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.

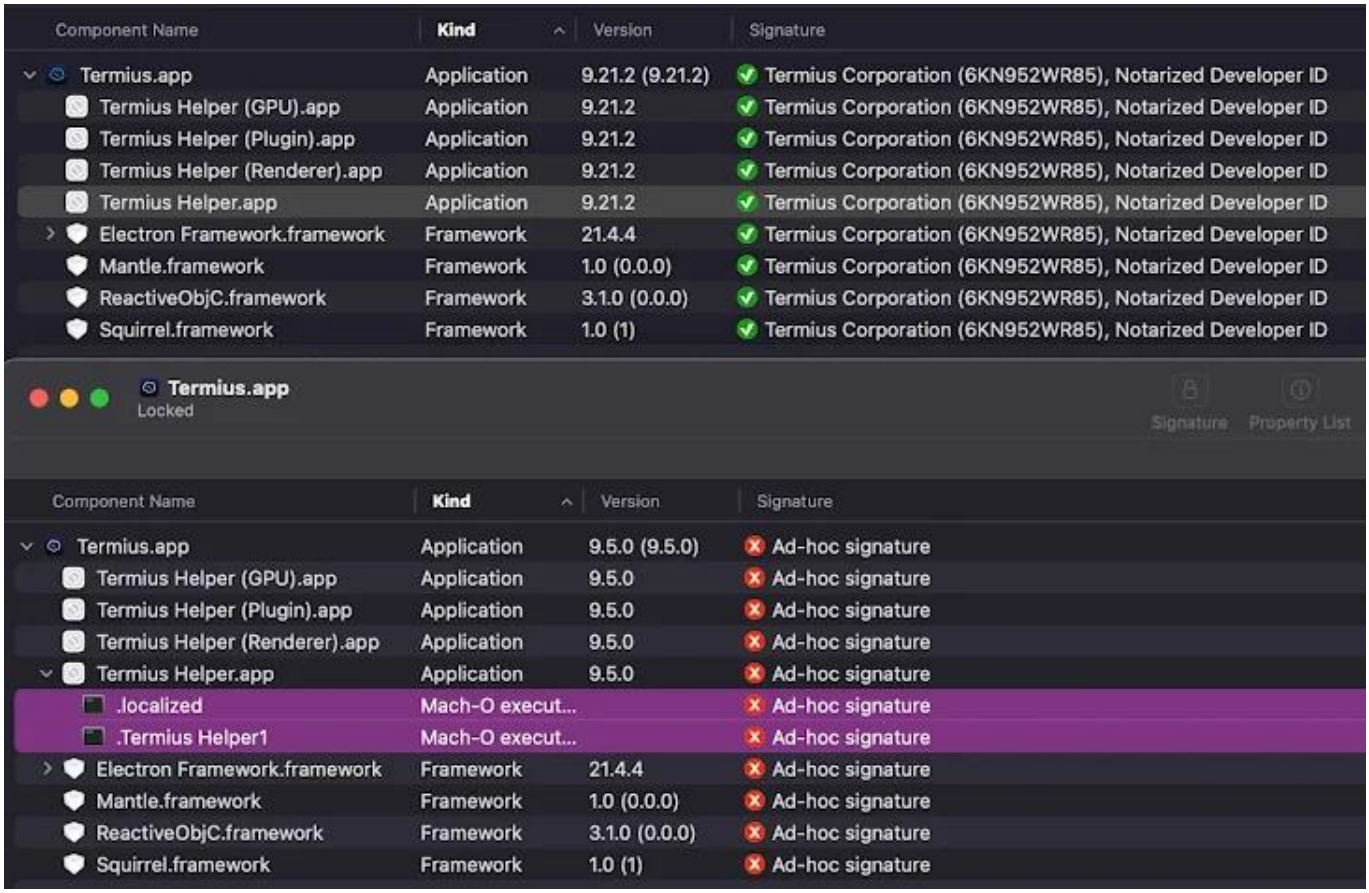
El primer registro de ZuRu se remonta a septiembre de 2021, cuando un usuario en el portal chino Zhihu alertó sobre una campaña maliciosa que manipulaba búsquedas de *iTerm2* —una terminal auténtica de macOS— para redirigir a víctimas a sitios engañosos y distribuir el malware.

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.”*