Stalkerware and security risks for businesses

Some legitimate, useful and necessary applications can be turned into Stalkerware if they fall into the hands of a hacker.

Stalkerware is a familiar term for people working in the field of information security, referring to applications running on computers and smartphones capable of collecting and sending all information related to the owner. own equipment for many other subjects. Stalkerware can access all areas of the device, from photo galleries, text messages and emails, to audio recording via microphones, record browsing activity and even keystrokes. possessed unaware.

Some legitimate, useful and necessary applications can be turned into Stalkerware if they fall into the hands of a hacker.

Stalkerware applications are considered to be a dangerous security threat because they can extract different types of sensitive data from an individual or a business without suffering the owners' knowledge, thereby causing damage. serious.

With its superior spy capabilities, Stalkerware is one of the biggest security threats businesses today face, besides ransomware and a few other types of malicious code.

Stalkerware classification

Stalkerware applications can be classified into 3 groups as follows:

1. Some applications that are completely legal, useful and necessary on the system can be turned into Stalkerware if they fall into the hands of hackers. For example, after gaining access to a smartphone, a hacker could install malicious code and turn all apps on the device into spying apps.

2. Some legitimate applications, designed to monitor children's behavior and activities, can be abused by hackers and turn into spy apps.
3. Some spying apps hide the normal application that requires the device to be jailbroken to use.

Stalkerware's security risks for businesses

Depending on the type, Stalkerware will have a different impact on an organization or business:

1. Document the organization's internal operations and send it to third parties.
2. Allows hackers to gain access to an important device in the system, thereby accessing and stealing valuable internal data.
3. The stolen data may be publicly disclosed or sold illegally, used for unauthorized purposes, causing great damage to organizations and enterprises.

Against threats from Stalkerware

An essential tactic to protect your business against the threat of Stalkerware is monitoring external connections. Besides, every member on the system should:

1. Notice, closely monitor the security status on the device that you are using.
2. Regularly clean the system, remove unused applications.
3. Regularly check the operation history of the device.
4. Use a combination of strong passwords and login authentication methods. Do not share your password with any other objects.