Novo WinRAR Zero-Day Explorado por Hackers RomCom - Against Invade

Data: 2025-08-12 08:21:25

Autor: Inteligência Against Invaders

Uma vulnerabilidade recém-descoberta no WinRAR foi explorada pela Rússia Romcom.

De acordo com um comunicado publicado por pesquisadores da ESET hoje, a falha, rastreada como CVE-2025-8088, permite que os invasores ocultem arquivos maliciosos em um arquivo que são implantados silenciosamente durante a extração.

Um patch foi lançado em 302025 de julho e os usuários são incentivados a atualizar imediatamente.

Como funciona o ataque

A vulnerabilidade de travessia de caminho, habilitada por meio de fluxos de dados alternativos, afeta vários componentes, incluindo os utilitários de linha de comando do Windows do WinRAR, UnRAR.dll e o código-fonte UnRAR portátil.

Ao criar arquivos para parecerem inofensivos, os invasores ocultam DLLs maliciosas e arquivos LNK que são implantados nos diretórios do sistema, permitindo a persistência e a execução do código.

Entre 18 e 21 de julho, a RomCom usou e-mails de spear-phishing para atingir empresas financeiras, de manufatura, defesa e logística na Europa e no Canadá. Os e-mails carregavam iscas de solicitação de emprego com anexos de arquivos RAR.

De acordo com a ESET, nenhum compromisso bem-sucedido foi observado durante esta campanha.

Leia mais sobre táticas avançadas de ameaças persistentes: Grupos APT russos intensificam ataques na Europa com explorações de dia zero e limpadores

Os pesquisadores de segurança identificaram três cadeias de ataque distintas:

- Agente mítico: Usou o sequestro de COM para executar uma DLL maliciosa, que então descriptografou e executou o código shell vinculado a um servidor de comando e controle (C2)
- Variante do SnipBot: Entregue por meio de um executável PuTTY CAC modificado que só era executado se o sistema mostrasse sinais de uso no mundo real, como um grande

número de documentos abertos recentemente

- MeltingClaw (RustyClaw): Um downloader escrito em Rust que recuperou cargas adicionais de servidores remotos

Cada cadeia aproveitou verificações de domínio codificadas ou técnicas anti-análise para evitar a detecção em ambientes de teste.

Um padrão de explorações de dia zero

RomCom, também conhecido como Storm-0978, Tropical Scorpiusor UNC2596, tem um histórico de exploração de vulnerabilidades anteriormente desconhecidas.

Em junho de 2023, abusou do CVE-2023-36884 no Microsoft Word e, em outubro de 2024, encadeou duas vulnerabilidades, incluindo CVE-2024-9680 no Firefox, para fornecer backdoors. O grupo se envolve em ataques com motivação financeira e espionagem direcionada.

A ESET observou que outro agente de ameaça não identificado começou a explorar o CVE-2025-8088 logo após o RomCom. A velocidade do lançamento do patch da equipe WinRAR, apenas um dia após ser informada, foi destacada como crítica na redução da exposição.

Os especialistas em segurança recomendam atualizações imediatas do WinRAR e componentes relacionados para mitigar o risco dessa falha.