



| Flash |

Increased Demand for X Accounts in Dark Web Forum

F-2024-02-28a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web,

February 28, 2024

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 (EST) on February 28, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | Increased Demand for X Accounts in Dark Web Forum

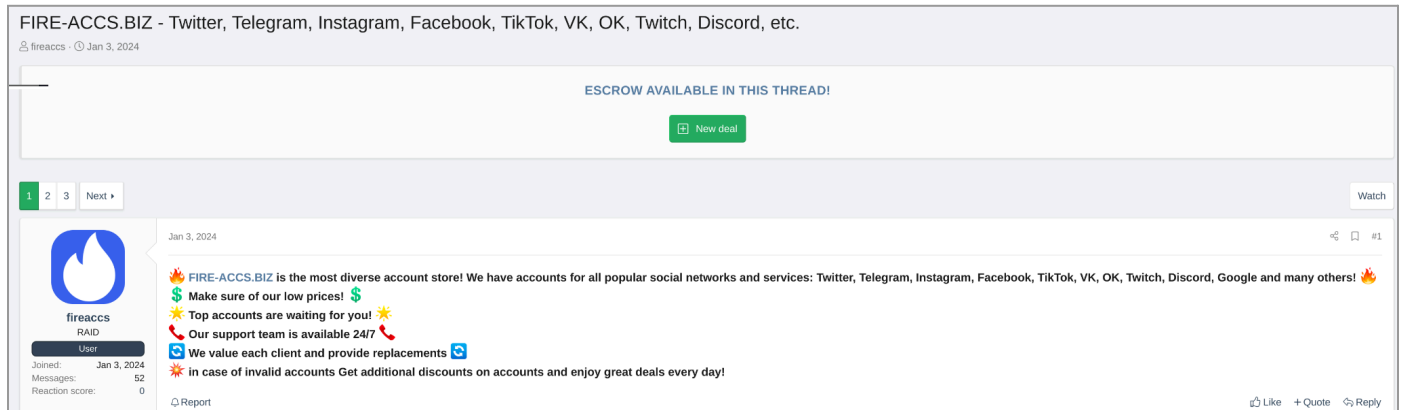
> Key Findings

- A new shop with exceptionally high numbers of social media accounts for sale, which first began trading under the name fireaccs[.]biz on the dark web forum xss on January 4, 2024, is gaining momentum amongst threat actors.
- On the store, X (formerly Twitter) accounts are significantly more numerous and in demand compared to other social media platforms. This is very likely indicative of their favor amongst a wide array of threat actors, given the perceived benefits of operating on X to advertise, brag, or disseminate content to a wider audience than on other platforms.

| Details

A public shop that began trading under the name fireaccs[.]biz on the dark web forum xss on January 4, 2024, is gaining momentum amongst threat actors and has exceptionally high numbers of social media accounts associated with various different platforms for sale. The thread is operated by untested threat actor “fireaccs”, who updates the shop on a daily basis to meet customer demands. As a public shop, customers are able to buy goods without negotiating with the vendor.

- While such shops are not uncommon in deep and dark web (DDW) marketplaces, fireaccs is notable primarily for the sale of hundreds of thousands of X accounts in just several weeks—a rate that remains at a steady pace.
- The shop offers the sale of both new “bot” accounts and “aged” accounts, some of which are advertised with followers. Though the latter is more expensive, the former are selling in much higher numbers.



Xss post advertising fireaccs' services

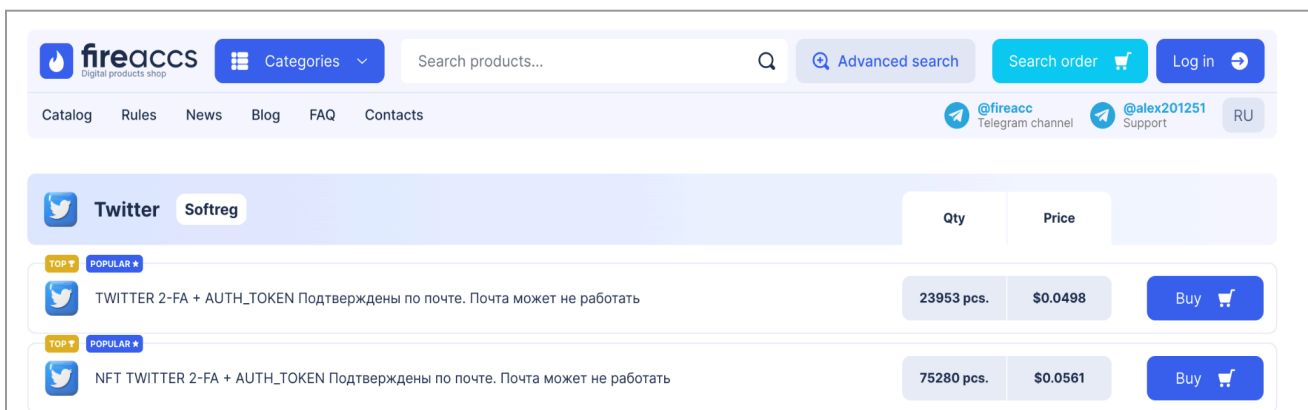
Source: ZeroFox Intelligence

On the store, X accounts are significantly more numerous and in demand compared to other social media. This is very likely indicative of their favor amongst a wide array of threat actors, given the perceived benefits of operating on X versus other platforms. X accounts are almost certainly being increasingly implicated in various types of cybercrime that target individuals and organizations. This is enabled, to some extent, by:

- The allegedly lower levels of active internal regulation of accounts by X in comparison to its predecessor, Twitter. This results in fewer instances of accounts being suspended or banned for conveying controversial speech or otherwise violating the platform's user guidelines.
- The ability of threat actors to leverage licit as-a-service tools to bypass Know Your Customer (KYC) protocols, which are often associated with the creation of social media accounts. This aids the automated registration of large numbers of accounts for a small price and in a short period of time—accounts which are then used to conduct various nefarious activities without fear of reprisal.
- The inherent anonymity often associated with X in comparison to other social media platforms, where users expect profiles to contain overt links to other

legitimate profiles as a display of authenticity. This enables and encourages antisocial behavior.

- The ability for users to engage with audiences far beyond their immediate following. This increases the opportunity available for malicious messages or services to be publicized.
- The payments from the platform to users that are part of the Creator Ads Revenue Sharing Program and receive at least 5 million organic impressions on a post. This encourages the posting of contentious or inflammatory language that may be more likely to be widely shared.

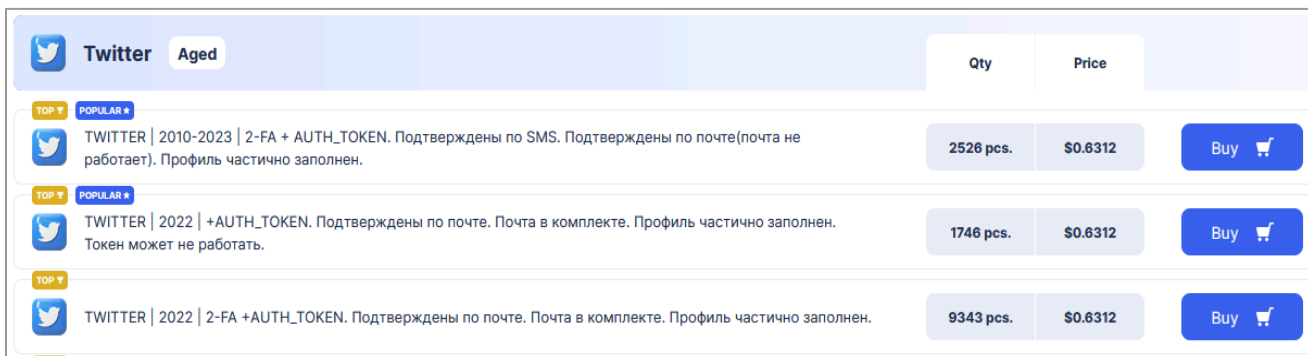


The screenshot shows the Fireaccs website interface. At the top, there is a navigation bar with the Fireaccs logo, a search bar, and links for Categories, Search products, Advanced search, Search order, and Log in. Below the navigation bar, there are links for Catalog, Rules, News, Blog, FAQ, and Contacts. The main content area displays a list of X accounts for sale under the 'Twitter' category. The accounts are listed with their quantity, price, and a 'Buy' button. The accounts are categorized as 'Softreg' and 'Aged'.

Category	Qty	Price	Action
Twitter Softreg			
TOP POPULAR TWITTER 2-FA + AUTH_TOKEN Подтверждены по почте. Почта может не работать	23953 pcs.	\$0.0498	Buy
TOP POPULAR NFT TWITTER 2-FA + AUTH_TOKEN Подтверждены по почте. Почта может не работать	75280 pcs.	\$0.0561	Buy

Fireaccs advertising of X accounts

Source: ZeroFox Intelligence



The screenshot shows the Fireaccs website interface, specifically the 'Aged' category for X accounts. The accounts are listed with their quantity, price, and a 'Buy' button. The accounts are categorized as 'Aged' and 'Softreg'.

Category	Qty	Price	Action
Twitter Aged			
TOP POPULAR TWITTER 2010-2023 2-FA + AUTH_TOKEN. Подтверждены по SMS. Подтверждены по почте(почта не работает). Профиль частично заполнен.	2526 pcs.	\$0.6312	Buy
TOP POPULAR TWITTER 2022 +AUTH_TOKEN. Подтверждены по почте. Почта в комплекте. Профиль частично заполнен. Токен может не работать.	1746 pcs.	\$0.6312	Buy
TOP POPULAR TWITTER 2022 2-FA +AUTH_TOKEN. Подтверждены по почте. Почта в комплекте. Профиль частично заполнен.	9343 pcs.	\$0.6312	Buy

Fireaccs advertising of "aged" X accounts

Source: ZeroFox Intelligence

Fireaccs sells accounts in both the Russian and English language, indicating a broad marketplace of customers who are almost certainly procuring accounts to conduct a diverse array of malicious activities known to take place on X. These are very likely to include:

- Non-fungible token (NFT) scams, which can include rug-pulling, the use of social engineering techniques to access users' NFT account details, bidding scams, and the spreading of misinformation intended to artificially inflate NFT prices. Many X accounts sold on fireaccs claim to be optimized toward the use of NFTs and blockchain accounts.
- Crypto scams, which are very likely on an upward trajectory in 2024. Threat actors use bot accounts to manipulate the prices of cryptocurrencies and deliver crypto wallet-draining malware using phishing techniques, such as displaying malicious, redirecting ads to users.
- Verification scams, whereby threat actors masquerading as X staff offer users the platform's popular blue checkmark in exchange for personal details, money, or both. Only users who have purchased X Premium are eligible to receive the blue tick on their profiles, as well as some notable public figures still associated with the now-legacy Twitter verification program.¹



fireaccs
RAID-массив

Пользователь

Joined: Jan 3, 2024
Messages: 52
Reaction score: 0

Saturday at 9:03 AM

Новые поставки:

- АККАУНТЫ TWITTER | ОТЛЕЖКА 10+ ДНЕЙ. ПОДТВЕРЖДЕНЫ ПО ПОЧТЕ @RAMBLER, ПОЧТА РАБОТАЕТ. ПОЛ (MIX). ПРОФИЛЬ ЗАПОЛНЕН. TOKEN В КОМПЛЕКТЕ.
- Telegram - Ручная регистрация | Ru | мужской аккаунт | Русское имя | Пароль в комплекте | формат tData
- ★ Instagram - качественный авторег TRUSTY-PRO ★ | ✓ Включен БИЗНЕС-профиль (ПРОФ РЕЖИМ) + добавлен АВАТАР ✓ | ✓ В формате IAM ✓
- Facebook - авторег, GEO:FR, E-MAIL, SMS, добавлен аватар, формат Логин:пароль:почта, Куки, юзерагент, EAAB токен
- Discord аккаунты Авторег - подтверждены по почте | В комплекте пароля почты нет, Токен есть | Пол Mix | Зарегистрированы на Mix ip

Report



fireaccs
RAID-массив

Пользователь

Joined: Jan 3, 2024
Messages: 52
Reaction score: 0

Sunday at 11:51 AM

Новые поставки:

- TWITTER 2-FA | 0-100 подписчиков | Подтверждены по почте. Профиль частично заполнен.
- Telegram Account verified with (+1) USA number.
- INSTAGRAM | 2018 | В комплекте почта (Onet.pl).
- Facebook 2017 With 50+ Friends
- ★ GMAIL TRUST NUMBER ★ CONFIRMED SUBMAIL INCLUDED

Report

X accounts for sale, advertised in both Russian and English

Source: ZeroFox Intelligence

¹ [hXXps://help.twitter\[.\]com/en/managing-your-account/about-x-verified-accounts](https://help.twitter.com/en/managing-your-account/about-x-verified-accounts)

Recommendations

- Ensure social media accounts are configured with organic security features, such as phishing-resistant multi-factor authentication and complex, unique passwords.
- Report accounts suspected as fake or those conducting malicious activity through the platform's internal report function.
- Be aware of the activity stemming from accounts with a recent creation date, limited activity, or those with seemingly nonsensical names.
- Ensure enterprise engagements taking place over social media platforms move to more secure channels when appropriate, protecting internal and customer data.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of ransomware and digital extortion (R&DE) threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- 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.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.

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%