Cyber food for thought: when fridges go rogue...

By Colin Thornton

1 Nov 2016

For most of us, it is difficult to imagine a scenario in which our fridge is being used by terrorists to hijack important websites and access confidential data. Scarily, that scenario is closer to everyday reality than and evil sci-fi plot. So you might soon have far more to worry about than a fridge devoid of tasty snacks.

Wavebreak Media Ltd via 123RF

Let's look at what happened last weekend, for example: hackers attacked a company called Dyn, which is in charge of routing (directing) an enormous amount of internet traffic. The hackers installed software on devices like webcams and printers - without anyone realising what was happening. That software was then triggered to hit Dyn with a ton of traffic. The company suffered a disastrous crash, with the internet effectively giving a busy signal across a wide swathe of the United States.

This sophisticated attack comes at a time when election-related hacking (Clinton campaign emails) already has a lot of people concerned about cybersecurity.

Dyn officials stated that the attacks stemmed from tens of millions of devices connected to the Internet – closed-circuit video cameras, digital video recorders and even thermostats – that were infected with malware. The attacks came in waves and from IP addresses around the world, shifting across regions.

Reports have indicated that members of a shadowy hacker collective that calls itself New World Hackers claimed responsibility for the attack via Twitter. The group said they organised networks of connected "zombie" devices that threw a staggering 1.2 terabytes per second of data at the Dyn-managed servers.

Following the global fallout, a Chinese electronics company called Xiongmai Technology Co. recalled some products sold in the U.S. that authorities say were used in the internet takedown. Notably, security researchers say Xiongmai made some of the parts for the devices used to carry out the attack. Now, those parts are getting some security upgrades – and other companies similar to Xiongmai will surely be doing some internal checkups of their own.

Attacking the blind spots

Arguably, the core problem is that in the rush to connect all devices to the internet (the Internet of Things or IoT) designers and manufacturers are overlooking online security. So although it's really cool to think that you can manage your home media system from your phone, or check with your fridge on whether or not the milk has expired, it's not that cool when you become an unwitting accomplice to wide scale, international hacking!

The Dyn cyber disaster also raises key questions around what else hackers could do with our connected devices. For example, your home entertainment system may not have a microphone, but did you know that you could use a speaker as a microphone? This means that if your home entertainment system is entirely digital and connected to the internet, a hacker could use it to eavesdrop on your private life. And if your home alarm system is also connected, what's stopping hackers from seeing when you aren't home? These are certainly the more extreme examples, but there are lots of subtle breaches of privacy that could take place.

Policing of IoT?

There are also critical questions to be asked around data, and the ownership of data. For example, when IoT fridges come out with cameras, wouldn't it be tempting for these manufacturers to sell data about your eating habits to marketing companies?

From a legal perspective, for instance, can you or the manufacturers of these devices be held accountable if one of them is 'hijacked' for a cyber attack? And from a technical standpoint, what should you do about making sure you're safe when the time comes? Should you install a firewall at home? Will you need to buy and keep special security software up-to-date? Perhaps there will soon be some sort of international IoT security standard – and if so, who will police these standards?

So the next time you stand in front of your fridge at midnight, don't be surprised if there is far more to chew on than yesterday's leftovers…the cyber security threat is real, and we all need to make sure that we're prepared and ready.

ABOUT THE AUTHOR

Colin Thornton, CEO, Dial a Nerd.