Issued 1/10/17

FTC goes after D-Link for Poor Security in Routers & Cameras

The U.S. Federal Trade Commission is cracking down on D-Link for selling wireless routers and internet cameras that can easily be hacked, the regulator said Thursday.

Thousands of consumers are at risk, the FTC said in a complaint filed against the Taiwanese manufacturer charging D-Link with repeatedly failing to take reasonable measures to secure the products. The action comes as hackers have been hijacking poorly secured internet-connected products to launch massive cyberattacks that can force websites offline.

Recently, a notorious malware known as Mirai has been found infecting routers, cameras, and DVRs built with weak default passwords. Among those flaws, were guessable login credentials embedded in D-Link camera software, using the word "guest" for both the username and password. In addition, D-Link also failed to patch vulnerabilities in the product software, including a command injection flaw that would have given hackers remote control over a device. "We can’t say whether we will take action against similar companies," an FTC spokesman said on Thursday. However, shoddy security has also been found in numerous IoT products in recent years, and lately, security experts have been urging the U.S. government to issue tough regulations to stop the problem.

In D-Link’s case, the security flaws could have paved the way for hackers to spy on consumers and steal their data via a compromised web camera or internet router, the FTC claims. The FTC's complaint, filed in the U.S. District Court for Northern California, is seeking an injunction against D-Link to prevent further violations. In addition to D-Link, the FTC has also gone after PC maker Asus over similar problems found with its routers and cloud computing service. Asus agreed to a settlement with the FTC last February.