detección de Virus Sobre el Dispositivo

Para la realización de las pruebas de escaneo y detección de malware se tuvo en cuenta la detección de malware en diferentes formatos, así como el consumo de recursos y la eficiencia sobre cada uno de los antivirus probados:

12.1 Pruebas Clamav Antivirus

Se realiza diferentes tipos de escaneos desde un directorio en particular hasta un escaneo total de los archivos del Sistema Operativo, con el propósito de medir tiempos de escaneo promedio con Clamav.

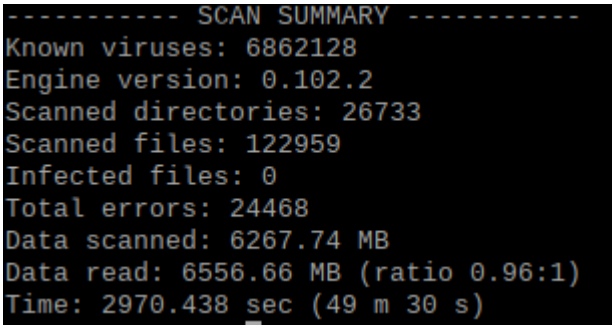

Imagen 38. Escaneo total del sistema operativo con ClamAV.

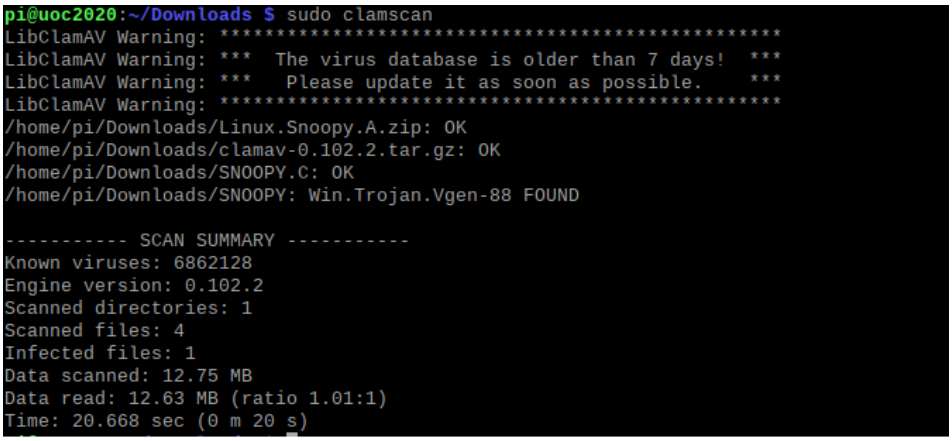

Imagen 39. Detección de virus.

Adicionalmente se toman el porcentaje de consumo de CPU:

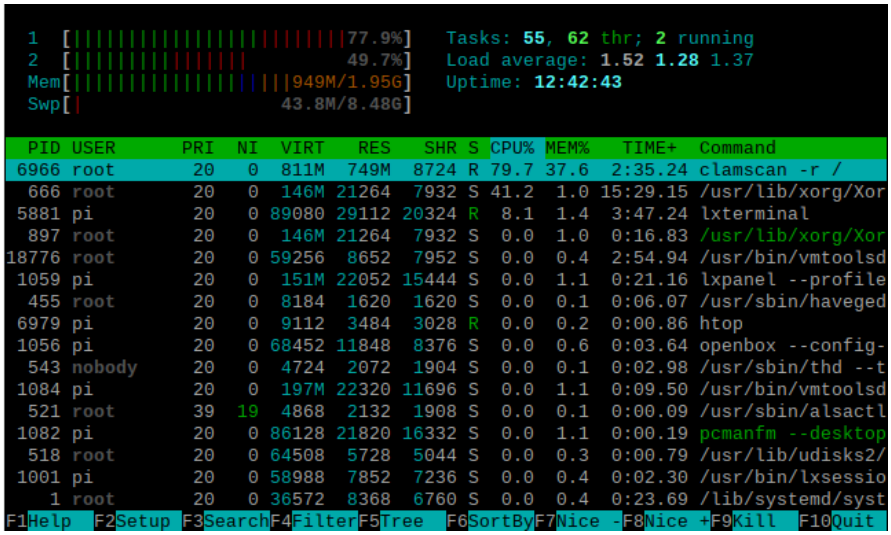

Imagen 40. Consumo de recursos con ClamAV.

12.2 Pruebas Comodo Antivirus

De la misma manera se realiza diferentes tipos de pruebas con el propósito de medir tiempos de escaneo promedio con Comodo.

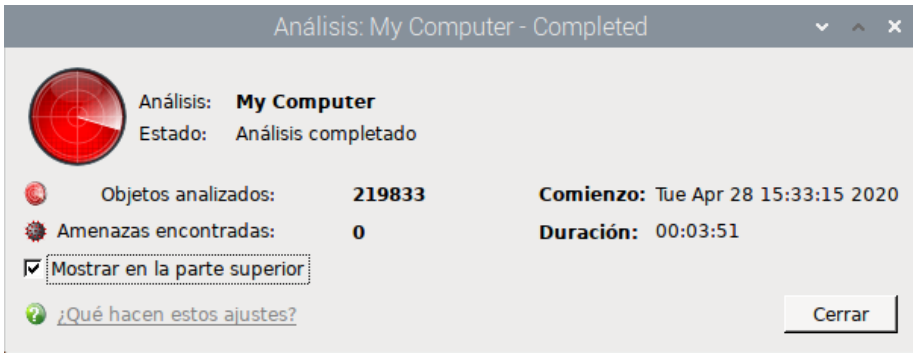

Imagen 41. Escaneo total del sistema operativo con Comodo.

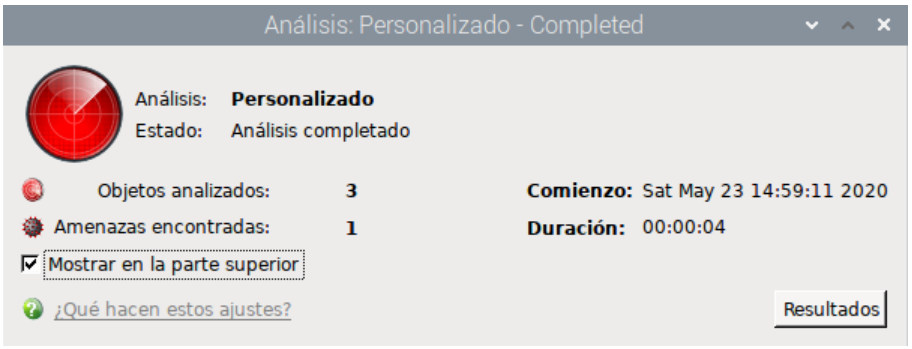

Imagen 42. Detección de virus.

Se toma, el porcentaje de consumo de CPU en varias oportunidades con el fin de obtener un promedio del consumo:

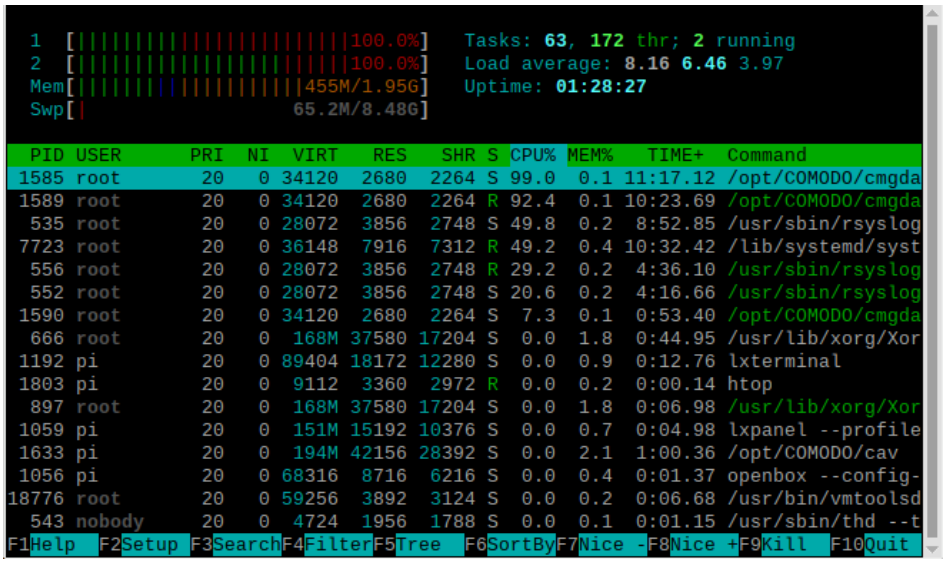

Imagen 43. Consumo de recursos con Comodo.

12.3 Pruebas con PyAvScac-IoT.py

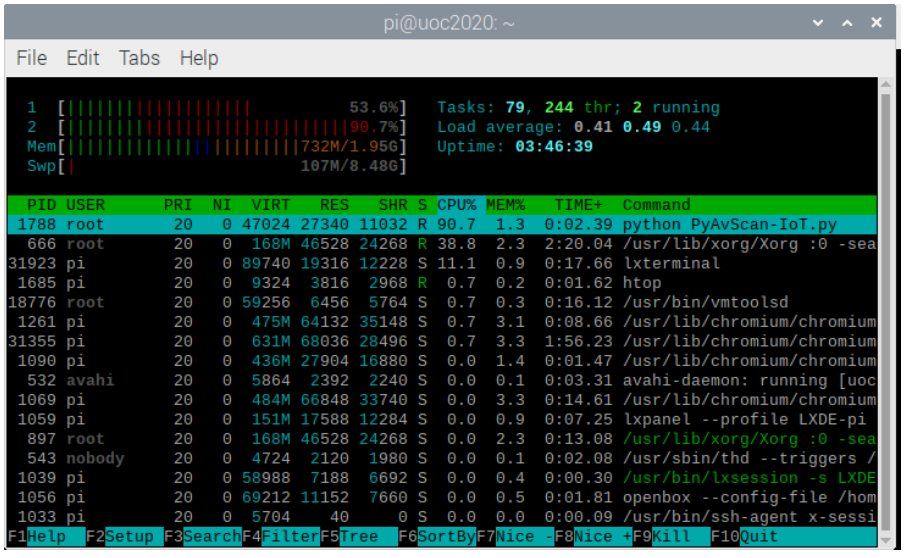

Imagen 44. Consumo de recursos con PyAvScac-IoT.py.

12.4 Resultados de las pruebas realizadas

Para la realización de esta prueba se utilizó el escaneo total de los archivos del sistema operativo y de acuerdo a los datos obtenidos plasmados en la siguiente gráfica, cada uno de los antivirus evaluados tiene sus pros y contras, ya que para el caso de Comodo el tiempo promedio de escaneos fue de 18 minutos pero el consumo de procesador estuvo en 100%, por otro lado ClamAv se mantuvo en un promedio de 77% en el consumo de procesador pero sus tiempos se duplicaron con respecto a Comodo, sin embargo para el caso del script en Python el consumo de procesador se mantuvo en un promedio de 61% pero los tiempos de escaneos se evidenciaron en 60 minutos aproximadamente.

Comodo		ClamAv		PyAvScac-IoT	
% CPU	Tiempo	% CPU	Tiempo	% CPU	Tiempo
100%	15 min	77%	49 min	65%	65 min
100%	30 min	72%	20 min	56%	45 min
100%	14 min	82%	26 min	71%	39 min
100%	13 min	75%	25 min	63%	89 min
100%	18 min	77%	30 min	61%	59,5 min

Tabla 7. Comparación de porcentaje vs Tiempo.

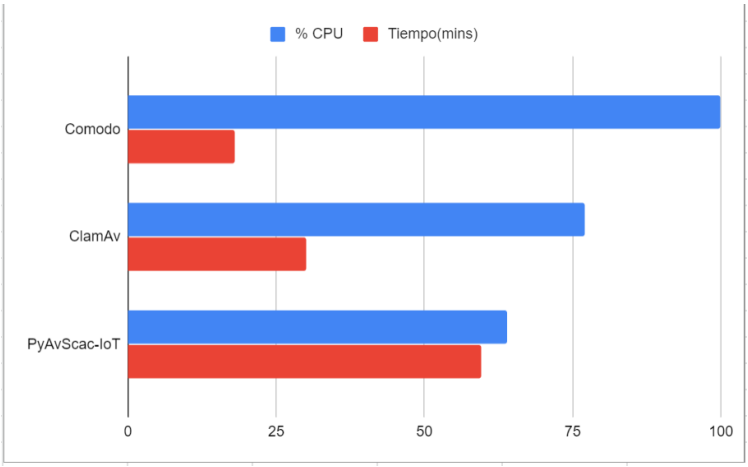

Imagen 45. Consumo de recursos vs tiempo Utilizado.

12.5 Conclusión a los resultados obtenidos

Los dispositivos IoT son generalmente microcomputadores que no presentan una capacidad de computo grande en comparación a un Ordenador de escritorio de hoy, por esta razón al momento de elegir un sistema de antivirus es muy importante saber la capacidad de computo que se tiene ya que esta puede ser afectada drásticamente por alguna solución, es decir si contamos

con un dispositivo con gran capacidad de computo respecto al promedio del mercado podemos optar por implementar un antivirus para ayudar a mitigar los riesgos a los que se expone, sin embargo si se disponen de dispositivos con muy poca capacidad, en mejor aplicar un correcto aseguramiento y velar por tener las últimas actualizaciones del sistema, esto con el fin de prestar un buen servicio al usuario final, evitar degradaciones de uso y poner una barrera importante frente a amenazas como botnets.

13. Adquisición del Dispositivo

Dentro de los requisitos evaluados para la selección del dispositivo IoT, se tuvo en consideración el costo y la cantidad de dispositivos desplegados en internet, por esta razón se acude a Shodan.io, uno de los buscadores de información de hosts más grandes de internet, este identifica alrededor de 194,257 dispositivos Raspberry el cual se eligió para este Trabajo [40]:

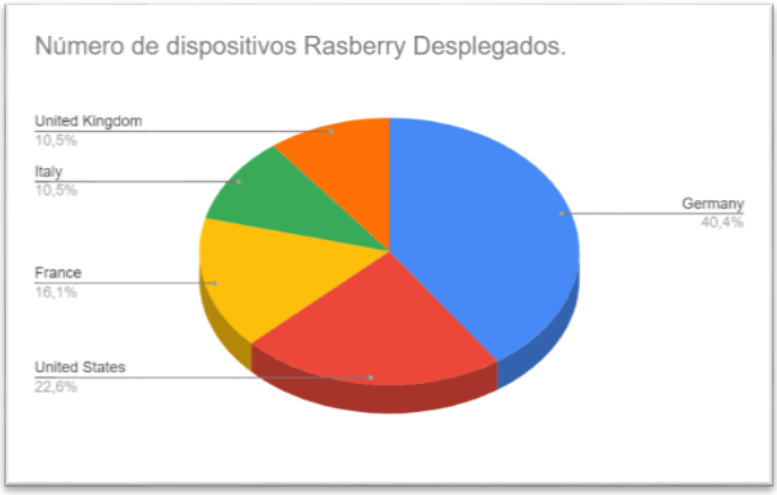

Imagen 46. Top países con dispositivos Raspberry desplegados.

Para la adquisición del dispositivo se realiza la compra de una Raspberry Pi 3 modelo B por un costo aproximado a los 40 USD, esta es una pequeña una placa de computadora de tamaño reducido desarrollado en el Reino Unido por la Fundación Raspberry PI (Universidad de Cambridge) que se utiliza actualmente tanto para el ámbito académico como el productivo, debido a su alto número de proyectos digitales, desde máquinas de música hasta estaciones meteorológicas [41].

A continuación se relaciona la imagen del dispositivo adquirido:

Imagen 47. Dispositivo adquirido para pruebas.

Caracteristicas del dispositivo:

Característica	Descripción
Procesador	Broadcom BCM2387 chipset. 1.2GHz Quad-Core ARM Cortex-A53 (64Bit)
GPU	Dual Core Video Core IV® Multimedia Co-Processor. Provides Open GL ES 2.0, hardware-accelerated Open VG, and 1080p30 H.264 high-profile decode. Capable of 1Gpixel/s, 1.5Gtexel/s or 24GFLOPs with texture filtering and DMA infrastructure
Memoria RAM	1GB LPDDR2
Almacenamiento	Push/pull Micro SDIO Micro SD 16 GB Clase 10.
Poder	Micro USB socket 5V1, 2.5A
Ethernet	10/100 BaseT Ethernet socket
Salida de Video	HDMI (rev 1.3 & 1.4) Composite RCA (PAL and NTSC)
Salida	Audio Output 3.5mm jack HDMI USB 4 x USB 2.0 Connector
Radio Frecuencia	IEEE 802.11 b / g / n Wi-Fi. Protocol: WEP, WPA WPA2, algorithms AES-CCMP (maximum key length of 256 bits), the maximum range of 100 meters. IEEE 802.15 Bluetooth, symmetric encryption algorithm Advanced Encryption Standard (AES) with 128-bit key, the maximum range of 50 meters.

Tabla 5. Características del Dispositivo de pruebas.

14. Configuración del Dispositivo

En la configuración del dispositivo se realiza la descarga del sistema operativo Raspbian en su última versión de Kernel 4.19, la cual está diseñada específicamente para este dispositivo, este software está basado en Linux debían y viene con una interfaz gráfica muy amigable para el usuario [42].

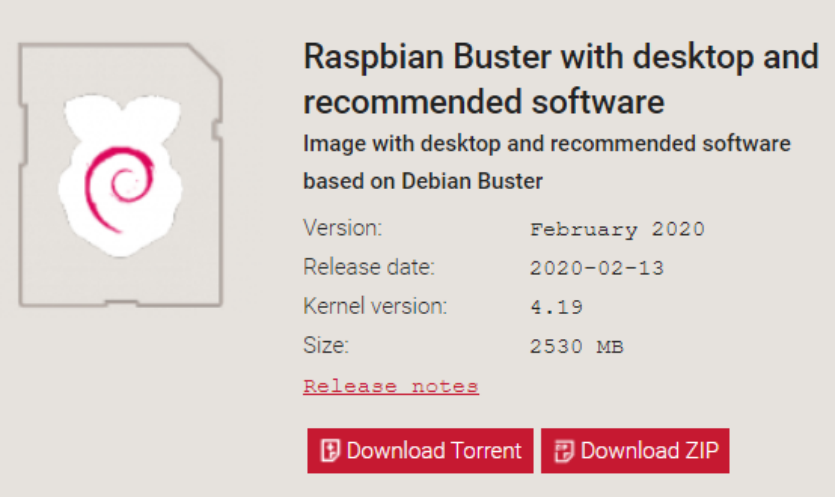

Imagen 48. Descarga de Raspbian.

Se realiza la creación de la imagen sobre la tarjeta Micro SD adquirida para poder correr el sistema operativo Raspbian, para esto se utiliza el software Rufus 3.9.1624 (Open Source) el cual permite crear la imagen desde el archivo .ZIP comprimido [43]:

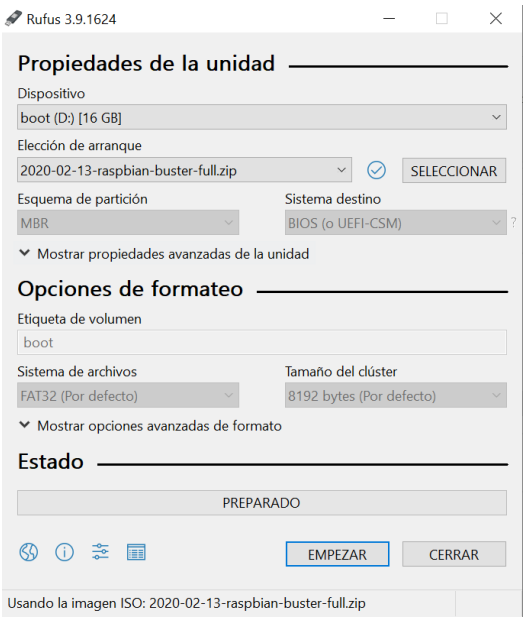

Imagen 49. Creación de imagen.

Ahora se procede a ejecutar el sistema operativo desde el dispositivo:

Imagen 50. Ejecución del sistema operativo.

Y se realiza el cambio de contraseña por defecto:

Usuario: Pi
Password: piuoc2020

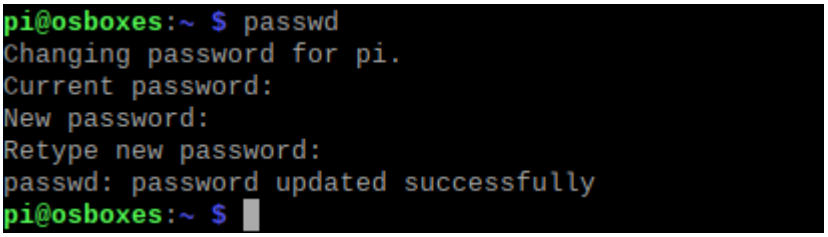

Imagen 51. Cambio de contraseña sobre el usuario PI.

15. Aseguramiento Dispositivo IoT

El Aseguramiento, Hardening o Endurecimiento de un sistema informático consiste en reducir, minimizar, limitar y evitar las amenazas o los peligros que se pueden presentar sobre dicho sistema, esto se consigue, estableciendo unas medidas específicas de seguridad con el objetivo de estar preparados ante un ataque informático.
Esencialmente consiste en cerrar todos los puertos que no van a ser utilizados o no son necesarios para el correcto funcionamiento del sistema, así como la eliminación del software y configuraciones adicionales que no se requieren, la idea general es que cada sistema debe cumplir con única función, de manera que los sistemas que cumplen con varias funciones deben limitarse a la prestación de un solo servicio sobre la red [44].

A continuación se relacionan las principales actividades durante un proceso de Hardening en un sistema informático:

- Actualización del sistema operativo a la última versión posible, con el fin de obtener los parches de seguridad y remediaciones de fallas anteriores sobre el sistema.
- Cambio de todas las claves por defecto de fábrica.
- Desinstalación de todo el software que sea innecesario.
- Depuración de todos los usuarios que no se requieren.
- Depuración de todos los servicios que no se requieren.
- Cierre de todos los puertos que no son estrictamente necesarios.
- Backup constantes como respaldo de datos que se consideren importantes.
- Activación y configuración de firewall.
- Ahora bien con el fin de brindar las herramientas necesarias para asegurar un dispositivo IoT, se realiza la creación de la guía completa de aseguramiento como entregable, basado en los estándares internacionales CIS [45] y las mejores prácticas publicadas por parte del fabricante del dispositivo que se toma como modelo, una Raspberry Pi 3 modelo B [46].

Anexo 1: TFM-GuiaAseguramiento-IoT-Raspbian.pdf

16. Conclusiones

Durante cada una de las fases del proyecto y con toda la información recolectada, se ha evidenciado la magnitud y el impacto que tiene la tecnología IoT en cada una de las áreas donde están siendo implementadas, así como los riesgos que implica desplegar un dispositivo de manera inadecuada en internet. En efecto todos estos peligros llevan a concentrar focos de infección de malware de varios tipos, desde Ransomware, Spyware, hasta Cryptomining, haciéndolos cada vez mucho más lucrativos, sofisticados y eficientes para los ciberdelincuentes.

De igual manera, se ha podido identificar las principales causas por las cuales los dispositivos IoT se han convertido en el huésped perfecto para el malware, en especial para las botnets, ya que su propagación obedecen a las malas prácticas tanto por parte del usuario final como del fabricante, siendo las contraseñas por defecto y la falta de actualizaciones constantes de firmware y software las principales causas de acceso no autorizado a estos dispositivos, haciendo que las amenazas continúen evolucionando y dirigiéndose a estos dispositivos con mayor fuerza, ya sea incluyendo nuevas técnicas para evitar ser detectados o contemplando métodos mucho más lucrativos como el minado de criptomonedas.

Por otro lado, en la fase de investigación de botnets actuales para este año 2020, es interesante ver cómo están siendo creadas desde cero a diferencia de muchas otras del pasado, donde se acudía a foros de mercado negro y proyectos de código abierto para su implementación, lo que hacía mucho más fácil su detección, debido a que las firmas de antivirus y los comportamientos eran prácticamente idénticos obligándolos a probar nuevos métodos de infección y propagación para alcanzar un mayor éxito.

A pesar de todo y aunque las amenazas en la red continúen, el panorama es alentador, ya que cada día crece el número de mecanismos y medidas para detectar estas actividades malintencionadas, así como la concientización por parte de los usuarios finales quienes compran e implementan estas plataformas para mejorar su calidad de vida y de las empresas de seguridad, quienes empiezan a prestar su atención a este problema ofreciendo hosts especializados para la protección del hogar y de las empresas.

Finalmente, el propósito de este trabajo es ayudar a mitigar el problema actual de los dispositivos IoT no asegurados, por tal motivo se hace una llamada de atención a los fabricantes para que implementen nuevas y mejores medidas de control, como por ejemplo obligar al usuario a cambiar la contraseña por defecto del dispositivo una vez este sea iniciado y para el usuario final, quien debe utilizar la tecnología de manera responsable, teniendo en cuenta una balanza entre la seguridad y el servicio prestado, por esta razón se enumeran las siguientes características a la hora de tener en mente la compra, implementación y puesta en marcha de un dispositivo IoT:

- Implementación de certificados SSL sobre dispositivos expuestos a internet, para evitar fugas de información.
- Actualización constante de dispositivos por parte del fabricante, solucionando errores de seguridad mediante parches y la instalación por parte del usuario como prioridad.
- La modificación de contraseñas por defecto, a credenciales robustas y sobre protocolos cifrados.
- Implementación de un sistema antivirus que permita mitigar las amenazas comunes si se tiene el acceso a la administración del dispositivo.
- Aunque la mayoría de las soluciones de antivirus para dispositivos Iot se enfocan a un hardware especializado para la red donde se encuentra, si se cuenta con los recursos, se debe implementar este tipo de dispositivos con el fin de mitigar ataques y controlar la salud de nuestra red.

17. Trabajo Futuro

Además de la investigación realizada, la entrega de este trabajo viene con dos anexos importantes:

- Un formato de aseguramiento para dispositivos IoT que utilicen un Sistema Operativo Raspbian (basado en Debian).
- Un script en Python que permite realizar la función de antivirus Ligero evaluando las últimas firmas de botnets de la investigación.

Con los resultados del presente TFM y los anexos presentados anteriormente, las líneas de trabajo que pueden seguirse son las que relaciono a continuación:

- Modificación del script realizado en Python, agregando nuevas funcionalidades, haciendo pruebas para diferentes dispositivos e incrementando las firmas del malware más reciente.
- Creación de formatos de aseguramiento para diferentes tipos de dispositivos en el mercado, realizando su publicación mediante un sitio accesible para el uso por parte de los diseñadores de soluciones en dispositivos de este tipo.
- Buscar nuevos criterios para dar soluciones a este tipo de problemáticas sobre los dispositivos.

18. Glosario

Un glosario es una recopilación de términos que permite disponer de toda la información sobre un tema en específico con un orden alfabético [47], a continuación se relacionan los términos técnicos del presente trabajo:

- **Botnet:** Grupo de dispositivos conectados y controlados de forma remota por parte de un atacante.
- **Command and Control:** Servidor Host que permite controlar una o varias Botnets mediante el envío y recepción de mensajes.
- **DDOS:** Ataque distribuido de denegación de servicio, permite dejar sin servicio a un dispositivo con el envío masivo de peticiones desde diferentes puntos.
- **Host:** Ordenador físico o virtual que permite alojar un servicio.
- **Internet of Things:** Concepto que abarca la interconexión de dispositivos cotidianos a internet.
- **Máquina virtual:** Fragmento de software que emula un host físico, creando una capa de abstracción.
- **Malware:** Del inglés “malicious software”, es un programa malicioso que sirve realizar acciones dañinas en un ordenador.
- **Payload:** Carga útil o preciada de un código para la ejecución de una vulnerabilidad.
- **Sandbox:** Entorno de prueba de software, que permite realizar la ejecución de código maliciosos de manera segura para su estudio.
- **SSH:** Del inglés “Secure Shell”, es un protocolo de acceso remoto a un servidor mediante un túnel de cifrado haciendo la conexión de manera segura.
- **Telnet:** Protocolo de acceso remoto a un servidor sin cifrado.
- **Troyano:** Malware que se presenta como un programa legítimo, pero al ejecutarse realiza una acción dañina.

19. Bibliografía

[1] 2. Real Academia Española, «Sociedad,» [En línea]. Available: https://dle.rae.es/sociedad.

[2] oracle.com, «¿Qué es Internet of Things (IoT)?,» [En línea]. Available: https://www.oracle.com/co/internet-of-things/what-is-iot.html.

[3] E. G. &. A. Colon, «The Best Smart Home Devices for 2020,» PCMAG DIGITAL GROUP, 19 11 2019. [En línea]. Available: https://www.pcmag.com/news/the-best-smart-home-devices-for-2020.

[4] A. C. d. Ingenieros, «Malware en la era del IoT,» [En línea]. Available: https://acis.org.co/portal/content/NoticiaDelSector/malware-en-la-era-del-iot.

[5] H.-H. K.-S. K. M.-J. C. Hyo-Sik Ham, «Linear SVM-Based Android Malware Detection for Reliable IoT Services,» 31 01 2014. [En línea]. Available: https://www.hindawi.com/journals/jam/2014/594501/.

[6] P. M. a. H. V. P. Saleh Soltan, «BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid,» 2018.

[7] D. M. Indhumathi, «Survey of Virus Collection and Antivirus Detection,» 2020.

[8] Eset, «Malware,» [En línea]. Available: https://www.eset.com/es/caracteristicas/malware/.

[9] Mcafee, «Mcafee, What Is Malware?,» [En línea]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-malware.html.

[10] C. o. I. Security, «Top 10 Malware November 2019,» 11 2019. [En línea]. Available: https://www.cisecurity.org/blog/top-10-malware-november-2019/.

[11] Mcafee, «McAfee Labs Threats Report,» 08 2019. [En línea]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

[12] U. 4. P. A. Networks, «2020 Unit 42 IoT Threat Report,» 10 03 2020. [En línea]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

[13] Avast, «avast.com,» avast, [En línea]. Available: https://www.avast.com/es-es/c-botnet.

[14] D. Fisher, «Kaspersky,» 13 04 2013. [En línea]. Available: https://www.kaspersky.es/blog/que-es-un-botnet/755/.

[15] C. Faro, «kaspersky.com,» kaspersky.com, 3 03 2020. [En línea]. Available: https://usa.kaspersky.com/about/press-releases/2020_things-just-got-real-61-of-businesses-already-use-iot-platforms-despite-security-risks.

[16] Checkpoint, «February 2020's Most Wanted Malware: Increase in Exploits Spreading the Mirai Botnet to IoT Devices,» checkpoint, [En línea]. Available: https://blog.checkpoint.com/2020/03/11/february-2020s-most-wanted-malware-increase-in-exploits-spreading-the-mirai-botnet-to-iot-devices/.

[17] bitdefender, «bitdefender.com,» [En línea]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf.

[18] Trendmicro, «Command and Control [C&C] Server,» [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server.

[19] Goolge.com, «The Go Project,» [En línea]. Available: https://golang.org/project/.

[20] P. Litvak, «Kaiji: New Chinese Linux malware turning to Golang,» [En línea]. Available: https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/.

[21] analyze.intezer.com, «Malicious Kaiji,» [En línea]. Available: https://analyze.intezer.com/#/files/9f090a241eec74a69e06a5ffed876c7a37a2ff31e171924673b6bb5f1552814c.

[22] academiaeset.com, «Introducción al Análisis de Malware,» [En línea]. Available: https://www.academiaeset.com/default/store/13599-analisis-de-malware.

[23] spamhaus.org, «The Top 10 Worst,» [En línea]. Available: https://www.spamhaus.org/statistics/botnet-cc/.

[24] F. S. D. P. O. K. E. L. A. K. Victor Chebyshev, 20 05 2020. [En línea]. Available: https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/.

[25] Mcafee, «What is antivirus?,» [En línea]. Available: https://www.mcafee.com/en-us/antivirus.html.

[26] Eset, «Complete Antivirus Software for all of your devices,» [En línea]. Available: https://www.eset.com/uk/antivirus-software/.

[27] N. J. Rubenking, «The Best Antivirus Protection for 2020,» 25 03 2020. [En línea]. Available: https://uk.pcmag.com/antivirus/8141/the-best-antivirus-protection-for-2020.

[28] R. Tyrsina, «Best IoT antivirus and antimalware solutions [2020 Guide],» 28 11 2019. [En línea]. Available: https://windowsreport.com/iot-antivirus-anti-malware/.

[29] bitdefender, «A closer look at how it works,» [En línea]. Available: https://www.bitdefender.com/box/.

[30] Symantec, «Norton Core,» [En línea]. Available: https://us.norton.com/core.

[31] F-secure, «SENSE security router,» [En línea]. Available: https://www.f-secure.com/en/home/products/sense.

[32] vmware.com, «Virtualización,» [En línea]. Available: https://www.vmware.com/co/solutions/virtualization.html.

[33] microsoft.com, «Run Hyper-V in a Virtual Machine with Nested Virtualization,» 18 12 2018. [En línea]. Available: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization.

[34] cloudshare.com, «What Is Nested Virtualization?,» cloudshare.com, [En línea]. Available: https://www.cloudshare.com/virtual-it-labs-glossary/what-is-nested-virtualization.

[35] techopedia.com, «Sandbox,» [En línea]. Available: https://www.techopedia.com/definition/27681/sandbox-software-development.

[36] clamav.net, «Documentation,» [En línea]. Available: https://www.clamav.net/documents/introduction.

[37] antivirus.comodo.com, «Free Comodo Antivirus Software,» [En línea]. Available: https://antivirus.comodo.com/free-antivirus.php?af=7639.

[38] virusshare.com, «Hashes,» [En línea]. Available: https://virusshare.com/hashes.4n6.

[39] Y. A. A. Matta, «PyAvScan-IoT,» [En línea]. Available: https://github.com/yealvare1000/PyAvScan-IoT.

[40] shodan. [En línea]. Available: https://www.shodan.io/search?query=raspbian . [Último acceso: 01 06 2020].

[41] raspberrypi.org, «What is a Raspberry Pi?,» [En línea]. Available: https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/.

[42] raspberrypi.org, «Raspbian,» raspberrypi, [En línea]. Available: https://www.raspberrypi.org/downloads/raspbian/.

[43] Rufus.io, «Rufus,» [En línea]. Available: https://rufus.ie/.

[44] ciset, «¿Qué es el hardening de sistemas operativos?,» 18 03 2020. [En línea]. Available: https://www.ciset.es/publicaciones/blog/746-hardening.

[45] cisecurity.org, «Cybersecurity Best Practices,» [En línea]. Available: https://www.cisecurity.org/cybersecurity-best-practices/.

[46] raspberrypi.org, «Securing your Raspberry Pi,» [En línea]. Available: https://www.raspberrypi.org/documentation/configuration/security.md.

[47] uned.es, «glosario,» [En línea]. Available: https://www2.uned.es/iued/guia_actividad/glosario.htm.

20. Anexos

- *TFM-GuiaAseguramiento-IoT-Raspbian.pdf*
- Script Pyton PyAvScan-IoT.py, firmasdescargadas.txt, archivosSistema.txt