Novel obfuscation leveraged by Hive ransomware

By SC Staff

Published: 2022-03-31 · Archived: 2026-04-05 17:41:45 UTC

Ransomware, Threat Management, Risk Assessments/Management, Breach

The Hive ransomware gang has been leveraging a novel obfuscation approach involving IPv4 addresses and numerous conversions resulting in Cobalt Strike beacon downloads, BleepingComputer reports. The new technique dubbed "IPfuscation" was identified by Sentinel Labs researchers who examined various 64-bit Windows executables, all of which had Cobalt Strike-delivering payloads. Hive has obfuscated the payload by impersonating ASCII IPv4 addresses but converting the file from string to binary prompts the appearance of shellcode. Researchers found that upon completion, the shellcode will be executed by the malware through direct SYSCALLs or proxy execution. More IPfuscation variants have been observed by researchers, with IPv6, MAC, and UUID addresses also being leveraged by the ransomware group. The findings suggest that static signature dependence alone is inadequate in detecting malicious payloads. Organizations should also deploy behavioral detection, artificial intelligence-based analysis, and holistic security approaches for their endpoints to better detect IPfuscation techniques, according to researchers.

Get essential knowledge and practical strategies to protect your organization from ransomware attacks.

Related

Brokk purportedly hacked by Play ransomware, data leaked

SC StaffApril 3, 2026

Brokk, a leading Swedish global remote-controlled demolition machinery manufacturer, had a 4 GB dataset allegedly stolen from its systems exposed by the Russia-linked Play ransomware operation, which threatened to leak all pilfered data should it refuse to fulfill the demanded ransom, reports Cybernews.