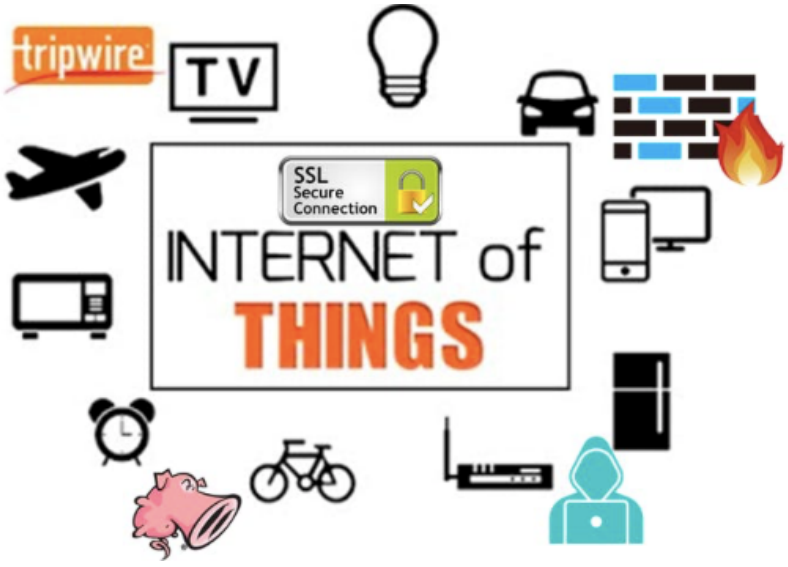
Volume #4 - Issue #178
September 21st, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Protecting Your Internet Connected Devices



Americans use an average of 13 internet connected devices (know as IoT devices) every day. And for the first time last year, IoT devices outnumbered people on Earth — 8.4 billion vs. 7.4 billion. By 2020, experts predict there will be 26 billion IoT devices in existence. As manufacturers

race to meet the demands of an increasingly wired world, cyber criminals are cropping up to exploit weaknesses in IoT infrastructure.

Smart technology has migrated from our phones and laptops to our Nest thermostats, Apple TVs and Roomba vacuums. These devices clean our floors and bring us our favorite TV shows, but what happens when they are suddenly wired to attack? That nightmare scenario became a reality in October 2016, with an attack that almost took down the internet. For hours, internet traffic ground to a halt as some of the world's most popular websites, including PayPal, Reddit and Netflix, became unreachable. The massive denial-of-service (DDoS) attack targeted Dyn, a company that acts as one of the internet's giant switchboards.

To overwhelm the servers at Dyn, hackers turned harmless IoT devices like thermostats and DVRs into a zombie army of malicious bots — flooding Dyn's DNS servers with tens of millions of unique requests.
Executed by New World Hackers as a "power test", the shadowy hacking group used a malware known as Mirai, which scans the internet for vulnerable IoT devices that would make perfect botnets.

There isn't much value in hacking a smart toaster or a thermostat, but their network access is very valuable to would-be hackers. Since 2015, AT&T has picked up a 458% increase in vulnerability scans done by hackers looking to exploit IoT devices. This is especially alarming to retailers, healthcare providers and restaurants, who increasingly rely on tabletop payment devices and hand-held tablets for placing orders, recording patient symptoms and completing mobile checkouts.

The breakneck speed and constantly evolving nature of the Internet of Things has created a fragmented security landscape where network operators, IoT manufacturers, content providers and end users all act

independently. After it took down wide swaths of the internet, the Mirai botnet succeeded in shutting down the internet infrastructure of Liberia. These attacks are alarming signs that someone is honing cyber weapons and using a small nation as its test case. Many experts fear that the worst is yet to come.

In the near future, could cyber criminals careen a self-driving car off the road? Or hack into a thermostat and steal a tech company's most sensitive data? So far, these fears have largely gone unfounded. But a recent WikiLeaks revelation detailed how the CIA has developed tools for hacking into smart TVs so they could listen into meetings at conference rooms and hotels.

While privacy concerns have traditionally trumped fears of cybercrime for IoT consumers, public cloud integration could increase risks of cryptocurrency mining, ransomware attacks and the hacking of vehicles and medical equipment. State and non-state actors will increasingly hack IoT devices for intelligence purposes, and these tools will likely filter down into the hacking community. While 90% of IoT devices on the market collect personal information, 80% did not require a password complex enough to deter hacking, and 70% used unencrypted network services.

IoT devices are so hard to secure because they rely on a wide variety of operating systems, hardware and program languages — many of which are obsolete. And unlike traditionally secure devices like phones and laptops, very few protections are built in to the operating systems of seemingly harmless devices like toasters and alarm clocks. Building out security features is costly and time consuming — objectives that run counter to the red-hot IoT market. Since many of these devices run on generic, Linux-based hardware and software, they often have unused functionality that can be used as a back door for nefarious purposes. Many are also

designed for immediate use without a password, leaving them vulnerable to enterprising hackers. Since security is overlooked as products are rushed to market, only 48% of IoT manufacturers focus on security from the earliest phases of development, less than half issue regular updates and only 20% have IoT security experts on staff.

When it comes to protecting yourself from IoT cyberattacks, decide whether you really need a smart device. When it comes to devices like toasters, consider whether the benefits of the device outweigh the vulnerabilities it adds to your network and your personal information. If you determine that a smart device is worth the risk, segment your network so that IoT devices are isolated from sensitive personal and business information.

Once you've set up an alternate network for your IoT devices, change the default credentials to a difficult password. The Mirai botnet was so effective because it scanned the internet looking for IoT devices shipped with default logins, trying out 60 generic passwords like "admin," "12345" or "password" to gain access.

Other important IoT safeguards include erasing potential malware by disconnecting and reconnecting a device from its power source, checking for firmware updates and disabling Plug n' Play supports that make devices discoverable on the internet.

Thank you for subscribing to our email!