Novel obfuscation leveraged by Hive ransomware

scmagazine.com/brief/breach/novel-obfuscation-leveraged-by-hive-ransomware

March 31, 2022

SC StaffMarch 31, 2022

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.

SC Staff

Related

Ransomware

GoodWill ransomware stipulates acts of kindness

SC StaffMay 27, 2022

Organizations impacted by the GoodWill ransomware gang are being ordered by attackers to carry out good deeds before being able to download a tool for file decryption.

Ransomware

Industrial Spy ventures into ransomware

SC StaffMay 27, 2022

Newly-discovered data extortion marketplace Industrial Spy has entered the ransomware game, with MalwareHunterTeam discovering a new Industrial Spy malware sample containing a ransom note.

Ransomware

VMware ESXi servers under attack from novel Cheers ransomware

SC StaffMay 26, 2022

Vulnerable VMware ESXi servers are being impacted by the new Cheers, or Cheerscrypt, ransomware strain.