

Sector Under Attack: Technology

eCrime, state-sponsored intrusions, and supply chain compromise remain key threats to the technology sector.



149 out of 280+
adversaries currently tracked by
CrowdStrike target the technology sector¹

Attack Trends in Technology

#1

Most targeted sector for the past several years, with 26% more interactive intrusions than the next most targeted sector in Q1 2026²

↑30%

Increase in initial access broker advertisements for technology entities from April 1, 2025, to March 31, 2026, compared to the previous year²

572

Technology entities named on dedicated leak sites from April 2025 to March 2026²

How Adversaries Achieve Their Objectives



Exploit legitimate credentials and engage in social engineering to gain access without raising alarms



Abuse trusted workflows across developer environments, cloud services, and SaaS applications



Attack across domains to maintain persistence, move laterally, and exfiltrate data

Key Adversaries Targeting Technology Institutions



STARDUST CHOLLIMA

STARDUST CHOLLIMA targets technology entities by exploiting trust in software development workflows. Their tactics include social engineering, malicious dependencies, and compromised packages, enabling credential and financial data theft, cryptocurrency theft, and downstream risk across the software supply chain.



SNARKY SPIDER

Active since 2025, SNARKY SPIDER conducts rapid data theft operations using social engineering and compromised credentials. The adversary targets integrated business applications to exfiltrate customer data and then likely outsources extortion to collaborating threat actors.



MURKY PANDA

Identified in 2023, MURKY PANDA targets technology entities through cloud-focused credential attacks. In mid-2025, CrowdStrike observed the threat actor using anonymized infrastructure to conduct password spraying attacks against Microsoft Azure environments. This activity impacted more than 340 primarily U.S.-based entities across sectors, with technology among the most affected.

Questions for Defenders

- Do you know which adversaries are targeting your environment?
- Are you ready to stop social engineering, credential abuse, and supply chain attacks in their tracks?
- Are all of your user credentials, cloud assets, and endpoints protected?

¹ Adversaries tracked by CrowdStrike Counter Adversary Operations as of 06/03/2026
² CrowdStrike 2026 Technology Threat Landscape Report