Threat Actors Target the Entire Retail Supply Chain





A report by Black Kite found that threat actors treat wholesalers and retailers as one organization, as their level of connection makes them particularly vulnerable.

“When we think about the supply chain, we often picture logistics and warehouses, but today the real threat is the expanded ecosystem,” said Ferhat Dikbiyik, Chief Research & Intelligence Officer, Black Kite. “The bottom line is that wholesale and retail’s greatest risk is their shared supply chain, and as we have seen time and time again, just one vulnerability in a common vendor can create systemic impact affecting both simultaneously. The era of checklist compliance is over. Third party risk management programs must evolve by securing the weak points across every partner in the ecosystem.”

One of the report’s findings is the widespread presence of compromised credentials, meaning that initial access has already been granted to a majority of the industry. In fact, over 70% of major retailers, nearly 60% of wholesalers, and 52% of the supply chain have exposed credentials.

Additional key findings include:

- 17% of retail ransomware victims had revenue over $1B, demonstrating that threat actors prioritize ”big game hunting” in the retail sector – a specific target for high-value extortion.
- 39% of wholesale ransomware victims had revenue in the mid-market range of $20M–$100M as attackers play a ‘volume game’ on smaller enterprises.

- 42% of critical supply chain vendors are exposed to at least one vulnerability from the CISA Known Exploited Vulnerabilities (KEV) Catalog, listing flaws currently under active attack.
- Two vendor categories — Professional & Technical Services (793) and Information (705) — totaling 1,498 companies — dominate the supply chain, outnumbering physical categories by a significant margin.

Read the report.

https://www.securitymagazine.com/articles/102174-threat-actors-target-the-entire-retail-supply-chain