



# **| Brief |**

## **The Underground Economist: Volume 4, Issue 15**

B-2024-08-08a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web

**August 8, 2024**

## 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 August 8, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# Brief | The Underground Economist: Volume 4, Issue 15

## Malicious Stealer Log Marketplace Advertised for Sale

On July 30, 2024, user “2Easy.Shop”—which is almost certainly synonymous with the official handle of the malicious marketplace 2EasyShop—posted in the dark web forum Exploit, claiming that 2EasyShop, its digital infrastructure, and its domain will be auctioned and sold to the highest bidder. The minimum bid is USD 150,000, bid increments are set at USD 10,000, and the instant purchase price is USD 200,000. While the auction is set to take place in Exploit, it is not known if it will occur publicly.

2EasyShop, described by the poster as a “ready-made, configured, highly profitable business”, is a dark web marketplace that specializes in advertising and selling stealer logs.

- Stealer logs are compilations of various types of information that has been stolen from devices and networks infected with a strain of malware known as a stealer. Typically, stealer logs are composed of information such as URL login and password combinations, personally identifiable information (PII), personal financial information (PFI), network and system information, and web browser data such as cookies and session tokens.
- The diversity of information found in stealer logs ensures an ongoing demand from a vast array of cyber threat actors, who leverage it to enable initial network access, enhance social engineering attacks, or conduct fraudulent activities.

## 2Easy.Shop - Logs Marketplace

By 2Easy.Shop, July 30 in Auctions

Ready-made, configured, highly profitable business.

- Top server, domain.
- Logs for 4 years (displayed on shop windows by sellers, not for personal use).
- Contacts of all (30+) sellers for the entire period of work.
- Telegram channel 1800+ subscribers <https://t.me/+UOi2JQYKnsGavS5q>
- Access to forums (54 forums), EXCEPT Exploit and WWH, is discussed separately.

We are also discussing the transfer of contacts of partners - with whom cooperation has been agreed and placement of individual sales branches on the site. Self-regs, bank accounts, CC, e-gifts, DOC'S, socks vpn, DDOS, fullz, call center, liken sphere, cash out and so on. The list is VERY long.

Start 150k\$

Step 10k\$

Blitz 200k\$

### **Exploit post advertising the auction of 2EasyShop**

*Source: ZeroFox Intelligence*

According to the advertisement, the purchase also includes:

- A supply of private stealer logs that have not been circulated elsewhere and contact details of over 30 sellers (likely individuals leveraging established malware distribution operations that regularly sell on 2EasyShop);
- An associated Telegram channel and access to 54 unspecified forums in which to advertise via a 2EasyShop official handle; and
- A long list of contacts and alluded-to capabilities that are very likely indicative of access to fraudulent services, such as bank accounts created leveraging stolen PII.

On August 3, 2024, 2Easy.Shop reposted the rules of the auction and claimed that the auction time will be extended by 72 hours. As of August 6, 2024, the thread has received no visible traction and no new announcements have been posted, though it is unknown if conversation or negotiations are taking place by private means.

2EasyShop launched in approximately 2018 and experienced significant initial growth. Despite claims of overly assertive administrative staff and the site generally featuring

older and lower quantities of logs than rival sites, the shop quickly became a competitor to other stealer log marketplaces, such as Genesis and Russian Market. The platform is fully automated (meaning customers can create an account, add funds, and make purchases all without interacting with sellers), and a diverse array of information is available due to sellers leveraging a number of different stealers.

However, in recent years 2EasyShop has become associated with frequent and lengthy periods of interrupted service and administrative issues.

- In Q2 2023, 2EasyShop's previous domain was hijacked by threat actors who conducted subsequent phishing attacks targeting the platform's customers, damaging its reputation.
- In February 2024, 2EasyShop's administrators claimed to have lost access to customers' wallets. While no further detail was made available surrounding this issue, it was followed by periods of downtime.

|                              |                               | Country                                                                                | Seller     | Files                                                                                           | Info                 | Date upload      |                         |
|------------------------------|-------------------------------|----------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------|----------------------|------------------|-------------------------|
| <a href="#">Links (413)</a>  | <a href="#">Cookie (4364)</a> |  RS | DarkSeller |  archive.zip | <a href="#">Info</a> | 19/11/2023 19:38 | <a href="#">1.56 \$</a> |
| <a href="#">Links (1272)</a> | <a href="#">Cookie (8471)</a> |  IQ | DarkSeller |  archive.zip | <a href="#">Info</a> | 18/11/2023 11:38 | <a href="#">1.95 \$</a> |
| <a href="#">Links (62)</a>   | <a href="#">Cookie (992)</a>  |  BR | DarkSeller |  archive.zip | <a href="#">Info</a> | 18/11/2023 11:24 | <a href="#">1.95 \$</a> |
| <a href="#">Links (1174)</a> | <a href="#">Cookie (2369)</a> |  TR | DarkSeller |  archive.zip | <a href="#">Info</a> | 13/11/2023 20:11 | <a href="#">2.47 \$</a> |
| <a href="#">Links (555)</a>  | <a href="#">Cookie (5330)</a> |  SI | DarkSeller |  archive.zip | <a href="#">Info</a> | 13/11/2023 19:49 | <a href="#">2.47 \$</a> |
| <a href="#">Links (154)</a>  | <a href="#">Cookie (1404)</a> |  MA | DarkSeller |  archive.zip | <a href="#">Info</a> | 13/11/2023 19:09 | <a href="#">2.47 \$</a> |
| <a href="#">Links (452)</a>  | <a href="#">Cookie (1129)</a> |  GR | DarkSeller |  archive.zip | <a href="#">Info</a> | 13/11/2023 18:57 | <a href="#">2.47 \$</a> |
| <a href="#">Links (156)</a>  | <a href="#">Cookie (1283)</a> |  EG | DarkSeller |  archive.zip | <a href="#">Info</a> | 13/11/2023 18:46 | <a href="#">2.47 \$</a> |
| <a href="#">Links (211)</a>  | <a href="#">Cookie (409)</a>  |  YE | DarkSeller |  archive.zip | <a href="#">Info</a> | 26/10/2023 08:46 | <a href="#">1.30 \$</a> |
| <a href="#">Links (281)</a>  | <a href="#">Cookie (764)</a>  |  YE | ALLL       |  archive.zip | <a href="#">Info</a> | 12/10/2023 12:51 | <a href="#">6.50 \$</a> |

## 2EasyShop marketplace, showing stealer logs available for purchase

Source: ZeroFox Intelligence

While 2EasyShop did not specify a reason for listing the platform for sale on Exploit, it is likely the culmination of a series of errors and issues that resulted in a diminishing reputation and customer base. Other stealer log marketplaces have grown significantly in popularity—notably the recently-launched dark web service Exodus, which quickly drew significant attention.

Given the very likely growing demand among various types of cyber threat actors for the information contained within stealer logs, it is likely that a sale will take place. If the auction fails, there is a roughly even chance that the site will remain closed until a sale occurs, though the asking price may be reduced. Should the platform become non-operational, a number of sellers that primarily use 2EasyShop would very likely move to Russian Market, Genesis, Telegram-based services, or smaller deep and dark web (DDW) marketplaces.

A successful deal at the asking price would very likely reinvigorate 2EasyShop, resulting in more reliable service, an increased supply of logs, and a higher volume of sales that almost certainly pose a threat to individuals and organizations.

## **| Alleged Drug Enforcement Administration Numbers Advertised for Sale in Latest Snowflake Breach**

Only July 30, 2024, threat actor “Sp1d3rHunters” posted in the popular hacking forum BreachForums, advertising a data breach that targeted a North America-based pharmaceutical company. The breach allegedly consists of 3 terabytes of information related to “prescribers”, which very likely includes PII such as names and contact details. Sp1d3rHunters also alludes to the breach containing 1.6 million Drug Enforcement Administration (DEA) Registration Numbers.

- DEA Registration Numbers are unique identifiers assigned under the U.S. Controlled Substances Act (CSA) to certain health care providers (such as doctors, nurses, dentists, and veterinarians) and others whose job duties require prescribing and distributing controlled substances.
- The Sp1d3rHunters alias was recently changed from “Sp1d3r”, very likely in an attempt to establish the long-suspected connection to the alias “ShinyHunters.”
- After registering in the DDW forum exploit on May 30, 2024, the threat actor was responsible for posting several data breaches related to the May 23, 2024, breach of the cloud-based service provider Snowflake. In this most recent post, Sp1d3rHunters alleges the victim is also connected to the Snowflake data breach.

**For Sale: 1.6m Medical DEA numbers and prescriber details from [REDACTED]**

We bring to you another raped Snowflake with over 3TB of data from [REDACTED]

**What is a DEA number?**

"A DEA number (DEA Registration Number) is an identifier assigned to a health care provider (such as a physician, physician assistant, nurse practitioner, optometrist, podiatrist, dentist, or veterinarian) by the United States Drug Enforcement Administration allowing them to write prescriptions for controlled substances"

Write your own prescriptions for controlled drugs like Adderall, oxycodone, oxycontin, xanax, methadone and more.

**Exclusive Price**

[REDACTED] If you do not want this data to be sold, you can buy it back for **\$3million USD**.

You can't reset DEA numbers. Each doctor has to go through the hassle of manually submitting a request for a new number with the DEA. And you know how the US government is. It'll take them months to process it. The doctors won't even know if their DEA numbers have been compromised, so they're just left waiting until they find out their numbers were hacked. And you better believe people are going to use this data to write a ton of fake prescriptions.

**Online Sale Price**

- \$10,000 for 10 DEA numbers
- \$25,000 for 50 DEA numbers
- \$50,000 for 100 DEA numbers

Numbers sold in packages only. No individual sales. Middleman required for sale.

Contact (XMPP ONLY): sp1d3rhunters@jabber.ua

**Sample:**

Here are 50 prescriber numbers with the DEA number partially masked.

**Sp1d3rHunters' BreachForums post advertising data breach**

Source: ZeroFox Intelligence

The asking price for the data is USD 3 million, which—due to its exorbitant nature—is almost certainly an extortion attempt to incentivize the victim organization or even the U.S. government to purchase the data. Sp1d3rHunters directly addresses the victim in the post, alluding to the widespread impact that they foresee should the data not be purchased. The threat actor also reinforces this by specifying the breach remediation steps, which they allege would involve a lengthy process of practitioners re-applying for DEA numbers.

The data can also be purchased in smaller quantities for lower prices:

- USD 10,000 for 10 DEA numbers (USD 1,000 each)
- USD 25,000 for 50 DEA numbers (USD 500 each)
- USD 50,000 for 100 DEA numbers (also USD 500 each)

These offers are almost certainly aimed at other threat actors frequenting BreachForums and also very likely serve the secondary purpose of instilling urgency in the victim organization. While the latter two offers are slightly cheaper, the notable price of each DEA number is very likely reflective of the value and demand that Sp1d3rHunters perceives this information to have within DDW marketplaces.

Despite the U.S. medical sector ensuring numerous failsafes are in place to ensure that controlled substances are protected and accounted for, the acquisition of DEA numbers is likely to be attractive to a variety of financially-motivated threat actors. This information could be used to produce fraudulent prescriptions, either for private use or to supply illicit controlled-substance markets. The PII could also be used to conduct enhanced social engineering attacks against other organizations across the sector or to grant threat actors access to the sensitive systems used by healthcare professions.

## **| AI-Powered Tool to Target Cryptocurrency Wallets in Development**

On July 25, 2024, untested threat actor “Michelangelo” posted in the primarily Russian-speaking dark web forum Exploit advertising a new artificial intelligence (AI)-powered tool designed to facilitate “complex, sophisticated, and large-scale” attacks targeting cryptocurrency wallets. Rather than searching for buyers, Michelangelo appears to be seeking other threat actors able to cooperate in development—particularly those able to integrate the tool into their own projects.

- A list of features is included in the advertisement, the majority of which are centered around user convenience, flexibility, and the ability to manage and monitor attacks in real time. These include command line and web interfaces, task scheduling, and real-time monitoring and analytics.
- Other details specify the tool’s ability to facilitate and enhance password-checking and brute-forcing processes. Among these is the use of machine learning algorithms to conduct AI-enhanced password prediction and automate password spraying leveraging previously-obtained information, as well as the ability to use chosen rules and custom dictionaries.

**Hub for sophisticated complex attacks on crypto wallets using AI and optimized distributed computing**

By Michelangelo, Thursday at 04:22 PM in [Other] - everything else

**About the project:**

- **CLI and web interface**: Convenient tools for launching and managing attacks, as well as monitoring the process in real time.
- **Cloud Integration**: Support for AWS, Google Cloud and Azure to scale attacks and securely store data and configurations.
- **Support for various wallets and files**: MetaMask, Exodus, Electrum, Bitcoin Core, Blockchain, etc.
- **Task Scheduler and Notifications**: Ability to schedule attacks, notification system (mail, SMS, messengers) and logging with analytics.
- **Manage and distribute tasks between GPUs**: Support and optimize GPU utilization and maximize performance.
- **Password Storage Database**: Utilize password database, automatically update and manage the database.
- **Monitoring and analytics**: Real-time attack tracking via web interface and CLI, generate reports on attack results.
- **Intelligent password mining**: Using machine learning algorithms to analyze and adapt attacks, predicting passwords based on big data analysis.
- **Adaptive Attacks**: Changing attack strategy in real time, dynamic resource reallocation.
- **Team Management**: Task allocation and collaboration on attacks, ability to share dictionaries and configurations.
- **Automated Recovery**: Automatic data recovery after successful password cracking, integration with backup systems.
- **Attacks using known data (Password Spraying)**: Using information about previous passwords to generate additional variants.
- **Integration with external data sources**: Analyzing leaked databases to update password dictionaries, integration with data leak analysis services.
- **Parallel attack execution**: Support for multi-threaded attacks, optimize resource allocation.
- **Custom dictionaries and rules**: Create and use custom dictionaries, set of instructions for generating additional password variants.
- **Computing Resources**: Utilize powerful computing resources and the ability to manage all aspects of the farm.
- **Scalable Attack Vector**: Realization of more than 16 types of attacks.

And this is not the whole list of functions, we are actively working 24/7 and expanding the functionality.

**Michelangelo's Exploit post advertising new tool***Source: ZeroFox Intelligence*

The advertisement does not specify exactly how the tool enables attacks or the necessary prerequisites, but it is likely that a threat actor would first need to obtain initial network access. Once established, the tool likely leverages the victim's hardware resources to conduct password mining and spraying processes, attempting to gain access to local crypto wallets.

- The "Passwords" that Michelangelo claims the tool can obtain could relate to those guarding an account, the private keys associated with cryptocurrencies, or the recovery seeds associated with security codes used to perform recovery efforts.
- However, given the tool's apparent reliance upon optimized GPU utilization, it is very likely that it seeks to obtain private keys able to grant full access to the cryptocurrency.

Upon gaining access to the victim's cryptocurrency, the funds can be transferred to a wallet owned by the attacker before various laundering techniques, such as the use of tumblers, obfuscate the funds.

The tool is currently under development, and its completion timeline is not specified. Given its likely need to be deployed to victim networks, Michelangelo's sought-after collaborators almost certainly include threat actors able to provide initial network access, malware operators able to embed the tool within malicious software (thereby providing a delivery method), or botnet operators who are seeking to exploit large numbers of compromised credentials. It is unknown if the tool will be sold to a single buyer, multiple buyers, or provided as a subscription-based service.

While tools with brute-forcing and password-mining capabilities are not new, this tool allegedly contains innovative features that reflect an appetite among cybercriminals to develop and commercialize malicious techniques able to target the growing cryptocurrency economy.

## **| Project Showcased in Dark Web Competition Leverages AI Automation**

On July 23, 2024, positive-reputation, English-speaking actor "Mr\_Stuxnot" announced their contribution to a dark web forum video creation contest. The project, posted in the xss forum and dubbed "XSS AGENT", functions as an "AI-powered autonomous command and control" (C2). XSS AGENT was presented in video format in line with the rules of the competition and was also made available for download.

- The xss forum holds a number of competitions encouraging actors to develop and showcase insights and share expertise with other interested parties in dark web communities. Contributions are usually either tools that have been developed to conduct malicious activities, proof of concepts (PoCs), or articles seeking to share knowledge related to cyberattack vectors and tactics, techniques, and procedures (TTPs).
- In April 2024, xss moderators held their eighth iteration of the [// XSSware] competition, which offered a USD 20,000 reward distributed amongst the top seven contestants. Contributions ranged from cryptocurrency/non-fungible token

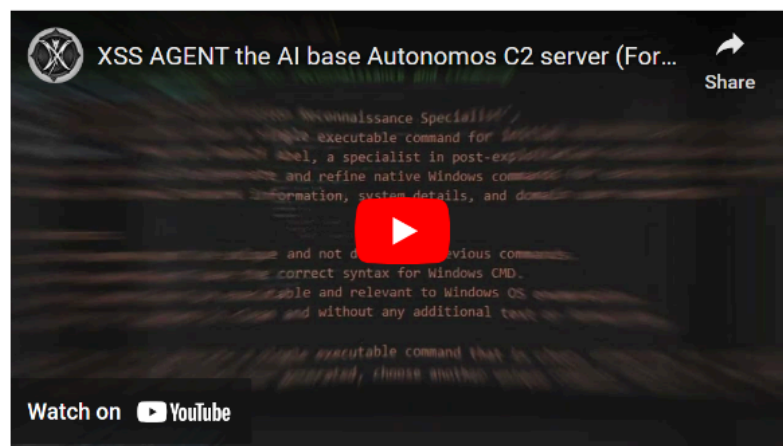
(NFT) drainer kits to stealer malware to brute forcing tools that target virtual private networks (VPNs).

Jul 23, 2024

Hello everyone, first of all, I would like to thank the sponsor of the competition, even though we don't know who they are! **(Thanks!)**

**(XSS AGENT)** is a proof of concept of an AI-based autonomous post-exploitation system that, after receiving initial access, would automate control servers to automate the post-exploitation process.

While the dream of commanding a full office with thousands of AI agents working 24/7 to literally torment our enemies with attacks from autonomous system is still in the early research stages for regular people without government budgets. In the meantime, we can play with



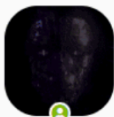
### **Mr\_Stuxnot's xss post advertising XSS AGENT**

*Source: ZeroFox Intelligence*

The function of XSS AGENT is to perform malicious post-exploitation tasks after initial network access has been gained. The PoC allegedly demonstrates the integration of AI and large language models (LLMs) with attacker-controlled C2 servers in order to conduct automated exploitation.

Mr\_Stuxnot received criticism from another well-regarded Russian-speaking actor "dunkel", who expressed doubt as to both the usability of the tool and whether the instructions outlined would conflict with LLM regulations. Mr\_Stuxnot defended the project, pointing out that this is a PoC in the early stages of development and that the LLM used (Dolphin 2.9 Llama 3 8b) is uncensored and will not restrict use. As of August 8, 2024, the competition has concluded, though organizers have not revealed results.

Wednesday at 7:49 AM



**Mr\_Stuxnot**  
CD-диск

Пользователь

Joined: Jun 8, 2023  
Messages: 12  
Reaction score: 6

Yesterday at 12:23 PM

Hello everyone, first of all, I would like to thank the sponsor of the competition, even though we don't know who they are! **(Thanks!)**

**(XSS AGENT)** is a proof of concept of an AI-based autonomous post-exploitation system that, after receiving initial access, would automate the steps an attacker would want to take. The objective is to demonstrate that we can integrate AI with command and control servers to automate the post-exploitation process.

While the dream of commanding a full office with thousands of AI agents working 24/7 to literally torment our enemies with attacks from all directions is compelling, this is still just a product of my imagination for now. The technology to create such an autonomous system is still in the early research stages for regular people without government budgets. In the meantime, we can play with local proof-of-concepts and let our imagination take us far!

1 - It is made very clear that this is a proof of concept! (This will not automatically give you access to Pentagon files when initiated!)

2 - Your statement is incorrect: (Because all LLMs have protection against "generation of potentially harmful" ones).

In fact, the model used in the project is uncensored: <https://huggingface.co/cognitivecomputations/dolphin-2.9-llama3-8b> this means that the questions asked to the model will not go through ethical filters!

### Mr\_Stuxnot's xss post defending XSS AGENT

Source: ZeroFox Intelligence

XSS AGENT is very unlikely to pose an imminent threat to individuals and organizations, due to it being in the early stages of development and the immaturity of the technology required to create automated tools such as these. However, the intent to create such tools is almost certainly indicative of a general appetite among threat actor communities to harness AI in the ongoing pursuit of attack automation, lowered entry barriers, and circumvention of cyber defense measures.

## **| 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.
- Ensure social media accounts are configured with organic security features, such as phishing-resistant MFA and complex, unique passwords.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                                |                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |