



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

July 8, 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 July 5, 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 Brief – Underground Economist: Volume 4, Issue 13	2
ZeroFox Intelligence Flash Report – New Extended Validation Code Signing Service Advertised	2
 Cyber Intelligence Key Findings	4
Kimssuky Using TRANSLATEXT Browser Extension to Steal Sensitive Data	4
Threat Actors Target Multiple Arabian Entities Citing Political Reasons for the Attacks	4
Latest Intel CPUs Impacted by New Indirector Side-Channel Attack	5
 Deep and Dark Web Intelligence Key Findings	7
Actor Claims to Leak Data From Virginia Department of Elections	7
Ransomware Targeting Florida Department of Health	7
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2024-2973	9
CVE-2024-6387	10
 Ransomware and Breach Intelligence Key Findings	12
Ransomware Intelligence: Infosys McCamish Says LockBit Stole Data of 6 Million People	12
Breach Intelligence: Global Data Breaches Paralyze Systems	13
 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 Brief – Underground Economist: Volume 4, Issue 13

On June 18, 2024, positive reputation actor “thanhvnth” announced the sale of verified X (formerly Twitter) “Blue” accounts on the Russian-speaking community xss. Such services are widespread in deep and dark web (DDW) marketplaces, and ZeroFox has observed a significant uptick in the number of threat actors selling X accounts since the start of 2024. On June 16, 2024, a positive-reputation actor known as “spam_assistant” announced a new tool called Data Fusion in the dark web forum Exploit. On June 14, 2024, positive-reputation actor “USDoD” posted a thread on the social media platform X advertising a banner for their new hacking forum, “Breach Nation.” On June 13, 2024, prominent and well-regarded threat actor IntelBroker registered an account on the popular illicit hacking forum BreachForums—one day after removing themselves from the platform. Shortly after rejoining, IntelBroker resumed publishing numerous high-profile data leaks.

ZeroFox Intelligence Flash Report – New Extended Validation Code Signing Service Advertised

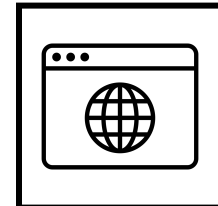
Untested actor “enryu” advertised a new extended validation (EV) code signing service on the primarily Russian-speaking dark web forum Exploit. According to the advertisement, illicit validation certificates can be purchased, which allow malicious webpages to bypass security protocols such as SmartScreen, Windows User Account Control, and Windows Defender, as well as some antivirus (AV) software provided by third parties. Illicit validation certificates offer cyber threat actors the ability to augment a wide array of malicious activities, such as the deploying of disruptive malware to target networks, enhanced social engineering attacks, or data theft resulting in operational disruption, extortion or fraud. Given the versatility offered by initial network access, services such as these are very likely to appeal to a wide range of threat actors with varying intents and motivations, leading to their continued development, competitiveness, and innovation.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

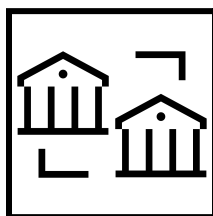
[Kimsuky Using TRANSLATEX Browser Extension to Steal Sensitive Data](#)

What happened: A North Korea-linked group named Kimsuky has deployed a malicious web browser extension called TRANSLATEX to target South Korean academia studying North Korean politics. The extension, disguised as a legitimate translation tool, steals sensitive information such as emails, passwords, and browser screenshots by bypassing security measures.



- **What this means:** The stolen data, including credentials and sensitive information, could potentially be used for espionage, identity theft, phishing attacks, or further cyber operations. Moreover, the use of sophisticated techniques like masquerading as legitimate software highlights the evolving tactics of threat actors to deceive and exploit users. TRANSLATEX has other capabilities, such as capturing browser screenshots that can provide insights into user activities and potentially confidential information. It can also delete browser cookies that could disrupt user sessions, enabling attackers to perform unauthorized actions or maintain persistent access. Its ability to fetch commands from a remote server allows for dynamic control over infected machines, facilitating additional espionage or malware deployment.

[Threat Actors Target Multiple Arabian Entities Citing Political Reasons for the Attacks](#)



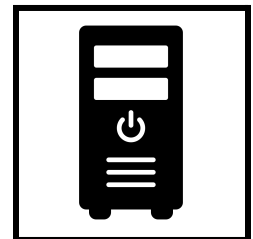
What happened: ZeroFox has observed threat actor SN_Blackmeta claiming to target prominent entities in the United Arab Emirates (UAE), including two banks, a news agency, and a news channel. In a second wave of attacks, the same actor [claimed](#) to have targeted two more UAE companies, a bank and a telecommunications company. Meanwhile, threat actor Anonymous KSA has [claimed](#) to have carried out cyberattacks against several websites of Saudi Arabian ministries, including communications, economy, defense, sports, and civil service. Both of the threat actors have cited their support for Palestine as the motive for these cyberattacks.

- **What this means:** SN_Blackmeta has allegedly disabled the critical infrastructure and disrupted incoming and outgoing transfers of one of the targeted banks. On the other hand, Anonymous KSA has claimed that the targeted ministry websites have “dropped in most countries.” Geopolitical stances have often driven cyber warfare. Instances of this behavior are frequent nowadays, with a significant portion associated with the two major ongoing wars, the Russia-Ukraine War and the Israel-Hamas War. Several threat actors,

like SN_Blackmeta and Anonymous KSA, have announced their allegiances and are participating in attacks that reflect their support. Pro-Palestine hackers will likely increase their activity targeting the United Arab Emirates and Saudi Arabian entities due to their evolving diplomatic ties with Israel and perceived shifts in support for the Palestinian cause. Additionally, targeting influential nations like the UAE and Saudi Arabia garners significant international attention, highlighting the Palestinian issue. It is important to note that irrespective of the motives behind such cyberattacks, the civilian population is almost always caught in the crossfire and is subjected to financial losses and psychological threats.

Latest Intel CPUs Impacted by New Indirector Side-Channel Attack

What happened: Researchers have discovered a new type of high-precision Branch Target Injection (BTI) attack dubbed “Indirector” affecting modern Intel processors, including chips from the Raptor Lake and the Alder Lake generations. It exploits vulnerabilities in the Indirect Branch Predictor (IBP) and Branch Target Buffer (BTB), two hardware components in modern Intel CPUs, to manipulate speculative execution and potentially steal sensitive data.



- **What this means:** The discovery of the “Indirector” attack on modern Intel processors underscores significant vulnerabilities in speculative execution mechanisms crucial for performance optimization in CPUs. The IBP and BTB, critical components in modern processors for branch prediction, are vulnerable to targeted attacks due to flaws in their design, such as indexing, tagging, and entry-sharing mechanisms. By exploiting flaws in these, attackers can manipulate these components to execute unauthorized code and potentially extract sensitive data from affected systems. Indirectors exploit the vulnerabilities through methods like iBranch Locator, IBP/BTB injections, and ASLR bypass, enabling speculative execution and potential data inference using cache side-channel techniques like timing measurements.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Actor Claims to Leak Data From Virginia Department of Elections

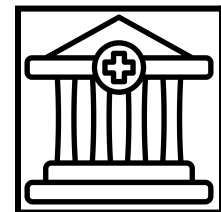


What happened: On June 29, 2024, well-regarded and established threat actor IntelBroker claimed to have leaked a database from the Virginia Department of Elections on the predominantly English-language dark web forum, "BreachForums." The leaked package contains 65,000 rows of candidate ID, candidate name, total votes, party, election name, election ID, office ID, and number of seats. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

- **What this means:** An electoral database containing sensitive information of over 6 million Virginia voters was made available on the dark web forum, "BreachForums." This breach potentially exposes voters to identity theft and other forms of fraud. Moreover, it undermines public trust in the electoral system, which is crucial for maintaining democratic processes. The incident highlights the urgent need for enhanced cybersecurity measures in election infrastructure and emphasizes the importance of protecting voter data from unauthorized access.

Ransomware Targeting Florida Department of Health

What happened: On July 3, 2024, ZeroFox observed an update on the RansomHub ransomware leak site targeting the Florida Department of Health, United States. ZeroFox has detected more than 100 ransomware and digital extortion victims in the government sector in the past year, of which close to 80 percent are in the U.S.-Canada region.



- **What this means:** The recent cyberattacks on the Florida Department of Health are in line with a growing trend of ransomware and digital extortion in the government sector that can have significant ripple effects. These attacks highlight the growing threat of cybercrime to national security and critical infrastructure. This could lead to heightened tensions between nations, particularly if state-sponsored actors are suspected of involvement. The breach of health department data could have implications for public health policy and trust in government health institutions.

| Exploit and Vulnerability Intelligence |

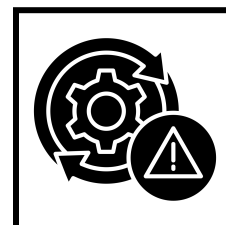
| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in cloud security, networking, technology, hardware and telecommunications, and industrial automation domains. Hackers are exploiting a critical vulnerability tracked as [CVE-2024-0769](#) that affects all D-Link DIR-859 WiFi routers to collect account information from the device, including passwords. Juniper has [released](#) patches for multiple vulnerabilities that affect Juniper Secure Analytics (JSA). Google [announced](#) a major Pixel security update, warning that one patched vulnerability, CVE-2024-32896, has been exploited. This zero-day bug is a high-severity elevation of privilege issue. Cybersecurity researchers have observed vulnerability [CVE-2024-6387](#) in Linux OpenSSH secure communications suite, which has the potential to expose systems to remote attackers who could cause a denial of service and possibly execute arbitrary code. Two vulnerabilities have been [detected](#) in Rockwell Automation PanelView Plus that have the potential to be weaponized by threat actors to execute arbitrary code and trigger a denial-of-service (DoS) condition.

Notable vulnerabilities:

[CVE-2024-2973](#)

What happened: Juniper Networks has urgently addressed a critical vulnerability (CVE-2024-2973) impacting its Session Smart Routers and Conductors. This **CRITICAL** flaw (CVSS score of 10.0) allows attackers in high-availability configurations to bypass authentication, gaining complete control over the devices.



- **What this means:** The vulnerability's severity, marked by its maximum CVSS score, necessitates immediate patching to prevent potential exploitation by malicious actors targeting network infrastructure vulnerabilities. If exploited, it enables attackers to bypass authentication in high-availability configurations. This allows them to gain unauthorized control over affected devices, potentially compromising network integrity and exposing sensitive data to malicious activities.
- **Affected products:**
 - Session Smart Router & Conductor:
 - All versions before 5.6.15
 - From 6.0 before 6.1.9-Its
 - From 6.2 before 6.2.5-sts
 - WAN Assurance Router:
 - 6.0 versions before 6.1.9-Its
 - 6.2 versions before 6.2.5-sts

CVE-2024-6387



What happened: A critical vulnerability (CVE-2024-6387) in OpenSSH's server (sshd) affecting Glibc-based Linux systems can expose Linux systems to remote attackers who could cause a denial of service and possibly execute arbitrary code. This vulnerability, dubbed as "RegreSSHion," is a reappearance of the already fixed CVE-2006-5051 bug. Approximately 700,000 internet-facing instances are potentially vulnerable, posing a significant risk of full system

compromise.

- **What this means:** Although this vulnerability was patched several years ago, changes or updates have inadvertently introduced this vulnerability. This [incident](#) highlights the crucial role of thorough regression testing to prevent the reintroduction of known vulnerabilities into the environment. According to the [advisory](#), exploiting CVE-2024-6387 can result in a full system compromise and takeover, allowing threat actors to execute arbitrary code with the highest privileges, bypass security mechanisms, steal data, and maintain persistent access to the system.
- **Affected products:** All versions of OpenSSH earlier than 4.4p1.

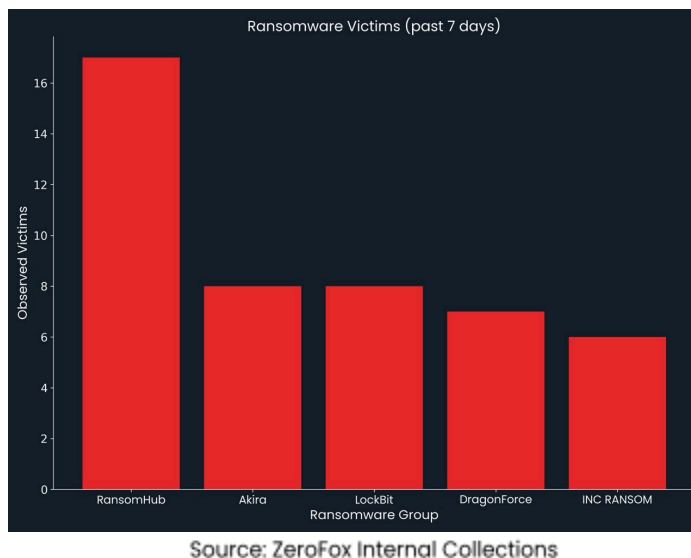
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: Infosys McCamish Says LockBit Stole Data of 6 Million People

What happened: Infosys McCamish (IMS) confirmed that the breach in November 2023 which LockBit had claimed, has actually affected more than 6 million people. According to the [official](#) notification, the impacted data included email address and password, Driver's License number or state ID number, financial account information, and more. In other news, [Patelco Credit Union](#) has recently experienced a ransomware attack leading to the shutdown of several banking systems for containment and remediation efforts. The

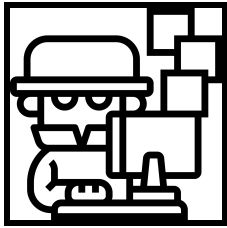
organization has enlisted a third-party cybersecurity firm to aid in the investigation and recovery. Meanwhile, ZeroFox has observed over 80 ransomware attacks in the past seven days, mostly in the manufacturing sector primarily conducted by the RansomHub ransomware group. Forty-five percent of these industries were from North America and Europe.



Source: ZeroFox Internal Collections

- **What this means:** The November cyberattack impacted many of IMS' clients, which include prominent financial institutions. The data compromised varies from one individual to another and includes personally identifiable information (PII) such as Social Security number (SSN), date of birth, medical treatment/record information, biometric data, email address and password, username and password, driver's License number or state ID number, financial account information, payment card information, passport number, tribal ID number, and U.S. military ID number. A ransomware attack on financial businesses such as banks, insurance companies, or accounting firms can paralyze critical systems and compromise sensitive data. This exposed personal data creates opportunities for identity theft and fraud, potentially causing financial harm to affected individuals. Moreover, the stolen data can be used for future cyberattacks, including targeted malware distribution, phishing and financial scams, exploiting the compromised information to gain unauthorized access to accounts or conduct further breaches.

Breach Intelligence: Global Data Breaches Paralyze Systems



What happened: This week, multiple data breaches across industries and countries occurred. South Africa saw a cyberattack paralyze its National Health Laboratory Service (NHLS). NHLS is still [recovering](#) from the attack that disrupted systems and deleted backups in late June 2024. The cyberattack blocked laboratories' information systems communicating with other medical databases resulting in delays in lab testing across public health facilities.

Healthcare fintech firm [HealthEquity](#) has reported a data breach resulting from a partner's compromised account, which was used to access the company's systems and steal protected health information. The breach was discovered when the company detected anomalous behavior from the partner's personal device and launched an investigation. This investigation revealed that hackers had compromised the partner's account, gaining unauthorized access to HealthEquity's systems and subsequently exfiltrating sensitive health data. [FIA](#) (Fédération Internationale de l'Automobile), the governing body for Formula 1 (F1), also reported this week that personal data was accessed by attackers who compromised multiple FIA email accounts through a phishing attack. The breach at FIA not only compromised the privacy of individuals associated with the organization but also highlighted the pervasive threat of phishing attacks in the digital age. Alabama's education superintendent [announced](#) that some data was breached during a hacking attempt at the Alabama State Department of Education. However, employee bank account and direct deposit information were not at risk, as this information is not stored on state servers. The attack was interrupted and stopped by IT professionals before the hackers could access all their targets. The hackers were believed to be attempting to encrypt data and extort a ransom for its release. A federal criminal investigation is ongoing, as the attack is suspected to involve foreign hackers. In the dark web, ZeroFox has observed threat actor "IntelBroker" breach [Cognizant](#) and the [Virginia Department of Elections](#). The well-regarded and established threat actor IntelBroker claimed to have leaked a database associated with Cognizant Insurance Model Office for OIPA on the predominantly English-language dark web forum, "BreachForums," as well as a database associated with the Virginia Department of Elections.

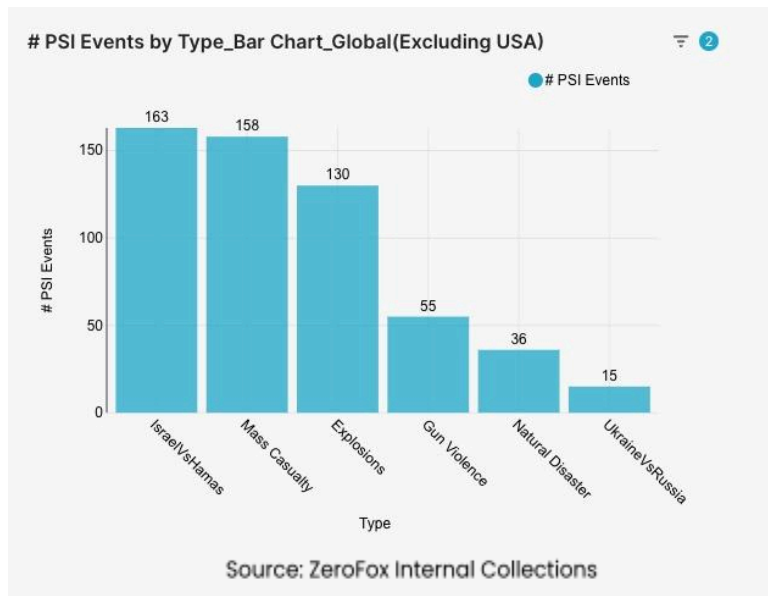
- **What this means:** The disruption in South Africa's national healthcare service could potentially worsen the existing stress on its healthcare systems, especially amid a monkeypox outbreak that has reportedly caused three deaths since May. Public hospitals and clinics are now facing increased pressure on their testing capabilities as systems need to be shut down to recover from the ransomware attack. This will further delay the processing of lab tests in public health facilities, compounding the challenges faced by the healthcare sector during this critical time. With the increasing frequency of ransomware attacks targeting healthcare organizations, these breaches highlight systemic vulnerabilities that could compromise patient privacy and care quality, potentially

endanger lives by impeding access to critical health information and causing systemic disruptions in medical services. With access to personal data from FIA email accounts, threat actors can potentially engage in identity theft, phishing campaigns targeting individuals associated with FI, and even attempting to exploit vulnerabilities within FI's digital infrastructure. This breach could further lead to compromised confidentiality of strategic information, sponsor relationships, and sensitive operational details. Prompt action by the FIA to mitigate unauthorized access demonstrates a proactive approach to data security while notifying relevant data protection regulators ensures transparency and compliance with legal obligations. Data breaches at educational institutions endanger student privacy and safety. The unauthorized access compromised sensitive customer data, including personally identifiable information (PII) such as emails, usernames, phone numbers, hashed passwords, authentication credentials, and more. This raises concerns about the potential misuse of this information by malicious actors, such as identity theft or phishing attacks targeting affected users. IntelBroker claimed that Cognizant suffered a data breach this month that exposed 40,000 users' databases and 12 million rows of line documents on their internal site. The leaked database reportedly includes policy number, role code, client name, company code, role sequence number, next bill extract date, role payment mode, and more. The threat actor claimed to have uploaded one of the Virginia Department of Elections databases for BreachForums users.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

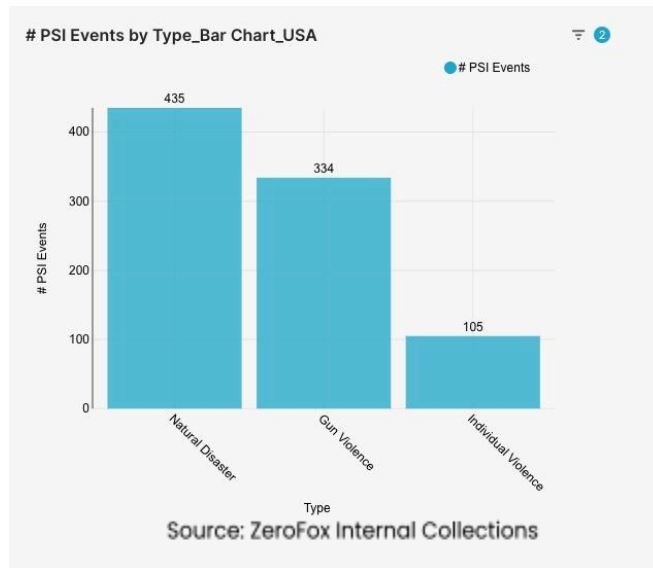


What happened: Excluding the United States, there was a 3 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon; approximately 82 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 12 percent from the previous week. Additionally, events related to Russia's war in Ukraine decreased by 21 percent. The top

three most-alerted subtypes were explosions, which saw a 17 percent increase from the previous week; gun violence, which increased by 12 percent; and natural disasters, which decreased by 14 percent.

- **What this means:** Both explosions as well as alerts related to the Israel-Hamas War increased quite significantly last week; coupled with Lebanon having one of the highest mass casualty rates, the numbers do correlate in relation to various events that happened this week. For instance, [Hezbollah](#) has said one of its senior commanders was killed in an Israeli air strike in southern Lebanon, with the Iran-backed armed group retaliating with a barrage of rockets against Israel. While Israel is redirecting its efforts more towards Lebanon, Palestine still has the highest number of casualties this week; the Israeli military has also ordered Palestinians to leave a wide sweep of land to the east of the southern Gaza city of Khan Younis. The total number of natural disasters globally did decrease this week, but those that did happen had a major impact, such as Hurricane [Beryl](#). Climate experts have forecasted this year's hurricane season to be "extremely active," predicting 17 to 25 named storms this season, with as many as 13 of those becoming hurricanes. While these events typically do not begin until August, this year has seen higher-than-normal ocean temperatures, raising the chance for earlier storms.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and individual violence. Natural disaster alerts typically involve fires and severe weather; gun violence alerts are instances in which there is a confirmed or likely confirmed victim; and individual violence refers to instances of stabbing. The top two states that had the most gun violence alerts were Illinois and California, which together made up over one-quarter of this week's nationwide total (28 percent). Gun violence across the United States overall decreased by 11 percent from

the week prior. The top two contributors to natural disaster alerts this week were California and New York, and natural disaster alerts across the country decreased by 1 percent. Individual violence alerts increased by 14 percent, and the top contributing states were California and New York as well.

- **What this means:** While these events may not have had an impact on crime numbers this week, it is important to note that the Supreme Court has recently made a wave of potentially controversial decisions, including deciding to immunize President Trump, the overturning of the Chevron decision, allowing continued access to mailed abortion pills, the rejection of a settlement involving Purdue Pharma, limiting of social media content censorship, etc. The number of hot-button issues, coupled with the looming presidential election this fall, may ruffle feathers amongst voters enough to spark demonstrations. Individual violence alerts, or stabbings, saw a decent increase this week, with cities such as New York contributing to these numbers; for instance, there was a fatal [stabbing](#) in the Bronx due to a road rage incident, as well as another in a [Brooklyn](#) apartment complex a few days prior. Natural disaster alerts did not see a significant change from last week, as [wildfires](#) continue to wreak havoc across the nation, with Alaska attempting to contain over 60.

Interested in more ZeroFox Threat Intelligence? ZeroFox produces 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%