Data Sheet | DARKTRACE

Industry Spotlight: Retail

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.

At a Glance

- ✔ Protects hundreds of retail customers globally
- ✔ Self-Learning AI technology which safeguards transformation projects
- ✔ Autonomous Response surgically disrupts cyber-threats before they do damage
- ✔ Cyber AI Analyst automates security investigations

MADE® | chrono24 The World's Watch Market | Kmart
Freddy's Frozen Custard & Steakburgers | LAURA | Zappos.com
photobox | JIMMY CHOO | Berry Gardens
ebay classifieds group | Rentalcars.com | Bassadone Automotive Group
TREK | Pizza Hut | pizza pizza

How Cyber-Criminals are Exploiting Shifts in the Retail Industry

Cyber-criminals use sophisticated schemes to target retailers and the vast amounts of personal and financial information of their customers. Usually this threat landscape intensifies seasonally - Darktrace observed a 128% increase in trojan attacks through November and December 2020 relative to the previous months. Even outside of the holiday period, the volume of attacks affecting the retail industry doubled in early 2021, due in part to global shifts toward remote working.

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 ecommerce, including online skimming, have steadily increased.

Of concern is the sector's increasing reliance 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.

> “When we talk about great security – AI is absolutely part of it. A combination of humans and AI is what works today for security.”

Leon Shepherd, CIO, Ted Baker

> “The retail industry is a constant target for cyber-attacks, which is why we selected Darktrace’s innovative technology to detect potential attacks before they cause damage.”

Dane Sandersen, Global Security Director, Trek

An Immune System Approach for eCommerce

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.

Inspired by the human immune system, the technology 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's Autonomous Response technology, Antigena, then surgically 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, 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.

Threat Find: Stopping Sodinokibi Ransomware in its Tracks

In August 2020, Darktrace discovered a Sodinokibi ransomware infection in a retail customer. Sodinokibi is an example of Ransomware-as-a-Service (RaaS), a worrying trend which allows lower-level threat actors to launch advanced attacks.

The attack started when a device began engaging in anomalous administrative activities, before writing an unusual executable file and sharing it with other internal locations. The device then proceeded to encrypt multiple files on the network and write ransom notes. Immediately after, the device performed several network scans, looking for further open channels to exploit. This happened in minutes, showing just how quickly ransomware can move through company networks.

Darktrace's Self-Learning AI alerted the security team at every step, allowing the customer to respond to the in-progress attack. If Antigena had been active, the attack would have been shut down as soon as it had begun, stopping any malicious activity in seconds.

> "Having Darktrace AI technology constantly learning and improving is just so much better than auditing tools."

James Bywater, IT Infrastructure Manager, PizzaHut

Threats by Numbers

Number 1 most targeted sector by ransomware in 2020.

$ 4.2 billion paid by retail organizations to double-extortion ransomware in 2020.

70% of shopping occurred online in December of 2020, compared to 55% in 2019.

Darktrace's SaaS console highlights anomalous user activity to surface cloud and SaaS-based threats