Cyber-espionage group uses popular messenger's brand for targeted attacks

Kaspersky Lab researchers have discovered a wave of cyber-espionage targeted attacks aimed at Central Asian diplomatic organisations.

Source: pixabay.com

The Trojan called “Octopus”, disguised as a version of a popular and legitimate online messenger, was attracting users amid the news of a possible ban on Telegram messenger in the region. Once installed, Octopus provided attackers with remote access to victims’ computers.

Threat actors are constantly seeking exploitable modern trends and adjusting their methods in order to jeopardise users’ privacy and sensitive information across the world. In this case, the possible prohibition of the widely used Telegram messenger allowed threat actors to plan attacks using the Octopus Trojan, subsequently providing the hackers with remote access to a victim’s computer.

Threat actors distributed Octopus within an archive disguised as an alternative version of Telegram messenger for Kazakh opposition parties. The launcher was disguised with a recognisable symbol of one of the opposition political parties from the region, and the Trojan was hidden inside.

Once activated, the Trojan gave the actors behind the malware opportunities to perform various operations with data on the infected computer, including, but not limited to, deletion, blocks, modifications, copying and downloading. Thus, the attackers were able to spy on victims, steal sensitive data and gain backdoor access to the systems.

The scheme has some similarities with an infamous cyber-espionage operation called Zoo Park, in which the malware used for the APT was mimicking a Telegram application to spy on victims.

Using Kaspersky algorithms that recognise similarities in software code, security researchers discovered that Octopus could have links to DustSquad - a Russian-speaking cyber-espionage actor previously detected in former USSR countries in Central Asia, as well as Afghanistan, since 2014. Within the last two years the researchers have detected four of their campaigns with custom Android and Windows malware aimed both at private users and diplomatic entities.

“We have seen a lot of threat actors targeting diplomatic entities in Central Asia in 2018. DustSquad has been working in the region for several years and could be the group behind this new threat. Apparently, the interest in this regions’ cyberaffairs is growing steadily. We strongly advise users and organisations in the region to keep an eye on their systems and instruct employees to do the same,” says Denis Legezo, a security researcher at Kaspersky Lab.