Industry Spotlight: Retail

DARKTRACE

AT A GLANCE:

- Self-Learning AI technology safeguards transformation projects
- Darktrace RESPOND stops cyber-threats before they do damage
- Cyber AI Analyst automates security investigations

As retailers increase their reliance on digital systems to maximize ease of use and personalization for consumers, threat actors are adapting to exploit the changing cyber landscape. Businesses around the world are turning to Self-Learning AI to discern the first signs of anomalous behavior indicative of cyber-attacks, detecting and disrupting never- before-seen threats that fly under the radar of legacy security tools.

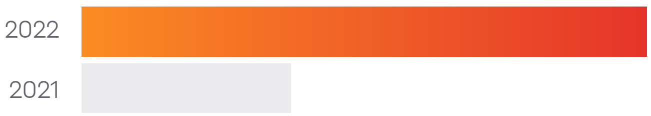
Industry Challenges

As online shopping remains popular, Darktrace's retail sector report reveals that over the course of 2022, criminals increasingly turned toward credential theft, spoofing and stuffing to target this multi-billion-dollar industry's online infrastructure.

Notably:

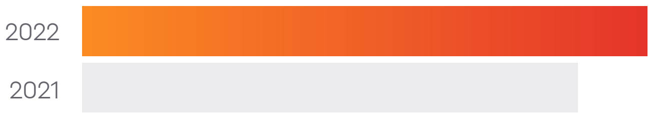
US Retail Sector:

Credential theft, spoofing, and stuffing accounted for over 170% more of all observed cyber incidents in 2022 compared to 2021



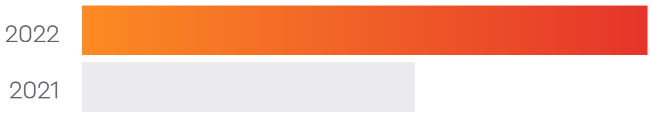
UK Retail Sector:

Credential theft, spoofing, and stuffing accounted for over 14% more of all observed cyber incidents in 2022 compared to 2021



Australian Retail Sector:

Credential theft, spoofing, and stuffing accounted for over 70% more of all observed cyber incidents in 2022 compared to 2021



As commerce continues to thrive online, robust cyber security stacks have become crucial for survival. If a business' website is taken offline as a result of an attack, the losses can be calamitous and even fatal to operations. Over the past year, threats to e-commerce, including online skimming, have steadily increased.

In recent years, the retail industry has increasingly relied on internet-connected devices. The typical retail environment has a device to people ratio of 5:1, meaning that for every 100 employees there are 500 devices that need to be secured.

Such distributed networks complicate cyber security and increase the attack surface available for threat actors.

Cyber-criminals continue to target connected and online Point of Sale (POS) systems because many retailers still do not use end-to-end encryption. For example, memory-scraper malware, which scans for and then exfiltrates bank card data from POS systems, remains a major risk.

Self-Learning AI for Retail and E-Commerce

Leading retailers around the globe have turned to Darktrace to protect their evolving digital ecosystems from sophisticated attacks. Leveraging Self-Learning AI, Darktrace identifies and stops novel and unpredictable threats across the enterprise, from ransomware and POS attacks, to spear phishing campaigns and website hacks.

Darktrace's AI works by continuously learning what 'normal' looks like for every user and device in a business, as well as all the connections between them. This enables the AI to detect the subtlest signals of a threat seconds after it emerges – no matter how sophisticated, novel, or unpredictable. Darktrace RESPOND then contains and neutralizes the threat at machine speed, ensuring business operations continue unimpeded.

To augment and uplift security teams, this capability is complemented by Cyber AI Analyst, a component of Darktrace DETECT and RESPOND, which autonomously investigates, triages, and reports on security incidents. The reports Cyber AI Analyst generates put teams in a position to take action when threats strike, with this process reducing time to triage by up to 92%

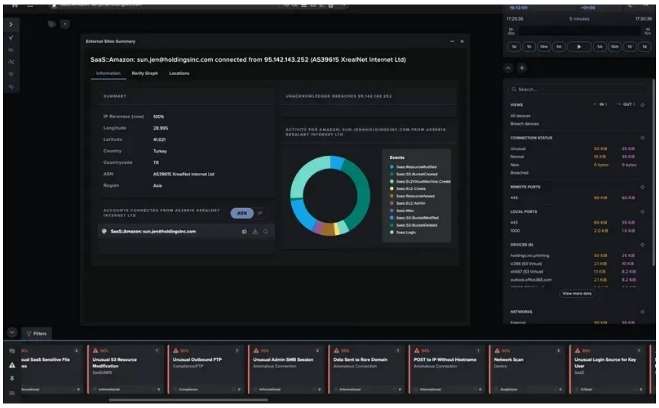
Operative across the entire digital ecosystem, from cloud and SaaS applications to email environments and IoT, Darktrace helps teams defend sensitive client data and financial records wherever they are located.

> Whether a targeted campaign or an accidental compromise, I know that Darktrace's AI will catch in-progress threats, safeguarding our corporate and industrial systems before the horse has bolted.
>
> / IT Manager, Retail

Attack Case Study

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.



External Sites Summary

SaaS::Amazon: sun.jen@holdingsinc.com connected from 95.142.143.252 (AS39615 XrealNet Internet Ltd)

SUMMARY

IP Rareness (now): 100%
Longitude: 28.995
Latitude: 41.021
Country: Turkey
Countrycode: TR
ASN: AS39615 XrealNet Internet Ltd
Region: Asia

ACCOUNTS CONNECTED FROM AS39615 XREALNET INTERNET LTD

SaaS::Amazon: sun.jen@holdingsinc.com

UNACKNOWLEDGED BREACHES 95.142.143.252

ACTIVITY FOR AMAZON: SUN.JEN@HOLDINGSINC.COM FROM AS39615 XREALNET INTERNET LTD

Figure 1: Darktrace analyzes network data in the cloud alongside control plane events.

DARKTRACE

Evolving threats call for evolved thinking™

darktrace.com

info@darktrace.com

Scan to LEARN MORE