YOUNG PROFESSIONALS: OFFERING OPPORTUNITIES TO RETAIN MILLENNIALS
TECHNOLOGY: SECURITY TIPS FOR INTERNET OF THINGS DEVICES
SPECIALTY LINES: 2017 PREVIEW

Rough Notes®

PROPERTY & CASUALTY AGENTS AGENCY MARKETING • INSURANCE MARKETS • NEW PRODUCTS
DECEMBER 2016

AGENCY OF THE MONTH:

CAROLINAS AGENCY HONORS THE PAST, LOOKS AHEAD

ALSO: NEW AND EMERGING INSURANCE PRODUCTS FOR 2017

HACKERS ARE FINDING WAYS TO EXPLOIT THE IoT

Recent DDoS attacks alarm consumers to secure connected devices

> *It's important to implement safeguards at home and in your agency to ensure security of the information you send. And it's important to encourage customers to do so as well.*

By Jerry Fetty

On October 21, a series of Distributed Denial of Service (DDoS) attacks on domain name system provider Dyn temporarily blocked consumer traffic to nearly 70 major Internet companies, including Amazon, Netflix, Twitter, and Reddit. A DDoS attack uses a multitude of hacked systems to attack a single target with a flood of requests; these requests are designed to overload the system and stop legitimate requests from getting through.

Because of its deep and widespread reach, the Dyn DDoS attack grabbed headlines worldwide. But it wasn't the first such major event. A month earlier, on September 16, *Krebs on Security*, a popular security news and information blog written by former *Washington Post* reporter Brian Krebs, was hit by a major DDoS attack. Although the attack did not succeed in knocking Krebs' site offline, it was reportedly one of the largest DDoS assaults ever up until that time, at one point causing 665 gigabits of traffic per second.

In addition to its size, what made the Krebs incident somewhat different from prior DDoS attempts is the initial indication that the attack had been launched with the help of a botnet that had taken over millions of hacked "Internet of Things" (IoT) devices that had weak or hard-coded passwords. A description attributed to *CyberTrend* magazine says a botnet is a series of Internet-connected computers or other devices infected with a self-replicating back-door Trojan that lets cybercriminals force the network to perform unauthorized commands en masse.

The use of a botnet is troubling, considering the explosive growth of the Internet of Things, which is forecasted by Gartner to reach 26 billion devices by 2020. Today, seemingly every commercially available product has a corresponding app or some sort of connectivity to the Web. Among the more common are security cameras, TVs, home alarms, refrigerators, garage door openers, remote power outlets, and thermostats.

BullGuard, a consumer security company headquartered in Europe, recently reported that vulnerabilities were

discovered in 4.6% of 100,000 devices checked by the company's free consumer scanner. With current estimates placing the number of IoT devices at 4 billion, this means there could be 184 million vulnerable devices being used today, providing a rich target for cyber criminals.

Even items with seemingly little intrinsic value are being manufactured with Internet connectivity. Take, for example, the BB-8$^{\text{TM}}$ droid toy built by Sphero. This commercially available app-controlled robotic ball has been painted like BB-8, the mischievous droid from *Star Wars Episode VII: The Force Awakens*, and marketed to people who want their very own droid.

In a recent report by Pen Test Partners, a U.K.-based vulnerability testing firm, security experts were able to exploit a bug and hack into a BB-8 toy through its integrated wireless communication system. This allowed them to inject code into the phone, which doubles as the device's remote. Hackers were able to take full control of the device in what is called a man-in-the-middle attack.

50-plus Internet of Things examples

- Air purifiers
- Audio speakers
- Bike locks
- Blood pressure monitors
- Cargo sensors and monitors
- Clothing
- Disease and health monitoring devices
- Dog houses
- Door locks
- Drones
- Egg trays
- Employee communication devices
- Energy consumption monitors
- Environmental spill detectors/trackers
- Ergonomics monitors
- Espresso makers
- Forklifts
- Garage door openers
- Gardening devices
- GPS trackers
- Health and fitness trackers
- Helmet concussion sensors
- Home hubs
- Home inventory order buttons
- Home security systems
- Home vents
- Indoor air quality sensors
- Key finders
- Kitchen appliances
- Laundry appliances
- Light bulbs
- Lighting controls
- Mattress covers
- Medical alert watches
- Oral hygiene devices
- Outlets
- Pet health monitors
- Pet locators
- Pill bottles
- Portable fish-finders
- Remote controls
- RFID platforms and devices
- Robots
- Running shoes
- Sleep trackers
- Telematics sensors
- Thermostats
- Toilets
- Umbrellas
- Virtual/augmented reality devices
- Water-leak sensors
- Weather monitors
- Window/door monitors
- Window blind controls

A man-in-the-middle attack is similar to the game of "telephone" or "whisper down the lane" you played as a kid. A person shares a message and the recipient receives it, but in the process of relaying the message, each person seems to add or omit some crucial element of the message. Just imagine that instead of the sentence "Jane runs through the forest," the message being interrupted and manipulated is a customer's credit card number.

With the advent of wireless systems, an increasing number of entities are at risk for this kind of hack.

This is why it's important to implement safeguards at home and in your agency to ensure security of the information you send, whether you're sending instructions to a toy from your smartphone or an essential file from a PC to your server. Now more than ever, you need to make sure that commands are sent securely and reach the recipient in the way the sender intends. It's important to encourage customers to do so as well.

Precautions such as remote monitoring and management that include intrusion detection, and other protocols that assist with cyber security, are good solutions to combat potential network security. (Your agency's IT provider can discuss these issues and recommend the appropriate solution at the network level.)

Here are three simple tips for increasing your Internet of Things device's security:

Use strong passwords on your devices. Many IoT devices arrive with weak passwords that can easily be hacked. If you are able to change the password on your device, do so.

Vary your passwords. Don't use the same password for all of your IoT devices.

Watch for upgrades. As vulnerabilities in Internet devices are found, companies will be forced to issue critical updates, so assume updating will be needed on your devices. ■

The author

Jerry Fetty is founder and CEO of SMART I.T. Services, Inc., an independent agent-focused information technology service company and developer of myAGENCYcloud. Reach him at jerry.fetty@smartservices.com.