



| Brief |

The Underground Economist: Volume 5, Issue 12

B-2025-06-20a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

June 20, 2025

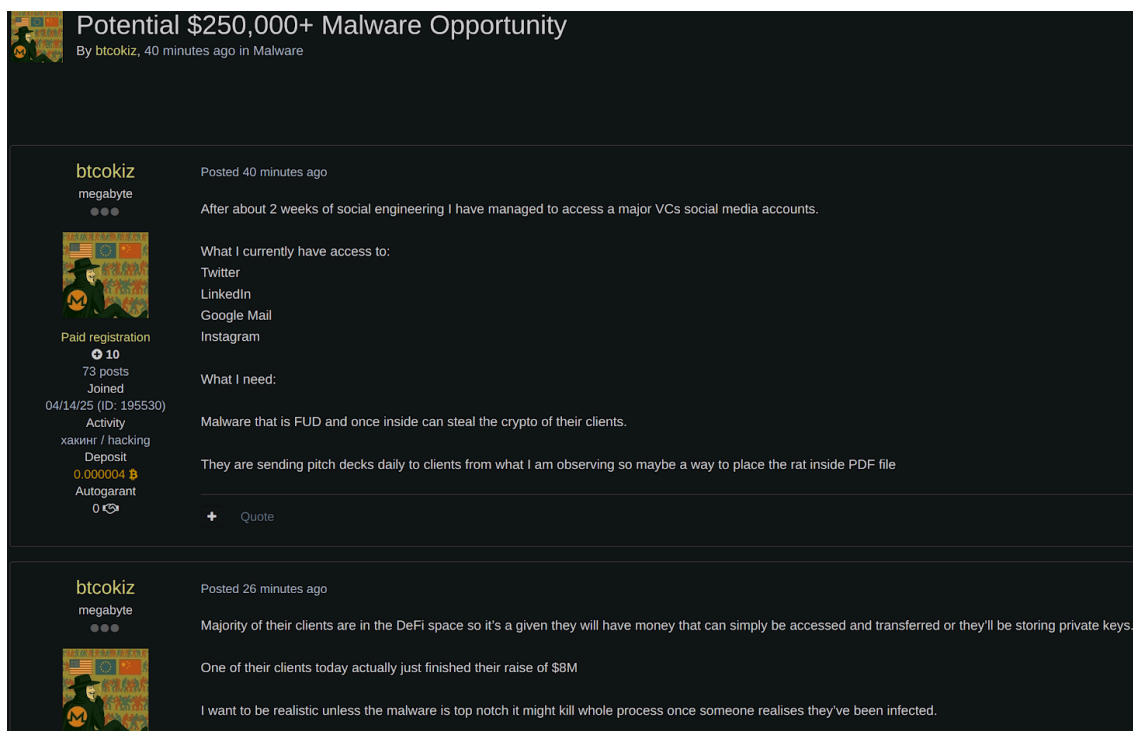
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 June 20, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 12

| Unusual Social Engineering Campaign-based Malware Opportunity Advertised

On June 17, 2025, an actor using the alias “btcokiz” posted in the dark web forum Exploit seeking fully undetectable (FUD) malware to steal cryptocurrency from the clients of an unnamed “major venture capitalist” (VC). This took place following the actor's supposed two week-long social engineering campaign that allegedly succeeded in obtaining access to social media accounts associated with VC—including X (formerly Twitter), LinkedIn, Gmail, and Instagram. Btcokiz indicated they will combine their already-obtained access to the VC's social media accounts with the sought-after malware in order to steal cryptocurrency from the VC's clients.

- Clients or associates of VCs, who are often entrepreneurs or investors, very likely often assume legitimacy of any communications between them, largely due to their perceived professionalism and stature.
- Bicokiz noted that the malware required for this campaign must be highly advanced and capable of bypassing sophisticated protections, including private key authorization mechanisms for cryptocurrency transfers.
- The title of the post, “Potential \$250,000+ Malware Opportunity”, indicates that the actor likely expects to generate at least USD 250,000 from the proposed operation, though it is unclear how btcokiz arrived at this number.



btcokiz's Exploit post

Source: ZeroFox Intelligence

Btcokiz claimed to have observed the allegedly compromised VC regularly sending their clients pitch decks, very likely referring to investment-related presentation documents. According to the actor, this pattern can be exploited via the insertion of remote access trojans (RATs) into these PDF files. Given that many of the clients “are in the DeFi” space, btcokiz speculates that “they will have money that can simply be accessed and transferred.”

No further detail on the proposed attack vector or collaboration is given, though btcokiz likely anticipates a deployed RAT facilitating the exfiltration of the data necessary to gain access to cryptocurrency hot wallets, such as private keys and seed phrases. Such activity conducted successfully could also facilitate the exfiltration of other types of personally identifiable information (PII) or the deployment of further malicious software.

The impact or likely success of such an operation is unclear, given there is a lack of information surrounding the actor's efficacy and user security protocol configuration likely varies across DeFi platforms. However, there is a likely chance that successful attacks are not attributed to the VC or the shared pitch decks, with victims instead exploring other avenues of DeFi compromise. Should btcokiz maintain the established access to VC social engineering accounts, there is a likely chance that similar, subsequent exploit opportunities will occur.

| Further Access to U.S. Institutions Advertised on DarkForums

On June 11, 2025, the actor "shine" posted three times in the deep web forum DarkForums, advertising network access to U.S. government institutions via remote code execution (RCE). According to the advertisements, the RCE is enabled via a custom script.


- Shine is a recently registered user on DarkForums that 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 deep web site BreachForums on April 15, 2025.

The three advertisements allegedly facilitate access to an unnamed police department in the state of New Jersey, an unnamed city government in the state of Georgia, and an unnamed city government in the state of California.

110

SELLING USA Police Department in New Jersey

shine



3
REP

0
LIKES

Today, 01:04 AM

#1

Access Type: RCE via script
Revenue: Unknown, government entity.
Initial Access OS: Linux


Contact: PM me for contact details.

I do not work via %.

119

SELLING USA City Government in Georgia

shine



3
REP

0
LIKES

Today, 01:06 AM

#1

Access Type: RCE via script
Revenue: Unknown, government entity.
Initial Access OS: Linux


Contact: PM me for contact details.

I do not work via %.

122

USA City Government in California

shine



3
REP

0
LIKES

Today, 01:10 AM

#1

Access Type: RCE via script
Revenue: Unknown, government entity.
Initial Access OS: Linux

Contact: PM me for contact details.

I do not work via %.

Shine's DarkForums Post

Source: ZeroFox Intelligence

Shine's previous activity in DarkForums is limited; however the actor posted in DarkForums on May 19, 2025, advertising access to an unspecified U.S. government organization with an alleged annual revenue of USD 80 billion. Later on the same day, shine advertised network access to five additional, allegedly compromised entities and included some minimal details as to the nature of the access available:

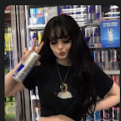
- U.S. municipal government in California – RCE
- U.S. local bank – RCE
- Chinese Ministry website – Secure Shell (SSH) Access

- Chinese furniture company – Domain Admin Access
- Hong Kong executive government entity – RCE

136

SELLING USA Government Entity - \$80billion Revenue RCE

shine



2

REP

0

LIKES

DarkForums Members

Yesterday, 01:31 PM

#1









Access Type: RCE via script

Revenue: \$80kkk / \$80billion

Initial Access OS: Linux

Contact: PM me for contact details.

I do not work via %.

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

Shine's DarkForums posts

Source: ZeroFox Intelligence

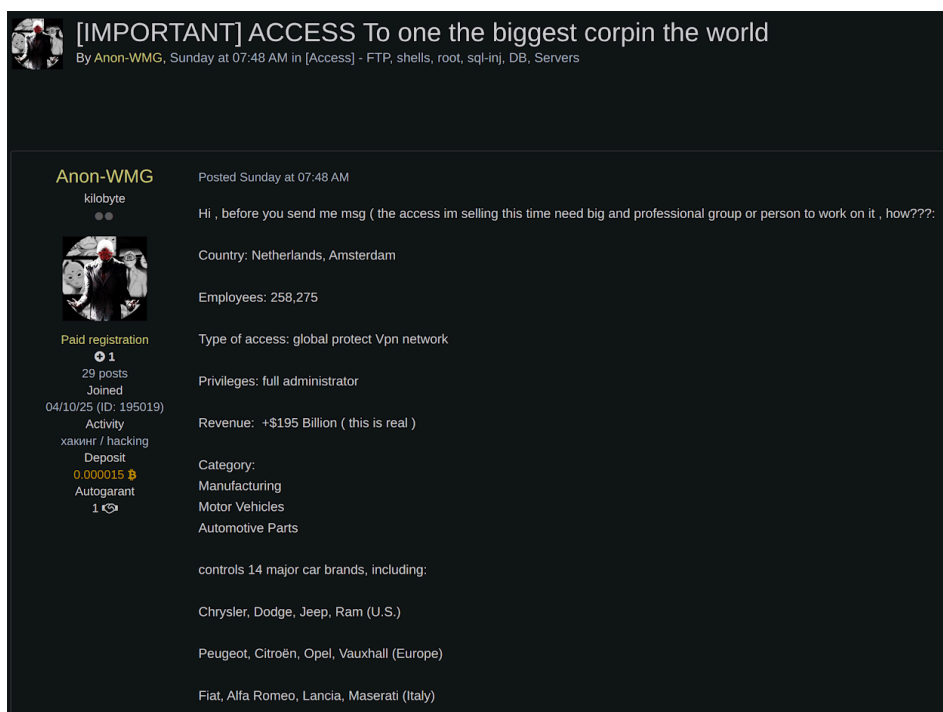
Shine's posts received no reactions or comments in the following days. Their previous activity in DarkForums is limited with no established reputation observed, rendering the actor's reliability and that of their services unclear as of the writing of this report. It is likely that shine was active on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

Network access via RCE to government institutions is very likely to be perceived as potentially lucrative by financially motivated actors seeking either digital extortion targets or targets for hack-and-leak type attacks or state-affiliated cyber collectives seeking to obtain sensitive PII associated with government officials.

| Global Protect VPN Access of a Major Automaker Company Advertised on Dark Web Forum

On June 8, 2025, threat actor “Anon-WMG” posted on the predominantly Russian-language dark web forum Exploit, advertising Global Protect VPN credentials for an unnamed Netherlands-based automotive parts manufacturing company. According to Anon-WMG, the company “controls” 14 major brands (including Chrysler, Dodge, Jeep, Ram, Peugeot, Citroën, Opel, Vauxhall, Fiat, Alfa Romeo, Lancia, and Maserati) and has an annual revenue of USD 195 billion.

- The unnamed company is very likely to be the multinational automaker Stellantis N.V., based upon the stated location, annual revenue, and associated brands.



[IMPORTANT] ACCESS To one the biggest corpin the world
By Anon-WMG, Sunday at 07:48 AM in [Access] - FTP, shells, root, sql-inj, DB, Servers

Anon-WMG
kilobyte
●●

Posted Sunday at 07:48 AM

Hi , before you send me msg (the access im selling this time need big and professional group or person to work on it , how???:

Country: Netherlands, Amsterdam

Employees: 258,275

Type of access: global protect Vpn network

Privileges: full administrator

Revenue: +\$195 Billion (this is real)

Category:
Manufacturing
Motor Vehicles
Automotive Parts

controls 14 major car brands, including:

Chrysler, Dodge, Jeep, Ram (U.S.)

Peugeot, Citroën, Opel, Vauxhall (Europe)

Fiat, Alfa Romeo, Lancia, Maserati (Italy)

Paid registration
1
29 posts
Joined
04/10/25 (ID: 195019)
Activity
хакинг / hacking
Deposit
0.000015 \$
Autogrant
1

Anon-WMG's advertisement on Exploit

Source: ZeroFox Intelligence

According to Anon-WMG, utilizing the VPN access demands skilled professionals who can bypass internal certificate requirements in order to connect to the network. ZeroFox has observed that similar accesses for Global Protect VPN have been advertised on Exploit for

between USD 200 to USD 2,000. However, it is likely that Anon-WMG has offered the price at USD 6,500 due to the size and perceived potential payoff of the alleged access.

- As of the writing of this report, the advertisement has not generated notable interest from fellow forum users, however, it is likely that potential buyers are privately reaching out via Tox and Session as directed by Anon-WMG.
- The threat actor stated their willingness to share data samples, as well as sell the credentials via escrow—increasing the likely legitimacy of the offer.

```
Why i said need professionals:

You can login from web portal of global protect that let download global protect vpn using creds ( user,pass )

The problem is when you try to access to network inside or connect to it from inside vpn

It ask for certificate ( required)
If can't bypass this , you can't access network ( even using admin creds )

Price : 6500$

If you can bypass the certificate , you will have access to all the corp and all hosts, machines, websites.....

If u interested :

Tox: ECD4739233761637C0F7482A6816CF4E6C7BBC56B3F7FDD42899F2FBC0A40F0AB4DA0405AE9F

Session: 050703f6dfb92285446258528b0cc3127d49a6de9f9d1ecb996e4b27bb6b41d751

Samples , proofs only using escrow ( sensitive info )

Good luck
```

Anon-WMG's post about the alleged access

Source: ZeroFox Intelligence

If as advertised, financially motivated threat actors (such as sophisticated ransomware collectives) would almost certainly be interested in obtaining the offered credentials. Further, some actors would very likely perceive potential value in obtaining the access and bypassing internal certificate requirements to establish further access, which could then be resold. The advertised credentials are very likely to be time-sensitive due to routine password changes and security alerts, which—along with the difficulty of bypassing a certificate requirement—will likely deter many potential buyers seeking a low-risk, high-payoff opportunity.

| Mobile Numbers Advertised for Sale in Dark Web Forum

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



The screenshot shows a forum post by user Machine1337. The user profile on the left indicates they joined on Jan 18, 2024, with 124 messages and a reaction score of 10. The post content, dated Saturday at 3:17 PM, lists prices for mobile numbers: 100K → \$150, 500K → \$500, 1M → \$1000, with a contact link https://t.me/Machine1337. The post includes several green checkmark icons and text: 'Freshly Scraped & Verified', 'High Accuracy & Active Numbers', and 'Country/Region Targeting Available'. It also features a red download icon with the text 'Contact me now for pricing & samples!'. Below this is a 'LIMITED-TIME DEALS' section with a fire icon, showing the same price list. A yellow warning icon states 'Stock updates hourly – Prices rise at 1M sold!'. A crypto icon indicates 'CRYPTO ACCEPTED (USDT) | Escrow Available'. At the bottom, a red download icon points to 'FREE SAMPLE 100K+: Here'.

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

- 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 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%