ZEROFOX INTELLIGENCE

# Profile

## The Gentlemen

P-2026-05-07a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Threat Actor, Ransomware, Dark Web

May 7, 2026


# | Profile | The Gentlemen

**Created on:** May 6, 2026
**Intelligence Cut-off**: 10:00 AM (EDT) on May 5, 2026

## | Key Findings

- The Gentlemen is a ransomware-as–service (RaaS) collective active since at least September 2025 that publishes victim data on its dark web-hosted blog. As of April 2026, The Gentlemen has conducted at least 346 attacks, averaging 43 per month.
- The Gentlemen is almost certainly financially motivated; neither its dark web leak site nor its public statements on dark web forums, social media, or covert communication channels indicate any political stance, ideological messaging, or affiliation with a specific cause.
- The Gentlemen employs a double extortion model with a silent encryption mode, as indicated by the file encryptions and ransom notes in confirmed attacks. The group actively solicits initial access brokers (IABs) for Virtual Private Networks (VPNs) and botnets and purchases targets' data from infostealer logs.
- The collective's target pool has included a national human rights institute, a university, and the healthcare sector, suggesting the group or its affiliates do not exclude public sector organizations despite their typically lower ransom-paying capacity.
- ZeroFox assesses that The Gentlemen is likely a technically mature threat actor group based on its observable Operations Security (OPSEC) posture, which presents a mixture of defensive security measures and credibility-driven self-exposure.

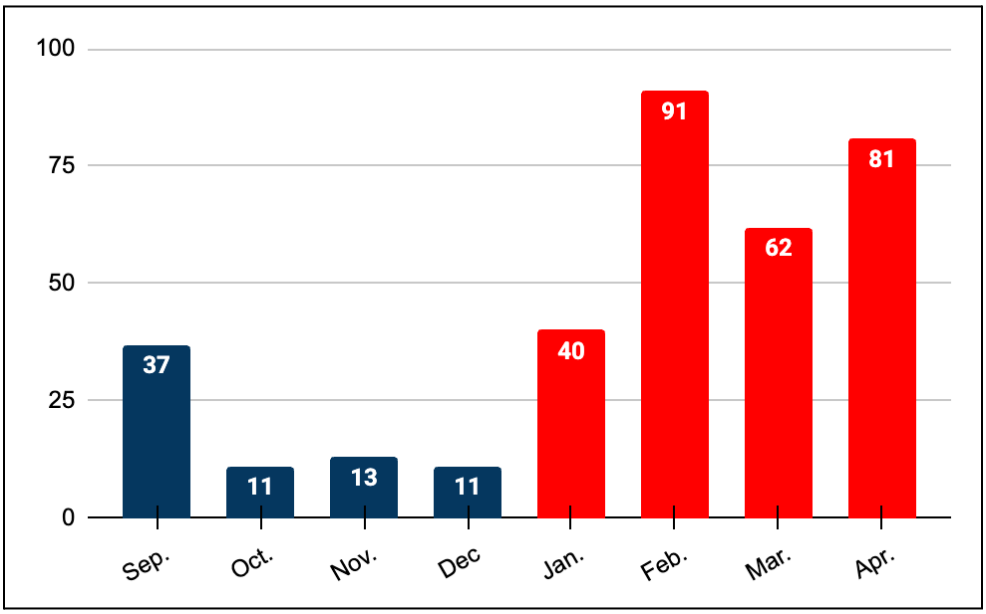
| | |
|---|---|
| **First Observed** | September 9, 2025 |
| **Origin** | Russian Federation/Commonwealth of Independent States (CIS) (high confidence) |
| **Alias** | N/A |
| **Motivation** | Financial gain |
| **Targeted Industries** | - Manufacturing<br>- Healthcare<br>- Professional services<br>- Financial services<br>- Technology<br>- Education |
| **Targeted Nations** | - Indonesia<br>- Thailand<br>- Philippines<br>- Malaysia<br>- United Kingdom<br>- Italy<br>- Spain<br>- Germany<br>- France<br>- Colombia<br>- Mexico<br>- Brazil<br>- Argentina<br>- United States<br>- Canada |
| **Tool** | Proprietary, custom-built ransomware |
| | Note: This list should not be treated as exhaustive. |

**The Gentlemen overview**

*Source: ZeroFox Intelligence*

## History

The Gentlemen is a RaaS collective active since at least September 2025 that publishes victim data on its dark web-hosted blog. Since claiming its first attack, the collective has remained consistently active. As of April 2026, The Gentlemen has conducted at least 346 attacks, averaging 43 per month.

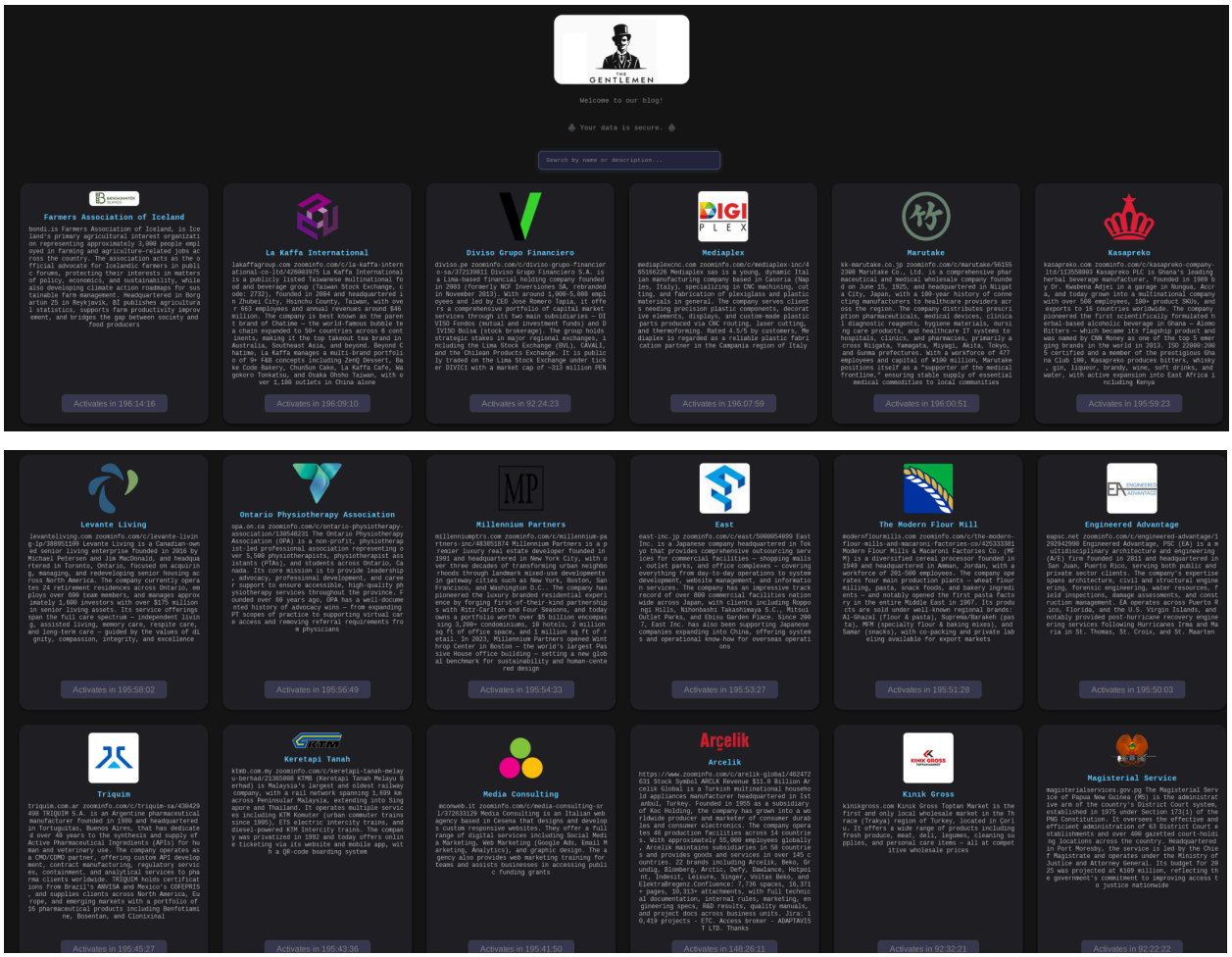



**The Gentlemen's incidents per month (September 2025–April 2026)**

*Source: ZeroFox Intelligence*

- The Gentlemen claimed its first known victim on September 9, 2025. In February 2026, the collective began publicly advertising its affiliate program, placing operational onset approximately five months before public affiliate recruitment began.
- The group operates a dedicated Tor-based leak site and has advertised its affiliate program on at least two Russian-language dark web forums (T1erOne and Rehub). As of writing, the group's leak site and any clearnet mirrors were occasionally inaccessible, likely indicating limited online persistence capabilities.
- The Gentlemen's forum posts and its affiliate communications are written in Russian. The group explicitly prohibits attacks targeting CIS countries, a

long-standing convention among Russian-language cybercriminals to avoid domestic law enforcement exposure.




**Victims added to The Gentlemen's leak site on May 5, 2026**

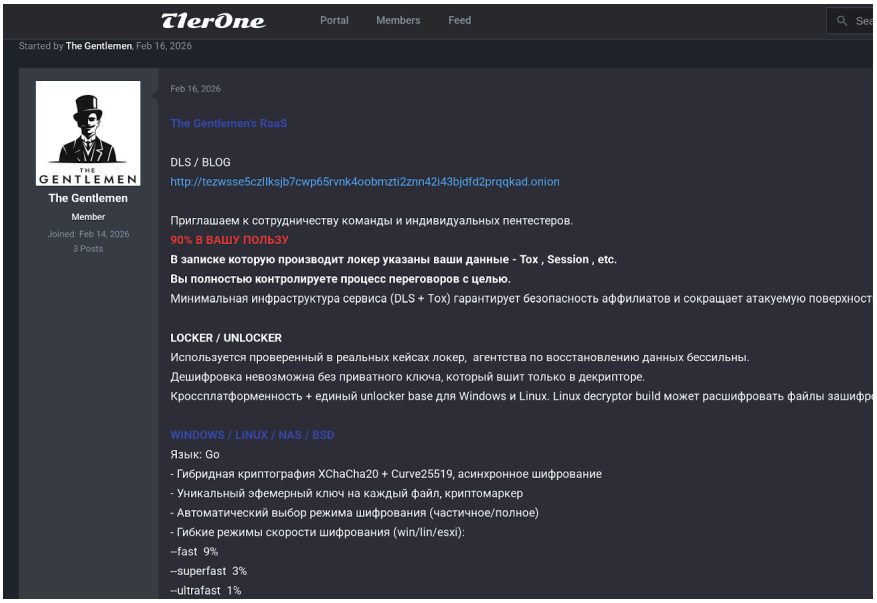
*Source: ZeroFox Intelligence*

## Motivations and Victim Profile

The Gentlemen is almost certainly financially motivated; neither its dark web leak site nor its public statements on dark web forums, social media, or covert communication channels such as Telegram indicate any political stance, ideological messaging, or affiliation with a specific cause. The collective's CIS exclusion clause is likely, and conventionally interpreted as, aimed toward risk management rather than an ideological statement.

- The collective's RaaS model is almost certainly consistent with profit-driven criminal activity and includes a 90/10 percent revenue split in favor of the affiliates, a USD 1,500 onboarding deposit refunded after first successful payment, and a stated willingness to purchase access from IABs on a percentage-of-ransom basis.
- As of April 2026, The Gentlemen updated its offer to a 97/3 percent split (affiliate/operator) for data-only targets (exfiltration without encryption), likely to adapt to market conditions and attract affiliates who prefer lower operational risk.

The group has compromised organizations across multiple countries and sectors. The collective's target pool includes a national human rights institute, a university, and the healthcare sector (including hospitals and provider clinics); this suggests the group (or its affiliates) does not exclude public sector organizations despite their typically lower ransom-paying capacity and likely indicates The Gentlemen's disregard for ethical hygiene.




**The Gentlemen's original recruitment post on T1erOne, dated February 16, 2026. The listed features include dedicated leak site (DLS) link, 90/10 affiliate split, locker/unlocker decryption, and Windows/Linux/NAS/BSD platform list with Go-based encryptor details.**
*Source: ZeroFox Intelligence*

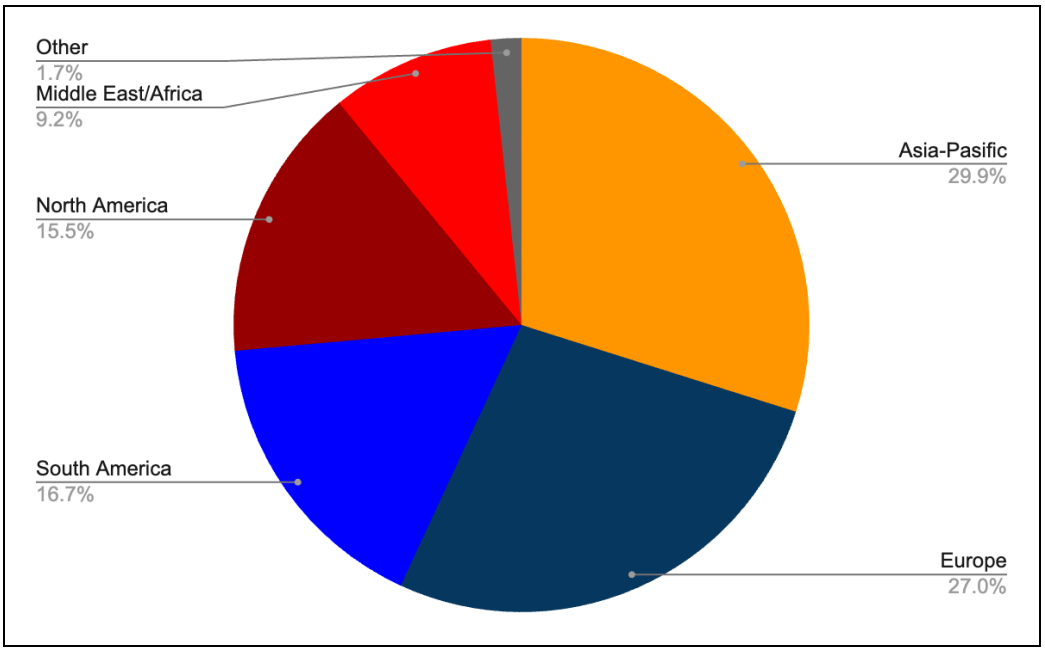
The Gentlemen targets victims across a wide range of industries, with a notable concentration in the following sectors:

- Manufacturing
- Healthcare
- Professional services
- Financial services
- Technology
- Education

Additional affected sectors include:

- Government or public sector
- Retail
- Transport
- Energy

Geographically, the majority of The Gentlemen's victims span South East Asia, including Indonesia, Thailand, Philippines, and Malaysia. The group has also targeted organizations operating in Western Europe, predominately in the United Kingdom, Germany, Spain, France, and Italy. In addition, The Gentlemen's victims have been identified across regions in South America, North America, the Middle East, and Africa, indicating a very broad global targeting scope.



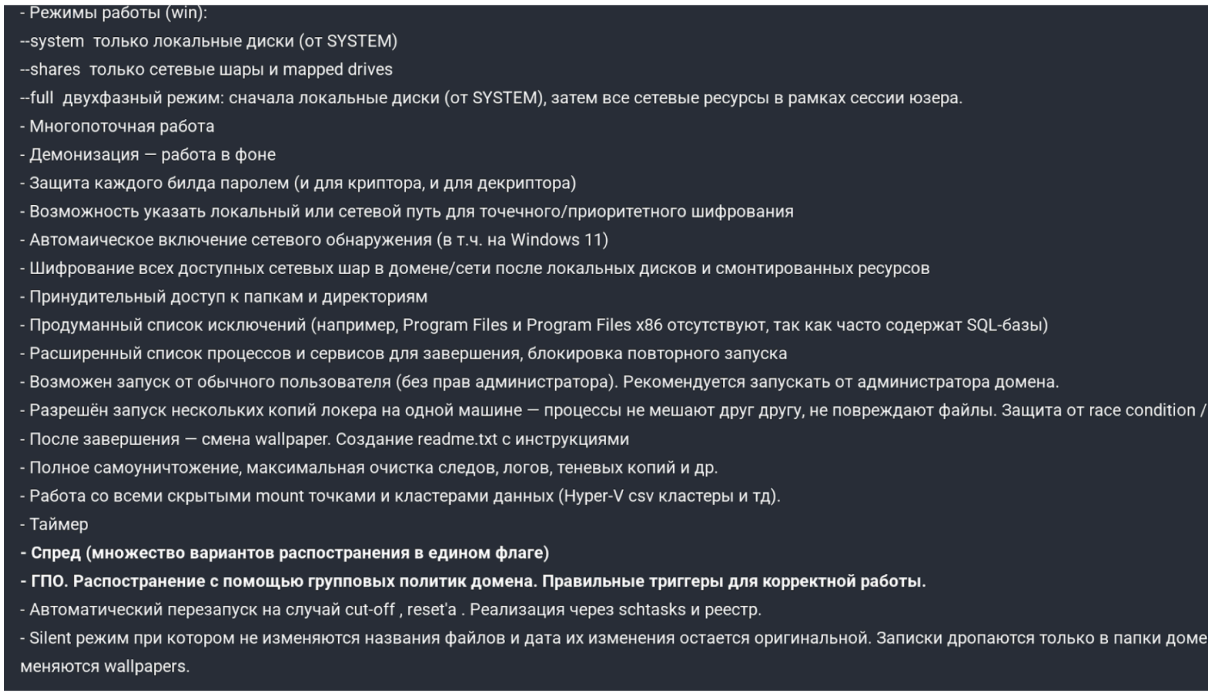

**The Gentlemen's incidents by region**

*Source: ZeroFox Intelligence*

## Tactics, Techniques, and Procedures (TTPs)

The Gentlemen employs a double extortion model with a silent encryption mode, as indicated by the file encryptions and ransom notes in confirmed attacks. The group actively solicits IABs for VPNs and botnets and purchases targets' data from infostealer logs—likely indicating its systematic use of credential markets as its sourcing channel.

- The double extortion approach involves both encrypting the victim's files and exfiltrating sensitive data from compromised systems. Victims are provided with instructions on how to initiate contact with the group to negotiate ransom payment.
- The Gentlemen claims that the silent encryption mode enables the following capabilities: file names and time stamps are unchanged, ransom notes are dropped only in domain and local admin folders, and wallpapers are not changed. Notably, ZeroFox has not observed this same evasion approach in competing RaaS offerings.




**The Gentlemen's T1erOne thread (Part 2). The listed features include, but are not limited to, operating modes, process kill list, silent encryption mode, and self-deletion.**
*Source: ZeroFox Intelligence*

Exfiltrated data is hosted on The Gentlemen's dedicated leak site or, per its affiliate terms, uploaded to a public cloud or agreed resource prior to encryption. The operator offers spam-to-inbox delivery to corporate mailboxes with open tracking and phone-based victim contact, with call recordings provided; the group likely runs or contracts out a multi-channel extortion support service.

- The group appears to utilize a disclosure delay, as observed in confirmed attacks; this likely serves as a deliberate hold period during negotiations before data is made public, which is consistent with extended re-extortion attempts prior to posting any data.
- However, the use of double extortion ensures that victims remain exposed even if they independently restore their systems or recover encrypted files through backups. If the ransom demand is not paid, The Gentlemen maintains the ability to publish the illicitly obtained data on its dark web blog.

## Operational Security

ZeroFox assesses that The Gentlemen is a technically mature threat actor group based on its observable OPSEC posture, which presents a mixture of defensive security measures and credibility-driven self-exposure. All affiliate contact is handled entirely through Tox, ransom note metadata includes only affiliate-controlled contact data (Tox and Session), and the infrastructure surface is deliberately minimal.

- The Gentlemen claim that its USD 1,500 affiliate deposit and the requirement to provide a pre-encryption target date before receiving a build are countermeasures against law enforcement infiltration.
- This likely indicates the collective's awareness of defensive measures for OPSEC and enables the group to frame these efforts as a security feature for affiliates.

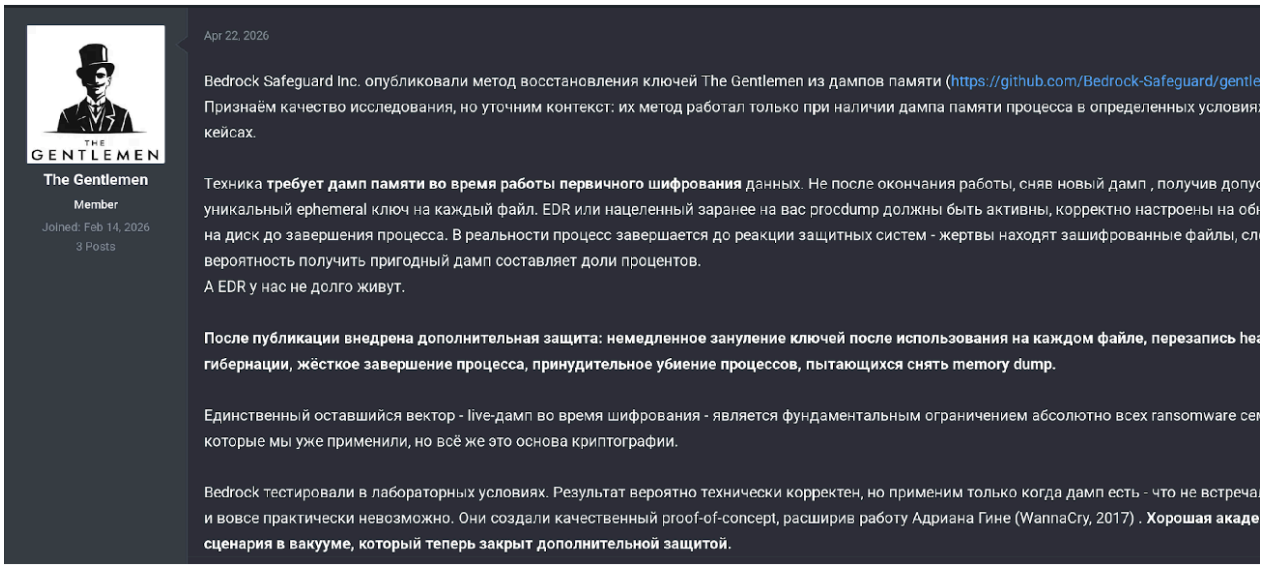
However, The Gentlemen has also self-linked to three clearnet security vendor reports and a ransomware tracking aggregator within its public advertising post. While this is likely intended to signal credibility to prospective affiliates, it reduces the group's obscurity and confirms that the actors monitor or are aware of their own public coverage.

- As of writing, the group's leak site and any clearnet mirrors were occasionally inaccessible, likely indicating limited online persistence capabilities that can be attributed to instability, takedown activity, or routine maintenance.

In the beginning of April, a Bedrock Safeguard decryptor publication surfaced as the first known public decryptor for The Gentlemen's ransomware—which was reportedly assessed as cryptographically unbreakable prior to the publication.

- On April 22, 2026, The Gentlemen publicly responded to the publication of the Bedrock Safeguard decryptor—a significant and observable OPSEC event from the group.
- The Gentlemen's issued a timely, technically detailed rebuttal and deployed a same-day defensive patch. This indicates the collective's development cycle is, and will very likely continue to be, responsive to cybersecurity researchers, which

has direct implications for the durability of any recovery tooling developed against The Gentlemen's ransomware family.




**The Gentlemen's response to Bedrock Safeguard decryptor and announcement of defensive patch with details of updated features**

*Source: ZeroFox Intelligence*

## 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 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% |