This app will self-destruct: How Belarusian hackers created an alternative Telegram for activists

Daryna Antoniuk

December 29th, 2022

When a 25-year-old activist from Minsk who goes by Pavlo was detained by Belarusian KGB security forces last summer, he knew they would search his phone, looking for evidence of his involvement in anti-government protests.

The police officer asked for Pavlo's password to Telegram, the most popular messenger app among Belarusian activists, which he gave him. The officer entered it and… found nothing. All secret chats and news channels had disappeared, and after a few minutes of questioning Pavlo was released.

Pavlo's secret? A secure version of Telegram, developed by a hacktivist group from Belarus called the Cyber Partisans. Partisan Telegram, or P-Telegram, automatically deletes pre-selected chats when someone enters the so-called SOS password.

P-Telegram is used by activists in Belarus and Iran, as well as Ukrainians living in Russia-occupied territories, according to Yuliana Shemetovets, Cyber Partisans' spokesperson.

The Belarusian app is indistinguishable from the original, as it is built on Telegram's open-source code. However, it promises something that many social networks fail to provide – security for its users.

And as the app's popularity continues to grow, Cyber Partisans — known primarily for cyberattacks against the Belarusian government and high-profile data leaks — are planning to improve it further. Until now, hacktivists spent money from their own pockets on the app, but they have taken steps to obtain grant funding from foreign organizations.

“Foreigners don't want to sponsor our cyberattacks because it's a gray area, but digital security always sparks interest,” Shemetovets told The Record.

Voice of protest

Telegram helped start a revolution in Belarus in the summer of 2020 when thousands of people flooded the streets to protest the results of the presidential election rigged by the country's dictator Alexander Lukashenko.

Protestors used the app to organize and coordinate mass rallies, post updates, photos, and videos, and keep morale up. At that time, Telegram was one of the few sources of information that was not censored or banned by the state.

Telegram news channel Nexta Live, for example, grew from several hundred thousand followers to more than 2 million in the days following the election. Nexta covered the protests in Belarus amid nationwide internet blackouts, publishing footage of police violence, real-time locations of pro-regime security forces, and protesters' pleas for help.

The Belarusian authorities couldn't block the Telegram channel, so in October 2020 they declared Nexta an extremist organization to scare its subscribers, but to no avail.

A Nexta Live Telegram post about the case of three Belarusian men accused of sabotaging a rail line for Russian troops and supplies.

Telegram was the perfect app for the Belarusian protesters. It allows huge chat groups of up to 200,000 people, including encrypted secret chats. The app has virtually no content moderation, allowing people to post footage that Facebook or Instagram would ban or flag as sensitive.

Telegram combines the features of a messenger and a social network like Twitter. It has been adopted by protesters in Hong Kong and Iran, as well as by cybercriminals who use Telegram to advertise their services and publish data leaks.

Since the app was founded in 2013 by Russian tech entrepreneur Pavel Durov and his brother, its growth has been remarkable, reaching 700 million monthly users in June this year.

Telegram's popularity among activists has its drawbacks — the app has attracted the attention of law enforcement agencies in countries where free speech is suppressed, in particular Russia, China, Iran and Belarus.

Lukashenko repeatedly expressed his irritation at the inability to block Telegram in Belarus. In an interview in 2020, he lamented that even if he shuts down the internet in the country, Telegram channels will continue to work from Poland, where many Belarusian activists fled during the protests.

Lukashenko ordered the so-called *siloviki* — pro-regime security forces — to detain “suspicious” people on the streets or in the subway and check their Telegram to identify those who support the protests.

One of the activists was detained while walking in a park, where the police were looking for people who had painted the trees in red and white, the colors of the Belarusian protests. The police officer checked the activist's phone but did not find any evidence there, because he used P-Telegram.

Many Cyber Partisans have repeatedly been in situations where the police checked their phones, according to Shemetovets. They created the app primarily to protect themselves during searches.

Secure alternative

Belarusian hacktivists launched P-Telegram in 2021. About 10,000 people have already downloaded it from GitHub, but the total number of users may be higher, as there are other ways to install the app, but they are harder to track, according to Shemetovets.

The app is developed by a group consisting of three people and several testers — they focus solely on the product and are not involved in cyberattacks.

Shemetovets declined to identify them. Anti-government activity in Belarus is considered treason and is punishable by the death penalty.

The main security feature of P-Telegram is the SOS password — a fake password, which, when entered, activates a number of predefined actions. For example, after entering a fake password, P-Telegram can automatically log out of the account, delete selected chats and channels, and even send a notification about the arrest of the account owners to their friends or families.

P-Telegram also allows other activists to remotely activate the SOS password on the detainee's phone. For this, they need to send a code word to any of the shared Telegram chats.

Another feature on P-Telegram automatically takes photos of law enforcement officers on the front camera when they enter a fake password. “We warn users that this can be dangerous, as this photo will be stored on the phone, revealing that a person may use Partisan Telegram,” Shemetovets said.

Cyber Partisans are constantly updating their app, fixing bugs, and adding new features. They also regularly conduct independent audits to ensure that P-Telegram complies with all security measures.

A recent audit by Open Technology Fund’s Red Team Lab proved that it is almost impossible for "casual observers without technical knowledge and specialized equipment" to identify the existence of P-Telegram on a device.

All Cyber Partisans safety features “performed as expected, and no additional application vulnerabilities were found,” the audit said.

There are also a few shortcomings. The researchers indicated that P-Telegram occupies significantly more space on a disk than the standard version of Telegram. It is "unlikely" that developers will be able to get rid of this vulnerability because "P-Telegram will always be larger than the original," the audit said.

The researchers also observed that the key used to sign official release versions of P-Telegram could be found in two public GitHub repositories, meaning that threat actors could use them to create a malicious version of the app and convince users to install it. Shemetovets told The Record that Cyber Partisans have already addressed this issue.

Other risks

Although P-Telegram protects the data of activists illegally detained by law enforcement officers, the app cannot protect it from Telegram itself.

Telegram doesn't use end-to-end encryption by default, which would ensure that the information is only accessible to the people in the conversation, not to the messaging service.

WhatsApp and Signal, for example, use end-to-end encryption in all their chats and calls, while Telegram only has this option in so-called “secret chats.” This means that the app’s key organizing feature — large groups — are not secured end-to-end, security experts told The Record.

In addition to encryption, Telegram has another problem — it came from Russia. Before founding the app, Pavlo Durov ran Russia’s social media giant VKontakte but was pushed out by pro-Kremlin interests and emigrated to Dubai, where Telegram is now based.

Durov often clashed with the Russian government. In 2017, a Moscow court fined Telegram $11 million after Durov allegedly refused to disclose user information following an FSB request. In 2018, Russia imposed a two-year ban on Telegram due to alleged user privacy issues, but the app has continued to thrive in the country.

Cyber Partisans advise their users to use secret chats so that Telegram cannot pass their information to Belarusian security services in the future. "So far we don't see Telegram being interested in that," Shemetovets said.

Telegram has been blocked temporarily or permanently by governments in Iran, China, Vietnam, and Pakistan. State policy regarding Telegram in some of these countries had the opposite effect as what was intended — interest in the app only increased.

Over 45 million Iranians, half of the population, used Telegram in 2021 despite it being blocked by the government to “safeguard the national interest.”

In September this year, Iranian activists warned that the country’s government was using Telegram to "identify and harm" protesters who took to the streets after a young Kurdish woman died in custody following her arrest by the morality police for wearing an improper hijab.

With the outbreak of protests in Iran, Cyber Partisans translated their app into Persian after being approached by local activists.

During the war, P-Telegram has also become popular in Ukraine, or rather in the Ukrainian territory occupied by Russia. Russian authorities check the Telegram of local residents to see if they have sent any information about the location of Russian troops to the Ukrainian military, or if they read Ukrainian media, according to Shemetovets. P-Telegram can protect them during these searches, she added.

Cyber Partisans have no connection with the Russian opposition and hacktivist groups: "We do not trust them and do not see protest potential in Russia," Shemetovets said.

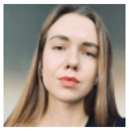
Neither Belarusian nor Russian special services have yet tried to shut down P-Telegram. Shemetovets believes they have other problems. "They can't even secure their own systems," she told The Record.

News

No previous article

No new articles

Daryna Antoniuk



is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.