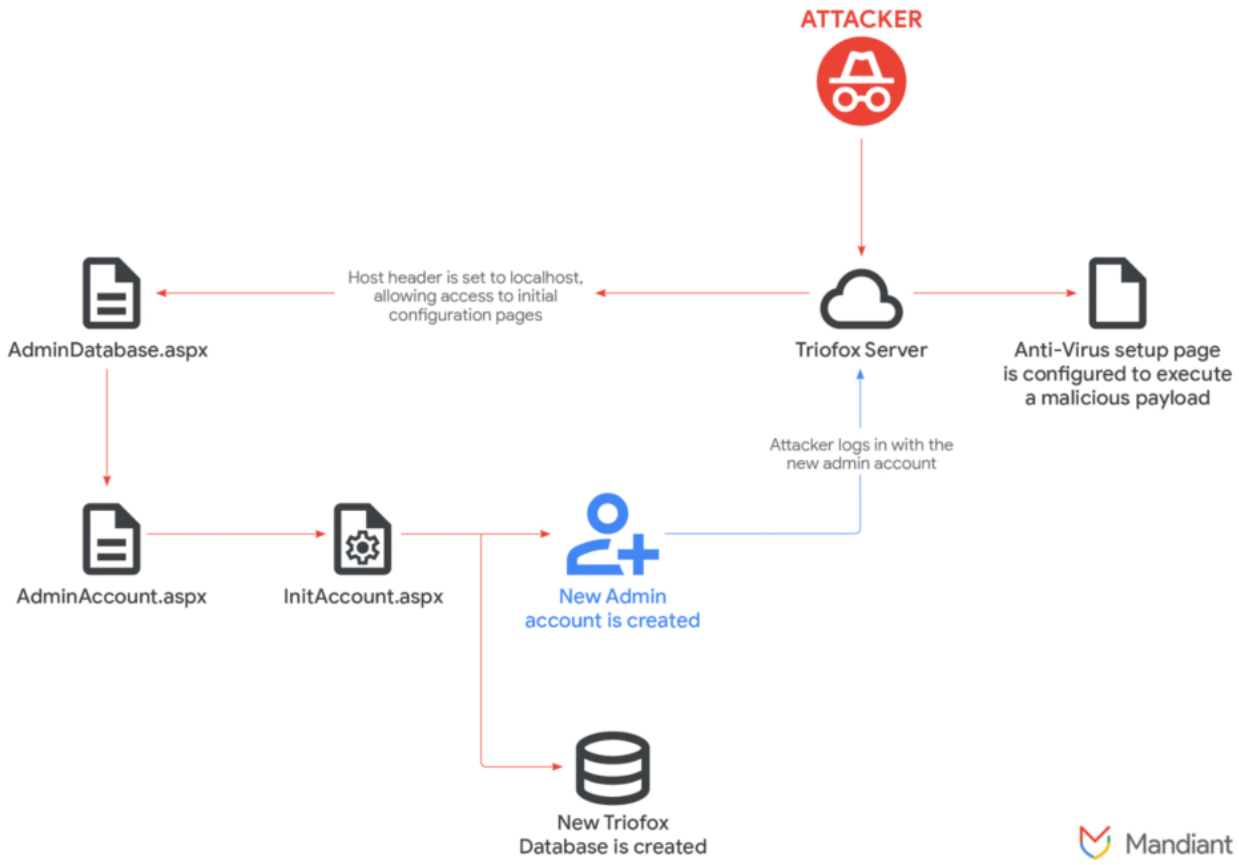
Google Mandiant Threat Defense informó el lunes que detectó la explotación de una vulnerabilidad 0-Day ya corregida en la plataforma de intercambio de archivos y acceso remoto Triofox de Gladinet.

La falla crítica, registrada como CVE-2025-12480 (puntuación CVSS: 9.1), permitía a un atacante eludir la autenticación y acceder a las páginas de configuración, lo que posibilitaba la subida y ejecución de cargas útiles arbitrarias.

La compañía de seguridad indicó que identificó a un grupo de amenaza etiquetado como UNC6485 explotando el fallo desde el 24 de agosto de 2025, casi un mes después de que Gladinet publicara parches en la versión 16.7.10368.56560. Cabe señalar que CVE-2025-12480 es el tercer defecto en Triofox que ha sido activamente explotado este año, tras CVE-2025-30406 y CVE-2025-11371.

"Se añadió protección para las páginas de configuración inicial," según las notas de la versión del software. *"Estas páginas ya no pueden ser accesadas una vez que Triofox ha sido configurado."*

Mandiant explicó que el actor malicioso aprovechó la vulnerabilidad de acceso no autenticado para entrar en las páginas de configuración y, mediante el proceso de instalación, crear una nueva cuenta administrativa nativa llamada Cluster Admin. Esa cuenta recién creada fue usada después para llevar a cabo actividades posteriores.



"Para lograr la ejecución de código, el atacante inició sesión con la cuenta Admin recién creada. El atacante subió archivos maliciosos para ejecutarlos utilizando la función antivirus integrada," afirmaron los investigadores Stallone D'Souza, Praveeth DSouza, Bill Glynn, Kevin O'Flynn y Yash Gupta.

"Para configurar la función antivirus, al usuario se le permite indicar una ruta arbitraria para el antivirus seleccionado. El archivo configurado como ubicación del escáner antivirus hereda los privilegios de la cuenta del proceso padre de Triofox, ejecutándose en el contexto de la cuenta SYSTEM."

Según Mandiant, los atacantes ejecutaron su script malicioso (*"centre_report.bat"*)

configurando la ruta del motor antivirus para apuntar al script. El script estaba diseñado para descargar un instalador del sistema Zoho Unified Endpoint Management (UEMS) desde 84.200.80[.]252 y usarlo para desplegar programas de acceso remoto como Zoho Assist y AnyDesk en el equipo.

El acceso remoto proporcionado por Zoho Assist se empleó para realizar reconocimiento y, a continuación, intentos de cambiar contraseñas de cuentas existentes y añadirlas a administradores locales y al grupo *Domain Admins* para escalar privilegios.

Para evitar la detección, los actores descargaron herramientas como Plink y PuTTY para establecer un túnel cifrado hacia un servidor de mando y control (C2) por el puerto 433 vía SSH, con el objetivo final de permitir tráfico RDP entrante.

Aunque el propósito final de la campaña sigue sin estar claro, se recomienda a los usuarios de Triofox actualizar a la versión más reciente, auditar las cuentas administrativas y verificar que el motor antivirus de Triofox no esté configurado para ejecutar scripts o binarios no autorizados.