2022

Q3 Financial Sector

Quarterly Threat Landscape Scorecard

TLP:CLEAR A-2022-10-31a

ZEROFOX

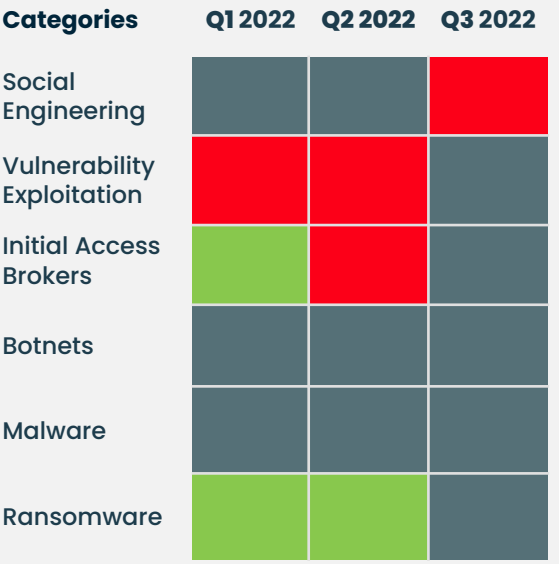
Q3 2022 Financial Sector Threat Overview

The threat to financial sector organizations remained broadly consistent in Q3 2022, with the ongoing war in Ukraine continuing to shape the cyber threat landscape. There were increases in particular aspects of the social engineering threat to financial organizations, including 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 v2.0 (FIDO2) and certificate-based authentication. The sustained high pace of vulnerability disclosures, particularly in software commonly-used by financial organizations, will very likely strain out-of-cycle patch management processes and increase the likelihood of vulnerabilities not being patched in a timely manner. Financial organizations should note an ongoing shift in the Initial Access Broker (IAB) market, with a fall in advertisements pertaining to financial organizations likely reflecting an ongoing move towards brokers making sales in private channels rather than advertising in open forums. Botnet and malware deployment remained high, including infostealers and banking trojans. Digital extortion attempts against financial victims remain below 2021 levels, likely caused in part by difficulty eliciting victims' payments. While there have been fewer attacks against "big game" financial sector organizations, 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 Financial Sector in Q3 2022

- Increased threats from SMS-phishing, callback phishing, and techniques to bypass MFA
- Vulnerabilities in third-party software used by financial organizations and the pace of exploitation
- Card skimmers deployed and compromised payment systems and e-stores
- Malware disguised in fake finance-related applications targeting customers
- IABs moving towards private means of communication with sellers, making identification and mitigation more difficult
- Changes to digital extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications
- Russia-backed and aligned threat actors seeking to target financial entities
- Saturated infostealer and banking trojan markets sustaining low barriers to entry and high pace of new Indicators of Compromise.

Financial Sector Threats



Q3 Key Findings:

- Financial organizations likely face an increased threat of smishing, callback phishing (vishing), and phishing techniques that bypass MFA.
- Vulnerabilities in software commonly-used by financial organizations were added to CISA's Known Exploited Vulnerabilities (KEV) catalog.
- Illicit access to large financial entities was increasingly being sold via private or direct communication channels.
- While there were fewer ransomware and digital extortion attempts against "big game" financial sector targets, incidents highlighted the high 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.

ZEROFOX

SOCIAL ENGINEERING

The overall threat to the financial sector from social engineering remained broadly consistent, although ZeroFox Intelligence has identified categories of increased threat. Financial organizations should note a likely increased threat from smishing attacks targeting employees, either directly or via enterprise third-party providers, as well as customers.[1,2,3] Analysis also indicates an increasing 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.[4]

Threat actors have begun leveraging Adversary-in-the-Middle (AiTM) techniques to bypass MFA, including through Phishing-as-a-Service (PhaaS) operations that have historically targeted financial and e-commerce entities. PhaaS outfits operating this quarter included Robin Banks, used to target customers of multiple, well-known financial institutions.

Threat actors continued to leverage topical lures to entice engagement with malicious emails. Malware distribution via malicious email attachments and job scams targeting the sector remained highly prevalent.[5,6] Impersonating phishing domains and open redirects should be continually monitored and taken down to avoid customers being defrauded or providing an intrusion vector for threat actors, as was observed this quarter. [7,8]

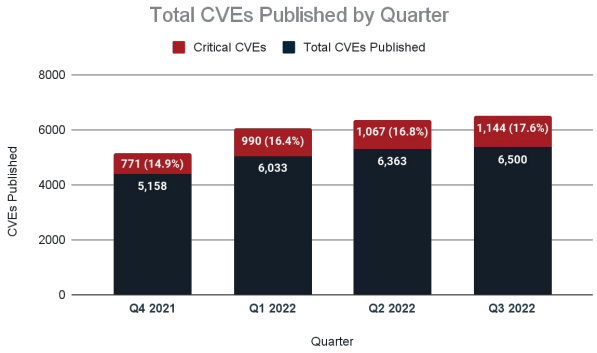
› Forward Look:

- Smishing of financial organizations' employees and customers is likely to continue on an upward trajectory.
- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.
- Customers are likely to be increasingly targeted with financial-relief scams given the ongoing strain on global financial markets.

› Recommendations:

- Communicate to employees about emerging trends in social engineering scams and how to conduct safe means of authentication.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand threats to your organization.

Indication of increase in threat from previous quarter



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

VULNERABILITY EXPLOITATION

The most widely reported examples of vulnerability exploitation in Q3 2022 remained in commonly-used software modules and network perimeter infrastructure. Sustained periods of high vulnerability disclosures place strain on out-of-cycle patch management processes, with new disclosures in Q3 2022 impacting 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 financial organizations are stated to be customers.[10]

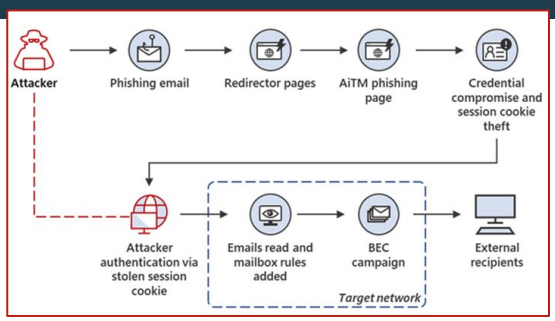
› Forward Look:

- 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.

No notable change in threat from previous quarter



AiTM Phishing Campaign Overview
Source: hXXps://www.microsoft[.]com

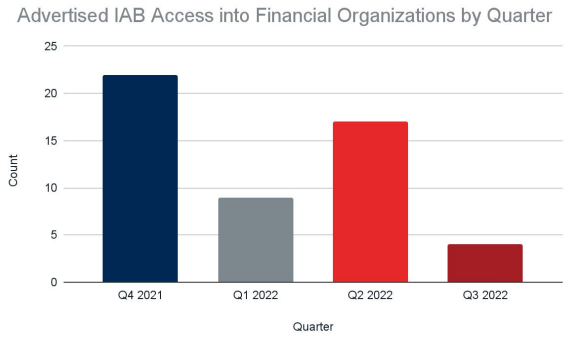
FOOTNOTES

[1] hXXps://www.securityweek[.]com/european-central-bank-head-targeted-hacking-attempt
[2] hXXps://www.securityweek[.]com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations
[3] hXXps://www.bleepingcomputer[.]com/news/security/revolut-hack-exposes-data-of-50-000-users-fuels-new-phishing-wave/
[4] hXXps://threatpost[.]com/callback-phishing-security-firms/180182/
[5] hXXps://thehackernews[.]com/2022/07/researchers-uncover-new-attempts-by.html
[6] hXXps://www.bleepingcomputer[.]com/news/security/north-korean-hackers-target-crypto-experts-with-fake-coinbase-job-offers/
[7] hXXps://cyberwarzone[.]com/chase-bank-customers-beware-of-new-phishing-campaign/
[8] hXXps://www.infosecurity-magazine[.]com/blogs/japanese-credit-card-phishing/
[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

The fall in advertised access to financial organizations in Q3 2022 likely reflects a shift towards brokers preferring private channels rather than advertising in forums to avoid law enforcement scrutiny; brokers are selling to well-established buyers out of an abundance of caution according to threat actor chatter observed by ZeroFox Intelligence. Access to financial firms in the United States and western Europe posted in open channels are becoming increasingly rare.[11] Financial organizations may increasingly be targeted via illicit access to managed service and software providers.



Source: ZeroFox Intelligence

› Forward Look:

- Illicit access to large financial entities will likely increasingly be sold via private or direct communication methods.
- The IAB market will very likely remain volatile.

› 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

There was no notable change in threat to financial organizations from botnets, which continued to pose a threat via stealing credentials and remotely-controlling infected devices. In Q3 2022, ZeroFox Intelligence ingested almost 45 million credentials harvested by infostealer families commonly deployed by botnets, of which RedLine was most active.[16] Financial organizations should be wary of being targeted directly or systems leveraged in politically-motivated Distributed Denial of Service (DDoS) attacks such as those seen against Taiwan and much of Europe.[17,18] Emotet's resurgence continued, reportedly infecting almost 1.3 million devices since the start of 2022 including financial organizations and now pushing Quantum and BlackCat ransomware.[19]

› Forward Look:

- The threat of financial organizations' systems being targeted or leveraged in botnet attacks by Russia-aligned entities is likely to increase.
- Emotet is expected to pose an increasing threat to financial organizations in the coming months given its resurgence.

› 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

ZeroFox Intelligence observed no major changes in the threat to the financial industry from malware deployment in Q3 2022. Low barriers to entry and the pace of trojan updates continued to sustain a high threat.[12] App stores remained one of the most prolific means of distributing malware.[13] E-skimmers and supply chain attacks against payment systems enabled threat actors to infect multiple downstream users and siphon the payment information of hundreds of thousands of victims.[14,15] ZeroFox Intelligence assesses with low confidence that the threat from the most popular loaders has increased, with Bumblebee and ChromeLoader now 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.
- ZeroFox Intelligence anticipates an increased threat from Russia-linked threat actors targeting financial institutions with malware containing destructive components.

› Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise (IOCs) and metadata related to Malware and Ransomware.

No notable change in threat from previous quarter

FOOTNOTES

[11] ZeroFox Intelligence Internal Collections
[12] hXXps://heimdalsecurity[.]com/blog/a-new-and-upgraded-version-of-sharkbot-malware-has-been-detected/
[13] hXXps://www.bleepingcomputer[.]com/news/security/adware-on-google-play-and-apple-store-installed-13-million-times/
[14] hXXps://www.bleepingcomputer[.]com/news/security/hackers-breach-software-vendor-for-magento-supply-chain-attacks/
[15] hXXps://www.securityweek[.]com/hundreds-ecommerce-domains-infected-google-tag-manager-based-skimmers
[16] ZeroFox Intelligence Internal Collections
[17] hXXps://www.reuters[.]com/world/asia-pacific/taiwan-defence-ministry-website-hit-by-cyber-attacks-amid-china-tensions-2022-08-04/
[18] hXXps://nsm[.]no/aktuelt/malrettede-tjenestenektangrep-mot-norske-nettsteder
[19] 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 ransomware and digital extortion threat to financial organizations remained broadly consistent with previous quarters in Q3 2022. Extortion attempts remain below 2021 levels, likely caused in part by difficulty eliciting payments from victims.[20] ZeroFox Intelligence observed fewer attacks against "big game" financial sector organizations, although incidents this quarter again highlight the high threat of attacks against third-party providers that could impact multiple downstream customers.[21] The supply chain threat is compounded by developments in extortion tactics, with ALPHV/BlackCat providing leaked victim data in a searchable format.[22] While not a novel tactic, LockBit announced a move into conducting DDoS attacks against victims as a pressure tactic, which may see other groups adopt similar methods.[23] 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 Black Basta - flagged in Q2 2022 as an emerging actor - continued an upward trajectory. Security teams should be wary of updated versions of strains that frequently target the sector and their associated IOCs, including Hive and BlackCat, as well as the unusually high number of new strains identified this quarter.[24] In coming months, the industry may see an increased extortion threat from Medusa Locker, which was identified targeting financial organizations and industry software, and Karakurt, which—while its increase in activity in Q3 2022 was predominantly targeted towards the healthcare sector—is linked to the former Conti operation that was a prolific targeter of financial institutions.[25,26]

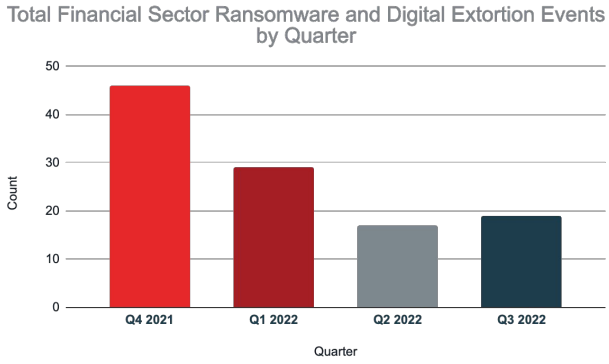
› Forward Look:

- ZeroFox Intelligence anticipates the threat of digital extortion to financial 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.

No notable change 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 , which are all techniques that are included in 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 v2.0 (FIDO2) and certificate-based authentication.[27] FIDO2 aims to maximize security with minimal impact on user experience. It supports passwordless, two-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 and dark web publishing or brokering exploits related to phishing-resistant MFA.[28]

FOOTNOTES

[20] ZeroFox Intelligence Internal Collections
[21] hXXps://www.cpomagazine[.]com/cyber-security/identity-management-firm-entrust-suffers-a-security-breach-ransomware-gang-obtains-files/
[22] hXXps://blog.cyble[.]com/2022/07/06/alphv-ransomware-expands-its-arsenal-of-extortion-techniques/
[23] hXXps://www.itworldcanada[.]com/article/lockbit-ransomware-gang-adding-ddos-attacks-to-its-threats/500301
[24] Lilith, Cheers, Yaniuowang, Omega, RedAlert and BlanLian, Royal, Monster, Agenda, PlayCrypt
[25] hXXps://www.cisa[.]gov/uscert/ncas/alerts/aa22-181a
[26] hXXps://www.cisa.gov/uscert/ncas/alerts/aa22-152a
[27] hXXps://fidoalliance[.]org/specifications/
[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.

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

OUTLOOK

The cyber threat to the financial sector is unlikely to change significantly in the near term. However, 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.

Social engineering scams will almost certainly remain evolutionary rather than revolutionary, and we expect threat actors to increasingly seek to bypass MFA to compromise corporate environments. In coming quarters, ZeroFox Intelligence also anticipates increased targeting of authentication providers. Furthermore,, ZeroFox Intelligence anticipates a Q4 2022 increase of scams targeting financial organizations' customers by impersonating trusted parties, particularly in the run-up to Black Friday and the winter holidays.

Pro-Russia threat actors and state-linked entities have begun targeting countries and organizations with malware in retaliation for perceived stances taken during the war. ZeroFox Intelligence expects this trend to continue, likely impacting sector organizations perceived as being unsupportive of - or opposed to - Russia. Financial organizations should expect to be increasingly targeted via third-party providers, particularly those afforded trusted access within a network.

ZeroFox Intelligence anticipates a continued increase in IABs leveraging private means of communication to sell access, as well as leveraging 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 21, 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.