CROWDSTRIKE

2025 GLOBAL THREAT REPORT

One of the most trusted analyses of the modern cybersecurity threat landscape, the CrowdStrike 2025 Global Threat Report delivers unparalleled insights into the critical events and trends that defined 2024 and the adversaries behind them.

There were 26 newly named adversaries in 2024, raising the total to 257 actively tracked by CrowdStrike.

Download the Full Report

Today's adversaries are operating with unprecedented speed and adaptability

00:51

51 seconds was the fastest recorded eCrime breakout time, and the average eCrime breakout time was **48 minutes**

79% of detections were malware-free, as adversaries adopted hands-on-keyboard and other stealth tactics to evade detection

Social engineering tactics aim to steal credentials

442% explosive growth in vishing operations between the first and second half of 2024

Generative AI drives new adversary risks

304 FAMOUS CHOLLIMA incidents CrowdStrike responded to in 2024 — 40% involved insider threats, and some used genAI to generate fake resumes and LinkedIn profiles

China expanded its cyber espionage enterprise

150% increase in China-nexus activity across all sectors, with a **200-300%** surge in key industries including financial services, media, and manufacturing

Cloud-conscious actors continue to innovate

26% increase in cloud intrusions in 2024 — **35%** of cloud incidents in the first half of 2024 achieved initial access through valid account abuse

Stolen credentials are increasingly being used

****

50% increase in access broker advertisements year-over-year

Adversaries are exploiting vulnerabilities to gain access

52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access, highlighting the urgent need to secure entry points by patching vulnerable systems