Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

thehackernews.com/2018/04/iot-hacking-thermometer.html

April 16, 2018

Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on.
But of much greater concern, enterprises are unable to secure each and every device on their network, giving cybercriminals hold on their network hostage with just one insecure device.

Since IoT is a double-edged sword, it not only poses huge risks to enterprises worldwide but also has the potential to severely disrupt other organisations, or the Internet itself.

There's no better example than Mirai, the botnet malware that knocked the world's biggest and most popular websites offline for few hours over a year ago.

We have another great example that showcases how one innocent lookinginsecure IoT device connected to your network can cause security nightmares.

Nicole Eagan, the CEO of cybersecurity company Darktrace, told attendees at an event in London on Thursday how cybercriminals hacked an unnamed casino through its Internet-connected thermometer in an aquarium in the lobby of the casino.

According to what Eagan claimed, the hackers exploited a vulnerability in the thermostat to get a foothold in the network. Once there, they managed to access the high-roller database of gamblers and "then pulled it back across the network, out the thermostat, and up to the cloud."

Although Eagan did not disclose the identity of the casino, the incident she was sharing could be of last year, when Darktrace published a report [PDF], referencing to a thermometer hack of this sort on an unnamed casino based in North America.

The adoption of IoT technology raises concerns over new and more imaginative cybersecurity threats, and this incident is a compelling reminder that the IoT devices are theoretically vulnerable to being hacked or compromised.

> "There's a lot of internet of things devices, everything from thermostats, refrigeration systems, HVAC [air conditioning] systems, to people who bring in their Alexa devices into the offices," said Eagan.
> "There's just a lot of IoT. It expands the attack surface and most of this isn't covered by traditional defenses."

Manufacturers majorly focus on performance and usability of IoT devices but ignore security measures and encryption mechanisms, which is why they are routinely being hacked. Therefore, people can hardly do anything to protect themselves against these kinds of threats, until IoT device manufacturers timely secure and patch every security flaws or loopholes that might be present in their devices.

The best way you can protect is to connect only necessary devices to the network and place them behind a firewall.

Also, keep your operating systems and software up-to-date, make use of a good security product that protects all your devices within the network, and most importantly, educate yourself about IoT products.

Have something to say about this article? Comment below or share it with us onFacebook, Twitter or our LinkedIn Group.