SOCRadar®

Top Cyber Threats for E-commerce

2021

Threat Landscape Report

CONTENTS

Introduction 03

Executive Summary & Key Findings 03

Why E-commerce and Online Retailers are Being Attacked? 04

Threats to E-commerce Institutions 05

Most Targeted Countries 06

Threats in E-commerce 07

Phishing 08

E-skimming or Digital-skimming 09

Credential Stuffing 11

Fraud 12

Ransomware 13

DDOS Attacks 14

Recommendations 14

How Can SOCRadar Help 15

INTRODUCTION

Executive Summary

According to United Nations trade and development experts, E-commerce retail sales jumped from 16% to 19% in 2020. Moreover, online retail sales in the U.S. increased 32.4% year-over-year in 2020. The same trend continued with a 39% increase in the first quarter of this year. Consumers started using online shopping more frequently for items from groceries to school supplies. This growing market became even more interesting for money-motivated threat actors.

E-commerce business owners are aware of the increasing cyber security issues and taking measures accordingly. In the VMWare Carbon Black 2020 Cybersecurity Outlook Report, 77% of businesses surveyed purchased new security products last year, and 69% increased security personnel. However, big and small, E-commerce shops still became prime targets for web skimming attacks, extortion, DDoS threats, vulnerabilities, and supply-chain threats. The threat landscape of e-commerce is expanding with new technologies, automated tools, and bot armies. Threat actors` most dangerous attack vector is web skimming. Obfuscated malware stays hidden when stealing credit card information using compromised third-party libraries.

Key Findings

- The number of posts targeting E-commerce institutions increased by 37% in the third quarter of 2021 compared to the first quarter of the same year.
- The percentage of deep web posts targeting e-commerce industry has reached 8.3% in 2021.
- SOCRadar detected almost 10,000 phishing domains impersonating retail e-commerce sites registered in 2021.
- SOCRadar recorded 6.44 million leaked account information on the dark web most so far 2021 only in the E-commerce industry, which could be used for account takeovers.

Why E-commerce and Online Retailers are Being Attacked?

Since the start of the Covid-19 Pandemic, how we do business and have dramatically changed. The stocks of big online retailers like Amazon, Costco, Walmart are soaring to new heights. Firms with no online presence got the hardest hit through the pandemic. On the other hand, this online activity created new opportunities for cybercriminals. Online retail and e-commerce sites became prime targets for cyber attacks.

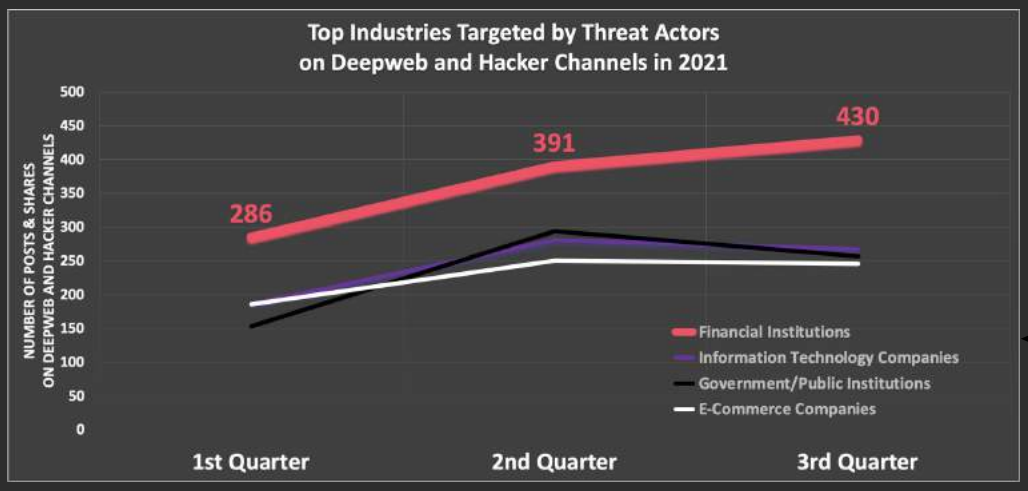
There are many reasons for this continuing trend of cyber attacks on e-commerce. First of the many reasons is the high expectations of the customer experience through shopping medium, either a website or mobile app. When companies try to improve customer satisfaction, they try to create a hassle-free, frictionless experience. When a verification for identification or payment process fails, it is straightforward for the customer to try a different site among the many choices available. Therefore, an unfinished transaction is a current and future business loss for the company. To provide the frictionless experience that customer demand, companies either ease their cyber security requirements or involve third-party vendors, expanding the external attack surface.

The second reason for cyberattacks on e-commerce and online retailers is the high value of the customer data like credit card transactions and general personal details. Especially, big retail companies have a wealth of data on their frequent users to provide a unique and pleasant experience. This kind of personal data makes the customer more vulnerable to different attack vectors like social engineering.

We also need to add the payments systems and IoT devices to the expanded attack surface mentioned above. The past cyber-attacks showed that PoS devices could be the low-hanging fruit for hackers. It is easy to install malware on them. Unprotected IoT devices also could be a foothold for cybercriminals.

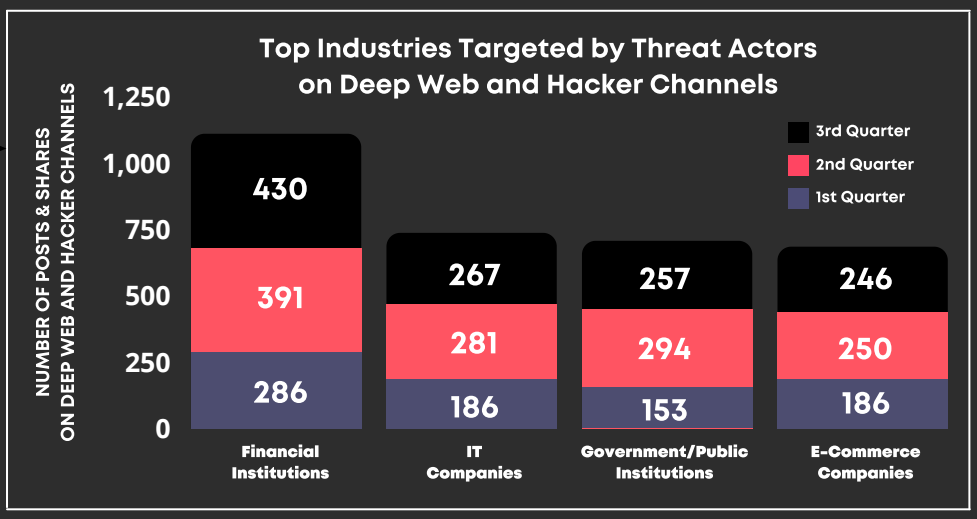
Deep Web Threats to E-commerce Institutions

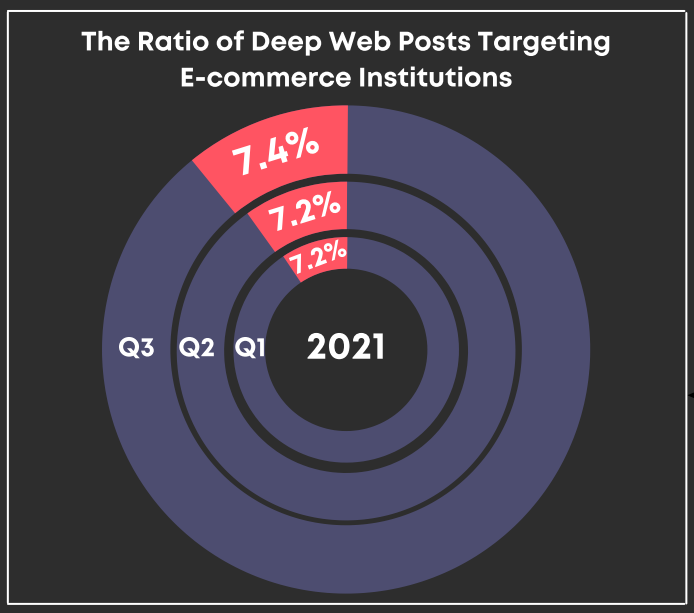
SOCRadar Research Team analyzed around ten thousand posts and shares on darknet/ deep web forums and hacker channels on different mediums. 7.3% of these posts were about the e-commerce industry.



E-commerce is one of the top four industries targeted by threat actors concerning the total number of posts and shares on deep web and hacker channels together with the finance industry, IT firms, and government/public institutions.

The number of posts targeting E-commerce institutions increased by 37% in the third quarter of 2021 compared to the first quarter of the same year.

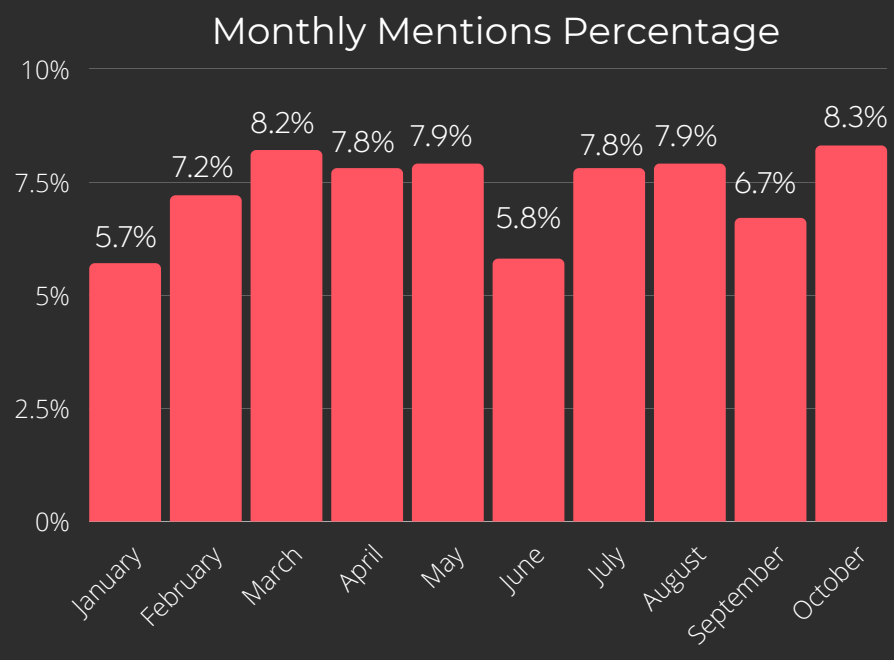




7.4%

As mentioned above, 7.3% of the deep web posts were about e-commerce — their distribution for quarters of 2021.

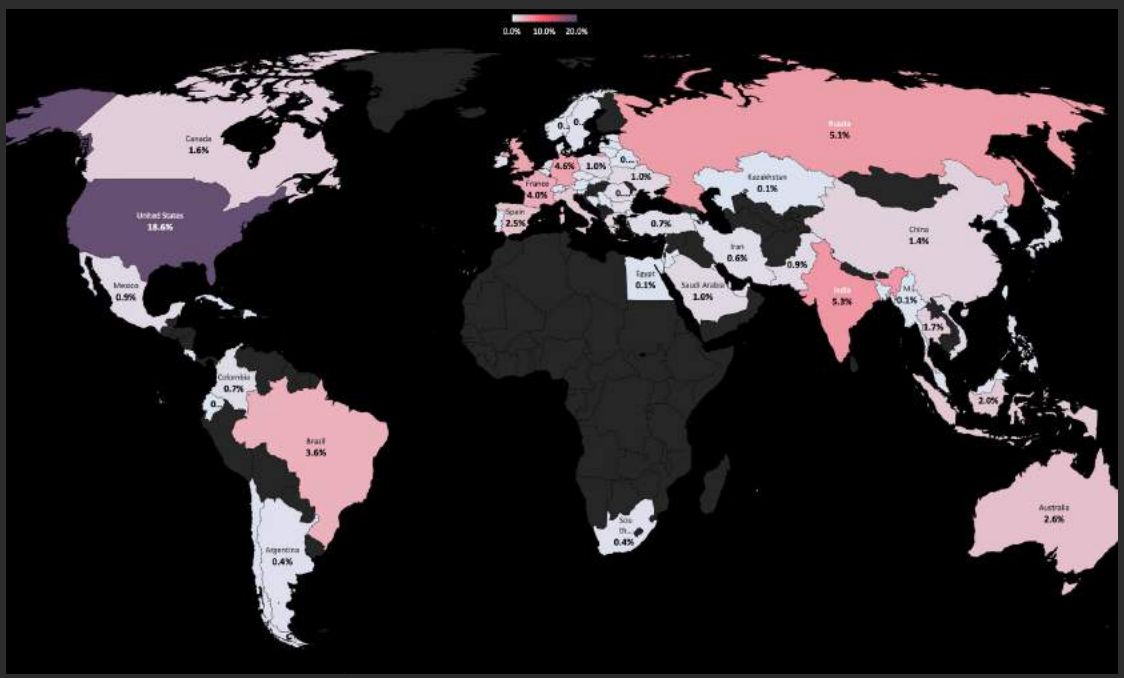
The percentage of deep web posts targeting e-commerce firms has reached 8.3% in October of 2021. SOCRadar Research Team observes an increase in the number of deep web mentions targeting e-commerce during the holiday seasons.



Most Targeted Countries

Concerning the deep web post and hacker channel shares targeting e-commerce institutions, the most targeted countries in the first three quarters of 2021 are:

1. US
2. India
3. Russia
4. Germany
5. UK
6. France
7. Brazil
8. Australia
9. Spain
10. Italy



SOCRadar opens the door of the deep web securely and efficiently with its search engine for deep web: ThreatHose.

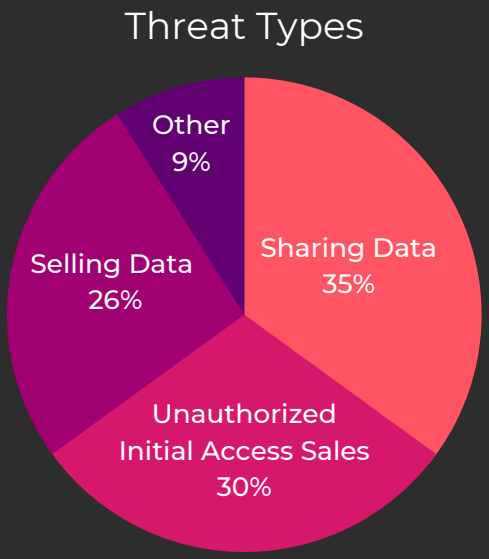
Request a free deep web report today to see what threat actors post about your company.

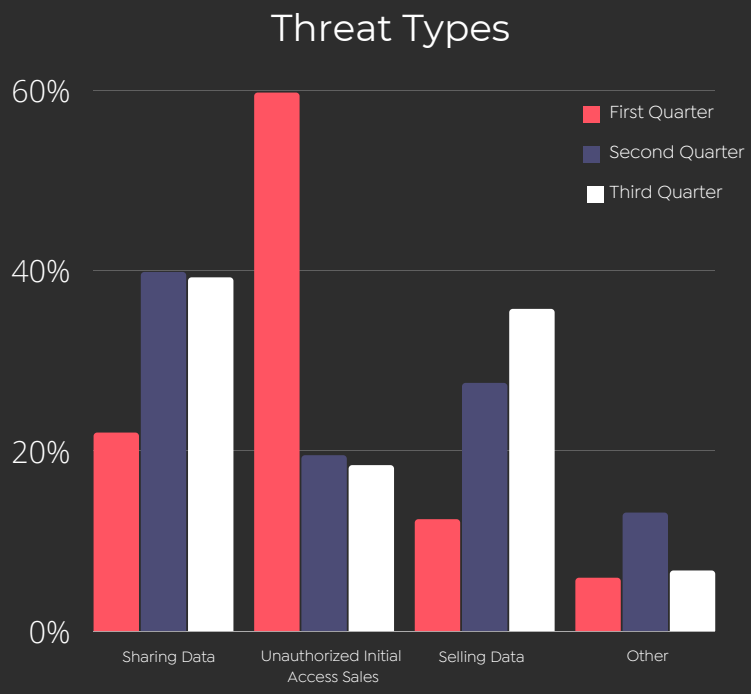
Threats in E-commerce

The majority of deep web posts targeting E-commerce institutions are related to sensitive data changing hands, either being sold or shared by threat actors. The exposed data on sale includes credit card information, employee PII data, and customer databases.

With unauthorized initial access sales, E-commerce's most significant problem is the databases in the wrong hands.

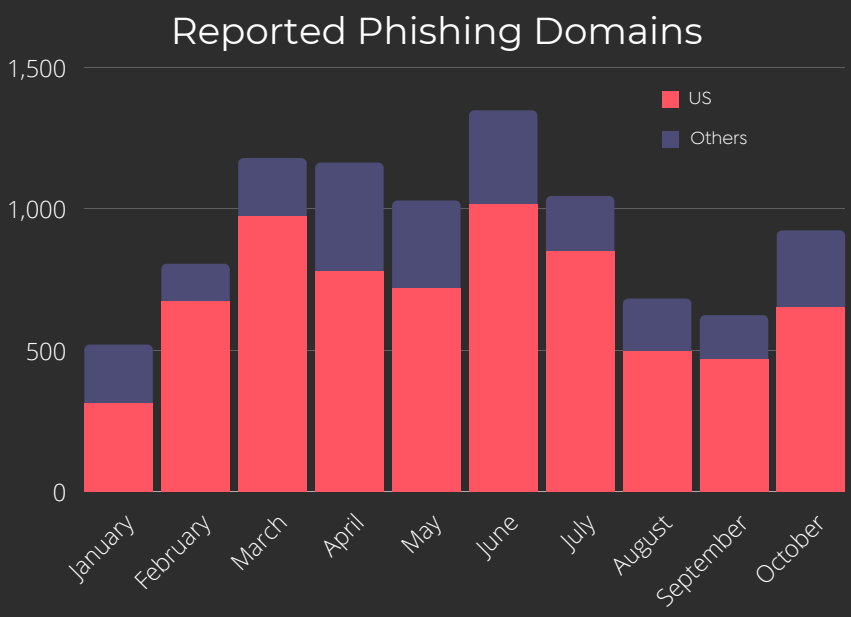
Compared to many other industries, Ransomware is not a significant threat vector for E-commerce. Threat actors try to stay as long as possible to maximize their data collection using tactics like skimming or phishing. While the initial access sales have lost their popularity in time, data sharing increases towards the end of the year.





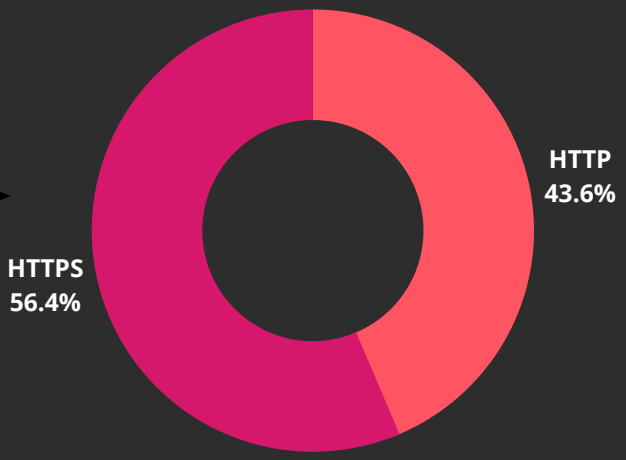
Phishing

Phishing is a tactic that targets victims primarily through emails and SMS. Emails appear to be from a legitimate source, but their main objective is to steal their personal information or login credentials by using impersonation.

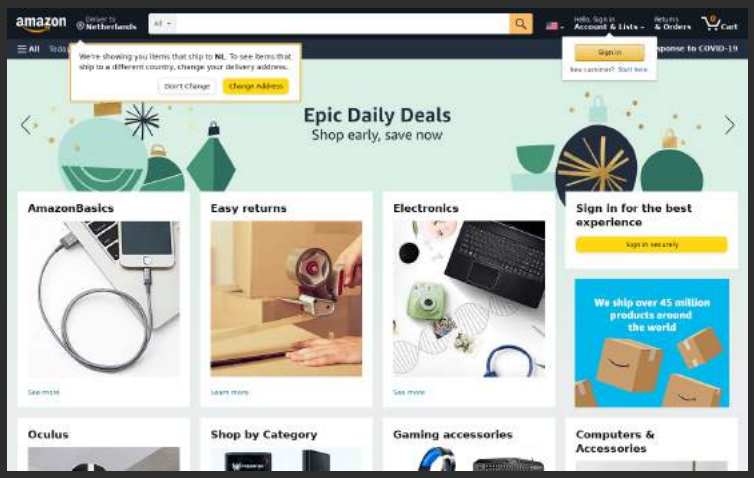


SOCRadar detected almost 10,000 phishing domains impersonating retail e-commerce sites like Amazon.com registered in 2021. Threat actors use phishing domains to lure customers and employees into stealing their credentials and accessing the company systems.

While threat actors prefer free registrars to register these phishing domains, they also might get an SSL/TLS certificate to convince the victims about the website's legitimacy. Seeing the HTTPS at the beginning of the URL with a nice padlock sign next to it gives a false sense of security to the users. SOCRadar discovered that 56% of the phishing domains impersonating e-commerce sites have a valid SSL certificate.



In 2021, phishing is still one of the dominant attack vectors in cybercrime. According to PhishLabs reports, phishing attacks increased more than 30% over 2020, and there were twice as many attacks compared to the previous year as of September 2021.

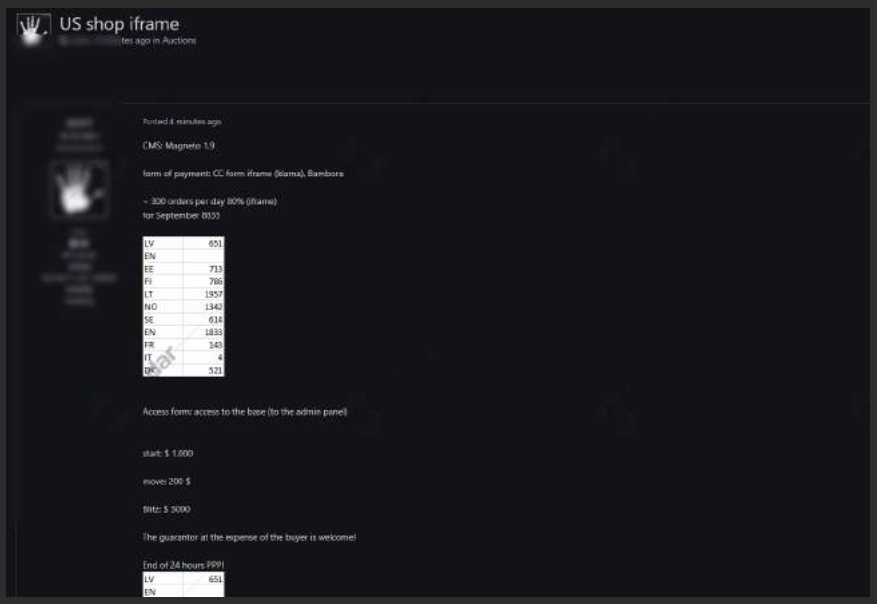


(A phishing site impersonating Amazon.com from SOCRadar archive)

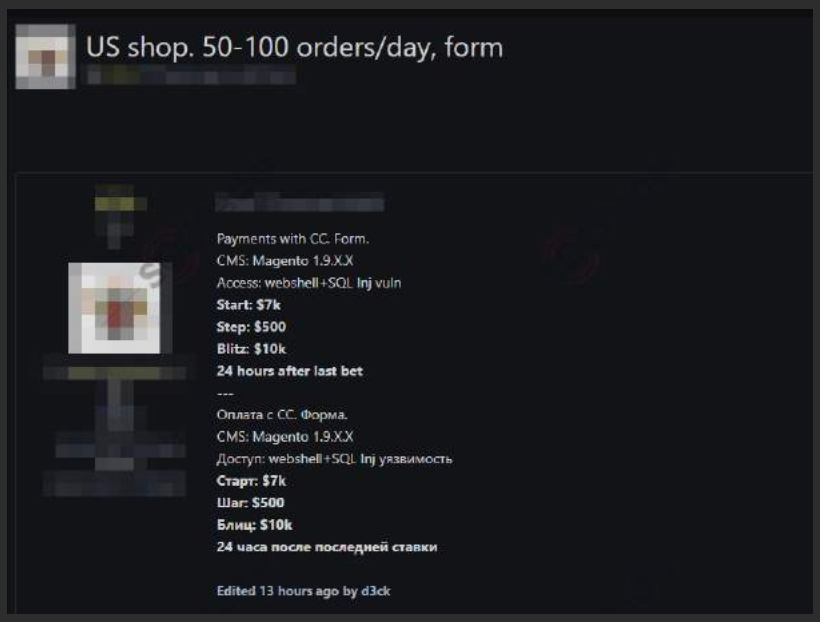
Interestingly, people over 65 were the fastest-growing segment of e-commerce shoppers in the first quarter of 2021. This segment lacks experience with phishing sites, making them an easy target for phishing attacks.

E-skimming or Digital-skimming

This attack refers to malicious code infecting checkout pages of e-commerce websites. These codes are challenging to detect, and they "sniff" the credit card data. Once a checkout page or a website is infected, the credit card information from every transaction will be "skimmed" without the knowledge of both trading parties. The common term for these kinds of threats and attacks is Magecart. Magecart is an umbrella term used to describe the hackers or groups of hackers responsible for carrying out these attacks



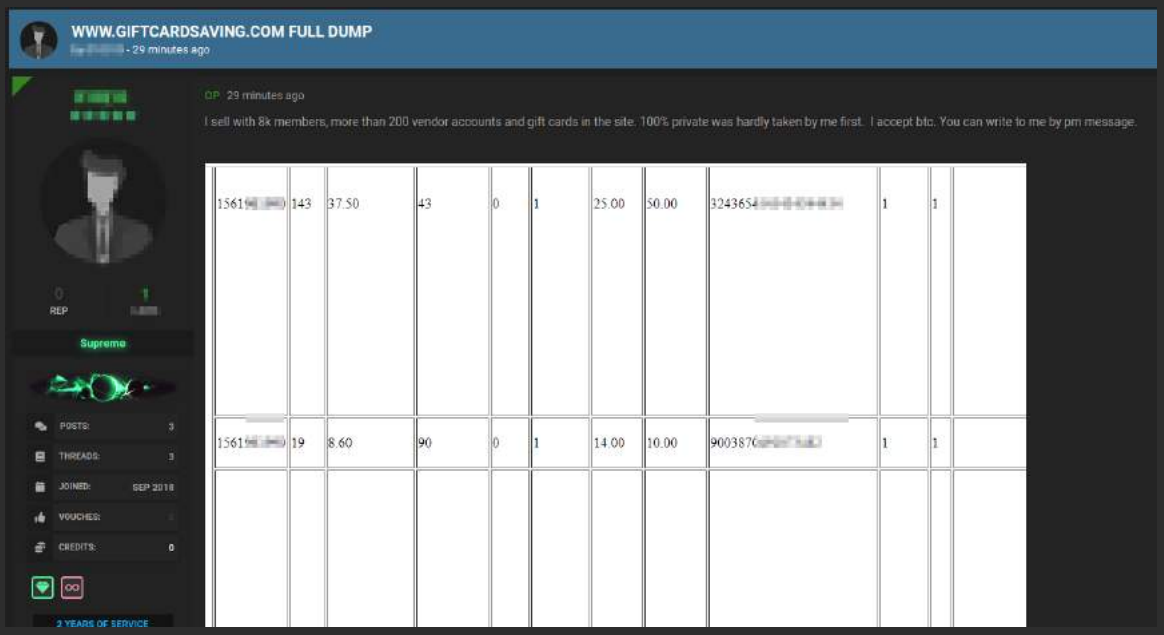
Magento 1.x



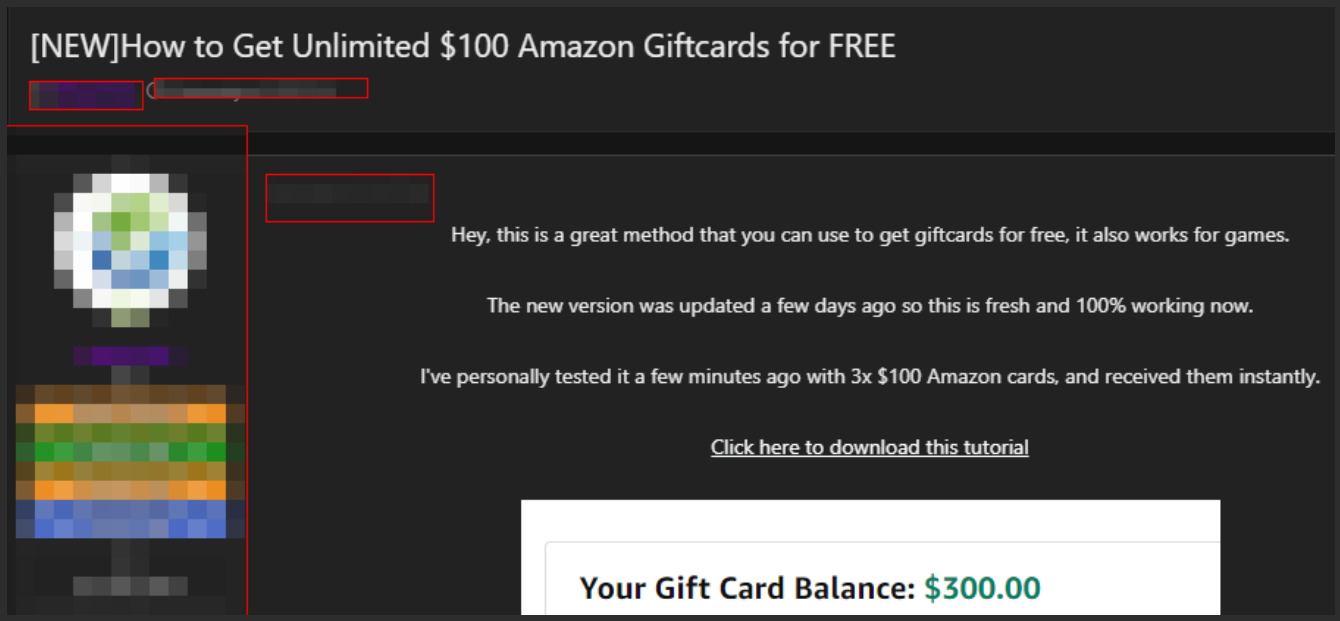
As mentioned above Magecart, both refer to the attacks exploiting the Magento 1.x and the hacker group(s) using this method. After the Covid-19 started, e-skimming attacks rose 26 percent in 2020. First, Magecart skimmers can gain access to the websites using malicious or compromised third-party JavaScript libraries. Then, they use obfuscation tactics to keep the malware undetected for long periods. For instance, skimmers hid the malicious code in a PNG file image for a FAQ icon in the Tupperware.com attack; clicking on the icon then triggered the fake payment form to load.

Even though, Magecart attacks got famous with high-value UK targets like **British Airways, Ticketmaster, Tupperware, and Newegg**. Owners manage many small shop websites. These shop owners are, most of the time, not aware of best practices in cyber security. Because of this, many small shops lack software patches and updates. For example, more than 200,000 webshops were still using Magento 1.x, one week after it reached the end of life in June 2020.

The posts in October so far set another bar with more than 14 million credit card information to be sold on the black markets. Half of them are from a single list posted on October 12.

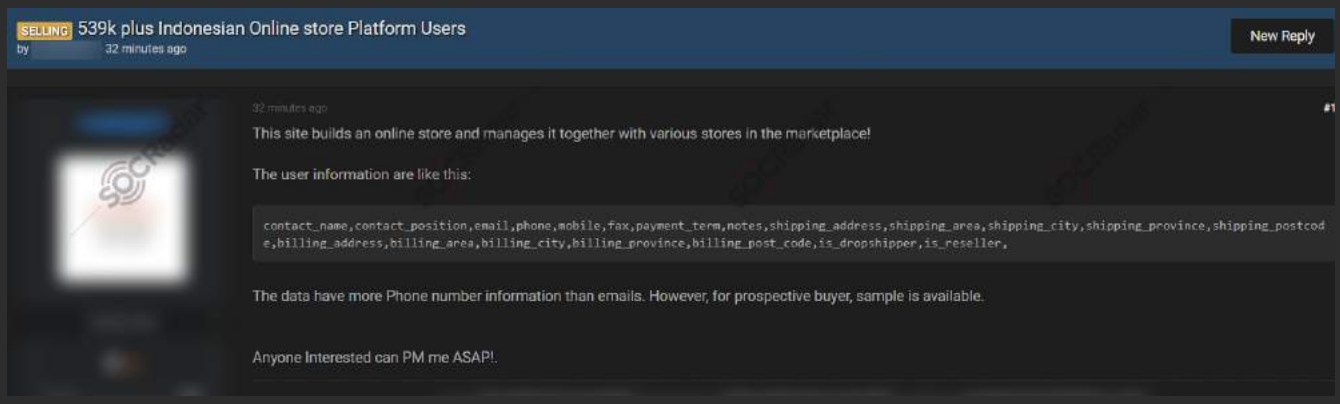


One of the ways that threat actors "cash-out" stolen credit card and account info is to buy and sell less traceable gift cards. However, sometimes threat actors can steal the gift cards for the algorithm creating the gift cards.



Credential Stuffing

Credential stuffing is a technique in which attackers try lists of compromised user credentials from previous data leaks to access another system. This attack assumes that many users recycle their usernames and passwords for different services. Automated bots will try all the credentials for multiple sites, creating another list of successful logins. The statistic shows that this attack has a chance of success around 0.1%.



SOCRadar recorded 6.44 M leaked account information on the dark web most so far 2021 only in the E-commerce industry. SOCRadar strictly monitors the black market where credit card and account information is sold in bulk.

Radware reports 52% lower in-store traffic in Cyber Week, the five biggest shopping days of the year from Thanksgiving to Cyber Monday, compared to the same period in 2019. However, the amount spent on online shopping increased by more than 20%. During this period, shoppers spent $34.4 billion, breaking the all-time high record.

Cyber Week, the five biggest shopping days of the year from Thanksgiving to Cyber Monday, was a blockbuster in 2020. The ongoing Covid-19 pandemic, combined with most consumers sheltering at home, resulted in 52% lower in-store traffic compared to the same period in 2019. Still, online spending surged by 21.6% to $9 billion, making Black Friday of 2020 the second-biggest day ever in terms of online spending (just behind Cyber Monday 2019). E-commerce records were broken as shoppers spent $34.4 billion over the period, a dramatic 20.7% jump over the previous year. However, there was a thousand-fold increase in bad bot traffic to some e-commerce websites, especially on log-in pages.

The broad availability of massive databases of breach credentials, such as "Collection #1-5," made 22 billion username and password combinations openly available in plaintext to the hacker community.

More sophisticated bots that simultaneously attempt several logins and appear to originate from different IP addresses. These bots can often circumvent simple security measures like banning IP addresses with too many failed logins.

Fraud

- A study from Juniper Research states that the value of losses due to eCommerce fraud will rise 18% this year, from $17.5 billion in 2020 to over $20 billion by 2021. A successful cyber attack could have a massive impact on the company because of the direct losses from business disruption and repairment, lost future business over reputational damage, penalties from regulatory bodies like GDPR.

- Credit card fraud involves stolen payment card information (PCI). It could be a neighbor kid trying to buy the latest game using a stolen PCI found in a forum or a complicated code running thousands of stolen PCIs from the dark web to purchase batches of goods using bots to sell on the black market.

- Another form of fraud is account takeover. Attackers illegally obtain access to personal and confidential data such as passwords control victims' online accounts and digital assets. Then, the malicious actor uses the control to commit illegal acts like placing bulk orders to make sellers' inventory unavailable. Account takeover is increased since the recent data breaches like Ubiquiti, Microsoft Exchange, U.S. Cellular, etc.

- However, the most basic form of fraud does not involve hacking, called refund fraud. Refund fraud, a form of social engineering, consists in obtaining a refund under pretenses. For example, a consumer could try to return the used item or claim that the shipped package has never arrived.

- Most of the time, indirect and following fraud costs hurt merchants more than direct costs. Fraud increases the workload of customer support teams, leads to customer dissatisfaction (brand reputation damage).

Ransomware

Especially after the Covid-19 pandemic started, the ransomware news became part of our daily routine, and attacks like Colonial Pipeline directly affected everyday life. There are similar trends in the e-commerce sector. A recent Sophos report shows that 44% of retail organizations were hit by ransomware in the last year, and 54% of these attacks were successful, and customer data was encrypted. Almost one-third of the companies whose data was encrypted paid average ransomware of $150K, but they only got back two-thirds of their data on average. The average bill from recovering from a ransomware attack in the retail sector (downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more) was US$1.97 million

DDOS Attacks

Denial of Service is a cyber-attack allowing threat actors to render the website unusable for legit users by sending an overwhelming traffic volume. In the case of a distributed denial of service (DDoS) attack, multiple sources, multiple bots from untraceable IP addresses send constant traffic to the target server to crash. As a result, it could cause business disruption, which could significantly bother during the peak business periods. Threat actors use DDoS attacks to put pressure on ransomware victims or as an extortion tactic.

In February 2020, Amazon Web Services defended against a DDoS attack with a peak traffic volume of 2.3 Tbps (Terabits per second), the largest ever recorded. Amazon said that the attack was mitigated by AWS Shield, a service designed to protect customers of Amazon.

RECOMMENDATIONS

Threat actors target e-commerce firms because they have money and a wealth of information on their clients, the same as money for the threat actors. There are some precautions that could be taken to protect your website and your clients' personal information. For those, SOCRadar can help.

1. Keeping Track of the Vulnerabilities on Digital Assets

There are particular vulnerabilities and sometimes zero-days that threat actors exploit. SOCRadar discovers almost all of your digital assets and their vulnerabilities. SOCRadar's External Attack Surface Mapper tracks your digital assets and the software versions installed on the assets and their vulnerabilities. Therefore, you stop attacks before they start.

2. Identifying and Monitoring Threat Actors

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only actives and specific regions and sectors. Monitoring the threat landscape and threat actors will make your defenses stronger. SOCRadar's threat intelligence threat feeds, IOCs, IOAs will give you the proactive readiness you need.

3. Phishing Control

Social engineering and phishing are still the starting attack vectors for many cyber attacks. In addition to your company's training for not clicking untrusted links and email attachments without verifying their authenticity, SOCRadar can discover impersonating and typo-squatting domains which could be used for phishing campaigns against your customers and employees.

4. Dark Web and Deep Web Awareness

Threat actors often find their way into systems by purchasing credentials or intelligence from dark and deep web forums and chatter channels. SOCRadar monitors these channels and creates alarms and incidents for anything related to your company.

In addition to these steps, there are more things to protect yourself, such as:

- You could create strict identity and access management policies by utilizing multiple-factor authentication (MFA) and one-time-password (OTP) technologies for your employees.
- User and payment verification for clients. Research shows most people agree with increased protection in check-out pages as long as an explanation is provided.
- You could protect your endpoints, including POS and IoT devices using trusted security hardware software as much as possible.
- You must have backup policies and practices. In addition, you should have multiple recent copies (preferably at least one offline) of your critical data and settings and configurations of your security devices.

HOW CAN WE HELP?

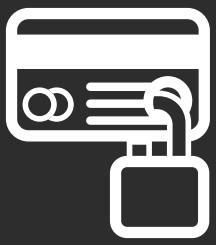
SOCRadar provides extended cyber threat intelligence (XTI) that combines,

- Cyber Threat Intelligence,
- Digital Risk Protection, and
- External Attack Surface Management Services.

SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the era of transformation.

Darknet and Deep Web Monitoring

SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye achieves further to provide in-depth insights into financially-targeted APT groups and threat landscape.



Credit Card Monitoring

Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers' PII

Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

360-Degree Visibility

Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

See SOCRadar in action!

Free Access Now

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management . Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with strong AI algorithms and a highly talented analyst team, together they eliminate false positives.

FOLLOW US!

CONTACT US info@socradar.io +1 (571) 249-4598 4000 Legato Road, Suite 1100 Fairfax, VA 22033 USA