WinRAR 0-day exploatat în campanii de phishing (CVE-2025-8088)

Introducere	Vulnerabilitatea ***CVE-2025-8088***, o problemă de tip directory traversal în WinRAR, a fost exploatată ca zero-day de grupul rusesc RomCom (Storm-0978) pentru a distribui malware prin campanii de phishing. Aceasta permite atacatorilor să scrie fișiere arbitrare în locații sistem sensibile (e.g., dosarele de autopornire Windows), ducând la execuția de cod la distanță (RCE). A fost remediată în WinRAR 7.13, lansat pe 30 iulie 2025
Identificatori	
CVE Scor	8.4 (RIDICAT)
Produs afectat	WinRAR (Windows) – inclusiv componentele Windows RAR/UnRAR, UnRAR.dll și sursele portable UnRAR pentru Windows. Versiunile ≤ 7.12 sunt vulnerabile.
Versiune remediată	WinRAR 7.13
Analiza Vulnerabilității	
Mecanism Tehnic	• Tip: Directory traversal cu utilizarea *Alternate Data Streams (ADS)* pentru ascunderea fișierelor malitioase. • Condiții de Exploatare: ✓ Versiuni afectate: ***WinRAR ≤ 7.12***, UnRAR.dll, codul sursă portabil UnRAR. ✓ Sistemul operativ: Doar Windows (versiunile Unix/Android sunt neafectate). • Fluxul Atacului: ✓ Atacatorul creează o arhivă RAR malitioasă cu căi relative (e.g., *../../malware.exe*). ✓ La extragere, WinRAR suprascrie căile definite de utilizator cu cele malitioase din arhivă. ✓ Fișierele sunt plasate în *%AppData%\Microsoft\Windows\Start Menu\Programs\Startup* (pentru execuție automată la logare)
PoC	Structura arhivei malitioase: „evil_archive.rar ├── legit_document.pdf # Document legit pentru mascare └── ..\..\Windows\Tasks\malware.exe # Cale relativă către locație sistem” Un PoC public este disponibil pe GitHub, dar link-urile active sunt rare pentru a limita abuzul.
Indicatori & artefacte utile în investigație	• Evenimente de fișiere: creare/modificare fișiere executabile/script în folderele Startup imediat după rularea *WinRAR.exe*. • Jurnale EDR/Defender: proces-chain „*WinRAR.exe* → scrieri în căi neașteptate (în afara folderului de extracție selectat) → nou proces la logon”. • Politici E-mail: atașamente *.rar* provenite din afara organizației ce conțin fișiere executabile sau căi relative neobișnuite. (Derivat din mecanismul tehnic al vulnerabilității.) • Nu au fost publicate în sursele citate IOC-uri concrete (hash-uri/C2) pentru această rundă de atacuri; actualizați acest raport dacă ESET publică detalii suplimentare.

WinRAR 0-day exploatat în campanii de phishing (CVE-2025-8088)

<table>
<tr><td rowspan="4">IoCs</td><td>Tip</td><td>Valoare</td><td>Descriere</td></tr>
<tr><td>Fișier RAR</td><td>cv_submission.rar, Eli_Rosenfeld_CV2 – Copy (10).rar</td><td>Arhive malitioase în campaniile RomCom</td></tr>
<tr><td>URL-uri</td><td>hXXps://fex[.]net/s/bttyrz4</td><td>Hostare documente false (FROZENBARENTS)</td></tr>
<tr><td>C2 Domenii</td><td>http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611</td><td>Server C2 pentru IRONJAW (APT28)</td></tr>
<tr><td>Campanii de Atac și Actorii Amenințării</td><td colspan="3">• Grupul RomCom (Storm-0978)
❖ Afiliere: Aliniat cu Rusia, legat de grupări ransomware (Cuba, Industrial Spy) 13.
❖ Tactici:
✓ Phishing: Email-uri cu arhive RAR mimetizate ca CV-uri (e.g., Eli_Rosenfeld_CV2 – Copy (10).rar) 9.
✓ Zero-Day Exploatat: A 3-a vulnerabilitate zero-day utilizată de RomCom în 2 ani (după CVE-2023-36884 și CVE-2024-9680) 9.
❖ Ținte: Guverne, infrastructură critică, sectoare financiare 8.
• Alți Actori
❖ APT28 (FROZENLAKE): Exploatează CVE-2023-38831 pentru a fura date din browsere prin scriptul IRONJAW 7.
❖ APT40 (ISLANDDREAMS): Atacuri împotriva Papuei-Noua Guinee cu backdoor-ul BOXRAT</td></tr>
<tr><td rowspan="4">Sectoare Țintă</td><td>Sector</td><td>Regiune</td><td>Tactici</td></tr>
<tr><td>Financiar</td><td>Europa, Canada</td><td>Spear-phishing cu CV-uri</td></tr>
<tr><td>Apărare</td><td>Global</td><td>Arhive cu teme militare</td></tr>
<tr><td>Energie</td><td>Ucraina</td><td>Invitații false la școli</td></tr>
<tr><td>Referință</td><td colspan="3">https://www.uptycs.com/blog/threat-research-report-team/cve-2023-38831-winrar-zero-day
https://securityaffairs.com/180967/hacking/phishing-attacks-exploit-winrar-flaw-cve-2025-8088-to-install-romcom.html
https://www.bleepingcomputer.com/news/security/winrar-zero-day-flaw-exploited-by-romcom-hackers-in-phishing-attacks/
https://www.opswat.com/blog/decoding-the-winrar-cve-2023-38831-vulnerability-with-opswat
https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/
https://cybersecuritynews.com/winrar-0-day-in-phishing-attacks/</td></tr>
</table>