Ataques de phishing exploram a falha do WinRAR CVE-2025-8088 para ins

Data: 2025-08-09 08:07:47

Autor: Inteligência Against Invaders

Ataques de phishing exploram a falha do WinRAR CVE-2025-8088 para instalar o RomCom

A falha CVE-2025-8088 do WinRAR, corrigida na v7.13, foi explorada como um dia zero em ataques de phishing para instalar o malware RomCom.

A falha do WinRAR CVE-2025-8088, um bug de travessia de diretório corrigido na versão 7.13, foi explorado como um dia zero em ataques de phishing para entregar malware RomCom, Bleeping Computer Relatado pela primeira vez.

A falha é uma vulnerabilidade de travessia de caminho que afeta a versão Windows do WinRAR. Os invasores podem explorar a vulnerabilidade para executar código arbitrário criando arquivos maliciosos. Os pesquisadores Anton Cherepanov, Peter Košinár e Peter Strý?ek, da ESET, divulgaram a falha.

Os invasores podem criar arquivos que colocam executáveis nas pastas de inicialização do Windows, fazendo com que sejam executados no login e permitindo a execução remota de código

Os pesquisadores da ESET disseram ao Bleeping Computer que os agentes de ameaças exploraram ativamente a vulnerabilidade em ataques de spear-phishing para entregar Backdoors RomCom.

“A ESET observou e-mails de spearphishing com anexos contendo arquivos RAR”, disse Strý?ek ao BleepingComputer.

Esses arquivos exploraram o CVE-2025-8088 para fornecer backdoors RomCom. O agente de ameaças por trás do RomCom (também conhecido comoUAT-5647,Tempestade-0978,Escorpião tropical, UAC-0180,UNC2596) é suspeito de ser um grupo de ciberespionagem ligado à Rússia.

A RomCom já realizou ataques de extorsão de ransomware e roubo de dados. No final de 2024, Romcom Explorado duas vulnerabilidades de dia zero do Firefox e do navegador Tor em ataques a usuários na Europa e na América do Norte.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,RomCom)