A Hackers Dream, Your Smart House

Bernie Crump, Founder, MobileM2M Inc.

Hackers used to be mischievous teenagers hacking for fun. Now there's big money in it, which has attracted unscrupulous businesses and organized crime. With no industry or federal standards that require security measures, smart home devices are easy targets for hackers.

These computer criminals barely have to break a sweat to exploit vulnerabilities in internet-connected household appliances. Everything connected to your network is a potential target, from your wireless router to your DVR, Smart TV's and gaming consoles. Quite literally, everything with WiFi capability in your home is a target.

Frequently, your infected smart home devices aren't even the real victims of a hack. While some people may notice a drop in performance or increased power consumption, most never realize that a device has been compromised.
That's intentional.

Compromised devices can be used directly by the hackers or rented out as part of a botnet army on the dark web. Co-opted devices can be used to spy on you or enlisted as part of a robot network is used for malicious activity:

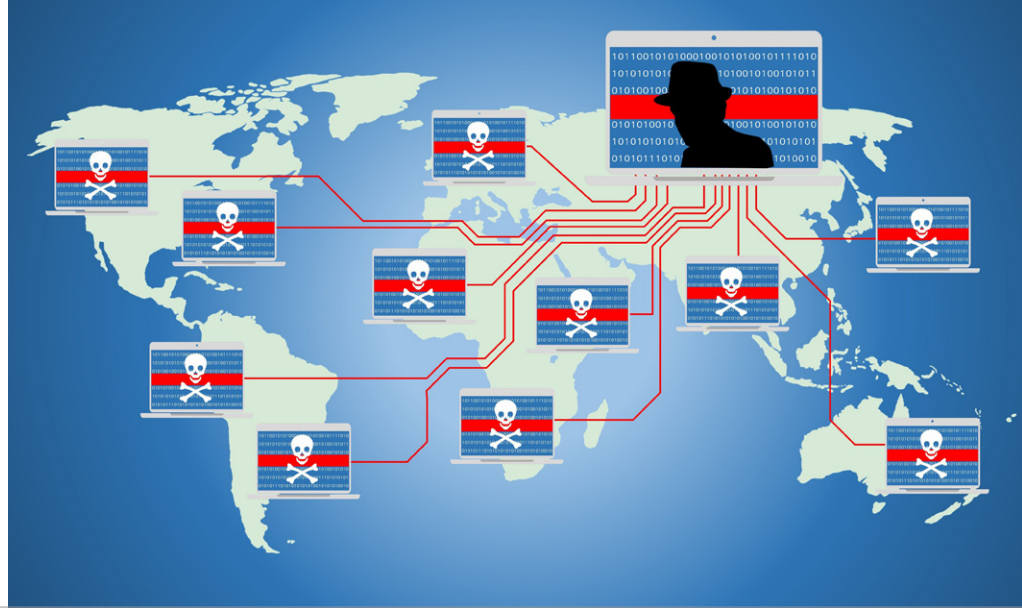
Distributed denial-of-service attack (DDoS) – A simple software command directs infected devices to collectively flood a specific web address with meaningless requests for services, which effectively paralyzes the site and brings business transactions to a halt.

Click fraud – The botnet is instructed to behave like a legitimate user who is browsing specific sites and "clicking" on ads, which artificially inflates web traffic and siphons ad revenue.

Cryptocurrency mining – There is power in numbers, and hackers are using easily co-opted smart devices to mine BitCoin and other cryptocurrencies. Hackers use your device, network, and power as a "free" resource. A report from CNBC and Mobile World Congress said that 15,000 devices could be hacked to mine $1,000 worth of cryptocurrency over four days.[1]

A Hacker can be in a car parked outside of your home, or on the other side of the planet

Cybercriminals don't have to even live in your hemisphere to locate and co-opt your smart devices. It's time to start asking how secure your home network truly is. Do you trust that your router was set up correctly and has the latest security settings? Do you have confidence that device manufacturers have done their due diligence to ensure their products can't be hacked and used against you or others?



70% of Smart Devices Vulnerable to Attack

An HP study revealed that "70% of the most commonly used Internet of Things (IoT) devices contain vulnerabilities, including password security, encryption, and general lack of granular user access permissions."[2] Using several kinds of testing tools, they uncovered an average of 25 vulnerabilities per device on common consumer items such as webcams, thermostats, sprinkler controls, and security systems.

- 70% did not encrypt communications to the internet and local network.
- 50% of the devices' mobile applications performed unencrypted communications to the cloud, internet, or local network.
- 70% would enable a potential attacker to determine valid user accounts through account enumeration or the password reset feature.
- 60% did not use encryption when downloading software updates. Some downloads could even be intercepted so the software files could be viewed or modified.

As manufacturers rush to get smart products on the market, their eagerness "opens the doors for security threats ranging from software vulnerabilities to denial-of-service (DOS) attacks to weak passwords and cross-site scripting vulnerabilities."[2]

The inevitability of smart devices being compromised

The inevitability of smart devices being compromised by hackers is starting to catch the attention of the government.

The FTC recently took the network equipment manufacturer D-Link to task for having serious security vulnerabilities despite claiming that their devices have "advanced network security."[3] Security flaws found included weak login credentials, mishandled software patches, and unsecured credentials on the mobile app.[3,4]

While the lawsuit was dismissed because the FTC wasn't able to provide concrete examples of how D-Link devices were hacked and subsequently used against consumers, the potential for exploiting smart devices remains. Until tougher regulations are put in place, consumers are at the mercy of manufacturers to install the right security measures.

One of the best ways to decrease the risk of smart home devices being hacked is to limit how often they are connected to the network. Turning off your router when you are asleep, away at work, or not using any devices significantly reduces the likelihood of your devices being discovered and compromised.

Off Hours™ keeps the network OFF, turning it on only when it's needed. The system controls how often your home network is connected to the internet, limiting the window of time smart TVs and other IoT devices are exposed to hackers. When your network is always on, your exposure risk is at 100%%, but limiting your network time to four hours a day lowers your exposure to less than 20%. With customizable scheduling, you decide when your home is Off Hours™.

References

1. https://www.cnbc.com/2018/03/01/thousands-of-iot-devices-can-be-hacked-to-mine-cryptocurrency-avast.html
2. http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676>
3. http://www.networkworld.com/article/3154815/security/ftc-goes-after-d-link-for-shoddy-security-in-routers-cameras.html
4. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate


OFF
HOURS