Smart Manufacturers Face a Security Conundrum as they Tackle Emerging 5G Threats

Trend Micro Research reveals multiple proof-of-concept attacks on connected systems

DALLAS, May 27, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, released in-depth research highlighting new threats to 4G/5G campus networks, many of which capitalize on the difficulty organizations have in patching critical OT environments.

The report details multiple attack scenarios and possible mitigations, using a testing environment designed to mimic a smart factory campus network.

To read a fully copy of the report, *Attacks From 4G/5G Core Networks: Risks of the Industrial IoT in Compromised Campus Network,* please visit: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-transition-to-5g-security-implications-of-campus-networks.

"Manufacturers are at the cutting edge of IIoT deployment, gearing up with 5G to tap the power of connectivity everywhere to drive greater speed, safety and efficiency. But with new technology comes new threats added to legacy challenges," said Yohei Ishihara, security evangelist for Trend Micro. "As the report warns, many are stuck in a bind—unable to afford the downtime necessary to patch critical system vulnerabilities that may otherwise be exploited. Fortunately, our extensive research also highlights multiple mitigations and best practices to protect the smart factories of today and tomorrow."

The report identifies several key entry points for attackers to compromise a core 4G/5G network:

- **Servers hosting core network services:** targeting of vulnerabilities and weak passwords in these standard COTS x86 servers.
- **VMs or containers:** these can also be exposed if the latest patches aren't applied promptly.
- **Network infrastructure:** appliances are often overlooked during patching cycles.
- **Base stations:** also contain firmware which needs to be updated from time-to-time.

Once the attacker gets in the core network from any of these entry points, they will attempt lateral movement in a bid to intercept and change network packets. By attacking industrial control systems in smart manufacturing environments like the test site, attackers could steal sensitive data, sabotage production, or hold organizations to ransom.

From the 11 attack scenarios demonstrated, one of the most potentially damaging involves targeting Microsoft Remote Desktop Protocol (RDP) servers, which are commonly used by IT and field engineers. The upgrade to 5G doesn't automatically protect RDP traffic, so attackers could use this access to download malware and ransomware, or directly hijack industrial control systems. RDP v 10.0 is the most secure version and may offer some protections against these attacks, but again it may be difficult for organizations to upgrade.

Among the recommendations made in the report to protect 4G/5G campus networks are:

- VPN or IPSec to protect remote communication channels, including to remote sites and base stations
- Application-layer encryption (HTTPS, MQTTS, LDAPS, encrypted VNC, RDP v10, and secure industrial protocols like S7COMM-Plus)
- EDR, XDR or MDR to monitor attacks and lateral movement inside the campus and the containerized core network
- Proper network segregation with VLAN or SDN
- Prompt patching, where possible, of servers, routers and base stations
- Anomaly detection products, like Trend Micro Mobile Network Security, which are campus network-aware and provide a robust way to cut off unlisted device/SIM card pairs

Building a mobile network in an enterprise environment involves both the end users as well as various stakeholders, including service providers and integrators. In addition, private 4G / 5G networks are large-scale infrastructure and have a long life, so once built, they are difficult to replace or modify. Therefore, it is essential to implement "security by default" to identify and mitigate security risks at the design stage.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks

platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---