Hacker swipes Snapchat source code publishes it . Now you can run your own version

by MATTHEW HUGHES — SECURITY

Hacker swipes Snapchat's source code, publishes it on GitHub

99 SHARES

https://tnw.to/3pwiQ

Snapchat doesn't just make messages disappear after a period of time. It also does the same to GitHub repositories — especially when they contain the company's proprietary source code.

So, what happened? Well, let's start from the beginning. A GitHub with the handle i5xx, believed to be from the village of Tando Bago in Pakistan's southeastern Sindh province, created a GitHub repository called Source-Snapchat.

Hard Fork?

Hard Fork.

HARD FORK

At the time of writing, the repo has been removed by GitHub following a DMCA request from Snap Inc (we'll get to that later), so we can't take a closer look and see what it contains. That said, there are a few clues to its contents.

What you see when you visit the repo.

The repository has a description of "Source Code for SnapChat," and is written in Apple's Objective-C programming language. This strongly suggests that the repo contained part or whole of the company's iOS application, although there's no way we can know for certain. It could just as easily be a minor component to the service, or a separate project from the company.

There are two other clues to the identity of the person who published the leaked Snapchat code.

According to the i5xx GitHub account, his name is Khaled Alshehri. This should be taken with a grain of salt, however. For starters, there's nothing stopping the user from listing a fake name. Furthermore, according to several people TNW has spoken to, the surname "Alshehri" isn't especially common in Pakistan.

The profile also links to an online business in Saudi Arabia offering a mixed bag of tech services, from security scanning and iCloud removal, to software development and the sale of iTunes giftcards.

Four days ago, GitHub published a DMCA takedown request from Snap Inc., although it's likely the request was filed much earlier. GitHub, like many other tech giants including Google, publishes information on DMCA takedown requests from the perspective of transparency.

The language used in the DMCA request is fascinating, and conveys a sense of genuine panic in the organization, which in turn suggests that the contents of the repository are legitimate. Rather than using formal legal terminology, the request is predominantly written in all-caps.

To the question "*Please provide a detailed description of the original copyrighted work that has allegedly been infringed. If possible, include a URL to where it is posted online*," the GitHub representative wrote:

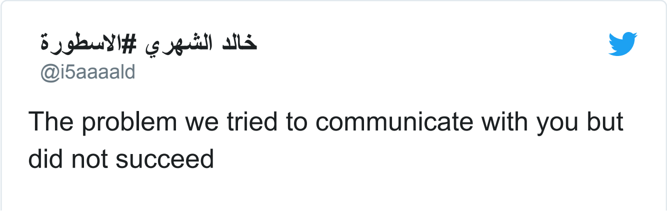
> *"SNAPCHAT SOURCE CODE. IT WAS LEAKED AND A USER HAS PUT IT IN THIS GITHUB REPO. THERE IS NO URL TO POINT TO BECAUSE SNAP INC. DOESN'T PUBLISH IT PUBLICLY."*

The most fascinating part of this saga is that the leak doesn't appear to be malicious, but rather comes from a researcher who found something, but wasn't able to communicate his findings to the company.

According to several posts on a Twitter account believed to belong to i5xx, the researcher tried to contact SnapChat, but was unsuccessful.

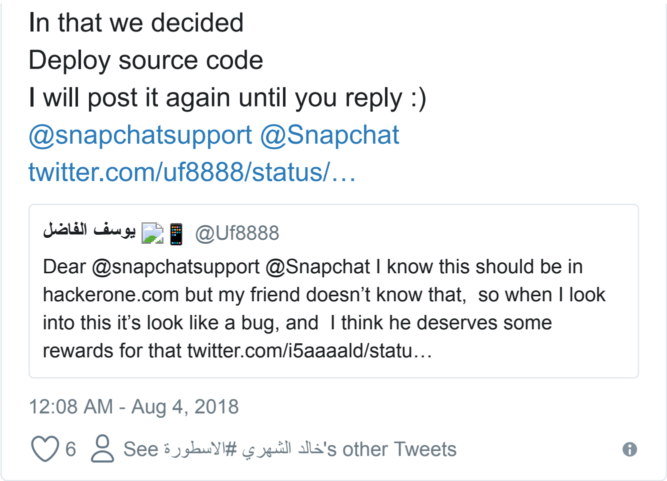
"The problem we tried to communicate with you but did not succeed In that we decided [sic] Deploy source code," wrote i5xx.

The account also threatened to re-upload the source code. "I will post it again until you reply :)," he said.



خالد الشهري #الاسطورة
@i5aaaald

The problem we tried to communicate with you but did not succeed



In that we decided
Deploy source code
I will post it again until you reply :)
@snapchatsupport @Snapchat
twitter.com/uf8888/status/…

يوسف الفاضل 📱 @Uf8888

Dear @snapchatsupport @Snapchat I know this should be in hackerone.com but my friend doesn't know that, so when I look into this it's look like a bug, and I think he deserves some rewards for that twitter.com/i5aaaald/statu…

12:08 AM - Aug 4, 2018

♡ 6 See خالد الشهري #الاسطورة's other Tweets

For what it's worth, it's pretty easy for security researchers to get in touch with Snap Inc. The company has an active account on HackerOne, where it runs a bug bounty program, and is extremely responsive.

According to HackerOne's official statistics, the site replies to initial reports in 12 hours, and has paid out over $220,000 in bounties.

Snap Inc explicitly says it rewards researchers based on severity. I'd imagine that the company's internal infosec team would regard leaked source code as a fairly critical security problem.

The other thing that's especially interesting is that it seems as though the source code remained online for a long period of time before it was removed. I5xx's commit history shows eighteen commits, all occurring between May 23 and 24, and pertaining to the same repository.

As I mentioned, GitHub published Snap's takedown request four days ago. That suggests that the repository was potentially online for over two months.

TNW has reached out to Snap for comment. If we hear back from the company, we'll update this post.