NTT | Security Holdings

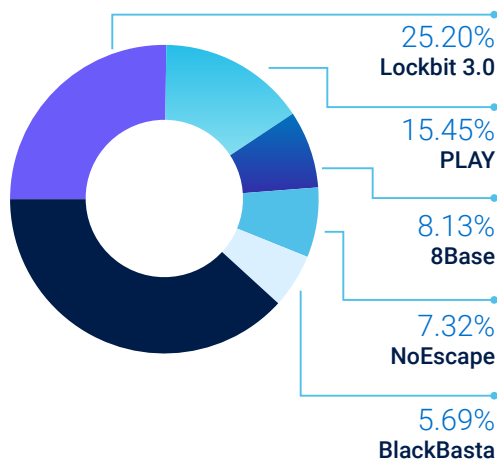# Retail sector

## Notable news & breaches

- Ducktail malware targets the fashion industry
- GambleForce, an SQL injection gang, targets APAC retail and gambling websites
- Magecart campaign targets e-commerce websites due to rogue WordPress plugin
- Several high profile US-based ransomware victims in December — including La Jolla and Kraft Heinz
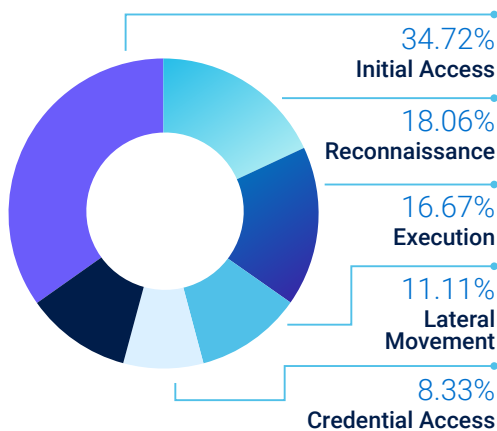
## Noteworthy Malware

### DuckTail

In Q4 2023, Ducktail malware began to target marketing teams in the retail space. Specifically targeting fashion companies, the actors leveraged real products from popular companies to deliver the malware disguised as a PDF.
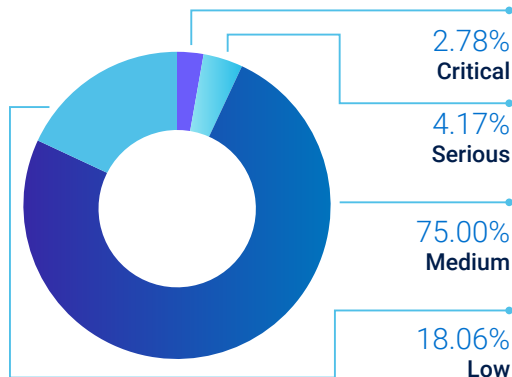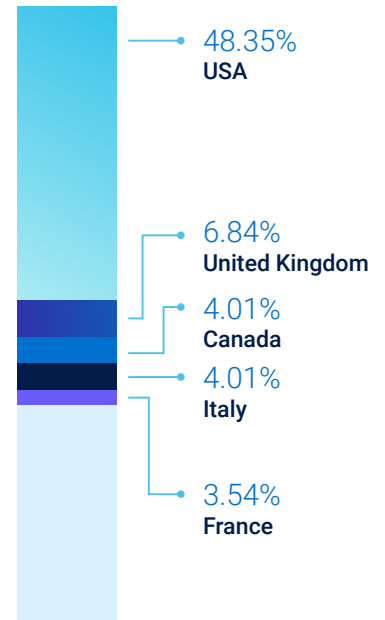
## Top ransomware

25.20%
**Lockbit 3.0**

15.45%
**PLAY**

8.13%
**8Base**

7.32%
**NoEscape**

5.69%
**BlackBasta**

## Incident MITRE tactics

34.72%
**Initial Access**

18.06%
**Reconnaissance**

16.67%
**Execution**

11.11%
**Lateral Movement**

8.33%
**Credential Access**

## Incident severity

2.78%
**Critical**

4.17%
**Serious**

75.00%
**Medium**

18.06%
**Low**

## Ransomware victim locations

48.35%
**USA**

6.84%
**United Kingdom**

4.01%
**Canada**

4.01%
**Italy**

3.54%
**France**

## Monthly victim trending

| Ransomware | Oct | Nov | Dec |
|---|---|---|---|
| **Lockbit 3.0** | 5 | 12 | 14 |
| **PLAY** | 2 | 10 | 7 |
| **8Base** | 3 | 3 | 4 |
| **NoEscape** | 5 | 4 | 0 |
| **BlackBasta** | 1 | 2 | 4 |

## Recommendation

Revisit web application security and integrations. We have seen an increase in web application based attacks targeting retail, especially e-commerce platforms, as the majority of retail attacks are financially motivated.