Estado Actual De Los Ataques Cryptojacking, Con Énfasis En Aplicaciones web.

Autores.
Luis Francisco Diaz Peñuela(1).
Luis.diaz02@usc.edu.co

Luis Miguel Celorio Celorio(2).
Luis.celorio00@usc.edu.co

Director.
Diego Fernando Loaiza(3)
Buitrago
Diego.loaiza02@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de [Ingeniería En Sistemas] (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de [Ingeniería En Sistemas] (2)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de [Ingeniería En Sistemas] (3)

Resumen

El cryptojacking, una amenaza persistente en el ámbito de la ciberseguridad se centra en el uso clandestino de recursos informáticos para minar criptomonedas, para empezar las criptomonedas son una moneda digital que tiene un cifrado criptográfico, las cuales usan el sistema blockchain para su intercambio u transacciones, ahora bien, enfatizando en las aplicaciones web lo más común en el cryptojacking como su nombre lo indica, crypto haciendo referencia a las criptomonedas y jacking haciendo referencia a secuestro cuya palabra en inglés es hijacking, es secuestrar el hardware que se haya vulnerado, además de que los atacantes explotan vulnerabilidades en el software de servidores web o inyectan código malicioso en aplicaciones y scripts del lado del cliente.

Al comprometer la infraestructura, ejecutan operaciones de minería de criptomonedas sin el conocimiento del propietario del sistema, el estado actual de los ataques cryptojacking, va en aumento, con el pasar de los años, ideándose por parte de los atacantes informáticos novedosas maneras de infectar equipos mediante aplicaciones web, para evitar esto se debe tener conciencia de ciberseguridad, tener antivirus actualizados además de verificar en todo momento el rendimiento de nuestros dispositivos, navegar de manera segura en sitios confiables con un nivel de seguridad robusto.

El cryptojacking ha sido investigado a lo largo prácticamente desde la creación de las monedas digitales, por diversos Ingenieros, científicos, analistas, hasta propios inversores o compradores de estas monedas, ya que abarca un tema critico de seguridad y vulneración de derechos, tomando todo este conocimiento tanto de estudios como de artículos, investigaciones, realizados por las comunidades mencionadas anteriormente se busca integrar todo el conocimiento, ofreciéndolo en el actual articulo con un estudio propio realizado para este.

Revisando el número de ataques cryptojacking que ocurren, de por qué están en auge, porque se espera su aumento, las condiciones, circunstancias y normativas a nivel global, que propician su aumento, lo cual ha llevado también a repercutir en otro tipo de mercados, economías, además de directamente en las victimas.

Por lo tanto este articulo tiene como objetivo investigar el estado actual de los ataques cryptojacking, con énfasis en aplicaciones web, dando a conocer todo el ámbito en el que se desarrolla esta práctica, conociendo en primera medida que son las criptomonedas o monedas digitales, el medio por el cual estas pueden ser obtenidas además de las herramientas para su almacenamiento transacción y comercio, desarrollando para su explicación en que consiste esta práctica, sus maneras de operar, para finalmente concluir con el estado actual de estos ataques cryptojacking, recomendando buenas prácticas al usuario para evitar ser vulnerado.

Palabras Clave: criptomoneda, cryptojacking, blockchain, ciberseguridad, hardware, software, web, atacantes, vulnerabilidad, seguridad, aplicaciones, servidores, dispositivos, sistema, cifrado.

Abstract

Cryptojacking, a persistent threat in the field of cybersecurity focuses on the clandestine use of computer resources to mine

cryptocurrencies, for starters cryptocurrencies are a digital currency that has a cryptographic encryption, which use the blockchain system for their exchange or transactions, now emphasizing on web applications the most common in cryptojacking as its name suggests, crypto referring to cryptocurrencies and jacking referring to hijacking whose word in English is hijacking, is to hijack hardware that has been breached in addition to that, attackers exploit vulnerabilities in web server software or inject malicious code into client-side applications and scripts. By compromising the infrastructure, they execute cryptocurrency mining operations without the knowledge of the owner of the system, the current state of cryptojacking attacks, is increasing, over the years, being devised by computer attackers novel ways to infect computers through web applications, to avoid this we must have cybersecurity awareness, fear updated antivirus in addition to verify at all times the performance of our devices, navigate safely in reliable sites with a robust level of security.

Keywords: cryptocurrency, cryptojacking, blockchain, cybersecurity, hardware, software, web, attackers, vulnerability, security, applications, servers, devices.

1. INTRODUCCIÓN

El cryptojacking es una amenaza a la seguridad de nuestros ordenadores, servidores o dispositivos que cuenten un con una cpu o gpu capaces de minar criptomonedas, sin embargo, hay que enfocarse en primera medida en estos términos y conocer bien ha que se refiere cada uno de ellos para poder comprender el alcance que tienen los ataques de cryptojacking en nuestra cotidianidad. Primero pues, así se empieza por aclarar los términos generales que acompañan el entramado de este tipo de ataques.

Desde los inicios de las criptomonedas, tomando en cuenta que las mismas no son más que activos digitales, en este caso en concreto una moneda con codificación criptográfica lo cual las hace uno de los activos digitales más seguros, junto con su robusto sistema de intercambio y comercialización como es el blockchain el cual es una cadena de bloques con información codificada que permite tener un nivel de seguridad bastante alto, sin duda en su momento una innovación bastante confiable desde la parte de la ciberseguridad financiera, sin embargo como todo en el mundo digital y más con un fenómeno como la interconectividad global no ha escapado a los atacantes informáticos, en este caso viendo afectados a los usuarios más comunes de la red por el alto riesgo y poca seguridad que manejan los usuarios comunes, pero también grandes empresas con servidores bastante robustos e infraestructuras grandes con seguridad alta(Tanana, 2020).

Por lo cual se puede tomar como punto de partida que en la era digital actual, el fenómeno del cryptojacking ha emergido como una amenaza significativa, con un enfoque creciente en las aplicaciones web. El estado actual de los ataques de cryptojacking revela una evolución constante de técnicas maliciosas dirigidas a comprometer la potencia de procesamiento de las computadoras de los usuarios para la minería de criptomonedas sin su conocimiento(Eskandari et al., 2018).

Este fenómeno, impulsado por el lucrativo incentivo financiero que proporciona la minería de criptomonedas, plantea desafíos críticos para la seguridad cibernética. En particular, las aplicaciones web se han convertido en un objetivo principal, aprovechando vulnerabilidades y brechas de seguridad para infiltrarse de manera silenciosa. Este panorama resalta la necesidad apremiante de medidas proactivas de seguridad, la conciencia del usuario y la colaboración entre la industria y la comunidad para salvaguardar la integridad de las aplicaciones web y proteger a los usuarios contra este tipo de amenazas emergentes(Meland et al., 2019).

Habiendo ya tenido claros los conceptos y lo grave que es esta amenaza en la actualidad puede empezar a hablarse de las formas de prevenirla o de que en caso contrario estemos siendo directamente afectados por este tipo de ataques saber que hacer para manejar el problema, para así poder solucionarlo cabe recalcar que es un tema de prevención y seguridad lo que nos permitirá estar libres de este tipo de amenazas, siempre teniendo la vanguardia en seguridad informática, apoyados de elementos como los antivirus, actualizaciones, cortafuegos, directivas, y toda herramienta a nuestra disposición para tener un nivel de seguridad alto en nuestros dispositivos ya sea que se trate de servidores, ordenadores de alto poder o nuestra tablet o smartphone(Varlioglu et al., 2022).

Para finalizar comentar resultados de la investigación consagrada y sus recomendaciones para buenas prácticas de seguridad comentando el estado de los ataques de cryptojacking en la actualidad es una forma efectiva de terminar, siempre teniendo

en cuenta que no estamos a salvo en la red en ningún momento y que ninguna medida que tomemos para protegernos esta de más.

1.1 CONOCIENDO EL CRYPTOJACKING.

El mundo actual se encuentra en busca de nuevas formas tecnológicas e innovadoras a la hora de generar riqueza o dinero, incorporando cada vez una seguridad más robusta para así tratar de mitigar acciones criminales que comprometan los activos de personas o empresas, en cuyo caso son activos tecnológicos, en este punto se hablara de una amenaza que está azotando a las distintas monedas digitales que se conocen como criptomonedas, y como son los usuarios finales, personas del común o incluso servidores de alta potencia usados para distintos tipos de servicios, los que see han visto afectados por este tipo de ataques que ponen en desbalance el equilibrio de esta economía digital además de poner en apuros a las personas o servicios que dependen del hardware que es infectado por ese mal cibernético usado por atacantes hacia las aplicaciones web.

Para poner en contexto esta amenaza se debe primero hablar de las criptomonedas, esta variante de dinero, que ahora está tomando un auge importante en la economía, no es más que una moneda digital que utiliza métodos criptográficos complejos para su emisión y sus intercambios, en la actualidad se manejan distintos tipos de estas monedas las cuales tienen un valor variable dependiendo de su oferta y demanda, por lo cual una definición que también pueden tomar las criptomonedas es la de activo digital (Cabrera Soto et al., 2022).

Al ser un activo digital altamente codiciado, ya que su manejo y obtención puede pasar más desapercibido, por entes reguladores, están en la mira de muchas personas, cuyos escrúpulos se pueden poner en tela de juicio al realizar actividades de dudosa moralidad, para obtener este tipo de monedas digitales, prácticamente sin dejar huellas o registros rastreables para poder generar una trazabilidad y encontrar a quien está detrás de estas actividades.

Con el tema de las criptomonedas abordado, otro punto importante es el tema de su seguridad y como estos activos digitales tienen uno de los sistemas más seguros a la hora de su comercialización o transacciones por no hablar de su emisión, el principal componente en la seguridad de las criptomonedas es el blockchain una tecnología que acogió a las criptomonedas este se basa en el hashing, que tal vez para el que no esté familiarizado con el término no es más que un método criptográfico, el cual permite transformar datos u cadenas de caracteres de cualquier longitud en valores hash, esto permite que se pueda tener bastante confianza a la hora de realizar una transacción, ya que este tipo de seguridad es muy difícil de vulnerar, se puede producir un tipo de ataque o fraude más por descuido del propietario que por una falla de seguridad del blockchain(Di Pierro, 2017)

Mencionando de manera particular al usuario, ya que se ha probado que la seguridad blockchain es de las más confiables, se advierte que los usuarios finales no solo son las principales víctimas de este tipo de ataques si no también, que muchas veces por descuido o desconocimiento de los sistemas de información o de las mismas herramientas que estos utilicen deja muchas puertas abiertas, muchas oportunidades de que sus equipos tecnológicos se vean vulnerados.

El cryptojacking no sería posible si no existiera la minera de criptomonedas, ya que esta es la base de la cual se desprende el problema en cuestión. Más adelante se profundizará como esta práctica va estrechamente ligada con el cryptojacking, pero por el momento para recalcar su relación con este tipo de ataques, y explicar que es, no es más que mencionar que la minería de criptomonedas es una de las principales fuentes de obtención de este tipo de activos digitales, para ello en el mayor número de casos se recurre al hardware específicamente procesadores, memorias RAM o tarjetas gráficas, estas últimas siendo las más usadas para minar, se puede minar dependiendo de que tipo de moneda se quiera con la ayuda de un dispositivo móvil, hasta servidores, aunque hay granjas completas de "rigs" de minería, dispuestos para tal tarea, este "rig" no es más que una computadora acondicionada con muchas tarjetas gráficas para exprimir su poder y minar criptomonedas(Val Gangonells, 2020).

Se debe recalcar que el cryptojacking es un problema de ciberseguridad, por lo cual es un asunto de buenas prácticas y prevención, el implementar medidas para minimizar el riesgo de sufrir vulneraciones por parte de atacantes dedicados al cryptojacking, no está de más siempre tener actualizados nuestros sistemas, todas sus funciones de seguridad activas, pero lo más importante saber navegar por internet, conocer los riesgos de cada uno de los movimientos que se hagan por la web. Para así poder verse menos implicados en este tipo de desafortunados hechos, una forma de detectar un ataque de cryptojacking de manera rápida es por qué en nivel de gasto de recursos de la máquina que esté al servicio, tenga un mayor gasto de estos(Tanana & Tanana, 2020).

1.1.2 **¿Qué Es El Cryptojacking?**

Habiendo identificado y dado un contexto acerca de lo que compone principalmente a los elementos relacionados con el cryptojacking, se puede empezar a desglosar el término, empezando por su escritura en sí, ya que desde su gramática nos da pistas a lo que el término hace alusión, tenemos su primera parte "crypto" que no hace más que referencia a las criptomonedas, ya su otro componente "jacking" que no es más que una derivación de la palabra secuestro en inglés la cual es "hijacking", esto quiere decir acaso que el cryptojacking secuestra la divisa digital, en esencia y siendo puntual sería un no de primera instancia es algo que se explicara más adelante(Pérez Lietor, 2020).

El crytojaking no se encarga de secuestrar las monedas que estén almacenadas en cualquier billetera digital o inclusive en un dispositivo de almacenamiento, tiene una forma de actuar más oscura, la cual plantea al usuario o administrador del sistema un reto, ya que este tipo de ataques empieza a mostrar los síntomas muy tarde cuando ya muchas veces el equipo de cómputo en cuestión ha sido invadido (Sigler, 2018).

A si como se menciona, muchas veces es muy tarde cuando la amenaza es detectada, esta puede haber vulnerado no solo el sistema infiltrándose en él, sino también aprovechándose del hardware y es aquí donde los problemas vienen en gran medida desencadenando una tortuosa odisea, ya que para un desconocedor del mundo informático e inclusive para entusiastas, puede ser difícil realmente dar con un diagnóstico preciso de qué amenaza ha infectado el dispositivo (Khiruparaj et al., 2021).

Podríamos decir que inclusive para alguien experimentado en el ámbito informático esta clase de ataques son un dolor de cabeza, ya que por el simple hecho de estar conectado a la red, te hace vulnerable y una presa en toda regla para todo tipo de personas con objetivos oscuros dentro del internet, los cuales buscan cualquier descuido para dañarte, y poder sacar beneficio de esto, como mencionábamos anteriormente, el problema está en la detección temprana de estas vulneraciones, además de los importantísimos planes estratégicos de gestión TI para no solo detectarlas a tiempo si no también prevenirlas.

Cualquier dispositivo puede sufrir de este tipo de ataques, aunque, los atacantes tratan de conseguir blancos de alto poder computacional o de un hardware robusto, nadie esa a salvo frente a esta amenaza, ya que cualquiera es un blanco potencial desde dispositivos móviles, computadores de escritorio o portátiles, servidores, cualquier dispositivo que cuente con el hardware requerido para minar criptomonedas es un blanco potencial (Carlin et al., 2020).

¿La pregunta es por qué?, porque somos todos posibles blancos de un ataque de cryptojacking, bueno para empezar este tipo de malware que infecta nuestras computadoras lo hace por diversos medios el principal como cualquier otro malware es la web, pero ¿qué pasa cuando ya estamos infectados?, su funcionamiento puede parecer simple pero no lo es, dependiendo de la moneda que el atacante desee obtener con nuestro dispositivo, esté ira peor comparado con otro dispositivo que no esté infectado o puede que vaya peor o mejor que un dispositivo igual que esté minando otro tipo de criptomoneda (F. Gomes & Correia, 2020).

Se puede entonces interpretar el cryptojacking como el secuestro de un dispositivo, sin el consentimiento u conocimiento de su propietario para poder utilizar los recursos del mismo, para así poder empezar a minar criptomonedas, esto ocasionando una falla a nivel de rendimiento de los componentes del equipo por la fatiga de la tarea, porque para ser honestos minar criptomonedas es una tarea que incluso los equipos especiales como los rig de minería ven una fatiga importante y deben de estar refrigerados, mayormente por refrigeración líquida, y un ambiente con aire acondicionado,

para evitar el sobrecalentamiento y aumentar un poco la vida útil de los componentes(Urdaneta Bernal, 2018).

Imagine la carga computacional, o para referirnos en términos más prácticos la carga de trabajo que debe tener el equipo de cómputo, especialmente los componentes principales que ya hemos mencionado que son los que se ven más afectados a la hora de minar dependiendo del tipo de criptomoneda como lo pueden llegar a ser las memorias RAM, el procesador o la tarjeta gráfica, esto implica no solo la perdida de rendimiento a la hora de realizar cualquier tarea sino un desgaste significativo en los componentes, pudiendo esto es casos extremos donde no se tomen medidas llegar a la pérdida del componente o incluso la pérdida total del dispositivo, no solo hay que verlo como un ataque a nuestro hardware sino una vulneración de nuestra intimidad y privacidad por el hecho de una colación por una puerta trasera a nuestro sistema(Xu et al., 2023).

Habiendo ya desentrañado que es y cómo funciona el cryptojacking debemos hablar de la seguridad y lo que implica que este tipo de ataques lleguen a nuestros dispositivos, no solo estamos hablando que toman posesión de nuestro hardware, para que este malware pueda empezar a utilizarlo en beneficio propio para obtener ganancias, estamos hablando de una intromisión total a nuestro sistema, y si este fue el caso muy probablemente no solo se puedan llegar a conformar con utilizar nuestros dispositivos como centros de minado, sino que este tipo de ataques pueden derivar en otros que afecten nuestra estabilidad emocional y que urgen en la intimidad más discreta que preferimos mantener oculta(Anita. & Vijayalakshmi., 2019).

Se debe entonces prestar bastante importancia porque en el mundo de los ciberataques es muy común que una vez hallada una vulnerabilidad esta sea explotada no solamente por un atacante sino por varios, entonces un dispositivo se puede volver una madriguera de ciber atacantes y malwares intentando sacar provecho del mismo, por lo cual esto puede derivar en la adquisición de nuevos malware, como lo son el ransomware el phishing, virus informáticos, los cuales generan que todos nuestros datos, nuestra identidad, nuestra privacidad sea usurpada, vulnerada, haciendo entonces que nuestra privacidad e identidad, sean usurpadas, poniendo e riesgo nuestra salud mental y nuestra reputación(Kshetri et al., 2023).

1.1.3 **Estado actual de los ataques cryptojacking, con énfasis en aplicaciones web.**

Llegados a este punto se empezará a discutir el tema principal del artículo el cual tiene como premisa hablar acerca del estado actual de los ataques cryptojacking, con énfasis en aplicaciones web, se espera que el mundo del cryptojacking a este punto ya sea más entendible para el lector pues se han expuesto los diferentes componentes que rodean a este malware, además de que se ha explicado cómo funciona y su forma de atacar, por lo cual se espera que a partir de ahora el lector tenga claro todos los términos que se mencionaran a continuación.

Estando al tanto de que el cryptojacking es un tipo de malware que secuestra nuestro dispositivo para obtener criptomonedas con el hardware, y de cómo este infecta nuestro dispositivo, nos queda saber que tan recurrente es, que tantos ataques se dan, o se manifiestan, y por qué una de las principales puertas de la infección son las aplicaciones web, hemos dicho que es un problema de ciberseguridad que está íntimamente ligado más que a cualquier cosa y como comúnmente sucede al usuario final, ya que muchas veces este es una presa fácil por su desconocimiento, a la hora de navegar por la web, así se hayan implementado políticas de seguridad robustas el usuario que manipula la máquina básicamente es el responsable de que su dispositivo se pueda ver infectado por este malware(Di Tizio & Nam Ngo, 2020).

Por lo cual sabiendo que el usuario del dispositivo es el que abre el camino de los atacantes a su dispositivo, ahora la pregunta es ¿Por qué las aplicaciones web? Como casi todos los malware o virus, estos provienen de la web, porque en ella hay tanto cosas buenas, como malas y aunque los navegadores día tras día se esfuercen para implementar medidas de seguridad más robustas para proteger a sus usuarios, estos están desprovistos ante las distintas formas en las que un hacker encuentra la forma de invadir el sistema del usuario que navega por la web(Jayasinghe & Poravi, 2020).

Por ende la principal causa de infección es la navegación descuidada por parte del usuario, esto pues navegando por sitios no seguros, sin certificados de seguridad ni protocolos de seguridad, o dejándose llevar por links que a la final lo que hacen es de forma sutil, instalar programas en el dispositivo, entre estos el cryptojacking que casi siempre en la mayoría de caso es una inyección de código o script que se ejecuta en segundo plano y empieza a descargar e instalar todo lo necesario para

el minado sin que la persona se dé cuenta hasta que sea muy tarde(Razali & Mohd Shariff, 2019).

Aunque con el auge de este tipo de ataques inclusive se han dispuesto medidas por parte de terceros o de agentes privados para mitigar este tipo de ataques, ya que una cosa es infectar una computadora de un usuario normal, y otra muy distinta es infectar un servidor o servidores cuyo capacidad de cómputo y hardware es mucho más potente, por lo cual y como no podía ser de otra forma una de las medidas que se plantean y están teniendo mucho efecto es la capacidad de evitar o detectar el cryptojacking mediante la inteligencia artificial, entrenándolas mediante el machine learning, para pasar después a deep learning y esta tenga la facultad de tomar decisiones que lleven a una seguridad más automatizada y fiable(Petrov et al., 2020).

Ahora bien, ya que abordamos la problemática de las aplicaciones web y como estas son la principal fuente de vulneraciones hacia los sistemas, la principal puerta de entrada para los atacantes es hora de hablar el estado de los ataques cryptojacking, porque estos más que verse mermados con el pasar de los años y las nuevas maneras de minar u obtener criptomonedas han ido en aumento teniendo un auge mayor en los últimos años, y como el cryptojacking no solo se presta para el control del sistema para minar si no puede ser explotado en mayores escalas la actividad de los atacantes utilizando este método ha aumentado (Zimba et al., 2019).

Según un estudio de (Saad et al., 2019), donde se analizaron estadísticamente distintos sitios web y scripts tanto benignos como maliciosos con aprendizaje profundo no supervisado para el cryptojacking teniendo una precisión del 96.4% se evidencia que los ataques de cryptojacking han ido en aumento como se mencionaba antes, se podría decir que están más activos que nunca debido al apogeo de las criptomonedas.

Desde que el sistema cripto tomo relevancia en el escenario global ya siendo incluido inclusive por gobiernos en sus economías, trajo consigo la gran avalancha de ataques que vemos hoy, de todo tipo hacia el sistema financiero digital de las criptomonedas debido a su mismo valor actual comercial, siendo una muy redituable acción atacar y apoderarse de este tipo de activos digitales o de utilizar a terceros sin su consentimiento como es el caso del cryptojacking para poder obtenerlas.

El apogeo de las criptomonedas y la diversidad de estas mismas hacen que el cryptojacking sea más rentable que nunca, aunque se hayan impuesto medidas restrictivas a su minado, a su obtención por fuera de medios oficiales, además de las regulaciones impuestas por ciertos países, siguen siendo un sistema de moneda digital difícil de rastrear por las tecnologías que esta usa, por lo cual alguien pueda minar dogecoin una moneda relativamente fácil de minar de bajo costo en el mercado y que después fácilmente se puede pasar a otra cripto como bitcoin o Ethereum, y no dejar pista rastreable de todos estos movimientos, además de que cabe resaltar que se puede hacer desde cualquier parte del mundo donde las leyes del país donde un usuario fue vulnerado, puede que no sean las mismas en el país del atacante(Bijmans et al., 2019).

Este es el principal problema de los delitos informáticos, que al hacerse desde países lejanos, las leyes o las autoridades competentes se ven de manos atadas por las jurisdicciones de cada uno de sus países, ya que no pueden actuar e implementar su sistema de justicia en otro país y menos si no se tienen buenas relaciones, por lo cual muchos de los delitos como el cryptojacking quedan impunes(G. Gomes et al., 2020).

Se puede afirmar entonces que el estado de los ataques cryptojacking, con énfasis en las aplicaciones web están en auge y su porcentaje es uno de los más altos comparados con otros malware si bien no es el más común, si ocupa una porción bastante grande según un informe de Sonicwall para el año 2021 los ataques cryptojacking fueron de 97,1 millones en el año 2021 (Group, 2022), esta cifra es bastante grande y nos muestra que cualquiera de nosotros puede ser un blanco y tener una vulneración, la recomendación es siempre estar a la vanguardia de las actualizaciones de seguridad, y siempre ser precavidos a la hora de navegar por la web.

Al tener estas cifras tan exacerbantes en cuanto a ataques de este tipo a nivel global y solo de los cuales se tiene registro se puede inferir que su estado actual no solo está en su momento más elevado si no, que su tendencia es al alza, tan solo en el último mes del año 2021 diciembre para ser exactos, hubo 13,6 millones de ataques de este tipo, lo cual preocupa bastante, siendo dirigido principalmente hacienda equipos de dominio público o estatal.

Se espera que para el año 2022, su aumento sea aún más significativo llegando inclusive a verse reflejado en cifras de hasta

en un 250% comparado con los datos del mismo periodo pasado, basándonos en estas estimaciones, el aumento de este tipo de ataque se debe a la poca rentabilidad que se genera a la hora de minar criptomonedas debido a la regulaciones que se están empezando a emitir por parte de distintos gobiernos (Group, 2022).

Para el año 2023 los ataques cryptojacking se aumentaron en un 659% comparado con los ataques del año 2021 para un total de ataques de 696.03 millones registrados, se ve una curva de crecimiento sumamente exponencial a medida que va pasando el tiempo.((MSP)», s. f.).

No solo debido a la regulaciones de diferentes gobiernos que inclusive están invirtiendo en monedas digitales y cuyo plan a futuro es volverlas moneda nacional, si no también debido a que el sistema de minado era insostenible a largo plazo debido a que cada transacción en los pool de minado a la hora de estos depositar el porcentaje de ganancias obtenidas por el minero, daban un tipo de decimales extra en cada operación a modo de un tipo de interés por utilizar estos pool, esto desde comienzos del año 2021 se terminó, haciendo insostenible la minería de criptomonedas.

Este cambio desemboco en que se pasara de tener la crisis de las tarjetas gráficas, a en la actualidad estar vendiendo GPU´s de gama alta hasta en 25 dólares ya usadas, todos estos cambios en el paradigma lo que ha hecho que el cryptojacking valla en aumento y sea de los principales problemas de ciberseguridad durante los años venideros debido a que si no es con recursos propios la minería de criptomonedas sigue siendo rentable para los atacantes informáticos.

2.CONCLUSIONES

Habiendo llegado a la conclusión de este artículo, se aprecia la manera en que se manifiesta la sinergia en todos los elementos del sistema cripto, a pesar de que es uno de los sistemas financieros más seguros, ha llegado a ser vulnerado no de manera directa, si no que vulnera al usuario de cualquier tipo de hardware capas de minar criptomonedas, esto nos permite decir que ningún sistema está exento de fallas o vulnerabilidades y que el factor humano siempre es una de las principales causas.(Harish et al., 2021).

Claramente dar a conocer las partes que componen al sistema cripto para poner en contexto todo el funcionamiento del cryptojacking, explicando cómo funciona el sistema financiero de las monedas digitales, permite tener un entendimiento profundo de por qué se practican este tipo de ciberataques cuyas repercusiones caen sobre usuarios finales los cuales son los más vulnerados.

Se pudo apreciar que la integración de la inteligencia artificial la cual también llego al sistema cripto para ayudar a la detección del cryptojacking, por lo cual es una herramienta que se está integrando en muchos sistemas actualmente y servirá de manera íntima con cada sistema mediante el machine y deep learning(Caprolu et al., 2021).

No debemos olvidar siempre como es que mantener las medidas de seguridad correspondientes y saber navegar en la web nos puede ayudar a liberarnos no solo del cryptojacking si no de una infinidad de malwares los cuales pueden causar mucho daño a nuestros dispositivos, es imperativo seguir las recomendaciones de seguridad no solo de nuestro sistema si no de los expertos(Saad et al., 2018).

En ultimas instancias se menciona las causas que desembocan en por que el cryptojacking ha ido en aumento y por qué seguirá en aumento de una manera exponencial, debido a cambios en la economía global, decisiones políticas, cambios en el sistema de minado de los pool a la hora de transferir ganancias, lo cual en ultimas permite que los ciberataques de este tipo sean más frecuentes, ya que son lucrativos además de ser más rentable infectar equipos ajenos para realizar la tarea de minar criptomonedas, que hacer una inversión en equipos propios que no justifique el gasto.

Gracias a la información recopilada en los artículos, de los autores citados en este artículo, se pudo llevar a cabo la investigación y descripción de todos los puntos tratados, para así dar forma a una revisión de un compendio de conocimiento que formo la estructura, además de la base de este artículo en cuestión, ayudando a la interpretación de estos para dar la idea final, por supuesto el resultado que se quería para este fin el cual era revisar el estado actual de los ataques cryptojacking con énfasis en aplicaciones web.

Para concluir al final el articulo mostro que el estado actual de los ataques cryptojacking con énfasis es las aplicaciones web, está más activo que nunca, con 13.6 millones de casos registrados en el año 2022, además de variantes de este, y como las personas son infectadas, aunque no solo personas si no también sitios web y empresas, las cuales son más provechosas para la rentabilidad del atacante, al estas tener más poder y capacidad de minado con un hardware más robusto por lo cual han padecido el flagelo de este tipo de ciberataques(Yulianto et al., 2019).

3.REFERENCIAS

Anita., N., & Vijayalakshmi., M. (2019). Blockchain Security Attack: A Brief Survey. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1-6. https://doi.org/10.1109/ICCCNT45670.2019.8944615

Applied Sciences | Free Full-Text | Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks. (s. f.). Recuperado 30 de noviembre de 2023, de https://www.mdpi.com/2076-3417/12/7/3234

Bijmans, H. L. J., Booij, T. M., & Doerr, C. (2019). Just the Tip of the Iceberg: Internet-Scale Exploitation of Routers for Cryptojacking. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 449-464. https://doi.org/10.1145/3319535.3354230

Cabrera Soto, M., Lage Codorniu, C., Cabrera Soto, M., & Lage Codorniu, C. (2022). Criptomonedas: ¿qué son y qué pretenden ser?*. *Economía y Desarrollo*, *166*(1). http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S0252-85842022000100008&lng=es&nrm=iso&tlng=es

Caprolu, M., Raponi, S., Oligeri, G., & Di Pietro, R. (2021). Cryptomining makes noise: Detecting cryptojacking via Machine Learning. *Computer Communications*, *171*, 126-139. https://doi.org/10.1016/j.comcom.2021.02.016

Carlin, D., Burgess, J., O'Kane, P., & Sezer, S. (2020). You Could Be Mine(d): The Rise of Cryptojacking. *IEEE Security & Privacy*, *18*(2), 16-22. IEEE Security & Privacy. https://doi.org/10.1109/MSEC.2019.2920585

Di Pierro, M. (2017). What Is the Blockchain? *Computing in Science & Engineering*, *19*(5), 92-95. Computing in Science & Engineering. https://doi.org/10.1109/MCSE.2017.3421554

Di Tizio, G., & Nam Ngo, C. (2020). Are You a Favorite Target For Cryptojacking? A Case-Control Study On The Cryptojacking Ecosystem. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 515-520. https://doi.org/10.1109/EuroSPW51379.2020.00075

Díaz, G. (2018, julio 10). Cryptojacking en China afectó más de 1 millón de computadoras en 2 años. *CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas*. https://www.criptonoticias.com/seguridad-bitcoin/cryptojacking-china-afecto-mas-1-millon-computadoras-2-anos/

El Informe de Ciberamenazas 2024 de SonicWall se adentra en las profundidades de los ciberataques y refuerza la necesidad de proveedores de servicios gestionados (MSP). (s. f.). *SonicWall*. Recuperado 25 de junio de 2024, de https://www.sonicwall.com/es-mx/news/sonicwall-threat-data-exposes-depths-of-cyberattacks-propels-the-need-for-managed-service-providers-msps/

Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. (2018). A First Look at Browser-Based Cryptojacking. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 58-66. https://doi.org/10.1109/EuroSPW.2018.00014

Gomes, F., & Correia, M. (2020). Cryptojacking Detection with CPU Usage Metrics. *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 1-10. https://doi.org/10.1109/NCA51143.2020.9306696

Gomes, G., Dias, L., & Correia, M. (2020). CryingJackpot: Network Flows and Performance Counters against Cryptojacking. *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 1-10. https://doi.org/10.1109/NCA51143.2020.9306698

Group, I. D. M. (2022, junio 24). *Aumentarán las variantes y las técnicas nuevas de cryptojacking | Endpoint*. IT Digital Security; IT Digital Media Group. https://www.itdigitalsecurity.es/endpoint/2022/06/aumentaran-las-variantes-y-las-tecnicas-nuevas-de-cryptojacking

Harish, R., kumar, A. A., Kumar, V. A., & Amritha, P. P. (2021). Facilitating Cryptojacking Through Internet Middle Boxes. En T. Sengodan, M. Murugappan, & S. Misra (Eds.), *Advances in Electrical and Computer Technologies* (pp. 41-52). Springer Nature. https://doi.org/10.1007/978-981-15-9019-1_4

Jayasinghe, K., & Poravi, G. (2020). A Survey of Attack Instances of Cryptojacking Targeting Cloud Infrastructure. *Proceedings of the 2020 2nd Asia Pacific Information Technology Conference*, 100-107. https://doi.org/10.1145/3379310.3379323

Khiruparaj, T. P., Abishek Madhu, V., & Sathia Bhama, P. R. K. (2021). Unmasking File-Based Cryptojacking. En J. D. Peter, S. L. Fernandes, & A. H. Alavi (Eds.), *Intelligence in Big Data Technologies—Beyond the Hype* (pp. 137-146). Springer. https://doi.org/10.1007/978-981-15-5285-4_13

Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2023, noviembre 24). *cryptoRAN: A review on cryptojacking and ransomware attacks w.r.t. banking industry -- threats, challenges, & problems*. arXiv.Org. https://arxiv.org/abs/2311.14783v1

Meland, P. H., Johansen, B. H., & Sindre, G. (2019). An Experimental Analysis of Cryptojacking Attacks. En A. Askarov,

R. R. Hansen, & W. Rafnsson (Eds.), *Secure IT Systems* (pp. 155-170). Springer International Publishing. https://doi.org/10.1007/978-3-030-35055-0_10

Pérez Lietor, Á. (2020). *Introducción al Cryptojacking y creación de website maliciosa*. https://ebuah.uah.es/dspace/handle/10017/40887

Petrov, I., Invernizzi, L., & Bursztein, E. (2020, junio 18). *CoinPolice:Detecting Hidden Cryptojacking Attacks with Neural Networks*. arXiv.Org. https://arxiv.org/abs/2006.10861v2

Razali, M. A., & Mohd Shariff, S. (2019). CMBlock: In-Browser Detection and Prevention Cryptojacking Tool Using Blacklist and Behavior-Based Detection Method. En H. Badioze Zaman, A. F. Smeaton, T. K. Shih, S. Velastin, T. Terutoshi, N. Mohamad Ali, & M. N. Ahmad (Eds.), *Advances in Visual Informatics* (pp. 404-414). Springer International Publishing. https://doi.org/10.1007/978-3-030-34032-2_36

Saad, M., Khormali, A., & Mohaisen, A. (2018, septiembre 6). *End-to-End Analysis of In-Browser Cryptojacking*. arXiv.Org. https://arxiv.org/abs/1809.02152v1

Saad, M., Khormali, A., & Mohaisen, A. (2019). Dine and Dash: Static, Dynamic, and Economic Analysis of In-Browser Cryptojacking. *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 1-12. https://doi.org/10.1109/eCrime47957.2019.9037576

Sigler, K. (2018). Crypto-jacking: How cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, *2018*(9), 12-14. https://doi.org/10.1016/S1361-3723(18)30086-1

Tanana, D. (2020). Behavior-Based Detection of Cryptojacking Malware. *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 0543-0545. https://doi.org/10.1109/USBEREIT48449.2020.9117732

Tanana, D., & Tanana, G. (2020). Advanced Behavior-Based Technique for Cryptojacking Malware Detection. *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 1-4. https://doi.org/10.1109/ICSPCS50536.2020.9310048

Urdaneta Bernal, C. (2018). *Expansión y optimización de recursos de RIG de minería de criptomonedas*. http://repository.udistrital.edu.co/handle/11349/13873

Val Gangonells, O. (2020). *La minería en criptomonedas* [Bachelor thesis, Universitat Politècnica de Catalunya]. https://upcommons.upc.edu/handle/2117/178297

Varlioglu, S., Elsayed, N., ElSayed, Z., & Ozer, M. (2022). The Dangerous Combo: Fileless Malware and Cryptojacking.

SoutheastCon 2022, 125-132. https://doi.org/10.1109/SoutheastCon48659.2022.9764043

Xu, G., Dong, W., Xing, J., Lei, W., Liu, J., Gong, L., Feng, M., Zheng, X., & Liu, S. (2023). Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. *Digital Communications and Networks*, *9*(5), 1169-1179. https://doi.org/10.1016/j.dcan.2022.04.030

Yulianto, A. D., Sukarno, P., Warrdana, A. A., & Makky, M. A. (2019). Mitigation of Cryptojacking Attacks Using Taint Analysis. *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 234-238. https://doi.org/10.1109/ICITISEE48480.2019.9003742

Zimba, A., Wang, Z., & Mulenga, M. (2019). Cryptojacking injection: A paradigm shift to cryptocurrency-based web-centric internet attacks. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 40-59. https://doi.org/10.1080/10919392.2019.1552747