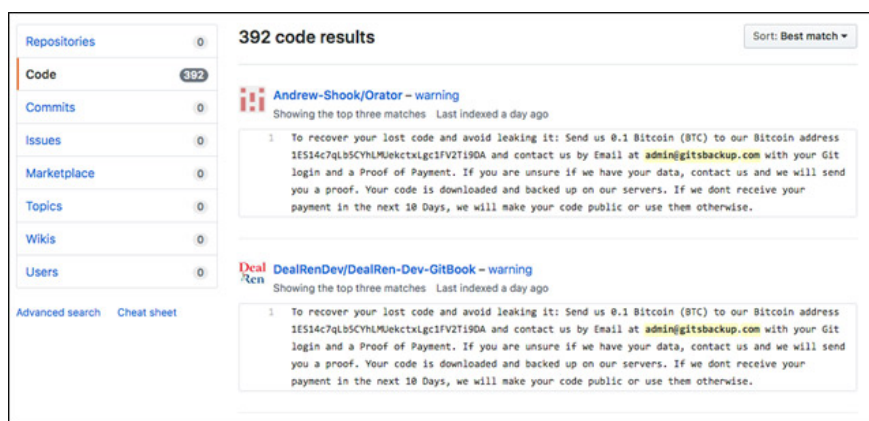


# It was GitHub's turn to be ransomed

GitHub has been hacked for more than a day, causing code and commit repositories to disappear.

Increasingly, data attacks have increased, popular services have been at least once stolen by hackers. Recently GitHub, the largest online code-sharing and storage platform in the world, has been attacked, leaving hundreds of developers losing the entire code archive and committing.

The hackers have left a message to more than 390 victims as follows: "To restore your code repository and avoid leaks, send us 0.1 Bitcoin (BTC - about 566 USD) to your wallet. Bitcoin address: ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA. Contact via email [admin@gitsbackup.com](mailto:admin@gitsbackup.com) with your Git login account with proof of payment (Proof of Payment). If you are not sure we have your data, contact us and we will send you proof. Your code store has been downloaded and backed up on our service. If we do not receive payment in the next 10 days, we will publicize your code repository or use them for other purposes. "



Besides, other services such as GitLab and Bitbucket also suffer from similar disasters, about more than 1,000 BitBucket accounts are affected. This attack took place within 1 day and was prevented in time. The luckier thing is that the code is not deleted but only changed the commit header so it is easy to recover.

Before this situation, GitLab's Security Manager, Kathy Wang, advised the accounts to use password management tools to store passwords, increase security rather than saving them in plaintext form. (unencrypted text) on the relevant repository. Some other developers also advised victims to contact the support team of GitHub, GitLab and Bitbucket before paying any ransom to hackers.

You finished reading the article "**It was GitHub's turn to be ransomed**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.