ATTACKS FROM 4G/5G CORE NETWORKS

Risks of the Industrial IoT in Compromised Campus Networks

5G is projected to have an impact on the future, though its effects are already being felt today. A part of this conversation is the 4G/5G campus network, which is being rolled out in smart factories, remote power stations, harbors, healthcare facilities, and other industries. Previously defined as an interconnection of LANs exclusive to a limited area, a campus network now denotes a cellular communication system that comprises of a core network and multiple base stations.

Campus networks demonstrate the deepening role of telecom technologies in industrial environments. However, aside from highlighting new threats, it also underscores how IT and operational technology (OT) professionals might be lacking the necessary knowledge to mitigate telecom-related threats. To narrow this knowledge gap, we created our own campus network, where we not only simulate potential attack scenarios but also suggest ways to prevent them.

KEY FINDINGS

- The entry points from where attackers can compromise a core network include the server hosting core networking services, a virtual machine (VM) or a container, the network infrastructure, and base stations.
- Attack scenarios range from scenarios that are already known in the field of IT to attacks that are telecom-specific.
- Examples of common attacks that we were able simulate are DNS, MQTT, Modbus/TCP hijacking, SIM swapping, and remote desktop attacks. These common attacks stem from the IP network and should be familiar to IT professionals.
- Cellular-specific attack scenarios that we uncovered include SMS brute-force, fake GTP, and APN-related weaknesses. These are attacks that can only be delivered via a cellular network. IT professionals might also be less familiar with these.

SECURITY RECOMMENDATIONS

- Use application layer encryption, such as HTTPS, MQTTS, LDAPS, or any well-designed industrial protocol.
- Rely on proper network segregation, VLAN, and IPsec as valuable defenses for industrial facilities that run campus networks.
- Apply the latest patches for operating systems, routers, and base stations as soon as they are available to prevent threats from affecting open campus networks.
- Use VPN or IPsec to help protect remote communication channels, remote sites, and base stations.

CONCLUSION

More organizations will likely adopt campus networks in the future to meet the evolving demands of the present and keep up with the continuing development of 5G technology. In doing so, they need to be wary of the threats that we discuss as these could freeze operations, expose important information, and lower quality of production, among other consequences.

Read more about campus network security in our research paper at http://bit.ly/corenetworkattacks.

TREND MICRO™ | research