INSTITUTO SUPERIOR TECNOLÓGICO EUROAMERICANO

PROYECTO DE TESIS

Previo a la obtención del Título de Tecnólogo en Informática mención Networking

TÍTULO DEL PROYECTO DE TESIS

Análisis de técnicas, vectores de infección, y detección de atacantes de criptomonedas

PROPUESTA

Investigación sobre la amenaza creciente de criptominería; ejecución de una simulación de malware de criptominería y planteamiento de estrategias basadas en el nivel de éxito que tienen al momento de reconocer, detectar y mitigar actividad maliciosa relacionada con la minería ilegal de criptomonedas.

Autor:
Daniel André Peñaherrera Barriga

Tutor:
Ing. Luis Andrés López Molina

AÑO
2020

INSTITUTO SUPERIOR TECNOLÓGICO EUROAMERICANO

CARRERA DE: INFORMÁTICA

DIRECTIVOS

Ing. ANTONIO MARQUES FIRMINO, MSc.
RECTOR

Ing. WALTER MALDONADO DE LA CRUZ, MSc
VICERRECTOR

Ing. ANTONIO MARQUES GUTIERREZ
SECRETARIO GENERAL

ACEPTACIÓN DEL TUTOR

Fecha:

Ing. ANTONIO MARQUES FIRMINO, MSc.

RECTOR

Ciudad.

Tengo el bien de informar que el egresado: Peñaherrera Barriga Daniel André con cédula de identidad: 0959066796, diseñó y ejecuto el Proyecto de investigación con el tema: Análisis de técnicas, vectores de infección, y detección de atacantes de criptomonedas. El mismo que ha cumplido con la directrices y recomendaciones dados por el (la) suscrito (a).

El autor ha ejecutado satisfactoriamente las diferentes etapas constitutivas del proyecto. Por lo expuesto se procede a la aceptación que pone a vuestra consideración el informe de rigor para los efectos legales correspondientes.

TUTOR (A)

Ing. Luis Andrés López Molina

ACEPTACIÓN DE LA PROPUESTA

Fecha:

Ing. ANTONIO MARQUES FIRMINO, MSc.

RECTOR

Ciudad.

Tengo bien informar que el egresado Peñaherrera Barriga Daniel André con cédula de identidad 0959066796, diseñó, elaboró e implemento la propuesta: Análisis de técnicas, vectores de infección, y detección de atacantes de criptomonedas.

El mismo que ha cumplido con las directrices y recomendaciones técnicas dadas por el suscrito.

El autor ha ejecutado satisfactoriamente las diferentes etapas constitutivas del desarrollo de la propuesta técnica; por lo expuesto se procede a la APROBACIÓN y pone a vuestra consideración el informe de rigor para los efectos legales correspondientes.

Atentamente

_____

Ing. Walter Maldonado de la Cruz, MSc.

VICERRECTOR ACADÉMICO

FECHA:

DERECHOS DE AUTOR

Ing. WALTER MALDONADO DE LA CRUZ, MSc.

VICERRECTOR ACADÉMICO

Ciudad.

Para los fines legales pertinentes comunico a usted que los derechos intelectuales del Proyecto de Investigación:

Análisis de técnicas, vectores de infección, y detección de atacantes de criptomonedas.

Pertenecen al INSTITUTO TECNOLÓGICO SUPERIOR EUROAMERICANO.

Atentamente

_____

Nombre Egresado Peñaherrera Barriga Daniel André

C.I.: 0959066796

EGRESADO.

DEDICATORIA

La realización de este proyecto de investigación no sería posible sin el soporte de mi familia; especialmente el de mi madre, cuyo apoyo incondicional me impulsa a ser la mejor versión posible de mí.

Y a mi amada, Valeria, cuya indiferencia por el manejo de su información personal me sirvió como motivación para llevar a cabo este trabajo investigativo.

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma al INSTITUTO SUPERIOR TECNOLÓGICO EUROAMERICANO

Nombre Egresado Peñaherrera Barriga Daniel André
C.I.: 0959066796
EGRESADO.

EUROtec. TECNOLÓGICO EUROAMERICANO

TECNOLÓGICO ACREDITADO CEAACES 2016

CERTIFICADO DE GRAMATÓLOGO

1 de diciembre del 2020

Por medio de la presente, certifico que he revisado la redacción y la ortografía del contenido de la tesis con el Tema:

"ANÁLISIS DE TÉCNICAS, VECTORES DE INFECCIÓN, Y DETECCIÓN DE ATACANTES DE CRIPTOMONEDAS"

Elaborado por el alumno: **DAŃIEL ANDRÉ PEÑAHERRERA BARRIGA**, previo a la obtención del Título de: TECNÓLOGO EN INFORMÁTICA MENCIÓN NETWORKING. Para el efecto he procedido a leer y analizar de manera profunda el estilo y la forma del contenido concluyendo que:

- Se denota la pulcritud de la escritura en todas sus partes
- La acentuación es precisa
- Se utilizaron los signos de puntuación de manera acertada
- En todos los ejes temáticos se evita los vicios de dicción
- Existe concreción y exactitud en las ideas
- No incurre en errores en la utilización de las letras
- La aplicación de la sinonimia es correcta
- Se maneja con conocimiento y precisión la morfosintaxis
- El lenguaje es pedagógico, académico, sencillo y directo por lo tanto de fácil Comprensión.

Recomendación.- Antes de imprimir revisar con mucha precaución las faltas ortográficas, recordar que las mayúsculas también se tildan.

Mejorar formato del índice, no está el espacio para el informe del gramatólogo, hojas en blanco de más. Tomar en cuenta estas recomendaciones antes de imprimir.

Por lo expuesto y en uso de mis derechos como Lcda. en Ciencias de la Educación mención literatura y español, recomiendo la VALIDEZ ORTOGRÁFICA de su tesis previo a la obtención del título de: TECNÓLOGO EN INFORMÁTICA MENCIÓN NETWORKING

Atentamente

Lcda. Pacheco Berrazueta Susana Emilia
DOCENTE UNIVERSITARIO
REG: 2311-13-164182

ACTA DE VEREDICTO FINAL
PARA LA SUSTENTACIÓN DE TESIS

En la ciudad de Guayaquil al , el **INSTITUTO SUPERIOR TECNOLÓGICO EUROAMERICANO**, convoco al tribunal integrado por los señores Mgs. Antonio Marques Firmino **(Rector),** Mgs.Walter Maldonado de la Cruz **(Vicerrector Académico) ,** Ing. Antonio Marques Gutierrez (**Secretario**), Ing. Luis Andrés López Molina **(Docente),** en calidad de jurado calificador para la sustentación de tesis de grado del alumno egresado:

PEÑAHERRERA BARRIGA DANIEL ANDRÉ

De la carrera de "TECNOLOGÍA EN INFORMÁTICA"

Después de haber observado y realizado las preguntas respectivas este TRIBUNAL resuelve:

APROBAR ☐ **NO APROBAR** ☐ **SUSPENDER** ☐

EL TEMA:

ANÁLISIS DE TÉCNICAS, VECTORES DE INFECCIÓN, Y DETECCIÓN DE ATACANTES DE CRIPTOMONEDAS.

En la ciudad de Guayaquil al ___ día de _____ del 20__, el **INSTITUTO SUPERIOR TECNOLÓGICO EUROAMERICANO**, otorga el título de:

TECNÓLOGO EN INFORMÁTICA MENCIÓN NETWORKING

MGS. ANTONIO MARQUES FIRMINO
Promotor - Rector

MGS. WALTER MALDONADO CRUZ
Vicerrector Académico

ING. ANTONIO MARQUES GUTIERREZ
Secretario

DANIEL ANDRÉ PEÑAHERRERA BARRIGA
Egresado

ÍNDICE GENERAL

ABREVIATURAS

FTP	Archivos de Transferencia
TI	Tecnologías de la Información
HTML	Lenguaje de Marca de salida de Hyper Texto
HTTP	Protocolo de transferencia de Hiper Texto
HTTPS	Protocolo de transferencia de Hiper Texto Seguro
Ing.	Ingeniero
ISP	Proveedor de Servicio de Internet
JS	Javascript
XMR	Monero (Criptomoneda)
CPU	Unidad Central de Procesamiento
RAM	Memoria de Acceso Aleatorio
API	Interfaz de Programación de Aplicaciones
URL	Localizador de Fuente Uniforme
www	World Wide Web (red mundial)
OS	Sistema Operativo
MAEC	Caracterización Enumeración y Atributos de Malware
DDoS	Negación de Servicio Distribuida
C2	Comando y Control
P2P	Peer-to-peer
CCSS	Estándar de seguridad de criptomonedas
RAT	Troyano de Acceso Remoto
MaaS	Malware as a Service
TTP	Tácticas, Técnicas y Procedimientos
BYOD	Bring Your Own Device
PII	Información Personal Identificable
PoW	Prueba de Trabajo
PoS	Prueba de Participación
TLD	Top-Level Domain

SIMBOLOGÍA

α	Alfa
β	Beta

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

INSTITUTO TECNOLÓGICO SUPERIOR EUROAMERICANO

ANÁLISIS DE TÉCNICAS, VECTORES DE INFECCIÓN, Y DETECCIÓN DE ATACANTES DE CRIPTOMONEDAS

Autor: Daniel André Peñaherrera Barriga
Tutor: Ing. Luis Andrés López Molina, Msc.

Resumen

El cibercrimen es un negocio multimillonario, durante el 2019 se generaron ingresos de aproximadamente $3.500,00 millones de dólares. Uno de los ataques más comunes a sistemas es la minería dinero electrónico, mejor conocida como: “criptominería ilegal”, siendo esta una de las actividades ilícitas que más dinero genera dentro de este negocio. Cabe destacar que la criptominería no es una actividad ilegal; existen varias empresas alrededor del mundo dedicadas a minar criptomonedas de manera legal. Sin embargo, la actividad se vuelve ilícita cuando una persona logra penetrar la seguridad de sistemas vulnerables y explota aquella vulnerabilidad para poder utilizar los recursos de aquel sistema vulnerado, para así realizar la criptominería.

La presente investigación enlaza los resultados de las pruebas realizadas en CPU junto con los textos existentes. Como resultado, se plantearán dos

estrategias; de esta manera se podrán establecer medidas para detectar efectivamente la actividad maliciosa de criptominería.

Las dos estrategias que se plantean en este trabajo investigativo se basan en el nivel de éxito que tienen al momento de reconocer y detectar actividad maliciosa relacionada con la minería ilegal de criptomonedas. Estas medidas se dividen en su factor de éxito: La más efectiva, llamada "Alfa" (**α**), y la menos efectiva, llamada "Beta" (**β**).

INSTITUTO TECNOLÓGICO SUPERIOR EUROAMERICANO

ANALYSIS OF TECHNIQUES, INFECTION VECTORS AND DETECTION OF CRYPTOCURRENCY ATTACKERS

Autor: Daniel André Peñaherrera Barriga
Tutor: Ing. Luis Andrés López Molina, Msc.

Abstract

Cybercrime is a multi-million dollar business, generating revenues of approximately $ 3,500.00 million dollars in 2019. One of the most common attacks on systems is electronic money mining, better known as: “illegal crypto mining”, this being one of the illicit activities that generates the most money within this business. It should be noted that crypto mining is not an illegal activity; there are several companies around the world dedicated to mining cryptocurrencies legally. However, the activity becomes illicit when a person manages to penetrate the security of vulnerable systems and exploits that vulnerability in order to use the resources of that compromised system to carry out cryptomining.

The present investigation links the results of the tests carried out in CPU together with existing texts. As a result, two strategies will be proposed; In this

way, measures can be established to effectively detect malicious cryptomining activity.

The two strategies proposed in this investigative work are based on the level of success they have in recognizing and detecting malicious activity related to illegal cryptocurrency mining. These measures are divided into their success factor: The most effective, called “Alpha” (**α**), and the least effective, called “Beta” (**β**).

INTRODUCCIÓN

Las criptomonedas y su mercado han crecido exponencialmente durante la última década; tomando como ejemplo a la criptomoneda Bitcoin, cuyo valor inicial, durante marzo de 2010, fue de $0.0008. En la actualidad, esta criptomoneda posee un valor de $11.808,30.

Con base a lo expuesto en el párrafo anterior, podemos notar que el mercado del dinero electrónico se ha vuelto más lucrativo y accesible para todo público. Inevitablemente, cuando algo (en este caso, las criptomonedas) empieza a ganar valor y asequibilidad, sólo es cuestión de tiempo para que usuarios indeseados se presenten.

En la actualidad, los cibercriminales han adaptado estrategias para monetizar el uso de un sistema con poca o nula supervisión; aprovechando la poca seguridad, acceden al sistema y logran monetizar, aprovechándose de los recursos del sistema para realizar la criptominería ilegal.

Existen varias estrategias para comprometer sistemas y luego poder realizar la minería de criptomonedas, algunas de las estrategias comprenden insertar código malicioso que se ejecutará en el navegador web, haciendo que este efectúe operaciones de criptominería. Otra de estas estrategias consiste en infectar sistemas informáticos con malware. Este último, al ser accionado, ejecutará una aplicación para realizar la minería de criptomonedas.

Las empresas que desarrollan y venden software suelen clasificarlo en grupos, dependiendo de sus funciones y capacidades. Por ejemplo, tecnologías de bases de

datos, suites de organización laboral y productividad, y sistemas operativos. De la misma manera, las comunidades dedicadas a la investigación y desarrollo de seguridad en software usualmente clasifican el malware -software malintencionado- en grupos o tipo basados en sus funciones. MITRE, una organización estadounidense sin ánimo de lucro, desarrolló un lenguaje estandarizado llamado Caracterización Enumeración y Atributos de Malware (MAEC), con la finalidad de que los investigadores compartan información de una manera estructurada sobre el malware analizado. Las etiquetas provenientes del malware son utilizadas dentro de MAEC para poder vincular instancias o familias de malware a grupos o tipos de malware ya definidos (MITRE, 2020).

(TrendMicro, 2020) explica:

> Una botnet (abreviatura de bot *network*) es una red de equipos y dispositivos secuestrados infectados con malware bot y controlados de forma remota por un pirata informático. La red de bots se utiliza para enviar spam y lanzar ataques distribuidos de denegación de servicio (DDoS), y puede alquilarse a otros ciberdelincuentes. Las botnets también pueden existir sin un servidor de comando y control (C&C) mediante el uso de la arquitectura *peer-to-peer* (P2P) y otros canales de administración para transferir comandos de un bot a otro.

Mirai es un claro ejemplo de un bot que logró infectar a más de 600.000 dipositivos de Internet de las Cosas (IoT), por ejemplo, cámaras IP, enrutadores domésticos y sistemas de almacenamiento adjunto en la red (NAS). (Manos Antonakakis, 2017).

Mirai es capaz de escanear continuamente los dispositivos enlazados a IoT y los infecta accediendo mediante telnet con las credenciales de acceso que vienen por defecto, cargando su código malicioso en la memoria principal del dispositivo, de esta forma queda infectado hasta que es reiniciado. “Mirai incluye una tabla de máscaras de red a las cuales no infecta, dentro de las que se encuentran redes privadas y direcciones pertenecientes al Servicio Postal de los Estados Unidos, el Departamento de Defensa, IANA, Hewlett-Packard y General Electric” (Bekerman, 2016). Por su forma de replicarse, la cual es autorreplicable, este bot es considerado como un gusano informático. (Barwise, 2010) comenta:

> “Un gusano informático es un programa informático de malware independiente que se replica a sí mismo para propagarse a otras computadoras”

Mirai puede identificar a los dispositivos IoT vulnerables empleando una tabla de más de 60 nombres de usuario y contraseñas predeterminados de fábrica, y se conecta a ellos para infectarlos con el malware (Moffitt, 2016). Una vez infectados, los dispositivos se conectan a los servidores de comando y control para recopilar detalles del ataque y el objetivo. Luego producen grandes cantidades de tráfico de red, falsificado para parecer legítimo, en los servidores de destino. Con cientos de miles de estos funcionando en conjunto, no es difícil cerrar la mayoría de los sitios. Estos dispositivos convertidos en botnet seguirán funcionando correctamente para el propietario desprevenido, aparte del ancho de banda lento ocasional, y su comportamiento de botnet puede pasar desapercibido indefinidamente. (Moffitt, 2016)

El ransomware, un tipo distinto de malware, cifra los datos de la víctima y exige el pago -usualmente en dinero electrónico- para descifrarlos. Durante el 2016, el malware Necurs distribuyó un troyano bancario llamado Dridex. Los correos electrónicos fueron utilizados como principal vector de infección (Kessem, 2017)

Los troyanos de acceso remoto (RAT) son programas que brindan la capacidad de permitir la vigilancia encubierta o la capacidad de obtener acceso no autorizado a la PC de la víctima. Los troyanos de acceso remoto a menudo imitan comportamientos similares a las aplicaciones keylogger al permitir la recopilación automatizada de pulsaciones de teclas, nombres de usuario, contraseñas, capturas de pantalla, historial del navegador, correos electrónicos, lotes de chat, etc. obtener acceso remoto no autorizado a la máquina de la víctima a través de protocolos de comunicación especialmente configurados que se establecen en la infección inicial de la computadora de la víctima. (Malwarebytes, 2016). Estos servicios se utilizan comúnmente como software de soporte técnico legítimo y pueden estar permitidos por el control de aplicaciones dentro de un entorno de destino. Las herramientas de acceso remoto como VNC, Ammyy y Teamviewer se utilizan con frecuencia en comparación con otro software legítimo comúnmente utilizado por los atacantes (MITRE, 2018)

Las herramientas de acceso remoto pueden establecerse y usarse después del compromiso como canal de comunicaciones alternativo para el acceso redundante o como una forma de establecer una sesión interactiva de escritorio remoto con el sistema de destino. También se pueden utilizar como un componente de malware

para establecer una conexión inversa o una conexión posterior a un servicio o sistema controlado por el adversario (MITRE, 2018)

El malware presentado anteriormente representa una muestra de las herramientas desarrolladas por cibercriminales y actores patrocinados por el estado. Estos grupos pueden beneficiarse económicamente del malware en diversas maneras. Los cibercriminales han sido vistos adoptando el malware-as-a-service (MaaS) (Moreno, 2016). El arrendamiento de software y hardware para la realización de ciberataques. Los propietarios de servidores MaaS proporcionan acceso de pago a una botnet que distribuye malware. Normalmente, a los clientes de dichos servicios se les ofrece una cuenta personal a través de la cual controlar el ataque, así como soporte técnico (Kaspersky, s.f.). Aparte de los ingresos obtenidos al ofrecer este tipo de servicios, los cibercriminales también pueden lucrarse con la información sustraída de los sistemas comprometidos. Ejemplos de este tipo de acciones que el malware puede realizar en nombre de los cibercriminales incluyen: el robo de credenciales, transferencias de fondos, registro de pulsaciones de teclas y robo de carteras de criptomonedas. Según el tipo de información obtenido de estos sistemas comprometidos, un ciberdelincuente puede optar por cobrar (comprar cosas con la información robada de las víctimas) o vender el contenido a partes interesadas.

Las criptomonedas tienen niveles de regulación inherentemente bajos y no están gobernadas por una autoridad central, lo que significa que las transacciones no pueden monitorearse de cerca. Esto los convierte en un refugio para la actividad delictiva en todo el mundo (Marria, 2019).

Una criptomoneda es un activo digital diseñado para funcionar como un medio de intercambio en el que los registros de propiedad de monedas individuales se almacenan en un libro mayor existente en una forma de base de datos computarizada que utiliza criptografía sólida para proteger los registros de transacciones, para controlar la creación de más monedas, y para verificar la transferencia de propiedad de la moneda (Greenberg, 2011).

La arquitectura P2P basada en la comunidad es lo que hace que las criptomonedas independientes de una autoridad central (Lansky, 2018). Debido a que la criptomoneda está descentralizada y no está regulada por ningún estado. El aspecto pseudo-anónimo de la criptomoneda se logra mediante la limitación del conocimiento de la identidad del propietario de la cuenta a los socios comerciales (Lansky, 2018).

Actualmente existen varias criptomonedas en el mercado. La primera criptomoneda, Bitcoin, fue creada por Satoshi Nakamoto y el primer bloque de Bitcoin se extrajo el 3 de enero de 2009. Bitcoin, como muchas otras criptomonedas, gira en torno a una lista digital de transacciones llamada libro mayor distribuido o *ledger* que es mantenido por todos los miembros de la red Bitcoin. La red *Bitcoin* es P2P, el libro mayor distribuido se utiliza para realizar un seguimiento de las entradas (Bitcoins recibidos), o salidas (Bitcoin gastados). Las firmas digitales son utilizadas para firmar los mensajes de las transacciones realizadas. La firma digital es utilizada para firmar un mensaje que se ha generado mediante una función criptográfica, una clave privada y el mensaje contenido (Driscoll, 2013). Todos los miembros pertenecientes a la red Bitcoin tienen una

copia del libro mayor distribuido que se usa para rastrear transacciones. Las cadenas de transacciones permiten a los miembros ver el historial de propiedad de Bitcoins, la transición de entradas a salidas (Driscoll, 2013). Uno de los principales problemas abordados por Bitcoin es la condición de carrera que existe cuando se cambia el ledger están propagando la red Bitcoin (Driscoll, 2013). Bitcoin usa una cadena de bloques para configurar el orden de las transacciones, lo que, a su vez, mitiga la condición de carrera. Cuando una transacción de Bitcoin ocurre, los mensajes de transacción se envían a un grupo de transacciones no confirmadas. Miembros en la red Bitcoin puede formar un conjunto de transacciones no confirmadas en un bloque. Las transacciones dentro se considera que este bloqueo ha ocurrido al mismo tiempo (Driscoll, 2013). Bitcoin utiliza la función hash SHA256 para poder procesar el texto de un bloque y un número aleatorio llamado *nonce* (Driscoll, 2013). El problema matemático es resuelto cuando el hash resultante tiene un número específico de ceros iniciales (Driscoll, 2013). Resolver el problema matemático, los miembros de la red Bitcoin deben ejecutar continuamente la función hash con un *nonce* (número que sólo puede usarse una vez) diferente hasta que se encuentre la respuesta. El primer miembro capaz de encontrar las transmisiones de respuesta de su bloque y las transacciones dentro de ese bloque se agregan al final de la cadena de bloques (Driscoll, 2013). Resolver el problema matemático requiere muchos recursos de sistemas, resultando en un uso elevado de GPU y CPU. Los miembros que resuelven bloques son recompensados en Bitcoin. El proceso de resolver un bloque se llama minería.

Bitcoin fue la primera criptomoneda, pero no es la única. De acuerdo con el sitio especializado en divisas CoinMarketCap (fundado por Brandon Chez en 2013), reporta que, hasta agosto de 2020, existen 6.088 criptodivisas en el mercado, la suma de sus valores genera un total aproximado de tres mil trescientos setenta y dos millones de dólares ($3.372.000.000). Algunas de estas criptomonedas se crearon como alternativas para abordar las deficiencias percibidas de Bitcoin. Una estas criptomonedas se llama Monero. Monero fue creada en abril de 2014 y comparte muchos de los mismos conceptos encontrados en Bitcoin. Una de las diferencias que se pueden destacar giran en torno al uso de el algoritmo CryptoNote. La resistencia al uso del hardware especializado aumenta la posibilidad de igualdad de condiciones para los miembros de la red. Monero pudo lograr el anonimato total implementando la siguiente clave características: firmas de anillo, direcciones ocultas y transacciones confidenciales de anillo (RingCT) (Gekkoin, s.f.). Las firmas de anillo son un tipo de firma digital que incluye un grupo de claves, no resulta factible para cualquier persona, aparte del firmante del mensaje, saber qué clave se utilizó. RingCT se utiliza para ocultar la cantidad de monedas cambiadas en una transacción (Gekkoin, s.f.). Algunos tipos de criptomonedas completamente anónimas son: DASH, Zcoin, Komodo, PIVX, NAV Coin, Verge, ZenCash, y Zcash (Agrawal, 2020). La naturaleza de anonimato de estas criptomonedas sirve como atractivo para llamar la atención de los cibercriminales mientras estas ganan valor en el mercado.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

Ubicación del Problema en un Contexto

Durante el transcurso de la última década, la comunidad de ciberseguridad ha podido observar diversos cambios en los malware implementados por ciberdelincuentes. Las estructuras dentro de su código se vuelven cada vez más complejas, utilizando técnicas tales como la ofuscación, el polimorfismo y el cifrado. Algunos de estos cambios en el malware fueron una respuesta directa a las tecnologías de detección que por su parte pretendían emplear mejores y más efectivas técnicas para el rastreo de software malicioso, por ejemplo, troyanos bancarios que emplean técnicas de evasión de antivirus (también conocido como Anti-AntiVirus), mientras que otros supusieron un cambio de táctica, por ejemplo, extorsionar a los usuarios cifrando sus archivos, mejor conocido como ransomware. Un ejemplo de un cambio más reciente es la mayor y mejor inclusión de software o código dedicado a la criptominería, empleado por los ciberdelincuentes. De hecho, el malware dedicado a la criptominería no es un tema nuevo y desconocido. En el 2011, Karl Dominguez, un ingeniero de respuesta hacia amenazas perteneciente a la compañía multinacional de ciberseguridad y defensa Trend Micro, publicó: “Trend Micro se encontró recientemente con una botnet que convierte un sistema infectado en un minero involuntario de Bitcoin…las Bitcoins son generadas por una aplicación de minería

gratuita de Bitcoins" (Dominguez, 2011). El malware, detectado como BKDR_BTMINE.MNR, instala el software de minería en los sistemas infectados. Utiliza los recursos del sistema para resolver bloques de Bitcoin con el fin de generar más Bitcoins. (Dominguez, 2011).

Situación Conflicto. Nudos Críticos

El crecimiento de las criptodivisas parece no tener fin; hasta la realización de este trabajo investigativo, en el mercado existe un total de 5209 criptodivisas, todas ellas amasan una capitalización del mercado valorado en más de $536 mil millones de dólares (CoinLore, 2020).

Gráfico 1

Capitalización del mercado de criptodivisas, desde 2013 a 2020

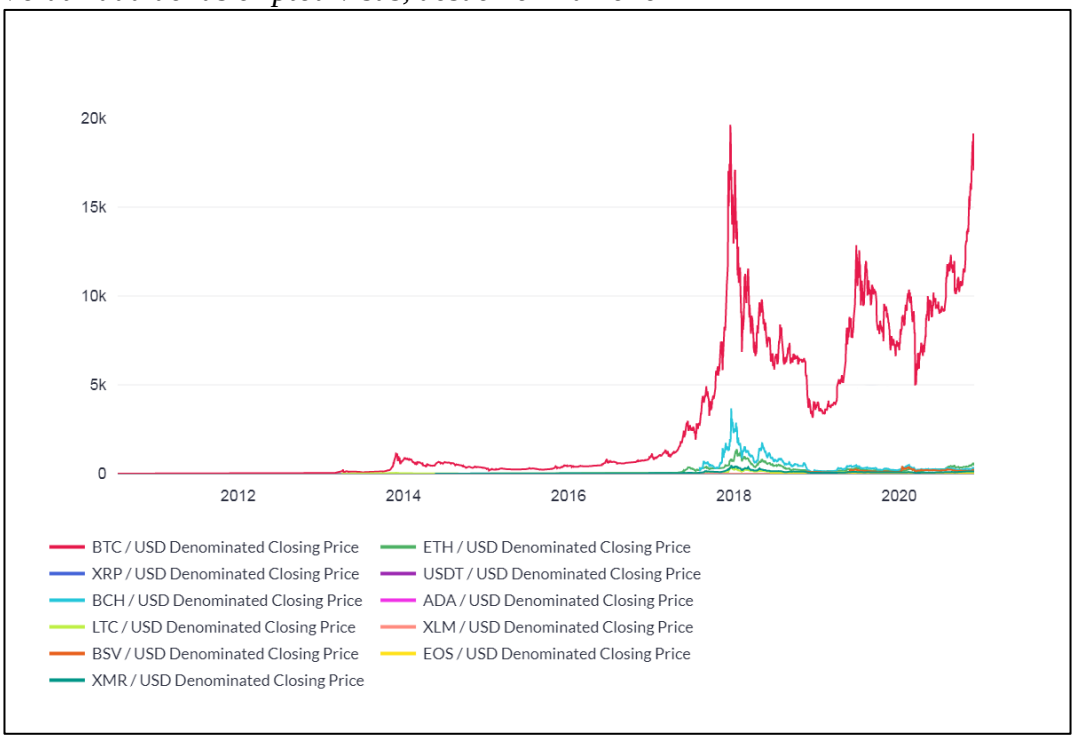
Nota. El gráfico representa la capitalización del mercado de criptodivisas comprendido entre 2013 y 2020, alcanzando su pico máximo en 2018. Tomado de CoinMarketCap, 2020. (https://coinmarketcap.com/es/charts/).

Características de las criptodivisas

Volatilidad. En los mercados de criptomonedas, esta volatilidad posiblemente ha causado pérdidas a los inversores, pero también ha convertido a los inversores, millonarios, en multimillonarios "de la noche a la mañana". Todavía es ingenuo ser adoptado como una moneda corriente en la sociedad, pero posee el potencial sustancial de convertirse en un vehículo de inversión para ayudar a los inversores a obtener beneficios. (Gupta, 2020).

Gráfico 2

Volatilidad de las criptodivisas, desde 2012 a 2020



Nota. El gráfico muestra la volatilidad de las monedas a lo largo de los años, se puede notar que Bitcoin es la moneda más volátil que existe. 2020. (https://network-charts.coinmetrics.io/)

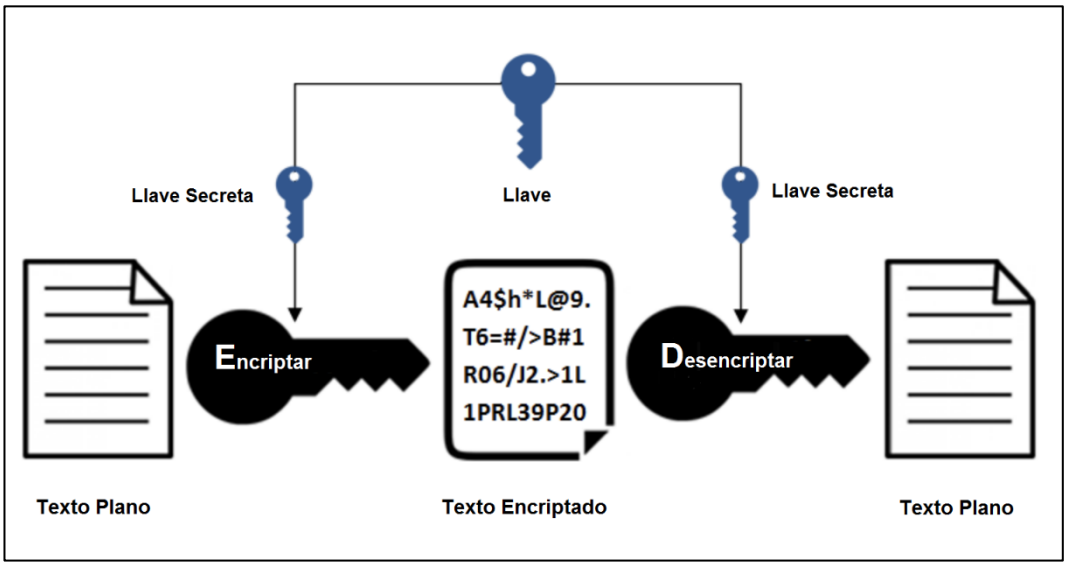
Seguridad. En 2014 se introdujo un estándar de seguridad en el espacio de las criptomonedas, conocido como CCSS (Cryptocurrency Security Standard) para proporcionar una guía específica para la gestión segura de las criptomonedas. Este estándar es actualmente el estándar de referencia para cualquier sistema de información que maneja y administra carteras criptográficas como parte de su lógica comercial.

La criptografía utilizada en las criptomonedas también juega un rol esencial, dado que asegura que las transacciones no se vean comprometidas por terceros, algunos de los métodos criptográficos utilizados son:

- Criptografía de clave simétrica: La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad (diciéndola en alto, mandándola por correo electrónico u ordinario o haciendo una llamada telefónica).

Figura 1

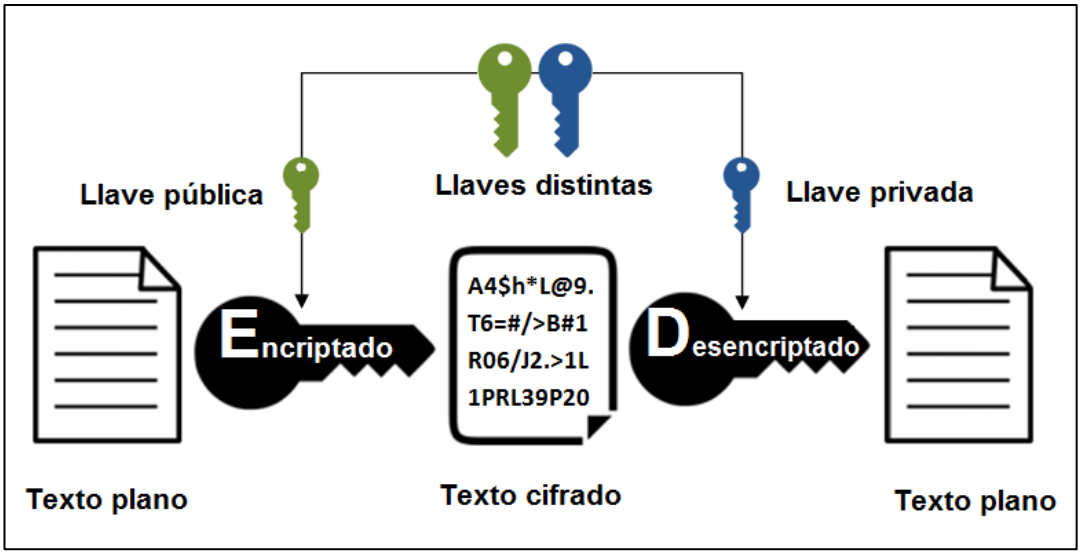
Proceso de criptografía simétrica



- Criptografía de clave asimétrica: La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca).

Figura 2

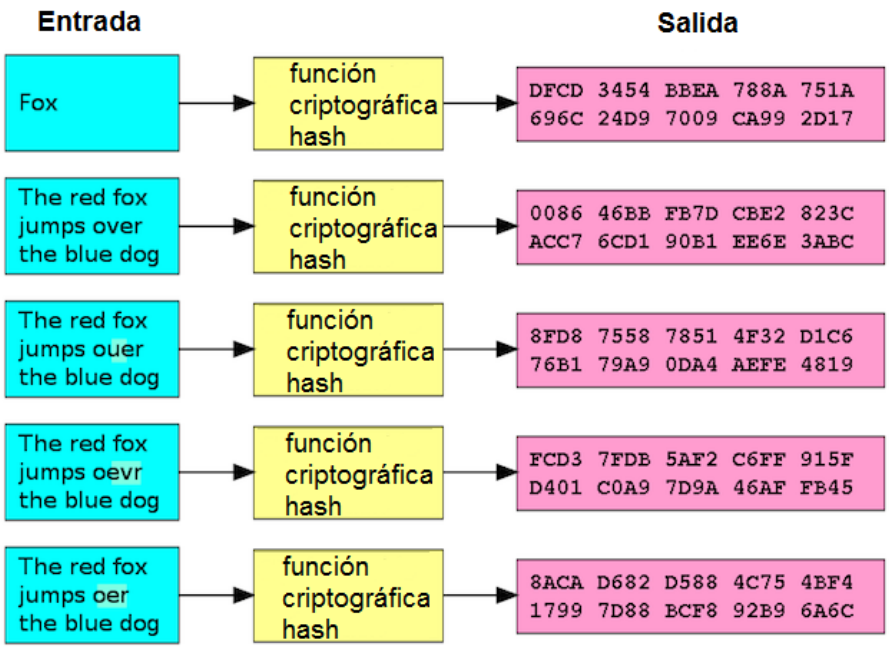
Proceso de criptografía simétrica



- Hash. Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Figura 3

Ejemplo de ejecución de la función hash



Descentralizadas. “Las *blockchains* están políticamente descentralizadas (nadie las controla) y arquitectónicamente descentralizadas (no hay un punto central de falla de infraestructura) pero están lógicamente centralizadas (hay un estado comúnmente acordado y el sistema se comporta como una sola computadora).” (Buterin, 2017).

Figura 4

Diferencia entre redes centralizadas, descentralizadas, y distribuidas

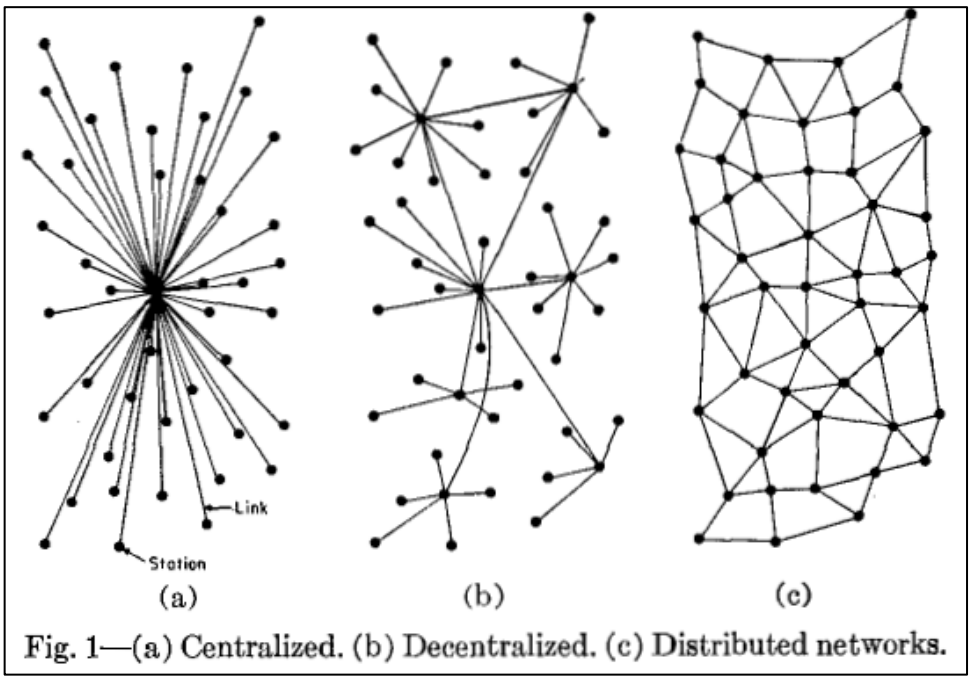


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

El crimen cibernético se ha convertido en un gran negocio, en el cual todos los ataques tienen dos puntos en común: el anonimato y la baja probabilidad de ser descubierto. Al igual que en el resto de los casos de hurto, cada malhechor utiliza sus propios métodos y las motivaciones son distintas. No obstante, existen variaciones regionales en el modo en que los usuarios perciben las actividades del cibercrimen.

Se necesitan muchos recursos informáticos para extraer algo más que una cantidad trivial de criptomonedas. Durante el auge de las criptomonedas, los mineros estaban construyendo máquinas poderosas y haciéndolas funcionar durante todo el día. Las tarjetas gráficas dedicadas, que tradicionalmente se han comercializado para jugadores y diseñadores 3D, subieron de precio y se ensamblaron granjas de servidores enteras con el único propósito de extraer criptomonedas. El mercado de criptomonedas se desplomó en 2018. “A principios de año, bitcoin estaba valorado en $ 14,268 frente al dólar estadounidense. Poco

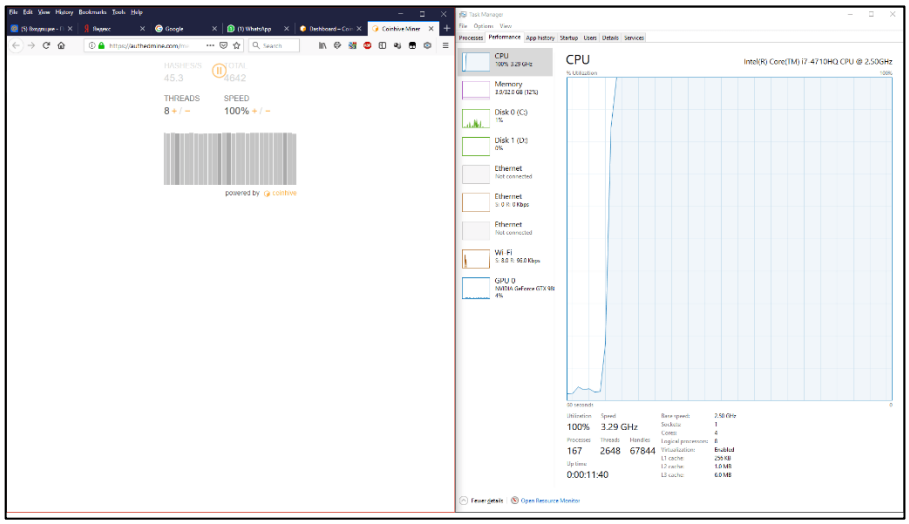
después, la criptomoneda fue testigo de un aumento de precios del 23 por ciento, que vio su valor aumentar a $ 17,568. Desde entonces, bitcoin siguió perdiendo su valor y nunca volvió a la marca de $ 17,000. El punto más bajo del primer trimestre para el valor de bitcoin fue el 6 de febrero de 2018, cuando su precio fue de $ 6,048. En la actualidad, el precio de bitcoin fluctúa alrededor de $ 7,400." (Makadiya, 2018). La gente pronto descubrió que el valor de las criptomonedas que sus máquinas podían extraer ni siquiera era suficiente para pagar el consumo eléctrico.

Un estudio reciente de Kaspersky "cuantificó el consumo de energía y los impactos ambientales de la minería de criptomonedas. Algunas estimaciones sugieren que la cantidad total de energía consumida por los mineros de Bitcoin en todo el mundo es comparable al consumo total de energía de la República Checa, un país con más de 10 millones de habitantes" (Lurye, 2019).

Aquel estudio utilizó computadoras de 18 voluntarios, se pudo determinar experimentalmente el aumento en el consumo de energía de 21 dispositivos diferentes al extraer Monero en CoinHive (el servicio de minería de criptomonedas más común).

Figura 5

Consumo de CPU durante la minería de criptomonedas



Nota. Adaptado de *Assessing the impact of protection from web miners*, Kaspersky, 2019.

Los mineros de criptomonedas menos honorables pronto encontraron la solución perfecta: usar la computadora de otra persona para hacer el trabajo y hacer que ellos paguen la factura, de esta manera nació el cryptojacking. La investigación realizada por Kaspersky, cuya base fue la protección del negocio ante esta creciente amenaza, afirma que: "Utilizando muchas de las mismas tácticas que se utilizan para difundir ransomware, los delincuentes ahora están infectando millones de computadoras en miles de redes con malware de cryptojacking, que extrae monedas digitales y envía los fondos directamente a sus billeteras digitales anónimas" (Kaspersky, 2019).

Los piratas informáticos tienen dos formas principales de hacer que la computadora de la víctima extraiga criptomonedas en secreto. (Nadeau, 2020) afirma:

> "Una es engañar a las víctimas para que carguen código malicioso de criptominería en sus computadoras…el otro método es inyectar un script en un sitio web o un anuncio que se envía a varios sitios web. Una vez que las víctimas visitan el sitio web o el anuncio infectado aparece en sus navegadores, el script se ejecuta automáticamente".

Causas y Consecuencias del Problema

La causa principal de la minería ilegal de criptomonedas es el poder lucrarse con esta actividad con un riesgo medio; el anonimato que brindan las diferentes criptomonedas durante las transacciones impide que se pueda rastrear a los atacantes. Esta actividad ilícita se ha visto en auge durante la última década dado que su factor ganancia-riesgo está más que equilibrado. Como consecuencia, los ciberatacantes que utilizan esta técnica maliciosa son comunes hoy en día, atacando a usuarios comunes por medio de phishing al abrir correos electrónicos.

Delimitación del Problema

Las limitaciones del proyecto incluyen: (a) las pruebas sólo se realizaron en el sistema designado de prueba, otras CPU o GPU pueden producir resultados diferentes; (b) las pruebas basadas en el sistema se basaron en los textos

revisados, otros tipos de malware pueden minar criptomonedas de forma más sigilosa; (c) las pruebas se realizaron con limitaciones en la interacción del usuario; y (d) las pruebas se realizaron con la configuración predeterminada del malware ya desarrollado por el atacante, otros ciberatacantes pueden optar por minar de forma más o menos agresiva.

Formulación del Problema

El uso no autorizado de recursos en sistemas vulnerados para la ejecución de minería ilegal de criptomonedas.

Evaluación del Problema

Delimitado: Las pruebas realizadas están limitadas a una sola muestra de malware.

Claro: La investigación mostrará las métricas que se presentaron durante las pruebas de ejecución.

Evidente: Mediante la experimentación, la recolección de datos y la presentación de estos, se podrá evidenciar la veracidad de los resultados obtenidos durante el desarrollo de este trabajo.

Relevante: El trabajo investigativo es relevante porque: a) Explica el funcionamiento de una amenaza informática presente y creciente, y b) Propone soluciones para evitar ser víctimas de este malware.

Factible: El presente proyecto de investigación resulta factible dado que las soluciones planteadas pueden ser implementadas en un entorno de trabajo real.

Identifica los productos esperados: Los resultados esperados de este trabajo investigativo abarcan con todo lo propuesto, dentro de las limitantes previamente expuestas.

Alcances del Problema

El presente trabajo investigativo sólo tomará en cuenta el estudio de la literatura existente y el análisis de los resultados provenientes de la experimentación con software dedicado a la minería ilegal de criptomonedas. Las

pruebas se realizarán: (a) en un ambiente aislado (virtualización) para prevenir que el malware pueda escalar a la red "real" y de esta manera evitar su replicación y ejecución dentro de la red, puede que el comportamiento del malware cambie al llegar a detectar que se encuentra en un ambiente virtualizado; (b) sólo se realizará la prueba de un malware, puede que existan otros tipos de malware que se encuentran dentro de la misma categoría, pero que resulten más agresivos.

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo general

Analizar el funcionamiento, describir, y registrar el comportamiento del malware de criptomonedas, así como también proponer medidas de seguridad y respuesta para evitar que los usuarios se conviertan en víctimas de esta creciente práctica ilegal.

Objetivos específicos

- Demostrar el principal vector de infección que usan los atacantes para poder infiltrar su malware en los terminales de cómputo
- Examinar el malware y describir el funcionamiento dentro de un ambiente de ejecución controlado
- Sugerir medidas de detección y respuesta frente al malware de criptominería.

JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

El propósito de esta investigación es poder explicar el funcionamiento del software malicioso dedicado a la minería ilegal de criptomoneda, y proponer métodos eficaces de detección de este tipo de actividad. Para ganar un mejor entendimiento del malware de la criptominería, se analizarán informes de análisis de criptomineros maliciosos. Asimismo, este trabajo de investigación documentará el impacto de las aplicaciones de criptomineros en el CPU del

sistema de prueba. El estudio permitirá mostrar las tácticas, técnicas y procedimientos (TTP) utilizados en el malware y los procedimientos utilizados por los cibercriminales para infectar los sistemas.

Los métodos de detección expuestos en este trabajo investigativo servirán para ilustrar a los lectores y proporcionar una base sólida para mejorar sus capacidades de detección y respuesta frente a la creciente amenaza de malware de criptominería.

Este texto investigativo abordará dos preguntas principales relacionadas con el análisis y detección de malware de criptominería.

1. ¿De qué manera suelen ser atacadas e infectadas las víctimas con malware de criptominería?
2. ¿Cuáles son las técnicas detectables que son utilizadas dentro del malware de criptominería?

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DEL ESTUDIO

Investigaciones en el extranjero

El lucro se constituye como una de las principales motivaciones para la realización del cibercrimen. Independientemente de que los cibercriminales sean actores independientes y solitarios, una organización criminal o grupos financiados por el Estado, la sola idea de acumular riqueza resulta increíblemente atractiva, y más aún cuando el riesgo es bajo en comparación con la ganancia.

Una investigación realizada por el Instituto Ponemon, un instituto dedicado a la investigación de la protección de la privacidad, información y políticas de seguridad publicó, en conjunto con Palo Alto Networks, un estudio sobre la motivación de los cibercriminales a la hora de cometer delitos informáticos. En este estudio, se encuestaron a 304 expertos en amenazas provenientes de Estados Unidos, el Reino Unido y Alemania. Se creó ese panel de expertos en base a su participación en las actividades del Instituto Ponemon y conferencias de seguridad dentro del campo de TI.

Un segundo estudio, publicado por el IBM X-Force Incident Response and Intelligence Services (IRIS) muestra un resumen de las amenazas más prominentes del año pasado. Los datos y conocimientos en aquel estudio se derivan de los servicios de seguridad gestionados por IBM: servicios de respuesta de incidentes, pruebas de penetración, servicios de gestión de vulnerabilidades. Los equipos de investigación de IBM X-Force analizan datos de cientos de millones de terminales protegidos y servidores, junto con datos derivados de los sensores de spam y honeynets. IBM Security Research también ejecuta trampas de spam alrededor del mundo y supervisa decenas de millones de spam y ataques de

phishing a diario, analizando miles de millones de páginas web e imágenes para detectar campañas de ataque, actividades fraudulentas y abuso de marca.

Un tercer estudio, el Trustwave Global Security Report, nos brinda una amplia perspectiva sobre los nuevos vectores de ataque e infección que fueron tendencia durante el último año. Se exploraron distintos esquemas y tendencias usados por cibercriminales que abarcan desde extorsión sexual hasta cryptojacking.

Los estudios anteriormente mencionados sirven como base para desarrollar los antecedentes de este trabajo investigativo. A pesar de que no se enfocan totalmente en el cryptojacking, son de gran utilidad dado que muestran las tendencias, esquemas y métodos de los atacantes al momento de intentar penetrar en la organización.

Un cuarto estudio, enfocado al cryptojacking y al manejo de criptomonedas en el mundo criminal, realizado por Groysman (2018), denominado: "Revolution in Crime: How Cryptocurrencies Have Changed the Criminal Landscape" nos muestra el porqué la minería ilegal de criptomonedas enfocado a las industrias, especialmente a las industrias de tecnología, en donde se utilizan grandes centros de cómputo para ofrecer sus servicios, es un negocio rentable y en aumento constante. El uso de criptomonedas como Monero, que tienen un mayor anonimato en comparación a sus demás contrapartes, hace que sea la moneda favorita para ser minada por este tipo de individuos.

Esta tesis examinará las formas en que varias criptomonedas han impactado a ciertos delitos tradicionales. Si bien el crimen siempre está evolucionando con la tecnología, las criptomonedas cambian las reglas del juego, ya que proporcionan información anónima y descentralizada. sistemas de pago que, si bien se pueden rastrear en un sentido reactivo a través de la cadena de bloques, los delincuentes consideran que tienen mejores usos para ellos que las monedas fiduciarias tradicionales, como la capacidad de enviar dinero relativamente rápido a otra parte sin pasar por un intermediario, o la capacidad de ocultar el origen del dinero para el lavado de dinero propósitos. Cada semana hay nuevas criptomonedas inundando el mercado, y no parece que disminuirá pronto.

Para el desarrollo de la experimentación, el registro de métricas y análisis del comportamiento del malware, se basó en las prácticas mencionadas revisadas dentro de la mayor bibliografía consultada, siendo esta Practical Malware Analysis, escrita por Sikorski y Honig (2012). Este texto nos sirve como guía práctica para poder desarrollar análisis (estáticos y dinámicos), así como también nos brinda un enfoque en el comportamiento y funcionalidad del malware antes, durante y después de su ejecución.

Por último, un trabajo de investigación desarrollado por Burgess el al., (2020), titulado You Could Be Mine(d): The Rise of Cryptojacking nos brinda un mayor enfoque sobre cómo este método de enriquecimiento ilícito pudo lograr mantenerse relevante a pesar de que se encontraron maneras de mitigar los ataques. Claro está que su enfoque tuvo que cambiar; pasó de ser un simple script de JS insertado en el código de una página web a ser un código bien elaborado, usando, por ejemplo, técnicas de ofuscación, para así poder llegar a los centros de cómputo de la organización.

Este último trabajo investigativo sirve para explicar y comprender cómo ha evolucionado esta técnica para mantenerse útil y relevante. Si bien se han creado métodos para mitigar los ataques, los cibercriminales se vieron obligados a cambiar la estructura del código, buscar nuevos vectores de infección, y cambiar su objetivo.

FUNDAMENTACIÓN TEÓRICA

Las criptomonedas basadas en blockchain han surgido como una innovación en los sistemas distribuidos, lo que permite un almacenamiento de transacciones transparente y correctamente distribuido. Para prevenir el abuso y mejorar la confiabilidad en las criptomonedas, se utilizan varios mecanismos de prueba, como la Prueba de trabajo (PoW) y la Prueba de Participación (PoS). En Bitcoin, una de las criptomonedas basadas en blockchain más prominentes, llamada PoW, se usa para incrustar confiabilidad en el sistema. En Bitcoin, los mineros individuales extraen nuevas monedas a través de extensas operaciones de hash,

que luego son verificadas por nodos distribuidos en una red peer-to-peer (P2P) (Saad, 2018). Sin embargo, el uso de PoW en Bitcoin ha dado lugar a abusos: un atacante puede emplear varias técnicas para abusar de los recursos públicos con fines de minería y realizar cálculos de hash extensos sin costo alguno o a un costo significativamente bajo.

Una de esas técnicas que ha surgido recientemente se llama cryptojacking, que implica subcontratar cálculos de hash en criptomonedas basadas en PoW. El criptojacking es el uso de los recursos del sistema de un dispositivo objetivo para calcular hashes y obtener ganancias de la minería sin el consentimiento del propietario del dispositivo objetivo. El cryptojacking convencional implicaba la instalación de un software binario en una máquina de destino que resolvía en secreto PoW y comunicaba los resultados a un servidor remoto.

> El vector de ataque principal para estos ataques son las credenciales comprometidas que se utilizan para infiltrarse en entornos, activar instancias informáticas y realizar operaciones de minería. Como resultado, las organizaciones deben instituir políticas estrictas de acceso de usuarios y monitorear atentamente las actividades de los usuarios para detectar comportamientos anómalos. (Badhwar, 2018)

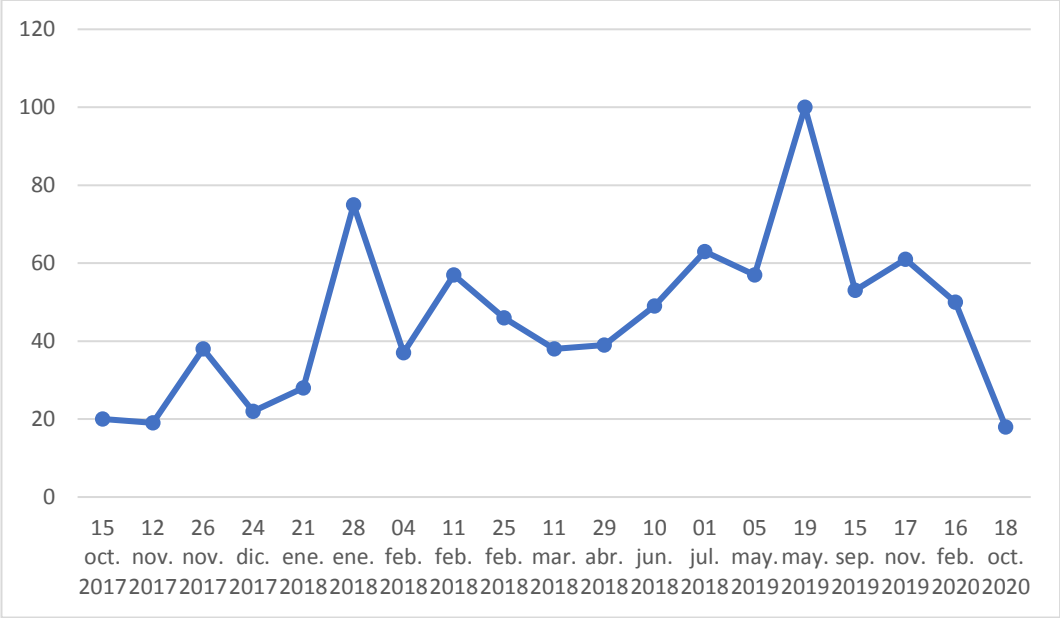
El uso convencional de este cryptojacking requería permiso del usuario para descargar el software y una conexión a Internet persistente para de esta manera poder comunicar el resultado de PoW hacia el adversario o al servidor dropzone controlado por él. Sin embargo, el cryptojacking convencional resultó inviable por varias razones. En primer lugar, no todos los dispositivos tienen una conexión permanente a Internet cuando se necesitan para enviar resultados de PoW; el PoW es sensible al tiempo y, si no se recibe inmediatamente después de ser resuelto, se vuelve obsoleto con facilidad. En segundo lugar, los proveedores de servicios de antivirus pueden identificar fácilmente los binarios utilizados para el cryptojacking y detectarlos.

Justo antes del mediodía del 6 de marzo, Windows Defender Antivirus bloqueó más de 80.000 instancias de varios troyanos sofisticados que presentaban técnicas avanzadas de inyección de procesos cruzados, mecanismos de persistencia y métodos de evasión. Las señales basadas en el comportamiento junto con los modelos de aprendizaje automático impulsados por la nube descubrieron esta nueva ola de intentos de infección. Los troyanos, que son nuevas variantes de Dofoil (también conocido como Smoke Loader), llevan una payload de minero de monedas. En las siguientes 12 horas, se registraron más de 400.000 casos, el 73% de los cuales se produjeron en Rusia. Turquía representó el 18% y Ucrania el 4% de los encuentros mundiales. (Microsoft Defender ATP Research Team, 2018).

Inicialmente diseñado como una fuente de ingresos benigna alternativa a la publicidad en línea, el cryptojacking en el navegador fue facilitado por servicios en línea como Coinhive, que proporcionaba plantillas JavaScript para el cryptojacking. Coinhive proporciona scripts para minar Monero, una criptomoneda difícil de rastrear, y para recompensar a los mineros en función de los valores hash agregados que aportan. Los informes de búsqueda de términos de Google para "Cryptojacking", "Monero" y "Coinhive" de mayo de 2017 a octubre de 2020 demuestran el creciente interés en el cryptojacking como fenómeno global, como se puede apreciar en el gráfico 3.

Gráfico 3

Interés en el cryptojacking durante 2017 a 2020



Autor: Daniel Peñaherrera B.

Fuente: Google Trends (2020)

El uso del cryptojacking como reemplazo de la publicidad también ha sido testigo de un gran debate. Por ejemplo, algunos sitios web populares como "The Pirate Bay", entre otros, comenzaron a utilizar el cryptojacking como un sustituto de los ingresos de la publicidad en línea.

> Los operadores de Pirate Bay habían afirmado en septiembre que estaban probando Coinhive como una alternativa a la ejecución de anuncios en el sitio, sin embargo, BleepingComputer informa que el minero de criptomonedas se está ejecutando junto con los anuncios habituales del sitio en este momento. Al usar Coinhive, los usuarios informaron un alto uso de la CPU cuando visitaban el sitio de torrents, lo que ralentizaba sus computadoras. (Shaikh, 2017).

Generalmente, los atacantes utilizan dos estrategias principales para el uso no autorizado de la máquina de una víctima para extraer monedas digitales a través del cryptojacking: instalando un binario en la máquina o usando un script en el navegador. El primero carga el código de minería en la máquina de la víctima

como un binario independiente (o una infección de un binario). Como tal, requiere información sobre la máquina de destino, incluido su sistema operativo y las construcciones de hardware. Por ejemplo, un binario de cryptojacking malicioso desarrollado para Windows no se puede ejecutar en Linux. Sin embargo, la segunda estrategia es independiente de la plataforma, el JavaScript de cryptojacking se ejecuta al cargar el sitio web en el navegador de la víctima. En ambos casos, el código de minería funciona en segundo plano mientras la víctima inconsciente está usando su máquina. El enfoque de este artículo es el último tipo, que destacamos detalladamente a continuación. En el resto de este artículo, nos referiremos al caso de abuso de cryptojacking, en el que un adversario inyecta scripts de cryptojacking para extraer criptomonedas.

FUNDAMENTACIÓN SOCIAL

El presente proyecto tiene como finalidad social el ilustrar a los usuarios con pocos o nulos conocimientos informáticos; usuarios de aplicativos ofimáticos y demás, que no poseen una cultura de la ciberseguridad o que no sea muy efectiva. La implementación de este proyecto puede llegar a significar la evasión de un ataque de seguridad hacia una empresa (y todo lo que este engloba) por medio del eslabón más débil de toda compañía: un empleado mal informado.

FUNDAMENTACIÓN LEGAL

En Ecuador por medio del Código Orgánico Integral Penal (COIP), en la sección novena, desde del Artículo 178 hasta el Artículo 234 del COIP, se sanciona los delitos informáticos que atenten contra la seguridad de información confidencial, revelación ilegal de datos, daños financieros, accesos no autorizados, entre otros (Código Orgánico Integral Penal, 2018). En la siguiente tabla se

muestra, de forma detallada, los artículos, la actividad que sanciona y la pena que se impone a los culpables.

Tabla 1

Artículos en el COIP que aplican a la criptominería ilegal

Artículo en el COIP	Se comete cuando	Pena
Artículo 190.- Apropiación fraudulenta por medios electrónicos	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones.	Pena privativa de libertad de uno a tres años
Artículo 231.- Transferencia electrónica de activo patrimonial	La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero.	Pena privativa de libertad de tres a cinco años.
Artículo 232.- Ataque a la integridad de sistemas	• Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o	Pena privativa de

informáticos	distribuya de cualquier manera, dispositivos o programas informáticos maliciosos. • Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. • Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana.	libertad de tres a cinco años. Pena privativa de libertad de cinco a siete años.
Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.	Pena privativa de libertad de tres a cinco años.

Hipótesis

Los ataques causados por cryptojacking consumen grandes recursos del sistema víctima; ralentizándola enormemente, inutilizando el terminal de cómputo.

Variables de la Investigación

Variable independiente

Cantidad de uso de CPU y GPU establecido en el código del cryptomalware.

Variable dependiente

Rendimiento del terminal de cómputo.

DEFINICIONES CONCEPTUALES

La utilización de programas maliciosos para el lucro ilegal por medio del uso de los recursos del computador de la víctima sin el consentimiento de esta última.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

DISEÑO DE LA INVESTIGACIÓN

Modalidad de la Investigación

La modalidad escogida para este presente trabajo investigativo será la investigación de campo, dado que a través de esta modalidad se establecen las relaciones entre la causa y el efecto, y se predice la ocurrencia del caso o fenómeno.

Tipo de investigación.- El tipo de investigación experimental será el modelo investigativo empleado en este trabajo, dado que existirá la manipulación de la variable independiente y se medirá el efecto de la variable independiente sobre la variable dependiente. Todo lo anteriormente mencionado será utilizado con el fin de intentar determinar las causas y consecuencias del fenómeno establecido en esta investigación. Este tipo investigativo pretende resolver; no solo el qué sino el porqué, y cómo ha llegado la problemática al lugar en donde se encuentra actualmente por medio de la experimentación y el procesamiento de la información recolectada.

Métodos de investigación.- El método escogido para la realización de este proyecto investigativo fue el método de análisis, dado que dentro de aquel método todo se descompone en varios elementos que luego se pasan a estudiar de manera minuciosa, como es el caso de malware; se deben estudiar e investigar sus componentes individualmente para poder entender el comportamiento de este y la correlación que existe entre los componentes.

POBLACIÓN Y MUESTRA

Población

La población de la investigación son personas, entre las edades de 18 a 45 años, ecuatorianas, con un nivel de conocimiento informático que va desde el uso de herramienta ofimáticas, hasta programadores.

Muestra

La división de la población se basó en la habilidad y conocimientos informáticos que los individuos poseen.

Tabla 2

Síntomas que presenta el equipo ante una aparente infección

Síntoma	Cantidad
El rendimiento del equipo baja considerablemente	16
Cambios en archivos y directorios	6
El equipo se inhibe	4
Crasheo del sistema	2
TOTAL	**28**

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Técnica

Dado que la presente investigación intenta simular los efectos del malware de criptominería actuando dentro de un sistema comprometido y mostrar las consecuencias de la ejecución de este malware, se utilizarán las siguientes técnicas de recolección de datos:

- Fichaje documental
- Lectura Científica
- Análisis de Contenido
- Observación de Campo

Tabla 3

Instrumentos

Técnica	**Instrumento**
Fichaje Documental	Fichas de cryptomalwares
Lectura Científica	Reportes de comportamiento e infecciones causadas por cryptomalware, creación y manejo de laboratorios de malware
Análisis de Contenido	Interpretación de datos recolectados
Observación de Campo	Monitor de rendimiento de Windows, Wireshark, Process Monitor - Sysinternals

Instrumentos de Investigación

Los instrumentos utilizados durante la recolección de la información son los siguientes:

- Encuestas dirigidas a usuarios informáticos, cuyo nivel varía entre novato hasta avanzado.
- Un sistema operativo Windows 7 Professional 64 bits dentro de un entorno virtual
- Una laptop Lenovo i3 7020u a 2,3 GHz con 12 GB de RAM y 1TB de capacidad en disco duro (se designaron 4GB de RAM y 20 GB de disco duro para el sistema operativo virtualizado). Se creará un ambiente virtual con conexión a internet. La instalación será con una imagen ISO del sistema operativo Windows 7 Professional 64 bits. Se garantiza que los procesos son confiables dado que, al ser un sistema operativo recién instalado, no se

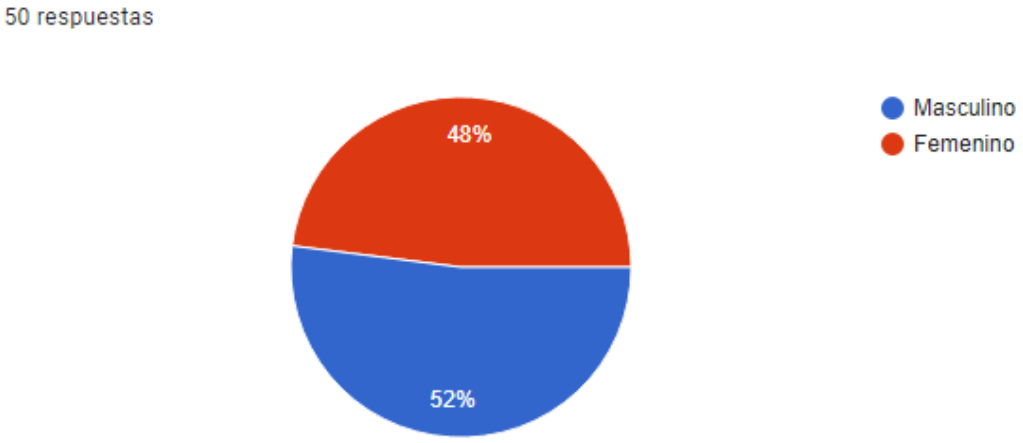
ha añadido ningún programa que pueda llegar a afectar al proceso de levantamiento de información.

- Monitor de rendimiento de Windows. Una aplicación nativa del sistema operativo que permite ver el rendimiento del sistema, las aplicaciones y los procesos relacionados a estas.
- Wireshark. Un monitor de paquetes de red.
- PEiD. Una herramienta que detecta los empaquetadores, criptografías y compiladores, y firmas digitales más comunes.
- Resource Hacker. Un compilador y decompilador de recursos en ejecutables.
- WinMD5. Herramienta que sirve para verificar el algoritmo criptográfico que usa el malware y obtenerlo.
- VirusTotal. Sitio web que proporciona de forma gratuita el análisis de archivos, páginas web y hashes.
- Any.run. Sandbox en línea que permite analizar malware, está basado en la nube.

Recolección de la Información

Gráfico 4

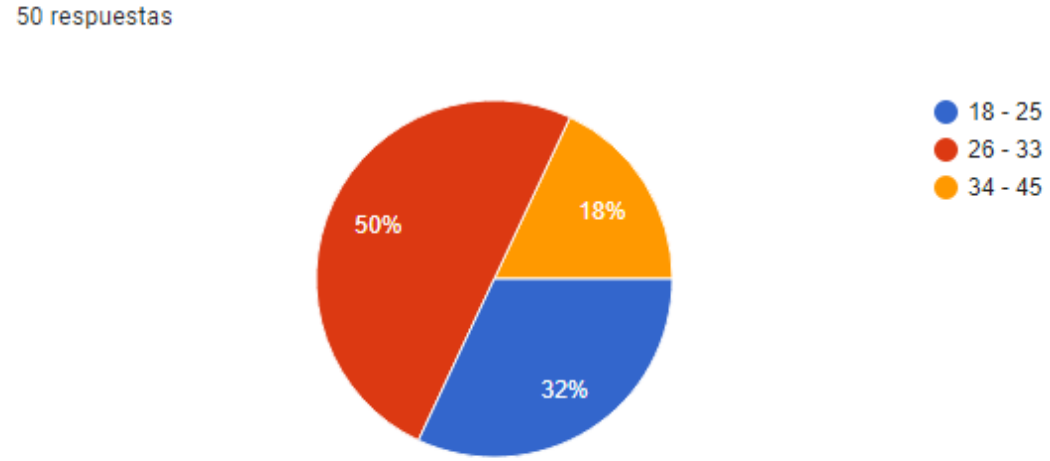
¿Cuál es su género?



Fuente: Encuesta elaborada por autor
Elaborado por: Autor

Gráfico 5

¿Cuál es su edad?

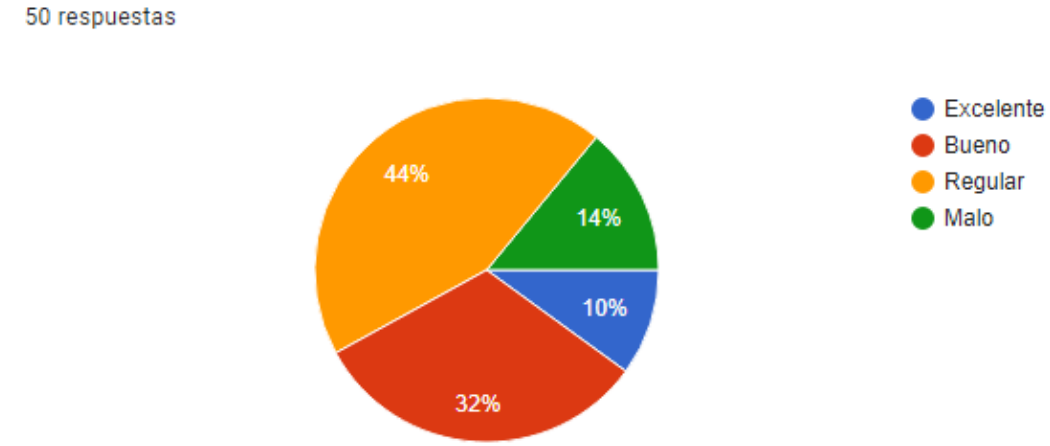


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 6

Defina el nivel de conocimiento general sobre seguridad informática que posee

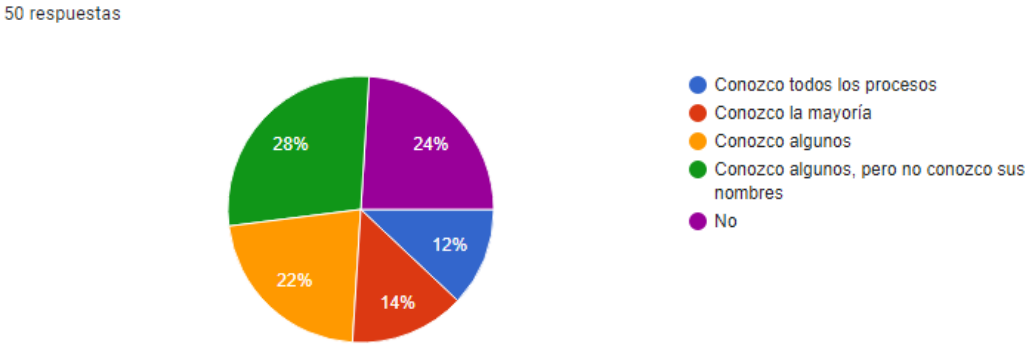


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 7

¿Conoce usted los procesos que se manejan detrás de una página web?

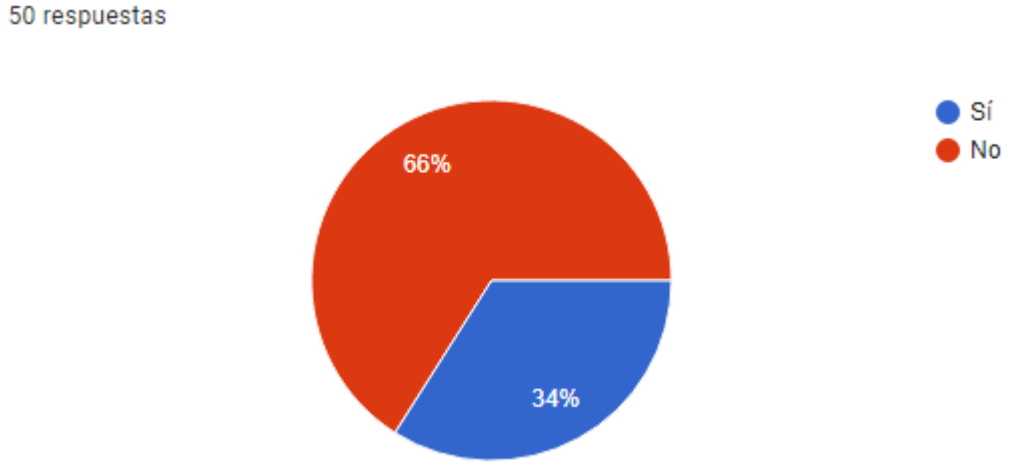


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 8

¿Conoce qué es cryptojacking?

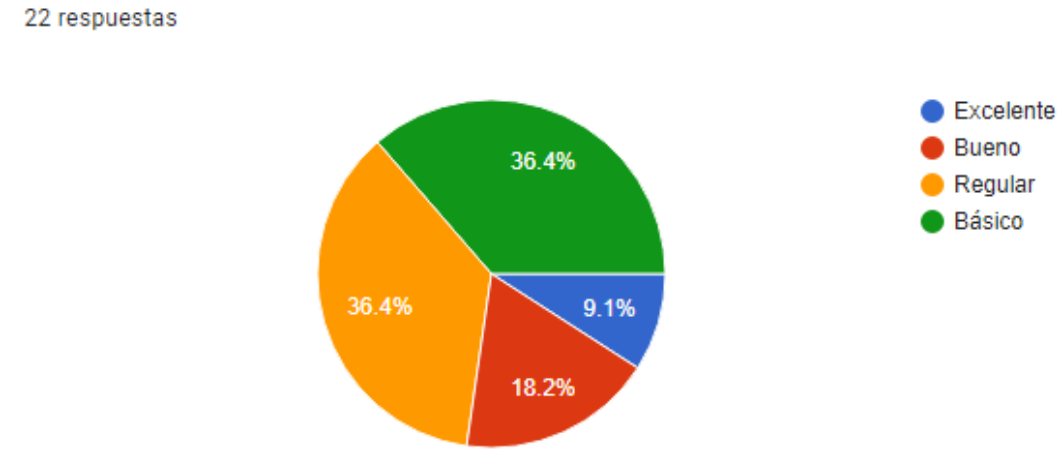


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 9

Indique su nivel de conocimiento sobre cryptojacking

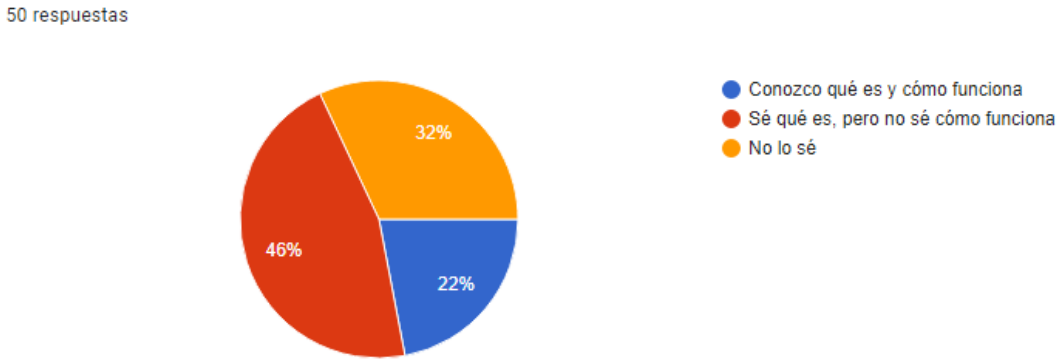


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 10

¿Conoce qué es y cómo funciona la criptominería?

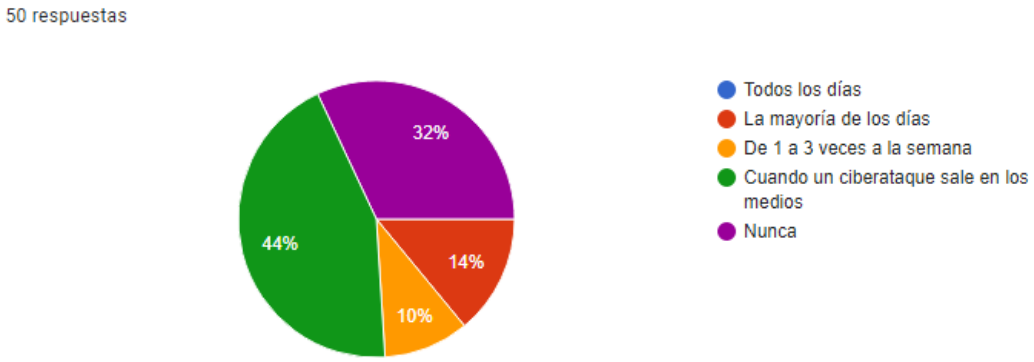


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 11

¿Con cuánta frecuencia suele buscar información sobre ataques de ciberseguridad?

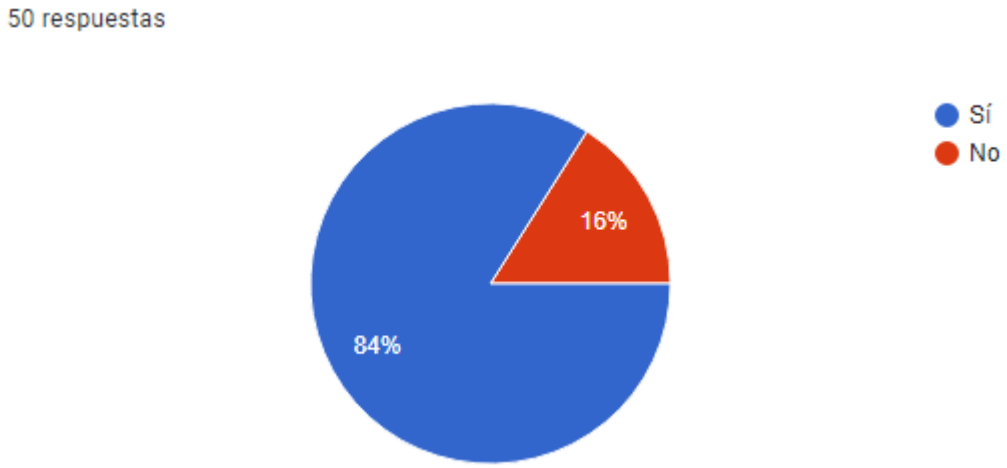


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 12

¿Posee usted experiencia laboral? (Si su respuesta es "No", favor pasar a la pregunta #12)

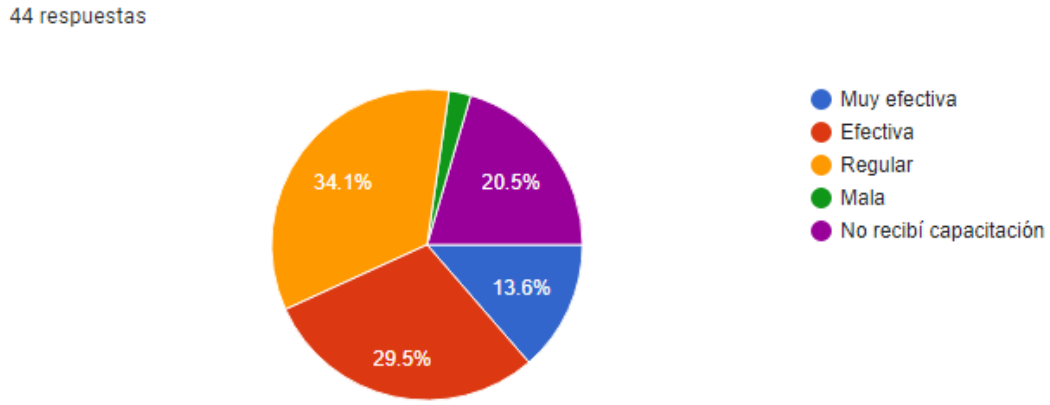


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 13

¿Qué tan efectiva considera usted que fue la capacitación de ciberseguridad recibida en su trabajo?

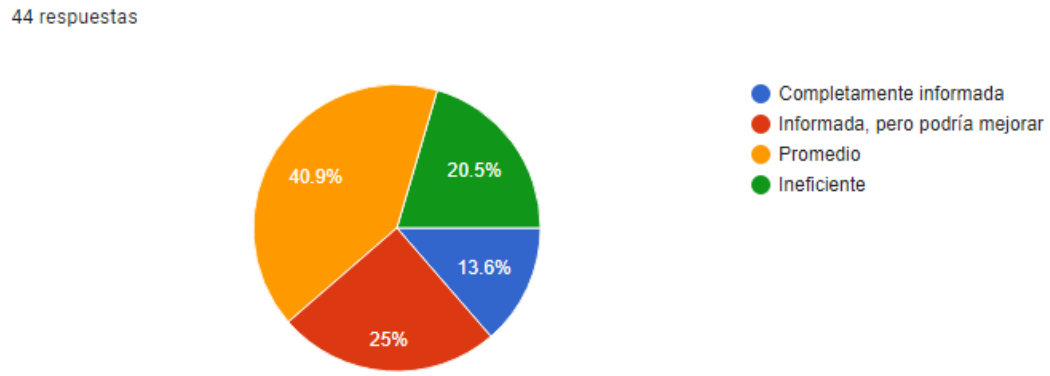


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 14

¿Cómo considera usted a la cultura de ciberseguridad de sus compañeros de trabajo?

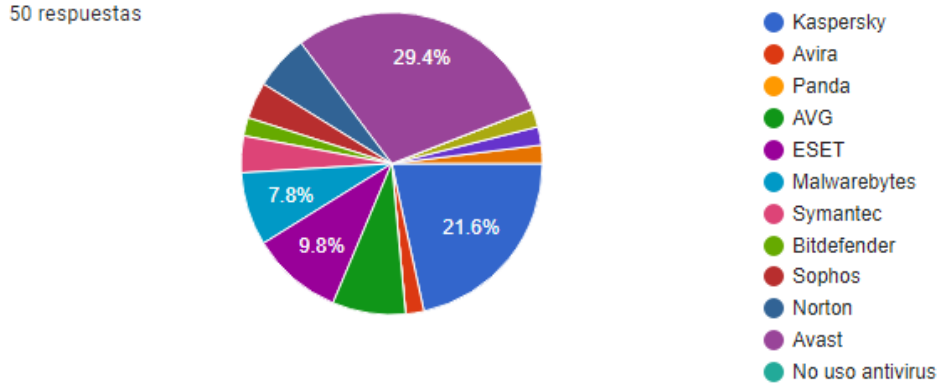


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 15

¿Cuál de estos antivirus tiene instalado en la mayoría de sus dispositivos?

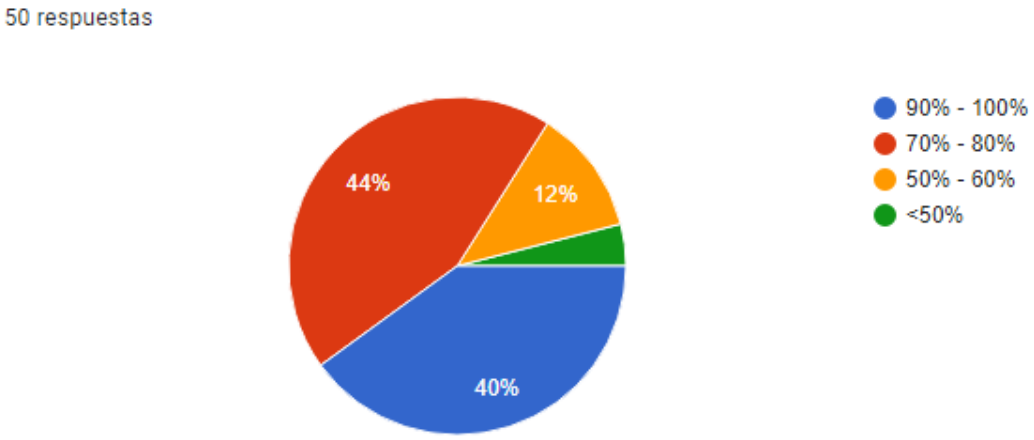


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 16

¿Qué tan confiable considera que es su antivirus?

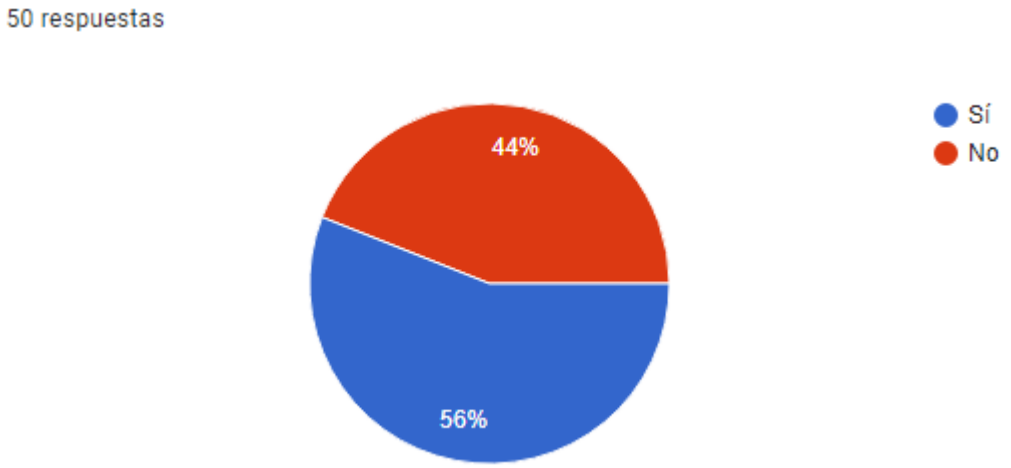


Fuente: Encuesta elaborada por autor

Responsable: Autor

Gráfico 17

¿Sabe cómo visualizar los recursos utilizados (monitor de rendimiento) en su computadora?



Fuente: Encuesta elaborada por autor

Responsable: Autor

Procesamiento y Análisis

La experimentación se llevó a cabo, como se mencionó anteriormente, en un ambiente aislado (virtualizado), con el fin de evitar la propagación del malware hacia la red física "real", previniendo así la reproducción de este malware dentro de los diversos dispositivos conectados a la red.

Figura 6

Instalación del sistema operativo dentro del ambiente virtualizado

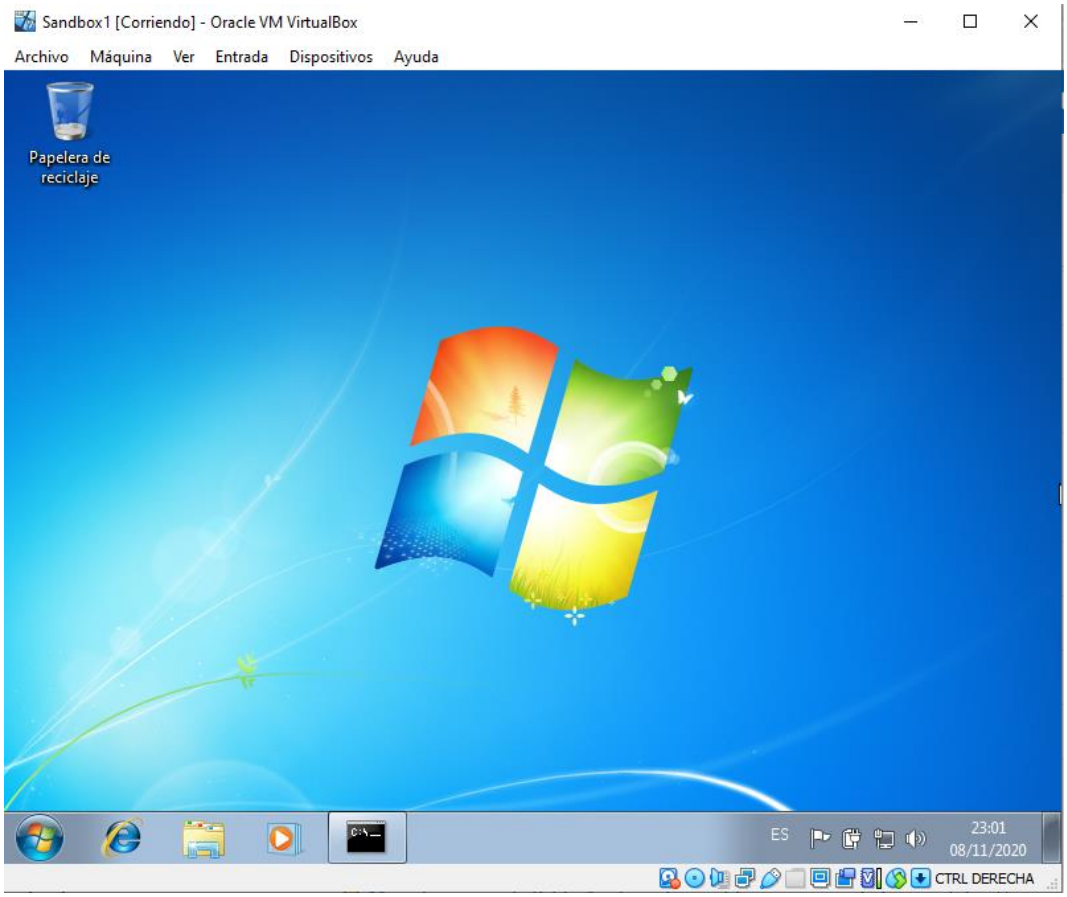
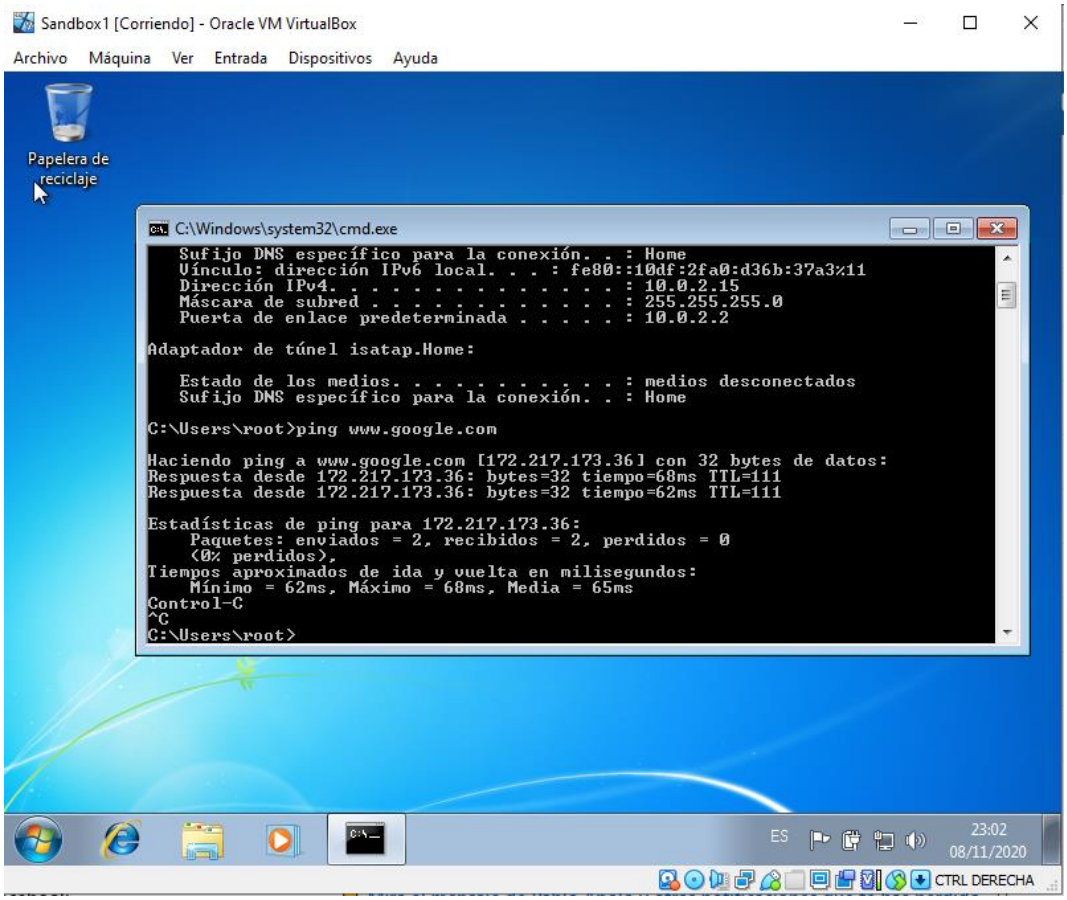


Figura 7

Prueba de conexión a Internet dentro del nuevo sistema operativo



Nota. La conexión a Internet es imprescindible para la correcta ejecución del malware, dado que este último necesita conectarse a un DNS, y luego, al servidor del atacante.

Figura 8

Descarga del malware desde any.run

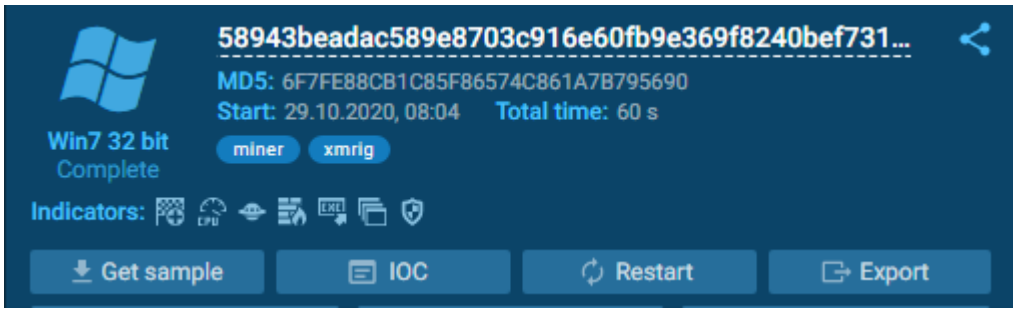


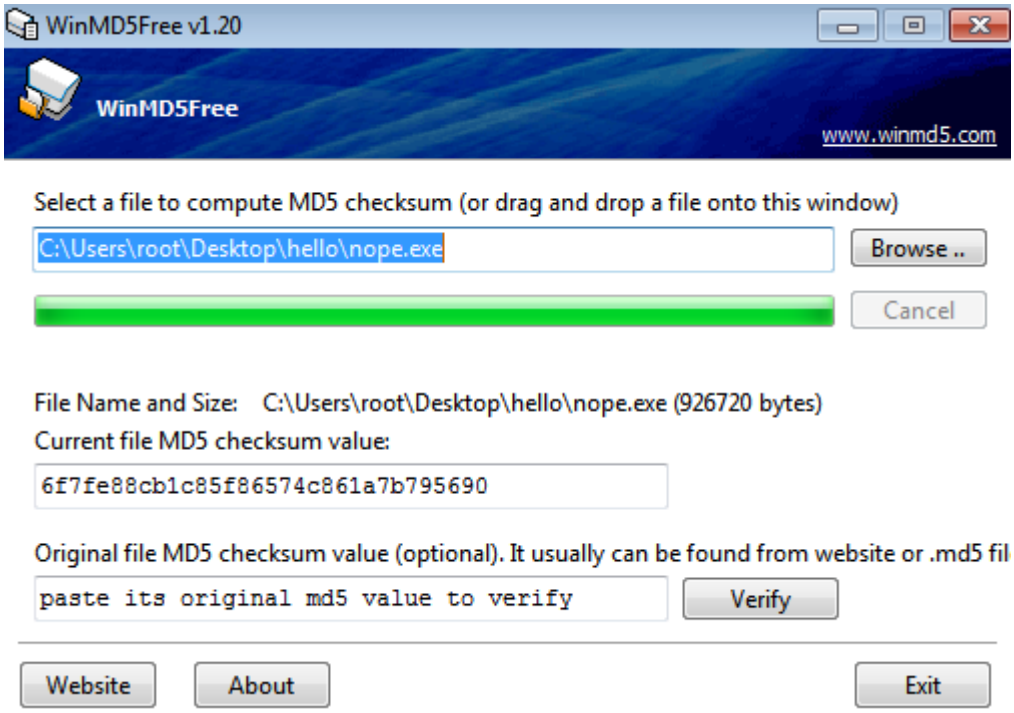
Figura 9

Instalación de herramientas para recolección de datos

Nota. Se instalaron varias herramientas, entre ellas: Process Monitor, Wireshark, WinMD5, PEiD, entre otras; así como también se muestra el malware descargado en formato .rar.

Figura 10

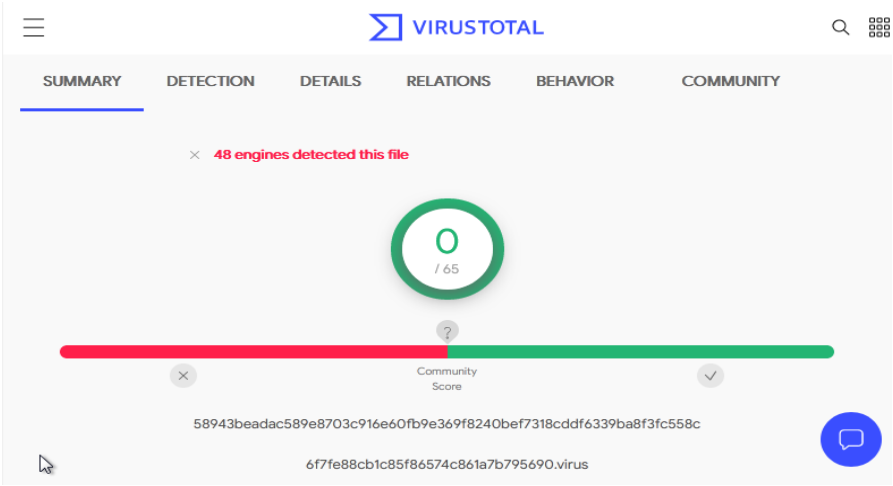
Análisis básico estático del malware por medio de WinMD5



Nota. Se obtiene el MD5 del malware que servirá para comprobar si ha sido reportado con anterioridad

Figura 11

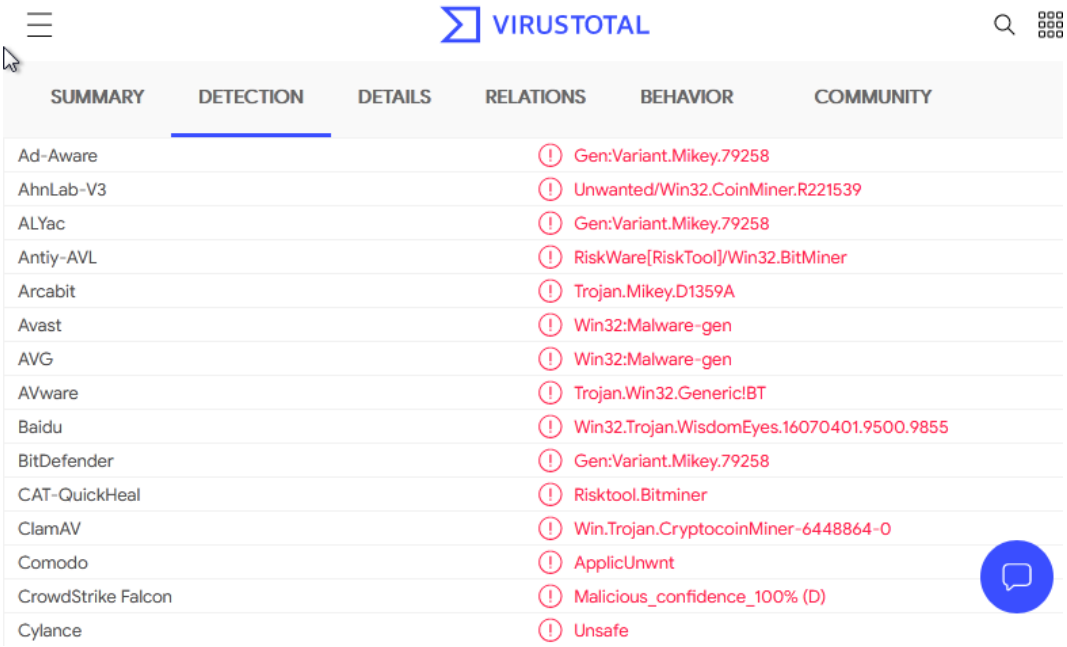
Escaneo de archivo en VirusTotal



Nota. El archivo ya fue reportado con anterioridad. Sin embargo, ninguno de los miembros del portal le dio una calificación negativa.

Figura 12

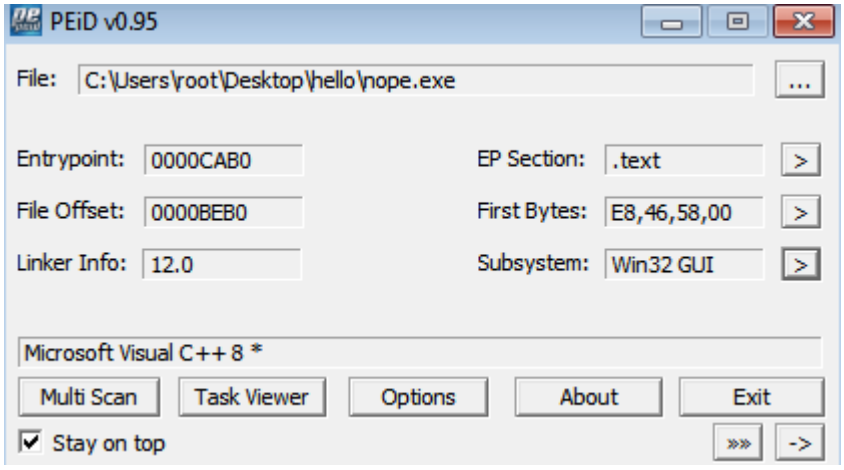
Análisis de los antimalware online dentro de VirusTotal



Nota. Se confirma gracias a los motores antivirus que la muestra de malware descargada es maliciosa.

Figura 13

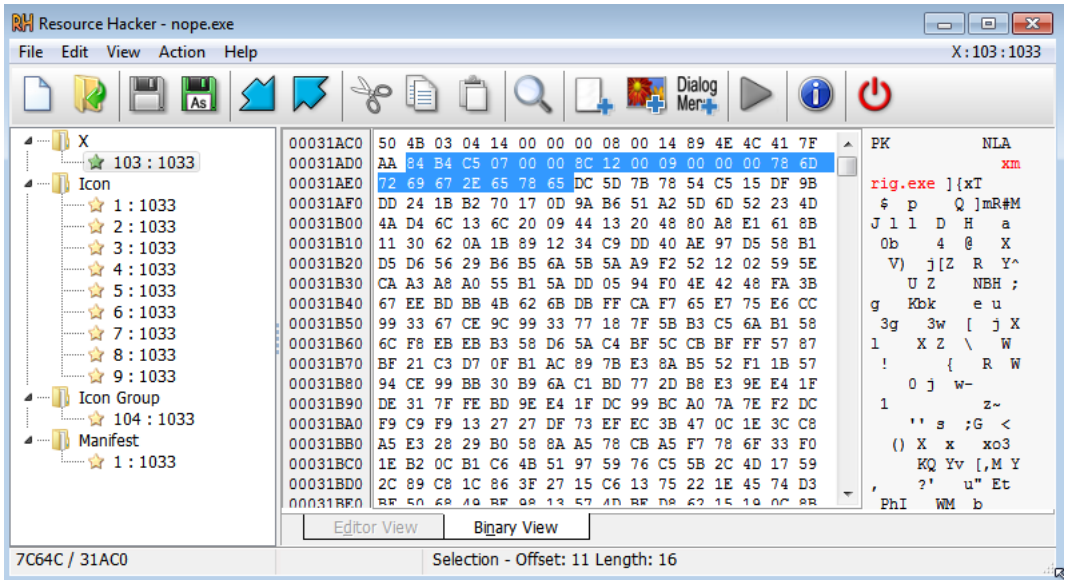
Escaneo del malware por medio de PEiD



Nota. La herramienta nos muestra que el archivo malicioso fue compilado en C++.

Figura 14

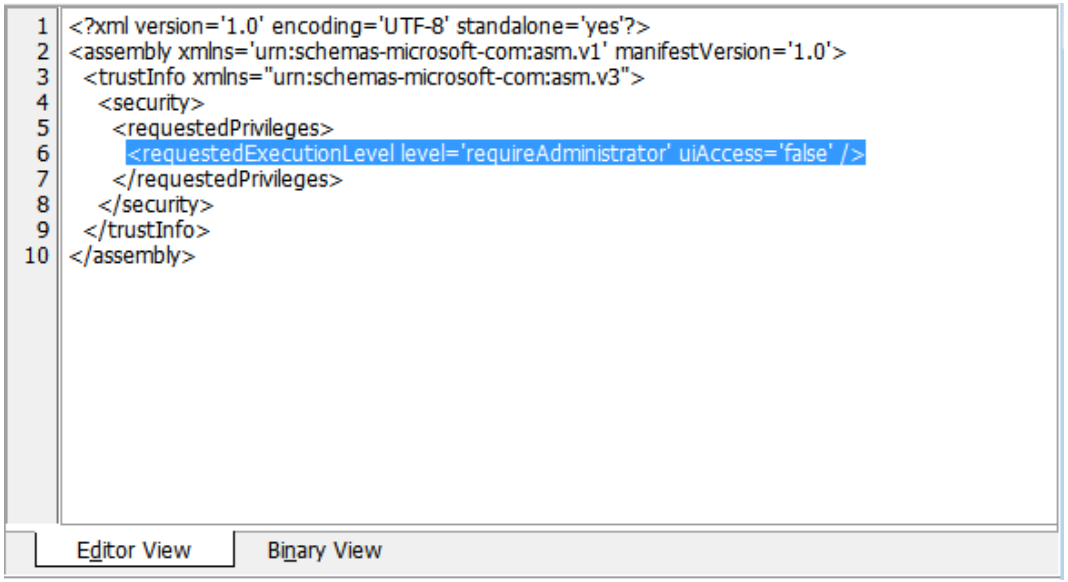
Escaneo del malware por medio de Resource Hacker



Nota. El escaneo del código revela que el malware es un ejecutable, llamado xmrig.exe.

Figura 15

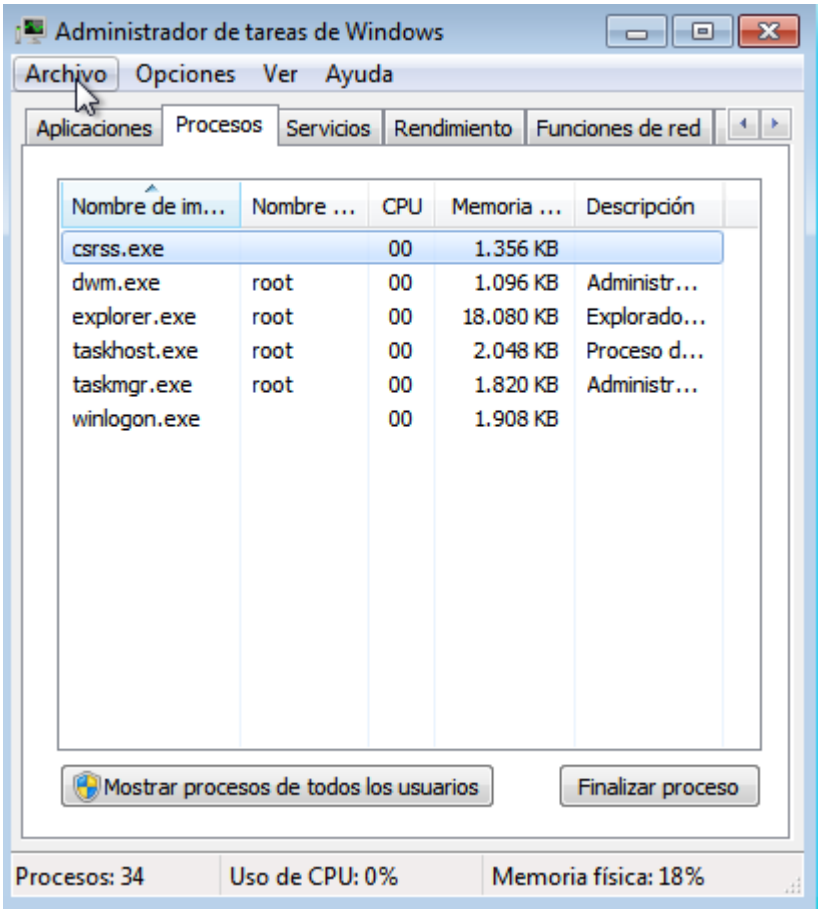
Nivel de privilegio de administrador durante ejecución del malware



El escaneo revela que el malware solicita y se ejecuta con permisos de administrador, probablemente para poder impedir el cierre de la aplicación.

Figura 16

Uso de recursos antes de ejecutar el malware

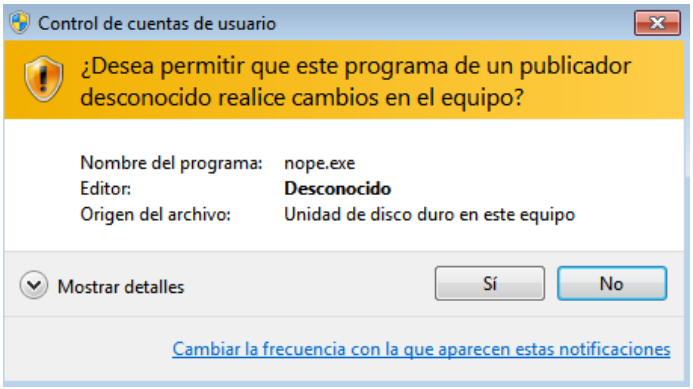


Nota. Se cerraron todas las aplicaciones antes de tomar la imagen.

Se puede constatar que, antes de ejecutar el malware, el uso de CPU era increíblemente bajo, con tan sólo 34 procesos siendo ejecutados y de 0% a 15% de uso.

Figura 17

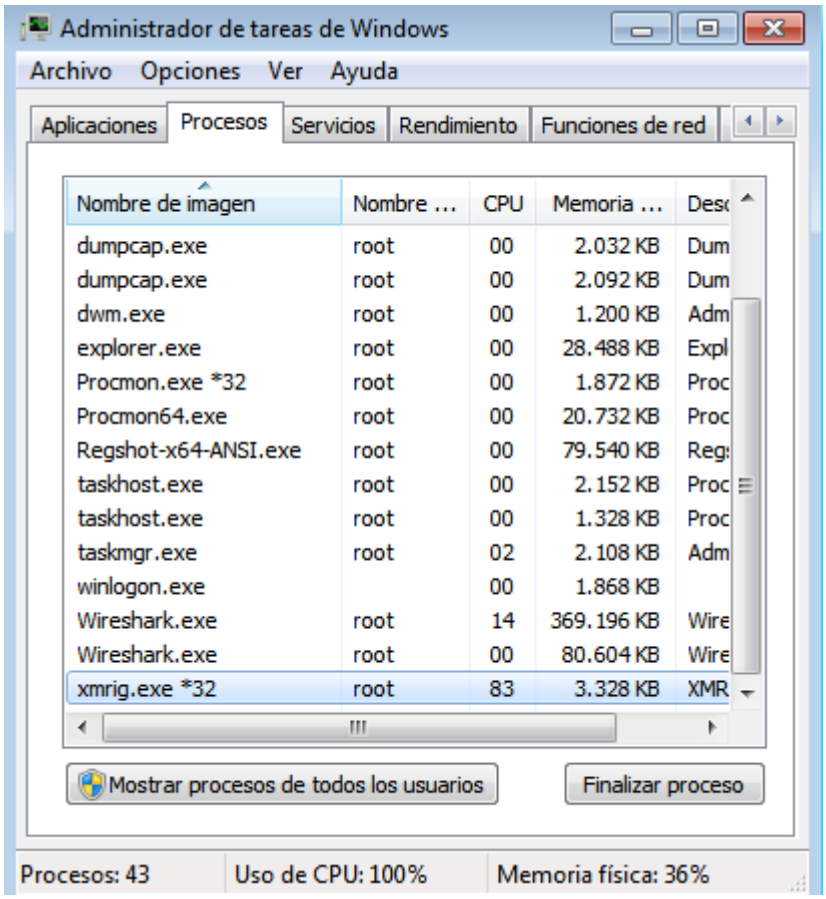
Ejecución del malware



Nota. Al ser un ambiente de pruebas, se renombró como “nope.exe”.

Figura 18

Uso de recursos después de ejecutar el malware

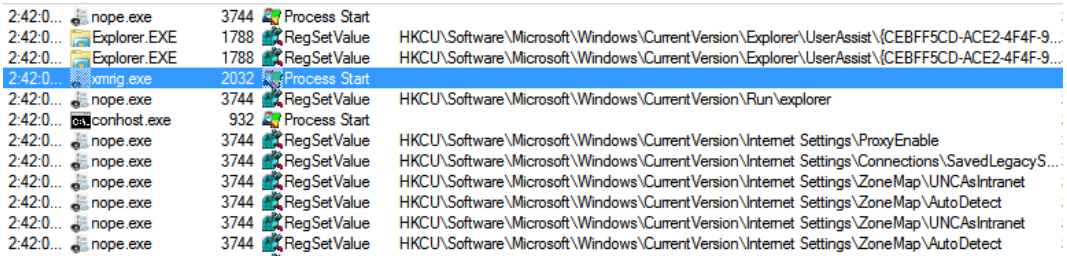


Nota. Se puede apreciar el proceso siendo ejecutado; el consumo de CPU es excesivo.

A pesar de estar ejecutando demás aplicaciones, estas no sobrepasaban el 20% de uso del CPU antes de ejecutar el malware.

Figura 19

Escaneo del sistema por medio de Process Monitor luego de ejecutar el malware

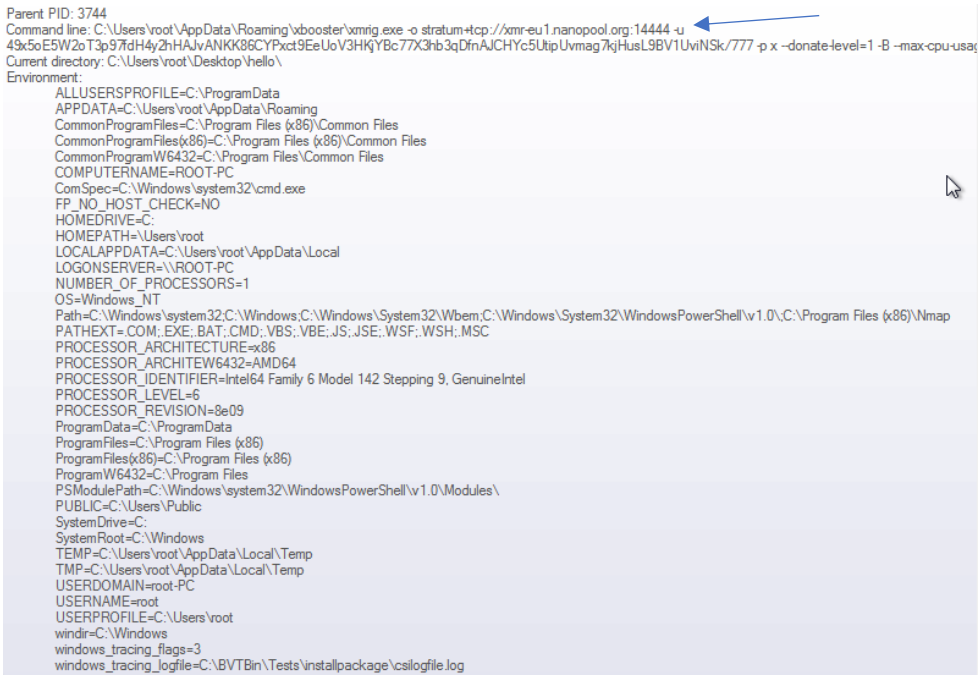


Nota. Se puede apreciar que luego de que el proceso “nope.exe” inicie, inmediatamente inicia el ejecutable empaquetado “xmrig.exe”, este último intenta conectarse a un servidor por medio de Internet, y logra hacerlo satisfactoriamente.

La línea de código que el malware utiliza se puede apreciar dentro del Process Monitor

Figura 20

Comandos de ejecución del malware



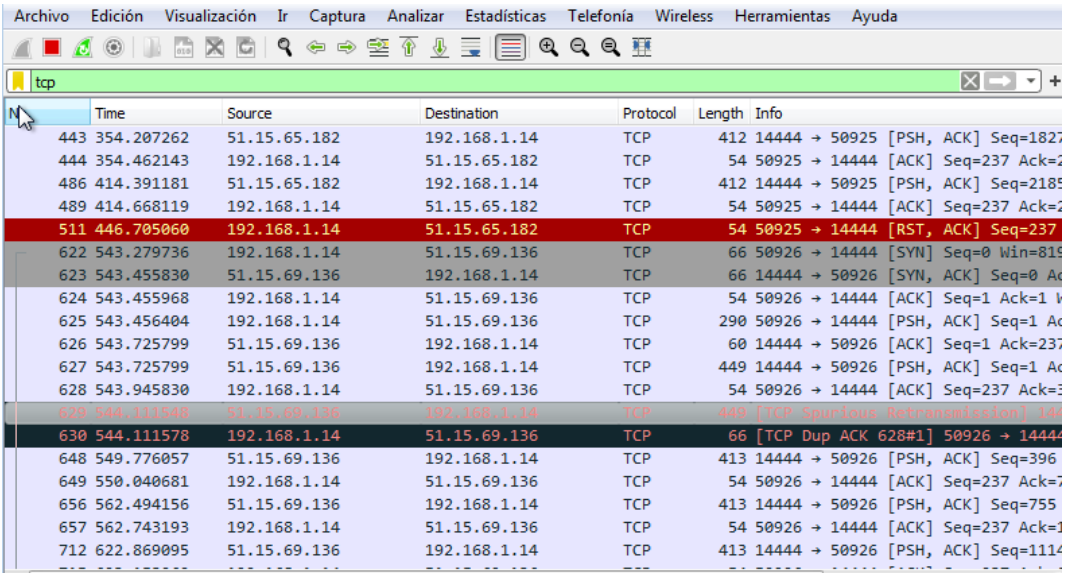
El comando de ejecución del malware es el siguiente:

```
"C:\Users\root\AppData\Roaming\xbooster\xmrig.exe -o
stratum+tcp://xmr-eu1.nanopool.org:14444 -u
49x5oE5W2oT3p97fdH4y2hHAJvANKK86CYPxct9EeUoV3HKjYBc77X3hb3qDfnAJCH
Yc5UtipUvmag7kjHusL9BV1UviNSk/777 -p x --donate-level=1 -B --max-
cpu-usage=90 -t 1"
```

Este comando de ejecución nos indica que se conecta a un *pool* de monero, por medio del puerto 14444; va a una billetera de monero; sigue un ciclo de 100 minutos en el cual se dedica a minar durante 99 minutos, y luego se pone en pausa durante 1 minuto. El uso máximo permitido por este malware es de 90%, su ciclo es infinito, y sólo puede ser detenido si logra ser eliminado.

Figura 21

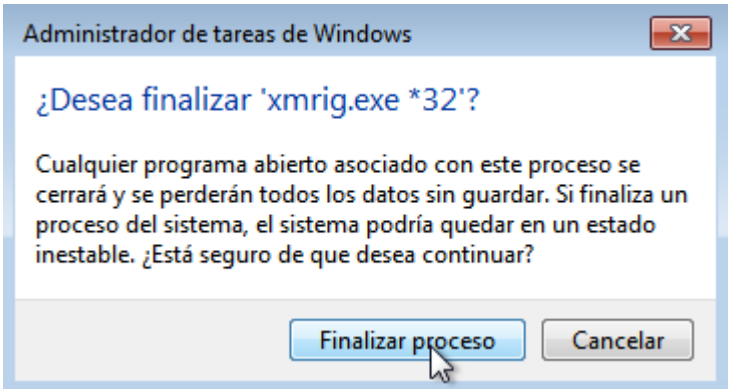
Escaneo de los paquetes de red por medio de Wireshark luego de la ejecución del malware



Nota. Se puede apreciar que el malware utiliza el protocolo TCP para comunicarse con distintos servidores.

Figura 22

Intento de finalizar el proceso por medio del administrador de tareas de Windows

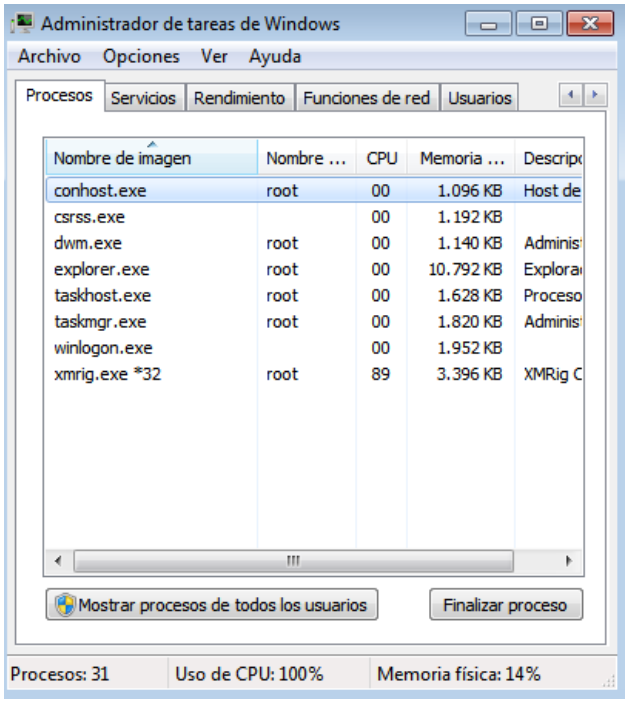


Nota. Es posible finalizar el proceso desde el administrador de tareas de Windows, siempre y cuando el usuario esté haya iniciado sesión con una cuenta de administrador.

Luego de finalizar el proceso, los valores del rendimiento del CPU vuelven a su estado original (oscilando entre 0% y 25% de uso). Se envía a reiniciar el equipo para cerciorarse de que el malware ya fue detenido.

Figura 23

Verificación del malware luego del reinicio

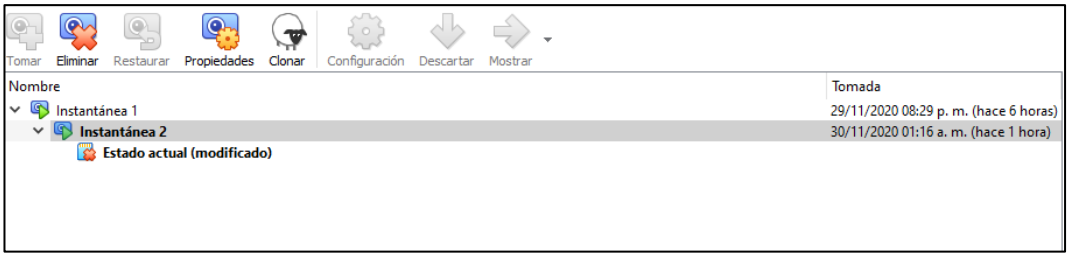


Se verificó que el reinicio no tuvo efecto alguno para eliminar el malware, al parecer las propiedades administrativas hacen que pueda volver a iniciarse junto con el arranque del sistema operativo.

Para poder solucionar el problema, fue necesario restaurar el sistema operativo desde un *snapshot* que se realizó antes de la ejecución del malware. Usar un antivirus no es posible en esta situación dado que este último impediría que el malware se comporte naturalmente, obstruyendo el objeto de este estudio.

Figura 24

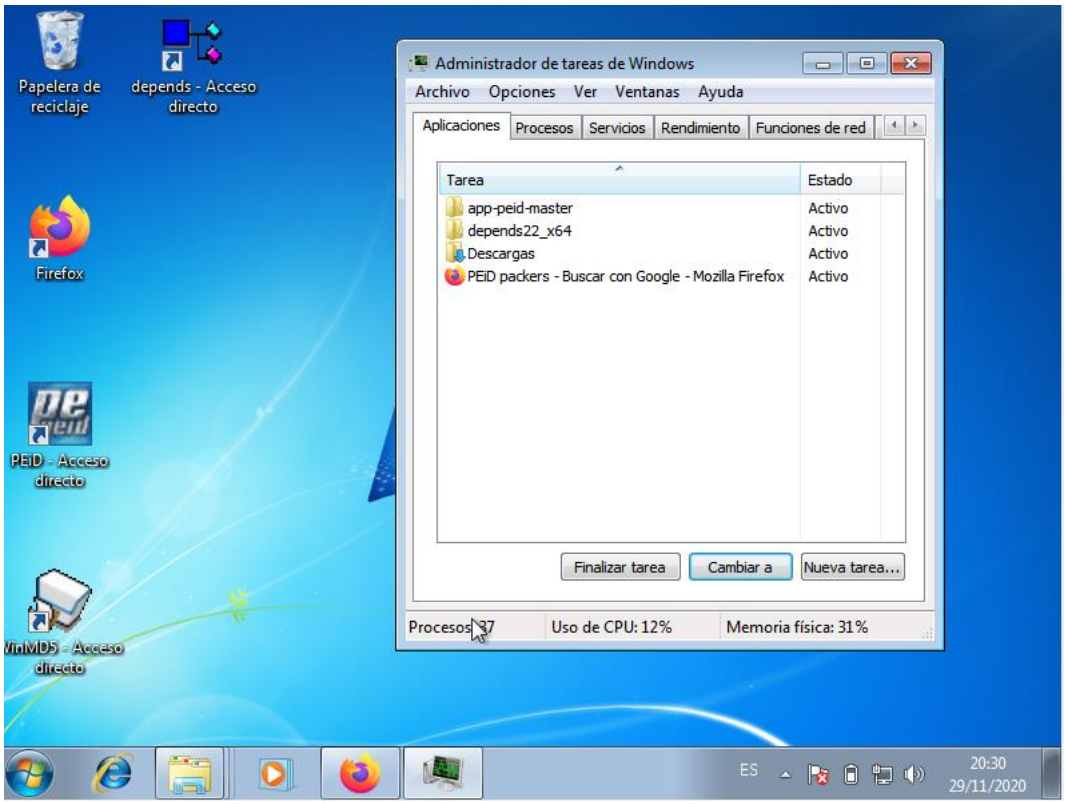
Restauración del sistema operativo a partir de una snapshot



Una vez restaurado el sistema operativo, proceso que no duró más de 2 minutos, se verificó el rendimiento de este último.

Figura 25

Uso de recursos luego de la restauración del sistema operativo por medio de un snapshot



Se pudo constatar que, luego de la restauración, no había ningún proceso en ejecución cuyo uso de CPU supere el 20% de consumo.

Validación de la Hipótesis

Luego de culminar el análisis del malware se pudo constatar que la ejecución de este archivo malicioso eleva abruptamente el uso de los recursos del sistema, ralentizando enormemente al terminal de cómputo. En este caso, el malware fue programado para consumir los recursos del CPU de la víctima (usualmente suelen consumir los recursos de las GPU), así como también tiene instrucciones de no sobrepasar el 90% de uso de CPU.

CAPÍTULO IV

PROPUESTA TECNOLÓGICA

Análisis de factibilidad

El presente trabajo investigativo resulta factible al poder ser empleado en práctica, dentro de un ambiente empresarial real.

Considerando los bajos costos de implementación, la facilidad de implementación en un ambiente laboral

La factibilidad consiste en definir las posibilidades de éxito que tendrá un proyecto propuesto. Al evaluar la factibilidad del sistema se realiza un "análisis técnico para determinar los efectos sobre el hardware y software existente y análisis operacional para medir el impacto de la aplicación sobre las operaciones de la organización

Factibilidad Operacional

La urgencia de implementar las medidas explicadas en este trabajo investigativo es grande, tomando en cuenta las infecciones y ataques realizados a individuos y empresas diariamente.

Al no considerarse como una medida de gran complejidad técnica, podrá ser adoptada por todo el personal informático de la institución.

Factibilidad Técnica

El análisis desarrollado en el capítulo anterior nos refleja que la solución es factible y viable; se puede entrenar y capacitar a las personas encargadas del área de sistemas para que puedan adoptar la medida de mayor efectividad, y al personal que no pertenece a esa área, pero que sí es de carácter informático, pueden implementar la medida de menor efectividad.

Factibilidad Legal

La investigación no viola o vulnera leyes vigentes establecidas dentro de la Constitución del Ecuador, y no podrá ser objeto de infracciones que podrían imposibilitar el ejecutar este trabajo investigativo en un ambiente empresarial.

Factibilidad Económica

El presente proyecto resulta factible económicamente dado que las herramientas utilizadas para realizar los diversos diagnósticos y análisis son *open-source* y *freeware;* no requieren de un pago de licencia para su uso, distribución, actualización o mantenimiento.

Etapas de la metodología del proyecto

Inicio.

La fase de inicio es crucial en el ciclo de vida del proyecto, ya que es el momento de definir el alcance y proceder a la selección de las herramientas adecuadas para la realización del análisis del malware. Previo a esto, se investigaron las causas, consecuencias, y vigencias de la problemática para constatar que se trata de una problemática vigente.

Planificación.

Esta es a menudo la fase más difícil para un director de proyecto, ya que tiene que hacer un importante esfuerzo de abstracción para calcular las necesidades de personal, recursos y equipo que habrán de preverse para lograr la consecución a tiempo y dentro de los parámetros previstos. Se planificó y creó un conjunto completo de planes de proyecto que establecen una clara hoja de ruta.

Ejecución

En base a la planificación, habrá que completar las actividades programadas, con sus tareas, y proceder a la entrega de los productos intermedios. Es importante

velar por una buena comunicación en esta fase para garantizar un mayor control sobre el progreso y los plazos.

Entregables del proyecto

Tabla 4

Entregables del proyecto

N.	Nombre	Descripción	Origen
1	Acciones Correctivas	-En la actualidad, los cibercriminales han adaptado estrategias para monetizar el uso de un sistema con poca o nula supervisión; aprovechando la poca seguridad, acceden al sistema y logran monetizar, aprovechándose de los recursos del sistema para realizar la criptominería ilegal. - La solución a la problemática previamente expuesta es simple; se debe brindar las herramientas al personal informático de la empresa para que puedan ejecutar el monitoreo. Al personal no informático, pero con acceso a un terminal de cómputo se lo debe ilustrar mediante entrenamientos para evitar la propagación del malware dentro de la empresa.	Gestión del Proyecto

2	Componente de Software	El conjunto de herramientas de código abierto utilizadas durante la ejecución de este trabajo investigativo, así como también en la ejecución del código malicioso y el posterior estudio de sus partes individuales será utilizado por el personal encargado para el monitoreo de la empresa.	Implementación de Software
3	Configuración de Software	El conjunto de software de código abierto utilizado en este trabajo puede ser adaptado, tomando en consideración las necesidades de la empresa y el nivel de formación del personal encargado.	Implementación de Software

Criterios de validación de la propuesta

Este contexto se plantea con los siguientes objetivos, que se derivan de forma lógica del desarrollo de la tesis hasta el momento:

- *Validar* el carácter práctico de la propuesta mediante el análisis de su comportamiento a través del ensayo de su funcionamiento mediante diversos casos de aplicación.
- *Glosar* mediante ejemplos prácticos las ideas contenidas a lo largo de la tesis para facilitar su comprensión y la estimación de su alcance

Las características a verificar

De los capítulos anteriores de esta tesis, pueden extraerse tres rasgos principales de la propuesta, en los que se ha hecho énfasis en repetidas ocasiones:

- *Potencialidad*: capacidad de analizar el problema y de afinar en la estimación
- *Aplicabilidad*: capacidad de ser aplicada en los diferentes contextos descritos
- *Flexibilidad*: capacidad de adaptación según el grado de simplificación que se desee

Criterios de aceptación del Producto o Servicio

Los criterios de aceptación son definidos por el encargado del proyecto; estos criterios describen los requisitos que el producto debe cumplir para estar terminado.

En el caso de este proyecto, los criterios de aceptación se pueden englobar de esta manera:

- Un trabajador de la empresa abre un correo de un remitente desconocido, este correo poseía cryptomalware oculto en su contenido
- El sistema logra detectar que existe una petición hacia un servidor desconocido desde el terminal infectado
- El sistema evita que el malware ya insertado en el terminal siga ejecutándose, mitigando así su propagación por la red
- El encargado estudia los vectores de infección del malware

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Una criptomoneda es una moneda digital o virtual que está protegida por criptografía, lo que hace que sea casi imposible falsificarla o gastarla dos veces. Muchas criptomonedas son redes descentralizadas basadas en la tecnología *blockchain*, un libro mayor distribuido reforzado por una red dispar de computadoras. Una característica definitoria de las criptomonedas es que generalmente no son emitidas por ninguna autoridad central, lo que las hace teóricamente inmunes a la interferencia o manipulación del gobierno (Sonnenshein, 2020).

Este proyecto de investigación tiene como objetivo consolidar y ampliar el cuerpo de conocimientos para esta amenaza creciente y ofrecen recomendaciones para la detección de malware de criptominería. El análisis realizado en esta investigación combinó la literatura existente para 1 variedad de malware de criptominería, y examinó lo siguiente: (a) cómo las víctimas suelen ser atacadas e infectadas con malware de criptominería, y (b) técnicas detectables utilizadas por malware de criptominería. Además de la literatura existente, se realizaron pruebas para determinar el impacto del software de criptominería en la CPU de un sistema. La información recopilada fue sintetizado y utilizado para recomendar dos estrategias de detección de alto nivel.

Teniendo en cuenta todos estos factores, las recomendaciones implicaron tres aspectos del seguimiento: (a) monitoreo basado en el sistema, (b) monitoreo de la utilización de la CPU y (c) monitoreo basado en la red. Un enfoque óptimo sería agregar los eventos o alertas producidos por las herramientas de monitoreo y correlacionar las características de uso de actividades del proceso, la red y los eventos de la CPU. Un enfoque no tan óptimo incluiría capacidades de monitoreo parcial o total sin correlación.

Recomendaciones

La información presentada en esta investigación destaca algunas de las técnicas utilizadas y acciones llevadas a cabo por malware de criptominería. Las técnicas identificadas se extrajeron de análisis con análisis adicional realizado, cuando sea posible, para llenar los vacíos en la información existente.

Las pruebas descritas en la sección Procesamiento y análisis mostraron el impacto potencial de la criptominería y las aplicaciones empleadas por malware tienen un sistema infectado. Los resultados de las pruebas en la investigación destacan un impacto distinguible en la utilización de la CPU del sistema de prueba, la información extraída de la literatura, y los resultados de las pruebas descritas en la investigación.

Alfa **(α)**. Alternativa óptima

Un enfoque óptimo para detectar criptomineros maliciosos debe incluir tanto el sistema como seguimiento de la actividad de la red. Los datos de los eventos del sistema o los datos de alerta en el caso de una alteración en la seguridad, deben ser

rastreable hasta la fuente de datos, contener información temporal que se puede utilizar para crear una línea de tiempo y ser accesible a través de una plataforma de búsqueda capaz de unificar los eventos para proporcionar una visión holística del entorno supervisado.

Monitoreo basado en sistema. Gran parte de la información extraída del análisis existente destaca que el malware de criptominería causa varios cambios en el sistema. Ejemplos de estos cambios incluyen:

- la creación de archivos, por ejemplo, la escritura de un criptominer y la configuración de soporte archivos en el disco o escribiendo malware en la carpeta de inicio de Windows para su persistencia;
- la creación de procesos, por ejemplo, cuando el malware ejecuta el criptominer;
- la creación de conexiones de red, por ejemplo, cuando los troyanos logran comunicarse con servidores C2 o servidores de carga útil.

Utilización del CPU. Otro cambio en el sistema que se destaca en la investigación fue el impacto las aplicaciones de criptominería que tienen en la utilización de la CPU. Los resultados de las pruebas descritas en los métodos de investigación muestran un alto uso de la CPU cuando las aplicaciones de criptominería realizan operaciones mineras. Varias aplicaciones de monitoreo del sistema pueden alertar e informar cuando el uso de la CPU supera un umbral definido por el usuario. Un enfoque para realizar esto, usando aplicaciones nativas de Windows, implican el

uso de Performance Monitor de Microsoft y Process Monitor, también de Microsoft.

Monitoreo basado en red. El monitoreo de la red proporciona otra fuente de datos útil para detectar malware de criptominería. Todo el malware de criptominería mencionado en la literatura involucró actividad de red, ya sea malware de criptominería que se comunica con servidores C2 o aplicaciones de criptominería descargadas que se conectan a grupos de minería Un enfoque de monitoreo de red óptimo debe tener visibilidad del tráfico cruzar la frontera de Internet y la capacidad de rastrear las comunicaciones a un sistema específico.

Además, las operaciones de monitoreo de la red implicarían recopilar lo siguiente:

- datos de flujo que contienen detalles del protocolo, por ejemplo, datos de encabezado HTTP, pregunta de DNS y datos de respuesta;
- datos de captura de paquetes (PCAP) para respaldar la investigación adicional y proporcionar contexto para los datos de flujo recopilados.

Beta (**β).** Un enfoque menos óptimo

Un enfoque menos óptimo para detectar malware de criptominería se limitaría a uno o más fuentes de seguimiento que no están correlacionadas. Este enfoque de detección puede depender únicamente de un producto de seguridad de punto final que utiliza un enfoque de firma, heurístico o predictivo, pero sin incluir la utilización de la CPU del sistema o la información detallada de la red. Un ejemplo sería la detección de un artefacto conocido del troyano Bondnet, pero con la

detección perdida de su componente de criptominería recién compilado. La oportunidad perdida en el ejemplo anterior puede haberse detectado correlacionando la utilización de CPU del criptominero y el tráfico de red causado por el intento de conexión hacia los servidores.

Alternativamente, un enfoque de detección puede depender únicamente de un firewall de red o de un sistema de detección y prevención de intrusos. Usar únicamente el monitoreo basado en red puede detectar comunicaciones realizadas mediante criptominería de malware a infraestructura maliciosa o grupos de minería; sin embargo, si el proceso de comunicación con la infraestructura y el sistema cambia al binario, el proceso se perderá.

Si la supervisión del sistema, la red y el CPU se realizan sin agregación ni correlación, podrán ocurrir alertas o eventos individuales, pero serán difíciles de clasificar dado que los datos están dispersos y las líneas de tiempo deberán crearse manualmente. Además, en entornos mayores, puede llegar a ser insostenible investigar los eventos o alertas debido al volumen de actividad aparentemente independiente. Si bien este enfoque para detectar malware de criptominería es considerado menos óptimo, es mejor tener algunas capacidades de detección que ninguna capacidad.

BIBLIOGRAFÍA

Agrawal, H. (21 de agosto de 2020). *9 Anonymous Cryptocurrencies You Should Know About*. Obtenido de Coinsutra: https://coinsutra.com/anonymous-cryptocurrencies/

Barwise, M. (9 de septiembre de 2010). *WebWise*. Obtenido de BBC: http://www.bbc.co.uk/webwise/guides/internet-worms

Bekerman, D. (26 de octubre de 2016). *Breaking Down Mirai: An IoT DDoS Botnet Analysis.* Obtenido de Imperva: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

Buterin, V. (06 de febrero de 2017). *Vitalik Buterin*. Obtenido de Medium: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Código Orgánico Integral Penal. (05 de febrero de 2018). *Ministerio de Defensa.* Obtenido de Código Orgánico Integral Penal: https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

CoinLore. (2020). *Top 100 Coins*. Obtenido de CoinLore: https://www.coinlore.com/coins

Dominguez, K. (4 de septiembre de 2011). *Bitcoin Mining Botnet Found with DDoS Capabilities*. Obtenido de TrendMicro: https://blog.trendmicro.com/trendlabs-security-intelligence/bitcoin-mining-botnet-found-with-ddos-capabilities/

Driscoll, S. (14 de julio de 2013). *How Bitcoin Works Under the Hood*. Obtenido de Imponderable Things: http://www.imponderablethings.com/2013/07/how-bitcoin-works-underhood.

Gekkoin. (s.f.). *Monero: the first anonymous cryptocurrency*. Obtenido de Gekkoin: https://gekkoin.com/blog/monero_the_first_anonymous_cryptocurrency

Greenberg, A. (20 de abril de 2011). *Crypto Currency*. Obtenido de Forbes: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html?sh=968cbaa353ee

Gupta, S. (5 de Marzo de 2020). *Cryptocurrency Volatility – A Friend Or A Foe*. Obtenido de AiThority: https://aithority.com/guest-authors/cryptocurrency-volatility-a-friend-or-a-foe/

Kaspersky. (2019). *How to protect your business from the increasing risks of cryptojacking*. Obtenido de Kaspersky: https://www.kaspersky.com/blog/secure-futures-magazine/cryptojacking-2019/28951/

Kaspersky. (s.f.). *Malware-as-a-service (MaaS)*. Obtenido de Kaspersky IT Encyclopedia: https://encyclopedia.kaspersky.com/glossary/malware-as-a-service-maas/

Kessem. (24 de abril de 2017). *The Necurs Botnet: A Pandora's Box of Malicious Spam*. Obtenido de Securityintelligence: https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

Lansky, J. (enero de 2018). *Possible State Approaches to Cryptocurrencies*. Obtenido de Journal of Systems: https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies

Lurye, S. (17 de septiembre de 2019). *Assessing the impact of protection from web miners*. Obtenido de SecureList: https://securelist.com/electricity-and-mining/93292/

Makadiya, P. (3 de abril de 2018). *Cryptocurrency Market Down 54% in Q1 2018, Losses Top $500 Billion*. Obtenido de CryptoGlobe: https://www.cryptoglobe.com/latest/2018/04/crypto-market-down-q1-2018/

Malwarebytes. (9 de junio de 2016). *MalwarebytesLabs*. Obtenido de Remote Access Trojan (RAT): https://blog.malwarebytes.com/threats/remote-access-trojan-rat/

Manos Antonakakis, T. A. (17 de agosto de 2017). *Usenix.* Obtenido de Usenix: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

Marria, V. (4 de febrero de 2019). *How Cryptocurrencies Are Empowering Cybercriminals*. Obtenido de Forbes: https://www.forbes.com/sites/vishalmarria/2019/02/04/how-cryptocurrencies-are-empowering-cybercriminals/?sh=2766a45c37c5

Michael Sikorski, A. H. (2012). *Practical Malware Analysis.* San Francisco: William Pollock.

MITRE. (17 de octubre de 2018). *Command and Control*. Obtenido de MITRE ATT&CK: https://attack.mitre.org/tactics/TA0011/

MITRE. (2020). *MAEC Overview*. Obtenido de MAEC : http://maecproject.github.io/documentation/overview/

Moffitt. (16 de octubre de 2016). *Webroot Threat Blog*. Obtenido de Source Code for Mirai IoT Malware Released: https://www.webroot.com/blog/2016/10/10/source-code-mirai-iot-malware-released/

Moreno. (31 de marzo de 2016). *Malware as a Service: As Easy As It Gets*. Obtenido de WebRoot: https://www.webroot.com/blog/2016/03/31/malware-service-easy-gets/

Nadeau, M. (9 de julio de 2020). *CSO*. Obtenido de CSOonline: https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

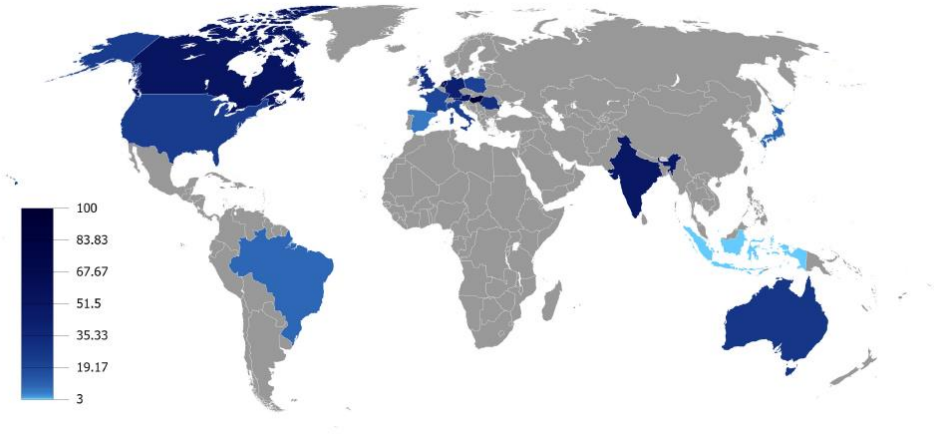
Saad, e. a. (6 de septiembre de 2018). *End-to-End Analysis of In-Browser Cryptojacking.* Obtenido de arxiv.org: https://arxiv.org/pdf/1809.02152.pdf

Sonnenshein, M. (5 de mayo de 2020). *Cryptocurrency*. Obtenido de Investopedia: https://www.investopedia.com/terms/c/cryptocurrency.asp

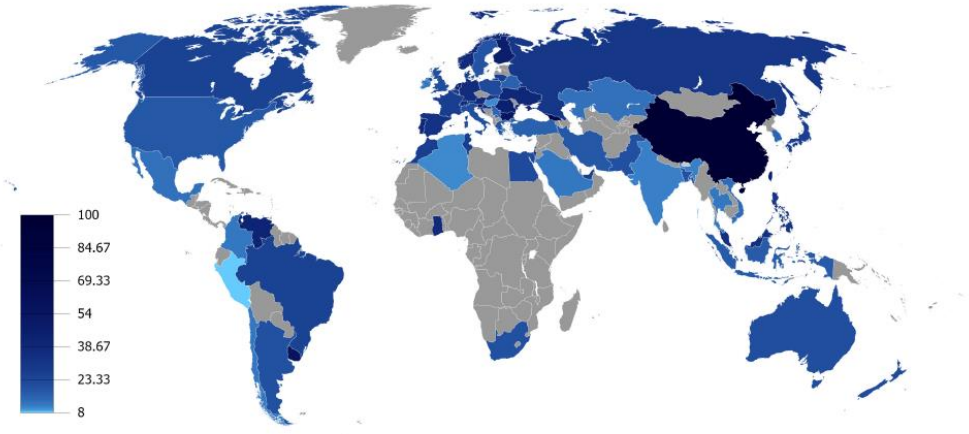
TrendMicro. (2020). *Botnet*. Obtenido de TrendMicro: https://www.trendmicro.com/vinfo/us/security/definition/botnet

ANEXOS

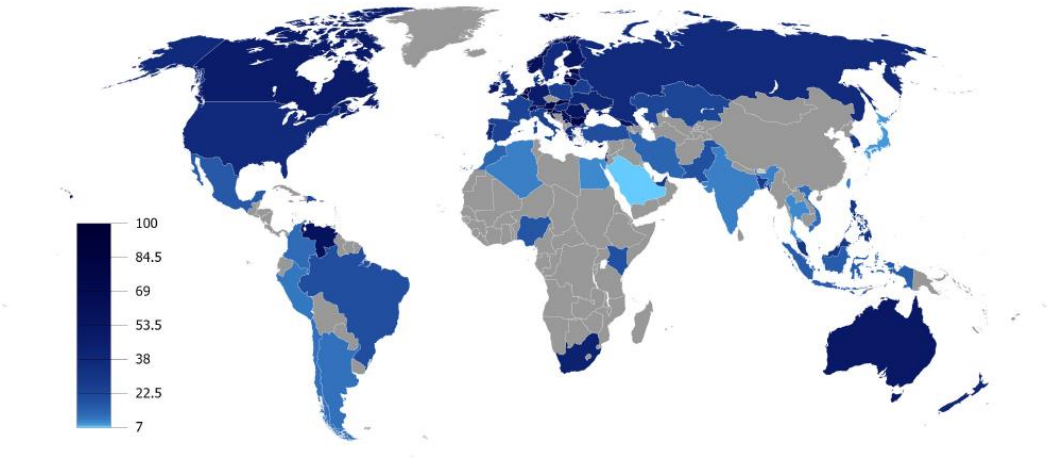
Anexo 1.1 Distribución mundial de búsqueda del término "*Cryptojacking*" en Google



Anexo 1.2 Distribución mundial de búsqueda del término "*Coinhive*" en Google



Anexo 1.3 Distribución mundial de búsqueda del término “Monero” en Google



Anexo 1.4 Distribución de sitios web de cryptojacking en relación al TLD

Rango	TLD	Tipo	Sitios	%Sitios
1	.com	genérico	1945	34.1%
2	.net	genérico	359	6.2%
3	.si	país	358	6.2%
4	.online	genérico	349	6.1%
5	.ru	país	242	4.2%
6	.org	genérico	191	3.3%
7	.sk	país	169	2.9%
8	.info	genérico	169	2.9%
9	.br	país	157	2.7%
10	.site	nuevo	116	2.0%
11	otros	-	1648	28.8%
Total	-	-	5703	100%

Anexo 1.5 Historia de usuario y Criterio de aceptación

Enunciado de la historia				**Criterios de aceptación**			
Rol	**Característica / Funcionalidad**	**Razón / Resultado**	**Número (#) de escenario**	**Criterio de aceptación (Título)**	**Contexto**	**Evento**	**Resultado / Comportamiento esperado**
Como un gerente de compañía	Necesito tener un software de monitoreo que evite ser víctima del cryptojacking	Con la finalidad de evitar pérdidas monetarias a mi compañía	1	Usuario no experimentado	En caso que un usuario no experimentado	ejecute cryptomalware	el sistema prevendrá la propagación del malware

Anexo 1.6 Muestras tomadas de la base de malware

Cat.	Platforms	M	M_d	B	D	E	c_l	T	η	V	η_1	n_1	η_2	n_2	params	sloc	physical	M_s
Cryptojacking	deepMiner	184	44.2	14.1	113.0	4,810,434	4,667	267,246	554	42,533	47	2,440	507	2,227	75	416	499	67.8
	Authedmine	168	26.5	19.7	82.8	4,912,255	6,096	272,903	844	59,259	41	3,247	803	2,849	73	633	784	62.8
	Hashing	138	29.1	7.2	94.6	2,185,379	2,794	124,138	342	24,393	38	1,469	315	1,415	37	412	505	68.2
	Miner	133	27.7	9.3	90.5	2,537,930	3,239	140,996	403	28,032	39	1,690	364	1,549	49	479	617	64.1
	Coinhive	131	27.5	9.1	94.8	2,608,021	3,226	144,890	368	274,970	37	1,697	331	1,529	48	476	594	63.7
	Crypto-loot	128	39.7	11.4	88.1	3,034,935	3,788	168,607	546	34,443	45	1,962	501	1,826	62	322	389	70.3
	Freecontent	117	28.3	8.1	89.4	2,180,394	2,884	121,133	350	24,373	38	1,469	312	1,415	37	412	505	62.7
	JSEcoin	64	17.2	10.2	62.9	1,945,165	3,257	108,064	716	30,888	45	1,878	671	1,379	49	372	412	64.7
	Mean (μ)	130.3	29.9	11.3	88.9	3,026,191	3,755.1	168,121	516.4	33,925	41.3	1,981.5	475.1	1,773.6	53.8	440.3	538.1	64.9
	SD. (σ)	35.9	8.4	3.9	13.8	1,180,403	1,109.9	65,577	185.1	11,856	3.9	599.3	182.8	519.3	14.8	93.2	126.3	2.8
Malicious	20160209	92	21.5	5.6	25.1	423,925	1,833	23,551	580	16,826	27	1,032	553	801	22	427	503	44.4
	20161126	62	15.3	4.2	24.6	315,735	1,563	17,540	292	12,800	17	798	275	765	0	403	481	90.5
	20170110	14	4.4	15.0	26.7	1,211,305	4,704	67,294	782	45,210	15	2,740	767	1,964	232	313	564	93.6
	20170507	6	24.0	5.9	11.1	199,917	1,864	11,106	777	17,897	18	942	759	922	1	25	890	71.7
	20160927	3	1.4	4.0	32.5	393,555	1,575	21,864	204	12,084	13	957	191	618	0	213	98	23.2
	20170322	2	18.1	11.8	7.1	253,442	3,514	14,080	1,123	35,607	9	1,762	1,114	1,752	3	11	1,738	90.9
	20170303	2	8.6	0.2	9.4	8,338	147	463	63	878	13	73	50	74	4	23	55	78.7
	20160407	1	33.3	0.1	2.7	207	19	11	16	76	5	12	11	7	0	3	3	78.9
	20170501	1	0.9	2.1	3.3	21,464	758	1,192	322	6,314	5	431	317	327	0	105	105	35.9
	20160810	1	12.5	0.5	11.9	20,148	275	1,119	70	1,685	6	255	64	20	0	8	13	60.4
	Mean (μ)	18.4	14	4.9	15.5	284,803.7	1,625.2	15,822	422.9	14,938	12.8	900.2	410.1	725	26.2	153.1	445	66.9
	SD. (σ)	31.9	10.5	5	10.8	364,470.8	1,508.9	20,248	374.8	15,045	6.9	834.7	372.5	686.6	72.6	171.9	543.5	24.9
Benign	The Boat	2,135	69.3	110.8	392.0	130,285,522	31,916	7,238,084	1,364	332,361	59	17,341	1,305	14,575	852	3,084	3,349	66.7
	IBM Design	2,119	68.3	110.9	397.1	132,237,213	32,018	7,346,511	1,351	332,981	59	17,393	1,292	1,4625	853	3,103	3,372	66.7
	Histography	1,743	40.7	95.2	249.5	71,325,242	26,627	3,962,513	1,704	285,833	55	14,963	1,649	11,663	803	4,278	5,043	59.4
	Know Lupus	1,006	28.1	92.9	170.4	47,474,425	25,120	2,637,468	2,181	278,600	54	13,424	2,127	11,696	615	3,583	4,288	65.2
	tota11y	815	38.8	59.4	227.7	40,563,065	17,486	2,253,503	1,167	178,157	52	9,764	1,115	7,722	412	2,099	2,336	62.9
	Masi Tupungato	784	58.2	47.1	185.0	26,199,193	14,296	1,455,510	958	141,585	43	7,875	915	6,421	238	1,347	1,470	67.2
	Fillipo	703	42.9	43.1	194.3	25,139,766	12,900	1,396,653	1,045	129,377	54	7,132	991	5,768	269	1,637	1,770	61.5
	Leg Work	412	75.7	34.0	241.3	24,651,056	11,100	1,369,503	589	102,143	45	5,835	544	5,265	66	544	633	65.9
	Code Conf	409	27.8	41.1	197.1	24,336,420	12,500	1,352,023	939	123,437	49	7,162	890	5,338	315	1,469	1,753	64.9
	Louis Browns	368	35.6	21.2	106.7	6,792,400	6,529	377,355	862	63,667	51	3,393	811	3,136	68	1,034	1,357	53.3
	Mean (μ)	1,049.4	48.5	65.6	236.1	52,900,430	19,049.2	2,938,912	1,216	196,814	52.1	10,428.2	1,163.9	8,621	449.1	2,217.8	2,537.1	63.4
	SD. (σ)	694	17.8	33.6	92.8	44,755,377	9,151.2	2,486,409	459.8	100,856	5.3	4,999	456.7	4,165	310.3	1,225.4	1,418.2	4.3