Make sure social meeting apps are legit

With the rise of physical distancing, Kaspersky experts investigated the threat landscape for social meeting applications to make sure users are safe and their communication experience is enjoyable.

Subsequent analysis detected around 1300 files that have names similar to prominent applications like Zoom, Webex, and Slack. Social meeting applications currently provide easy ways for people to connect via video, audio or text when no other means of communication are available. However, cyber fraudsters do not hesitate to use this fact and try to distribute various cyber threats under the guise of popular apps.

Amid those 1300 files, 200 various threats were detected. The most prevalent are two adware families – DealPly and DownloadSponsor.

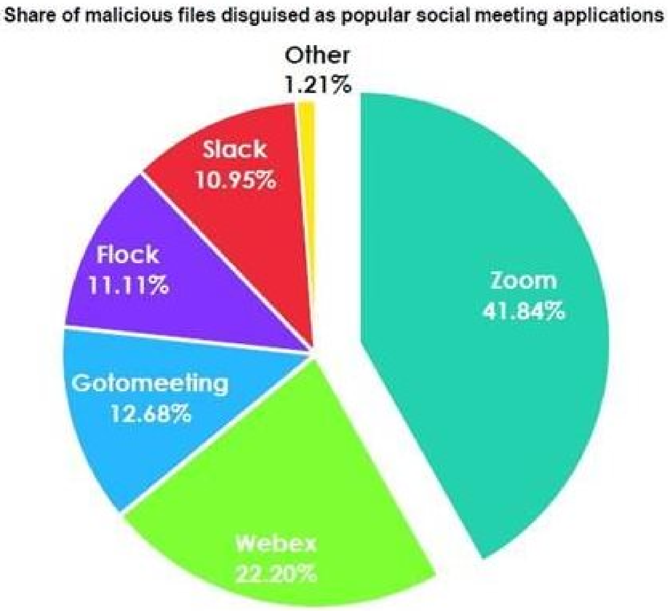

Image supplied

Both families are installers that show ads or download adware modules. Such software typically appears on users' devices once they are downloaded from unofficial marketplaces.

While adware is not a type of malicious software, it can still pose a privacy risk. There are products successfully detect and block DealPly and DownloadSponsor.

Apart from adware, in a few cases, Kaspersky experts found threats disguised as .lnk files – shortcuts to applications. In fact, the vast majority of them were detected as Exploit.Win32.CVE-2010-2568 - a quite old, yet still widespread malicious code that allows the attackers to infect some computers with additional malware.

The real "king" of social meeting applications in terms of the one whose name is most used by criminals to try to distribute cyber threats is Skype. Kaspersky experts were able to find 120,000 various suspicious files that use the name of this application. Moreover, unlike the names of other apps, this particular name is used to distribute not only adware but also various malware - particularly Trojans.

Source: pixabay.com

"To be clear: it doesn't look like there is a dramatic spike in the number of attacks or number of files that are disguised as popular social meeting apps. The actual numbers of these files that we are seeing in the wild are quite moderate. They are not moderate when it comes to Skype, but this application, due to its popularity, has traditionally been a target for cyber threat actors for many years. At the same time, we consider it important to let people know about the existence of such threats.

In the current landscape, when most of us are working from home, it is extremely important to make sure that what we use as a tool for online social meeting is downloaded from a legitimate source, set up properly and doesn't have severe unpatched vulnerabilities," comments Denis Parinov, a security expert at Kaspersky.