



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

May 27, 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 24, 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 – First Potential BreachForums Successor Announced	2
ZeroFox Intelligence Flash Report – GhostSec Announces Return to Hacktivism	2
ZeroFox Intelligence Brief – Competitive South African Elections Bring Physical and Cyber Risks	2
ZeroFox Intelligence Flash Report – NATO Data Leak Shared on Deep Web Forum	3
 Cyber Intelligence Key Findings	5
YouTube Becomes Latest Battlefield for Phishing, Deepfakes	5
SEC Adds New Incident Response Rules for Financial Sector	5
BreachForums Returns with New Onion Site	5
 Deep and Dark Web Intelligence Key Findings	8
Pro-Russia Threat Actor Claims Cyberattack on U.S. Medical Supply Store	8
Threat Actor Advertised Network Access Bundle to 56 European Companies	8
Pro-Russian Hacktivist Group Claims Attack Against NATO Allied Air Command	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-4835	11
CVE-2024-27130	11
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: First Nations Health Authority Hit by INC Ransomware	14
Breach Intelligence: Western Sydney University Data Breach Exposed Student Data	14
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	18
 Appendix A: Traffic Light Protocol for Information Dissemination	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – First Potential BreachForums Successor Announced

On May 16, threat actor “USDoD” announced on X (formerly, Twitter) their intent to launch a new, open-source data breach forum named Breach Nation. USDoD stated their intent for Breach Nation to serve as a successor to BreachForums, which was severely disrupted on May 15 by a law enforcement (LE) operation that seized the forum’s [.]st domain, a [.]onion domain, and a Telegram channel. There is a roughly even chance that Breach Nation will become a popular forum for threat actors seeking to discuss techniques, tactics, and procedures (TTPs) related to data breach attacks, publicize results, and sell stolen information. It is likely that, in the coming months, other BreachForums members, moderators, and staff will seek to capitalize upon its disruption by creating and advertising new forums.

ZeroFox Intelligence Flash Report – GhostSec Announces Return to Hacktivism

On May 15, 2024, the threat group “GhostSec” announced on its official Telegram channel its intention to abandon financially motivated cybercrime and resume hacktivism activities.

GhostSec is a member of the Five Families, a collective of hacking groups that has conducted financially, ideologically, and politically-motivated attacks against industries across the globe. GhostSec's renewed focus on hacktivism is very likely enabled by its financial success in leveraging GhostLocker ransomware-as-a-service (RaaS) in ransomware and digital extortion (R&DE) activity. In the short to medium term, GhostSec is likely to attempt disruptive and undermining attacks against the Israeli government, as well as other state institutions that are politically and ideologically misaligned with the group.

ZeroFox Intelligence Brief – Competitive South African Elections Bring Physical and Cyber Risks

Post-independence South Africa is set to have its most competitive elections ever on May 29, 2024. The African National Congress (ANC) Party, which has governed South Africa since the end of apartheid in 1994, is highly likely to lose its majority for the first time. Without a majority, the ANC will need to form a coalition to continue leading the government, which has made this campaign season especially contentious. Political parties hoping for the opportunity to make it into the government are likely escalating their campaign rhetoric online and threatening violence. After 30 years of controlling

the government virtually unchallenged, the ANC will have difficulty forming a coalition with any of the main opposition parties and is campaigning similarly to maintain as large a share of the vote as possible.

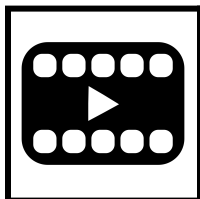
ZeroFox Intelligence Flash Report – NATO Data Leak Shared on Deep Web Forum

On May 19, 2024, threat actor “Sumo” announced a data leak pertaining to a NATO school’s e-learning platform on the Russian-speaking deep web forum Cronos. It is likely that the data breach originated from an SQL injection vulnerability that was privately advertised for sale on Telegram in January 2024. The vulnerability allegedly implicated an unknown NATO entity. It is very likely that the intended use of this data is social engineering and other fraudulent activity, with a likely chance it has already been leveraged in attacks by financially-motivated threat actors.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

[YouTube Becomes Latest Battlefield for Phishing, Deepfakes](#)



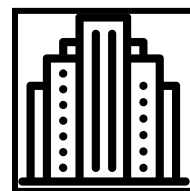
What happened: Cybersecurity researchers have flagged YouTube as a growing platform for malicious activities, with instances of phishing, malware distribution, and fraudulent investment schemes on the rise. Researchers have identified five potential ways in which threat actors can exploit YouTube: phishing emails targeting creators, compromised video descriptions with malicious links, channel hijacking for spreading threats such as cryptocurrency scams, leading viewers to fake websites and imitating reputable companies to distribute malware, and social engineering through video content to deceive users into downloading malicious software.

- **What this means:** The exploitation of YouTube by malicious actors poses a significant threat, as the platform's immense user base makes it a prime target for spreading scams and disinformation. Researchers have highlighted Lumma Stealer and RedLine for their association with these nefarious activities, indicating a concerning trend of exploitation. From compromising large accounts to utilizing deepfake technology, these tactics undermine trust and security on a widely used platform, potentially leading to financial losses and the spread of false information among users. European authorities have previously identified efforts by Russian-affiliated and other non-state actors to erode the European Union (EU)'s credibility via YouTube.

[SEC Adds New Incident Response Rules for Financial Sector](#)

What happened: The Securities and Exchange Commission (SEC) has announced new data breach reporting regulations for certain financial firms, updating Regulation S-P for the first time in 24 years.

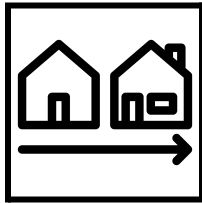
- **What this means:** These amendments aim to address the evolving risks posed by technology and data breaches in the financial sector, requiring institutions to develop incident response programs and notify affected individuals promptly. Financial organizations are required to notify individuals of data breaches within 30 days, providing details of the incident and the type of data compromised, as well as guidance on how affected customers can safeguard themselves.



[BreachForums Returns with New Onion Site](#)

What happened: A week after an LE operation took down BreachForums, one of the biggest deep and dark web (DDW) forums, ZeroFox observed an update on Telegram channel Jacuzzi 2.0

announcing a new onion site for BreachForums. Soon after the LE takedown, BreachForums' official



Telegram channel confirmed that the clearnet domain for BreachForums had been recovered. Initially, users were unable to create accounts, and old "personas" (credentials) were not being recognized. However, at the time of reporting, the site seems to be letting in users with their original credentials.

➤ **What this means:** The recent LE operation to take down BreachForums marks the second such attempt in two years. However, researchers have

reportedly noted that these sites often revive under different and new domains. With the announcement of the new onion site, BreachForums' administrators will likely try to secure it against future raids. Meanwhile, other underground players are attempting to launch rival platforms. On May 16, threat actor USDoD-TA [announced](#) on X the launch of a new project with the domains breachnation[.]io and databreached[.]io. The post claimed that the websites will go live in July this year. ZeroFox assesses that actors previously associated with BreachForums likely have copies of the data they leaked on the marketplace. They will likely release this data on other forums to gain initial traction, continuing to expose sensitive and confidential information to other threat actors.



ZEROFOX®

Weekly Intelligence Brief

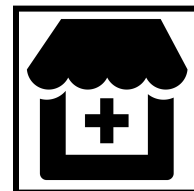
TLP:GREEN

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

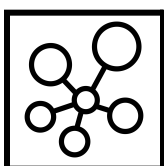
Pro-Russia Threat Actor Claims Cyberattack on U.S. Medical Supply Store

What happened: On May 22, 2024, pro-Russian hacktivist group “Just Evil” claimed on its Telegram channel to have conducted a cyberattack against the U.S.-based medical supply store CWI Medical. The attack encompassed the defacement of the store’s website, as well as the alleged theft of the personal, payment, and purchase history information of 105,000 customers dating back to 2013. The defaced website displays a photo of Russian President Vladimir Putin alongside the statements, “Your defense is as weak as your president’s health” and “With love from Russia.” The threat actor also includes a link to its Bitcoin wallet to which donations can be made.



- **What this means:** Just Evil, led by KillNet founder and former leader “KillMilk”, emerged on the pro-Russia hacktivist scene in January 2024. Since then, the group has claimed attacks on entities across the globe, including the United States, the United Kingdom (UK), Moldova, Lithuania, and Germany. The group has primarily directed attacks at government and political targets, as well as the aviation sector. KillMilk is likely seeking to reestablish their reputation within the pro-Russia hacktivist community after stepping down from KillNet leadership and will likely engage in additional high-profile activity in the near future. Additionally, the statement “Your defense is as weak as your president’s health” made on CWI Medical’s defaced website leverages a typical technique pro-Russia hacktivists use to push propaganda in attempts to sway global elections in favor of Russian interests. Here, the group is fanning ongoing political tensions among voters leading up to the 2024 U.S. presidential election, reiterating a prominent criticism by President Joe Biden’s domestic political opponents about his health and age.

Threat Actor Advertised Network Access Bundle to 56 European Companies

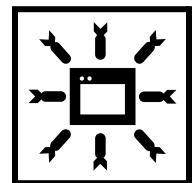


What happened: On May 21, 2024, moderately credible threat actor “Кот Ученый” (also known as “Cat_Scientist”) advertised a network access bundle on the predominantly Russian-language dark web forum xss. The actor claimed the bundle came with domain user and domain administrator rights to 56 unnamed, separate European companies. The European countries included were Austria, Belgium, France, Italy, Spain, Sweden, Switzerland, and the UK. According to Cat_Scientist, the companies generate between USD 5 million and USD 100 million in revenue. The actor charged USD 5,000 for the access bundle and provided their TOX ID for contact information.

- **What this means:** As the actor is moderately credible, it is likely that Cat_Scientist's claims and the network access bundle are legitimate. Other threat actors could purchase the access bundle to conduct a large number of attacks in quick succession. The bundle 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.

Pro-Russian Hacktivist Group Claims Attack Against NATO Allied Air Command

What happened: On May 22, 2024, pro-Russian threat actor group "Nightmare" claimed to have executed a successful distributed denial-of-service (DDoS) attack against North Atlantic Treaty Organization (NATO). According to a post on the group's Telegram channel, the attack was carried out against NATO Allied Air Command; the post included four check-host links in an attempt to verify the attack.



It is unclear what, if any, NATO infrastructure was rendered inoperable during the attack.

- **What this means:** Nightmare is a relatively new, pro-Russian hacktivist group that has been in operation since mid-March 2024. While the group has a limited attack history, its attacks are directed exclusively against NATO. The group's site overtly claims allegiance to the Russian Federation. While little is known about the group or its composition, separate DDW reporting indicates Nightmare has ties to other prominent, pro-Russian hacktivist threat actors such as NoName057(16). ZeroFox has observed an increase in attacks by hacktivist collectives whereby there is a network effect in the propaganda value when perpetrated by like-minded groups. We expect this trend to continue, as it is a low-risk/high-reward tactic to increase media attention for a cause.

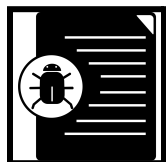
| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent entities in software solutions, network security, network-attached storage (NAS), and other industries. Google Chrome [addressed](#) another zero-day vulnerability in the Chrome browser being actively exploited in the wild. Major cloud platforms with Fluent Bit integrated are in danger of potential denial-of-service (DoS), remote code execution (RCE), and data breaches through the [CVE-2024-4323](#) vulnerability. VMware ESXi infrastructure is especially vulnerable (CVE-2024-22273) to ransomware attacks according to a [report](#). A cross-site scripting (XSS) condition exists within certain GitLab [versions](#), which can allow attackers to craft a malicious page to exfiltrate sensitive user information. Ivanti recently [released](#) fixes for several critical security vulnerabilities in Endpoint Manager (EPM). U.S. Cybersecurity and Infrastructure Security Agency (CISA) [added](#) CVE-2023-43208, a NextGen Healthcare Mirth Connect flaw, to its Known Exploited Vulnerabilities (KEV) catalog. Rockwell Automations advised its clients to take mitigation measures against [several flaws](#) impacting Rockwell industrial control system (ICS) devices.

Notable vulnerabilities:

[CVE-2024-4835](#)



What happened: An XSS condition exists in VS code editor (Web IDE). By leveraging this condition, an attacker can craft a malicious page to exfiltrate sensitive user information. GitLab has released versions 17.0.1, 16.11.3, and 16.10.6 for GitLab Community Edition (CE) and Enterprise Edition (EE) to patch this bug.

➤ **What this means:** This **HIGH** severity vulnerability with a CVSS score of 8.0 could allow attackers to take over user accounts in XSS attacks. Compromised GitLab accounts pose risks such as supply chain attacks, whereby attackers can introduce malicious code potentially compromising an organization's repositories.

Affected products:

- GitLab versions 15.11 before 16.10.6
- 16.11 before 16.11.3
- 17.0 before 17.0.1.

[CVE-2024-27130](#)

What happened: A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute code via a network.



➤ **What this means:** This **HIGH** severity vulnerability with a CVSS score of 7.2 is unpatched at the time of writing and can potentially compromise Network Attached Storage (NAS) devices.

Affected products:

- QTS 5.1.7.2770 build 20240520 and later
- QuTS hero h5.1.7.2770 build 20240520 and later



ZEROFOX®

Weekly Intelligence Brief

TLP:GREEN

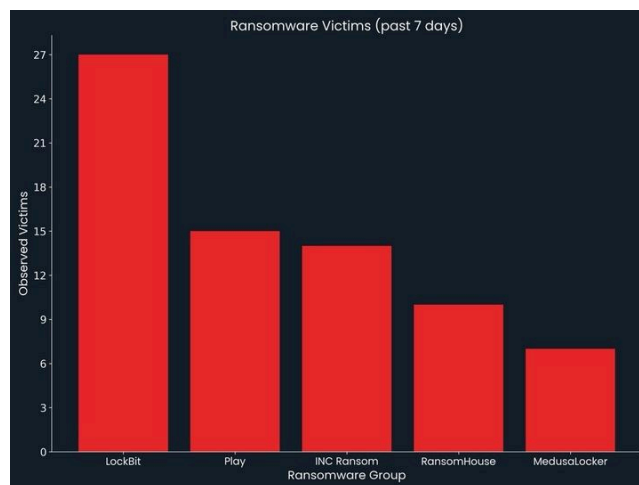
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: First Nations Health Authority Hit by INC Ransomware

Ransomware

What happened: In the past week, ZeroFox has detected over 100 ransomware attacks, most of which have targeted the manufacturing sector. LockBit conducted the majority of the attacks. About 60 percent of the ransomware attacks were detected in North America. Other active actors include the Play and INC ransomware groups. First Nations Health Authority (FNHA) intercepted unauthorized access to its corporate network following a cybersecurity incident detected on May 13; ZeroFox has observed INC ransomware posting screenshots as evidence on its leak site.



Source: ZeroFox Internal Collections

- **What this means:** FNHA's prompt response thwarted server encryption, but the exposure of employee information and personal data highlights the persistent threat to healthcare data security. The stolen data further poses the risk of identity theft and targeted cyberattacks against both employees and affected individuals. The incident reflects the concerning trend of healthcare organizations being recurrent targets of cyber threats. Meanwhile, LockBit seems to be increasing its attack tempo after LE operations took its leak site down.

Breach Intelligence: Western Sydney University Data Breach Exposed Student Data

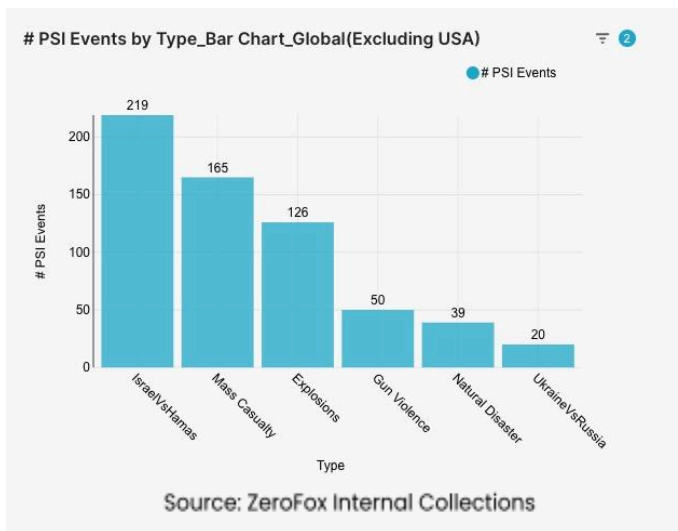


What happened: Threat actors breached Western Sydney University's Microsoft 365 and Sharepoint environment, potentially utilizing the Solar Car Laboratory infrastructure. The breach exposed data for approximately 7,500 individuals.

- **What this means:** The breach compromised sensitive information for thousands of students and staff, necessitating personalized notices and involving authorities like the NSW Police and cybersecurity firms for investigation. This intrusion was discovered in January 2024. Ongoing investigations highlight the potential for further data exposure. Threat actors could exploit stolen data for identity theft, financial fraud, or targeted phishing attacks, necessitating continuous vigilance and response efforts from

affected individuals and institutions. The university has deemed post-breach security measures sufficient to prevent future incidents and has secured a court injunction to halt data dissemination.

| Physical and Geopolitical Intelligence |



Physical and Geopolitical Intelligence Key Findings

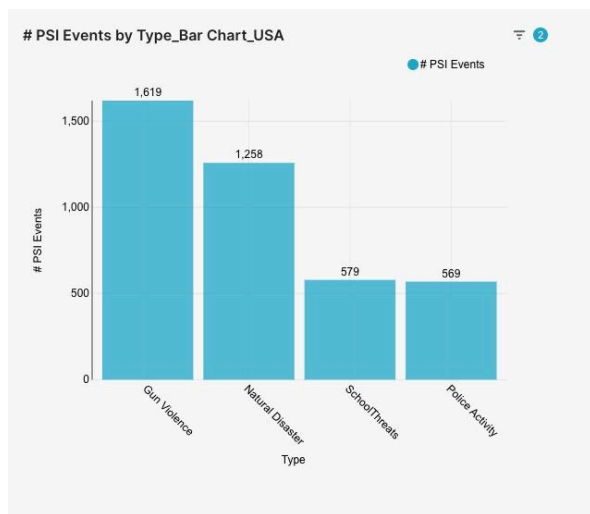
Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 16 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and

Ukraine (in that order); approximately 76 percent of these events were explosions. General alerts related to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries) decreased by 4 percent from the previous week; notably, Palestine and Israel accounted for almost half of all international explosions alerted (45 percent). Additionally, events related to Russia's war in Ukraine decreased by 33 percent. The top three most-alerted subtypes were explosions, which saw a 6 percent decrease from the previous week; gun violence, which decreased by 38 percent; and natural disasters, which decreased by 38 percent as well.

- **What this means:** This week saw a decrease across the board in mass casualty instances, explosions, and events related to the Israel-Hamas conflict; as Palestine and Israel accounted for almost half of all explosions, it makes sense that these figures would correlate. The reason for the decrease may be due to President Benjamin Netanyahu declaring that Israel is ready to discuss new ceasefire talks; additionally, while the offensive on Rafah continues on, U.S. President Joe Biden has remarked that the [operation](#) has been more targeted and limited and has not involved major military operations. Additionally, Iranian president Ebrahim Raisi was killed in a helicopter accident over the weekend; as the Iranian government supports both Hamas and Hezbollah, this could have led to a pause in operations as well. Natural disasters also saw a significant decrease; any of these events have been caused by climate changes related to El Niño, which has notably and recently [weakened](#), whereas La Niña is not expected to start until June. In short, the climate is in a transitional phase, which may explain the recent decrease in natural disasters.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disaster, and police activity. 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 23 percent of this week's nationwide total. Gun violence across the United States increased by 23 percent from the week prior. The top two contributors to natural disaster alerts this week were Florida and Texas, and natural disaster alerts across the country increased by 12 percent. The police

activity subtype is used to alert evacuations, lockdowns, and heavy police presence for which the reason is not yet known at the time of alerting; California and Florida were the top two contributing states this week for this subtype, and police activity across the country as a whole increased by 6 percent. Alerts related to schools, excluding protests, decreased by 9 percent.

- **What this means:** Both gun violence and police activity saw an increase this week, and (similar to previous weeks) California and Illinois were top contributors to the overall number of alerts. This past week saw record-high [temperatures](#) in several areas across the country; as mentioned in previous ZeroFox intelligence briefs, high temperatures often [correlate](#) with an increase in shootings. Additionally, natural disasters increased in the past week, as hotter temperatures often spark wildfires and other climate changes. There has also been heightened tornado activity this week; for example, authorities in [Iowa](#) have confirmed that four people were killed and at least 35 were injured in a twister. Finally, instances related to schools decreased again this week, as noted in the previous week. As more schools begin their summer break, there may be an even further decline of this number.

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%