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 that powered this attack, it was determined that it was meant to target IoT devices, 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? The 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.

Being that there are known to be other competing botnets comprised of IoT devices, we suspect that more 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! A business must be proactive in ensuring an IoT device is installed correctly and is updated appropriately to decrease its vulnerability to be compromised.

What Should Organizations Do?

- Make an inventory of all IoT usage. It's impossible to defend the unknown.
- If the IoT platform comes with a default ID and password, change them. Attackers know these platforms and their defaults.
- When changing the password use 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, but not at the expense of complex passwords.
- 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

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today we provide a wide range of property casualty insurance, life insurance, retirement products, mortgage insurance and other financial services to customers in more than 100 countries and jurisdictions. Our diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.