



FLASH

TWITTER DATA LEAK

ZEROFOX INTELLIGENCE

F-2023-01-05a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Hacking, Data Theft

January 5, 2023



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 (EST) on January 5, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Twitter Data Leak

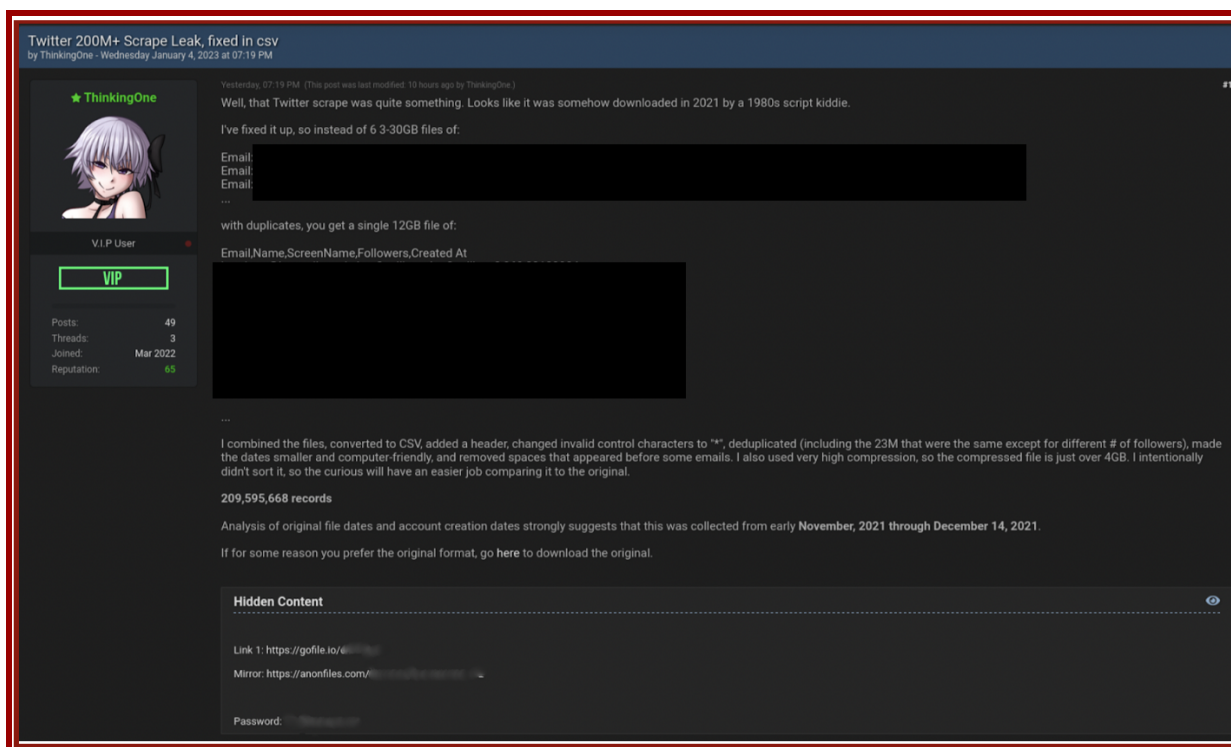
Key Findings

- A threat actor has shared what they claim is Twitter data of 200 million users in a hacker forum.
- The leaked data includes names, email addresses, and usernames and is completely publicly available.
- The leaked data is likely a result of a Twitter API vulnerability that was previously patched.
- At this time, security researchers have not independently verified how much of this data, if any, is reused from previously-leaked Twitter data.
- The presence of the email account data in the leak increases the likelihood of phishing, impersonation, and other social engineering attacks.

Analyst Commentary

On the heels of a December 2022 leak of data for 5.3 million of its users, Twitter has experienced another possible leak of user data. This time, threat actor “ThinkingOne” has shared names and email addresses associated with at least 200 million Twitter users on a popular English-speaking deep web hacker forum, Breached. ZeroFox Intelligence assesses ThinkingOne to be fairly reputable, and the data can be accessed for eight forum credits (about USD 2). Unlike the December 2022 leak, the entirety of this newest data is made publicly available.¹ Of those 200 million records, 100,000 have been confirmed as verified users, indicating that some of the impacted accounts include notable celebrities and organizations. In addition, Twitter users that have made attempts to remain anonymous on the platform may have their associated email addresses and correlated names now made publicly available.

¹ [hXXps://cybernews\[.\]com/news/235-million-twitter-user-data-leak/](https://cybernews[.]com/news/235-million-twitter-user-data-leak/)



Post on Breached forum by ThinkingOne

Source: ZeroFox Intelligence

Several threat actors took advantage of a Twitter API vulnerability before it was patched in January 2022, leaking and selling scraped user datasets. Beginning in July 2022, threat actors have been observed selling and circulating large datasets of scraped Twitter user profiles containing both private and public data on various online hacker forums and cybercrime marketplaces. More such leaks are anticipated in the future as a result of other breaches using the same bug prior to it being patched. At this time, it has not been determined what Twitter data has been reused from previous leaks or how much of it is real data, although many accounts have been confirmed as legitimate.² Should all the data be confirmed as legitimate, it would indicate that roughly 54 percent of all 468.4 million Twitter users were impacted by this leak.³

Recommendations

- Update Twitter account passwords immediately and regularly change them every 4-6 weeks.
- Update any accounts that utilize the same password as your Twitter account.
- Do not share personal information or contact information on Twitter.

² [hXXps://www.bbc\[.\]com/news/technology-64153381](https://www.bbc.com/news/technology-64153381)

³ [hXXps://www.statista\[.\]com/statistics/303681/twitter-users-worldwide/](https://www.statista.com/statistics/303681/twitter-users-worldwide/)



- Beware of unsolicited Direct Messages (DMs). Phishing attacks often use DMs to lure unsuspecting users to a login page, where they are asked to provide their username and password. Moreover, use your judgment and discretion while clicking URLs in DMs.
- Block and report spam. If you receive spam via @replies, block and report the account as spam. Block suspicious accounts, spammers, and bots from following you.
- Consider making your feed private. Once the [“Protect My Tweets”](#) feature is turned on, tweets will only be available to your approved followers. Please note that unprotecting your tweets will cause any previously-protected tweets to be made public.
- Check for impersonations and monitor your brand regularly, as someone else may use your name to impersonate you or your brand on Twitter. This can lead to grave reputation problems for your business, professional, and personal life.
- Engage ZeroFox’s ongoing monitoring services to identify impersonation accounts and, when identified, utilize ZeroFox’s disruption services to have those accounts removed.



Appendix: 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.