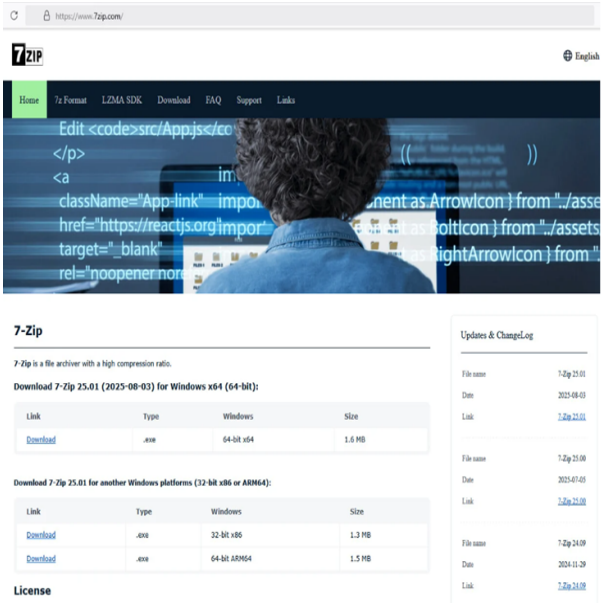
Boletín de alerta

Boletín Nro.: 14
Fecha de publicación: 11/02/2026
Tema: Alerta 2026-14 Distribución de versión troyanizada de 7zip
Traffic Light Protocol (TLP): White

Descripción

Recientemente se ha identificado una campaña activa de malware que abusa de la popularidad de un software ampliamente utilizado para comprometer sistemas de usuario final. En este caso, los atacantes distribuyen una versión troyanizada de 7-Zip, una herramienta legítima de compresión de archivos, mediante un sitio web falso visualmente casi idéntico al oficial. El dominio utilizado, 7zip[.]com, suplanta al legítimo 7-zip.org, lo que facilita que usuarios descarguen el instalador malicioso sin levantar sospechas, especialmente cuando el enlace proviene de tutoriales, videos o recomendaciones externas.



Sitio web malicioso del 7-Zip falso

El mecanismo de infección y persistencia

El instalador malicioso cumple una doble función. Por un lado, instala correctamente 7-Zip, permitiendo al usuario utilizar la aplicación sin notar anomalías inmediatas. De forma paralela y silenciosa, despliega una serie de binarios adicionales diseñados para convertir el equipo comprometido en un nodo proxy residencial, permitiendo que terceros enruten tráfico a través de la conexión de la víctima. Este comportamiento no busca el robo inmediato de información, sino el abuso de infraestructura, lo que

dificulta la detección temprana al no generar síntomas evidentes en el sistema.

Desde el punto de vista técnico, la infección introduce varios archivos ejecutables y librerías dentro del directorio C:\Windows\SysWOW64\hero\, una ubicación que no corresponde a ninguna instalación legítima de 7-Zip. Estos binarios son registrados como servicios de Windows para garantizar persistencia tras reinicios del sistema. Además, el malware modifica reglas del firewall local utilizando utilidades nativas del sistema operativo, permitiendo el tráfico de red de estos procesos sin generar alertas visibles para el usuario.

Un aspecto relevante de esta campaña es que el instalador estuvo firmado digitalmente mediante un certificado Authenticode que posteriormente fue revocado. Esto sugiere un intento deliberado de aumentar la tasa de éxito de la infección evadiendo controles básicos de seguridad y mecanismos de advertencia del sistema operativo. Aunque el certificado ya no es válido, los sistemas que no realizan validación estricta de firmas o que confían en binarios previamente descargados pueden seguir siendo vulnerables.

Comportamiento en la red y el sistema

Una vez activo, el componente principal establece comunicación con infraestructura externa controlada por los atacantes. A través de esta comunicación, el equipo pasa a formar parte de una red de proxies residenciales, lo que puede ser utilizado para ocultar actividades maliciosas, evadir bloqueos geográficos o distribuir tráfico abusivo desde direcciones IP legítimas. Desde la perspectiva de una organización, esto representa un riesgo significativo, ya que un endpoint comprometido puede generar tráfico anómalo que afecte la reputación de la IP corporativa o viole políticas de uso aceptable.

A nivel de red, este tipo de amenaza puede manifestarse como conexiones salientes constantes hacia dominios poco comunes, uso de puertos no estándar desde estaciones de trabajo y patrones de tráfico incompatibles con el perfil normal del usuario. En entornos corporativos con EDR o SIEM, resulta clave correlacionar la instalación reciente de software con la creación de nuevos servicios, procesos persistentes y cambios en la configuración de seguridad del endpoint.

Respuesta y verificación interna

Para los equipos de IT y Ciberseguridad, la detección interna no debe centrarse únicamente en la presencia de 7-Zip, sino en cómo y desde dónde fue instalado. La existencia de servicios desconocidos asociados a binarios en rutas inusuales, especialmente bajo SysWOW64\hero\, es un fuerte indicador de compromiso. Asimismo, cualquier modificación no autorizada de reglas de firewall local o tráfico saliente persistente hacia dominios no relacionados con funciones de negocio debe considerarse sospechosa y analizarse en profundidad.

Más allá de la remediación técnica, esta campaña refuerza la necesidad de controles preventivos. La restricción de descargas de software desde dominios no autorizados, el uso de catálogos internos de aplicaciones aprobadas y la validación estricta de firmas digitales reducen significativamente la superficie de ataque. De igual forma, la concientización de usuarios sigue siendo un componente crítico, ya que el vector inicial no es una vulnerabilidad del software, sino el error humano inducido por suplantación de

marca.

El listado de Indicadores de Compromiso (IoCs) es el siguiente

Rutas de archivos:

- C:\Windows\SysWOW64\hero\Uphero.exe
- C:\Windows\SysWOW64\hero\hero.exe
- C:\Windows\SysWOW64\hero\hero.dll

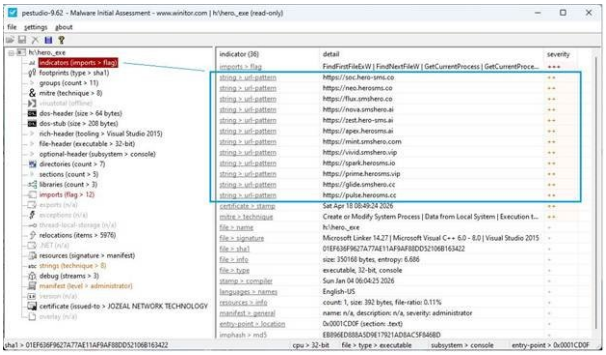
Hashes de archivos:

- e7291095de78484039fdc82106d191bf41b7469811c4e31b4228227911d25027 (Uphero.exe)
- b7a7013b951c3cea178ece3363e3dd06626b9b98ee27ebfd7c161d0bbcfbd894 (hero.exe)
- 3544ffefb2a38bf4faf6181aa4374f4c186d3c2a7b9b059244b65dce8d5688d9 (hero.dll)

Indicadores de red:

Dominios:

- soc.hero-sms[.]co
- neo.herosms[.]co
- flux.smshero[.]co
- nova.smshero[.]ai
- apex.herosms[.]ai
- spark.herosms[.]io
- zest.hero-sms[.]ai
- prime.herosms[.]vip
- vivid.smshero[.]vip
- mint.smshero[.]com
- pulse.herosms[.]cc
- glide.smshero[.]cc
- svc.ha-teams.office[.]com
- iplogger[.]org



IPs observadas:

- 104.21.57.71

- 172.67.160.241

Información adicional:

- https://www.malwarebytes.com/blog/threat-intel/2026/02/fake-7-zip-downloads-are-turning-home-pcs-into-proxy-nodes?utm_campaign=brandsocial&utm_medium=social&utm_source=twitter
- https://exchange.xforce.ibmcloud.com/osint/guid:c143a0e13eac40fd951147baeb3ec42b
- https://x.com/anyrun_app/status/1942905210294124892?s=20