REPORT

Security Predictions and Recommendations

2024 Key Forecasts

2023 Conclusions

ZeroFox Intelligence

November 2023

Executive Summary

2023 | CONCLUSIONS

Cyber threats are constantly evolving as adversaries leverage new tools and diversify tactics, techniques, and procedures to overcome defenses. At the same time, increasingly turbulent geopolitical events continue to shape threat activity and influence attacker motivations, presenting greater risk and unpredictability for organizations across regions and verticals.

Every day, ZeroFox investigates and responds to the latest threats facing its customers by delivering timely and accurate intelligence to mitigate risks and reduce uncertainty around the evolving threat landscape. In our annual forecast, we share this intelligence with customers and the wider security community by offering insights and predictions for the year ahead while considering activity and trends observed over the previous 12 months. These predictions are accompanied by recommendations to help security teams prepare for the most anticipated threat developments and combat the adversaries behind them.

The ZeroFox Intelligence 2024 Forecast, reflects the collective analysis of our intelligence leaders and experts across the globe—including those operating in the underground—and share our expectations for:

- Ransomware and Digital Extortion
- Initial Access Brokers
- Social Engineering
- Artificial Intelligence
- The Convergence of Cyber and Physical Threats
- Threats to Elections
- Zero-Day Exploits

ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-55%	95-99%

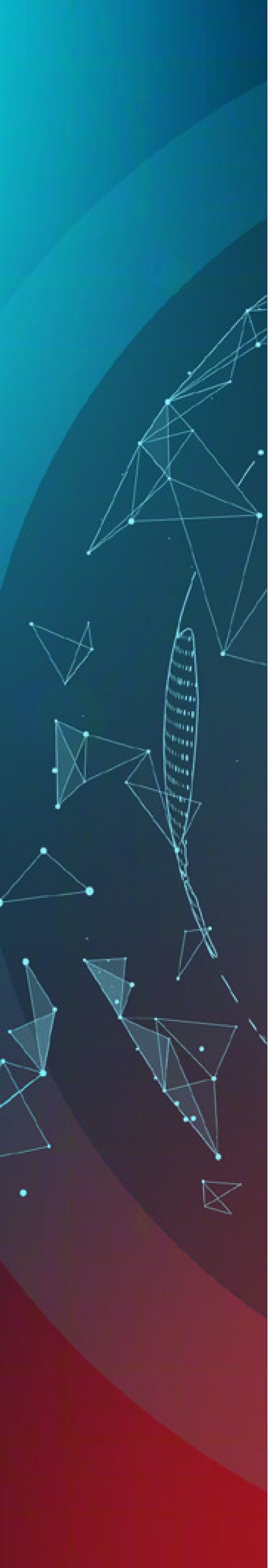


Table of Contents

2024 Key Forecasts

Combining an unmatched depth and breadth of intelligence experience and resources, ZeroFox Intelligence assesses the current threat landscape to determine new, emerging, and evolving threats which security teams can use to plan for 2024 and beyond.

- The threat from ransomware and digital extortion will very likely remain elevated in 2024, following a record number of extortion incidents observed in 2023. Ransomware groups are likely to continue diversifying their targets over the next year, encompassing small to medium-sized organizations that are more likely reliant upon an aging network infrastructure and often lack sufficient cybersecurity awareness and expertise. Additionally, newly-formed ransomware groups are expected to demonstrate proficiency faster than ever before, largely owing to the proliferation of off-the-shelf tools that will continue to lower entry barriers for would-be threat actors.
- Initial access brokers (IABs) will almost certainly continue to pose a significant threat to organizations across industries in 2024. The vast majority of access deals will continue to take place off-forum, as IABs will likely continue to prefer private means of communication to sell access and leverage trusted relationships with specific buyers. Illicit access sales are also very likely to continue underpinning the threat from ransomware operators, with security teams needing to be increasingly aware of IABs targeting them directly and indirectly via their upstream operating partners.
- The threat from social engineering will likely continue on an upward trajectory in 2024.
- Measured growth in the use of artificial intelligence (AI) for both malicious and defensive applications is anticipated, particularly in information operations (including to spread mis-, dis-, and malinformation), social engineering campaigns, and various threat actor tactics, techniques, and procedures (TTPs). It is likely that AI will continue to be leveraged and experimented with to accelerate reconnaissance of high-value or weak targets, to speed the identification and exploitation of vulnerabilities, and to facilitate malicious payload development and delivery.
- Critical infrastructure sectors, such as finance, energy, and healthcare, will likely continue to see the greatest cyber-physical threats. Organizations within these sectors will remain the most attractive targets for threat actors, who are expected to continue pursuing lucrative outcomes in the form of intelligence collection, disruptive impacts, and ransom payments. It is also very likely that geopolitical factors will continue to influence the probability for major cyber events that can have severe or catastrophic physical impacts.
- Multiple key elections taking place in 2024 are expected to drive an increase in various threat actor campaigns throughout the year, including an uptick in election-related scams, disruptive threats, and the spread of disinformation. Both malicious and non-malicious actors will likely increase their use of generative AI and synthetic media to create more effective and persuasive content during 2024 elections, exacerbating the threat posed by mis- and disinformation.
- An uptick in both the discovery and exploitation of zero-day vulnerabilities in 2024 is predicted, likely underpinned by a shift in the tactics of cybercriminal adversaries as they continue to pivot away from traditional methods of data exfiltration toward a heightened focus on exploiting vulnerabilities for increased financial gain.

Ransomware & Digital Extortion

2024 Key Forecasts | 2023 Conclusions

Ransomware and digital extortion will almost certainly pose a significant threat to organizations across industries in 2024. A record number of incidents were observed by ZeroFox Intelligence in 2023, reflecting consistently higher than average activity throughout the year.[1] This now-plateaued trajectory is likely to continue steadily into 2024, with a roughly even chance that Q1 will be characterized by a brief reduction in activity as observed in previous years.[2]

Organizations within the manufacturing and technology sectors will likely continue to face the biggest threat from ransomware and digital extortion. This is due in part to threat actors targeting fragile and increasingly complex supply chains and capitalizing upon the industry's likely low tolerance for operational disruption and subsequent higher payout rates.

Ransomware and digital extortion attacks against U.S.-based organizations are very likely to account for more than 50 percent of global attacks in 2024, as has been observed in previous years.[3] This is due largely to the diversity of potential U.S.-based targets and the country's lucrative digital infrastructure, although deteriorating Russia-US relations and the continued lack of a formal extradition agreement are also likely to continue enticing Russia-based threat actors to conduct attacks with impunity.

Ransomware groups will likely continue to diversify their targets over the next year, encompassing small- to medium-sized organizations that are more likely reliant upon an aging network infrastructure and soften lack sufficient cybersecurity awareness and expertise. Organizations operating networks associated with mass amounts of personal data will likely become increasingly-prized targets, as ransomware groups seek to imitate Clop's successful 2023 targeting of Managed File Transfer (MFT) solutions.[4]

Alongside Clop ransomware groups, such as Medusa Locker, Royal, 8Base, and Play, increased their attack frequency during 2023—as did prominent larger outfits such as APLHV/BlackCat and Lockbit.[5]

A host of newer groups were also observed conducting attacks, with Akira and Lost Trust among the most prolific.[6] Throughout 2023, ransomware groups leveraged an array of new TTPs that are very likely to continue facilitating successful attacks in 2024. The pivoting away from encryption in favor of data exfiltration is one such adaptation, likely utilized by ransomware groups seeking lower-risk attack methods.[7] An increase in the use of malware facilitating detection evasion has also been observed, as well as double-extortion attacks characterized by the use of numerous attack vectors with the aim of granting the attacker additional leverage over the victim.[8]

[1] ZeroFox Internal Collections

[2] ZeroFox Internal Collections

[3] ZeroFox Internal Collections

[4] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-158a

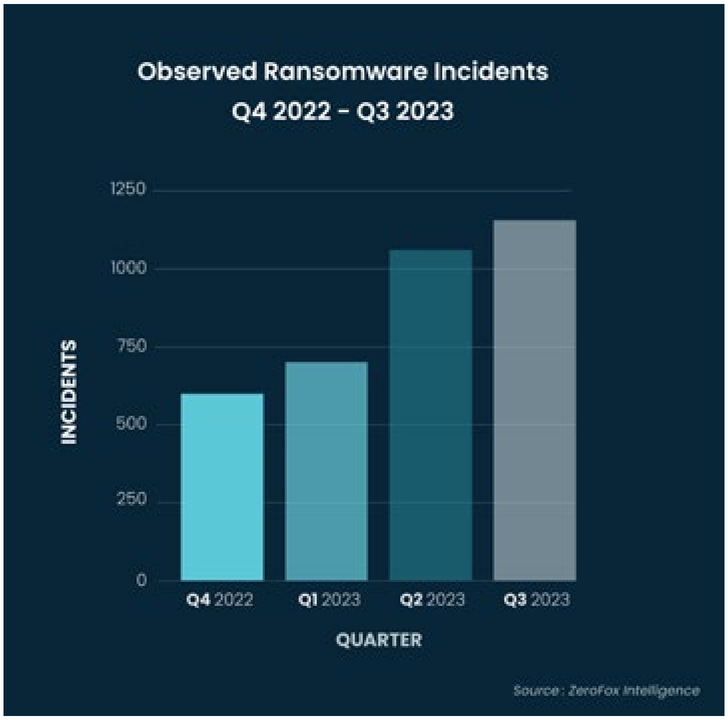
[5] ZeroFox Internal Collections

[6] ZeroFox Internal Collections

[7] hXXps://www.axios[.]com/2023/01/13/ransomware-gangs-cut-out-encryption

[8] hXXps://www.bleepingcomputer[.]com/news/security/fbi-dual-ransomware-attack-victims-now-get-hit-within-48-hours/

Newly-formed ransomware groups are expected to demonstrate proficiency faster than ever before in 2024, due to a number of proliferating as-a-service tools that continue to lower entry barriers to would-be threat actors. Ransomware-as-a-Service (RaaS) models are likely to continue becoming more competitive in deep and dark web (DDW) marketplaces, leading to the availability of increasingly sophisticated attack tools, more comprehensive exploitation kits and cheaper options affordable to lower-level threat actors. Financially motivated actors will likely also find themselves increasingly able to obtain critical network vulnerabilities which can be leveraged in ransomware attacks. This follows a current trend of critical vulnerabilities very likely becoming more numerous, exacerbated by the growing affluence of prominent threat groups that are increasingly able to purchase expensive zero-day vulnerabilities. [9]



Source : ZeroFox Intelligence

Recommendations from ZeroFox Intelligence

- Ensure critical data is backed up to secure off-site or cloud servers. Sensitive or proprietary data should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.
- Maintain a comprehensive understanding of the organization's technology stack and implement a patch-management process. Prioritization should not disregard vulnerabilities of a lower criticality, which may already be exploited "in the wild."
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures, and key authorities.
- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new ransomware targets.

[9] hXXps://www.csoonline[.]com/article/648572/ransomware-victim-numbers-surge-as-attackers-target-zero-day-vulnerabilities.html

Initial Access Brokers

2024 Key Forecasts | 2023 Conclusions

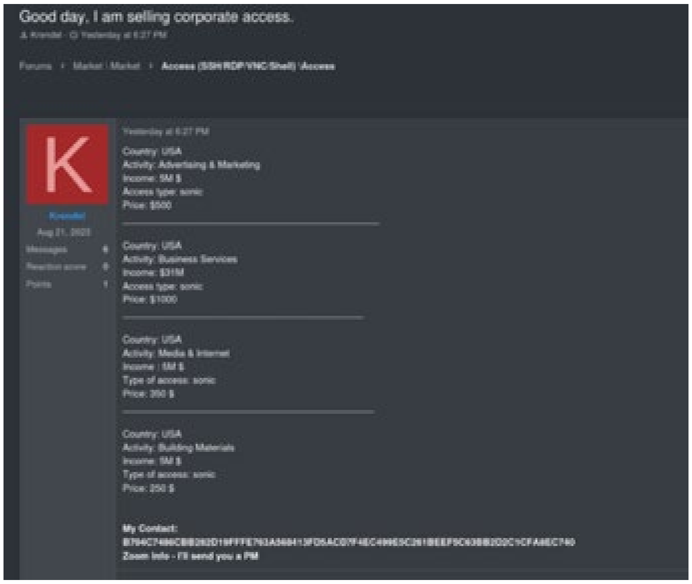
IABs continue to pose a significant risk to the cyber threat landscape, both private and public sector alike. Throughout regular (DDW) threat actor engagements, ZeroFox noted a significant increase in attack vectors shifting toward third-party vendors of major corporations and government entities.

This is due to the potentially weaker security postures of third parties hired by larger organizations, and the elevated privileges and accesses that come with being integrated into the larger entity. Compared to previous quarters, ZeroFox Intelligence noted a high, but similar, number of instances of brokers selling access on major DDW forums.

ZeroFox recommends configuring devices with the principle of Zero Trust and least privilege.

Of note, ZeroFox Intelligence observed a large number of private, off-forum sales taking place under the radar, between access brokers, and (typically) ransomware actors and affiliates, in addition to those attempting direct extortion plays with data exfiltration. The vast majority of access deals likely take place off-forum, as observed by researchers that are directly engaged with access brokers on covert channels. Moreover, the cost of securing said accesses off-forum are significantly lower, meaning frequent buyers of accesses can arrange discounts and even be alerted in advance to upcoming accesses that will be listed for sale. In some cases, these special arrangements lead to ransom attacks that cannot be predicted by DDW monitoring-only prevented by a tight security posture and proper training against social engineering, phishing, good company cyber hygiene, et cetera.

VPN access to four separate U.S.-based companies advertised on the predominantly Russian language Deep Web forum "RAMP."


Good day. I am selling corporate access.

Krendel · Yesterday at 6:27 PM

Forums › Market \ Market › **Access (SSH/RDP/VNC/Shell) \Access**

Krendel

Aug 21, 2023

Messages 6

Reaction score 0

Points 1

Yesterday at 6:27 PM

Country: USA
Activity: Advertising & Marketing
Income: 5M $
Access type: sonic
Price: $500

Country: USA
Activity: Business Services
Income: $31M
Access type: sonic
Price: $1000

Country: USA
Activity: Media & Internet
Income : 5M $
Type of access: sonic
Price: 350 $

Country: USA
Activity: Building Materials
Income: 5M $
Type of access: sonic
Price: 250 $

My Contact:
B794C7486CBB282D19FFFE763A568413FD5ACD7F4EC499E5C261BEEF5C63BB2D2C1CFA6EC740
Zoom Info - I'll send you a PM

Source: ZeroFox Intelligence

Through direct engagement, ZeroFox researchers observed that each access broker, unsurprisingly, has a set of proprietary tools that enable network or server compromise, and that they typically focus exclusively on that attack vector, assuming the broker is carrying out the attacks. In some cases, certain individuals carry out the attacks, and others specialize in brokering the access deal on DDW. These tools range from scanning and brute forcing tools, to social engineering techniques, to zero-day exploits. Similarly, certain access brokers specialize in only one operating system (OS), which, as would be expected, tends to be their OS of choice.

Recommendations from ZeroFox Intelligence

- Proactively monitor for potential network access sales to obtain critical early warning of an impending cyberattack and to help identify malicious actors, including insiders, meaning to harm your network.
- Configure devices with the principle of zero trust and least privilege.
- Periodically review edge device configurations and audit perimeter security.
- Regularly scan for software updates and implement them as quickly as practical.
- Enable multi-factor authentication (MFA) wherever possible.
- Disable PowerShell wherever possible.
- Employ ZeroFox Threat Intelligence feeds to get ahead of threat actor activity.

Social Engineering

2024 Key Forecasts | 2023 Conclusions

The threat from social engineering will likely remain on an upward trajectory in 2024. Threat actors continue to evolve traditional phishing techniques such as the use of malicious attachments, delivered by email or popular messaging applications such as Zoom and MS Teams.[10] Microsoft's disabling of default VBA macros in its Office program will very likely continue driving an increase in both the use of file types omitting mark-of-the-web controls, such as archive files (RAR) and Windows Shortcut files (LNK), and the use of Adobe, Google, and Dropbox files to facilitate HTML smuggling.[11]

Attacks associated with search engine optimization (SEO) poisoning are very likely to remain a threat, as threat actors continue to find success in leveraging SEO cloaking—the manipulation of search engine web crawlers, malicious redirects, and website compromise attacks. When conducting look-alike domain and email spoofing attacks, threat actors are likely to increasingly harness the perceived authenticity offered by the use of paid TLDs, such as .com, rather than free ones, such as .tk and .ga.

The use of real-time, MFA-bypassing techniques is very likely to continue on an upward trajectory, as threat actors circumvent the popular and fast-proliferating tool often considered secure. MFA fatigue and OAuth consent phishing are likely to remain threats, and various types of "in-the-Middle" (itM) attacks capable of token theft and session hijacking are very likely to become increasingly sophisticated and more difficult to detect.

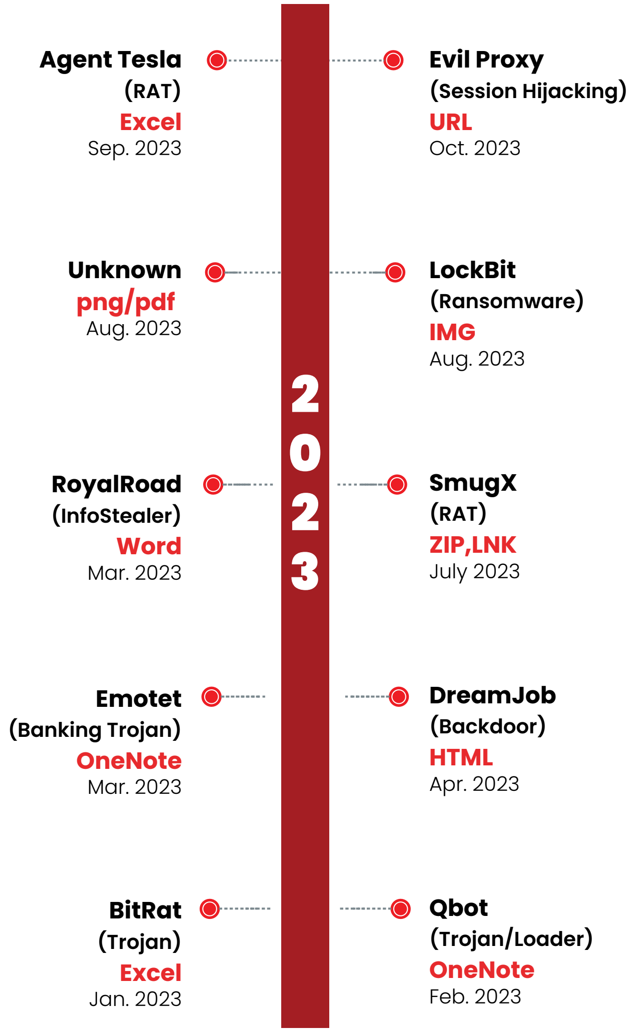
> *ZeroFox recommends adopting an organization-wide zero-trust cybersecurity architecture, ensuring that access to devices, networks and information is kept at what is minimally required for operations based upon a principle of least privilege.*

[10] hXXps://www.bleepingcomputer[.]com/news/security/microsoft-teams-phishing-attack-pushes-darkgate-malware/

[11] hXXps://learn.microsoft[.]com/en-us/deployoffice/security/internet-macros-blocked

Phishing-as-a-Service (PhaaS) operations are very likely to continue proliferating in DDW marketplaces, with off-the-shelf packages offering services of an increasingly-wide range of prices and sophistication. These services will very likely continue to lower the barriers to entry for threat actors, enabling less technically-skilled individuals to conduct itM, MFA-bypassing, and session stealing attacks.

Phishing campaigns leveraging malicious attachments Jan. 2023 - Oct. 2023



Source: ZeroFox Intelligence

Recommendations from ZeroFox Intelligence

- Adopt an organization-wide, zero-trust cybersecurity architecture, ensuring that access to devices, networks, and information is kept at what is minimally required for operations based upon a principle of least privilege. Continuously test and scrutinize the legitimacy of trust in place.
- Ensure staff are educated on contemporary social engineering techniques, emerging trends, and how to report suspected phishing attempts.
- Protect remote end-point devices with phishing-resistant MFA protocols compliant with FIDO2 or PKI standards. Introduce WebAuth security with the use of external, physical authenticators. Perform risk assessments to identify high-risk devices, networks, and individuals.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.

Threats from Artificial Intelligence

2024 Key Forecasts | 2023 Conclusions

Measured growth in the use of AI is expected for both malicious and defensive applications, particularly in information operations (mis-, dis-, and malinformation), social engineering, and traditional cyber TTPs. The complicated nature of AI, as well as the complexity of leveraging it, will lead to a modest but steady increase in the capability to defend, inform, protect, and, unfortunately, abuse digital and cyber assets and the people who rely on them.

In the case of information operations, AI will continue to be used in support of malicious activities such as impacting elections and stirring discontent. It will also be used to accelerate the pace and realism of media used to trick victims into divulging high-value credentials and other sensitive information. Lastly, attempts will be made to repurpose open-source and commercial tooling not only to generate malicious media, but also to accelerate reconnaissance of high-value or weak targets, speed the identification and exploitation of vulnerabilities, and facilitate malicious payload development and delivery.

Recommendations from ZeroFox Intelligence

- Enhance your current cybersecurity program to formally account for the risks and rewards of AI, including hiring or contracting a subject matter expert (SME) to support activities that involve leveraging AI for defensive purposes and defending from AI-enabled threats.
- Take increasing advantage of AI-enabled open source cybersecurity tooling as well as commercial solutions to strengthen the efficacy of your cybersecurity program.
- Maintain situational awareness and a strong operational response capability regarding AI-enabled threats by heavily leveraging ZeroFox Enterprise and ZeroFox Intelligence capabilities.

Convergence between Cyber & Physical

2024 Key Forecasts | 2023 Conclusions

The growing threat posed by cyber-physical convergence—that is, the physical impact resulting from a cyberattack, or vice versa—will continue to be driven by a multitude of factors, including (but not limited to) digital transformation strategies, technological advancements, geopolitical events, and the constantly-evolving threat landscape. Broadly underpinning the threat is the proliferation of internet of things (IoT) devices and their adoption within commercial and industrial environments and the merging of information and operational technology (IT/OT) infrastructure. This, along with the absence of secure design principles and device security in many IoT/OT networks, continues to rapidly expand the attack surface and weaken network security, posing significant and enduring challenges for both cyber and physical security teams across industries.

The greatest cyber-physical threats will continue to lie within critical infrastructure sectors such as finance, energy, and healthcare, where organizations and facilities face the most significant risk from physical disruption and are unable to afford even minor periods of operational downtime. These sectors will almost certainly remain the most attractive targets for most nation-state or state-sponsored actors as well as ransomware collectives, who are expected to continue pursuing the most lucrative outcomes in the form of intelligence collection, disruptive impacts, and ransom payments. Such threat actors will continue to leverage and develop custom-made tools for targeting critical IT/OT infrastructure, allowing them to compromise networks and laterally move to establish footholds in supply chains, or disrupt the target organization's operations directly. In addition, many critical infrastructure organizations also continue to rely on legacy equipment that is often outdated or no longer maintained, such as industrial control systems (ICS) or healthcare equipment, further increasing their risk. Key trends observed in 2023 highlight this, including an increase in vulnerabilities discovered in OT infrastructure (particularly within ICS) and an increase in OT and IoT-specific malware.[12] [13]

Geopolitical factors will very likely continue to influence the probability for major cyber events that can have severe or catastrophic physical impacts.
For instance, it is likely that Russia will continue to conduct disruptive and destructive cyberattacks against Ukraine (and other nations in support) in response to developments on the ground. Notably in 2023, Russian state-backed threat actors were observed pivoting from their focus on conducting destructive attacks on Ukraine's critical infrastructure in favor of espionage campaigns targeting law enforcement, private businesses, and media organizations. Similarly, while military conflict between China and Taiwan is unlikely in 2024, further deterioration in China-Taiwan relations would very likely result in China escalating the severity of its offensive cyber campaigns against Taiwan's infrastructure, increasing the chances of significant physical implications.

Recognizing the growing threats facing critical infrastructure, governments across the globe noticeably increased their efforts to establish stronger cybersecurity standards in 2023, with a focus on securing sectors that are integral to human safety, national security, and economy. This includes the European Union NIS 2 Directive released in January 2023, the U.S. National Cybersecurity Strategy in March 2023, and the revision of Australia's 2018 Security of Critical Infrastructure, also in March. In short, these frameworks introduce many new regulations that aim to improve the capabilities and processes to prevent, detect, and respond to security incidents specifically within critical sectors. While such measures will likely continue to strengthen the security and resilience of critical sectors in the long term, these are unlikely to significantly reduce the threat over the next 12 months; security for IoT and OT will very likely struggle to keep up with the overall pace of

Recommendations from ZeroFox Intelligence

- Given the increasing convergence between cyber and physical threats, greater collaboration between physical and cybersecurity teams is becoming more necessary. Organizations should look to establish strong communication between their security pillars, ensuring that they have access to real-time alerting tools and technology that can help proactively get ahead of the incidents that could have operational impacts on bo7th sides of the house.
- Organizations should subscribe to ZeroFox Intelligence monitoring and alerting to maintain awareness and keep apprised of geopolitical developments that may impact their operations, as well as have broader cyber and physical ramifications.

The greatest cyber-physical threats will continue to lie within critical infrastructure sectors, such as finance, energy, and healthcare, where organizations and facilities face the most significant risk from physical disruption.

[12] hXXps://synsaber[.]com/resources/research-reports/ics-cve-reports/ics-cve-research-first-half-2023

[13] hXXps://www.nozominetworks[.]com/blog/new-nozomi-networks-labs-report-august-2023

Threats to Elections

2024 Key Forecasts | 2023 Conclusions

An increase in malicious activity targeting elections is expected in 2024, including an uptick in scams, hacktivism, and the spread of disinformation.
The U.S. presidential election in November 2024 will act as the culmination to a series of crucial elections taking place across the globe next year and will draw the attention of both financially-and politically-motivated threat actors. The U.S. poll is also likely to dominate media interest due to controversies surrounding the election and its previous iterations and since its outcome often impacts the outlook of the global economic and political landscape. However, general elections are also due to be held in countries such as India, Indonesia, Mexico, Taiwan, and the United Kingdom, as well as in the European Parliament—all of which are equally expected to drive an increase in various threat actor campaigns throughout 2024 and shape global geopolitics over the coming years.

> *ZeroFox recommends always questioning the credibility of sources and considering the date the content was published.*

Scams/Social Engineering

A rise in social engineering campaigns is anticipated in 2024, targeting audiences, election workers, and government officials, and organizations. Threat actors invariably aim to capitalize on the heightened interest and media coverage of high-profile elections to conduct financial fraud, harvest credentials, compromise networks, and deploy malicious payloads. Therefore, election-themed phishing lures and scams, such as fraudulent voter registrations, surveys, and donations, and malicious domains impersonating legitimate election-related websites are very likely to increase.

Individuals and organizations connected to the events, such as government and media entities or trusted third-parties, will also likely face an increased threat from tailored spear-phishing campaigns. There will also likely be a rise in social media impersonations of election campaign officials for the purpose of baiting potential followers into scams and interacting with malicious attachments.

Disruptive / Destructive Attacks / Hacktivism

Disruptive and destructive attacks are likely to impact election-related organizations and infrastructure. Disruptive attacks are almost certain to increase before and during elections, and are most likely to occur through data leaks, website defacements, and distributed denial-of-service (DDoS), whereas ransomware attacks could pose both a disruptive and destructive threat depending on the specific aim of the threat actors. Notably, the August 2023 exposure of compromised voter data in the United Kingdom highlights threat actors' desire to target election infrastructure.[14] While this incident is unlikely to directly influence the outcome of the United Kingdom's election next year, such attacks can have equally damaging consequences in that they could erode public confidence in the integrity of democratic processes, and the security of the state itself.

Politically-motivated hacktivists will be highly intent on increasing efforts to disrupt electoral processes and access to public infrastructure ahead of the 2024 elections. For instance, Russian-aligned actors and hacktivist collectives, such as KillNet and its affiliates, remain motivated to campaign against Western nations or those in opposition to Russia's invasion of Ukraine, and are very likely to target the U.S. and other Western elections in an attempt to undermine state institutions. However, attacks are likely to be largely confined to the defacement and temporary denial of service to websites associated with elections; they are unlikely to cause significant or catastrophic impact to the events or affect their outcome.

Disinformation

The threat from disinformation campaigns is almost certain to increase in the lead up to, during, and following the U.S. and other key elections in 2024. Disinformation—along with misinformation and, to a lesser extent, malinformation—has become pervasive during election cycles, increasingly blurring the line between fact and fiction and growing more capable of causing reputational damage to individuals and organizations. Over the next 12 months, disinformation will be propagated by both state and non-state actors (foreign and domestic) in an attempt to influence and provoke audiences, undermine and discredit political figures and the integrity of results, and shape favorable policy decisions to suit political and strategic goals. Such actors will continue to leverage a variety of traditional and social media platforms to amplify their narratives, including—but not limited to—inauthentic news websites, compromised accounts, false personas, bot networks, streaming services, messaging applications, and dark web channels.

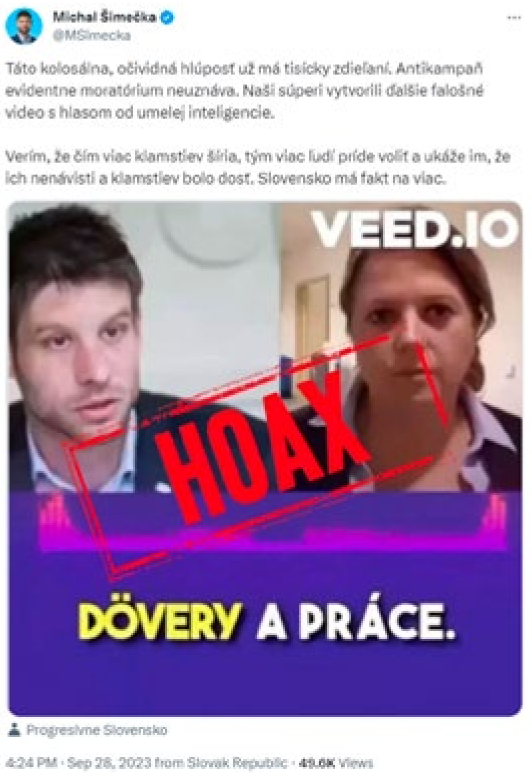
As observed in previous election cycles, influence operations are expected to weaponize disinformation to target specific audiences and micro-communities by leveraging frequently disputed issues; threat actors will attempt to widen existing ideological and societal divisions and, in some cases, incite unrest. U.S. voters, for instance, are very likely to experience an increase in distorted facts and manipulated media relating to race relations, immigration, border control, and gun policies. Broader geopolitical topics such as immigration, gender rights, climate and environmental concerns, and the ongoing Russia-Ukraine conflict will also be leveraged in tandem with localized issues and equally manipulated to influence audiences. Disinformation actors will also remain opportunistic and capitalize on incidents as they unfold to elicit extreme or reactionary responses, as most recently demonstrated by the wave of disinformation surrounding events pertaining to the Israel-Hamas War in October 2023.[15]

Threat actors, as well as political figures, will likely increase their use of generative AI tools and synthetic media to create more effective and persuasive content in 2024. In addition, ZeroFox Intelligence also predicts that the use for sophisticated, AI-driven disinformation to create major political scandals will increase next year; this which could significantly impact public

[14] hXXps://www.electoralcommission[.]org[.]uk/media-centre/electoral-commission-subject-cyber-attack
[15] hXXps://www.zerofox[.]com/blog/navigating-the-mis-and-disinformation-minefield-in-the-current-israel-hamas-war/

perception of electoral candidates, or have physical security implications, such as political protests and acts of violence. Many high-profile examples observed throughout 2023 illustrated the threat posed by deepfakes and other forms of AI-generated text, audio, and images when leveraged as a tool to spread disinformation for political gain.[16] [17] [18] Moreover, these incidents also highlighted a growing appetite for political candidates to openly leverage AI-generated content to discredit and undermine opposition figures. Such occurrences are expected to develop in 2024 due to the notably high number of national-level elections being held globally, as well as the advancement of AI capabilities and continued experimentation of tools by both malicious and non-malicious actors.

In the run up to Slovakia's general election in September 2023, a deepfake of politicians discussing how to commit electoral fraud spread across social media platforms, casting doubt among voters.



Michal Šimečka
@MSimecka

Táto kolosálna, očividná hlúposť už má tisícky zdieľaní. Antikampaň evidentne moratórium neuznáva. Naši súperi vytvorili ďalšie falošné video s hlasom od umelej inteligencie.

Verím, že čím viac klamstiev šíria, tým viac ľudí príde voliť a ukáže im, že ich nenávisti a klamstiev bolo dosť. Slovensko má fakt na viac.

Progresívne Slovensko

4:24 PM · Sep 28, 2023 from Slovak Republic · 49.0K Views

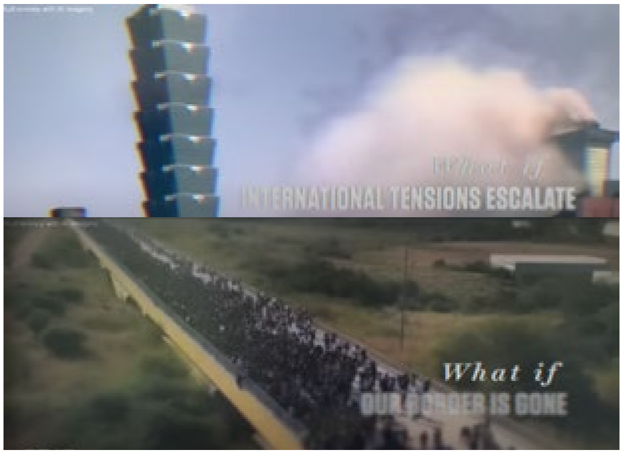
Source: hXXps://fakty.afp[.]com/doc.afp.com.33WY9LF

Recommendations from ZeroFox Intelligence

To combat against the threat of disinformation:

- Always question the credibility of sources and consider the date the content was published.
- Use fact-checking websites like FactCheck.org, the News Literacy Project, and NewsGuard.
- For individuals or organizations that find themselves a victim of disinformation, have a crisis response plan in place to evaluate the content and formulate an approach to neutralize and contain the incident.
- Utilize the ZeroFox Platform to identify and mitigate the threat of executive impersonation.

In April 2023, a Republican National Committee ad against President Biden was created entirely with AI-generated images that depicted fictional crises in the event that Biden is re-elected.



Source: hXXps://www.youtube[.]com/watch?v=kLMMxgtxQ1Y

[16] hXXps://www.electoralcommission[.]org[.]uk/media-centre/electoral-commission-subject-cyber-attack
[17] hXXps://www.forbes[.]com/sites/mattnovak/2023/04/25/gop-releases-first-ever-ai-created-attack-ad-against-president-biden/?sh=480ff75e219a
[18] hXXps://fortune[.]com/2023/05/15/turkeys-deepfake-influenced-election-spells-trouble/

Zero-Day Exploits

2024 Key Forecasts | 2023 Conclusions

Traditionally, zero-day exploits-renowned for their efficacy and scale-have been the purview of well-funded, nation-sponsored groups as they come at a premium and possess a limited lifespan due to rapid patching once identified. In 2024, a shift in the tactics of cybercriminal adversaries is anticipated as they pivot away from traditional methods of data exfiltration towards a heightened focus on exploiting vulnerabilities for increased financial gain. Notably, ransomware collectives like CL0P are actively engaged in the development of zero-day exploits, resulting in a significant annual rise in victim counts.

Attackers are expected to prioritize characteristics inherently associated with zero-day exploits in their exploits: stealth and simplicity. While the discovery of such vulnerabilities requires substantial resources and carries a brief window of opportunity, it does not guarantee successful exploitation. Nevertheless, an uptick in both the discovery and exploitation of zero-day vulnerabilities is expected. Furthermore, the spectrum of targeted software, encompassing (IoT) devices and cloud solutions, is poised to expand-accompanied by a diversification of actors involved in exploiting them.

To counter the evolving threat landscape of zero-day exploitation in 2024, organizations should focus on:

- Continuous vulnerability assessment
- Proactive patch management
- Zero-day readiness
- Comprehensive user training
- Network segmentation
- Behavior-based security measures
- Threat intelligence integration and sharing
- Multi-factor authentication
- Robust data backup strategies
- Well-practiced incident response drills

Such proactive measures are critical to enhancing cybersecurity resilience in the face of these evolving risks.

About ZeroFox

The leader in External Cybersecurity

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-aservice 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.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400