Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

October 17, 2017

Alert Number
I-101717a-PSA

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

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

Common Internet of Things Devices May Expose Consumers to Cyber Exploitation

In conjunction with National Cyber Security Awareness Month, the FBI is re-iterating the growing concern of cyber criminals targeting unsecure Internet of Things (IoT) devices. The number of IoT devices in use is expected to increase from 5 billion in 2016 to an estimated 20 to 50 billion by 2020. Once an IoT device is compromised, cyber criminals can facilitate attacks on other systems or networks, send spam e-mails, steal personal information, interfere with physical safety, and leverage compromised devices for participation in distributed denial of service (DDoS) attacks.

IoT refers to a network of physical devices, vehicles, buildings, and other items (often called “smart devices”) embedded with electronics, software, sensors, actuators, and network connectivity enabling these objects to collect and exchange data. Below are examples of IoT devices:

- Home automation devices (e.g., devices which control lighting, heating and cooling, electricity, sprinklers, locks);
- Security systems (e.g., alarm systems, surveillance cameras);
- Medical devices (e.g., wireless heart monitors, insulin dispensers);
- Wearables (e.g., fitness trackers, clothing, watches);
- Smart appliances (e.g., refrigerators, vacuums, stoves);
- Office equipment (e.g., wireless printers, computer mouse, outlets, interactive whiteboards);
- Entertainment devices (e.g., DVRs, TVs, gaming systems, music players, toys); and
- Hubs (devices that control other IoT devices through a single app).

As more businesses and homeowners use Internet-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet provides new vulnerabilities for malicious cyber actors to exploit. In 2016 and 2017, cyber actors have demonstrated the ease in which IoT device vulnerabilities can be compromised and leveraged. Deficient security capabilities, difficulties in patching vulnerabilities, and a lack of consumer security awareness provide cyber actors with opportunities to exploit these devices.

- In September 2016, cyber actors using the Mirai botnet infected IoT devices—including routers, cameras, and digital video recorders—for the purpose of conducting DDoS attacks. The actors exploited openly accessible devices via the Internet with common default usernames and passwords.

- In February 2017, a hacker compromised more than 160,000 printers with open connections to the Internet by scanning for those with specific open ports. The hacker claimed the devices were part of a botnet and sent print jobs to the affected printers.

- In August 2017, a cyber actor released a list of over 33,000 usernames and passwords for IoT devices, including cameras, DVRs, and routers. While the majority of these devices were located in Asia and China, many of the devices were also found in the United States. A researcher conducted a test against this list and discovered many of these devices were almost instantly exploited, often taking less than two minutes between discovery and infection.

Unsecured or poorly secured devices provide opportunities for cyber criminals to intrude on private networks and gain access to other devices and information attached to these networks. Cyber criminals often take advantage of default usernames and passwords to merge IoT devices with others into a large botnet. These botnets can facilitate DDoS attacks against popular Web sites or network resources. These attacks cause Web sites to run slow, prevent users from being able to connect, or potentially take down multiple Web sites associated with the network under attack.

Consumer Protection and Defense

It can be difficult to determine if an IoT device has been compromised. However, there are many reputable resources and tools available that search for vulnerable network devices. The following recommendations can be implemented to help secure IoT devices from cyber attacks.

- Change default usernames and passwords. Many default passwords are collected and posted 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 encryption.
- Isolate IoT devices on their own protected networks.
- Configure network firewalls to block traffic from unauthorized IP addresses and disable port forwarding.

- Review and implement device manufacturer security recommendations, if available. Consider turning devices off when not in use.
- Research your options when shopping for new IoT devices. When conducting research, use reputable Web sites that specialize in cyber security analysis, provide reviews on consumer products, and support consumer advocacy.
    - Look for products from manufacturers with a track record of providing security to their Internet-connected products. Look for companies that offer firmware and software updates, and identify how and when these updates are provided.
    - Identify what data is collected and stored by the devices, including whether you can opt out of this collection, how long the data is stored, whether it is encrypted in storage, and if the data is shared with a third party. Also identify what protections and policies are in place in case there is a data breach.
- Ensure all IoT devices are up to date and security patches are incorporated when available.
- Use current cyber security best practices when connecting IoT devices to wireless networks and when connecting remotely to an IoT device.
- Invest in a secure router with robust security and authentication.
    - Most routers will allow users to whitelist, or specify which devices are authorized to connect to a local network. Whitelisting can be used to identify malicious network traffic from unauthorized devices and prevent them from making a connection.

Additional Resources

For additional information on cyber threats to IoT devices, please refer to “Internet of Things Poses Opportunities For Cyber Crime,” available at https://www.IC3.gov/media/2015/150910.aspx and “Internet-Connected Toys Could Present Privacy and Contact Concerns for Children,” available at https://www.IC3.gov/media/2017/170717.aspx.

Victim Reporting

If you suspect your IoT device(s) may have been compromised, contact your local FBI office and/or file a complaint with the Internet Crime Complaint Center at www.IC3.gov.