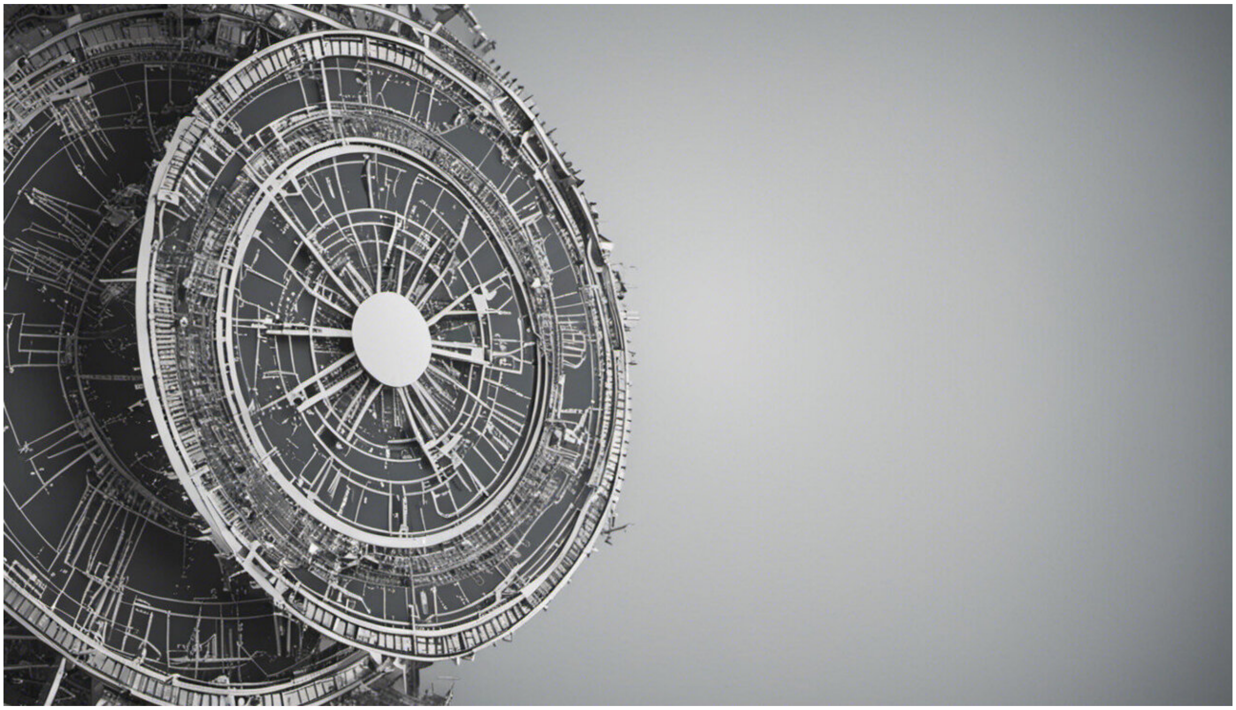
PHYS.ORG

The quiet threat inside 'internet of things' devices

January 11 2019, by Charles T. Harry



Credit: AI-generated image (disclaimer)

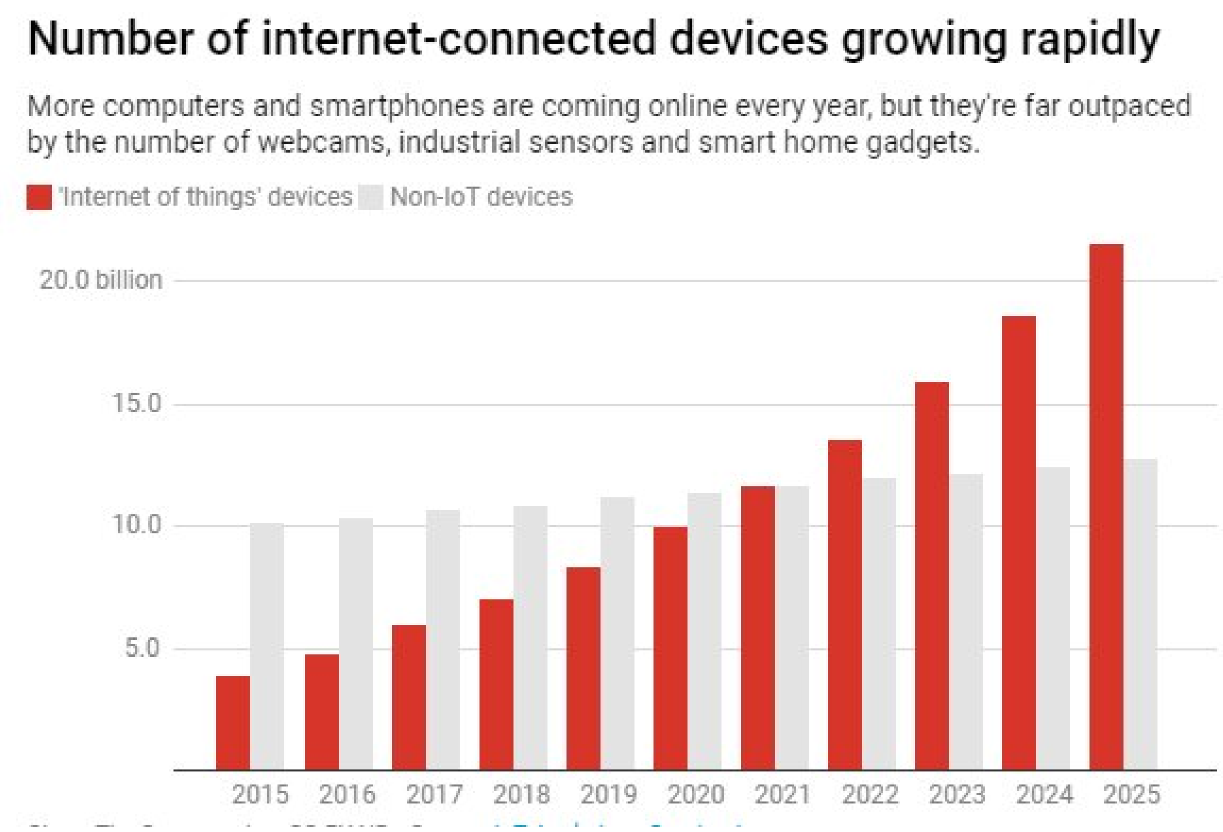
As Americans increasingly buy and install smart devices in their homes, all those cheap interconnected devices create new security problems for individuals and society as a whole. The problem is compounded by businesses radically expanding the number of sensors and remote monitors it uses to manage overhead lights in corporate offices and detailed manufacturing processes in factories. Governments, too, are getting into the act – cities, especially, want to use new technologies to improve energy efficiency, reduce traffic congestion and improve water quality.

The number of these "internet of things" devices is climbing into the tens of billions. They're creating an interconnected world with the potential to make people's lives more enjoyable, productive, secure and efficient. But those very same devices, many of which have no real security protections, are also becoming part of what are called "botnets," vast networks of tiny computers vulnerable to hijacking by hackers.

Botnets have caused problems on the internet, from sending vast amounts of spam mail to disrupting websites around the world. While traditionally most botnets are comprised of laptop and desktop computers, the growth of unsecured devices such as industrial sensors, webcams, televisions and other smart home devices is leading to a growing disruptive capability.

Tiny computers everywhere

The "internet of things" includes countless types of devices – webcams, pressure sensors, thermometers, microphones, speakers, stuffed animals and many more – made by a vast array of companies. Many of these manufacturers are small and unknown, and don't have popular brands or public reputations to protect. Their goals are to produce lots of devices to sell as cheaply as possible. Customers' cybersecurity isn't a real concern for them.



Credit: Chart: The Conversation, CC-BY-ND Source: IoT Analytics

These devices' variety means they're useful for lots of things, but also means they have a wide range of vulnerabilities. They include weak passwords, unencrypted communications and insecure web interfaces. With thousands, or hundreds of thousands, of identically insecure devices scattered all over the world, they're a wealth of targets ripe for the hacking.

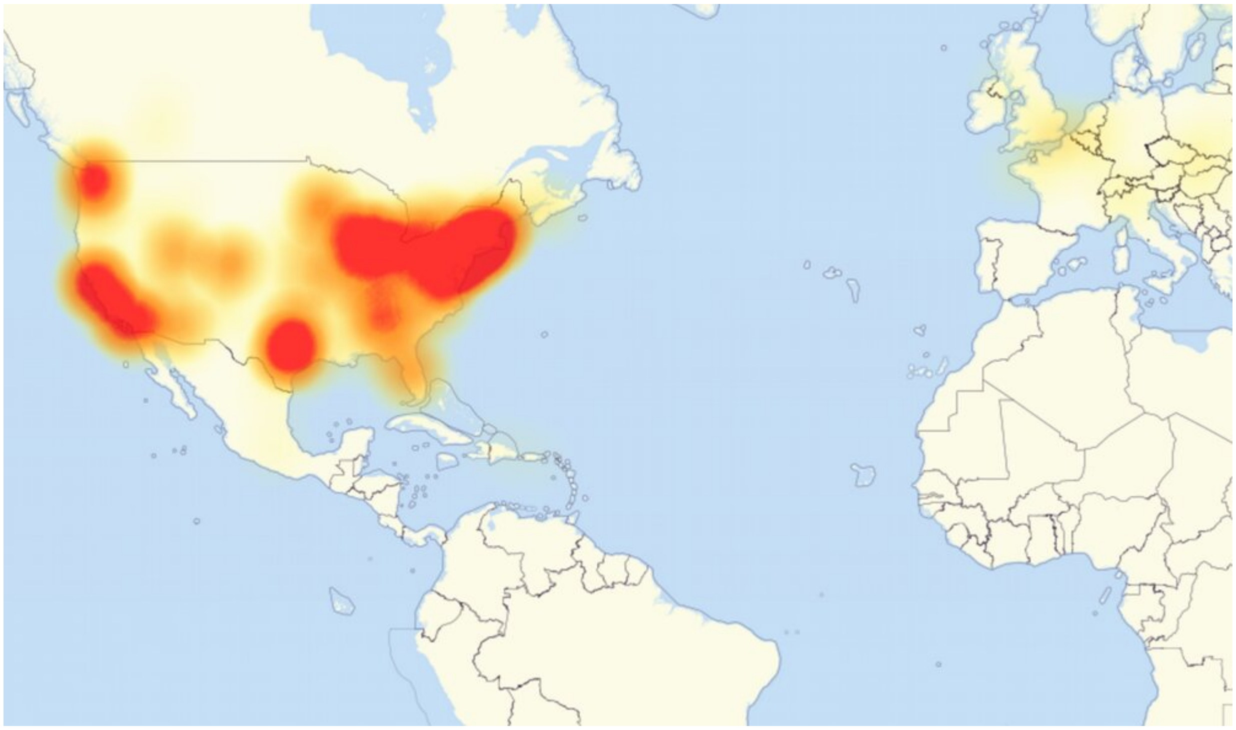
If, for instance, a manufacturer has set an unchangeable administrative password on a particular type of device – it happens more often than you might think – a hacker can run a program searching the internet for those devices, and then logging in, taking control and installing their own malicious software, recruiting the device into a botnet army. The devices run normally until the hackers issue instructions, after which they can do more or less anything a computer might do – such as sending meaningless internet traffic to clog up data connections.

Credit: AI-generated image (disclaimer)

Blocking internet access

That type of attack when emanating from thousands of devices at once, called a "distributed denial of service," can shut down companies' servers or even block wide swaths of the internet from being publicly accessible. A major DDoS attack in 2016 interrupted connections to Amazon, Netflix and Paypal from customers on the east coast of the U.S.

That attack was linked to a botnet-control software program created by three teenagers seeking to use more than 100,000 hijacked webcams and other internet-connected devices from around the world to gain an advantage over other players of the "Minecraft" online video game.



A botnet took down connections through a major internet company in October 2016. Credit: DownDetector/Wikimedia Commons, CC BY-SA

The size and scale of these attacks – and the broad range of devices that can contribute to them – make this both a private problem and a public one. People want to secure the devices in their homes and pockets, of course. Yet the same networks that stream television shows and music also link burglar alarms to police, manage traffic lights in congested areas and let self-driving cars talk to each other.

All that activity can be drowned out if hackers flood the internet, or sections of it, with meaningless messages. Traffic would stall across towns, even counties, and police officers would have a hard time communicating with each other to try to straighten everything out. Even small devices, in their hundreds of thousands, all around the world, can work together to have huge repercussions both online and in the physical world.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: The quiet threat inside 'internet of things' devices (2019, January 11) retrieved 26 April 2024 from https://phys.org/news/2019-01-quiet-threat-internet-devices.html