5 Internet of Things Attacks:
Deadly Dolls and Killer Cars

It's no secret: millions of IoT devices have terrible security. Yet people continue to buy them and they continue to surface in cyberattacks.

But does the internet of things pose a real threat? What types of IoT attacks are being launched? What vulnerabilities are being found?

Let's look at some of the nastiest threats to emerge from the land of internet-connected gadgets, widgets, and gizmos.

#1. IoT Dolls that Spy on Kids

Parents in Germany were shocked to learn a doll bought for children could be used to spy on them.

Federal Network Agency, a telecommunications watchdog in Germany, advised parents in Feb. 2016 to destroy the talking doll, called My Friend Cayla.

Cayla could connect to a smartphone via Bluetooth, giving the doll internet access. This connection allowed it to converse with children, answering simple questions such as, "What's two times two?"

Unfortunately, the IoT doll also recorded children's conversations and stored them in an online server (yikes!).

And it gets worse — the poor security of the doll's Bluetooth connection could easily allow an attacker to connect and use the toy as a spying device.

The U.S. Federal Trade Commission filed a complaint against Cayla's manufacturer, Genesis Toys, in Dec. 2016.

Here's the first paragraph of the FTC's complaint:

> *This complaint concerns toys that spy. By purpose and design, these toys record and collect the private conversations of young children without any limitations on collection, use, or disclosure of this personal information. The toys subject young children to ongoing surveillance and are deployed in homes across the United States without any meaningful data protection standards. They pose an imminent and immediate threat to the safety and security of children in the United States.*

While no evidence of the doll being used in an IoT attack has surfaced, the size of the vulnerability and the potential impact on children are eye-opening.

#2. Click to Disable a Car's Brakes

Chrysler recalled 1.4 million vehicles in 2015 after security researchers demonstrated massive security gaps in the computer systems of Jeep Cherokees.

From a laptop miles away, Charlie Miller and Chris Valasek seized control of an SUV's brakes, transmission, and steering, all without physical access to the vehicle.

While a car is too large to consider a "gadget," its internet connectivity qualifies it for membership in the internet of things.

 | 214.379.4200 | support@avaren.com

AVAREN

Leveraging zero-day vulnerabilities and an IoT feature that kept the car connected to a cellular network, anyone with the vehicle's IP address could connect to it, according to Wired.

After connecting, the researchers pivoted to a chip in the car's head unit and rewrote its code.

This allowed them to issue commands through the car's internal computer network and control components such as the engine and brakes.

The researchers demonstrated terrifying control of the car – including the ability to disable its brakes, transmission, and engine.

Chrystler issued a patch to resolve the vulnerability and issued a recall – but when is the last time you patched a car's firmware?

#3. IoT Thermostat Held for Ransom

Security researchers not only compromised an IoT thermostat at Def Con 24, but also demonstrated how an attacker could lock the device and demand a ransom to restore functionality.

The team, Pen Test Partners, began the attack by searching for device information on the thermostat through the FCC ID Search page.

Some of the thermostat's hardware information and multiple product images were found through the search.

Upon further inspection, the hackers determined the thermostat had an SD card port used to customize its settings. The hackers used this feature to access the device's firmware.

Not only was the firmware easily accessed and unzipped, but it was also running in root by default, making it easy for the team to gain root access.

Even worse – after a little hacking, the team could inject malicious code into the IoT device without any additional authentication.

After creating a full-functioning version of ransomware, the attackers loaded it to the device via the SD port. The attack was successful.

The thermostat now showed a wallpaper displaying the text, "Ha! You Suck! Pay 1 Bitcoin to get control back."

#4. Teddy Bear Database Hacked

CloudPets, released by Spiral Toys, is a cute concept. The line of stuffed animals allows parents and children to record and share voice messages with each other.

For example, a traveling father can use the toy's smartphone app to send his daughter a voice message. Back at home, his daughter can listen to the message on her stuffed animal and record a response.

Similar to the Cayla doll mentioned above, the toys use Bluetooth to connect to a smartphone to gain internet access. This connection is used to send the voice recordings to a data base, where they are stored.

Unfortunately, more than 2 million of these deeply personal recordings were found unprotected in an online database, along with data on about 800,000 customer accounts.

"During the time the data was exposed, at least two security researchers, and likely malicious hackers, got their hands on it," according to Motherboard.

The exposed data included the email account used to set up a CloudPets account, the birth day and month of children, and the relationship of the account holder to the child.

Although the account passwords were encrypted, the company did not enforce ANY requirements for password strength. Entries such as "password" and "123" were allowed, which hackers could easily guess.

#5. IoT Attack Against Dyn

One of the most widely covered cyberattacks of 2016 used IoT devices to launch a massive DDoS attack.

DNS service provider Dyn estimates 100,000 endpoints flooded its architecture on Oct. 21, resulting in congestion and outages for websites such as Twitter, PayPal, Amazon, and Netflix.

To launch the attack, hackers used a botnet created with the Mirai strain of malware.

Mirai scans the web for vulnerable IoT devices, infects them, and secretly persists awaiting commands from the attacker.

Security cameras and DVRs allegedly comprise the bulk of infected devices in the Mirai botnet, although other hacked IoT devices, such as routers, are also present.

During the IoT attack against Dyn, traffic surges from the botnet are estimated to have peaked at a record-breaking 1.2 Tbps, although this is unconfirmed.

Consider the financial and reputational damage inflicted on Dyn by the attack.

Now also consider the cascading effect as services such as PayPal and Netflix were knocked offline, also hurting their reputations and bottom lines.

The destructive potential of attacks that use the internet of things is clear.

Why Should You Care?

Some of the examples above cite the work of security researchers to uncover vulnerabilities and potential attacks, not cybercriminals actually launching attacks.

But the threat is real – and it could be on your network.

Poorly secured firmware in thousands of routers, IP cameras, and other devices have created a vast landscape of insecure systems.

Sure, your company is not likely to buy a Cayla doll for the office, but what about an IP camera? Or how about a $30 wifi router? Many of these devices are just as dangerous.

Always choose devices that include software updates, and choose devices that update automatically when possible.

Always change default passwords, and ban the use of such devices on networks that house sensitive data.Filter email for spam and malware

This should go without saying – but be sure to use an effective email filter to remove dangerous and distracting messages from the inbox.

The email should be filtered by geography (i.e. if you do not do business in Russia, then you should not receive emails from Russia).

Also make use of blacklists and whitelists – explicitly defining who is and who is not allowed to send inbound emails to the company.

•••