Article

IoT devices can be hacked in minutes

Each internet-connected lightbulb is another entrance for hackers looking to break into your network.

A number of internet-connected devices are so lacking in even the most basic cybersecurity protocols that it's possible to hack them in as little as three minutes, allowing cyberattackers to steal data, conduct espionage on enterprise activities, or even cause physical damage. The poor security in Internet of Things products -- including IP connected security systems, connected climate control and energy meters, smart video conferencing systems, connected printers, VoIP phones, smart fridges, and even smart lightbulbs -- pose an inherent risk to the security of organizations which deploy them, researchers have warned.

These vulnerabilities can be easily exploited to plant backdoors and launch automated IoT botnet DDoS attacks. While hacking these devices might be so simple, the consequences could be dire and long-lasting. For example, if hackers were able to break into one of these devices -- something which could be as simple as remotely taking control of it by using the default factory login credentials -- they could aid criminals in performing physical break-ins by turning off cameras and opening and closing doors.

The researchers say smart video conferencing systems, connected printers, and VoIP phones all represent easy IoT-connected targets which provide a gateway for hackers to snoop on the targeted organization by listening into calls or using the insecure systems to reach other parts of the network and make off with private information.

To learn more about steps you can take to protect your network and to schedule an assessment of your network please contact us today.