Will 5G make us more vulnerable to cyber attacks?

The new generation of 5G mobile networks is beginning to be deployed increasingly popular in countries around the world.

The new generation of 5G mobile networks is beginning to be increasingly deployed in countries around the world, bringing promises about the bright future of a seamless and seamless connectivity standard between all the utilities of the technological world, with the advantage of reliability, high stability, large capacity and especially unprecedented low latency.

However, besides the obvious benefits mentioned above, security issues with 5G are also factors that should be paid more attention. We've talked a lot about the economic benefits 5G brings to every individual and business, and rarely spends time talking about the security risks this connectivity standard causes. These could be new, more sophisticated threats, more difficult to control, related to things we have known even recently.

Identify 5G security holes

According to a study by security firm Acckey with the participation of more than 2,600 business and technology executives in 12 key industrial sectors in Europe, North America and Asia-Pacific, there are up to 62% of these people fear that 5G will make their companies more vulnerable to cyber attacks. The root cause of this concern lies in the security issues stemming from the virtualized nature identified by the software of 5G compared to the hardware platform of previous LTE mobile communications standards.

The central role of 5G in the IoT world is a set of strengths and weaknesses in which endpoint systems are localized and sometimes beyond the control of security platforms. The 5G network promises to bring positive

points in device connectivity, authentication, and encryption, but the flip side is the underlying security gaps in those processes.

The nature of the way signals and data are routed in a 5G / IoT network can lead to Mobile Network (MNmap) mapping, where an attacker can map devices connected to the network, Identify each device and associate it with a specific person. They then deploy Man-in-the-middle (MiTM) attacks that help them gain control of device information before security systems can detect and block it.

In addition, there are supply chain security challenges with platform components that address inherent security holes. This can be clearly seen in backlink vulnerabilities thought to be intentionally built in mobile networks based on equipment from some big manufacturers like Huawei.

The backdoors will allow malicious agents to gain a target location, eavesdrop on calls and facilitate them to spread ransomware over 5G networks targeting mobile carriers.

Other vulnerabilities mentioned in the field of wireless and IoT include SIM SIMing, authentication key exchange protocol (AKA) and a series of backdoor vulnerabilities of the base station.

IoT in all areas, from smart homes, medical devices, machine to machine (M2M) to smart cities, power grids and autonomous vehicles are all vulnerable targets. All of these provide an attacker with multiple ways to gain unauthorized access or control over connected IoT devices and transfer data over 5G networks.

However, everything can be solved if we have an accurate and comprehensive understanding of the problem we are facing. 5G network security is still a 'wild west' with everything changing day by day, so businesses need to be proactive in building limited scenarios to cope with security risks. Collaborate with IoT / IT security experts to help them plan from scratch. Systems must be carefully designed for security to optimize safety inspection effectiveness, provide a reliable and protected product.