Key insights of the report

Ransomware extortion tactics have been evolving. **Quadruple extortion is the newest tactic**, while double extortion is currently the most common tactic. And ransomware groups continue to seek additional ways to generate profit, such as by pressuring victims and weaponizing compliance.

More than US$724 million in cryptocurrency was extorted from strains linked to the TrickBot malware family, which is used by ransomware groups. The Akamai Hunt Team recently observed this malware in connection with four malicious scheduled tasks on five customer assets.

GenAI and LLMs increase the frequency and scale of ransomware attacks by enabling individuals with less technical expertise to launch sophisticated campaigns, as demonstrated by groups like FunkSec.

The emergence of hybrid ransomware hacktivist groups that are leveraging RaaS platforms to amplify impact (e.g., CyberVolk, Stormous, KillSec, Dragon RaaS, and DragonForce) demonstrates a significant shift in the ransomware landscape in which **political and ideological motives are becoming more intertwined with financial crime**.

The hacktivist groups Head Mare, Twelve, and NullBulge often use LockBit ransomware (built from leaked or publicly available builders) for political disruption. NullBulge specifically uses it to **target online communities and platforms that are operating with AI and online gaming tools**.

Although cryptominers pose a unique danger, their goals and the strategies they employ are similar to those of ransomware groups. Notably, nearly **50% of the cryptomining attacks we analyzed targeted nonprofit and educational organizations**, likely because they possess substantial computational resources and are less secure than other industries.