Chapter 4: Analyzing “Badness”

“Sometimes, bad *is* bad.”

Huey Lewis & The News, Sports, Chrysallis Records, 1983

This chapter will continue the exploration of the AlienVault IP Reputation database that began in Chapter 3 and assumes the reader is familiar with the description of the data set and has at least followed along with the preliminary analyses. As stated in the introduction of the book, no attempt has been made to incorporate consideration of or conduct analyses on Internet Protocol (IP) version 6 (IPv6) addresses and all the examples found in this chapter will be based on IPv4. Given the slow adoption and migration to IPv6 plus the plethora of “badness” still on IPv4 networks, this should not be a practical limitation in any way, shape or form.

The struggle to protect, defend and understand our modern networks begins and ends—more often than not—with an IP Address. IP addresses are defined in RFC 791, the “Internet Protocol / DARPA Internet Program / Protocol Specification” (http://tools.ietf.org/html/rfc791), which has an elegant and succinct way of describing them:

“A name indicates what we seek. An address indicates where it is. A route indicates how to get there.”

Global entities slice and dice them for public and private use; devices, systems and applications log them for future reference; network management systems test, group, display and report on them; and, security tools make critical decisions based upon them. But, what— exactly—*is* an IP address and what part can/do they play in the quest for finding and mitigating “badness”?

Dissecting The “IP Address”

32-bit integer (“how does your computer see an IP address?”) + machine info

Part of a subnet / logical layout / MAC addresses, perhaps has a hostname (DNS)

Larger context: part of a global network organized by ASNs (BGP)

Lager context: Has a physical location

Mapping Outside the Continents

USE CASE: Visualizing AlienVault ASN data (force-directed network graphs of malhost ASN groupings)