RSA FirstWatch

Link by Link: Crafting the Attribution Chain

Will Gragido, Sr. Manager RSA First Watch

William.gragido@rsa.com

May , 2013

#RSAC @RSAConference

RSA EMC²

Agenda

- Introduction
- Definition
- Explain
- Breadcrumbs
- Linkage
- Why Should We Care

#RSAC @RSAConference

Link by Link: Building the Attribution Chain

#RSAC @RSAConference

Defining Attribution

- There is no universally agreed to definition for attribution
- I like the following:
  - Definition:
    - Attribution is the assignment of ownership of a threat act or action to a threat actor or agent
- Discipline of Psychology
  - Offers a few key definitions to consider as we discuss attribution
    - Explanatory Attribution
      - Answers the question 'why' someone does one thing or another
    - Interpersonal Attribution
      - Answers the question 'why' something occurs when 2 or more causes are present

Attribution Explained

- Why should you and I care about attribution?
  - For many people attribution is the 'holy grail'
- Without attribution analysis there can be no lawful resolution
  - Many parties are interested in this
  - Difficult due to a number of things not the least of which are geography and international law
- According to the experts (not me) Attribution analysis is:
  - A paramount argument for the use of active defense measures is the ability of one state to hold another state responsible for a cyber attack
  - Attribution is necessary for creating and supporting a system of deterrence
    - E.g. "we know who and where you are."

Attribution Explained

- Attribution is difficult!!!
  - It doesn't help when people falsely claim responsibility for attacks
- Categories of Actors
  - Non-State Sponsored
  - State Sponsored
- Types of Actors
  - Criminal
  - Sub-national
  - Nation state

A Word About Cyber Attacks

- **Cyber Attacks are:**
  - Plentiful
  - Looming
  - Frequent
  - Sophisticated and unsophisticated
  - Result of Criminal, Sub-national and State Sponsored activity…sometimes all three
  - Motivated by:
    - Politics
    - Philosophy
    - Profit
    - Agenda
  - Impact everything that means anything to us: our enterprises, our brands, our livelihoods, and way of life
- Cyber attacks are serious business and often misunderstood at the macro level
  - And if we are misunderstanding them at the macro level, are totally misunderstanding them at the micro level?

 *#RSAC @RSAConference*

A Word About Cyber Attacks

- What is really under attack during a cyber attack?
  - An asset?
  - A person?
  - A system
  - An entire ecosystem?
  - Or is it the confidence in that which is supposed to protect us(e.g. prescriptive controls etc.) that is under attack?
- At their core…
  - Cyber attacks are psychological attacks
    - Preying on our fears
    - Preying on the confidence we place in systems
  - Rose McDermott, Brown University
    - "Decision Making Under Uncertainty"
    - Complexities that arise from our natural desire to favor certainty (feigned or real) in the face of conflict*

Breadcrumbs

- The ‘juicy’ bits that get left behind a threat or actor
- These are akin to ‘artifacts’
- Often if one pays enough attention during forensic analysis of both hosts and networks a trail emerges
- Following the trail is dependent upon sound link analysis

Linkage

Linkage

- Definition:
  - An associative relation
    - Between people
    - Between data
    - Between threats
    - Between everything and everyone
    - Six Degrees of Kevin Bacon
- Help establish the attribution chain

#RSAC @RSAConference

Linkage

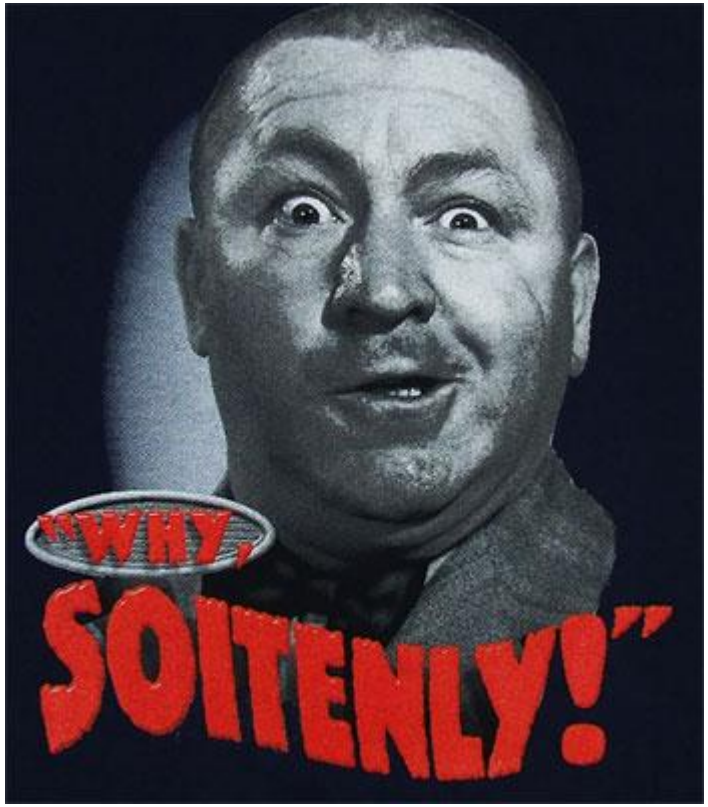
- Tell a lot about things that by themselves say very little
  - E.g. an IP address believed to be associated with a C2 that is associated with a domain registered in Hong Kong to a known threat actor
- Aid in telling the story
- Are not the story in and of themselves
- Require study and scrutiny
- Warrant a multi-dimensional analytic process be conducted

Linkage

- There are no short cuts in establishing the attribution chain
- The linkage helps define the chain or the path to the threat actor
- Being able to identify linkages expedites the crafting of the chain but does not constitute a short cut

Should We Care?

Is attribution really that big of a deal?



#RSAC @RSAConference

Should We Care?

Reality is that attribution is a HUGE deal that has a lot of people working day and night on solving it

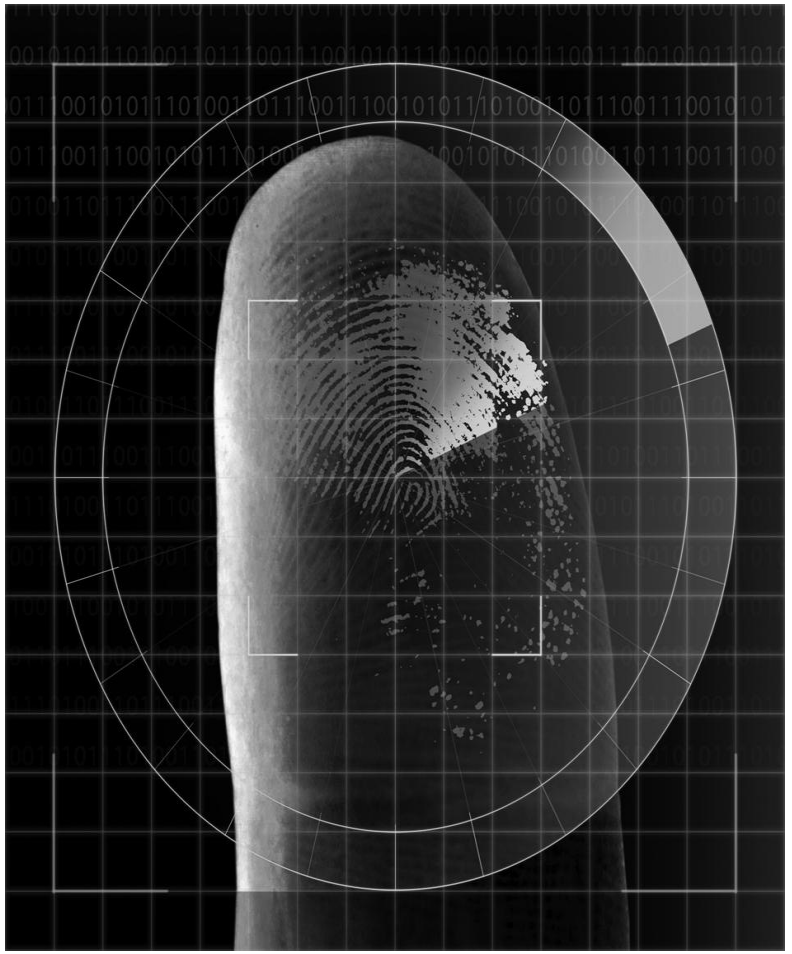
#RSAC @RSAConference

Should We Care?

- Attribution is one the greatest challenges that we face as an industry today
- Everyone is talking about it but some are afraid of the consequences…
- **Because** at the end of the day we need to know who is responsible for what is occurring

Should We Care?

- **Attribution is not a trivial matter**
  - Proving the identity of a threat actor or agent requires a great deal of work and patience
    - It requires **evidence**
    - **Being wrong is not optimal in attribution analysis**
  - Collaboration between investigators, victims and law enforcement is a essential



Should We Care?

- Four main concepts to grasp regarding attribution:
  - Ownership (Machine(s) used in threat act or action)
  - Location (Geo Intelligence)
  - Threat actor or agent (HUMINT)
  - Aggregate Identity of individual or group

#RSAC @RSAConference

Should We Care?

- There are two core types of attribution that investigators must be concerned with:
  - Technological attribution
  - Human attribution
- Broken down in a bit more detail these forms or attribution answer the following questions:
  - Who?
  - Why?
  - How?
  - From Where (Geo Intelligence)?
  - Frequency
  - Stages of attack / IOCs
  - Evidence / Artifacts
  - Infrastructure (C2/ Covert Channel)
  - Threat actor / agent
  - Affiliation

Should We Care?

- In order to establish concrete Attribution one must establish the following:
  - **Agreement**
    - Amongst multiple parties
    - Corroboration
  - **Uniqueness**
    - Signatures
    - Approaches
    - IOCs
    - Be ware the false flag!
  - **Regularity**
    - Frequency
    - Repetition
    - Execution path

Should We Care?

- Take Aways
- Attribution analysis provides:
  - A clearer picture of who the threat actor or agent is and what their intentions are toward ourselves and others
  - An opportunity to share intelligence within the research community
    - Provided we can circumnavigate the cultural, legal, and national security impediments that present themselves from time to time
  - The opportunity to better prepare ourselves for the next encounter with a threat actor or agent
  - The opportunity to seek criminal (where appropriate based on jurisdiction) prosecution for damages

Should We Care?

- Take Away's
  - Attribution is often discussed in the literal, HUMINT 'who done it' sense
  - It's also often quite misunderstood due to the absence and omission of psychology in the chain establishment process
  - Establishing 'linkage' or relationships is paramount in establishing attribution
  - Mature attribution can lead to effective deterrence
    - Active Defense anyone?

Questions and Answers

#RSAC @RSAConference