How to protect your internet-of-things devices

December 20 2017, by Sam Wood, The Philadelphia Inquirer

Credit: CC0 Public Domain

Internet-connected devices are nearly ubiquitous, with computer circuitry now found in a variety of common appliances. They can include security cameras, DVRs, printers, cars, baby monitors, and

refrigerators—even "smart" lightbulbs and clothing. Collectively those devices are called the internet of things.

The internet of things is a big, juicy target for criminals. Up to a million devices were hijacked to create the Mirai botnet which was used to extort companies and bring a university computer system in New Jersey to its knees. The botnet was later exploited to bring down vast swaths of the internet in a sustained attack on Oct. 21, 2016.

Paras Jha, a former Rutgers University student, pleaded guilty Dec. 8 with two other men who admitted they wrote the Mirai code. Named after an obscure anime film character, Mirai scoured the internet for unsecured devices and easily found them.

Once discovered, the Internet of things devices were hijacked by the Mirai malware and became part of a botnet that launched assaults on internet service providers and scores of websites. Jha, 21, allegedly monetized the botnet by demanding ransom to call off the attacks, using it to inflate the number of advertising clicks on websites, and renting it out to other hackers for their own nefarious ends.

The attacks on Rutgers' computer system may have cost the school $9 million, prosecutors said. Rutgers officials told NJ.com the cost of enhancing security was one of the reasons the school hiked tuition in 2016.

When Jha discovered federal investigators were closing in, he released the Mirai source code to the world to cover his tracks. The code is still circulating online and causing damage, according to Brian Krebs, of KrebsOnSecurity.com.

Krebs advises taking these precautions to keep your Internet of things devices protected:

Avoid connecting your devices directly to the internet.

Change the default credentials to a complex password that only you will know and can remember.

Check the defaults, and make sure things like UPnP (Universal Plug and Play—which can easily poke holes in your fire wall without you knowing it) are disabled.

Avoid Internet of things devices that advertise built-in Peer-to-Peer (P2P) capabilities. P2P Internet of things devices are notoriously difficult to secure, and research repeatedly has shown that they can be reachable even through a fire wall remotely over the internet. That's because they're configured to continuously find ways to connect to a global, shared network so that people can access them remotely.

When it comes to Internet of things devices, cheaper is definitely not better. There is no direct correlation between price and security, but history has shown that less expensive devices tend to have the most vulnerabilities.

The Department of Justice also offers these tips to protect internet-connected devices.

Do your research. Consider the security features of your Internet of things devices before buying. If the device uses a password, make sure it allows you to change it.

Update firmware when available. Internet of things devices can be susceptible if not regularly patched. Only install updates from known and reputable sites.

Disconnect your insecure Internet of things devices. Outdated security?

Can't update passwords? Then unplug it.

Turn off Internet of things devices when not in use, or periodically if otherwise always on. Malware is stored in memory and can often be erased by turning the device off and back on.

Protect routers and Wi-Fi networks. Use your router's built-in fire wall, confirm it's enabled.

Avoid using public Wi-Fi to check Internet of things devices from a smartphone.

Use antivirus and intrusion-detection products.

Ask for help, or hire help, if you can't figure out fire walls or how to "segment" your network of Internet of things devices.

Some free online resources can help determine whether your devices are susceptible to being accessed by Mirai or other malware. Be cautious and use only well-known sources.

If you suspect your Internet of things device is infected, turn it off and on again to purge the device's memory. Change the password. File a report with the internet Crime Complaint Center.