Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2015

Alert Number
I-091015-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device
- Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT Risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety. The main IoT risks include:

- An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices. The UPnP describes the process when a device remotely connects and communicates on a network automatically without authentication. UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Cyber actors can change the configuration, and run commands on the devices, potentially enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping;
- An exploitation of default passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information;
- Compromising the IoT device to cause physical harm;
- Overloading the devices to render the device inoperable;
- Interfering with business transactions.

What an IoT Risk Might Look Like to You?

Unsecured or weakly secured devices provide opportunities for cyber criminals to intrude upon private networks and gain access to other devices and information attached to these networks. Devices with default passwords or open Wi-Fi connections are an easy target for cyber actors to exploit.

Examples of such incidents:

- Cyber criminals can take advantage of security oversights or gaps in the configuration of closed circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers. Many devices have default passwords cyber actors are aware of and others broadcast their location to the Internet. Systems not properly secured can be located and breached by actors who wish to stream live feed on the Internet for anyone to see. Any default passwords should be changed as soon as possible, and the wireless network should have a strong password and firewall.
- Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting. The exploits allow criminals to obtain administrative privileges on the automated device. Once the criminals have obtained the owner's privileges, the criminal can access the home or business network and collect personal information or remotely monitor the owner's habits and network traffic. If the owner did not change the default password or create a strong password, a cyber criminal could easily exploit these devices to open doors, turn off security systems, record audio and video, and gain access to sensitive data.
- E-mail spam attacks are not only sent from laptops, desktop computers, or mobile devices. Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail. Devices affected are usually vulnerable because the factory default password is still in use or the wireless network is not secured.
- Criminals can also gain access to unprotected devices used in home health care, such as those used to collect and transmit personal monitoring data or time-dispense medicines. Once criminals have breached such devices, they have access to any personal or medical information stored on the devices and can possibly change the coding controlling the dispensing of medicines or health data collection. These devices may be at risk if they are capable of long-range connectivity.

- Criminals can also attack business-critical devices connected to the Internet such as the monitoring systems on gas pumps. Using this connection, the criminals could cause the pump to register incorrect levels, creating either a false gas shortage or allowing a refueling vehicle to dangerously overfill the tanks, creating a fire hazard, or interrupt the connection to the point of sale system allowing fuel to be dispensed without registering a monetary transaction.

Consumer Protection and Defense Recommendations

- Isolate IoT devices on their own protected networks;
- Disable UPnP on routers;
- Consider whether IoT devices are ideal for their intended purpose;
- Purchase IoT devices from manufacturers with a track record of providing secure devices;
- When available, update IoT devices with security patches;
- Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it operate on a home network with a secured Wi-Fi router;
- Use current best practices when connecting IoT devices to wireless networks, and when connecting remotely to an IoT device;
- Patients should be informed about the capabilities of any medical devices prescribed for at-home use. If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor;
- Ensure all default passwords are changed to strong passwords. Do not use the default password determined by the device manufacturer. Many default passwords can be easily located on the Internet. Do not use common words and simple phrases or passwords containing easily obtainable personal information, such as important dates or names of children or pets. If the device does not allow the capability to change the access password, ensure the device providing wireless Internet service has a strong password and uses strong encryption.