



| Brief |

The Underground Economist: Volume 5, Issue 7

B-2025-04-11a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

April 11, 2025

Scope Note

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 9:00 AM (EDT) on April 11, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 7

| MySQL DataBase Advertised in Dark Web Forum

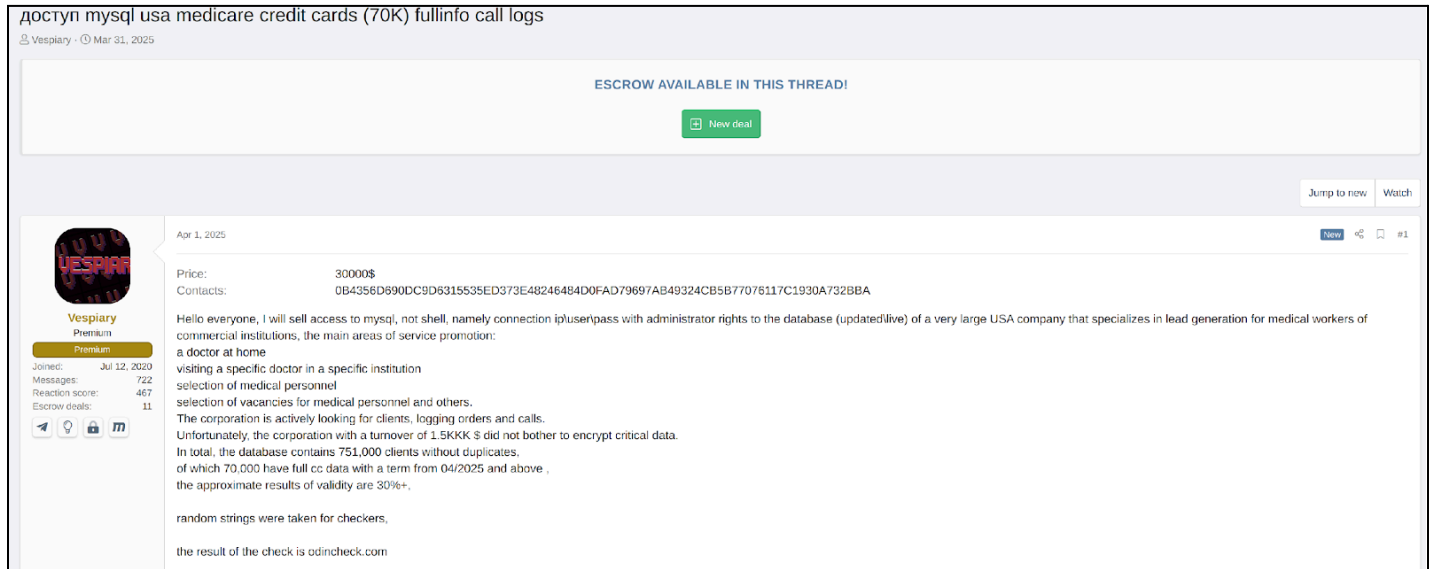
On April 1, 2025, a Russian-speaking actor known as “Vespiary” advertised unauthorized access to a MySQL database belonging to a large, unnamed U.S.-based organization on the xss forum. According to the advertisement, buyers will gain live access to unencrypted information associated with 751,000 clients, none of which are duplicates.

The data allegedly includes comprehensive credit card details connected to 70,000 clients, 30 percent of which have been verified as valid using various open source tools such as pickup24[.]cc and odincheck[.]com.

- The allegedly compromised organization is described as specializing in “lead generation” for medical professionals working in commercial institutions, generating an annual revenue of USD 1.5 billion. Access to the data set is being advertised for sale for USD 30,000.

Vespiary has a strong reputation on xss, having completed at least 11 transactions via escrow since joining the forum in July 2020. While ZeroFox has observed no feedback from other actors within the forum, Vespiary’s reputation adds credibility to their services and the proposed sale. As of the writing of this report it is unclear if a sale has been made, with communications almost certainly taking place via private messaging channels.

If the data and access is as advertised, a purchase could enable a buyer to conduct targeted social engineering campaigns and financial fraud against a large number of victims.



доcтyn mysql usa medicare credit cards (70K) fullinfo call logs

Vespiary · Mar 31, 2025

ESCROW AVAILABLE IN THIS THREAD!

New deal

Jump to new Watch

Apr 1, 2025

Vespiary
Premium

Joined: Jul 12, 2020
Messages: 722
Reaction score: 467
Escrow deals: 11

Price: 30000\$
Contacts: 0B4356D890DC9D6315535ED373E48246484D0FAD79697AB49324CB5B77076117C1930A732BBA

Hello everyone, I will sell access to mysql, not shell, namely connection (plugin/pass with administrator rights to the database (updated/live) of a very large USA company that specializes in lead generation for medical workers of commercial institutions, the main areas of service promotion:

- a doctor at home
- visiting a specific doctor in a specific institution
- selection of medical personnel
- selection of vacancies for medical personnel and others.

The corporation is actively looking for clients, logging orders and calls. Unfortunately, the corporation with a turnover of 1.5KKK \$ did not bother to encrypt critical data. In total, the database contains 751,000 clients without duplicates, of which 70,000 have full cc data with a term from 04/2025 and above, the approximate results of validity are 30%+.

random strings were taken for checkers,

the result of the check is odincheck.com

xss post by Vespiary advertising MySQL access

Source: ZeroFox Intelligence

| Blackfield Claims Possession of Sensitive U.S Officials' Data

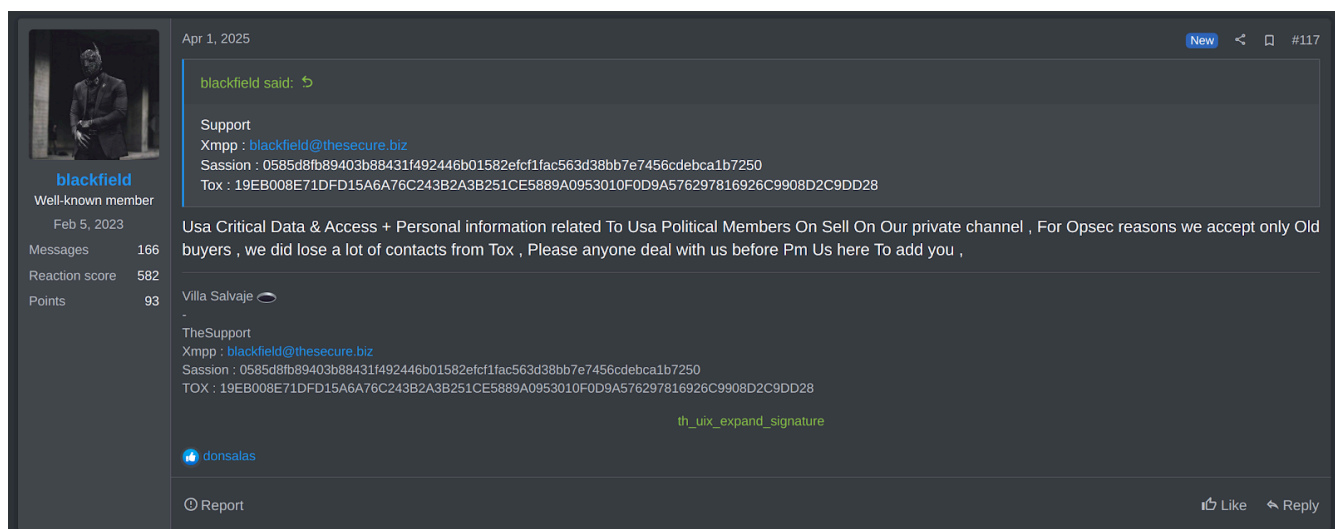
On April 1, 2025, threat actor “blackfield” posted on the Russian language dark web forum RAMP, claiming to have gained access to “critical” data related to U.S. political personnel. Blackfield provided minimal information on the stolen data but alluded that it includes personal identifiable information (PII). According to the advertisement, only “old buyers” will be engaged due to operational security (OPSEC) concerns. Interested parties were encouraged to make contact via the encrypted messaging platform Tox.

- ZeroFox previously reported on separate statements by blackfield, whereby they claimed responsibility for numerous data breaches targeting primarily Israel-based victims.

- Most recently, on March 15, 2025, blackfield warned that upcoming attacks would target U.S.-based entities and would be conducted in such a manner as to appear to originate from China, Iran, or North Korea.

Blackfield is a pro-Palestinian threat actor and carries a positive reputation within deep and dark web (DDW) forums, with more than 500 positive reaction points from fellow forum members. The actor is very likely primarily ideologically motivated, with the majority of their victims being based within nations perceived as hostile toward Gaza.

While recent activity shows blackfield shifting their focus from Israeli to U.S. targets, this development very likely reflects an expansion of their operational remit, rather than a cessation of attacks on Israeli entities.



blackfield claims to have access to U.S. officials' PII

Source: ZeroFox Intelligence

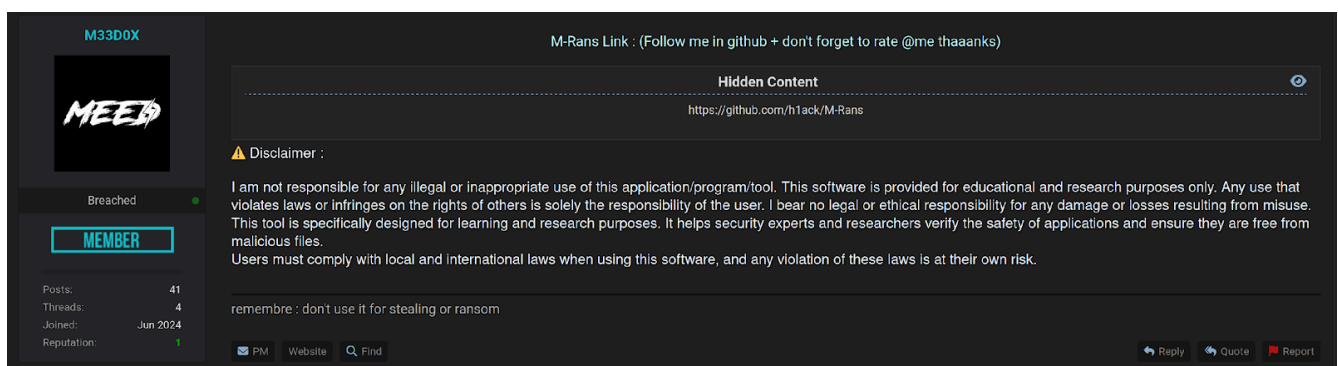
ZeroFox assesses that the compromised data set is likely genuine, as indicated by the actor's decision to limit transactions to previously verified buyers, a tactic commonly used to maintain OPSEC and avoid detection. This approach likely indicates that the actor is handling sensitive or high-value data—or is displaying a degree of caution intended to make potential buyers think this is the case.

- Since the actor is claiming the stolen information is “critical,” it is likely that detailed insights about the data will be disclosed only to vetted buyers.
- Blackfield’s insistence on verified buyers is likely a filtering mechanism to identify genuinely interested parties, which may also serve to limit the buyer pool.
- Given that RAMP frequently hosts politically and ideologically aligned actors, it is likely that similarly minded buyers will deem the alleged information potentially lucrative.

While it is unclear which entity and individuals were compromised and what information was stolen, any compromised data associated with U.S. political personnel is very likely to attract the interest of both financially and politically motivated threat actors seeking to conduct social engineering, mis- and dis-information campaigns, and data theft.

| Free Ransomware Source Code Advertised on BreachForums

On April 1, 2025, a user known as “M33D0X” and “MEED” posted in the hacking forum BreachForums advertising a malware kit named “M-RANS” and also shared a link to a GitHub resource where the full source code can be found. According to the post, the ransomware kit was developed by the actor. ZeroFox rarely observes the advertisement and provision of free malware within DDW forums.



Meed's original post on BreachForums

Source: Zerofox Intelligence

The actor claims that M-RANS is currently the most dangerous malware available and is “100 percent” free to use. MEED added a disclaimer, stating that they accept no responsibility for any illegal or inappropriate use of the tool. MEED states the software is being provided for educational and research purposes only.

The offer allegedly contains a comprehensive kit, including both an encrypting malware and post-breach extortion message.

- As of the writing of this report, the only responses to the advertisement have been from unrecognized actors communicating mostly from accounts with a low credibility score.
- Some actors speculated that the offering could be a trap designed to monitor, track, and collect data on would-be attackers attempting to leverage it in digital extortion attacks.

If the malware is as advertised, it will very likely appeal to a range of financially motivated threat actors, such as digital extortion collectives that have the experience and illicit network access required to conduct ransomware attacks. The offering is unlikely to gain significant traction or interest prior to the public posting of positive feedback.

| New Malware Targeting Android Devices Announced

On March 28, 2025, untested threat actor "droid" advertised a new Android malware named “Nillious” on the dark web forum Exploit, seeking collaborators able to provide their own traffic and target designated applications within specific countries. According to the post, Nillious is compatible with Android versions 9-15. The targeting of victims located within the Commonwealth of Independent States (CIS) countries is not permitted and is likely blocked via the detection of installed Russian-language keyboards.

- The actor provided a demo of the malware, which is hosted on an anonymous online storage service: [hXXps://gofile\[.\]io/d/YqbB4i](https://gofile.io/d/YqbB4i)

As of the writing of this report, the post has garnered minimal feedback from other forum members regarding its legitimacy and effectiveness. It is very likely that newly developed

malicious tools like this have a higher chance of bypassing Android security protocols, leading to a potentially significant, emerging threat.

- ZeroFox observed that the malware was also advertised within the dark web forum xss in January 2025, though for a price of USD 2000.



Nillious Android Malware
By droid, Friday at 11:31 PM in Malware

droid
byte
•

Paid registration
• 0
2 posts
Joined
01/24/25 (ID: 186807)
Activity
virology / malware
Deposit
0.000018\$
Car warranty


Posted Friday at 11:31 PM

Support Android 9 - 15
HVNC
Keylogger
Blackscreen (Target won't able to click while enabled)
Updatescreen (Target won't able to click while enabled)
Customscreen (HTML Design - Target won't able to click while enabled)
Mute device
Application list filter Bank and Crypto apps
Recieve real time notification through telegram bot when a target opens app (the target apps are listed in a json file so you can update anytime)
Antiuninstall
Pin and Pattern injections
Custom injection
Automated Telegram bot for dropper service to bypass android 13+ restrictions
Both panel and payload is from scratch. Payload written using the latest API of Android SDK (35)
CIS Countries Blocked

Exploit post by droid advertising Nillious malware

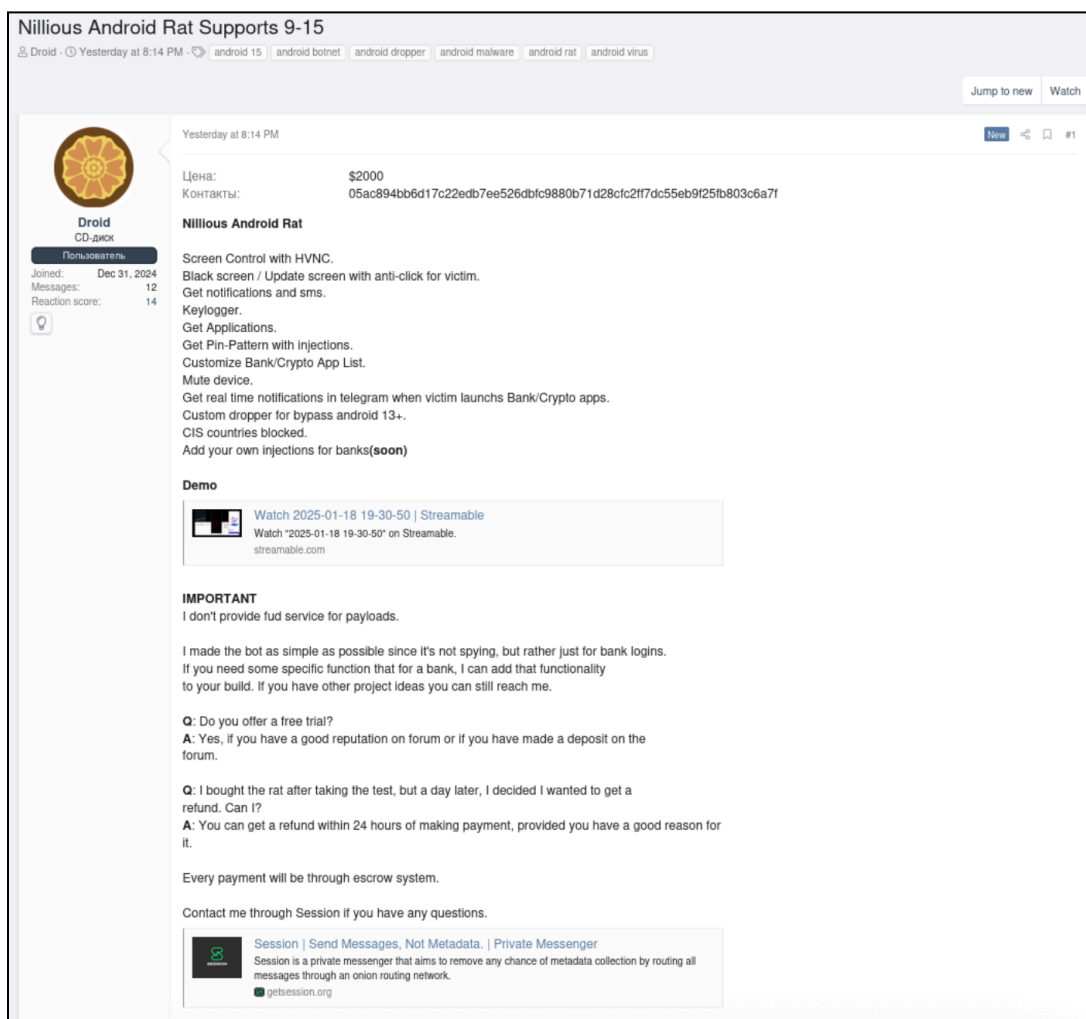
Source: ZeroFox Intelligence

According to droid, Nillious' payload is built from scratch using the latest Android SDK API 35 and utilizes Telegram as the command and control (C2) infrastructure for the malware (regardless of the target using Telegram). It allegedly comes embedded with a hidden virtual network computing (hVNC) component, which obfuscates malicious activity. The keylogger feature allegedly tracks the target's keystrokes, enabling password theft.

- Using screen manipulation like "black screen of death," the malware prevents users from interacting with the system. Other features include the muting of alerts by antivirus systems, a list of banking and cryptocurrency apps, and anti-uninstall protection.

- Notably, the malware is advertised as being protected against uninstall, highlighting a differentiating feature in comparison to the majority of Android-based malware which is removed upon device reset.

User “PigaFreak” replied to the post, accusing droid of conducting scams in the xss forum which resulted in a ban. Droid subsequently denied the accusation, blaming the ban on a disagreement over fund deposits with the xss administrators.



The screenshot shows a forum post on a platform with a dark theme. The post is titled "Nillious Android Rat Supports 9-15" and is by a user named "Droid" with a profile picture of a yellow flower. The post content includes a price of \$2000, a long alphanumeric contact string, and a list of features for the "Nillious Android Rat" malware. The features listed are: Screen Control with HVNC, Black screen / Update screen with anti-click for victim, Get notifications and sms, Keylogger, Get Applications, Get Pin-Pattern with injections, Customize Bank/Crypto App List, Mute device, Get real time notifications in telegram when victim launches Bank/Crypto apps, Custom dropper for bypass android 13+, CIS countries blocked, and Add your own injections for banks(sooon). There is a "Demo" section with a video player showing a streamable video. An "IMPORTANT" section states that the author does not provide a free trial and that payments are made through an escrow system. A Q&A section follows, with questions about a free trial and a refund, and answers explaining the payment process. The post ends with a contact instruction to use Session for private messages.

Nillious Android Rat Supports 9-15

Yesterday at 8:14 PM

Цена: \$2000
Контакты: 05ac894bb6d17c22edb7ee526dbfc9880b71d28cfc2ff7dc55eb9f25fb803c6a7f

Nillious Android Rat

Screen Control with HVNC.
Black screen / Update screen with anti-click for victim.
Get notifications and sms.
Keylogger.
Get Applications.
Get Pin-Pattern with injections.
Customize Bank/Crypto App List.
Mute device.
Get real time notifications in telegram when victim launches Bank/Crypto apps.
Custom dropper for bypass android 13+.
CIS countries blocked.
Add your own injections for banks(sooon)

Demo

Watch 2025-01-18 19-30-50 | Streamable
Watch "2025-01-18 19-30-50" on Streamable.
streamable.com

IMPORTANT

I don't provide fud service for payloads.

I made the bot as simple as possible since it's not spying, but rather just for bank logins.
If you need some specific function that for a bank, I can add that functionality to your build. If you have other project ideas you can still reach me.

Q: Do you offer a free trial?
A: Yes, if you have a good reputation on forum or if you have made a deposit on the forum.

Q: I bought the rat after taking the test, but a day later, I decided I wanted to get a refund. Can I?
A: You can get a refund within 24 hours of making payment, provided you have a good reason for it.

Every payment will be through escrow system.

Contact me through Session if you have any questions.

Session | Send Messages, Not Metadata. | Private Messenger
Session is a private messenger that aims to remove any chance of metadata collection by routing all messages through an onion routing network.
getsession.org

xss post by droid advertising Nillious malware

Source: ZeroFox Intelligence

Droid's displayed geographical proclivities and the seeking of partnerships with specific requirements indicate that the malware is likely ready to be deployed against Android devices located in regions outside of CIS. Due to the lack of feedback and seller reputation, the threat posed by Nillious cannot be determined. However, droid likely intends to operate this malware as-a-service, receiving a share of profits.

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 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

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%