DRAGOS

Safeguarding Civilization

Hunting with the Diamond Model

Sergio Caltagirone

@cnoanalysis

DiamondModel.org

“Intelligence analysts should be self-conscious about their reasoning process. They should think about how they make judgments and reach conclusions, not just about the judgments and conclusions themselves.“ Richards J. Heuer Jr

“Intrusion analysis is as much about tcpdump as astronomy is about telescopes.“ Chris Sanders

DRAGOS

Hunting

- What is hunting? The search for the undiscovered
- Hunting is hypothesis testing
- Hunting is the most expensive information security endeavor
  - Filled with assumptions
  - Risks of little/no return
- A proper strategy supports successful hunting

A Hunting Strategy

1. What are you hunting?
   - Exactly what activity are you hunting – define by kill chain phase
   - Your goal
2. Where are you hunting?
   - Visibility
3. How are you hunting?
   - Tools & approaches
4. When are you hunting?
   - A strategy must be time-bound

Building a Hunting Approach - Why

Define your hypothesis

We hypothesize adversaries establish infrastructure prior to operations

We hypothesize adversary X continues to structure their domains using a certain pattern

We hypothesize adversary X continues to use name server Y

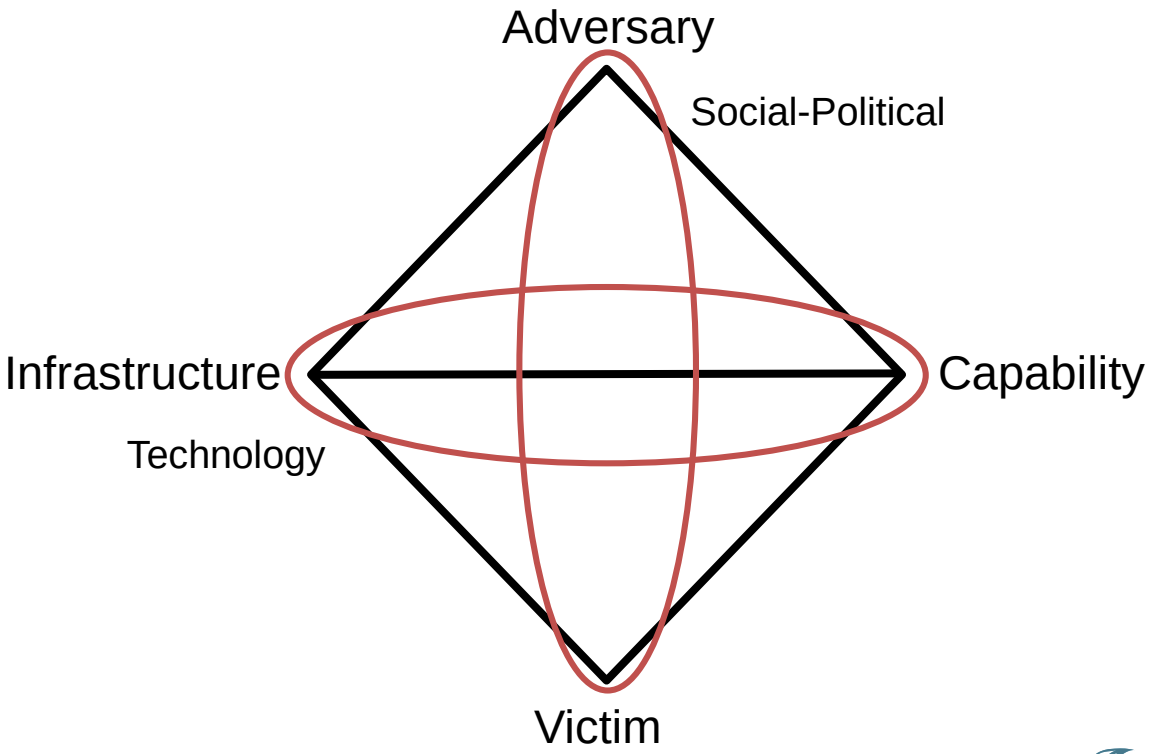
Example Hunting Strategy & Approach

Why	HYPOTHESIS: Adversaries establish infrastructure prior to ops, adversary X continues to structure their domains the same, they continue to use the same name server and same name structure
What	GOAL: monitoring nameserver for new names matching the pattern – find new names prior to operations providing proactive defense. Identify victims in domain name
Where	The baddomains.com name server
How	Query baddomains.com name server every morning identifying the domains not seen the previous day and any domains with the known pattern.
When	Leverage this strategy for 1 month to provide for any dips in adversary activity during that period

Discovery through ‘centered approaches’

Centered approaches enable the discovery of new activity

- Victim-centered
- Capability-centered
- Infrastructure-centered
- Technology-centered
- Social-political-centered
- Adversary-centered



Safeguarding Civilization

Sergio Caltagirone
@cnoanalysis