



| Brief |

The Underground Economist: Volume 5, Issue 10

B-2025-05-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

May 22, 2025

Scope Note

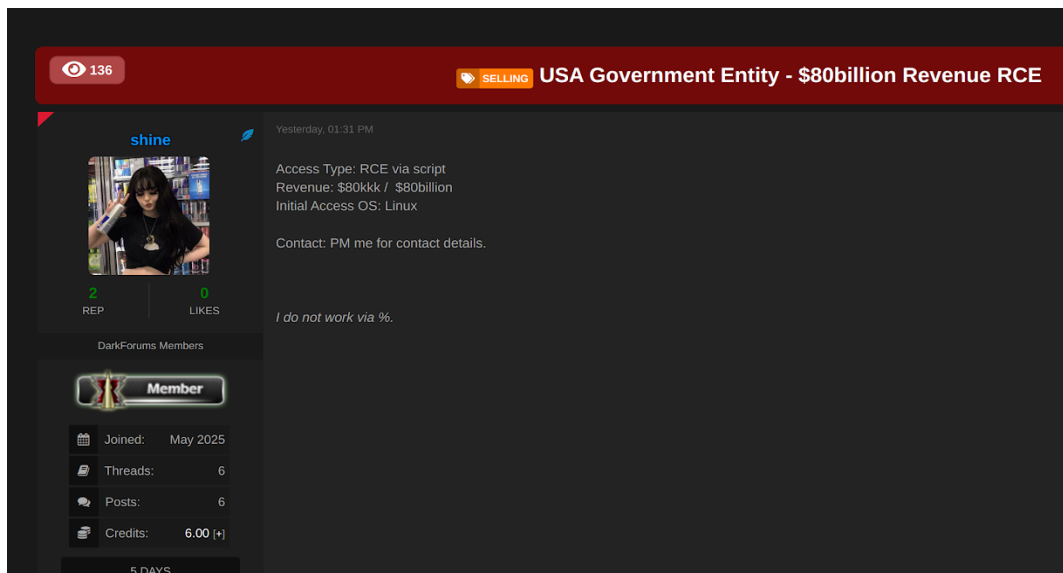
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 May 22, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 10

| Alleged Network Access Associated with U.S. and Chinese Institutions Advertised on DarkForums

On May 19, 2025, actor “shine” posted in the deep and dark web (DDW) forum DarkForums, advertising access to an unspecified U.S. government organization with an alleged annual revenue of USD 80 billion. According to the advertisement, the remote code execution (RCE) is enabled via a custom script.

- Shine is a newly-registered user on DarkForums, having joined in May 2025; they stated in the post that they are offering network access for fixed prices and are not interested in profit-sharing deals, providing only initial access services.
- ZeroFox has observed an increase of activity and traffic on the DarkForums platform since the recent and ongoing closure of the DDW site BreachForums on April 15, 2025.



Shine's post on DarkForums

Source: ZeroFox Intelligence

Later on the same day, shine advertised network access to five additional, allegedly compromised entities and included some minimal detail as to the nature of the access available:

- U.S. Municipal Government in California – RCE
- U.S. Local Bank – RCE
- Chinese Ministry Website – Secure Shell (SSH) Access
- Chinese Furniture Company – Domain Admin Access
- Hong Kong Executive Government Entity – RCE

 shine	 SELLING USA Government Entity - \$80billion Revenue RCE	Access Market	0	118	 Yesterday, 01:31 PM Last Post shine
 shine	 SELLING USA Municipal Government in California *.gov RCE	Access Market	0	113	 Yesterday, 05:57 AM Last Post shine
 shine	 SELLING Hong Kong Executive Government Entity *.gov.hk RCE	Access Market	0	118	 Yesterday, 05:55 AM Last Post shine
 shine	 SELLING Chinese Government *.gov.cn SSH Access	Access Market	0	168	 Yesterday, 12:43 AM Last Post shine

Access advertised on DarkForums

Source: ZeroFox Intelligence

Shine's previous activity in DarkForums is limited with no established reputation observed, rendering the actor's reliability and that of their services unclear as of the writing of this report. It is likely that shine was active on BreachForums prior to its recent disruption, with many actors seemingly perceiving DarkForums as the most lucrative and convenient alternative.

Advertisements implicating both alleged China-based and Western-based entities are rarely observed within DDW forums. While China-based entities are not considered "off-limits" in the majority of forums—in part due to them not falling within the category of Commonwealth of Independent States (CIS), the targeting of which is often forbidden—the majority of network compromises observed implicate Western targets. The inclusion of both is very likely indicative of shine's financial motivations, with a roughly even chance that the actor is not Russia-based.

| Salt Typhoon Data Advertised on DarkForums

On May 18, 2025, actor "ChinaBob" advertised the sale of files allegedly containing data associated with several companies that have previously leveraged the services of "Salt Typhoon" on the DDW forum DarkForums. A price for the data was not advertised, with ChinaBob instead requesting that interested parties contact them directly. ChinaBob is new to DarkForums, having joined in May 2025, and as such has a limited—albeit positive—reputation. As of the writing of this report, the data has allegedly been sold to an unspecified buyer.

- Salt Typhoon is an advanced persistent threat (APT) group that almost certainly is closely associated with China's Ministry of State Security (MSS). The collective has previously been linked to several high-profile cyber incidents targeting well-known companies, including Verizon, AT&T, and T-Mobile.¹
- In the post, ChinaBob provided sample data of the victim organizations, accessible via two GoFile download links. Using these links, ZeroFox obtained images seemingly depicting both stolen customer data and a configuration file from a compromised router.

¹ [hXXps://www.armis\[.\]com/blog/breaking-down-salt-typhoon/](https://www.armis[.]com/blog/breaking-down-salt-typhoon/)



ChinaBob's DarkForums post

Source: ZeroFox Intelligence

The data available for purchase allegedly contains personal identifiable information (PII)—including employee names, phone numbers, email addresses, and passwords—as well as internal communications between employees and officials “under investigation”, though it is not clear to what these investigations pertain. ChinaBob provided a list of organizations that have allegedly acquired the services of of Salt Typhoon, which includes the following:

- People's Liberation Army of China, Unit 61419
- Unit 152 (*unclear what this refers to*)
- Unit 0718 (*unclear what this refers to*)
- Beijing Foreign Service Office, Room 3
- Qinghai 9711 Institute
- Chengdu Bureau of Economy and Information Technology
- Qi'anxin Legendsec Information Technology (Beijing) Co., Ltd.
- Beijing Integrity Technology Group Co., Ltd.
- Beijing Jingyuan Shengda Information Technology Co., Ltd.
- Beijing VenusTech Information Security Technology Co., Ltd.
- Institute of Information Engineering, Chinese Academy of Sciences
- Granpect Co., Ltd.
- Yu Yang

- Beijing Huanyu Tianqiong Information Technology Co., Ltd.

银行账号 (Bank Account)	买方 (Buyer)	Buyer	银行账号 (Bank Account)
38070101040055544	中国人民解放军61419部队	People's Liberation Army of China 61419 Unit	51050144643600001907
134000424883	一五二单位	152 Unit	51050144643600001907
29122001040037948	0718单位	0718 Unit	51050144643600001907
0200080509000147090	北京市对外服务办公室第三室	Beijing Foreign Service Office Room 3	51050144643600001907
105003634701	青海九七一一所	Qinghai 9711 Institute	51050144643600001907
129372893643	成都市经济和信息化局	Chengdu Bureau of Economy and Information Technology	51050144643600001907
110902261210404	奇安信网神信息技术(北京)股份有限公司	Qi'anxin Legendsec Information Technology (Beijing) Company Limited	51050144643600001907
112012830005657	永信至诚科技集团股份有限公司	Beijing Integrity Technology Group Company Limited	51050144643600001907
0200002909200327278	北京京垣圣达信息技术有限公司	Beijing Jingyuan Shengda Information Technology Company Limited	51050144643600001907
861583890110001	北京启明星辰信息安全技术有限公司	Beijing VenusTech Information Security Technology Company Limited	51050144643600001907
200049629217001003	中国科学院信息工程研究所	Institute of Information Engineering of the Chinese Academy of Sciences	11050111293000000298
01090334600120105391851	北京国鸿科技有限公司	Granpect Company Limited	11050111293000000298
6216910106443440	余洋	Yu Yang	51050164722700000252
11050111293000000298	北京寰宇天穹信息技术有限公司	Beijing Huanyu Tianqiong Information Technology Company Limited	51050164722700000252

Sample data provided by ChinaBob

Source: ZeroFox Intelligence

The specific relationship between the organizations listed by ChinaBob and Salt Typhoon is unclear as of the writing of this report. However, there is a likely chance that the listed organizations—many of which are public or semi-public—have previously sought the services of Salt Typhoon, likely in the pursuit of corporate espionage or other intelligence-gathering initiatives against unknown targets.

If the data for sale is as advertised, it is very likely to appeal to an array of actors, including government intelligence organizations and rival corporations, as well as financially motivated actors seeking to conduct digital extortion activity.

Access to Israeli Internet Exchange Advertised on xss

On May 13, 2025, newly registered actor “HAX0RTeam” posted in the Russian-speaking dark web forum xss advertising alleged unauthorized network access to the Israeli Internet Exchange (IIX) for a notably high price of USD 150,000. No specific technical details about the access were disclosed in the post.

- The IIX is a critical internet exchange point (IXP) that facilitates the direct exchange of Israeli internet traffic between internet service providers (ISPs), content delivery networks (CDNs), and other network operators within the country.
- On October 7, 2023, Hamas launched an attack on Israel which led to a major escalation of conflict in Gaza that, despite various ceasefires, is ongoing.

- On May 19, 2025, Israeli Prime Minister Benjamin Netanyahu announced plans to take control of the entire Gaza Strip, a move that has been condemned by countries such as the United Kingdom, France, and Canada.²

HAX0RTeam claimed in the post that the access would enable potential buyers to:

- Intercept sensitive communications between Israeli government agencies, institutions, and influential organizations
- Obtain valuable intelligence on internal operations
- Manipulate and redirect traffic to exfiltrate data, conduct espionage, or deploy malware
- Launch targeted attacks against critical Israeli infrastructure
- Steal intellectual property, financial data, or other sensitive information
- Disrupt essential infrastructure and services
- Enable further exploitation and deep infiltration



HAX0RTeam
floppy disk
User

Joined: May 11, 2025
Messages: 1
Reaction score: 1

Today at 12:43 PM

Price: 150000
Contacts: TOX: E44AB527E7BA075C7F57390D69488E1E54F8BF7B724D9A4E4350B927F8C2D4062CBFAD484443

Access to Israel's IIX network - \$150,000

We are pleased to introduce you to the Israeli Internet eXchange (IIX) network.

Features:

- Hack sensitive communications between Israeli government agencies, institutions, and influential organizations
- Gain valuable information and insight into their operations
- Manipulate and redirect traffic to steal data, spy, or plant malware
- Conduct targeted attacks on key Israeli targets
- Steal intellectual property, financial data, or sensitive information
- Disrupt critical infrastructure and services
- Open the door to further exploitation and infiltration

Price: \$150,000
Payment methods: Escrow welcome (XMR/BTC)

HAX0RTeam's post on xss, May 13, 2025

Source: ZeroFox Intelligence

Notably, the advertisement is HAX0RTeam's first and only post, having joined the forum on May 11, 2025. ZeroFox has not observed the threat actor's name in other known forums, though it is a common alias within hacker communities and is often linked to the "1337"

² [hXXps://www.ft.com/content/8f1f3372-ecfc-46ed-9003-14b240613388](https://www.ft.com/content/8f1f3372-ecfc-46ed-9003-14b240613388)

(Leet) culture, which strongly suggests that the user has historical connections in the hacker community.

- The xss forum imposes strict protocols for new-user registrations to prevent previous users from returning after being banned, eliminate users who do not meaningfully contribute, facilitate trust between buyers and sellers, and mitigate scraping by cyber threat intelligence companies.

It is likely that HAX0RTeam was able to establish an account on the forum by either contacting the administrators directly, with an exception being made due to the prominence of the advertisement, or by being vouched for by existing and reputable members.

HAX0RTeam's claims about the types of subsequent exploitation that could be conducted by buyers are extremely varied in nature. Further, they seemingly omit any mention of the significant technical expertise that would very likely be required to achieve them—even once in possession of the network access. As such, this data is likely to appeal primarily to entities in possession of the knowledge, tools, and funds necessary to deploy information-stealing malware or conduct Man-in-the-Middle (MitM) or session hijacking activity. Despite HAX0RTeam's offering, the theft of "sensitive communications between Israeli government agencies" would likely be significantly more difficult to achieve due to their common use of encryption methods and various types of closed networking.

| Actor Seemingly Claims Responsibility for Recent Breaches

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 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.
- 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.

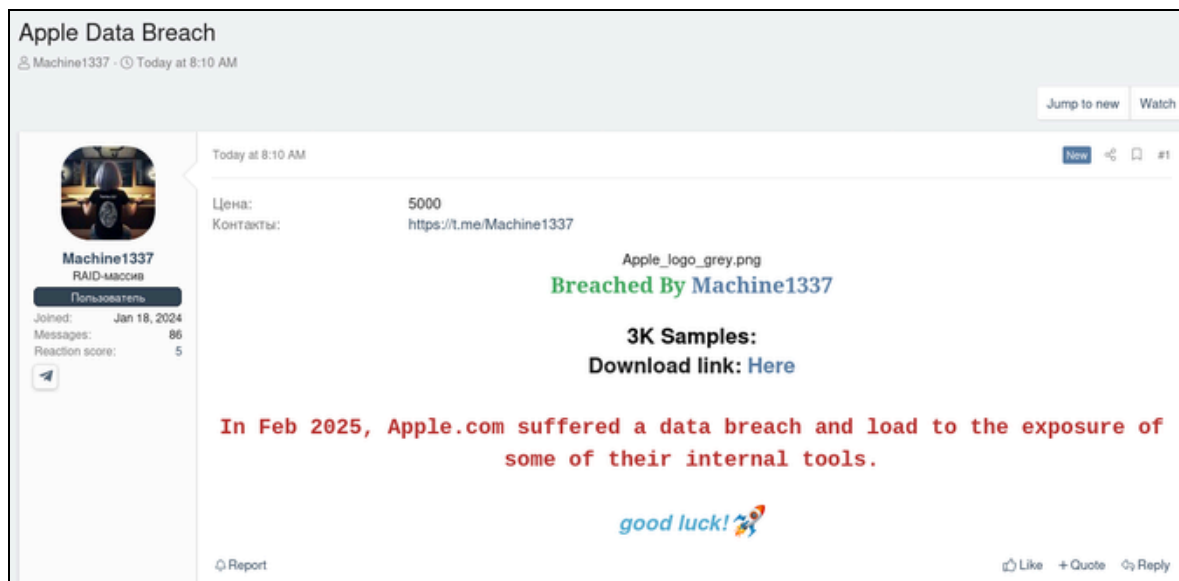


Machine1337's xss post

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 lead 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 5,000.³ Steam issued a statement claiming that the stolen data cannot be linked to other PII and that the breach remains under investigation.⁴ Machine1337's post gained some traction from fellow xss users, many of whom are claiming the sample data is inaccessible.

- Reporting suggests the incident may be the result of a supply-chain compromise implicating cloud communications organization Twilio, which has publicly denied these claims.⁵ 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

³

³ [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/)

⁴ [hXXps://store.steampowered\[.\]com/news/app/593110/view/533224478739530145](https://store.steampowered.com/news/app/593110/view/533224478739530145)

⁵ [hXXps://hackread\[.\]com/hacker-twilio-sendgrid-data-breach-customer-data/](https://hackread.com/hacker-twilio-sendgrid-data-breach-customer-data/)

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.

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.⁶

- 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.⁷

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

⁶ [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)

⁷

[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/)

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:"
- "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.

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

- 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 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%