ZEROFOX®

ZeroFox Releases New Research Highlighting Evolution of Threats Targeting Financial Services

May 26, 2022

Company processed over 460,000 takedowns in Q1 2022, observing a significant rise in frequency and sophistication of FinServ targeted cyberattacks

May 26, 2022 07:00 ET | Source: ZeroFox, Inc.

WASHINGTON, May 26, 2022 (GLOBE NEWSWIRE) —ZeroFox, a leading external cybersecurity provider, today announced new insights on the frequency and sophistication of cyberattacks. From February to April 2022, ZeroFox processed over 460,000 takedowns for customers. This represents an over 200% year-over-year increase in takedowns processed. The release of its Financial Services Quarterly Threat Landscape Q1 2022 assessment outlines the key changes to cyber threats facing the financial sector and illustrates specific threat categories of interest including: social engineering, vulnerability exploitation, botnets, Initial Access Brokers (IABs), malware, ransomware, and blockchain threats. The assessment also includes geopolitical factors that place additional pressure on the financial services sector, as economic instability often opens a back door for cyber threat actors. ZeroFox's financial services assessment research reveals a significant rise in the frequency and sophistication of cyberattacks, with 63% of organizations reporting that they were breached in the last year.

Key Findings from ZeroFox Intelligence:

- Social Engineering was one of the most frequently reported intrusion tactics leveraged in Q1 2022. ZeroFox has observed an increase in conversation hijacking which can make it more difficult for victims to identify nefarious activity.
- It is highly likely the threat to the financial sector from Common Vulnerabilities and Exposures (CVEs) and previously unknown software vulnerabilities (zero-days) increased in Q1 2022.
- Blockchain threats and scams against crypto platforms increased in Q1 2022 and are expected to continue.
- Despite a drop in the number of identified ransomware and digital extortion attacks against the financial sector in Q1 2022, ZeroFox anticipates the threat will increase in coming quarters as the immediate desire to appear politically neutral in Russia's invasion of Ukraine dissipates. This quarter saw a notable increase from 'hack-and-leak' groups that claimed to be ransomware operations.

ZeroFox currently tracks, reviews and updates critical baseline data for the financial services industry as part of its commitment to provide security teams with timely, relevant and action-oriented intelligence to understand the external attack surface, disrupt adversaries and protect the integrity of any financial institution. The assessment provides medium/high forecasting intelligence to help internal cybersecurity teams become more proactive in their cyber modeling preparedness. In addition, security teams looking for relevant and actionable intelligence around vulnerabilities, threat actors, as well as for tactics, techniques, and procedures (TTPs), and trends in the criminal underground, can find consistent reporting from this research.

"Our quarterly assessments provide significant insight into market sectors where cyber vulnerabilities represent opportunities to not only hurt an individual or institution but the financial ecosystem of a community or country. Our reports empower customers to gain a more comprehensive understanding of the external threats facing their internal cyber security teams," said AJ Nash, Vice President of Intelligence, ZeroFox. "Our findings highlight serious gaps in the areas of data and identity theft via phishing sites, malware and ransomware attacks. Financial services professionals will benefit from our report through improved situational awareness while also gathering key takeaways and next steps for how to protect their business against cyber threats."

ZeroFox has made significant investments in adversary disruption services, leveraging a Global Disruption Network to go beyond traditional takedown services and remove fraud and external cyberattacks at the source. The over 460,000 takedowns processed in Q1 2022 represent protection against malicious domains, social media impersonations, phishing campaigns, credential theft and more. Over the past few months, ZeroFox has made its threat intelligence data more accessible than ever by offering customers multiple ways to operationalize the intelligence to defend against ransomware, phishing, fraud, credential theft and vulnerabilities.

To download the full report with access to recommendations for what to do to protect your business, visit https://www.zerofox.com/resources/quarterly-threat-landscape-report-2022-q1/.

About ZeroFox
ZeroFox, a leader in external cybersecurity, provides enterprises external threat intelligence and protection to disrupt threats to brands, people, assets and data across the public attack surface in one platform. With global coverage across the surface, deep and dark web and an artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, 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. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. Visit www.zerofox.com for more information.

ZeroFox
Media Inquiries:
Malory Van Guilder
zerofox@skyya.com

Investor Relations
Marc P. Griffin, ICR
Marc.Griffin@icrinc.com