

Q2 Retail Sector

Quarterly Threat Landscape Scorecard

TLP: WHITE S-2022-07-29a



Q2 2022 Retail Sector Threat Overview

Threat actors continued to exchange ideas on how to maneuver within the economic and political constraints brought on by the conflict in Ukraine. Social engineering campaigns remained a persistent threat to retail organizations, including increased use of fraudulent applications, fake Windows 11 upgrades, and employment related scams to steal credentials and deploy trojans. Vulnerability exploitation also continued to grow, averaging almost 70 CVEs disclosed per day, up from 56 per day at the end of 2021. The pace of vulnerability disclosure likely represents a new normal. The threat to the retail sector from Initial Access Brokers continued to fall in Q2, despite the market showing signs of resurgence in other sectors. The threat to retail organizations from ransomware and digital extortion likely slightly increased. Ransomware threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics. While the ongoing war in Ukraine continued to be the primary driver of geopolitical risk, possible EU and NATO expansion - and new sanctions on Russia - will likely trigger Russia state-backed groups to target high profile entities.

Key Cyber Threats to the Retail Sector in Q2 2022

	State-linked and financially motivated threat actors targeting key personnel in job-related scams		Malware disguised in fake banking and finance-related applications targeting customers
	Vulnerabilities in third party software used by retail organizations, and the pace of exploitation		Saturated Infostealer and banking trojan markets, with releases of new strains and old strains updating capabilities
	Russia-backed and aligned threat actors targeting high profile retail entities		More stealthy skimmers targeting e-stores and payment systems
	Ransomware and digital extortion outfits conducting high profile attacks against the retail sector		Changes to extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications

Retail Sector Threats

Categories	Q1 2022	Q2 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

> Q2 Key Findings:

- Cybercriminals are increasingly concerned with challenges converting cryptocurrency to fiat currency
- Social engineering campaigns increasingly used LNK shortcut files, fake Windows upgrades, and employment scams.
- The threat from Common Vulnerabilities and Exposures and previously unknown software vulnerabilities likely increased.
- The threat from IABs continued to fall in Q2, despite the IAB market showing signs of resurgence in threat to other sectors.
- There was a negligible change in the threat from botnets, despite widespread media attention
- The threat to retail organizations from ransomware and digital extortion likely slightly increased. Eliciting payment from victims may be getting more difficult.

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 5:00 PM (EDT) on July 28, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



SOCIAL ENGINEERING

Social engineering campaigns continued to leverage malicious email attachments to target retail organizations and their customers, with increased use of .LNK files. ZeroFox Intelligence observed an increase in fraudulent applications, fake Windows 11 upgrades and employment related scams to deploy trojans and infostealers.

Forward Look:

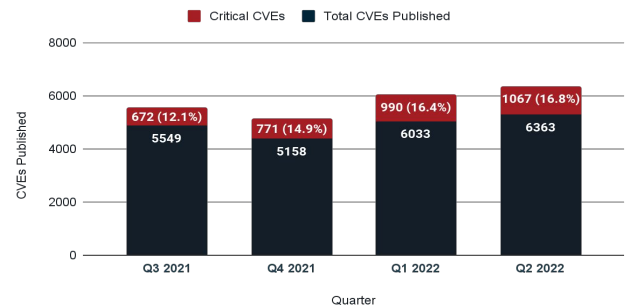
- Fake applications will increasingly be used to target customers.
- Malicious email attachments will continue to be used to disseminate malware.
- Job-related scams will target desirable employees at a high pace, particularly those with elevated access levels.

Recommendations:

- Communicate what legitimate job postings look like to get ahead of fake offers.
- Engage the ZeroFox Intelligence Team to conduct an Attack Surface Assessment to understand the threat posed to you.

No notable change in threat from previous quarter

Total CVEs Published by Quarter



Source: [hXXps://nvd.nist.gov](https://nvd.nist.gov)

VULNERABILITY EXPLOITATION

Retail organizations faced an unprecedented threat from disclosed vulnerabilities, particularly in cloud and network perimeter infrastructure—including routers, firewalls, and commonly-used software modules. The importance of efficient patching was exacerbated by widespread reporting of vulnerabilities, enabling threat actors to rapidly target vulnerable systems.

Forward Look:

- Vulnerabilities in the cloud and network perimeter infrastructure will likely continue to dominate the exploit landscape.
- The scale and pace of exploit disclosures likely represent a new normal for the vulnerability landscape.

Recommendations:

- Utilize ZeroFox platform's Intelligence Search interface to investigate Vulnerabilities and associated Exploits.
- Ensure a thorough understanding of the technology stack and patching schedule, as well as those of operating partners.

Indication of increase in threat from previous quarter

INITIAL ACCESS BROKERS (IABs)

The threat to the retail sector from IABs continued to fall in Q2, despite the IAB market showing signs of resurgence in threat to other sectors. Adverts focused on entities participating in high-profile events. Threats often trend against particular industries for a period of time before moving on and spiking against others. Disruption to IAB operations is keeping supply below 2021 levels.

Forward Look:

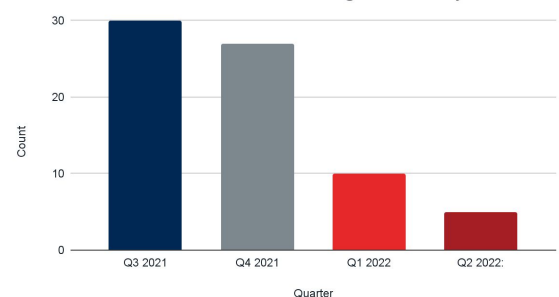
- The threat to retail from IABs will likely increase given strong demand from buyers and disruption to IABs' operations is likely temporary.
- Threat actors may be pushed increasingly to more private means to sell illicit access, making identifying activity more difficult.

Recommendations:

- Utilize 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 an impending cyberattacks.

Indication of decrease in threat from previous quarter

Advertised IAB Access into Retail Organizations by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

[hXXps://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/](https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/)
[hXXps://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information](https://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information)
[hXXps://www.infosecurity-magazine.com/news/linkedin-impersonated-brand/](https://www.infosecurity-magazine.com/news/linkedin-impersonated-brand/)
[hXXps://nvd.nist.gov](https://nvd.nist.gov)
 ZeroFox Intelligence Internal Collections



BOTNETS

Most organizations around the world saw a negligible change in the threat from botnets in Q2 2022. Russia-aligned groups began targeting entities that vocally opposed the war in Ukraine with botnet attacks, though not at the scale or breadth expected. Botnets deploying info stealers continued to pose a high threat to retail organizations. Retail organizations should note Emotet's resurgence which, at its peak, was one of the largest and most capable botnets in history.

Forward Look:

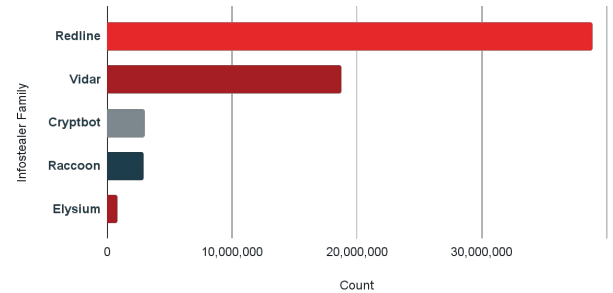
- Botnets leveraged by Russia-aligned entities could exacerbate geopolitical tensions.
- The continued resurgence of Emotet indicates it may pose a significant threat to retail organizations in the coming months.

Recommendations:

- Utilize the ZeroFox platform's Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains and Compromised Account Credentials. Proactive monitoring of botnet logs may give a critical early warning of an impending cyberattack.

No notable change in threat from previous quarter

Q2 2022: Credentials Ingested from Information Stealer Families Commonly Used by Botnets



Source: ZeroFox Intelligence

MALWARE

The threat from malware deployment across the landscape remained high in Q2 2022. The threat to retail organizations was underpinned by the high rate of new trojans emerging and older trojans launching new campaigns. The most capable skimming operations are attacking fewer targets but employing more advanced techniques to obfuscate malicious code.

Forward Look:

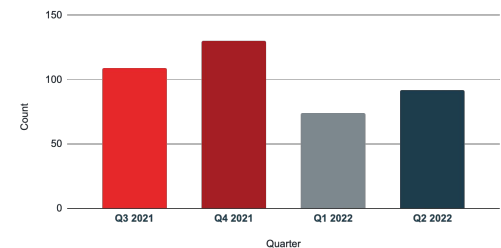
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors and drive down the price of acquiring highly-capable malware.
- Rapid modification to trojans to exploit newly disclosed vulnerabilities will place increased importance on having a robust patching program.

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

Total Retail Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

RANSOMWARE

The threat to the retail sector from ransomware and digital extortion likely slightly increased in Q2 2022, with a higher frequency of attacks and threat actors demonstrating greater capability than in attacks that took place in Q1 2022. This increase was not seen across all sectors. Threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics.

Forward Look:

- ZeroFox Intelligence anticipates the threat to the retail sector will most likely continue to 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 increase in threat from previous quarter

FOOTNOTES

[hXXps://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/](https://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/)
[hXXps://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/](https://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/)
[hXXps://securityaffairs.co/wordpress/131705/malware/ermac-2-0-android-banking-trojan.html](https://securityaffairs.co/wordpress/131705/malware/ermac-2-0-android-banking-trojan.html)
[hXXps://www.bleepingcomputer.com/news/security/microsoft-credit-card-stealers-are-getting-much-stealthier/](https://www.bleepingcomputer.com/news/security/microsoft-credit-card-stealers-are-getting-much-stealthier/)
[hXXps://www.crn.com/news/security/mandiant-no-evidence-of-lockbit-2-0-ransomware-attack-at-this-point-](https://www.crn.com/news/security/mandiant-no-evidence-of-lockbit-2-0-ransomware-attack-at-this-point-)



QUARTERLY SPOTLIGHT

In Russian-language Deep and Dark Web forums, concerns center around the fate of cryptocurrency funds and strategies to exchange them for fiat currency. They also perceive that only cryptocurrencies can be sent or wired to Russia for financial support. Cyber actors will pivot and adapt in near real-time to offset temporary disruptions to their financial gains. They will likely rely on institutions in geopolitically indifferent or supportive countries. They will continue to seek methods that use stable financial institutions. Once they exchange rubles for cryptocurrency, they will look to convert digital currency into hard currency—most likely U.S. dollars—that can be offshored to non-Russian banks.

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 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.

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 NOT share TLP:
AMBER information with members of their own organization and only as widely as necessary to act on that information.

TLP : GREEN

HOW IT IS USED

Sources may use TLP:
GREEN 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:
GREEN 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.

TLP : WHITE

HOW IT IS USED

Sources may use TLP:
WHITE 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 NOT share TLP:
WHITE information with members of their own organization and only as widely as necessary to act on that information.

OUTLOOK

Russia's invasion of Ukraine will likely continue to heavily influence the cyber threat landscape. The conflict and the resulting humanitarian and economic crises will almost certainly continue to be leveraged by threat actors in social engineering scam lures. Vulnerabilities in cloud infrastructures, perimeter security devices, and commonly-used software modules will likely continue to dominate the exploit landscape. ZeroFox Intelligence anticipates pro-Russian threat actors and state-linked entities will likely increasingly target countries and organizations with malware in retaliation for perceived stances taken during the war. If ransomware operators struggle to elicit payments from victims, it is likely they will resort to more extreme pressure tactics, attempting to cause greater operational downtime, reputational damage, and even legal ramifications.

ZEROFOX INTELLIGENCE
July 22, 2022

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

