2022

Q3 Retail Sector

Quarterly Threat Landscape Scorecard

TLP:CLEAR A-2022-10-31b

ZEROFOX

Q3 2022 Retail Sector Threat Overview

The threat to retail sector organizations in Q3 2022 remained broadly consistent with previous quarters, with the ongoing war in Ukraine continuing to shape the cyber threat landscape. Retail organizations faced an increased threat from smishing, callback phishing, and threat actors leveraging techniques to bypass multi-factor authentication (MFA). ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online Version 2.0 (FIDO2) and certificate-based authentication. The sustained high pace of vulnerability disclosure, including in widely-used e-commerce platforms, will very likely strain out-of-cycle patch management processes and increases the risk of vulnerabilities not being patched in a timely manner. The shift to Initial Access Broker (IAB) market sales being made in private channels rather than advertising in open forums will likely continue and make identifying and mitigating access sales ahead of compromise increasingly challenging. Botnet and malware deployment remained high, including infostealers and trojans. Digital extortion attempts against retail targets remain below 2021 levels, likely caused in part by difficulty eliciting payments from victims. Incidents in Q3 2022 highlighted the high threat of attacks against third-party providers that could implicate multiple downstream customers.

Key Cyber Threats to the Retail Sector in Q3 2022

- Increased SMS-phishing, callback phishing, and techniques to bypass MFA
- Malware disguised as fake retail applications targeting customers
- IABs moving towards private means of communication with sellers
- State-linked and financially motivated threat actors targeting key personnel in job-related scams
- Skimmers deployed and compromise of payment systems and e-stores
- Vulnerabilities in third-party software used by retail organizations and the pace of exploitation
- Changes to digital extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications
- Saturated infostealer and trojan markets sustaining low barriers to entry and high pace of new Indicators of Compromise (IOCs)

Retail Sector Threats

Categories	Q1 2022	Q2 2022	Q3 2022
Social Engineering			
Vulnerability Exploitation			
Initial Access Brokers			
Botnets			
Malware			
Ransomware			

KEY

- Indication of decrease in threat from previous quarter
- No notable change in threat from previous quarter
- Indication of increase in threat from previous quarter

Q3 Key Findings:

- Retail organizations likely face an increased threat of smishing, callback phishing (vishing), and phishing techniques that bypass MFA.
- Vulnerabilities in widely-used ecommerce platforms were leveraged in attacks against the retail sector, long after patches were released.
- Illicit access to retail entities was increasingly being sold via private or direct communication channels.
- E-skimmers and other malware continued to be deployed at a high frequency against payment systems.
- Ransomware and digital extortion attempts against the retail sector this quarter highlighted the threat of attacks against third-party providers.

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 12:00 PM (EDT) on October 10, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

©2022 ZeroFox, Inc. All rights reserved. All other trademarks are property of their respective owners.

SOCIAL ENGINEERING

ZeroFox Intelligence assesses that aspects of the broader social engineering threat to the retail sector increased in Q3 2022. There was likely an increased threat from smishing attacks targeting employees, either directly or via enterprise third-party providers, and customers.[1,2] Analysis indicates an increased threat of callback phishing (vishing), adding legitimacy to malicious emails by impersonating security teams and encouraging victims to return a phone call to authenticate fraudulent activity.[3] Threat actors increasingly leveraged techniques to bypass MFA, including Adversary-in-the-Middle (AiTM) now incorporated into broader Phishing-as-a-Service (PhaaS) offerings.

Threat actors continued to leverage topical lures to entice engagement with malicious emails. Threat actors targeted customers by impersonating retailers and leveraging rudimentary phishing emails, text messages, and voice calls, typically for financial gain.[4] ZeroFox Intelligence anticipates an increased threat to retail customers leading up to Black Friday and the holidays, which will likely see a higher volume of impersonation scams for financial gain.

Malicious email attachments and job scams remained a prominent means of distributing malware against retail targets.[5,6] Impersonating phishing domains and open redirects should be continually monitored and taken down to avoid customers being defrauded, as they provide an intrusion vector for threat actors.

› Forward Look:

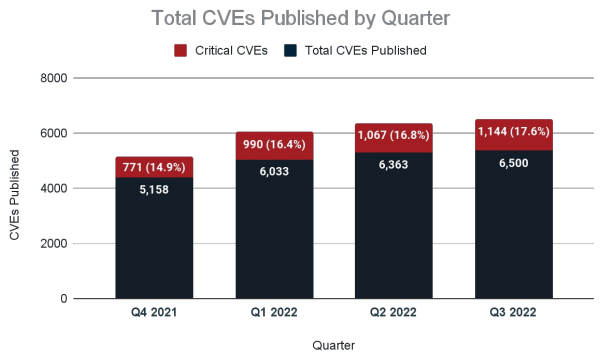
- Smishing attacks against retail organizations' employees and customers are likely to continue on an upward trajectory.
- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.
- Retail customers are likely to be increasingly targeted with social engineering scams in Q4 2022, particularly in light of the volume of attacks surrounding Black Friday and the holidays.

› Recommendations:

- Communicate to employees emerging trends in social engineering scams and how to conduct authentication safely.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand the threat posed to your organization.

No notable change in threat from previous quarter

Indication of increase in threat from previous quarter



Source: hXXps://nvd.nist[.]gov

VULNERABILITY EXPLOITATION

Vulnerability exploitation in Q3 2022 continued to focus on exploits in commonly-used software modules and network perimeter infrastructure. Widely-used e-commerce platforms continued to be leveraged in attacks against the retail sector, including a campaign leveraging a critical vulnerability in Magento despite security updates being released in February 2022.[7,8] Sustained periods of high-vulnerability disclosures place strain on out-of-cycle patch management processes, with new disclosures in Q3 2022 Apple operating systems, Atlassian Confluence, Google, Microsoft Windows and Exchange, and Whatsapp.[9] Critical vulnerabilities in Zoho ManageEngine and Zimbra email servers were added to CISA's Known Exploited Vulnerabilities (KEV) catalog in Q3 2022, of which multiple retail organizations are stated to be customers.[10]

› Forward Look:

- Vulnerabilities in commonly-used software modules and network perimeter infrastructure will likely continue to dominate the exploit landscape.

› Recommendations:

- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Ensure a thorough understanding of your technology stack and patching schedule, as well as those of operating partners.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.

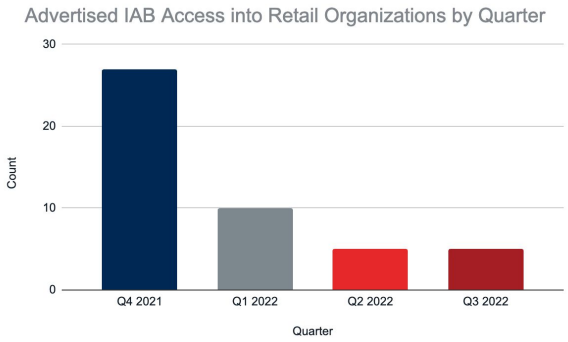
FOOTNOTES

[1] hXXps://www.securityweek[.]com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations
[2] hXXps://news.trendmicro[.]com/2022/08/26/usps-bank-of-america-amazon-netflix-home-depot-cvs-pharmacy-labor-day-fanatics-phishing-scams/
[3] hXXps://threatpost[.]com/callback-phishing-security-firms/180182/
[4] hXXps://news.trendmicro[.]com/2022/09/23/when-we-were-young-scam-amazon-paypal-irs-ray-ban-phishing/
[5] hXXps://thehackernews[.]com/2022/07/researchers-uncover-new-attempts-by.html
[6] hXXps://www.bleepingcomputer[.]com/news/security/hackers-trojanize-putty-ssh-client-to-backdoor-media-company/
[7] hXXps://www.bleepingcomputer[.]com/news/security/critical-magento-vulnerability-targeted-in-new-surge-of-attacks/
[8] hXXps://thehackernews[.]com/2022/07/hackers-exploit-prestashop-zero-day-to.html
[9] hXXps://nvd.nist[.]gov
[10] hXXps://www.cisa[.]gov/known-exploited-vulnerabilities-catalog

©2022 ZeroFox, Inc. All rights reserved. All other trademarks are property of their respective owners.

INITIAL ACCESS BROKERS (IABs)

A shift towards brokers making sales in private channels likely drove the fall in the number of posts in open forums advertising illicit access into retail organizations in Q3 2022, judging from threat actor chatter observed by ZeroFox Intelligence. This is not necessarily indicative of a reduction in threat, as IABs are prefering to sell to well-established buyers out of an abundance of caution to avoid law enforcement scrutiny and unwanted attention. Access to retailers based in the United States and western Europe in particular is becoming increasingly rare in open channels.[11] It is likely retail organizations will face an increased threat from illicit access sold into third-party service and software providers.[12]



Source: ZeroFox Intelligence

› Forward Look:

- Illicit access to large retail entities will likely increasingly be sold via private or direct communication methods.
- Retail organizations may be increasingly targeted via access sold into third-party vendors.

› Recommendations:

- Employ ZeroFox's Threat Intelligence Feeds to get ahead of threat actor activity.
- Proactively monitor for potential network access sales to obtain critical early warnings of impending cyberattacks.

No notable change in threat from previous quarter

BOTNETS

The threat to retail organizations from botnets in Q3 2022 remained broadly consistent with previous quarters. The greatest threat to the sector comes from harvested credentials; this quarter ZeroFox Intelligence ingested almost 45 million credentials harvested by infostealer families commonly deployed by botnets, of which RedLine was most active.[18] Retail organizations likely face a comparably lower threat of being targeted by politically-motivated Distributed Denial-of-Service (DDoS) attacks than other sectors, though will likely continue to face a high threat of devices on their networks being remotely controlled for use in botnet attacks against other entities.[19,20] Emotet's continued resurgence should be of increasing concern to retail organizations; it has indiscriminately infected almost 1.3 million devices across multiple industries since the start of 2022 and is now pushing Quantum and BlackCat ransomware.[21]

› Forward Look:

- Retail organizations will likely be less affected by botnet targeting by Russia-aligned entities.
- Emotet is expected to pose an increasing threat to retail organizations in the coming months.

› Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains and Compromised Account Credentials.

No notable change in threat from previous quarter

MALWARE

Malware deployment against the retail sector remained high in Q3 2022, but ZeroFox Intelligence observed no notable change in threat. E-skimmers and supply chain attacks continued to be deployed against payment systems, with attacks this quarter enabling threat actors to infect multiple downstream users and siphon payment information of thousands of victims.[13,14] Fraudulent apps on app stores remained one of the most prolific means of distributing malware to retail customers.[15,16] Low barriers to entry and the pace of trojan updates continued to sustain a high threat.[17] Security teams should note a likely increased threat from popular loaders, with Bumblebee and ChromeLoader deploying some of the most capable malware strains available.

› Forward Look:

- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.
- The retail sector will likely face an increased threat from malicious browser extensions targeting e-commerce sites.

› Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.

No notable change in threat from previous quarter

FOOTNOTES

[11] ZeroFox Intelligence Internal Collections
[12] hXXps://techcrunch[.]com/2022/08/01/wiseasy-android-payment-passwords/
[13] hXXps://www.bleepingcomputer[.]com/news/security/hackers-breach-software-vendor-for-magento-supply-chain-attacks/
[14] hXXps://www.securityweek[.]com/hundreds-ecommerce-domains-infected-google-tag-manager-based-skimmers
[15] hXXps://www.bleepingcomputer[.]com/news/security/adware-on-google-play-and-apple-store-installed-13-million-times/
[16] hXXps://www.securityweek[.]com/14-million-users-install-chrome-extensions-inject-code-ecommerce-sites
[17] hXXps://heimdalsecurity[.]com/blog/a-new-and-upgraded-version-of-sharkbot-malware-has-been-detected/
[18] ZeroFox Intelligence Internal Collections
[19] hXXps://www.reuters[.]com/world/asia-pacific/taiwan-defence-ministry-website-hit-by-cyber-attacks-amid-china-tensions-2022-08-04/
[20] hXXps://nsm[.]no/aktuelt/malrettede-tjenestenektangrep-mot-norske-nettsteder
[21] hXXps://www.advintel[.]io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022

©2022 ZeroFox, Inc. All rights reserved. All other trademarks are property of their respective owners.

RANSOMWARE

The retail sector likely saw a slight reduction in the overall threat from ransomware and digital extortion in Q3 2022. While the industry remained one of the most frequently targeted, extortion attempts remained below 2021 levels, likely caused in part by difficulty eliciting payments from victims.[22] ZeroFox Intelligence identified fewer attacks against "big game" retail targets, with recorded incidents targeting the sector highlighting the threat of attacks against retail supply chains.[23,24] The supply chain risk is compounded by developments in extortion tactics, with ALPHV/BlackCat providing leaked victim data in a searchable format.[25] While not a novel tactic, LockBit announced a move towards conducting DDoS attacks against victims as a pressure tactic, which may see other groups adopt similar methods.[26] The updating of exfiltration tool Exmatter with data corruption functionality indicates a possible move towards ransomware gangs destroying data rather than encrypting it, using the exfiltrated copies as the means of recovering data.

LockBit remained the sector's primary digital extortion threat and was responsible for nearly one-third of all attacks. Black Basta, flagged in Q2 2022 as an emerging actor, continued its upward trajectory. Security teams should be wary of updated versions of strains that frequently target the sector and their associated IOCs, including Hive, as well as the unusually high number of new ransomware strains identified this quarter.[27]

In coming months, there is an even chance ransomware and digital extortion attacks against the retail sector will increase, particularly leading up to Black Friday and the holidays. Threat actors may perceive that disruption to retailers' operations at such a critical time may make them more likely to pay extortion demands.

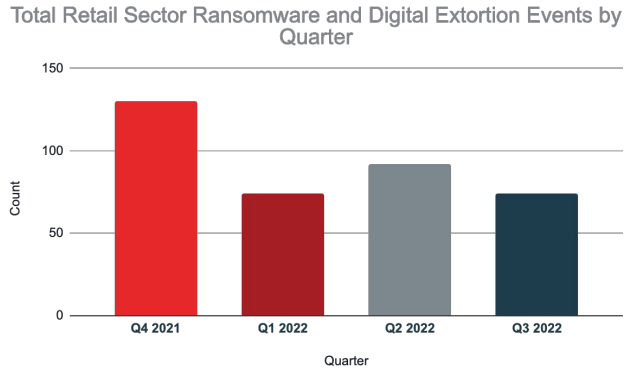
› Forward Look:

- ZeroFox Intelligence anticipates the threat of digital extortion to retail organizations will most likely increase.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational damage, and legal ramifications.

› Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.
- Should an organization be impacted by a ransomware event, engage ZeroFox Intelligence for support.

Indication of decrease in threat from previous quarter



Source: ZeroFox Intelligence

QUARTERLY SPOTLIGHT

Organizations must adapt their approach to security as threat actors pivot to circumvent or intercept MFA. Weak MFA methods such as SMS verification codes have long been exploited by threat actors to compromise enterprise systems. However, analysis indicates an increase in recent months of threat actors leveraging phishing techniques where traditionally-strong MFA gives little or no protection. These techniques include AiTM phishing, MFA fatigue or spamming—as encouraged by Lapsus$—and OAuth Consent phishing attempts and are now baked into widely-distributed phishing kits.

Phishing-resistant MFA attempts to limit a corporation's risk of social engineering attacks and should be implemented in conjunction with a broader Zero Trust initiative.

ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online Version 2.0 (FIDO2) and certificate-based authentication.[28] FIDO2 aims to maximize security while minimally impacting user experience. It supports passwordless, second-factor, and multi-factor user authentication with embedded or external authenticators. All FIDO protocols are based on Public Key Infrastructure.

While phishing-resistant MFA will not protect against all attacks, ZeroFox Intelligence has yet to observe threat actors on the deep or dark web publishing or brokering exploits related to phishing-resistant MFA.[29]

FOOTNOTES

[22] ZeroFox Intelligence Internal Collections
[23] *Ibid.*
[24] hXXps://www.bleepingcomputer[.]com/news/security/7-eleven-denmark-confirms-ransomware-attack-behind-store-closures/
[25] hXXps://blog.cyble[.]com/2022/07/06/alphv-ransomware-expands-its-arsenal-of-extortion-techniques/
[26] hXXps://www.itworldcanada[.]com/article/lockbit-ransomware-gang-adding-ddos-attacks-to-its-threats/500301
[27] Lilith, Cheers, Yanluowang, 0mega, RedAlert and BianLian, Royal, Monster, Agenda, PlayCrypt
[28] ZeroFox Intelligence identified an academic paper that describes a potential weakness in FIDO UAF that could allow threat actors to bypass verification if they have a malware implant.
[29] hXXps://fidoalliance[.]org/specifications/

©2022 ZeroFox, Inc. All rights reserved. All other trademarks are property of their respective owners.

OUTLOOK

ZeroFox Intelligence assesses the threat to the retail sector will likely increase next quarter, with the landscape more greatly impacted by seasonal trends than other sectors. Threat increases will most likely come from social engineering attempts against employees or customers and digital extortion attempts. It is likely either a swift resolution to Russia's war in Ukraine or a rapid downturn in global economic conditions could catalyze changes to the nature of the threat.

ZeroFox Intelligence anticipates a Q4 2022 increase in the volume of social engineering scams targeting the retail sector. Social engineering scams will likely increase in volume in coming months but are unlikely to change significantly in approach. The majority will involve rudimentary phishing attempts targeting organizations' customers by impersonating trusted parties, particularly in the run-up to Black Friday and the winter holidays. ZeroFox Intelligence also anticipates a continued upward trend of threat actors leveraging tactics to bypass MFA to compromise corporate environments, as well as increased targeting of authentication providers.

There is an even chance ransomware and digital extortion attacks against the retail sector will increase in Q4 2022. Threat actors may perceive that disruption to retailers' operations during a critical seasonal period may make them more likely to pay extortion demands. This could also include ransom DDoS attacks in which threat actors render retailers' websites inoperable until payment is made.

ZeroFox Intelligence anticipates a continued increase in IABs leveraging both private means of communication to sell access and trusted relationships with specific buyers. There is no indication the threat will decrease, with buyers still seeking to obtain access via brokers. However, the ability to identify and mitigate access sales ahead of compromise will very likely become increasingly challenging, amplifying the importance of partnerships with third-party security vendors that have access to private channels.

ZEROFOX INTELLIGENCE

October 25, 2022

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP:RED

HOW IT IS USED

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP:AMBER

HOW IT IS USED

Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that TLP:AMBER+STRICT restricts sharing to the organization only.

TLP:GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP:CLEAR

HOW IT IS USED

Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready To See For Yourself?

› Request a Demo:
Sign up on zerofox.com/request-a-demo

› Learn More:
Visit zerofox.com
Contact us at sales@zerofox.com / 855.736.1400

©2022 ZeroFox, Inc. All rights reserved. All other trademarks are property of their respective owners.