Fortinet ha publicado correcciones para una vulnerabilidad crítica que afecta a FortiWeb, la cual podría permitir que un atacante no autenticado ejecute comandos arbitrarios en la base de datos en instancias vulnerables.

Identificada como CVE-2025-25257, esta falla cuenta con una puntuación CVSS de 9.6 sobre un máximo de 10.0.

"Una neutralización inadecuada de elementos especiales utilizados en una instrucción SQL ('Inyección SQL') [CWE-89] en FortiWeb podría permitir que un atacante no autenticado ejecute código SQL no autorizado a través de solicitudes HTTP o HTTPS manipuladas," señaló Fortinet en un aviso emitido esta semana.

La vulnerabilidad afecta a las siguientes versiones:

- FortiWeb de la 7.6.0 a la 7.6.3 (Actualizar a la 7.6.4 o superior)
- FortiWeb de la 7.4.0 a la 7.4.7 (Actualizar a la 7.4.8 o superior)
- FortiWeb de la 7.2.0 a la 7.2.10 (Actualizar a la 7.2.11 o superior)
- FortiWeb de la 7.0.0 a la 7.0.10 (Actualizar a la 7.0.11 o superior)

Kentaro Kawane, de GMO Cybersecurity, quien recientemente fue reconocido por reportar una serie de fallos críticos en Cisco Identity Services e ISE Passive Identity Connector (CVE-2025-20286, CVE-2025-20281 y CVE-2025-20282), ha sido acreditado como el descubridor de esta vulnerabilidad.

Según un análisis publicado hoy por watchTowr Labs, el problema radica en una función llamada *"get_fabric_user_by_token"*, vinculada al componente Fabric Connector, el cual sirve como puente entre FortiWeb y otros productos de Fortinet.

Esta función es invocada por otra función denominada *"fabric_access_check"*, la cual es llamada desde tres diferentes puntos de acceso API: */api/fabric/device/status*, */api/v[0-9]/fabric/widget/[a-z]+* y */api/v[0-9]/fabric/widget*.

El problema ocurre porque los datos controlados por el atacante —enviados mediante un encabezado de autorización Bearer token dentro de una solicitud HTTP especialmente diseñada— se transfieren directamente a una consulta SQL sin una sanitización adecuada que garantice que no contengan código malicioso.

El ataque podría escalar a ejecución remota de código si se incorpora una instrucción *SELECT ... INTO OUTFILE* para escribir una carga maliciosa en un archivo del sistema operativo subyacente, aprovechando el hecho de que la consulta se ejecuta con privilegios del usuario "mysql", pudiendo activarse posteriormente con Python.

"La nueva versión de la función sustituye la antigua consulta con formato de cadena por sentencias preparadas – un intento razonable para evitar inyecciones SQL directas," afirmó el investigador de seguridad Sina Kheirkhah.

Como medida temporal hasta que se apliquen los parches correspondientes, se recomienda a los usuarios desactivar la interfaz administrativa HTTP/HTTPS.

Dado que en ocasiones anteriores actores maliciosos han explotado vulnerabilidades en dispositivos Fortinet, es crucial que los usuarios actualicen a la versión más reciente lo antes posible para reducir riesgos potenciales.

Investigadores en ciberseguridad han descubierto una grave vulnerabilidad que permite que claves APP_KEY filtradas de Laravel sean utilizadas de forma maliciosa para obtener capacidades de ejecución remota de código en cientos de aplicaciones.

> *«La APP_KEY de Laravel, crucial para cifrar datos sensibles, se filtra con frecuencia de forma pública (por ejemplo, en GitHub)»,* señaló GitGuardian. *«Si un atacante accede a esta clave, puede aprovechar una falla de deserialización para ejecutar código arbitrario en el servidor, comprometiendo tanto los datos como la infraestructura».*

La empresa, en conjunto con Synacktiv, informó que logró extraer más de 260,000 claves APP_KEY desde GitHub entre 2018 y el 30 de mayo de 2025, identificando más de 600 aplicaciones Laravel vulnerables en el proceso. GitGuardian indicó que se detectaron más de 10,000 claves únicas en GitHub, de las cuales 400 fueron confirmadas como funcionales.

La APP_KEY es una clave de cifrado aleatoria de 32 bytes que se genera al instalar Laravel. Se guarda en el archivo `.env` de la aplicación y se emplea para cifrar y descifrar datos, generar cadenas aleatorias seguras, firmar/verificar datos y crear tokens de autenticación únicos, siendo así un componente crítico de seguridad.

GitGuardian advirtió que la función `decrypt()` de Laravel presenta una vulnerabilidad, ya que deserializa automáticamente los datos descifrados, lo que abre la puerta a una posible ejecución remota de código.

> *«En aplicaciones Laravel, si un atacante obtiene la APP_KEY y logra invocar la función `decrypt()` con una carga maliciosa, puede ejecutar código remotamente en el servidor web Laravel»*, explicó el investigador de seguridad Guillaume Valadon.
>
> *«Esta vulnerabilidad fue inicialmente documentada como CVE-2018-15133, que afectaba versiones anteriores a Laravel 5.6.30. Sin embargo, el vector de ataque sigue vigente en versiones más recientes cuando los desarrolladores configuran explícitamente la serialización de sesiones en cookies mediante `SESSION_DRIVER=cookie`, como lo demuestra la CVE-2024-55556«.*

Cabe señalar que la CVE-2018-15133 ha sido explotada en entornos reales por actores maliciosos relacionados con el malware AndroxGh0st, tras escanear la red en busca de aplicaciones Laravel con archivos `.env` mal configurados.

Análisis adicionales revelaron que el 63% de las exposiciones de APP_KEY provienen de

archivos `.env` (o variantes), que comúnmente también contienen otros secretos sensibles como credenciales de bases de datos, tokens de almacenamiento en la nube, y datos confidenciales de plataformas de comercio electrónico, herramientas de soporte al cliente, e incluso servicios de inteligencia artificial.

Más preocupante aún es que aproximadamente 28,000 combinaciones de APP_KEY y APP_URL fueron expuestas simultáneamente en GitHub. De ellas, cerca del 10% resultaron válidas, lo que deja a 120 aplicaciones vulnerables a ataques triviales de ejecución remota de código.

Dado que la configuración APP_URL especifica la URL base de la aplicación, la exposición conjunta de APP_URL y APP_KEY permite a los atacantes potencialmente acceder directamente a la aplicación, obtener cookies de sesión y tratar de descifrarlas usando la clave filtrada.

Eliminar secretos de los repositorios no es suficiente, especialmente si ya han sido clonados o almacenados en caché por herramientas de terceros. Los desarrolladores necesitan contar con un proceso claro de rotación de claves, complementado con monitoreo continuo que detecte futuras apariciones de cadenas sensibles en logs de CI, compilaciones de imágenes, y capas de contenedores.

> *«Los desarrolladores nunca deben simplemente borrar las APP_KEY expuestas de los repositorios sin una rotación adecuada»,* advirtió GitGuardian. *«La respuesta correcta incluye: rotar inmediatamente la APP_KEY comprometida, actualizar todos los sistemas productivos con la nueva clave e implementar monitoreo continuo de secretos para evitar nuevas filtraciones».*

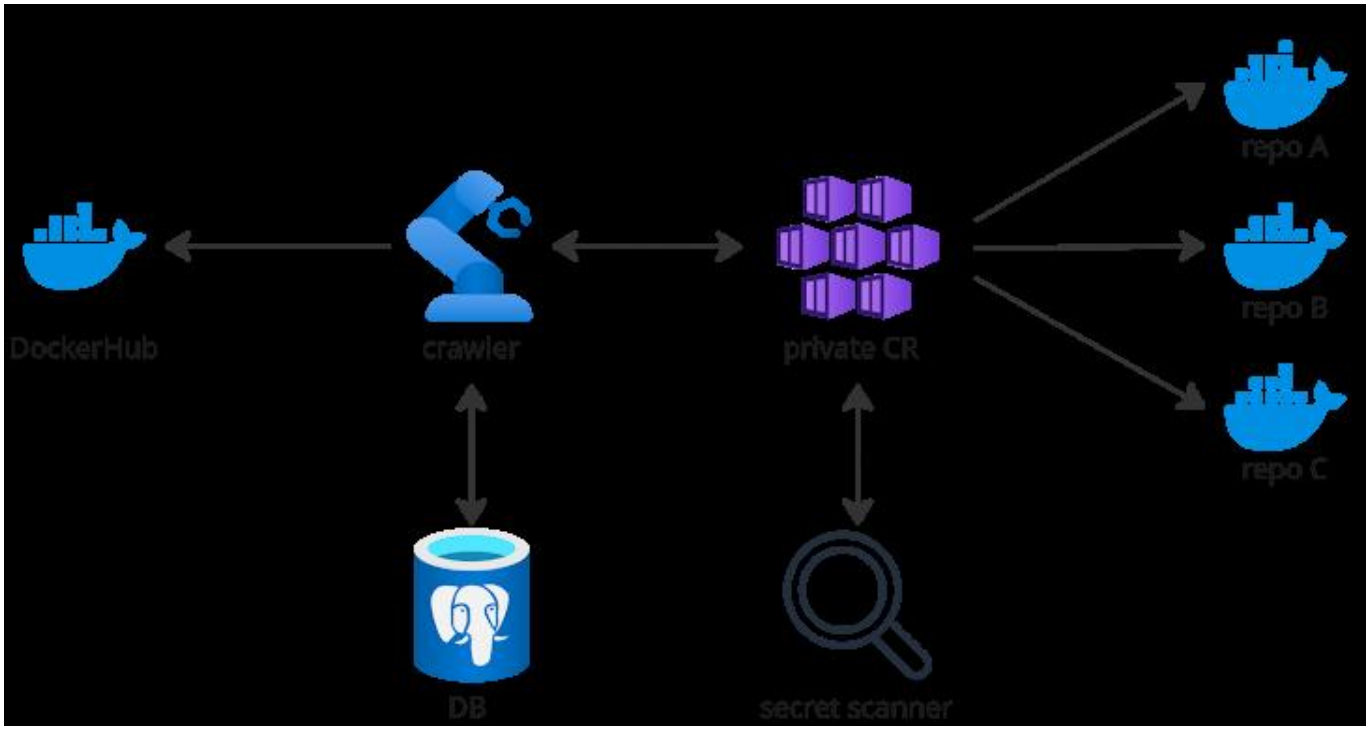
Este tipo de incidentes se enmarca también dentro de una categoría más amplia de vulnerabilidades de deserialización en PHP, donde herramientas como phpggc permiten a atacantes crear cadenas de gadgets que activan comportamientos inesperados durante la carga de objetos. En entornos Laravel con claves expuestas, estos gadgets pueden llevar a

una ejecución total de código sin necesidad de vulnerar la lógica de la aplicación.

Esta revelación se produce después de que GitGuardian informara haber encontrado «la asombrosa cifra de 100,000 secretos válidos» en imágenes de Docker accesibles públicamente en el registro de DockerHub. Entre ellos se incluyen credenciales relacionadas con Amazon Web Services (AWS), Google Cloud y tokens de GitHub.

Un análisis reciente de Binarly sobre más de 80,000 imágenes de Docker únicas, correspondientes a 54 organizaciones y 3,539 repositorios, también descubrió 644 secretos únicos, entre ellos credenciales genéricas, JSON Web Tokens, cabeceras de autorización básica HTTP, claves API de Google Cloud, tokens de acceso AWS y de CircleCI.

> *«Los secretos aparecen en una amplia variedad de archivos, incluyendo código fuente, archivos de configuración e incluso archivos binarios grandes, lugares donde muchos escáneres actuales no detectan nada»,* dijo la compañía. *«Además, la inclusión de repositorios Git completos dentro de imágenes de contenedores representa un riesgo de seguridad grave y frecuentemente ignorado».*



Y eso no es todo. La rápida adopción del Model Context Protocol (MCP) para habilitar flujos de trabajo automatizados en aplicaciones empresariales de IA ha abierto nuevos vectores de ataque, siendo especialmente preocupante la filtración de secretos desde servidores MCP publicados en repositorios de GitHub.

GitGuardian descubrió que 202 de estos servidores filtraron al menos un secreto, lo que representa un 5.2% del total de repositorios MCP analizados —una cifra que, según la empresa, es *«ligeramente superior al 4.6% observado en todos los repositorios públicos»,* lo que convierte a los servidores MCP en una nueva fuente de filtraciones de secretos.

Aunque esta investigación se centra en Laravel, el problema de fondo—secretos mal protegidos en repositorios públicos—afecta también a otros entornos. Las organizaciones deben considerar el uso de escaneo centralizado de secretos, guías específicas para reforzar la seguridad de Laravel, y patrones de desarrollo seguros para el manejo de archivos `.env` y secretos dentro de contenedores.

Expertos en ciberseguridad han identificado nuevos elementos vinculados a *ZuRu*, un malware dirigido a macOS que se disemina por medio de versiones alteradas de software auténtico.

Según un reciente informe publicado por *SentinelOne* en colaboración con *The Hacker News*, el malware fue detectado a finales de mayo de 2025, haciéndose pasar por la herramienta de gestión de servidores y cliente SSH multiplataforma llamada *Termius*.

> *"El malware ZuRu sigue atacando a usuarios de macOS que buscan herramientas legítimas de trabajo, ajustando su método de carga y comunicación C2 para instalar puertas traseras en los equipos afectados",* afirmaron los investigadores Phil Stokes y Dinesh Devadoss.

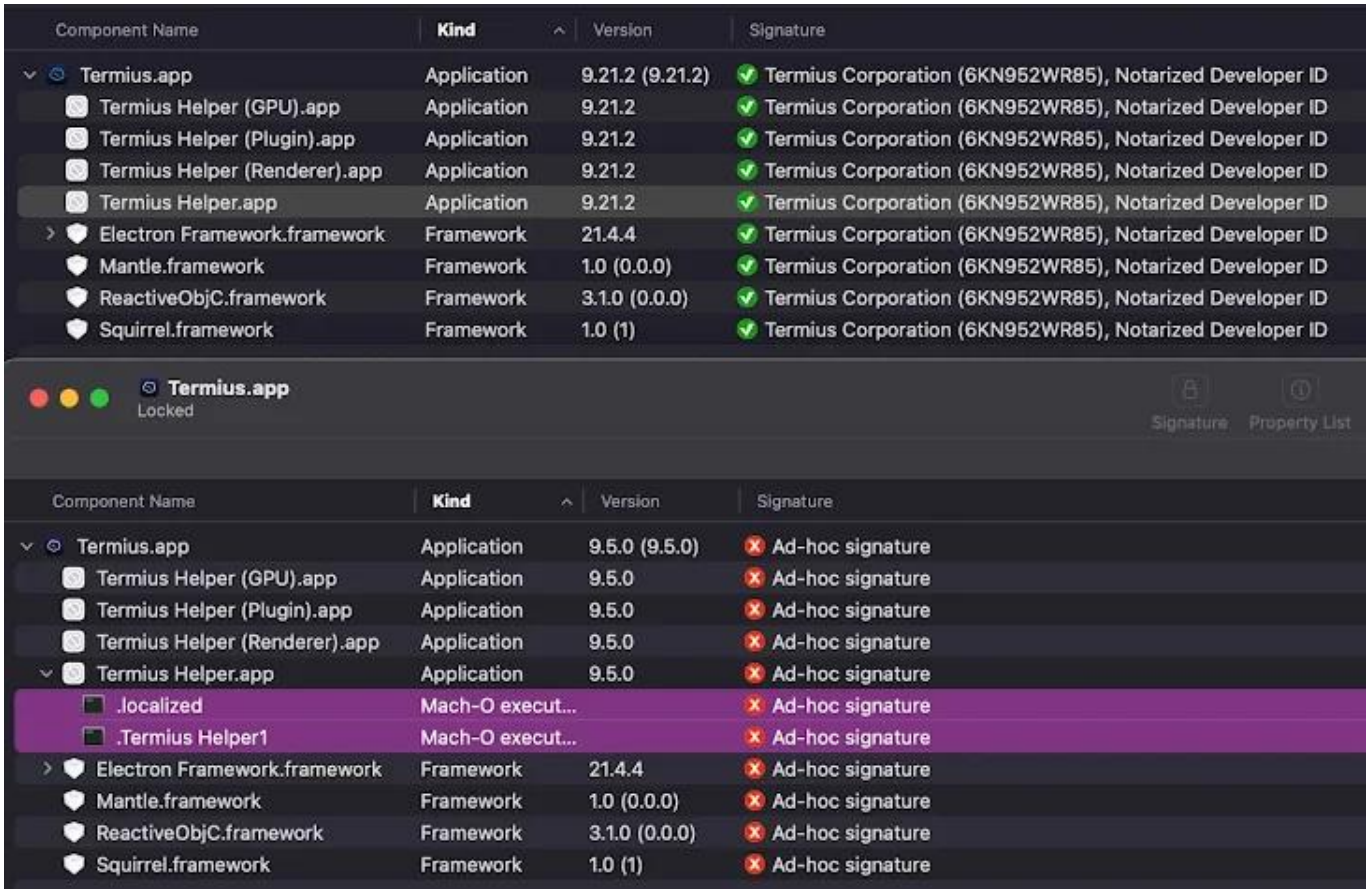
El primer registro de ZuRu se remonta a septiembre de 2021, cuando un usuario en el portal chino Zhihu alertó sobre una campaña maliciosa que manipulaba búsquedas de *iTerm2* —una terminal auténtica de macOS— para redirigir a víctimas a sitios engañosos y distribuir el malware.

En enero de 2024, el laboratorio *Jamf Threat Labs* identificó un malware distribuido mediante aplicaciones piratas para macOS que compartía características con ZuRu. Algunas de las apps comprometidas más conocidas incluyen *Remote Desktop* de Microsoft para Mac, *SecureCRT* y *Navicat*.

El uso de resultados patrocinados en buscadores como vector de propagación sugiere que los atacantes detrás de ZuRu actúan de forma más casual que dirigida, enfocándose especialmente en usuarios que buscan herramientas de administración remota o de bases de datos.

Tal como en las versiones detectadas por Jamf, los componentes más recientes de ZuRu incorporan una versión manipulada de la herramienta de post-explotación de código abierto *Khepri*, que permite controlar remotamente los sistemas comprometidos.

> *"El malware se distribuye en una imagen de disco .dmg, la cual contiene una copia intervenida de la app original Termius.app"*, explicaron. *"Como se ha modificado el paquete de la app, los atacantes reemplazaron la firma original del desarrollador por una firma improvisada para pasar los controles de seguridad de macOS."*



La app alterada incluye dos binarios adicionales dentro del paquete *Termius Helper.app*: uno llamado *".localized" que descarga y activa un beacon C2 de Khepri desde "download.termius[.]info"*, y otro llamado ".Termius Helper1", que es simplemente una copia renombrada del auxiliar legítimo de Termius.

> *"Si bien Khepri ya había sido empleado en variantes anteriores de ZuRu, esta nueva*

> *forma de manipular una aplicación difiere de los métodos previos utilizados por el grupo atacante”,* señalaron los analistas.
>
> *“En ediciones anteriores, los desarrolladores del malware modificaban el ejecutable principal del paquete agregando un comando de carga que enlazaba una biblioteca externa (.dylib), la cual funcionaba como cargador para el backdoor de Khepri y sus mecanismos de permanencia.”*

El cargador no solo descarga el beacon de Khepri, sino que también asegura que el malware se mantenga activo en el sistema, verificando si ya está instalado en la ruta “/tmp/.fseventsd” y comparando el hash MD5 del archivo con el del servidor.

Si el valor hash no coincide, se descarga una versión actualizada. Esta función probablemente actúe como mecanismo de actualización, aunque SentinelOne también plantea que podría usarse para verificar la integridad del archivo y evitar corrupción.

La variante de Khepri integrada actúa como un implante de comando y control que permite al atacante realizar reconocimiento del sistema, transferencia de archivos, ejecución y control de procesos, así como ejecución de comandos con retorno de salida. La comunicación con el beacon se realiza a través del servidor “ctl01.termius[.]fun”.

> *“La nueva edición de macOS.ZuRu mantiene la estrategia del atacante de modificar aplicaciones legítimas empleadas por desarrolladores y personal de TI”,* concluyeron los investigadores.
>
> *“El cambio de técnica —de la inyección Dylib a la alteración de una aplicación auxiliar embebida— parece buscar evadir mecanismos específicos de detección. Aun así, el uso continuo de ciertas tácticas, como los patrones en dominios, nombres de archivo y técnicas de persistencia, indica que siguen teniendo éxito en*

> *entornos sin protección de endpoints adecuada.”*

Los usuarios de criptomonedas son el objetivo de una campaña activa de ingeniería social que utiliza falsas empresas emergentes para engañarlos y hacer que descarguen malware capaz de robar activos digitales, tanto en sistemas Windows como macOS.

> *«Estas operaciones maliciosas se hacen pasar por compañías de inteligencia artificial, videojuegos y Web3, utilizando cuentas falsas en redes sociales y documentación de proyectos alojada en plataformas legítimas como Notion y GitHub»*, explicó la investigadora Tara Gould de Darktrace en un informe.

Esta elaborada estafa en redes sociales lleva activa un tiempo, y una versión anterior, en diciembre de 2024, utilizó plataformas falsas de videollamadas para engañar a las víctimas con la excusa de discutir oportunidades de inversión, luego de contactarlas por apps de mensajería como Telegram.

Los usuarios que descargaban el supuesto software de reuniones eran infectados de forma sigilosa con malware tipo stealer como Realst. Esta campaña fue nombrada *Meeten* por la empresa Cado Security (adquirida por Darktrace a principios de este año), en referencia a uno de los servicios de videoconferencias falsos utilizados.

Dicho esto, hay indicios de que esta actividad podría estar ocurriendo desde al menos marzo de 2024, cuando el equipo de Jamf Threat Labs descubrió un dominio llamado *meethub[.]gg* utilizado para distribuir el malware Realst.

Los hallazgos más recientes de Darktrace indican que esta campaña no solo continúa siendo una amenaza activa, sino que ahora abarca una mayor variedad de temáticas, como inteligencia artificial, videojuegos, Web3 y redes sociales.

Además, se ha observado que los atacantes aprovechan cuentas comprometidas en X (antes

Twitter), tanto de empresas como de empleados —principalmente aquellas verificadas— para acercarse a sus objetivos y dar una apariencia legítima a sus falsas organizaciones.

> *«Utilizan sitios frecuentemente empleados por compañías de software como X, Medium, GitHub y Notion»,* señaló Gould. *«Cada empresa falsa cuenta con un sitio web profesional que incluye empleados, blogs de productos, documentos técnicos y hojas de ruta.»*

Una de estas compañías ficticias es Eternal Decay (@metaversedecay), que afirma ser un juego basado en blockchain, y ha compartido imágenes legítimas alteradas digitalmente en X para aparentar que participa en conferencias. El objetivo es construir una presencia en línea creíble que aumente la posibilidad de que las víctimas se infecten.

Algunas de las otras empresas falsas identificadas son las siguientes:

- BeeSync (X cuentas: @BeeSyncAI, @AIBeeSync)
- Buzzu (X cuentas: @BuzzuApp, @AI_Buzzu, @AppBuzzu, @BuzzuApp)
- Cloudsign (cuenta X: @cloudsignapp)
- Dexis (cuenta X: @DexisApp)
- KlastAI (cuenta X: Enlaces a la cuenta X de Pollens AI)
- Lunelior
- NexLoop (cuenta X: @nexloopspace)
- NexoraCore
- NexVoo (cuenta X: @Nexvoospace)
- Pollens AI (X cuentas: @pollensapp, @Pollens_app)
- Slax (X cuentas: @SlaxApp, @Slax_app, @slaxproject)
- Solune (X cuenta: @soluneapp)
- Swox (X cuentas: @SwoxApp, @Swox_AI, @swox_app, @App_Swox, @AppSwox, @SwoxProject, @ProjectSwox)
- Wasper (X cuentas: @wasperAI, @WasperSpace)
- YondaAI (cuenta X: @yondaspace)

El ataque comienza cuando una de estas cuentas controladas por los atacantes contacta a una víctima a través de X, Telegram o Discord, invitándola a probar su software a cambio de un pago en criptomonedas.

Si la víctima acepta participar, es redirigida a un sitio web ficticio, donde se le pide ingresar un código de registro proporcionado por el supuesto empleado, para así descargar una aplicación en formato Electron para Windows o una imagen de disco (DMG) para macOS, dependiendo del sistema operativo.

En equipos Windows, al ejecutar la aplicación maliciosa, la víctima ve una pantalla de verificación de Cloudflare, mientras en segundo plano se analiza el sistema y se descarga un instalador MSI que se ejecuta de forma oculta. Aunque no se conoce con certeza el contenido del malware, se sospecha que se trata de un ladrón de información.

En macOS, por otro lado, la descarga lleva a la instalación del conocido malware Atomic macOS Stealer (AMOS), diseñado para robar documentos, datos de navegadores web y monederos de criptomonedas, y enviar esta información a servidores externos.

El archivo DMG también contiene un script que configura persistencia en el sistema mediante un *Launch Agent*, asegurando que la app se ejecute automáticamente al iniciar sesión. Además, descarga y lanza un binario en Objective-C/Swift que registra el uso de la aplicación y los tiempos de interacción del usuario, los cuales son transmitidos a un servidor remoto.

Darktrace también señaló que esta campaña comparte tácticas similares con las empleadas por un grupo de tráfico conocido como Crazy Evil, que engaña a las víctimas para que instalen malware como StealC, AMOS y Angel Drainer.

> *«Si bien no está claro si estas campañas [...] pueden atribuirse a Crazy Evil o a alguno de sus subgrupos, las técnicas utilizadas son similares»*, dijo Gould. *«Esta campaña demuestra el esfuerzo que hacen los actores de amenazas para hacer que estas empresas falsas parezcan legítimas, con el fin de robar criptomonedas,*

> *además del uso de nuevas variantes de malware diseñadas para evadir detección.»*

Si eres jugador frecuente del casino online de Betano Chile Casino https://betanobet-cl.com/casino/, seguramente ya sabes que las tragamonedas son uno de los juegos más accesibles, entretenidos y repletos de posibilidades de ganancia. Pero si tu objetivo es jugar con inteligencia y estrategia, no basta con elegir por estética o popularidad. Hay un dato técnico fundamental que puede marcar una gran diferencia a largo plazo: el RTP, o retorno al jugador.

En este artículo, te contamos todo lo que necesitas saber sobre este indicador y te presentamos el ranking con las 10 tragamonedas con el RTP más alto disponibles actualmente en Betano Chile. Con esta información podrás seleccionar mejor tus juegos, aprovechar tus depósitos y, por qué no, acercarte más a esa jugada que tanto estás esperando.

¿Qué significa RTP en una tragamonedas?

El RTP (Return to Player, en inglés) representa el porcentaje teórico del dinero apostado que una tragamonedas devuelve a los jugadores a lo largo del tiempo. Por ejemplo, si una tragamonedas tiene un RTP del 97%, significa que, estadísticamente, por cada $100 apostados, se devuelven $97 en premios.

Es importante aclarar que el RTP no refleja lo que pasará en una sola sesión. Este porcentaje se calcula en base a millones de giros, por lo que no garantiza resultados a corto plazo. Aun así, cuanto más alto sea el RTP, mejores son las probabilidades a favor del jugador. Por eso, cada vez más usuarios experimentados eligen juegos con RTP elevados, especialmente en casinos serios como Betano Chile APP, donde esta información está disponible y verificada.

¿Por qué es tan importante conocer el RTP antes de jugar?

Cuando ingresas a la sección de tragamonedas de Betano, podés encontrar cientos de títulos distintos, con diferentes temáticas, funciones especiales y mecánicas. Pero lo que muchos no ven es que detrás de cada uno hay una matemática diseñada para determinar la frecuencia y el tamaño de los premios.

Jugar sin conocer el RTP es como apostar a ciegas. Dos tragamonedas con el mismo diseño pueden tener retornos al jugador muy distintos. Y si bien ningún juego asegura ganancia, elegir aquellos con RTP más alto te sitúa en una posición estadísticamente más favorable. Además, si combinas esto con promociones activas, bonos de bienvenida y apuestas gratuitas, puedes maximizar aún más el valor de cada giro.

Las 10 tragamonedas con mayor RTP en Betano Chile

A continuación, te detallamos el ranking con las tragamonedas con mejor retorno teórico al jugador que podés encontrar hoy en la plataforma de Betano. Todas estas opciones están disponibles tanto en versión de escritorio como en la app móvil para Android e iOS.

1. Dead or Alive 2 – RTP: 98.0%
   Con temática de western, esta tragamonedas de NetEnt es ideal para jugadores que buscan emoción y grandes premios. Es de alta volatilidad, lo que significa que paga con menor frecuencia pero ofrece premios muy altos.
2. White Rabbit – RTP: 97.7%
   Inspirada en Alicia en el País de las Maravillas, este título de Big Time Gaming usa la mecánica Megaways y ofrece una experiencia envolvente con expansión de carretes y giros adicionales.
3. Guns N’ Roses – RTP: 96.98%
   Esta tragamonedas musical de NetEnt no solo destaca por su banda sonora legendaria, sino también por sus funciones especiales como multiplicadores aleatorios

y giros gratis temáticos.

4. Immortal Romance – RTP: 96.9%
   Una historia de vampiros y romance que se ha convertido en clásico de Microgaming. Cuenta con múltiples personajes y bonificaciones desbloqueables.
5. Secrets of Christmas – RTP: 96.7%
   Perfecta para los que disfrutan del espíritu navideño todo el año. Incluye comodines, multiplicadores y una ronda de bonificación con regalos.
6. Christmas Carol Megaways – RTP: 96.6%
   Una versión de Pragmatic Play del clásico de Dickens. Utiliza Megaways, lo que genera miles de combinaciones posibles y bonificaciones variables.
7. Rick and Morty Megaways – RTP: 96.6%
   Basada en la exitosa serie animada, esta tragamonedas incluye múltiples funciones de bonificación inspiradas en los personajes. Ofrece mucha interacción y buenos pagos.
8. Jingle Spin – RTP: 96.5%
   Otro juego de NetEnt con temática navideña, aunque más moderno y con funciones como giros misteriosos, monedas multiplicadoras y comodines aleatorios.
9. Starburst – RTP: 96.1%
   Clásico de clásicos. Simple, colorido y muy fluido. Ideal para quienes buscan sesiones más tranquilas y juegos de baja volatilidad.
10. Mega Fortune – RTP: 96.0%
    Famosa por sus jackpots progresivos. Aunque el RTP base es de 96%, sus botes acumulados pueden cambiar la vida de un jugador en un solo giro.

¿Cómo elegir bien entre estas tragamonedas?

Todas las tragamonedas del ranking tienen RTP elevado, pero también presentan diferencias importantes en cuanto a volatilidad, diseño, complejidad y tipos de bonificación. Por eso, tu elección no debe basarse solo en el porcentaje de retorno, sino también en tu estilo de juego.

Si quieres sesiones largas y tranquilas, con premios frecuentes aunque más pequeños, te conviene un juego como Starburst o Secrets of Christmas. En cambio, si prefieres jugársela por premios grandes aunque menos frecuentes, Dead or Alive 2 o Mega Fortune pueden ser

las mejores opciones.

Además, considera si estás jugando con fondos propios o con alguna promoción activa. Betano Chile suele ofrecer bonos de bienvenida de hasta $200.000 CLP para nuevos usuarios, más giros gratis y torneos temporales. Aprovechar estas promociones en tragamonedas con RTP alto mejora tu rentabilidad a largo plazo.

Estrategias para aprovechar al máximo tu juego

Aunque las tragamonedas son juegos de azar, existen algunas buenas prácticas que puedes aplicar para aumentar tus posibilidades. Primero, siempre revisa el RTP y la volatilidad del juego antes de apostar. Segundo, si juegas con bonos, elige juegos que cuenten para liberar el rollover. Y tercero, establece un presupuesto diario o semanal para jugar con responsabilidad.

Conclusión

Saber elegir una tragamonedas no solo implica que te guste su estética o temática, sino que también sepas interpretar datos clave como el RTP. En Betano Chile, esta información está siempre visible, lo que permite a los jugadores actuar con mayor conciencia y tomar decisiones más inteligentes. Recuerda jugar con responsabilidad.

Los actores maliciosos están aprovechando interfaces expuestas del Java Debug Wire Protocol (JDWP) para obtener capacidades de ejecución de código y desplegar mineros de criptomonedas en sistemas comprometidos.

> *“El atacante utilizó una versión modificada de XMRig con una configuración codificada de forma fija, lo que le permitió evitar argumentos sospechosos en la línea de comandos, que usualmente son detectados por los defensores. La carga*

> *útil empleaba proxies de pools de minería para ocultar la dirección de su billetera de criptomonedas, impidiendo así que los investigadores rastrearan su origen»,* señalaron los investigadores de Wiz, Yaara Shriki y Gili Tikochinski, en un informe publicado esta semana.

La empresa de seguridad en la nube —que está en proceso de adquisición por Google Cloud— indicó que detectó esta actividad a través de sus servidores honeypot con TeamCity, una herramienta popular para integración y entrega continua (CI/CD).

JDWP es un protocolo de comunicación utilizado en Java con fines de depuración. Permite a los desarrolladores usar un depurador para trabajar con una aplicación Java que se ejecuta en otro proceso, ya sea en la misma máquina o de forma remota.

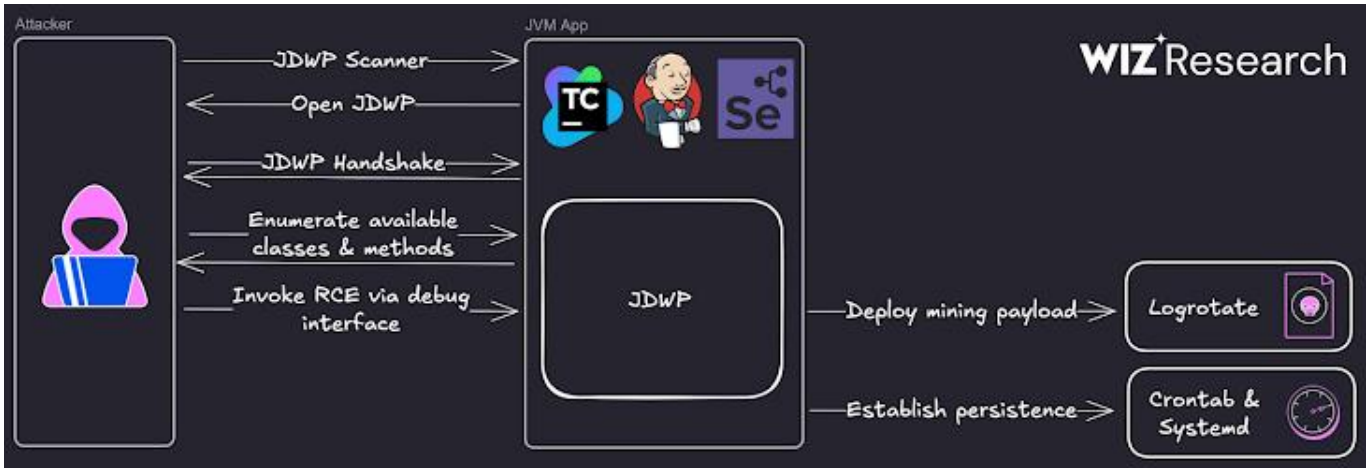
Sin embargo, dado que JDWP carece de mecanismos de autenticación o control de acceso, exponer este servicio a Internet representa un vector de ataque que puede ser explotado como punto de entrada, permitiendo el control total sobre el proceso Java en ejecución.

En resumen, esta mala configuración puede ser usada para inyectar y ejecutar comandos arbitrarios, establecer persistencia y ejecutar cargas maliciosas.

> *“Aunque JDWP no está activado por defecto en la mayoría de las aplicaciones Java, sí es ampliamente utilizado en entornos de desarrollo y depuración. Muchas aplicaciones populares inician automáticamente un servidor JDWP al ejecutarse en modo debug, frecuentemente sin advertir al desarrollador sobre los riesgos. Si no se protege adecuadamente o se deja expuesto, puede permitir vulnerabilidades de ejecución remota de código (RCE)»*. explicó Wiz.

Algunas de las aplicaciones que pueden activar un servidor JDWP en modo debug incluyen TeamCity, Jenkins, Selenium Grid, Elasticsearch, Quarkus, Spring Boot y Apache Tomcat.

Datos de GreyNoise muestran que más de 2,600 direcciones IP han estado escaneando endpoints JDWP en las últimas 24 horas, de las cuales más de 1,500 son clasificadas como maliciosas y otras 1,100 como sospechosas. La mayoría de estas direcciones provienen de China, Estados Unidos, Alemania, Singapur y Hong Kong.



En los ataques monitoreados por Wiz, los actores maliciosos explotan el hecho de que la Máquina Virtual de Java (JVM) escucha conexiones del depurador en el puerto 5005, lo que les permite escanear la red en busca de puertos JDWP abiertos. En la siguiente etapa, se envía una solicitud JDWP-Handshake para verificar si la interfaz está activa y así establecer una sesión.

Una vez confirmada la exposición e interactividad del servicio, los atacantes ejecutan un comando curl para descargar y ejecutar un script shell de tipo dropper que realiza una serie de acciones:

- Elimina procesos de minería competidores o que usen alto CPU.
- Descarga una versión modificada del minero XMRig desde un servidor externo (“awarmcorner[.]world”) a la ruta `~/.config/logrotate`, adaptado a la arquitectura del sistema.
- Establece persistencia mediante tareas cron, asegurando que la carga se vuelva a

descargar y ejecutar al iniciar sesión, reiniciar o en intervalos de tiempo programados.
- Se elimina a sí mismo al finalizar.

> *"Al ser de código abierto, XMRig facilita a los atacantes su personalización. En este caso, eliminaron toda la lógica de análisis de argumentos y codificaron la configuración directamente. Este ajuste no solo simplifica la distribución, sino que también permite que la carga se haga pasar por el proceso logrotate de forma más convincente».* explicó Wiz.

Aparece el nuevo botnet Hpingbot

Este hallazgo coincide con el análisis de NSFOCUS sobre un nuevo y ágil malware escrito en Go, llamado Hpingbot, capaz de infectar sistemas Windows y Linux para convertirlos en parte de una botnet que lanza ataques DDoS, utilizando hping3, una herramienta de red que permite enviar paquetes ICMP/TCP/UDP personalizados.

Una característica destacada de este malware es que, a diferencia de otros troyanos basados en familias conocidas como Mirai o Gafgyt, Hpingbot es una cepa completamente nueva. Desde al menos el 17 de junio de 2025, se han emitido varios cientos de comandos DDoS, apuntando principalmente a Alemania, Estados Unidos y Turquía.

> *"Es una nueva familia de botnets desarrollada desde cero, que demuestra una gran capacidad de innovación y eficiencia en el uso de recursos existentes, como distribuir las cargas a través de Pastebin y lanzar ataques DDoS con hping3, lo que mejora su sigilo y reduce considerablemente los costos de desarrollo y operación,"* señaló la empresa china de ciberseguridad.

Hpingbot se propaga aprovechando configuraciones débiles en SSH, mediante un módulo autónomo que realiza ataques de fuerza bruta por medio de "password spraying" para

obtener acceso inicial.

Los comentarios de depuración en alemán presentes en el código fuente indican que la versión más reciente aún podría estar en pruebas. El ataque, en términos generales, implica el uso de Pastebin como punto de referencia para obtener una dirección IP ("128.0.118[.]18"), la cual se emplea para descargar un script.

Ese script detecta la arquitectura del CPU del sistema infectado, finaliza versiones previas del troyano y recupera la carga principal encargada de iniciar ataques DDoS por medio de TCP y UDP. También implementa persistencia y elimina el historial de comandos para ocultar la infección.

En un giro interesante, desde el 19 de junio, los atacantes han comenzado a usar nodos infectados por Hpingbot para distribuir otro componente DDoS en Go, que, aunque comparte el mismo servidor C2, ya no usa Pastebin ni hping3, sino que implementa funciones integradas de inundación UDP/TCP.

Otro detalle relevante es que, aunque la versión de Windows no puede utilizar hping3 para lanzar ataques DDoS —ya que se instala mediante el comando de Linux `apt -y install`—, la capacidad del malware de descargar y ejecutar cargas adicionales sugiere que los atacantes podrían estar buscando más que solo interrumpir servicios, convirtiendo la botnet en una red de distribución de malware.

> *"Es importante destacar que la versión para Windows de Hpingbot no puede utilizar directamente hping3 para lanzar ataques DDoS, pero su actividad sigue siendo muy frecuente, lo que indica que los atacantes no se están limitando a los ataques de denegación de servicio, sino que también buscan aprovechar su funcionalidad para descargar y ejecutar cargas arbitrarias."*

Un tribunal del estado de California, EE.UU., ha ordenado a Google pagar 314 millones de dólares por haber utilizado de forma indebida los datos móviles de los usuarios de

dispositivos Android, incluso cuando estos se encontraban en reposo, para enviar información de manera pasiva a la compañía.

El fallo pone fin a una demanda colectiva que fue presentada por primera vez en agosto de 2019.

Según los demandantes, el sistema operativo Android de Google usaba el plan de datos móviles de los usuarios para transmitir diversa información a Google, sin su conocimiento ni autorización, incluso cuando los dispositivos estaban inactivos.

> *«Aunque Google podría haber diseñado estos envíos para que se realicen únicamente cuando los teléfonos están conectados a una red Wi-Fi, en cambio optó por permitir que también ocurran mediante redes móviles»,* afirmaron.
>
> *«El uso no autorizado de los datos móviles por parte de Google infringe la legislación de California y obliga a la compañía a compensar a los demandantes por el valor de los datos consumidos en beneficio propio y sin su aprobación.»*

Los denunciantes sostuvieron que estas transmisiones sucedían incluso cuando las apps de Google no estaban abiertas, sino funcionando en segundo plano, y los dispositivos permanecían inactivos, consumiendo así datos móviles sin que el usuario lo supiera.

En una de las pruebas citadas, se detectó que un teléfono Samsung Galaxy S7, con configuración predeterminada y aplicaciones preinstaladas, vinculado a una cuenta nueva de Google, enviaba y recibía diariamente 8.88 MB de datos móviles, de los cuales un 94% eran comunicaciones entre el dispositivo y Google.

Durante un periodo de 24 horas, se registraron alrededor de 389 transmisiones de datos, las cuales contenían principalmente archivos de registro con métricas del sistema operativo, estado de la red y lista de aplicaciones abiertas.

> *«Los archivos de registro no suelen requerir transmisión inmediata, y podrían ser enviados más tarde cuando haya conexión Wi-Fi disponible»,* se lee en los documentos judiciales.
>
> *«Google también podría permitir que los usuarios configuren Android para que esas transferencias pasivas solo ocurran con Wi-Fi, pero aparentemente ha decidido no hacerlo. En su lugar, Google ha preferido aprovecharse del plan de datos móviles de los demandantes.»*

Pero eso no fue todo. En la demanda también se mencionó un experimento de 2018 que mostró que un dispositivo Android que permanecía aparentemente inactivo y sin moverse, pero con el navegador Chrome abierto en segundo plano, generaba alrededor de 900 transmisiones pasivas en 24 horas.

En contraste, un iPhone que se mantenía inmóvil con Safari abierto en segundo plano enviaba «significativamente menos información», destacando que el sistema operativo de Apple otorga mayor control al usuario sobre la transmisión de datos en segundo plano.

Tras el juicio iniciado el 2 de junio de 2025, el jurado falló a favor de los demandantes, concluyendo que la empresa tecnológica era responsable de realizar estas transmisiones de datos pasivas, imponiendo a los usuarios lo que calificaron como «cargas obligatorias e inevitables […] en beneficio y conveniencia de Google.»

En declaraciones a Reuters, Google anunció que apelará la decisión, argumentando que estas transmisiones están relacionadas con «servicios esenciales para la seguridad, el rendimiento y la fiabilidad de los dispositivos Android.» La compañía también señaló que estos envíos están detallados en sus términos de uso y que cuenta con el consentimiento del usuario.

El veredicto del jurado llega casi dos meses después de que Google aceptara pagar cerca de 1.400 millones de dólares para resolver dos demandas en el estado de Texas, donde se le acusaba de rastrear la ubicación de los usuarios y almacenar datos de reconocimiento facial

sin consentimiento.

Esta decisión también coincide con una apelación de Meta frente al fallo de la Comisión Europea en abril de 2025, que determinó que su modelo de «pagar o dar consentimiento» violaba la Ley de Mercados Digitales (DMA) de la región, y le impuso una multa de 200 millones de euros (227 millones de dólares).

> *«La decisión exige que Meta ofrezca un servicio con anuncios menos personalizados de manera gratuita, sin considerar el coste, el impacto o la eficacia, imponiendo así un modelo de negocio posiblemente insostenible»,* afirmó la empresa.
>
> *«Esta medida ignora la realidad comercial de que, en una economía de mercado, Meta tiene derecho a recibir una compensación justa por los servicios innovadores y valiosos que los usuarios eligen utilizar, un principio clave para mantener la innovación y el crecimiento económico.»*

Investigadores en ciberseguridad han revelado dos vulnerabilidades en la herramienta de línea de comandos Sudo, utilizada en sistemas Linux y otros sistemas operativos similares a Unix, que podrían permitir a atacantes locales escalar privilegios y obtener acceso como root en sistemas vulnerables.

A continuación se describen brevemente las fallas encontradas:

- CVE-2025-32462 (puntuación CVSS: 2.8) – Las versiones de Sudo anteriores a la 1.9.17p1, cuando se utilizan con un archivo sudoers que incluye un host que no es ni el sistema actual ni «ALL», permiten que los usuarios autorizados ejecuten comandos en máquinas distintas a las esperadas.
- CVE-2025-32463 (puntuación CVSS: 9.3) – En versiones anteriores a Sudo 1.9.17p1, usuarios locales pueden obtener acceso como root porque el archivo «/etc/nsswitch.conf» puede ser tomado desde un directorio controlado por el usuario

cuando se utiliza la opción –chroot.

Sudo es una utilidad de consola que permite a usuarios con bajos privilegios ejecutar comandos como si fueran otro usuario, comúnmente el superusuario. Su objetivo es aplicar el principio de mínimo privilegio, es decir, permitir que se realicen tareas administrativas sin necesidad de acceso completo.

La configuración del comando se gestiona mediante el archivo «/etc/sudoers», el cual especifica *"quién puede ejecutar qué comandos como qué usuarios, en qué máquinas, y también puede controlar aspectos especiales como si se requiere contraseña para ciertos comandos".*

El investigador Rich Mirch, de Stratascale, quien descubrió y reportó ambas vulnerabilidades, explicó que CVE-2025-32462 había pasado desapercibida por más de 12 años. Esta falla está relacionada con la opción -h (host) de Sudo, que permite consultar los privilegios de sudo para un host diferente. Esta funcionalidad fue incorporada en septiembre de 2013.

No obstante, debido a un error, era posible ejecutar comandos permitidos para un host remoto en la máquina local, si se usaba Sudo con la opción host apuntando a un sistema ajeno.

> *"Esto afecta principalmente a entornos que comparten un archivo sudoers común entre múltiples sistemas. Los entornos que utilizan sudoers basados en LDAP (como SSSD) también se ven afectados»,* explicó el responsable del proyecto Sudo, Todd C. Miller, en un comunicado.

En cuanto a la segunda vulnerabilidad, CVE-2025-32463, esta aprovecha la opción -R (chroot) de Sudo para ejecutar comandos arbitrarios como root, incluso si dichos comandos no están definidos en el archivo sudoers. Esta falla ha sido clasificada como crítica.

> *"La configuración predeterminada de Sudo es vulnerable. Aunque la falla involucra la característica chroot de Sudo, no requiere que existan reglas de Sudo definidas para el usuario. Por lo tanto, cualquier usuario local sin privilegios podría escalar sus permisos a root si el sistema tiene instalada una versión vulnerable»,* indicó Mirch.

En otras palabras, esta vulnerabilidad permite que un atacante engañe a Sudo para que cargue una biblioteca compartida manipulada, creando un archivo «/etc/nsswitch.conf» dentro de un directorio raíz personalizado, lo que puede resultar en la ejecución de código malicioso con privilegios elevados.

Miller señaló que la opción chroot será eliminada completamente en futuras versiones de Sudo, ya que permitir a los usuarios definir su propio directorio raíz es "propenso a errores".

Tras una divulgación responsable realizada el 1 de abril de 2025, ambas fallas fueron corregidas en la versión Sudo 1.9.17p1, publicada a finales del mes pasado. Diversas distribuciones de Linux han emitido sus propios avisos de seguridad, ya que Sudo viene instalado por defecto en muchas de ellas:

- CVE-2025-32462 afecta a: *AlmaLinux 8 y 9, Alpine Linux, Amazon Linux, Debian, Gentoo, Oracle Linux, Red Hat, SUSE y Ubuntu*.
- CVE-2025-32463 afecta a: *Alpine Linux, Amazon Linux, Debian, Gentoo, Red Hat, SUSE y Ubuntu*.

Se recomienda a todos los usuarios aplicar las actualizaciones correspondientes y asegurarse de que sus distribuciones de Linux estén protegidas con los paquetes más recientes.

Investigadores en ciberseguridad han descubierto más de 40 extensiones maliciosas para el navegador Mozilla Firefox, diseñadas para robar secretos de billeteras de criptomonedas, poniendo en riesgo los activos digitales de los usuarios.

"Estas extensiones se hacen pasar por herramientas legítimas de billeteras de plataformas

ampliamente utilizadas como Coinbase, MetaMask, Trust Wallet, Phantom, Exodus, OKX, Keplr, MyMonero, Bitget, Leap, Ethereum Wallet y Filfox”, dijo Yuval Ronen, investigador de Koi Security.

Se afirma que esta campaña a gran escala ha estado activa al menos desde abril de 2025, y que se han subido nuevas extensiones a la tienda de complementos de Firefox tan recientemente como la semana pasada.

Se ha descubierto que las extensiones identificadas inflan artificialmente su popularidad, añadiendo cientos de reseñas de cinco estrellas que superan con creces el número real de instalaciones activas. Esta estrategia busca darles una apariencia de legitimidad, haciendo creer que son extensamente utilizadas y engañando a los usuarios para que las instalen.

Otra táctica empleada por el actor de amenazas consiste en hacer pasar estos complementos como herramientas auténticas de billeteras, utilizando los mismos nombres y logotipos.

El hecho de que algunas de las extensiones reales fueran de código abierto permitió a los atacantes clonar su código fuente e inyectar funcionalidades maliciosas para extraer claves de billeteras y frases semilla desde sitios web objetivo y enviarlas a un servidor remoto. También se ha encontrado que estas extensiones maliciosas transmiten las direcciones IP externas de las víctimas.

A diferencia de los fraudes de phishing convencionales, que dependen de sitios web o correos electrónicos falsos, estas extensiones operan dentro del navegador del usuario, lo que las hace mucho más difíciles de detectar o bloquear con herramientas tradicionales de seguridad en el dispositivo.

“Este enfoque de bajo esfuerzo y alto impacto permitió al atacante mantener una experiencia de usuario esperada mientras reducía las probabilidades de detección inmediata”, comentó Ronen.

La presencia de comentarios en ruso dentro del código fuente, así como metadatos obtenidos

de un archivo PDF recuperado del servidor de comando y control (C2) utilizado en la operación, apuntan a un grupo de actores de amenazas de habla rusa.

Todos los complementos identificados, excepto MyMonero Wallet, han sido eliminados por Mozilla. El mes pasado, el desarrollador del navegador afirmó haber desarrollado un *"sistema de detección temprana"* para identificar y bloquear extensiones fraudulentas de billeteras cripto antes de que ganen popularidad y sean usadas para robar activos de los usuarios mediante engaños para que ingresen sus credenciales.

Para mitigar los riesgos que suponen estas amenazas, se recomienda instalar extensiones únicamente de editores verificados y revisar su comportamiento para asegurarse de que no cambien de forma silenciosa después de su instalación.

Reformulación con palabras distintas (respetando citas):

Expertos en seguridad informática han revelado la existencia de más de 40 extensiones maliciosas para el navegador Firefox que tienen como objetivo sustraer datos confidenciales de billeteras de criptomonedas, comprometiendo los fondos digitales de los usuarios.

«Estas extensiones simulan ser herramientas oficiales de billeteras reconocidas como Coinbase, MetaMask, Trust Wallet, Phantom, Exodus, OKX, Keplr, MyMonero, Bitget, Leap, Ethereum Wallet y Filfox», afirmó Yuval Ronen, investigador de la firma Koi Security.

Según se reporta, esta operación ha estado activa desde al menos abril de 2025, y continúan apareciendo nuevas versiones en la tienda de complementos de Firefox, incluso tan recientemente como la semana anterior.

Los complementos maliciosos descubiertos recurren a una técnica para aparentar ser populares, acumulando cientos de calificaciones con cinco estrellas, muchas más que las instalaciones reales. Con esto buscan generar una percepción falsa de fiabilidad, logrando que usuarios desprevenidos los instalen.

Otro método utilizado por los atacantes consiste en replicar los nombres e íconos de las billeteras legítimas para dar una apariencia auténtica a las extensiones.

Debido a que algunos de estos complementos originales son de código abierto, los atacantes pudieron copiar su base de código e introducir funciones dañinas que capturan frases semilla y claves privadas desde los sitios web que visita la víctima, enviándolas posteriormente a un servidor externo. Además, se ha comprobado que las extensiones maliciosas recolectan también la dirección IP pública del usuario afectado.

A diferencia de los ataques de phishing tradicionales que dependen de enlaces o correos falsos, estas extensiones operan desde dentro del propio navegador del usuario, lo que las vuelve más difíciles de identificar o neutralizar con soluciones comunes de protección.

"Este método de bajo costo y gran efectividad permitió al atacante ofrecer una experiencia normal al usuario mientras evitaba ser detectado rápidamente", indicó Ronen.

El hallazgo de anotaciones en idioma ruso dentro del código y los metadatos extraídos de un archivo PDF localizado en el servidor C2 utilizado en la operación sugieren que se trata de un grupo de ciberdelincuentes de habla rusa.

Excepto por MyMonero Wallet, todos los complementos maliciosos han sido retirados por Mozilla. El mes pasado, la empresa anunció que ha implementado un *"sistema de detección anticipada"* capaz de reconocer y frenar extensiones de billeteras fraudulentas antes de que se popularicen y consigan engañar a los usuarios para que entreguen sus credenciales.

Para reducir la exposición ante estas amenazas, se aconseja descargar extensiones únicamente desde desarrolladores confiables y comprobar que su comportamiento no se altere tras la instalación.

Investigadores en ciberseguridad han identificado una vulnerabilidad crítica en el proyecto *Model Context Protocol (MCP) Inspector* de la empresa de inteligencia artificial Anthropic, la

cual podría permitir la ejecución remota de código (RCE) y dar acceso total al sistema afectado.

La vulnerabilidad, registrada como CVE-2025-49596, tiene una puntuación CVSS de 9.4 sobre 10, indicando una severidad muy alta.

> *"Se trata de una de las primeras fallas críticas de ejecución remota en el ecosistema MCP de Anthropic, lo que revela una nueva clase de ataques basados en navegador dirigidos a herramientas de desarrollo de IA"*, declaró Avi Lumelsky de Oligo Security en un informe publicado la semana pasada.
>
> *"Al obtener ejecución de código en el equipo de un desarrollador, los atacantes pueden robar información, instalar puertas traseras y moverse lateralmente por redes —lo que plantea riesgos importantes para equipos de IA, proyectos de código abierto y empresas que utilizan MCP."*

Presentado por Anthropic en noviembre de 2024, MCP es un protocolo abierto que estandariza cómo las aplicaciones basadas en modelos de lenguaje (LLM) integran y comparten datos con herramientas o fuentes externas.

MCP Inspector es una herramienta para desarrolladores que permite probar y depurar servidores MCP, los cuales exponen capacidades específicas mediante el protocolo, facilitando que un sistema de IA acceda a información más allá de su entrenamiento.

Está compuesto por dos partes: un cliente con interfaz interactiva para pruebas y depuración, y un servidor proxy que actúa como puente entre la interfaz web y diversos servidores MCP.

Sin embargo, es fundamental tener presente que este servidor no debe estar expuesto a redes no confiables, ya que tiene permiso para ejecutar procesos locales y conectarse con cualquier servidor MCP especificado.

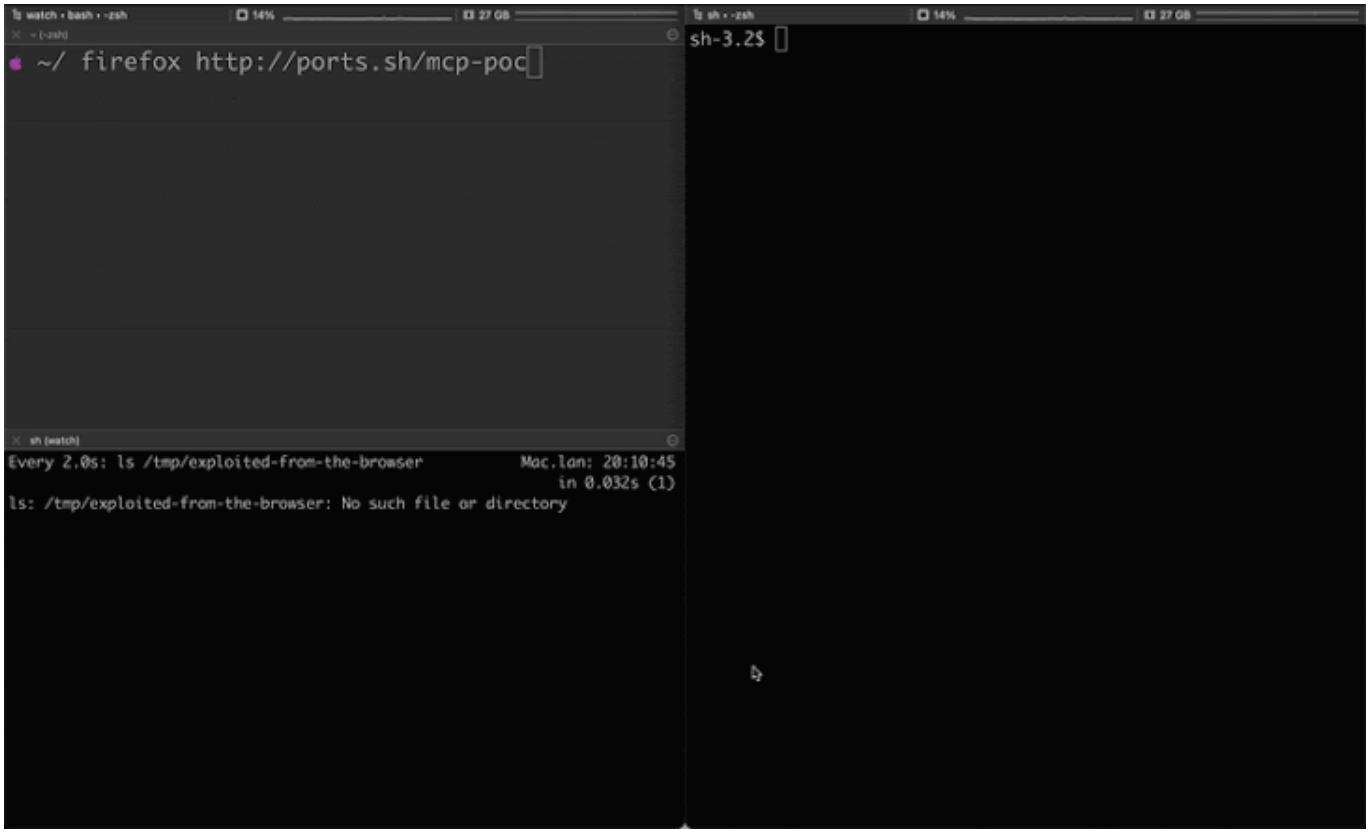
Este detalle, sumado al hecho de que los desarrolladores suelen iniciar la herramienta con configuraciones predeterminadas que carecen de autenticación y cifrado, genera graves riesgos de seguridad, según Oligo.

> *"Esta mala configuración crea una superficie de ataque considerable, ya que cualquier persona en la red local o en internet podría interactuar y explotar estos servidores",* advirtió Lumelsky.

El ataque aprovecha la combinación de una falla ya conocida en navegadores modernos, llamada 0.0.0.0 Day, junto con una vulnerabilidad CSRF en Inspector (CVE-2025-49596), permitiendo la ejecución de código simplemente al visitar un sitio web malicioso.

> *"Las versiones de MCP Inspector anteriores a la 0.14.1 son vulnerables a ejecución remota de código debido a la falta de autenticación entre el cliente Inspector y el proxy, permitiendo solicitudes no autenticadas que ejecutan comandos MCP vía stdio",* indicaron los desarrolladores en el aviso sobre CVE-2025-49596.

0.0.0.0 Day es una vulnerabilidad con 19 años de antigüedad presente en navegadores actuales que puede ser usada por sitios maliciosos para acceder a redes locales. Se basa en el manejo inseguro de la IP 0.0.0.0, que puede resultar en ejecución de código.



> *"Los atacantes pueden explotar esta falla mediante una página web diseñada para enviar peticiones a servicios locales corriendo en un servidor MCP, logrando así ejecutar comandos arbitrarios en el equipo del desarrollador"*, explicó Lumelsky.
>
> *"El hecho de que la configuración por defecto exponga estos servidores a tales ataques significa que muchos desarrolladores podrían estar abriendo sin saberlo una puerta trasera a sus sistemas."*

En concreto, la prueba de concepto (PoC) utiliza el endpoint Server-Sent Events (SSE) para enviar una solicitud maliciosa desde una página web controlada por el atacante, con el objetivo de ejecutar código en la máquina donde se ejecuta la herramienta, incluso si solo escucha en localhost (127.0.0.1).

Esto es posible porque la dirección 0.0.0.0 indica al sistema operativo que debe escuchar en todas las interfaces IP del equipo, incluyendo la interfaz de bucle local (localhost).

En un escenario de ataque, un atacante podría crear una página web falsa y engañar a un desarrollador para que la visite. En ese momento, un script malicioso embebido en la página enviaría una petición a 0.0.0.0:6277 (puerto por defecto del proxy), instruyendo al servidor MCP Inspector a ejecutar comandos arbitrarios.

Además, el ataque puede incorporar técnicas de DNS rebinding para generar registros DNS falsos que apunten a 0.0.0.0:6277 o 127.0.0.1:6277, eludiendo controles de seguridad y logrando ejecución remota de código.

Tras una divulgación responsable en abril de 2025, los responsables del proyecto corrigieron el fallo el 13 de junio, lanzando la versión 0.14.1, que incorpora un token de sesión para el proxy y validación de origen para bloquear el vector de ataque.

> *"Aunque los servicios en localhost parezcan seguros, muchas veces están expuestos a internet debido a las capacidades de enrutamiento en navegadores y clientes MCP"*, indicó Oligo.
>
> *"La solución agrega autorización (que antes faltaba por defecto), además de validar los encabezados Host y Origin en las peticiones HTTP, asegurando que el cliente proviene de un dominio confiable. Ahora, por defecto, el servidor bloquea ataques de DNS rebinding y CSRF."*

Europol anunció el lunes el desmantelamiento de una red de fraude de inversiones en criptomonedas que lavó 460 millones de euros (540 millones de dólares) de más de 5,000 víctimas en todo el mundo.

La operación, según la agencia, fue ejecutada por la Guardia Civil española con el apoyo de

autoridades policiales de Estonia, Francia y Estados Unidos. Europol indicó que la investigación sobre este grupo criminal comenzó en 2023.

Además, cinco presuntos responsables del esquema fraudulento fueron arrestados el 25 de junio de 2025. Tres de las detenciones ocurrieron en las Islas Canarias y las otras dos en Madrid.

«Para llevar a cabo sus actividades fraudulentas, los cabecillas de la red criminal supuestamente utilizaron una red de colaboradores distribuidos por todo el mundo para recaudar fondos mediante retiros de efectivo, transferencias bancarias y transacciones en criptomonedas», señaló Europol.

Este tipo de estafas siguen con frecuencia un patrón conocido como fraude de confianza o "romance crypto" (antes llamado «pig butchering»), en el que los estafadores ganan la confianza de las víctimas durante semanas o meses—usualmente a través de apps de citas o conversaciones amigables—antes de persuadirlas para invertir en plataformas falsas de criptomonedas. Detrás de escena, los delincuentes usan ingeniería social, como paneles de trading falsos y diálogos preestablecidos, para mantener la ilusión. Una vez depositado el dinero, se transfiere entre múltiples cuentas en un proceso conocido como "layering", dificultando su rastreo por las autoridades.

Se cree que los ciberdelincuentes establecieron una red bancaria y corporativa en Hong Kong, a través de la cual canalizaron los fondos ilícitos utilizando un laberinto de pasarelas de pago y cuentas a nombre de diversas personas y en distintos intercambios.

Este acontecimiento llega poco después de que el Departamento de Justicia de EE.UU. presentara una demanda de decomiso civil para recuperar más de 225 millones de dólares en criptomonedas vinculadas a fraudes de confianza que operaban desde Vietnam y Filipinas.

Europol describió la *"escala, variedad, sofisticación y alcance"* de estos fraudes en línea como *"sin precedentes"*, y advirtió que podrían superar al crimen organizado tradicional debido al uso creciente de tecnologías de inteligencia artificial.

> *«La integración de inteligencia artificial generativa por parte de grupos criminales transnacionales dedicados al fraude digital es una tendencia compleja y preocupante observada en el sudeste asiático, y representa un multiplicador de poder para las actividades delictivas»,* afirmó John Wojcik, analista regional de la UNODC, a finales del año pasado.

Según un informe de INTERPOL de la semana pasada, los delitos cibernéticos representan más del 30% de todos los crímenes reportados en África Occidental y Oriental. Esto incluye estafas en línea, ransomware, suplantación de correos empresariales (BEC) y extorsión sexual digital.

«El cibercrimen continúa superando a los sistemas legales diseñados para detenerlo», declaró INTERPOL, agregando que *«el 75% de los países encuestados dijeron que sus marcos legales y capacidad de enjuiciamiento necesitaban mejoras».*

Una de las razones por las que este tipo de fraude es tan difícil de combatir es porque los criminales se aprovechan de vacíos legales y leyes internacionales fragmentadas. Muchos estafadores ahora usan identidades sintéticas—personas ficticias creadas con datos robados o generados por IA—para registrar cuentas o alquilar acceso a bancos. También reclutan *«mulas financieras»* que transfieren dinero, muchas veces sin saber que participan en un crimen.

Para ejecutar este tipo de estafas de inversión, personas desprevenidas de Asia y África son atraídas al sudeste asiático con promesas de empleos lucrativos, pero luego son retenidas contra su voluntad en *«centros de estafa»* operados por grupos del crimen organizado transnacional provenientes de China.

Amnistía Internacional ha identificado al menos 53 de estos centros en Camboya, donde, según la organización, *"han ocurrido o siguen ocurriendo violaciones a los derechos humanos, incluyendo trata de personas, tortura, trabajos forzados, trabajo infantil, privación de libertad y esclavitud».*

Muchas de las personas reclutadas fueron inicialmente engañadas con ofertas de empleo en tecnología o ventas. Una vez en el lugar, les confiscan los pasaportes y las obligan a estafar a otros bajo amenazas de violencia o endeudamiento.

El año pasado, el Instituto de Paz de EE.UU. reveló que las ganancias del fraude digital en Camboya superan los 12,500 millones de dólares al año, lo cual equivale a la mitad del producto interno bruto (PIB) formal del país.

La operación ilegal ha tenido tanto impacto que la Embajada de la India en Camboya mantiene una advertencia destacada en su sitio web, exhortando a los ciudadanos a estar alertas para no caer en manos de traficantes de personas que ofrecen falsos empleos bien remunerados. La advertencia señala que los solicitantes de empleo son obligados a realizar estafas financieras en línea y otras actividades ilegales.

Agregando más contexto a esta actividad criminal, un reciente informe de ProPublica indicó que canales de Telegram en idioma chino están promocionando entre estafadores la posibilidad de alquilar cuentas bancarias estadounidenses en Bank of America, Chase, Citibank y PNC, las cuales luego se usan para lavar dinero. Telegram ha comenzado a tomar medidas contra algunos de estos canales.

Meta, por su parte, dijo haber detectado y eliminado al menos siete millones de cuentas de Facebook vinculadas a centros de estafa en Asia y Medio Oriente desde principios de 2024, según declaró la compañía al medio de periodismo de investigación.

Investigadores en ciberseguridad han descrito dos métodos innovadores que pueden utilizarse para interrumpir las botnets dedicadas a la minería de criptomonedas.

Según un nuevo informe publicado hoy por Akamai, estos métodos aprovechan el diseño de diversas arquitecturas comunes de minería para detener el proceso de minado.

«Desarrollamos dos técnicas aprovechando las topologías de minería y las políticas de los

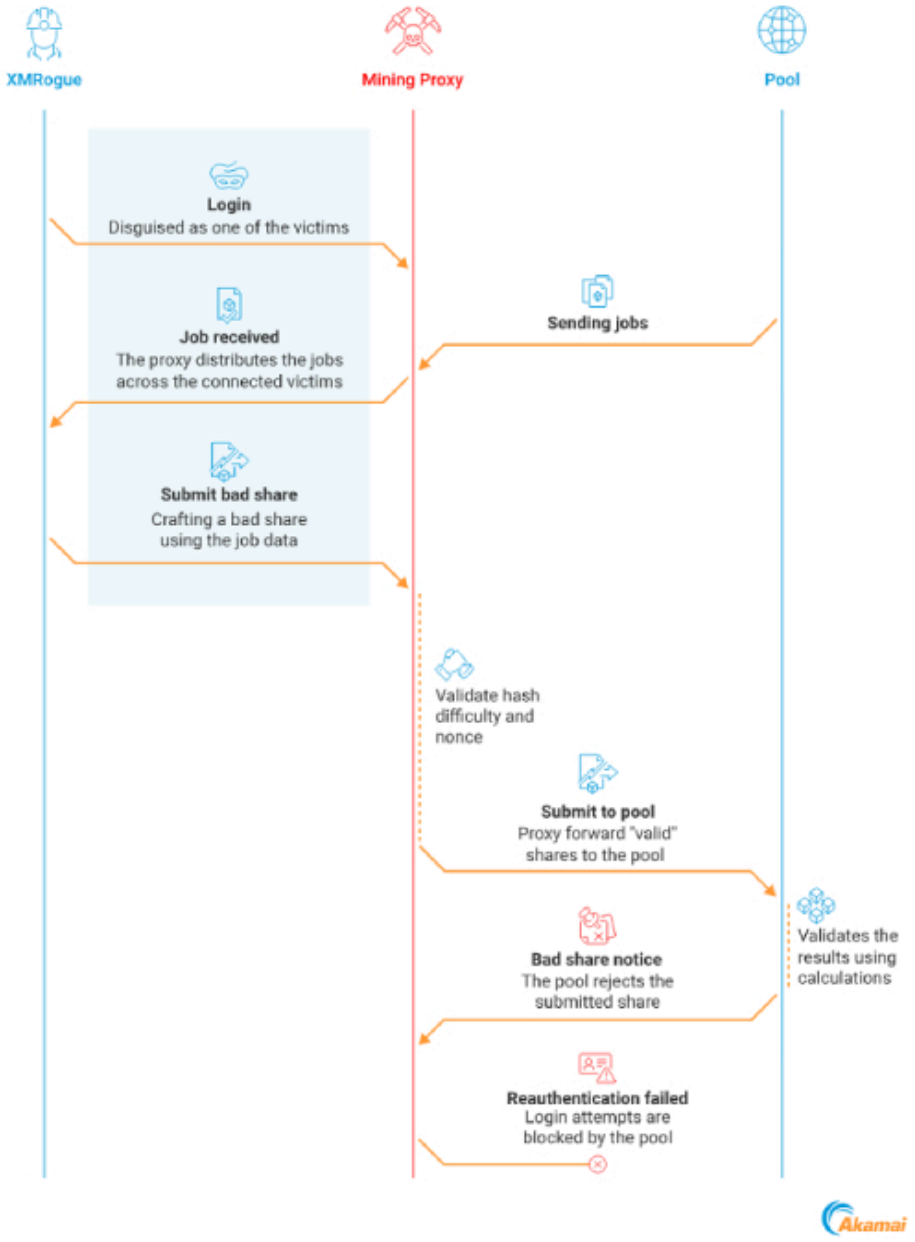
pools, lo que nos permite reducir la efectividad de una botnet de criptominería hasta el punto de apagarla por completo. Esto obliga al atacante a realizar cambios drásticos en su infraestructura o incluso a abandonar la campaña por completo,» explicó el investigador de seguridad Maor Dahan.

La compañía de infraestructura web indicó que estas técnicas se basan en explotar el protocolo de minería Stratum, provocando que el proxy de minería o la cartera del atacante sea bloqueada, interrumpiendo así toda la operación.

La primera de las dos estrategias, llamada “acciones inválidas”, consiste en lograr que el proxy de minería sea expulsado de la red, lo que provoca que toda la operación se detenga y que el uso del CPU de la víctima caiga de un 100% a 0%.

Aunque un proxy de minería actúa como intermediario y oculta el pool de minería del atacante —y, por ende, sus direcciones de cartera—, también se convierte en un punto único de fallo cuando se altera su funcionamiento normal.

«La idea es sencilla: al conectarnos como mineros a un proxy malicioso, podemos enviar resultados inválidos de trabajos de minería —acciones erróneas— que pasarán el filtro del proxy y llegarán al pool,» explicó Dahan. *«El envío repetido de acciones inválidas acabará por hacer que el proxy sea bloqueado, deteniendo efectivamente las operaciones de minería de toda la botnet.»*



Para lograrlo, se utiliza una herramienta interna desarrollada por Akamai llamada XMRogue, que simula ser un minero, se conecta al proxy de minería, envía acciones inválidas de forma continua y finalmente provoca el bloqueo del proxy en el pool.

El segundo enfoque diseñado por Akamai se aplica en casos donde el minero víctima está conectado directamente a un pool público sin pasar por un proxy. Se aprovecha el hecho de que un pool puede suspender temporalmente una cartera si detecta más de 1,000 trabajadores asociados a ella.

En otras palabras, si se generan más de 1,000 intentos de conexión simultánea usando la cartera del atacante, el pool suspenderá esa cartera por una hora. Sin embargo, esta no es una solución definitiva, ya que el atacante podría recuperar el acceso una vez que cesen las conexiones múltiples.

Akamai subrayó que, si bien estas técnicas han sido aplicadas principalmente contra mineros de Monero, pueden adaptarse a otras criptomonedas también.

«Las técnicas presentadas arriba demuestran cómo los defensores pueden desactivar campañas maliciosas de criptominería sin afectar las operaciones legítimas del pool, simplemente aprovechando sus propias políticas,» señaló Dahan.

«Un minero legítimo podrá recuperarse rápidamente de este tipo de ataques, ya que puede cambiar fácilmente su IP o cartera localmente. Pero para un criptominero malicioso, esto implicaría modificar toda su botnet. Para los mineros menos sofisticados, esta defensa podría inutilizar por completo la botnet.»