EIGHT DEGREES OF

Kevin Bacon

ON THE INTERNET

You've heard of 'Six Degrees of Kevin Bacon,' the game that challenges players to connect the prolific actor with any other actor via their film roles in six steps or less. With RiskIQ, we can do something similar, only using web assets.

LEGEND: DATA PIVOT

A CYBER SECURITY COMPANY AND ITS THREAT RESEARCH TOOL

Host Pairs
www.riskiq.com

- Host pairs are generated when RiskIQ crawls web pages and identifies references or redirections to other websites
- Crawlers observed the RiskIQ website referencing the PassiveTotal blog using an image source reference

A PHONE NUMBER

WHOIS Records
blog.passivetotal.org

- WHOIS records must contain a valid email address and phone number
- PassiveTotal was registered with 1&1 web hosting using privacy protection services. Through the WHOIS record for the domain, PassiveTotal links to a phone number in Pennsylvania belonging to "1&1 support"

A COUNTRY MUSIC STAR

Passive DNS
1-877-206-4254

- Passive DNS is a system of record that stores DNS resolution data for a given location, record, and time period
- 1&1's support phone number leads to thousands of other websites registered with 1&1, including www.stephaniechapman.com, a musician based in Nashville, TN.

AN EXPIRED SSL CERT

OSINT
www.stephaniechapman.com

- From October 27th, 2010 to present day, RiskIQ observed www.stephaniechapman.com resolving to 68.71.99.147, an IP address based in the United States and associated with Peak 10
- Open source intelligence reveals a music profile piece from BMI on Stephanie Chapman and her music career, the resolving IP of which (68.71.99.147) associates with several other domains featuring various artists. Many of these domains have an expired SSL certificate, 82be100c22f790c364e68467c04900ee17e00014.

A WEB DEVELOPMENT FIRM

Subject names
Certificate 82be100c22f790c364e68467c04900ee17e00014

- SSL certificates contain data describing the domain it applies to and who issued it
- Based on the subject common name, the broken SSL certificate shared by www.stephaniechapman.com and many other domains was issued for www.musiccitynetworks.com

AN IP ADDRESS

Passive DNS
www.musiccitynetworks.com (subject name)

- Music City Networks is a web company offering services in e-commerce, site development, and fulfillment
- Passive DNS information showed a resolution to 209.62.112.34 between the time periods of September 2009 and January 2010

A DOMAIN BELONGING TO KEVIN BACON

209.62.112.34

- Over 1,000 domains have used this IP address as their host at some point in time
- Many of the domains associated with this IP address are that of country music stars or artists—it's very likely that Music City Network was tasked with building and setting up hosting for many of these artists
- One of these domains is www.baconbros.com

A BAND CALLED BACON

- The Bacon Brothers is a Folk Rock band featuring Kevin Bacon and his brother Michael
- Yes, Kevin Bacon has a band called the Bacon Brothers. He plays guitar

VIEW THE WHITE PAPER

RISKIQ®