



Weekly Intelligence Brief

Classification: TLP:GREEN

May 6, 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 3, 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 May 2024 Geopolitical Brief	2
 Cyber Intelligence Key Findings	4
CISA Issues Guidelines to Mitigate Risks from AI to U.S. Critical Infrastructure	4
Hackers Claim to Have Infiltrated Belarus' Main Security Service	4
UK Passes New Law to Secure Smart Devices by Disabling Default Passwords	5
 Deep and Dark Web Intelligence Key Findings	7
Threat Actor Group R00tKIT Announces Return to Telegram	7
Pro-Russian Threat Actor Group UserSec Conducts Attacks in the UK	7
Threat Actor Punktir Auctioning Two Network Access Bundles to Companies Worldwide	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2024-26305	10
CVE-2024-4406	11
 Ransomware and Breach Intelligence Key Findings	13
Ransomware Intelligence: LockBit Targets French Hospital	13
Breach Intelligence: FBCS Warns of Data Breach Impacting 1.9 Million	13
 Physical and Geopolitical Intelligence 	15
 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	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence May 2024 Geopolitical Brief

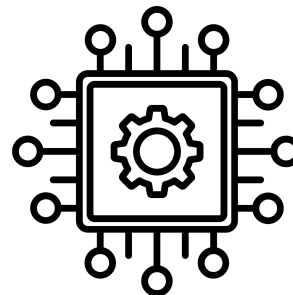
U.S. military aid package should allow Ukraine to better resist Russia militarily until late 2025, after which the question of Western resolve to back Ukraine will re-emerge. An Israeli incursion into Rafah could worsen anti-Israel protests in the United States and see Hamas' allies escalate their military activity in the region. A ceasefire between Israel and Hamas will likely assuage protesters somewhat and calm tensions in the region, which escalated after Israel and Iran broke historic norms by directly targeting each other in April. Expect widespread protests in Argentina in the first half of May, where protesters are seeking to block the senate from approving a key austerity bill. Protests in Georgia are pitting EU supporters against those who wish for closer ties with Russia. Chad is holding elections while trying to balance its historic reliance on Western military support with local support for greater ties with Russia. South Africa will hold its most contentious elections since apartheid, and the fight for votes could turn violent. A presidential inauguration in Taiwan presents China with another opportunity to threaten the island militarily. Panama's presidential elections look like a foregone conclusion unless the Supreme Court bans the leading candidate, which could lead to social unrest. Haiti's Transitional Council already looks inadequate, and its political future will likely be determined by an international police mission. The Singapore leadership transition taking place in mid-May is the most significant in decades, with locals uncharacteristically angry over perceived political corruption. Fuel shortages and a consistently high cost of living could trigger violent protests in Nigeria.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

CISA Issues Guidelines to Mitigate Risks from AI to U.S. Critical Infrastructure

What happened: CISA has released new guidelines, including a four-part mitigation strategy, to fortify U.S. critical infrastructure against three significant types of risks from artificial intelligence (AI): AI-enabled attacks on infrastructure, direct assaults on AI systems, and flaws in AI design threatening infrastructure operations. The four-part strategy emphasizes organizational culture to manage AI risks effectively. It stresses the need for a culture prioritizing safety and security, promoting transparency, and integrating security into core business functions. Furthermore, the guidelines advocate for comprehensive mapping to tailor risk assessment and mitigation to individual organization's AI usage and risk profiles.



- **What this means:** The document emphasizes a proactive approach, urging organizations to embed risk management into their culture and operations. It highlights the importance of understanding AI's context and risks, along with developing systems to assess and track those risks. Additionally, it provides guidance on prioritizing and acting upon AI-related safety and security risks. The Department of Homeland Security has further pledged to update these guidelines to adapt to evolving AI landscapes, underscoring the critical importance of addressing AI risks for national security and public safety. Cyberattacks against U.S. critical infrastructure have increased in the past few months, with threat actors targeting government contractors and departments. Reports have also warned about the use of AI to target critical infrastructure in the months leading up to the U.S. elections.

Hackers Claim to Have Infiltrated Belarus' Main Security Service



What happened: Belarusian hacker activist group "Cyber-Partisans" claims to have breached the network of the country's main KGB security agency and accessed the personnel files of over 8,600 employees. The attack is reportedly in retaliation for the KGB chief accusing the group of plotting attacks on critical infrastructure, including a nuclear power plant. According to a Cyber-Partisans spokesperson, the group tried to infiltrate the KGB network for several years before successfully gaining access to its website

and database.

- **What this means:** This cyberattack is yet another case of geopolitical affairs cascading into the cyber landscape; Cyber-Partisans claims that the KGB is carrying out the largest

political repressions ever in Belarusian history. Even though the KGB has yet to acknowledge the attack, its website displayed an empty page on Friday, hinting at disruption. Cyber-Partisans strengthened its claim by publishing admin details and server logs on Telegram. The group has also claimed responsibility for recently infiltrating the networks of a major fertilizer plant, pressuring the government to release political prisoners. Prior attacks targeted state media and Belarusian Railways. The group has threatened to escalate its activity if the government refuses to accept its demands.

UK Passes New Law to Secure Smart Devices by Disabling Default Passwords

What happened: A new United Kingdom (UK) law, the Product Security and Telecommunications Infrastructure Act, requires manufacturers of smart devices to stop supplying devices that use default passwords and provide a minimum length of time for important security updates.



➤ **What this means:** Default passwords subject devices to easy discovery on the internet, where these passwords are likely to be shared, leaving the devices vulnerable to cyberattacks. The new law will help customers choose smart devices that are designed to protect them against cyberattacks. Manufacturers will be required to meet basic cybersecurity measures such as providing the time period for which the device will receive important security updates and a point of contact for reporting security issues to mitigate the risks associated with cyberattacks.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor Group R00tKIT Announces Return to Telegram

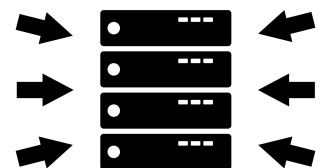


What happened: On April 28, 2024, pro-Russia and pro-Israel hacktivist group “R00TKIT” announced its return to Telegram under the same channel name, R00TKITOFF. At the time of the post, the group claimed to currently have 8,750 members in the channel and announced its goal to reach at least 10,000 members. R00TKIT encouraged users to share the channel within their networks to help the group rebuild its Telegram presence.

- **What this means:** R00TKIT’s return to Telegram comes only 10 days after the group announced the closure of its channel on April 18 and almost two weeks after it claimed to have temporarily disrupted the clearnet site belonging to popular English-language dark web forum “BreachForums.” In the April 18 post, the group explained that it was “transitioning back to operating in the shadows” due to security concerns, likely in response to the high level of attention it received after claiming the attack on BreachForums. However, R00TKIT likely intended to only pause its Telegram activity for a short period of time, as Telegram provides the group with a platform to significantly grow its operations and follower base. In light of the fact that R00TKIT is a rather sophisticated actor and the limited time that the channel was down, it will likely not take long for the group to rebuild its Telegram presence.

Pro-Russian Threat Actor Group UserSec Conducts Attacks in the UK

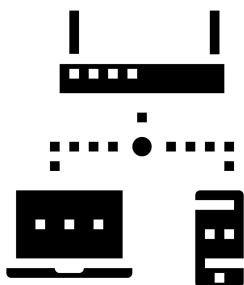
What happened: On April 29, 2024, pro-Russian threat actor group “UserSec” announced attacks against the UK. The distributed denial-of-service (DDoS) attacks were reportedly carried out with the unspecified support of two other pro-Russian threat actor groups: “Noname057(16)” and “Cyber Army of Russia.” The attacks, which were announced on UserSec’s Telegram channel, were directed against the real estate and logistics sectors.



- **What this means:** These attacks come on the heels of UserSec announcing a pending campaign against NATO nations. UserSec has been active primarily in support of the Russian invasion of Ukraine, with their attacks focused on a multitude of NATO targets; its preferred method of attack is DDoS. UserSec’s alliance with other pro-Russian hacktivist groups is not a new phenomenon but demonstrates the increased risk from such groups

supporting each others' efforts. This trend is likely to continue as alliances of convenience against common adversaries emerge.

Threat Actor Punktir Auctioning Two Network Access Bundles to Companies Worldwide



What happened: On April 29, 2024, well-regarded threat actor "Punktir" advertised an auction for a Cisco network access bundle to 81 undisclosed worldwide companies on predominantly Russian-language dark web forum Exploit. The following day, the actor [advertised](#) an auction for a Citrix access bundle to 57 unnamed worldwide companies on the forum. According to Punktir, the sources of both access bundles were "installs" services. The actor also claimed that the access bundles are lists of unique domains with logins and passwords but has specified that the list excludes school and government domains (.edu and .gov),

as well as Russia, Soviet Union, and Ukraine domains (.ru, .su, and .ua). The starting bid for the access bundle was USD 100 USD, with a minimum bid of USD 100 and an instant purchase price of USD 2,000.

- **What this means:** As the actor is well-regarded, it is likely that Punktir's claims are credible and the network access bundles are legitimate. Other threat actors could purchase either of these access bundles to conduct a large number of attacks in quick succession. These bundles could also be beneficial for ransomware groups, as they could gain access to potential victim companies for a low cost compared to what they might receive for each ransom to increase their profit margin.

| 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. Aruba Networking released an [advisory](#) addressing 10 vulnerabilities, including four critical remote code execution (RCE) flaws. GitLab [addressed](#) a critical vulnerability (CVE-2023-7028) being exploited in the wild. The flaw impacts all authentication mechanisms in certain versions. CISA and the FBI have jointly issued an [advisory](#) urging software companies to address path traversal vulnerabilities in their products before deployment. Cisco has released software [updates](#) that address multiple vulnerabilities in Cisco IP Phone firmware vulnerabilities.

Notable vulnerabilities:

[CVE-2024-26305](#)

What happened: This vulnerability is a buffer overflow vulnerability in the underlying Utility daemon that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). This

CRITICAL vulnerability is assigned a CVSS score of 9.8.

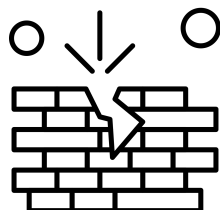
➤ **What this means:** Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system. Enabling the Enhanced PAPI Security feature using a non-default key will prevent exploitation of this vulnerability in ArubaOS 8.x.



Affected products:

- ArubaOS 10.5 to 10.5.1.0 and below
- ArubaOS 10.4 to 10.4.1.0 and below
- ArubaOS 8.11 to 8.11.2.1 and below
- ArubaOS 8.10 to 8.10.0.10 and below
- ArubaOS 10.3
- ArubaOS 8.9
- ArubaOS 8.8
- ArubaOS 8.7
- ArubaOS 8.6
- ArubaOS 6.5.4
- SD-WAN 8.7.0.0-2.3.0
- SD-WAN 8.6.0.4-2.2

CVE-2024-4406



What happened: This vulnerability allows remote attackers to execute arbitrary code on affected installations of Xiaomi Pro 13 smartphones. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. This **HIGH** vulnerability is rated with a CVSS score of 8.8.

➤ **What this means:** The specific flaw exists within the integral-dialog-page.html file. When parsing the integralInfo parameter, the process does not properly sanitize user-supplied data, which can lead to the injection of an arbitrary script. An attacker can leverage this vulnerability to execute code in the context of the current user.

Affected products:

- Xiaomi Pro 13



ZEROFOX®

Weekly Intelligence Brief

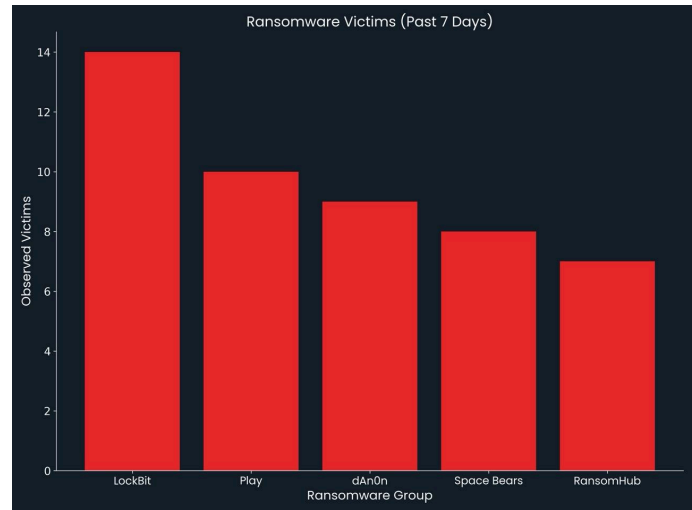
TLP:GREEN

Ransomware and Breach Intelligence

| Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: LockBit Targets French Hospital

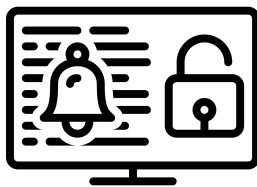
What happened: ZeroFox observed an update on LockBit 3.0's leak site naming French hospital Hôpital de Cannes – Simone Veil (CHC-SV) as a victim. Meanwhile, CHC-SV has [announced](#) its refusal to pay the ransom demanded by LockBit. CHC-SV has also pledged to notify all individuals impacted by the attack. The hospital announced a major disruption in its network on April 17 and took its systems offline to contain the damage from the cyberattack. Additionally, ZeroFox has recorded 12 more ransomware incidents attributed to LockBit since last week.



Source: ZeroFox Internal Collections

- **What this means:** Ransomware groups have been increasingly targeting the healthcare industry; there was a recent major attack against Change Healthcare, where two groups demanded ransoms from the victim company. The consequences of CHC-SV refusing to pay LockBit's ransom demands remain unclear. Since LockBit's takedown in February, the group has been unable to conduct any significant attacks. Additionally, ZeroFox Intelligence has also observed LockBit recording the highest ransomware activity this week, indicating the group's recovery.

Breach Intelligence: FBCS Warns of Data Breach Impacting 1.9 Million



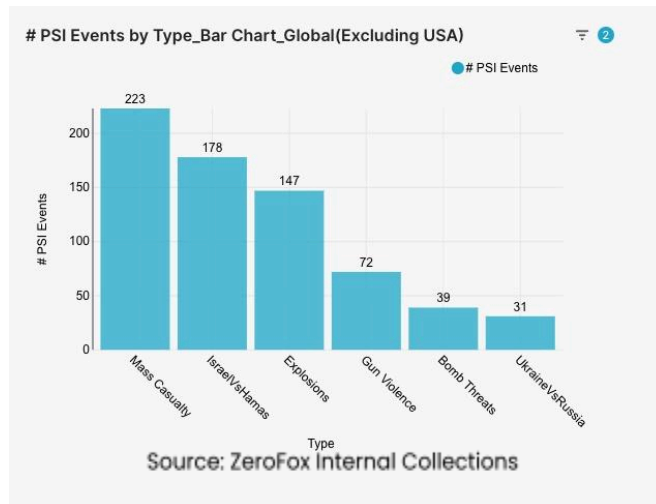
What happened: Financial Business and Consumer Solutions (FBCS) has suffered a data breach that impacted over 1.9 million individuals in the United States. Unauthorized access was detected in specific systems within the agency's network, potentially exposing sensitive information such as full names, Social Security Numbers (SSN), dates of birth, account details, and driver's license numbers or ID cards.

- **What this means:** The data breach poses increased risks of phishing, fraud, and social engineering attacks for the affected individuals. While FBCS has implemented additional security measures to prevent future breaches, recipients of the data breach notification

are advised to stay vigilant against unsolicited communications and monitor their accounts and credit reports for any suspicious activity.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 7 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Ukraine, Palestine, and Lebanon, in that order; approximately 66 percent of these events were explosions, and 17 percent were bomb threats. Notably, this is the first time in several weeks that Palestine has not been the top contributor to

the number of mass casualty events alerted; however, general alerts related to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries) increased by 13 percent. Conversely, events related to the Ukraine conflict decreased by 24 percent. The top three most-alerted subtypes were explosions, which saw a 16 percent decrease from the previous week; gun violence, which increased by 3 percent; and bomb threats.

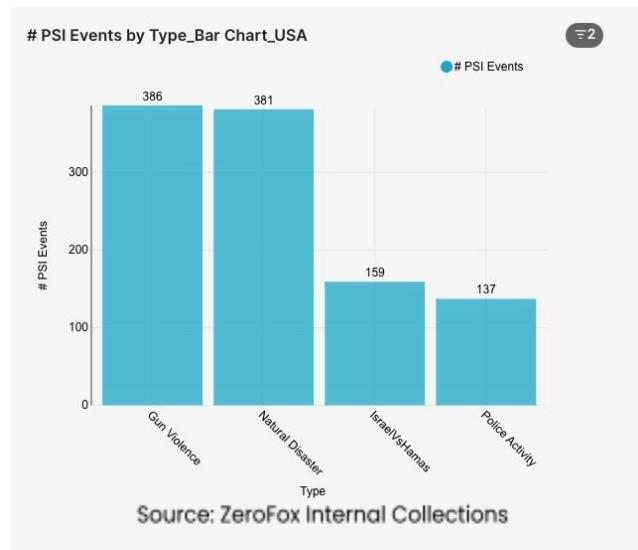
- **What this means:** While Palestine was not the top contributor to mass casualty events alerted this week, the overall amount of alerts in relation to this particular conflict did increase from the week prior. Lately, the focus has been on Rafah, as Israeli President Netanyahu has vowed to send in ground troops to the area with or without a hostage deal; just this week, Israeli airstrikes on Rafah have [killed](#) over 20 people, and the fate of millions of civilians seeking refuge there is to be determined. As for Ukraine, despite the recent U.S. aid package, the country continues to experience attacks in its major cities such as Odesa and Kharkiv; additionally, the U.S. State Department released a statement late Wednesday in which it [accused](#) Russia of violating the Chemical Weapons Convention (CWC) by using the choking agent chloropicrin against Ukrainian forces. This—along with Russia's repeated attacks on oil refineries, army bases, and power reserves—may be the reason why Ukraine was the top contributor of mass casualty events this week. Mass casualty events overall (excluding the United States) did decrease somewhat, but not by a significant enough amount to speculate on any major shifts in the global conflict sphere.

Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disasters, and police activity; notably, these are the same top three as the two previous weeks. 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 California, which together made up over 20 percent of this week's nationwide total. Gun violence

across the United States increased by 12 percent from the week prior. As structure fires and wildfires currently fall under the natural disaster scope, the majority of natural disasters alerted this week consist of these events. The top two contributors to the natural disaster alerts this week were California and Texas. 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; California and Texas were the top two contributing states this week for this subtype as well. Nationwide protest activity as a whole increased by 25 percent from the week prior, and the percentage of protests that were in relation to the conflict in Palestine increased by 130 percent, marking the biggest percentage increase in several weeks.

- **What this means:** For the past three weeks, ZeroFox has witnessed the same top three most-alerted incidents subtypes, with gun violence being the most alerted. What causes this pattern is a topic of frequent debate; while correlation does not necessarily equal causation, areas with a larger volume of and [easier](#) access to firearms typically see higher levels of shootings. Gun violence often occurs in major cities such as Los Angeles and Chicago, which elucidates why California and Illinois contribute a significant amount to overall gun violence instances. Texas and California, the top two contributors to this week's natural disaster alerts, have experienced wildfires as well as structure fires this week, possibly due to drier climates in those particular areas. For protest activity, the drastic increase in protests regarding the Israel-Hamas war may be explained by the continued nationwide college campus movement, which has sparked controversy due to the use of higher levels of law enforcement to control the crowds, student arrests, teacher strikes, and physical clashes amongst demonstrators and police. The exact number of arrests remains unclear but is believed to have [exceeded](#) 1,300 since the start of the latest bout of protests



two weeks ago, with more students being detained on Wednesday evening. Despite efforts by law enforcement to clear out protester encampments, this has not deterred students from continuing to host demonstrations.

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%