ADT Sued, Claimed 'Easily Hacked'

Author: Brian Rhodes, Published on Nov 17, 2014

A lawsuit has been filed against ADT.

The class action complaint claims ADT's wireless systems are 'easily hacked', that ADT knows this and yet engages in 'deceptive and misleading marketing statements.'

In this note, we examine the details and the technical claims.

The Lawsuit

The class action complaint filing claims "*ADT's deceptive and unlawful business acts and practices in connection with the sale of wireless home security equipment*" and alleges "*ADT's failure to encrypt or otherwise secure its wireless signals*" violates commercial trade practice acts in several states.

The lawsuit seeks "*requiring ADT to change its marketing materials and to secure its customers' wireless systems*" plus various damages.

At this date, no claims of specific damages or loss due to the exploit are listed with the suit.

Claims

The lawsuit alleges that ADT's wireless security systems are susceptible to easy exploits that criminals can execute.

Vulnerable: The core weakness the suit claims is that ADT uses unencrypted wireless communication between sensors and the main panel, so that criminals can sniff out and 'jam' actual alarms from being triggered with inexpensive software defined radio gear easily purchased for <$15.

Alternatively, the suit claims hackers can trigger a flood of false alarms, potentially resulting in users refusing to arm it out of frustration. The other scenario paints a situation where local police fail to eagerly respond to a 'routine' call from a notoriously errant system, leaving the facility vulnerable to real heists 'or worse'.

The main external reference the complaint makes is a July 2014 Forbes article where a cybersecurity reseacher claims to have hacked ADT wireless systems:

> "He was able to play around with an ADT system thanks to the graciousness of his girlfriend's father, who had one at home. The different vendors' products all had the same problem: legacy wireless communications from the 90s that failed to encrypt or authenticate signals. He could be pick up the signals being sent from sensors on windows and doors to the main control system using a cheap SDR, meaning he could see transmissions from sensors — which are sent even when the system is unarmed — and track when people were opening and closing windows and doors. With a more sophisticated SDR, he could interfere with transmissions, setting the alarm off falsely by telling it doors were opening when they weren't or jamming the system so that it wouldn't go off, even if doors did open. He could do this from 65 to 250 yards away– basically a house over."

Issues With the Claims

On the surface, the claim could bear out as a risk at least for some ADT systems. However, one aspect of an 'ADT System' not addressed in the suit is there is no single or even typical alarm system. While unencrypted wireless could prove a vulnerability for some residential grade and older intrusion systems, ADT installs over 20 different systems. Several of those prominently feature 'spread spectrum' and 128 AES encrypted wireless technology that at least makes sniffing out and tampering with systems difficult.

Interestingly, ADT's flagship Pulse offering is Z-Wave based, and makes no explicit claims about encrypting wireless intrusion sensors, but does claims that the wireless video surveillance element uses WPA2 encryption between the camera and hub, and then HTTPS between local hub and cloud servers.

Not Just ADT

While ADT is the target of the suit, it bears emphasizing the potential risk is not only an ADT problem. Indeed, other wireless alarm systems sold by incumbents like Vivint and Monitronics are likely equally vulnerable to the same basic exploit.

Improving Security

Hacking unsecured wireless is neither new nor exotic, and multiple defenses are available to mitigate risk. Some basic steps include:

- *Go Wired*: Wireless cannot be hacked if it is not used. More costly (labor intensive), wired intrusion systems are still available and the mainstay of 'high-security' alarm systems. Simply choosing wired systems eliminates the potential risk described in the lawsuit.
- *Use Spread Spectrum:* When using wireless 'spread spectrum' or 'frequency hopping' connectivity between sensors and panels makes zeroing in or jamming a particular link extremely difficult. The nature of spread spectrum means the connection frequency intermittently shifts between endpoints, and the phrase 'trying to hit a moving target' describes the difficulty.

Who is the Plaintiff?

The plaintiff is Dale A. Baker and the law firm is Zimmerman Law Offices, who says their main part of their practice, with 18 years of experience, is class action lawsuits. According to the attorney, Baker has an ADT Pulse system installed at his home.

> "His system was erroneously activated 2 times and police had to come to his house. He subsequently learned that their were wireless systems that were encrypted that would prevent would be burglars from interfering with the wireless systems. He felt he had an obligation to inform other people that they are not as safe in their homes as ADT may lead them to believe and also is seeking to have ADT modify this product to encrypt the wireless signals so they can not be intercepted."

Those looking to join the class action lawsuit may contact Zimmerman Law Offices.