ZeroFox Releases 2024 Threat Forecast Report Assessing Next Year's External Cyber Threat Landscape

November 7, 2023

Report anticipates heightened threats from ransomware, initial access brokers, and generative AI; as well as significant risk tied to upcoming elections

WASHINGTON, D.C., Nov. 07, 2023 (GLOBE NEWSWIRE) -- ZeroFox (Nasdaq: ZFOX), a leading provider of external cybersecurity, today released its annual 2024 Threat Forecast Report outlining key predictions and recommendations from ZeroFox Intelligence. Combining depth and breadth of intelligence experience and access, the 2024 Threat Forecast offers security teams insight on threat trends and steps to address an evolving external attack surface. Key takeaways include an anticipated significant increase in attack vectors shifting toward third-party vendors of major corporations and government entities, the use of generative AI and synthetic media by both malicious and non-malicious actors to create more persuasive fake content, and geopolitical conditions contributing to increased cyber incidents.

The cyber threat landscape evolved significantly in 2023, as threat actors embraced new tools and diversified tactics to overcome defenses. ZeroFox Intelligence observed a record number of ransomware and digital extortion incidents this year, reflecting consistently higher-than-average activity of prolific cybercriminal gangs such as Cl0p throughout the year.

"2023 was a banner year for cyber threat advancements, as we saw the explosion of generative AI tools. Additionally, significant global conflicts radically alter the threat landscape in multiple regions. This report reflects the collective efforts of our intelligence leaders and experts across the globe to better understand these evolving threats - including those operating in the underground economy – and empower security teams to defend against, deter, and disrupt the adversaries most likely to threaten their security," said AJ Nash, ZeroFox VP & Distinguished Fellow of Intelligence. "Throughout 2024, ZeroFox Intelligence will keep reporting on the most significant threat developments and continue advancing collection capabilities to provide customers with a more holistic view of their external cyber risk."

The 2024 Threat Forecast Report includes in-depth assessments of anticipated external threat trends including:

- **Ransomware and digital extortion (R&DE):** ZeroFox Intelligence predicts the threat from ransomware and digital extortion will very likely remain elevated in 2024, following a record number of extortion incidents observed in 2023, as newly-formed ransomware groups demonstrate proficiency faster than ever before.
- **Initial access brokers (IABs):** ZeroFox Intelligence predicts IABs will pose a significant threat to organizations across industries in 2024, with illicit access sales underpinning the threat from ransomware operators.
- **Social engineering:** The threat from social engineering will likely continue on an upward trajectory in 2024, as threat actors continue to evolve traditional phishing techniques.
- **Artificial intelligence (AI):** ZeroFox Intelligence anticipates measured growth in the use of AI for both malicious and defensive applications, particularly in information operations (including to spread mis-, dis-, and malinformation), social engineering campaigns, and various threat actor tactics, techniques, and procedures (TTPs).
- **Physical and cybersecurity convergence:** ZeroFox Intelligence predicts the greatest cyber-physical threats will lie within critical infrastructure sectors, as geopolitical factors will continue to influence the probability for major cyber events that can have severe or catastrophic physical impacts.
- **Election-related threats:** ZeroFox Intelligence expects key elections in 2024, including the US Presidential Election, will drive an uptick in election-related scams, disruptive threats, and the spread of disinformation.
- **Zero-day vulnerabilities:** ZeroFox Intelligence predicts a rise in both the discovery and exploitation of zero-day vulnerabilities in 2024, as adversaries pivot away from traditional methods of data exfiltration toward a heightened focus on exploiting vulnerabilities for increased financial gain.

Beyond predictions for next year, the report also offers security practitioners strategic recommendations to counter external cyber threats and enhance cybersecurity resilience. ZeroFox is proud to share its industry-leading intelligence with customers and the wider security landscape to mitigate risk and reduce uncertainty around the evolving threat landscape. The complete ZeroFox 2024 Threat Forecast is available for download here.

About ZeroFox
ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate, and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers, including some of the largest public sector organizations as well as finance, media, technology and retail companies to stay ahead of adversaries and address the entire lifecycle of external cyber risks. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries. Visit www.zerofox.com for more information.

Media Inquiries
Maisie Guzi, ZeroFox

press@zerofox.com

Investor Relations
Todd Weller, ZeroFox
investor@zerofox.com