Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia

07.03.2022

Matthew Prince

At Cloudflare, we've watched in horror the Russian invasion of Ukraine. As the possibility of war looked more likely, we began to carefully monitor the situation on the ground, with the goal of keeping our employees, our customers, and our network safe.

Helping protect Ukraine against cyberattacks

Attacks against the Internet in Ukraine began even before the start of the invasion. Those attacks—and the steady stream of DDoS attacks we've seen in the days since—prompted us to extend our services to Ukrainian government and telecom organizations at no cost in order to ensure they can continue to operate and deliver critical information to their citizens as well as to the rest of the world about what is happening to them.

Going beyond that, under Project Galileo, we are expediting onboarding of any Ukrainian entities for our full suite of protections. We are currently assisting more than sixty organizations in Ukraine and the region—with about 25% of those organizations coming aboard during the current crisis. Many of the new organizations are groups coming together to assist refugees, share vital information, or members of the Ukrainian diaspora in nearby countries looking to organize and help. Any Ukrainian organizations that are facing attack can apply for free protection under Project Galileo by visiting www.cloudflare.com/galileo, and we will expedite their review and approval.

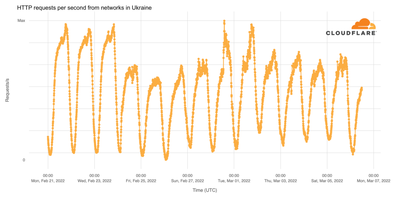
Securing our customers' data during the conflict

In order to preserve the integrity of customer data, we moved customer encryption key material out of our data centers in Ukraine, Russia, and Belarus. Our services continued to operate in the regions using our Keyless SSL technology, which allows encryption sessions to be terminated in a secure data center away from where there may be a risk of compromise.

If any of our facilities or servers in Ukraine, Belarus, or Russia lose power or connectivity to the Internet, we have configured them to brick themselves. All data on disk is encrypted with keys that are not stored on site. Bricked machines will not be able to be booted unless a secure, machine-specific key that is not stored on site is entered.

Monitoring Internet availability in Ukraine

Our team continues to monitor Internet patterns across Ukraine. While usage across the country has declined over the last 10 days, we are thankful that in most locations the Internet is still accessible.



We are taking steps to ensure that, as long as there is connectivity out of the country, our services will continue to operate.

Staying ahead of the threat globally

Cyber threats to Ukrainian customers and telecoms is only part of the broader story of potential cyberattacks. Governments around the world have emphasized that organizations must be prepared to respond to disruptive cyber activity. The US Cybersecurity and Infrastructure Security Agency (CISA), for example, has recommended that all organizations—large and small—go "Shields Up" to protect themselves from attack. The UK's National Cyber Security Centre has encouraged organizations to improve their cyber resilience.

This is where careful monitoring of the attacks in Ukraine is so important. It doesn't just help our customers in Ukraine — it helps us learn and improve our products so that we can protect all of our customers globally. When wiper malware was identified in Ukraine, for example, we adapted our Zero Trust products to make sure our customers were protected.

We've long believed that everyone should have access to cybersecurity tools to protect themselves, regardless of their size or resources. But during this time of heightened threat, access to cybersecurity services is particularly critical. We have a number of free services available to protect you online — and we encourage you to take advantage of them.

Providing services in Russia

Since the invasion, providing any services in Russia is understandably fraught. Governments have been united in imposing a stream of new sanctions and there have even been some calls to disconnect Russia from the global Internet. As discussed by ICANN, the Internet Society, the Electronic Frontier Foundation, and Techdirt, among others, the consequences of such a shutdown would be profound.

The scope of new sanctions issued in the last few weeks have been unprecedented in their reach, frequency, and the number of different governments involved. Governments have issued sweeping new sanctions designed to impose severe costs against those who supported the invasion of Ukraine, including government entities and officials in Russia and Belarus. Sanctions have been imposed against Russia's top financial institutions, including Russia's two largest banks, fundamentally altering the ability of Russians to access capital. The entire break away territories of Donetsk and Luhansk, including all of the residents of those regions, are subject to comprehensive sanctions. We've seen sanctions on state-owned enterprises, elite Russian families, and the leaders of intelligence-directed disinformation outlets.

These sanctions are intended to make sure that those who supported the invasion are held to account. And Cloudflare has taken action to comply. Over the past several years, Cloudflare has developed a robust and comprehensive sanctions compliance program that allows us to track and take immediate steps to comply with new sanctions regulations as they are implemented. In addition to an internal compliance team and outside counsel, we employ third party tools to flag potential matches or partial ownership by sanctioned parties, and we review reports from third-parties about potential connections. We have also worked with government experts inside and outside of the United States to identify when there is a connection between a sanctioned entity and a Cloudflare account.

Over the past week, our team has ensured that we are complying with these new sanctions as they are announced. We have closed off paid access to our network and systems in the new comprehensively-sanctioned regions. And we have terminated any customers we have identified as tied to sanctions, including those related to Russian financial institutions, Russian influence campaigns, and the Russian-affiliated Donetsk and Luhansk governments. We expect additional sanctions are likely to come from governments as they determine additional steps are appropriate, and we will continue to move quickly to comply with those requirements as they are announced.

Beyond this, we have received several calls to terminate all of Cloudflare's services inside Russia. We have carefully considered these requests and discussed them with government and civil society experts. Our conclusion, in consultation with those experts, is that Russia needs more Internet access, not less.

As the conflict has continued, we've seen a dramatic increase in requests from Russian networks to worldwide media, reflecting a desire by ordinary Russian citizens to see world news beyond that provided within Russia.

We've also seen an increase in Russian blocking and throttling efforts, combined with Russian efforts to control the content of the media operating inside Russia with a new "fake news" law.

The Russian government itself, over the last several years, has threatened repeatedly to block certain Cloudflare services and customers. Indiscriminately terminating service would do little to harm the Russian government, but would both limit access to information outside the country, and make significantly more vulnerable those who have used us to shield themselves as they have criticized the government.

In fact, we believe the Russian government would celebrate us shutting down Cloudflare's services in Russia. We absolutely appreciate the spirit of many Ukrainians making requests across the tech sector for companies to terminate services in Russia. However, when what Cloudflare is fundamentally providing is a more open, private, and secure Internet, we believe that shutting down Cloudflare's services entirely in Russia would be a mistake.

Our thoughts are with the people of Ukraine and the entire team at Cloudflare prays for a peaceful resolution as soon as possible.

Discuss on Twitter | Discuss on Hacker News | Discuss on Reddit

Ukraine | Russia | Belarus | Internet Traffic | Security

Follow on Twitter
Matthew Prince | @eastdakota
Cloudflare | Cloudflare

RELATED POSTS

March 04, 2022 4:10PM

Internet traffic patterns in Ukraine since February 21, 2022

Cloudflare operates in more than 250 cities worldwide where we connect our equipment to the Internet to provide our broad range of services...

By John Graham-Cumming

Cloudflare Radar, Internet Traffic, Ukraine