# Myriad Problems of Zoom: Mistakes in Goodwill or Malevolent Negligence
## by Boran Göher

Founded in 2011, the video-conference software Zoom has seen a massive surge in its popularity after the COVID-19 outbreak. Going from 10 million to 300 million users amidst the outbreak, the company has almost multiplied its user count by 30. This rapid growth was not without its downsides for the company however, amplifying and bringing into light the many problems Zoom has concerning privacy and security. With all these in mind, it should be no surprise that the question of whether Zoom could have prevented, or at least alleviated, these problems is a hotly debated one.

Although the worldwide popularity of Zoom is only a few months old, its widespread usage within business circles can be traced back to 2013, when the company released its standalone application. As such, it would be hardly appropriate to consider only these last months when investigating the history of problems the company has faced.

The company has been facing issues nonstop since the first wave of spoofing in 2018, where a significant number of users were tricked into logging in to fake websites which led to their accounts being compromised. Zoom has since experienced issues with data mining, unauthorized recording of calls, calls being accidentally routed through Chinese servers, its controversial redefinition of end-to-end encryption, the famous incidents of “zoombombing “and many more topics. It seems that perhaps the root cause of all these problems is the “ease of use at any cost” policy the company pursues, causing some very important security options to be turned off by default and some of its problems being swept under the rug.

Yet some prominent tech writers were reluctant to blame Zoom for all these problems, as they felt it was an inevitable outcome for a company with the growth rate of Zoom. Some have also stated that soon, Zoom just might become the safest video conference software because of how enthusiastic the company has been to fix its issues. “Zoom will soon be the most secure conferencing tool out there.” says cybersecurity journalist Kim Zetter. Proponents of this opinion also find support from the CEO of Zoom, Eric Yuan, who stated that “…due to this COVID-19 crisis, we moved too fast.” And that they hope to fix their “missteps”. To accomplish this, the company seems to, at least partially, have backed down from their “ease of use at any cost” policy.

Most people hold the opposite opinion though, considering it negligence by the company as the main cause of problems. They argue that the company is responsible for the lion’s share of problems, citing the company’s dishonest statements about end-to-end encryption and call routing systems. Zoom originally advertised their system as end-to-end encrypted but as people looked more into it, it turned out that this was not the case. This means that Zoom could access the specifics of a private conversation when they claimed that they could not. In the case of call routing Zoom has stated that, with the increased user load, they couldn’t keep up the correct routing practices which allowed some foreign calls to go through Chinese servers without the users’ knowledge. Critics use these two specific cases to argue that ill-minded ignorance is the

cause of Zoom's problems and that the company's "ease of use at any cost" policy is a flimsy cover for its dishonest advertising and malicious coding practices.

If there is one thing both sides agree on, though, it is that Zoom has started to take the correct steps towards solving its issues and should become a much more secure and reliable software as time passes. Amidst all this, one thing remains sure; Zoom remains massively popular despite all its issues and it seems that it is not going to be losing that popularity easily.