



| Brief |

The Underground Economist: Volume 5, Issue 5

B-2025-03-14b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

March 14, 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 March 14, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

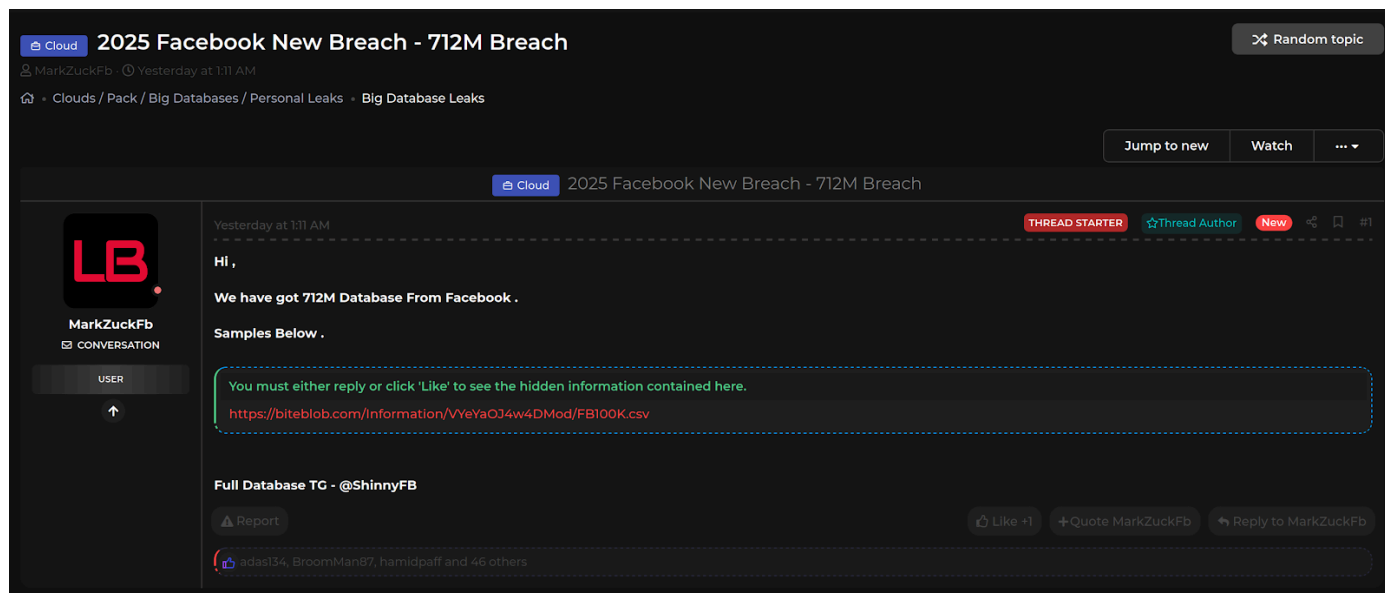
Brief | The Underground Economist: Volume 5, Issue 5

| Threat Actor Advertises 712 Million Facebook User Records

On March 10, 2025, newly registered and English-speaking threat actor “MarkZuckFb” posted on the dark web forum LeakBase advertising a data breach composed of 712 million unique user records obtained from the social media platform Facebook. MarkZuckFb included a sample of 100,000 lines of user data in the advertisement, which included accounts registered with government email addresses. The actor further stated they would reveal the full database’s price to interested buyers, along with a proof of concept (PoC).

Upon inspection of the sample data, it was found to include names, email addresses, geolocations, phone numbers, and birth dates. Despite the absence of passwords, this type of data, in this quantity, is almost certain to appeal to a range of threat actors interested in conducting social engineering attacks, identity theft, or other fraudulent activity.

MarkZuckFb’s post quickly received numerous positive responses from other LeakBase users stating that the advertisement and associated data appear legitimate. However, given MarkZuckFb’s relatively short length of time on the forum, there is a roughly even chance that the breach is either fabricated or exaggerated in order to conduct a scam or draw attention to other advertisements.



MarkZuckFb's advertisement in Leakbase

Source: ZeroFox Intelligence

| Windows Zero-Day Vulnerability Advertised for Sale

On March 7, 2025, Russian-language threat actor "Uxcodea" announced the sale of a Windows zero-day local privilege escalation (LPE) exploit for a price of USD 70,000 on the dark web forum xss. Uxcodea also claims to possess additional zero-day vulnerabilities affecting unspecified targets that will be revealed only during private negotiations.

- To date, Uxcodea has completed one previous transaction on xss using an escrow service.
- Although Uxcodea joined the xss forum on February 16, 2024, ZeroFox did not identify sufficient information to establish either the threat actor's credibility or the likelihood of the advertisement being legitimate.

A zero-day LPE vulnerability can allow attackers with low-level user access to a network to enhance their privileges to administrator or system-level control. This type of exploit is almost certainly considered valuable for malware operators, advanced persistent threat (ATP) groups, and digital extortion collectives.

ZeroFox has observed an influx in alleged zero-day vulnerabilities being advertised for sale in deep and dark web (DDW) forums in recent months, alongside a significant uptick in the attack tempo of several ransomware and digital extortion (R&DE) collectives. Given the potential value of an LPE-enabling zero-day vulnerability in the deployment of malware, there is a roughly even chance that a direct correlation exists.

Oday WIN LPE 70k + other Odays

Uxcodea · Friday at 4:03 PM

ESCROW AVAILABLE IN THIS THREAD!

New deal

NO AVATAR

Uxcodea

floppy disk

User

Joined: Feb 16, 2024

Messages: 5

Reaction score: 1

Escrow transactions: 1

Friday at 4:03 PM

Price: 70000

Contacts: 3395291A2B465BB1ACC3D47548733F81685298410CA552D3017175E382B1D9096FF8226AA9E1

WinLPE for sale, works everywhere
Work strictly through the guarantor
Also often there are other Oidei information about which I do not want to publish publicly.
70k
All details in personal correspondence
Tox: 3395291A2B465BB1ACC3D47548733F81685298410CA552D3017175E382B1D9096FF8226AA9E1
Report

NO AVATAR

Uxcodea

floppy disk

User

Joined: Feb 16, 2024

Messages: 5

Reaction score: 1

Escrow transactions: 1

Yesterday at 3:25 PM

Still relevant, I provide the video only to people who have a reputation on the forum due to the fact that there are a lot of "interested" people
. Sale to one person.
Report

Uxcodea's advertisement in xss

Source: ZeroFox Intelligence

| Malicious Google Administrator Service Offered for Sale

On March 3, 2025, a Russian-speaking threat actor known as “serginhose” resumed accepting orders for their “Google Admin/Moderator Services” on the dark web forum Exploit. This service originally launched on September 2, 2024, and serginhose’s announcement that they will resume this service was posted on February 28, 2025. Serginhose has a relatively short history on Exploit, having joined on July 15, 2024; at this time, the actor maintains a fragile reputation on the forum. However, ZeroFox has not yet observed any disputes regarding the service serginhose has offered.

The service allegedly enables the downloading of information available on a competitor’s Google account. In addition, the service includes various blocking and unblocking features advertised, which allegedly include enabling the provision of a legitimate reason to have a Google account blocked or unblocking. The actor provided a disclaimer that unblocking a Google account may not be successful and that they cannot guarantee the results. Serginhose’s asking price is USD 800 for accessing sensitive Google account information and USD 150 for account blocking/unblocking.

It is likely that serginhose has unauthorized access to Google administrator resources, such as Google Takeout. If legitimate, this service could have a severe impact on businesses that rely on Google management services. These Google services are web-based tools that allow management of an organization’s Google Workspace, users, devices, security, and policies by administrators. Unauthorized access could allow a threat actor illicit access to an organization’s private and proprietary data, such as:

- Gmail: messages, attachments, and contacts
- Google Drive: documents, sheets, presentations, forms, and sites
- Google Calendar: events and invitations
- Chrome: browser data and extensions
- Google My Business: business profile data and performance insights

serginhose
megabyte
● ● ●



Paid registration
02
84 posts
Joined
07/15/24 (ID: 172535)
Activity
other / other
Deposit
0.037768\$
Car warranty
000

Posted Friday at 05:06 AM

We are accepting orders again from Monday

Google admins service:
- Downloading all information from a competitor's account
Cost: \$800.

- The exact reason for blocking
Cost: \$150.

We work **exclusively on prepayment basis**.
Request fulfillment time may take up to 24 hours.

+ Quote

Aged Google Ads Accounts With Spending History and Google Admins Service

serginhose's Exploit post advertising Google administrative service

Source: ZeroFox Intelligence

Administrators have unique privileges to download data for the entire organization, which include shared drives. Within an organization's Google Workspace, Google Takeout is selected by default. This feature—along with other security breaches, like compromised log-in credentials or phishing attacks—can leave a business' data vulnerable to threat actors. In this case, alleged access to Google administrative resources could result in a mass export of sensitive data to competitors or actors.

| 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%