Could your kettle bring down the internet?

October 25 2016, by Ansgar Koene And Derek Mcauley

Credit: AI-generated image (disclaimer)

How could a webcam help bring down some of the world's most popular websites? It seems unlikely but that's what happened recently when hackers attacked the internet infrastructure run by US firm Dyn, knocking out services including Paypal, Twitter and Netflix. More accurately, the attacked involved potentially hundreds of thousands of surveillance cameras and digital video recorders connected to the internet that had been weaponised by the hackers.

They were infected with malicious software that turned them into a "botnet", a network of devices controlled by an outside force. This was then used to flood Dyn's infrastructure with activity, grinding it to a halt. These so-called distributed denial of service (DDOS) attacks are a common technique among cybercriminals. But this was only the second recorded time a DDOS attack involved what's known as Internet of Things devices – devices other than PCs and mobiles that are connected to the internet.

Such a high-profile attack demonstrates just how serious the security flaws are in the tech industry's current approach to the Internet of Things. Without a significant change in the way these devices are designed and used, we can expect to see many more instances of internet-enabled cameras, TVs and even kettles used for nefarious purposes. They are perhaps even becoming part of a hacking service for hire.

Until now, concerns about the Internet of Things have largely focused on privacy. Hackers have shown they can gain control of internet-enabled security cameras and even baby monitors to spy on people's homes. Even if you cover up your webcam when you're not using it – as it seems Facebook founder Mark Zuckerberg does – devices like internet-enabled TVs and thermostats could also allow criminals or governments to monitor your movements.

There has been an (unspoken) attitude in many parts of the tech industry that because users often ignored privacy settings on social media showed they didn't really care about the issue. But with the weaponising of Internet of Things devices, there is a growing possibility that manufacturers could be held to account for security vulnerabilities through lawsuits and damages claims brought by corporate victims of DDOS attacks.

One problem is that, unlike PCs or smartphones, many of these devices

are meant to perform their tasks without drawing attention to the fact they are really computers. They're designed to be turned on and left to do their job with minimal human interaction. Yet one of the reasons people often run security checks and discover malicious software on their PCs is because they start to run more slowly or with minor errors. Internet of Things users are less likely to notice similar problems and have fewer options for determining what the problems is if they do.

Credit: AI-generated image (disclaimer)

Similarly, most Internet of Things devices are not able to automatically update their core software, something that is commonplace and expected of PC operating systems and smartphones. Instead the devices require manual updates often with quite complex procedures. So it is common for their security software never to be updated.

Network solutions

In order to fix these security problems, the tech industry needs to move from the current development process of building simple devices to designing better security measures into the basic systems. We're probably more likely to see change happen faster if lawsuits damage the reputation and profits of Internet of Things manufacturers and force them into adopting better security measures.

One way to do this would be to limit devices to communications within the home intranet rather than permit direct access to the global internet. These could be run and protected by a data management device, such as the Databox, that would act as a gatekeeper between the internet and the home and would be easier to monitor and update. It would provide an extra level of security that would be especially useful for older devices that no longer receive software updates.

Another approach would be to design more bespoke software instead of running generic versions of the free, open-source Linux operating system. The recent attack appears to have exploited a vulnerability in the "BusyBox" software that was based on Linux in this way.

While there is nothing wrong with using open-source software, manufacturers should really use it as a starting point for creating a tailored system including only the features that are actually needed for the device. All software has vulnerabilities that will eventually be discovered and require patching. The more features the software has, the larger the code is and the more chances there are for vulnerabilities to be discovered before they are patched.

As long as cybersecurity problems seemed to only affect internet of things device users, most people have been willing to accept the risks of simple, insecure design for the sake of rapid innovation. But now the

threat of attacks from botnets has made Internet of Things cybersecurity an issue for all internet users to worry about. It is time for developers to grow up and take responsibility for their designs or risk interference from regulators.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation