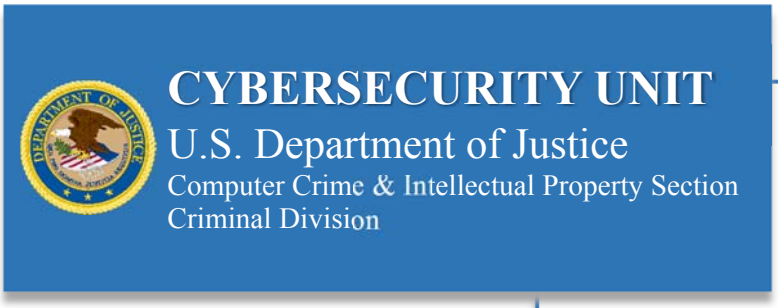

Securing Your "Internet of Things" Devices

(July 2017)

Introduction

In recent years, the dramatic growth of Internet-connected devices has transformed how people, households, and businesses interact with each other and the physical world. Connected devices as diverse as security cameras, digital video recorders, printers, wearable devices, "smart" lightbulbs, and Internet connected-appliances have come to be collectively known as the "Internet of Things" ("IoT"). IoT devices represent a growing constellation of gadgets and tools designed to collect, exchange, and process information over the Internet to furnish their users with convenient access to an array of services and information.

Unfortunately, IoT devices have also become an increasingly attractive target for criminals. To attack IoT devices, cyber criminals often probe the devices for security vulnerabilities and then install malicious software ("malware") to surreptitiously control the device, damage the device, gain unauthorized access to the data on the device, and/or otherwise affect the device's operation without permission. Installed malware may not only compromise the operation and information security of the infected IoT device, but can also provide hackers a conduit for penetrating other electronic devices on the same network. Unless appropriate precautions are taken, malware can quickly spread across networks of IoT devices without a user opening a file, clicking on a link, or doing anything other than turning on an Internet-connected device.

Although malware has existed for many years, the burgeoning popularity of IoT devices has significantly increased the number of Internet-accessible targets that may be exploited; the advent of a new generation of malware dedicated to exploiting IoT devices is largely to blame. For instance, Dyn, a company that monitors and routes Internet traffic, was a victim of a distributed denial of service ("DDoS") attack in October 2016 that was launched from thousands of IoT devices infected with the "Mirai" malware. Unlike more conventional forms of malware,

the Mirai code was written specifically to allow a remote user to infect IoT devices and use them as an army of machines capable of transmitting internet traffic without the device owners' knowledge. On October 21, 2016, thousands of Mirai-infected IoT devices were directed to unleash a torrent of traffic that overwhelmed Dyn's systems. Many high-traffic websites that used Dyn's Internet services (for example, Paypal, Twitter, Netflix, and CNN) were rendered wholly or sporadically inaccessible for substantial periods of the day.

The interruption of Internet service associated with the Dyn disruption underscores the significant, systemic harm that may be caused by malware dedicated to exploiting the security vulnerabilities of IoT devices. To help prevent and/or mitigate the impact of future crimes involving IoT devices, the Criminal Division's Cybersecurity Unit and the Consumer Technology Association are providing the following suggestions to owners of IoT devices. While these measures are intended specifically for IoT devices, many are more generally applicable and are also sound practices to institute when using most Internet-connected devices.[1]

Protecting Your IoT Devices

There are a number of precautions you may take to shield your IoT devices from cyber intrusions and prevent them from being commandeered to launch cyber attacks. The following measures will allow you to enjoy your IoT devices while also better securing your IoT devices against malware and safeguarding your data and privacy.

- **Do your research**. If you decide to purchase an IoT device, do your research to ensure that the manufacturer takes cybersecurity seriously. For instance, if the device uses a password, make sure the IoT device allows you to change its password. (Some devices come with default passwords that cannot be changed.) Also, consider whether you are confident that the manufacturer will deliver timely security updates to combat new malware and security threats. Having a device that is configured to easily download security updates increases the chance that the device will be using the latest protections. To keep cyber criminals out of your home, business, car, or anywhere else you may choose to use an IoT device, it is important to make security features part of the considerations you weigh when buying an IoT device.

[1] This guidance is intended for IoT-device users who do not have a technical background. For a more technological discussion of mitigating IoT threats, visit the U.S.-CERT web site at https://www.us-cert.gov/ncas/alerts/TA16-288A.

- **Secure your IoT device immediately after purchase.** An IoT device that is not properly secured may be exploited within minutes of being connected to the Internet.[2] With this in mind, do not let the excitement of acquiring a new IoT device distract you from securing it before putting it to use. Before installing your new device, visit the manufacturer's website and download any new security patches for known vulnerabilities. Also, without exception, immediately reset any default passwords with secure passwords.

- **Adopt secure password practices**. Proper password security is critical to information security, regardless of whether that password protects an IoT device, desktop computer, router, Wi-Fi connection, or online account. Passwords should be difficult to guess, avoid incorporating information about you that is readily available on the Internet (for example, through social media), and be unique to each secured device or router. To make passwords complex enough to thwart password-cracking software, use a combination of upper- and lower-case letters, numbers, and symbols. To help keep track of multiple passwords, consider using a password-management program that can maintain and safeguard your passwords.

- **Continue to update your firmware when available.** Your IoT device has software embedded on it called "firmware" that may be susceptible to exploitation if not regularly updated and patched. To keep your IoT devices secure, you should register each of your devices for any automated firmware updates that are offered by the manufacturer. If automatic updates are not available, it is well worth the effort to periodically check the manufacturer website for firmware updates and device patches to ensure your IoT devices are current and running the latest and most secure firmware updates. Only install updates from known, reputable sites.

- **Consider disconnecting your insecure IoT device.** Even some relatively new IoT devices may have outdated security and may not allow you to change administrator passwords or update the device's firmware. If your IoT devices cannot, at a minimum, be updated with strong passwords or receive security patches, they may be vulnerable to malware infection. You should consider disconnecting such devices and replacing them with newer, secure models.

- **Turn off IoT devices when not in use or periodically if otherwise always on.** The malware used in some recent cyber attacks is stored in memory and can often be erased with a "power cycle," that is by turning the device off then back on. Accordingly, as a rule of thumb, you should always turn off any smart devices when they are not in use,

[2] Andrew McGill, The Inevitability of Being Hacked, The Atlantic, Oct. 28, 2016, *available at* https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/.

such as video cameras and devices with microphones that can be compromised and used to invade your privacy. IoT devices that are in regular use (for example, thermostats) should be restarted periodically.

- **Protect your routers and Wi-Fi networks.** To keep your IoT devices secure, it is also important to secure the home routers and Wi-Fi networks to which they regularly connect. Use your home wireless router's built-in firewall (that is, log in to the router per the manufacturer's instructions and confirm that the firewall feature is enabled; ports 25, 80, and 443 are sufficient for most needs). Also, use secure password practices for managing your router (described above) and consider using media access control (MAC) address filtering to limit the devices able to access your network.[3] Disabling the Universal Plug and Play ("UPnP") on your router can also enhance the security of your network, though it may cause problems for some applications, such as media servers and players. You should only enable UPnP if necessary.[4]

- **Avoid a single point of failure**. One vulnerable IoT device may allow an intruder to penetrate your entire network and access other devices on your network. To minimize the potential harm caused by a single compromised device, keep passwords complex and unique for each device and router. Further, most routers allow you to "segment" your home network so that IoT devices do not have access to the entire network. For instance, you may set up one network for your computers, printers, and other computing devices, a second network for Internet connected-appliances, and a third network for mobile devices. To keep your visitors from infecting your network with malware, many routers also offer "guest" networking that shields your devices from those of your guests. Consult your router's manual for further direction. The more you segment your networks, the harder it will be for hackers to access your devices and information.

- **Pay attention to mobile device security.** When remotely checking your IoT devices from a smartphone or tablet, it is generally good practice to avoid using public Wi-Fi networks that are not password protected. Insecure connections can make your IoT device vulnerable to hacking. However, if you must use an unsecured, public Wi-Fi

[3] A MAC address is a sequence of numbers and letters assigned by a manufacturer to the networking hardware it produces. It serves as a unique identifier assigned to a network device. Network operators use MAC addresses to identify pieces of hardware connected to their networks. If MAC address filtering is enabled, a router will check the MAC addresses of devices seeking to access the network against a list of approved addresses before letting them do so. If a device's address matches one on the router's approved list, access is granted; otherwise, its access is blocked.

[4] UPnP is a feature that allows different brands and types of devices on a network to discover each other and to access each other's services automatically with little or no user action. UPnP and wireless technology such as WIFI and Bluetooth makes it possible for two devices to form a peer-to-peer network, or even to connect to the Internet without a user's knowledge or permission.

network (for example, at an airport, café, or hotel), you should consider using your smartphone or tablet to initiate a virtual private network ("VPN") connection to your local network before opening your IoT-connected applications.[5] Some newer smartphones or tablets have pre-loaded VPN software, while many others support downloadable VPN applications. Although not foolproof, a VPN connection creates a secure "tunnel" to your local network that will make it difficult for anyone to eavesdrop on such sessions and acquire login credentials for your IoT devices.

- **Consider using anti-virus and intrusion detection products that protect IoT devices.** These products are capable of protecting IoT devices in much the same manner as anti-virus software can protect laptop and desktop computers. They can detect abnormal behavior on any device communicating on your network, including a tablet, digital video recorder, or Internet-connected refrigerator. These relatively new products are typically hardware devices that connect to your home network, but software-only versions of this capability are also available. As IoT devices proliferate, so too will software and hardware security products that may help secure IoT devices. Keep abreast of such developments and consider adopting them.

- **Get technical assistance with IoT security.** You may not feel comfortable installing, configuring and maintaining the security of your IoT devices, routers, and Wi-Fi networks by yourself. Turning off features like UPnP, configuring a firewall, or "segmenting" your network, may seem daunting. If you feel uncomfortable, consider asking more technology-proficient friends or family to provide help, or paying to have your IoT devices and routers properly installed and secured. The Consumer Technology Association also offers a guide, Recommended Best Practices for Securing Home Systems, to ensure that your home network is safe and up to date. Investing the time and effort at the outset can prevent difficulties later.

Has Your IoT Device Already Been Compromised?

It can be difficult to determine whether your IoT device is infected by the Mirai malware or some other IoT-targeting malware. An infected IoT device may still function correctly but suffer occasionally from sluggish performance as a result of surreptitiously engaging in botnet activity while performing its regular functions.

Some free online resources can help you determine whether your IoT devices are susceptible to being accessed from outside your network by Mirai or similar malware. However, exercise due

[5] A VPN is a service that can create an encrypted communications channel over the Internet that will permit a computer or other device (for example, a mobile phone) to connect to the user's home or office network. VPNs allow a user to access the resources on a home or office network from anywhere over the Internet as if the user were physically located at her home or office.

caution when using such resources to ensure they are not malware disguised as security software. Be particularly careful if they are not provided by well-known, reputable sources and require you to download and install programs on your computer.

If you determine that your IoT device has been compromised by Mirai or similar malware, turn it off and then on again after several seconds to purge the device's memory, as instructed above. Malware, such as Mirai, often resides in an IoT device's memory, so purging the memory will remove the malware. If your device was compromised because of poor password management, change your password and follow good password management practices as described above before reconnecting it to the Internet. Also, we encourage you to file a report regarding your compromised IoT device with the Internet Crime Complaint Center at the following link: https://www.ic3.gov.