White Paper
TLP: WHITE

Threat actors looking for a steal: Key threats impacting retail industry

Key findings

- The retail industry is a highly targeted vertical, a trend Intel 471 assesses is certain to continue since defrauding retailers remains a lucrative pursuit for financially motivated threat actors.
- The risk posed to retailers with significant e-commerce operations is very likely to persist due to significant interest from cybercriminals seeking access to entities that process large volumes of valuable customer and payment card data.
- Looking ahead, Intel 471 expects a higher volume of cyber threats targeting the retail industry as we move into and past the holiday shopping season. We base this assessment on our observations of threat actor activity on underground marketplaces, publicly reported incidents and Intel 471's collection and reporting that align with General Intelligence Requirements (GIRs) for the retail industry.

Overview

Our analysis of the cybercriminal underground revealed a variety of flourishing malware and fraud offers and services impacting retailers. This included ransomware, supply chain attacks to compromise third parties, point-of-sale (PoS) malware, digital skimmers, JavaScript (JS) sniffers and abuse of e-commerce platforms to steal customer and payment card information. We also observed threat actors conduct gift card and reward program fraud by leveraging account takeover (ATO) attacks and account-checking malware that compromised customer accounts of retailers. According to Intel 471's Intelligence platform (TITAN), we released 108 Information Reports (IRs), 30 Finished Intelligence (FINTEL) products and 232 Spot Reports (SPOTREPs) tagged with the GIR for the retail, wholesale and distribution industry from Jan. 1, 2021, to Nov. 10, 2021. We also expect to see a higher volume of cyber threats targeting the retail industry into the holiday shopping season and in the following months after it.

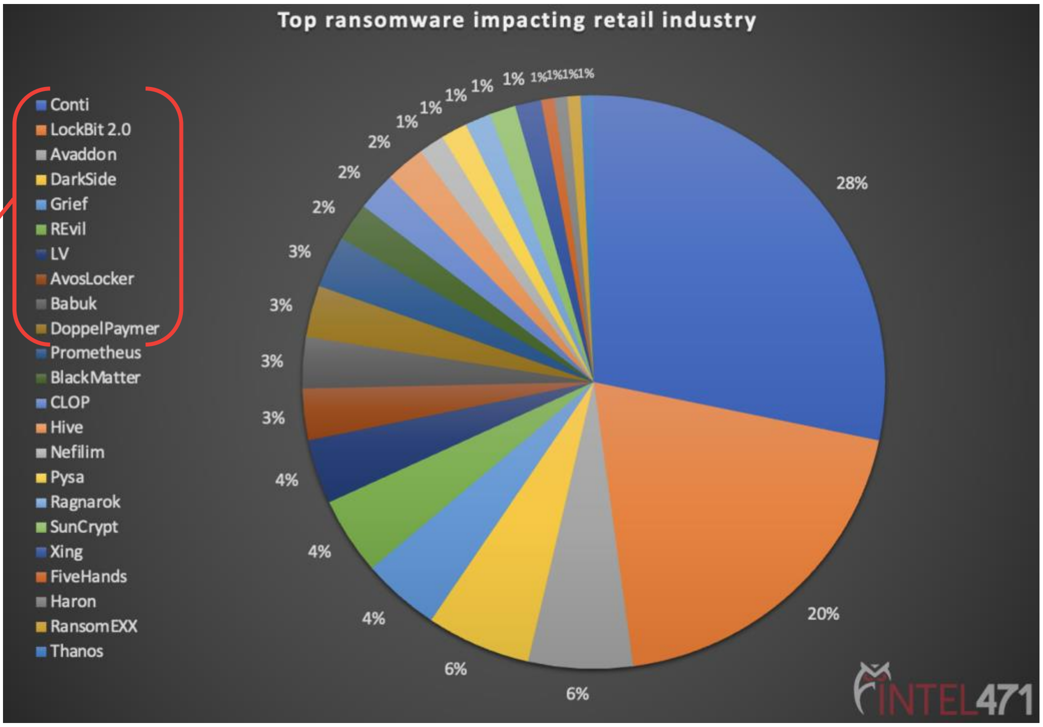
This report examines the retail industry's threat landscape. The following threats were identified and assessed as the most common targeting retailers:

- Ransomware-as-a-service (RaaS).
- Supply chain attacks and third-party risk.
- Payment fraud leveraging PoS malware, digital skimming attacks and JS sniffers for card-not-present (CNP) fraud, and the theft of customer and payment card information.
- Retail fraud involving ATO and credential-stuffing attacks using account-checking tools, including abuse of e-commerce payment platforms.

Ransomware-as-a-service

Ransomware continues to be a prominent threat emanating from the underground. The volume of ransomware attacks shows no signs of slowing and likely will continue to rise. RaaS operators persist in their attempt to evolve their tactics, techniques and procedures (TTPs), while also indiscriminately expanding their range of targets. Intel 471's breach data from Jan. 1, 2021, to Nov. 10, 2021, indicated 140 ransomware-associated breach events impacted the retail industry. Intel 471 identified the top 10 ransomware variants that pose a threat to the retail industry based on number of reported breach events:

1. Conti.
2. LockBit 2.0.
3. Avaddon.
4. DarkSide.
5. Grief.
6. REvil.
7. LV.
8. AvosLocker.
9. Babuk.
10. DoppelPaymer.



Graph 1: The graph depicts the breakdown of ransomware variants that impacted the retail industry from Jan. 1, 2021, to Nov. 10, 2021.

Retail entities impacted by RaaS programs in 2021 included the U.S.-based company Transform SR Brands LLC d/b/a Transformco, the U.S.-based giftware and home decor product provider Enesco LLC, the U.S.-based apparel wholesaler Perrin Inc., the Canada-based grocery retail store chain Goodness Me! And the Spain-based apparel brand El Ganso operated by Acturus Capital SL.

When it comes to initial access vectors for RaaS affiliates and operators, Intel 471 identified several techniques threat actors leveraged from our research for our monthly Breach Reports. Initial access TTPs included the exploitation of public-facing applications, external remote services and valid accounts. Threat actors also often used structured query language-injection (SQLi) and remote code execution (RCE) vulnerabilities to gain access to target networks and databases. Ransomware operators and/or affiliates likely also purchased compromised Citrix, remote desktop protocol (RDP) and virtual private network (VPN) accounts for initial access.

In 2021, Intel 471 tracked the growing and increasingly close relationship between ransomware operators or affiliate programs and access brokers selling compromised access and data. This was a significant trend since it offered a shortcut for ransomware operations to leverage existing access to corporate networks or repurpose stolen data to conduct attacks against the retail industry. In October 2021, an underground actor allegedly sought to partner with corporate network access brokers to conduct ransomware attacks using two popular ransomware strains. The actor claimed to operate in a team and offered network access brokers high percentages of the ransom payment for each victim provided. The actor specifically expressed interest in attacking high-revenue targets in all industries, likely including those in the retail industry.

Ransomware attacks remain a significant threat to retail entities due to their potential impact on critical e-commerce operations, which can inflict vast financial losses, especially if downtime occurs during busy shopping periods. RaaS programs also likely will continue to leverage double extortion or name-and-shame tactics with their attacks. Our assessment is based on observations of these tactics in ransomware negotiations and their success rate, which also resulted in other ransomware groups adopting them. Ultimately, this is reflective of the dynamics at play in the underground economy when successful and effective methods are commoditized and achieve wider adoption by other actors. Considering ransomware affiliates and operators increasingly used these tactics, the release or auction of sensitive customer data online if ransoms are not paid can negatively impact the reputation of retailers and erode consumer trust.

Supply chain, third-party attacks

The retail industry's business operations such as e-commerce, manufacturing and distribution rely heavily on the support of an extensive, global network of supply chains, third-party services and vendors. Unfortunately, this reliance also broadens the attack surface for retailers and provides cybercriminals with additional vectors to exploit. Previous research on data risk in the third party and supply chain ecosystem revealed about 54% of companies do not monitor the security practices of vendors and only about 29% believe their third-party vendors would notify them of any potential compromises.[1] Without established trust and transparency between retailers and third-party vendors, organizations could be increasingly vulnerable to supply chain attacks where threat actors gain entry into e-commerce platforms, networks and systems of retailers.

Recent high-profile supply chain attacks such as the December 2020 SolarWinds incident that impacted thousands of customers and the Citrix breach disclosed in March 2019 that exposed several terabytes of data from the company's server, highlight the evolving third-party risk and supply chain threat landscape. Cybercriminals are acutely aware of these third-party dependencies and continue to attempt to increase the sophistication of attacks by targeting profitable organizations and their proprietary information via this route. Gaining access to third party or supply chain networks could grant cybercriminals sufficient access upstream to leverage and exploit possible downstream access for further illicit use. It is a difficult, time-consuming and prohibitively expensive operation for corporations to recover from a system compromise that impacts customers on such a large scale. In comparison to an individual attempting to recover from a network or data breach, such an event represents a more critical threat to retailers with large e-commerce platforms.

Intel 471 continues to observe underground threat actors attempting to compromise upstream organizations to gain access to downstream credentials, networks and other data in bulk. For example, in June 2021, an actor allegedly compromised a digital marketing and data aggregation company, which the actor claimed multiple downstream customers were impacted by the alleged breach. Databases from the impacted organizations were offered for sale after the upstream victim reportedly ceased communications during a ransom negotiation. In parallel with the first common threat to the retail industry, ransomware attacks also pose a significant threat to supply chains. We observed the operators of the NEFILIM ransomware variant claim the compromise of MAS Holdings, a Sri Lankan lingerie and apparel manufacturer that produces clothing for well-known global retail brands. The NEFILIM operators leaked 9 GB of data on their blog and allegedly stole nearly 300 GB total.

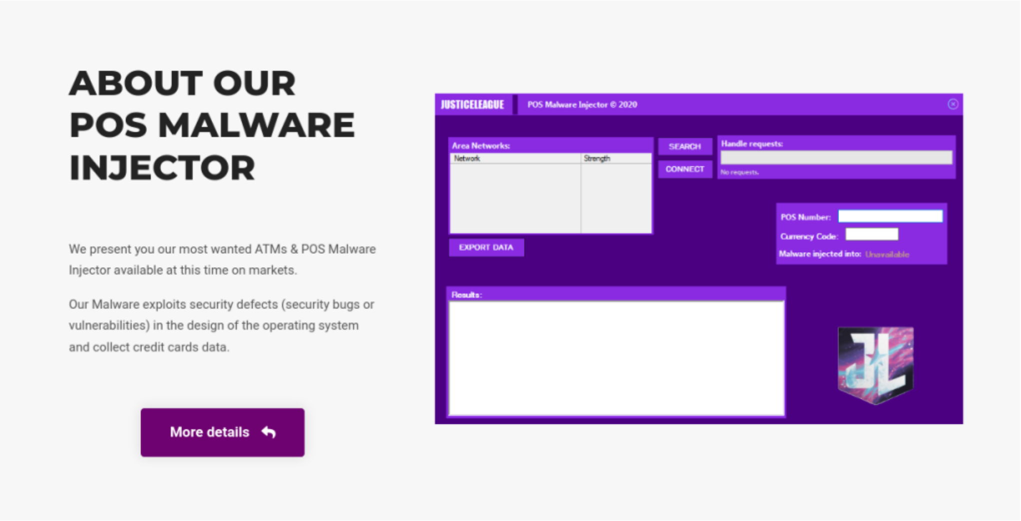
Third-party services and supply chains likely will remain an attractive vector of compromise for cybercriminals seeking to conduct attacks against organizations in the retail industry, due to valuable stored customer and payment card data that can be monetized on underground marketplaces. Businesses within the industry could have excellent control over their own networks, however, organizational compromise remains a significant risk if retailers are not also monitoring, or at least generating some dialogue about, the security standards of those they work with who have access to their sensitive data or systems. While risk of compromise remains one of the most serious impacts of third-party or supply chain attacks, retailers still can feel the effects of such incidents even if they do not result in a breach of their data or networks. If upstream businesses that retailers rely on are knocked out by a cyberattack, downstream entities whose operations depend on them also can suffer from the interruption or even standstill in business operations. This could result in significant financial loss.

Payment fraud

Point-of-sale malware

The use of PoS malware is not a new phenomenon among the underground community. For years, threat actors utilized PoS malware as a key tool in their fraudulent schemes since it presented another attack vector to steal valuable customer and payment information. Additionally, digital skimming malware became a convenient option for threat actors since it does not require physical access to a PoS terminal and can be leveraged against an entire e-commerce platform that includes thousands of stores running it.

In 2021, Intel 471 observed several actors engage in PoS malware-related activity. In February 2021, a known underground actor, **JusticeLeague**, advertised PoS malware dubbed ATM & POS Malware Injector on multiple underground marketplaces. This PoS malware allegedly operated as a data sniffer that did not require additional action from the user. Its key features included payment transaction data output in a result box that included Track 1 and Track 2 data and the card’s corresponding personal identification number (PIN). Payment card data collected via this PoS malware likely was used in further fraudulent activity or offered for sale as a product on criminal marketplaces or dump shop services.



ABOUT OUR POS MALWARE INJECTOR

We present you our most wanted ATMs & POS Malware Injector available at this time on markets.

Our Malware exploits security defects (security bugs or vulnerabilities) in the design of the operating system and collect credit cards data.

More details

Image 1: The image depicts part of the JusticeLeague shop's homepage.

As the use of digital payments and online shopping continues to rise, threat actors will persist in refining methods to exploit electronic PoS systems used to process card payments. Therefore, PoS malware will remain an attractive attack vector for cybercriminals who seek to defraud unsuspecting shoppers as they return to shop in person and online during and after the 2021 holiday season.

Skimmers, sniffers

Digital skimmers and JavaScript (JS) sniffers also became an increasingly popular attack vector among cybercriminals since they represent a low-cost, high-reward venture that is highly effective and profitable. Digital skimming attacks target e-commerce websites by injecting malicious JS code into an online checkout page, which enables threat actors to steal credit card and personally identifiable information (PII) in real time. In a typical digital skimming attack, the malicious code will check the customer and payment account number inputs before exfiltrating the stolen data to a command and control (C2) server that belongs to the attacker. Subsequently, the stolen credit card information and PII is monetized on criminal marketplaces or used to make fraudulent purchases. As a reflection of their popularity, Intel 471 observed threat actors install JS sniffers to intercept user data entered on compromised retail websites running e-commerce platforms such as Magento, OpenCart and Shopify.

In February 2021, an underground actor announced a special offer for their web-based payment card sniffer. Actors could rent the sniffer for US $690 and have it installed on their server for free. The actor also claimed to have an exploit for a zero-day vulnerability in Magento that allegedly allowed attackers to upload a web shell on compromised websites that ran Magento versions 1.x and 2.x. In April 2021, a separate underground actor recruited partners for their malware-as-a-service (MaaS) affiliate program. Partners allegedly would be required to deploy "private" JS payment card data sniffers to compromised websites and would receive as much as 75% of the profit from successful attacks. The actor claimed the malware was a multipurpose web-based sniffer tailored to be injected into Magento, OpenCart, osCommerce and other e-commerce platforms that do not rely on inline frames (iFrames) or user redirection to third-party payment websites. The malware also could grab cardholders' IP addresses, online store passwords and basic card details.

The prevalence of e-commerce store options and expected rise in online shopping during and after the 2021 holiday season, expands the attack surface for threat actors to exploit the retail industry via a variety of payment fraud methods.

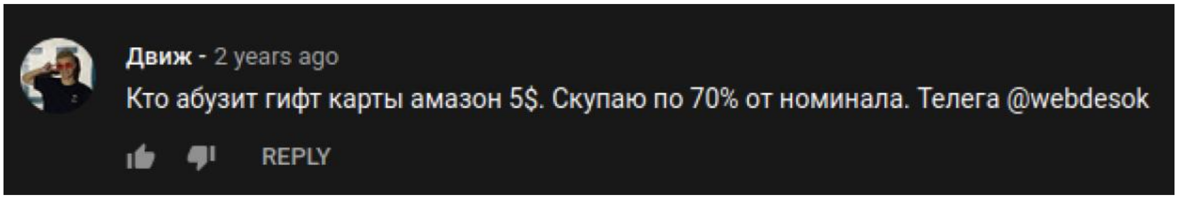
Retail fraud

Gift cards, rewards accounts

Monetizing or cashing out on illicit activity often is the ultimate end goal for financially motivated threat actors. This is supported by Intel 471's review of threat actor activity and discussions about gift card and rewards fraud. Gift card and reward program fraud is popular since gift cards can easily be traded or sold online for a percentage of the actual value. This activity was observed for several years prior to this report and impacts businesses and customers alike. The actors who successfully conduct gift card and reward account fraud will likely continue due to the low-effort of the operation. Similar to payment card fraud tactics and techniques used to steal victim information, we observed trends such as ATO activity related to gift card trading and cashing out.

Additionally, Intel 471 have previously reported on the existence of marketplace services offering tutorials on carding and fraudulent cashout operations against high-profile retail organizations, which included Apple, Best Buy and Walmart. Gift cards and reward programs allow for some degree of anonymity and the lack of associated PII makes them difficult to track. Moreover, gift card transactions or reward redemptions do not need to be reported or logged and typically are smaller in value compared to possible credit or debit card transactions.

In April 2021, we reported on an actor seeking to purchase digital gift cards to online merchants such as Amazon, Disney, Nordstrom, Pandora and Sephora. We identified that the actor communicated with at least five other individuals regarding buying and/or selling gift cards, including an actor who allegedly offered a cashback service. In August 2021, a possible Russian underground actor expressed interest in purchasing e-gift cards issued by e-commerce retailers, digital distribution services and other prominent retailers. The actor also purchased prepaid and virtual credit cards and would pay as much as 85% of the cards' value to then resell or cash out, alongside regularly cooperating with other e-gift card buyers on popular underground forums.


Движ - 2 years ago

Кто абузит гифт карты амазон 5$. Скупаю по 70% от номинала. Телега @webdesok

Image 2: The image depicts a comment on a YouTube video where an actor using the name onechiche stated, "Who targets $5 Amazon gift cards? I'll buy them at 70% of their value. Telegram:@webdesok."

Similar to e-gift cards, another customer benefit from the transition to online shopping was the inclusion of rewards points that could be applied to future purchases at a cash value. Loyalty and rewards accounts are not unique to the retail industry and similar activity was observed in other consumer and industrial product industries such as the aviation, hospitality and restaurant and food services industries. The creation of personal accounts with payment card information and rewards points offered threat actors another target for monetization against retail services. Targeting reward program accounts can be highly lucrative for actors. On the low end, access to lists with rewards accounts that held 14,000 to 75,000 points were priced from US $10 to US $50. On the high end, access to lists with rewards accounts that held about 335,000 to 880,000 rewards points were priced from US $200 to US $600.[2]

Intel 471 observed threat actors abusing reward programs to obtain and sell gift cards for different services. For instance, we observed a threat actor who allegedly had an extensive history in account checking and providing proof of monetizing Hilton Honors accounts on Amazon. One user of the actor’s service provided a positive review that stated the user could cash out and receive an Amazon gift card after purchasing access to a rewards account. Intel 471 also observed several users paying US $50 to US $875 for access to rewards points, which then were converted into gift cards. We continue to see threat actors apply tools and services to meet the goals of other financially motivated fraudulent activity, even for the purpose of obtaining access to rewards points to begin the process of cashing out.

Account takeover common attack tactic

ATO using account-checking tools and compromised credentials is a common tactic leveraged in fraudulent attacks against the retail industry. Most of the ATO attacks observed were automated credential-stuffing attacks. Threat actors typically automate ATO attempts by leveraging account-checking tools and botnets to test thousands of stolen passwords at once. Automated ATO attacks like these enable actors to scale capabilities by maximizing the chances of gaining access to accounts. Compromised retail customer accounts are a popular target for underground actors because they can act as an initial access vector. Additionally, threat actors can attempt to avoid detection by appearing as a legitimate customer within the compromised account and steal user payment information and rewards points, or modify the account for the attacker’s benefit.

Intel 471 observed multiple underground actors leveraging account-checking techniques to target retailers and acquire information stored within customers’ online shopping accounts. First observed in 2017 and still active at the time of this report, a familiar underground actor was known to conduct brute-force and account-checking attacks using tools based on the Private Keeper framework and operated multiple underground marketplaces for brute-forced accounts. In 2021, we observed one of the actor’s shops offering compromised accounts from online stores and services, which were obtained from credential-stuffing attacks. Inventory featured compromised accounts of 104 online stores and services including Aeropostale, Anthropologie, Gucci, Fabletics, Harvey Nichols, Sports Direct, thredUP and Tory Burch.

We also observed another underground actor, demonstrating ATO-related TTPs in reported attacks, including creating brute-force and account-checking software based on Private Keeper. The actor also was involved in digital gift card and loyalty program account fraud and expressed interest in retailers including Adidas, Best Buy, Columbia, H&M, Kohl’s, Lacoste, Levi's, Lowe's, Mango, Nike, Puma, Quicksilver, Tommy Hilfiger, Under Armour, Vans and Zara. Based on this interest in gift card fraud activity, we cannot rule out the possibility that the actor has leveraged ATO techniques to gain access to the digital gift cards and possibly rewards accounts as well.

The underground marketplace hosts an entire ecosystem focused on ATO activity, in addition to threat actors who offer account-checking and brute-force tools, combination lists, configuration files and information-stealer malware. Dedicated marketplaces, such as Genesis Store, are specifically tailored to offer compromised valid accounts including those of top retailers. The Genesis Store offered about 13,100 compromised accounts for Alibaba[.]com, 79,100 for Amazon[.]com, 52,000 for Apple[.]com, 180 for BestBuy[.]com and 1,000 for Walmart[.]com at the time of this report. The now-ubiquitous presence of credential marketplaces creates a centralized way for threat actors to buy and sell highly specific credentials targeting all industries including retail.

Outlook

The retail industry continues to be impacted heavily by cybercriminal activity; a trend Intel 471 assesses is almost certain to continue since defrauding retailers remains a highly lucrative pursuit for cybercriminals. We base this assessment on observed threat actor activity on underground marketplaces, publicly reported incidents and Intel 471's collection and reporting that align with GIRs for the retail industry.

Threat actor activity impacting the retail industry is expected to persist in two categories:

1. Malware threat types that can impact retail organizations, such as ransomware, supply chain attacks, PoS malware, digital skimmers, JS sniffers and abuse of e-commerce platforms to steal customer and payment card information.
2. Fraud-related retail-centric threat types that impact the customer and business, such as fraudulent attacks leveraging ATO tools and services, along with the abuse of compromised retail accounts and reward programs to steal and resell gift cards.

Looking ahead, Intel 471 expects increased threat actor activity impacting the retail industry during and following the busy 2021 holiday shopping season, as opportunistic cybercriminals seek to exploit increased e-commerce activity. This poses significant risk to global retail operations due to ongoing interest from cybercriminals in targeting entities that process large volumes of valuable customer and payment card data.

Intel 471's range of intelligence products can assist retail security teams in defending against fraud and retail-centric threats and mitigating the above risks. Our Adversary Intelligence provides security teams with visibility into the activity of underground actors targeting retailers, including insight into their TTPs and operations. Teams also can monitor for compromised customer credentials proactively via Intel 471's Credential Intelligence service, track weaponized malware via our Malware Intelligence and determine patch prioritization of vulnerabilities of e-commerce platforms via our Vulnerability Dashboard.

MITRE ATT&CK Techniques

This report uses the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework.

Technique Title	ID	Use
Resource Development [TA0042]		
Compromise Accounts	T1586	Threat actors acquired compromised accounts for attacks and to support operations through underground marketplaces.
Compromise Infrastructure	T1584	Threat actors may compromise third-party infrastructure such as servers, domains and web services that can be used during targeting.
Compromise Infrastructure: Domains	T1584.001	Threat actors compromised domains or subdomains belonging to retailers.
Initial Access [TA0001]		
Exploit Public-Facing Application	T1190	Threat actors leveraged vulnerabilities to gain initial access.
Supply Chain Compromise	T1195	Threat actors targeted supply chains to gain access to victims.
Valid Accounts	T1078	Threat actors will obtain and abuse credentials of existing retail customer accounts to gain initial access.
External Remote Services	T1133	Threat actors may leverage compromised credentials to gain access to VPN and Citrix accounts and other remote access mechanisms.
Execution [TA0002]		
Exploitation for Client Execution	T1203	Threat actors exploited software vulnerabilities for code execution on remote systems to gain initial access.
Command and Scripting Interpreter: JavaScript	T1059.007	Digital skimming attacks and JS sniffers use malicious JS code to execute and target e-commerce websites.
Credential Access [TA0006]		
Brute Force	T1110	Threat actors launched brute-force techniques to gain access to customer accounts using password hashes obtained from underground marketplaces.
Brute Force: Credential Stuffing	T1110.004	Threat actors leveraged credential-stuffing attacks to gain access to customer accounts.
Impact [TA0040]		
Data Encrypted for Impact	T1486	Threat actors encrypted data on target systems to render them inaccessible and extracted monetary compensation from a victim in exchange for decryption.

GIRs

1.1.1	Ransomware malware
1.1.5	Information-stealer malware
1.1.9	Point-of-sale (PoS) malware
1.2.2	Ransomware-as-a-service (RaaS)
2.1	Vulnerabilities
4.1.1	Cashout
4.1.5	Prepaid or gift card fraud
4.2.1	Payment card fraud
4.2.1.1	Online payment card skimming
4.2.2	Compromised credentials
4.2.2.1	Credential combination list(s)
4.2.3	Compromised personally identifiable information (PII)
4.2.5	Compromised network or system access
4.3.2	Account checking and credential stuffing
4.3.2.1	Account-checking configuration files(s)
4.3.3	Account brute forcing
5.5.3	Information or data breach
5.5.4	Blackmail
5.5.5	Supply chain attack tactic
6.1.1.7	Retail, wholesale and distribution industry
6.2.2	Asia
6.2.4	Europe
6.2.6	North America

Sources

[1] 01Nov2018 Ponemon Institute Report: Data Risk in the Third-Party Ecosystem: Third Annual Study
hxxps://www[.]ponemon[.]org/userfiles/filemanager/nvqfztft3qtufvi5gl60/

[2] 23June2021 Intel 471 Blog: Cybercriminals shop around for schemes targeting retail
hxxps://intel471[.]com/blog/retail-cybercrime-threats-2021