

► REPORT

ZeroFox Intelligence **2022 Conclusions / 2023 Forecast**

Security Predictions and Recommendations



JANUARY 2023

Table of Contents

Executive Summary	3
2022 Conclusions	3
2023 Forecast & Recommendations	4
Ransomware	5-7
Multi-Factor Authentication Exploitation	8-9
Malware	10-11
Exploits and Vulnerabilities	12-13
Initial Access Brokers	14-15
Social Engineering	16 - 18
Convergence between Cyber and Physical	19- 22



Executive Summary

2022 | CONCLUSIONS

Geopolitical developments throughout the world, in particular the war in Ukraine, were influential on cybersecurity in 2022. This war greatly disrupted cyber threat actor collaboration and focus areas and likely influenced a 2022 drop in observed ransomware and digital extortion from a 2021 peak, although the threats to organizations remained high.

Additional observations included threat actors increasingly moving towards real-time multi-factor authentication (MFA)-bypassing solutions and leveraging phishing techniques in which traditionally-strong MFA gives little or no protection. The number of illicit access sales posted in open forums in 2022 also fell in number from the 2021 peak, likely reflecting limitations to the supply from Initial Access Brokers (IABs) rather than reduced demand from buyers. The fall in activity is likely explained by Russia's invasion of Ukraine, with some IABs implicated in the conflict; continued disruption to underground marketplaces (e.g., RaidForums) where access sales have appeared regularly; and IABs seeking more private or direct communication methods to sell illicit access. There has also likely been a shift towards brokers preferring private channels rather than advertising in forums to avoid law enforcement scrutiny.

Information stealers continued to pose a significant threat to individuals and organizations in 2022, with the top five stealers observed by ZeroFox Intelligence in 2022 having been Redline, Raccoon, Vidar, Azorult, and Meta. ZeroFox ingested 312,573,712 total compromised credentials from logs collected this year. ZeroFox Intelligence also observed a notable increase in the number of critical vulnerabilities published within the National Institute of Standards and Technology (NIST) database, and organizations experienced significant challenges associated with those vulnerabilities.

Social engineering remained one of the most prevalent methods leveraged by threat actors in 2022 to harm end-users, targeting companies directly and impersonating them to lure third parties or members of the public. Threat actors continued to evolve their social engineering approach, but the practice did not fundamentally change. The increased use of Adversary-in-the-Middle techniques to bypass MFA—including the increased adoption of widely-distributed phishing kits—demonstrated threat actors' ability to adapt to emerging security practices.

Convergence between the cyber and physical realms continued throughout 2022, and two defining themes emerged. The first involved cyber threat actors attacking organizations, with the cyberattack then ultimately disrupting physical operations. The second theme related to cyber activity accompanying real-world physical developments, as demonstrated frequently during the Russia-Ukraine conflict. While physical conflicts were occurring on the ground, threat actors were concurrently bombarding entities in Russia and Ukraine with cyberattacks, creating multiple attack vectors throughout the conflict. While this is not a new tactic, the amount of effort put forth towards online information battles to sway reporting and public opinion both domestically and internationally has been a significant development.



2023 | **FORECAST & RECOMMENDATIONS**

- Ransomware and digital extortion will very likely remain some of the greatest cyber threats to organizations globally in 2023. ZeroFox Intelligence anticipates an increase in ransomware “hack-and-leak” tactics, with threat actors removing the encryption angle in attacks and instead relying on data exfiltration and ransom demands. It is also likely that payloads deployed by extortion collectives will increasingly incorporate data corruption functionality.
- Threat actors will likely increasingly focus on exploiting weaknesses in MFA in 2023, with a more significant number of attacks against identity and access management services and increased adoption of “in-the-middle” techniques in “as-a-service” offerings.
- Information stealers like Redline, Raccoon, and Vidar will likely be used increasingly, given the longevity of their marketplaces, fueling widespread support from their developers and community. In addition, the extensive range of applications and cryptocurrencies targeted by these information stealers will likely expand and grow in 2023.
- ZeroFox Intelligence assesses that the number of critical Common Vulnerabilities and Exposures (CVEs) reported for 2023 will likely increase, given the general upward trend observed over the past five years.
- ZeroFox Intelligence expects the threat from IABs to continue in 2023, despite the volatility associated with the continuation of Russia’s war in Ukraine. ZeroFox Intelligence anticipates a continued increase in IABs leveraging private means of communication to sell access, as well as leveraging trusted relationships with specific buyers.
- While the social engineering threat is unlikely to change significantly in 2023, threat actors are expected to continue to adapt their techniques, increasingly leveraging more sophisticated approaches into widely-distributed phishing kits. In addition, ZeroFox Intelligence expects an increase in the use of phishing domains and alternative malicious attachments to macro-enabled documents.
- Tactics developed and utilized throughout the war in Ukraine by cyber threat actors to target entities on the opposing side for political gains are likely to be utilized in 2023 to target organizations for financial gains as well.



Ransomware

2022 | CONCLUSIONS

Ransomware and digital extortion remained some of the most significant cyber threats to organizations in most sectors and locations globally, despite a fall in incidents in 2022 compared with the 2021 peak.¹ This was likely caused partly by geopolitical events and increased difficulty eliciting payments from victims. ZeroFox Intelligence observed increased attacks against third-party software providers and upstream supply chains; with the threat compounded by developments in extortion tactics.

Russia's invasion of Ukraine very likely disrupted threat actors' operations. Double extortion² became standard practice, and threat actors leveraged new tactics that included hacking corporate websites to display ransom notes and providing leaked victim data in an open and searchable format.³ The rise of data theft and extortion without any data encryption taking place indicates threat actors possibly view data leaks to be of greater concern to victims than file encryption and operational disruption.⁴

Increased professionalization of the cybercriminal marketplace made it easier for threat actors to conduct intrusions, exfiltrate data, and deploy payloads. The growth of Ransomware-as-a-Service (RaaS) lowered the barriers to entry and drove diversification in the Tactics, Techniques, and Procedures (TTPs) observed across deployments of a given payload, making identification and disruption more difficult.⁵ Ransomware attacks increasingly involved a web of interconnected parties: IABs selling access; developers providing encryption and exfiltration tooling; and ransomware affiliates deploying payloads against the victim and managing ransom negotiations.



Increased adoption of stronger MFA types, such as phishing-resistant MFA, will likely drive threat actors to target identity and access management providers directly.

¹ ZeroFox Intelligence Internal Collections

² Double extortion is a tactic used by ransomware threat actors to not only encrypt a victim's data, but also exfiltrate and sell the stolen data.

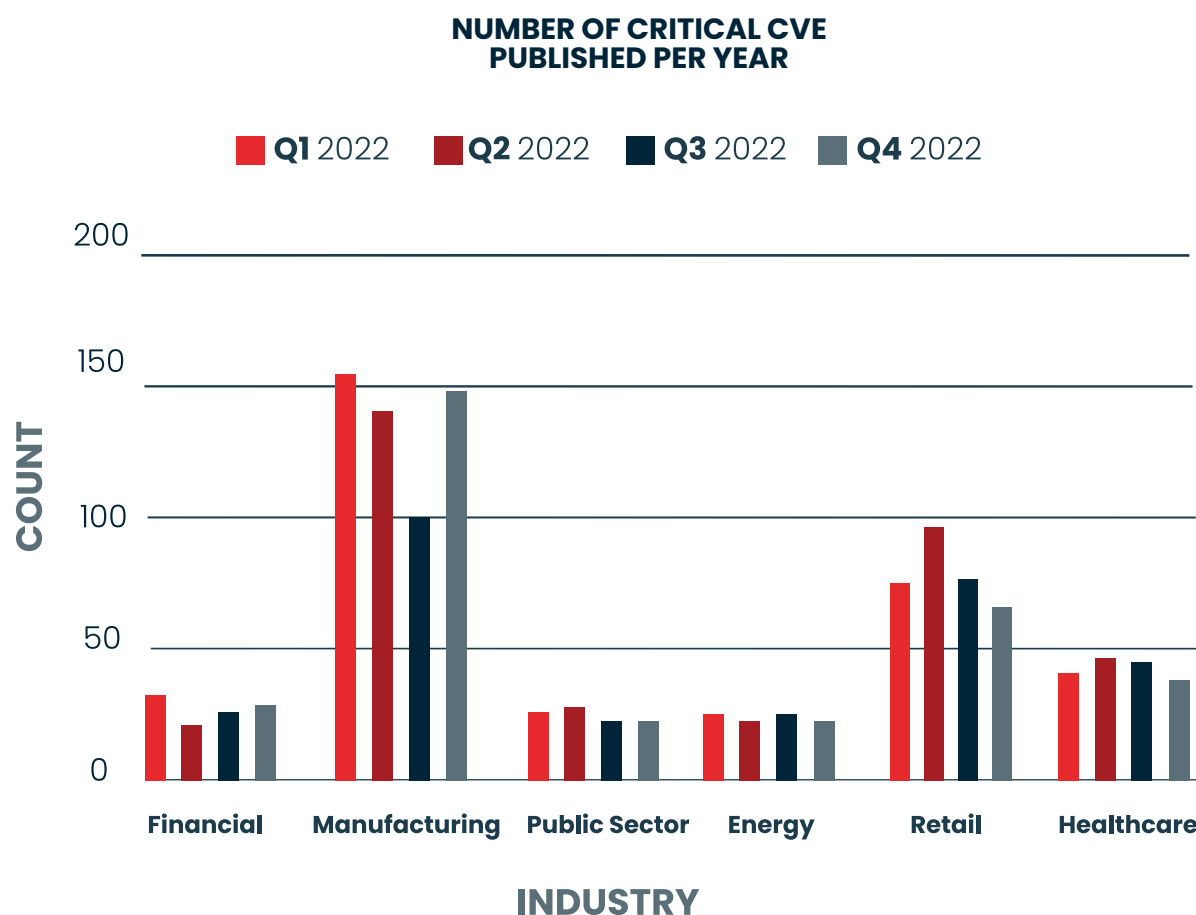
³ [hXXps://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/](https://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/)

⁴ [hXXps://www.ic3.gov/Media/News/2022/220601.pdf](https://www.ic3.gov/Media/News/2022/220601.pdf)

⁵ ZeroFox Intelligence Internal Collections



LockBit emerged as the primary digital extortion payload, leveraged in nearly a quarter of attacks in 2022.⁶ The closing of Conti's operations in mid-2022 following the leak of its source code very likely led to a dispersal of the threat rather than a reduction, with Conti's developers splintering and joining other collectives and its affiliates pivoting to deploy other payloads.⁷ Black Basta was the most successful of the multitude of new strains that emerged, quickly establishing itself as a critical threat and the fifth most-prolific strain in 2022.



Source: ZeroFox Intelligence

⁶ ZeroFox Intelligence Internal Collections

⁷ <https://thehackersnews.com/2022/05/experts-analyze-conti-and-hive.html>



Ransomware

2023 | FORECAST & RECOMMENDATIONS

Ransomware and digital extortion will very likely remain some of the greatest cyber threats to organizations globally in 2023. Security practices are unlikely to increase sufficiently and geopolitical environments are unlikely to change substantially enough to undermine bulletproof jurisdictions, which might result in a notable reduction in threat. RaaS offerings will very likely continue to underpin the threat, with continued diversification in TTPs during the deployment of given strains. Manufacturing and retail sectors will likely remain most at-risk from ransomware attacks, though ZeroFox Intelligence anticipates the energy sector and supply of goods across Europe will face an increased threat from Russia-aligned threat actors. Smaller nation-states will also likely see an increased threat from extortion collectives.

ZeroFox Intelligence anticipates an increase in “hack-and-leak” tactics, with threat actors removing the encryption angle of their attacks and instead relying on data exfiltration and ransom demands. Payloads deployed by extortion collectives will also likely increasingly incorporate data corruption functionality.⁸ Threat actors may resort to more extreme pressure tactics to elicit payment from victims under threat of significant reputational damage and legal ramifications. It is a realistic possibility that extortion operatives will increasingly collaborate, passing leaked data between them and resulting in victims being required to pay ransom demands to multiple entities before their data is removed from various leak sites.

⁸ [hXtps://securityaffairs\[.\]co/136226/cyber-crime/exmatter-tool-shift-extortion-tactics.html](https://securityaffairs[.]co/136226/cyber-crime/exmatter-tool-shift-extortion-tactics.html)

RECOMMENDATIONS

- Provide user training programs to fight against social engineering attacks, disable unused remote access ports, and patch disclosed vulnerabilities as quickly as possible.
- Ensure proper network segmentation and implement a recovery plan, including maintaining multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location.
- Enable MFA and disable PowerShell wherever possible.
- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new ransomware targets.
- Should your organization be impacted by a ransomware event, engage with the ZeroFox DarkOps team by utilizing the [RFI button](#) in the ZeroFox platform.



Multi-Factor Authentication Exploitation

2022 | CONCLUSIONS

Threat actors continued to evolve their social engineering approach to undermine multi-factor authentication (MFA), either by intercepting or circumventing authentication codes via email accessed with stolen user credentials. They increasingly moved towards real-time MFA bypassing solutions, leveraging phishing techniques where traditionally-strong MFA gives little or no protection. This includes “in-the-middle” techniques, MFA fatigue—as encouraged by Lapsus\$—and OAuth Consent phishing attempts.

In 2022, real-time phishing by acting as a reverse proxy likely increased, with threat actors intercepting traffic—including second-factor codes—between the user and login pages. “In the middle” techniques have been increasingly adopted into Phishing-as-a-Service operations. Early detection and disruption can be difficult, as victims are unlikely to be aware of threat actors positioned between them and the legitimate destination before granting threat actors authenticated sessions within enterprise environments.



Multi-Factor Authentication Exploitation

2023 | FORECAST & RECOMMENDATIONS

ZeroFox Intelligence anticipates increased threat actor focus on exploiting weaknesses in MFA in 2023, with a greater number of attacks against identity and access management services and increased adoption of “in-the-middle” techniques in “as-a-service” offerings. Threat actors will very likely continue to exploit traditionally weak types of MFA viewed as low-hanging fruit, such as SMS-based authentication.

However, increased adoption of stronger MFA types, such as phishing-resistant MFA, will likely drive threat actors to target identity and access management providers directly. Credentials obtained in these breaches could enable threat actors to launch attacks that appear to originate within an enterprise’s environment, making detection more difficult.

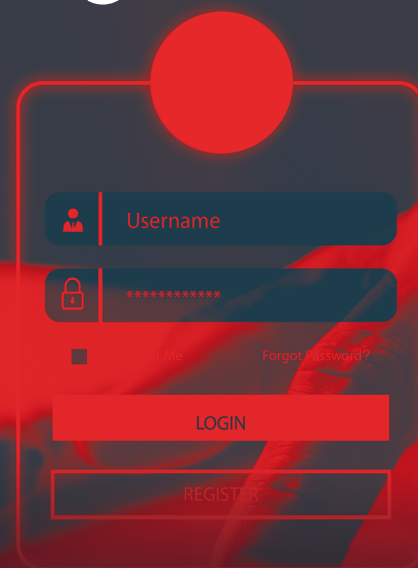
RECOMMENDATIONS

- Implement phishing-resistant MFA methods that support Fast ID Online v2.0 (FIDO2) and certificate-based authentication in conjunction with a broader Zero Trust initiative.
- Remain vigilant and deny MFA requests not specifically triggered through logging in or requesting device enrollment. These requests are typically immediate and should not randomly appear throughout the day.

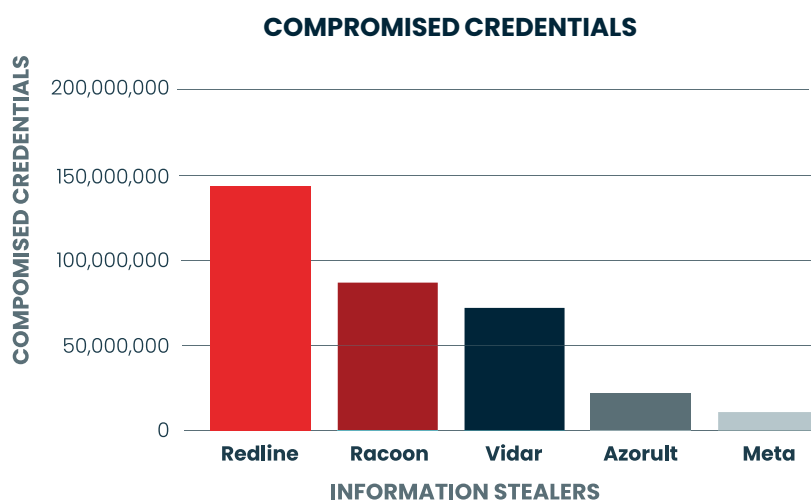


Malware

2022 | CONCLUSIONS



Information stealers continued to pose a significant threat to individuals and organizations in 2022. ZeroFox ingested 312,573,712 total compromised credentials from logs collected this year. Redline, Raccoon, Vidar, Azorult, and Meta were the top five information stealers observed by ZeroFox this year. Between 2021 and 2022, Redline, Raccoon, and Vidar each maintained their first, second, and third places in our observations, respectively. Raccoon's popularity is particularly noteworthy, considering its brief three-month hiatus early in 2022. These families continue to see strong followings among various threat actors and are readily deployed as-a-service against inadequately-protected systems and users.



Source: ZeroFox Intelligence



Malware

2023 | **FORECAST & RECOMMENDATIONS**

ZeroFox assesses that criminal marketplaces will continue to be a hotspot for cyber criminals to acquire stolen credentials in 2023. Given the prevalence and longevity of marketplaces, ZeroFox asserts that the increased usage of information stealers like Redline, Raccoon, and Vidar will continue to fuel widespread support from their developers and community. Moreover, given their efficacy and growing popularity, the extensive range of applications and cryptocurrencies targeted by these information stealers will likely expand and grow in 2023.

ZeroFox predicts that competition among infostealers will continue to increase, which will invariably encourage innovation among developers to build better, more sophisticated, and easier-to-use services as they try to distinguish themselves from competitors.

As infostealers significantly lower barriers to entry for low-level threat actors, ZeroFox does not foresee a downward trend in the use of these malicious tools. Logs provided from these information stealers aid in gaining additional access to other services through credential harvesting or obtaining other sensitive information. Additionally, infostealers occasionally provide the ability to deploy additional payloads, allowing threat actors to go beyond just harvesting credentials. The versatile nature of information stealers and their capability to steal a variety of sensitive data makes them a threat to all organizations across all industries.

RECOMMENDATIONS

- Consider a security policy that only allows managed devices to connect to company resources.
- Discourage password reuse between any two accounts, personal or otherwise.
- Discourage the use of business emails when registering on public websites.
- Enforce MFA for accounts wherever possible. Do not choose SMS or email options if stronger methods, such as push notifications and number matching, are available.
- Create access policies informed by continuous, contextual, and risk-based verification across users and their associated devices.
- Access the ZeroFox platform's [Intelligence Search](#) interface to investigate Indicators of Compromise (IOCs) and metadata related to Malware and Ransomware.



Exploits and Vulnerabilities

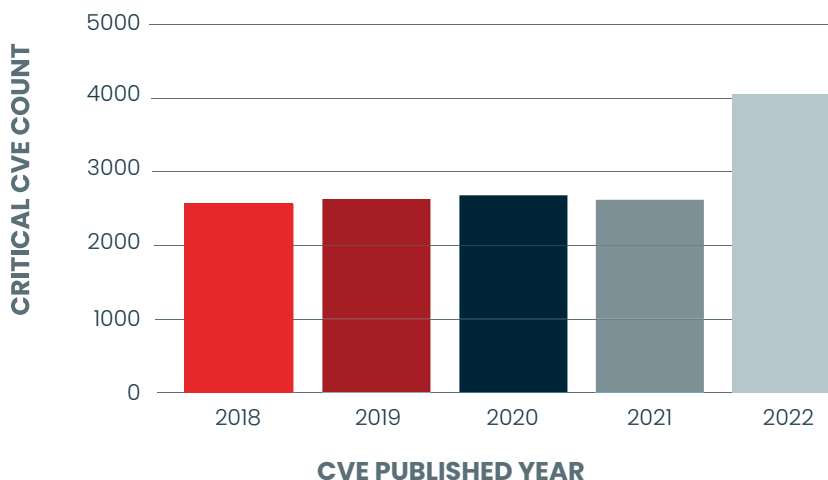
2022 | CONCLUSIONS

The release of Log4Shell in 2021 provided direction for researchers and threat actors to analyze frameworks or modules. This year, two more exploits that have been labeled with the moniker “4Shell” have been released: Spring4Shell (CVE-2022-2296) and Text4Shell (CVE-2022-42889). While the new “4Shell” exploits released this year are harder to utilize, they continue to highlight a glaring problem in today’s software development. Namely, vulnerabilities that exist in packages that are bundled and imported in a wide range of applications will likely continue to appeal to attackers looking to maximize their effectiveness. Threat actors are likely to take the time to find consistent inputs from various applications that ultimately lead to the same vulnerable endpoint, allowing them to write one exploit for a multitude of applications.

Overall this year, ZeroFox Intelligence has observed a significant increase in the number of critical vulnerabilities published within the NIST database. A general trend of finding vulnerabilities is increasing year after year, with the only exception being in 2021 when the number of critical CVEs identified decreased slightly from the prior year.

This significant increase in reported critical vulnerabilities will likely force companies to increase their frequency of applying and checking for new patches for their public-facing endpoint, which may cause significant downtime. To maintain this patch cycle, companies may be forced to allocate more human and financial capital. This increased expenditure may hinder a company’s bottom line.

**NUMBER OF CRITICAL CVE
PUBLISHED PER YEAR**



Source: [hXXps://www.services.nvd.nist.gov](https://www.services.nvd.nist.gov)



Exploits and Vulnerabilities

2023 | FORECAST & RECOMMENDATIONS

With the increased reporting of vulnerabilities found in 2022 and the overall general uptrend of CVE reporting in the five years observable above, ZeroFox Intelligence predicts that critical CVE reporting for 2023 will either increase or roughly stay at the level of 2022. ZeroFox has not seen any indication that the rate of discovering new vulnerabilities will slow down in 2023. With this risk of new vulnerabilities being discovered, ZeroFox recommends limiting access to applications via the internet as much as possible without hindering business operations. For applications that need to be accessible to the internet, we recommend monitoring for and alerting on suspicious or out-of-the-ordinary behavior.



ZeroFox recommends limiting internet-facing applications as much as possible without hindering business operations.

RECOMMENDATIONS

- ZeroFox Intelligence recommends investing in and maintaining security solutions that monitor and report suspicious activity, especially on applications exposed to the internet.
- Companies should verify that they have a frequent update and patch cycle to keep their applications up to date.
- ZeroFox recommends limiting internet-facing applications as much as possible without hindering business operations. Other applications should be behind a corporate firewall and accessible by employees via a VPN.
- In addition to patching, ZeroFox recommends adding your Assets' Technology Stack in the ZeroFox Platform and enabling the Vulnerability Intelligence rule.
- Use the ZeroFox Platform's Intelligence Search interface to investigate vulnerabilities that may apply to your environment and their associated exploits. Vulnerabilities are sourced from the NIST database and enriched by ZeroFox analysts with an attack surface risk score, potential impact, and remediation steps.



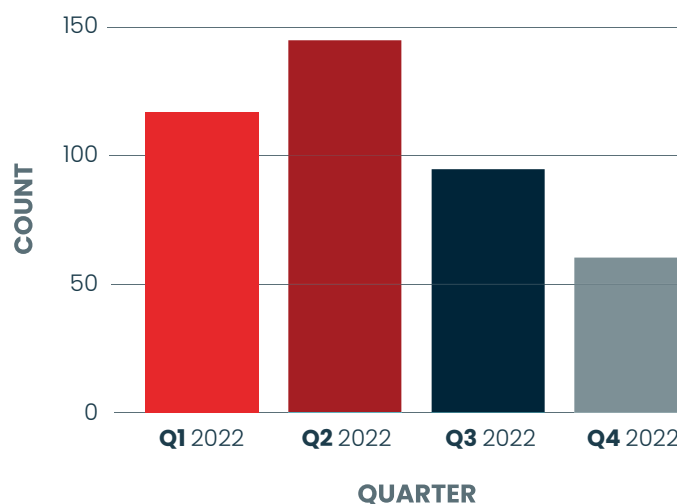
Initial Access Brokers

2022 | CONCLUSIONS

Illicit access sales posted in open forums in 2022 fell in number from the 2021 peak. This likely reflected limitations to the supply from IABs rather than a lack of demand from buyers. During 2022, the IAB landscape remained highly volatile—more so than other cyber threats—with access sales typically trending against particular industries for a period of time before moving on and spiking against others. ZeroFox Intelligence identified spikes in advertising access to entities participating in high-profile events in bids by threat actors to maximize their own brand awareness. Typically, threat actors continued to avoid specifying what type of access they were selling, instead listing the level of access—either user or admin—to entice buyers.

The fall in activity is likely in part explained by Russia's invasion of Ukraine, with some IABs implicated in the conflict, continued disruption to underground marketplaces (e.g. RaidForums) where access sales have appeared regularly, and IABs seeking more private or direct communication methods to sell illicit access. The shift towards brokers preferring private channels rather than advertising in forums is an attempt to avoid law enforcement scrutiny and a preference on who to sell to. Brokers sold to well-established buyers—often ransomware operatives—out of an abundance of caution. Access to entities in the United States and Western Europe posted in open channels became increasingly rare throughout the year, as did access to managed service and software providers.

ADVERTISED IAB ACCESS SALES BY QUARTER



Source: ZeroFox Intelligence



Initial Access Brokers

2023 | **FORECAST & RECOMMENDATIONS**

The IAB threat will very likely rebound in 2023 and will remain influenced by developments in Russia's war in Ukraine. ZeroFox Intelligence anticipates a continued increase in IABs leveraging private means of communication to sell access, as well as leveraging trusted relationships with specific buyers. There is no indication the threat will decrease, with buyers still seeking to obtain access via brokers, although illicit access to large, Western, or European entities advertised in open forums will likely become increasingly rare. Identifying and mitigating access sales ahead of compromise will very likely become increasingly challenging, amplifying the importance of partnerships with third-party security vendors that have access to private channels. Illicit access sales are 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.

RECOMMENDATIONS

- 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 MFA wherever possible.
- Disable PowerShell wherever possible.
- Employ ZeroFox Threat Intelligence feeds to get ahead of threat actor activity.



Social Engineering

2022 | CONCLUSIONS

During 2022, social engineering remained one of the most prevalent methods leveraged by threat actors to harm end-users, targeting companies directly and impersonating them to lure third parties or members of the public. Campaigns of this nature were demonstrably effective, enabling threat actors to steal user credentials, deploy malicious payloads, and conduct payment fraud against individuals and organizations. They continue to offer a great return on investment and are highly cost-efficient.

Threat actors continued to evolve their social engineering approach, but the practice did not fundamentally change. The increased use of Adversary-in-the-Middle (AiTM) techniques to bypass MFA, including the increased adoption of widely-distributed phishing kits, demonstrates threat actors' ability to adapt to emerging security practices.

Targeted campaigns drove the greatest changes in social engineering, with targeted smishing and telephone-oriented attack delivery campaigns increasing. Corporate email accounts of employees were regularly targeted using highly-sophisticated techniques that included lateral phishing and MFA fatigue. Approaches of this nature are persuasive and can have a catastrophic impact on enterprise networks.

ZeroFox Intelligence also identified an increase in domain shadowing, where threat actors create multiple malicious subdomains under compromised domains to host phishing pages, steal sensitive user information and credentials, and distribute malware.

Threat actors registered multiple subdomains that can be discarded and rotated quickly to avoid detection. The malicious pages do not impact the operation of the legitimate site, and an address bar may display the main domain, capitalizing on the reputation and goodwill of the targeted entity.

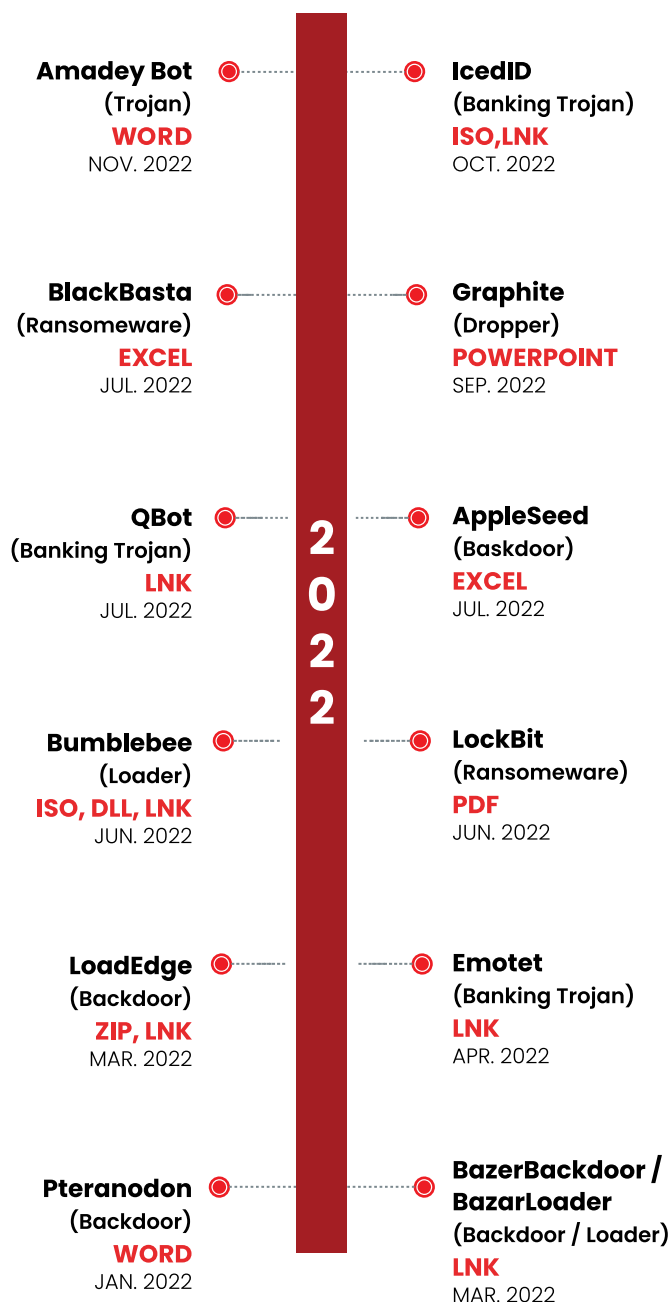
The threat from social engineering campaigns remained evolutionary rather than revolutionary, indicating that exploiting human error remains lucrative for threat actors. Threat actors continued to leverage topical lures to entice engagement with malicious emails, and malware distribution via malicious email attachments remained highly prevalent. While macro-enabled documents continued to be leveraged throughout 2022, ZeroFox Intelligence identified threat actors increasingly leveraging Windows image files (ISO), archives (RAR), and Windows Shortcut files (LNK) to deploy malicious payloads.⁹ This is very likely in part driven by Microsoft's February 2022 announcement that Visual Basic Application (VBA) macros would be disabled by default—making it more likely users would be alerted to potentially unsafe files that are downloaded from the internet that may contain malware.¹⁰ Mark-of-the-Web controls cannot be applied to LNK files, which are Windows shortcuts that instruct legitimate applications like PowerShell, CMD, and MSHTA to open attachments, folders, or applications. This results in the execution of the malware without warning to the user.

⁹ [hXtps://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-link-shortcut-files-malware/](https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-link-shortcut-files-malware/)

¹⁰ [hXtps://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/](https://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/)



SELECT SOCIAL ENGINEERING CAMPAIGNS LEVERAGING MALICIOUS ATTACHMENTS IN 2022



Source: ZeroFox Intelligence

The threat from Telephone Oriented Attack Delivery (TOAD)—or callback phishing—likely increased in 2022. Threat actors call their victims directly and convince them to install software on their devices that enables follow-on malicious activity. While cold approaches like traditional vishing remain prevalent, threat actor TTPs evolved to increasingly leverage hybrid approaches, using phishing or smishing messages to initiate a follow-on phone conversation.¹¹ Campaigns in 2022 added legitimacy to malicious emails by impersonating security teams and encouraging victims to return a phone call to authenticate fraudulent activity.¹²

Threat actor tactics continued to evolve their social engineering approach in order to undermine MFA, either by intercepting or circumventing authentication codes. Widespread adoption of MFA and users' move away from SMS-based authentication in favor of more secure methods have driven threat actors towards real-time MFA bypassing solutions. Threat actors have increasingly leveraged phishing techniques where traditionally-strong MFA gives little or no protection. This includes "in-the-middle" techniques; MFA fatigue, as encouraged by Lapsus\$; and OAuth Consent phishing attempts.¹³ While not a novel technique, the use of reverse proxies for AiTM attacks is assessed to be on an upward trajectory. In 2022, AiTM has been increasingly adopted into Phishing-as-a-Service (PhaaS) operations, including operations that have historically targeted financial and e-commerce entities. Victims are unlikely to be aware of threat actors positioned between them and the legitimate destination, granting threat actors authenticated sessions within enterprise environments.^{14 15}

¹¹ [hXXps://www.twilio.com/blog/august-2022-social-engineering-attack](https://www.twilio.com/blog/august-2022-social-engineering-attack)

¹² [hXXps://www.bleepingcomputer.com/news/security/hackers-impersonate-cybersecurity-firms-in-callback-phishing-attacks/](https://www.bleepingcomputer.com/news/security/hackers-impersonate-cybersecurity-firms-in-callback-phishing-attacks/)

¹³ [hXXps://www.csoonline.com/article/3674156/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html](https://www.csoonline.com/article/3674156/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html)

¹⁴ [hXXps://www.bleepingcomputer.com/news/security/robin-banks-phishing-service-returns-to-steal-banking-accounts/](https://www.bleepingcomputer.com/news/security/robin-banks-phishing-service-returns-to-steal-banking-accounts/)

¹⁵ [hXXps://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web](https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web)



Social Engineering

2023 | FORECAST & RECOMMENDATIONS

ZeroFox Intelligence assesses that the social engineering threat is unlikely to change significantly in 2023. However, threat actors are expected to continue to adapt their techniques, increasingly leveraging more sophisticated approaches into widely-distributed phishing kits. Additionally, ZeroFox expects an increase in the use of more believable phishing domains and alternative malicious attachments to macro-enabled documents. However, social engineering campaigns are unlikely to move entirely away from malicious macro-enabled documents in the near term. The use of alternative file types will likely increase, alongside a rise in the use of malicious URLs.

ZeroFox also anticipates the threat from smishing and TOAD will continue. While low-sophistication campaigns will almost certainly continue to be widespread, capable threat actors are expected to increasingly adopt hybrid social engineering approaches, including leveraging sensitive information obtained from previous data breaches to appear legitimate.

PhaaS offerings are very likely to remain highly prominent. They offer a great return on investment for both developers and campaign operators and are a highly cost-efficient way to harvest credentials. ZeroFox anticipates kits will increasingly adopt MFA-bypassing capabilities, particularly leveraging “in the middle” techniques to compromise enterprise environments.

While ongoing monitoring for and attempting removal of impersonating domains can substantially reduce this threat, mitigating phishing domains will likely continue to be a “whack-a-mole” problem whereby threat actors leverage continually evolving rotations and variations of domain names in social engineering campaigns.

RECOMMENDATIONS

- ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support FIDO2 and certificate-based authentication in conjunction with a broader Zero Trust initiative. While phishing-resistant MFA will not protect against all attacks, ZeroFox Intelligence has yet to observe threat actors on the deep and dark web publishing or brokering exploits related to phishing-resistant MFA.
- Scan all incoming files received via email to mitigate the risk associated with increased use of LNK, ISO, and RAR files to flag potential malware delivery.
- Communicate to employees about emerging trends in social engineering scams and how to conduct safe means of authentication.
- Malicious phishing domains and open redirects should be monitored and taken down to avoid customers being defrauded or providing an intrusion vector for threat actors.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand threats to your organization.



Name:
John James

DOB:
01-16-1980

SSN:
555-54-4444

Acme Corp

Title:
Project Manager

Annual Income:

Convergence between Cyber and Physical

2022 | CONCLUSIONS

Over the past several years, the threat to cyber and physical spaces has converged significantly. Ransomware attacks such as the 2021 Colonial Pipeline intrusion emphasized how cyberattacks can cause significant real-world, physical impacts. Throughout 2022, two defining themes emerged for how the cyber and physical realms can converge. The first involved cyber threat actors attacking organizations, with the cyberattack ultimately interrupting physical operations. The second theme relates to cyber activity accompanying real-world physical developments, as demonstrated frequently during the Russia-Ukraine conflict. While physical attacks were occurring on the ground, threat actors were concurrently conducting cyberattacks against Russian and Ukrainian entities. Lastly, the continuing growth of the metaverse will also present further challenges in mitigating physical security risks associated with virtual reality.

There were several occurrences throughout 2022 where ransomware attacks either disrupted operations or caused actual physical damage. One of the starkest examples was Lincoln College in Lincoln, IL, which was forced to close down entirely in May 2022 due to a previous ransomware attack that rendered its admissions and institutional data unusable.¹⁶

Additionally, there were instances where ransomware attacks impacted healthcare organizations, causing systems to go offline and providers to have to perform work manually or postpone appointments entirely.¹⁷ Furthermore, in June 2022, a cyberattack on a steel mill in Iran ultimately led to the outbreak of a fire on the premises. Dubbed "Predatory Sparrow," the group responsible launched the attack in response to actions taken by the Iranian government.¹⁸ These types of attacks highlight long-standing concerns that cyberattacks could cause real-world physical damage.

Concerns also remain around the safety of electrical grids throughout the world. At the Pwn2Own conference in April 2022, white hat hackers demonstrated how vulnerable these power grids are to cyberattacks by hacking an industrial control system open source communications protocol utilized heavily by critical infrastructure organizations worldwide.¹⁹ In addition, the frequent physical attacks on substations in the United States, as well as the regular conflict attacks on electrical infrastructure in Ukraine, demonstrate the far-reaching impacts that taking even a small section of the electrical grid offline can have and lending further credence to concerns about electrical grids being targeted in cyber attacks.

¹⁶ <https://www.nbcnews.com/tech/security/ransomware-attack-covid-combine-shutter-illinois-college-rcna24905>

¹⁷ <https://www.1011now.com/2022/10/13/chi-health-announces-system-outages-due-ransomware-attack/>

¹⁸ [https://www.bbc.com/cdn\[.\]ampproject.org/c/s/www.bbc.com/news/technology-62072480.amp](https://www.bbc.com/cdn[.]ampproject.org/c/s/www.bbc.com/news/technology-62072480.amp)

¹⁹ <https://gizmodo.com/hackers-breach-power-grid-opc-ua-pwn2own-2022-1848825967>



Conducting cyber operations concurrently with on-the-ground physical attacks also allowed governments to maintain plausible deniability; that is, it appeared possible that the threat actors acted in a manner sympathetic to one side without directly being tasked by its officials. This increased the various fronts to be attacked; indeed, Russia launched a significant number of cyberattacks right before it invaded Ukraine in February 2022, ostensibly to confuse and distract Ukrainian defenses as it prepared to invade Ukraine.²⁰ In addition to that, mis- and disinformation campaigns from both sides were prevalent, which served to exacerbate already heightened international tensions. As an example, misinformation was observed shortly after Russia invaded Ukraine, social media users misrepresented footage from a video game showing close combat between fighter jets, claiming the clip showed the Ukrainian air force fighter pilot dubbed the “Ghost of Kyiv” shooting down a Russian air force fighter jet.²¹ It is not clear if this began with the intent to deceive but was propagated by many individuals that likely thought the footage was legitimate. The video was flagged as “out of context” by Twitter, although similar content on Ukraine’s official Twitter account did not get flagged.

Disinformation has also been widespread during the war in Ukraine. One of the main premises for Russia’s invasion was the allegation that Ukraine was carrying out genocide in Donbas – claims that have since been debunked as baseless. In March 2022, Meta removed a deepfake of Ukrainian President Zelensky in which he appeared to call on the military to lay down their arms.²² Ukraine has also spread disinformation, such as the Snake Island stand – likely an attempt to boost morale. In August 2022, Ukraine shut down a bot farm of 1,000,000 bots used to spread disinformation on social networks.²³

²⁰ <https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion>

²¹ <https://apnews.com/article/fact-checking-548180451272>

²² <https://www.infosecurity-magazine.com/news/russia-uses-deepfake-zelensky/>

²³ <https://www.bleepingcomputer.com/news/security/ukraine-takes-down-1-000-000-bots-used-for-disinformation/>

Footage incorrectly alleged to be the “Ghost of Kyiv,” engaged with by over 20,000 users and flagged as “out of context” by Twitter



Olegi
@ItsOlegi21

...

Ukrainian pilot who is 6-0 shoots down a Russian Su-35 with his Mig-29. He’s been nicknamed the ghost of Kyiv, and is the first pilot since WW2 to achieve ace status!



Stay informed

This media is presented out of context [Find out more](#)

11:01 AM · Feb 25, 2022 · Twitter for iPhone

2,915 Retweets 880 Quote Tweets 22K Likes

Source: https://twitter.com/ItsOlegi21/status/1497164782952239104?s=20&t=NfaX2G2awdaWhkEKAQ2O_g



Despite the virtual essence of the metaverse, physical security threats are already prevalent within online environments. Reporting shows that sexual harassment and stalking are among some of the personal security issues faced by metaverse participants.^{24,25} This type of behavior within virtual spaces is not new and has occurred for some time in online gaming, forums, and social media platforms. As the metaverse grows, ZeroFox Intelligence assesses that this behavior will likely remain pervasive and poses complicated questions over the legal boundaries between the physical and virtual worlds. In addition, the use of personalized avatars—which will continue to improve in quality—means that threats are also likely to feel more directed or personal.

24 [hXXps://www.bbc.co.uk/news/technology-60247542](https://www.bbc.co.uk/news/technology-60247542)

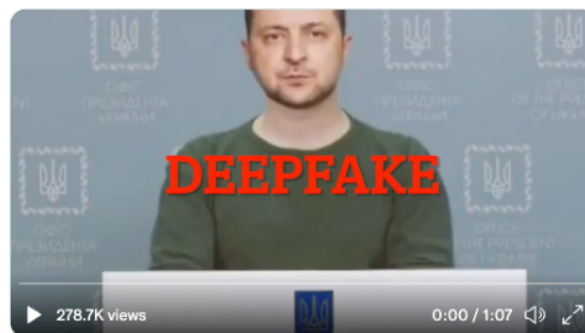
25 [hXXps://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html](https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html)

Deepfake of President Zelensky, March 2022



Mikael Thalen
@MikaelThalen

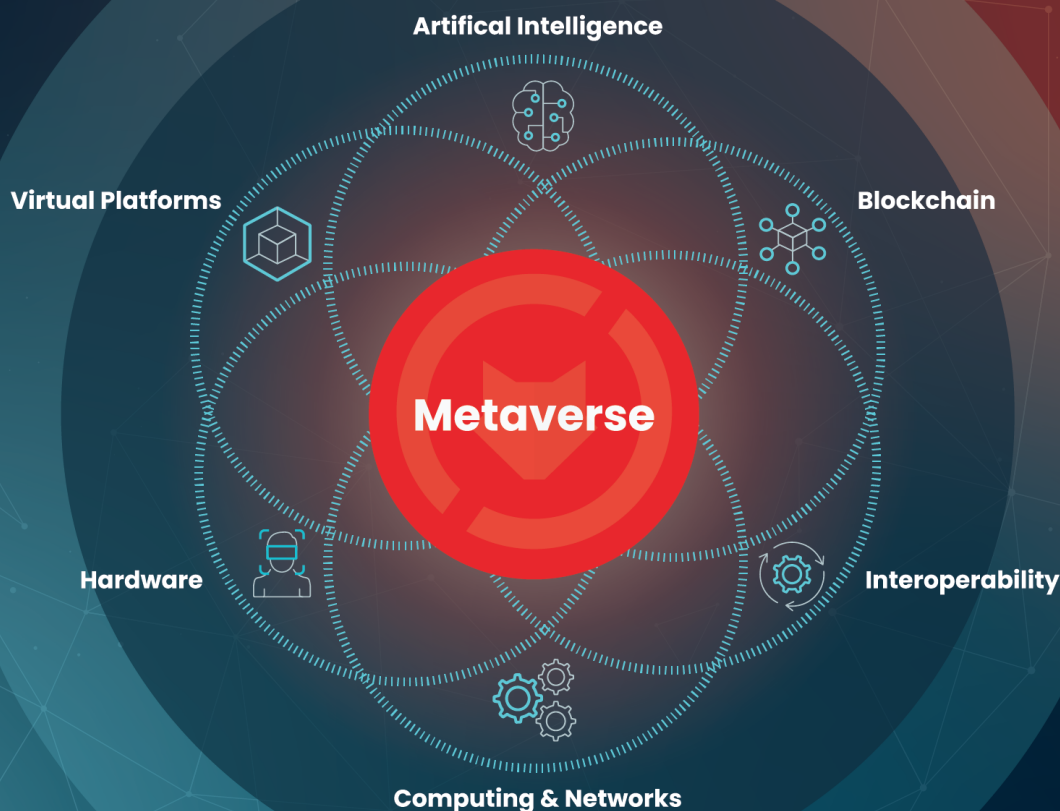
A deepfake of Ukrainian President Volodymyr Zelensky calling on his soldiers to lay down their weapons was reportedly uploaded to a hacked Ukrainian news website today, per [@Shayan86](#)



3:53 PM · Mar 16, 2022 · Twitter Web App

467 Retweets 371 Quote Tweets 856 Likes

Source: [hXXps://twitter.com/MikaelThalen/status/1504123674516885507](https://twitter.com/MikaelThalen/status/1504123674516885507)



Source: [hXXps://www.services.nvd.nist.gov](https://www.services.nvd.nist.gov)



Convergence between Cyber and Physical

2023 | FORECAST & RECOMMENDATIONS

Tactics developed and utilized throughout the war in Ukraine by cyber threat actors to target entities on the opposing side for political gains are likely to be utilized in 2023 to target organizations for financial gains as well. As the conflict in Ukraine continues, cyberattacks on both sides are likely. What remains to be seen is how conscription efforts, particularly in Russia, will impact threat actor activity should these actors be called into active military duty.

Additionally, critical infrastructure remains a concerning target for cyber threat activity. As demonstrated by white hat hackers in 2022, this infrastructure, which underpins the very workings of society, remains vulnerable to attacks that could take it offline, potentially causing physical outages and disrupting not only organizations but everyday life for citizens. The potential for these types of attacks remains worrisome as geopolitical disputes—such as those between Russia and Ukraine, as well as China and Taiwan—often elicit backlash towards countries showing real or perceived support for one side of the conflict over another.

Traditional security threats—both cyber and physical—are also likely to be accompanied by fresh challenges in the metaverse, which will almost certainly present an unprecedented attack surface. There are also several risks related to data privacy and intellectual property within the metaverse due to new technologies and unregulated digital assets. Since data privacy laws around the globe are already inconsistent, most legislation will almost certainly need to be revised to cover the many potential data pitfalls of metaverse platforms and technologies.

RECOMMENDATIONS

- Given the increasing convergence between cyber and physical threats, physical and cyber security teams within organizations should look to establish strong communication in order proactively get ahead of incidents being observed by each team that may have broader operational impacts.
- Organizations should maintain awareness of geopolitical developments by subscribing to ZeroFox geopolitical team monitoring and alerting in order to keep apprised of developments that may impact their operations as well as have broader cyber and physical ramifications.
- ZeroFox Intelligence recommends that organizations secure their metaverse real estate, including for their brands and key personnel.
- Companies participating within the metaverse might also need to consider collaborative enforcement or tracking mechanisms for sanctions imposed on offending parties to mitigate these risks, as traditional sanctions may fail to deter malicious behavior in the metaverse.



About ZeroFox

The leader in External Cybersecurity

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.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400