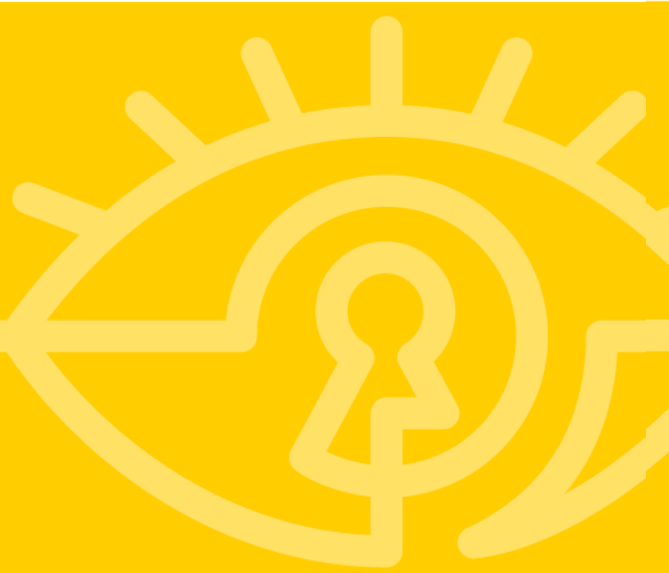
RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-R04

Ghosts In The Shadows

STEPHEN BRENNAN
S.VP Cyber Network Defence
DarkMatter LLC
darkmatter.ae
@StephensLogic



AN INTRODUCTION

DARKMATTER

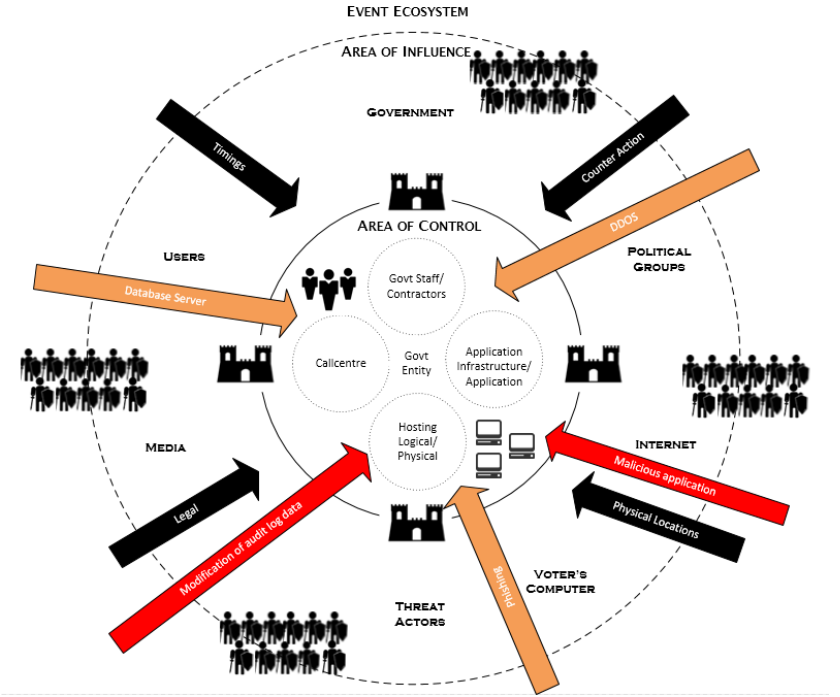
WHY LIMITED STEALTH OPERATIONS

- Exponential attack surface, threat actor growth & evolution
- Current Strategies are ineffective
- Challenge exceeds resources
- Business & clients demand more security from less (budget & friction)
- New Platforms require new (unproven solutions)

DARKMATTER

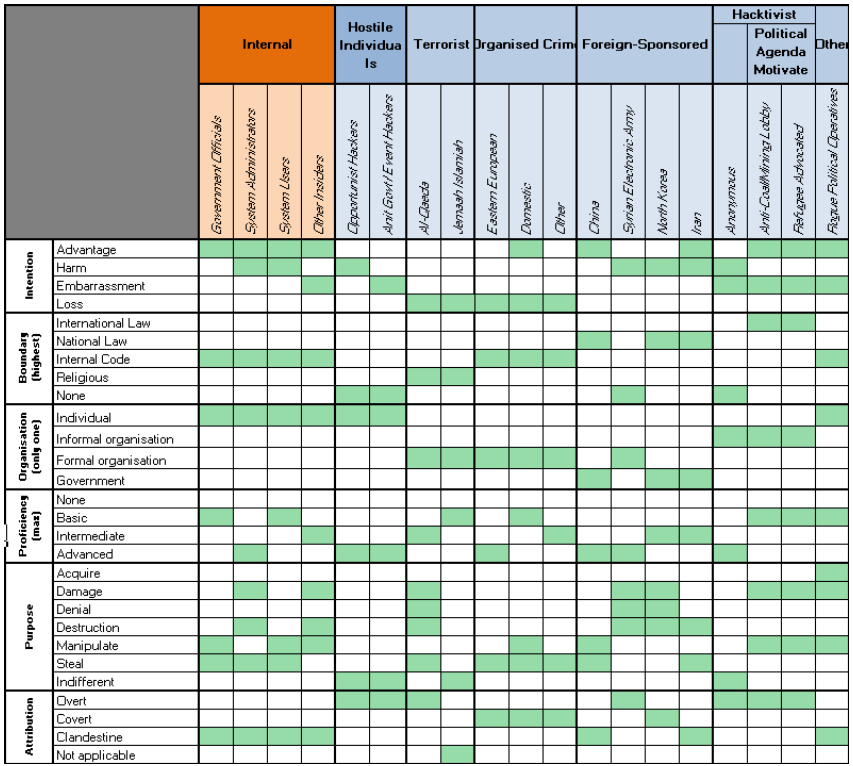
ANF-01 Hunter To The Hunted

- Wargame
  - Specialists
  - Attack tree
  - Action – Reaction – Counteraction
- Threat course of action
  - Wargame analysis
  - Most Dangerous
  - Most Likely



ANF-01 Hunter To The Hunted

- Research Actors
- Attribution
- Capability synopsis
- Ecosystem Analysis



		Internal				Hostile Individuals		Terrorist		Organised Crime			Foreign-Sponsored				Hacktivist			Other
		Government Officials	System Administrators	System Users	Other Insiders	Opportunist Hackers	Anti Govt / Event Hackers	Al-Qaeda	Jemaah Islamiah	Eastern European	Domestic	Other	China	Syrian Electronic Army	North Korea	Iran	Anonymous	Anti-Coalition/Iraq Lobby	Refugee Advocated	Rogue Political Operatives
Intention	Advantage	■	■	■	■						■		■		■	■		■	■	■
	Harm		■	■		■								■	■	■	■			
	Embarrassment				■		■										■	■	■	■
	Loss							■	■	■	■	■								
Boundary (highest)	International Law																	■	■	
	National Law												■		■	■				
	Internal Code	■	■	■	■					■	■	■								■
	Religious							■	■											
	None					■	■							■			■			
Organisation (only one)	Individual	■	■	■	■	■	■													■
	Informal organisation																■	■	■	
	Formal organisation							■	■	■	■	■		■						
	Government												■		■	■				
Proficiency (max)	None																			
	Basic	■		■					■		■							■	■	■
	Intermediate				■			■				■			■	■				
	Advanced		■			■	■			■			■	■			■			
Purpose	Acquire																			■
	Damage		■		■			■						■	■			■	■	■
	Denial							■						■	■					
	Destruction		■		■			■						■	■	■				
	Manipulate	■		■	■						■		■			■		■	■	■
	Steal	■	■	■				■		■	■	■	■			■				
	Indifferent					■	■		■								■			
Attribution	Overt					■	■	■						■			■	■	■	
	Covert									■	■	■			■					
	Clandestine	■	■	■	■								■			■				■
	Not applicable								■											

DARKMATTER

LIMITED STEALTH OPERATIONS

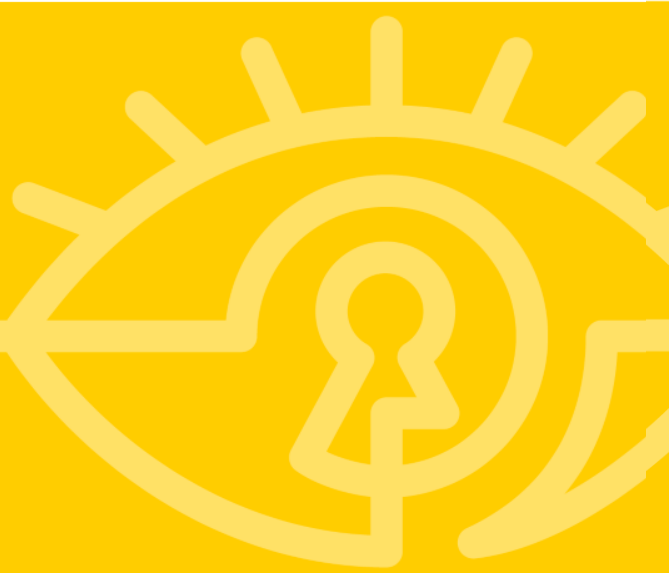
- Execution of the Intelligence plan
- Predetermined focal points
- Monitor the Threat Actors – Command & Control
- Feed into SOC / Threat Intelligence Platform
- Expose privileged Data Data Analytics & Big Data

DARKMATTER

WHO ARE THE THREAT ACTORS

- World Trade / Globalisation Activists
- Environmental Groups
- Regional Political Activism
- Non-State Sponsored Terrorism
- Organized Crime
- Nation States / Governments
- Insider Threats

- Information Hacktivisists
- General Attacker Threats
- Illegal Information Brokers and Freeland Agents
- Trusted 3rd Partners
- Corporate Intelligence
- Investigation Companies
- Competitors, Contractors, Corporations
- Untrained Personnel

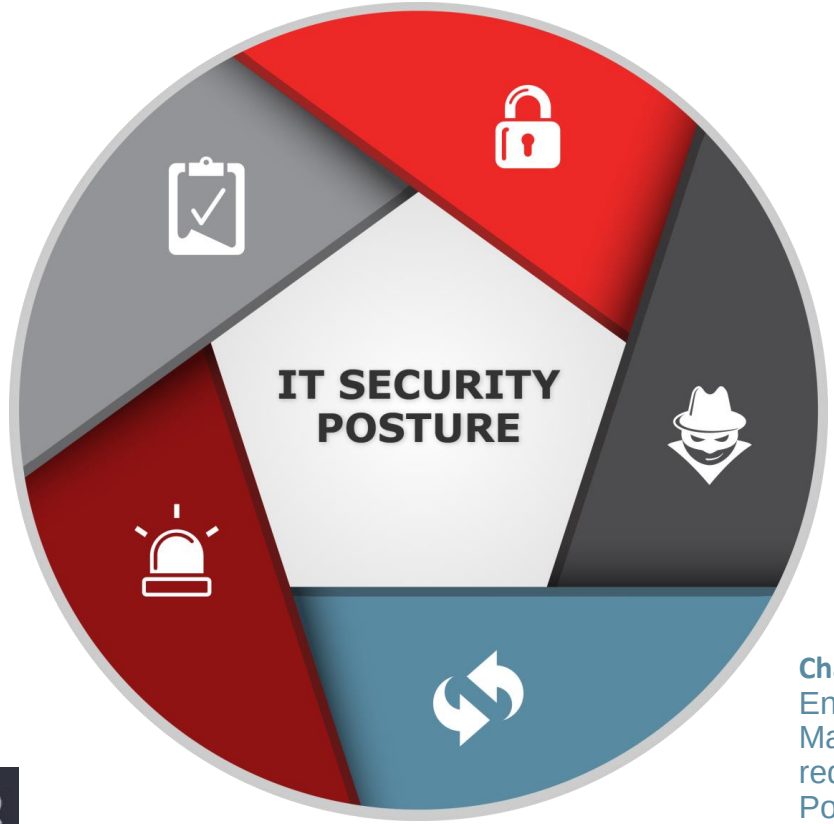


BE OFFENSIVE

DARKMATTER

BE OFFENSIVE

Compliance Management
System hardening.
Compliance to Regulations & Policy



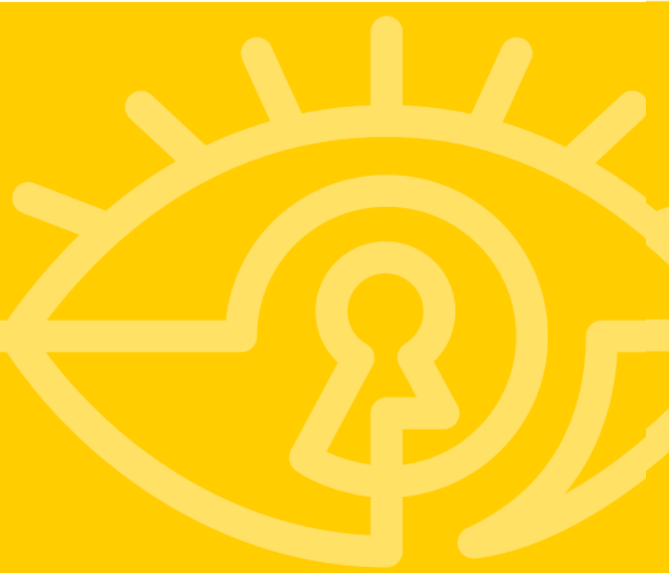
Vulnerability Management
Status of Security Patching
Wintel, Desktop, Unix

Threat Management
Status of Anti Virus, NIPS, Email & URL Content Filtering

Incident Management
Security Related Incidents
AV, NIPS, SPAM, SRT

Change Management
Ensure Change Management requests adhere to Policy

DARKMATTER

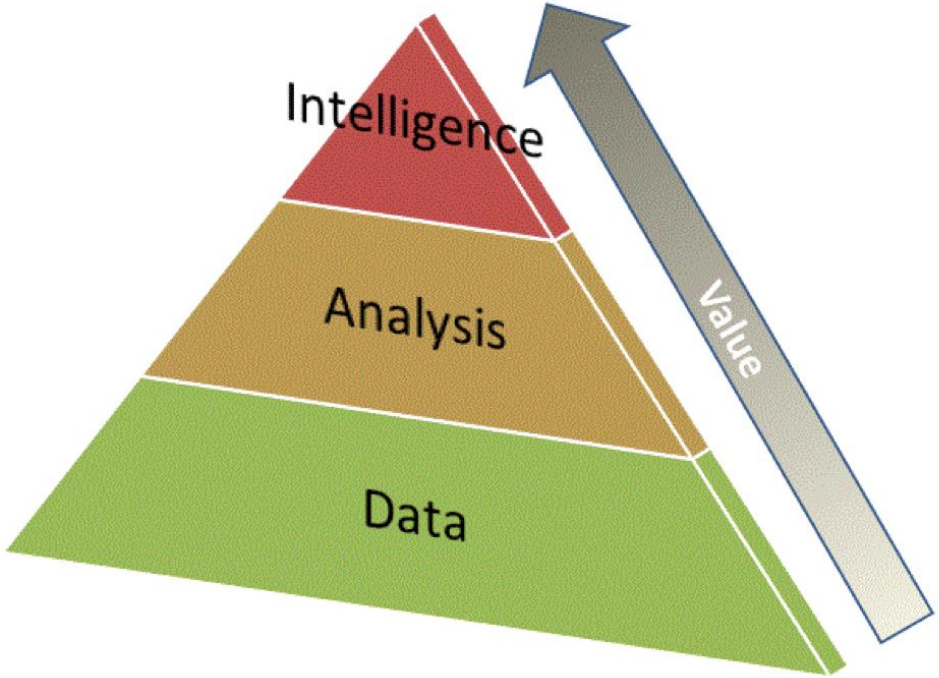


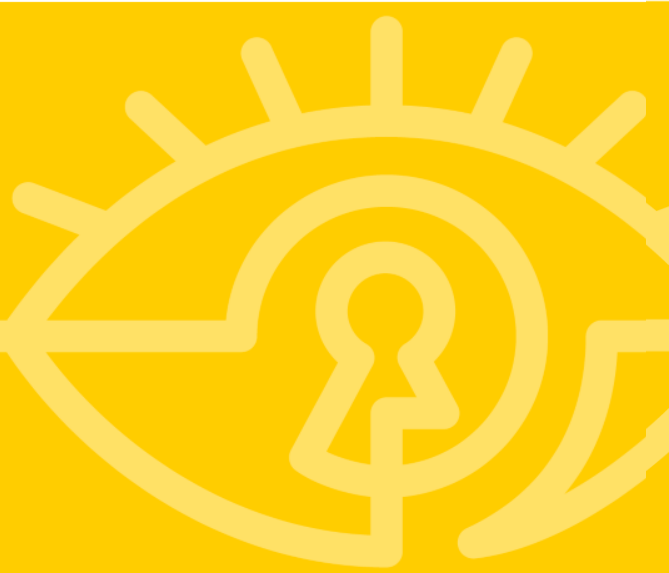
HONOUR YOUR PROFESSIONALS

DARKMATTER

HONOR YOUR PROFESSIONALS

- Establish Ethics
- Threat actor focus
- Intelligence Analysis
- Collection planning
- Proactive approach

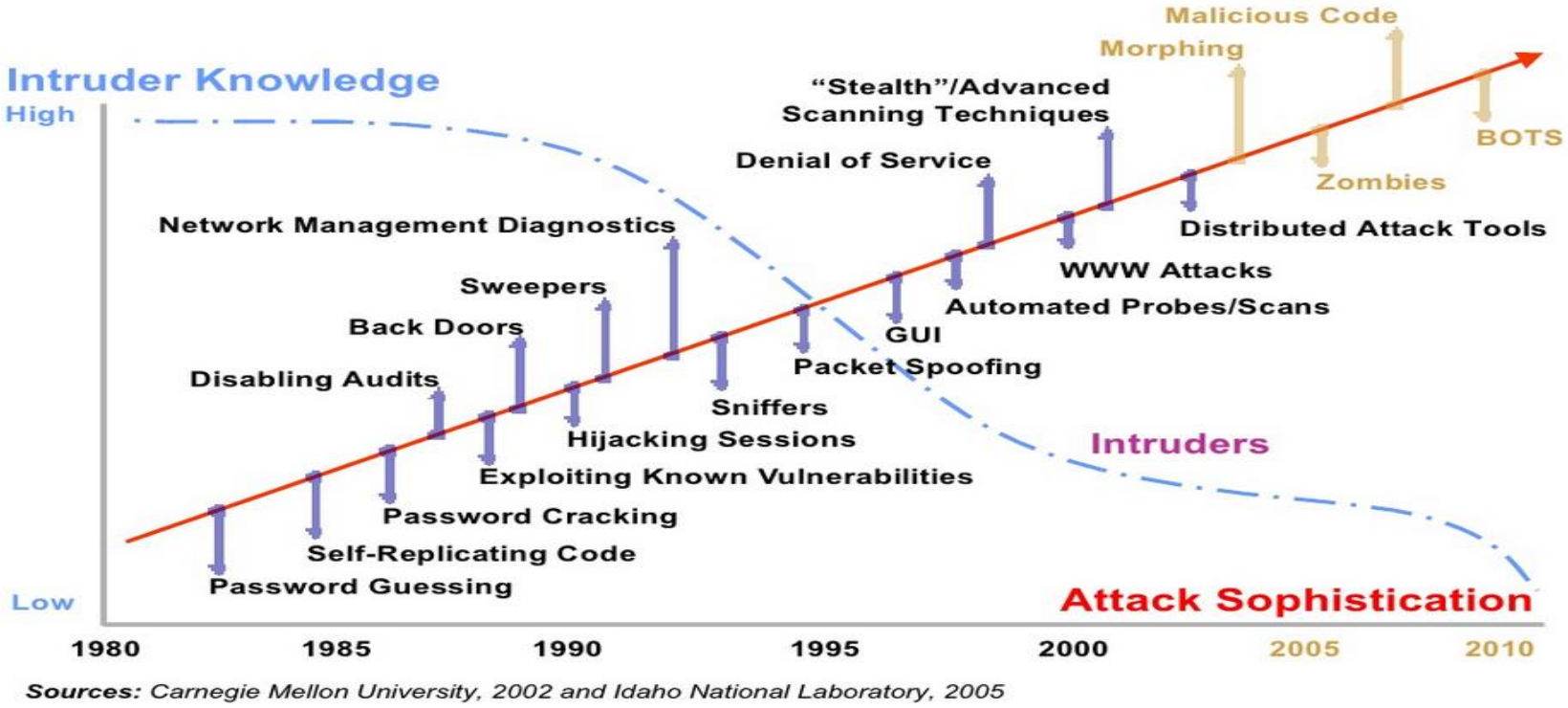




OWN THE INTERNET

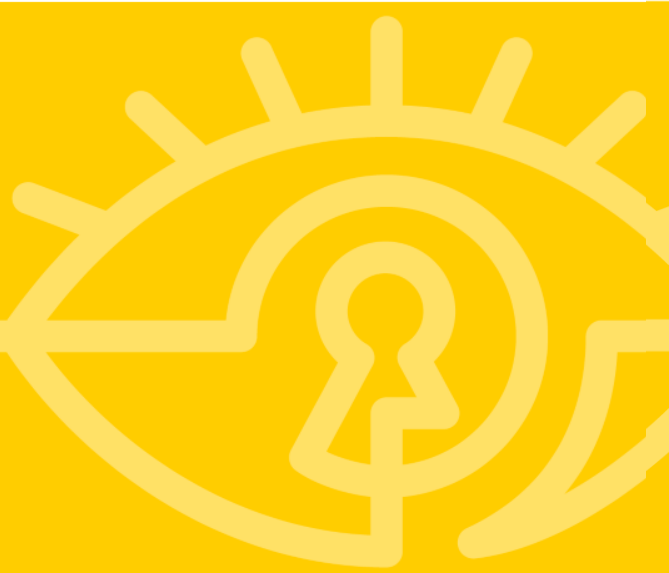
DARKMATTER

OWN THE INTERNET



Sources: *Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005*

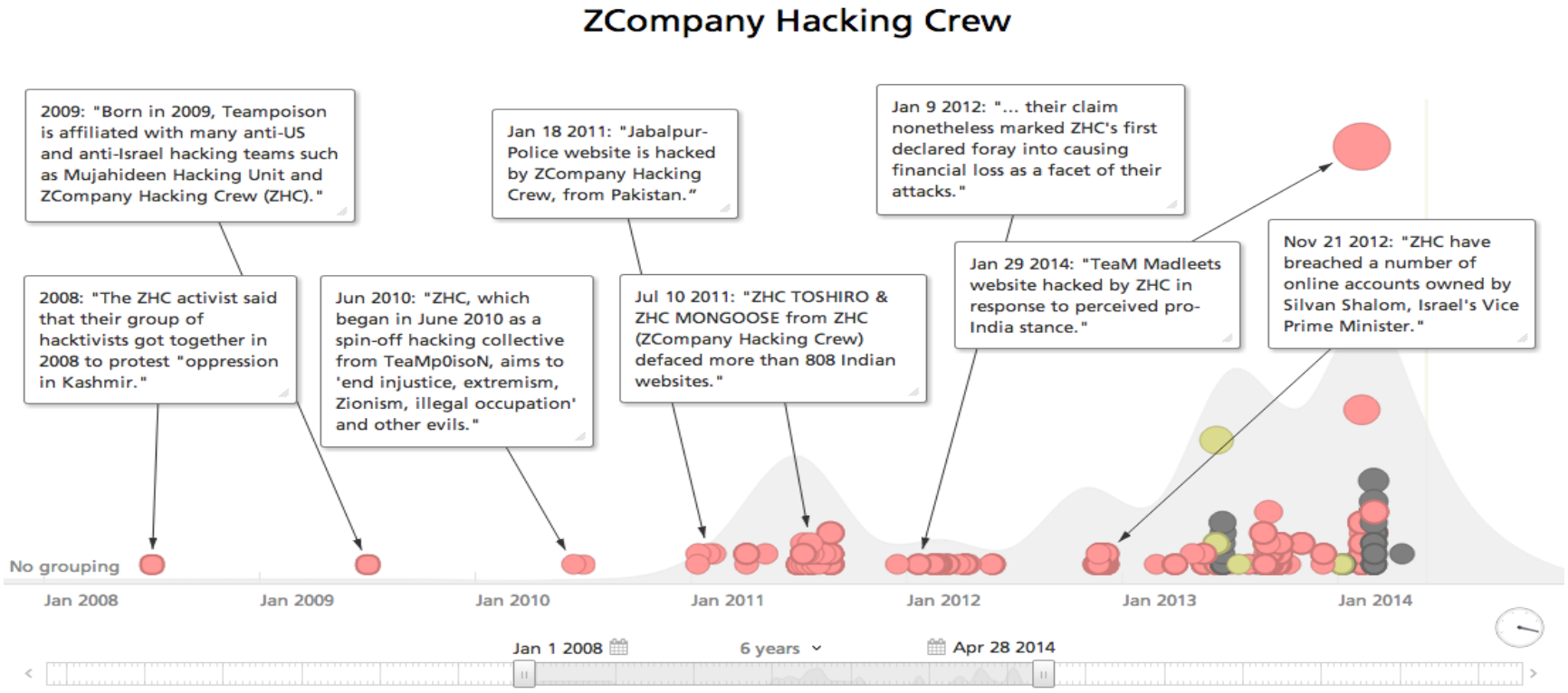
DARKMATTER



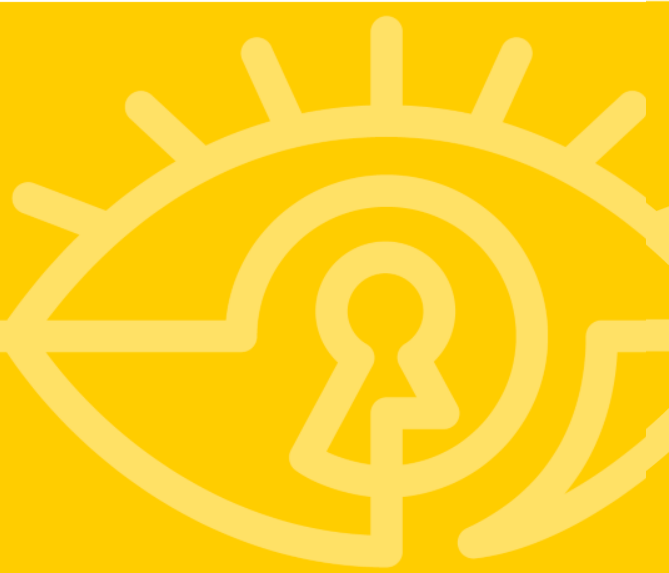
KNOW YOUR HISTORY

DARKMATTER

KNOW YOUR HISTORY



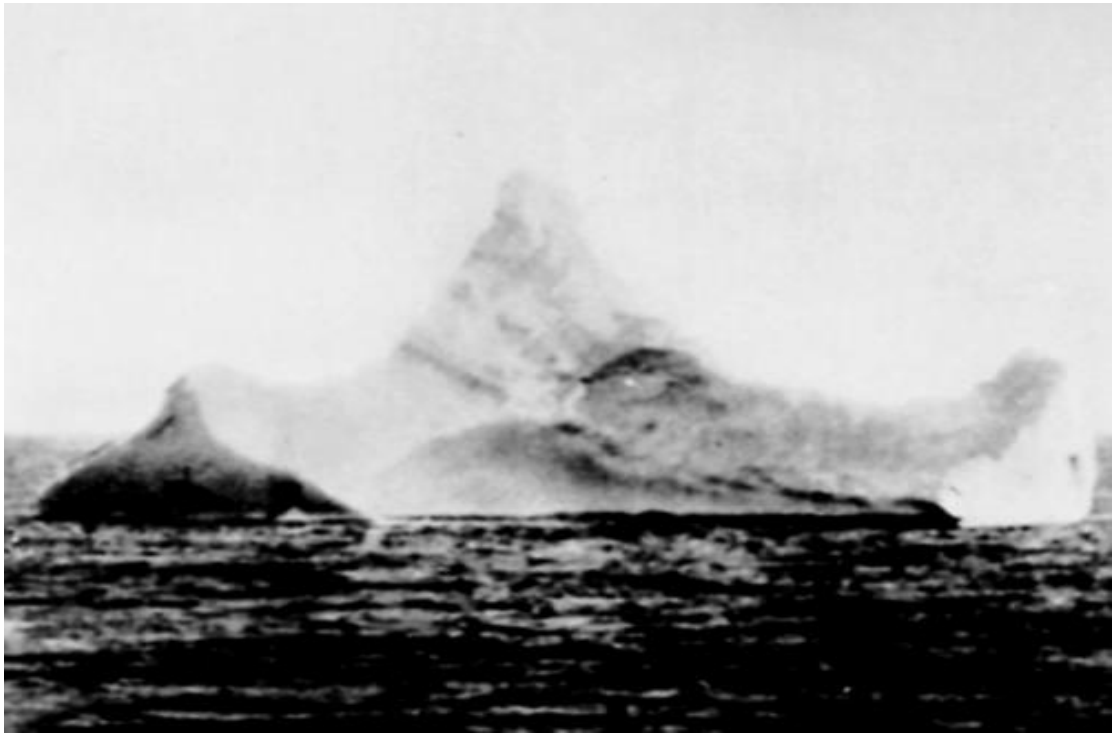
Source and Copyright: RecordedFuture

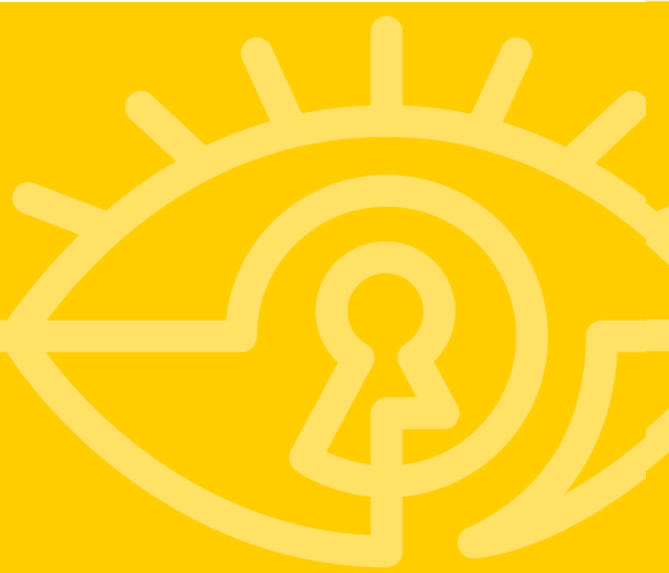


DO NOT IGNORE ANALYSIS

DARKMATTER

DO NOT IGNORE ANALYSIS

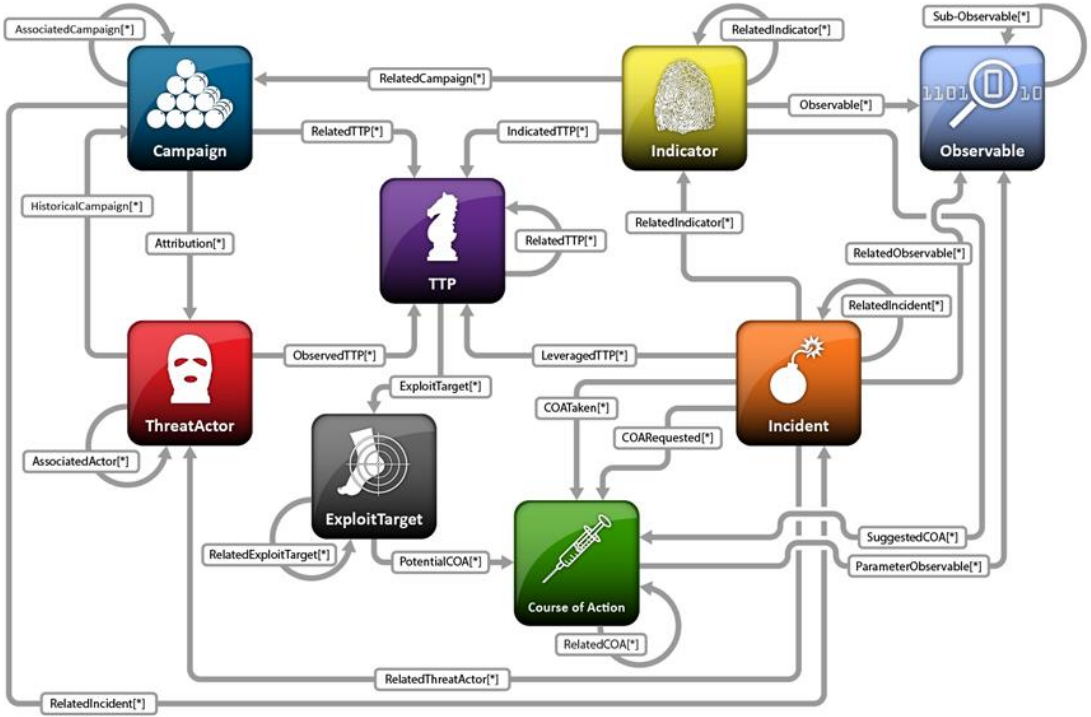




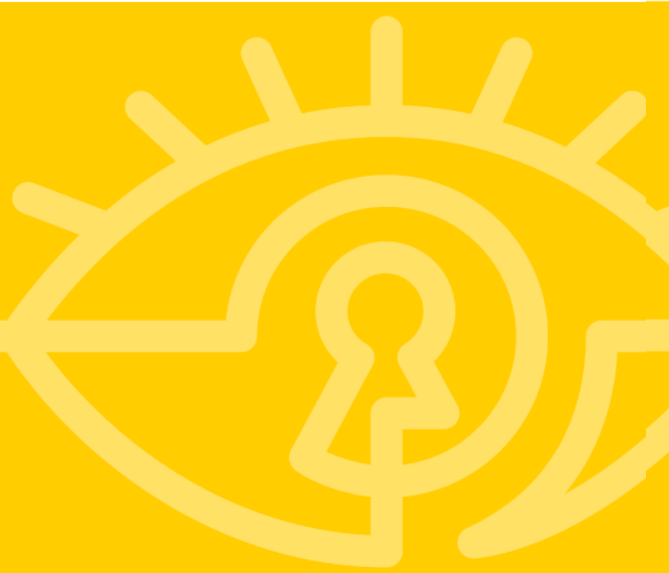
DO NOT ISOLATE

DARKMATTER

DO NOT ISOLATE



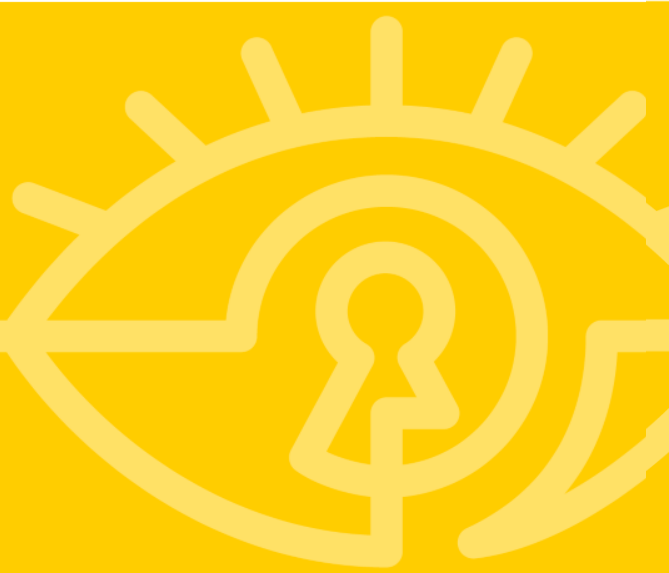
- Observables
- Indicators
- Incidents
- Adversary RRPs
- Exploit Targets
- Courses of Action
- Campaigns
- Threat Actors
- Reports



TRAIN YOUR PEOPLE

DARKMATTER

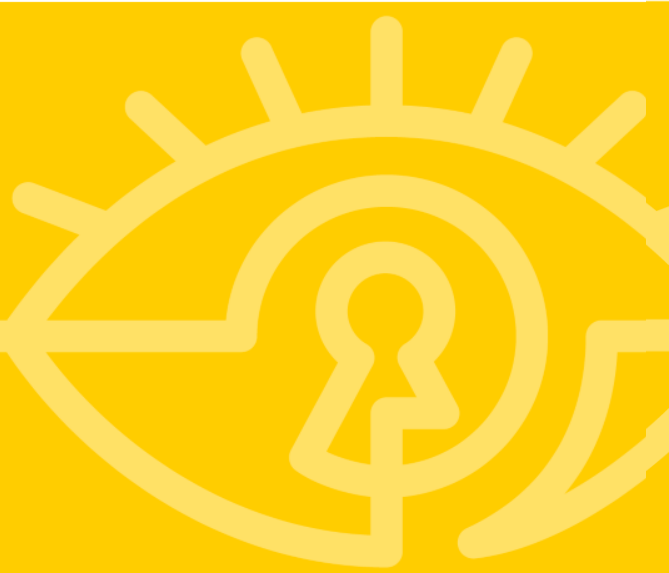
TRAIN YOUR PEOPLE



DO NOT BE MARGINALISED

DARKMATTER

DO NOT BE MARGINALISED



DO NOT LOITER

DARKMATTER

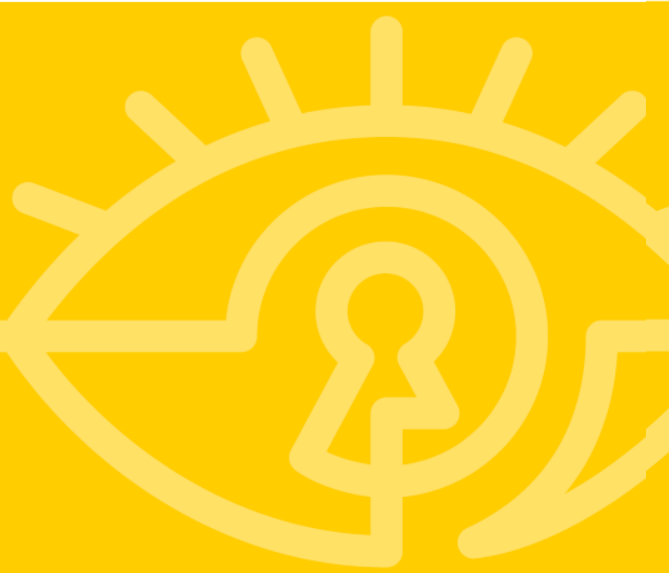
ACTIONS

317
MILLION
New malware detected in 2014 alone

+500%
Increase in mobile malware over 1 year

295
DAY
average time it took to detect the top 5 zero-day exploits in 2014

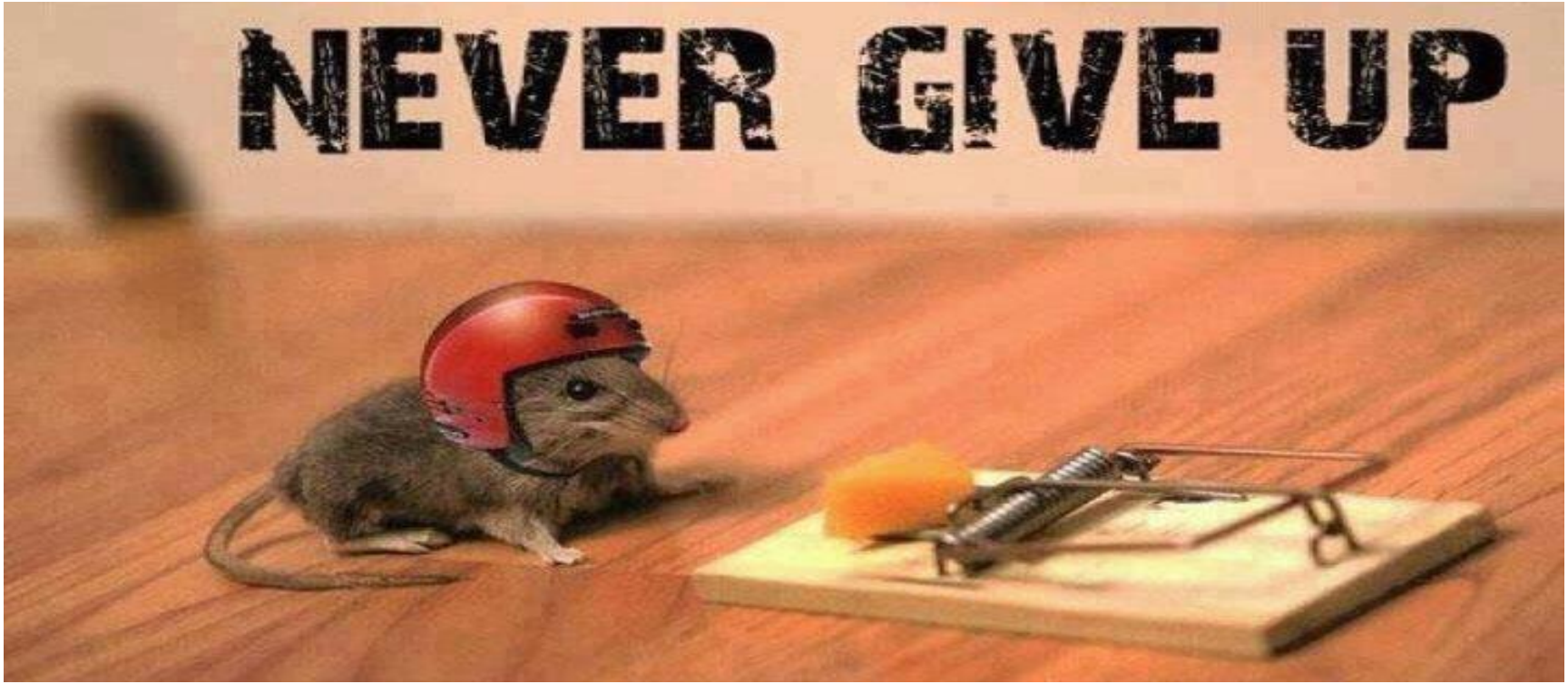
DARKMATTER

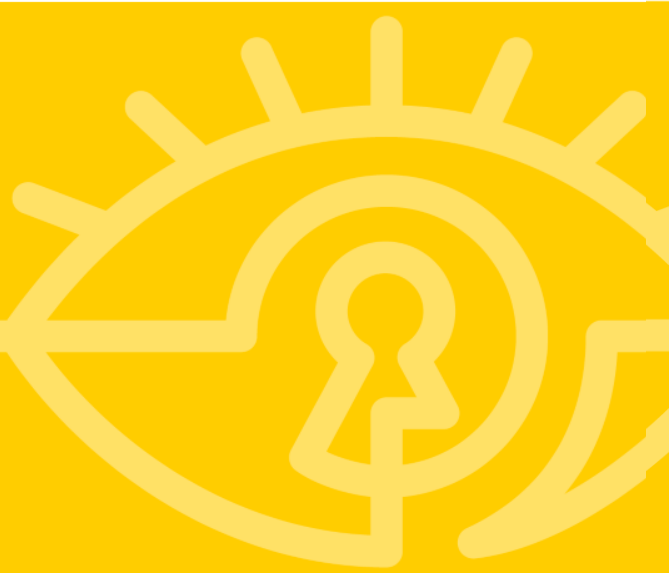


NEVER GIVE UP

DARKMATTER

NEVER GIVE UP





SO WHAT NOW? AKA NICE STORY

DARKMATTER

SUMMARY

- Threat Intelligence is a Training Indicator of Campaigns
- Limited Stealth Operations Allow You To
  - Gather Intelligence Offensively (Passively)
  - Enrich Information Security and Risk Management Plans
- This Is Applicable to Everyone
  - Not Purely The Domain of The Paranoid and Nation States
- Threat Actors Often Use The Path Of Least Resistance

HOMEWORK - APPLY

- Check Out ANF-F01 Hunted To The Hunter (RSA USA 2015)
- Think like a Threat Actor (Research your Threat Actors)
- Categorize and prioritize
- Develop Online Identifies and Intelligence Collection plan
- Monitor Threat Actors
- Do not be tempted by the dark side (Ethics)
- DON’T PANIC

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-R04

Thank You and Questions?

STEPHEN BRENNAN

S.VP Cyber Network Defence
DarkMatter LLC
darkmatter.ae
@StephensLogic

#RSAC