Security threats in the retail sector

Positive Technologies

ptsecurity.com

Main conclusions

- Over the course of 2020 and 2021, cyberattacks on retail increased by 117% against 2018 through 2019.

- 70% of attacks on retailers in 2021 targeted sensitive information. Most thefts were of personal data (32% of stolen information), payment card details (21%), customer databases (13%), and intellectual property (13%).

- The main consequences of cyberattacks in the retail industry are financial losses, reputational damage, fines, and lawsuits from customers.

- Ransomware was used in 79% of all attacks in 2021, an increase of 40 pp compared to 2020.

- Approximately 70% of all dark web adverts soliciting website hacking services were seeking to gain unauthorized access to websites. Dealers are most interested in online stores, where prices for access range from $50 to $2,000.

- Most cybersecurity incidents in the retail sector affect customers (which reduces their trust in retailers) or the operability of websites and infrastructure. Both types of attack entail serious financial losses for retailers and damage to their business.

Cyberthreats are increasing as e-commerce flourishes

The global e-commerce market is expanding, with a growth of 16.3% in 2021 compared to 2020.

Cybercriminals are increasingly setting their sights on prospering industries and businesses, and the retail sector has not escaped their attention. Hackers targeting retail typically seek to steal either money or customer data. E-commerce has expanded significantly over the past year. Burgeoning sales volumes mean that ever more customers are entrusting personal and banking details to online stores. This makes the sector increasingly attractive to cybercriminals. Attacks on retail accounted for 3% of all cyberattacks in 2021.

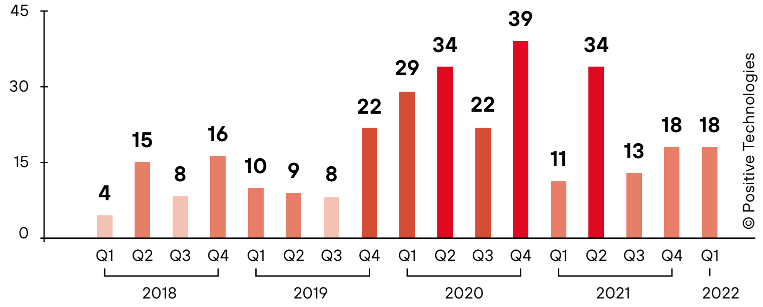


Figure 1. Number of cyberattacks[1] on retail businesses from Q1 2018 through Q1 2022

The number of cyberattacks on retail in 2020–2021 increased by 117% compared to 2018–2019.

[1] Widespread campaigns targeting a large number of organizations in the space of one quarter (such as Magecart attacks) were counted as a single incident.

Risks to retailers

The success of any retail business is directly dependent on its customers, and any incident that harms customers will have repercussions for business. Confidence in a retailer can be shaken by incidents like bank card details being stolen and used to extract funds from customers' accounts, as well as by visible disruption to the store's operation and the failure to deliver purchased goods. Loss of customer confidence in an online store equates to loss of income and potential bankruptcy for the business.

Another important factor in the success of any business is financial stability, and unpredictable financial losses are among the most harmful consequences of cyberattacks. Retailers face their own specific financial risks: for example, an attacker can reduce the price of expensive goods in an online store. If the attack goes unnoticed and the retailer sells and ships the goods at the reduced price, the company will lose money.

The most typical consequences of cyberattacks on retailers are:

- Financial losses
- Reputational damage
- Fines
- Lawsuits from customers

Some typical attacks on retailers and their potential consequences are illustrated below.

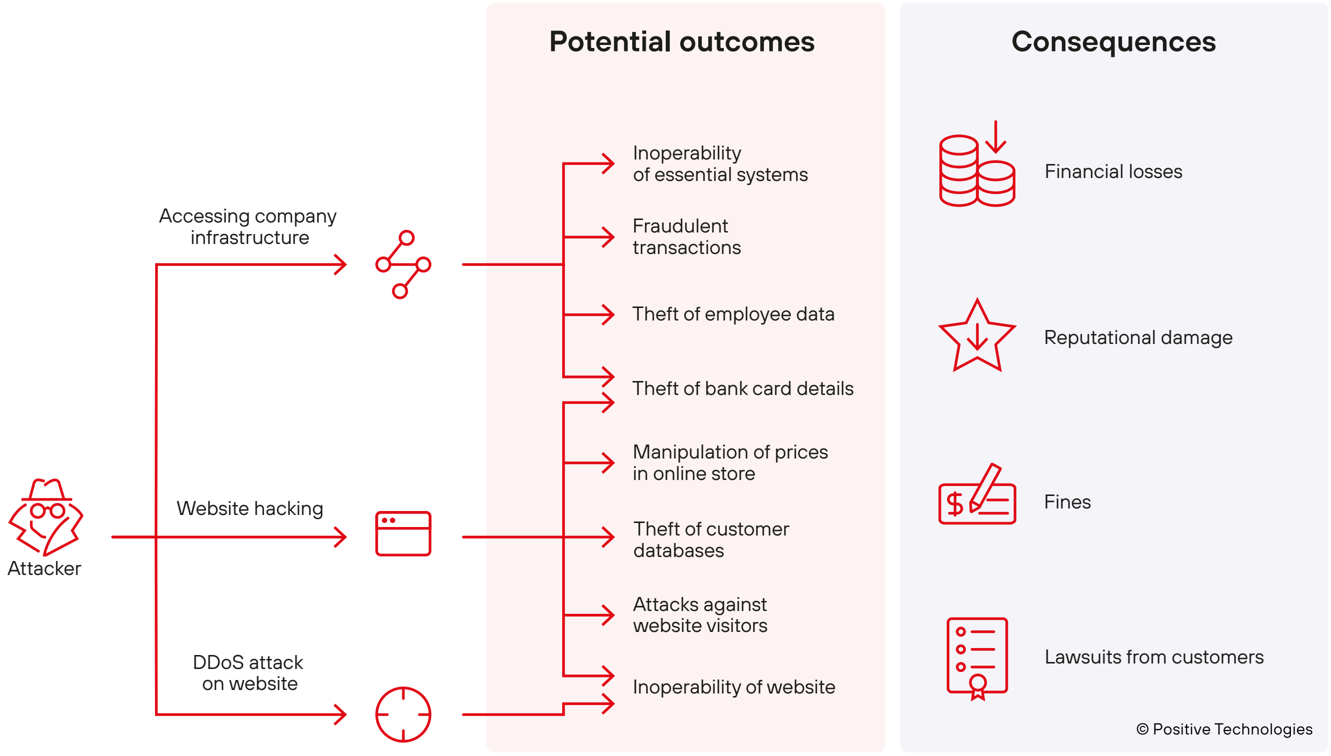


Figure 2. How cyberattacks affect retailers

Let's examine the two most damaging types of security incident for retailers: data theft and sales disruption.

Data theft

According to our research, 70% of attacks on retailers in 2021 targeted sensitive information. The most frequently targeted information was personal data (32% of stolen information), bank card details (21%), customer databases (13%), and intellectual property (13%). Attackers were able to obtain this information simply by hacking the company's website or gaining access to its internal network.

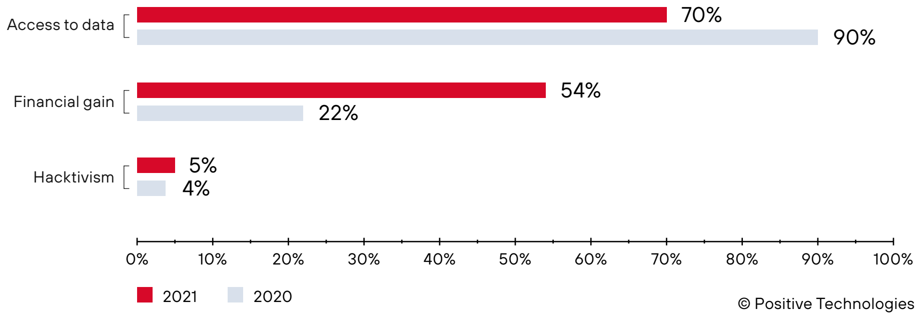


Figure 3. Motives for attacks on retailers in 2021 (percentage of incidents)

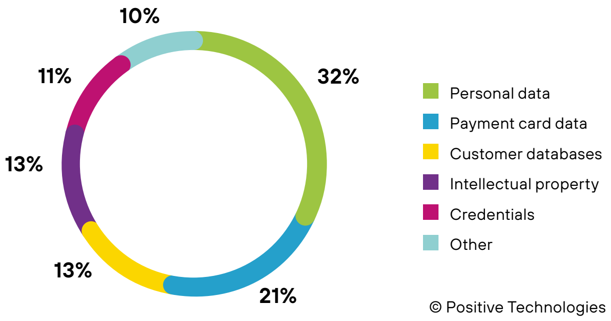
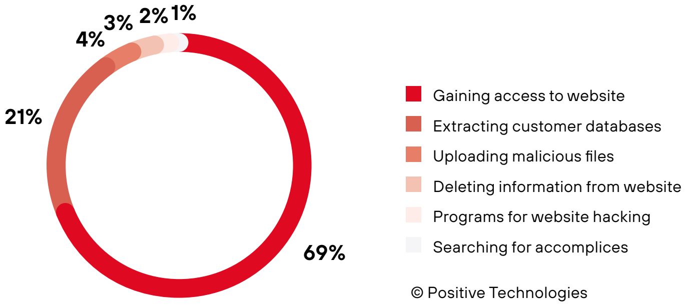


Figure 4. Types of data stolen in attacks on retail in 2021

In our Custom hacking services study, we analyzed adverts on dark web forums dedicated to website hacking services. We found that approximately 70% of posts soliciting hacking services were aimed at gaining access to websites. Not only can attackers steal sensitive information, they can also sell website access to dealers.



© Positive Technologies

Figure 5. Posts on dark web hacking forums by type

Online stores are of the greatest interest to attackers because they process card payments. Attackers can inject JavaScript code into a website to collect bank card details entered by customers.

Example attack: in the fall of 2020, more than 2,000 online stores based on CMS Magento were attacked using a zero-day vulnerability that enabled hackers to inject malicious code into the stores' websites and steal customer's bank card details. The group that first carried out the attack called itself *Magecart*. The technique proved so successful that many imitators soon appeared. Later the technique itself became known as a Magecart attack.

When attackers gain privileged access to an online store, they can steal databases and gain access to the personal accounts of its customers. Attackers can use stored card details to make purchases, or they can use vulnerabilities in the online store system to order goods without making any payment at all. Access to online stores is bought and sold for prices ranging between $50 and $2,000.

Example attack: in April 2021, 895,000 gift certificates worth a total of $38 million were put up for sale on the dark web. The database contained certificates from 3,010 companies including Airbnb, Amazon, American Airlines, Chipotle, Dunkin' Donuts, Marriott, Nike, Subway, Target, and Walmart. The gift card data is presumed to have been obtained in an attack on the online gift card store Cardpool. The entire database was sold for just $20,000.

In March 2022, data leaked from a Russian food delivery service was published on the internet. The leak contained names, phone numbers, and addresses of more than 6.8 million customers. It was later combined with information leaked from other sources, including online stores, traffic police, and other delivery services. The merged data was put online in a publicly accessible interactive map that provided access to personal information including phone numbers, passport details, social network pages, and vehicle details.

Another method used in attacks on retailers involves gaining access to the internal network of the target company and attacking from within, for example by infecting devices with malware, or accessing POS terminals or other internal resources. In 2021 we examined the vulnerability of corporate IT systems to external attacks. We found that attackers could access the internal network of every company we inspected.

Example attack: attackers stole credit card data belonging to 2 million customers of South Korean E-Land Retail by hacking into the company's internal networks and installing malware on POS terminals. Over the course of a year they harvested data that could be used to clone credit cards that would be viable for making in-store purchases, and then executed a ransomware attack that led to the temporary closure of almost half the company's stores.

Sales disruption: causes and consequences

Retailers lose income when attacks bring down online storefronts, ERP systems, payment terminals, and other infrastructure involved in making sales. Attackers can also disrupt the operation of warehousing and logistics systems, which can lead to the spoilage of perishable goods. A DDoS attack or website defacement might disrupt the operation of an online store, while a ransomware attack can have serious consequences for infrastructure. Our 2021 threatscape analysis found that 79% of malware attacks on retailers involved the use of ransomware.

Example attack: in the spring of 2021, Dutch warehousing and transport company Bakker Logistiek was hit by a ransomware attack that brought the company's operations to a standstill. It was unable to accept orders, determine what goods were in storage or in what locations, or plan delivery routes. The incident led to an acute shortage of food products, especially cheese, in the largest Dutch supermarket chain Albert Heijn.

Preparedness is key to mitigating potential losses

Most threats in the retail sector are related to attacks on companies' websites and infrastructure, or attacks on their customers that subsequently damage customer confidence. Either way, the result is the same: retailers risk fines, loss of income, theft of goods, and expensive repairs to their infrastructure. The threshold of acceptable risk is different for every organization.

In order to implement preventive security measures, companies need to identify the events (such as website unavailability, customer card theft, or online purchasing fraud) that would result in unacceptable consequences for them and thoroughly assess the risk of these events occurring. To do this, we recommend using a cyberrange. A cyberrange allows you to test scenarios of cyberattacks which lead to critical consequences (taking into account related business processes and systems), determine the criteria for their occurrence, assess the performance of security tools and anti-fraud systems, and then plan measures and actions to protect against cyberattacks and minimize their consequences.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com

Positive Technologies is a leading global provider of information security solutions. Over 2,300 organizations worldwide use technologies and services developed by our company. For 20 years, our mission has been to counter hacker actions before unacceptable damage is done to a business or entire industries.

Positive Technologies is the first and only cybersecurity company in Russia to go public on the Moscow Exchange (MOEX: POSI).

Follow us on social media (Twitter, Habr) and in the News section at ptsecurity.com.