



| Flash |

Actor Seemingly Claims Responsibility for Recent Breaches

F-2025-05-16b

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Threat Actor, Data Breach, Digital Extortion

May 16, 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 1:00 PM (EDT) on May 16, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Actor Seemingly Claims Responsibility for Recent Breaches

| Key Findings

- A prominent and well-regarded threat actor known as “Machine1337” (who is also known as “EnergyWeaponUser”) has claimed responsibility for at least seven recent cyberattacks within both the primarily Russian-speaking dark web forum xss and the actor’s Telegram channel.
- Posts by the actor alluded to unspecified data allegedly stolen from Apple Inc., Steam, Huawei, Temu, and Snapchat. While data samples were seemingly made available, forum users claim that they are not accessible.
- Separately, on May 15, 2025, the U.S.-based cryptocurrency exchange platform Coinbase released a statement acknowledging a recent breach that resulted in stolen customer data.
- On May 15, 2025, ZeroFox observed that Machine1337 posted a message on their Telegram channel that stated “CoinBase: Coming soon”. While this does not indicate Machine1337 is directly involved in the Coinbase compromise, it does suggest a possible connection between the actor and this recent breach incident, which has yet to be officially claimed by any threat actor or group.

Details

A prominent and well-regarded threat actor known as both Machine1337 and EnergyWeaponUser has claimed responsibility for at least seven recent cyberattacks within both the primarily Russian-speaking dark web forum xss and the actor's Telegram channel.

- Machine1337 is a likely English-speaking threat actor that first registered on the xss forum in January 2024. Based on the actor's history, it is likely that the actor is or has been associated with the prominent threat actors "Intelbroker" and "Zjj", as well as the hacker collective "CyberN*ggers".
- In October 2024, Machine1337 and Intelbroker were almost certainly involved in a prominent network breach of the U.S.-based digital communications organization Cisco.
- As of the writing of this report, Machine1337 has been banned from xss for seven days ending May 22, 2025. According to a moderator notice, the account was banned for "spam activity" following several posts.



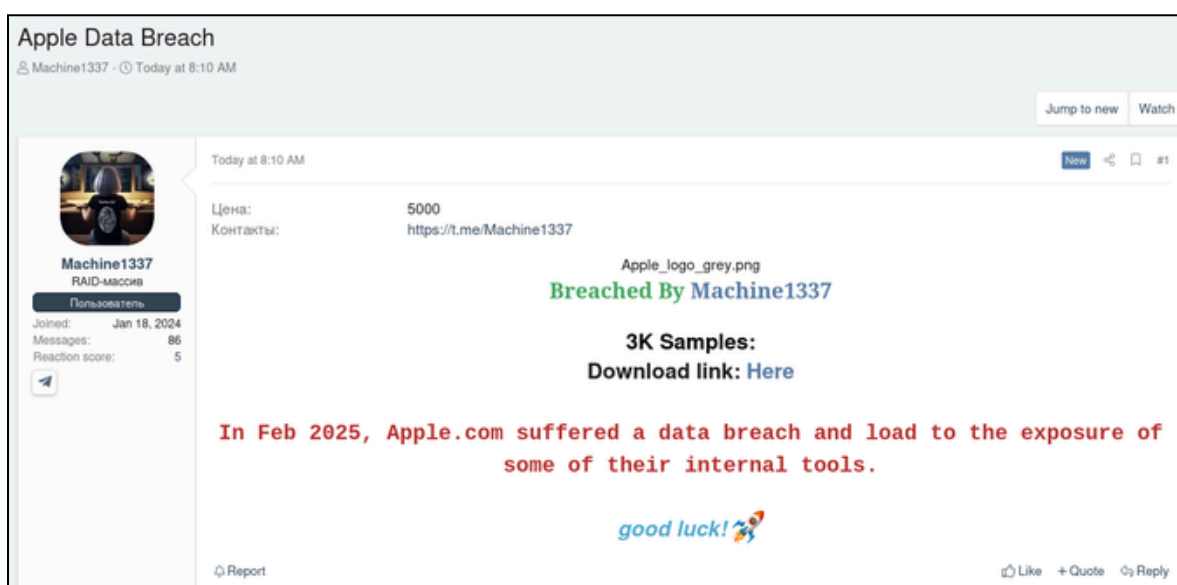
Moderator notice on Machine1337's xss profile

Source: ZeroFox Intelligence

On May 14, 2025, Machine1337 posted in xss, claiming to have obtained data stolen from numerous technology companies based in the United States and China. According to the actor's post, the breaches vary in extent and the type of data stolen, with limited

samples made available. All of the alleged breaches seemingly took place between February and May 2025.

The actor alleged that the U.S.-based technology giant Apple Inc. suffered a “data breach and load to the exposure of some of their internal tools.” The extent of the breach is not specified, though Machine1337 provided a link to a supposed data sample of 3,000 records. The post gained minimal traction in the xss forum, and some users reported that the link provided to sample data does not function. The allegedly stolen data is available for a purchase price of USD 5,000.



Machine1337's xss advertisement of alleged Apple Inc. compromise

Source: Zerofox Intelligence

U.S.-based technology organization Steam allegedly suffered a data breach comprising 89 million user records, one-time access codes, and user phone numbers, which is also available for USD 5,000.¹ Steam issued a statement claiming that the stolen data cannot be linked to other personally identifiable information (PII) and that the breach remains under investigation.² Machine1337's post gained some traction from fellow xss users, many of whom are claiming the sample data is inaccessible.

¹

[hXXps://www.bleepingcomputer\[.\]com/news/security/twilio-denies-breach-following-leak-of-alleged-steam-2fa-codes/](https://www.bleepingcomputer.com/news/security/twilio-denies-breach-following-leak-of-alleged-steam-2fa-codes/)

² [hXXps://store.steampowered\[.\]com/news/app/593110/view/533224478739530145](https://store.steampowered.com/news/app/593110/view/533224478739530145)

- Reporting suggests the incident may be the result of a supply-chain compromise implicating cloud communications organization Twilio, which has publicly denied these claims.³ In April 2025, an actor named “Satanic” advertised an alleged Twilio data breach in the hacking forum BreachForums, though the claims remain unsubstantiated.

U.S.-based social media company and instant messaging app Snapchat was also allegedly breached, resulting in five million records being stolen; these are available for USD 2,000. Machine1337 does not specify the type of user data stolen but offers a data sample comprising 3,000 records.

China-based technology companies Huawei and Temu were also allegedly victims of a breach. ZeroFox has not observed any public statement from either organization, and the correlating xss threads gained very little traction.

- Machine1337 is offering 129 million unspecified “records” they claim were stolen from Huawei, which are available for USD 20,000. A sample of 3,000 records was made available for download.
- The actor is also advertising 17 million unspecified “records” allegedly stolen from Temu for USD 5,000. A sample of 3,000 records was made available for download.



Machine1337's xss advertisement of alleged Huawei compromise

Source: ZeroFox Intelligence

³ [hXXps://hackread\[.\]com/hacker-twilio-sendgrid-data-breach-customer-data/](https://hackread[.]com/hacker-twilio-sendgrid-data-breach-customer-data/)

Separately, on May 15, 2025, the U.S.-based cryptocurrency exchange platform Coinbase released a statement acknowledging a recent breach resulting in stolen customer data, which was subsequently leveraged to facilitate social engineering attacks. The attackers reportedly attempted to extort Coinbase for USD 20 million, which was not paid.⁴

- Coinbase alleges that the compromise was facilitated by an unnamed threat actor that bribed customer support agents, offering financial incentive in exchange for “copied data from Coinbase’s customer support tools.” The stolen information reportedly resulted in users mistakenly sending funds to the attackers.

The data extracted by the attacker reportedly includes PII, masked Social Security numbers, government ID images, Coinbase user transaction history, and masked bank account information.

- Coinbase also asserted it will be investing more resources into insider-threat detection, security threat simulation, and automated responses to prevent future incidents.⁵

Coinbase confirmed via its statement that login credentials, private keys, and access to customer wallets were not impacted by the breach. However, if leaked, the impacted data would likely afford actors the ability to conduct further social engineering campaigns targeting Coinbase users. Such subsequent attacks would likely leverage Coinbase customers’ PII to impersonate official communications and manipulate users into sharing passwords and multifactor authentication codes or transferring assets into the possession of malicious actors.

On May 15, 2025, ZeroFox observed that Machine1337 posted a message on their Telegram channel that stated “CoinBase: Coming soon”. The image included in the post contained several messages in Spanish, along with password reset URLs associated with Coinbase. The messages, translated from Spanish, were:

- “Reset your Coinbase password via this link:”

⁴ [hXXps://www.coinbase\[.\]com/en-gb/blog/protecting-our-customers-standing-up-to-extortionists](https://www.coinbase.com/en-gb/blog/protecting-our-customers-standing-up-to-extortionists)

⁵

[hXXps://www.bleepingcomputer\[.\]com/news/security/coinbase-discloses-breach-faces-up-to-400-million-in-losses/](https://www.bleepingcomputer.com/news/security/coinbase-discloses-breach-faces-up-to-400-million-in-losses/)

Flash | Actor Seemingly Claims Responsibility for Recent Breaches

F-2025-05-16b

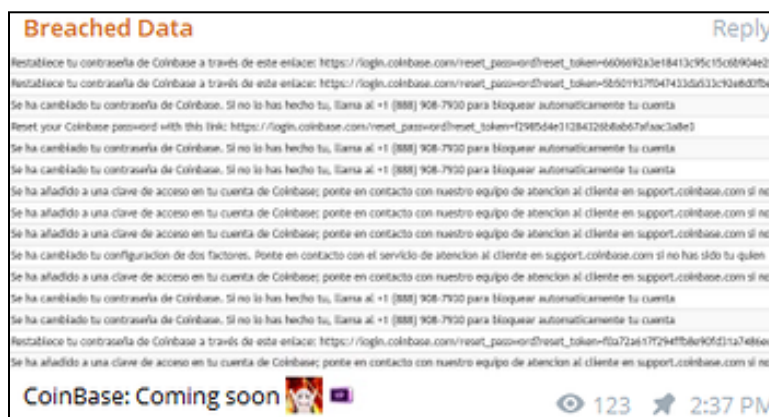
TLP:CLEAR



- “Your Coinbase password has been changed. If you haven't changed it yourself, please call +1 (888) 908-7930 to automatically lock your account.”

The meaning and context for the inclusion of these messages are unclear as of the writing of this report, and they do not provide evidence of Machine1337's involvement in a compromise of Coinbase. However, they do allude to a possible connection between Machine1337 and this recent incident, which has yet to be officially claimed by any threat actor or group.

There is a roughly even chance that the password reset messaging alludes to misleading communications that could be deployed against Coinbase users during targeted social engineering campaigns, resulting in victims interacting with malicious links that they believe to have originated from official Coinbase platforms.



Machine1337's Coinbase announcement post on Telegram

Source: ZeroFox Intelligence

It is likely that Machine1337 is involved, to an unknown extent, in the Coinbase data breach. If this is the case, there is a likely chance that subsequent information will be posted to the actor's Telegram channel or xss account in the coming days claiming responsibility for the breach, seeking collaborators, or offering associated data for sale.

| Recommendations

- Users should adhere to Coinbase's statement and recommendations to safeguard the integrity of secured account and wallet information.
 - Coinbase security guidance
<https://www.coinbase.com/en-gb/blog/protecting-our-customers-standing-up-to-extortionists>
- Users should ensure Steam accounts are secure by adhering to the platform's official guidance.
 - <https://help.steampowered.com/en/faqs/view/6639-EB3C-EC79-FF60>
- Organizations should deploy a holistic patch management process and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Organizations should adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege and implement network segmentation to separate resources by sensitivity and/or function.
- Organizations should implement phishing-resistant multi-factor authentication (MFA), enforce secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Organizations should ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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.

WHEN SHOULD IT BE USED?

Green

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.

Clear

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%