

Sector Under Attack: Retail

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



79 out of 281+

adversaries currently tracked by CrowdStrike target retail¹

Attack Advancements in Retail



Fourth most

targeted industry by interactive intrusions in 2024²

↑ 55%

increase in interactive intrusions year-over-year⁴



↑ 313%

year-over-year increase in access broker advertisements³

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 Retail Institutions



PUNK SPIDER ↗

Identified in April 2023, this adversary is behind Akira ransomware and a leak site, using repurposed software and open-source tools for attacks. The group exfiltrates data and encrypts files to extort victims.



RECESS SPIDER ↗

This BGH adversary operates PLAY ransomware and the GRB_NET tool for evasion. The group initially exploited WordPress vulnerabilities but now uses a novel method, OWASSRF, for remote code execution.



SCATTERED SPIDER ↗

This adversary targets retail 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 Hub](#) or download the [CrowdStrike 2026 Global Threat Report](#)

1. Adversaries tracked by CrowdStrike Counter Adversary Operations as of 3/06/2025
2. CrowdStrike 2025 Global Threat Report

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