KUDELSKI SECURITY

THE IMPACT OF (THE LACK OF) IOT SECURITY

There have now been 2 massive rounds of DDoS attacks recently using Internet of Things devices. The first round of attacks took down OVH, an Internet Hosting Provider and cloud hosting service, and KrebsOnSecurity. The second round just occurred, and brought down Dyn, a major DNS hosting provider. This latest attack impacted many sites, including Twitter, Amazon, and Netflix. KrebsOnSecurity has a good article explaining the impact and cause [here].

So why is this happening now? The general feeling is that the release of the Mirai botnet source code has given an IoT army to anyone who wants it. Mirai took advantage of default passwords in IoT devices, and amassed enough resources to produce over 620GB of DDoS Traffic. With the source code released, anyone can run the program to take over the same IoT devices. However, the botnet is really just a symptom. A symptom of the current disregard of security best practices by some in the IoT industry.

In this attack, the botnet is benefiting from IoT device white-labeling. Many IoT vendors will include chips and devices from other manufacturers upstream and sell them as their own. In this case, according to this Flashpoint report, a Chinese manufacturer was providing DVR, NVR, and IP based camera boards to downstream manufacturers. These boards had default usernames and passwords that were effectively unmodifiable. In addition, they also included default-enabled services that allowed easy access to these accounts.

For an IoT manufacturer, there are two points where this attack could have been prevented. First, the Chinese manufacturer should have done a security analysis of their device and removed the account. Second, the IoT downstream vendor should have done a security analysis of any chip or board they were including in their product. They could have asked the upstream provider to fix the issues or provided countermeasures in their own product.

Realistically, all IoT vendors do not have the security expertise to architect robust, safe systems that are hardened against attack. That said, IoT vendors need to become more security conscious. They need to pressure their industry to enable security by default as well as embrace already common corporate practice of external penetration testing and security assessments to assess their devices, for the safety and security of us all.

The problem with this is that there is nowhere for IoT vendors to turn for this expertise and support. On that topic there is more to come, and very soon. Stay tuned…

Kudelski Security Team
request@kudelskisecurity.com