Meduza is facing the most intense cyberattack campaign in its history

Friday 5 April 2024, by Meduza.io (Date first published: 12 March 2024).

In February 2024, the Russian authorities launched a series of cyberattacks against Meduza more intense than any we've ever faced. The assault began around the time of Alexey Navalny's death — about a month before Russia's upcoming presidential election. Meduza has faced similar attacks before, of course; we've been dealing with them for practically our entire existence, and they became especially intense after the start of the full-scale war in Ukraine. But our tech team has never encountered threats at this scale before.

Blocking our mirror servers

Like many independent Russian media outlets, Meduza uses mirror servers: additional servers that contain copies of our original site. The Russian authorities are aware of this, and they do their best to find these servers and block them, prompting us to launch new ones. Since Meduza was blocked in Russia (immediately after the start of the full-scale war), it's taken the Russian government about two weeks on average to find and block each new server we set up. Since mid-February, however, they've been finding and blocking our servers with increasing frequency; at the moment, it's happening about once every 10–20 minutes.

Disabling our site

Attackers are increasingly trying to disable our website using methods like DDoS attacks, in which our site is bombarded with requests, causing it to either slow down significantly or become inaccessible to legitimate users. Just a few days ago, Meduza recorded one attack in which traffic to our site surged to about 200 times its usual level. We expect to see similar or even larger attacks during Putin's upcoming election.

Attempts to destroy our crowdfunding channels

Meduza is only able to exist — and withstand the Russian authorities' pressure — thanks to financial support from our readers. So it's no surprise that the authorities are doing their best to bring down our crowdfunding infrastructure. Three to four times a minute, attackers try to enter stolen credit card information into our payment system, hoping to break it and force banks to stop working with us. Just like with DDoS attacks, we know how to deal with these tactics, but their frequency has skyrocketed in recent weeks.

Attempts to hack into our journalists' accounts

Since the start of this year, Google has alerted us to multiple hacking attempts by state-sponsored attackers. These kinds of attacks have been rare in the past. We've also seen a sharp increase in explicit threats, demands to remove specific content, phishing attacks, password reset attempts, and even simple spam attacks. Some Meduza employees have been signed up for thousands of email newsletters, with the hackers evidently hoping to overwhelm them and cause them to overlook password reset emails.

Attacks across platforms

In 2024, we noticed an unusual surge in subscribers to our Telegram channel. These new followers are likely part of a plan to report the channel en masse for alleged violations of Telegram's terms of service. Around the same time, the email newsletter platform Mailchimp began experiencing technical issues in Russia, which caused problems for Meduza's Kit and Signal newsletters for five days. Additionally, bots have been flooding our app with negative reviews, complaining about our content online, and creating clones of our employees' accounts and contacting their acquaintances.

What does it all mean?

Meduza, for better or for worse, has an enormous amount of experience working under difficult conditions. And while we don't have direct evidence, we believe this campaign is an attempt to completely destroy Meduza (one of many, but an extremely aggressive one). This is a high-value hit job: the Russian authorities, along with Kremlin-affiliated organizations and hackers, are willing to spend an enormous amount of resources to destroy our infrastructure. But this is only part of the story. By all appearances, this attack is part of a series of events (local Internet outages, blockages of websites that haven't been officially banned, attempts to interfere with messaging apps) that look like preparations by the authorities to impose sweeping Internet blockages — not just against websites but on the level of entire platforms and communication channels.

How can you help?

We can only withstand these attacks with the support of our readers. If you'd like to contribute, sign up here for a recurring donation to Meduza. This is the easiest way to help us fight for freedom of speech and a free Russia.

Thank you for standing by our side during these dark times.

Meduza

P.S.

Meduza

https://meduza.io/en/feature/2024/03/12/meduza-is-facing-the-most-intense-cyberattack-campaign-in-its-history?s=09