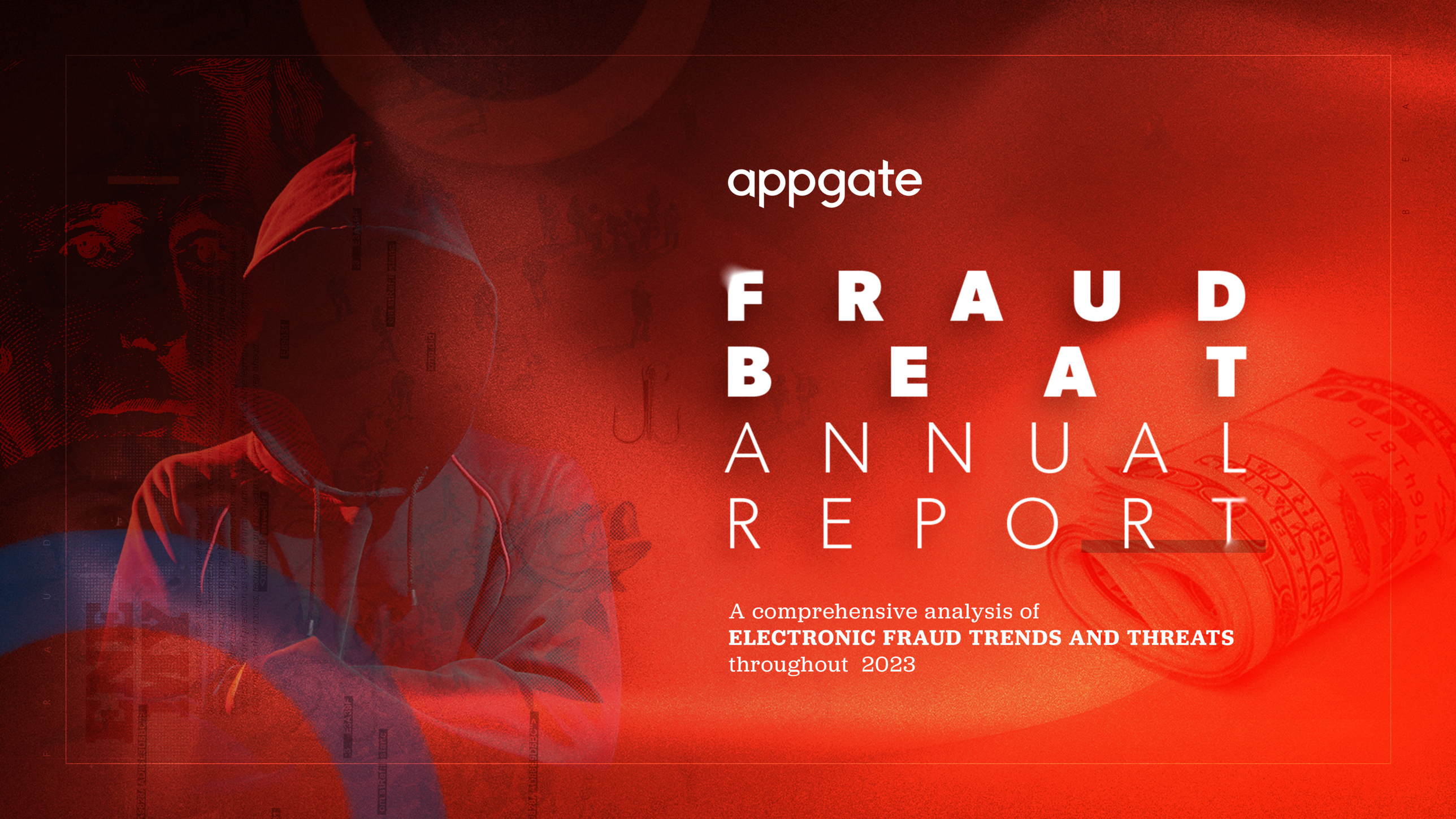


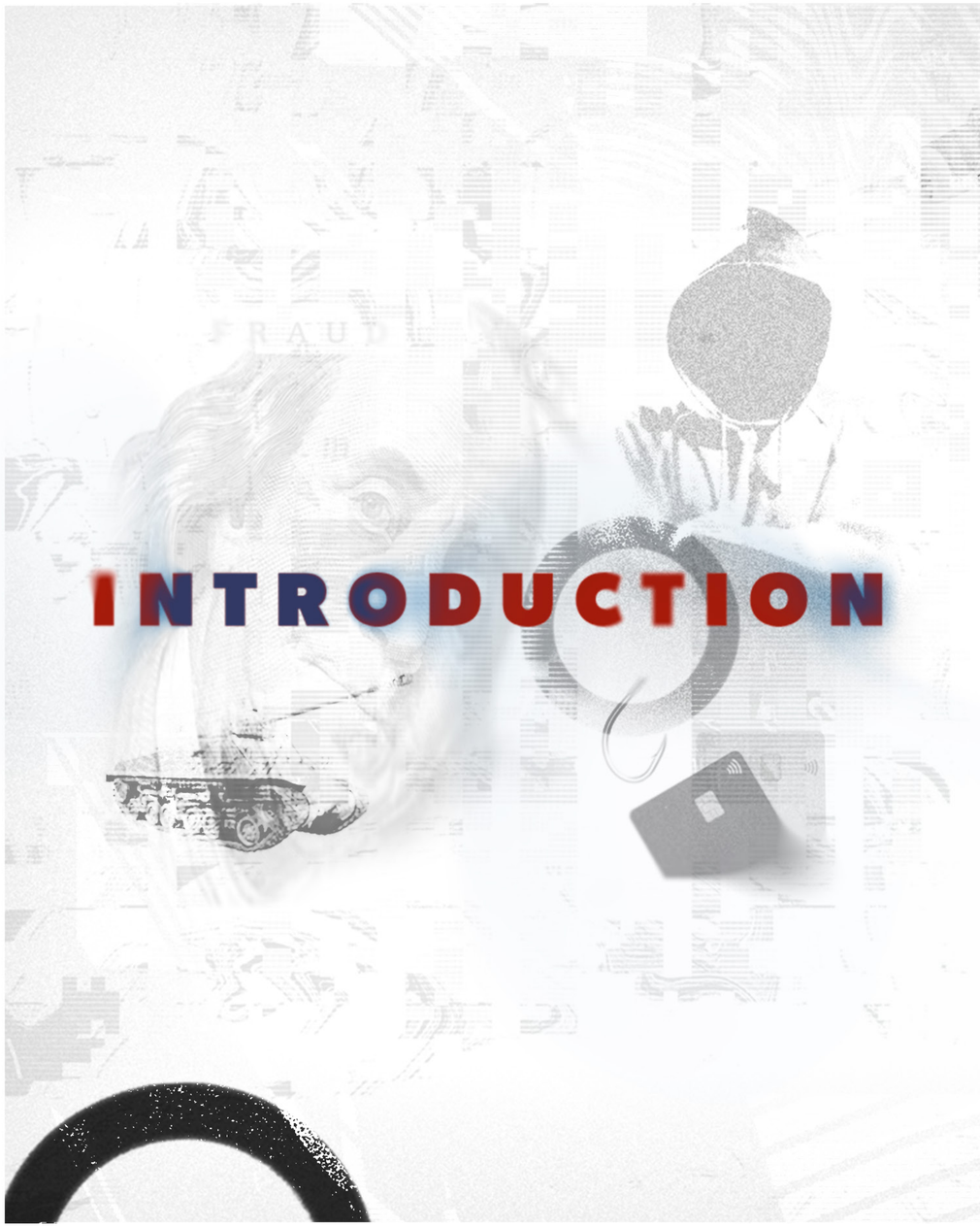
appgate

FRAUD BEAT ANNUAL REPORT

A comprehensive analysis of
ELECTRONIC FRAUD TRENDS AND THREATS
throughout 2023

appgate

TABLE OF CONTENTS



INTRODUCTION

In 2023 we saw a rise in familiar adversarial attack techniques including phishing, branding, information disclosure and malware. Remote and hybrid workforces significantly expanded attack surfaces presenting an opportunity for threat actors to target businesses and consumers. Staying proactive in the face of evolving threats poses a considerable challenge, as fraudsters continually adopt novel strategies. In 2024, we predict new levels of sophistication and precision as cybercriminals harness the power of machine learning and artificial intelligence (AI) to improve their tactics, techniques and procedures (TTPs) to stay one step ahead.

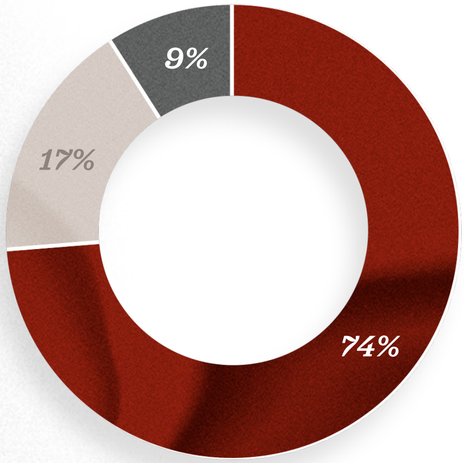
The 2023 Faces of Fraud study, conducted annually with ISMG, provides valuable information on different attacks, fraud schemes and other major challenges faced by financial institutions:

- **83%** of respondents cited rapid evolution of fraud schemes as their greatest vulnerability
- Only **19%** said they have the ability to identify a fraud attack in real-time
- **55%** of respondents have limited or no visibility to identify the impacts of a phishing attack
- **34%** of respondents expected monetary fraud losses to increase in 2023
- **77%** noted that the number of fraud incidents has remained steady or increased

Appgate's cybersecurity and fraud solutions and services are designed to address the current threat landscape, and anticipate and neutralize emerging threats. With cutting-edge technology that supports adaptive strategies, we empower organizations to strengthen their defenses against ever-evolving cyberthreats.

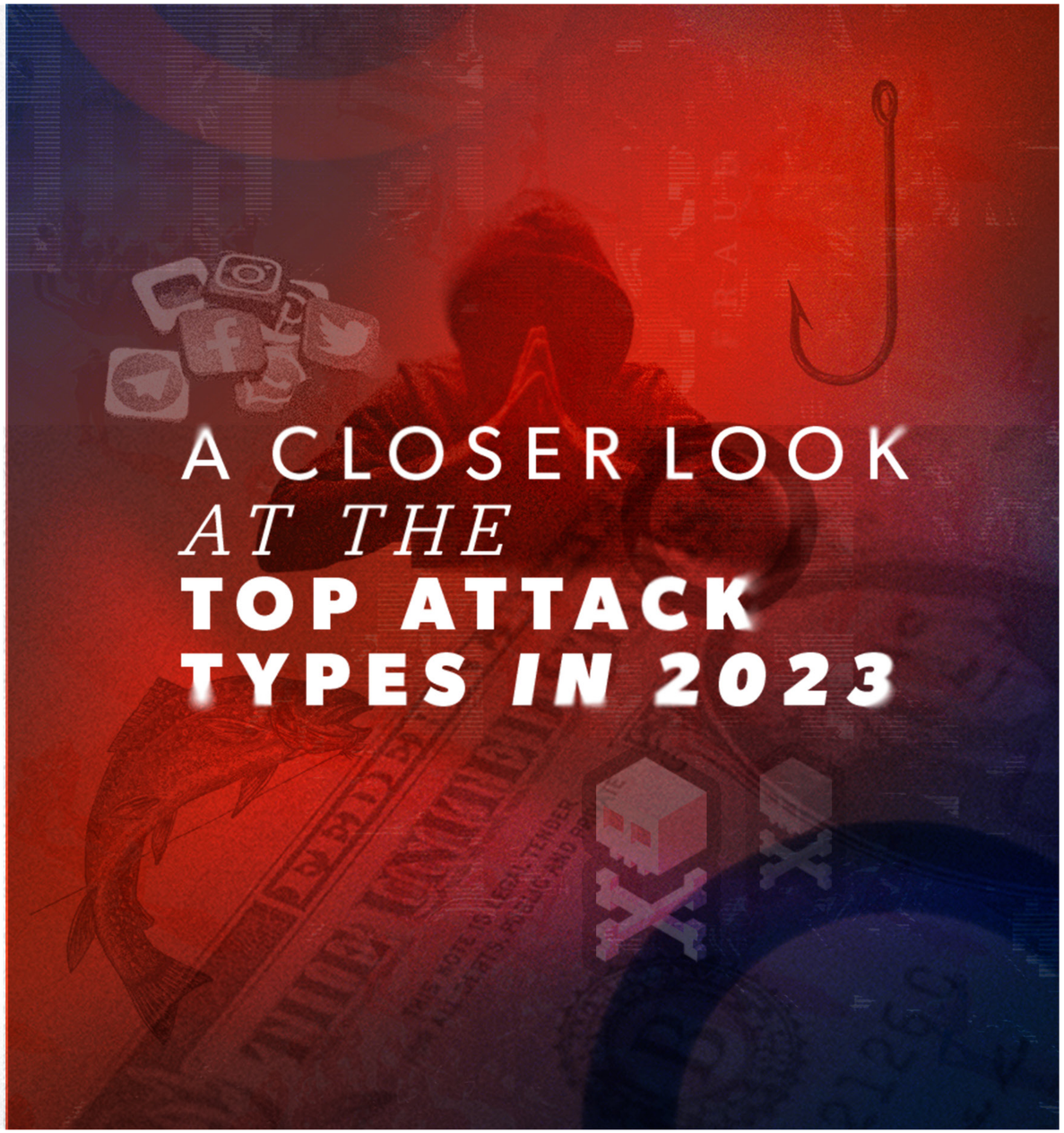
Appgate's Security Operations Center (SOC) analysts tracked these trends in 2023:

- **74%** of fraud incidents were due to phishing; the type of attack most used by cybercriminals
- The second type of attack most used by cybercriminals was the use of unauthorized use of brands (trademark), which represented **17%** of attacks
- Information disclosed were **9%** of the total incidents



TOP 3
Attacks Types in 2023

- Phishing
- Unauthorized use of trademark
- Information disclosed



There is a significant growth of 77% in fraud, when analyzing the year-on-year trends of Appgate's SOC management comparing 2023 vs 2022. Let's see how they increased depending on the type of attack:

- **322%** increase in information disclosure incidents underscores personal and professional data becoming a high-value target
- **81%** increase in phishing incidents underscores the escalating sophistication of attack techniques
- **51%** increase in incidents related to unauthorized use of brands (trademark) underscores the trend of cybercriminals continuing to impersonate a brand to attack users/customers

TREND ANALYSIS: 2022 vs. 2023

A DEEPER DIVE INTO PHISHING ATTACKS

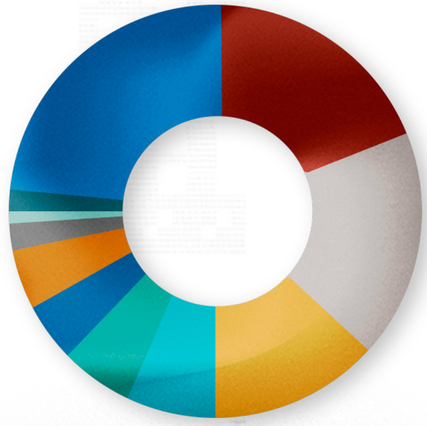
Our SOC findings reveal a concerning trend ... phishing attacks surged by an alarming 81% between 2022 and 2023. This sharp increase underscores the persistent and adaptive nature of cybercriminals who continue to exploit vulnerabilities with heightened sophistication. As organizations navigate an increasingly digital world, the prevalence of phishing underscores the critical importance of robust cybersecurity measures. Appgate's cutting-edge solutions not only address current threats but are strategically engineered to anticipate and counteract emerging threats, providing a proactive defense against the escalating threat of phishing attacks.

According to the Anti-Phishing Working Group, a global industry association, "In the first quarter of 2023, APWG observed 1,624,144 phishing attacks. This is a record high in our observations -- the worst quarter for phishing that APWG has ever observed.

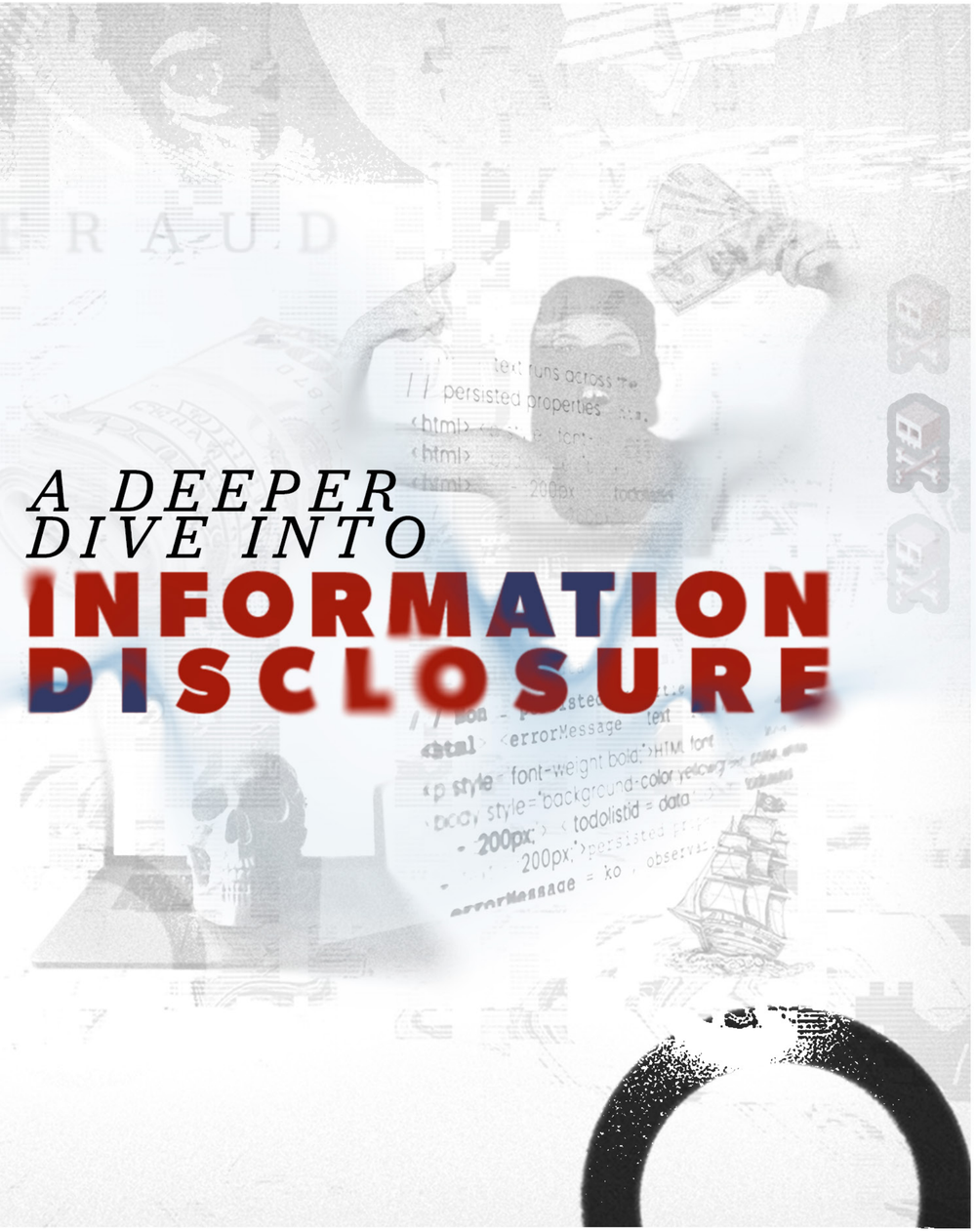
The total was up from 888,585 in 4Q 2022, and above the 1,270,883 phishing attacks in 3Q 2022, which was the record at the time.

TOP INDUSTRIES TARGETED BY PHISHING ACCORDING TO THE APWG:

Financial Institution	*23.5%*
SaaS, Webmail	*18.8%*
Social Media	*18.2%*
Other	*12.9%*
Logistics/Shipping	*7.0%*
Payment	*5.4%*
Telecom	*4.6%*
eCommerce/Retail	*4.3%*
Government	*2.3%*
Crypto	*1.6%*
Gaming	*1.4%*



A DEEPER DIVE INTO INFORMATION DISCLOSURE



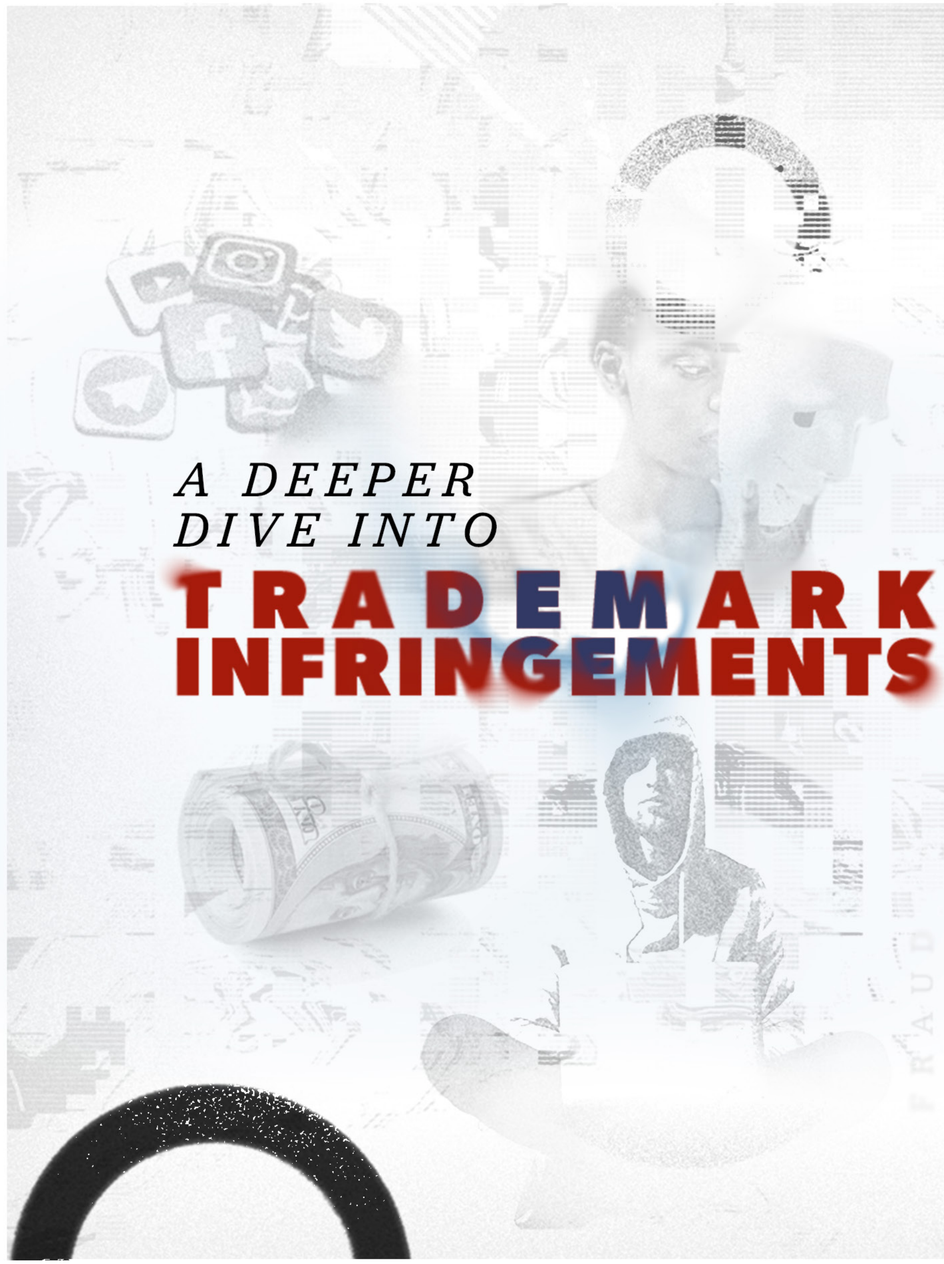
There was a notable 322% increase in information disclosure attacks, but how can this affect your organization? Information disclosure incidents pose significant risks to individuals and organizations, as the exposed data could be exploited for malicious purposes such as identity theft, financial fraud, or corporate espionage. It's crucial for businesses to implement robust cybersecurity measures, conduct regular assessments, and deploy advanced solutions to detect and mitigate vulnerabilities. The likelihood of information disclosure incidents and ensures the protection of sensitive data.

Information leaks in 2023 had a significant impact throughout the year, with organizations experiencing reputational consequences and legal costs. This is in addition to the risk of identity theft and possible consumer fraud, which almost always results in a decrease in trust in the impacted organizations.

The Verizon 2023 Data Breach Investigations report highlights that 74% of all violations include the human factor as an attack inducer (error, abuse of privileges, use of stolen credentials or social engineering). The same report shows that in 83% of violations there is the presence of internal actors, where the main motivation for the attacks continues to be economic benefit in 95% of cases. In addition, the report identifies credential theft, phishing and vulnerability exploitation as the three main ways attackers gain access to an organization's network.

Along these lines, **information disclosure attacks are expected** to continue growing in frequency and impact by 2024.

During 2023, the average cost of a data breach reached a historic level of USD 4.45M. In the specific case of Latin America, the average cost increased by 32% compared to 2022. reaching USD 3.86M, the above according to a report from IBM - Cost of a Data Breach Report 2023.



A DEEPER DIVE INTO

TRADEMARK INFRINGEMENTS

There was a substantial **51% increase in incidents** related to the unauthorized use of brands, specifically trademark infringements. This surge underscores the growing threat posed by cybercriminals exploiting brand identities for malicious purposes.

Protecting the integrity of a brand is paramount in today's digital landscape, where unauthorized usage can lead to reputational damage, loss of consumer trust, and financial repercussions.

Appgate's cybersecurity and fraud solutions and services are crafted to detect and mitigate such incidents promptly and provide proactive measures to safeguard your brand's digital presence.

ON RADAR: MOBILE ATTACKS

Our analysis reveals a concerning shift ... malicious attacks have transitioned from desktop browsers to mobile apps and devices, aligning with the increased online presence of end users on mobile platforms. Cybercriminals are adeptly exploiting security vulnerabilities and employing various techniques such as SMS phishing and QRishing to compromise mobile devices and exfiltrate sensitive data, posing a significant threat to account security.

It is crucial to recognize the paramount importance of staying ahead of these trends, especially given the central role mobile devices play in our daily lives. This holds particular significance for financial services organizations, where the widespread use of peer-to-peer (P2P) applications by consumers adds an additional layer of vulnerability.

While it may be impossible to control or limit users' activities on their devices, organizations can take proactive measures to reduce their mobile risk exposure.

Appgate's cybersecurity solutions are tailored to address these dynamic threats, offering robust protection against mobile attacks and empowering organizations to safeguard sensitive data effectively.

In the Faces of Fraud 2023 survey, we asked respondents about their experience with mobile fraud and these were the results:

35%
Increase in fraud across the mobile channel

30%
More SMS attacks

28%
Increased creation of fraudulent accounts through the mobile channel

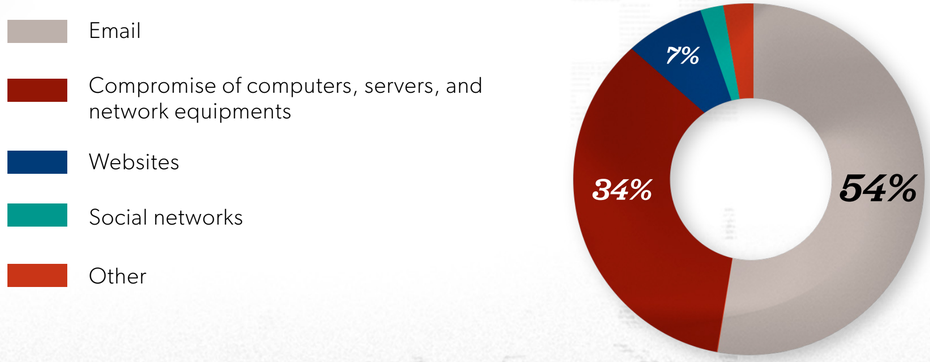
ON RADAR: MALWARE

Malware as a service (MaaS) is a popular trend that cybercriminals use to weaponize malicious campaigns. It has created a complex cyber black market network that creates a threat actor entry point that can be used for more sophisticated attacks.

As cyberthreats evolve, cybersecurity solutions must also evolve to stay ahead of bad actors. So, when a new MaaS threat is created, its fundamental goal is to evade and hide from the offensive threat hunting and proactive defensive measures of targeted organizations. Anti-virus solutions, for example, will try to scan the file or a code loaded directly in the memory using various methods and techniques to look for suspicious characteristics or behaviors. That's why a malware campaign needs to leverage creative methods to make payloads undetectable by intended victims ... at least for a little while.

At Appgate, we have a proprietary malware analysis tool developed by the MART team that allows for rapid assessments of a wide range of malware attacks. This is a powerful tool to combat cyberthreats because, according to the IBM - Cost of a Data Breach Report 2023, the impact of cyberattacks on financial institutions is significant as they lose approximately USD $5.9M per data breach and the primary methods for spreading malware in organizations are through email (54%) and compromise of computers and servers (35%).

Malware reaches individuals' devices when users visit infected websites (55%) or open attachments and links in emails (29%). Official app stores can also become sources of infection when attackers manage to bypass security systems and pass off their programs as legitimate.

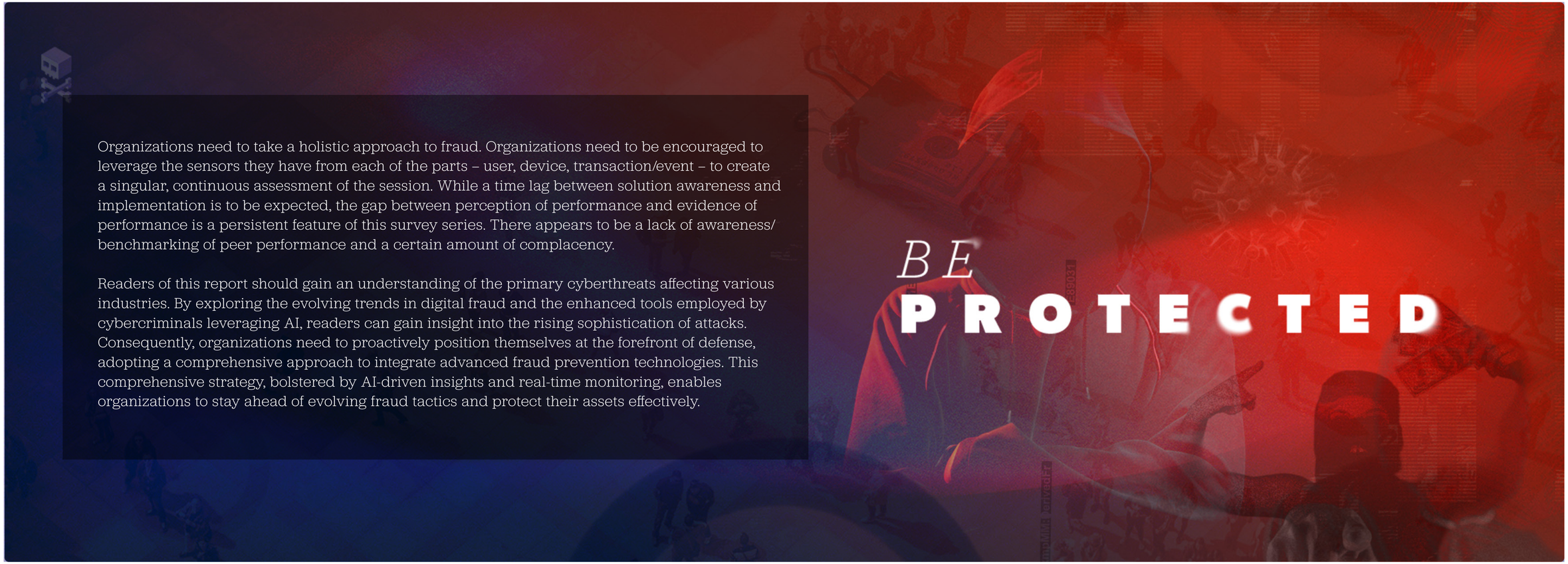


According to the 2023 Faces of Fraud report, the most concerning types of fraud attacks are:

- **52%** of respondents specified information disclosure: Safeguarding sensitive data becomes paramount to mitigate the risks associated with information exposure. AI plays a pivotal role in identifying and mitigating potential vulnerabilities by continuously monitoring data access patterns and detecting suspicious activities in real-time.
- **50%** of respondents specified electronic fraud: The pervasive nature of digital financial crime underscores the critical importance of securing online transactions against fraudulent activities. AI-powered fraud detection systems leverage advanced algorithms to analyze vast amounts of transactional data, enabling organizations to detect and prevent fraudulent transactions more effectively.
- **44%** of respondents specified phishing: As one of the most prevalent cyber threats, phishing remains a persistent concern, emphasizing the need for robust defenses against deceptive tactics aimed at stealing sensitive information. AI-driven phishing detection technologies utilize machine learning algorithms to analyze email and website content, identifying phishing attempts with greater accuracy and speed.

As cybercriminals advance TTPs, organizations must remain proactive in implementing comprehensive cybersecurity measures to protect against these emerging threats. Leveraging AI technology, our innovative solutions provide advanced protection and peace of mind in an increasingly digital landscape.

appgate



Organizations need to take a holistic approach to fraud. Organizations need to be encouraged to leverage the sensors they have from each of the parts – user, device, transaction/event – to create a singular, continuous assessment of the session. While a time lag between solution awareness and implementation is to be expected, the gap between perception of performance and evidence of performance is a persistent feature of this survey series. There appears to be a lack of awareness/benchmarking of peer performance and a certain amount of complacency.

Readers of this report should gain an understanding of the primary cyberthreats affecting various industries. By exploring the evolving trends in digital fraud and the enhanced tools employed by cybercriminals leveraging AI, readers can gain insight into the rising sophistication of attacks. Consequently, organizations need to proactively position themselves at the forefront of defense, adopting a comprehensive approach to integrate advanced fraud prevention technologies. This comprehensive strategy, bolstered by AI-driven insights and real-time monitoring, enables organizations to stay ahead of evolving fraud tactics and protect their assets effectively.

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple, and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises, and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.

appgate

FRAUD BEAT ANNUAL REPORT