Shodan

Shodan Vulnerability Assessment & IoT

The Shodan website is a “search engine for Internet-connected devices.” There are a ton of connected devices out there that are constantly broadcasting data, video, audio, etc. This probably does not come as a huge surprise in general, but maybe it hits a little harder when the devices are close to home. This assignment will attempt to look at some IoT devices that you are personally aware of.

Instructions

1) Go to the search engine at shodan.io (Links to an external site.)Links to an external site.

2) You don’t have to log in to run an assessment, but it helps provide more comprehensive search returns, like the maps. I logged in with my Google account, but Facebook, Twitter, etc. logins are also available. The Login button is at the top right.

Device are located and identified by the content of its "banner" object. This is metadata that is publicly transmitted and includes things like SSIDs, IP addresses, etc. You should use filters when you perform a search, otherwise your search returns will be limited by the contents of a device's banner. Filters include "country:", "org:", "city:"

3) **Freestyle Search:** Search your hometown or something “close to home.” Example: city:Starkville

4) Report what you find. Can you identify any businesses, individuals, etc? What type of data seems to be broadcasting?

5) **Third Floor Search:** Run a second search, this time the IP address 130.18.86.48. What device is this? Can you tell when the SSL certificate expires on this device?

6) Now search 130.18.86.47. What about its SSL certificate?

Like most search engines, you sometimes find results that are relevant to what you are attempting to find and sometimes you don’t, but that is the spice of life, isn’t it?

Revision #1
Created 27 February 2019 20:05:34 by Aaron Kimbrell
Updated 27 February 2019 20:07:21 by Aaron Kimbrell