# Analyzing Russian SDK Pushwoosh and Russian Code Contributions

margin.re/2022/12/analyzing-russian-sdk-pushwoosh-and-russian-code-contributions/

Justin Sherman

December 13, 2022

by Justin Sherman

Dec 13, 2022

Reuters recently reported on November 16 that Pushwoosh, the maker of a software development kit (SDK), was falsely representing itself as an American company when in fact the technology company is based in Russia. Its code is reportedly used in thousands of Apple and Google app store applications, and the Centers for Disease Control and Prevention (CDC) and the US Army reportedly removed apps containing Pushwoosh code due to security concerns. Cybersecurity journalist Brian Krebs followed this news by reporting that one of Pushwoosh's developers is Yuri Shmakov, a Russian programmer who in 2013 admitted to writing the Pincer Android Trojan.

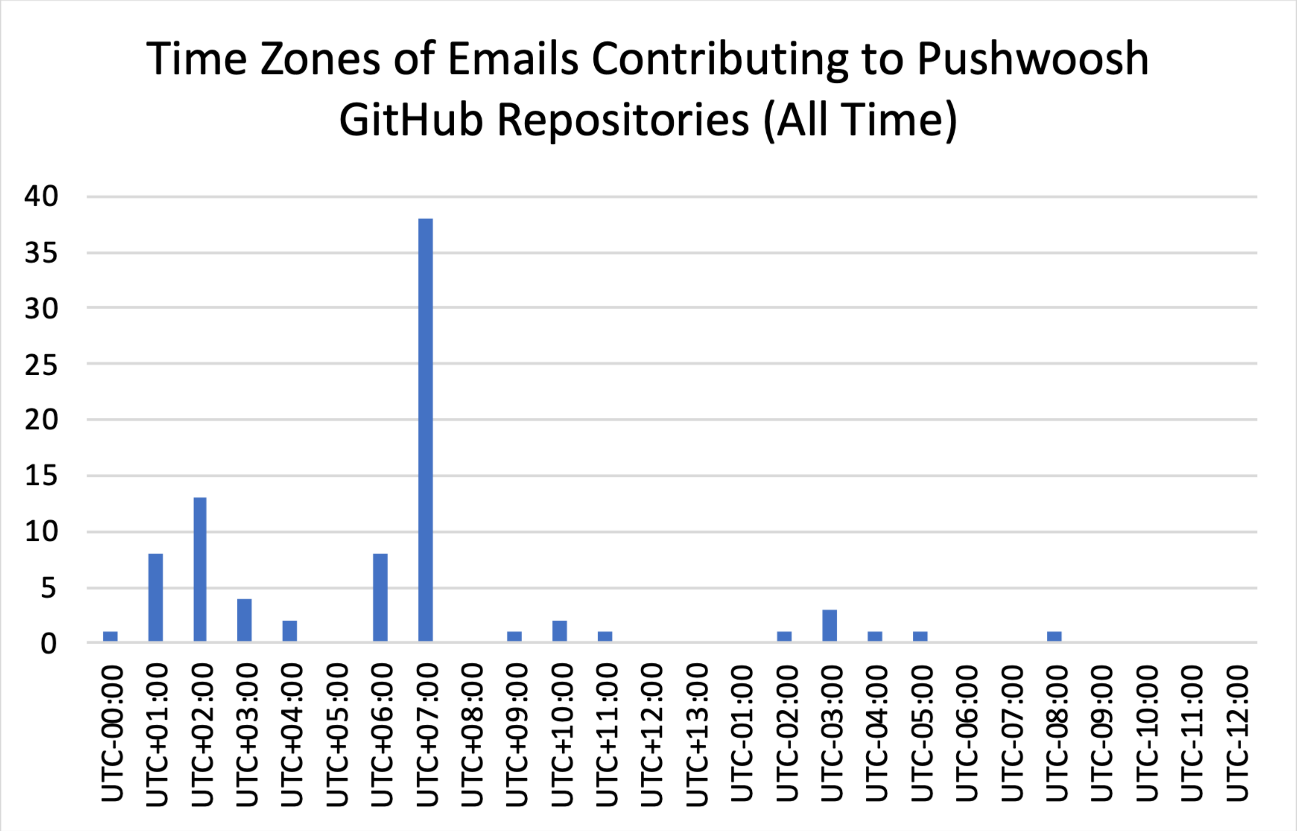
Per the journalists at Reuters, Pushwoosh has presented itself as a US-based company but, in the reporters' words, "is headquartered in the Siberian town of Novosibirsk, where it is registered as a software company" and "is registered with the Russian government to pay taxes in Russia."

Since the Reuters story, Margin Research, as part of its work on the Defense Advanced Research Projects Agency (DARPA)'s SocialCyber effort, has also been looking into Pushwoosh and its Russian connections. To do so, we ingested data from Pushwoosh's GitHub, ran SocialCyber artificial intelligence (AI) analysis on the data, and supplemented that automated analysis with manual analysis of the data and related open-source information.

We found that over time, many contributors to Pushwoosh's GitHub code base appear to be located in Russia, as well as Europe. Several individuals contributing to the Pushwoosh GitHub code base appear to use multiple email addresses. In at least one case, an individual appears to have used an alias first name rather than his actual, full name to push Git code. And, despite Pushwoosh's claims to the contrary, the vast majority of contributions to Pushwoosh's GitHub code base since February 2022 appear to have come from Russian time zones.

## Mapping Contributors' Time Zones

We started by ingesting the data from Pushwoosh's 35 GitHub repositories—including various SDKs made by the company—and processing it using Margin Research's SocialCyber capabilities. First, we found that most emails contributing to Pushwoosh's collection of GitHub repositories, over time, appear to be based in Russia (see below figure). These time zones were identified based on the time zone from which each email contributed the most.



**Source:** Margin Research analysis of Pushwoosh GitHub repository data.

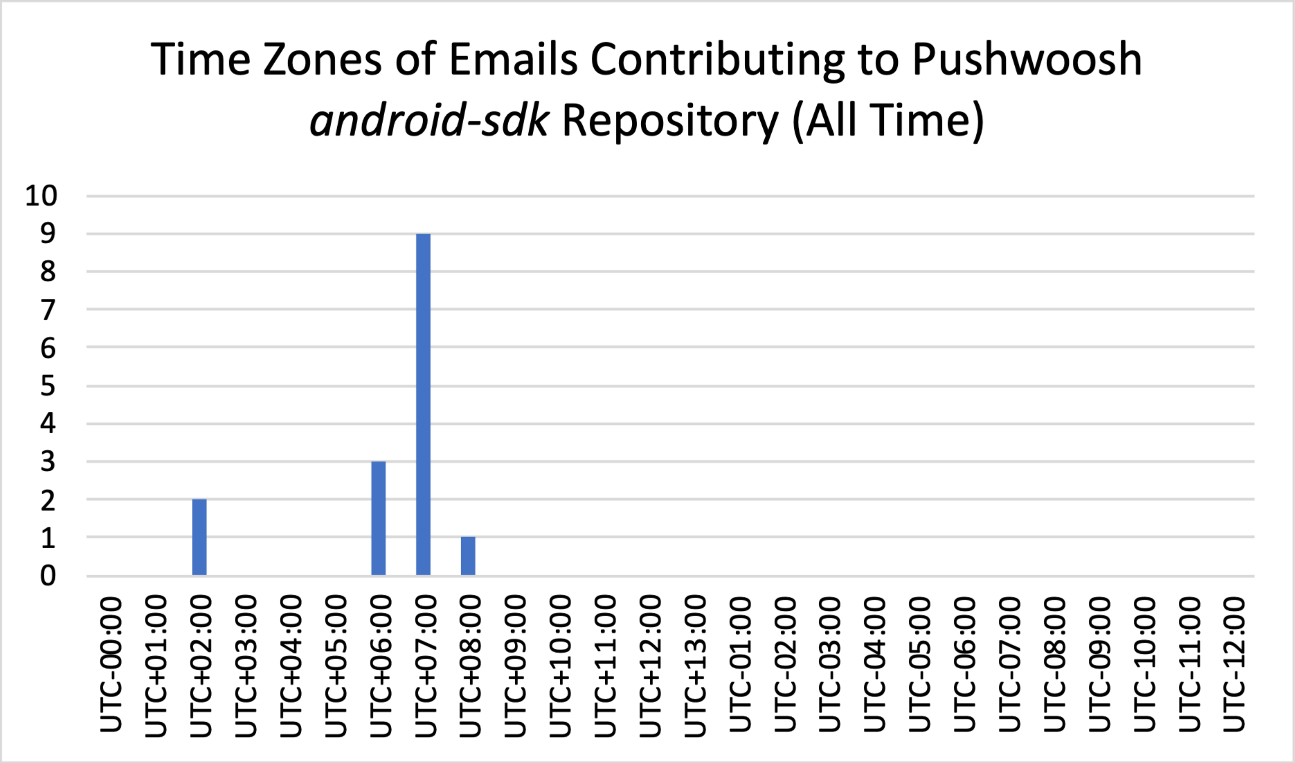
Specifically, 38 emails contributing to Pushwoosh's GitHub appear to be located in the UTC+07:00 time zone, which encompasses Krasnoyarsk, Russia as well as Mongolia, Cambodia, and Indonesia. 13 emails contributing appear to be located in the UTC+02:00 time zone, which encompasses Kaliningrad, Russia as well as Central Africa (from Botswana and the Democratic Republic of the Congo to Egypt, Libya, and South Africa).

And 8 emails contributing appear to be based in the UTC+01:00 time zone, which spans Central Europe—including Albania, Belgium, France, Denmark, the Czech Republic, Italy, Hungary, and Germany. A few other contributions were made from additional time zones, including from the UTC-02:00 time zone, covering Brazil and South Georgia and the South Sandwich Islands; the UTC-03:00 time zone, covering Argentina, Brazil, Chile, Suriname, and Uruguay, among others; and the UTC-08:00 time zone, covering parts of Canada, Mexico, and the United States.

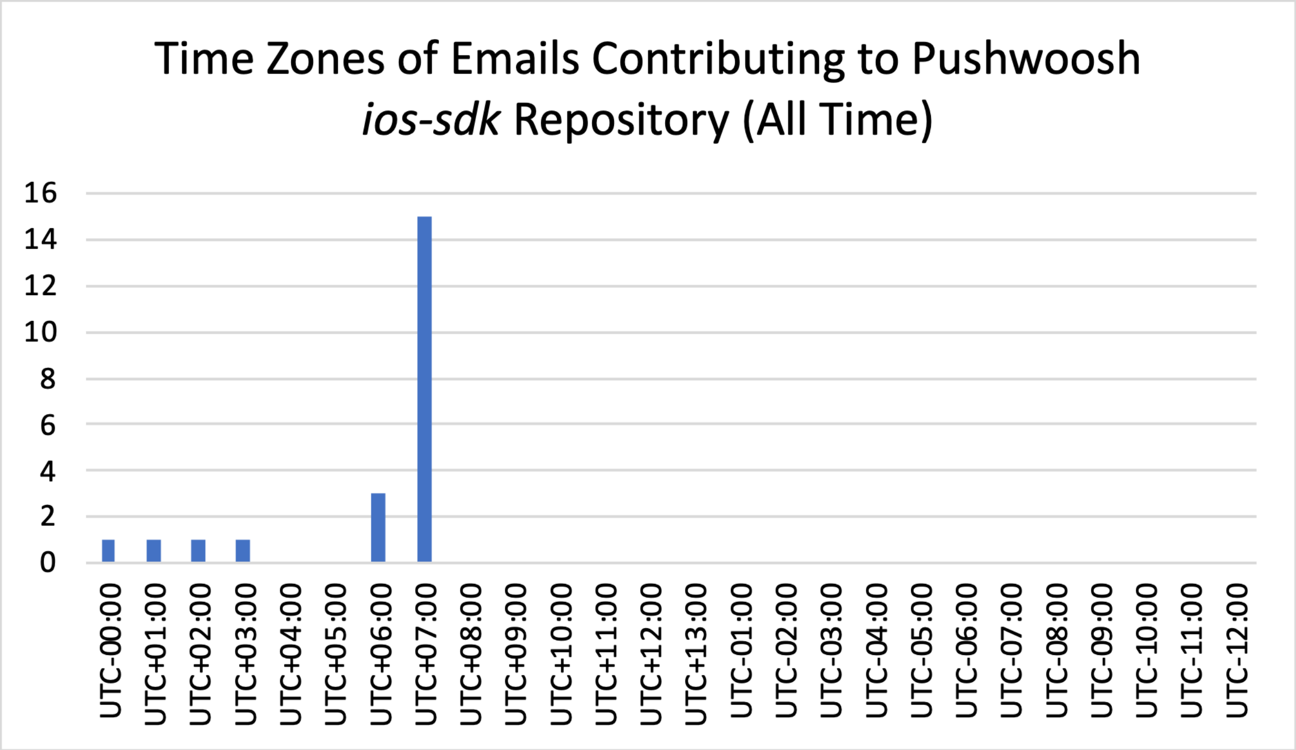
Notably, a few of the contributors appeared to have multiple email addresses that contributed from multiple time zones. For example, several individuals appeared to contribute from multiple places in Russia, and one contributor appeared to contribute from both UTC+01:00 (covering Central Europe) and UTC+02:00 (covering Kaliningrad, Russia as well as Central Africa).

It is also worth noting that some contributors did not appear to use their real name when contributing to the code base; in line with Krebs' reporting, for instance, we also identified one "Michael Shmakov" to actually be Yuri Shmakov, a Russian developer at the company Arello Mobile who has previously developed malware. Other individual contributors appeared to use multiple email addresses. This analysis refers to the time zones associated with the email addresses contributing to the Pushwoosh GitHub repositories, though methodologically, a different visualization could be produced that focuses on contributors as individuals (e.g., clustering emails together if seemingly used by the same person).

We were able to produce this same time zone analysis on specific repositories within Pushwoosh's overall GitHub code base. As demonstrative examples, the below two graphs capture this email contributor time zone analysis for Pushwoosh's android-sdk repository and its ios-sdk repository. Both analyses indicate that, over time, most email addresses contributing to the android-sdk and ios-sdk appear to contribute code from Russia.



**Source:** Margin Research analysis of Pushwoosh GitHub repository data.



**Source:** Margin Research analysis of Pushwoosh GitHub repository data.

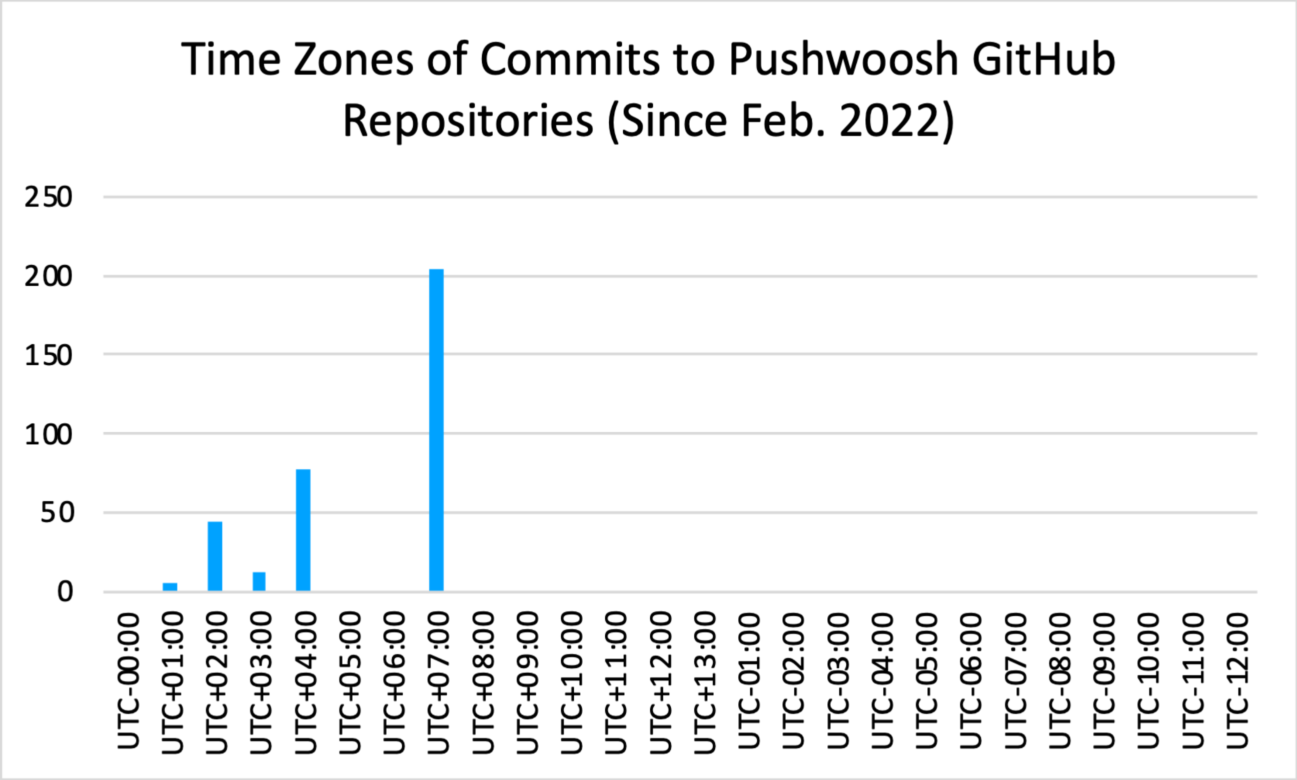
This kind of deeper dive into specific GitHub repositories could be carried out for any of the other Pushwoosh repositories of interest.

## Assessing Apparent Post-February Contributions from Russia

We additionally found evidence refuting one of the central claims made by Pushwoosh in response to the Reuters investigation.

Pushwoosh published a blog post on November 15 stating that “Pushwoosh Inc. used to outsource development parts of the product to the Russian company in Novosibirsk, mentioned in the article. However, in February 2022, Pushwoosh Inc. terminated the contract.” The company’s blog post added: “Since the COVID-19 pandemic, Pushwoosh has been operating globally. Our dedicated engineering and support teams are currently located all over the globe, including Thailand, Germany, Argentina, Mexico, Serbia, Georgia, Turkey, Kazakhstan, Israel, and more.”

**Based on Margin Research’s analysis, this claim about terminating outsourcing to Russia is not true.** Since February 2022, several individuals who appear to be contributing from Russia have committed code to Pushwoosh’s GitHub code base. There have been 344 commits to Pushwoosh’s GitHub repositories since February 2022, and 338 (roughly 98%) of those commits appear to fall within the UTC+02:00 to UTC+12:00 time zones, which cover the entire range of time zones in Russia. Overall, most of the 334 commits since February 2022 have come from the UTC+07:00 time zone (see below graph).



**Source:** Margin Research analysis of Pushwoosh GitHub repository data.
Specifically, 204 commits appear to have come from the UTC+07:00 time zone. 78 commits appeared to come from the UTC+04:00 time zone. And 44 commits appeared to come from the UTC+02:00 time zone, 12 appeared to come from the UTC+03:00 time zone, and 6 appeared to come from the UTC+01:00 time zone.

For example, one contributor has made multiple commits to one of Pushwoosh’s GitHub repositories since February 2022—with an email address that appears to be contributing from UTC+03:00, which covers Moscow, Russia. Another contributor has made numerous commits to one of Pushwoosh’s SDKs since February 2022 and uses email addresses associated with UTC+07:00 (which includes the Krasnoyarsk, Russia area).

The commits cover a wide range of updates to the GitHub repositories for Pushwoosh. Based on the messages uploaded alongside these 344 commits, some code pushes were updates of README files or application displays; others yet updated the permissions associated with a repository’s code or fixed compilation issues within the code.

This information appears to contradict the claim made by Pushwoosh about its use of Russian developers to build code since February.

## Conclusion

This analysis underscores the importance of leveraging openly available data to assess the open-source code ecosystem—as well as in assessing potential misrepresentations of a code base’s origins.

The fact that Russian developers are contributing to an open-source software ecosystem does not immediately mean anything nefarious is underway. Russian developers have built software products or contributed to software products used in many parts of the world with no Russian government involvement. In this particular case, though, it is worth contextualizing the heavy Russian code contributions to Pushwoosh alongside (a) Reuters’ reporting that Pushwoosh misrepresented itself as a US company and (b) Pushwoosh’s claim that it terminated its contract with what it calls a Russian outsourcer in February 2022.

Going forward, this kind of analysis—and the capabilities that underpinned it—may prove highly useful to cybersecurity and national security professionals looking to understand open-source code and identify situations within the broader landscape that may create security risks.