ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

# How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic

**Authors:** *Mingshi Wu, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin, Eric Wustrow*

**In Proceeding of**: *USENIX Security Symposium 2023*

## Summary

One of the cornerstones of censorship circumvention is ***fully encrypted protocols***. In early November 2021, the Great Firewall of China (GFW) deployed a new censorship technique that passively detects---and subsequently blocks---fully encrypted traffic in real time. The GFW's new capability affects a large set of popular censorship circumvention protocols, including but not limited to Shadowsocks, VMess, and Obfs4.

In this work, we measure and characterize how the GFW has been censoring fully encrypted traffic. Our understanding of the GFW's new censorship mechanism helps us ***derive several practical circumvention strategies.*** We ***responsibly disclosed our findings and suggestions*** to the developers of different anti-censorship tools, ***helping millions of users*** successfully evade this new form of blocking. In addition, we work hard to ***communicate our research findings,*** spreading awareness of censorship to a broad range of audiences, from non-technical users in censored areas, to the experts in the anti-censorship community.

## 1. Widespread adoption of our solution

As detailed in *Section 8.3 Responsible Disclosure* of our USENIX Security 2023 paper, our research findings and solutions have been deployed by and integrated into all mainstream fully-encryption based anti-censorship tools, including but not limited to ***Shadowsocks, V2Ray, Outline by Google Jigsaw, Lantern, Psiphon, Conjure, and ExpressVPN***. ***Each of these tools has millions of users*** and our work has protected them from the latest censorship by multiple nations, including the GFW:

> *On November 16, 2021, ten days after the GFW employed this new blocking [10], we revealed details of this new blocking to the public [37, 38]. With the development of our understanding of this new blocking, we derived and evaluated different circumvention strategies. We responsibly and promptly shared our findings and suggestions with the developers of various popular anti-censorship tools that have millions of users , including Shadowsocks [22], V2Ray [59], Outline [42], Lantern [20], Psiphon [21], and Conjure [33].*
>
> *On January 13, 2022, we shared our first circumvention strategy with a group of developers. This solution, detailed in Section 8.1, requires minimal code changes to the clients and no changes to the servers. By January 14, 2022, Shadowsocks-rust developer zonyitoo, V2Ray developer Xiaokang Wang and Sagernet*

> *developer nekohasekai had already added this circumvention solution as an option to their clients [72, 62, 48]. On October 4, 2022, database64128 implemented a user-customizable version of this strategy on Shadowsocks-go [18]. On October 25, 2022, Outline developers adopted a highly customizable solution for their client [56]. On October 14, 2022, we released a modified Shadowsocks [8] that employed the popcount-altering strategy we detailed in Section 8.2.*

## 2. Millions in China and Iran helped by our contributions

The updated anti-censorship tools have been used by various major censorship circumvention service providers ***in both China and Iran***. Our proposed anti-censorship strategies ***are still used today***, helping millions of users bypass censorship every day:

> *As of February 14, 2023, all circumvention strategies adopted by these tools are reportedly still effective in China. In January 2023, Outline developers reported that the number of Outline servers (that opted-in for anonymous metrics) had doubled since they adopted the mitigation above. In January 2023, a large circumvention service provider in China (that asked not to be named at this time) also implemented our proposed scheme and has also found success.*
>
> *While we did not study countries other than China, our proposed circumvention strategies are reported to be also working in Iran, another country that reportedly blocks and throttles fully encrypted proxies [65]. On February 13, 2023, Lantern developers reported that the adopted protocol "accounted for the majority of our Iran traffic" since January 2023. On February 13, 2023, a different circumvention service provider reported that, after enabling Outline's mitigation feature in November 2022, their services turned from being completely blocked to serving 850k daily users from Iran.*

## 3. Spreading awareness of censorship to a diverse group of audiences

We work to inform anti-censorship tool developers and users in censored areas of evolving censorship incidents. We publish our reports in both English and Chinese, and ***have more than 2 millions views to date***. Additionally, our Tweets on this work have ***hundreds of thousands of views and thousands of likes***.

## 4. Reproducibility and open access data

In an effort to stimulate future anti-censorship research, we ensure that our code and dataset is open to the public. We received ***all three artifact evaluation badges*** from the USENIX Security Artifact Evaluation Committee, confirming the reproducibility of our work. In addition, our publicly available dataset has received ***100+ stars*** on Github, indicating strong researcher engagement.

## 5. Community Recognition

Our work won the ***Best Practical Paper Award*** from the 2023 Free and Open Communications on the Internet (FOCI'23), further demonstrating its value and impacts in the anti-censorship research community. By submitting our work to CSAW'23, we hope to spread out the awareness of Internet censorship to an even broader range of audiences.

**https://gfw.report**
**@gfw-report**
**@gfw_report**