



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 16, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. 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 (EST) on December 13, 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 – How Unrest in France and Europe Benefits its Adversaries	2
 Cyber and Dark Web Intelligence Key Findings	4
U.S. Treasury Issues Sanctions Against PRC Firm for Hacking Firewalls and Attempted Ransomware Attacks	4
Romania Elections Annulled; Integrity Compromised	4
Ukraine's Military Companies Baited with Doctored Emails	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-12286	8
CVE-2024-50623	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Targets Healthcare and Manufacturing, While Tactics Diversify	11
Data Breaches Weaponized by Different Threat Actors	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

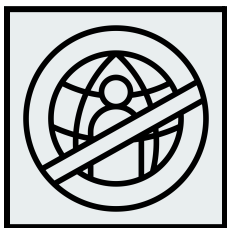
| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief – How Unrest in France and Europe Benefits its Adversaries

On December 4, 2024, France's Assemblée Nationale (the lower house of parliament) voted to remove Prime Minister Michel Barnier from office after just three months. Barnier's tenure was not only the shortest in the history of the French Fifth Republic but also came after France experienced its longest-ever period without a government. A PM replacement has been named, but the political dynamics that created this paralysis and dysfunction are not expected to change for the foreseeable future. Therefore, further short-lived governments are likely, leaving France poorly suited to address major domestic political issues.

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



U.S. Treasury Issues Sanctions Against PRC Firm for Hacking Firewalls and Attempted Ransomware Attacks

What happened: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned cybersecurity company Sichuan Silence and one of its employees, both based in the People's Republic of China (PRC), for their roles in the April 2020 compromise of tens of thousands of firewalls worldwide. Many of the victims were U.S. critical infrastructure companies. The sanctioned employee exploited a zero-day vulnerability in a firewall product to deploy malware on approximately 81,000 firewalls worldwide, stealing credentials and attempting to deploy the Ragnarok ransomware variant.

- **What this means:** The purpose of the exploit was to use the compromised firewalls to steal data, including usernames and passwords. Meanwhile, the Ragnarok ransomware variant disables anti-virus software and encrypts the computers on a victim's network if they attempt to remedy the compromise. Given that a considerable number of the targets were associated with U.S. critical infrastructure, the compromise had the potential to cause widespread damage and harm to human life. Meanwhile, Sichuan Silence supplied PRC intelligence and others with tools to exploit network routers, posing significant risks to U.S. national security, foreign policy, and the stability of critical infrastructure sectors. This incident is yet another example of China's sustained cyber espionage efforts against the United States specifically targeting critical infrastructure. Such operations—including the recent breach of U.S. telecommunication networks that impacted government officials—are likely indicative of broader strategic goals. China is likely striving to continue to gather intelligence, compromise security, and maintain persistent access to confidential networks in pursuit of potential geopolitical leverage.

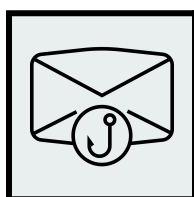


Romania Elections Annulled; Integrity Compromised

What happened: A Romanian constitutional court annulled the first round of votes in Romania's presidential election due to allegations of Russian interference, forcing a complete restart of the electoral process. This incident follows allegations that a pro-Russian TikTok influence campaign was actively promoting one of the candidates, who won the first round of the elections. Intelligence

revealed USD 381,000 in undeclared spending on unmarked political content and linked cyberattacks to state-sponsored actors targeting electoral data. Disinformation amplified pro-Russian narratives, leveraging influencers and bypassing platform controls. The European Union (EU) intervened via the Digital Services Act, compelling TikTok to preserve records and escalating monitoring during the electoral process.

- **What this means:** One of the main motives for targeting by Russia is likely Romania's current geopolitical stance, including its alignment with EU policies and its support for Ukraine in the ongoing Russia-Ukraine war. Moreover, Romania is a member of the North Atlantic Treaty Organization (NATO), an organization that has [condemned](#) Russia's attacks on Ukraine "in the strongest possible terms." Under these circumstances, Russia likely saw the possibility of influencing Romania's stance by pushing out disinformation campaigns supporting a seemingly pro-Russia candidate in the Romanian presidential elections. The development also comes just as Georgian Prime Minister Irakli Kobakhidze's decision to suspend talks about the country's EU membership has [met](#) with widespread public disapproval, large protests, and accusations of pro-Russian sentiments. Russia is likely trying to intervene where there is a political divide, as it [did](#) with the Georgian elections in October. (Georgia was a part of the Soviet Union until [1991](#), while Romania was a Soviet Union satellite until [1989](#).) Russia's unwarranted cyber presence in both countries is a likely indication of its pursuit of a political foothold in regions where it once had control. These operations deepen mistrust in democratic institutions, challenge NATO unity, and complicate the EU's collective security strategies. In Romania, the revelations could solidify EU regulatory momentum, but they also highlight the imminent threats of digital-era election manipulation.



Ukraine's Military Companies Baited with Doctored Emails

What happened: Ukraine's CERT-UA [confirmed](#) that hacking group "UNC4221" targeted defense and military companies with phishing emails from a Ukrainian business organization. The campaign aimed to compromise employees of Ukraine's defense contractors and forces. This group is suspected to be linked to Russia and has been observed targeting messaging services, such as Telegram and Whatsapp, and military systems like Kropyva.

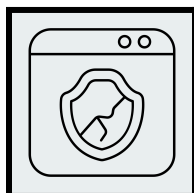
- **What this means:** Since the start of the Russia-Ukraine war, pro-Russia actors have been observed zeroing in on critical Ukrainian entities like defense organizations. In this case, UNC4221 targeted Ukraine's critical infrastructure with phishing emails disguised as invitations to a legitimate conference hosted by the Ukrainian League of Industrialists and

Entrepreneurs (ULIE). According to the CERT-UA, the cyberattacks aimed to obtain unauthorized remote access to computers of employees using specialized software tools—in particular, MESHAGENT and ULTRAVNC. The attack aimed to deceive recipients and compromise sensitive systems. What makes this phishing campaign particularly dangerous is that it exploits a legitimate event and trusted organization to appear credible, increasing the likelihood of employees opening the emails. By targeting defense and military companies, the attackers compromised sensitive systems aiming to steal critical data, likely impacting national security. Additionally, targeting military systems exposes sensitive information, disrupts operations, and damages critical infrastructure.

| **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 technology, software development, industrial control systems (ICS), and government services. The Update Backup Restore & Monitoring plugin for WordPress is [vulnerable](#) to Local File Inclusion in all versions up to, and including, 2.17.0 via the “filename” parameter of the “umbrella-restore” action. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. In the December 2024 [edition](#) of its Patch Tuesday release, Microsoft released security updates for 71 flaws, including one actively exploited zero-day vulnerability. Microsoft has listed all the vulnerabilities and their affected products in [this](#) advisory. Apple has recently [released](#) critical security updates for iOS 18.2 and macOS Sequoia 15.2 to address a wide range of vulnerabilities, including kernel exploits, WebKit flaws, and a severe bug in libexpat. In [CVE-2024-53247](#), a low-privileged user that does not hold the “admin” or “power” Splunk roles could perform a Remote Code Execution (RCE). This vulnerability is among the 10 high-severity vulnerabilities [addressed](#) in Atlassian’s December security bulletin. Recently, the Cybersecurity and Infrastructure Security Agency (CISA) [released](#) 10 ICS advisories providing timely information about current security issues, vulnerabilities, and exploits surrounding ICS. The successful exploitation of [CVE-2024-49849](#) could allow an attacker to execute arbitrary code within the affected devices. This vulnerability has been given a 7.8 CVS score.

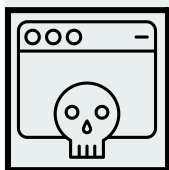


CRITICAL

CVE-2024-12286

What happened: The MOBATIME Network Master Clock DTS 4801, used globally in healthcare and transportation, has a critical vulnerability that allows remote attackers to exploit default credentials and gain full control over the system. CISA has released an ICS advisory on December 10, 2024, about this bug.

- **What this means:** Successful exploitation of this vulnerability could allow an attacker to take control of the operating system for this product. It is likely to be leveraged by threat actors to disrupt critical time-sensitive systems, potentially affecting services in healthcare and transportation where accurate time synchronization is essential for operations and safety.
- **Affected products:**
 - Network Master Clock – DTS 4801: FW Version 00020419.01.02020154

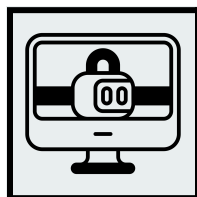
**HIGH****CVE-2024-50623**

What happened: CVE-2024-50623 is a zero-day flaw in Cleo's LexiCom, VLTransfer, and Harmony software where an unrestricted file upload and download could lead to RCE.

- **What this means:** Despite previous patches, attackers have found a way to exploit the software. This allows them to execute malicious code on vulnerable systems and potentially steal sensitive data. It is essential for organizations using Cleo software to apply the latest security patches immediately to mitigate the risk of attacks.
- **Affected products:**
 - Cleo Harmony versions before 5.8.0.21
 - VLTrader versions before 5.8.0.21
 - LexiCom versions before 5.8.0.21

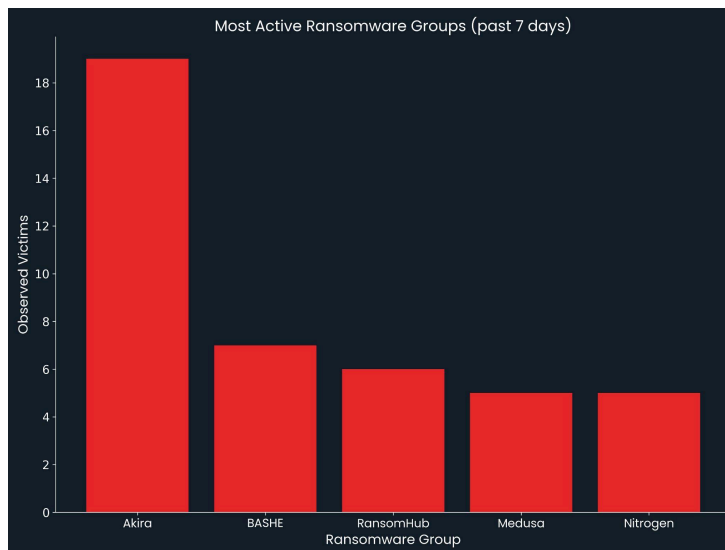
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Targets Healthcare and Manufacturing, While Tactics Diversify

What happened: In the past week, ZeroFox observed close to 100 ransomware attacks, most of which targeted entities in North America. The most affected sectors were manufacturing and healthcare, while the most active group was the Akira ransomware group. Artivion, a medical device manufacturer, confirmed a ransomware attack on November 21, 2024. The attackers reportedly encrypted certain files and stole sensitive data. The company has further stated that the incident has had no impact on “overall financial condition or results of operations.” According to the U.S. Securities and Exchange Commission (SEC), [Artivion](#) continues to provide its products and services to customers, but the incident has caused disruptions to some order and shipping processes, as well as to certain corporate operations, which have largely been mitigated. The Black Basta ransomware group has been observed diversifying its methodologies and has [adopted](#) new social-engineering tactics, including email bombing and impersonation, to target victims. It employs remote access tools like AnyDesk and malicious QR codes to deploy payloads such as Zbot and DarkGate for credential harvesting and further attacks. Recently, the Department of the Treasury’s OFAC [sanctioned](#) cybersecurity company Sichuan Silence and one of its employees, both based in the PRC, for compromising tens of thousands of firewalls worldwide in April 2020. Many of the victims were U.S. critical infrastructure companies.



Source: ZeroFox Internal Collections

- > **What this means:** Artivion has confirmed that the incident involved encryption of some files, which the threat actors are likely to use in further extortion attacks or to specifically target individuals whose information could be included in the encrypted files. The healthcare industry has large repositories of sensitive information that actors can leverage for financial gain, making it a lucrative target for ransomware attacks. ZeroFox has

detected around 480 ransomware and digital extortion victims in the healthcare sector in the past year, indicating that the sector has been facing recurring ransomware attacks. Threat actors can misuse the exposed data from healthcare systems to target customers in follow-on attacks like spear phishing, extortion scams, and blackmail. Such ransomware attacks also cause considerable financial losses to healthcare firms and have far-reaching repercussions. Healthcare organizations are often more likely to pay ransomware demands to protect sensitive patient data and to restore services immediately. Black Basta's new methods blend social engineering with custom malware and will likely facilitate environment, reconnaissance, credential theft, and VPN exploitation. The group disguises itself as support personnel or IT staff of the targeted organization and tricks users via email-bombing tactics to install legitimate remote access software that is later used to deliver additional payloads, including a custom credential harvesting program. Such evolutionary tactics are likely to complicate detection and response efforts. The sanctioned Sichuan Silence employee exploited a zero-day vulnerability in a firewall product to deploy malware on approximately 81,000 firewalls worldwide, stealing credentials and attempting to deploy the Ragnarok ransomware variant. Given that a considerable number of the compromised targets were associated with U.S. critical infrastructure, the compromise had the potential to cause widespread damage and harm to human life. Meanwhile, Sichuan Silence supplied PRC intelligence and others with tools to exploit network routers, posing significant risks to U.S. national security, foreign policy, and the stability of critical infrastructure sectors.



Data Breaches Weaponized by Different Threat Actors

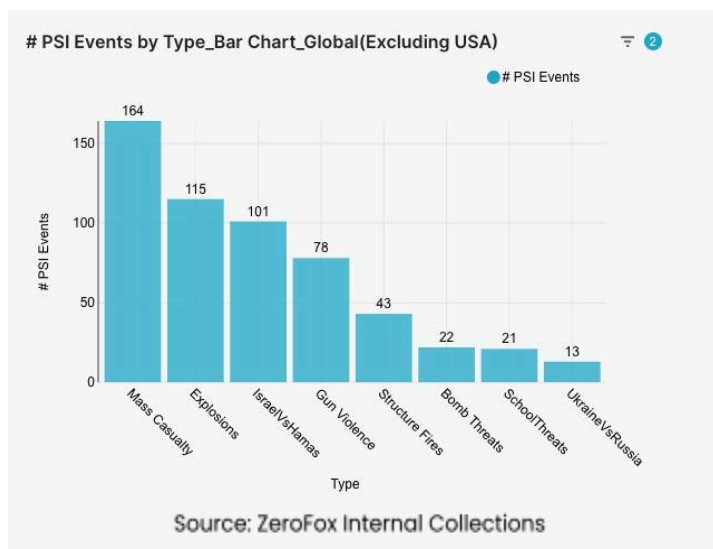
What happened: On December 10, 2024, threat actor "SSL_Dragon" [claimed](#) to have leaked a database associated with the Thailand division of Oppo, a China-based smartphone manufacturer, on the predominantly English-language dark web forum BreachForums. Hungary's Information Office (IH), Budapest's external intelligence agency, reportedly [spied](#) on European Anti-Fraud Office (OLAF) investigators by wiretapping phones, hacking laptops, and tailing them to access sensitive information. EagleMsgSpy, a new Android spyware reportedly linked to Chinese law enforcement, [steals](#) sensitive data like messages, call logs, recordings, and location from mobile devices. The U.S. Department of Justice (DOJ) [charged](#) 14 individuals and two firms employing North Korean IT workers who used fake identities to secure remote jobs, earning USD 88 million and obtaining sensitive data for the Democratic People's Republic of North Korea (DPRK or North Korea) over six years. Some of these "workers" extorted employers by threatening to release

sensitive data.

- **What this means:** SSL_Dragon alleges that the compromised data from Oppo includes over 22 million customer records and the personal details of staff from Oppo's HR system. If true, the breach likely impacts databases and internal systems, such as OppoHR, microservices, phone IMEI, big data, dealer partners, finance, warehouse, and iOppo platform details. Hungary's alleged cyber-espionage campaign is likely to undermine efforts to combat fraud and corruption, harming international financial interests. The stolen data may be weaponized for blackmail, extortion, or doxxing, endangering officials and compromising investigations. Meanwhile, EagleMsgSpy upgrades are likely suggestive of efforts to refine its capabilities for broader and more high-profile surveillance of targets, including individuals, organizations, and governments. Additionally, EagleMsgSpy poses a significant threat due to its extensive data-collection capabilities and stealthy operation. Its association with Chinese law enforcement agencies raises concerns about potential misuse and surveillance by the government of its people. The North Korean IT workers gained employment through fraud, exfiltrated sensitive information from U.S. companies, and siphoned money back to the DPRK, allegedly employing tactics to evade sanctions and detection. Such scams exploit businesses seeking to engage large numbers of contract workers quickly, cause damages beyond financial loss, expose sensitive corporate information, and enable weapons proliferation.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



Physical Security

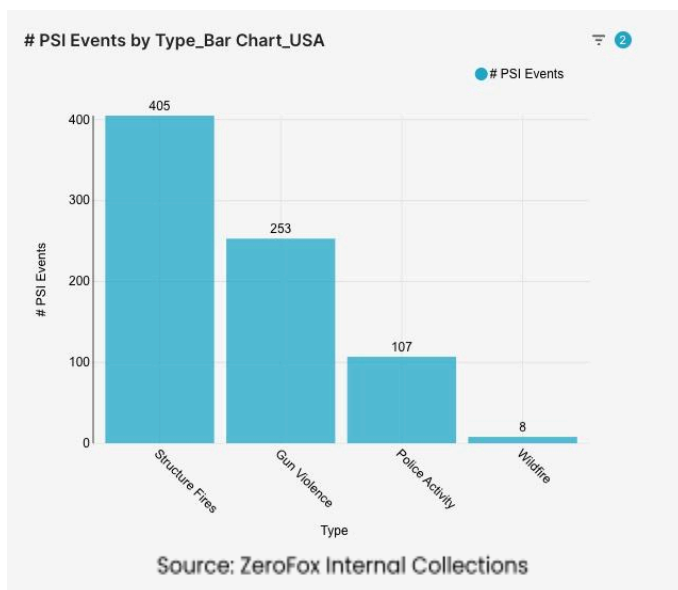
Intelligence: Global

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, Syria, and India, in that order.

Approximately 70 percent of these events were explosions, and the three aforementioned countries accounted for about 36 percent of all mass casualty alerts. General alerts related to

the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 25 percent from the previous week. Events related to Russia's war in Ukraine decreased by 7 percent. The top three most-alerted subtypes were explosions, which saw a 22 percent decrease from the previous week; gun violence, which decreased by only 1 percent; and structure fires, which increased by 19 percent. Global protest activity decreased by 30 percent. Notably, bomb threats increased by 100 percent, and India was the top contributor to this number.

- > **What this means:** This week saw the end of the Assad regime in Syria, as the Syrian rebels [seized](#) the capital of Damascus unopposed on Sunday, causing President Bashar al-Assad to flee to Russia. Additionally, Israel has since [attacked](#) Syria more than 400 times and, despite UN protests, has launched a military incursion into the buffer zone that has separated the two countries. Israeli President Benjamin Netanyahu has explained that the incursion was to prevent weapons from falling into the hands of military extremists. How Hayat Tahrir al-Sham (HTS) plans to govern Syria now is yet to be seen. In India, at least 40 [schools](#) received a bomb threat by email in Delhi on Monday. Upon investigation, however, no evidence of any explosives was found. Schools, railway stations, and airports in India have been subject to hundreds of bomb threats this year, which have later turned out to be hoaxes. Finally, structure fires saw a fairly significant increase this week, which is to be expected as the holiday season brings with it the use of flammable decor.



Physical Security

Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top three states that had the most gun

violence alerts were Illinois, California, and New York, which together made up 39 percent of this week's nationwide total. Gun violence across the United States overall decreased by 2 percent from the week prior. Police activity alerts increased by 32 percent, and the top contributing states were California and Texas. Structure fires increased by 9 percent, and the top two states for this subtype were Texas and New York. Notably, wildfires had a 700 percent increase this week, and the top contributing state was California.

- **What this means:** This week, the most drastic increase seen pertained to wildfires, which is due to the [Franklin](#) Fire spreading over Malibu and causing the evacuation of thousands of people. Since its formation on Dec. 9, the blaze has grown to 4,035 acres, and containment stands at only 7 percent currently. Structure fires also saw a fairly significant increase this week, which is to be expected as the holiday season brings with it the use of flammable decor. Illinois had the highest gun violence numbers this week; one person was killed and six others were injured in a shooting in [Cicero](#) over the weekend, which was the result of a car chase and subsequent crash. California was one of the top contributors to the police activity incident type this week, as well as to the Schoolthreats qualifier. Police activity involves law enforcement presence for generalized threats or for unknown reasons, which often happen at schools. For example, [Tamalpais](#) High School in Mill Valley, CA, had a shelter-in-place order on Tuesday, which turned out to be due to a bomb threat. No weapons or explosives were discovered, according to law enforcement officials.

| 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%