ZEROFOX INTELLIGENCE

Flash

Mobile Numbers Advertised for Sale in Dark Web Forum

F-2025-06-13b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Dark Web, Threat Actor, PII

June 13, 2025

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 June 13, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Mobile Numbers Advertised for Sale in Dark Web Forum

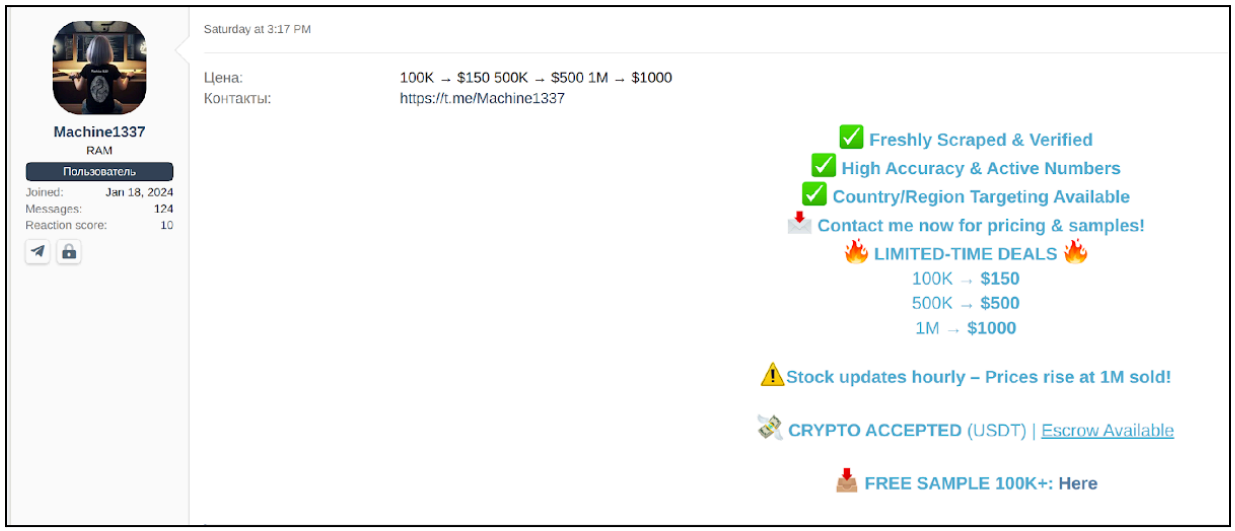
| Key Findings

- On June 7, 2025, the actor "Machine1337" posted on the predominantly Russian-speaking dark web forum xss, advertising the sale of mobile numbers from at least 20 companies.
- Machine1337 claimed that the mobile numbers are "freshly scraped and verified" and offered access to a free sample of the data in the post. It is unclear whether these numbers are associated with personal or corporate mobile phones.
- While access to phone numbers would not directly facilitate a cyberattack, it could enable an attacker to conduct various types of social engineering activity that can result in subsequent exploitation.
- The phone numbers could also be leveraged in the facilitation of various types of fraud activity—particularly if a buyer is able to enrich the data by correlating other types of personally identifiable information (PII) to the phone numbers.

Details

On June 7, 2025, the actor Machine1337 posted on the predominantly Russian-speaking dark web forum xss advertising the sale of mobile numbers from at least 20 companies. Machine1337 claimed that the mobile numbers are “freshly scraped and verified” and offered access to a free sample of the data in the post. It is unclear whether these numbers are associated with personal or corporate mobile phones.

- Machine1337 first registered on the xss forum in January 2024 and is a likely English-speaking threat actor. Based on their history, it is very likely that Machine1337 is or has been associated with several prominent threat actors, including, but not limited to, “IntelBroker” and “Zjj”.
- In October 2024, Machine1337 and IntelBroker were almost certainly involved in a prominent network breach of the U.S.-based digital communications organization Cisco.
- ZeroFox reported on previous Machine1337 activity earlier in June 2025, when the actor claimed responsibility on both xss and their Telegram channel for the breaches of at least seven technology companies based in the United States and China.[1]



Machine1337’s xss post

Source: ZeroFox Intelligence

[1] https://www.zerofox.com/intelligence/the-underground-economist-volume-5-issue-10/

Quantities of phone numbers are advertised for sale for the following costs: 100,000 for USD 150; 500,000 for USD 500; and one million for USD 1,000. Machine1337 shared the below list of 20 companies allegedly included in the data set, stating there were more but providing no further details:

- InDriver, a U.S.-based international ride-sharing company
- Yahoo, a U.S.-based web portal and search engine
- LinkedIn, an U.S.-based business and employment-oriented social network
- Sony, a Japan-based multinational conglomerate
- OLX, a Netherlands-based online market place
- EA, a U.S.-based video game company
- Gate, a Turkey-based cryptocurrency exchange
- Binance, a cryptocurrency exchange
- Facebook, a U.S.-based social media site
- TikTok, a U.S. and Singapore-based social media site
- Apple, a U.S.-based technology company
- Coinbase, a cryptocurrency exchange
- KuCoin, a Seychelles-based cryptocurrency exchange
- Snapchat, a U.S.-based social media site
- Microsoft, a U.S.-based technology company
- Bumble, a U.S.-based dating application
- Freelancer, an Australia-based freelancing and crowdsourcing marketplace
- PAYSAFE, an Austria-based e-commerce company
- Zoho, an India-based technology company
- Adobe, a U.S.-based software company

The origin of this data is unknown, though its advertisement represents a slight deviation in Machine1337's activity, given the actor is typically observed advertising information relating to a single victim organization.

While access to phone numbers would not directly facilitate a cyberattack, it could enable an attacker to conduct various types of social engineering activity that can result in subsequent exploitation. Financially motivated actors could use these phone numbers to conduct various types of phishing attacks, such as voice phishing (vishing) or SMS

phishing (smishing). Both methods can facilitate credential theft, account compromise, or business email compromise (BEC).

The phone numbers could also be leveraged to conduct various types of fraud activity. Should a buyer be able to enrich the data by correlating other types of PII to the phone numbers, they could carry out SIM-swapping attacks that ultimately lead to compromised communications.

Recommendations

- If a caller is unknown or unexpected, end the call and contact the organization they claim to be from via a phone number featured on an official website.
- Attempt to verify the identity of a caller. Legitimate organizations will expect this type of scrutiny and should offer sufficient verification.
- Malicious callers may pose security questions to increase their perceived authenticity. Do not divulge personal information until the caller's identity has been verified.
- Do not call a different number upon a caller's request. This number could be spoofed to increase perceived legitimacy.
- Deny an attacker's reliance upon victim engagement or curiosity. If an SMS message seems suspicious, do not engage.
- Ensure security software is installed and updated on mobile devices, helping to block malicious communications and preventing execution of harmful payloads.
- Be aware of multi-factor authentication (MFA) phishing. Attackers attempt to steal MFA tokens or verification information either by direct interception or by directing the victim toward a malicious web domain.
- Be aware of enticements, which may promise some form of reward for engaging with an enclosed link.

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%