STIX 2.1 → STIX 1.2

And the ‘Infinity Coding Possibilities’ problem

eclectic iq

INTELLIGENCE POWERED DEFENSE

Health Warnings:

None of this is new…but let’s get the basics right

Context is granularity – granularity is complex – do it to reach utopia

OASIS and Mitre tools/idioms

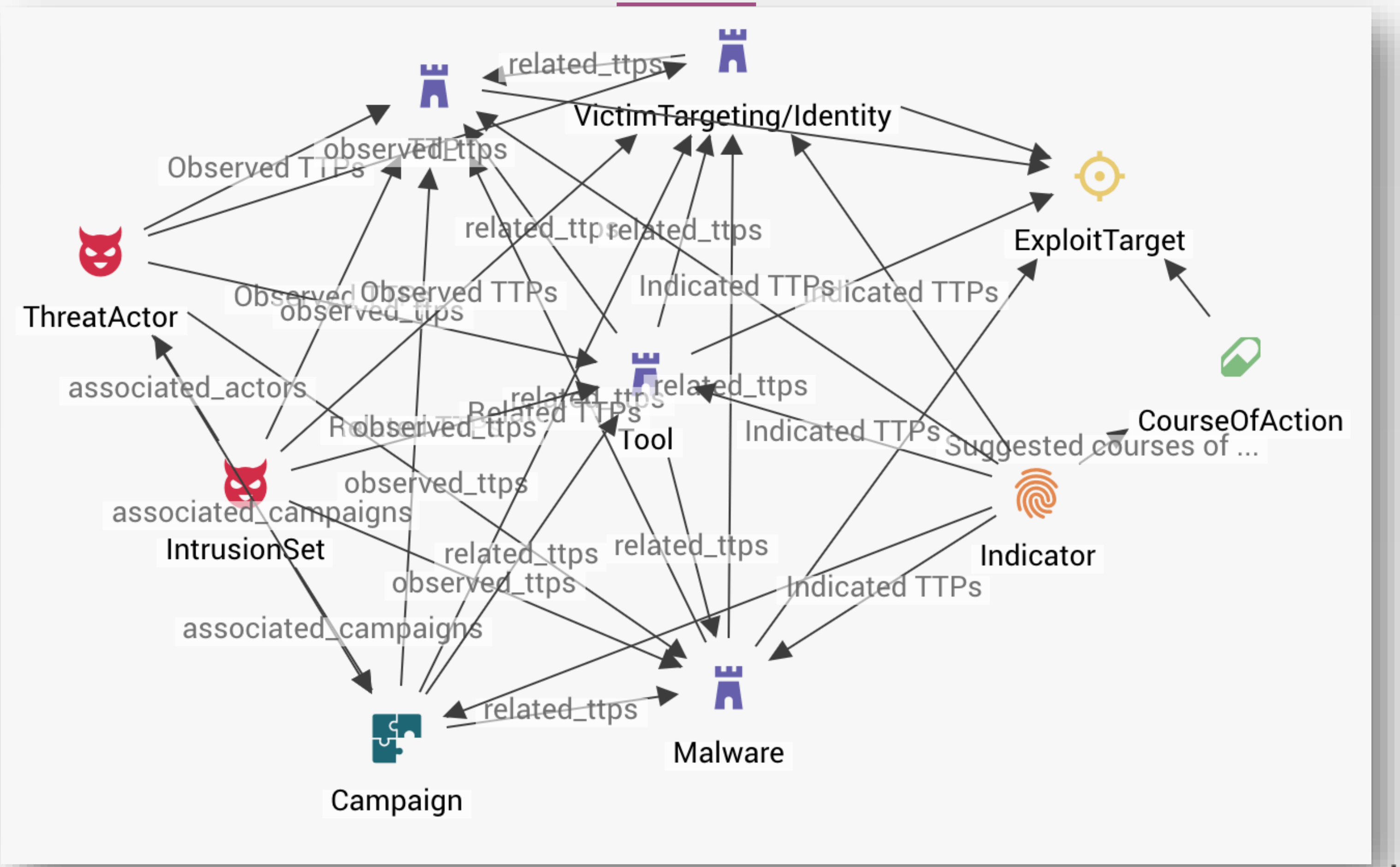
…I might get a bit ‘pokey’

This was a team effort

WHAT I HOPED FOR FROM STIX…

- Objectivity – compliment unstructured data with matter-of-fact
- Retraceable logic – I say what I mean and mean what I say
- Cross-reference(able) – 2 alien analysts can share and benefit

WHAT I GOT…



eclectic iq

RETCON

THE APPROACH

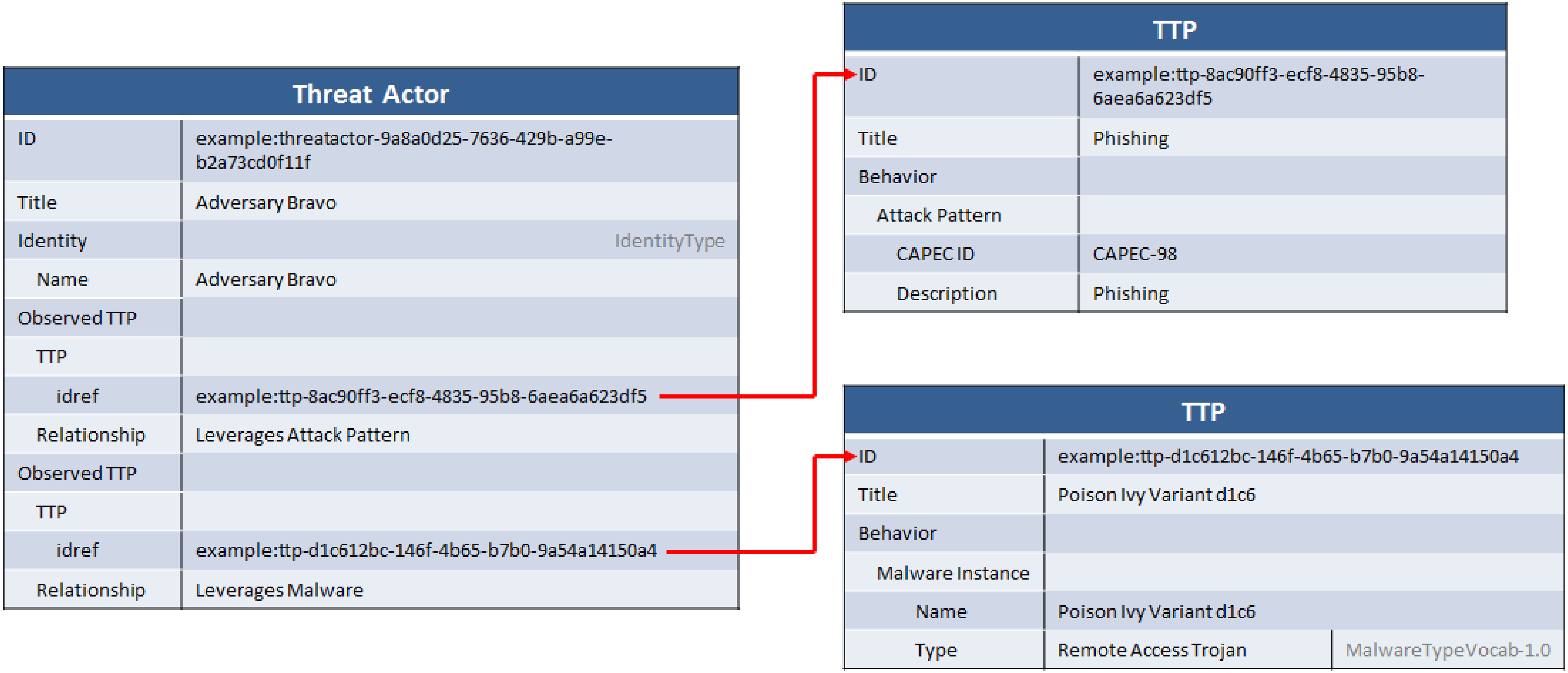
- Make RetCon for 2.x → 1.2
    - Encourage 2.x adoption
    - Not discourage 1.2 (just be glad people are using structured intel)
    - Make it actually work for Operations

- Make bottom-up context a standard
    - Consumers can actually derive context
    - …without needing a new data profile every taxii run
    - …and without shoe-horning the standard

- Integrate it with top-down Intel Analysis
    - Avoid low-granularity traps
    - Enable pivoting

Create a STIX Profile?!
…anyone?

TOP-DOWN
THREATACTOR → (LEVERAGES) → ATTACKPATTERN

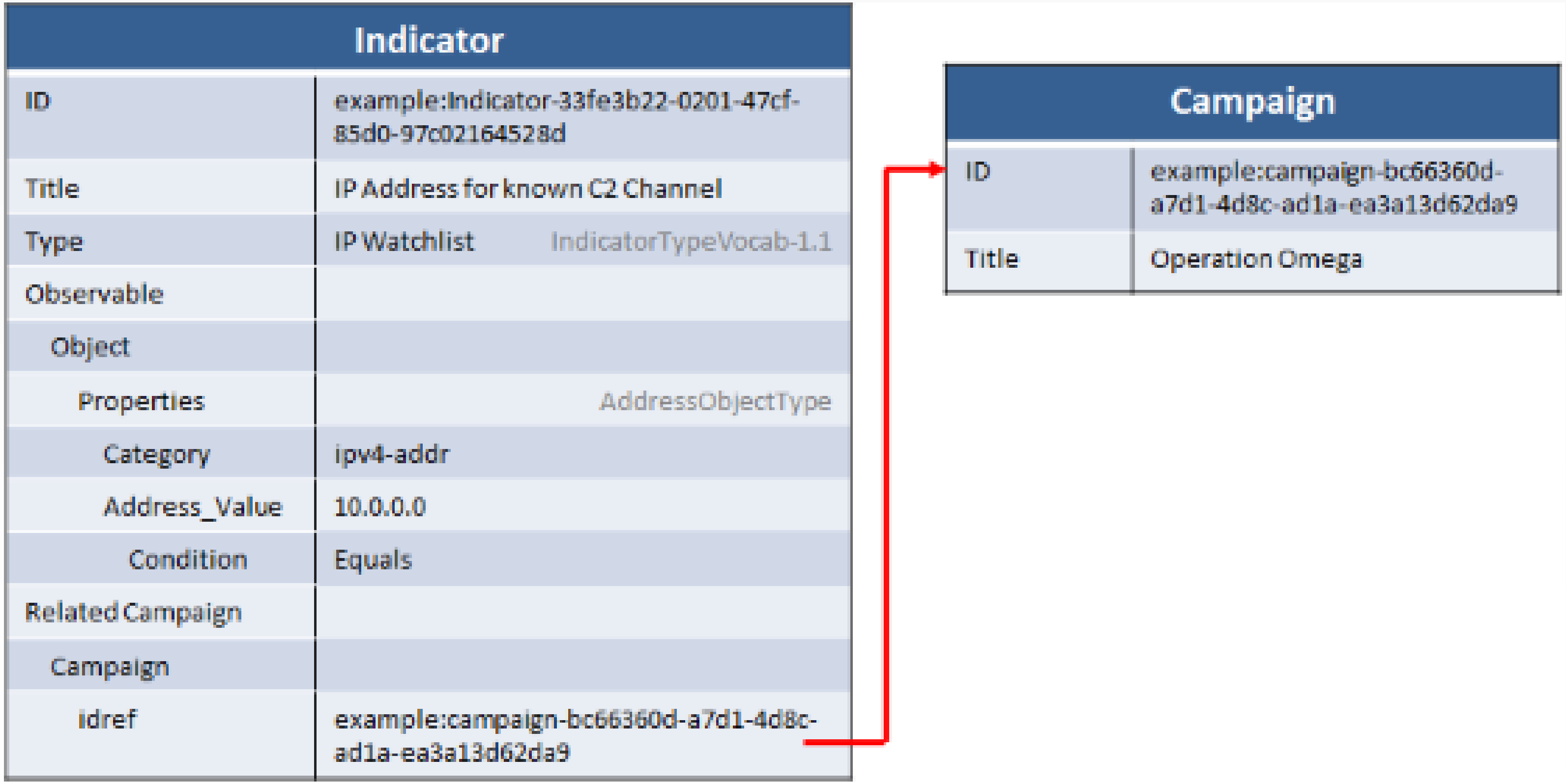


Threat Actor	
ID	example:threatactor-9a8a0d25-7636-429b-a99e-b2a73cd0f11f
Title	Adversary Bravo
Identity	IdentityType
Name	Adversary Bravo
Observed TTP	
TTP	
idref	example:ttp-8ac90ff3-ecf8-4835-95b8-6aea6a623df5
Relationship	Leverages Attack Pattern
Observed TTP	
TTP	
idref	example:ttp-d1c612bc-146f-4b65-b7b0-9a54a14150a4
Relationship	Leverages Malware

TTP	
ID	example:ttp-8ac90ff3-ecf8-4835-95b8-6aea6a623df5
Title	Phishing
Behavior	
Attack Pattern	
CAPEC ID	CAPEC-98
Description	Phishing

TTP		
ID	example:ttp-d1c612bc-146f-4b65-b7b0-9a54a14150a4	
Title	Poison Ivy Variant d1c6	
Behavior		
Malware Instance		
Name	Poison Ivy Variant d1c6	
Type	Remote Access Trojan	MalwareTypeVocab-1.0

BOTTOM-UP
INDICATOR → (INDICATES) → CAMPAIGN



Indicator	
ID	example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d
Title	IP Address for known C2 Channel
Type	IP Watchlist IndicatorTypeVocab-1.1
Observable	
Object	
Properties	AddressObjectType
Category	ipv4-addr
Address_Value	10.0.0.0
Condition	Equals
Related Campaign	
Campaign	
idref	example:campaign-bc66360d-a7d1-4d8c-ad1a-ea3a13d62da9

Campaign	
ID	example:campaign-bc66360d-a7d1-4d8c-ad1a-ea3a13d62da9
Title	Operation Omega

MACRO VS MICRO ENTITIES

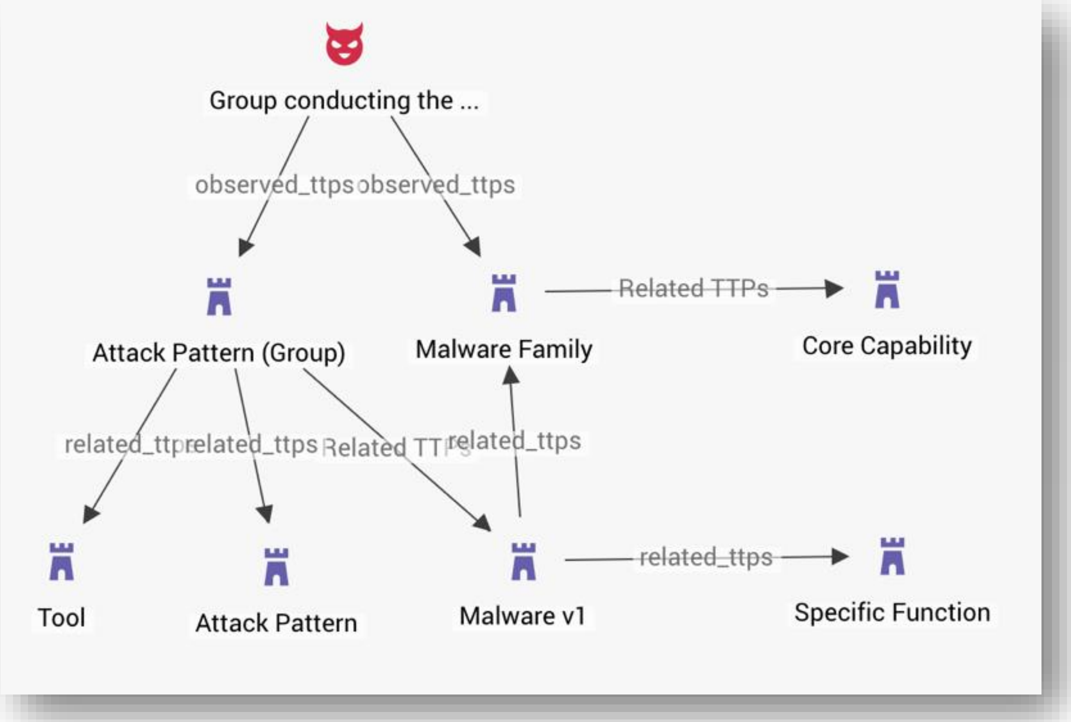
- Top-down thinks more ‘macro’:
  - What sectors does this actor target?
  - What are the motivations?
  - How do we track composite TTPs?
- Bottom-up thinks more ‘micro’:
  - What does this indicator mean?
  - What vulnerability is targeted?
  - How can I track this malware?
- Some cover both – we need to distinguish between them

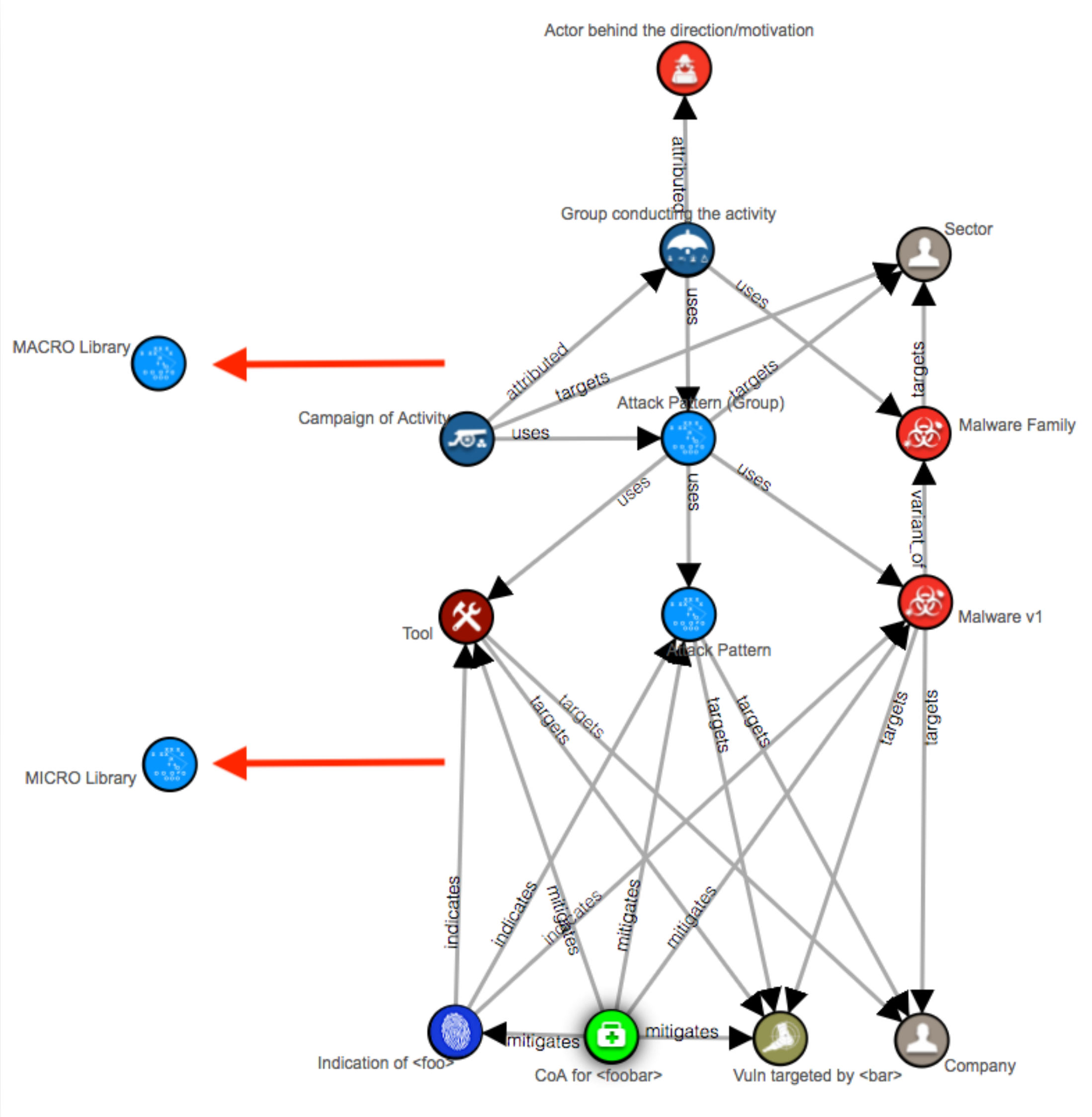
	Macro	Micro
ThreatActor	X	
IntrusionSet	X	
Campaign	X	
AttackPattern	X	X
Identity	X	X
Malware	X	X
CourseOfAction	X	X
Tool		X
Vulnerability		X
Indicator		X

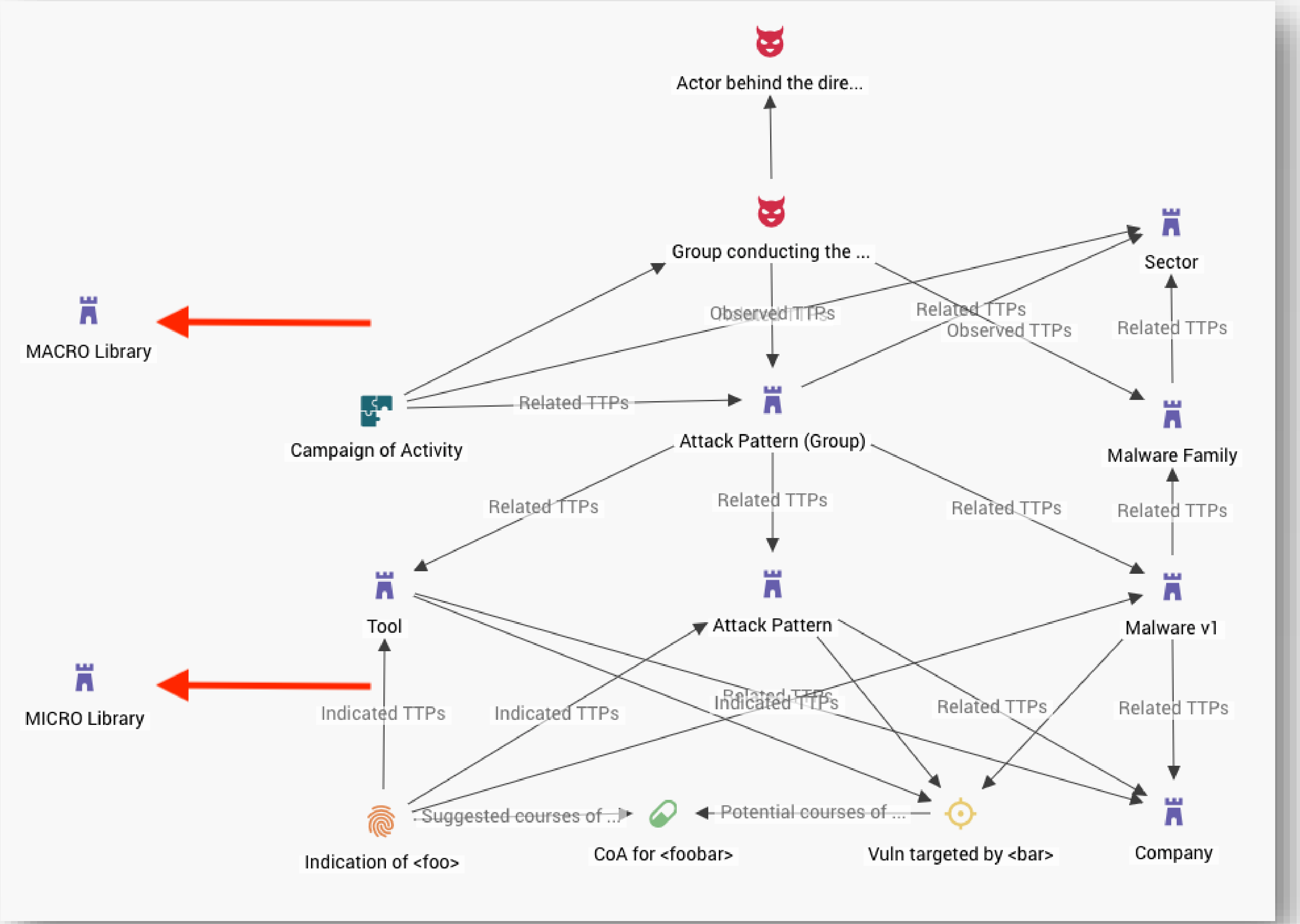
2.1	2.1 flavour	M/m	1.2	1.2 flavour
ThreatActor	☺	M	ThreatActor	Motivations, political tendencies, logistical capabilities
IntrusionSet	☺	M	ThreatActor	Hacker group, hands-on-keyboard, technical capabilities
Campaign	☺	M	Campaign	☺
AttackPattern	<directionality of relationship>	M	TTP	Characteristic ‘Attack Pattern’, top level grouping for complex combinations of other TTPs
AttackPattern	<directionality of relationship>	m	TTP	Characteristic ‘Attack Pattern’, specific TTP
Identity	identity-class: ‘sector’, etc	M	TTP	Characteristic ‘Victim Targeting’, sector/grouping level
Identity	identity-class: ‘organisation’, etc	m	TTP	Characteristic ‘Victim Targeting’, organisation/individual level
Malware	is_family: true	M	TTP	Characteristic ‘Behavior/Malware’, family-level
Malware	is_family: false	m	TTP	Characteristic ‘Behavior/Malware’, variant-level
CourseOfAction	???	M	CourseOfAction	???
CourseOfAction	???	m	CourseOfAction	???
Tool	☺	m	TTP	Characteristic ‘Tool’
Vulnerability	☺	m	ExploitTarget	:S
Indicator	☺	m	Indicator	Maintain pattern-style logic (more work here)

LIBRARY OBJECTS

- To establish a common language
- Identify functional overlaps
- Automate cross-correlation
- Implementation:
  - _to_ library object (versioning and supports 'uses' in 2.x)
  - Search before create-new!
  - Use existing standards
  - https://github.com/mitre/cti




Actor behind the direction/motivation
attributed
Group conducting the activity
Sector
uses
uses
MACRO Library
attributed
targets
targets
targets
Campaign of Activity
uses
Attack Pattern (Group)
Malware Family
uses
uses
uses
variant_of
Tool
Attack Pattern
Malware v1
targets
targets
targets
targets
targets
targets
MICRO Library
indicates
indicates
mitigates
indicates
mitigates
mitigates
mitigates
mitigates
Indication of <foo>
CoA for <foobar>
Vuln targeted by <bar>
Company

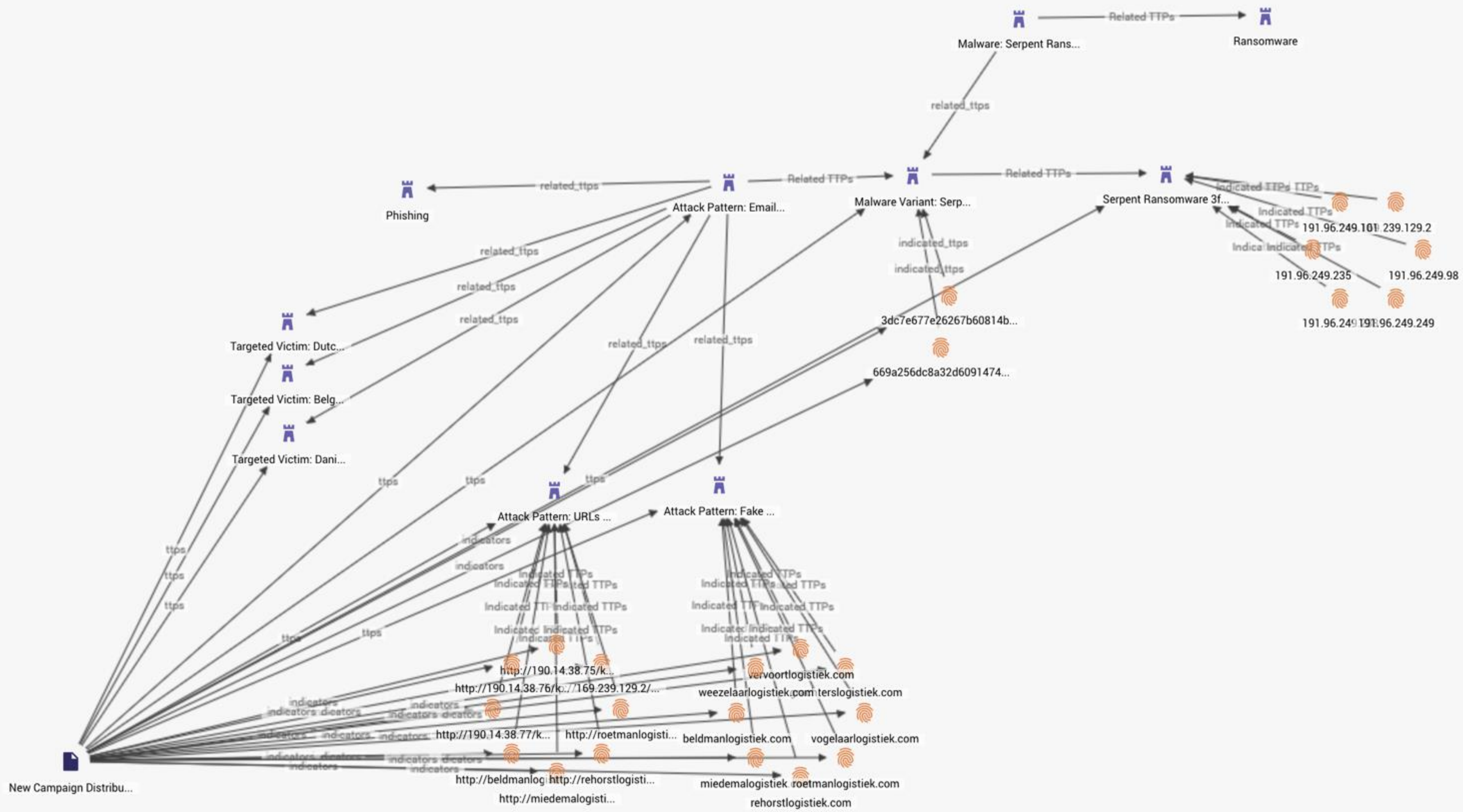

Actor behind the dire...
Group conducting the ...
Sector
MACRO Library
Observed TTPs
Related TTPs
Observed TTPs
Related TTPs
Campaign of Activity
Related TTPs
Attack Pattern (Group)
Malware Family
Related TTPs
Related TTPs
Related TTPs
Related TTPs
Tool
Attack Pattern
Malware v1
MICRO Library
Indicated TTPs
Indicated TTPs
Related TTPs
Indicated TTPs
Related TTPs
Related TTPs
Indication of <foo>
Suggested courses of ...
CoA for <foobar>
Potential courses of ...
Vuln targeted by <bar>
Company

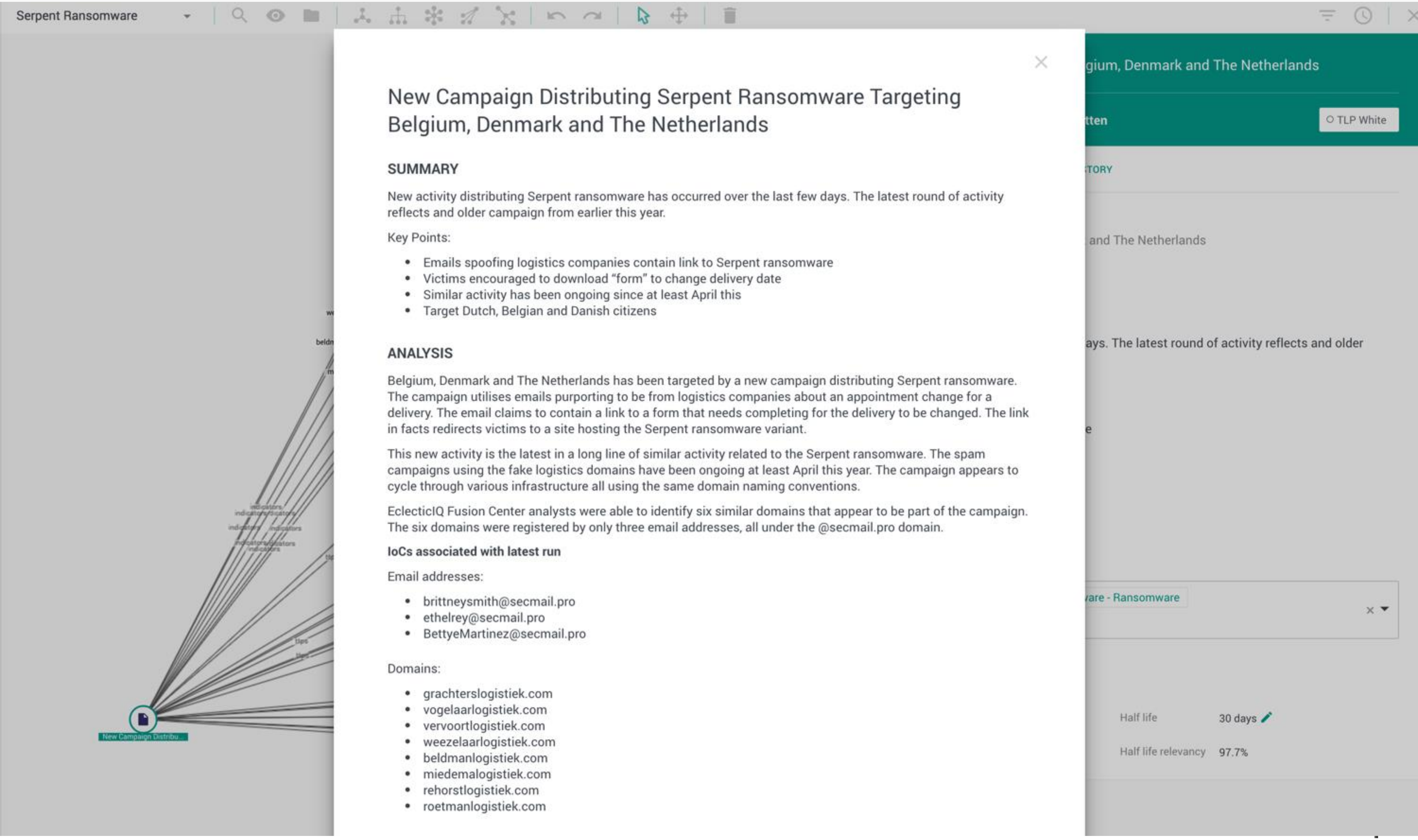
THE PRINCIPLES

- We, the under writ, do hereby agree to:
  - Not create relationships outside of this data model – if we need to this should be a BIG DEAL! Discussed and accepted/rejected
  - Not create orphaned entities (or at least review them periodically)
  - Use AttackPatterns as a pivot point between Micro and Macro data
  - By default: Macro→Macro, Micro→Micro
  - Build libraries of 'library objects' – preferably from existing libraries
  - Use 'library' objects as terminators in logic paths
  - Make a big deal out of creating a new 'library' object

- Most importantly:
  - Only create objective entities
  - Verify that our logic is independently retraceable
  - Both the model and the data must be extensible

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS


Malware: Serpent Rans...
Related TTPs
Ransomware
related_ttps
Phishing
Attack Pattern: Email...
Malware Variant: Serp...
Serpent Ransomware 3f...
Indicated TTPs
191.96.249.101
239.129.2
191.96.249.235
191.96.249.98
191.96.249
191.96.249.249
indicated_ttps
3dc7e677e26267b60814b...
669a256dc8a32d6091474...
Targeted Victim: Dutc...
Targeted Victim: Belg...
Targeted Victim: Dani...
ttps
Attack Pattern: URLs ...
Attack Pattern: Fake ...
indicators
http://190.14.38.75/k...
http://190.14.38.76/k...
//169.239.129.2/...
vervoortlogistiek.com
weezelaarlogistiek.com
terslogistiek.com
http://190.14.38.77/k...
http://roetmanlogisti...
beldmanlogistiek.com
vogelaarlogistiek.com
http://beldmanlog
http://rehorstlogisti...
http://miedemalogisti...
miedemalogistiek
roetmanlogistiek.com
rehorstlogistiek.com
New Campaign Distribu...



New Campaign Distributing Serpent Ransomware Targeting Belgium, Denmark and The Netherlands

SUMMARY

New activity distributing Serpent ransomware has occurred over the last few days. The latest round of activity reflects and older campaign from earlier this year.

Key Points:

- Emails spoofing logistics companies contain link to Serpent ransomware
- Victims encouraged to download “form” to change delivery date
- Similar activity has been ongoing since at least April this
- Target Dutch, Belgian and Danish citizens

ANALYSIS

Belgium, Denmark and The Netherlands has been targeted by a new campaign distributing Serpent ransomware. The campaign utilises emails purporting to be from logistics companies about an appointment change for a delivery. The email claims to contain a link to a form that needs completing for the delivery to be changed. The link in facts redirects victims to a site hosting the Serpent ransomware variant.

This new activity is the latest in a long line of similar activity related to the Serpent ransomware. The spam campaigns using the fake logistics domains have been ongoing at least April this year. The campaign appears to cycle through various infrastructure all using the same domain naming conventions.

EclecticIQ Fusion Center analysts were able to identify six similar domains that appear to be part of the campaign. The six domains were registered by only three email addresses, all under the @secmail.pro domain.

IoCs associated with latest run

Email addresses:

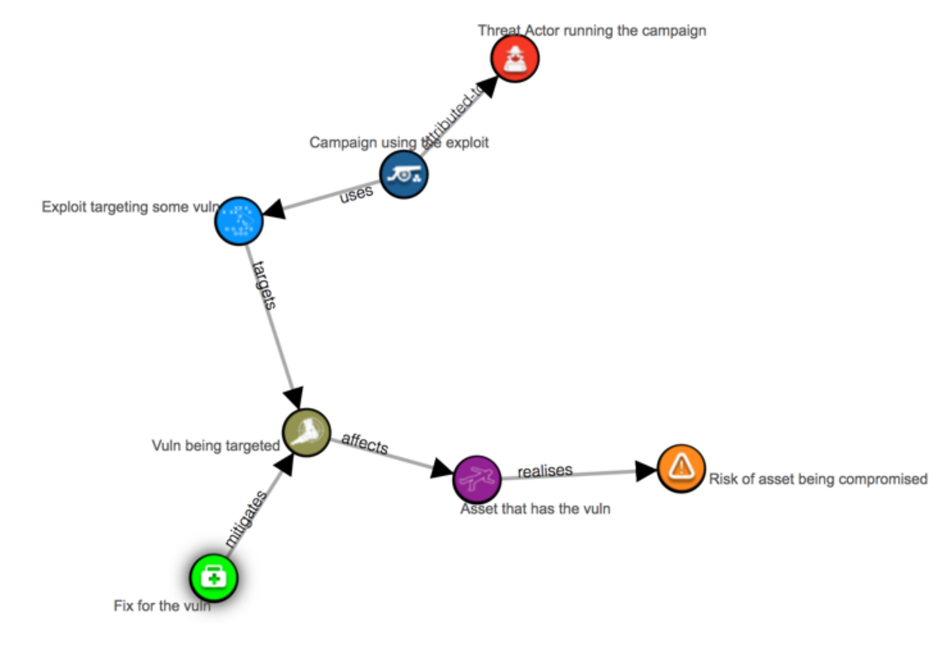
- brittneysmith@secmail.pro
- ethelrey@secmail.pro
- BettyeMartinez@secmail.pro

Domains:

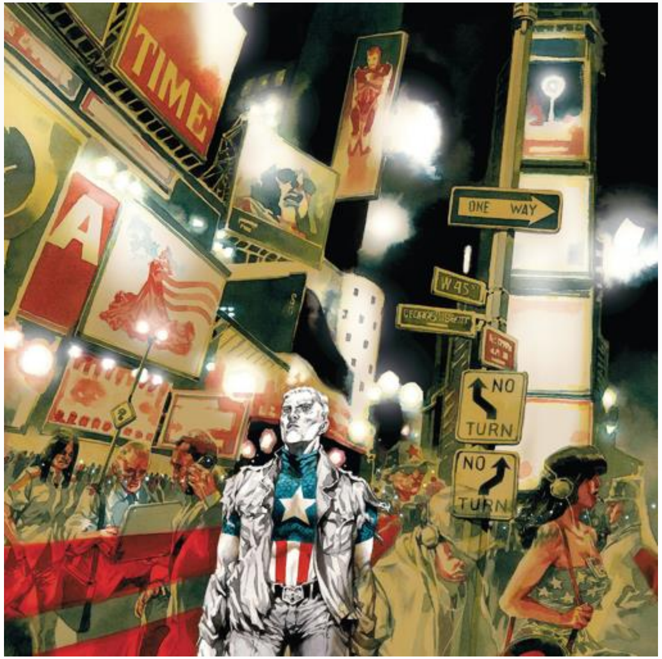
- grachterslogistiek.com
- vogelaarlogistiek.com
- vervoortlogistiek.com
- weezelaarlogistiek.com
- beldmanlogistiek.com
- miedemalogistiek.com
- rehorstlogistiek.com
- roetmanlogistiek.com

IDEAS FOR THE FUTURE

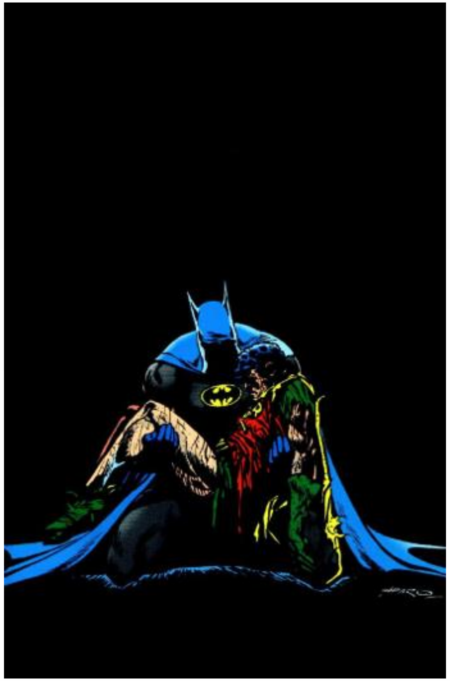
- Would love some feedback!
- Profile for use in stix-elevator
- stix-dropper? –DONE
  - https://github.com/oasis-open/cti-stix-slider
- Also this? -----------------------------→


Threat Actor running the campaign
attributed-to
Campaign using the exploit
uses
Exploit targeting some vuln
targets
Vuln being targeted
affects
realises
Risk of asset being compromised
Asset that has the vuln
mitigates
Fix for the vuln

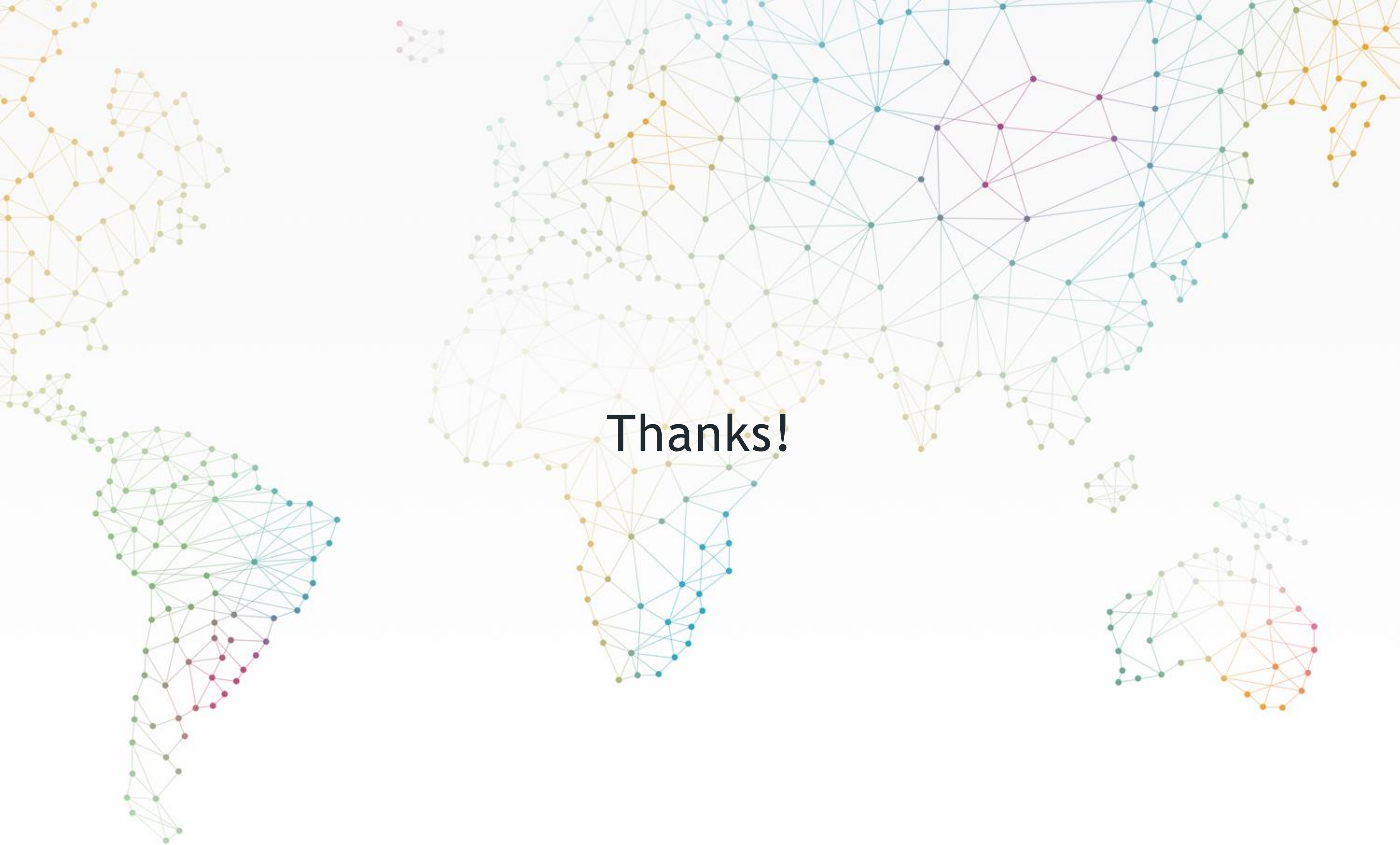
CHOOSE YOUR PATH…



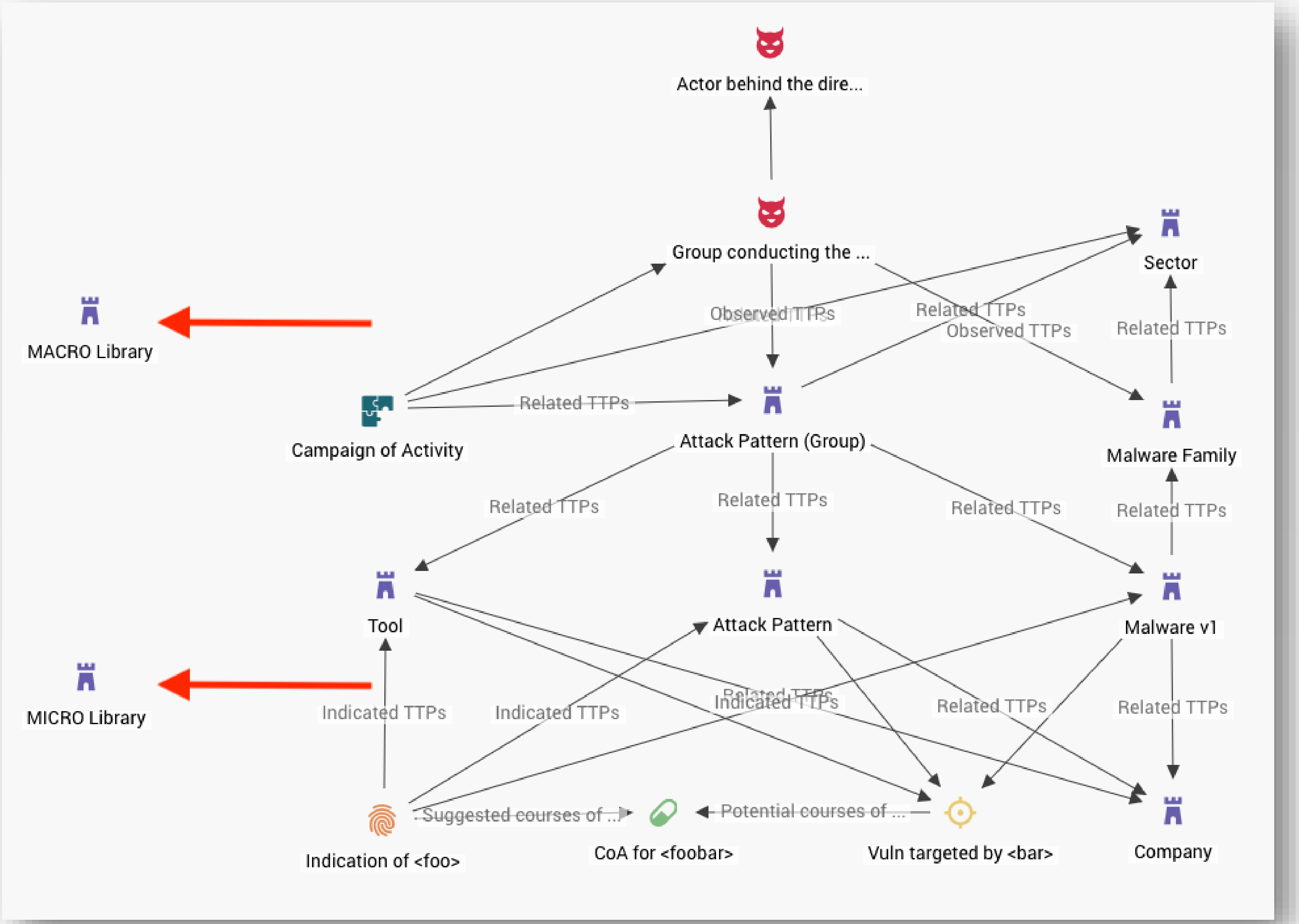
Standard: out of time



Jason Todd



Thanks!


Actor behind the dire...
Group conducting the ...
Sector
MACRO Library
Observed TTPs
Related TTPs
Observed TTPs
Related TTPs
Campaign of Activity
Related TTPs
Attack Pattern (Group)
Malware Family
Related TTPs
Related TTPs
Related TTPs
Related TTPs
Tool
Attack Pattern
Malware v1
MICRO Library
Indicated TTPs
Indicated TTPs
Related TTPs
Indicated TTPs
Related TTPs
Related TTPs
Suggested courses of ...
Potential courses of ...
Indication of <foo>
CoA for <foobar>
Vuln targeted by <bar>
Company