# Smarter homes open to more risk

## Multiple devices increase chances of cyberattack

*By Marissa Lang*


Gregory Bull / Associated Press 2016

Security experts are concerned that Internet-connected home devices could be threatened as hackers seek new targets.

Homes are getting smarter.

Appliances, lightbulbs, televisions, baby monitors and even the locks on the front door can be automated, Internet-enabled, connected.

Without even realizing, early adopters of what are known as Internet of Things devices may wind up with dozens of smart devices in their house, cybersecurity experts said. And that means smart homes aren't just homes anymore — they're networks.

A network is any number of devices that are hooked up to the same Internet connection and linked to each other for the purposes of sharing data and information.

This means a single computer, smartphone or central hub, like Amazon's Echo or Apple's HomePod, can control all the devices in one house. It also means that a hacker who gains entry into a home network can use that connection to manipulate more than just the refrigerator.

Preventing that — and more broadly securing at-home networks — has become the latest arms race in consumer security.

The problem? Many casual smart-device buyers may not know that even with their door locked and windows closed, cybercriminals can still find a way into their home.

"Most consumers struggle to keep up with keeping their systems patched on their computer and their smartphone — devices that literally remind them to update their system," said Tony Sager, the senior vice president at Center for Internet Security. "Now you're talking about who knows how many more things that people are going to struggle to keep track of, and the second you bring it home, it's talking to your home network."

A smart home's residents may not even be the primary target. Hacked smart-home devices, like thermostats, security cameras or appliances, could be used to generate bogus traffic designed to

overwhelm computer servers in what is known as a botnet attack. One of the biggest attacks of this sort struck last year, and all but shut down some of the most popular websites in the world.

Besides the inconvenience of not being able to use Twitter or shop on Amazon, and the discomfiting idea that you may have been unwittingly complicit in devastating cyberattacks, the only direct impact these digital home invasions have on device owners is slowed-down Internet speeds.

But as the popularity of smart devices increases, experts said, so too does the likelihood of a network-wide attack. And the worst- case scenario is the stuff of sci-fi nightmares:

Imagine being locked out of your home, or trapped inside, because a cybercriminal gained control over the locks on your doors. Imagine the thermostat being hijacked to make your home sweltering or freezing cold. Imagine hackers using the smart TV in your bedroom as a recording device or holding all the food in your refrigerator hostage while you're on vacation — threatening to let it spoil until you pay what they're asking. Now imagine all of that happening all at once.

If cybercriminals can figure out a way to make money by holding homes hostage, experts said, these types of standoffs may begin soon. One technique is called ransomware, in which a cybercriminal demands payment to unlock a computer or smartphone or return files they have encrypted.

"The more that connected devices interact with the physical world, the more that ransomware's success will hinge on controlling access instead of controlling data," said Tim Erlin, vice president of product management and strategy at security firm Tripwire. "As we move to more ... embedded devices, the consumer has less control. Unless the industry facilitates security features, it will become harder and harder for consumers to protect themselves from cyberattack."

Nearly 8.4 billion Internet-enabled devices will be connected worldwide by the end of 2017, according to estimates by research firm Gartner. Of those, 5.2 billion will be in people's homes.

By 2020, Gartner estimates, the number of Internet of Things devices in use will fall just short of 1.5 trillion.

"I think it's inevitable," said Ed Skoudis, an instructor with SANS Institute, a cybersecurity training company, of the wave of smart devices. "I think it's the future. I think it's here to stay."

Several security firms are already selling or plan to release devices that monitor the home as a network and allow people to keep track of devices and see when, or if, they become compromised.

There's the Bitdefender Box and F-Secure Sense box, which act as smart routers, screening traffic and devices coming into and out of your network; the oddly shaped Norton Core, which also provides data encryption and manages software updates; and most recently, Bullguard's pebble-like network defense system, Dojo.

Dojo, released late last month, plugs directly into a Wi-Fi router and acts as a firewall between your home and any external threats.

A smartphone app communicates security updates and threat levels — green is good, orange means there was a problem that Dojo automatically fixed and red means further action is needed.

If a threat is detected, the system can quarantine the device in question and, theoretically, isolate the malicious software and prevent it from leaking into and infecting other devices on the network.

"Most (devices) don't have any indicator that something is wrong, because it's just a thermostat or a baby monitor or a TV; it's just a machine with no interface, so you may not be getting notifications of slow browsing," said Yossi Atias, Bullguard's general manager for Internet of Things security. "If those devices got hacked, you would never know. It's still working, you may not notice anything different. That's the challenge."

Atias said he came up with the idea when his teenage daughter came home from school after a cybersecurity presentation and put a Band-Aid over the camera on her laptop.

She told him she had learned the only way to make sure no one is watching through her computer's camera was to cover it up.

"It just hit me, you know, we're not going to go around and put Band-Aids on every device in our home, and with most of them, it wouldn't help anyway," Atias said. "That's when I realized your home is not just a collection of a standalone devices. It's a network. And all of the cybersecurity risks that come with that suddenly apply to your home."

Atias said he has more than two dozen connected devices in his home. He has seen houses where that number rises to nearly 200.

Ransomware attacks have struck hotels, businesses and public utilities by capitalizing on weak network security. Once one computer is infected with malicious software known as malware, hackers can break into other devices on the network.

Malware can be planted by hackers who break into devices with easy-to-guess or hardwired passwords that never get changed, or when people click on a link from an unknown source.

Devices like Dojo are meant to act as an early warning and firewall, though they cannot prevent users from making risky decisions that imperil their data and the security of their devices, experts said.

On Friday, KQED, the San Francisco public broadcaster, saw its live radio stream go down and warned employees not to access their email or computers as it investigated what it called "suspicious activity." Several employees told The Chronicle that KQED was the victim of a ransomware attack.

And last month, a ransom-ware attack infected tens of thousands of computers in nearly 100 countries by exploiting machines with outdated software that hadn't been properly updated or patched. The malware, known as WannaCry, hit hospitals the hardest.

Also this year, cybercriminals hacked into the computer system of a hotel in the Austrian Alps that controlled the electronic key system. Guests, who had paid nearly $300 per night, were locked out of their rooms. The reservations system went down.

The hackers demanded $1,600 to return the hotel's system to normal — a ransom the hotel paid. But in the end, it opted for a more permanent fix: It installed no-tech manual door locks and swapped out key cards for actual keys.

"My best advice is don't be an early adopter of these (Internet of Things) devices," Sager said. "And if you are, be sure to be aware and take steps to secure your network as best you can. Otherwise, keep your manual locks and your dumb refrigerator and let the market figure out what's going on."

Marissa Lang is a San Francisco Chronicle staff writer. Email: **mlang@sfchronicle.com** Twitter: @Marissa_Jae