I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad Zero-Day
Tipo de Incidente: Explotación remota / Phishing dirigido
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR - figura referencial

Alerta sobre vulnerabilidad de Zero-day en WinRar que está siendo explotada por el grupo cibernético RomCom, rastreada como CVE-2025-8088, permite a los atacantes ocultar archivos maliciosos en un archivo comprimido o .rar que se despliegan silenciosamente durante la extracción.

III. INTRODUCCIÓN

WinRAR es una de las herramientas de compresión más usadas globalmente, con cientos de millones de usuarios. Su eficiencia en manejo de archivos y facilidad de uso la hacen indispensable, pero también la convierte en un blanco frecuente para atacantes que buscan aprovechar vulnerabilidades críticas para comprometer sistemas.

Investigadores de ESET Research descubrieron una vulnerabilidad en winRAR junto con herramientas relacionadas como el UnRAR.dll y su código fuente portátil, la cual fue identificada como CVE-2025-8088 de Path traversal (CWE-35): esta ocurre cuando una aplicación utiliza entradas externas (como parámetros de URL o datos de usuario) para construir rutas de acceso a archivos o directorios sin una validación adecuada. Esto permite a un atacante manipular las rutas para acceder a archivos o directorios

fuera del directorio previsto, comprometiendo la confidencialidad, integridad o disponibilidad del sistema.

La vulnerabilidad permite ocultar archivos maliciosos en un archivo comprimido, que se despliegan silenciosamente al extraerlo. ESET observo una DLL maliciosa de nombre msedge.dll en un archivo RAR que contenía rutas inusuales, tras un análisis más detallado, descubrieron que CVE-2025-8088 utiliza flujos de datos alternativos (ADS) para atravesar la ruta, los atacantes crearon especialmente el archivo para que aparentemente sólo contuviera un archivo benigno, mientras que contiene muchos ADS maliciosos.

Estos ADS pueden almacenar información oculta vinculada a un archivo visible como por ejemplo: un documento .txt que podría contener un ejecutable malicioso en su ADS, estos no se muestran al listar archivos con comandos básicos como dir en Windows, también muchos virus, ransomware y rootkits usan ADS para esconder código malicioso o configuraciones.

IV. VECTOR DE ATAQUE

Esta vulnerabilidad tiene un vector de ataque de tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H con un grado de severidad de 8.8.

Detalles de investigación de ESET Research

Dentro de un archivo .RAR se insertan múltiples ADS con rutas manipuladas que sean visualmente distractoras y otras rutas reales con payload (.dll, .lnk), el archivo RAR se envía a través de phishing, generalmente con temas relacionados a empleo, contratos, etc.

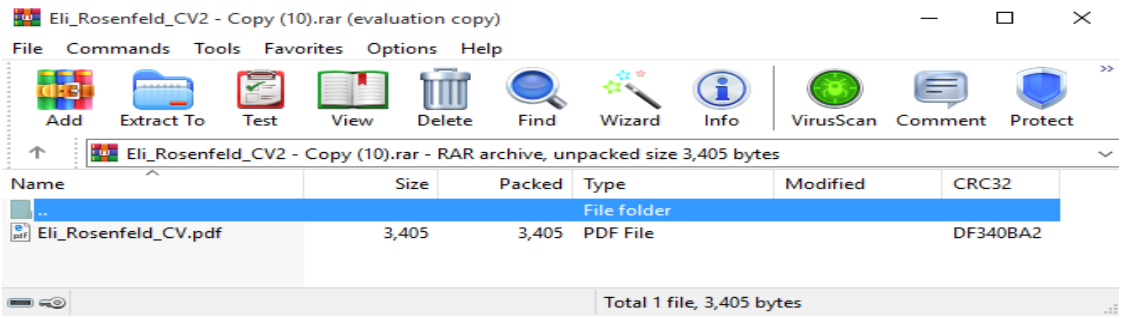

Figura 2.- Archivo muestra que desencadena ADS - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Una vez que la víctima abre el archivo aparentemente inofensivo, WinRAR lo descomprime junto con todos sus ADS, se despliega un archivo **DLL** malicioso en la

carpeta **%TEMP%** o **%LOCALAPPDATA%**. Del mismo modo, se despliega un archivo **LNK** malicioso en el directorio de inicio de Windows, lo que permite la persistencia mediante la ejecución de inicio de sesión del usuario.

Para garantizar un mayor éxito, los atacantes proporcionaron múltiples ADS con profundidades crecientes de elementos de ruta relativa del directorio principal (..\\). Sin embargo, esto introduce rutas inexistentes sobre las que WinRAR advierte de forma visible. Curiosamente, los atacantes añadieron ADS que contienen datos ficticios y que se espera que tengan rutas no válidas. Sospechamos que los atacantes los introdujeron para que la víctima no se diera cuenta de las rutas sospechosas de DLL y LNK.

WinRAR lanza múltiples advertencias sobre rutas no válidas para distraer al usuario, y solo al desplazarse hacia abajo en la interfaz gráfica del aplicativo se revelan las rutas sospechosas.

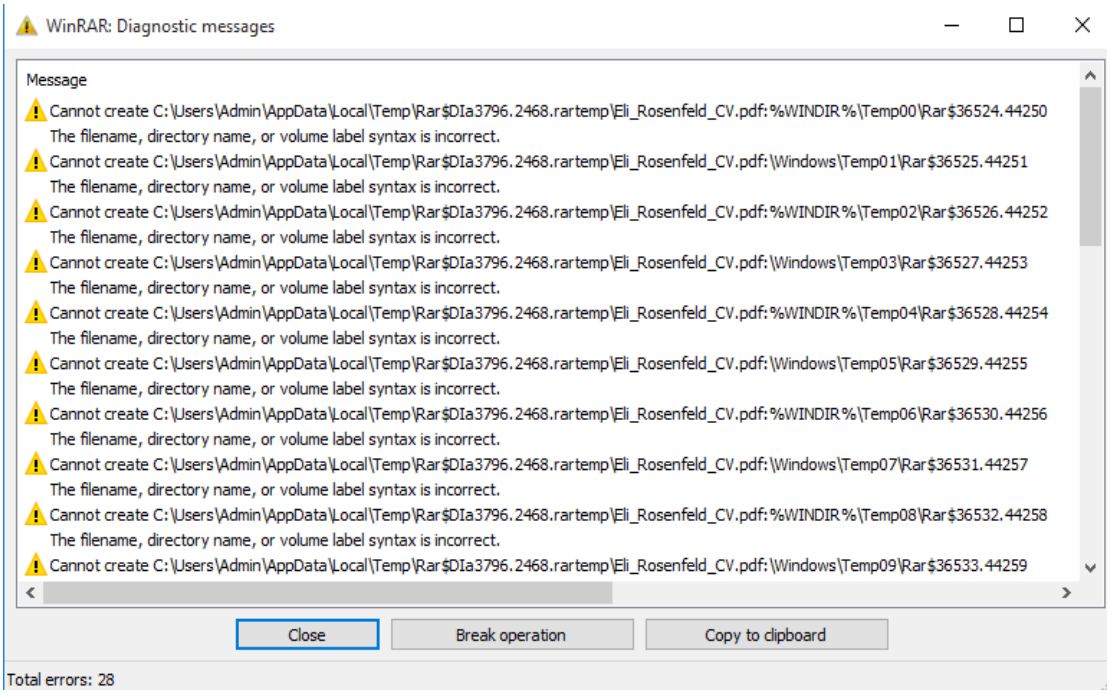

Figura 3.- Errores intencionales y ruido visual para que el usuario ignore lo mensaje realmente peligrosos - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

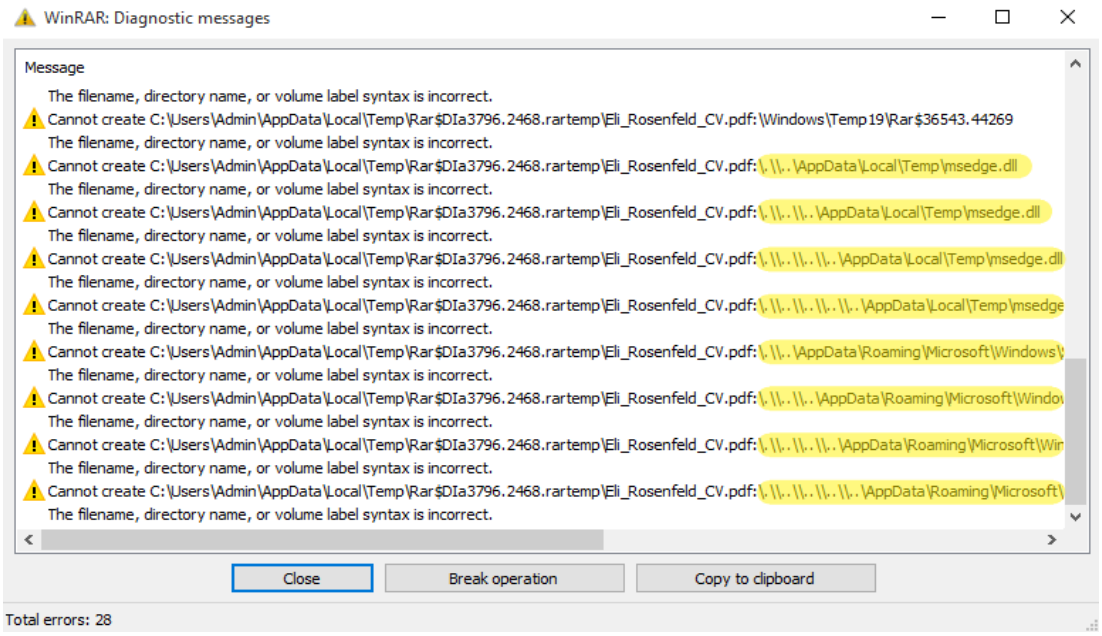

Figura 4.- Rutas sospechosas de DLL y LNK reveladas - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Dependiendo de la carga, se puede establecer una conexión C2, desplegar ransomware o realizar demás acciones maliciosas.

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Producto	Versión afectada	Estado actual
WinRAR	Hasta la versión 7.12	Vulnerable
WinRAR	Desde la versión 7.13	Corregido
RAR para Windows	Hasta 7.12	Vulnerable
UnRAR para Windows	Hasta 7.12	Vulnerable
UnRAR.dll	Hasta 7.12	Vulnerable
Código fuente de UnRAR (Windows)	Hasta 7.12	Vulnerable
RAR/UnRAR para Unix	N/A (no afectado)	Seguro
RAR para Android	N/A (no afectado)	Seguro

Tabla 1.- Productos y Versiones afectadas - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

VI. INDICADORES DE COMPROMISO

Nombre de detección
LNK/Agent[.]AJN

Nombre de detección
Win64/Agent[.]GPM
Win64/TrojanDownloader[.]Agent[.]BZV
Win64/Agent[.]GNV
Win64/Agent[.]GMQ

Tabla 2.- Nombre de Detección - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Infraestructura C2
162.19.175[.]44
194.36.209[.]127
85.158.108[.]62
185.173.235[.]134

Tabla 3.- Infraestructura C2 - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Dominios
gohazeldale[.]com
srlaptop[.]com
melamorri[.]com
campanole[.]com

Tabla 4.- Dominios - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Archivos sospechosos (nombres de muestra)
Adverse_Effect_Medical_Records_2025[.]rar
cv_submission[.]rar
Eli_Rosenfeld_CV2 – Copy (10)[.]rar
Datos adjuntos sin título 00170[.]dat
JobDocs_July2025[.]rar
Recruitment_Dossier_July_2025[.]rar
install_module_x64[.]dll
msedge[.]dll
Complaint[.]exe
ApbxHelper[.]exe

Tabla 5.- Archivos Sospechosos - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Hashes MD5
391325100384964325ed4ace788c8bc2
df9cfd04d8cda6dd8f7263af54f9e5b1
4c458b976b583cda61aa8fa2827ba2cc
ffa24cb3547347a9b442d80155b6f6f2
dfa98877f293a851421e2f2ef1553636

Tabla 6.- MD5 - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Hashes SHA-1
371A5B8BA86FBCAB80D4E0087D2AA0D8FFDCC70B

Hashes SHA-1
D43F49E6A58685B85422EDC647075FFD405D6741
F77DBA76010A9889C9EBE8420C96AEBC071B889
67068686005F6591FBFD303B7499C725F8466CF4
1F250E626E89A4F1792C3EAC6462694410F01C1A
C94A6BD6CE83354E831B208FED2A6FEAED6666
D13D2F88EDCEAB2934A0085E1B3034BF85BF83
AE687EF963C80A3788EC14064F5C441FFBA
AB790B81026E2D2B7384A354A5D0D512E
1AEA26A2E7A711F89D061E567E611E92F6FD68

Tabla 7.- SHA-1 - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

Hashes SHA-256
2a8fafa01f6d3863c87f20905736ebab28d6a5753ab708760c0b6cf3970828c3
107f3d1fe28b67397d21a6acca5b6b35def1aeb62a67bc10109bd73d567f9806
ec0be8f18315a2ee781de4855d63c8a087a1564557c42c66076f65c267120c894
8082956acb8016ae8ce16e4a777fe347c7f80fa857a6f9359fd636a30204e7
0517d413bebe2142e7737dcc1983b226d6593d1f4a681a7e79a8b4d8624cdf50

Tabla 8.- SHA-256 - CVE-2025-8088 - Explotación Activa de la Vulnerabilidad en WinRAR

VII. RECOMENDACIONES:

- Actualizar WinRAR a la versión 7.13 o superior.
- Si utilizas herramientas que dependen de UnRAR.dll o su código fuente portátil, asegúrate de actualizar estos componentes para corregir la vulnerabilidad.
- Configura WinRAR para que extraiga archivos únicamente en directorios seguros y controlados por el usuario, evitando ubicaciones sensibles como las carpetas de inicio automático de Windows.
- Educa a los usuarios sobre los riesgos de abrir archivos adjuntos de fuentes no confiables y fomenta la verificación de la legitimidad de los remitentes antes de interactuar con archivos comprimidos.
- Implementa sistemas de detección para identificar la presencia de archivos sospechosos, como accesos directos (.lnk) en carpetas de inicio, o DLLs desconocidas en directorios temporales. Además, supervisa las conexiones de red salientes hacia dominios no reconocidos
- Utiliza herramientas de protección avanzada contra amenazas y sistemas de análisis de archivos para detectar y bloquear actividades maliciosas relacionadas con esta vulnerabilidad

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CSIRT TELCONET (2025). WinRAR: Vulnerabilidad Zero-Day explotada en campañas de phishing. https://csirt.telconet.net/comunicacion/noticias-seguridad/winrar-vulnerabilidad-zero-day-explotada-en-campanas-de-phishing/

SEGU-INFO (2025). Vulnerabilidad Zero-Day en WinRAR se encuentra siendo explotada. https://blog.segu-info.com.ar/2025/08/vulnerabilidad-zero-day-en-winrar-se.html

SOC PRIME (2025). Detect CVE-2025-8088 Exploitation for RomCom Delivery. https://socprime.com/es/blog/detect-cve-2025-8088-exploitation-for-romcom-delivery/

SOCRADAR (2025). CVE-2025-8088: WinRAR Zero-Day Exploited in Targeted Attacks. https://socradar.io/cve-2025-8088-winrar-zero-day-exploited-targeted/

HISPASEC UNA AL DÍA (2025). WinRAR corrige un 0-day explotado: actualiza a 7.13 cuanto antes. https://unaaldia.hispasec.com/2025/08/winrar-corrige-un-0-day-explotado-actualiza-a-7-13-cuanto-antes.html

CVE DETAILS (2025). CVE-2025-8088 Detail. https://www.cvedetails.com/cve/CVE-2025-8088/

BLEEPINGCOMPUTER (2025). Details emerge on WinRAR zero-day attacks that infected PCs with malware. https://www.bleepingcomputer.com/news/security/details-emerge-on-winrar-zero-day-attacks-that-infected-pcs-with-malware/

ESET WELIVESECURITY (2025). Vulnerabilidad zero-day en WinRAR fue explotada activamente. https://www.welivesecurity.com/es/investigaciones/vulnerabilidad-zero-day-winrar-explotada-activamente/