ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 6, Issue 2

B-2026-01-15b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

January 15, 2026

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 7:00 AM (EST) on January 15, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

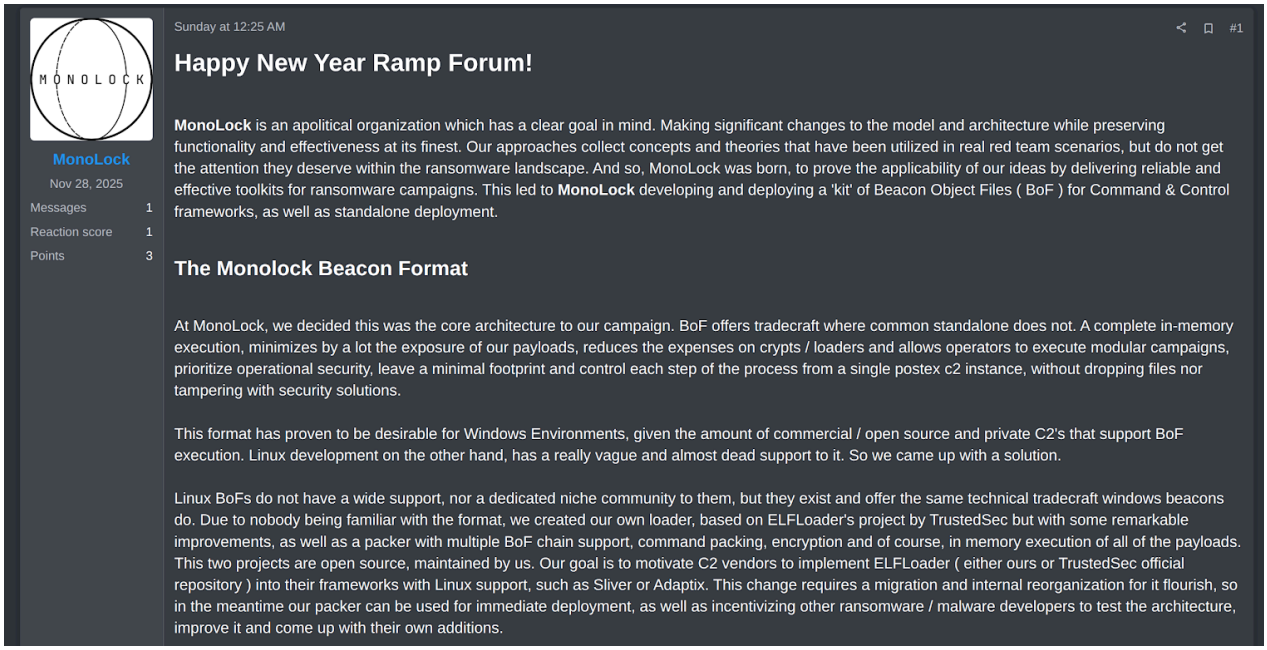
Brief The Underground Economist: Volume 6, Issue 2

New Beacon-Based RaaS for Sale on RAMP

On January 11, 2026, an actor known as "MonoLock" advertised a new beacon-based ransomware-as-a-service (RaaS) offering on the RAMP forum. According to the post, MonoLock is an apolitical organization with a primary objective of optimizing and operationalizing ransomware services. This includes continuous changes to the architecture of its offensive arsenal to improve performance.

- The beacon-based aspect of this RaaS likely refers to the use of beaconing mechanisms that are typically associated with the legitimate penetration testing tool Cobalt Strike.
- MonoLock likely functions by using the Beacon payload from Cobalt Strike as a key component of delivery in order to bypass malware detection efforts.
- MonoLock likely relies on the development and deployment of Beacon Object Files (BoFs) for their command-and-control frameworks. At present, MonoLock claims to support Windows, Linux, and VMware 64-bit systems.

The "MonoLock Zero Panel Theory" described in the post is presented as an innovative approach. According to MonoLock, their RaaS architecture does not support public extortion sites; the actor instead relies on communicating with victims via private channels in order to protect the public reputations of targeted companies.



Original MonoLock post on RAMP
Source: ZeroFox Intelligence

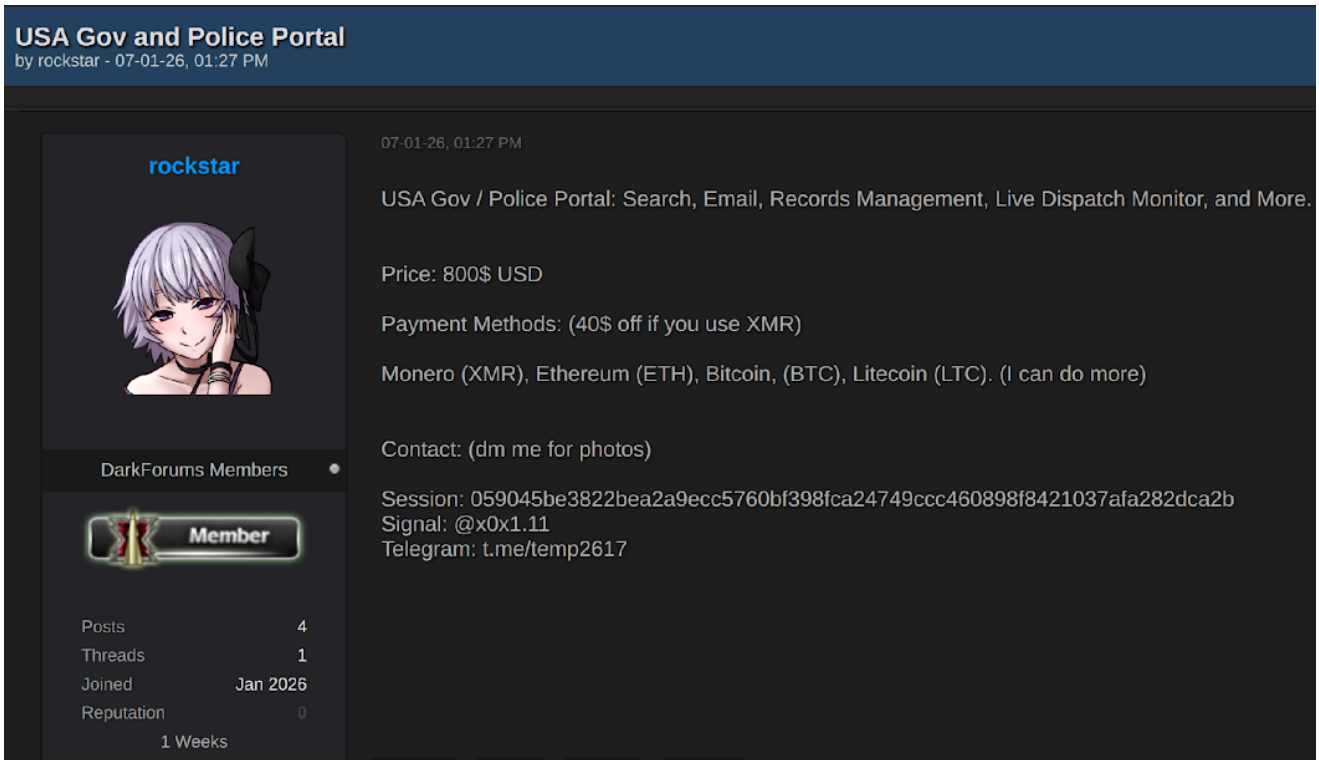
MonoLock is an untested poster on RAMP with a low reputation score. They joined RAMP in November 2025, and this appears to be the actor's first post. For these reasons, ZeroFox cannot determine MonoLock's credibility. However, if the service offered is legitimate, it would present a novel threat to potential victims, as it represents a RaaS with likely sophisticated detection avoidance.

Access to an Unnamed U.S. Government and Police Portal Advertised on Dark Web Forum

On January 7, 2026, newly registered and unvetted actor "rockstar" advertised the sale of unauthorized access to an unnamed U.S. government and police portal on the dark web forum DarkForums. According to rockstar, the buyer will receive access that includes a search portal, emails, management records, and a live dispatch monitor.

- The actor has indicated the price for the access is USD 800, which can be paid via various cryptocurrencies, but noted a USD 40 discount would be applied if the buyer uses Monero (XMR). ZeroFox assesses the price for such sensitive access is relatively low.

- Rockstar joined DarkForums in January 2026 and has not yet garnered any reputation; therefore, ZeroFox cannot judge the actor's credibility at this time.



rockstar's post on DarkForum
Source: ZeroFox Intelligence

Rockstar provided no samples or proof of the access in the post but stated that interested buyers could contact them for photos of the alleged access via Session, Signal, or Telegram; the actor also did not specify the type of access being offered. However, ZeroFox assesses that it is likely the actor possesses user credentials with medium-level privileges.

- Typically, if threat actors possess admin credentials, it is usually specified in the post and reflected in the price.

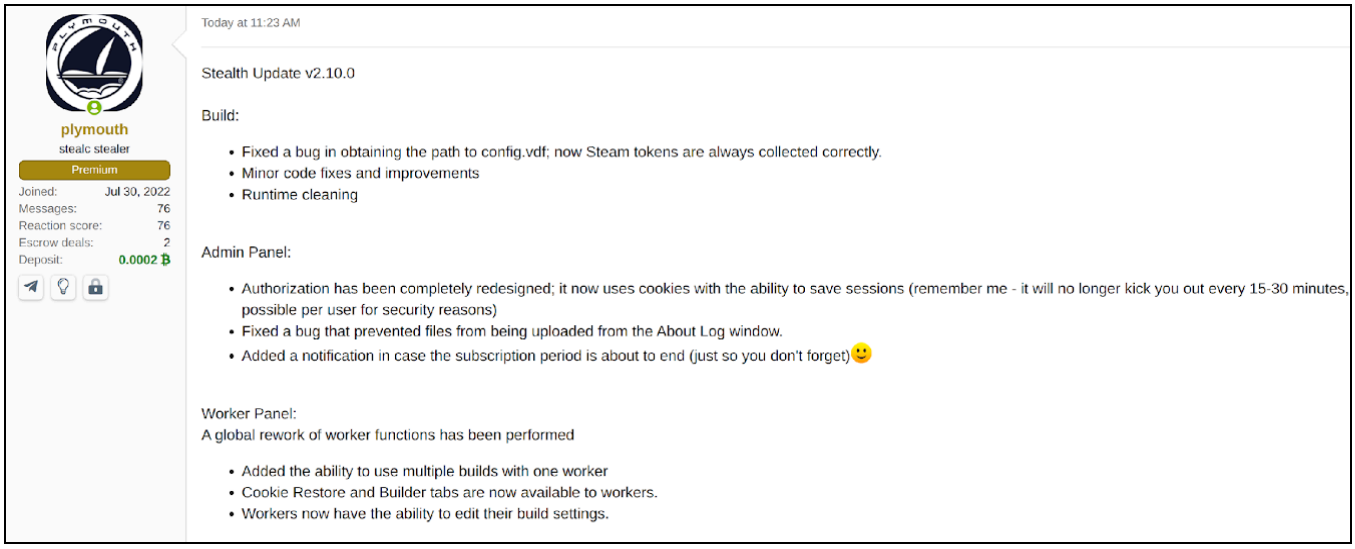
There is a roughly even chance that the access advertised is legitimate, the implications of which would likely be severe. Threat actors will likely seek such access for various malicious activities, including the collection of criminal records or other sensitive information. If rockstar's access is as advertised, it would likely enable threat actors that

buy it to conduct further campaigns such as surveillance, access to government or law enforcement intelligence, or identity fraud and financial crime.

Latest Version of StealC InfoStealer Announced

On January 7, 2026, established actor "plymouth" announced the release of Stealth Update v2.10.0 for the notorious infostealer StealC v2 on the dark web forum XSS. In the post, the actor outlined the updates that would be included in the new version of the malware and directed interested parties to contact them through a private message on the forum, Telegram, or Jabber.

- StealC is a widely used infostealer malware strain currently ranked third in terms of popularity within the Russian cybercrime market, with approximately 12 million infected devices recorded since early 2023.
- Plymouth joined XSS in July 2022 and has garnered a very positive reputation; they are recognized on the forum as the official seller of StealC infrastructure.



plymouth's XSS post
Source: ZeroFox Intelligence

In the post, plymouth indicated that most of the updates focus on improving the existing build and fixing minor issues (such as addressing previously identified bugs) rather than introducing major new features. Also, the actor claims the admin panel now has a complete redesign of the login authorization mechanism, which is likely an update to align with developing security protocols to better protect users of the malware.

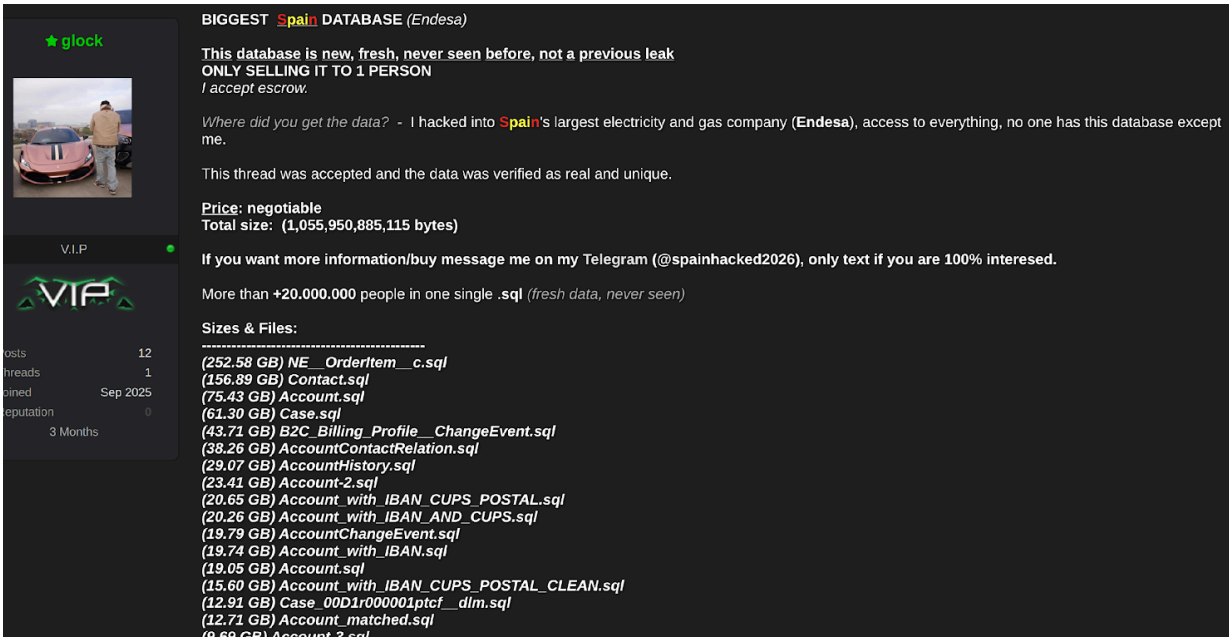
- StealC is among the infostealers that receive the most frequent updates. This continuous development keeps the malware among the most dangerous threats (alongside other prominent infostealers such as Lumma and Vidar) and is likely an attempt to remain competitive in the market.

Spanish Energy Company Breached

On January 4, 2026, newly registered and unvetted actor "spain" announced on dark web forum BreachForums that they had breached Endesa, a Spanish energy company. The actor claimed to have full access to all data stored by the company; they also claimed that this was a new breach and that they are the sole actor in possession of the data. Endesa subsequently confirmed that it had been breached.[1]

[1] hXXps://www.telemadrid[.]es/noticias/economia/Hackeo-a-Endesa-Energia-compromete-datos-sensibles-de-millones-de-clientes-0-2852114765--20260112104854.html

- On January 5, 2026, newly observed and unvetted actor "glock" posted the same advertisement on the dark web forum DarkForums. Both actors have the same profile picture and are almost certainly the same individual. Spain/glock was very likely attempting to enhance circulation of their advertisement to attract more potential buyers.
- Spain joined BreachForums in January 2026, and glock joined DarkForums in September 2025; neither persona has accumulated a positive reputation on the respective forums.
- Endesa is reportedly one of Spain's largest gas and electricity companies and documented a nine-month revenue of approximately EUR 16 billion from January to September 2025.[2]



glock's post on DarkForums
Source: ZeroFox Intelligence

According to spain/glock, the sales post was approved by both forums' moderation teams, and the data was verified—likely lending significant credibility to the post. The full dataset reportedly contains information pertaining to more than 20 million Spanish

[2] hXXps://www.endesa[.]com/en/press/press-room/news/economic-information/september-2025-results

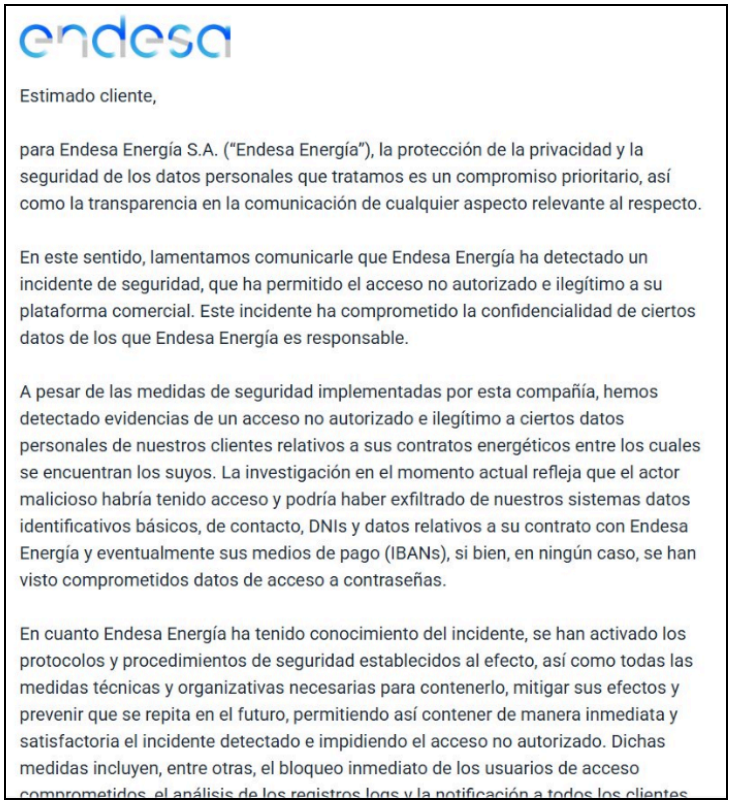
residents and exceeds 1 TB in size. The price is reportedly negotiable, and the actor stated that they will only sell to one person via escrow.

- The dataset allegedly contains highly sensitive personally identifiable information (PII) related to both Endesa customers and internal company business information.
- Foreigner Identity Numbers (NIEs), national ID numbers, names, emails addresses, International Bank Account Numbers (IBANs), phone numbers, and other personal details are among the most sensitive data listed in spain/glock's posts.

Endesa confirmed in a statement that a threat actor gained unauthorized and illegitimate access to its systems and extracted sensitive PII; however, online passwords were reportedly not extracted.[3] Endesa also warned customers that, although it had not detected any mishandling of the compromised data, it could be used for identity fraud and social engineering campaigns.

- In February 2024, the Spanish Data Protection Agency (AEPD) fined Endesa EUR 6.1 million for General Data Protection Regulation (GDPR) violations following a 2024 security breach that likely exposed customer data.[4]

[3] hXXps://www.europapress[.]es/portaltic/ciberseguridad/noticia-hackeo-endesa-energia-compromete-datos-sensibles-clientes-incluidos-dni-medios-pago-20260112100753.html
[4] hXXps://www.dataguidance[.]com/news/spain-aepd-fines-endesa-energ%C3%ADa-61m-data-protection



endesa

Estimado cliente,

para Endesa Energía S.A. ("Endesa Energía"), la protección de la privacidad y la seguridad de los datos personales que tratamos es un compromiso prioritario, así como la transparencia en la comunicación de cualquier aspecto relevante al respecto.

En este sentido, lamentamos comunicarle que Endesa Energía ha detectado un incidente de seguridad, que ha permitido el acceso no autorizado e ilegítimo a su plataforma comercial. Este incidente ha comprometido la confidencialidad de ciertos datos de los que Endesa Energía es responsable.

A pesar de las medidas de seguridad implementadas por esta compañía, hemos detectado evidencias de un acceso no autorizado e ilegítimo a ciertos datos personales de nuestros clientes relativos a sus contratos energéticos entre los cuales se encuentran los suyos. La investigación en el momento actual refleja que el actor malicioso habría tenido acceso y podría haber exfiltrado de nuestros sistemas datos identificativos básicos, de contacto, DNIs y datos relativos a su contrato con Endesa Energía y eventualmente sus medios de pago (IBANs), si bien, en ningún caso, se han visto comprometidos datos de acceso a contraseñas.

En cuanto Endesa Energía ha tenido conocimiento del incidente, se han activado los protocolos y procedimientos de seguridad establecidos al efecto, así como todas las medidas técnicas y organizativas necesarias para contenerlo, mitigar sus efectos y prevenir que se repita en el futuro, permitiendo así contener de manera inmediata y satisfactoria el incidente detectado e impidiendo el acceso no autorizado. Dichas medidas incluyen, entre otras, el bloqueo inmediato de los usuarios de acceso comprometidos, el análisis de los registros logs y la notificación a todos los clientes

Endesa's acknowledgement of breach to customers

Source: hXXps://x[.]com/H4ckmanac/status/2010634136176959799/photo/1

It is almost certain that spain/glock's advertisements on BreachForums and DarkForums will attract significant attention from potential buyers, especially considering that Endesa has confirmed the breach. Threat actors will very likely seek to use the data for social engineering—such as phishing or smishing (SMS phishing)—and identity fraud campaigns for financial gain.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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%