ZeroFox Releases 2022 Forecast Report Anticipating Increases in Ransomware, Third-Party Compromises and Malware-as-a-Service

February 10, 2022

New report details expected threat activity trends and recommendations for security teams to address external threats

WASHINGTON–(BUSINESS WIRE)–ZeroFox, a leading external cybersecurity provider, today published the “2022 Threat Intelligence Forecast,” detailing expected cybercriminal behavior trends including ransomware, malware-as-a-service, vulnerabilities and exploits. Within the report, the ZeroFox Intelligence team reviews 12 months of threat actor activity from 2021 and provides go-forward recommendations for security teams as we continue into 2022. Key takeaways include an assessment of increasing ransomware threats targeting the financial, manufacturing, retail and healthcare sectors, a predicted surge in data kidnapping attacks, and a continued upward trajectory of third-party compromises targeting vendors within larger supply chains.

> *“Throughout 2022, ZeroFox Intelligence will continue to expand capabilities and improve our collection and analytical tradecraft to answer even more requirements for our customers and address emerging threats at scale.”Tweet this*

Threat actors around the world made 2021 an extremely stressful year for security teams—perhaps the most challenging year on record. ZeroFox Intelligence observed record-setting ransomware incidents, more supply chain compromises, and increased geopolitical tensions in Europe and Asia. ZeroFox was also the first threat intelligence firm to discover a variant of ransomware called Colossus whose operators appeared to be highly familiar if not directly associated with other existing ransomware-as-a-service groups. Looking towards 2022, it is imperative that security teams understand the growing external cybersecurity threat landscape and criminal underground to appropriately resource their teams and employ strategies to effectively address emerging threat tactics, techniques, and procedures; not last year’s TTPs.

“In 2021, ZeroFox advanced our intelligence capabilities to further detect threat infrastructure and activities to provide timely, relevant and actionable intelligence to our customers. Leveraging that intelligence, our team of threat researchers, hunters and analysts is forecasting significant increases in the demand for Initial Access Brokers services, the use of Java-based vulnerabilities to recreate the success of Log4j, and the competition between infostealer developers,” said Brian Kime, Vice President of Intelligence Strategy and Advisory for ZeroFox. “Throughout 2022, ZeroFox Intelligence will continue to expand capabilities and improve our collection and analytical tradecraft to answer even more requirements for our customers and address emerging threats at scale.”

The 2022 Threat Intelligence Forecast report includes in-depth assessments of key external threat trends including:

- **Ransomware:** ZeroFox anticipates a continued increase in ransomware attacks and extortion activities particularly targeting the financial, manufacturing, retail, and healthcare sectors
- **Third-Party Compromises (TPC):** ZeroFox expects an increase in the use of third-party compromises as a means to distribute ransomware. The continued expansion of software supply chains will also likely contribute to a rise in TPC attacks
- **Malware-as-a-Service:** ZeroFox assesses that, in 2022, there will be an increase in the use of information stealers within underground criminal markets, providing a lucrative outlet for various cybercriminals to peddle stolen credentials from various stages of an organization’s network compromise
- **Initial Access Brokers:** ZeroFox assesses with high confidence that the demand for Initial Access Brokers services will continue to thrive in 2022, with more threat groups or individual actors attempting to sell access given the relatively low risk and high demand from various malicious groups
- **Vulnerabilities and Exploits:** ZeroFox predicts that nefarious actors will research more Java-based exploit avenues, focusing on common libraries exposed to attacker control content
- **Phishing-as-a-Service:** ZeroFox anticipates that cyber criminals will continue to use automation to fuel the growth of sophisticated Phishing-as-a-Service kits for sale and license
- **Cryptocurrency:** ZeroFox expects remittance-heavy economies to move towards digital currencies in 2022 at a faster pace, especially in the Middle East and Central Europe

“The 2022 Threat Intelligence Forecast is rooted in our global intelligence collection gathered from the past 12 months, combined with the expertise from our world-class team of analysts and researchers with extensive experience and unmatched access for researching activities in the criminal underground,” said AJ Nash, Vice President of Intelligence for ZeroFox. “In order to address the persistent and emerging threats that 2022 is sure to deliver, security leaders need access to forecasting data, geopolitical fluctuations and macroeconomic trends that provide indications and warnings of state-nexus and criminal threat actors’ next targets.”

This report offers security practitioners tactical and strategic recommendations for addressing new and continuing external threats. These recommendations are intended to help overburdened security teams struggling to keep pace with breaches, vulnerability disclosures and the media cycle of attacks by focusing their attention on relevant threats. With this report and beyond, ZeroFox Intelligence will continue to provide the vital intelligence needed to protect brands, assets, data and people against external threats.

The full 2022 Threat Intelligence Forecast is available for download at https://www.zerofox.com/resources/2022-threat-intelligence-forecast/

About ZeroFox

ZeroFox, the 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, comprehensive platform. With complete 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. Visit www.zerofox.com for more information.

Contacts

ZeroFox
Media Inquiries:
Dave Bowker, PAN Communications
ZeroFox@pancomm.com

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