RISKIQ®

Eight Degrees of Kevin Bacon:

Threat Research Edition

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 (e.g. Leslie Nielson was in Alien Dawn with Iva Franks Singer, who was in Final Analysis with Tony Genaro, who was in Tremors with Kevin Bacon).

With RiskIQ, we can do the same thing, only using web assets. What do we mean?

Kevin Bacon is a film actor, not a threat actor. But like threat actors, he has a digital footprint that spans the internet, the assets of which can be linked together and mapped using internet data sets. To prove it, we'll use RiskIQ PassiveTotal™—RiskIQ's threat research tool—to show how, via eight degrees of web separation, you can link Kevin Bacon to anyone or anything on the internet—even us.

PassiveTotal overcomes the challenges in discovering and proactively blocking malicious infrastructure with innovative techniques and research processes. With it, threat researchers can identify overlapping infrastructure using passive DNS, WHOIS, SSL certificates, and more.

Please note that with PassiveTotal, most threat researchers can make the connection between Kevin Bacon and RiskIQ in one or two pivots. But for the sake of showing the extent of the connections you can make, i.e. the extent to which you can expose an attacker's digital footprint, we're going to cycle through eight degrees of separation. From country music stars to e-cigarette sites, there's almost no limit to what you can uncover when you put PassiveTotal data sets to the test.

Here's how you can connect Kevin Bacon to RiskIQ

A Cybersecurity Company and its Threat Research Tool

Degree 1: www.riskiq.com

Data set: Host Pairs

RiskIQ links to the PassiveTotal blog via host pairs. Host pairs are generated when RiskIQ crawls web pages and identifies references or redirections to other websites. On July 07, 2016, crawlers observed the RiskIQ website referencing the PassiveTotal blog using an image source reference.

Statistics

- 13 unique IP resolutions (Cloudflare, Rackspace)
- 40 tracking codes (Google Plus, Twitter, Github, PassiveTotal,
- 102 host pairs (Vimeo, Marketo, Google Analytics, Optimizely)
- 73 components (Tracking pixels, CDNs, Apache, Wordpress)
- 10 OSINT links (LinkedIn, Crunchbase, Wikipedia)

Notables

Most of the content associated with RiskIQ is standard, but there's one website that also appears in the host pairs, www.roboknights.org, which happens to be a FIRST LEGO League team. RiskIQ observed this connection from May 22, 2016, to July 25, 2016, associated by the Lego team site referencing an image on RiskIQ's webpage.

A Phone Number

Degree 2: blog.passivetotal.org

Data set: WHOIS Records

The PassiveTotal blog links to a phone number in Pennsylvania through the WHOIS record for the domain. WHOIS records may not always be accurate, but generally, they must contain a valid email address and phone number. In this case, because PassiveTotal was registered with 1&1 Web Hosting using privacy protection services, the phone number (+1 (877) 206-4254) belongs to 1&1 support.

Statistics

- Five unique IP resolutions (Cloudflare)
- 12 tracking codes (Google Analytics, Github, Twitter)
- 23 host pairs (CDNs, Github, jQuery, Google)
- 25 components (Ad Exchange, Twitter, Ghost)
- 10 OSINT links (Vimeo, Dark Reading, Facebook)

Notables

Using the tracking pixels found on PassiveTotal, it's possible to walk back up an infrastructure chain to identify more services like the API website, RiskIQ services, and third-party vendors such as GreenHouse.

A Country Music Star

Data set: Passive DNS

Degree 3: 1-877-206-4254

1&1's support phone number leads to thousands of registered websites with themes ranging from tax filings and Tesla supply parts to hacking pages and stamp collector sites. There are tens of thousands of domains, including www.stephaniechapman.com, a site for a musician based in Nashville, TN. Her domain was also registered using 1&1 with privacy protection services.

Statistics

- 3K+ matching domain records
- Hundreds of unique email addresses (1&1-private-registration.com)
- Many domain registrations dating back ten years

Notables

Among the thousands of domains registered using 1&1 privacy protection services, there are a couple of interesting websites, such as bestsmokealarms.infom, e-cigarette-reviews.info, folkmetal.info, cheapswordsgalore.info, and japaneseantiquities.info

An Expired SSL Cert

Degree 4: www.stephaniechapman.com

Data set: OSINT

During the dates of October 27th, 2010 through present day, RiskIQ observed this domain resolving to the IP address 68.71.99.147. Based on the United States, this IP is associated with Peak 10.

Statistics

- Three unique resolutions (SoftLayer Technologies, Zayo Bandwidth, Peak 10)
- Coverage period - 2009/09/04 - 2016/08/12
- Registered in 01/2004 and expires 01/2017

Notables

Open source intelligence reveals a music profile piece from BMI on Stephanie Chapman and her music career. Exploring the other domains associated with the resolving IP address reveals more musical talent such as Kelly Clarkson, Roy Orbison, Don Derby, and Jason Petty. Several other artists, recording websites, and music networks are also sprinkled into the domain. Many of these domains have an expired SSL certificate, 82be100c22f790c364e68467c04900ee17e00014.

A Web Development Firm

Degree 5: Certificate 82be100c22f790c364e68467c04900ee17e00014

Data set: Subject names

Within the expired SSL certificate, there's data that describes the domain to which it applies, and who issued it. Based on the subject common name, this certificate was issued for www.musiccitynetworks.com.

Statistics

- 1,019 unique domain resolutions (Several music artists)
- 2 SSL certificates (both expired and issued to musiccitynetworks)
- Coverage period - 2010/10/27 - 2016/08/12
- Peak10 IT infrastructure provider

An IP Address

Degree 6: www.musiccitynetworks.com (subject name)

Data set: Passive DNS

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 during the time periods of September 2009 through January 2010.

Statistics

- Seven unique resolutions (Peak 10, SoftLayer Technologies, Enom)
- Public WHOIS links to the company
- One host pair (Additional company owned domain)
- 1 component (Redirector)
- 6 OSINT links (LinkedIn, TodoCast)
- Coverage period - 2009/09/02 - 2016/08/12

Notables

Following the host pair lead to mcninteractive.com reveals several other data set leads including trackers, more host pairs, components, and passive DNS resolutions.

A Domain Belonging to Kevin Bacon

Degree 7: 209.62.112.34

Over 1,000 domains have used this IP address as their host at some point in time including Kevin Bacon's band, Bacon Bros.

Statistics

- 1,023 unique resolutions (A lot of music artists)
- Coverage period - 2009/08/31 - 2016/08/11

Notables

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. It could be that the agents or producers of the artists have a contract deal with one main provider to create a web presence for each of their clients.

A Band Called Bacon

Degree 8: www.baconbros.com

And finally, we arrive at Kevin Bacon's official band website, Bacon Bros.

Statistics

- Five unique resolutions
- Privacy protected WHOIS
- 15 trackers (Twitter, Soundcloud, Google, Facebook)
- 24 host pairs (Twitter, Facebook, Huffington Post)
- 22 components (CDN, Apache, CentOS)
- 10 OSINT links (Facebook, Music venues)

Notables

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.

Many of the open source intelligence links lead to news articles profiling performances by Bacon Bros, including a performance at the San Diego County Fair. Following several of the tracker leads also reveals connections to a couple of other interesting domains including www.kennyrogers.com, foodtrucksnash.org, and eastoncorbinfans.com.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com