DARKTRACE
Evolving threats call for evolved thinking™

Retail Threat Trends Report / 2022

Industry Spotlight

DARKTRACE

CONTENTS

Executive Summary

The global retail sector continues to accelerate its move to greater digitization with commentators attributing the 'death of the high-street' to the trend. In the US alone, e-retail sales exceeded $5.2 trillion in 2021, and early estimates suggest the 2022 figure could be close to $6 trillion.[1] While online shopping continues to grow exponentially, it's not only online retail driving digitization. From warehouse logistics to sales analytics, to mergers and acquisitions, businesses are embracing digitization as a driver of efficiency. But along with all the advantages of greater interconnection, businesses must now grapple with the growing cyber risks associated with their expanded attack surfaces against the backdrop of cyber criminals seeking access to the rich data-stores held by organizations in the retail space.

Retail remains one of the most vulnerable sectors to cyber-attacks. Retail companies are very publicly visible organizations and contain vast amounts of personal and financial information which is easily monetized by criminals. Online shopping demands consumers to create dozens of unique accounts which improves user experience, but individuals often use the same credentials for multiple accounts which means that a data leak from one vendor could put multiple user accounts at risk.

Over the course of 2022, criminals increasingly turned toward credential theft, spoofing and stuffing to target this multi-billion-dollar industry's online infrastructure.

1. Marina Pasquali, E-commerce worldwide Digital & Trends Report 2022, Statista

The Data

This report compares data taken from January – October 2022 and January- October 2021. Darktrace fleet data shows that the global retail sector experienced an increase in credential theft, credential spoofing and credential stuffing.

US retail sector

'Unusual Login and New Email Rule (SaaS)' accounted for over **170% more** of all cyber incidents in the sector in 2022 compared to 2021. [2]

UK retail sector

'Unusual Login and New Email Rule (SaaS)' accounted for almost **14% more** of all cyber incidents in the sector in 2022 compared to 2021. [3]

Australian retail sector

'Unusual Login and New Email Rule (SaaS)' accounted for almost **70% more** of all cyber incidents in the sector in 2022. compared to 2021. [4]

MITRE ATT&CK Category: Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding start-up code.

2. Unusual Login and New Email Rule (SaaS) accounted for 174.04% (or 2.74x) more of all threat indicators seen in the US Retail sector in 2022 compared with 2021.

3. Unusual Login and New Email Rule (SaaS) accounted for 13.77% (or 1.13x) more of all threat indicators seen in the UK Retail sector in 2022 compared with 2021.

4. Unusual Login and New Email Rule (SaaS) accounted for 68.97% (or 1.68x) more of all threat indicators seen in the Australian Retail sector in 2022 compared with 2021.

Darktrace's Expert Analysis

Simply logging on to systems is the new "hack". In many of the high-profile attacks of the last year (notably those perpetrated by Lapsus$), uses of malware or offensive tooling were limited to just a few cases, with attackers now just re-purposing stolen credentials that allow them to simply "log on". This has been greatly enabled by the push for more use of Cloud and SaaS technologies that are accessible from anywhere, instead of the previously isolated on-premises environments that require physical presence. As online-retail becomes the norm, financial information becomes easier to reach for attackers, and hijacked accounts can even be used as money mules for other criminal activity.

The retail sector is evolving to meet this growing threat by investing in state-of-the-art security measures. According to forecasts, global security revenues in retail are headed for strong growth in the next few years, growing from $7 billion in 2019 to reach $12 billion by 2025.

Credential Stuffing

Typically when an organization is breached and usernames and passwords are stolen, that data is sought after by others who use it to perform credential stuffing attacks. Credential stuffing is simply the act of taking a username and password belonging to one service (such as a social media account or email service), and using those same details to try to log in to other websites or services. People tend to re-use passwords to make them easier to remember, but unfortunately this puts them at increased risk if any of the services those passwords belong to are compromised. This is why one of the first pieces of advice typically offered in the wake of an attack where user details are leaked is for those users to immediately change their passwords.

When employees at a retail organization are victimized by hackers, it can set off a domino effect by exposing the user data which is stored on their systems. Leaked user credentials will often lead to further credential stuffing attacks, which in turn lead to more cases of leaked credentials, and so each fuels the other in a vicious cycle.

Wherever possible, it is advisable to enable MFA for user accounts so that a username and password alone will not allow an attacker to access a user's account. Multi-factor authentication is an effective and important part of any mature business' cyber security posture, but the MFA attacks we have seen this year show MFA is no silver bullet.

Persistence attacks and credentials changes in the retail sector allow continual harvesting of data as users input more data into services.

What are attackers looking to achieve?

Online retail environments are fast paced and even outages of short durations can lead to significant costs to these businesses, as well as causing reputational damage with a knock-on effect for consumer trust. Transactional data from these environments is lucrative for attackers as credit card details can be sold for significant profits on the dark web. With a compromized account, criminals can easily purchase items using the linked payment details belonging to that user. Compromized PII data can also be used to commit identity fraud.

A number of different systems and technologies are often used in retail environments, especially when we look at online retail, and this means additional systems to secure and more vulnerabilities to manage across each of these systems. A key element in the online retail experience is trust. Customers trust retailers to protect their data. It's important for retailers to keep customers' trust or they may shop elsewhere.

Threat Story

UK

In August 2022 a well-known UK based automotive retailer was targeted by a never-before-seen attack, called a 'zero-day' in the cyber security industry. In the months before Darktrace had been brought in to defend the automobile retailer, one of their devices had become infected with malware that lay dormant, establishing a foothold and waiting for the right time to launch an attack. In August they did just that, but by then the business had deployed Darktrace's AI technology which caught the malware when it made multiple authentication attempts using spoofed credentials for one of the organization's security managers. If these attempts had not been caught and disabled, they could have undermined the entire security posture of the organization by allowing malicious software to gain control of the company's infrastructure from within.

US

During a trial of Darktrace's Proactive Threat Notification in July 2022, a large US retailer was alerted by Darktrace's AI technology to a sudden threat on their network. An internet-facing server downloaded a malicious executable (viruses, worms and Trojans are all malicious executables) from a rare endpoint. The malicious payload was cleverly disguised behind a legitimate Windows file name, so that any ordinary employee would be inclined to trust it. Despite this, Darktrace DETECT was able to identify the file as anomalous and alerted the security team at the customer organization, who contained the threat. If DETECT had not picked up the initial masquerading behaviour and the customer not been alerted, this could easily have led to lateral movement, an extensive infection, ransomware, or a data leak.

List of Contributors

Toby Lewis, Global Head of Threat Analysis

Hanah Darley, Head of Threat Research

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,100 people around the world and protects over 7,700 organizations globally from advanced cyber-threats.

Scan to LEARN MORE