Cyberint

Case Study

How Leading Online Retailers **Tackle Cybersecurity**

The old saying "time is money" rings especially true for digital retailers. Retailers who primarily depend on digital interactions can't afford any downtime, nor can they afford to ***lose sensitive customer information*** *as a result of a breach or a cyberattack.*

A 2018 study Ponemon institute found that the average cost per lost or stolen record is $148. For businesses that store information of hundreds of thousands of customers, **a breach can potentially cost tens of millions of dollars**. If we add losses resulting from other types of attacks, such as fraud and DDoS, the cost to retailers grows exponentially due to fraudulent purchases, defacements, loss of reputation and downtime.

In addition to direct monetary costs, retailers run the risk of losing customers to competitors and other channels. Customer churn rate of 22% (Statista, 2018) increases by 2.1% in case of data breach compromising personal identifiable information.

GROWTH OVER SECURITY

Most successful online businesses are focused on achieving exponential year-on-year growth. While growth is the primary aim of most retailers, a growth mindset often results in the prioritization of business-related investments and initiatives over cybersecurity objectives. For fast growing online and mobile retail companies with aggressive YoY growth targets, cybersecurity often becomes an afterthought, a decision that may prove costly in the long run.

At the same time, as retailers' reliance on digital channels grows, so does their potential attack surface. Not surprisingly, one leading digital fashion retailer specializing in online and mobile clothing sales worldwide, is a prime target for cyberattacks. **For this retailer, fortifying its overall business posture while enabling growth was a key challenge** that required implementing cyber defenses that serve as a business enabler – as opposed to being a standalone component in overall business strategy.

CHALLENGES

FRAUD

Fraudulent activities targeting the retailer are broad, ranging from fraudulent discount vouchers being sold on the Dark Web, to playbooks teaching people how to scam free clothes and refunds via the retailer's customer support.

In November and December of 2016, CyberInt provided the retailer's security team with 10 alerts indicating threat actors who either use or sell refund services for their website. Most of the alerts included concrete details for the identification of specific orders and accounts, and as a result of a joint effort by CyberInt and the retailer's security and fraud teams, the orders involved in fraudulent activity were cancelled and the accounts they originated from were blocked.

Threat actors were sharing playbooks that described how such scams can be carried out. By monitoring those playbooks on the Dark Web, **we were able to identify business processes that could reduce the success rate of such scams, while at the same time providing a higher level of service to legitimate claimants of refunds**.

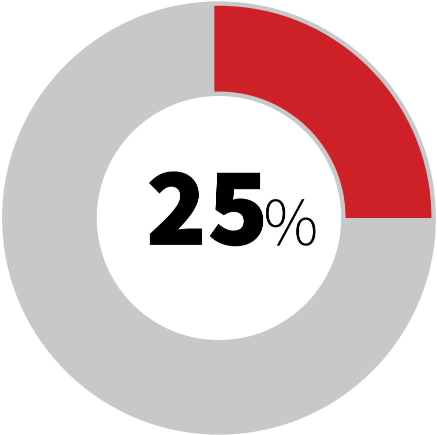
BRAND AND IP INFRINGEMENT

Cybercriminals often intentionally hijack brand names and tarnish reputations by creating copycat websites and social media accounts to trick customers into submitting their personal information. The retailer we work with has a well-known brand, so, it wouldn't take much for a cybercriminal to use domain names similar to their official domains and then lead unsuspecting customers to a fraudulent website masking itself as the retailer's website.

Other types of activities involve hijacking the brand where fraudulent clothes stores sell subpar items under the retailer's brand name or selling items via mobile apps using the their brand. **We identified over 200 apps that mimic the retailer's app, as well as hundreds of secondary market websites selling fraudulent and counterfeit goods posing as the retailer.**

As part of our Threat Intelligence coverage, we identified and took down phishing and IP infringing sites. These steps helped the retailer protect its brand and customers, while drastically reducing the time company staff would have needed to respond and take down these sites.

BREACHES, BRUTEFORCE, DDOS AND OTHER ATTACKS



Have technology to prevent a breach

Even with the best of intentions, companies often don't have the proper means to detect breaches with **only 25% have technology to prevent a breach**.

Combined with the fact that **retail remains one of the most targeted industries for cyberattacks**, online retailers need to be particularly vigilant.

Retailers that transact online have much at stake every minute their websites are not available. In March 2016, Amazon, the world's largest retailer, went down for approximately 13 minutes. Based on reported revenues of 107 billion in 2015, revenue lost due to

13 minutes of downtime amounted to **$2,646,501**

WHY ONE LEADING ONLINE FASHION RETAILER CHOSE CYBERINT AS ITS CYBER SECURITY PARTNER

With revenues of over £1.5 billion and hundreds of thousands branded and own-brand products, CyberInt's client, a leading UK online retailer, has an enormous customer base. This serves as a huge target for cybercriminals, who can make a profit selling the retailer' stolen personally identifiable and financial information.

> ***Online fashion retailers are vulnerable to the threats mentioned above, with constant threats of DDoS and brute force tools such as Sentry MBA.***

MANAGED SOC

In light of the many incidents the retailer was dealing with from both within its corporate network and from beyond the perimeter, one of the first things we did was put in place detection capabilities so we could detect potential attacks coming from endpoints, and identify activities such as lateral movements within the network.

We set up and are now running a complete Managed SOC that is fully integrated with our Argos™ Digital Risk Protection Platform. Gathering targeted and actionable intelligence, Argos™ pools both technological and human resources to generate real-time incidents of targeted attacks, data leakage and stolen credentials, and identifies threat actors in real time and provides contextual data about them.

Argos™ enables the retailer to receive real-time alerts on cyber-related issues such as DDoS, SQL injection, brute force and other threats. Alerts about these attacks are augmented with contextual data from Argos™, making them actionable.

AUGMENTING THE INTERNAL CYBERSECURITY TEAM

Like in most companies, qualified resources are always scarce. In order to support this retailer, we set up an onsite team at their premises to facilitate incident response capabilities to the alerts generated by the Managed SOC, and threats generated by the Argos™ Digital Risk Protection Platform. Our experts and analysts augment the internal team in taking care of threat management, incident response and defining proper protocols for security processes.

THREAT INTELLIGENCE

We frequently report on customer accounts being broken into and sold on the Dark Web. These accounts are flagged, their real owners are notified, and a password reset request is generated.

OUR OFFERING: BUSINESS CENTERED INSIGHT & ACTION

CyberInt understands that cyber defense should be part of everyday business and not function as a separate undertaking that's out of the loop of the online transactions that are targeted. That's what led this retailer to implement our Argos™ Digital Risk Protection Platform. In turn, customers recognize the retailer's commitment to security, which is a key differentiator in the industry.

Working with our dedicated team of analysts, the retailer can now:

- ***Constantly monitor threat actors' activities and identify the tools the cybercriminals use***
- ***Carry out threat intelligence investigations***
- ***Take down malicious and IP infringing sites***
- ***Detect and remove malicious content on all their social media channels***
- ***Continuously take the adversaries' perspective so they can better assess their own cyber defenses.***

SUMMARY

CyberInt platform services enable retail companies to take a proactive approach to cybersecurity while maintaining a business-as-usual approach and following its plans to realize exponential business growth. Retailers will also see a drastic reduction in fraudulent losses, improved time to detection and response, optimization of cyber defenses based on the changing threat landscape and continuous brand protection.

Cyberint

sales@cyberint.com

UNITED KINGDOM
Tel: +442035141515
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

ISRAEL
Tel: +972-3-7286777 | Fax: +972-3-7286777
Ha-Mefalsim 17 St | 4951447 | Kiryat Aryeh Petah-Tikva | Israel

SINGAPORE
Tel: +65-3163-5760
10 Anson Road | #33-04A International Plaza 079903 | Singapore