The Internet of Things and Cyber Risk

How You Could Be Victimized

Authored by Phil Kibler, Head of Cyber Risk Consulting, AIG

The purpose of this alert is to highlight recent Internet of Things (IoT)[1]-based denial of service (DoS) attacks. In October 2016, a massive distributed DoS attack was launched against Dyn, a large DNS provider, denying internet users on the U.S. East Coast access to a number of popular websites including Twitter, Amazon, PayPal, Spotify, Reddit, Netflix, and more.

Just a month prior in September, Brian Krebs (a popular cybersecurity journalist) suffered on his website what some are saying to be one of the largest DoS attack attempts ever seen. After analyzing the botnet powering this attack, it was determined that it specifically targeted IoT devices by logging in using default credentials that were never updated and then spreading to other connected devices. Having gained access to over 400,000 IoT devices, the botnet was able to launch the high volume denial of service attack as a result.

> A denial of service attack is when an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.[2]

Why is such an attack possible? What makes an environment vulnerable? One prevalent issue is that many organizations do not continuously update IoT devices after installing them. In addition, some IoT devices do not have the ability to receive patches to update security settings.

Given that there are other known competing botnets targeting IoT devices, we suspect that additional high-volume attacks like the ones described are possible. In fact, there is at least one other known IoT botnet that has compromised approximately one million devices![3] A business must be proactive in ensuring an IoT device is installed correctly and is updated appropriately to help decrease its vulnerability to be compromised.

What Can Organizations Do?

- Make an inventory of all IoT usage to help you better understand the scope of vulnerability.
- If the IoT platform comes with a default ID and password, change them. Attackers know these platforms and their defaults.
- When changing the password, consider using what is considered a "strong" password, which includes:
  - Eight characters minimum;
  - At least one number, one letter, and one capital letter; and
  - If allowed, at least one punctuation character.
- Passwords should be rotated regularly and should remain complex, e.g. not a location, name, or other easily guessable user information.
- Practice a regular timely patch schedule and/or enable automatic updates and patching to occur if the IoT platform allows.
- Disable unnecessary remote administration and features.
- Do not allow unfiltered access to the device from the Internet; only allow whitelisted (trusted) connections via IP filtering or other security controls.
- Do not enable universal plug and play on IoT devices.
- Use secure protocols where possible, like HTTPS and SSH for device communications.
- Include IoT devices in regular vulnerability management programs.

When your organization or employees suffer a cyber-attack, there's more than data at stake. In a rapidly changing landscape, a cyber breach or attack may cause property damage, broad business interruption, or harm to customers. That's why AIG provides clients with proactive risk services, comprehensive insurance coverage, and long-standing breach response and claims teams to help you stay ahead of cyber-related exposures. To learn more, visit www.aig.com/cyberedge.

[1] IoT devices are comprised of DVRs, IP cameras, refrigerators, smart meters, phones, coffee makers, thermostats, routers, cable modems, printers, televisions, eCigarettes, etc.
[2] https://www.us-cert.gov/ncas/tips/ST04-015
[3] http://thehackernews.com/2016/10/linux-irc-iot-botnet.html

11/16 2815D