IDENTIFICACIÓN DE HERRAMIENTAS PARA PREVENIR EL CRYPTOJACKING. UNA APROXIMACIÓN DE LITERATURA DESDE EL CASO DE COLOMBIA

IDENTIFICATION OF TOOLS TO PREVENT CRYPTOJACKING. AN APPROXIMATION OF LITERATURE FROM THE CASE OF COLOMBIA

John Edward Rueda Castañeda[1]
Jerson Samuel Tello[2]
Edward Estanling Cárdenas[3]
Vanessa García Pineda[4]

Fecha de recepción: 11/03/2023
Fecha de aprobación: 12/06/2023
***DOI:** https://doi.org/10.26495/re.v7i1.2438*

RESUMEN

La criptografía es un método utilizado para proteger la confidencialidad, integridad y autenticidad de los datos en tránsito o almacenados en servidores. Sin embargo, si se configura incorrectamente, puede ser vulnerable a ataques informáticos que buscan romper la seguridad criptográfica y acceder a los datos. De esta manera, esta investigación tiene como objetivo identificar de herramientas para prevenir el cryptojacking, para ello se llevó a cabo una revisión de literatura con el fin de identificar herramientas que permitan prevenir el cryptojacking, analizando también el contexto colombiano. Se encontraron varias herramientas, como software de detección de malware especializado, extensiones en el navegador que bloquean conexiones a sitios web de minería de criptomonedas y soluciones de seguridad. También se recomienda mantener los sistemas y software actualizados con los últimos parches y actualizaciones de seguridad para reducir el riesgo de vulnerabilidades. En conclusión, la criptografía es importante para proteger la seguridad de la información, pero su mal uso puede dar lugar a vulnerabilidades que pueden ser explotadas por los atacantes. Para prevenir el cryptojacking, se deben implementar prácticas recomendadas y utilizar herramientas tecnológicas adecuadas, como el software de detección de malware especializado y las extensiones del navegador. Además, mantener los sistemas de información con las últimas actualizaciones de seguridad, con el fin de proteger la seguridad de los datos y reducir el riesgo de ataques.

***Palabras clave:** cryptojacking, criptografía, privacidad, seguridad informática, vulnerabilidades.*

ABSTRACT

Cryptography is a method used to protect the confidentiality, integrity, and authenticity of data in transit or stored on servers. However, if configured incorrectly, it can be vulnerable to hackers seeking to break cryptographic security and gain access to data. In this way, this research aims to identify tools to prevent cryptojacking, for which a literature review was carried out in order to identify tools that allow cryptojacking to be prevented, also analyzing the Colombian context. Various tools were found, such as specialized malware detection software, browser extensions that

[1] Estudiante de Ingenierías de Sistemas, Corporación Universitaria Americana, Medellín-Antioquia, Colombia, johnrued7588@americana.edu.co , https://orcid.org/0009-0009-9615-3311
[2] Estudiante de Ingenierías de Sistemas, Corporación Universitaria Americana, Medellín-Antioquia, Colombia, tellojerson7176@americana.edu.co , https://orcid.org/0009-0001-4488-1175
[3] Estudiante de Ingenierías de Sistemas, Corporación Universitaria Americana, Medellín-Antioquia, Colombia, cardenasedward3579@americana.edu.co , https://orcid.org/0009-0000-7675-8764
[4] M. Res. En Gestión de Innovación Tecnológica, Cooperación y Desarrollo Regional, Corporación Universitaria Americana, Medellín-Antioquia, Colombia, vgarcia@americana.edu.co , https://orcid.org/0000-0003-3418-8956

block connections to cryptocurrency mining websites, and security solutions. It is also recommended to keep systems and software up to date with the latest patches and security updates to reduce the risk of vulnerabilities. In conclusion, cryptography is important to protect information security, but its misuse can lead to vulnerabilities that can be exploited by attackers. To prevent cryptojacking, you should implement best practices and use appropriate technology tools, such as specialized malware detection software and browser extensions. In addition, maintain information systems with the latest security updates, in order to protect data security and reduce the risk of attacks.

Keywords: *cryptojacking, cryptography, privacy, computer security, vulnerabilities.*

1. Introducción

La evolución tecnológica constante, impulsada por la presencia omnipresente de Internet y la computación en la nube ha llevado a un cambio significativo en la forma en que las personas realizan actividades, ya que muchas de ellas se llevan a cabo en entornos en línea y digitales, utilizando dispositivos electrónicos y ordenadores (Khan et al., 2023.). El cryptojacking es un delito en el que los ciberdelincuentes realizan actividades de intercambio y uso criptomonedas de forma ilegal a través de Internet, infectando los dispositivos de los usuarios (Sachan et al., 2022). Aunque aparentemente pueda parecer un delito inofensivo, este tipo de actividad ilícita puede generar grandes cantidades de criptomonedas, lo que lo convierte en un delito lucrativo para los delincuentes. Además de ser una violación a la privacidad y seguridad de los usuarios, el cryptojacking también conlleva otras consecuencias negativas (Chickowski, 2022).

De acuerdo con un artículo publicado por ESET (2017), el cryptojacking se considera un problema complejo porque se lleva a cabo sin el conocimiento ni el consentimiento de la persona afectada, lo que constituye una clara violación de la privacidad y seguridad de sus dispositivos (Wang et al., 2018). Esta práctica maliciosa puede propagarse mediante tácticas de phishing o la inserción de scripts en sitios web y anuncios, lo que aumenta su capacidad para infectar otros dispositivos y servidores (ESET, 2017). Como resultado, los dispositivos infectados experimentan una disminución en su rendimiento y una vida útil más corta debido al uso excesivo de recursos. Además, el aumento en el consumo de energía eléctrica se traduce en mayores gastos para los propietarios de los dispositivos infectados (ESET, 2017). Es importante destacar que los delincuentes informáticos pueden utilizar el cryptojacking para financiar actividades ilegales o apoyar a entidades de reputación dudosa, lo cual puede tener un impacto negativo en la reputación de las víctimas. De hecho, según McMillen de IBM X-Force (2017), los ataques de cryptojacking basados en la red aumentaron un 600 % en 2017, y los servicios financieros y de fabricación fueron las dos principales industrias objetivo (Sirosh, 2021).

De la misma forma el portal ChannelPartner (2018), afirma que el cryptojacking se ha convertido en un problema mundial debido a su naturaleza intrusiva. La práctica de utilizar el ordenador de otra persona sin su consentimiento para la criptominería conlleva diversas consecuencias negativas. En primer lugar, la víctima puede experimentar una disminución significativa en el rendimiento de su equipo, ya que los recursos se destinan a la criptominería en segundo plano. En segundo lugar, el cryptojacking puede generar costos adicionales para la víctima, como el aumento en la factura de la electricidad debido al mayor consumo energético. Además, el malware utilizado para introducir el software de cryptojacking en los dispositivos puede formar parte de una red más amplia de ciberdelincuencia, lo que pone en peligro la seguridad y privacidad de la información

personal y financiera de la víctima. Por último, el aumento en los ataques de cryptojacking puede indicar un incremento general en la actividad de ciberdelincuencia, lo cual representa una amenaza para la estabilidad y seguridad de la economía digital (ChannelPartner, 2018).

Es importante comprender las estrategias utilizadas por los atacantes para llevar a cabo el uso no autorizado de la máquina de una víctima con el fin de minar criptomonedas mediante cryptojacking. Según Liu et al., (2018), los atacantes emplean dos estrategias principales: la instalación de un binario en la máquina o el uso de un script en el navegador. En el primer enfoque, los atacantes cargan el código minero en la máquina de la víctima como un binario independiente o mediante una infección de un binario específico. Este método requiere información detallada sobre la máquina objetivo, incluyendo su sistema operativo y características de hardware (Liu et al., 2018). Esta forma de cryptojacking permite a los ciberdelincuentes obtener un mayor control sobre los recursos de la máquina comprometida, lo que les brinda una capacidad de minería más eficiente y lucrativa.

La segunda estrategia empleada por los atacantes implica el uso de un script en el navegador de la víctima. Este enfoque se aprovecha del poder de procesamiento de los visitantes sin su conocimiento. Difícil de detectar y sin carga adicional, puede pasar desapercibido mientras se utiliza el dispositivo para minar criptomonedas (SEON, 2023). Esta técnica es especialmente problemática, ya que puede afectar a un gran número de usuarios a través de sitios web infectados o anuncios maliciosos, lo que aumenta la propagación del cryptojacking y su impacto en la seguridad y privacidad de los usuarios. Teniendo en cuenta lo anterior, con el fin de profundizar más en los diferentes aspectos relacionados con el cryptojacking y las diferentes herramientas que pueden ser utilizadas para prevenir este tipo de ataques, este documento pretende brindar un contexto general sobre el avance respecto a los ataques y formas de prevenir el crypojacking a partir de una revisión de literatura y el contexto colombiano. Por tanto, el objetivo de esta investigación es identificar de herramientas para prevenir el cryptojacking a partir de una revisión de literatura.

2. Metodología

Para llevar a cabo esta investigación, se realizó una revisión de literatura, siguiendo las orientaciones de García y Macías (2022), en este artículo se proporcionó un enfoque integral y relevante para comprender esta metodología. Además, se realizó una revisión exhaustiva de la literatura relacionada con el tema del cryptojacking y las herramientas utilizadas para prevenir esta actividad delictiva. Para ello, se realizó una búsqueda de artículos científicos y técnicos en bases de datos académicas como IEEE Xplore, ACM Digital Library y Scopus, así como en motores de búsqueda académicos como Google Scholar. Los criterios de inclusión para la selección de artículos fueron los siguientes: Artículos publicados en los últimos 5 años, lo que permitió obtener información actualizada sobre el tema. De essta manera, se siguienron los criterios que García y Macías (2022) sugieren y con ello se tuvieron en cuenta los siguientes criterios de inclusión y exclusión:

- Artículos que abordaran específicamente el cryptojacking y las herramientas de prevención.

- Artículos escritos en inglés o español, ya que se buscó obtener una visión tanto internacional como local del problema.

- La estrategia de búsqueda se basó en términos clave relacionados con el cryptojacking, como "cryptocurrency mining malware", "cryptojacking prevention

tools", "cryptojacking detection", entre otros. Además, se consideraron términos específicos para el contexto colombiano, como "cryptojacking en Colombia" y "prevención de cryptojacking en Colombia".

- Tras la búsqueda inicial, se procedió a revisar los títulos y resúmenes de los artículos para evaluar su relevancia con respecto al tema de estudio. Posteriormente, se seleccionaron los artículos que cumplían con los criterios de inclusión y se leyeron en su totalidad para extraer la información relevante sobre las herramientas de prevención del cryptojacking.

- La información recopilada se analizó y se organizaron los hallazgos en categorías temáticas relacionadas con las herramientas de prevención identificadas en la literatura. Se presentan las principales herramientas encontradas, como software de detección de malware especializado, extensiones del navegador para bloquear conexiones a sitios web de minería de criptomonedas y soluciones de seguridad.

Es importante mencionar que esta investigación se enfocó en la recopilación y análisis de la literatura existente sobre el tema del cryptojacking y las herramientas de prevención. Esta metodología permitió obtener una visión general de las herramientas disponibles para prevenir el cryptojacking, así como identificar las principales tendencias y enfoques en el contexto colombiano. Los resultados y hallazgos de este estudio proporcionan una base para la comprensión y la implementación de medidas de prevención del cryptojacking en Colombia y otros contextos similares.

3. Resultados

Las herramientas diseñadas por el ser humano para prevenir el cryptojacking tienen una meta clara: evitar que nuestros sistemas sean vulnerados y se conviertan en un host zombi bajo el control de personas desconocidas. Estas herramientas se encargan de prevenir transacciones no autorizadas y la obtención de monedas digitales sin nuestro consentimiento.

Para lograr su cometido, estas herramientas han pasado por un proceso de desarrollo y pruebas que han implicado la superación de obstáculos y errores. Si bien no son perfectas, constantemente se corrigen y mejoran para ser más competentes en sus tareas. En la actualidad, estas herramientas se siguen mejorando y actualizando para su uso en una amplia gama de entornos, incluyendo hogares, sectores empresariales, educativos y gubernamentales.

Pérez Lietor, (2020) en su trabajo de grado menciona que Satoshi Nakamoto, seudónimo del creador de Bitcoin, tenía un objetivo claro cuando comenzó a desarrollar la tecnología que se convertiría en la base de las criptomonedas. Su objetivo no era crear una moneda virtual, sino un sistema de efectivo digital descentralizado que permitiera a las personas realizar transacciones de manera segura y sin la necesidad de una entidad central que controlara todo el proceso.

No se tenía la intención de crear una moneda virtual, sino un sistema de efectivo digital sin una entidad central. Para lograr esto, crearon una red de pagos distribuida llamada Blockchain, que permite evitar el doble gasto y solucionar otros problemas como el fraude (Pérez Lietor, 2020). El nacimiento de Bitcoin en 2008 fue el inicio de las criptomonedas, y desde entonces han surgido muchas más, cada una con características únicas, pero

compartiendo características comunes como la descentralización y la seguridad (Pérez Lietor, 2020; Huang et al., 2014).

Para lograr su objetivo, Satoshi comprendió que era necesario disponer de una red de pagos con cuentas, saldos y transacciones. El principal reto de estas redes es evitar la repetición inútil del gasto. En los sistemas de pago convencionales, el historial y el saldo actual de cada cuenta se almacenan en un único servidor. Pero Satoshi resolvió este problema de una manera diferente, creando Blockchain (Pérez Lietor, 2020).

Blockchain funciona de forma descentralizada, lo que significa que no hay un único punto de fallo. Para reemplazar la necesidad de un servidor centralizado que se ve en otras redes de pago, la propia red mantiene un registro de todas las transacciones que tienen lugar en la red. De esta manera, se evita el doble gasto y se solucionan otros problemas como el fraude (Shekhtman et al., 2023).

El nacimiento de Bitcoin en 2008 marcó el comienzo de las criptomonedas, y desde entonces han surgido muchas más con características únicas (Bhuiyan et al., 2023). Estas monedas digitales comparten atributos comunes, como la descentralización, la transparencia, la inmutabilidad y la seguridad. A diferencia de las monedas tradicionales, las criptomonedas no están controladas por una entidad central y pertenecen exclusivamente a sus propietarios (Bazzanella y Gangemi, 2023). Las transacciones son seguras gracias a la tecnología blockchain y las comisiones asociadas son considerablemente menores. Sin embargo, las criptomonedas también son más volátiles y pueden experimentar fluctuaciones significativas en su valor en cortos períodos de tiempo. Además, la mayoría de las criptomonedas establecen límites en la cantidad total de unidades para preservar su valor a largo plazo y evitar la sobreproducción (Hubrich, 2023).

Kim et al., (2021) indican que el cryptojacking al igual que otras amenazas de seguridad, ha sido abordado desde diferentes enfoques para mitigarlo y eliminarlo. Dado que el cryptojacking es un tipo de malware que involucra elementos criptográficos, existe una relación con otras formas de malware, como el crypto-ransomware. En este caso, se pueden identificar bloques de cifrado simétricos durante la etapa de explotación, lo que permite su detección mediante técnicas heurísticas utilizadas por proveedores de antivirus.

De esta manera, cuando se identifica un malware basándose en las herramientas que se han investigado o las que hay disponibles en el mercado a teniendo en cuenta los diferentes costos y tipos de licencias, los primeros escaneos presentados en el estado actual de una maquinan ayudan a distinguir las propiedades del archivo malicioso ejecutable. Estos escaneos pueden otorgar resultados prioritarios que son útiles para realizar un protocolo de intervención y análisis de datos explorados. Además, estas acciones pueden revelar puntos importantes en la evaluación de un punto inicial a un punto final, como el análisis profundo del tráfico de red, información del código inicial, las operaciones que colocan en conflicto la CPU y el monitoreo funcional de sitios infectados, todo ello considerando las interacciones del usuario realizadas. De acuerdo con lo anterior, en la figura 1 se observan los pasos a seguir, para prevenir el cyptojacking.

Figura 1. Pasos para prevenir el cryptojacking

Fuente: elaboración propia

1. Mantener el software actualizado: Asegurarse de que el sistema operativo, navegador y otros programas estén actualizados con las últimas versiones y parches de seguridad.

2. Usar un programa antivirus: Los antivirus pueden ayudar a detectar y prevenir el cryptojacking y otros tipos de malware.

3. Educarse: Educarse sobre el cryptojacking y cómo prevenirlo es una manera importante de protegerse contra este tipo de amenaza. Al comprender cómo funciona el cryptojacking y cómo los ciberdelincuentes pueden acceder a tus dispositivos, puedes tomar medidas para protegerte y evitar ser víctima de este tipo de ataque.

4. Usar extensiones anti-cryptomining: Las extensiones de navegador como uBlock Origin, No Coin y Miner Bloqueador – Anti-Miner.pueden ayudar a bloquear los mineros de criptomonedas en la web.

Teniendo en cuenta los pasos anteriores, a continuación, se presentan algunas medidas preventivas adicionales, para evitar el uso malintencionado de scripts. El Cryptojacking es una técnica malintencionada en la que un atacante utiliza el poder de procesamiento de otros dispositivos para minar criptomonedas sin su consentimiento, lo que puede causar un sobrecalentamiento y un mal funcionamiento en los dispositivos afectados. Para protegerse del Cryptojacking, los usuarios deben asegurarse de tener un software antivirus actualizado, evitar hacer clic en enlaces sospechosos y desconfiar de cualquier programa que exija un alto uso del procesador. Además, se recomienda utilizar ad-blockers y configurar adecuadamente la privacidad en los dispositivos para evitar ser víctimas de este tipo de ataques.

Los scripts son una amenaza en constante evolución para los usuarios de dispositivos electrónicos. Hay distintas alternativas de malware, pero dos destacan por encima de las demás. La primera consiste en scripts insertados en páginas web, que son el método más

común utilizado por los ciberdelincuentes. La segunda opción es mucho más peligrosa, ya que se trata de scripts que se instalan en un equipo víctima mediante un malware intrusivo. Estos pueden ser ejecutados en todo tipo de dispositivos, incluyendo móviles, tablets y ordenadores. Cuanta más potencia tenga el dispositivo, mayor será el rendimiento obtenido por el script. Existen, además, scripts no intrusivos que solicitan el consentimiento del usuario para utilizar su potencia de procesamiento. Si el usuario no acepta, el script no minará con su ordenador. Es importante que los usuarios estén alertas y tomen medidas preventivas para evitar Este, como el uso de software antivirus actualizado y la configuración adecuada de la privacidad en sus dispositivos.

3.1. Contexto en Colombia

La situación del cryptojacking en Colombia puede ser similar a la de otros países. Aunque los binarios maliciosos pueden no ser compatibles con todas las plataformas (Linux), la estrategia de JavaScript de cryptojacking que se ejecuta en el navegador es independiente de la plataforma. Esto significa que, independientemente del sistema operativo utilizado, cualquier persona con acceso a un navegador web podría ser víctima de un ataque de cryptojacking si visita un sitio web que ha sido comprometido (Castaño y Obando, 2019).

Dado que el código de minería trabaja en segundo plano mientras la víctima utiliza su ordenador, la persona afectada puede no ser consciente de que su dispositivo está siendo utilizado para minar criptomonedas. Por lo tanto, es importante que los usuarios estén informados sobre esta amenaza y tomen medidas preventivas, como el uso de software de seguridad actualizado y la verificación de la reputación de los sitios web que visitan.

En Colombia, se podrían llevar a cabo campañas de concientización y educación para informar a los usuarios sobre el cryptojacking y los pasos que pueden tomar para evitar ser víctimas de este tipo de ataques. También podrían implementarse medidas de seguridad en las redes y sistemas informáticos para detectar y prevenir el cryptojacking (Rosas Prado, 2022). El cryptojacking en el navegador se lleva a cabo inyectando un código JavaScript en un sitio web, lo que permite utilizar el poder de procesamiento del dispositivo de un visitante para minar una criptomoneda específica. Este código JavaScript se ejecuta automáticamente cuando se carga un sitio web y el visitante se convierte en parte de un pool de minería de cryptojacking. Es importante tener en cuenta que el visitante podría no ser consciente de que su dispositivo está siendo utilizado para minar criptomonedas mientras utiliza el sitio web infectado (Liu et al., 2018).

3.2. Algunas herramientas para prevenir el cryptojacking

Algunas de las herramientas que podrían ser utilizadas como forma de prevenir un ataque de cryptojacking se pueden observar en la tabla 1 y se describen más adelante.

Tabla 1 Herramientas autores y enfoque de prevención

Herramienta	Autor	Enfoque	Referencia
NoScript	Giorgio Maone	Bloqueo de scripts y contenido web no autorizado	Maone, (2007)
uBlock Origin	Raymond Hill	Bloqueo de Scripts y anuncios no deseados	Hill, (2014)

Malwarebytes	Malwarebytes Corporation	Detección y eliminación de malware, incluyendo cryptojacking	Malwarebytes Corporation (2006)
Avast Online Security	Avast	Bloqueo de sitios web maliciosos y detección de amenazas en línea	Avast (2023)
Norton Safe Web	NortonLifeLock	Protección contra sitios web maliciosos y análisis de reputación web	NortonLifeLock (2012)
Cisco Umbrella	Cisco	Filtro y protección contra amenazas web, incluyendo cryptojacking	Cisco (2005)
Bitdefender	Bitdefender	Protección contra malware y amenazas en línea, incluyendo cryptojacking	Bitdefender (2001)

Fuente: elaboración propia

NoMiner - Block Coin Miners. ("Chrome. Google" (2023). Esta es una extensión que te permite bloquear de manera sencilla los dominios que se dedican a la minería de criptomonedas en tu navegador.

(Chrome. Google, 2022). MinerBlock. Esta extensión de navegador es altamente eficiente y tiene como objetivo bloquear mineros de criptomonedas que se ejecutan en el navegador en toda la web.

(Chrome. Google, 2018). Miner Bloqueador – Anti-Miner. Esta extensión anti-minería para Chrome es fácil de usar y tiene como objetivo bloquear todos los scripts conocidos de minería de criptomonedas que se propagan en Internet y en tus sitios web favoritos. De esta manera, podrás navegar por la web sin tener que preocuparte por la extracción no autorizada de criptomonedas en tu dispositivo.

(Malwarebytes, 2023). Malwarebytes Premium es un ejemplo de un programa de ciberseguridad que no solo protege contra el cryptojacking, sino también contra otras amenazas en línea como el malware y el ransomware.

(Norton, 2017). Norton Security™: Es un paquete de software de seguridad en Internet robusto que puede ayudar a bloquear las amenazas de criptojacking. Este programa de seguridad integral no solo protege contra el criptojacking, sino también contra otras amenazas en línea, como malware, ransomware y virus.

(McAfee, 2022). McAfee LiveSafe es una completa solución de seguridad en línea que no solo ofrece protección antivirus contra virus, amenazas en línea y ransomware, sino también protección en tiempo real contra amenazas en línea, protección de la privacidad, y herramientas de seguridad para su identidad en línea.

(chrome.google.com, 2023). AdBlock. Un bloqueador de anuncios que puede bloquear anuncios web que contienen scripts de minería.

(chrome.google, 2023). Ghostery. Una extensión de navegador que bloquea scripts de rastreo y minería.

(chrome.google, 2023). uBlock Origin. Un bloqueador de anuncios que puede bloquear anuncios web que contienen scripts de minería.

(Bitdefender, 2023). Bitdefender Internet Security Es una completa solución de seguridad informática que protege contra una amplia gama de amenazas digitales, incluyendo virus, gusanos, troyanos, ransomware, exploits de día cero, rootkits y spyware.

4. Discusión

Protegerse del cryptojacking es diferente a protegerse de otros ataques de malware, ya que puede ocurrir incluso en sitios web legítimos comprometidos (Interpol, 2022). Las medidas de prevención más comunes incluyen utilizar algún tipo de solución antivirus en tu ordenador, no instalar software proveniente de sitios no oficiales, tener cuidado con las extensiones que añades a tu navegador, y con los enlaces que abres (García, 2019).

Es recomendable instalar extensiones como Minerblock, que bloquean todo tipo de cryptominers en la web, o utilizar herramientas integradas para bloquear la criptominería en navegadores como Opera y Firefox (IONOS, 2022). Algunos bloqueadores de anuncios como Adblock Plus y uBlock Origin también incluyen listas específicas para bloquear la minería (Glover, 2022; Kaspersky, 2022).

Es fundamental mantenerse actualizado con las actualizaciones disponibles para el sistema operativo y cualquier herramienta relacionada con la gestión de navegadores o páginas web (ESET, 2017). Por otro lado, desactivar JavaScript al navegar por Internet, ya que muchos de los scripts de cryptojacking utilizan JavaScript para llevar a cabo sus actividades ilícitas. Es importante monitorizar el consumo de recursos de tu ordenador de vez en cuando, especialmente cuando notes cambios en el rendimiento, lentitud, o que los ventiladores comiencen a hacer mucho ruido de pronto (Sirosh, 2021).

5. Conclusiones

La llegada de las criptomonedas ha abierto grandes posibilidades, pero también ha traído consigo una serie de riesgos y amenazas en términos de seguridad. Una de estas amenazas es el Cryptojacking, que consiste en el uso no autorizado de la potencia de procesamiento de otros usuarios de Internet para minar criptomonedas de manera masiva. Los ciberdelincuentes se han visto atraídos por las características de las criptomonedas, como su anonimato y transacciones seguras, y han desarrollado técnicas para obtenerlas ilegalmente. Además, las criptomonedas son utilizadas en la Deep Web para realizar transacciones ilegales, lo que aumenta el atractivo para los delincuentes. Por lo tanto, es importante que los usuarios adopten medidas de prevención y seguridad, como el uso de software antivirus y la configuración adecuada de la privacidad en sus dispositivos, para evitar ser víctimas del Cryptojacking y otros ataques cibernéticos relacionados con las criptomonedas.

El cryptojacking es un tipo de ataque informático en el que los hackers utilizan la potencia de procesamiento de un sistema sin el conocimiento o consentimiento del propietario para extraer criptomonedas ilegalmente. Para prevenirlo, se recomienda implementar prácticas recomendadas y utilizar herramientas tecnológicas adecuadas, como software de detección de malware especializado y extensiones del navegador que bloqueen sitios web de minería de criptomonedas. La configuración incorrecta de la criptografía puede llevar a vulnerabilidades y ataques informáticos que comprometen la seguridad de los datos. Además, mantener los sistemas y el software actualizados con los últimos parches y actualizaciones de seguridad es crucial para reducir el riesgo de vulnerabilidades.

El cryptojacking no solo viola la privacidad y seguridad de las personas, sino que también puede generar costos adicionales en términos de rendimiento del sistema y consumo de energía. Es importante comprender las estrategias utilizadas por los atacantes, como la instalación de binarios en la máquina o el uso de scripts en el navegador, para llevar a cabo el cryptojacking.

Finalmente, la revisión de la literatura identificó varias herramientas disponibles para prevenir y detectar esta actividad ilegal, y se recomienda su implementación en el contexto colombiano y en otros entornos. La criptografía sigue siendo importante para proteger la seguridad de la información, pero su mal uso puede dar lugar a vulnerabilidades explotables por los atacantes. Es esencial implementar medidas de seguridad y utilizar herramientas adecuadas para prevenir y detectarlo, así como mantener los sistemas actualizados para reducir el riesgo de ataques y proteger la seguridad de los datos.

Referencias

Avast. (2023). Avast Online Security. Recuperado de https://www.avast.com/Bitdefender.Bitdefender Internet Security. Recuperado de https://www.bitdefender.es/

Bazzanella, D., & Gangemi, A. (2023). Bitcoin: A new proof-of-work system with reduced variance. Financial Innovation, 9(1) doi:10.1186/s40854-023-00505-2

Bitdefender. (2001). Bitdefender. Recuperado de https://www.bitdefender.es/Kim, H.; Park, J.; Kwon, H.; Jang, K.; Seo, H. Convolutional Neural Network-Based Cryptography Ransomware Detection for Low-End Embedded Processors. Mathematics 2021, 9, 705.

Bhuiyan, R. A., Husain, A., & Zhang, C. (2023). Diversification evidence of bitcoin and gold from wavelet analysis. Financial Innovation, 9(1) doi:10.1186/s40854-023-00495-1

Castaño Quiroz, C. E., & Obando Ibarra, C. H. (2019). Mecanismos de protección en seguridad informática contra el Cryptojacking: Estudio de caso Industrias Estra. Revista CIES, 10(2), 145-164. ISSN 2216-0167.Rosas, A. F. (2022). El cibercrimen en Colombia y su evolución en los últimos dos años (2020-2021). Recuperado de: http://hdl.handle.net/10654/43617.

ChannelPartner (2018). El cryptojacking se convierte en un problema mundial. ChannelPartner. Recuperado de https://www.channelpartner.es/seguridad/noticias/1134676002502/cryptojacking-se-convierte-problema-mundial.1.html

Chickowski, E. (2022). What is cryptojacking? How to prevent, detect, and recover from it. CSO Online. https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

chrome.google. (2022). Miner Bloqueador - Anti-Miner. Obtenido de https://chrome.google.com/webstore/detail/miner-blocker-block-coin/ejpcojkcallnhphinmknkaoojohidegf?hl=es

chrome.google. (2022). MinerBlock. Obtenido de https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl

chrome.google. (2023). NoMiner - Block Coin. Miners.https://chrome.google.com/webstore/detail/nominer-block-coin-miners/jfnangjojcioomickmmnfmiadkfhcdmd?hl=es

chrome.google. (2023). "AdBlock — el mejor bloqueador de anuncios" Obtenido de https://chrome.google.com/webstore/detail/adblock-%E2%80%94-best-ad-blocker/gighmmpiobklfepjocnamgkkbiglidom?hl=es

chrome.google. (2023). Ghostery – Bloqueador de anuncios para privacidad. Obtenido de https://chrome.google.com/webstore/detail/ghostery-–-privacy-ad-blo/mlomiejdfkolichcflejclcbmpeaniij?hl=es

chrome.google. (2023). uBlock Origin. https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=es

Cisco. (2005). Cisco Umbrella. Recuperado de https://umbrella.cisco.com/

ESET. (2017). Cryptojacking. Recuperado de https://www.eset.com/es/caracteristicas/cryptojacking/

García, V., & Macías, J. A. (2022). Analysis of the Variables Leading to the Identification and Incorporation of Innovation Capabilities by Firms in the Colombian ICT Sector. INNOVAR, 32(84), páginas.

García, Y. (2019). Qué es el cryptojacking y cómo prevenirlo. Recuperado de https://planetampodcast.com/2019/08/que-es-el-cryptojacking-y-como-prevenirlo/

Glover, C. (2022), Cryptojacking: How the crypto boom is driving malware infections. https://techmonitor.ai/technology/cybersecurity/cryptojacking

Hill, R. (2014). uBlock Origin. Recuperado de https://ublockorigin.com/

Huang, D. Y., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., Mccoy, D., Savage, S., Weaver, A. N., Snoeren, C. and Levchenko. K. (2014). Bitcoin: Monetizing stolen cycles. In Proceedings of the 21st Network and Distributed System Security Symposium (NDSS).

Hubrich, S. (2023). Bitcoin in a multi-asset portfolio. Journal of Alternative Investments, 25(3), 63-80. doi:10.3905/jai.2022.1.177

Interpol. (2023). Cryptojacking. Obtenido de https://www.interpol.int/Crimes/Cybercrime/Cryptojacking

IONOS. (2022). Cryptojacking: cómo detectar y protegerse de la infección. Recuperado de https://www.ionos.es/digitalguide/servidores/seguridad/cryptojacking/

Kaspersky. (2023). ¿Qué es el cryptojacking? Definición y explicación. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cryptojacking

Khan, M. H., Ullah, S., Ahmad, T., & Buriro, A. (2023). A Real-Time Hybrid Approach to Combat In-Browser Cryptojacking Malware. *Applied Sciences*, *13*(4), 2039. https://doi.org/10.3390/app13042039

Kim, H. J., Shim, J. H., Park, J. H., Shin, H. T., Shim, J. S., Jang, K. T., ... & Lee, D. (2021). Single-cell RNA sequencing of human nail unit defines RSPO4 onychofibroblasts and SPINK6 nail epithelium. Communications biology, 4(1), 692. https://doi.org/10.1038/s42003-021-02223-w

Liu, C., Ding, X., Huang, X., & Liang, X. (2018). A First Look at Cryptojacking. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2-17. https://doi.org/10.1145/3243734.3243766

Malwarebytes Corporation. (2006). Malwarebytes. Recuperado de https://www.malwarebytes.com/

Malwarebytes. (2023). Cryptojacking: What it is and how to prevent it. Retrieved from https://www.malwarebytes.com/cryptojacking#:~:text=Malwarebytes%20Premium%2C%20for%20example%2C%20protects,you're%20protected%20against%20cryptojacking.

Maone, G. (2007). NoScript. Recuperado de https://noscript.net/

McAfee (2022). McAfee® LiveSafe™. Obtenido de https://www.mcafee.com/es-co/antivirus/mcafee-livesafe.html

McMillen, D. (2017). Network attacks containing cryptocurrency CPU mining tools grow
Norton. (2017). What Is Cryptojacking? Norton Blog. https://us.norton.com/blog/malware/what-is-cryptojacking.
NortonLifeLock. (2012). Norton Safe Web. Recuperado de https://co.norton.com/
Pérez Lietor, A. (2020). Las criptomonedas como instrumento de inversión. Universidad de Alcalá. Obtenido de https://ebuah.uah.es/dspace/bitstream/handle/10017/40887/TFG_Perez_Lietor_2020.pdf?sequence=1&isAllowed=y
Rosas Prado, A. F. (2022) El cibercrimen en Colombia y su evolución en los últimos dos años (2020-2021). [Tesis pregrado, Universidad Nueva Granada, Colombia] http://hdl.handle.net/10654/43617
Sachan, R. K., Agarwal, R., & Shukla, S. K. (2022, September). DNS based In-Browser Cryptojacking Detection. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)* (pp. 259-266). IEEE. https://arxiv.org/pdf/2205.04685.pdf
SEON. (2023). Cryptojacking. https://seon.io/es/recursos/glosario/que-es-cryptojacking/
Shekhtman, L. M., Sela, A., & Havlin, S. (2023). Percolation framework reveals limits of privacy in conspiracy, dark web, and blockchain networks. EPJ Data Science, 12(1) doi:10.1140/epjds/s13688-023-00392-8
Sirosh. D. (2021). What Is Cryptojacking, and How to Protect Your Assets Against It? https://www.infopulse.com/blog/cryptojacking-ways-mitigate-risks/sixfold. IBM X-Force SecurityIntelligence, September 2017.
Wang, W., Ferrel, B., Xu, X. (2018). SEISMIC: SEcure In-lined Script Monitors for Interrupting Cryptojacks. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 11099. p. 122-142. 23rd European Symposium on Research in Computer Security, ESORICS 2018. https://doi.10.1007/978-3-319-98989-1_7

Conflictos de interés

Los autores declaran no tener conflicto de interés.