



| Brief |

Dark Web Competition Offers Insight into Threat Actor Focus

B-2024-05-24a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Deep and Dark Web, Threat Actor, Malicious Software

May 24, 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 May 24, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Dark Web Competition Offers Insight into Threat Actor Focus

› Key Findings

- The results of Competition [// XSSware] on Russian-speaking dark web forum xss were announced on April 16, 2024. Projects focusing on obfuscation performed well, likely indicating a demand for accessible, free obfuscation tools within the threat actor community.
- While the direct impact is very likely limited, the competition and winning projects will likely contribute to increasing efficiency in attack vectors, particularly as the projects are free to access by members of the forum.
- The top three projects have predominantly been awarded due to their perceived potential rather than their immediate application—with the exception of the first place PowerShell Stealer, which allegedly boasts immediate application.
- It is very likely that the total prize money of USD 20,000 awarded in the course of Competition [//XSSware] will further fund threat actors in developing their malicious tools.

| Context

The results of Competition [// XSSware], a projects competition hosted on Russian-speaking dark web forum xss, were announced on April 16, 2024. Projects that addressed obfuscation performed well in the competition, which is likely indicative of the threat actor community demanding more accessible and cost-free obfuscation tools. While the direct impact is very likely limited, the competition and the winning projects will likely contribute to increasing efficiency in attack vectors, particularly as the projects are free to access by members of the forum. Additionally, exposure for the winning projects and threat actors will likely enhance their reputation, enabling increased potential for monetization of the tools in the future.

- By employing obfuscation methods, cybercriminals aim to operate covertly, evade detection, and impede attribution efforts, making it harder for defenders to identify and respond to their activities effectively.
- The top three projects have predominantly been awarded due to their perceived potential, rather than their immediate application. However, there is a roughly even chance that the PowerShell Stealer was awarded first place due to its alleged immediate application.

Competitions have been a distinctive feature of the Russian-speaking community forum xss. Established in 2018, these contests have sparked significant interest among threat actors and increased forum activity. Since their inception, the competitions have served as a conduit for disseminating valuable knowledge on attack vectors and tactics, techniques, and procedures (TTPs). The articles submitted within the xss competitions have provided unique insights and implementations not found elsewhere on the deep and dark web (DDW), diverging from the usual practice of merely re-publishing publicly available whitepapers.

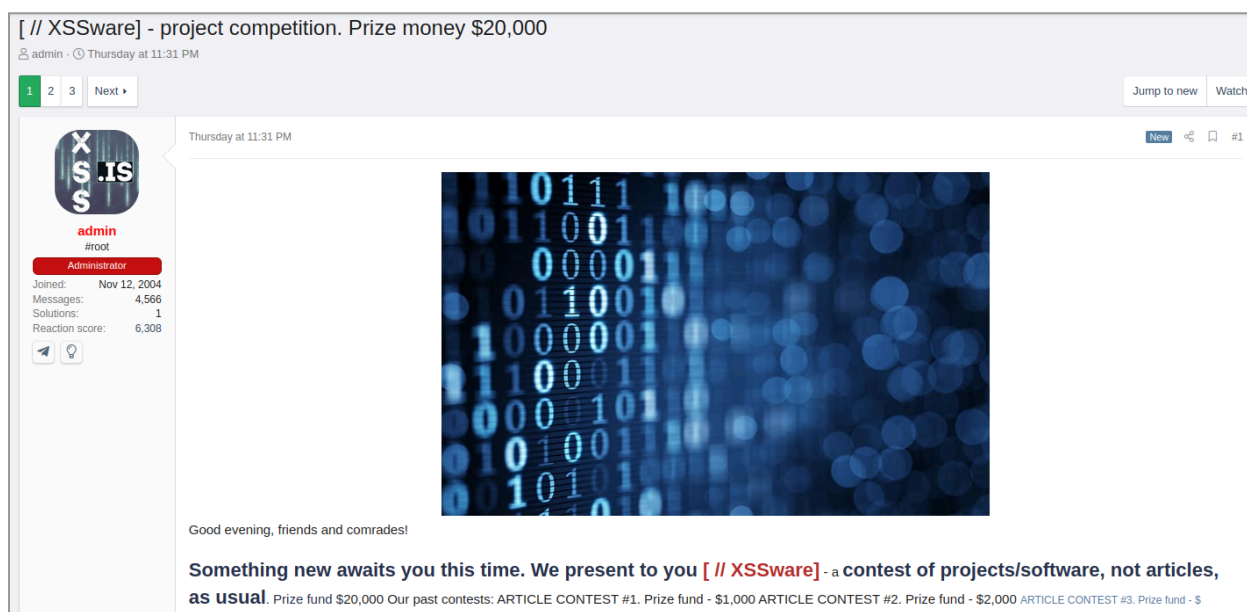
- Seven article competitions have taken place since 2018, with awards guaranteed by high-profile actors and teams.
- Article competition submissions are written exclusively in Russian, unlike other content in xss forums. Typically, Russian-speaking actors perceive themselves as “elite” threat actors that are superior to other language speakers; therefore, it is

very likely that this language submission requirement aims to limit the competition to Russian-speaking participants only.

- Rather than alluding to new trends, the competition identifies the current trends and practices of threat actors.

On November 2, 2023, the admin of xss forum announced the [// XSSware] competition would consist of entire project submissions instead of articles. The announcement stated the participants' submissions must consist of a new tool and explanation and that they must provide the ordinary user and forum with "knowledge, benefit, money or experience."

- The stated submission window was November 5, 2023, up until March 5, 2024.



Xxs admin announcement of revised competition

Source: ZeroFox Intelligence

Accepted topics for projects included all traditional attack vectors, such as phishing, fraud, and network vulnerabilities. Additionally, "AI for blackhat" was included, which continues to see an increased interest; while not established, its continuing rise in popularity and capability is very likely why it was included.

- Projects submitted very likely show that the competition continues to be a “trend confirmer” rather than a “trend setter.”
- Malicious AI tools used by cybercriminals bypass ethical safeguards, allowing the user to utilize its large language model (LLM) to enhance malicious software capabilities such as phishing.

| First Place – PowerShell Stealer

The first place finisher was actor “Crocuta”, who received 22 percent of the votes for their project “Stealer in PowerShell” submitted on March 4 2024. Intended to work on Windows systems, the malware is written primarily in PowerShell, except for a dynamic link library (DLL) file that is placed into Chrome's process to gain access to cookies stored in the victim's browser. The malware is capable of collecting passwords, and allegedly cookies can be unlocked while the browser is running without interruption to the victim. This allows for less interference to the user, very likely reducing the victim's awareness of the attack.

- Stealers are important to the DDW ecosystem. They enable the collection of the most widely important resource at present: logs containing login data to accounts registered with a multitude of services, such as online banking accounts.

Therefore, this data facilitates a multitude of attack vectors.

- The stealer is stated to support both Firefox and Chromium-based browsers.



Crocuta
HDD-drive
User

Joined: Dec 26, 2022
Messages: 24
Reaction score: 56

Mar 4, 2024

Hello world. Here's a powershell stiller. All the details are below.

Spoiler: What's interesting

- Collect Firefox based and Chromium-based browser passwords
- The Stiller itself is written almost entirely in powershell. The exception is the DLL that will be injected into the chrome process to unlock cookies. Let's talk about the unlock itself in the next paragraph. There is also a small insertion of C# code for importing rstrtmgr.dll, but here I can be forgiven, because pwsh simply does not know how to do this)
- Unlocking cookies when Chrome/Edge is running, etc. At the same time, the browser process is not killed, everything happens without unnecessary fawning.
- DLL to shellcode converter. I haven't seen the implementation of this on powershell in public. There's one hanging out on github, but there's C# code wrapped in pwsh. Here, everything is written in pwsh itself. We will use this functionality for the above-mentioned unlock of cookies. You take a DLL and its arguments, convert everything into shellcode and inject it into the browser process. The technique of the injection itself is not mine, but I do not claim to be its author.
- Server-side decryption of passwords and cookies, with the exception of old versions of chrome, where passwords are decrypted using DPAPI, and it is better to do this on the PC itself. As for the rest, everything is server-side, so as not to trigger avers in vain. Chromium decryption is done with the help of python libraries. FF decryption using NSS libraries, since they can be installed on nix servers with a single command.
- Sqlite powershell reader to read cookies and login data of chromium-based browsers.
- Added some tricks to bypass AMSI. They're a bit crutch, but they're working. Why crutches? Because in order to escape from detections without crutches, you need an ultimatum solution - a polymorphic obfuscator. It is not available for several reasons: it takes several months to write it, if not a year, and if you order it, then it will cost in oculion, so we have what we have) And in general, it would already be a separate project, as it were) But again, the current functionality is quite enough to solve our problems.
- The panel is written in python, Flask framework, and gunicorn is used as a WSGI server.

Crocuta's introduction to their submission

Source: ZeroFox Intelligence

PowerShell's ability to bypass Microsoft's antimalware scan interface (AMSI) is likely one of the main reasons for its utilization. This allows threat actors to employ the malware without the use of an encryptor, which would incur additional cost.

- PowerShell is a powerful scripting language built into Windows that is frequently abused by cybercriminals for malicious purposes.
- High-quality crypters and obfuscation services are expensive products on the DDW.

Spoiler: Why powershell

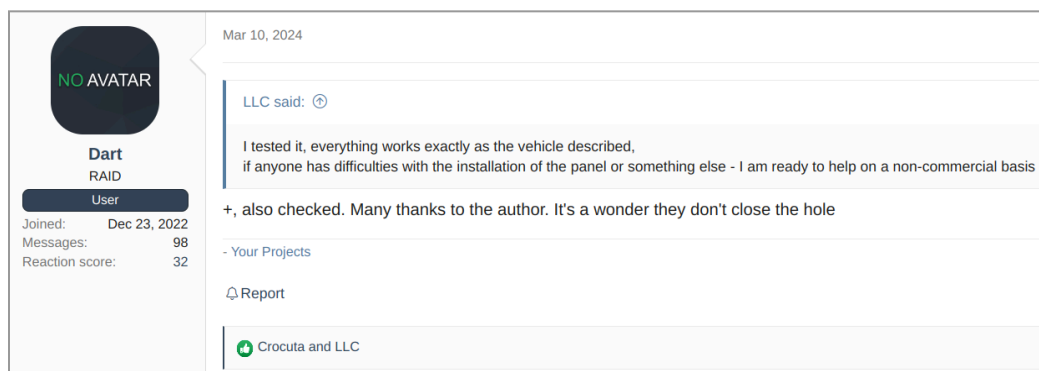
I understand that the topic is holyware, a bunch of posts have been written on the forum both in defense of pvs and against it. But I consider myself to be one of those who believe that, despite some drawbacks, PowerShell is almost perfect in terms of relative ease of avoiding detections. I started the powershell process, bypassed AMSI and do almost what you want, and no cryptos are needed. And it's all with .NET support. Of course, I agree that you need to look at it separately for each product, but for a stealer, pvsh is just fine.

Crocuta's explanation for their use of PowerShell

Source: ZeroFox Intelligence

On March 10 2024, actor "LLC" commented stating that they had tested the stealer, and it worked exactly as described. Other feedback on the project consisted of similar appraisals and comments from users that had allegedly tested its performance. While ZeroFox assumes the number of tests was quite limited, we assess there is a roughly even chance that the stealer was used on real victims.

- On March 10, 2024, actor "Dart" confirmed on LLC's post that they had also used the stealer and could confirm its application.



Actor Dart's confirmation the PowerShell stealer works

Source: ZeroFox Intelligence

The PowerShell Stealer project's success in the competition is very likely due to it allegedly being usable immediately. The malware's capability to eliminate the need for an encryptor or obfuscator while ensuring covert software implementation very likely allows threat actors to increase profitability without increasing risk. The project showed innovation (but is not unique to the DDW) and a new capability of being able to bypass AMSI without the need for payload obfuscation, very likely making it the most attractive technical development of the competition.

| Second Place – Access Miner

On January 5, 2024, respected actor "Alex_Ionescu" submitted their project "The Virtual Network Computing" (VNC) access miner", which was awarded second place in the competition. The project is based on a remote frame buffer (RFB) specifically designed to attack VNC protocol to establish control over a VNC-configured machine via a credentials match.

- Cybercriminals use RFB to remotely access and control systems, view and interact with desktops, establish backdoors, maintain persistent access, exfiltrate data, and move laterally within network privileges.
- This tool's ability to gain access to networks very likely suggests it would be used by access miners and blackhat pentesters. These actors work alongside ransomware groups and represent a critical process for their operations.
- The project is a distributed brute-system in which different modules work together to attack login portals on VNC-configured machines. It uses a free VPN service called SoftEther. The system has a "manager" module overseeing two "workflow" modules:
 - Workers – These modules filter and select targets.
 - Checkers – These modules attempt to log in to the selected targets.

Boot Process Introduction

XSS.is RFB Bruter is a distributed brute-force system for VNC directly from home via the TOR+VPN bundle on a virtual machine farm with support for backups, smartphone notifications via the "pushed" app, and filtering masks. The processed masscan log is used as an address source (although you can add addresses and ports "manually"), and the VPN uses the "SoftEther VPN" app and their great free VPN service — "VPN Gate", which will help us not to pay for a VPN. In addition to this excellent service, SoftEther VPN has a number of other important features, such as socks (TOR) support, as well as ICMP (ping) support. More on that below.

Like any other distributed system, the RFB Bruter XSS.is consists of a "manager" and "workflows". "Workflows", in turn, are divided into "checkers" and "workers": the former check the ip:port lists for the VNC banner (as well as delete unnecessary ones and skip inaccessible ones), while the latter brute-force passwords, and the "manager" manages all this business. "Workflows" and "manager" communicate with each other through a separate intranet adapter, only the "manager" has direct access to the outside world (to send notifications), the rest see the world only through the TOR+VPN bundle.

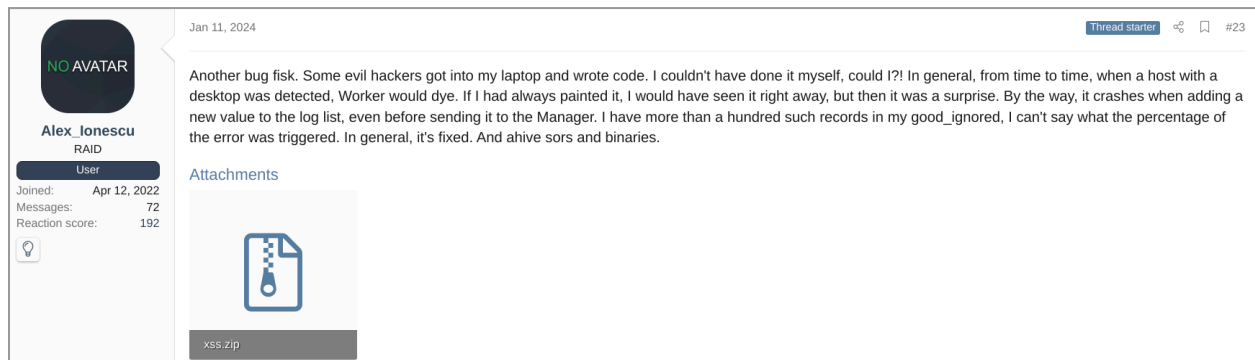
Please note that this is a system for "home" use: traffic between the manager and workflows is not encrypted in any way.

Initially, the system worked without a VPN, directly through TOR (Whonix Gateway), but this imposed a number of limitations: Whonix "overheated" from the number of connections and required regular reboots, and in addition, the connection to the host on which the search was going on often fell off (TOR tries to change addresses in chains, through this the end node is not always available). With a VPN, everything works much more stable and faster: the time it takes to resort the list of addresses for a brute force has increased tenfold, i.e. a larger number of combinations are sorted out in one pass. In addition, TOR does not allow you to check the availability of the network, unlike a VPN, which works perfectly with ICMP packets.

Actor Alex_Ionescu's description of their project

Source: ZeroFox Intelligence

While the submission received positive feedback, discussions were not indicative of testing and real-life usage of the tool as seen with the PowerShell project. However, the author has since released patches and bug fixes, indicating there is a roughly even chance it has been used to target victims and continues to be developed.



Actor Alex_Ionescu releasing a patch

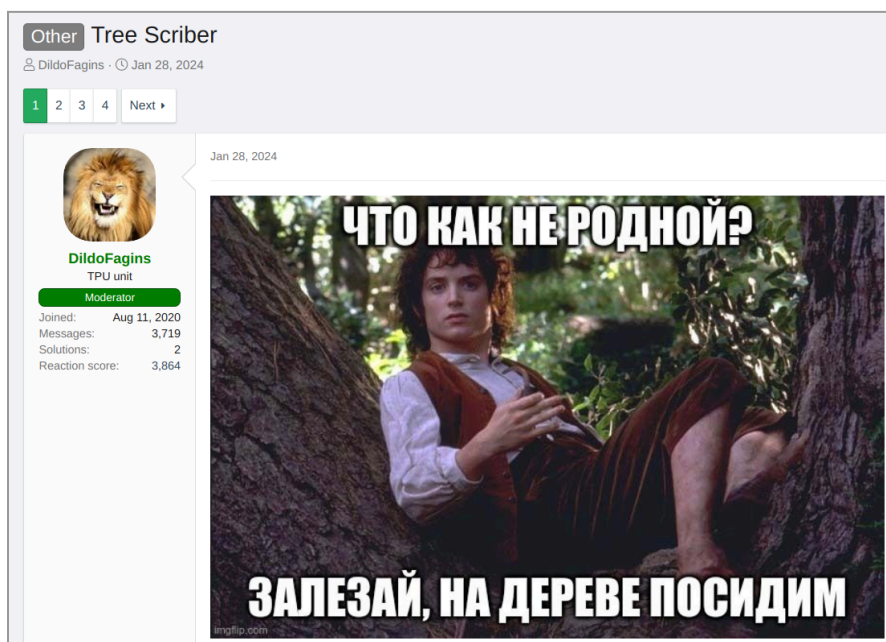
Source: ZeroFox Intelligence

It is very likely the importance of the function the tool performs for ransomware groups was a contributing factor towards the project's success in achieving second place. Access mining is an ever-increasing capability requirement by ransomware groups on the DDW. Therefore, it is very likely this tool's success is indicative of that current trend.

| Third Place – Obfuscator Tool

On January 28, 2024, section moderator and well-regarded threat actor “DildoFaggins” submitted their project “Tree Scriber”, an obfuscator tool that was awarded third place. The project’s premise is that “red team” tools are not able to function for long periods of time without obfuscation. Therefore, the project’s goal is to enhance the survivability of malware payloads, addressing a common need for malicious actors such as botmasters, stealer distributors, ransomware operators, and cryptocurrency miners.

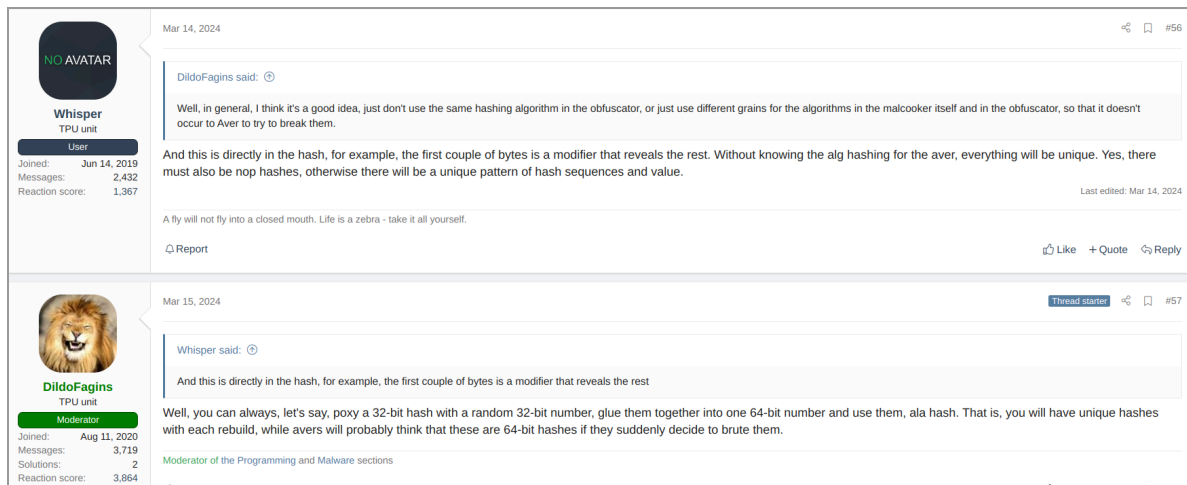
- The project published on xss offers a Python script that allegedly obfuscates malware payloads, providing a typically expensive service for free.
- Threat actor DildoFaggins stated that they regularly implement the Tree Scriber library to obfuscate their attack tools.
- DildoFaggins is a moderator of two xss forums: Programming and Malware.



Actor DildoFaggins announcing their submission

Source: ZeroFox Intelligence

While the feedback for this project was wholly positive, comments featured a multitude of questions and recommendations for the author. This suggests that the tool at present very likely remains in development, unlike the other two submissions.



Actor DildoFaggins and "Whisper"'s technical discussion

Source: ZeroFox Intelligence

The Tree Scriber and PowerShell stealer tools are likely both indicative of a community demand for more accessible and cost-free obfuscation tools. However, unlike the PowerShell stealer, Tree Scriber is very likely not in a readily usable state. There is a roughly even chance this tool placed third primarily due to DildoFaggins' credibility and reputation in the xss forum versus it having superior capabilities to those that scored lower in the competition.

Sponsorship and Prize Money

Competition [// XSSware] was sponsored by an unknown actor that is almost certainly affiliated with the "Angel Drainer" group, which advertises its Angel Drainer cryptocurrency and non-fungible token (NFT)-draining phishing software. It is very likely the aim of the sponsorship was to promote the Angel Drainer tool and other projects presenting an opportunity to enhance the drainer software and TTPs related to its deployment.

- Angel Drainer is a notorious phishing group that actively targets cryptocurrency users, stealing funds from their crypto wallets. The group's prioritization of reputation is very likely indicative of its sponsorship.
- The voting power of both Angel Drainer and xss was enhanced, giving them each a voting power of 5 percent of the total votes. On April 16, 2024, forum-wide voting was closed with 496 votes cast.

The total prize pool for the competition was USD 20,000, with the top seven participants receiving prizes ranging from USD 7,000 for first place to USD 500 for seventh place. It is very likely that the prize money awarded will further fund threat actors in developing their malicious tools.

The winner of the contest (1st place) receives a prize - \$7,000 2nd place - \$5,000 3rd place - \$3,000 4th place - \$1,000
5th place - **\$1,000**
6th place - \$800
7th place - \$800
8th place - **\$**

500
9th place -
\$500
10th place - **\$**

Competition prizes and sponsor announced

Source: ZeroFox Intelligence

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%