



Weekly Intelligence Brief

Classification: TLP:GREEN

May 13, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the cyber threat landscape. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on May 10, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence Flash Report – Malicious AI-Enhanced Bot Announced for Sale	2
ZeroFox Intelligence Brief – Russia Increases Use of Hybrid War Tactics After Aid to Ukraine	2
 Cyber Intelligence Key Findings	5
Iranian State-Sponsored Hackers Conduct Social Engineering Campaign Mimicking Journalists	5
United States Releases International Cyberspace Strategy	5
Zscaler Takes Test Environment Offline While Investigating Claims of Cyberattack	6
 Deep and Dark Web Intelligence Key Findings	8
Law Enforcement Reveals Identity of Alleged LockBit Leader	8
Threat Actor Advertised Zero-Day RCE Exploit on Forum	8
Pro-Palestinian Hacktivist Group Claims New Attack Against Saudi Infrastructure	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-26026 and CVE-2024-21793	11
CVE-2023-49606	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: City of Wichita Shuts Down IT Network After Ransomware Attack	14
Breach Intelligence: UK Ministry of Defence Breached	14
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Malicious AI-Enhanced Bot Announced for Sale

On May 6, 2024, untested threat actor "Average" started a thread in the Russian-speaking deep and dark web (DDW) community Exploit, advertising the development of a new artificial intelligence (AI)-powered one-time password (OTP) bot that can be leveraged in two-factor authentication (2FA) bypass attacks, as well as other social engineering activity. As of May 10, 2024, the bot is allegedly available for pre-order at a cost of USD 150, though the release date is unknown. Average claims that up to three "investors" are also needed, whose funds will assist in the tool's development. Investors will also receive access to a beta version of the bot, as well as "lifetime service." The advertisement of this bot is almost certainly indicative of a growing interest in unrestricted AI tools within both DDW communities and open web communities. Throughout 2024, threat actors of varied motives and capabilities are very likely to increasingly seek tools able to enhance their ability to conduct malicious cyber activity.

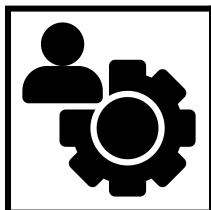
ZeroFox Intelligence Brief – Russia Increases Use of Hybrid War Tactics After Aid to Ukraine

The recently authorized U.S. military aid package to Ukraine is likely to empower Ukraine to stall Russia's recent military gains. Russia began increasing its operational tempo on the battlefield soon after voting on the aid package began, probably in a bid to advance as far as possible before the promised aid reaches frontline positions. Russia will likely increase its aggressive hybrid war strategy using tactics like disinformation campaigns, the weaponization of energy resources, sabotage, and cyber campaigns to limit the effectiveness of military aid to Ukraine and force a repeat of battlefield conditions seen in the early part of 2024. These hybrid attacks will likely seek to influence elections in key Western nations by making support to Ukraine a primary wedge issue and exacerbate underlying societal fissures around continued financial and military support for Ukraine. Attacks on critical infrastructure, energy targets, and online targeting of U.S. and European elections and politicians will likely reach a crescendo ahead of major elections, especially the U.S. presidential election.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Iranian State-Sponsored Hackers Conduct Social Engineering Campaign Mimicking Journalists

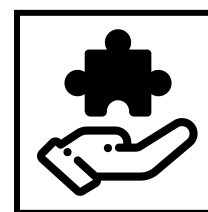


What happened: APT42, an Iranian state-sponsored cyberespionage group, is impersonating journalists and human rights activists to exfiltrate data and steal cloud operations credentials through spear phishing attacks. The hackers target prominent news outlets using deceptive domains and fake login pages, indicating a wide-ranging campaign since 2021. Researchers have associated the group with the Islamic Revolutionary Guard Corps Intelligence Organisation (IRGC-IO).

- **What this means:** Threat actors use a sophisticated tactic dubbed "typosquatting," whereby they create deceptive domains resembling legitimate ones. These domains often lead victims to fake login pages, especially those targeting news readers. APT42 hackers have been posing as various services to steal credentials, notably those deemed threatening to the Iranian regime. Furthermore, researchers have highlighted APT42's use of the malware backdoors NICECURL and TAMECAT distributed via this campaign. With tensions in the Middle East flaring, especially between Iran and Israel amid the Israel-Hamas war, Iranian hackers have been leveling up their attacks on organizations; state-sponsored, politically motivated attacks are the greatest threats.

United States Releases International Cyberspace Strategy

What happened: The U.S. Department of State has introduced the International Cyberspace and Digital Policy [Strategy](#) aimed at fostering an innovative, secure, and rights-respecting digital future. This strategy, developed in collaboration with other federal agencies, prioritizes digital solidarity—a collective commitment to shared goals and mutual support. It emphasizes building digital and cyber capacity to enhance security, resilience, and prosperity. Guided by three principles and four areas of action, the strategy promotes an open, inclusive, and secure digital ecosystem; aligns governance approaches with international partners; advances responsible state behavior; and strengthens global digital and cyber capacity to combat cyber threats.



- **What this means:** The demand for cybersecurity assistance—particularly in cyber defense, incident response, and combating criminal use of cryptocurrency—is increasing. Following recent cyberattacks, the United States and its allies are reportedly aiming to enhance shared threat intelligence and facilitate access to commercial cybersecurity services. With

this announcement, the State Department recognizes the necessity of close coordination across government agencies and with international partners, as well as leveraging private-sector expertise. Modernizing assistance mechanisms is essential to providing timely and comprehensive support.

Zscaler Takes Test Environment Offline While Investigating Claims of Cyberattack



What happened: Zscaler has discovered an exposed isolated test environment on a test server that it took offline after rumors of a threat actor selling access to its systems spread online. The company has engaged an incident response firm to investigate further.

➤ **What this means:** Zscaler has discovered unauthorized access on its network. The company's customer, production, and corporate environments remain secure and unaffected. The company is actively investigating the situation and taking appropriate measures to address any potential threats. ZeroFox has also [observed](#) threat actor "IntelBroker" advertising access to the "largest cybersecurity company" on predominantly English-language dark web forum BreachForums. The access is priced at USD 20,000 and allegedly includes confidential and highly critical logs packed with credentials, SMTP access, pointer authentication access, SSL passkeys, SSL certificates, and more.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

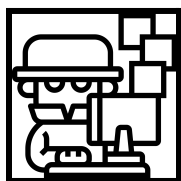
Law Enforcement Reveals Identity of Alleged LockBit Leader

What happened: On May 7, 2024, the U.S. Department of Justice and the United Kingdom (UK)'s National Crime Agency revealed the supposed identity of LockBit's leader, who is allegedly operating under the alias "LockBitSupp." Posting on the ransomware group's old data leak site previously seized in a February 2024 joint operation, the agencies identified LockBitSupp as 31-year-old Russian national Dmitry Yuryevich Khoroshev. The U.S. Department of State has offered up to USD 10 million for information leading to the arrest and/or conviction of Khoroshev in any country, and the U.S. Department of Treasury—along with authorities in the UK and Australia—has announced sanctions against Khoroshev. However, LockBit posted on its Telegram channel, denying that Khoroshev is the group's leader.



- **What this means:** LockBit took a highly-publicized hit to its reputation and operational capacity after a multi-national law enforcement (LE) coalition seized its data leak site in February. However, the group was able to quickly resurface on the dark web with new infrastructure and soon appeared to continue a normal operational tempo. It is currently uncertain how the disclosure of Khoroshev's identity will affect the group's operations moving forward. However, as of May 9, ZeroFox has observed the group leak data from an exceedingly large number of victims since the announcement two days prior, possibly signaling fear amongst group members and affiliates of additional, imminent LE disruption. ZeroFox will continue to monitor LockBit's activity for additional information, as it is highly likely that the group will announce more victims in the coming days.

Threat Actor Advertised Zero-Day RCE Exploit on Forum



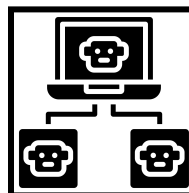
What happened: On May 2, 2024, untested threat actor "dimitry69" advertised a zero-day iOS ZeroClick Remote Code Execution (RCE) exploit on the predominantly Russian-language dark web forum xss. According to the actor, the exploit allows zero-click RCE on iOS devices via the iMessage application. The actor was charging USD 2.5 million for the exploit and stated interested buyers should reach out via Telegram for a proof of concept and more details.

- **What this means:** As dimitry69 is untested, their credibility cannot be confirmed. Threat actors typically purchase zero-day exploits, as they target a vulnerability that is unknown to the vendor and does not have a patch. This allows attackers to compromise systems, run malicious code, and steal data. Ransomware groups have targeted zero-day vulnerabilities to conduct large-scale attacks. As this vulnerability affects a commonly used product, the exploitation of it could have a major impact. However, based on the

uncommonly high price of the exploit, it is likely it will not be purchased, especially coming from an untested actor.

Pro-Palestinian Hacktivist Group Claims New Attack Against Saudi Infrastructure

What happened: On May 7, 2024, pro-Palestinian hacktivist group “Anonymous Arabia” claimed to have executed a cyberattack against the primary electricity company in Saudi Arabia. The attack, which was announced on the group’s Telegram channel, was a distributed denial-of-service (DDoS) attack carried out in retaliation for the Kingdom of Saudi Arabia (KSA)’s purported efforts to crack down on anti-Israeli internet content. Additionally, the Telegram post included the hashtag #HighSociety. It is unclear if High Society, a separate hacktivist collective, was directly involved or is otherwise being used to publicize the attack.



- **What this means:** Anonymous Arabia is a hacktivist group that has been active since shortly after the onset of hostilities between Israel and Hamas. The group has carried out a number of DDoS strikes against nations for what they claim are anti-Palestinian activities. Anonymous Arabia’s primary target has been Israeli infrastructure, including reportedly targeting the Iron Dome system and railroad infrastructure used to move military personnel and material. However, Anonymous Arabia has also targeted infrastructure in the United Arab Emirates (UAE), Egypt, and now the KSA for their perceived pro-Israel actions, as well as a number of media entities in India for airing pro-Israeli information. The hacktivist collective is likely to continue this operational pace while leveraging DDoS attacks to gain notoriety for its cause.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent entities in software solutions, network security domains, and U.S. national security. A critical vulnerability (CVE-2023-49606) has been [discovered](#) in the Tinyproxy software. More than half of the 90,310 hosts with a Tinyproxy service exposed to the internet are reportedly vulnerable to this flaw in the HTTP/HTTPS proxy tool. A firmware update vulnerability (CVE-2023-47166) [discovered](#) in the luci2-io file-import functionality of Milesight UR32L v32.3.0.7-r2 could allow unauthorized firmware updates, compromising its integrity. CVE-2023-47212 in the comment functionality of stb_vorbis.c v1.22 is a critical heap-based buffer overflow vulnerability that could allow an attacker to eventually [execute](#) an arbitrary code. Zoho has [disclosed](#) that APT actors have been actively exploiting CVE-2021-44077i in Zoho ManageEngine ServiceDesk Plus, which is a critical remote control execution bug. Meanwhile, Google has [released](#) security updates for several bugs, including a critical one in Pixel phones and the Pixel Tablet. Chipmaker NVIDIA has [patched](#) three bugs in its Windows ChatRTX application, including two high-severity flaws. Citrix has [disclosed](#) a PuTTY vulnerability (CVE-2024-31497) that enables attackers to reconstruct private keys via cryptographic signature observation, compromising key-based authentication.

Notable vulnerabilities:

[CVE-2024-26026](#) and [CVE-2024-21793](#)



What happened: F5 has patched two critical vulnerabilities in BIG-IP Next Central Manager. These flaws could allow hackers to seize admin control and create secret accounts on managed assets. CVE-2024-26026 and CVE-2024-21793 enable attackers to execute harmful SQL commands remotely via the manager's API.

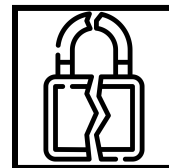
> **What this means:** SQL injection attacks involve inserting malicious SQL queries into input fields or parameters, exploiting security weaknesses in applications. This can lead to unauthorized access and data breaches. The Next Central Manager bugs can allow rogue accounts to be created for malicious purposes without detection.

Affected products:

- BIG-IP Next Central Manager versions 20.0.1 – 20.1.0.

CVE-2023-49606

What happened: A use-after-free vulnerability exists in the HTTP Connection Headers parsing in two Tinyproxy versions. A specially crafted HTTP header can trigger reuse of previously freed memory, which leads to memory corruption and possibly remote code execution as well. An attacker needs to make an unauthenticated HTTP request to trigger this vulnerability. Tinyproxy developers have provided a workaround while they work on publishing the patched version (Tinyproxy 1.11.2).



➤ **What this means:** This vulnerability can be triggered by an unauthenticated HTTP request, allowing an attacker to exploit it without authentication. By sending a carefully crafted HTTP Connection header, an unauthenticated threat actor can induce memory corruption, which in turn may enable remote code execution.

Affected products:

- Tinyproxy 1.11.1
- Tinyproxy 1.10.0



ZEROFOX®

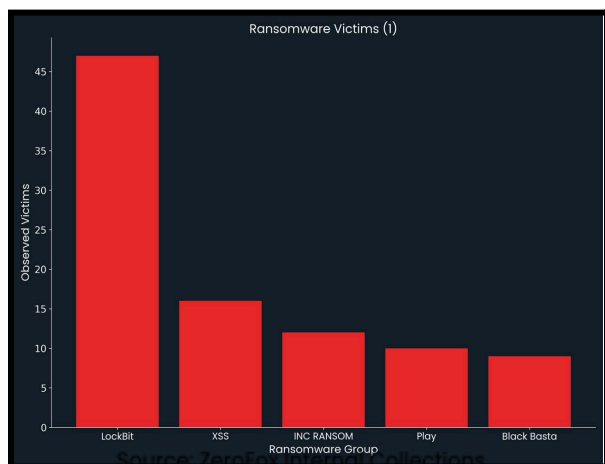
Weekly Intelligence Brief

TLP:GREEN

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: City of Wichita Shuts Down IT Network After Ransomware Attack



What happened: In the past seven days, ZeroFox has observed over 140 ransomware attacks, mostly on the manufacturing and technology sectors, of which over 55 percent of these targets were in North America and Europe. A majority of the attacks were claimed by LockBit. The group was responsible for approximately 30 percent of all ransomware activities in 2023.

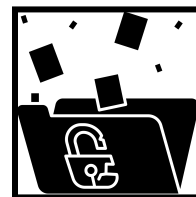
➤ **What this means:** LockBit has claimed almost 60 victims recently; one of its targets was the city of Wichita in Kansas, where the group encrypted certain city services data. Following the

ransomware attack, the city was forced to shut down parts of its network to prevent the attack from spreading. After the cyberattack, payment systems for the city—including those for water bills, court citations, and tickets—are reportedly down. Federal and local law enforcement authorities have been assisting with the aftermath of the attack.

Breach Intelligence: UK Ministry of Defence Breached

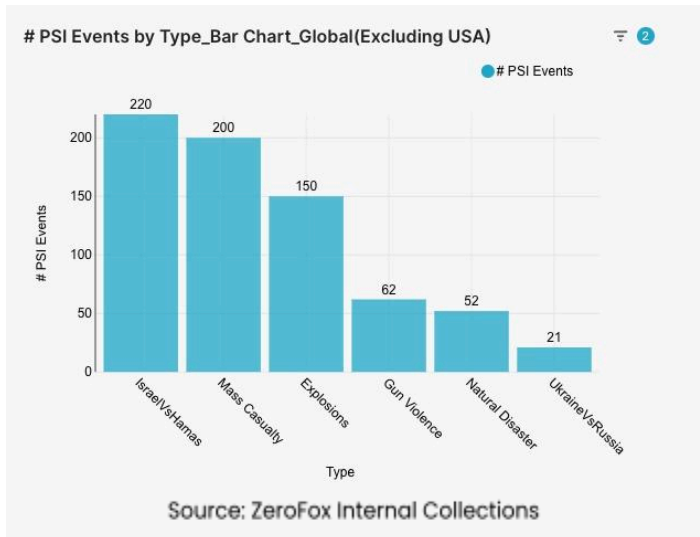
What happened: A breach in the UK's Ministry of Defence (MoD) compromised part of the Armed Forces payment network, exposing personal data of active, reserve, and retired personnel. The attack targeted an external system managed by a contractor that is separate from the MoD's core network.

- **What this means:** Even though the MoD has clarified that salary payments and pensions for veterans were not affected by the attack, it has also stated the attack appears to be the work of a malign actor and that state involvement cannot be ruled out. With 270,000 records exposed and the possibility of state involvement, the exposed information is likely to be used in future spear phishing or other cyberattacks.



Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

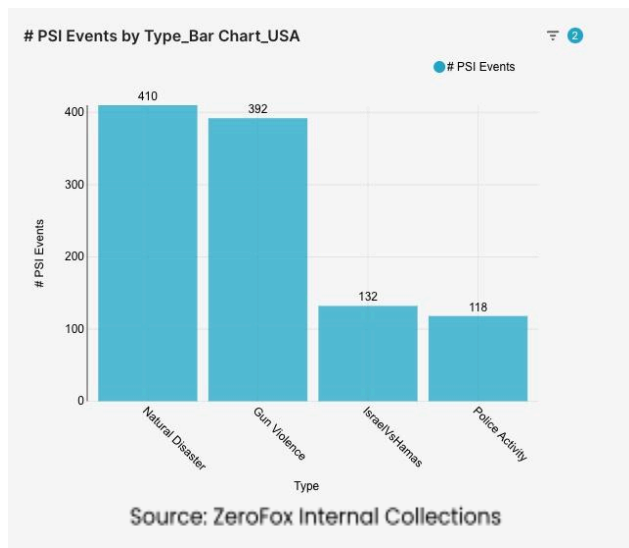


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 10 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Ukraine (in that order); approximately 75 percent of these events were explosions, and 15 percent were bomb threats. General alerts related to the Israel-Hamas war

(including protests, raids, and involvement in neighboring countries) increased by 24 percent from the previous week; notably, Palestine and Israel accounted for 43 percent of all international explosions alerted. Conversely, events related to Russia's war in Ukraine decreased by 32 percent. The top three most-alerted subtypes were explosions, which saw a 2 percent increase from the previous week; gun violence, which decreased by 14 percent; and natural disasters.

- **What this means:** While Ukraine contributed to the most mass-casualty events in the week prior, this past week saw a return to Palestine being the top contributor, likely due to Israeli forces launching their [offensive](#) on Rafah in the effort to seize the remaining Hamas strongholds. This may also explain the increase in explosions, however slight, as Palestine and Israel account for almost half of all reported explosions this week. Natural disasters replaced bomb threats as the third most-alerted incident subtype this week, as there have been several [extreme weather](#) events worldwide, such as flooding in Brazil and record-high heat waves across southeast Asia. Although gun violence as a whole decreased this week, it is notable that Georgia contributed to almost a quarter of these alerts. This may be due to heightened tensions, as tens of thousands of people have been protesting this week regarding a proposed [law](#) that critics see as a threat to media freedom and the country's aspirations to join the European Union.



Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and police activity; notably, this is the first time in several weeks that there have been more natural disaster alerts than gun violence alerts. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim (i.e., not simply shots fired). The top two states that had the most gun violence alerts were Illinois and

Ohio, which together made up almost one-third of this week's nationwide total. Gun violence across the United States increased by 2 percent from the week prior. The top three contributors to natural disaster alerts this week were Texas, California, and New York, and natural disaster alerts across the country increased by 8 percent. The police activity subtype is used to alert evacuations, lockdowns, and heavy police presence for which the reason is not yet known at the time of alerting; Texas, California, and Pennsylvania were the top three contributing states this week for this subtype. Nationwide protest activity as a whole increased by 6 percent from the week prior.

- **What this means:** Natural disasters replacing gun violence as the most alerted incident type this week is likely due to several instances of severe weather; just in the month of May alone, there have been 129 [tornado](#) reports across the country, along with multiple instances of flooding and heavy thunderstorms. Gun violence events nationwide did not show a substantial increase, but Ohio did replace California in the top two contributing states this week, with cities like Cincinnati and Cleveland being at the epicenter of these alerts. Gun violence, as well as police activity, have a pattern of being concentrated in states that have populated cities, like Los Angeles and Philadelphia. As for protests, law enforcement's attempts to crack down on the pro-ceasefire university demonstrations across the country appear to be somewhat futile, as the overall number of protests increased regardless.

Interested in more ZeroFox Threat Intelligence? ZeroFox researchers produce timely, relevant, and actionable [intelligence reporting](#) regularly to keep your team informed on developments in the threat landscape.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: 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%	80-95%	95-99%