

## Key Findings Q1 Financial Sector

- Financial organizations likely faced an increased threat of nefarious actors exploiting Common Vulnerabilities and Exposures (CVEs). Clop’s successful exploitation of CVE-2023-0669, a zero-day exploit in GoAnywhere MFT file transfer software, resulted in the most incidents in a single month by any extortion collective in ZeroFox Intelligence records. Financial sector organizations accounted for approximately 10 percent of victims.
- The threat to both employees and customers from smishing and callback phishing (vishing) remained high.
- The threat from ransomware and digital extortion very likely increased in Q1 2023, with incidents against financial sector targets reaching the highest levels since 2021.
- The overall threat to financial sector entities from botnets remained broadly consistent in Q1 2023. While European financial organizations likely faced an increased threat from Russia-aligned Distributed Denial of Service (DDoS) attacks, the impact of such attacks continued to be limited.
- Malware-as-a-service offerings sustained low barriers to entry for threat actors seeking to target financial sector entities.

## Financial Sector Threats

| Categories                 | Q2 2022 | Q3 2022 | Q4 2022 | Q1 2023 |
|----------------------------|---------|---------|---------|---------|
| Social Engineering         |         |         |         |         |
| Vulnerability Exploitation |         |         |         |         |
| 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

## Key Cyber Threats to the Financial Sector in Q1 2023



Vulnerabilities in commonly-used software modules used by financial organizations leveraged to compromise multiple downstream industry targets.



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.



Russia-backed and aligned threat actors seeking to target financial entities.



High threats from SMS-phishing, callback phishing, and techniques to bypass Multi-Factor Authentication.



Ransomware and digital extortion outfits conducting high-profile attacks against the financial sector.



Initial Access Brokers (IABs) selling illicit access to established buyers via private means of communication, making identification and mitigation more difficult.



Threat actors’ stealthy skimmers targeting e-stores and payment systems.



## SOCIAL ENGINEERING

ZeroFox Intelligence observed no significant change in the threat to the financial sector from social engineering campaigns in Q1 2023. Financially and politically-motivated actors conducted successful attacks against the sector, including leveraging phishing domains, smishing, and telephone-oriented attack delivery campaigns to target both employees and customers.[1,2] Employment-related scams remained widespread as a means to deploy malware to sector employees, and threat actors also leveraged sensitive information stolen in data leaks to target banking customers.[3,4,5] Threat actors leveraged topical financial lures—such as the closure of Silicon Valley Bank and the turmoil of other financial institutions—in low sophistication campaigns, encouraging customers to visit malicious domains and phishing pages that appear as legitimate subdomains of financial institutions or related to legitimate services.[6] ZeroFox Intelligence observed early indications of an increase in Search Engine Optimization (SEO) / Search Engine Results Pages (SERP) poisoning by strains known to target the sector.[7,8] ZeroFox Intelligence also noted an increase in malicious campaigns leveraging Google advertisements as a means of distributing and delivering malware.[9,10]

### Forward Look:

- Threat actors will likely increasingly deploy malicious pages offering customers financial or legal support or other fraudulent services.

### Recommendations:

- Communicate to employees and customers about emerging trends in social engineering scams.
- Leverage ZeroFox Intelligence's Attack Surface Assessment to understand the threats faced.

No notable change in threat from previous quarter

## INITIAL ACCESS BROKERS (IABs)

Illicit access to financial organizations advertised in open forums remained low in Q1 2023, with brokers continuing to leverage private channels for selling to well-established buyers.[11] This trend was reflected across almost all industries, with threat actors continuing to operate with an abundance of caution to avoid law enforcement scrutiny. Advert content continued to typically focus on vulnerabilities in remote working infrastructure, including Virtual Private Networks and Remote Desktop Protocol.

### Forward Look:

- The threat to financial organizations will likely continue to manifest via brokers leveraging private communication channels to sell access to established buyers.

### Recommendations:

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

No notable change in threat from previous quarter

## VULNERABILITY EXPLOITATION

Financial organizations likely faced an increased threat of nefarious actors exploiting CVEs, with Q1 2023 seeing the highest percentage of disclosed vulnerabilities rated critical (18.4 per cent) on record.[12] Exploits in commonly-used software modules and remote working infrastructure continued to dominate the landscape. Clap's successful January 2023 exploitation of CVE-2023-0669, a zero-day exploit in GoAnywhere MFT file transfer software, demonstrated the impact that targeting these CVEs can have. This resulted in the most incidents in a single month by any extortion collective in ZeroFox Intelligence records, and financial sector organizations accounted for approximately 10 percent of victims.[13] Other critical CVEs disclosed in Q1 2023 impacted SAP products, which are believed to be used by multiple financial sector companies. The Cybersecurity and Infrastructure Security Agency's (CISA) updates to its Known Exploited Vulnerabilities (KEV) catalog included high and critical severity vulnerabilities that almost certainly impact financial sector entities, including exploits impacting iOS operating systems, Google Chrome, Microsoft Windows, and Zoho ManageEngine.[14]

### Forward Look:

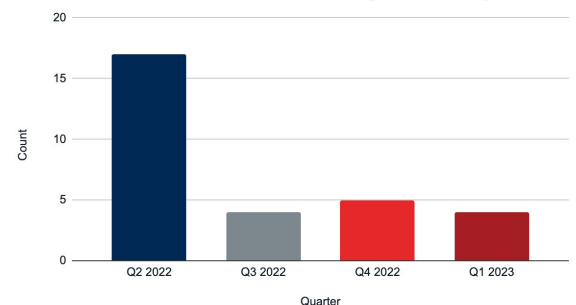
- Vulnerabilities in commonly-used software modules and remote working infrastructure will very likely continue to dominate the exploit landscape.

### Recommendations:

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

Indication of increase in threat from previous quarter

Advertised IAB Access into Financial Organizations by Quarter



Source: ZeroFox Intelligence

## FOOTNOTES

[1] <https://www.reuters.com/technology/german-finance-regulator-warns-godfather-malware-attacks-2023-01-09/>  
[2] <https://www.coinbase.com/blog/social-engineering-a-coinbase-case-study>  
[3] <https://thehackernews.com/2023/03/fokeadile-vishing-malware-targets-south.html>  
[4] <https://www.bleepingcomputer.com/news/security/hackers-use-fake-crypto-pb-offers-to-push-info-stealing-malware/>  
[5] <https://thehackernews.com/2023/01/hackers-using-stolen-bank-information.html>  
[6] <https://www.bleepingcomputer.com/news/security/cybercriminals-exploit-svb-collapse-to-steal-money-and-data/>  
[7] <https://blog.cylab.it/2023/02/01/qakbots-evolution-continues-with-new-strategies>

[8] <https://www.bleepingcomputer.com/news/security/emotet-malware-now-distributed-in-microsoft-onenote-files-to-evade-defenses/>  
[9] <https://www.bleepingcomputer.com/news/security/ransomware-access-brokers-use-google-ads-to-breach-your-network/>  
[10] <https://www.pcmag.com/news/batwarden-warns-of-scams-ads-on-google-posing-as-the-password-manager>  
[11] ZeroFox Intelligence Internal Collections  
[12] <https://nvd.nist.gov>  
[13] ZeroFox Intelligence Internal Collections  
[14] <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



## BOTNETS

There was no significant change in the threat to financial organizations from botnets in Q1 2023, which remained a high threat—predominantly from infostealers harvesting credentials—and enabled remote-control of infected devices.[15] With increasing use of internet-of-things, Distributed Denial of Service (DDoS) attacks got larger and more complex, but the impact of denial of service remained limited. European financial organizations—particularly those linked to governments—likely faced an increased threat from Russia-aligned groups that continued campaigns of Distributed Denial of Service (DDoS) attacks against countries that announced further support for Ukraine in Q1 2023, including Denmark, Latvia, Poland and Sweden.

### Forward Look:

- The threat to most financial organizations from botnets is unlikely to change considerably in the near-term.
- However, financial organizations in countries pledging support for Ukraine are likely to face continued high threats from Russia-aligned entities.

### 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

The threat to financial entities from malware deployment in Q1 2023 remained broadly consistent with previous quarters, with no significant change in capabilities observed. Malware-as-a-service offerings sustained low barriers to entry, with trojans targeting sector entities by facilitating the interception of two-factor authentication codes and keystroke recording.[16,17] Prolific malware strains were upgraded with more powerful loader capabilities, and threat actors were observed offering services to upload benign applications to mobile app stores to pass security checks—and then offering to update it with malicious code, infecting new users and previous installers.[18,19] E-skimmers and point of sale malware were successfully leveraged to infect downstream users and siphon payment information.[20,21]

### Forward Look:

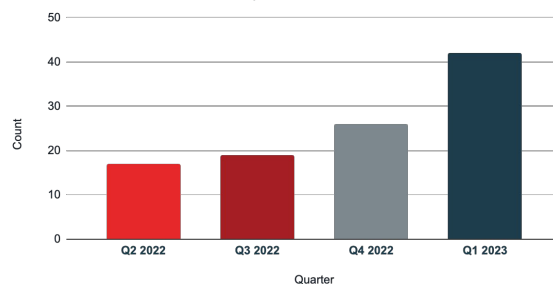
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.

### Recommendations:

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

No notable change in threat from previous quarter

Total Financial Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

## RANSOMWARE

Financial organizations very likely faced an increased threat from ransomware and digital extortion in Q1 2023. ZeroFox Intelligence identified a possible return of the targeting of “big game” financial sector organizations.[22] Third-party providers were leveraged to impact multiple downstream financial sector customers, with incidents in Q1 2023 highlighting the significant impact these attacks can have.[23]

Extortion incidents against sector targets reached the highest levels since 2021, driven by increased deployment of ALPHV and Clon, as well as Black Basta resuming operations. The financial sector did not see the same significant increase in LockBit deployment that other sectors saw. In March 2023, the Clon digital extortion collective added 102 victims to its leak site. This was the highest number of digital extortion incidents for a single month in ZeroFox Intelligence's records—and the first month in over a year LockBit has not been the most prolific strain.[24] The financial sector was the fourth most frequently targeted in Clon's campaign, behind healthcare, technology, and manufacturing, respectively.

### Forward Look:

- ZeroFox Intelligence anticipates a reduction in threat in Q2 2023, with Clon's campaign very likely finishing by April 2023.
- However, high levels of activity from ALPHV, Black Basta, and LockBit—as well as strains such as Money Message and Royal, which are on an upward trajectory—will sustain a high threat to financial sector organizations.

### Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise (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

[15] ZeroFox Intelligence Internal Collections  
[16] <https://thehackersnews.com/2023/01/spy-note-strikes-again-android-spyware.html>  
[17] <https://www.infosecurity-magazine.com/news/banking-trojan-piggyback-targets/>  
[18] <https://thehackersnews.com/2023/02/gootkit-malware-adopts-new-tactics-to.html>

[19] <https://www.bleepingcomputer.com/news/security/new-icedid-variants-shift-from-bank-fraud-to-malware-delivery/>  
[20] <https://www.bleepingcomputer.com/news/security/pos-malware-can-block-contactless-payments-to-steal-credit-cards/>  
[21] <https://thehackersnews.com/2023/03/new-tfx-atm-malware-targeting-mexican.html>  
[22] ZeroFox Intelligence Internal Collections  
[23] <https://www.reuters.com/technology/hackers-say-ransom-paid-case-derivatives-data-firm-ion-company-declines-comment-2023-02-03/>  
[24] ZeroFox Intelligence Internal Collections



## OUTLOOK

ZeroFox Intelligence anticipates that cyber threats facing the financial sector will continue to be heavily influenced by Russia's invasion of Ukraine; Russia-based threat actors are likely to direct their aggression against Western financial institutions they judge are unfriendly toward Russia.

ZeroFox Intelligence anticipates that the threat from ransomware and digital extortion operations may fall in Q2 2023 but will likely remain above 2022 levels, as threat actors are galvanized by recent successes. ZeroFox Intelligence anticipates an increase in low sophistication social engineering campaigns leveraging financial market instability to steal money, account data, conduct business email compromise attacks, or infect targets with malware, as well as a sustained high threat from smishing and vishing campaigns. In coming quarters, threat actors are expected to increasingly leverage Artificial Intelligence tools to aid the credibility of their social engineering campaigns.



April 28, 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](https://zerofox.com/request-a-demo)

### > Learn More:

Visit [zerofox.com](https://zerofox.com)

Contact us at [sales@zerofox.com](mailto:sales@zerofox.com) / 855.736.1400

