RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: AIR-W01

Evaluating Indicators As Composite Objects

Joe Slowik

Threat Intelligence & Detections Lead
Gigamon Applied Threat Research
@jfslowik

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

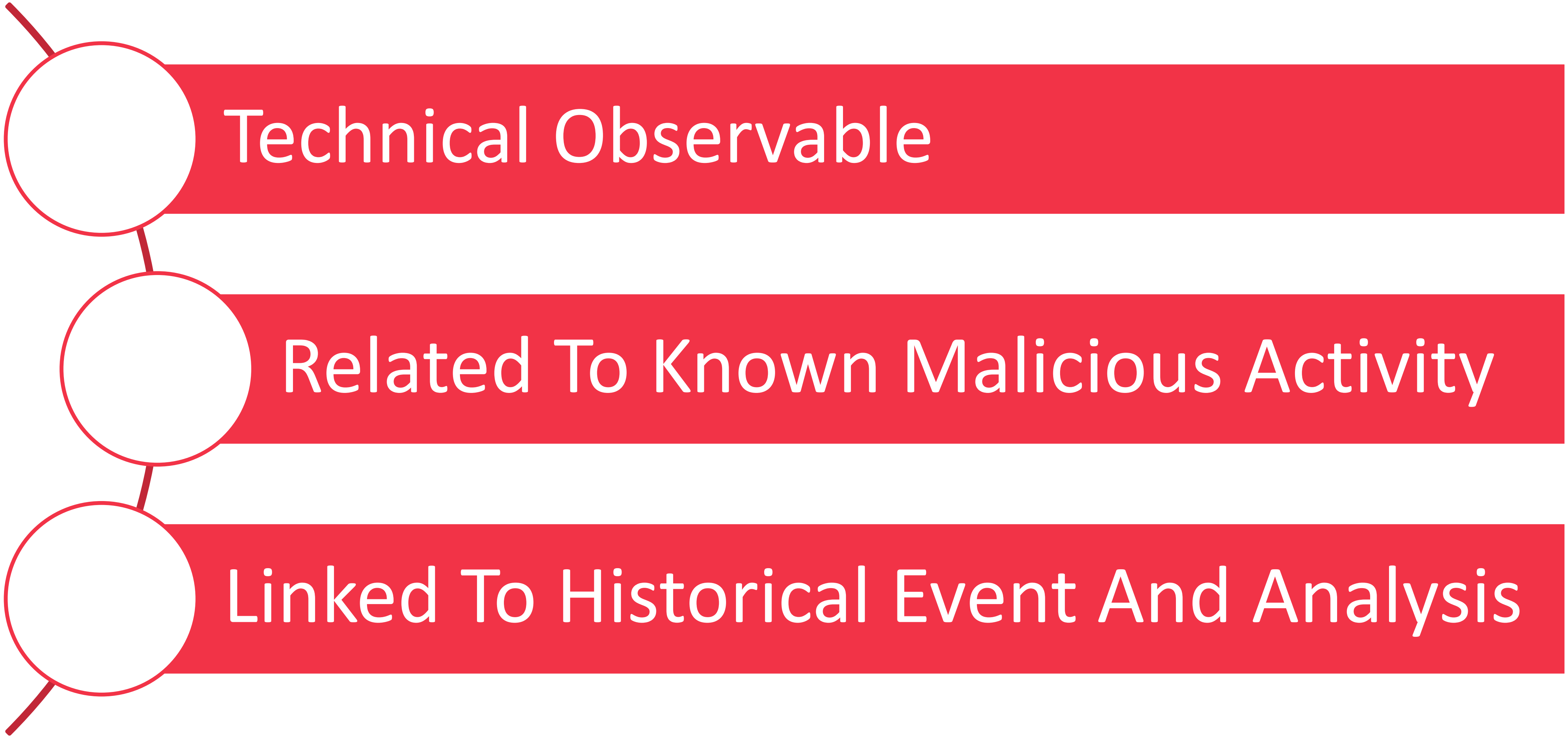
Hello!

- Current:
  - Gigamon Threat Intelligence & Detections Development Lead
  - Paralus CTI and ICS Education
- Previously:
  - DomainTools Security Research
  - Dragos ICS Threat Research and Analysis
  - Los Alamos National Laboratory Incident Response Lead
  - US Navy, “various”

Agenda

- Defining Indicators
- Indicators As Atomic Objects
- Indicators As Composite Objects
- Composites Yielding Adversary Behaviors

Indicators Of Compromise

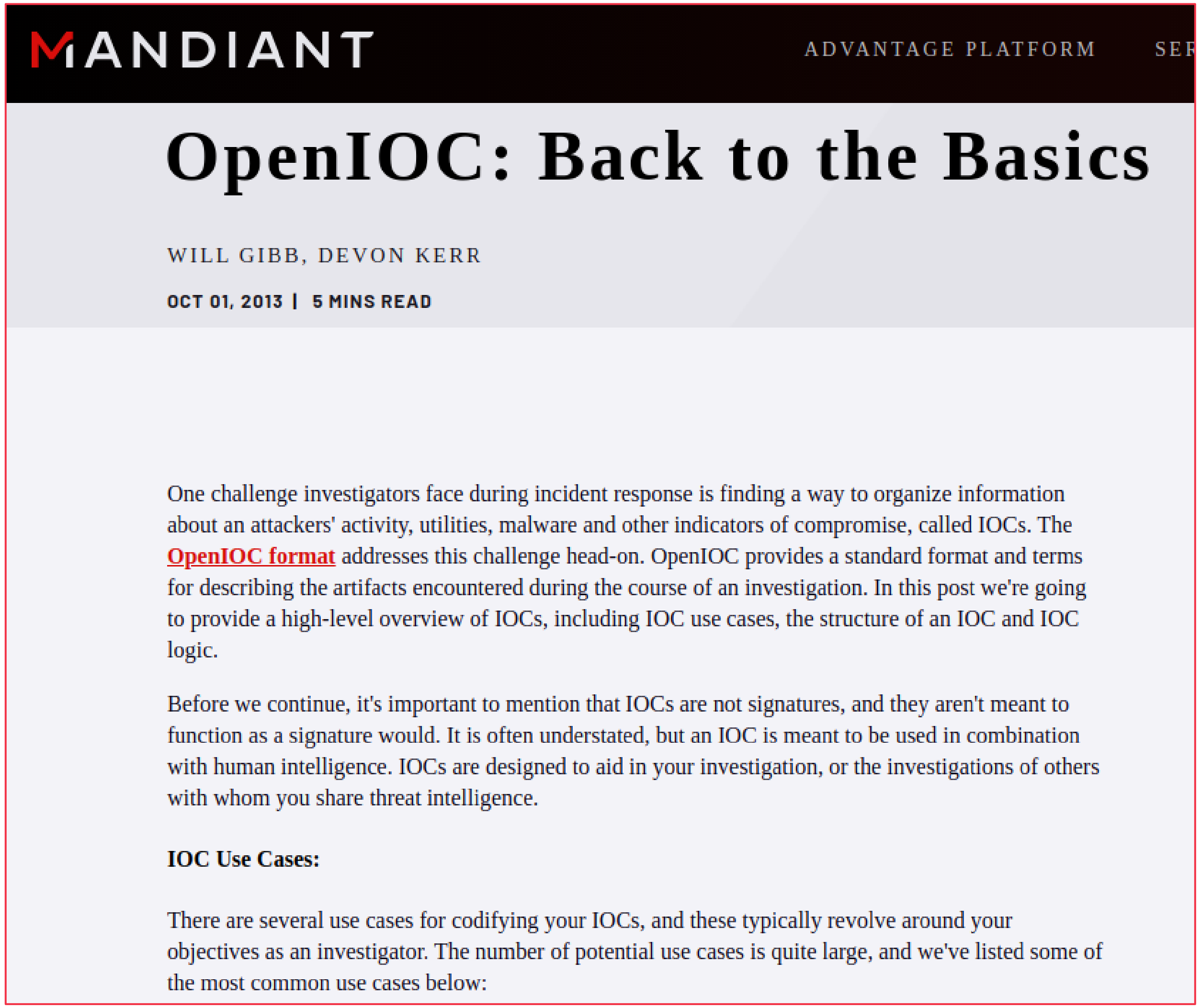


Technical Observable

Related To Known Malicious Activity

Linked To Historical Event And Analysis

Indicators Of Compromise



OpenIOC: Back to the Basics

WILL GIBB, DEVON KERR

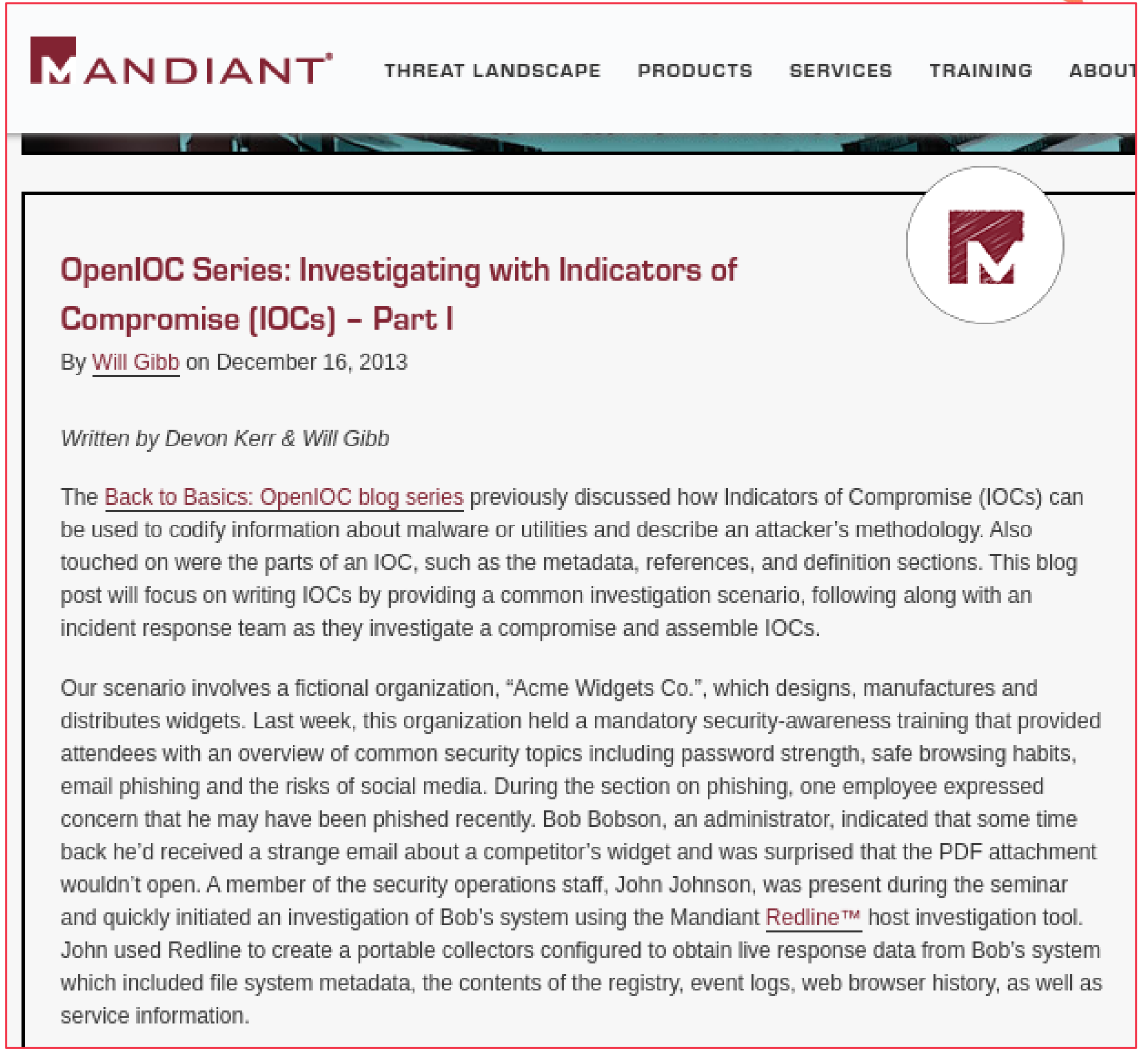
OCT 01, 2013 | 5 MINS READ

One challenge investigators face during incident response is finding a way to organize information about an attackers' activity, utilities, malware and other indicators of compromise, called IOCs. The OpenIOC format addresses this challenge head-on. OpenIOC provides a standard format and terms for describing the artifacts encountered during the course of an investigation. In this post we're going to provide a high-level overview of IOCs, including IOC use cases, the structure of an IOC and IOC logic.

Before we continue, it's important to mention that IOCs are not signatures, and they aren't meant to function as a signature would. It is often understated, but an IOC is meant to be used in combination with human intelligence. IOCs are designed to aid in your investigation, or the investigations of others with whom you share threat intelligence.

IOC Use Cases:

There are several use cases for codifying your IOCs, and these typically revolve around your objectives as an investigator. The number of potential use cases is quite large, and we've listed some of the most common use cases below:



OpenIOC Series: Investigating with Indicators of Compromise (IOCs) – Part I

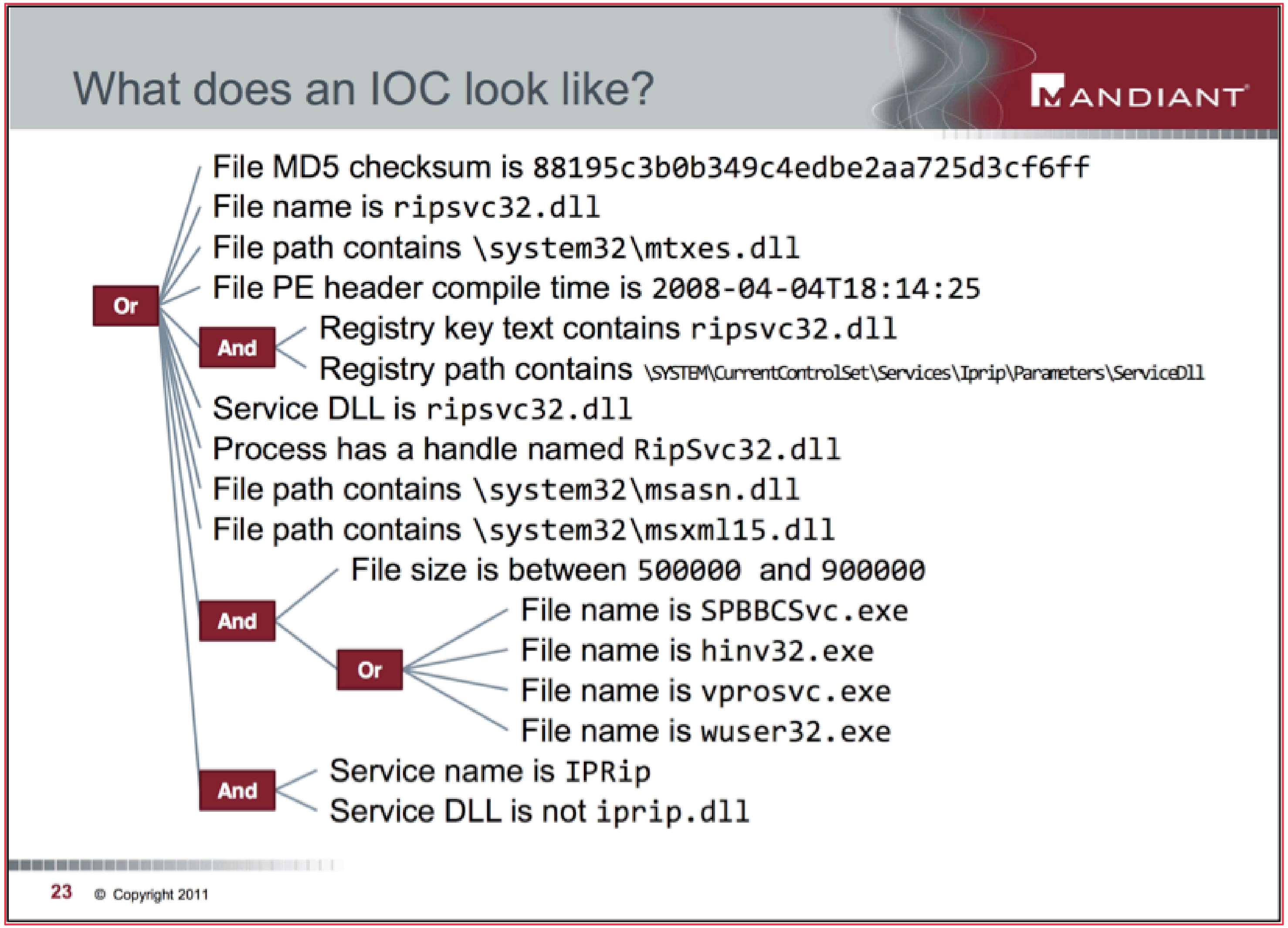
By Will Gibb on December 16, 2013

Written by Devon Kerr & Will Gibb

The Back to Basics: OpenIOC blog series previously discussed how Indicators of Compromise (IOCs) can be used to codify information about malware or utilities and describe an attacker's methodology. Also touched on were the parts of an IOC, such as the metadata, references, and definition sections. This blog post will focus on writing IOCs by providing a common investigation scenario, following along with an incident response team as they investigate a compromise and assemble IOCs.

Our scenario involves a fictional organization, "Acme Widgets Co.", which designs, manufactures and distributes widgets. Last week, this organization held a mandatory security-awareness training that provided attendees with an overview of common security topics including password strength, safe browsing habits, email phishing and the risks of social media. During the section on phishing, one employee expressed concern that he may have been phished recently. Bob Bobson, an administrator, indicated that some time back he'd received a strange email about a competitor's widget and was surprised that the PDF attachment wouldn't open. A member of the security operations staff, John Johnson, was present during the seminar and quickly initiated an investigation of Bob's system using the Mandiant Redline™ host investigation tool. John used Redline to create a portable collectors configured to obtain live response data from Bob's system which included file system metadata, the contents of the registry, event logs, web browser history, as well as service information.

Indicators Of Compromise



What does an IOC look like?

MANDIANT

- Or
  - File MD5 checksum is 88195c3b0b349c4edbe2aa725d3cf6ff
  - File name is ripsvc32.dll
  - File path contains \system32\mtxes.dll
  - File PE header compile time is 2008-04-04T18:14:25
  - And
    - Registry key text contains ripsvc32.dll
    - Registry path contains \SYSTEM\CurrentControlSet\Services\Iprip\Parameters\ServiceDll
  - Service DLL is ripsvc32.dll
  - Process has a handle named RipSvc32.dll
  - File path contains \system32\msasn.dll
  - File path contains \system32\msxml15.dll
  - And
    - File size is between 500000 and 900000
    - Or
      - File name is SPBBCSvc.exe
      - File name is hinv32.exe
      - File name is vprosvc.exe
      - File name is wuser32.exe
  - And
    - Service name is IPRip
    - Service DLL is not iprip.dll

23 © Copyright 2011

https://media.threatpost.com/wp-content/uploads/sites/103/2016/04/07000027/mandiant-IOC.png

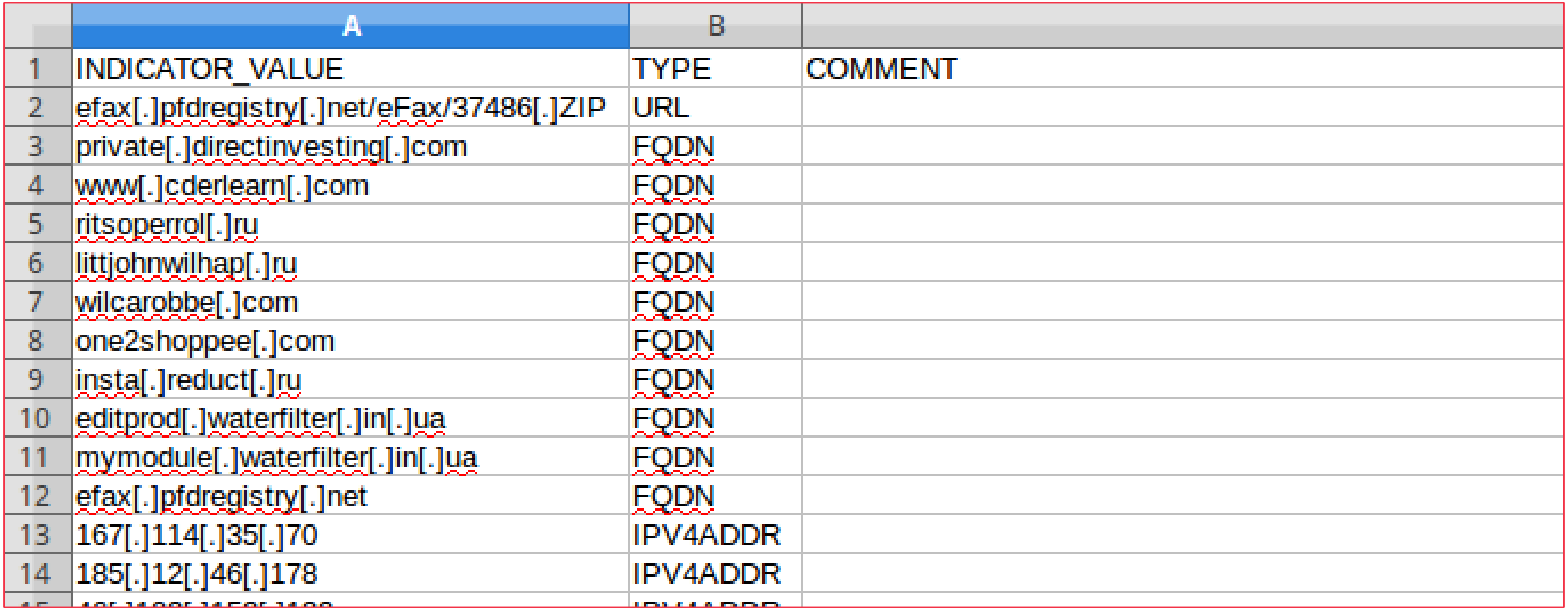
Indicators As Defined

Multiple Observations

Context Provided

Rooted In Incident Response

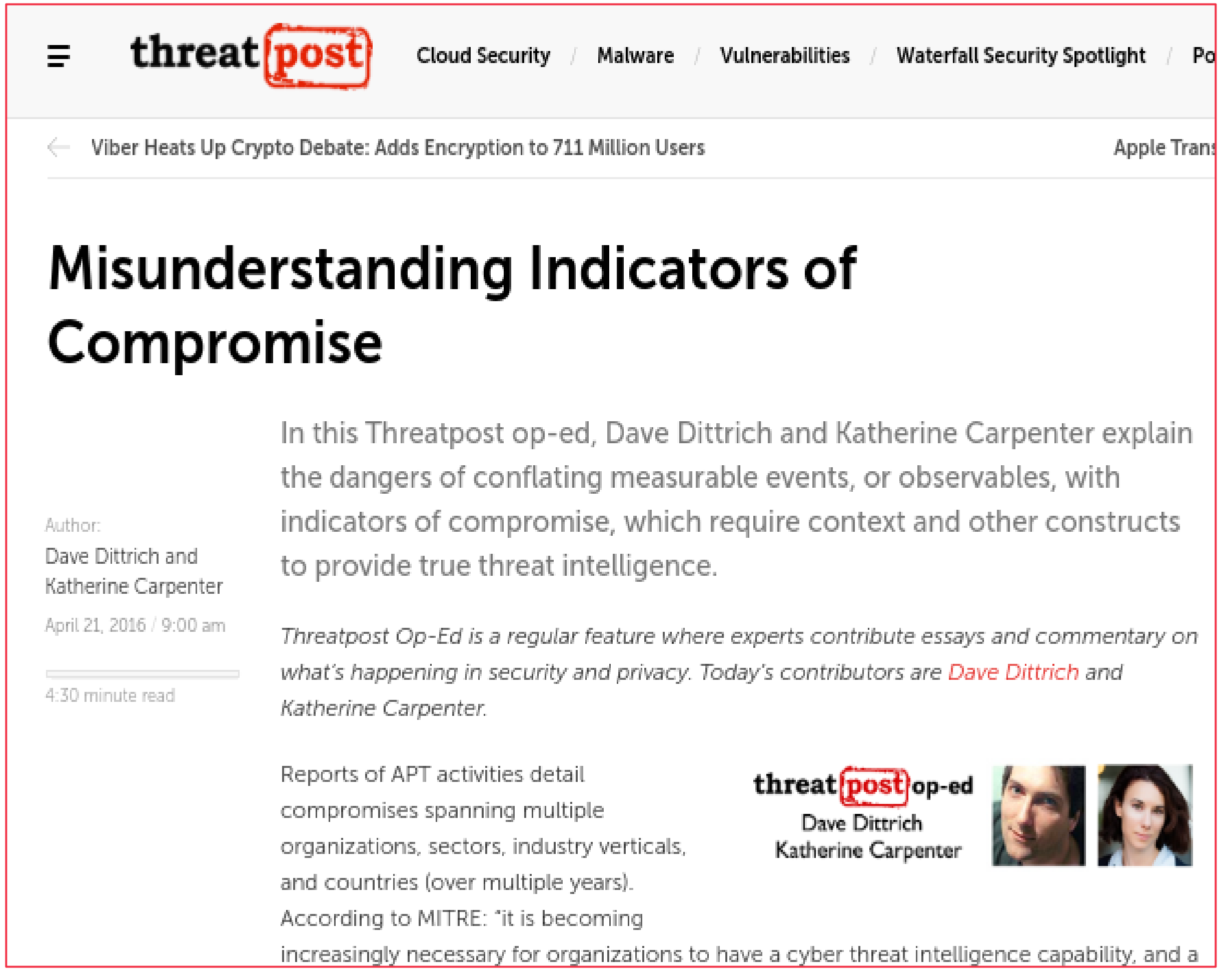
Indicators In Practice



	A	B	
1	INDICATOR_VALUE	TYPE	COMMENT
2	efax[.]pfdregistry[.]net/eFax/37486[.]ZIP	URL	
3	private[.]directinvesting[.]com	FQDN	
4	www[.]cderlearn[.]com	FQDN	
5	ritsoperrol[.]ru	FQDN	
6	littjohnwilhap[.]ru	FQDN	
7	wilcarobbe[.]com	FQDN	
8	one2shoppee[.]com	FQDN	
9	insta[.]reduct[.]ru	FQDN	
10	editprod[.]waterfilter[.]in[.]ua	FQDN	
11	mymodule[.]waterfilter[.]in[.]ua	FQDN	
12	efax[.]pfdregistry[.]net	FQDN	
13	167[.]114[.]35[.]70	IPV4ADDR	
14	185[.]12[.]46[.]178	IPV4ADDR	

https://www.us-cert.gov/sites/default/files/publications/JAR-16-20296A.csv

Debasement Of The IOC


threatpost
Cloud Security / Malware / Vulnerabilities / Waterfall Security Spotlight / Po
Viber Heats Up Crypto Debate: Adds Encryption to 711 Million Users
Apple Trans

Misunderstanding Indicators of Compromise

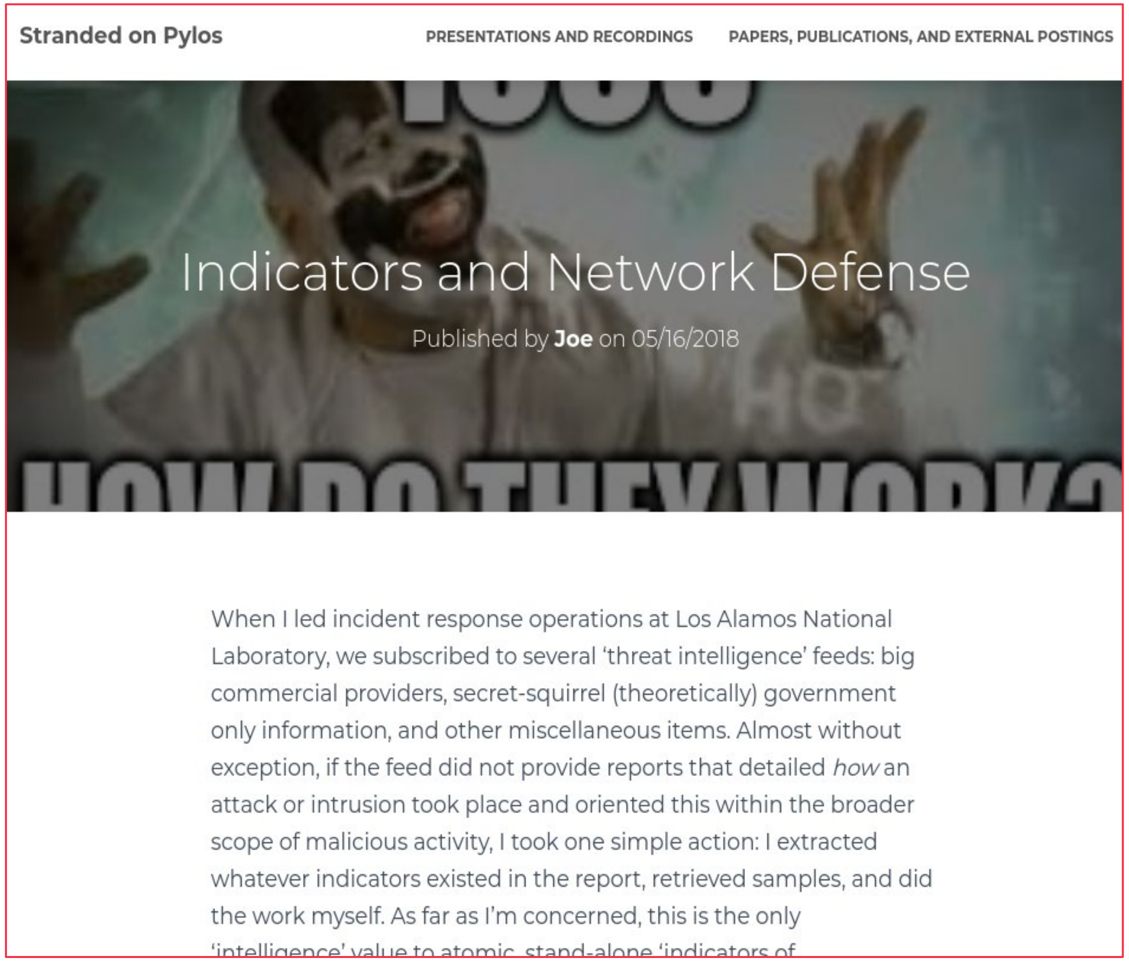
Author:
Dave Dittrich and Katherine Carpenter
April 21, 2016 / 9:00 am
4:30 minute read

In this Threatpost op-ed, Dave Dittrich and Katherine Carpenter explain the dangers of conflating measurable events, or observables, with indicators of compromise, which require context and other constructs to provide true threat intelligence.

Threatpost Op-Ed is a regular feature where experts contribute essays and commentary on what's happening in security and privacy. Today's contributors are Dave Dittrich and Katherine Carpenter.

threatpost op-ed
Dave Dittrich
Katherine Carpenter

Reports of APT activities detail compromises spanning multiple organizations, sectors, industry verticals, and countries (over multiple years). According to MITRE: "it is becoming increasingly necessary for organizations to have a cyber threat intelligence capability, and a

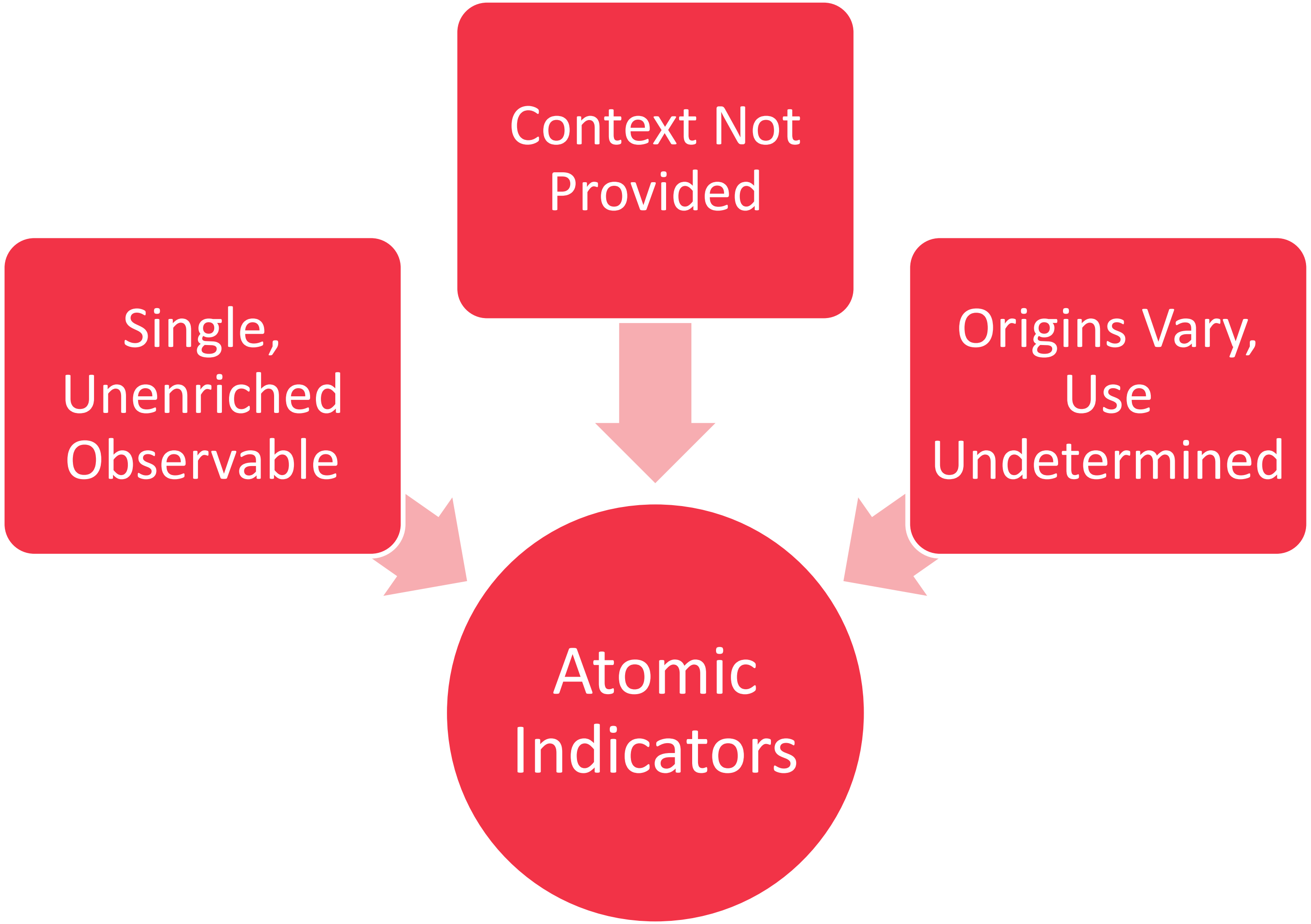

Stranded on Pylos
PRESENTATIONS AND RECORDINGS
PAPERS, PUBLICATIONS, AND EXTERNAL POSTINGS
HOW DO THEY WORK?

Indicators and Network Defense

Published by **Joe** on 05/16/2018

When I led incident response operations at Los Alamos National Laboratory, we subscribed to several 'threat intelligence' feeds: big commercial providers, secret-squirrel (theoretically) government only information, and other miscellaneous items. Almost without exception, if the feed did not provide reports that detailed *how* an attack or intrusion took place and oriented this within the broader scope of malicious activity, I took one simple action: I extracted whatever indicators existed in the report, retrieved samples, and did the work myself. As far as I'm concerned, this is the only 'intelligence' value to atomic, stand-alone 'indicators of

Indicators As Atomic Objects



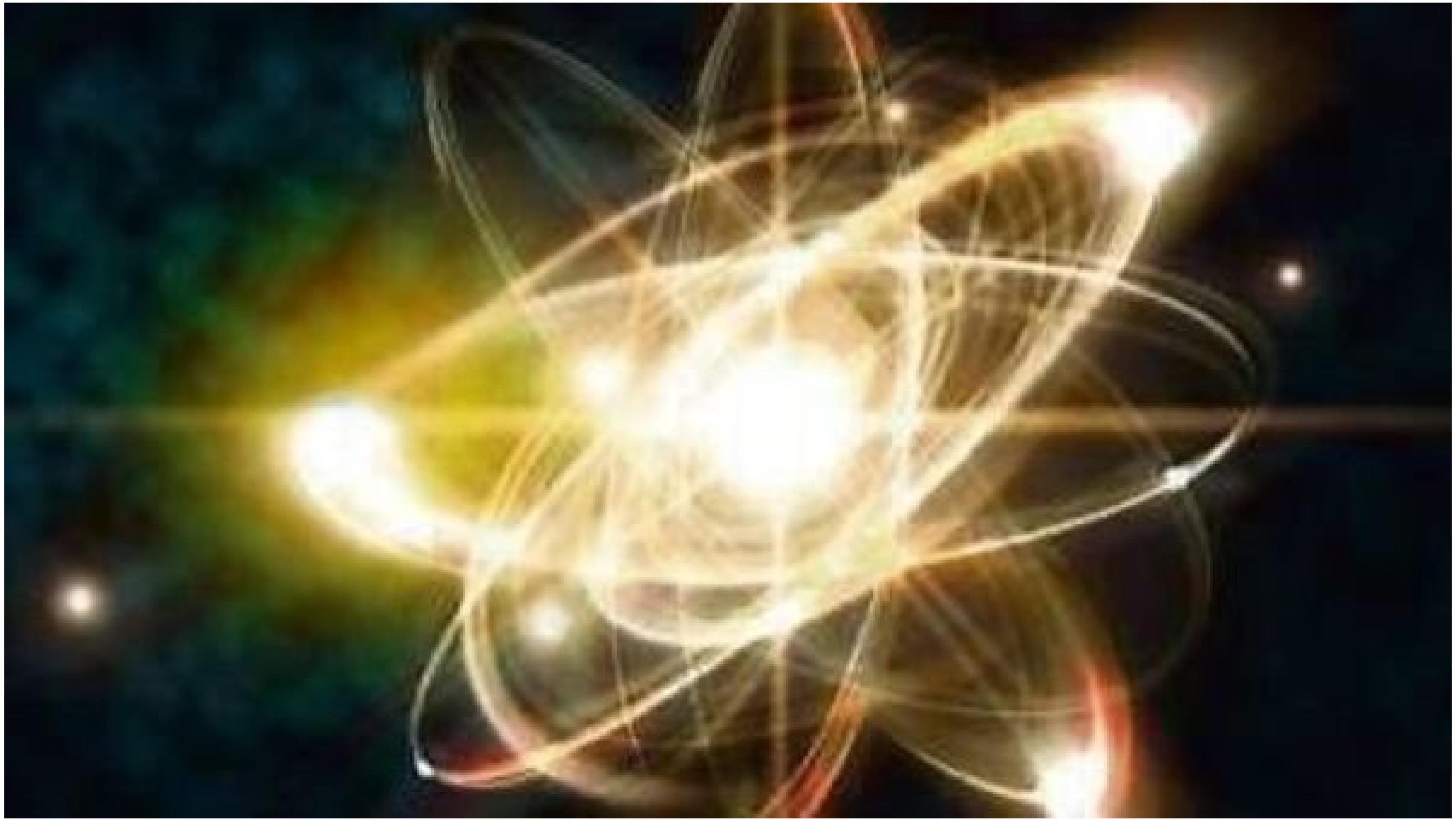
Context Not Provided

Single, Unenriched Observable

Origins Vary, Use Undetermined

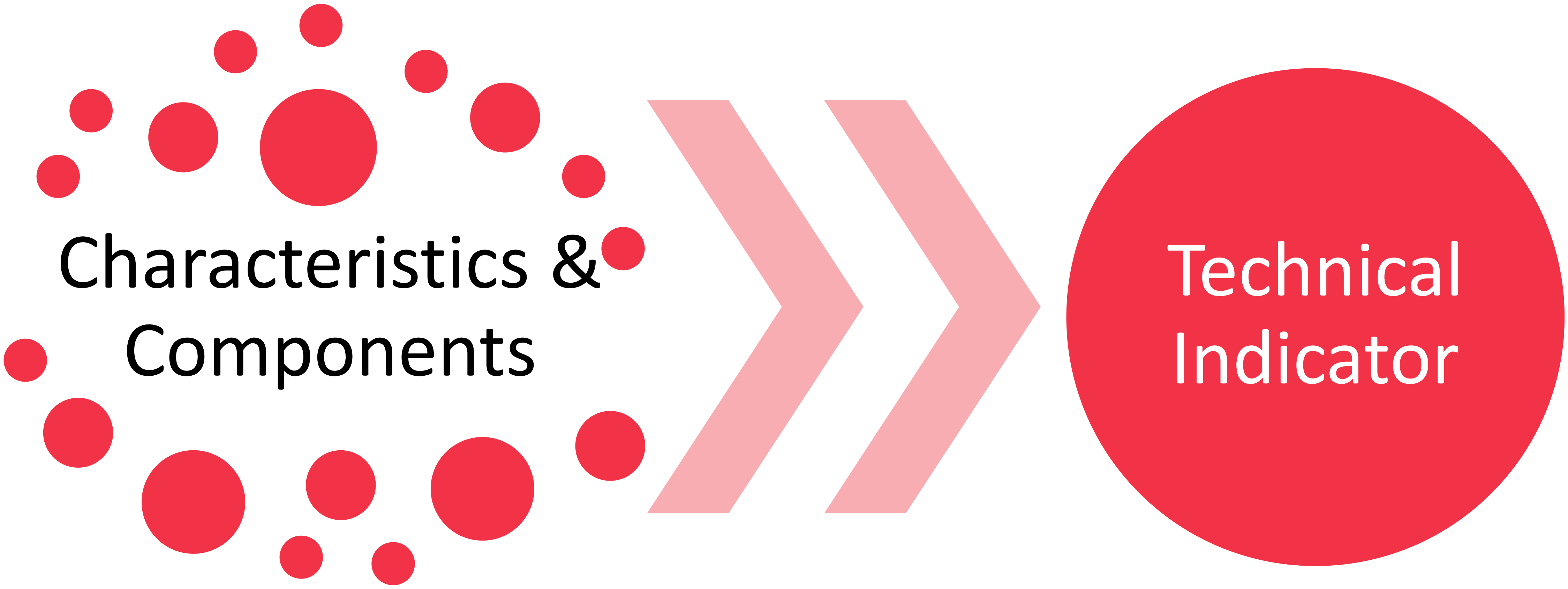
Atomic Indicators

“Splitting The Atom”



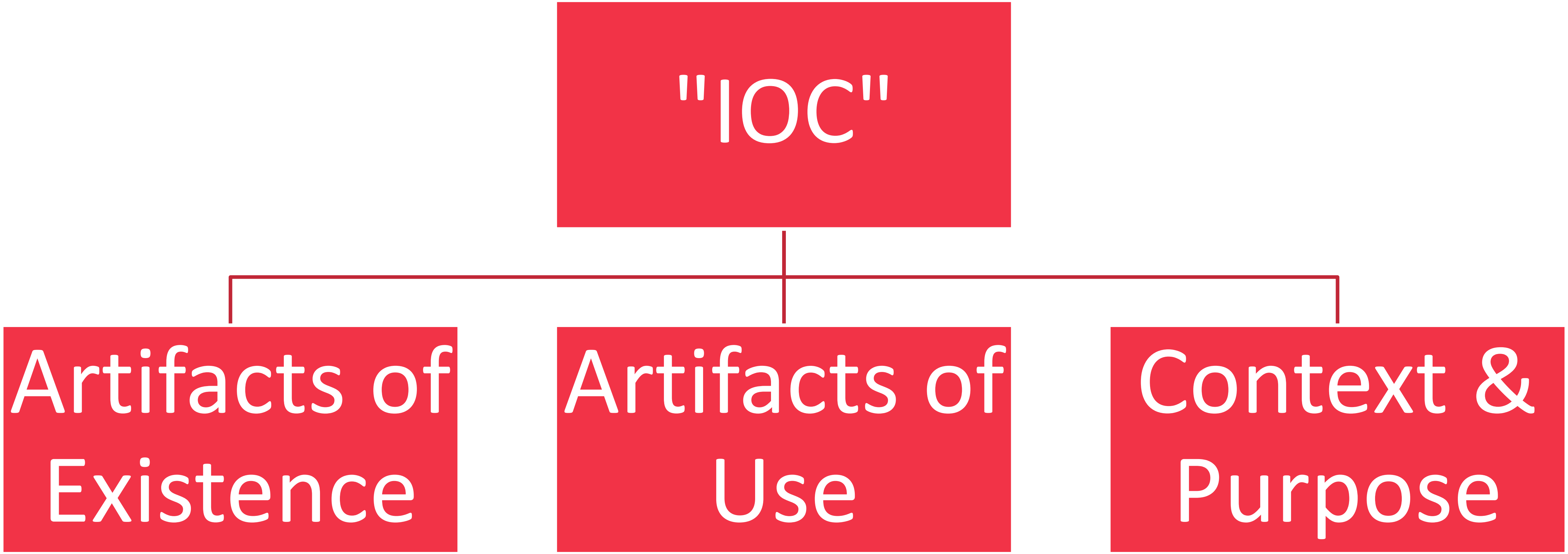
https://www.irishexaminer.com/cms_media/module_img/1961/980957_1_articlelarge_bn-901957_0b19cd2225664bfa9169b0ed90b84f61.jpg

Indicators As Natural Composites


Characteristics & Components

Technical Indicator

Identifying Subcomponents



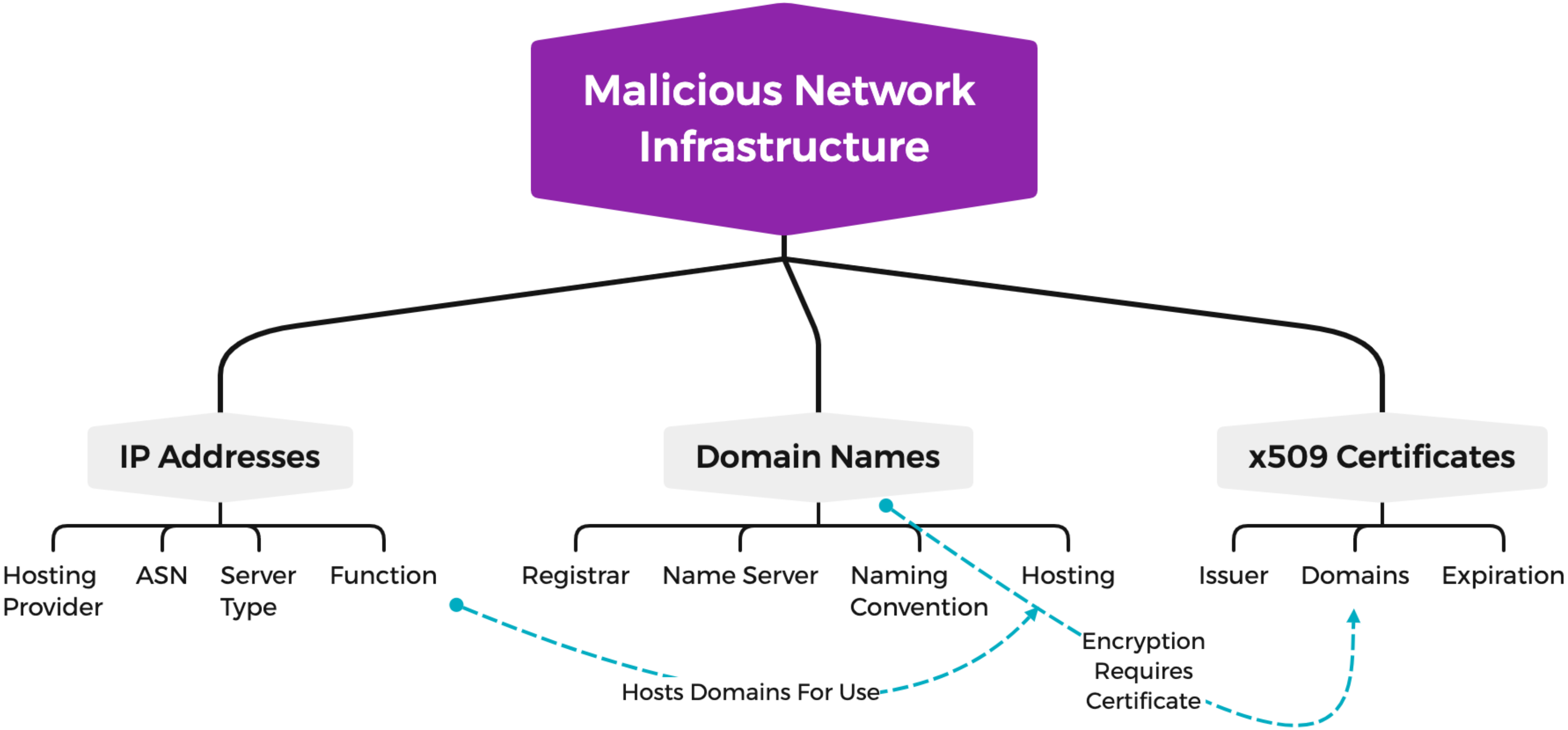
"IOC"

Artifacts of Existence

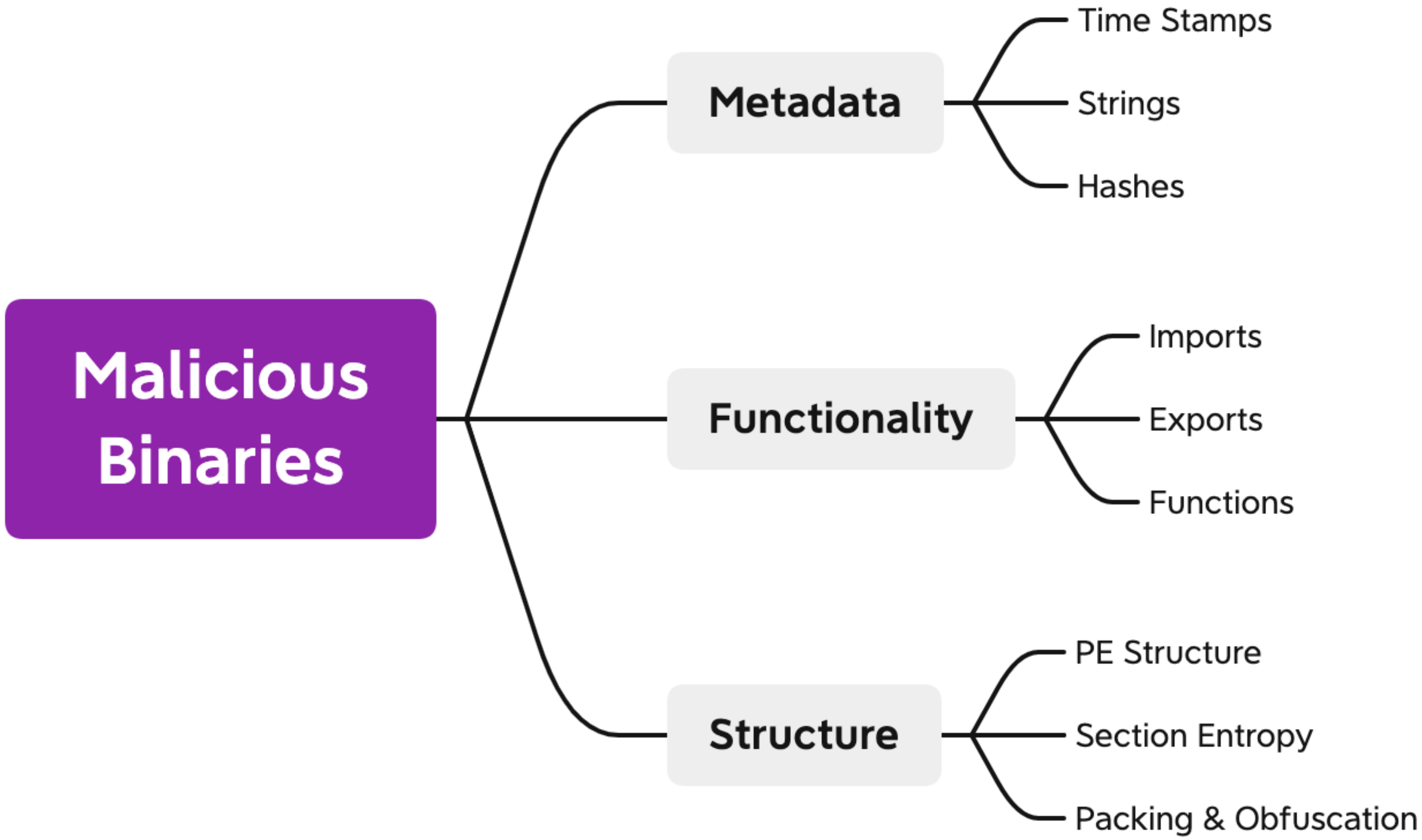
Artifacts of Use

Context & Purpose

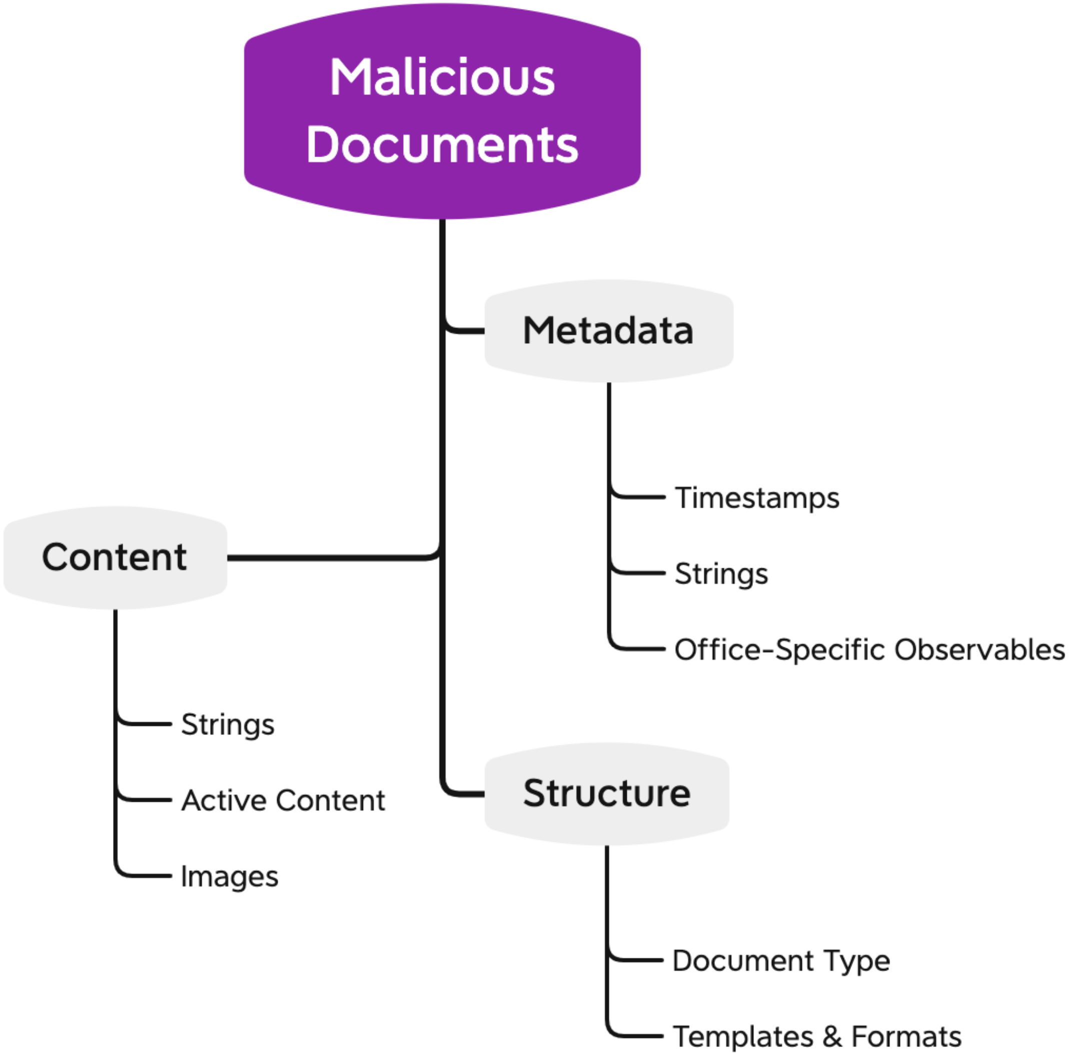
Example: Network Objects



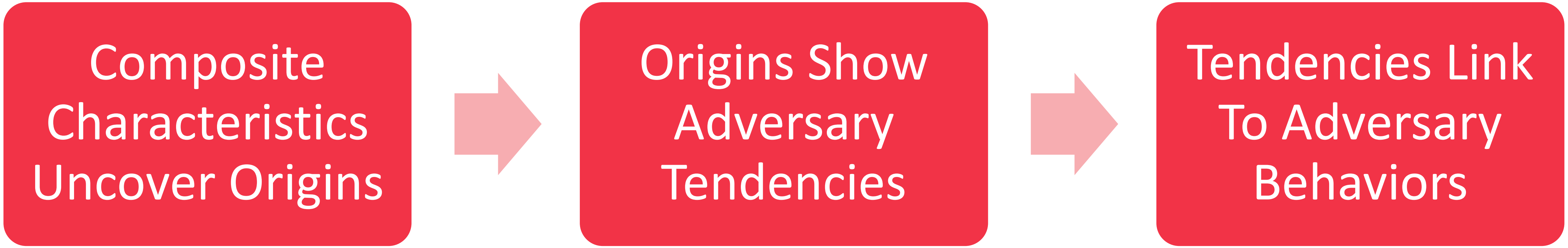
Example: PE Files



Example: Office Documents



Composite Characteristics

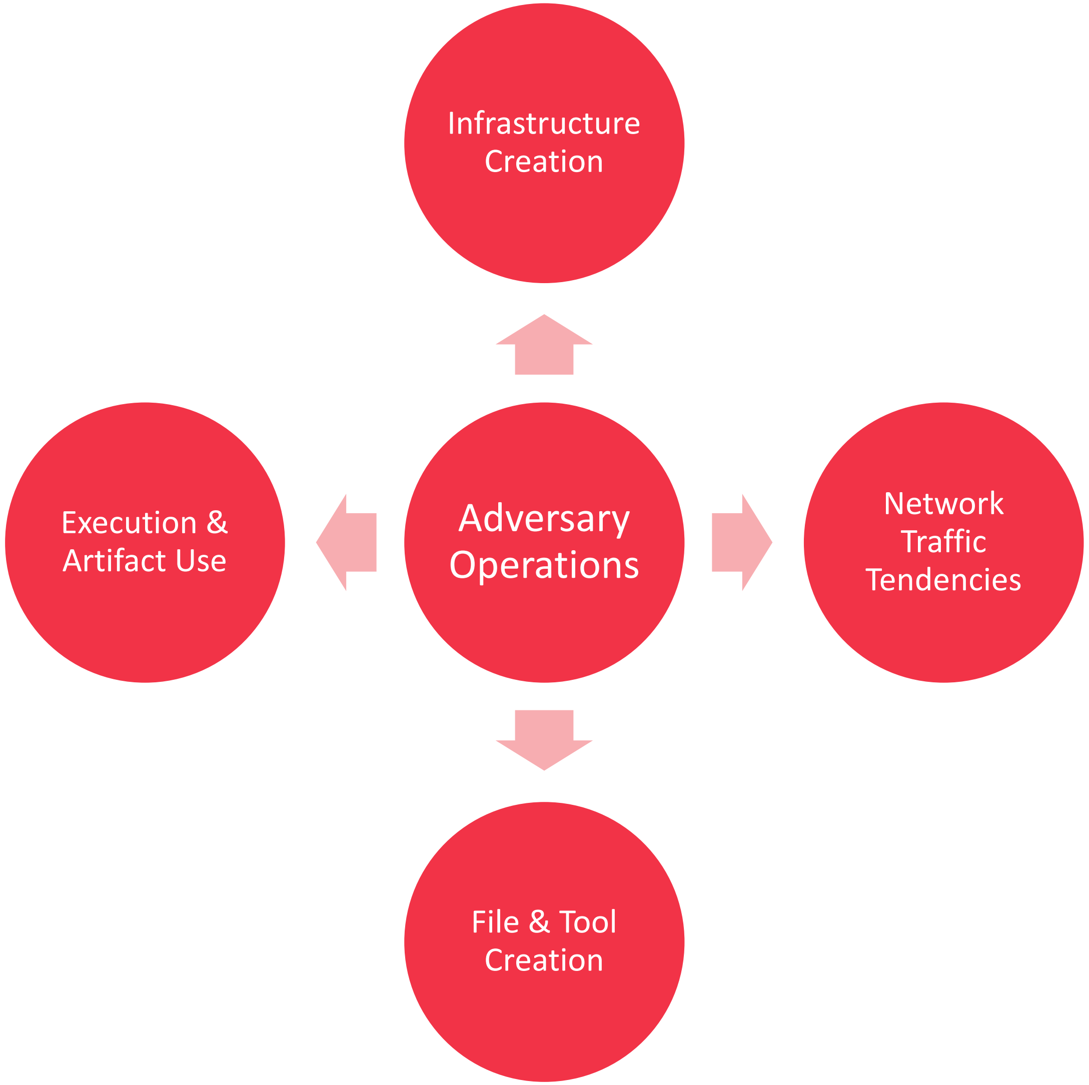


Composite Characteristics Uncover Origins

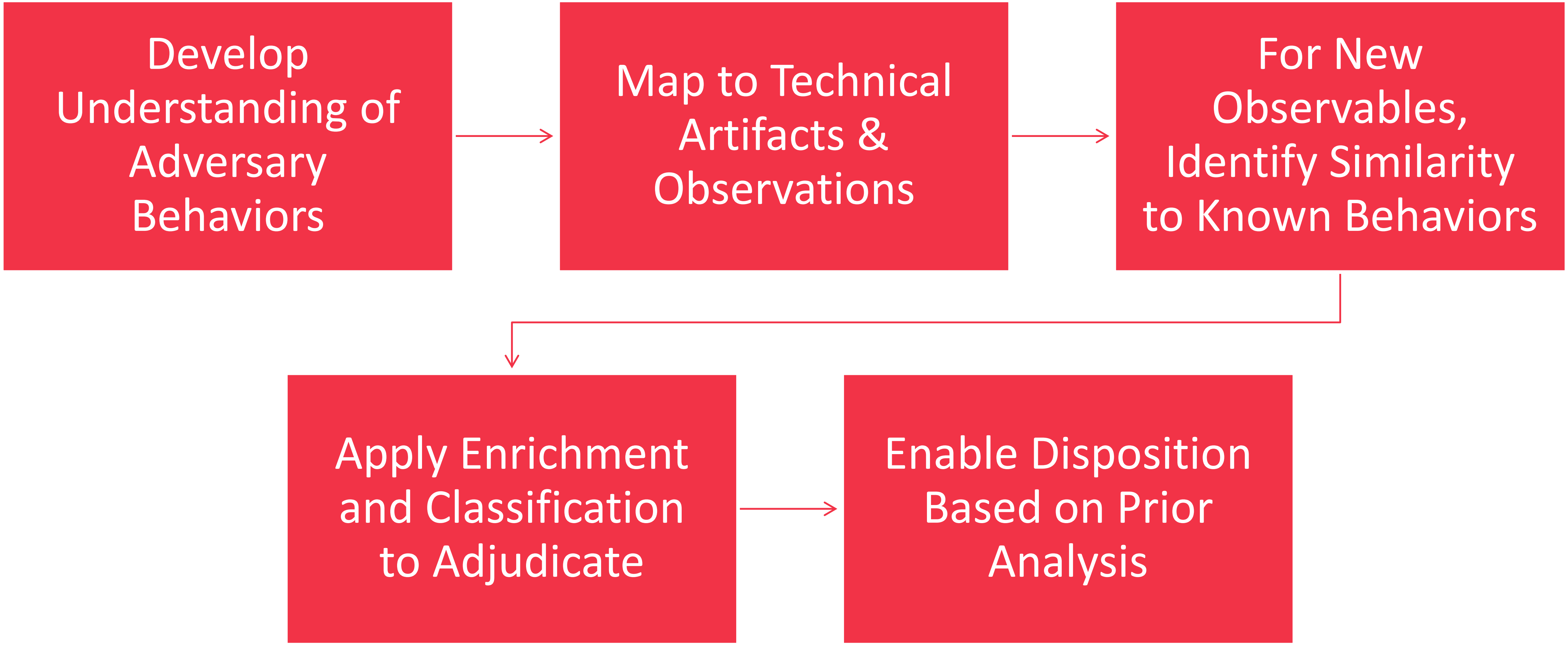
Origins Show Adversary Tendencies

Tendencies Link To Adversary Behaviors

Behavioral Identification & Pivoting



Indicator Classification



Develop Understanding of Adversary Behaviors

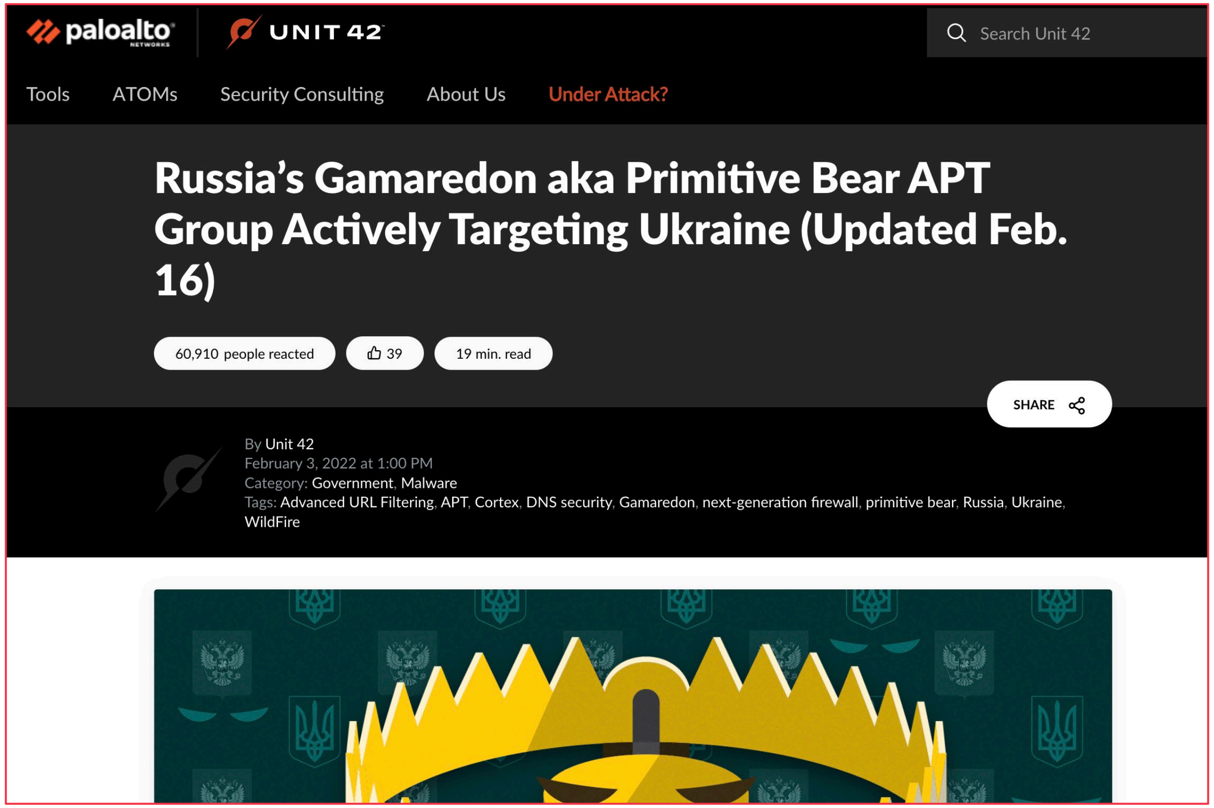
Map to Technical Artifacts & Observations

For New Observables, Identify Similarity to Known Behaviors

Apply Enrichment and Classification to Adjudicate

Enable Disposition Based on Prior Analysis

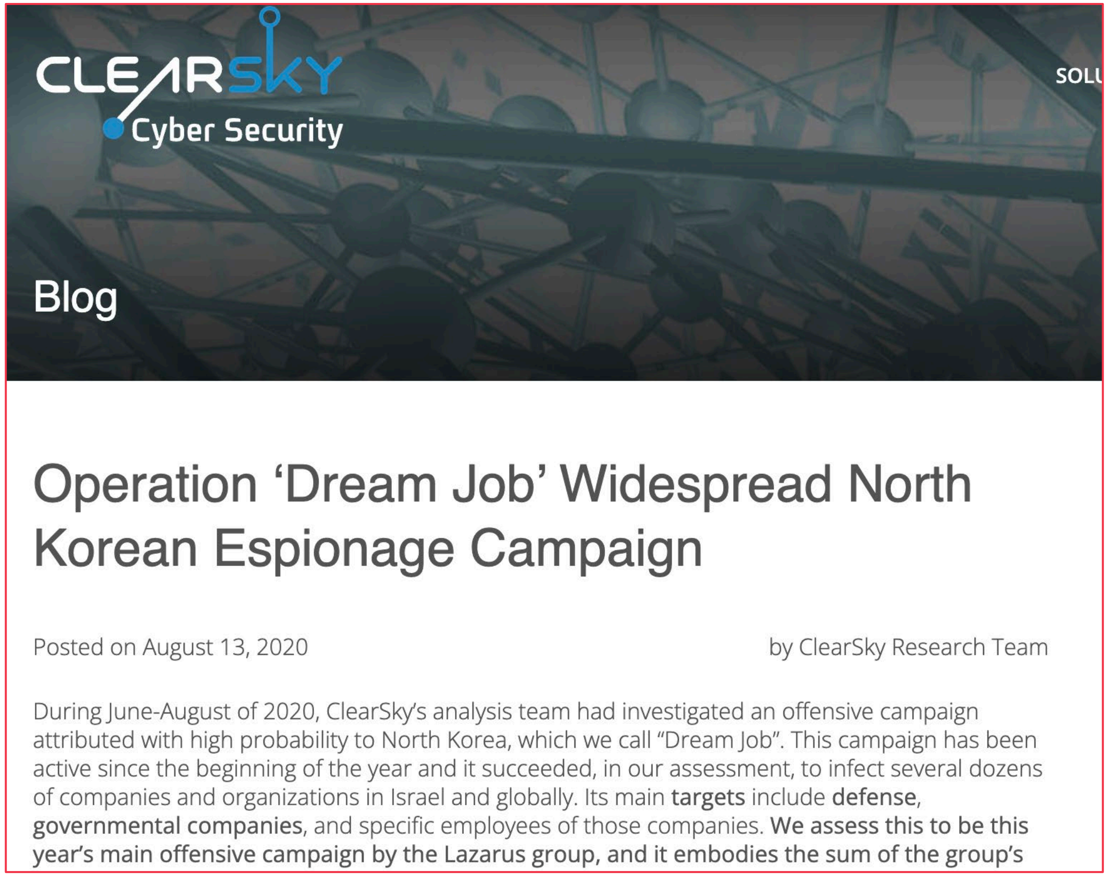
Examples



Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine (Updated Feb. 16)

60,910 people reacted | 39 | 19 min. read

By Unit 42
February 3, 2022 at 1:00 PM
Category: Government, Malware
Tags: Advanced URL Filtering, APT, Cortex, DNS security, Gamaredon, next-generation firewall, primitive bear, Russia, Ukraine, WildFire

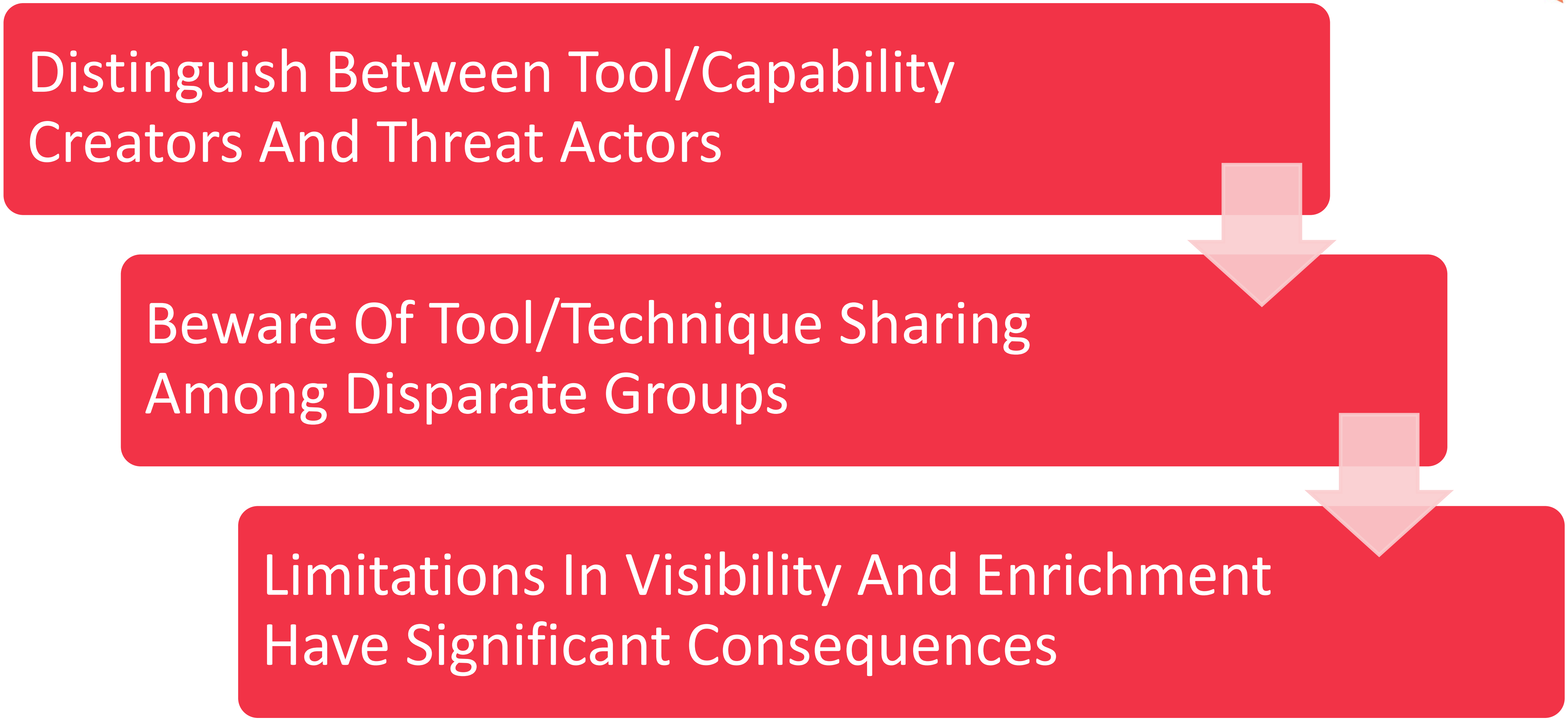


Operation 'Dream Job' Widespread North Korean Espionage Campaign

Posted on August 13, 2020 by ClearSky Research Team

During June-August of 2020, ClearSky's analysis team had investigated an offensive campaign attributed with high probability to North Korea, which we call "Dream Job". This campaign has been active since the beginning of the year and it succeeded, in our assessment, to infect several dozens of companies and organizations in Israel and globally. Its main **targets** include **defense**, **governmental companies**, and specific employees of those companies. **We assess this to be this year's main offensive campaign by the Lazarus group, and it embodies the sum of the group's**

Potential Pitfalls



Distinguish Between Tool/Capability Creators And Threat Actors

Beware Of Tool/Technique Sharing Among Disparate Groups

Limitations In Visibility And Enrichment Have Significant Consequences

Implementing In Your Environment!

- “Raw” Indicators Must Be Enriched & Analyzed!
- Enriched Indicators Yield Composite Structures!
- Composite Structures Enable Behavior & Tendency Identification!
- Understanding Behaviors Makes Pivoting And Enhanced Alerting Possible!

References & Resources

- “OpenIOC: Back to the Basics” – Will Gibb & Devon Kerr, Mandiant (https://www.mandiant.com/resources/openioc-basics)
- “Misunderstanding Indicators of Compromise” - Dave Dittrich & Katherine Carpenter (https://threatpost.com/misunderstanding-indicators-of-compromise/117560/)
- “Indicators and Network Defense” – Joe Slowik (https://pylos.co/2018/05/16/indicators-and-network-defense/)
- “Formulating a Robust Pivoting Methodology” – Joe Slowik, DomainTools (https://www.domaintools.com/content/formulating-a-robust-pivoting-methodology.pdf)
- “Analyzing Network Infrastructure as Composite Objects” – Joe Slowik, DomainTools (https://www.domaintools.com/resources/blog/analyzing-network-infrastructure-as-composite-objects)
- “Threat Intelligence and the Limits of Malware Analysis” – Joe Slowik, Dragos (https://www.dragos.com/wp-content/uploads/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf)

Questions?

Joe.slowik@gigamon.com / joe@paralus.co

@jfslowik