Growth is booming, reaching $ 38 billion but Zoom is facing security and privacy concerns

Despite the explosive growth in the number of users, Zoom is being doubted by security experts about the security and privacy of users.

Video call app maker Zoom is doing business aggressively as the corona pandemic forces millions of people around the globe to work from home.

Starting listing on the stock exchange in April 2018, and on Monday, the company's stock price soared 22% to $ 159.07 per share, the company's highest daily rate. . As of January 31, this year, Zoom stock has increased galloping to more than 100%.

The company has not disclosed its number of new users at the moment, but a document sent to investors last Friday showed that the spike in usage has led to an increase in infrastructure costs.

Zoom stock has been booming since the beginning of this year.

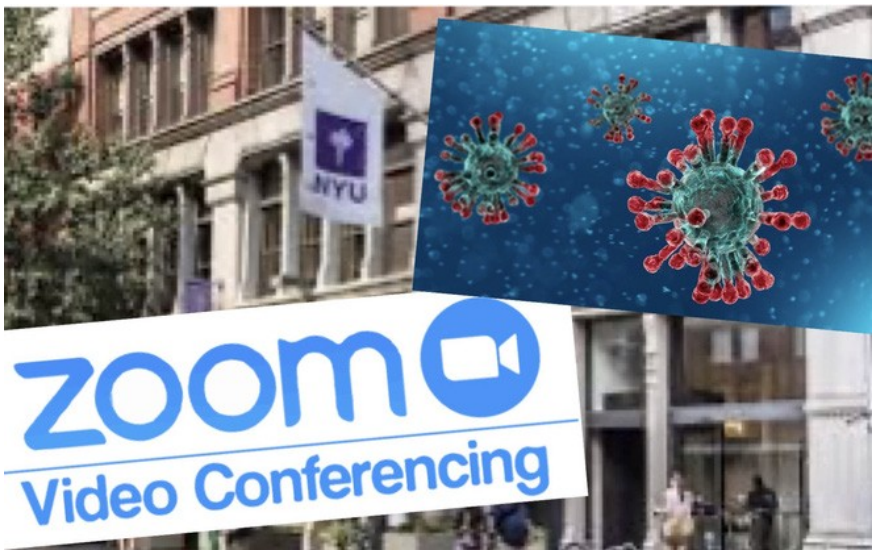
Over the past few weeks, the company has begun removing the 40-minute limit on online conferencing calls and releasing them free to schools in the US, the Middle East and Europe, when these places are forcing them. must be closed before the corona virus outbreak.

But while Zoom is constantly expanding its user base to hundreds of thousands of offices and schools around the world, security experts are also raising concerns regarding security and protection policies. company data.

Speaking with Business Insider, some cybersecurity experts emphasize an in-app feature that will allow meeting organizers on Zoom to track user interaction, easily. incorrect file sharing, and lack of clarity in company privacy policies.

Attackers can take advantage of Zoom as it becomes more and more popular

In January, cybersecurity firm Check Point Research discovered a flaw in the Zoom application that would allow hackers to listen to uninvited video conferencing meetings, and gain access to internal files. like other sensitive information.



The corona virus outbreak has caused demand for Zoom to skyrocket when demand for remote work explodes.

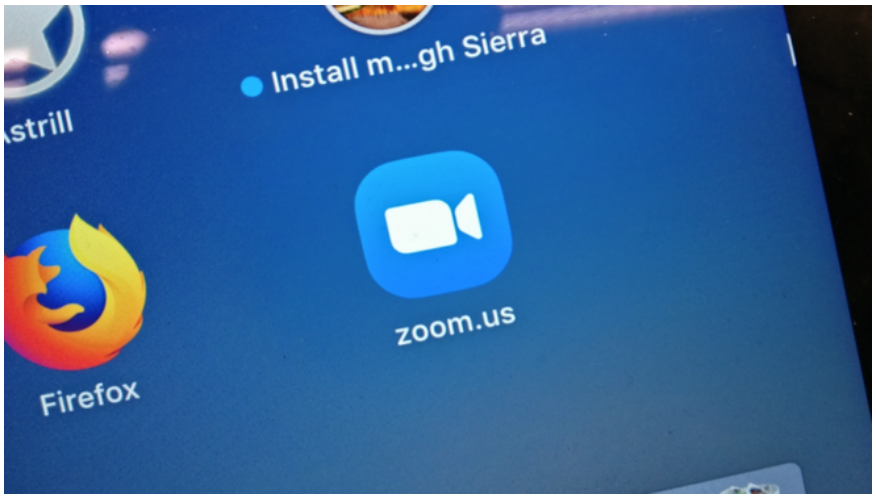
Tom Lysemose Hansen, CTO of security firm in Promon application, told Business Insider that Zoom's vulnerabilities " *have become clear* " after the incident.

" *As with any type of software, video conferencing platforms are vulnerable to hacking, and unfortunately, as more and more people start using this technology, hackers will start," he said. target them with increasing frequency* . "

Responding to Business Insider, Zoom said, the flaw that Check Point pointed out has been fixed before they were made public, adding that they have updated some features (Example ID verification in and Device Lock) to "limit the effectiveness of malicious tools."

Features on Zoom can allow superiors to track employees

But Mr. Hansen also criticized Zoom for a feature in another application "employee tracker", which allows meeting room owners to monitor whether other users have let the application run on the home screen in the last 30 seconds or not. is not.



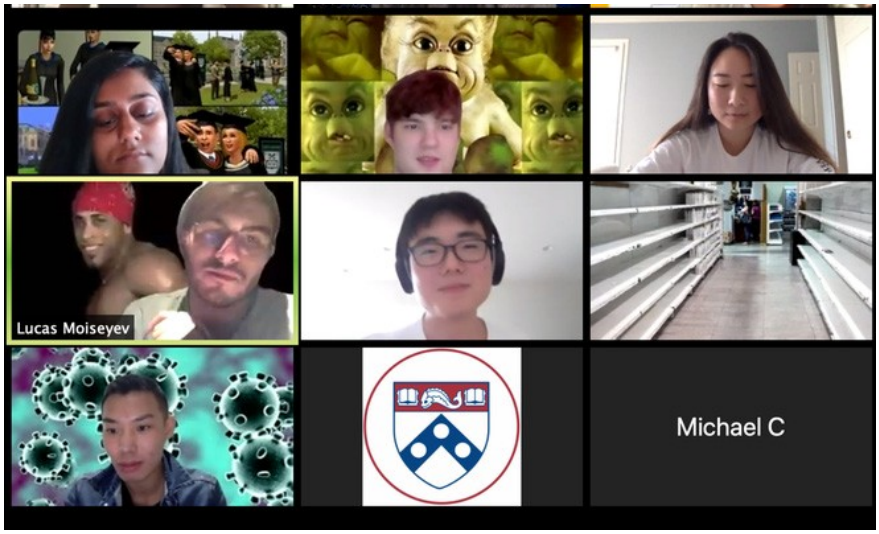
Camilla Winlo, director of privacy consultancy DQM GRC, agrees, saying the feature could be used by employers to mislead information.

" *It's like having someone open a document to take notes or play Solitaire in* ." She said. " *Organizations should provide detailed training on how these features should and should not be used, but to be honest, most people just want to work remotely and run applications soon. use it now* . "

Zoom indicates that the feature is disabled by default, and can only be enabled by the meeting organizer and appears only if the meeting organizer shares his screen.

" *A feature that allows meeting organizers to see signs of someone not paying attention to the Zoom app within 30 seconds only appears when the meeting organizer shares his screen* ." Zoom representative said.

" *If the organizer does not share his screen, there will be no indication of whether the meeting participants are interested in Zoom. It will also not monitor any audio or video content. of the meeting* . "



More recently, the " *Zoombombing* " issue has become more and more serious, as troublemakers can jump into public conference meetings and share inappropriate photos and other spam messages. Chipotle Company and many other organizations have been attacked by such troublemakers.

In response, Zoom released a new guide explaining how meeting organizers can prevent anonymous guests from sharing inappropriate files.

As its application becomes more and more popular, the company is facing more transparent calls for how to handle user data.

In an open letter published by the digital rights group, Access Now, last week, activists called on Zoom to publish " *a transparent report* ", as companies like Google and Microsoft have stated. Be clear about how they handle user data.

A spokesman for Zoom said the company " *does not sell user data in any form to anyone. . Zoom only collects user data to the extent necessary to provide operational support." and to improve our services, Zoom must collect technical information such as IP address, operating system details and user device details in order for our service to function. correctly* . "