

New Analyst/Agent Training – Academy plans

- A Key play-back of lessons learned is needed here – or at least some of them, ie....
    - Terrorist/Finance Groups – have shown (and stated) that they:
        - Are interested in exploiting any weakness in Western Culture/Society that -leads to them receiving a lot of $$$ Money.
        - Encourage their supporters to find ways to "make more money via the internet in one week" than any legitimate job could bring to over any given year.
    - We've identified clear ties to Terrorist Financing operations, (Post 911) through credible link-analysis done with US-CERT and the NCFTA.
    - The earliest sign/indicators of criminal conduct worthy of our attention – may manifest through on-line schemes (appearing to be random fraud scenarios) that :
        - 1) Terrorist Finance groups know will likely be viewed as "under the radar" and that,
        - 2) Key Law Enforcement agencies will choose to NOT ADDRESS, based on pre-conceived notions that these are "Low Priority" or somehow outside of one organizations Area of Responsibility or "AOR".

In formulating a strategy for "Success" in developing new analysts/agents, we should also note that:

- Bad guys do not formulate on-line schemes to defraud 1 victim, but more design such schemes to identify/focus on the broader population of potential victims – leading the highest volume of victims and $$$ obtained.
- More/Better intelligence is "always preferred". Who holds that intelligence & how it is leveraged is vital to our Intelligence development plans.

With this in mind, the following plan is offered:



Intelligence Development Plans:

In acknowledging the points above, (yes we need to say this out loud on occasion) we can also identify the best **spheres of intelligence** development to focus on, which should include:

(* Using fraud/complaint intel from IC3 and other sources)

- Part One - Early groundwork

Four key layers of early intelligence development:

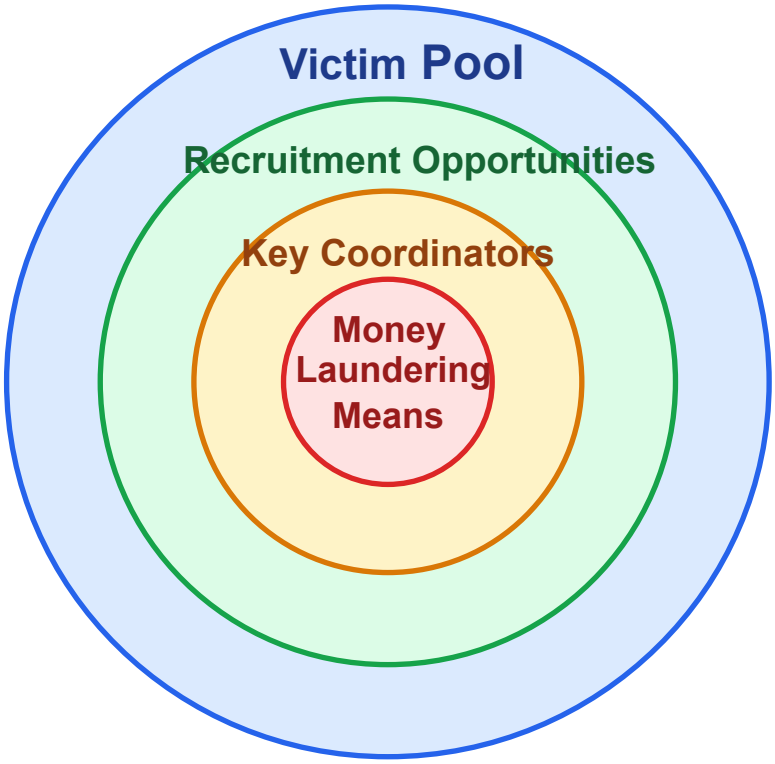
- How are victims being targeted?
    - How is Phish or Lure designed? - What are the "Emotional Hot Buttons"? (remember = Emotion will drive action much more than Logic/Security does)
    - Anything unique or noteworthy about the Phish-Kit – which might show a "signature" of responsibility? (this can pertain to Malware/infections also)
    - Are any on-line platforms targeted? If so- which and why?
    - What other Internet/ecommerce partners should be engaged?

- How are active participants in the scheme- recruited/developed?
    - How would we (as active intelligence developers) offer ourselves for recruitment? (Key output for Law Enforcement)
    - Are there on-line forums where participants are recruited? (Key output for Law Enforcement)

- Identify key coordinators – leaders at different levels (even if just an on-line Moniker) - (Key output for Law Enforcement)
        - Identify- where possible – inner circle of key coordinators -ie.. who appears to be closer- more interactive with each? (Key output for Law Enforcement)

- Short of becoming an "active participant" can we identify any method or preferred means for receiving/moving money $$? (Key output for Law Enforcement)

Intelligence Opportunities



*Each developed output area = increases the value of Intelligence provided to Law Enforcement & many Private Industry collaborators along the way.



- Part 2 -Moving Intel train forward:

Second Phase of Intelligence Development Plan:

- Clarify most logical/active areas (forums) for recruitment of active participants, include history, known/suspected owners or managers.
- Develop link analysis of identified key coordinators – circles of associates etc…
- Expand link analysis of money laundering mechanics – know and/or suspected.
- Develop opportunities for deeper/active intel development best coordinated via Law Enforcement.