Conti and Hive ransomware operations: What we learned from these groups' victim chats

By Cisco Talos

Published: 2022-05-03 · Archived: 2026-04-05 14:12:18 UTC

Tuesday, May 3, 2022 08:00

As part of Cisco Talos’ continuous efforts to learn more about the current ransomware landscape, we recently examined a trove of chat logs between the Conti and Hive ransomware gangs and their victims.

Ransomware-as-a-service groups have exploded in popularity over the past few years, with these groups continually adding new affiliates and tools. In the past, we’ve learned more about these groups by speaking directly with operators and examining these groups’ changing tactics, techniques and procedures (TTPs).

Talos researchers recently spent weeks combing through chat logs and other information we obtained from Hive and Conti operators' conversations with victims. These conversations had not previously been made public. The research paper we’re releasing today contains new insights into how Conti and Hive choose their targets, negotiate with victims, operate internally, and much more.
