washingtonpost.com

How a fish tank helped hack a casino

Alex Schiffer

3–4 minutes

Hackers are constantly looking for new ways to access people's data**.** Most recently, the way was as simple as a fish tank.

The hackers attempted to acquire data from a North American casino by using an Internet-connected fish tank, according to a report released Thursday by cybersecurity firm Darktrace.

The fish tank had sensors connected to a PC that regulated the temperature, food and cleanliness of the tank.

"Somebody got into the fish tank and used it to move around into other areas (of the network) and sent out data," said Justin Fier, Darktrace's director

of cyber intelligence.

The casino's name and the type of data stolen were not disclosed in the report for security reasons, Darktrace said. The report said 10 GB of data were sent out to a device in Finland.

"This one is the most entertaining and clever thinking by hackers I've seen," said Hemu Nigam, a former federal prosecutor for computer crimes and current chief executive of SSP Blue, a cybersecurity company.

Here is what you need to know about the Internet of things: a term used to describe devices like a thermostat or baby monitor that connect to the Internet. (Video: Sarah Parnass, Osman Malik/The Washington Post)

As more products with the ability to connect to the Internet become available, opportunities for hackers to access data through outside-the-box ways have risen. The report, which was first reported by CNN, comes a few days after the FBI warned parents about the privacy risks of toys connected to the Internet, which could help a

hacker learn a child's name, location and other personal information.

Fier said that with the recent FBI toy warning and the many ways by which hackers are trying to break into systems, he wouldn't be surprised if the government eventually got involved in regulating Internet of Things, IoT, products. But he said, even if it did, that would raise other questions.

"Everything has to go through FTC approval, I'd be curious to see if that happens on the cyber front," he said. "That you have to do the bare minimum to protect these products. But that's just for the U.S. How do you do this globally?"

As for what people can do to protect themselves against these kinds of attacks, **customers should educate themselves about IoT products and take advantage of any security protection the product offers, Nigam said. He added that people should use the latest operating systems and** software **and constantly update them.**

The fish tank incident was one of nine unique threats mentioned in Darktrace's annual report of

innovative hacks. Some of the other threats mentioned included hackers using company servers to acquire bitcoin, a digital form of currency, and former employees using their old login credentials to steal company data.