5G hackers: These eight groups will try to break into the networks of tomorrow

Organised cybercrime, rogue insiders and nation-state-backed hackers are among the groups that could soon be targeting 5G networks. But there are a few surprises on the list, too.

By Steve Ranger | ZD Net ~December 2, 2019

European computer security agency Enisa has listed the groups it thinks are most likely to attempt to hack into 5G networks, warning that security threats to telecoms infrastructure and beyond will expand with the arrival of next-generation mobile connectivity.

5G will introduce new risks because it will play a role in connecting up everything from smart cities, connected cars, automated factories and the internet of things.

"This will attract the attention of existing and new threat agent groups with a large variety of motives," Enisa said in a report into the security threats facing the next generation of mobile networks. It warned that 5G will introduce a set of new vulnerabilities that will expand the ways networks and connected devices could be attacked.

"These facts may cause an unprecedented shift of capabilities and objectives of existing threat agent groups in ways that have not been seen in the past," Enisa said.

The list of potential 5G threats includes:

Cyber criminals – Given the advanced capabilities of organised cybercrime, 5G is a likely target for them, either through attempts to steal data or via frauds. "Though not yet representing a significant monetizing vector, such attacks (or preparations hereto), will be part of their activities," Enisa predicted.

Insiders – These could be a key threat, mainly because they are in constant proximity with the core of 5G technology. The increased complexity of 5G might increase the amount of unintentional damage caused by clumsy insiders anyway, and dishonest insiders "may misuse their access to vital network function to cause high impact/large scale availability issues in the network itself," Enisa said. Disgruntled and dissatisfied insiders are also a target for other malicious groups, and could be recruited to abuse their insider knowledge for money.

Nation states – This is an important group due to their ability to compromise 5G networks and their potential motivation to do so, Enisa said: "Given the importance of 5G to the sovereignty of nation states, they will most probably be a target of state-sponsored attack." It is also "indisputable" that vendors of 5G components are in a better position to cause devastating attacks to the operation of self-developed components, Enisa said, especially when governments influence them, a possible nod to the ongoing debate about which companies from which nations should be allowed to build 5G infrastructure.

Military – 5G infrastructure will be one of the most vital components to protect in the technology landscape, Enisa said, and is also likely to be a technology of use to the military. "Such a development will amplify the protection requirements and the attractiveness of 5G as a target of cyberwar," Enisa said. "5G mobile networks are going to comprise a significant target for military operations, but also as a platform used for military purposes."

Enisa also put '**hacktivists**' on its list, but admitted that it's unclear how this group is going to be engaged in malicious activities surrounding 5G: "While the most probable is to see this group engaging in regional campaigns, it cannot be excluded that it could achieve high impact activities in national and even global 5G infrastructures". Enisa also warned that **corporations** may themselves be a threat to 5G networks as they will be interested in tracking the development of patents and intellectual property related to 5G infrastructure.

"Through the integration of multiple verticals, 5G will provide a single attack surface that once targeted, may result in damages in the physical space (e.g. hybrid threats)," Enisa said. And while acknowledging that there is little evidence for significant activity of **cyber terrorists**, Enisa noted that: "5G stakeholders will need to take the protection of this infrastructure very seriously to avoid high impact events that would cause severe harm to society".

Script kiddies – Individual junior hackers might still pose a threat to 5G because it has so many components, such as IoT devices, phones, and cloud storage spaces that are within the control of individuals, for example. "In the past, we have seen high impact attacks (e.g. DDoS) spreading from home devices and gadgets," Enisa said, adding that: "With the availability of high-speed 5G networks and interconnected devices, activities of this threat agent group may cause significant impact though cascaded events affecting upstream components of 5G operators."