



Weekly Intelligence Brief

Classification: TLP:GREEN

April 1, 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 March 29, 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 - UK Confirms Chinese State-Sponsored Cyberattacks	2
ZeroFox Intelligence Brief - Article 23 and Risks to Foreign Nationals in Hong Kong	2
ZeroFox Intelligence Flash Report - Terror Threat Ahead of European Summer Events	2
ZeroFox Intelligence Brief - Underground Economist: Volume 4, Issue 7	3
 Cyber Intelligence Key Findings	5
Elite Russian Hackers Targeting German Politicians	5
CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate SQL Injection Vulnerabilities	5
Two Chinese APT Groups Ramp Up Cyber Espionage Against ASEAN Countries	6
 Deep and Dark Web Intelligence Key Findings	8
Threat Actor Claims DDoS Attack Against U.S.-Based Electric and Natural Gas Utility Company	8
Actor BLBEV2 (aka DBLand) Selling Fortinet Access to Numerous Companies Worldwide	8
Actor EMorocco Claims to Have Access to the U.S. Social Security Administration	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2023-48788	11
CVE-2023-24955	12
 Ransomware and Breach Intelligence Key Findings	14
Hackers Threaten to Leak Data of NHS Scotland	14
Breach Intelligence: Hackers Breach Indian Critical Infrastructure	14
 Physical and Geopolitical Intelligence 	16
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – UK Confirms Chinese State-Sponsored Cyberattacks

On March 25, the United Kingdom (UK) government warned the public about Chinese state-sponsored entities, while two U.S. government agencies sanctioned alleged Chinese hackers linked to APT31. The UK government is wary of growing threats from Chinese state-sponsored entities targeting and undermining the country's democratic processes. The announcement attributed two cyberattacks against UK political entities to Chinese state-sponsored actors. The U.S. Justice Department and the Federal Bureau of Investigations (FBI) unsealed an indictment against seven alleged Chinese hackers associated with APT31 involved in targeting U.S.-based critics, businesses, and political officials over approximately 14 years.

ZeroFox Intelligence Brief – Article 23 and Risks to Foreign Nationals in Hong Kong

Article 23, an updated Hong Kong-specific national security law, went into effect on March 23. A previous version of the law that brought Hong Kong's legal system in line with mainland China's prompted mass protests in 2019 and 2020. The updated version expands the list of crimes to include accessing data that was previously legally permissible and increases the punishment for offenders. The broad and vague wording of Article 23 could be applied to a wide range of data types, like financial and economic growth figures that firms consider necessary for operations. Western firms that have used Hong Kong to access the Chinese market for years will likely experience a more difficult operating environment and a heightened risk of arrest for their employees.

ZeroFox Intelligence Flash Report – Terror Threat Ahead of European Summer Events

Several European countries have stepped up security following the attack carried out by Islamic State-Khorasan (IS-K) operatives in Moscow on March 22. Authorities in France and Germany, in particular, are in a heightened state of alert in the run-up to the Euro 2024 soccer tournament held across Germany and the Paris Olympics due to take place between June and August 2024. European authorities are warning that the Islamic State (IS) threat to Europe is at its highest level in years. The warning is likely a reflection of the increased threats since the outbreak of the Israel-Hamas war and the large upcoming spectator events rather than of the group's capabilities, which remain diminished.

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 7

On March 25, untested Russian-speaking threat actor “grossoman15” announced in the deep and dark web (DDW) forum Exploit the intent to launch a new credit card shop named “Tucker Carlson.” The actor specified that they are seeking Russian-speaking sellers that have access to card details from the United States, Canada, Australia, and the UK. The compensation for vendors is an average of USD 100 per 1,000 cards. On March, 24, 2024, vetted actor “SorterPassX” announced the launch of a Telegram-based, session cookies sales service on the Russian-speaking BlackHatForum (BHF). On March 13, 2024, untested actor “ZNAEM” posted an announcement in the Russian-speaking DDW forum WWH-Club advertising a new service named “Znaem Security Service.” The service offers “extensive” access to information from databases belonging to various Russian government departments. On March 11, 2024, actor “blackdatabase” announced the sale of custom phishlets for Evilginx3 on the DDW forum xss. The actor listed commonly used phishlets with prices starting at USD 500 for an outlook[.]com phishlet and ranging up to USD 5,000 for phishlets targeting banking services, including Wells Fargo and Chase.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

Elite Russian Hackers Targeting German Politicians



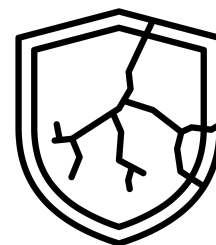
What happened: APT29 (also known as Midnight Blizzard, NOBELIUM, and Cozy Bear), a hacking group associated with Russian intelligence, targeted multiple members of German political parties intending to infiltrate their networks and steal data. The hackers attempted to phishing key German political figures by sending email invitations to a fictitious dinner event hosted by the Christian Democratic Union (CDU), Germany's center-right political party. The CDU acknowledged the ongoing threat of digital attacks from both domestic and foreign sources and confirmed receiving prompt information about the attack,

clarifying that the March 1 dinner event was fabricated.

- **What this means:** Researchers have observed that the phishing campaign targeting German politicians has been ongoing since February 2024, marking the first time APT29 has targeted political parties. The threat group sent phishing emails that tricked the victims into installing a backdoor malware strain, WineLoader, on their systems. Because APT29's malware delivery operations are reportedly aligned with Russia's geopolitical interests, the threat actor's interest is likely to expand beyond Germany. With the U.S. presidential election to be held in November this year, researchers assess that Western politicians are likely to become targets in future Russian intelligence-linked cyber espionage activity.

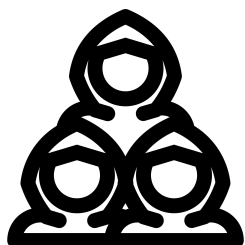
CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate SQL Injection Vulnerabilities

What happened: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the FBI have jointly released an alert in response to the recent, well-publicized exploitation of SQL injection (SQLi) defects in a managed file transfer application that impacted thousands of organizations. Additionally, the alert highlights the prevalence of this class of vulnerability. CISA and the FBI urge senior executives at technology manufacturing companies to mount a formal review of their code to determine its susceptibility to SQLi compromises. If found vulnerable, senior executives should ensure their organizations' software developers begin immediate implementation of mitigations to eliminate this entire class of defect from all current and future software products.



- **What this means:** SQL injection vulnerabilities involve inserting user-supplied input directly into an SQL command, allowing threat actors to execute arbitrary queries. SQLi vulnerabilities let threat actors steal sensitive information and tamper with, delete, or render information unavailable in a database. SQL injections succeed because software developers fail to treat user-supplied content as potentially malicious. CISA and the FBI recommend that software manufacturers adopt using prepared statements with parameterized queries as a standard practice in software development.

Two Chinese APT Groups Ramp Up Cyber Espionage Against ASEAN Countries



What happened: China-linked advanced persistent threat (APT) group Mustang Panda has attacked Myanmar and other Asian countries via phishing emails to deliver malware. Additionally, the actor was observed installing a variant of the PlugX backdoor called DOPLUGS. Another group called Earth Krahang has targeted more than 100 entities across 35 countries to deliver malware such as PlugX, ShadowPad, and more.

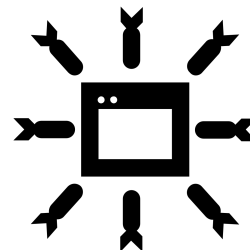
- **What this means:** Over the past three months, cybersecurity researchers have observed increased activities involving APTs associated with China targeting entities connected with the Association of Southeast Asian Nations (ASEAN) as part of cyber espionage campaigns. Mustang Panda has reportedly targeted entities in Myanmar, Philippines, Japan, and Singapore, attacking them with phishing emails designed to deliver two malware packages. One of the malware packages involves a ZIP file that contains an executable that, when launched, loads a DLL file and ultimately deploys a known Mustang Panda malware called PUBLOAD (this downloader was previously employed to drop PlugX). The second package is a screensaver executable that is used to retrieve next-stage malicious code from a remote IP address, including a benign program signed by a video game company renamed as WindowsUpdate[.]exe and a rogue DLL.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

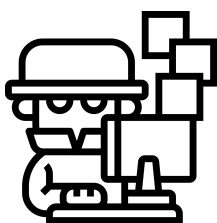
Threat Actor Claims DDoS Attack Against U.S.-Based Electric and Natural Gas Utility Company

What happened: On March 25, 2024, pro-Russian hacktivist group “Server Killers” claimed on their Telegram channel to have conducted a distributed denial-of-service attack (DDoS) against Energy East, a U.S.-based electric and natural gas utility company. In the same post, Server Killers also alleged to have attacked U.S.-based vehicle contract and warranty provider AulCorp. According to the group’s Telegram channel—which appears to date back to November 2023 and has remained highly active since its creation—the group has primarily targeted NATO member countries, particularly Luxembourg and Romania. In previous posts, Server Killers claimed to have targeted the nato[.]int domain and directly announced that it was engaged in a cyber war against NATO. However, this is the first time Server Killers has announced attacks on U.S.-based entities.



- **What this means:** While ZeroFox cannot confirm the legitimacy of these most recent claimed attacks, it is highly likely that Killer Servers will continue to post similar content in the short term, and there is a moderate chance that these posts will increasingly mention attacks against U.S. entities. Additionally, while cyberattacks against NATO by Russian threat actors are not novel, cyberattacks on critical infrastructure entities (such as the one allegedly targeting Energy East) have repeatedly proven to cause significant regional and global supply chain disruptions. This activity is likely to continue—if not increase—throughout 2024, particularly as the Ukraine-Russia and Israel-Hamas conflicts persist.

Actor BLBEV2 (aka DBLand) Selling Fortinet Access to Numerous Companies Worldwide



What happened: On March 23, 2024, untested threat actor “BLBEV2” advertised Fortinet VPN access to 26 undisclosed companies worldwide on the predominantly Russian-language dark web forum xss. That same day, untested [actor “DBLand” made an identical post on the predominantly English-language dark web forum BreachForums](#). The actor did not disclose the ultimate source of the data breach or how it was exploited but listed the

countries and revenue for each company. A majority of the companies were located in the Philippines and the United States, but some of the targets were also in Malaysia, Chile, France, Kuwait, India, Mexico, Tunisia, Pakistan, and Morocco. The actor charged a minimum price of USD 500 for the access depending on the company's details and requested that interested actors communicate via TOX, Jabber, or Telegram.

- **What this means:** Because of the timing and identical posts, as well as the use of the same contact information, it is highly likely the same actor is operating under different aliases across platforms. An actor could purchase all of these accesses for approximately USD 13,000 and conduct a large number of attacks. This could be beneficial for ransomware groups, as they could gain access to a potential victim company for a low cost compared to what they might receive for each ransom. Single access could also be purchased by lower-tier actors trying to evolve their capabilities by stealing a company's data and reselling it for a higher cost.

Actor EMorocco Claims to Have Access to the U.S. Social Security Administration

What happened: On March 27, 2024, threat actor group "EMorocco" claimed to have gained access to the U.S. Social Security Administration (SSA). The claim was posted to the group's Telegram channel and included a link containing what EMorocco claims are samples of leaked SSA data. EMorocco did not post any further information about the purported leak, what the group has access to, or when they plan to release more information. Based upon the secondary characteristics of the post, it appears the leak is in support of freeing Palestine.



- **What this means:** EMorocco, which is short for "Evil Morocco", is a relatively new threat actor whose capabilities and motives are unclear at this point. ZeroFox assesses with limited confidence that the threat actor may be a hacktivist group based upon the SSA leak being tied to pro-Palestinian activism. U.S. government organizations such as the SSA make for lucrative targets for cybercriminals, whether for financial gain or drawing attention to a cause, as they possess large amounts of potentially sensitive information such as citizens' personally identifiable information (PII). ZeroFox will continue to monitor EMorocco to identify further such attacks or leak of data.

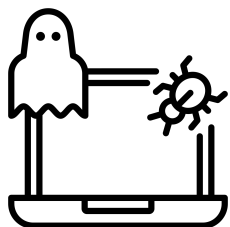
| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies in software solutions, asset management, and network security domains. CISA has added four vulnerabilities—CVE-2023-24955, CVE-2023-48788, CVE-2021-44529, and CVE-2019-7256—to its Known Exploited Vulnerabilities (KEV) Catalog, indicating that there is evidence of active exploitation. CVE-2023-24955 (CVSS score: 7.2/10) is a remote code execution (RCE) vulnerability in Microsoft SharePoint Server. Microsoft [patched](#) it with SharePoint updates released in May 2023. CVE-2023-48788 (CVSS score: 9.8/10) is an improper neutralization of special elements [used](#) in an SQL command (SQL Injection) vulnerability [CWE-89] in FortiClientEMS. CVE-2021-44529 (CVSS score: 9.8/10) is a code [injection](#) vulnerability in the Ivanti EPM Cloud Services Appliance, while CVE-2019-7256 (CVSS score: 10.0/10) is a Nice Linear eMerge E3-Series OS command [injection](#) vulnerability. Apple has [disclosed](#) details about a new vulnerability (CVE-2024-1580; CVSS score: 5.9/10.0) in some Apple iOS and iPadOS products. Threat actors have been exploiting a missing authentication vulnerability (CVE-2023-48022; CVSS score: 9.8/10) in the Ray AI framework to compromise hundreds of clusters. CVE-2023-48022 was [disclosed](#) in November 2023 by Anyscale, Ray AI's parent company. Mozilla has [released](#) security updates to patch two zero-day vulnerabilities that were exploited during a recent hackathon. An out-of-bounds access flaw (CVE-2024-29943) and a privileged JavaScript execution issue in event handlers (CVE-2024-29944) have been fixed in Firefox 124.0.1. Rockwell Automation has informed customers of 10 vulnerabilities discovered recently, six of which are in [Arena Simulation products](#); the rest are in Rockwell's FactoryTalk and PowerFlex products.

Notable vulnerabilities:

[CVE-2023-48788](#)



What happened: CVE-2023-48788 is an improper neutralization of special elements used in an SQL command (SQL injection) in Fortinet FortiClient Enterprise Management Server (EMS). Fortinet disclosed this vulnerability last month. It has now updated its advisory, adding that the vulnerability “is exploited in the wild.” This **CRITICAL** vulnerability has been assigned a CVSS score of 9.8.

➤ **What this means:** CVE-2023-4878 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted requests. At the time of writing, there is no information about attacks leveraging CVE-2023-4878. However, CISA has urged organizations to install patches or implement mitigations immediately. State-sponsored actors have previously exploited Fortinet product

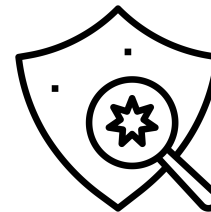
vulnerabilities in cyberattacks targeting critical infrastructure. Fortinet has released a patch for CVE-2023-4878 in FortiClientEMS versions 7.2.3 or above and 7.0.11 or above.

- **Affected products:**

- FortiClientEMS versions 7.2.0 through 7.2.2
- FortiClientEMS version 7.0 (7.0.1 through 7.0.10)

CVE-2023-24955

What happened: CISA has added a Microsoft SharePoint Server bug (CVE-2023-24955) to its KEV Catalog based on evidence of active exploitation. Microsoft has disclosed that, in a network-based attack, this **CRITICAL** severity bug can allow an authenticated attacker to execute code remotely on the SharePoint Server.



- **What this means:** Federal Civilian Executive Branch (FCEB) agencies have to remediate this vulnerability by the due date of April 16, 2024, to protect their networks against active threats. CISA advises applying mitigations per vendor instructions or discontinuing use of the affected products if mitigations are unavailable.

- **Affected products:**

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016

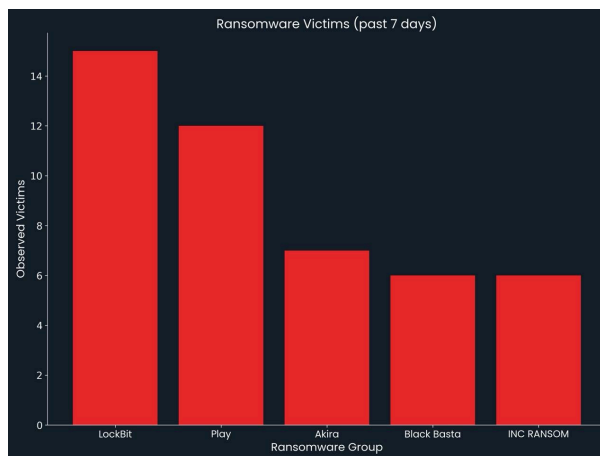
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Hackers Threaten to Leak Data of NHS Scotland

What happened: ZeroFox has observed the “INC Ransom” extortion gang claiming to have breached National Health Service (NHS) Scotland, and the adversary is threatening to release three terabytes of stolen data unless a ransom is paid.

- **What this means:** INC Ransom has shared images containing medical details and has posted sample documents with sensitive information about doctors and patients from NHS Scotland. ZeroFox



Source: ZeroFox Internal Collections

has also observed INC Ransom targeting enterprises from different countries such as Otolaryngology Associates (United States), Barrie and Community Family Health Team (Canada), Ejército del Per (Army of Peru), and more. The number of enterprises experiencing ransomware attacks has surged over time. ZeroFox has detected over 95 ransomware attacks over the past seven days primarily orchestrated by LockBit and Play; 59 percent of the attacks were from North America and Europe. Globally, the “Agenda” ransomware group (aliases: Qilin and Water Galura) has been attacking VMware vCenter and ESXi servers worldwide. The group has focused on the United States, Argentina, Australia, and Thailand and has been targeting industries critical to the economy, such as finance and law.

Breach Intelligence: Hackers Breach Indian Critical Infrastructure



What happened: Indian government entities and the energy industry have been hit with a cyberattack using a modified version of an open-source information stealer called HackBrowserData that can exfiltrate sensitive information. The information stealer was delivered via a phishing email masquerading as an Indian Air Force invitation letter. The threat actor has successfully compromised private energy companies, harvesting financial documents, personal details of employees, and details about drilling activities in oil and gas. The campaign has

compromised about 8.81 GB of data.

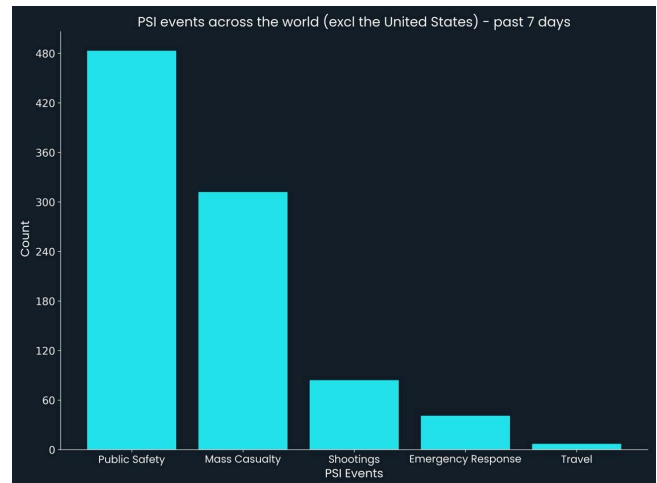
- **What this means:** The phishing email contained an ISO file comprising a Windows shortcut (LNK). The shortcut triggered the execution of a hidden binary present within the mounted optical disk image. The attacker used Slack channels as exfiltration points to upload confidential internal documents, private email messages, and cached web browser data after the malware's execution. Affected individuals and companies should be wary of unsolicited communication involving targeted emails or calls from unknown sources, as threat actors might use the leaked information for spear phishing attacks.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: During an attack on Crimea, Ukraine's navy reported that a Ukrainian missile hit a Russian naval reconnaissance vessel that had been previously captured from Kyiv during the 2014 annexation of Crimea. The struck vessel sustained damage from a Neptune anti-ship missile; the extent of the damage is still being assessed by Kyiv. In the Israel-Hamas war, the UN Security Council failed to pass a U.S.-led resolution for a cease-fire between Israel and Hamas in Gaza, with Russia and China voting against it. However, a resolution passed recently that emphasizes the need for a ceasefire during Ramadan, the release of hostages, and urgent aid delivery to Gaza's starving population. The conflict, ongoing for nearly six months, has led to significant casualties and an imminent famine in Gaza.



Source: ZeroFox Internal Collections

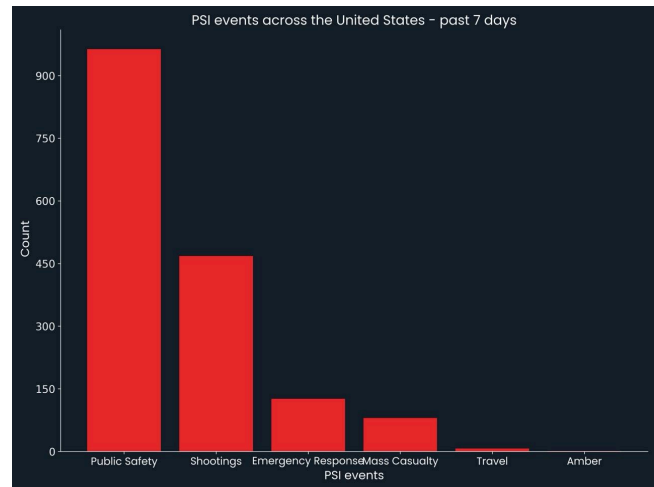
- **What this means:** Ukraine has dealt significant blows to Russia's Black Sea fleet, once instrumental for Moscow's power projection into the Mediterranean and Middle East, through the use of naval drones and missiles that have resulted in the loss of warships and even a submarine. Meanwhile, a U.S.-proposed UN draft for ending the Israel-Hamas war was vetoed, with 11 votes in favor, three against (Algeria, China, and Russia), and one abstaining (Guyana). Ambassadors supported a new draft by the "E-10" group calling for an immediate ceasefire, highlighting the urgent need for humanitarian aid and lifting barriers. Disagreements over draft elements persisted, with concerns raised about exclusions, while some called for swift action to address food shortages and pursue a two-state solution.

Physical Security Intelligence: United States

What happened: Investigations into the events leading up to the recent Francis Scott Key Bridge tragedy continue. The catastrophic collapse of the bridge sent eight construction workers into the freezing Patapsco River; four have been rescued and the other four are presumed dead. Shootings

in Illinois and New York increased by 6 and 20 percent from last week. This week, Illinois saw no instances of bomb threats; however, New York and California saw equal increases in bomb threats compared to last week. Additionally, Illinois experienced a decrease in gun violence by close to 33 percent. California also saw a decrease by almost 16 percent in gun violence, while New York saw an increase this week by 42 percent.

- **What this means:** New York, California, and Illinois had the highest number of public safety, shooting, and violence incidents this week. Meanwhile, in the Baltimore bridge incident, the overall casualties were greatly limited thanks to police intervention that diverted traffic off the bridge soon after the cargo ship sounded mayday alarms.



Source: ZeroFox Internal Collections

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%