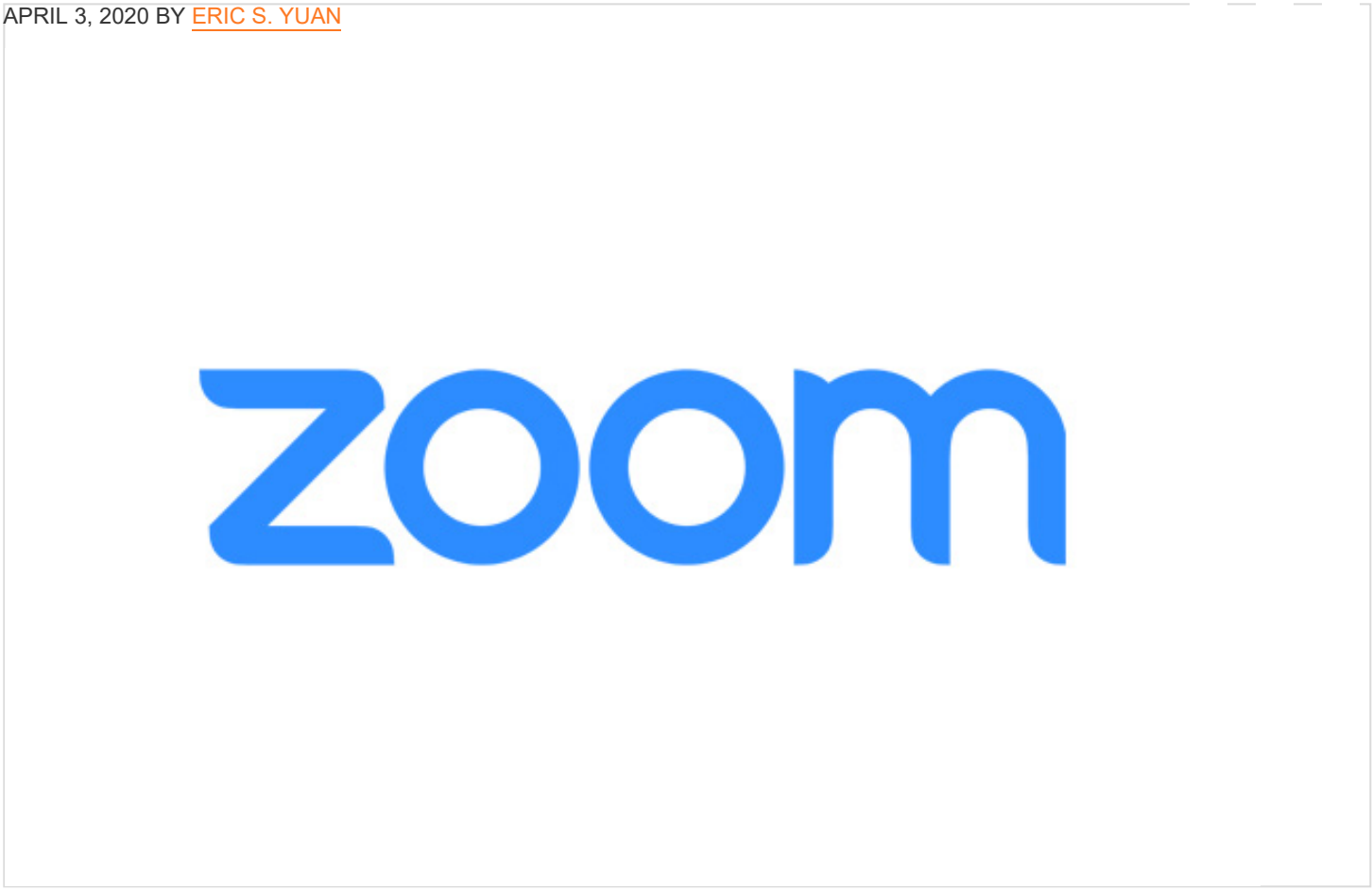
Response to Research From University of Toronto's Citizen Lab

APRIL 3, 2020 BY ERIC S. YUAN



We want to address research published by University of Toronto's Citizen Lab this morning. We've taken steps to address two primary topics — geo-fencing and meeting encryption — and are sharing these steps as part of our ongoing commitment to improve security and privacy.

In our urgency to come to the aid of people around the world during this unprecedented pandemic, we added server capacity and deployed it quickly — starting in China, where the outbreak began. In that process, we failed to fully implement our usual geo-fencing best practices. As a result, it is possible certain meetings were allowed to connect to systems in China, where they should not have been able to connect. We have since corrected this, and would like to use this blog post to explain how our system typically works, where our misstep occurred, and how we will prevent these kinds of problems in the future. We have also been working on improving our encryption and will be working with experts to ensure we are following best practices.

We appreciate the questions we are getting, and continue to work actively to address issues as we identify them. As video communications become more mainstream, users deserve to better understand how all these services work, including how the industry — Zoom and its peers — manages operations and provides services in China and around the world.

Geo-fencing

During normal operations, Zoom clients attempt to connect to a series of primary datacenters in or near a user's region, and if those multiple connection attempts fail due to network congestion or other issues, clients will reach out to two secondary datacenters off of a list of several secondary datacenters as a potential backup bridge to the Zoom

platform. In all instances, Zoom clients are provided with a list of datacenters appropriate to their region. This system is critical to Zoom's trademark reliability, particularly during times of massive internet stress.

Even during these periods of high traffic, Zoom's systems are designed to maintain geo-fencing around China for both primary and secondary datacenters — ensuring that users outside of China do not have their meeting data routed through Zoom's mainland China datacenters (which consist of infrastructure in a facility owned by Telstra, a leading Australian communications provider, as well as Amazon Web Services).

However, in February, Zoom rapidly added capacity to our Chinese region to handle a massive increase in demand. In our haste, we mistakenly added our two Chinese datacenters to a lengthy whitelist of backup bridges, potentially enabling non-Chinese clients to — under extremely limited circumstances — connect to them (namely when the primary non-Chinese servers were unavailable). This configuration change was made in February.

Importantly:

> Upon learning of the oversight yesterday, we immediately took the mainland China datacenters off of the whitelist of secondary backup bridges for users outside of China.
>
> This situation had no impact on our Zoom for Government cloud, which is a separate environment available for our government customers and any others who request the specifications of that environment.
>
> Zoom has layered safeguards, robust cybersecurity protection, and internal controls in place to prevent unauthorized access to data, including by Zoom employees — regardless of how and where the data gets routed.

Meeting Encryption

We recognize that we can do better with our encryption design. Due to the unique needs of our platform, our goal is to utilize encryption best practices to provide maximum security, while also covering the large range of use cases that we support. We are working with outside experts and will also solicit feedback from our community to ensure it is optimized for our platform. In accordance with the action plan I outlined in my note to our users on 4/1, we expect to have more to share on this front in the coming days.

More Work Ahead

We recognize how important it is that our systems operate in the manner that we intend — and that is expected of us from our users, even as we all adjust to the new demands this pandemic has brought us all. As part of the security program we announced earlier, we are implementing additional process and technical controls around our inter-region isolation.

We have an immense responsibility to get things right, particularly at a time like this. We know we have a long way to go to earn back your full trust, but we are committed to throwing ourselves into bolstering our platform's security with the same intensity that we committed to ensuring that everyone would be able to remain connected.

ANNOUNCEMENTS