



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

May 24, 2025

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 6:00 AM (EDT) on May 22 2025**; 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: Actor Seemingly Claims Responsibility for Recent Breaches	2
ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 10	2
 Cyber and Dark Web Intelligence Key Findings	4
Flaws in Webmail Products Exploited in Cyber Espionage Campaign	4
U.S. Justice Department Seizes Domains Behind Major Information–Stealing Malware Operation	5
Peter Green Chilled Joins Growing List of UK Retail Cyber Victims	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2025-46724	7
CVE-2025-47949	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Groups and their Trends	10
Major Data Breaches Observed this Week	13
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 Flash Report: Actor Seemingly Claims Responsibility for Recent Breaches

A prominent and well-regarded threat actor known as “Machine1337” (who is also known as “EnergyWeaponUser”) has claimed responsibility for at least seven recent cyberattacks within both the primarily Russian-speaking dark web forum xss and the actor’s Telegram channel. Posts by the actor alluded to unspecified data allegedly stolen from Apple Inc., Steam, Huawei, and Snapchat. While data samples were seemingly made available, forum users claim that they are not accessible. Separately, on May 15, 2025, the U.S.-based cryptocurrency exchange platform Coinbase released a statement acknowledging a recent breach that resulted in stolen customer data. On May 15, 2025, ZeroFox observed that Machine1337 posted a message on their Telegram channel that stated “CoinBase: Coming soon.” While this does not indicate Machine1337 is directly involved in the Coinbase compromise, it does suggest a possible connection between the actor and this recent breach incident, which has yet to be officially claimed by any threat actor or group.

ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 10

The Underground Economist is an intelligence-focused series illuminating dark web findings from our ZeroFox Dark Ops intelligence team.

Cyber and Dark Web Intelligence

| Cyber and Dark Web Intelligence Key Findings



Flaws in Webmail Products Exploited in Cyber Espionage Campaign

What we know:

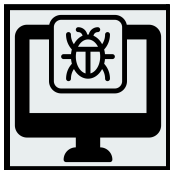
- State-sponsored hackers are running a cyber espionage campaign dubbed "RoundPress," exploiting zero-day vulnerabilities in multiple webmail products like Zimbra, RoundCube, Horde, and MDAemon to target high-value government entities.
- Russian state-sponsored threat group "APT28" (also known as "Fancy Bear" or "Sednit") is suspected to be behind the campaign.
- Government, military units, and critical infrastructure in Ukraine, Romania, Greece, Serbia, Ecuador, Bulgaria, and Cameroon have been targeted since at least 2023.

Background:

- The attack chain starts with a spear phishing email, often referencing political or current news. The HTML email body carries a malicious JavaScript payload designed to exploit a cross-site scripting (XSS) vulnerability in the webmail browser page.
- The target is only required to view the email; no other interaction, clicks, or redirections are needed to execute the payload.
- The attack leads to theft of credentials associated with the email account, email content, contacts, webmail settings, two-factor authentication (2FA), and login history.

What is next:

- The highly targeted nature of this spear phishing campaign likely indicates that hackers have access to the email addresses of victims. Hackers are likely to target government employees whose email addresses are available publicly or are obtained through compromise of vendors or third-party websites along the supply chain.
- Compromise of a single high-value email account is likely to give the attacker access to the email addresses of other high-value targets and also helps attackers move laterally across an organization or network.
- There is a roughly even chance that the attackers maintain persistent access to email conversations and file-sharing at the highest levels of government and military targets through compromised accounts, even if the malicious payload does not have persistence mechanisms.



U.S. Justice Department Seizes Domains Behind Major Information–Stealing Malware Operation

What we know:

- The Justice Department has unsealed two warrants to seize five internet domains used in operations associated with the LummaC2 information–stealing malware service. Meanwhile, Microsoft's Digital Crimes Unit (DCU) [filed a legal action against Lumma Stealer](#) after finding 400,000 Windows computers infected by the malware globally.

Background:

- Malware like LummaC2 is used to steal sensitive data, including login credentials, from victims to enable cybercrimes. The seized websites were used by LummaC2's operators to distribute the malware to affiliates and other cybercriminals.

Analyst note:

- Cybercriminals used LummaC2 to harvest victims' personal data, likely for sale on dark web forums or for financial fraud and identity theft. Shutting down these websites likely disrupted the distribution network of the malware service, preventing widespread exploitation of stolen information.



Peter Green Chilled Joins Growing List of UK Retail Cyber Victims

What we know:

- Peter Green Chilled, a major UK food distributor, has been hit by a ransomware attack, disrupting deliveries to supermarkets and small businesses.

Background:

- UK retail giants continue to face a wave of cyberattacks, with Peter Green Chilled the latest victim following recent incidents at Marks & Spencer and Co-op.

Analyst note:

- Retail companies like Peter Green Chilled are lucrative targets since they are connected to other major retailers, which could give threat actors access to a large customer database consisting of sensitive data like payment information, addresses, and passwords.

| **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, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added a total of [six vulnerabilities](#) to its Known Exploited Vulnerabilities (KEV) catalog and has released [13 Industrial Control Systems \(ICS\) vulnerabilities](#). Intel issued [microcode patches for several vulnerabilities](#) (CVE-2024-45332, CVE-2024-28956, and CVE-2025-24495), together known as “Spectre,” which can leak sensitive information from memory from its modern CPUs. CVE-2025-48017 is caused by improper pathname validation in the [Circuit Provisioning and File Import applications](#), allowing unauthorized file modification and upload. These newly patched [zero-day vulnerabilities](#) (CVE-2025-4918 and CVE-2025-4919) affect the Mozilla Firefox web browser. A [flaw in OpenPGP.js](#) enables attackers to spoof signed and encrypted messages. An authentication [vulnerability in AutomationDirect’s Modbus \(MB\) Gateway devices](#) enables possible remote attacks and configuration changes directly through the internet. An inference and serving engine for large language models (LLMs) known as [vLLM has a flaw \(CVE-2025-47277\) in versions 0.6.5 to 0.8.4](#) impacting only environments using the “PyNcclPipe” KV cache transfer integration with the V0 engine.



CRITICAL

CVE-2025-46724

What happened: Langroid, a Python framework for building LLM-powered applications, previously used “pandas eval()” in its “TableChatAgent” without sanitizing input. This left applications vulnerable to code injection when handling untrusted user input. The flaw was fixed in version 0.53.15 by adding input sanitization and warnings in the documentation.

- **What this means:** The framework previously allowed unsafe code execution through user inputs during data processing, which could compromise the system or expose sensitive data. Users are urged to update to the patched version to mitigate the risk associated with the flaw.
- **Affected products:**
 - Versions prior to 0.53.15

**CRITICAL****CVE-2025-47949**

What happened: This critical authentication bypass vulnerability in Security Assertion Markup Language (SAML) implementations enables attackers to impersonate administrative users by injecting unsigned malicious assertions into otherwise legitimately signed SAML responses.

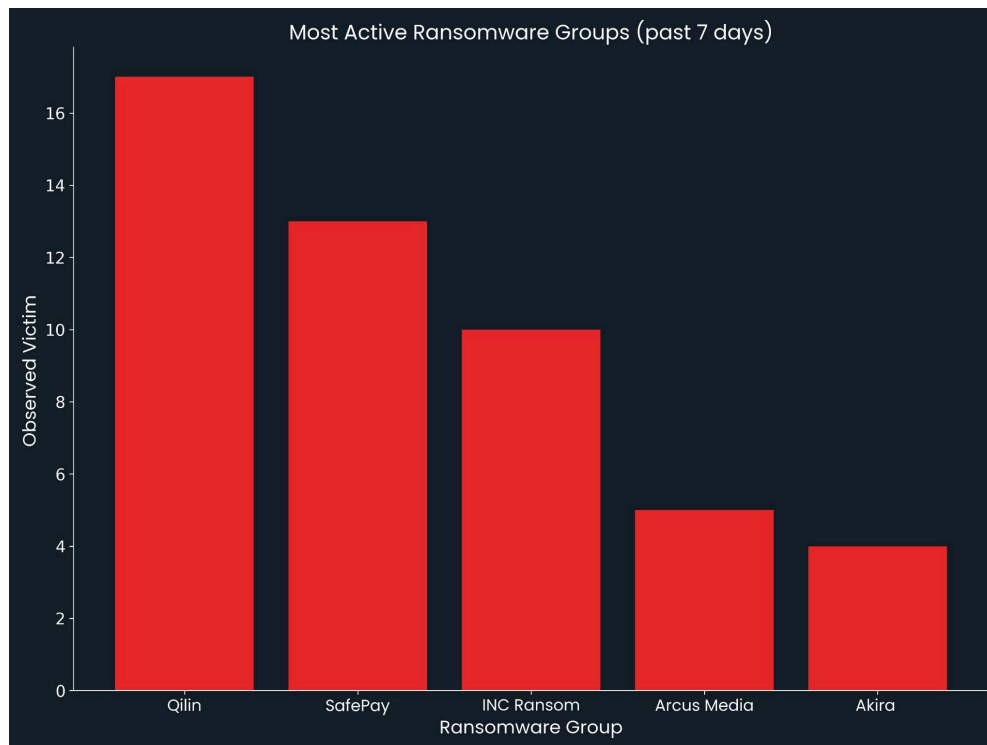
- **What this means:** The flaw enables attackers to bypass authentication and gain unauthorized access to sensitive systems. By injecting malicious assertions into valid SAML responses, attackers can impersonate high-privilege users, including administrators—likely leading to unauthorized access to sensitive systems, data breaches, and complete compromise of affected applications.
- **Affected products:**
 - All versions of Node.js library Samlify before 2.10.0

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

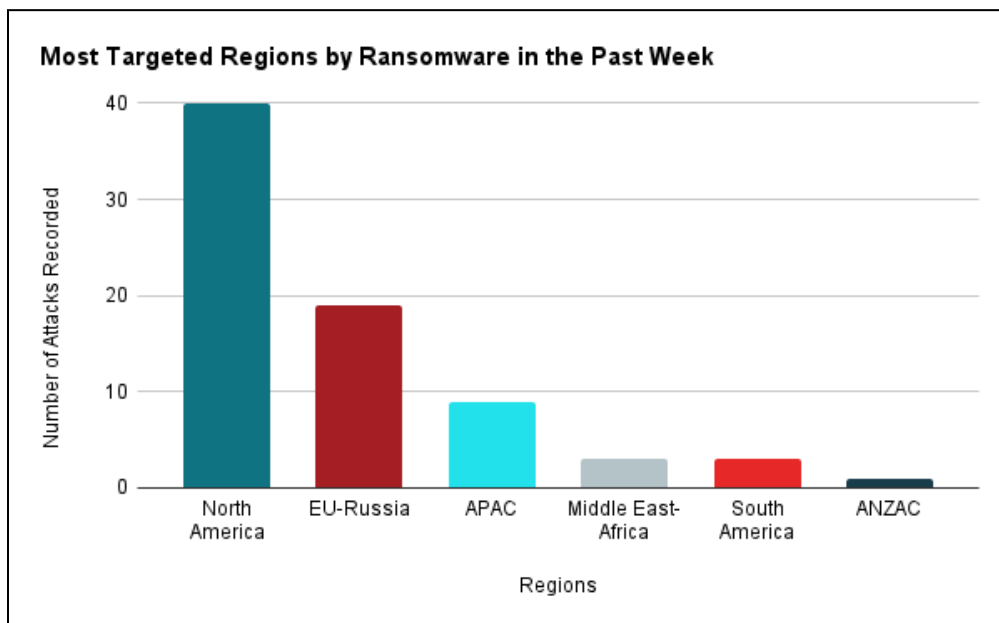


Ransomware Groups and their Trends



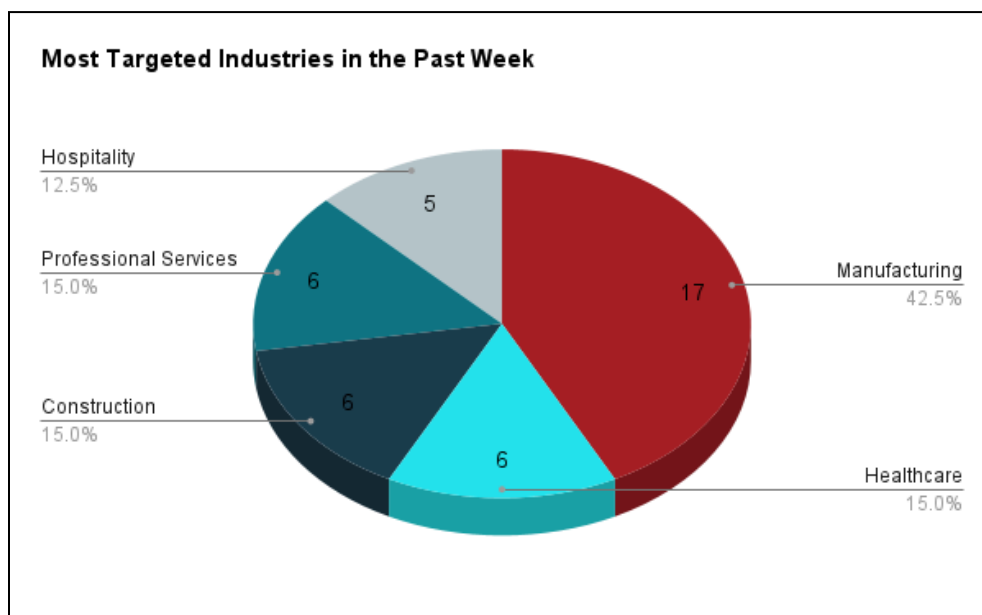
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Safepay, INC Ransom, Arcus Media, and Akira were the most active ransomware groups. ZeroFox observed at least 71 ransomware victims disclosed, most of which are located in North America. Qilin and SafePay accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past seven days, ZeroFox has observed that North America was the most targeted region by ransomware attacks, followed by EU-Russia.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing, healthcare, construction, professional services, and hospitality were the industries most targeted by ransomware attacks. The graph above shows the number of ransomware attacks suffered by each of these industries in the last week.



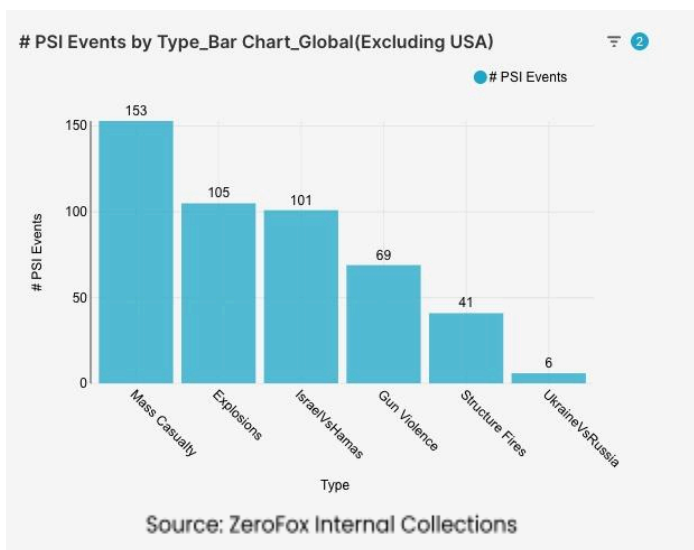
Major Data Breaches Observed this Week

Targeted Entity	Serviceaide	Legal Aid Agency	Coinbase
Impacted Entities/Infrastructure	483,000 Catholic Health patients	The agency's online digital services	Customer and corporate data affecting 69,461 individuals
Compromised Data Fields	Dates of birth, Social Security numbers, medical record numbers, health insurance information, treatment information, prescriptions, clinical information, usernames, passwords, and more	Legal aid applicants' personal data, including contact details, dates of birth, national ID numbers, criminal history, employment status, and financial data	Names, dates of birth, last four digits of Social Security numbers, masked bank account numbers, phone numbers, and more
Suspected Threat Actor	Undisclosed	Undisclosed	Possible insider attack
Country/Region	United States	United Kingdom	United States
Industry	Healthcare	Government	Finance
Possible Repercussions	This exposed information is likely to lead to other data breaches in supply chain attacks that involve third parties, networks, and accounts.	Threat actors are likely to abuse this data to conduct scams, exploit victims financially, and impersonate victims in identity fraud campaigns.	Threat actors could use this information to access victim accounts, transfer funds, and incriminate victims in financial fraud.

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical Security Intelligence: Global

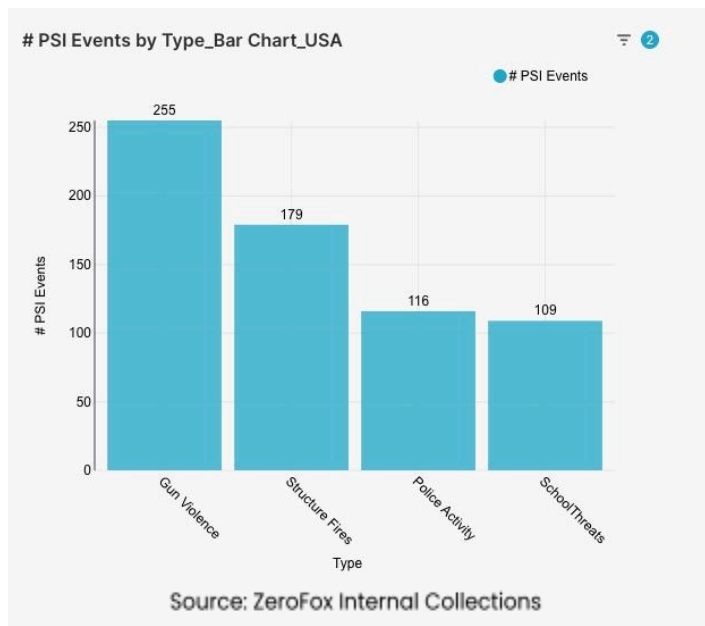


What happened: Excluding the United States, there was a 27 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, India, and Pakistan in that order. Approximately 69 percent of these events were explosions, and the three aforementioned countries accounted for about 39 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 8 percent from

the previous week. Events related to Russia's war in Ukraine increased by 200 percent. The top three most-alerted subtypes were explosions, which saw a 30 percent decrease from the previous week; gun violence, which decreased by 15 percent; and structure fires, which decreased by 13 percent. Global protest activity decreased by 8 percent.

- **What this means:** Over the past week, the intensity of attacks between Ukraine and Russia has escalated significantly. Russian forces have intensified their [assaults](#) near the strategically important town of Chasiv Yar, and Ukraine also unleashed waves of aerial and naval drones, striking Russian refineries, oil depots, airfields and ports. If Chasiv Yar falls, it would put Russia in a position to attack the last remaining free cities in Donetsk – Kostiantynivka, Druzhivka, Sloviansk, and Kramatorsk – which form Ukraine's main line of defence in the region. India and Pakistan have experienced continued tensions as well, primarily due to military confrontations and diplomatic maneuvers; however, while both India and Pakistan have claimed victory following a fragile [ceasefire](#) agreement, some experts fear that a return to hostilities is almost inevitable. In Palestine, which had the highest number of mass casualty alerts this week, 50 Palestinians were killed or remain missing after an Israeli [air strike](#) on a residential building in northern Gaza on May 23rd. Since March 18th, when Israel broke the ceasefire, at least 3,673 people have been killed, and the situation has remained volatile since.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, 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 two states that had the most gun violence alerts were Illinois and New York, which together made up 19 percent of this week's nationwide total. Gun violence

across the United States overall increased by 7 percent from the week prior. Police activity alerts increased by 14 percent, and the top contributing states were California and Texas. Structure fires increased by 5 percent, and the top two states for this subtype were California and New York. Notably, school-related threats (excluding protest activity) increased by 15 percent nationwide.

- **What this means:** Gun violence saw an increase this week, particularly in New York and Illinois. For instance, in New York City, a 7-year-old boy was [shot](#) in the Bronx on May 18th, marking the third minor to be wounded or killed in the borough within just a few days. This underscores the persistent issue of gun violence in urban areas. Structure fire alerts increased somewhat as well. California, in particular, is bracing for a challenging fire season due to a combination of above-average vegetation growth, drought conditions, and forecasted hot, dry weather. As for police activity, more outdoor activities and events typically correlate with heightened need for police presence, which is expected to rise even more as Memorial Day weekend approaches; alongside the celebrations, law enforcement agencies often observe an uptick in certain types of [criminal activity](#) during this time. Finally, school graduations are in session this month, which draw large crowds - and, inevitably, [security threats](#), which may explain the rise in school-related alerts this week. These are also expected to rise before summer break begins in June.

| 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%