



| Brief |

The Underground Economist: Volume 6, Issue 21

B-2026-10-08b

Classification: TLP:CLEAR

Criticality: LOW

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

October 8, 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 (EDT) on October 8, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 6, Issue 21

| Uncensored AI Model Advertised on Exploit

On October 5, 2026, moderately credible threat actor “edwofm” advertised a fully uncensored GLM 5.3 model dubbed “uncensored[.]monster” on the largely Russian-language dark web forum Exploit. This model is considered to be the leading global tool for defensive benchmarks, capable of uncovering thousands of real-world vulnerabilities.

- GLM 5.3 is a Chinese-origin, open weight artificial intelligence (AI) model made by Z.ai (formerly known as Zhipu AI). It is a 753B-parameter mixture-of-experts (MoE) large language model optimized for coding and long-horizon agentic tasks.¹

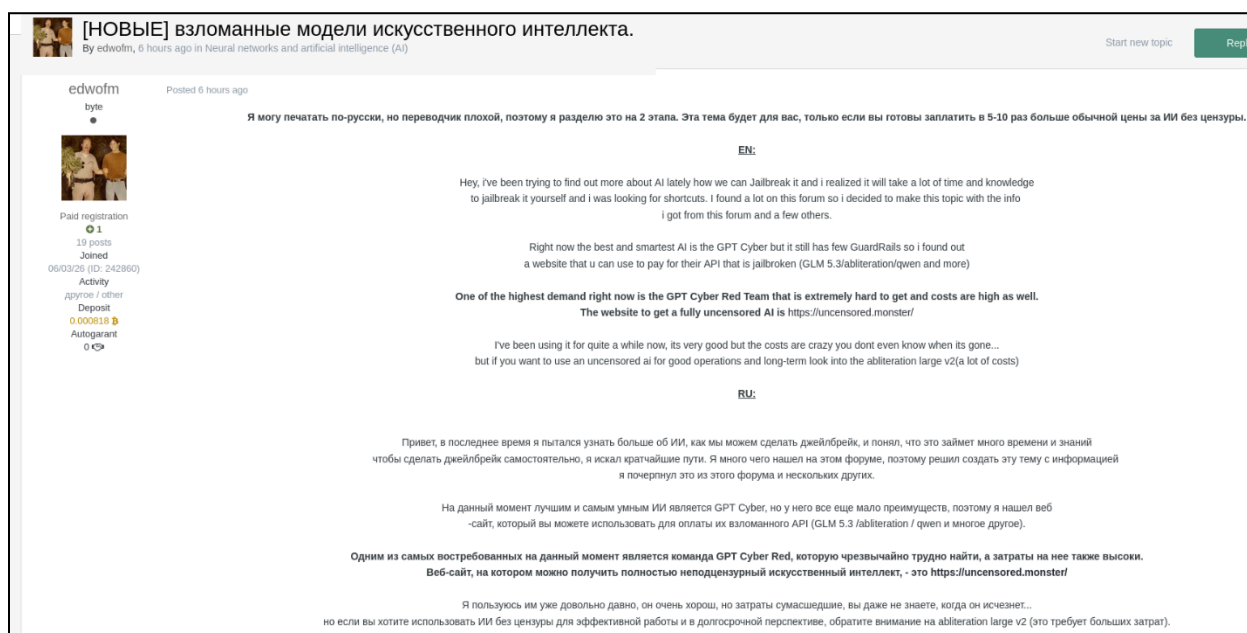
The threat actor claims that uncensored[.]monster specifically features AI-enhanced red team operations and general cybersecurity and Trust and Safety tasks. Additionally, the actor claims to have effectively leveraged the tool; however, the cost of operating the system is allegedly very high.

Uncensored[.]monster operates using a pay-as-you-go (PAYG) model with a starting price of USD 1, treating the AI model like a standard software-as-a-service (SaaS) offering. This almost certainly drastically lowers the financial and technical barriers for novice cybercriminals, eliminating the need for expensive GPU hardware or the expertise

¹ [hxxps://kie\[.\]ai/blog/what-is-glm-5-3](https://hxxps://kie[.]ai/blog/what-is-glm-5-3)

required to locally host and jailbreak open-source models; however, it is likely to cause pricing issues if edwofm's claim of high operating costs is legitimate.

The fact that the threat actor specifically tagged uncensored[.]monster as a "cybersecurity" tool suggests it can very likely be fine-tuned for offensive operations. Cybercriminals will very likely continue to develop methods to jailbreak open weight AI models, with an eye toward leveraging AI capabilities for offensive operations.



[НОВЫЕ] взломанные модели искусственного интеллекта.
By edwofm, 6 hours ago in Neural networks and artificial intelligence (AI)

edwofm
byte
•
Paid registration
19 posts
Joined
06/03/26 (ID: 242860)
Activity
другое / other
Deposit
0.0000018
Autogrant
0 КБ

Posted 6 hours ago

Я могу печатать по-русски, но переводчик плохой, поэтому я разделю это на 2 этапа. Эта тема будет для вас, только если вы готовы заплатить в 5-10 раз больше обычной цены за ИИ без цензуры.

EN:

Hey, I've been trying to find out more about AI lately how we can Jailbreak it and i realized it will take a lot of time and knowledge to jailbreak it yourself and i was looking for shortcuts. I found a lot on this forum so i decided to make this topic with the info i got from this forum and a few others.

Right now the best and smartest AI is the GPT Cyber but it still has few GuardRails so i found out a website that u can use to pay for their API that is jailbroken (GLM 5.3/abiteration/qwen and more)

One of the highest demand right now is the GPT Cyber Red Team that is extremely hard to get and costs are high as well.
The website to get a fully uncensored AI is <https://uncensored.monster/>

I've been using it for quite a while now, its very good but the costs are crazy you dont even know when its gone... but if you want to use an uncensored ai for good operations and long-term look into the abiteration large v2(a lot of costs)

RU:

Привет, в последнее время я пытался узнать больше об ИИ, как мы можем сделать джейлбрейк, и понял, что это займет много времени и знаний чтобы сделать джейлбрейк самостоятельно, я искал кратчайшие пути. Я много чего нашел на этом форуме, поэтому решил создать эту тему с информацией я почерпнул это из этого форума и нескольких других.

На данный момент лучшим и самым умным ИИ является GPT Cyber, но у него все еще мало преимуществ, поэтому я нашел веб-сайт, который вы можете использовать для оплаты их взломанного API (GLM 5.3 /abiteration / qwen и многое другое).

Одним из самых востребованных на данный момент является команда GPT Cyber Red, которую чрезвычайно трудно найти, а затраты на нее также высоки. Веб-сайт, на котором можно получить полностью неподцензурный искусственный интеллект, - это <https://uncensored.monster/>

Я пользуюсь им уже довольно давно, он очень хорош, но затраты сумасшедшие, вы даже не знаете, когда он исчезнет... но если вы хотите использовать ИИ без цензуры для эффективной работы и в долгосрочной перспективе, обратите внимание на abiteration large v2 (это требует больших затрат).

Original post on Exploit

Source: ZeroFox Intelligence

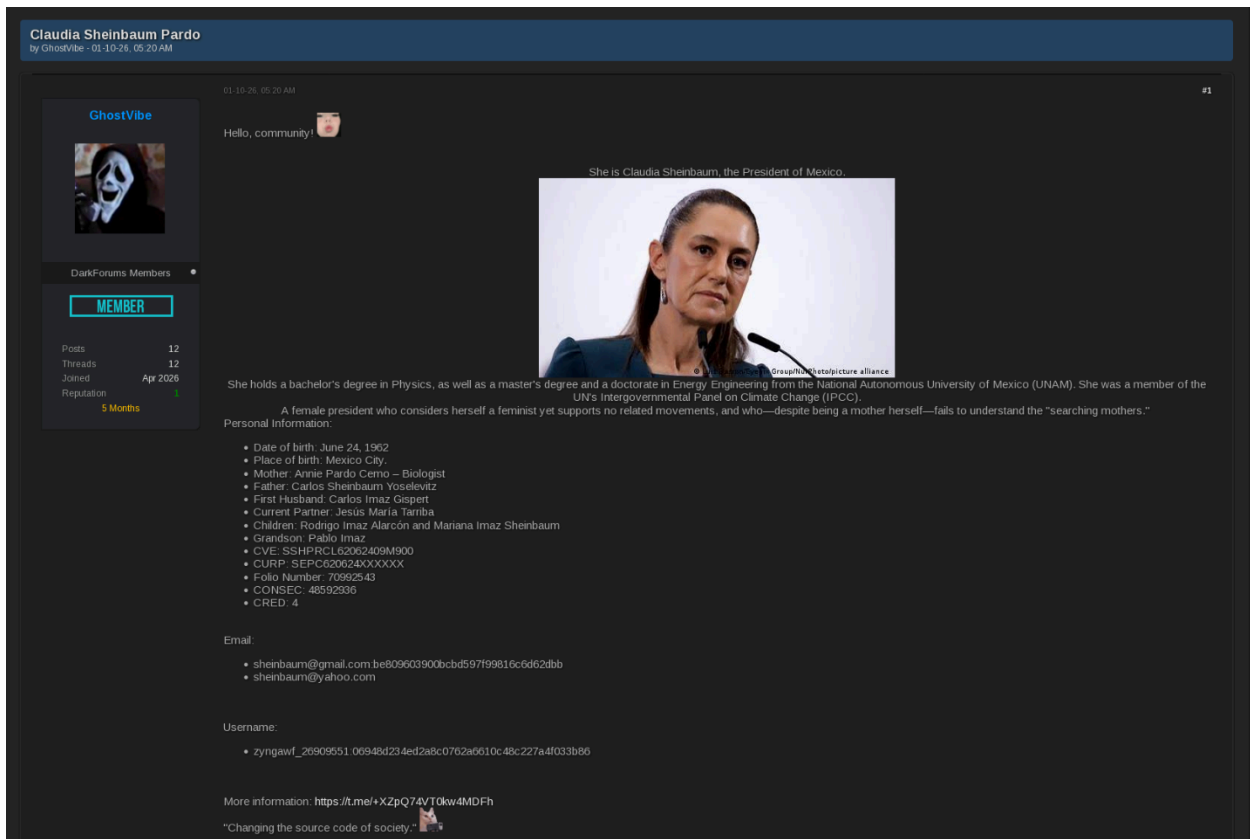
Threat Actor Published Alleged PII on Political Figures

On October 1, 2026, untested threat actor "GhostVibe" published data alleged to be personally identifiable information (PII) belonging to Mexican President Claudia Sheinbaum on the dark web community DarkForums. Records displaying email addresses, a username, a date and place of birth, relatives and partners, and public employee institutional identifiers are present within the post.

- GhostVibe stated that the president considers herself as a feminist but fails to support related movements and to recognize "searching mothers," a grassroots

network of women in Mexico who independently investigate mass graves, prisons, and terrain to find their lost relatives.

- The threat actor's claims suggest that they are ideologically motivated. GhostVibe has published seven additional doxxes, all sharing a similar format, affecting Mexican officials, businessmen, and a lawyer—all with threat actor commentary detailing ideological reasons for doxxing the targets.



The screenshot shows a forum post titled "Claudia Sheinbaum Pardo" by user "GhostVibe" on the "DarkForums" platform. The post includes a profile picture of a person in a white mask and a "MEMBER" badge. The main content of the post is a doxxing of Claudia Sheinbaum Pardo, the President of Mexico. It features a photograph of her and a detailed list of personal information, including her date of birth, place of birth, family members, education, and various identification numbers. The post also includes a brief biography and a list of email addresses and a username associated with her. The post is dated 01-10-26, 05:20 AM.

Claudia Sheinbaum Pardo
by GhostVibe - 01-10-26, 05:20 AM

01-10-26, 05:20 AM #1

GhostVibe
Hello, community!

She is Claudia Sheinbaum, the President of Mexico.

She holds a bachelor's degree in Physics, as well as a master's degree and a doctorate in Energy Engineering from the National Autonomous University of Mexico (UNAM). She was a member of the UN's Intergovernmental Panel on Climate Change (IPCC).

A female president who considers herself a feminist yet supports no related movements, and who—despite being a mother herself—fails to understand the “searching mothers.”

Personal Information:

- Date of birth: June 24, 1962
- Place of birth: Mexico City
- Mother: Annie Pardo Cemo – Biologist
- Father: Carlos Sheinbaum Yoselevitz
- First Husband: Carlos Imaz Gispert
- Current Partner: Jesus Maria Tariba
- Children: Rodrigo Imaz Alarcón and Mariana Imaz Sheinbaum
- Grandson: Pablo Imaz
- CVE: SSHPRCL62062409M900
- CURP: SEPC620624XXXXXX
- Folio Number: 70992543
- CONSEC: 48592936
- CRED: 4

Email:

- sheinbaum@gmail.com
- be809603900bcd597f99816c6d62dbb
- sheinbaum@yahoo.com

Username:

- zynqawf_29509551_06948d234ed2a8c0762a6510c48c227a4f033b86

More information: <https://t.me/+XZpQ74VT0kw4MDFh>

“Changing the source code of society.”

GhostVibe's post on DarkForums

Source: ZeroFox Intelligence

The threat actor is unvetted, and there is a roughly even chance the data posted is publicly available. GhostVibe is almost certainly motivated by ideology and is likely attempting to embarrass the president or draw attention to the cause of “searching mothers.” Politicians will almost certainly remain a highly sought after target for PII discovery and exploitation.

| Threat Actor Offers Alleged Zimbra Exploit for USD 15,000

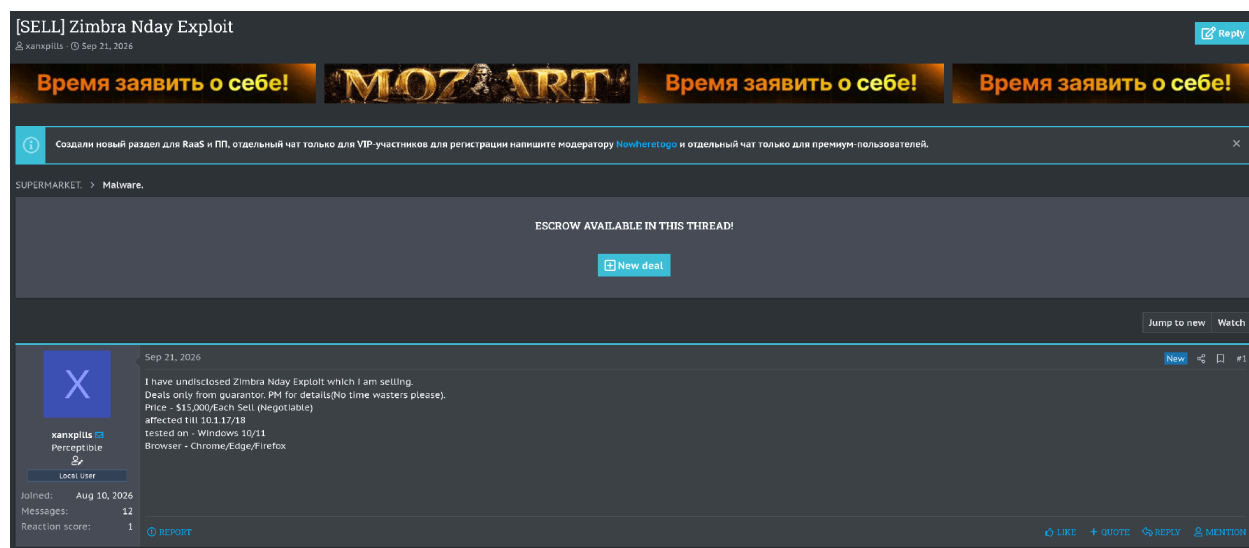
On September 21, 2026, untested threat actor “xanxpills” advertised an undisclosed “N-day” exploit in open-source email and collaboration platform Zimbra for USD 15,000 on the dark web forum ReHub. An N-day exploit targets a known vulnerability for which patches are typically available but remain unpatched on victim systems. The actor claimed the exploit affects Zimbra versions up to 10.1.17/18; was tested on Windows 10/11 using Chrome, Edge, and Firefox; and that transactions would be conducted through a guarantor.

- The advertisement provided no technical details, vulnerability identifier, proof-of-concept, or evidence demonstrating the exploit's capabilities. The actor said the price was negotiable.
- The alleged exploit does not claim to affect the latest available versions of Zimbra. Zimbra 10.1.20 was released in July 2026, and 10.1.21 was released on September 24—three days after the advertisement.
- Zimbra has a sustained history of targeting by financially and politically motivated actors, including the exploitation of zero-day vulnerabilities by espionage groups in 2023,² mass exploitation of CVE-2024-45519 in 2024,³ and continued exploitation by Russian state-supported actor LAUNDRY BEAR in 2025–2026.⁴ Successful exploitation of Zimbra is likely to result in sensitive data theft, including emails and personnel data of an organization.

² [hXXps://www.cisa\[.\]gov/news-events/cybersecurity-advisories/aa22-228a](https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-228a)

³ [hXXps://www.hipaajournal\[.\]com/critical-zimbra-flaw-being-mass-exploited/](https://www.hipaajournal[.]com/critical-zimbra-flaw-being-mass-exploited/)

⁴ [hXXps://www.cisa\[.\]gov/news-events/cybersecurity-advisories/aa26-204a](https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-204a)



Threat actor advertises alleged Zimbra exploit

Source: ZeroFox Intelligence

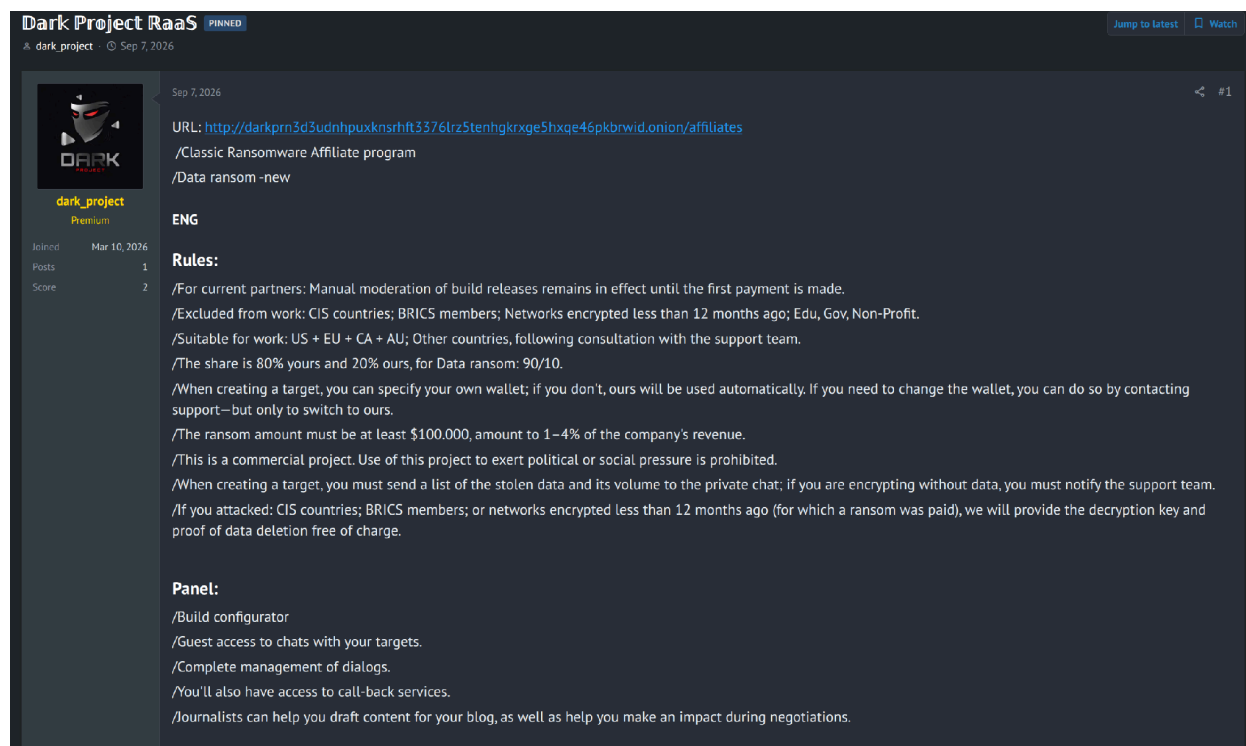
Despite Zimbra's history of high-impact exploitation, xanxpills' lack of both technical evidence and credibility make the advertised exploit's legitimacy uncertain. The actor has limited activity on ReHub, with only one other post seeking information on SmartScreen bypass techniques.

- If the actor's claim about the N-day exploit and affected versions is accurate, the underlying vulnerability likely already has a patch and may have a publicly available or independently developed proof-of-concept (PoC). However, this cannot be verified because the specific vulnerability has not been disclosed.
- There is a roughly even chance that the advertised tool is instead a readily available exploit chain that has already been tested across relevant platforms, reducing the need for additional testing or development by the buyer.

Collective Announces New RaaS Offering

On September 7, 2026, the well-regarded ransomware collective Dark Project RaaS announced its presence on two active dark web forums focused on ransomware partnerships: ReHub and TlerOne. The ransomware group is not new and has reportedly been involved in multiple cyberattacks.

- The group began operating in August 2026 and has already published data belonging to 26 victim organizations.



Dark Project RaaS post on Tier1

Source: ZeroFox Intelligence

Based on the group's synopsis, the Dark Project RaaS offering does not differ significantly from other ransomware-as-a-service (RaaS) operations. However, the operators have established explicit requirements and conditions that are mandatory for all partners using their ransomware. Partners are required to obtain a minimum ransom payment of USD 100,000 from each victim, with the ransom amount expected to represent approximately 1–4 percent of the victim organization's annual revenue. This requirement indicates that the RaaS is almost certainly targeting organizations with annual revenues exceeding USD 10 million.

- The operators exclude Commonwealth of Independent States (CIS) countries, BRICS member-states, educational institutions, government entities, and non-profit organizations from targeting.

- They identify the United States, European Union, Canada, and Australia as preferred target regions, while operations against organizations in other countries require prior consultation with the support team.

The RaaS operates on an 80/20 revenue-sharing model, with partners receiving 80 percent of ransom proceeds and Dark Project RaaS receiving 20 percent. For data-only extortion, the stated split is 90/10 in favor of partners. Partners can specify their own cryptocurrency wallet when creating a target; however, wallet changes are restricted and require contacting the support team, with changes apparently limited to switching to Dark Project RaaS' wallet.

Based on information provided by the threat actor, Dark Project RaaS is very likely a competent, well-structured RaaS operation. They almost certainly have defined partner requirements, financial thresholds, geographic targeting restrictions, and a relatively broad set of ransomware capabilities across enterprise environments. All of these factors very likely make Dark Project RaaS a viable threat that will almost certainly conduct ransomware attacks in the near future.

| 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%

| Appendix C: ZeroFox Intelligence Threat Actor Reputation Scale

Untested	Moderately Credible	Well-regarded	Prominent
Has garnered no reputation; credibility cannot be determined.	Has made up to 10 transactions; has been active on forum for at least three months.	Has at least 10 transactions; has been active on forum for three months to one year.	One of the most well-known and credible threat actors on the site; long-term, established presence on the forum of more than one year.