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.

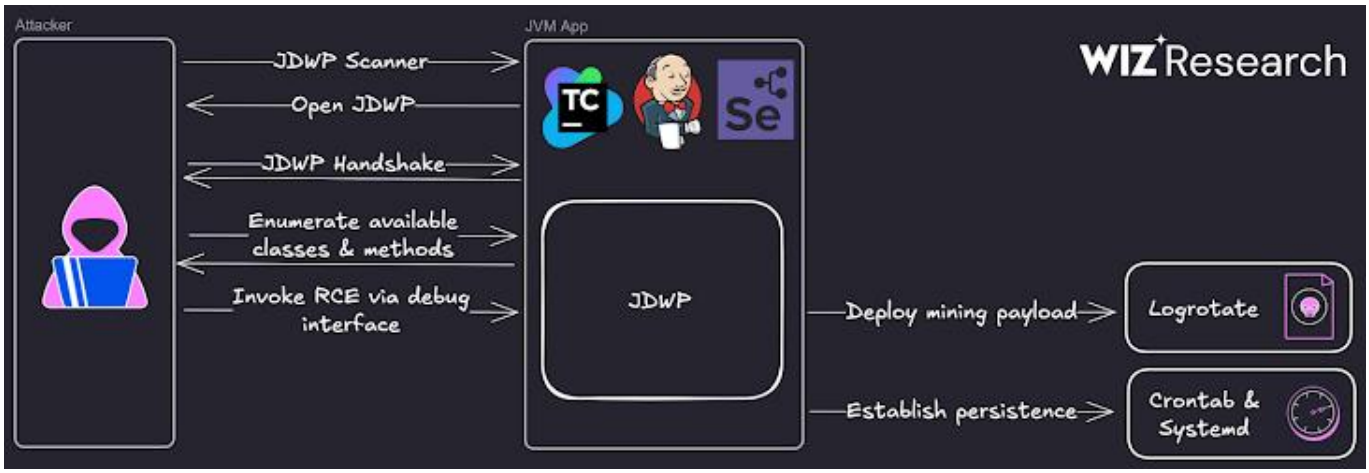
En resumen, esta mala configuración puede ser usada para inyectar y ejecutar comandos arbitrarios, establecer persistencia y ejecutar cargas maliciosas.

> *"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.

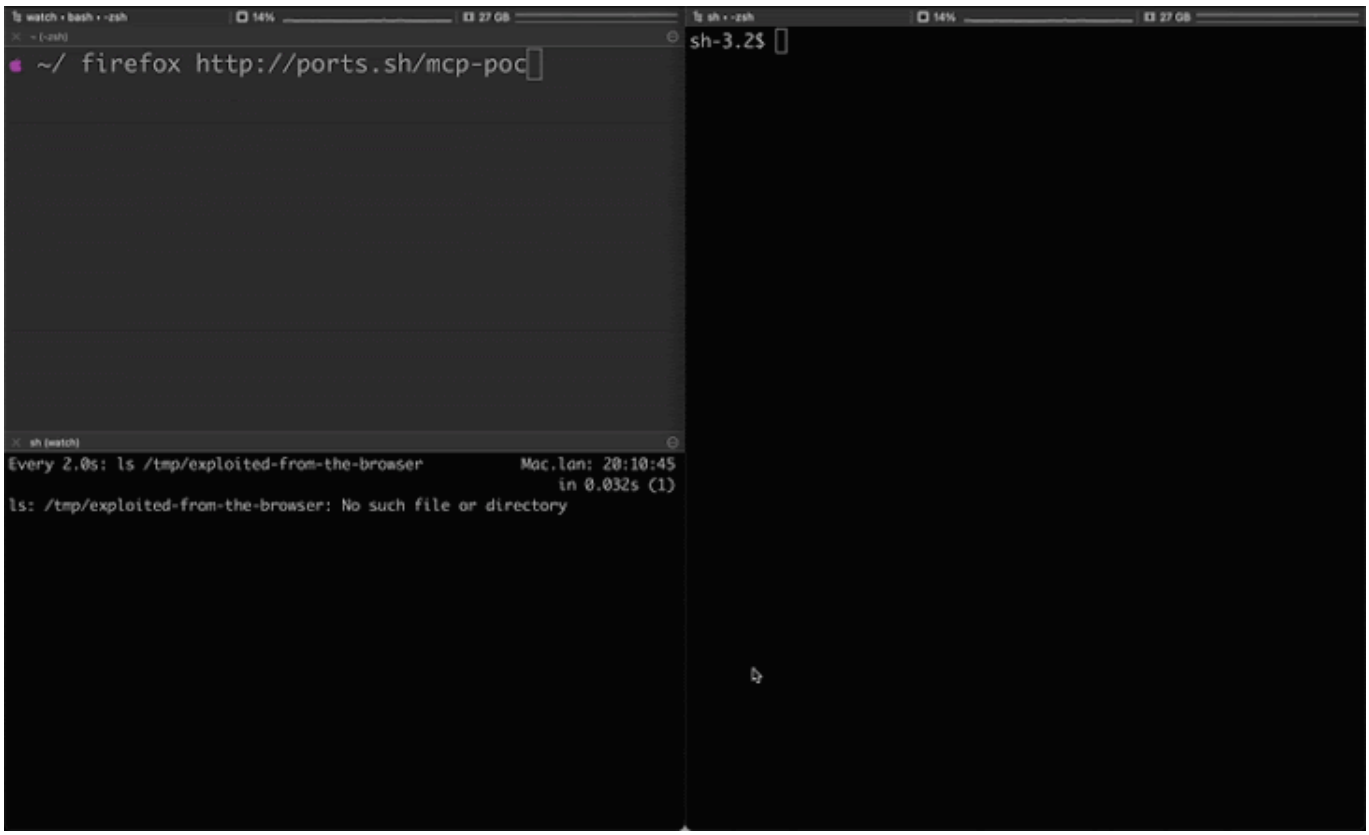
> *"Esta mala configuración crea una superficie de ataque considerable, ya que cualquier persona en la red local o en internet podría interactuar y explotar estos servidores",* advirtió Lumelsky.

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.

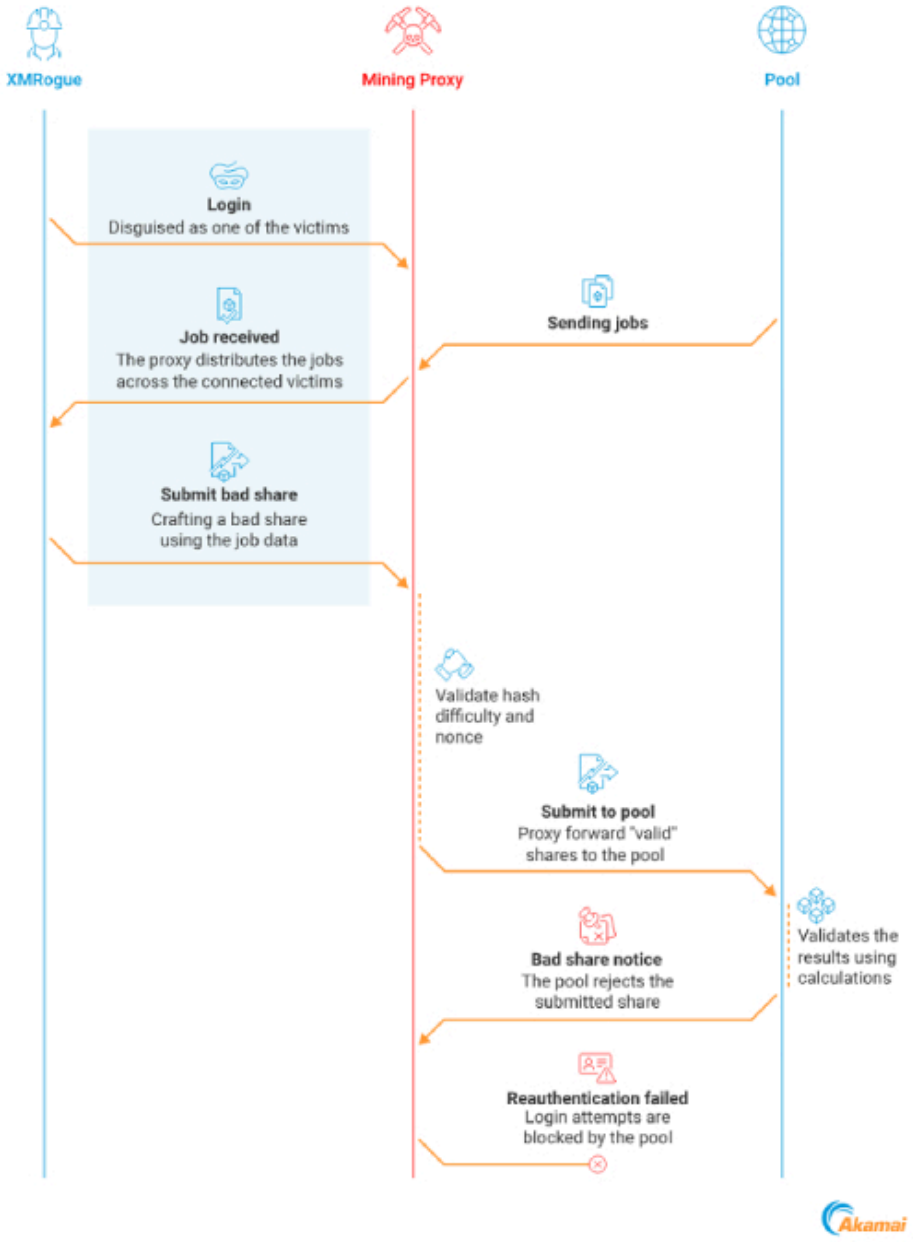
«Desarrollamos dos técnicas aprovechando las topologías de minería y las políticas de los pools, lo que nos permite reducir la efectividad de una botnet de criptominería hasta el punto de apagarla por completo. Esto obliga al atacante a realizar cambios drásticos en su infraestructura o incluso a abandonar 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.»

La Embajada de Estados Unidos en la India ha informado que los solicitantes de visas no inmigrantes F, M y J deberán configurar sus cuentas de redes sociales como públicas.

Esta nueva directriz tiene como objetivo facilitar a los funcionarios la verificación de la identidad y la elegibilidad de los solicitantes conforme a la legislación estadounidense. La Embajada estadounidense explicó que cada revisión de solicitud de visa constituye una *"decisión relacionada con la seguridad nacional".*

"Con efecto inmediato, todas las personas que soliciten una visa no inmigrante de tipo F, M o

J deberán cambiar la configuración de privacidad de todas sus cuentas personales de redes sociales a 'pública', con el fin de facilitar los controles necesarios para confirmar su identidad y su admisibilidad a Estados Unidos", señaló la embajada en una publicación en X.

Según las nuevas disposiciones, los estudiantes indios y demás personas interesadas en cursar estudios académicos, programas de formación vocacional o de intercambio deberán asegurarse de que sus perfiles en redes sociales estén visibles públicamente antes de enviar su solicitud de visa. No hacerlo podría resultar en la negación de la solicitud.

La embajada también recordó que desde 2019 se exige a los solicitantes de visas, tanto inmigrantes como no inmigrantes, proporcionar los identificadores de sus redes sociales en los formularios correspondientes.

Asimismo, indicó que toda la información "disponible" se utiliza como parte del proceso de evaluación y verificación de visas, con el fin de detectar a personas que no son admitidas en el país, incluyendo aquellas que podrían representar una amenaza a la seguridad nacional. No obstante, no detalló qué aspectos específicos se examinan en dicha revisión.

Otras embajadas estadounidenses en el mundo han emitido lineamientos similares. Por ejemplo, la Embajada de Estados Unidos en México señaló que los solicitantes deben proporcionar todos los nombres de usuario o identificadores de redes sociales que hayan utilizado en los últimos cinco años.

Esta medida se da pocas semanas después de que la administración del expresidente Donald Trump ordenara suspender la programación de citas para visas estudiantiles, con el objetivo de ampliar la revisión de redes sociales de los solicitantes. La semana pasada, el Departamento de Estado de EE. UU. anunció que se reanuda el proceso, aunque con nuevas condiciones que requieren que los solicitantes permitan el acceso del gobierno a sus cuentas en redes sociales.

"Estados Unidos debe actuar con precaución durante el proceso de emisión de visas para garantizar que quienes buscan ingresar al país no tengan intenciones de causar daño a los

estadounidenses o a nuestros intereses nacionales, y que todos los solicitantes puedan demostrar de forma creíble que cumplen con los requisitos de la visa que solicitan, incluyendo que participarán en actividades acordes con los términos de su entrada al país”, indicó el departamento.

Investigadores en ciberseguridad han revelado el funcionamiento interno de un malware para Android llamado AntiDot, que ha comprometido a más de 3,775 dispositivos en el marco de 273 campañas distintas.

> *“Operado por el actor de amenazas LARVA-398, motivado por fines económicos, AntiDot se comercializa activamente como un servicio de malware (MaaS) en foros clandestinos, y ha sido vinculado con una amplia variedad de campañas móviles,”* explicó PRODAFT en un informe.

AntiDot se promociona como una solución *“todo en uno”,* con funciones para grabar la pantalla del dispositivo mediante el abuso de los servicios de accesibilidad de Android, interceptar mensajes SMS y extraer información confidencial de aplicaciones de terceros.

Se sospecha que este botnet para Android se distribuye mediante redes de publicidad maliciosa o a través de campañas de phishing altamente dirigidas, adaptadas según el idioma y la ubicación geográfica de las víctimas.

La primera documentación pública de AntiDot apareció en mayo de 2024, cuando se detectó que se disfrazaba como actualizaciones de Google Play para robar información.

Al igual que otros troyanos en Android, cuenta con una gama de funcionalidades que incluyen ataques por superposición de pantalla, registro de pulsaciones y control remoto del dispositivo a través de la API MediaProjection. Además, establece una conexión WebSocket para comunicación en tiempo real entre el servidor externo y el dispositivo infectado.

En diciembre de 2024, Zimperium reveló detalles sobre una campaña de phishing móvil que distribuía una versión actualizada de AntiDot conocida como AppLite Banker, usando señuelos relacionados con ofertas de trabajo.

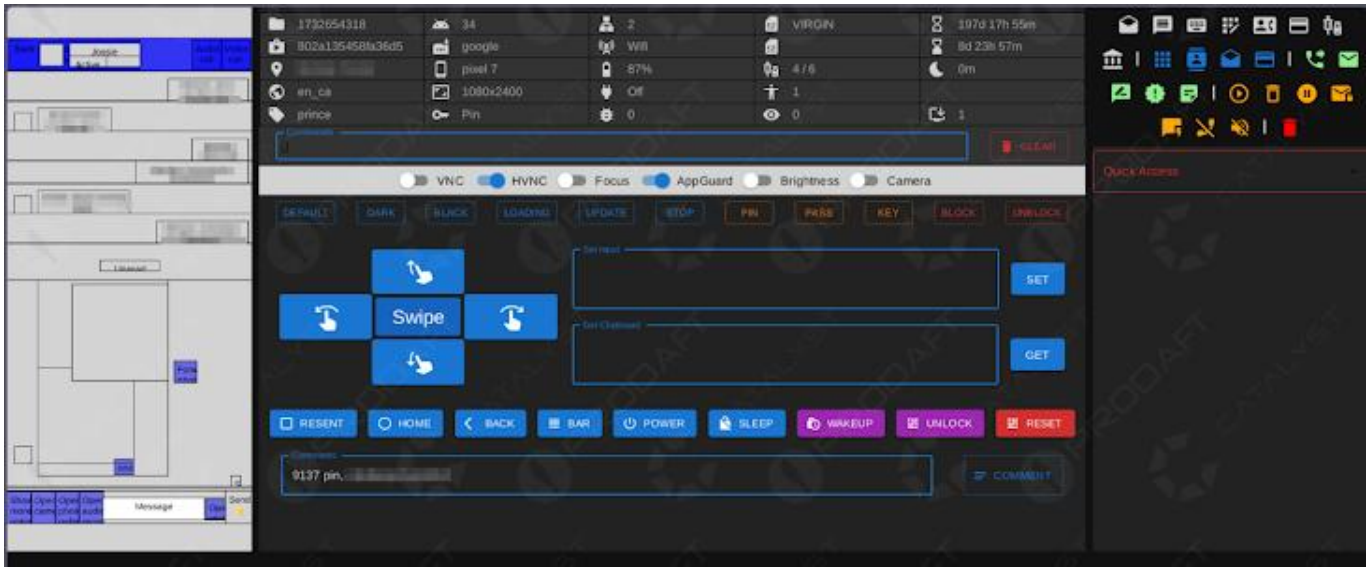
Los hallazgos más recientes de la empresa suiza de ciberseguridad indican que hay al menos 11 servidores C2 activos, que gestionan un mínimo de 3,775 dispositivos infectados distribuidos en 273 campañas diferentes.

Desarrollado en Java, AntiDot se encuentra fuertemente ofuscado utilizando un empacador comercial, lo cual dificulta su detección y análisis. Según PRODAFT, se entrega a través de un proceso en tres etapas, comenzando con un archivo APK.

> *"Al inspeccionar el archivo AndroidManifest, se observa que muchos nombres de clase no aparecen en el APK original,"* indicó la empresa. *"Estas clases ausentes se cargan dinámicamente durante la instalación mediante el empacador, e incluyen código malicioso extraído desde un archivo cifrado. Todo el mecanismo está diseñado específicamente para evadir el software antivirus."*

Al ejecutarse, AntiDot muestra una falsa barra de actualización y solicita permisos de accesibilidad. Una vez concedidos, descomprime y carga un archivo DEX que contiene las funciones del botnet.

Una función clave del malware es su capacidad para detectar nuevas aplicaciones abiertas por el usuario y mostrar una pantalla falsa de inicio de sesión desde el servidor C2 cuando se abren apps de criptomonedas o de pagos que interesan a los operadores.



También abusa de los servicios de accesibilidad para recolectar información detallada sobre lo que aparece en pantalla, y se configura como la aplicación predeterminada para SMS, lo que le permite interceptar mensajes entrantes y salientes. Adicionalmente, puede monitorizar llamadas telefónicas, bloquear números específicos o redirigirlas, abriendo nuevas vías para el fraude.

Otra capacidad importante del malware es su habilidad para vigilar en tiempo real las notificaciones que aparecen en la barra de estado, pudiendo silenciarlas o descartarlas para evitar que el usuario detecte actividad sospechosa.

PRODAFT también detalló que el panel C2 que permite controlar remotamente los dispositivos infectados está construido con MeteorJS, un framework JavaScript de código abierto para comunicación en tiempo real. El panel tiene seis pestañas principales:

- Bots: muestra la lista de dispositivos comprometidos junto con sus detalles.
- Injects: enumera las aplicaciones objetivo para los ataques por superposición y permite ver las plantillas usadas.
- Analytic: contiene el listado de apps instaladas en los dispositivos de las víctimas, útil para identificar nuevas aplicaciones populares a atacar.

- Settings: permite modificar la configuración principal, incluyendo la actualización de los ataques por inyección.
- Gates: gestiona los puntos de conexión de la infraestructura de bots.
- Help: proporciona recursos de soporte para el uso del malware.

> *"AntiDot representa una plataforma MaaS escalable y difícil de detectar, diseñada para el lucro financiero mediante el control continuo de dispositivos móviles, especialmente en regiones específicas por idioma o localización,"* señaló la empresa. *"El malware también utiliza inyecciones con WebView y ataques por superposición para robar credenciales, constituyendo una amenaza seria a la privacidad del usuario y la seguridad del dispositivo."*

El regreso de GodFather

Este descubrimiento coincide con el anuncio de Zimperium zLabs, que ha identificado una evolución avanzada del troyano bancario para Android conocido como GodFather, el cual ahora emplea virtualización local en el dispositivo para manipular aplicaciones legítimas de banca y criptomonedas y ejecutar fraudes en tiempo real.

> *"El núcleo de esta nueva técnica radica en la capacidad del malware de crear un entorno virtual completo e independiente dentro del dispositivo de la víctima. En lugar de imitar solo la pantalla de inicio de sesión, el malware instala una aplicación 'host' maliciosa que incorpora un framework de virtualización,"* explicaron los investigadores Fernando Ortega y Vishnu Pratapagiri.
>
> *"Dicho host descarga y ejecuta una copia real de la aplicación bancaria o de criptomonedas dentro de su entorno aislado controlado."*

Cuando el usuario abre la aplicación, es redirigido a la versión virtualizada, desde donde los

atacantes pueden observar todas sus acciones. Además, esta nueva versión de GodFather incluye mecanismos para evitar el análisis estático, como la manipulación de archivos ZIP y la inclusión de permisos irrelevantes en el archivo AndroidManifest.

Al igual que AntiDot, GodFather también se apoya en los servicios de accesibilidad para recopilar información y controlar el dispositivo comprometido. Si bien Google ha aplicado restricciones que impiden a las aplicaciones instaladas por fuera de Play Store activar estos servicios en Android 13, los atacantes pueden evadir esta medida mediante un enfoque de instalación por sesiones.

Este método de instalación por sesión es utilizado por tiendas de aplicaciones, apps de mensajería, correo y navegadores para manejar archivos APK.

Una pieza central del funcionamiento de este malware es su sistema de virtualización. En la primera fase, recopila la lista de aplicaciones instaladas y verifica si alguna coincide con las apps que tiene predefinidas como objetivos.

Si se detecta una coincidencia, el malware extrae información relevante de esas aplicaciones y luego instala una copia dentro de un entorno virtual gestionado por la propia app dropper. Así, cuando la víctima intenta abrir la aplicación bancaria real, GodFather intercepta la acción y redirige al usuario hacia la instancia virtualizada.

Cabe destacar que funcionalidades de virtualización similares ya habían sido identificadas anteriormente en otro malware para Android conocido como FjordPhantom, documentado por Promon en diciembre de 2023. Este enfoque representa un cambio de paradigma en las amenazas móviles, ya que supera las técnicas tradicionales de superposición de pantalla para robar credenciales e información confidencial.

> *"Aunque esta campaña de GodFather tiene un alcance global, afectando a casi 500 aplicaciones distintas, nuestro análisis indica que este sofisticado ataque de virtualización se enfoca actualmente en una docena de instituciones financieras en*

> *Turquía,"* informó la empresa.
>
> *"Una capacidad especialmente preocupante que presenta este malware es la posibilidad de robar las credenciales de desbloqueo del dispositivo, ya sea mediante patrón, PIN o contraseña. Esto representa un riesgo crítico para la privacidad del usuario y la seguridad del dispositivo."*

La empresa de seguridad móvil también advirtió que el uso indebido de los servicios de accesibilidad es una de las múltiples vías mediante las cuales las apps maliciosas logran escalar privilegios en Android, obteniendo permisos que exceden lo necesario para su funcionamiento. Esto incluye el mal uso de permisos otorgados por fabricantes (OEM) y la explotación de vulnerabilidades en aplicaciones preinstaladas que los usuarios no pueden eliminar.

> *"Evitar la escalada de privilegios y proteger el ecosistema Android contra apps maliciosas o con excesivos privilegios requiere más que concientización del usuario o parches reactivos — se necesita una defensa proactiva, escalable e inteligente,"* explicó el investigador en seguridad Ziv Zeira.

En una declaración, Google señaló que no ha detectado ninguna aplicación con este malware en Google Play, y que los usuarios de Android están protegidos contra esta amenaza gracias a Google Play Protect.

> *"Los usuarios de Android están protegidos automáticamente contra versiones conocidas de este malware mediante Google Play Protect, que viene activado por defecto en dispositivos con servicios de Google Play,"* indicó un portavoz. *"Google Play Protect puede alertar a los usuarios o bloquear apps que exhiban comportamientos maliciosos, incluso si estas provienen de fuentes externas a la*

> *tienda oficial."*

SuperCard X apunta a usuarios rusos

Estos hallazgos se suman a los primeros reportes de ataques dirigidos a usuarios en Rusia mediante SuperCard X, un nuevo malware para Android que puede llevar a cabo ataques de retransmisión NFC con el fin de realizar transacciones fraudulentas.

Según la empresa rusa de ciberseguridad F6, SuperCard X es una modificación maliciosa de una herramienta legítima llamada NFCGate, la cual permite capturar o manipular el tráfico NFC. El objetivo del malware es interceptar datos de tráfico NFC y también información de tarjetas bancarias mediante comandos enviados al chip EMV.

> *"Esta aplicación permite a los atacantes robar datos de tarjetas bancarias interceptando el tráfico NFC, para luego sustraer dinero de las cuentas de los usuarios,"* explicó el investigador Alexander Koposov en un informe publicado esta semana.

Los primeros ataques con SuperCard X fueron detectados a inicios de este año en Italia, donde se utilizó la tecnología NFC para retransmitir datos de tarjetas físicas hacia dispositivos controlados por atacantes, con los cuales realizaban retiros fraudulentos en cajeros automáticos o autorizaban pagos en terminales PoS.

Esta plataforma MaaS de habla china, que se promociona en Telegram como capaz de atacar clientes de bancos importantes en EE. UU., Australia y Europa, comparte una gran cantidad de código con NGate, otro malware Android que también ha sido vinculado al uso malicioso de NFCGate, en este caso en la República Checa.

Todas estas campañas tienen en común el uso de técnicas de smishing, es decir, mensajes de texto engañosos que convencen a la víctima de instalar un archivo APK bajo el pretexto

de ser una app útil.

Aplicaciones maliciosas en tiendas oficiales

Aunque la mayoría de los malwares mencionados hasta ahora requieren que los usuarios instalen manualmente las apps desde fuentes externas, nuevas investigaciones han descubierto aplicaciones maliciosas presentes en tiendas oficiales como Google Play Store y Apple App Store. Estas apps pueden recolectar datos personales e incluso robar frases semilla de billeteras de criptomonedas, con el objetivo de vaciar los fondos de las víctimas.

Una de las aplicaciones detectadas, llamada RapiPlata, se estima que fue descargada unas 150,000 veces tanto en dispositivos Android como iOS, lo cual demuestra la magnitud del problema. Este software pertenece a la categoría conocida como SpyLoan, que engaña a los usuarios ofreciendo préstamos con bajos intereses, pero en realidad los somete a extorsión, chantaje y robo de datos.

> *"RapiPlata apunta principalmente a usuarios en Colombia, ofreciendo préstamos rápidos,"* explicó Check Point. *"Más allá de sus prácticas abusivas de crédito, la aplicación realiza un extenso robo de datos. Tenía acceso a información sensible como mensajes SMS, registros de llamadas, eventos de calendario y aplicaciones instaladas — e incluso subía esta información a sus servidores."*

Por otro lado, las apps diseñadas para robar frases semilla de billeteras de criptomonedas fueron distribuidas mediante cuentas de desarrolladores comprometidas, sirviendo páginas de phishing a través de WebView para capturar las claves de recuperación.

Aunque dichas aplicaciones ya fueron eliminadas de las tiendas oficiales, el riesgo persiste, ya que pueden seguir circulando en tiendas de terceros. Se recomienda a los usuarios tener especial precaución al descargar aplicaciones relacionadas con finanzas o préstamos.

Investigadores en ciberseguridad han detectado una nueva campaña en la que actores maliciosos han publicado más de 67 repositorios en GitHub que aparentan contener herramientas de hacking basadas en Python, pero en realidad distribuyen cargas maliciosas camufladas.

Esta actividad, identificada por ReversingLabs con el nombre en clave *Banana Squad*, parece ser una continuación de una operación maliciosa que ya había sido detectada en 2023. En aquella ocasión, se utilizaban paquetes falsos en el repositorio Python Package Index (PyPI), los cuales fueron descargados más de 75,000 veces y estaban diseñados para robar información en sistemas Windows.

Los hallazgos amplían lo reportado previamente por el *Internet Storm Center* del SANS en noviembre de 2024, donde se describía una herramienta falsa llamada *steam-account-checker* alojada en GitHub. Esta herramienta tenía la capacidad de descargar sigilosamente otros scripts en Python para insertar código malicioso en la aplicación de billetera de criptomonedas *Exodus*, y así extraer datos sensibles hacia un servidor externo ("dieserbenni[.]ru").

El análisis más profundo del repositorio y de la infraestructura controlada por los atacantes llevó al descubrimiento de 67 repositorios en GitHub que imitan nombres de proyectos legítimos para engañar a los usuarios.

Hay indicios de que esta campaña apunta a personas que buscan programas como limpiadores de cuentas o trampas para videojuegos, incluyendo herramientas como *Discord account cleaner*, *Fortnite External Cheat*, *TikTok username checker* y *PayPal bulk account checker*. Todos los repositorios detectados han sido eliminados por GitHub.

> *"El uso de puertas traseras y código malicioso en repositorios públicos como los de GitHub está en aumento, y representa un riesgo creciente en la cadena de suministro de software,"* afirmó Robert Simmons, investigador de ReversingLabs.

> *"Para los desarrolladores que dependen de plataformas de código abierto, es fundamental verificar siempre que el repositorio realmente contenga lo que promete."*

GitHub como vector para distribuir malware

Este descubrimiento ocurre en un momento en que GitHub se ha convertido cada vez más en el objetivo de campañas que lo utilizan como canal para distribuir malware. Esta misma semana, Trend Micro informó haber identificado 76 repositorios maliciosos en GitHub operados por un grupo denominado *Water Curse*, utilizados para propagar malware en múltiples etapas.

Estas cargas están diseñadas para robar credenciales, información del navegador y tokens de sesión, además de brindar acceso remoto persistente a los sistemas comprometidos.

Por otro lado, Check Point reveló otra campaña que emplea un servicio criminal conocido como *Stargazers Ghost Network*, el cual apunta a usuarios de Minecraft utilizando malware escrito en Java. *Stargazers Ghost Network* hace referencia a una red de cuentas en GitHub que propagan malware o enlaces dañinos mediante repositorios de phishing.

> *"La red está compuesta por múltiples cuentas que distribuyen enlaces maliciosos y malware, y realizan acciones como marcar con estrellas, bifurcar y suscribirse a repositorios maliciosos para hacerlos parecer legítimos,"* indicó Check Point.

La compañía de ciberseguridad también concluyó que estas *"cuentas fantasma en GitHub son solo una parte del panorama general, con otras cuentas similares operando en diferentes plataformas como parte de un ecosistema mayor de Distribución-como-Servicio."*

Algunos aspectos de esta red fueron expuestos por Checkmarx en abril de 2024, destacando el patrón del grupo atacante de usar estrellas falsas y actualizaciones frecuentes para inflar

artificialmente la visibilidad de los repositorios en los resultados de búsqueda de GitHub.

Estos proyectos maliciosos están hábilmente disfrazados como herramientas legítimas relacionadas con videojuegos populares, trampas, rastreadores de precios de criptomonedas o predictores de multiplicadores en juegos de apuestas.

Estas campañas también coinciden con otra ola de ataques dirigida a cibercriminales novatos que buscan malware y herramientas listas para usar en GitHub, siendo infectados a través de repositorios con puertas traseras.

En un caso reportado este mes por Sophos, se descubrió que el repositorio *Sakura-RAT*, que contenía un troyano, infectaba a quienes compilaban el código en sus sistemas, instalando *stealers* de información y troyanos de acceso remoto (RATs).

Los repositorios identificados contienen hasta cuatro tipos distintos de puertas traseras, integradas en eventos *PreBuild* de Visual Studio, scripts en Python, archivos de salvapantallas y código JavaScript. Estas puertas traseras permiten robar datos, tomar capturas de pantalla, comunicarse por Telegram y descargar más malware como *AsyncRAT*, *Remcos RAT* y *Lumma Stealer*.

En total, Sophos indicó haber detectado al menos 133 repositorios comprometidos como parte de esta campaña, 111 de los cuales contenían la puerta trasera en *PreBuild*, mientras que los demás incluían backdoors en Python, salvapantallas o JavaScript.

Sophos añadió que estas actividades probablemente forman parte de una operación de distribución-como-servicio activa desde agosto de 2022, que ha utilizado miles de cuentas en GitHub para difundir malware incrustado en proyectos relacionados con trampas de videojuegos, exploits y herramientas de ataque.

Aunque no está claro el método exacto de distribución empleado, se sospecha que los actores también están aprovechando servidores de Discord y canales de YouTube para compartir enlaces a los repositorios maliciosos.

> *"No está confirmado si esta campaña está relacionada directamente con otras previamente identificadas, pero el enfoque parece ser efectivo y probablemente continúe bajo otras formas,"* señaló Sophos.
>
> *"En el futuro, es posible que el objetivo se desplace, y los atacantes enfoquen sus esfuerzos en otros grupos además de los cibercriminales inexpertos y jugadores que usan trampas."*

Chet Wisniewski, director y CISO de campo en Sophos, declaró que *"hay similitudes llamativas"* entre esta campaña y *Water Curse*. Estas incluyen:

- Repositorios con nombres casi idénticos
- Uso extensivo de cuentas en GitHub
- Enfoque común en aplicaciones desarrolladas con Electron
- Uso similar de los eventos *PreBuild* en Visual Studio
- Una referencia al correo electrónico "ischhfd83" ("ischhfd83@rambler[.]ru") como autor de los commits en GitHub

> *"Si estas campañas están directamente conectadas o simplemente forman parte de un mismo conjunto de amenazas que comparte código y metodología, es algo que requiere más investigación,"* concluyó Wisniewski.

Cloudflare anunció el jueves que bloqueó de forma automatizada el mayor ataque de denegación de servicio distribuido (DDoS) del que se tenga registro, alcanzando una velocidad máxima de 7.3 terabits por segundo (Tbps).

El ataque fue detectado a mediados de mayo de 2025 y tuvo como blanco a un proveedor de hosting cuya identidad no ha sido revelada.

> *«Los servicios de alojamiento y componentes esenciales del ecosistema de Internet se han convertido en objetivos frecuentes de ataques DDoS. Este ataque de 7.3 Tbps transfirió 37.4 terabytes en tan solo 45 segundos»,* explicó Omer Yoachimik, de Cloudflare.

En enero de este año, la empresa especializada en seguridad y servicios web informó que contuvo un ataque DDoS de 5.6 Tbps dirigido contra un proveedor de Internet del este asiático. Dicha ofensiva tuvo su origen en un botnet basado en una variante de Mirai, en octubre de 2024.

Posteriormente, en abril de 2025, Cloudflare también se defendió exitosamente de una oleada de 6.5 Tbps que se atribuye al botnet Eleven11bot, conformado por unas 30,000 cámaras IP y grabadores de video. Este ataque de alta intensidad se extendió por aproximadamente 49 segundos.

En contraste, la ofensiva de 7.3 Tbps se centró en una única dirección IP del proveedor de alojamiento, atacando en promedio 21,925 puertos de destino por segundo, con picos de hasta 34,517 puertos distintos.

El ataque empleó múltiples vectores y utilizó una combinación de técnicas como inundación por UDP, ataques de reflexión QOTD, echo, y NTP, además de variantes del botnet Mirai, ataques portmap y amplificación basada en RIPv1. La mayoría del tráfico malicioso (99.996%) correspondió a la modalidad de UDP flood.

Cloudflare destacó que la arremetida provino de más de 122,145 direcciones IP únicas, distribuidas entre 5,433 sistemas autónomos en 161 países. Entre los principales países de origen del tráfico malicioso se encuentran Brasil, Vietnam, Taiwán, China, Indonesia, Ucrania, Ecuador, Tailandia, EE. UU. y Arabia Saudita.

> *«Se observó un promedio de 26,855 IPs únicas por segundo, con un máximo registrado de 45,097»,* añadió Yoachimik.

> *«Telefónica Brasil (AS27699) generó la mayor parte del tráfico ofensivo, con un 10.5%. Le siguieron el Grupo Viettel (AS7552) con 9.8%, China Unicom (AS4837) con 3.9%, y Chunghwa Telecom (AS3462) con 2.9%. China Telecom (AS4134) fue responsable del 2.8%».*

La información se publica mientras el equipo XLab de QiAnXin atribuye al botnet RapperBot un ataque contra la firma de inteligencia artificial DeepSeek en febrero de 2025, señalando además que las versiones más recientes del malware buscan extorsionar a sus víctimas solicitando pagos de "protección" para evitar futuros ataques DDoS.

Los países con más dispositivos infectados por RapperBot son China, EE. UU., Israel, México, Reino Unido, Grecia, Irán, Australia, Malasia y Tailandia. Este botnet ha estado activo desde 2022.

Las campañas de RapperBot tienen como blanco enrutadores, dispositivos NAS y grabadores de video, a los que accede mediante contraseñas por defecto débiles o vulnerabilidades del firmware. Luego, instala software malicioso que se conecta con servidores remotos usando registros DNS TXT para recibir instrucciones de ataque.

Además, el malware emplea cifrados personalizados para ocultar los registros TXT y los dominios usados para el control del botnet.

> *«Desde marzo, ha incrementado notablemente su actividad, con más de 100 objetivos diarios y al menos 50,000 bots en funcionamiento»*, explicó la firma china de ciberseguridad.

> *«Las víctimas de RapperBot se distribuyen en múltiples sectores: administración pública, servicios sociales, organizaciones civiles, plataformas digitales, industrias manufactureras y financieras»,* concluyó.

En la última década, los casinos online en México han dejado de ser una curiosidad digital para convertirse en un fenómeno cultural y tecnológico en plena expansión. Lo que antes se limitaba a simples tragamonedas en la web, hoy es una experiencia inmersiva que combina inteligencia artificial, crupieres en vivo, realidad virtual y pagos con criptomonedas. Esta evolución no solo ha transformado la manera en que millones de mexicanos se entretienen, sino que también ha puesto al país en la mira como uno de los mercados emergentes más dinámicos del iGaming en América Latina con casinos como www.novibet.mx.

Impulsados por la conectividad móvil, la digitalización financiera y una creciente demanda por experiencias personalizadas, los casinos online han sabido adaptarse al ritmo acelerado de la innovación. Y lo mejor aún está por venir: el futuro apunta hacia el metaverso, la biometría y plataformas donde el juego será más social, más seguro y más inteligente que nunca.

En este post detallaremos las principales innovaciones que están redefiniendo a los casinos digitales en México y lo que podemos esperar de ellos en los próximos años.

1. Realidad Virtual (RV) y Realidad Aumentada (RA)

Los casinos digitales están adoptando entornos tridimensionales, permitiendo a los usuarios moverse por salones virtuales, interactuar en vivo con crupieres y jugadores, y sentir una experiencia casi física desde casa.

Mientras que la RV ofrece inmersión total con auriculares dedicados, la RA superpone elementos del casino en la realidad del jugador, accesible con un smartphone.

2. Transmisión en vivo con crupieres reales

El clásico “live dealer” se ha potenciado con mejoras tecnológicas: vídeo HD, chats en tiempo real y conexión social entre jugadores.

Esta modalidad combina lo mejor del casino físico —interacción humana, espontaneidad—

con la comodidad de jugar desde casa.

3. Inteligencia Artificial y personalización

La IA analiza patrones de juego para sugerir títulos, promociones o bonos personalizados, optimizando la experiencia del usuario.

También fortalece la seguridad, identificando comportamientos sospechosos o signos de adicción desde etapas tempranas y activando alertas preventivas.

Además, se cuenta con Chatbots y atención 24/7 lo que mejora la eficiencia en la resolución de dudas.

4. Blockchain y criptomonedas

La tecnología blockchain garantiza transacciones seguras, transparentes y auditables, además de permitir “provably fair”—juegos verificables por el usuario.

Las criptomonedas como Bitcoin o Ethereum ofrecen pagos rápidos, anónimos y con tarifas reducidas.

5. Big Data, Gamificación y Móvil-First

El análisis de Big Data permite adaptar promociones y diseñar programas de fidelización personalizados, con niveles, misiones y recompensas.

Asimismo, las plataformas adoptan un diseño “mobile-first”, ofreciendo apps optimizadas para torneos en vivo y uso por voz o gestos.

Fruto de la nube, ahora se puede jugar sin descargar, agilizando tiempos y reduciendo espacio en el dispositivo.

Lo que se espera a futuro de los casinos online

Mirando hacia el futuro, son diversas las expectativas que se proyectan sobre las casas de entretenimiento web:

Experiencias inmersivas y metaverso

Integración del metaverso por medio de casinos persistentes en 3D con avatares, propiedad virtual y socialización constante.

Avances en tecnología háptica con guantes y controladores que permiten sentir fichas, cartas o ruletas.

Pagos instantáneos y biométricos

Las criptomonedas se convierten en opción estándar.

Y los pagos biométricos —huella o reconocimiento facial— reducirán fricción y aumentarán seguridad.

IA avanzada y juego responsable

Algoritmos predictivos prevendrán adicciones e impulsarán estrategias de juego saludable.

IA podrá adaptar dinámicamente la dificultad del juego según habilidades del usuario.

Juegos de Habilidad y Social-gaming

Aparición de juegos que mezclan azar con estrategia, orientados a medir habilidad.

Más funciones sociales, competencias, torneos e integración con redes.

Aplicaciones 100 % móviles

Crecimiento de plataformas móviles que sustenten streaming, RV/AR y pago biométrico de forma ágil y nativa.

Los casinos online en México están evolucionando de simples plataformas de azar a ecosistemas digitales hiperpersonalizados, seguros, sociales e inmersivos. Con una regulación adaptativa y medidas de juego responsable, este sector promete convertirse en uno de los referentes del entretenimiento digital, marcando el camino hacia experiencias de juego más humanas y tecnológicamente avanzadas.