



Sector Under Attack: Telecommunications

Big game hunting (BGH), targeted intrusions, and hacktivism remain key threats to the telecommunications sector.



108 out of 255+
adversaries currently tracked by
CrowdStrike target telecommunications¹

Attack Advancements in Telecommunications



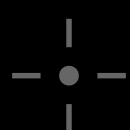
↑ 128%

increase in data leakage
exfiltration activity²



↑ 52%

increase in targeted
intrusion activity year-
over-year⁴



↑ 58%

increase in eCrime
BGH activity³

How Adversaries Achieve Their Objectives

Exploit legitimate credentials to gain access and
extend presence without raising alarms



Adapt sophisticated hands-on-keyboard attacks
to evade detection



Focus on cross-domain tradecraft to maintain
persistence, move laterally, and exfiltrate data

Key Adversaries Targeting Telecommunications Institutions



LIMINAL PANDA ↗

Since at least 2020, LIMINAL PANDA has targeted telecommunications entities, using custom tools that enable covert access, command and control, and data exfiltration.



OPERATOR PANDA ↗

Since at least November 2024, OPERATOR PANDA has conducted operations against the telecom and professional services sectors. OPERATOR PANDA relies heavily on exploiting internet-facing appliances for initial access.



SCATTERED SPIDER ↗

This adversary targets telecoms by leveraging sophisticated social engineering techniques to capture user credentials. The adversary often targets accounts belonging to IT personnel to gain access to tools that assist with lateral movement and account compromise.

Questions for Defenders

- Do you know who is targeting you?
- Are you prepared for the latest adversarial tactics and techniques?
- Are all of your user credentials, cloud assets, and endpoint assets protected?

Visit the [Adversary Universe](#) or download the [CrowdStrike 2025 Global Threat Report](#)

1. Adversaries tracked by CrowdStrike Counter Adversary Operations as of 03/06/2025
2. CrowdStrike Counter Adversary Operations 2024 trend data

3. CrowdStrike Counter Adversary Operations 2024 trend data
4. CrowdStrike 2024 Threat Hunting Report