Quorum Cyber

Threat Intelligence Retail Sector Threat Profile

TLP Status: CLEAR

☎ +44 333 444 0041

quorumcyber.com

Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	08/08/2023	Initial Report Drafted
1.0	09/08/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Retail Sector Threat Profile – 2023

Executive Summary

- Due to the abundance of sensitive data contained within retail sector organisations, it is highly likely that organisations across the sector could emerge as an attractive target for cybercriminals.
- Throughout Q1-Q3 of 2023, the three primary cyber-attack vectors that impacted retail sector organisations were: ransomware, stealware and supply chain attacks.
- The Quorum Cyber Threat Intelligence (TI) team detected numerous cyber-attack campaigns that involved financially motivated targeting of retail sector organisations, which included ransomware campaigns and the mass exploitation of a 3CX vulnerability.
- Quorum Cyber Threat Intelligence malware reports and threat actor profiles have been added to the end of the document to provide contextual details on the entities associated with the targeting of retail sector organisations throughout Q1-Q3 of 2023.

Threat Profile – 2023

Threat Profile Overview

Due to the abundance of confidential data contained within retail businesses, it is highly likely that companies across the sector could emerge as an attractive target for cybercriminals. Cybercriminal networks, including nation-state threat actors, almost certainly view organisations operating within the UK retail sector as a prime target as they seek to exfiltrate sensitive financial data in an attempt to engage in extortion attempts to complete their objectives which almost certainly includes enhancing financial income.

Retail Sector Threat Vectors

Throughout Q1-Q3 of 2023, the Quorum Cyber Threat Intelligence team detected that the three primary attack vectors targeting organisations in the retail sector were:

- Ransomware
- Stealware
- Supply chain attacks.

RANSOMWARE

Throughout Q1-Q3 of 2023 thus far, Ransomware-as-a-Service (RaaS) models continued to be utilised by a significant number of threat groups, thereby enabling those without sufficient tooling or infrastructure to achieve their objectives of data exfiltration and financial extortion against retail sector organisations. Targeting of the retail sector is likely due to the perceived amount of sensitive data pertaining to financial information. There are two main categories of threat actor that almost certainly seek to disrupt the sector. First are organised crime groups such as that aim to leverage stolen information for financial gain, and second, threat actors such as those sponsored by sanctioned nation-states will actively seek to target the UK retail sector in retaliation for the imposed sanctions placed upon the affiliated nations. Ransomware attacks from criminal groups will almost certainly continue to apply campaigns during the remainder of 2023 based on the potential for their objectives to be achieved.

Throughout Q1-Q3 of 2023, Clop, LockBit, ALPHV ransomware variants were detected to be the most prevalent strains targeting the retail sector. Related operations included the widespread MOVEit vulnerability campaign initiated by the Clop ransomware gang operators. Please refer to the ‘Associated Quorum Cyber Reporting’ section at the end of this report for links to Quorum Cyber Threat Intelligence malware reports for the ransomware variants listed above.

During the first half of 2023, RaaS operators continued to expand their attack surface by switching to additional malware payloads and expanded target sets. This has included ransomware operators, such as the LockBit gang, developing ransomware payloads for additional architectures including macOS and Linux. These developments indicate that it is likely that at least some ransomware operators are considering bypassing the typical Windows targets to expand their attack surface and remain relevant within the cyber threat landscape.

As expected, new ransomware variants continue to enter the cyber threat landscape. Relevant to the retail sector is the emergence of the Mallox ransomware strain that has been deployed by threat actors to specially target retail sector organisations.

STEALWARE

Retail sector organisations are likely to be a target for stealware operations used as cover for data exfiltration. Stealware variants have emerged as a notorious malware of choice for threat actors seeking to harvest data from target organisations. Stealware variants all employ similar attack vectors, including credential stealing, keylogging, PowerShell attack and process hollowing. A significant portion of detected credential and domain dark web leaks relating to stealware have come via Russian Market threat actors. This threat actor, along with many others, implements stealware variants for its credential stealing capabilities and resulting financial gain. Stealware can be bought as a service that can be subscribed to for affordable prices. The Quorum Cyber Threat Intelligence team has detected the following three stealware variants that have been deployed by threat actors throughout 2023:

- Raccoon Stealer
- RedLine Stealer
- Vidar Stealer.

Please refer to the 'Associated Quorum Cyber Reporting' section at the end of this report for links to dedicated malware reports for the stealware strains listed above.

SUPPLY CHAIN ATTACKS

As the cyber resilience of organisations continues to strengthen, threat actors have increasingly launched their attacks further along the supply chain, attempting to infiltrate third-party suppliers as an indirect mode of access into their primary target. It is therefore not enough just to consider one's own defences but rather due diligence is required with respect to third-party security measures.

A significant portion of retail sector organisations utilise third parties to provide services, and so should that third party be compromised, this naturally has a knock-on effect on the associated primary organisation. If a supply chain attack compromises an organisation, this can lead to significant damage. Critical services, such as those pertaining to distribution equipment production, will likely be impacted.

Retail Sector – Historical Attack Timeline

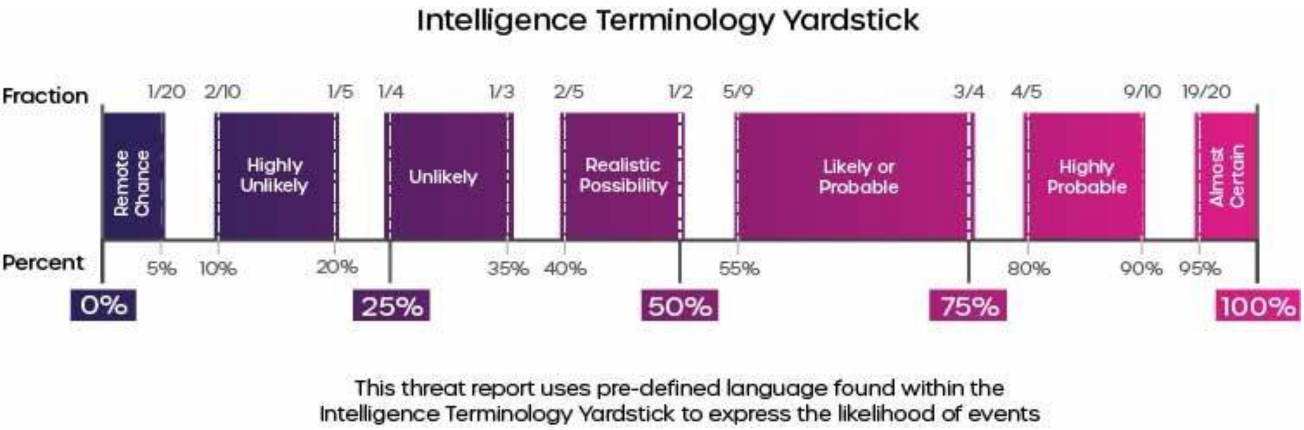
The table below outlines recent examples of cyber targeting in the retail sector:

Date of Attack	Victim	Attack Vector w/ Threat	Assessed Motivation
June 2022 – August 2023	Several retail sector organisations	Mysterious Team Bangladesh (DDoS)	Likely **Geopolitical**
July 2023	Franklins - European Bathrooms	Mallox Ransomware Operation	Likely **Financial**
July 2023	Estee Lauder	ALPHV and Clop Ransomware Operations	Likely **Financial**
May 2023	Pike Nurseries	LockBit 3.0 Ransomware Operation	Likely **Financial**
May 2023	Apple Users	Stealware (Atomic macOS Stealer Campaign)	Likely **Financial**
May 2023	IT Works! Global	ALPHV Ransomware Operation	Likely **Financial**
April 2023	Daregal	ALPHV Ransomware Operation	Likely **Financial**
March 2023	3CX	Supply Chain Attack	Likely **Financial**
February 2023	Fikes Products	LockBit 3.0 Ransomware Operation	Likely **Financial**

Associated Quorum Cyber Reporting

- **RedLine Stealer** - Malware Report[1]
- **Raccoon Stealer** - Malware Report[2]
- **LockBit 3.0 Ransomware** – Malware Report[3]
- **Clop Ransomware** – Malware Report[4]
- **FIN8** - Threat Actor Profile[5]

Intelligence Cut-off Date (ICoD): 09/08/2023 10:00 UTC



[1] RedLine Stealer Stealware - Quorum Cyber

[2] Raccoon Stealer Stealware - Quorum Cyber

[3] LockBit 3.0 Ransomware - Quorum Cyber

[4] Clop Ransomware - Quorum Cyber

[5] FIN8 Threat Actor Profile Overview - Quorum Cyber