ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 15

B-2025-08-01a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Threat Actor, Deep and Dark Web

August 1, 2025

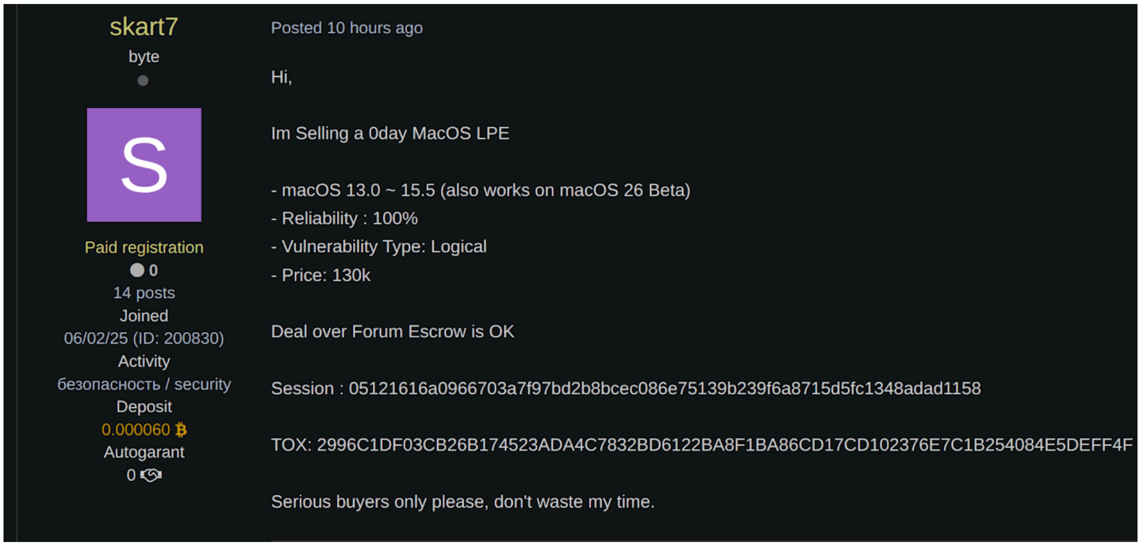
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 August 1, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 15

| MacOS LPE Zero-Day Vulnerability Advertised for Sale

On July 22, 2025, untested threat actor "skart7" posted in the dark web forum Exploit, advertising the sale of a zero-day Local Privilege Escalation (LPE) vulnerability for Apple's macOS for USD 130,000. Skart7 stated the alleged vulnerability is a logical flaw affecting macOS versions 13.0 to 15.5, including macOS beta releases, and asserted it has 100 percent reliability. The actors also specified that escrow payments would be accepted.

- Skart7 joined the Exploit forum in June 2025 and has yet to garner significant credibility within the forum. The actor has previously advertised various other zero-day vulnerabilities for sale on Exploit, with prices ranging from USD 30,000 to USD 130,000.
- While some forum members have displayed interest in skart7's previous advertisements, negotiations reportedly broke down over disputes regarding who would cover the escrow fee on Exploit.



skart7
byte

Paid registration
● 0
14 posts
Joined
06/02/25 (ID: 200830)
Activity
безопасность / security
Deposit
0.000060 ₿
Autogarant
0

Posted 10 hours ago

Hi,

Im Selling a 0day MacOS LPE

- macOS 13.0 ~ 15.5 (also works on macOS 26 Beta)
- Reliability : 100%
- Vulnerability Type: Logical
- Price: 130k

Deal over Forum Escrow is OK

Session : 05121616a0966703a7f97bd2b8bcec086e75139b239f6a8715d5fc1348adad1158

TOX: 2996C1DF03CB26B174523ADA4C7832BD6122BA8F1BA86CD17CD102376E7C1B254084E5DEFF4F

Serious buyers only please, don't waste my time.

skart7's Exploit post

ZeroFox Intelligence

Such a vulnerability has the potential to enable broader attack chains, allowing threat actors to disable security controls, gain deeper access into targeted systems, and possibly turn a single compromised endpoint into a foothold for long-term exploitation.

- Although LPE flaws require local access, they remain valuable in multi-stage attacks where initial access has already been gained, enabling privilege escalation, persistence, or lateral movement within macOS environments.
- The decision to list the macOS LPE vulnerability on a public forum like Exploit, rather than through vetted private brokers, is likely due to an urgency to monetize before the vulnerability is patched.
- Given that the vulnerability reportedly impacts beta versions too, it could pose a risk to software hobbyists—particularly Apple enthusiasts.

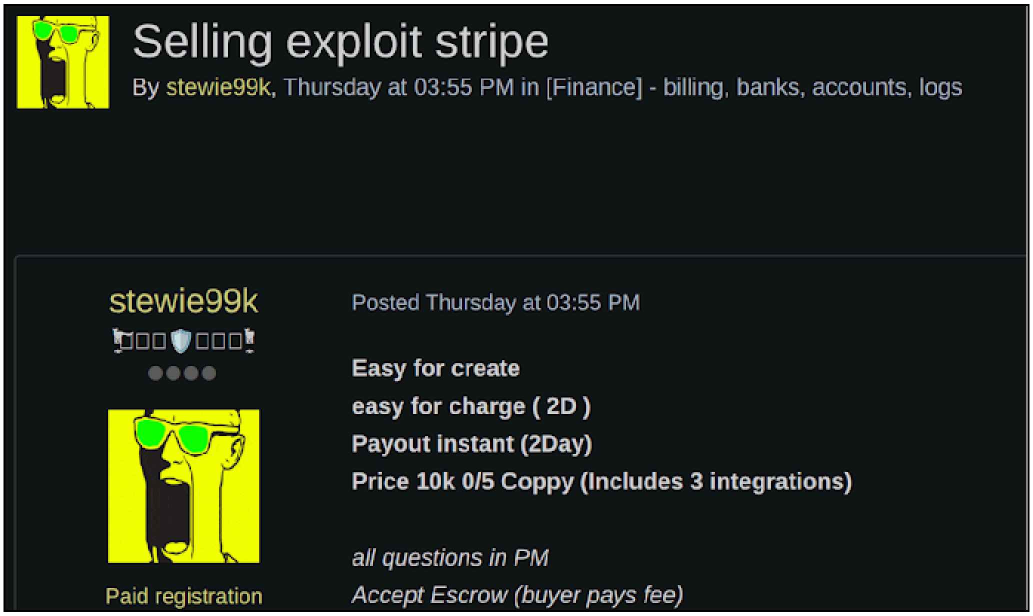
As of the writing of this report, the advertisement has been removed for unknown reasons; it is likely that potential buyers have privately reached out via Tox and Session as directed by skart7. The post likely generated interest from financially motivated threat actors seeking reliable LPE vulnerabilities to deploy information stealers or maintain persistence on high-value macOS systems. Such exploits can enable them to bypass user-level restrictions, escalate privileges, and monetize access through extortion, data theft, or resale on underground markets.

Stripe Exploit Advertised for Sale on Dark Web Forum

On July 17, 2025, an actor known as “stewie99k” posted on the dark web forum Exploit, advertising the sale of a vulnerability related to Stripe. According to the actor, the vulnerability enables potential buyers to charge two-dimensional cards, with payment processed within two days. Stewie99k provided no further details surrounding the nature of the vulnerability but specified that there are five copies available that can be purchased via escrow for USD 10,000 each.

- Stewie99k joined Exploit in February 2023 and has since established a positive reputation in the forum.
- There are two primary types of payment gateways: two-dimensional (2D) and three-dimensional (3D). 2D payment gateways typically only require a card number, expiration date, and card verification value (CVV) to process payments. 3D payment gateways usually require an extra security measure to process payments, such as a one-time-password (OTP) or biometric verification. As such, 2D payment gateways are more susceptible to fraudulent activity.
- Stripe is an Irish-American online payment processing platform and financial infrastructure company that reportedly processed USD 1.4 trillion in 2024.[1] As of February 2025, Stripe was reportedly used by half of the organizations listed in the Fortune 100, 80 percent of the Forbes Cloud 100, and 78 percent of the Forbes AI 50.[2]

[1] hXXps://stripe[.]com/newsroom/news/stripe-2024-update
[2] *Ibid*.



Selling exploit stripe

By stewie99k, Thursday at 03:55 PM in [Finance] - billing, banks, accounts, logs

stewie99k

Paid registration

Posted Thursday at 03:55 PM

Easy for create
easy for charge (2D)
Payout instant (2Day)
Price 10k 0/5 Coppy (Includes 3 integrations)

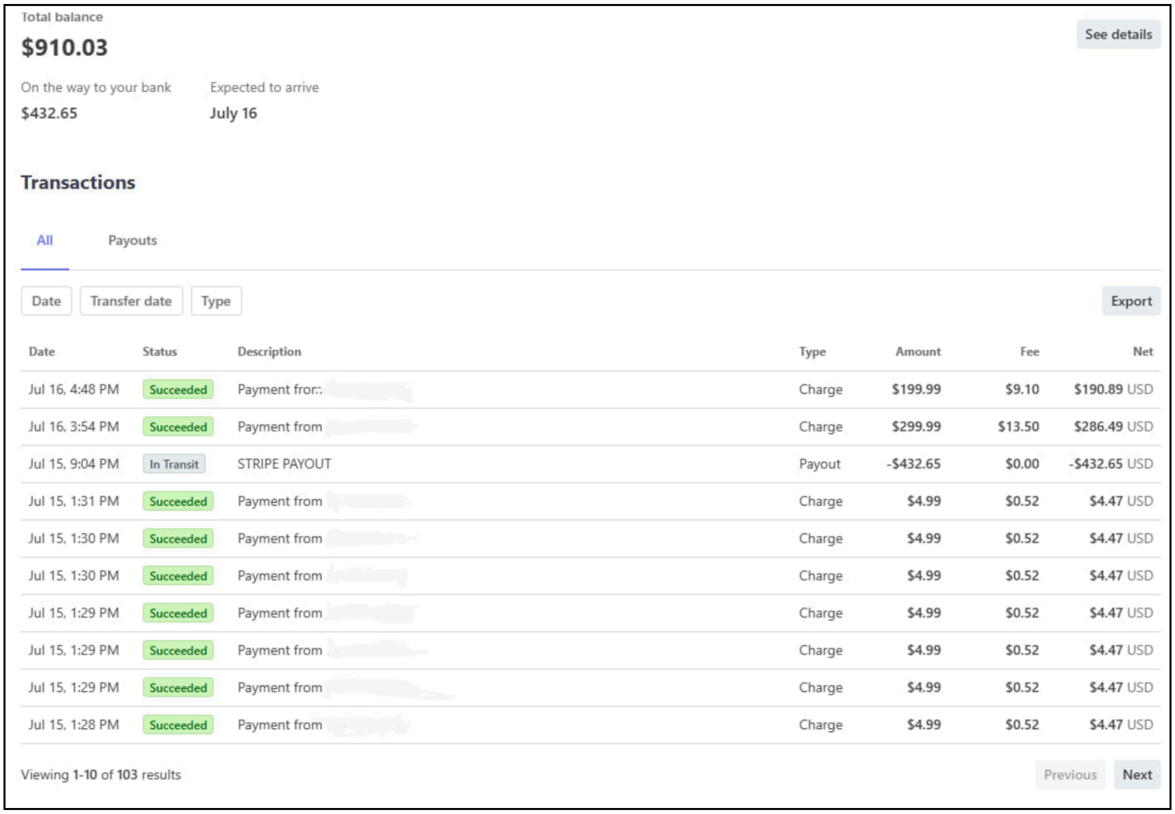
all questions in PM
Accept Escrow (buyer pays fee)

stewie99k's Exploit post

ZeroFox Intelligence

In the post, stewie99k shared several images of what appear to be successful Stripe payment gateway transactions, which have likely been conducted using compromised payment details. The actor outlined that potential buyers would need the following information to successfully exploit the vulnerability:

- A "bank drop", which typically refers to a bank account (sometimes a fake or stolen one) that is used as a temporary destination for fraudulent funds.
- Compromised personally identifiable information (PII) of a U.S. citizen—including name, address, and Social Security number (SSN)—which are very likely required by potential buyers to open a Stripe account and connect to the desired merchant.



Total balance

$910.03

On the way to your bank
$432.65

Expected to arrive
July 16

Transactions

Date	Status	Description	Type	Amount	Fee	Net
Jul 16, 4:48 PM	Succeeded	Payment fro [redacted]	Charge	$199.99	$9.10	$190.89 USD
Jul 16, 3:54 PM	Succeeded	Payment from [redacted]	Charge	$299.99	$13.50	$286.49 USD
Jul 15, 9:04 PM	In Transit	STRIPE PAYOUT	Payout	-$432.65	$0.00	-$432.65 USD
Jul 15, 1:31 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD
Jul 15, 1:30 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD
Jul 15, 1:30 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD
Jul 15, 1:29 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD
Jul 15, 1:29 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD
Jul 15, 1:29 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD
Jul 15, 1:28 PM	Succeeded	Payment from [redacted]	Charge	$4.99	$0.52	$4.47 USD

Viewing 1-10 of 103 results

Alleged successful Stripe transactions

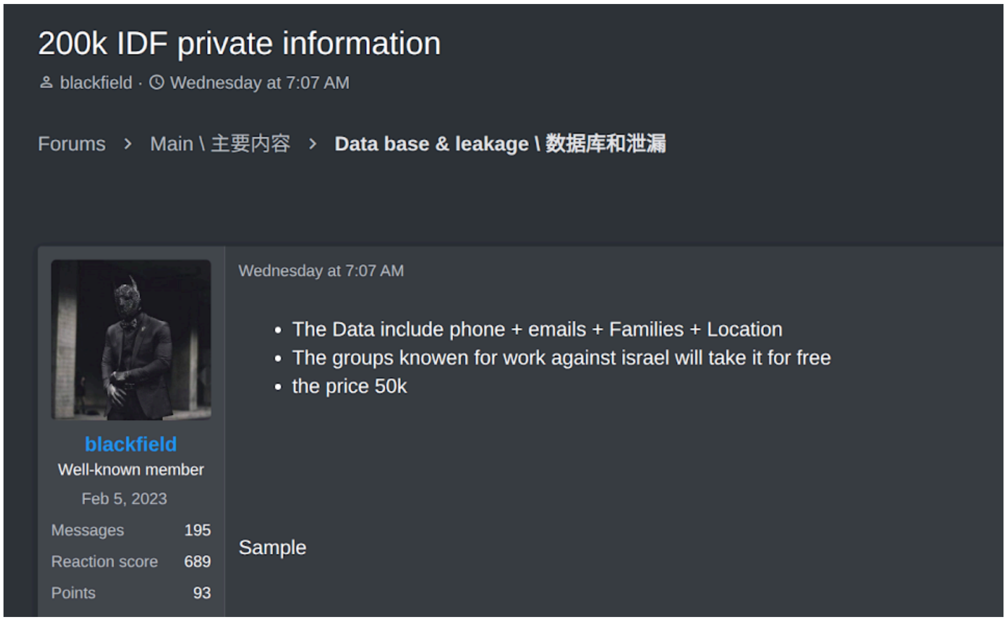
ZeroFox Intelligence

There is a roughly even chance that the vulnerability being advertised is legitimate, given the reputation of the seller. However, it is very likely that such a vulnerability, as advertised in the post, would have a short life span. Unauthorized payments are considered high-risk, and vulnerabilities enabling them are usually discovered and patched within days or even hours—especially if they are impacting an industry leader like Stripe.

PII Related to IDF Personnel Advertised for Sale

On July 16, 2025, the actor "blackfield" posted in the Russian-language dark web forum RAMP advertising the sale of PII associated with personnel of the Israeli Defense Forces (IDF). According to blackfield, the data set is available for USD 50,000 but will be provided for free to groups known to work against Israeli interests. The data set is allegedly comprised of 200,000 lines of PII, including:

- Names
- Phone numbers
- Email addresses
- Family information (very likely meaning information about the relatives of alleged IDF members, such as names and email addresses)
- Location details (very likely meaning the home addresses or military post locations of IDF members)


200k IDF private information

blackfield · Wednesday at 7:07 AM

Forums > Main \ 主要内容 > **Data base & leakage \ 数据库和泄漏**

blackfield
Well-known member
Feb 5, 2023

Messages	195
Reaction score	689
Points	93

Wednesday at 7:07 AM

- The Data include phone + emails + Families + Location
- The groups knowen for work against israel will take it for free
- the price 50k

Sample

blackfield's RAMP post

ZeroFox Intelligence

Blackfield included sample data in the post, which contained 54 lines of first and last names and accompanying email addresses of alleged IDF members. Notably, this sample did not include phone numbers, family information, or location details—likely because blackfield chose not disclose PII deemed more sensitive and valuable.

- Blackfield is part of the pro-Palestinian, anti-Israel hacktivist group Shadow, a collective responsible for numerous cyberattacks exclusively targeting Israeli infrastructure.
- The actor joined RAMP on February 5, 2023, where they have a "well-known member" reputation status.

- On March 15, 2025, blackfield announced on RAMP that they had gained access to sensitive documents associated with high-ranking IDF officers, Israeli political figures, and an Israel-based healthcare organization with an annual revenue of USD 1 billion.
- On April 1, 2025, blackfield posted on 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 PII.

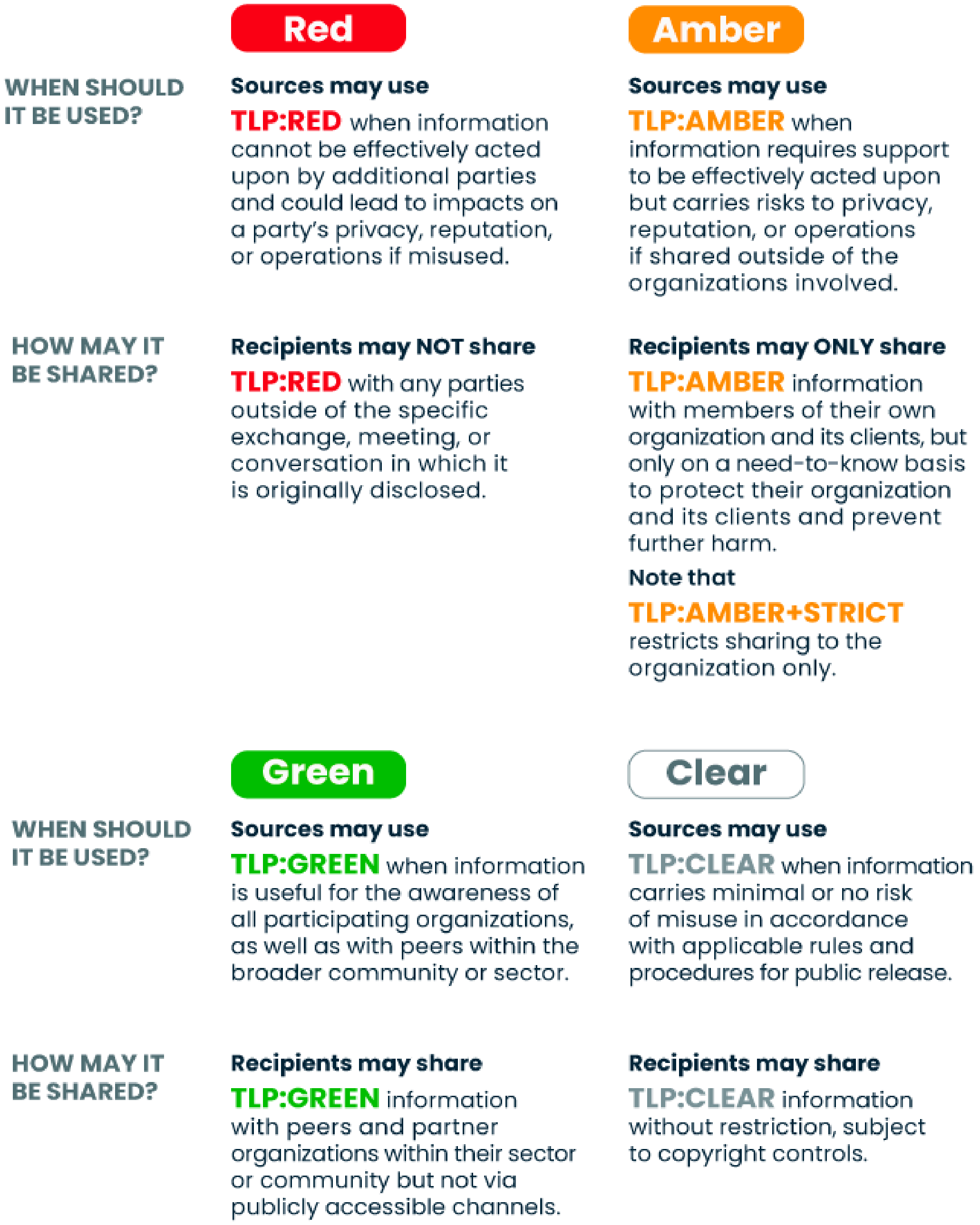
Like other pro-Palestinian hacktivist groups, blackfield displays an overt hostility towards Israel and Israeli-based entities, which almost certainly extends to allies such as the United States, European nations, the European Union (EU), the North Atlantic Treaty Organization (NATO), and the West in general. Future activity from blackfield is very likely to target those perceived as misaligned with the interests of Palestinian and Iranian entities. Despite the clear ideological motivation, blackfield very likely also seeks to simultaneously financially profit from their attacks.

The data set advertised is very likely genuine, based on blackfield's established reputation and similar past advertisements. The information advertised by blackfield almost certainly appeals primarily to other ideologically, politically, and financially motivated threat actors that would seek to leverage PII in disruption attacks, social engineering campaigns, or in the planning of physical targeting.

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

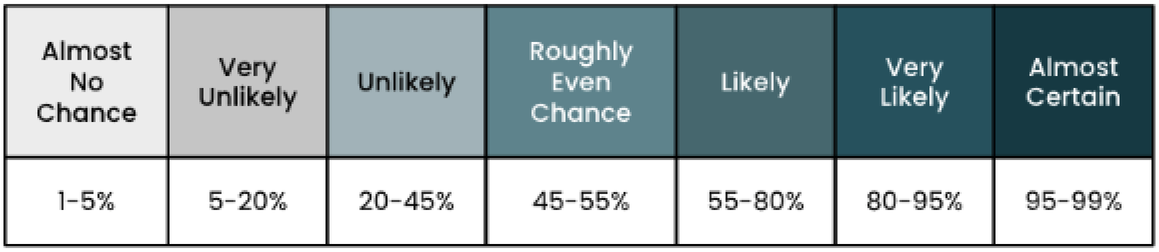


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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%