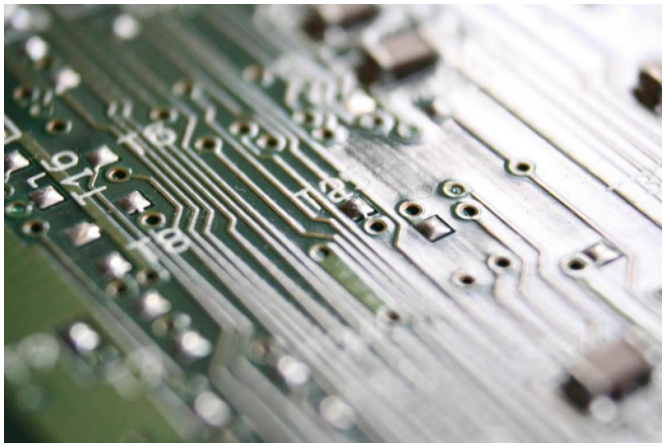
Hackers may hit home for the holidays

22 November 2015



Credit: Public Domain

It could be a merry holiday season for hackers, with millions of new and potentially vulnerable Internet-connected gadgets hitting the market.

Security experts say the vulnerabilities of "Internet of Things" devices such as fitness bands, smartwatches, drones and connected appliances could be exploited as consumers adopt these products for the holiday season.

Any connected device "can be a pivot point into your network," said Bruce Snell, cybersecurity and privacy director for Intel Security.

Although breaking into a wearable device or drone does not necessarily provide immediate value for a hacker, it can lead to a connection to a smartphone and data which is stored in the Internet cloud, security experts note.

"These could potentially install malware that sniffs out all the passwords on your network and sends them to a remote location," Snell told AFP.

For easier use, many consumer gadgets use relatively insecure connections and often require minimal use of passwords or other authentication.

Gary Davis, who heads consumer online safety for Intel, said the holidays could be a vulnerable time for consumers and a time for hackers to celebrate.

"With the excitement of getting new devices, consumers often are so eager to begin using them that they do not take time to properly secure them," he wrote.

In some cases, security can be improved by simply changing the password on the device, which may be something as simple as 1234 or 0000, but many people fail to do this.

"When you get that shiny new toy for Christmas, you want to just get it working," said Alastair Paterson, chief executive at the security firm Digital Shadows.

Exposing documents

Paterson noted that with a blurring of lines between work and leisure time, many people take home sensitive corporate material that can be then stored in a hackable home network.

In some cases, Paterson said, "just by connecting it to the home Wi-Fi network, they are exposing documents to the entire Internet."

The research firm Gartner earlier this month forecast that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020.

Juniper Research predicts "smart toy" sales will hit $2.8 billion this year, while noting that "vendors will likely require third-party software expertise to avoid PR disasters caused by hackers."

Smart home devices such as thermostats can be a gateway for hackers, according to a report this year by researchers at TrapX Labs.

The researchers took apart and then used a Nest thermostat as a point of attack for a home network

and were able to track the users' Internet surfing activity and get access to their private credentials.

The report said that even though Nest "is relatively secure," there is a concern "that the manufacturers of IoT devices at all points in the supply chain do not seem to have the economic incentives to provide initial cybersecurity... the manufacturers involved with IoT are obsessed with cost-cutting and minimal design footprints."

Northeastern University researchers found some smartphone fitness apps can leak passwords and location information over public Wi-Fi networks.

"Our devices really store everything about us on them: who our contacts are, our locations and enough information to identify us because each device has a unique identifier number built into it," said computer science professor David Choffnes, who led the study, which also developed a system to detect and fix data leaks.

Put on the kettle

Researchers at British security firm Pen Test partners said a similar vulnerability exists in Wi-Fi connected kettles and coffee-makers.

The devices allow users to turn the kettle on without getting up but it also means "a hacker can drive past your house and steal your Wi-Fi key," Pen Test's Ken Munro said in a blog post last month.

"If you haven't configured the kettle, it's trivially easy for hackers to find your house and take over your kettle."

California-based security firm Veracode found vulnerabilities in many smart home hubs that control systems such as garage doors or lighting.

Its study noted that cybercriminals could turn microphones on and listen to conversations or get notifications when a garage door is opened or closed, offering an opportunity to break into a given house.

A US Federal Trade Commission report highlighted the numerous risks for connected devices, while recommending that companies "build security into their devices at the outset."

The FTC also said companies "should limit the data they collect and retain, and dispose of it once they no longer need it" to minimize privacy risks.