Attacco WinRAR: come difendersi dalla falla zero-day

Maria Cattini | 15/09/2025 | Sicurezza digitale

Un semplice file RAR può diventare l'innesco di un attacco informatico devastante. È quanto emerso a luglio 2025, quando i ricercatori di **ESET** hanno individuato una vulnerabilità zero-day in WinRAR, il software di compressione installato su milioni di computer in tutto il mondo.
La falla, catalogata come **CVE-2025-8088**, permette agli aggressori di inserire **file eseguibili nascosti** all'interno di archivi apparentemente innocui. Una volta estratti, questi file vengono avviati al login o insieme ad applicazioni legittime come Microsoft Edge.

Come ha commentato l'ethical hacker Sandro Sana: *"WinRAR non è un pezzo di antiquariato digitale, è una bomba rimasta in casa per decenni."*

Attacco WinRAR: cosa è successo

Il gruppo di hacker **RomCom** (noto anche come **Storm-0978** e **Tropical Scorpius**), già protagonista di altri attacchi zero-day a Firefox e Microsoft Office, ha sfruttato la vulnerabilità path traversal di WinRAR per diffondere diversi payload malevoli.

• Data scoperta: 18 luglio 2025
• Segnalazione a WinRAR: immediata da parte di ESET
• Patch rilasciata: 30 luglio 2025 con la versione 7.13

La tecnica utilizzata si basa su **Alternate Data Stream (ADS)**: canali nascosti del file system NTFS che hanno permesso di occultare DLL e collegamenti Windows dentro archivi RAR.

Il trucco più insidioso? Inserire voci ADS collegate a percorsi fittizi. In questo modo l'utente riceve avvisi di errore apparentemente innocui, mentre in realtà si nascondono file eseguibili destinati a cartelle critiche del sistema.

Perché questa vulnerabilità è pericolosa

• Facilità d'attivazione: basta aprire l'archivio con WinRAR.
• Esecuzione automatica: i file vengono lanciati senza intervento dell'utente.
• Difficile da rilevare: gli avvisi mostrati sembrano normali notifiche di sistema.
• Distribuzione globale: WinRAR è ancora largamente usato in aziende e PC personali.

In altre parole, chi non aggiorna il software rischia di diventare **complice involontario** di una catena di infezioni malware.

Come proteggersi dall'attacco WinRAR

1. Aggiornare subito WinRAR

La patch che corregge CVE-2025-8088 è inclusa nella **versione 7.13**. Scaricarla direttamente dal

sito ufficiale di WinRAR è l'unico modo sicuro per eliminare la vulnerabilità.

2. Diffidare dagli archivi sospetti

Gli hacker spesso diffondono i file RAR malevoli via email di phishing o link ingannevoli. Evitare di aprire allegati provenienti da fonti non verificate resta la prima linea di difesa.

3. Monitorare i processi in avvio

Strumenti di sicurezza avanzati (come EDR o antivirus con funzioni di **behavior analysis**) possono segnalare comportamenti anomali legati a DLL o LNK estratti in cartelle sensibili.

4. Controllare gli aggiornamenti regolarmente

Non aspettare l'allarme mediatico: applicare aggiornamenti periodici a software e sistemi riduce il rischio di diventare vittima di exploit zero-day.

Cosa insegna il caso WinRAR

La vicenda evidenzia due aspetti chiave:

1. Le vulnerabilità non conoscono età. Anche software storici, ritenuti "sicuri perché consolidati", possono nascondere falle gravi.
2. L'anello debole è l'utente. Come ricorda Sandro Sana: "Il bug si corregge, l'incapacità di aggiornare no. E a quel punto non sei una vittima, sei il complice della tua stessa disfatta."

L'attacco a WinRAR dimostra come un programma usato quotidianamente da milioni di persone possa trasformarsi improvvisamente in una porta d'ingresso per i cyber criminali. Aggiornare alla **versione 7.13** non è una raccomandazione: è una necessità immediata.

□□ Se non l'hai ancora fatto, scarica l'aggiornamento dal sito ufficiale e verifica la tua sicurezza. Meglio perdere cinque minuti oggi che rischiare di compromettere l'intero sistema domani.

Un semplice file RAR può diventare l'innesco di un attacco informatico devastante. È quanto emerso a luglio 2025, quando i ricercatori di **ESET** hanno individuato una vulnerabilità zero-day in WinRAR, il software di compressione installato su milioni di computer in tutto il mondo.
La falla, catalogata come **CVE-2025-8088**, permette agli aggressori di inserire **file eseguibili nascosti** all'interno di archivi apparentemente innocui. Una volta estratti, questi file vengono avviati al login o insieme ad applicazioni legittime come Microsoft Edge.

Come ha commentato l'ethical hacker Sandro Sana: *"WinRAR non è un pezzo di antiquariato digitale, è una bomba rimasta in casa per decenni."*

Attacco WinRAR: cosa è successo

Il gruppo di hacker **RomCom** (noto anche come **Storm-0978** e **Tropical Scorpius**), già protagonista di altri attacchi zero-day a Firefox e Microsoft Office, ha sfruttato la vulnerabilità path traversal di WinRAR per diffondere diversi payload malevoli.

- Data scoperta: 18 luglio 2025
- Segnalazione a WinRAR: immediata da parte di ESET
- Patch rilasciata: 30 luglio 2025 con la versione 7.13

La tecnica utilizzata si basa su **Alternate Data Stream (ADS)**: canali nascosti del file system NTFS che hanno permesso di occultare DLL e collegamenti Windows dentro archivi RAR.

Il trucco più insidioso? Inserire voci ADS collegate a percorsi fittizi. In questo modo l'utente riceve avvisi di errore apparentemente innocui, mentre in realtà si nascondono file eseguibili destinati a cartelle critiche del sistema.

Perché questa vulnerabilità è pericolosa

• Facilità d'attivazione: basta aprire l'archivio con WinRAR.
• Esecuzione automatica: i file vengono lanciati senza intervento dell'utente.
• Difficile da rilevare: gli avvisi mostrati sembrano normali notifiche di sistema.
• Distribuzione globale: WinRAR è ancora largamente usato in aziende e PC personali.

In altre parole, chi non aggiorna il software rischia di diventare **complice involontario** di una catena di infezioni malware.

Come proteggersi dall'attacco WinRAR

1. Aggiornare subito WinRAR

La patch che corregge CVE-2025-8088 è inclusa nella **versione 7.13**. Scaricarla direttamente dal sito ufficiale di WinRAR è l'unico modo sicuro per eliminare la vulnerabilità.

2. Diffidare dagli archivi sospetti

Gli hacker spesso diffondono i file RAR malevoli via email di phishing o link ingannevoli. Evitare di aprire allegati provenienti da fonti non verificate resta la prima linea di difesa.

3. Monitorare i processi in avvio

Strumenti di sicurezza avanzati (come EDR o antivirus con funzioni di **behavior analysis**) possono segnalare comportamenti anomali legati a DLL o LNK estratti in cartelle sensibili.

4. Controllare gli aggiornamenti regolarmente

Non aspettare l'allarme mediatico: applicare aggiornamenti periodici a software e sistemi riduce il rischio di diventare vittima di exploit zero-day.

Cosa insegna il caso WinRAR

La vicenda evidenzia due aspetti chiave:

1. Le vulnerabilità non conoscono età. Anche software storici, ritenuti "sicuri perché consolidati", possono nascondere falle gravi.
2. L'anello debole è l'utente. Come ricorda Sandro Sana: "Il bug si corregge, l'incapacità di aggiornare no. E a quel punto non sei una vittima, sei il complice della tua stessa disfatta."

L'attacco a WinRAR dimostra come un programma usato quotidianamente da milioni di persone possa trasformarsi improvvisamente in una porta d'ingresso per i cyber criminali. Aggiornare alla **versione 7.13** non è una raccomandazione: è una necessità immediata.

□□ Se non l'hai ancora fatto, scarica l'aggiornamento dal sito ufficiale e verifica la tua sicurezza. Meglio perdere cinque minuti oggi che rischiare di compromettere l'intero sistema domani.