Simple Internet-connected devices can end up in complex online crimes

Any Internet-connected device, including the Fitbit Flex fitness bracelet, can become a drone. (Simon Dawson, Bloomberg)

By **CHRIS O'BRIEN**

MARCH 22, 2014, 11:00 AM

To keep an eye on his child via his smartphone, Marc Gilbert installed Internet-connected video baby monitors in his home in Houston.

One evening, Gilbert heard a stranger's voice bellowing obscenities from the monitor. He disconnected the device after realizing that it had been hacked.

"I'm a pretty technical guy, and I thought I knew how all this stuff should be hooked up," said Gilbert, who has written several letters to his congressman and other elected officials, trying to bring the security issue to their attention.

For decades, hackers have used the Internet to break into network routers, personal computers and advanced industrial devices.

But now, a whole new generation of often mundane, household devices is being connected to the Internet — and hackers are having a field day.

Thanks to smaller, cheaper processors, speedier wireless connections and the explosion of smartphones and tablets, it's becoming easier and more affordable to digitally link just about any object — sports equipment, watches, light bulbs, washing machines, thermostats.

If you can think of it, someone has probably stuck a sensor on it and connected it to the Internet.

Like a PC, the devices have operating systems and processors. And when they are connected to the Internet, hackers can break in and seize control.

Manufacturers and consumers haven't taken the same security precautions as they would with a PC, however, enabling hackers to turn seemingly innocuous gadgets into drones that can be used to spread malicious spam or launch a massive cyberattack — disrupting services or shutting down entire networks.

Even more frightening for many security experts is the prospect that the hackers could cause physical harm to people by shutting off thermostats, cars or even medical devices.

Such fears led doctors to turn off the wireless functionality of a heart implant in former Vice President Dick Cheney, out of concern that someone might hack it and attempt to kill him.

"It's the Wild West out there again," said Tommy Stiansen, co-founder of Norse Corp., a San Mateo, Calif., cybersecurity firm whose threat-detection team has discovered a wide range of devices being hacked. "The number of devices that have been compromised is staggering."

Such attacks are expected to multiply with the proliferation of Internet-connected devices. By 2050, analysts project, there will be 50 billion Internet-connected devices, or five such gadgets for every man, woman and child on the planet.

Consumers for the most part are helpless because they usually have no idea their gadgets have been commandeered.

A home wireless router can be configured to provide some rudimentary protections, but most users typically turn on the firewall or anti-virus software on their PCs, thinking that would be enough. And as such the wireless router becomes an unlocked door of sorts for hackers to gain access to the household devices.

This year, Proofpoint Inc., a Sunnyvale, Calif., cybersecurity company, tracked a global attack that sent 750,000 malicious emails from more than 100,000 gadgets — including home Wi-Fi routers, TVs, DVRs and even a refrigerator.

"How do you update the software on your refrigerator?" Proofpoint Chief Executive Gary Steele said. "I don't even know how you do that."

When Gilbert, a technician for an oil company, discovered that his baby monitor had been hacked, he ripped out the entire home network and rebuilt it from scratch.

His wife, he said, taped over webcams installed in their laptops and PCs. And he was particularly disturbed to learn there was even a search engine devoted to helping hackers find Internet-connected devices, sometimes including the passwords to gain access to them.

These attacks aren't limited to individuals: Businesses and large organizations also are getting slammed.

Employees are hooking up all sorts of gadgets to their companies' networks that their IT departments don't recognize or know how to manage. In other cases, businesses themselves are deploying unsecured Internet-connected devices to make their operations more efficient or to launch new services.

Norse and Sans Institute, an Internet security research and training firm, released a report last month that found Internet-connected devices in places such as hospitals, insurance firms and pharmaceutical companies had been infiltrated.

In addition to getting access to patient files and information, the attackers managed to invade radiology imaging software, conferencing systems, printers, firewalls, Web cameras and mail servers.

"What's concerning to us is the sheer lack of basic blocking and tackling within these organizations," said Sam Glines, CEO of Norse. "Firewalls were on default settings. They used very simple passwords for devices. In some cases, an organization used the same password for everything."

In such instances, companies such as Norse will contact large organizations and try to alert them to the breaches. Some companies take action; others prefer not to deal with it. Although some breaches are also reported to law enforcement agencies, most lack the resources to deal with what they perceive as a relatively trivial crime.

As bad as things are now, security experts fear that these attacks may cross over into the physical world. Hackers could access an Internet-connected smart lock and open the front door to burglars or tap into a smart meter and turn off the heat in a home during the winter, causing pipes to freeze and burst.

U.S. regulators are starting to take notice.

In September, the Federal Trade Commission announced its first settlement in an "Internet of things" security case. The FTC complaint said Trendnet Inc. had falsely advertised its security cameras and video baby monitors as being, well, secure.

According to the FTC, a hacker exploited a flaw in the cameras' software, and that led to other hackers posting links to the live feeds of 700 cameras. These feeds showed babies sleeping as well as kids playing and adults just wandering around.

One of those was a security camera that Casey Mahoney of Salisbury, N.C., had placed in his company's offices.

Mahoney was surprised when someone posted what they claimed was a link to a feed from the camera on the company's Facebook page. He assumed it was a link to spam or malware of some kind. But when he eventually clicked on it, he discovered it was indeed the video stream from his camera.

"I guess I wasn't too surprised because there's people out there and that's all they do. They just hack," he said. "Maybe I was a little surprised that a large company like Trendnet would have a flaw like that."

Security experts are calling on manufacturers to build more encryption into these devices and add safeguards that prevent them from running other programs.

"I'm sure it's slowly going to be addressed," said Johan Sys, managing principal of identity and access management for Verizon Enterprise Solutions. "The same thing happened in the mid-90s when everyone was joining the Internet. They had the same security problems. Now we're in that cycle again, and there's going to be some pain."

chris.obrien@latimes.com

Twitter: @obrien