Un actor de amenazas identificado como Mr_Rot13 ha sido vinculado a la explotación de una vulnerabilidad crítica recientemente revelada en cPanel para desplegar una puerta trasera denominada *Filemanager* en sistemas comprometidos.

El ataque aprovecha la vulnerabilidad CVE-2026-41940, una falla que afecta a cPanel y WebHost Manager (WHM), y que podría derivar en una omisión de autenticación permitiendo a atacantes remotos obtener control elevado sobre el panel de administración.

De acuerdo con un nuevo informe de QiAnXin XLab, la vulnerabilidad comenzó a ser explotada por múltiples actores maliciosos poco después de hacerse pública a finales del mes pasado, dando lugar a actividades como minería de criptomonedas, despliegue de ransomware, propagación de botnets e instalación de puertas traseras.

*"Los datos de monitoreo muestran que actualmente más de 2,000 direcciones IP de origen están involucradas en ataques automatizados y actividades cibercriminales dirigidas a esta vulnerabilidad"*, señalaron investigadores de QiAnXin XLab. *"Estas IP están distribuidas en múltiples regiones del mundo, principalmente en Alemania, Estados Unidos, Brasil, Países Bajos y otros territorios."*

El análisis adicional de la actividad maliciosa permitió identificar un script de shell que utiliza *wget* o *curl* para descargar un infectador desarrollado en Go desde un servidor remoto (*cp.dene.[de[.]com*). Este malware está diseñado para implantar una clave pública SSH en sistemas comprometidos con cPanel con el objetivo de mantener acceso persistente, además de desplegar una web shell PHP que permite subir y descargar archivos, así como ejecutar comandos de forma remota.

Posteriormente, la web shell se utiliza para inyectar código JavaScript capaz de mostrar una página de inicio de sesión personalizada destinada al robo de credenciales. La información sustraída es enviada a un sistema controlado por el atacante, codificado mediante el cifrado ROT13 y asociado al dominio *wrned[.]com*. Una vez transmitidos los datos, la cadena de ataque finaliza con la instalación de una puerta trasera multiplataforma capaz de comprometer sistemas Windows, macOS y Linux.

El infectador también posee capacidades para recopilar información sensible del sistema afectado, incluyendo historial de bash, datos SSH, información del dispositivo, contraseñas de bases de datos y alias virtuales de cPanel (valiases). Posteriormente, esta información es enviada a un grupo de Telegram compuesto por tres miembros y administrado por un usuario identificado como *"0xWR"*.

En la secuencia de infección analizada por QiAnXin XLab, *Filemanager* es distribuido mediante un script shell descargado desde el dominio *wpsock[.]com*. La puerta trasera ofrece funciones de administración de archivos, ejecución remota de comandos y acceso tipo shell.

Existen indicios de que el actor detrás de esta operación ha permanecido activo de forma encubierta durante varios años. Esta evaluación se basa en que el dominio de comando y control (C2) incrustado en el código JavaScript ya había sido utilizado anteriormente en una puerta trasera PHP llamada *"helper.php"*, cargada en la plataforma VirusTotal en abril de 2022. Además, el dominio fue registrado inicialmente en octubre de 2020.

*"Durante los seis años transcurridos desde 2020 hasta la actualidad, la tasa de detección de las muestras e infraestructura relacionadas con Mr_Rot13 ha permanecido extremadamente baja en los distintos productos de seguridad"*, concluyó QiAnXin XLab.