

Telegram issues \$200,000 in Bitcoins challenge to crack code

December 20 2013, by Nancy Owano



Telegram

taking back our right to privacy

(Phys.org) —Anyone able to crack the encryption code of Telegram's message text wins a handsome award, but it needs to be by Telegram's rules. To win the money, you need to decipher the message, find the secret email address, and send an email to it. But wait. We will let the two founders of Telegram say what they are up to in this contest:

"Starting today, each day Paul (+79112317383) will be sending a message containing a secret [email address](#) to Nick (+79218944725). In order to prove that Telegram crypto was indeed deciphered and claim your prize, send an email to the secret email address from Paul's

message. Your email must contain:- The entire text of the message that contained the secret email.- Your Bitcoin address to receive the \$200,000 in BTC.- A detailed explanation of the attack. Encrypted Telegram traffic from and to Paul's account is publicly available for download from this page. You can send Telegram messages to Paul and view his traffic in real time."

The two crypto-contest forces are Telegram founders Pavel and Nikolai Durov. To prove that the competition is run fairly, they intend to publish the participating keys necessary to decrypt the traffic as soon as a winner is announced. In case there is no winner by March 1, [encryption keys](#) will be published at that date.

If contestants are assured the contest is fair, they can also be assured that winning the prize will not be a piece of cake. Telegram is a messaging app with a focus on security as well as speed and simplicity. The company was started earlier this year, founded by the two founders of the social network VKontakte. Their site calls Telegram "the fastest and most secure messaging system in the world."

With Telegram, one can create group chats, share videos, send photos, and forward media. They also added Secret Chats, featuring end-to-end encryption to ensure that a message can only be read by its intended recipient. "We made it our mission to provide the best security on the market," they stated. They also noted that Telegram is free and will stay free—"no ads, no subscription fees, forever." How then can Telegram sustain itself? Their answer is, "We believe in fast and secure messaging that is also 100 percent free. Therefore Telegram is not a commercial project. It is not intended to sell ads, bring revenue or accept outside investment. If Telegram runs out of money, we'll invite our users to donate or add non-essential paid options."

As for the contest, the Telegram team regards the event as rewarding for

them, even if anyone wins. They said, "We will either find a vulnerability in our encryption algorithm and fix it, or get indirect evidence that decrypting our traffic is no easy task."

More information: telegram.org/crypto_contest
core.telegram.org/api

© 2013 Phys.org

Citation: Telegram issues \$200,000 in Bitcoins challenge to crack code (2013, December 20) retrieved 7 July 2024 from <https://phys.org/news/2013-12-telegram-issues-bitcoins-code.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.