2023

Q2 Financial Sector

Quarterly Threat Landscape Scorecard

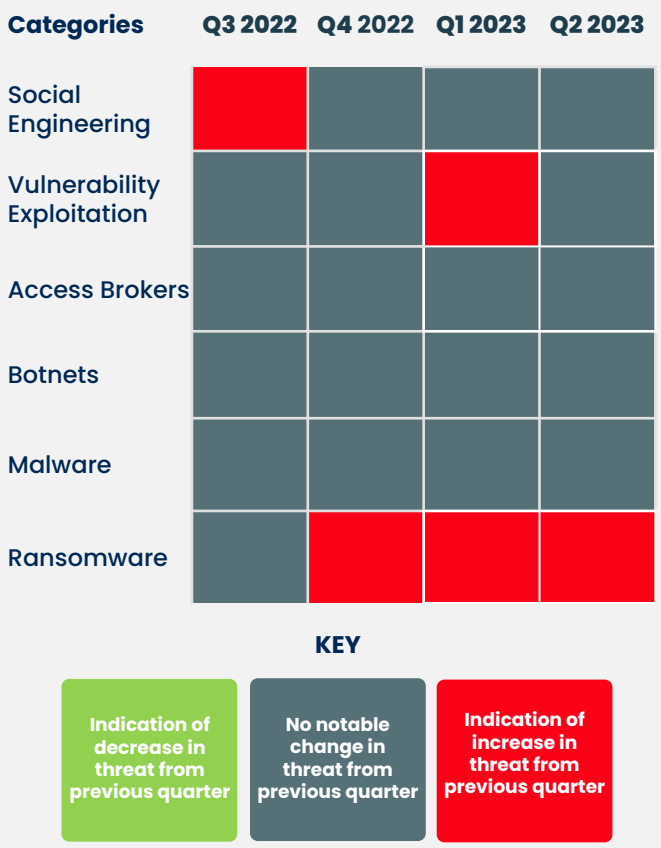
TLP:CLEAR A-2023-09-01a

ZEROFOX Intelligence

Key Findings Q2 Financial Sector

- The threat to financial organizations from ransomware and digital extortion (R&DE) very likely increased in Q2 2023, reaching the highest levels since 2021.
- Financial organizations faced a high threat of nefarious actors exploiting Common Vulnerabilities and Exposures (CVEs). Clop's successful May 2023 exploitation of CVE-2023-34362, a zero-day exploit in MOVEit file transfer software, demonstrated the potential impact these CVEs can have; approximately 16 percent of identified victims are in the finance industry.
- While Russia-aligned threat actors continued to target North American and European financial organizations with Distributed Denial of Service (DDoS) attacks, the impact of the attacks remained limited, typically rendering websites unusable for a short period of time.
- Search Engine Optimization (SEO) poisoning and leveraging of malicious Google ads to disseminate malware continued on an upward trajectory.
- Malware-as-a-service offerings sustained low barriers to entry for threat actors seeking to target financial sector entities.
- E-skimmer campaigns remained a persistent threat and were successfully leveraged to siphon banking customers' payment information.
- Illicit access to financial organizations advertised in open forums remained low in Q2 2023, with brokers continuing to leverage private channels for selling to well-established buyers.

Financial Sector Threats



Key Cyber Threats to the Financial Sector in Q2 2023

- Ransomware and digital extortion outfits conducting high-profile attacks against the financial sector
- Changes to digital extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications
- Malware disguised in fake banking and finance-related applications targeting customers
- Infostealer and trojan markets sustaining low barriers to entry and enabling easy theft of employee and customer credentials
- Threats from spear-phishing, smishing, vishing and techniques to bypass multi-factor authentication (MFA)
- Threat actors' stealthy skimmers targeting e-stores and payment systems
- Vulnerabilities in third-party software used by financial organizations
- Russia-backed and aligned threat actors seeking to target financial entities

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 July 10, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

ZEROFOX Intelligence

SOCIAL ENGINEERING

The threat to the financial sector from social engineering remained high in Q2 2023, with spear-phishing, smishing, and telephone-oriented attack delivery remaining prevalent. Threat actors leveraged topical lures, such as the end of the tax year, in financially-motivated campaigns.[1] Malicious apps and fraudulent app updates continued to be used to disseminate malware, posing a significant risk for financial organizations that have employees that sync personal devices with corporate networks.[2,3] There was continued variation in the use of attachment types in phishing emails, with threat actors increasingly turning to less traditional file types such as OneNote, restricted permission messages (RPMSG), and Windows Script.[4,5] Search Engine Optimization (SEO) poisoning continued on an upward trajectory, alongside the use of campaigns leveraging Google advertisements promoting popular software as a means of distributing and delivering malware.[6,7]

› Forward Look:

- ZeroFox Intelligence anticipates an increase in SEO poisoning and use of malicious Google ads as a means of distributing and delivering malware.

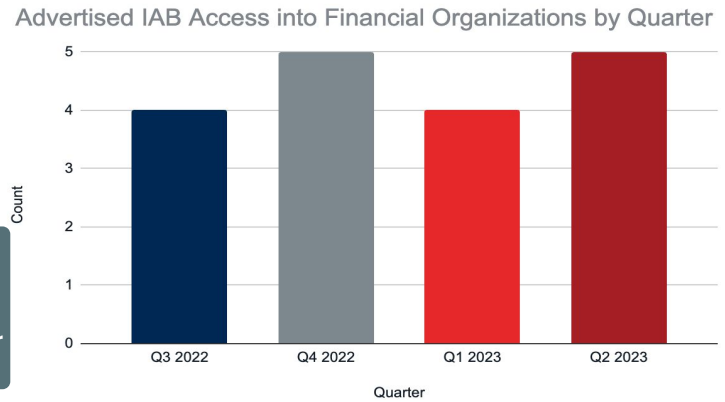
› Recommendations:

- Leverage ZeroFox to conduct ongoing monitoring for impersonating domains and provide alerts and support for mitigation.

No notable change in threat from previous quarter

INITIAL ACCESS BROKERS

There was likely little change in threat from nefarious actors advertising access into financial sector organizations in deep and dark web forums in Q2 2023, with posts remaining infrequent; this bucked an overall upward trend seen in most other sectors. Initial Access Brokers (IABs) likely continued leveraging private communication channels to sell directly to trusted buyers, including ransomware operators, with illicit access to large, Western, or European financial entities proving increasingly rare. Ad content continued to center around vulnerabilities in Virtual Private Networks, Remote Desktop Protocol, and broader remote working infrastructure.



Source: ZeroFox Intelligence

› Forward Look:

- The threat to the financial sector from IABs is expected to increase in coming quarters.
- IABs will continue to increasingly leverage private communication channels to give first refusal to established buyers.

› Recommendations:

- Proactively monitor for IAB operators advertising access to organizations directly, as well as to partners and suppliers.
- Subscribe to the ZeroFox Advanced Web Search and Dark Ops Curated Intelligence for early warnings and indicators of threat actor chatter.

No notable change in threat from previous quarter

VULNERABILITY EXPLOITATION

The threat of nefarious actors exploiting CVEs very likely remained high in Q2 2023. The Cybersecurity and Infrastructure Security Agency's (CISA) updates to its Known Exploited Vulnerabilities (KEV) catalog have included critical severity vulnerabilities that almost certainly impact finance, including exploits impacting iOS systems, Google Chrome, and Barracuda Email Security products.[8,9] Finance organizations were frequently impacted in attacks against third-party service providers. Clop's successful May 2023 exploitation of CVE-2023-34362, a zero-day exploit in MOVEit file transfer software, demonstrated the potential impact these CVEs can have; approximately 16 percent of identified victims are in the finance industry.[10]

› Forward Look:

- Vulnerabilities in commonly-used software modules and remote working infrastructure will very likely continue to dominate the exploit landscape.

› Recommendations:

- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.

No notable change in threat from previous quarter

FOOTNOTES

[1] hXXps://www.bleepingcomputer[.]com/news/security/irs-authorized-efilecom-tax-return-software-caught-serving-js-malware/
[2] hXXps://www.bleepingcomputer[.]com/news/security/new-android-fluhorse-malware-steals-your-passwords-2fa-codes/
[3] hXXps://www.bleepingcomputer[.]com/news/security/fake-in-browser-windows-updates-push-aurora-info-stealer-malware/
[4] hXXps://www.bleepingcomputer[.]com/news/security/microsoft-365-phishing-attacks-use-encrypted-rpmsg-messages/
[5] hXXps://thehackernews[.]com/2023/04/new-qbot-banking-trojan-campaign.html
[6] hXXps://www.bleepingcomputer[.]com/news/security/google-ads-push-bumblebee-malware-used-by-ransomware-gangs/
[7] hXXps://www.bleepingcomputer[.]com/news/security/romcom-malware-spread-via-google-ads-for-chatgpt-gimp-more/
[8] hXXps://nvd.nist[.]gov
[9] hXXps://www.cisa[.]gov/known-exploited-vulnerabilities-catalog
[10] ZeroFox Intelligence internal Collections

Q2 Financial Sector

Quarterly Threat Landscape Scorecard

TLP:CLEAR A-2023-09-01a

ZEROFOX Intelligence

BOTNETS

The threat to financial organizations from botnets remained broadly consistent in Q2 2023, continuing to pose a threat via stealing credentials and remotely-controlling infected devices. ZeroFox Intelligence ingested over 150 million credentials harvested by infostealer families commonly deployed by botnets, of which Raccoon was most active.[11] While frequent, the impact of DDoS attacks against the financial sector remained limited, typically rendering websites unusable for a short period of time. European and North American financial organizations continued to face the highest threat from DDoS attacks, particularly from Russia-aligned groups.

› Forward Look:

- The threat to most financial organizations from botnets is unlikely to change considerably in the near term.
- Russia-aligned threat actors' DDoS attacks against financial institutions will likely continue to have limited impact.

› Recommendations:

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

No notable change in threat from previous quarter

MALWARE

The threat to the financial sector from malware deployment very likely remained high. ZeroFox Intelligence continued to see a high prevalence of infostealer modules—often incorporated into broader trojans—facilitating data breaches and cyber espionage. In Q2 2023, prolific threat actors updated well-established strains such as Qbot, and launched new strains, including threat actors with a history of targeting the sector.[12,13] Dissemination of powerful loaders designed to facilitate the deployment of follow-on malicious payloads remained high.[14,15] App stores continued to be one of the most prolific means of distributing malware, with mobile malware remaining a considerable threat to financial sector customers.[16] E-skimmer campaigns remained a persistent threat and were successfully leveraged to siphon banking customers' payment information.[17]

› Forward Look:

- The malware threat to the financial sector is unlikely to change significantly in the short term.
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.

› Recommendations:

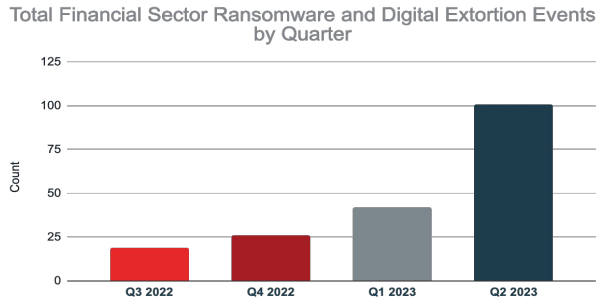
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to malware.

No notable change in threat from previous quarter

RANSOMWARE & DIGITAL EXTORTION

The threat to financial organizations from R&DE very likely increased in Q2 2023, reaching the highest levels since 2021.[18] While the number of R&DE incidents increased more than 50 percent across the landscape, the rise in the number of incidents impacting the financial sector was disproportionately up more than 140 percent. This increase was very likely underpinned by threat actors' successful exploitation of commonly-used software modules, such Clop's successful leveraging of a vulnerability in the MOVEit file transfer software.[19,20] Financial sector organizations face a heightened risk of being implicated in attacks against third-party providers; those based in North America remained the most frequently targeted by R&DE, with entities in Europe and APAC also seeing an elevated level of threat.

The increased threat to the sector is underpinned by greater deployment of well-established strains, including LockBit and ALPHV, as well as increasingly prominent strains, such as 8Base and Akira. In Q2 2023, ZeroFox Intelligence saw an increase in attacks from less-established threat collectives. 8Base—increasing its activity in Q2 2023—established itself as one of the most prominent threats to the sector. The strain predominantly targets small-to-medium sized businesses, with the financial sector remaining one of its primary targets.



Source: ZeroFox Intelligence

› Forward Look:

- R&DE attacks against the sector will likely fall in Q3 2023 but are anticipated to remain above 2022 levels.
- There is likely to be continued evolution of pressure tactics, as seen recently with Clop publishing stolen victim data on surface web domains.

› Recommendations:

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

Indication of increase in threat from previous quarter

FOOTNOTES

[11] ZeroFox Intelligence Internal Collections
[12] hXXps://thehackernews[.]com/2023/04/new-qbot-banking-trojan-campaign.html
[13] hXXps://www.bleepingcomputer[.]com/news/security/ex-conti-members-and-fin7-devs-team-up-to-push-new-domino-malware/
[14] hXXps://cyberwarzone[.]com/batloader-malware-dropper-continues-to-pose-a-threat-to-organizations-in-2023/?web_view=true
[15] hXXps://www.bleepingcomputer[.]com/news/security/new-pindos-javascript-dropper-deploys-bumblebee-icedid-malware/
[16] hXXps://www.bleepingcomputer[.]com/news/security/anatsa-android-trojan-now-steals-banking-info-from-users-in-us-uk/
[17] hXXps://www.bleepingcomputer[.]com/news/security/hackers-hijack-legitimate-sites-to-host-credit-card-stealer-scripts/
[18] ZeroFox Intelligence Internal Collections
[19] ZeroFox Intelligence Flash Report - Reports of Active Exploitation of MOVEit Transfer SQL Zero-Day Vulnerability, June 2, 2023
[20] ZeroFox Intelligence Flash Report - Clop Ransomware Collective Targets New Victims Across Multiple Sectors, June 15, 2023

OUTLOOK

ZeroFox Intelligence anticipates the R&DE threat to the financial sector will likely fall in Q3 2023, but it is expected to remain above 2022 levels.

Illicit access to Western financial sector entities posted in open forums will likely remain infrequent. However, the overall threat is expected to increase in coming quarters.

ZeroFox Intelligence anticipates little change to the social engineering threat to financial organizations in Q3 2023. SEO poisoning and the leveraging of malicious Google advertisements to disseminate malware will likely continue on an upward trajectory.

Financial organizations will very likely face a high threat of nefarious actors exploiting zero-days and CVEs in Q3 2023, with the proportion of disclosed vulnerabilities rated critical on an overall upward trajectory. Zero-day vulnerabilities in file transfer software will very likely remain an attractive target for threat actors, given the demonstrable success threat actors have had in Q1 and Q2 2023.

ZEROFOX Intelligence

September 1, 2023

APPENDIX A: ZEROFOX INTELLIGENCE PROBABILITY SCALE

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B: 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