

THREAT BULLETIN

# AR20221227-007 [Advisory Report] Twitter Account Data Leak Reported By Independent Researcher

TLP  
**White**

DESCRIPTION

**TLP: CLEAR (TLP v1 WHITE) = Disclosure is not limited.**

## Summary

On December 23, 2022, cybercrime intelligence company @RockHudsonRock tweeted that Ryushi, BreachForums member, was selling data associated with 400 million Twitter accounts.



**Hudson Rock @RockHudsonRock · Dec 24**

**BREAKING: Hudson Rock discovered a credible threat actor is selling 400,000,000 Twitter users data.**

The private database contains devastating amounts of information including emails and phone numbers of high profile users such as AOC, Kevin O'Leary, Vitalik Buterin & more (1/2).

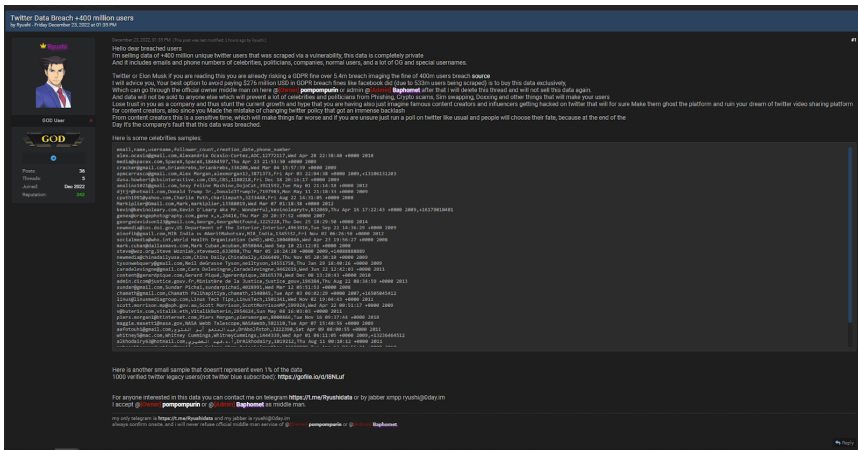
username	follower_count	creat
AOC	12772117	Wed Apr
SpaceX	18468597	Thu Apr
brjankrebs	356208	Wed Mar
alexanrogan13	3871575	Fri Apr
CBS	11880218	Fri Dec
DejaCat	3921592	Tue Mar
DonaldJTrumpJr	7197983	Mon Mar
chrislaporte	3233448	Fri Aug
markkipler	13388819	Wed Mar
kevinolearytv	832869	Thu Apr
GeorgeSotFouad	3225228	Thu Mar
Tatlerior	4963916	Wed Sep
ryanreid	435004	Fri Nov
resuban	855064	Wed Apr
stevanov	855064	Thu Mar
ChinaDaily	4266409	Thu Nov
netlyson	14551758	Thu Jan
Caradeleingne	9462619	Wed Jun
Agar-Apique	20865378	Wed Dec
Justice_gov	190294	Thu Aug
sundarpichai	4028991	Wed Mar
chswarth	1540845	Tue Apr
LinuxTech	1501341	Wed Nov
ScottHarrisonP	5099024	Wed Apr
vitalikbuterin	2964624	Sun Mar
pietseorgan	8000566	Tue Mar

370.2K 77 564 768

Show this thread

Tweet by @RockHudsonRock

According to Alon Gal, CTO of Hudson Rock, this information was likely acquired via an [API vulnerability](#). In his posting, Ryushi calls out Elon Musk to buy the data, threatening him with GDPR violations. The threat actor also provided a list containing account information of 1,000 high-profile Twitter users, one of which was already successfully hacked.



Original Post on BreachForums

As of December 23, 2022, MD-ISAC internal sources have not been able to confirm the authenticity of this data. External researchers, however, have reported that they believe this information to be correct and have validated the account data using independent verification.

**Recommended Action**

To protect the security of your accounts, you should reset all official Government Twitter accounts with a strong and unique password or passphrase.

It is highly recommended to enable multi-factor authentication (MFA) whenever possible and change your password regularly. Eliminating shared accounts or passwords will greatly reduce the chance of your credentials being used on other sites or services. Additionally, the use of a secure password manager will assist you in maintaining your unique passwords across multiple platforms.

**References**

- <https://www.linkedin.com/feed/update/urn:li:activity:7012389466937913344/>
- <https://hackerone.com/reports/1439026>
- <https://breached.vc/Thread-Selling-Twitter-Data-Breach-400-million-users>
- <https://twitter.com/RockHudsonRock/status/1606644986363400193>
- <https://twitter.com/RockHudsonRock/status/1607670630849155073>

**Incident Response**

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report activity related to this bulletin to the MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).
- Report any incidents to the MDSOC by [filling in this form](#).

**Contact Information**

To report suspicious or criminal activity related to information found in this Threat Bulletin, contact the Maryland Security Operations Center at (410) 697-9700 or by email at md-isac@maryland.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. Please state in the report if you are requesting incident response resources or technical assistance related to the incident.

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share this information without restriction. Information is subject to standard copyright rules.

For more information about Traffic Light Protocol (TLP) definitions and usage: <https://www.cisa.gov/tlp>

---