Mapping “Badness”

“Even before you understand them, your brain is drawn to maps”

Ken Jennings, author and Jeopardy champ

Maps have always been in the realm of geographers, but that realm has been steadily opening over the last few decades. Over the last computers and the Internet , now any yahoo can map out data on Google (the play there was intentional). And as we saw in Chapter 4, it’s possible to pull geo-location of IP addresses and get spatial data, and that’s what we’re going to focus on.

How do maps help us within information security?

The data we are going to use for this chapter comes to us from Symantec, who shared a list of clients infected with the ZeroAccess Botnet.

Chapter Use Case: ZeroAccess Botnet Analysis

What can you learn from just a set of lat/lon pairs?

Getting basic lat/long metadata (lat/lon -> country/city)

Visualizing lat/long data

Choropleth

Dot plot

Getting more advanced metadata (internet user population & income)

The quest for correlation

WEB CONTENT: ZeroAccess code & visuals

points on a globe

points in the U.S.

setting alpha on the map points

What is the bot infection per state given the # of internet users?

(choropleth on a state basis)