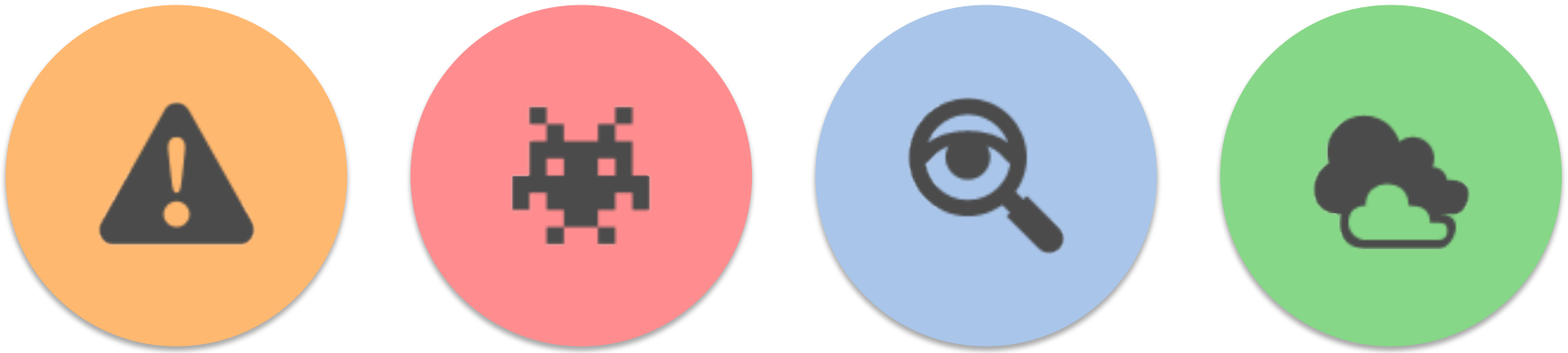
Recorded Future

CREATING AN INSIGHTFUL WORLD

Cyber Threat Intelligence

"Cloudy, with a risk of cyber attacks"

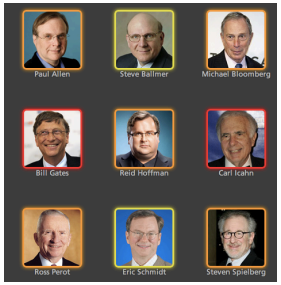
Staffan Truvé, PhD
Co-founder / CTO
truve@recordedfuture.com



Recorded Future Background

- Web Intelligence
- From data collection to structured data to signals to visualization/UI and API
- Customers include
  - Intelligence agencies
  - Special operations units
  - Department of Defense
  - Large corporates
    - Finance, manufacturing, energy, technology, pharma
  - Small cyber analysts, journalists, bloggers…
- Based in Cambridge, US and Göteborg, Sweden
  - 40+ staff

Location Monitoring



Executive Monitoring

Cyber Monitoring

Organization Monitoring

Google ventures

IQT IN-Q-TEL

IA VENTURES

Balderton capital

atlasventure

#7

The 15 Biggest Excesses in Google History

BY BRENDEN GALLAGHER | FEB 19, 2014 | 11:02 AM | PERMALINK

Image via Grand Youth

Predicting the Future

The investment team at Google has put some serious cash into Recorded Future, a company that attempts to create a crystal ball out of shitload of data. Apparently, the gamble paid off, as Recorded Future counts some of the largest companies in the world among its client base. From what we can tell, getting connected with Recorded Future is going to cost you a

#1

The 15 Biggest Excesses in Google History

BY BRENDEN GALLAGHER | FEB 19,

Image via Grand Youth

Predicting the F

The investment team at Goo
company that attempts to cr
paid off, as Recorded Future
base. From what we can tell,

The 15 Biggest Excesses in Google History

BY BRENDEN GALLAGHER | FEB 19, 2014 | 11:02 AM | PERMALINK

16 OF 16

Image via i09

Developing A Space Elevator

Any somewhat lazy would-be space explorers out there shouldn't get too excited, there is no space elevator yet (that we know of). Rumors have swirled that space elevators are one of the slate of wild projects in the secretive "Google X" agenda. Scientists feel that we don't have materials strong enough for a space elevator yet, so your dreams of an interstellar shopping mall will have to wait a little bit longer.

Why am I here?

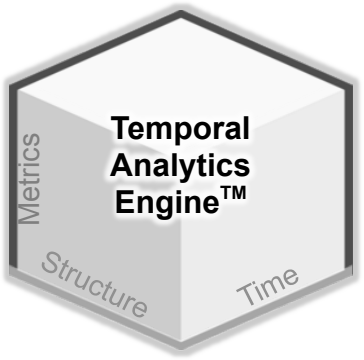
“In cyber security the web balances being the platform to create attacks and being the source of information to prevent attacks”

Oren Falkowitz, ex-Chief Data Scientist at United States Cyber Command/NSA

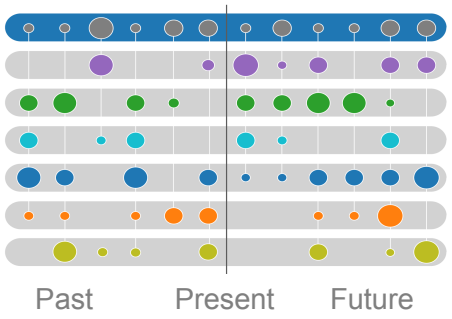
Web Intelligence

UNSTRUCTURED TEXT

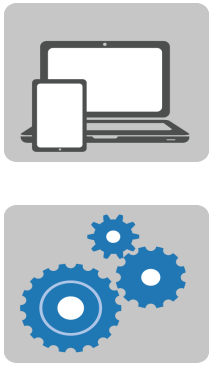
ORGANIZED FOR ANALYSIS



YIELDS NEW INSIGHTS



APPLICATIONS



API

US Patent US8468153


400,000+ Real-Time Sources
Millions of documents per day
Billions of Facts
5 Year History
8 Languages

Text Is Loaded with Temporal Signals

SEP 11 2013

Cyber attack (**OpIsraelReborn**)

52 references • 2 sources • United States

“Hackers joining venture for #OpIsraelReborn, Final day of cyber Attack over Israel on **11 September 2013.**”

SEP 4 2013

Cyber attack by **3xp1r3 Cyber Army**

10 references • 1 source • United States

“@biandykarditama **Bangladesh**’s Largest IT University Daffodil #hacked, server rooted by **3xp1r3 Cyber Army** | **http://t.co/Y1OOChPmyh.**”

AUG 22 2013

Phishing Cyber attack

15 references • 10+ sources • 2 countries

“Victims are usually targeted by that group with spear-phishing emails, which contain a malicious Microsoft Word or PDF attachment with the Poison Ivy code”

SEP 17 2013

Occupy Wall Street and **Monsanto Co** mentioned

14 references • 1 source • United States

“@wizardqi We are calling for #OccupyMonsanto activists to celebrate the 2nd anniversary of #OWS at your nearest #Monsanto facility on Tues. **Sept. 17.**”

AUG 24 2013

Military maneuver by Democratic Republic of the Congo in **Goma**

125 references • 10+ sources • United States

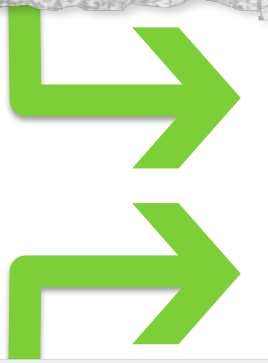
“Congo's U.N. mission, MONUSCO, said two mortar bombs fired by M23 struck the Ndosho neighborhood of Goma - a city of 1 million people - on **Saturday morning**, killing three civilians”

Temporal Analytics Engine

Reveals Links in Meaning Across Sources and Languages

"Please help us to destroy twitter and facebook account of Goldman Sachs february 14 #OpGm"

@YourAnonNews: Feb 7, 2013



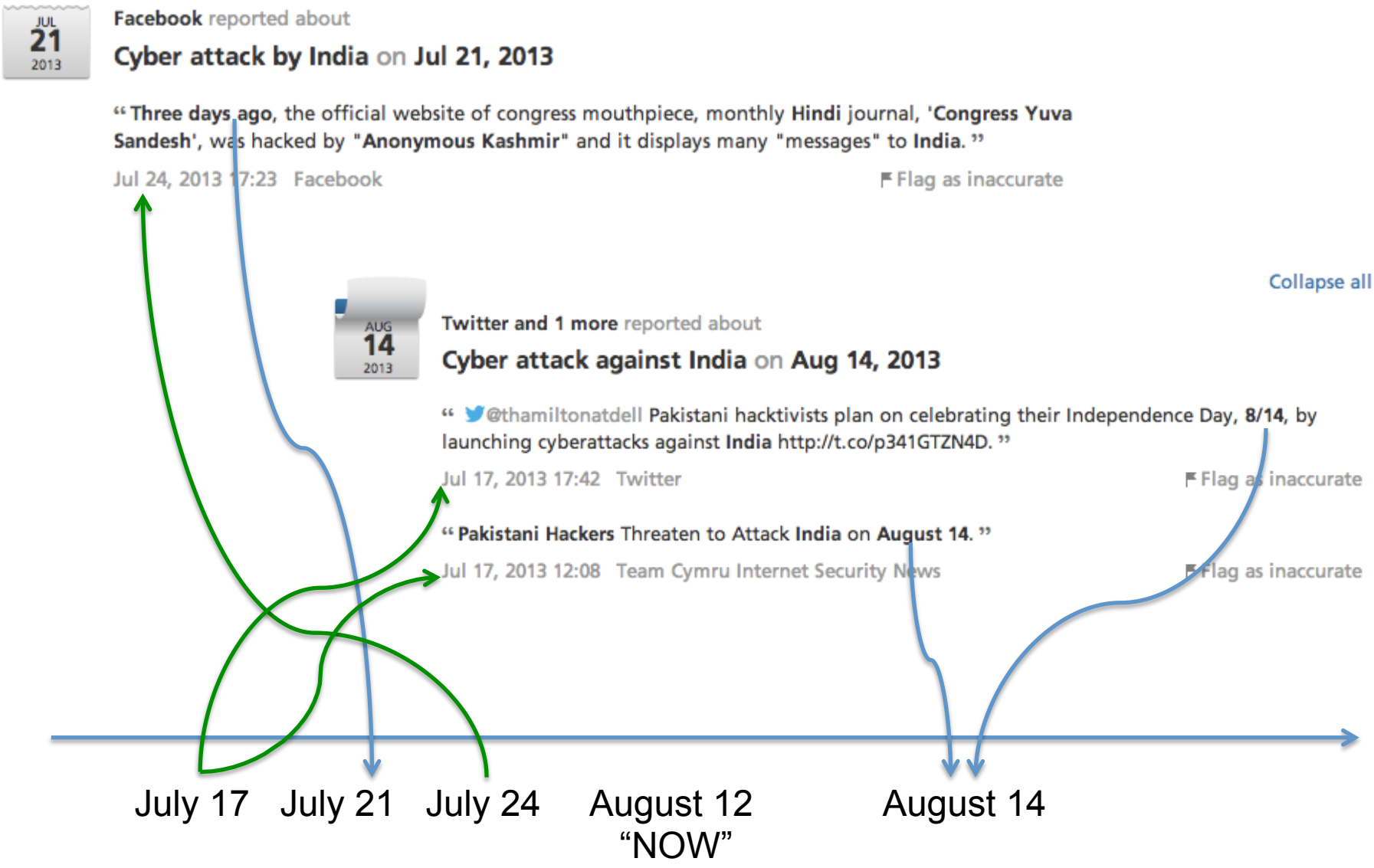
- February, Feb 14 [time]
- Anonymous [entity]
- Cyber attack [event]

Attackers, Targets, TTPs, Operations, Intetions, Times, Companies, People, Geos, IPs, CVEs, RegKeys, FileNames, URLs, Emails, Handles, Hashes

二月，国外黑客组织Anonymous表示，计划摧毁 Goldman Sachs 的网站。

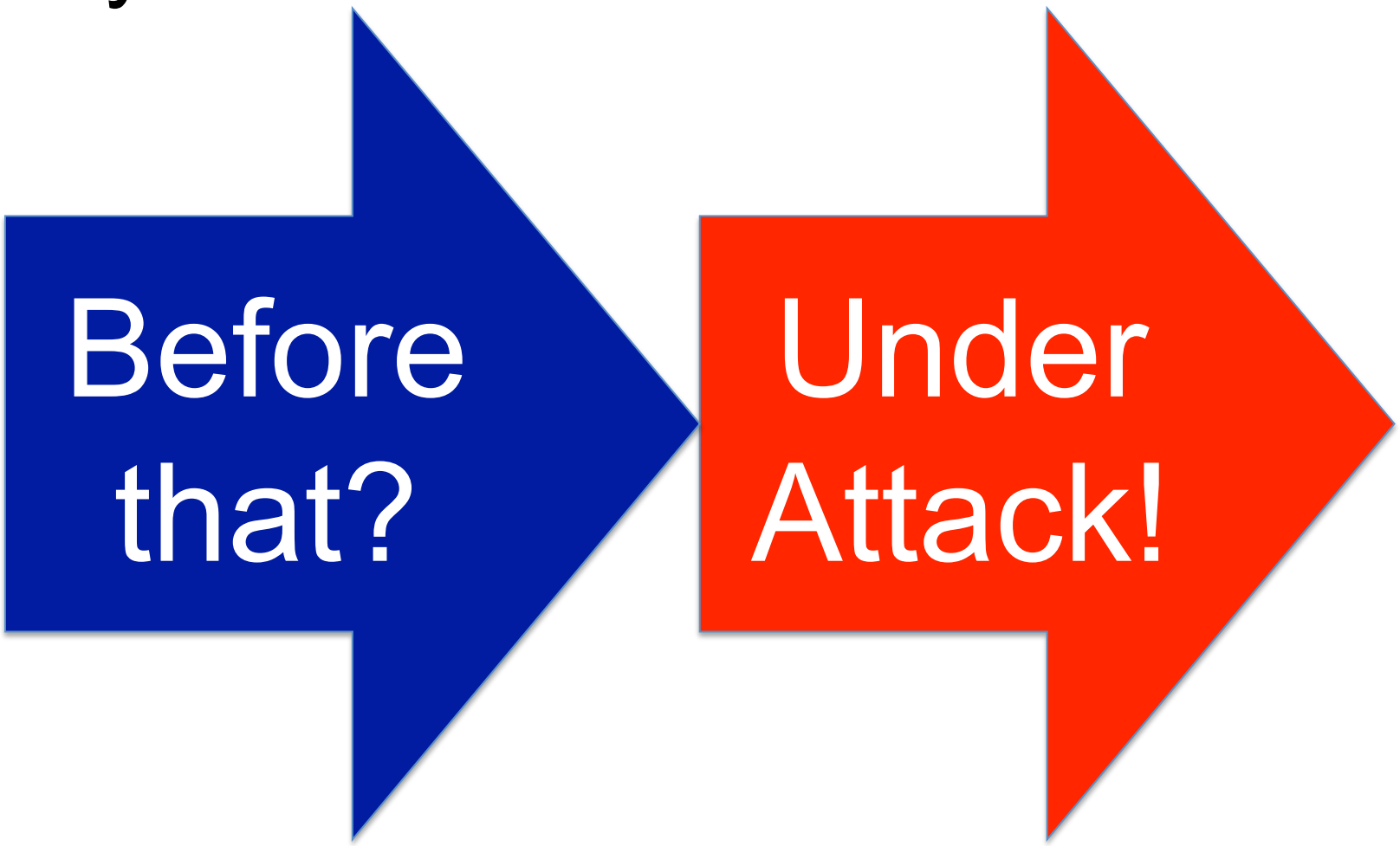
Blogger Jan 29, 2013

Time

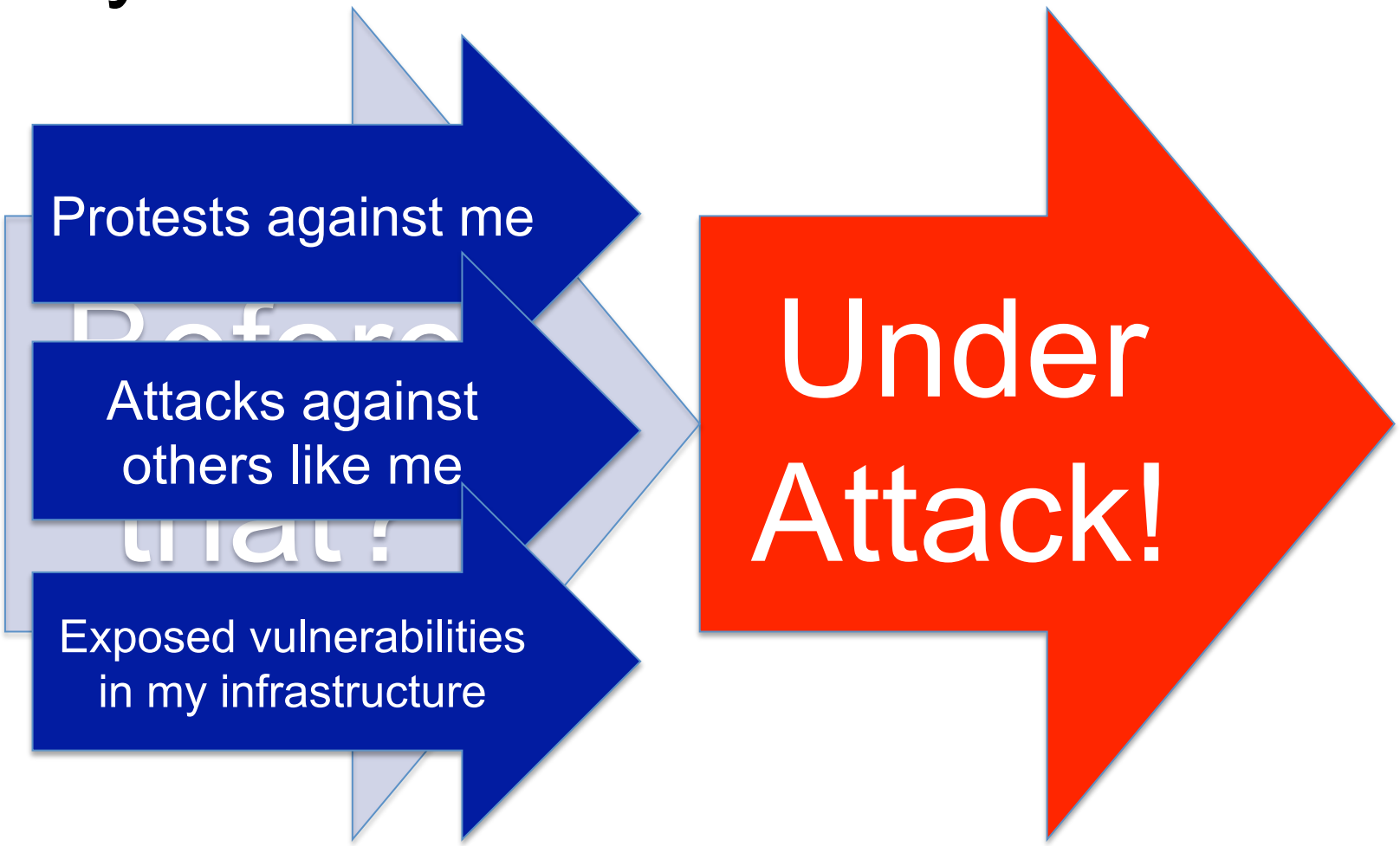

JUL
21
2013
Facebook reported about
Cyber attack by India on Jul 21, 2013
“Three days ago, the official website of congress mouthpiece, monthly Hindi journal, 'Congress Yuva Sandesh', was hacked by "Anonymous Kashmir" and it displays many "messages" to India.”
Jul 24, 2013 17:23 Facebook
Flag as inaccurate
Collapse all
AUG
14
2013
Twitter and 1 more reported about
Cyber attack against India on Aug 14, 2013
“ @thamiltonatdell Pakistani hacktivists plan on celebrating their Independence Day, 8/14, by launching cyberattacks against India http://t.co/p341GTZN4D.”
Jul 17, 2013 17:42 Twitter
Flag as inaccurate
“Pakistani Hackers Threaten to Attack India on August 14.”
Jul 17, 2013 12:08 Team Cymru Internet Security News
Flag as inaccurate
July 17
July 21
July 24
August 12
“NOW”
August 14

Why am I here?

Why am I here?

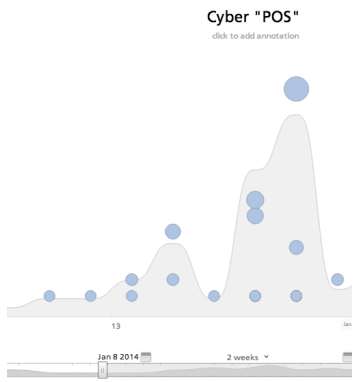


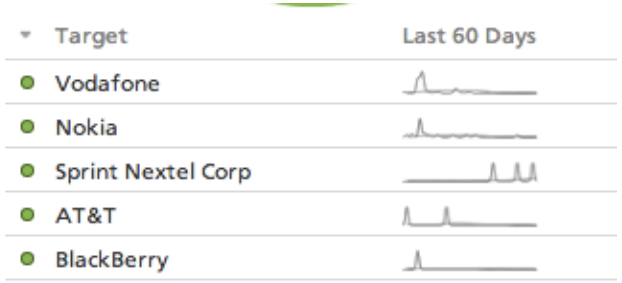
Why am I here?



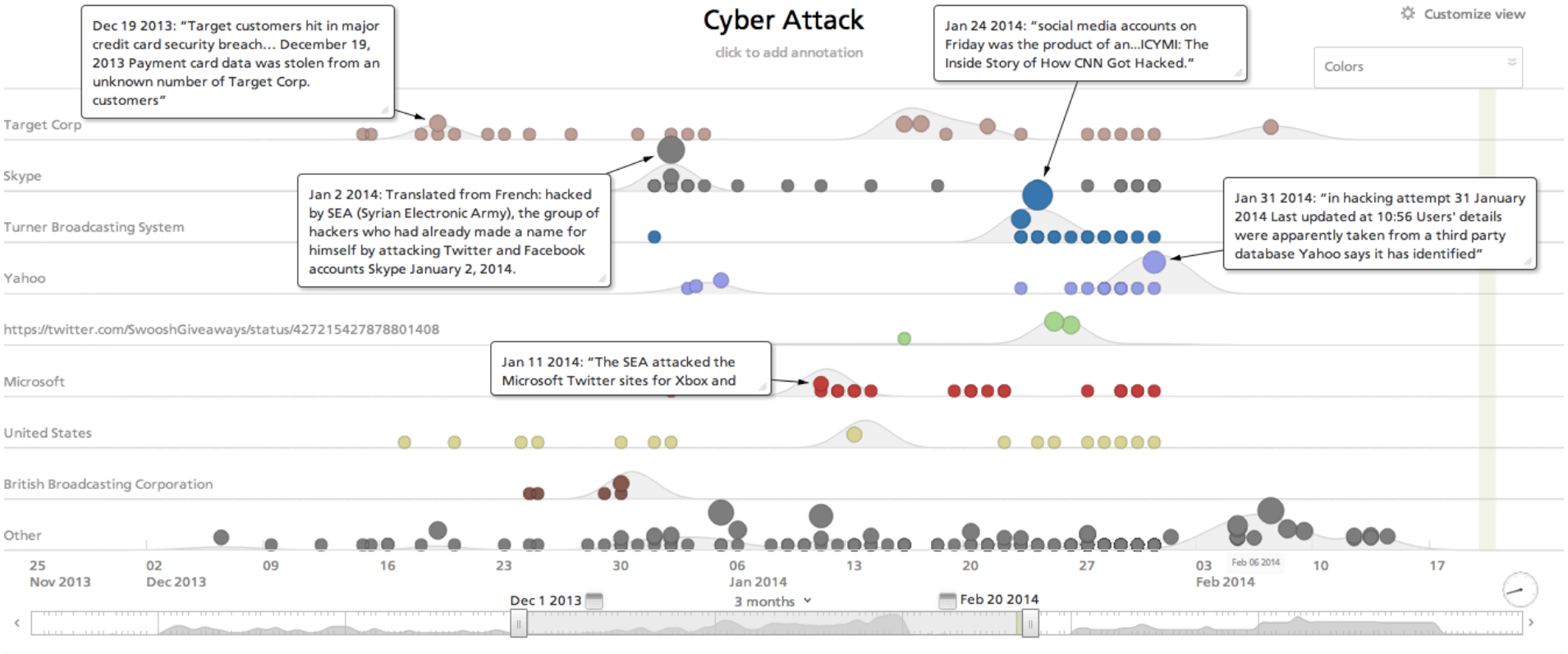
How?

- Early warning
  - Explicit predictions, calls to action
  - Trending attack vectors related to me
  - Trending attacks against “companies like me”
  - Anniversaries
  - Geopolitical, business context
    - G20, Olympics
    - Iranian leadership change
    - SEA - Obama

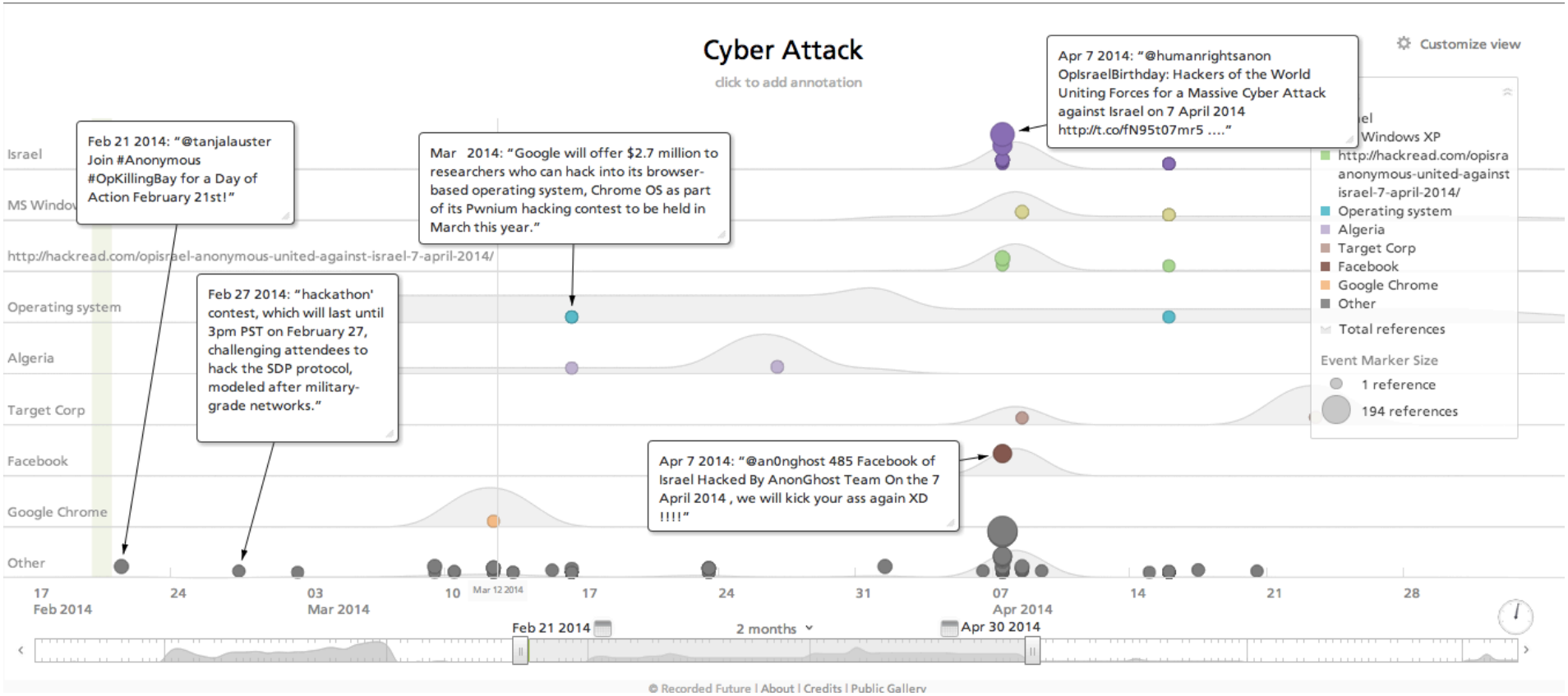




Rear mirror



Future?



Announcing the Future

Anonymous

AnonGh0st

Al Qassam Cyber Fighters

Mauritania Attacker

Islamic Ghost

Tunisian Hacker Team

Anonymous Algeria

Anonymous Turkey

Afghan Cyber Army

Staying Quiet

SEA

RedHack

Iranian Cyber Army

Pinoy Vendetta

Bangladeshi Grey Hat Hackers

Indonesian Cyber Army

Indian Cyber Army

Honker Union

HighTech Brazil HackTeam

Comment Crew

TeaMp0ison

ZCompany Hacking Crew

Teamr00t

Full Spectrum Threat Intelligence

OSINT on Cyber Threats

Security firms: RSA, McAfee, Verisign, Symantec, Cisco
Exploits & metadata: Spamhaus, Malwr.com, ShodanHQ
Black hat: Pastebin, HackerNews, ZoneH
Chat rooms/Forums: Russian, Chinese, Iranian...

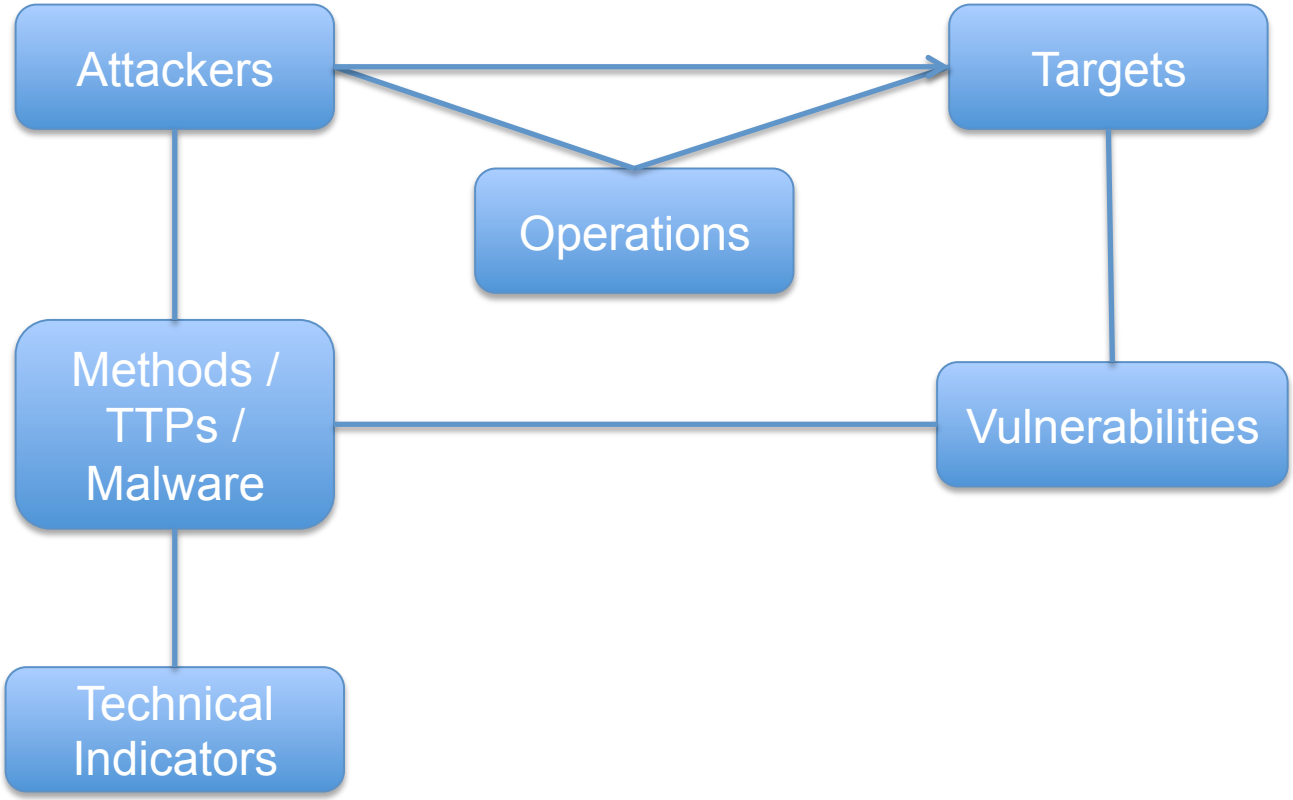
OSINT on Non-Cyber Threats

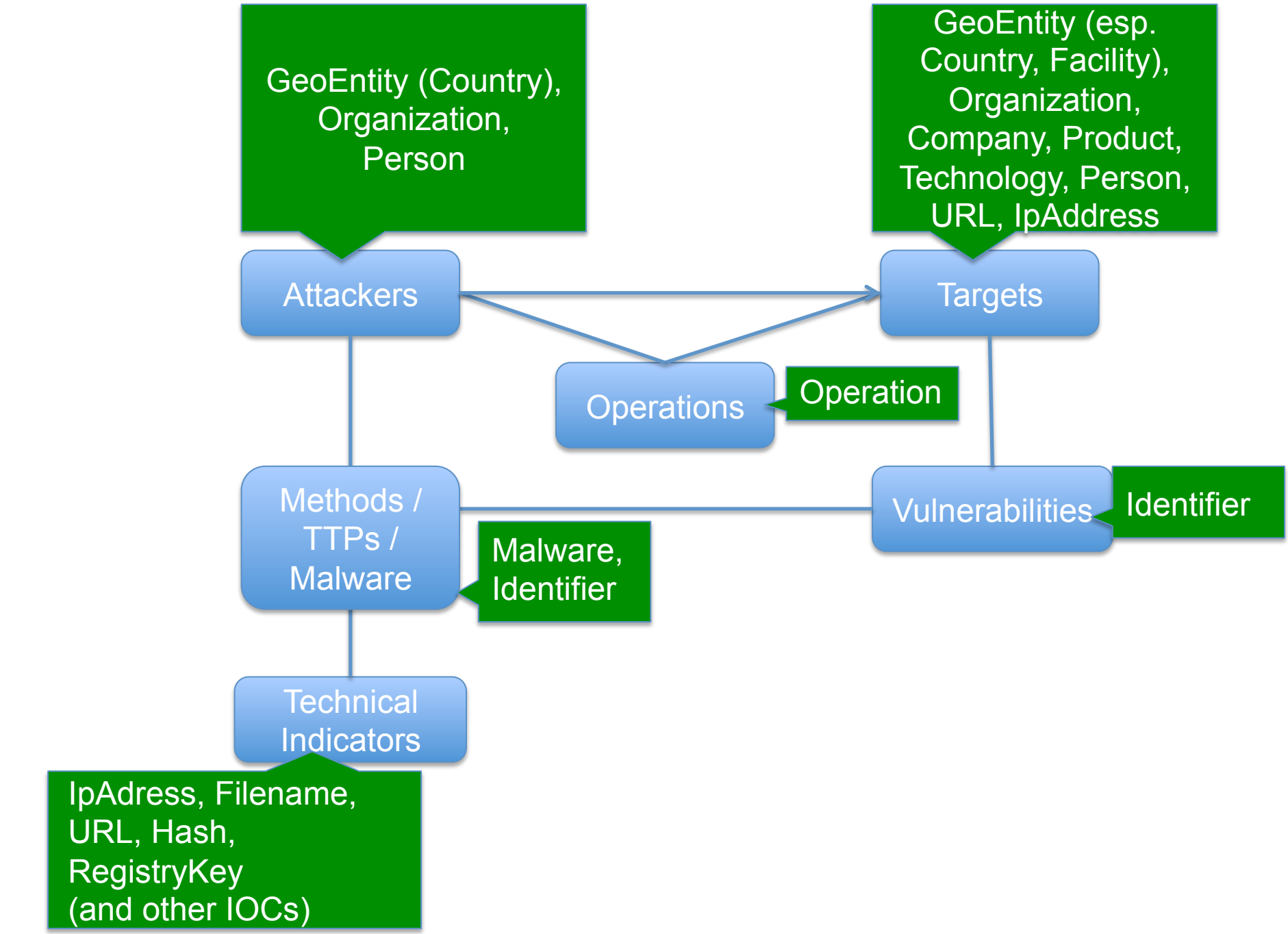
Protests, riots, attacks, bombings
Elections, coups, arrests, trials,
Rulings, convictions, disasters

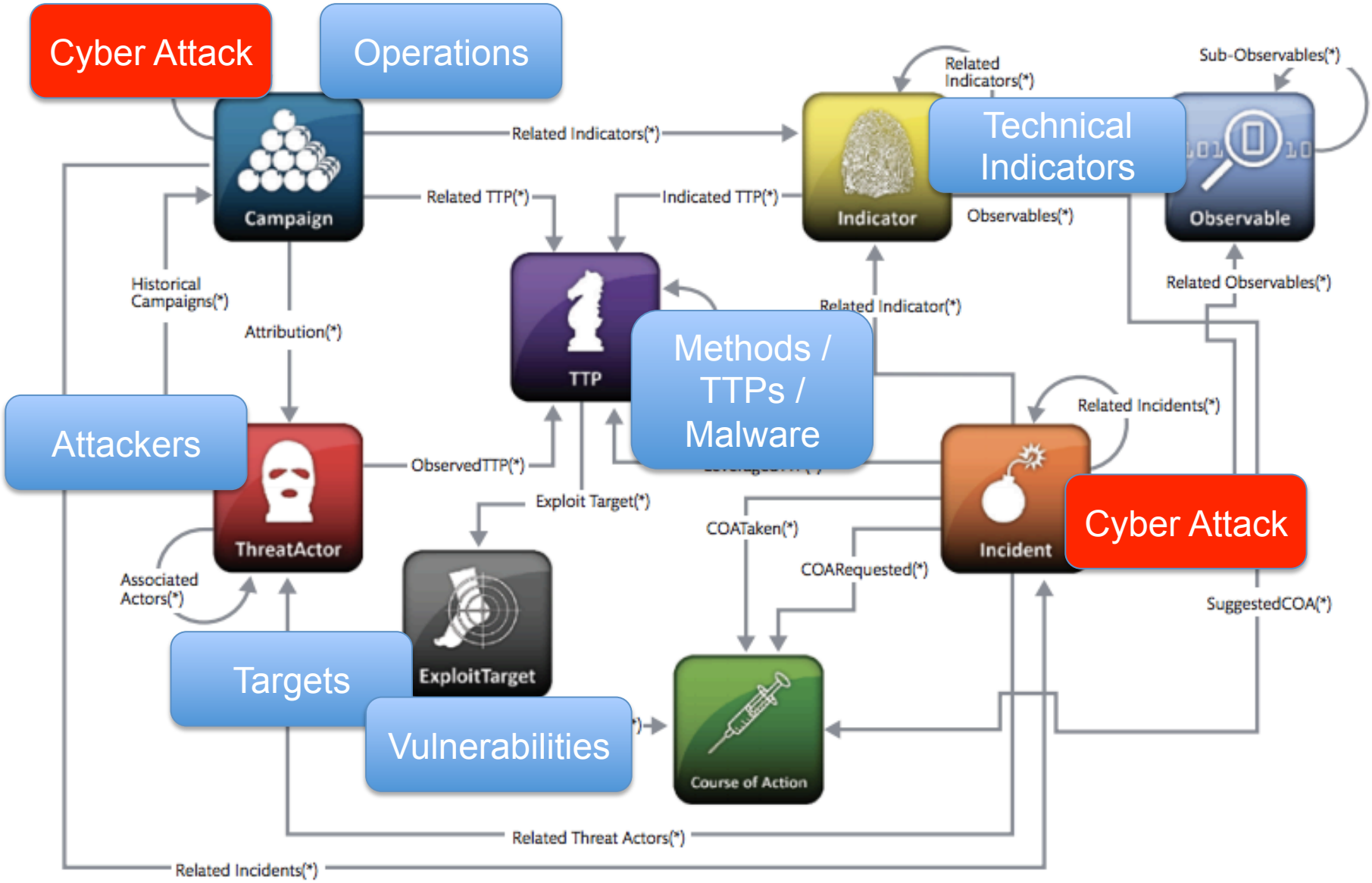
Cyber Threat Intelligence

FINANCIAL SERVICES ISAC
INFRAGARD
US-CERT
ICS-CERT
Palantir
ArcSight
MALTEGO
splunk>
Spotfire

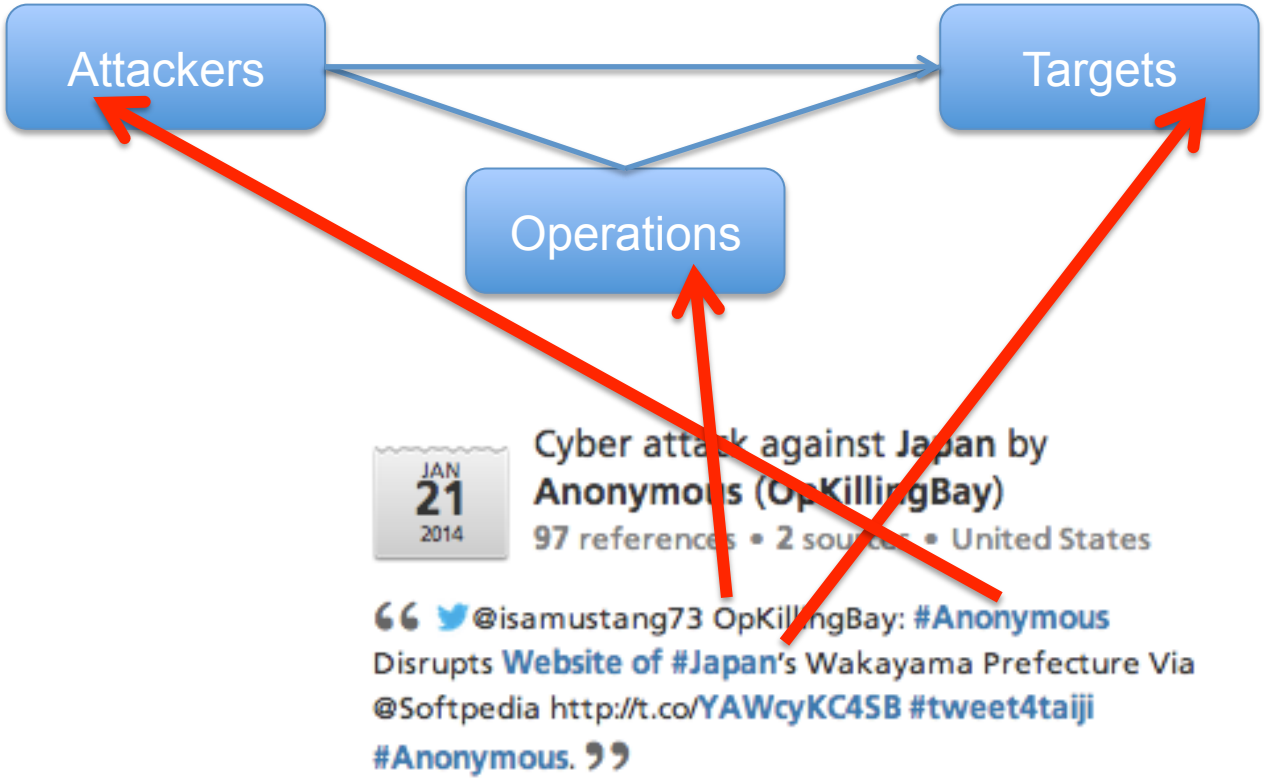
Anatomy of a Cyber Attack




GeoEntity (Country), Organization, Person
GeoEntity (esp. Country, Facility), Organization, Company, Product, Technology, Person, URL, IpAddress
Attackers
Targets
Operations
Operation
Methods / TTPs / Malware
Malware, Identifier
Vulnerabilities
Identifier
Technical Indicators
IpAdress, Filename, URL, Hash, RegistryKey (and other IOCs)



STIX Architecture


Attackers
Targets
Operations
JAN
21
2014
Cyber attack against Japan by
Anonymous (OpKillingBay)
97 references • 2 sources • United States
@isamustang73 OpKillingBay: #Anonymous
Disrupts Website of #Japan's Wakayama Prefecture Via
@Softpedia http://t.co/YAWcyKC4SB #tweet4taiji
#Anonymous.

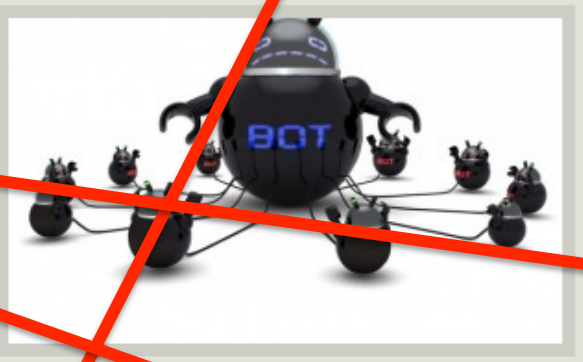

Attackers
Targets
Methods / TTPs / Malware
Technical Indicators
SEP
19
2013
Anonymous, http://t.co/4wpvUQ1PJp, DDoS and 1 more mentioned
references • source • United States
@samehfayed Anonymous: We Are Not Behind DDOS Attack on Sweden's SJ http://t.co/4wpvUQ1PJp #InfoSec.

Kaspersky identifies lethal cross platform Java DDoS botnet

THURSDAY, JANUARY 30TH, 2014 — Fahad Saleem

PERTH: A botnet malware has recently been discovered by the Kaspersky penetration testing gurus when they received a complex system for analysis. This malware owns the capability of affecting systems which run on Mac OS X, Linux and Windows and have Oracle's Java software framework in their list of installed items.

This cross platform is named 'HEUR:Backdoor.Java.Agent.a' by Kaspersky. This malware basically controls the CVE-2013-2465 and damages the system. The CVE-2013-2465 is quite exposed to this malware. This security glitch is found in Java u21 and its previous



Targets

Operations

Methods / TTPs / Malware

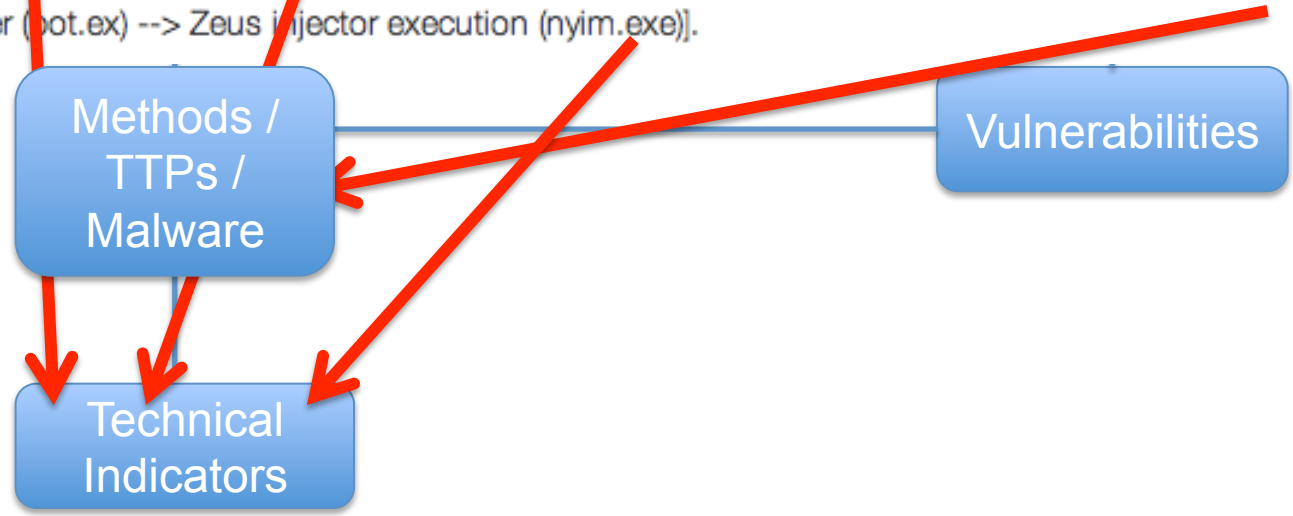
Vulnerabilities

Technical Indicators

Based on the MFT timeline data we can we that at 2012-11-27 23:05:27 the standard info access time of nyim.exe was updated matching the start time of our suspicious process from pslist. Working backwards from that point we quickly can identify several interesting items from the MFT timeline data:

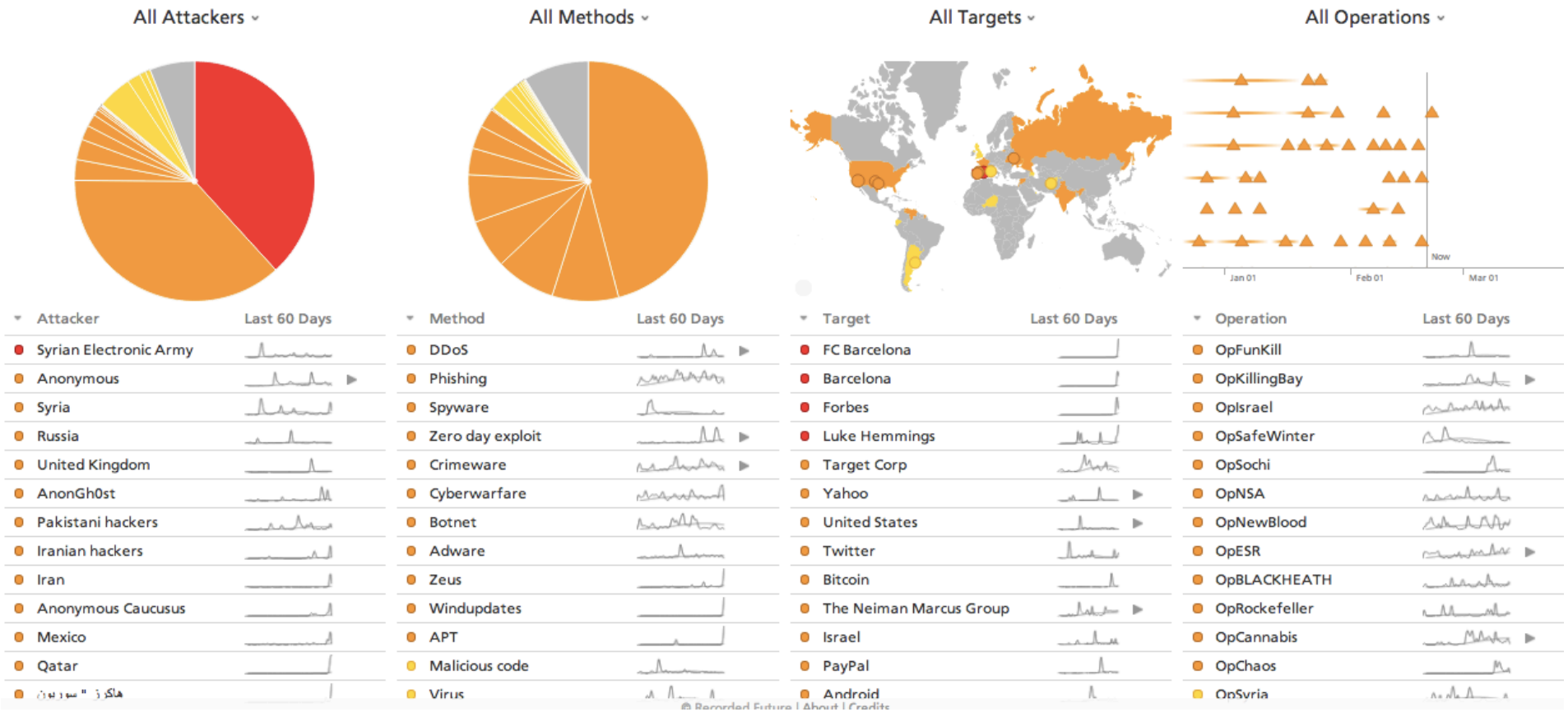
1. The *%APPDATA%/Xapa* and *%APPDATA%/Gabior* directories were created at the same time as our suspicious executable which is located at *%APPDATA%/Giawc/nyim.exe*. Two random directories along with another random directory containing a ".exe" all located within %APPDATA% is a fairly well known IoC for Zeus.
2. We can also see that bot.exe was MACB in the Administrator's desktop folder just before the malware was dropped and the "random" data directories were created.
3. Also, builder\builder\config.txt and builder\builder\zsb.exe seem to indicate that the Zeus builder was extracted based on results from Google for "zsb.exe and config.txt".

A bit farther down in the timeline I also noted the timestamps on the prefetch files ZSBEXE~1.PF, BOTEXE~1.PF and NYIMEX~1.PF. This seems to support the execution order you would suspect with someone testing Zeus [Zeus Builder (zsb.exe) --> Dropper (bot.ex) --> Zeus injector execution (nyim.exe)].

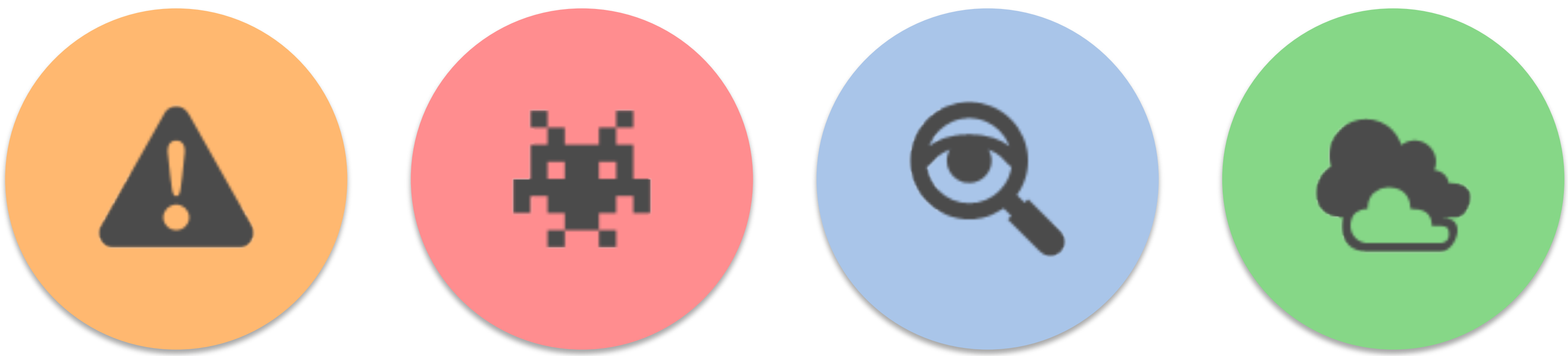


http://traceevidence.blogspot.com/2013/12/the-botmaster-jackcr-122713-memory-image.html

Cyber Intelligence App



Cyber Threat Intelligence Use Cases



Situational Awareness

Investigate Vulnerabilities

Research Actor/Method/Target

Update Threat Forecast

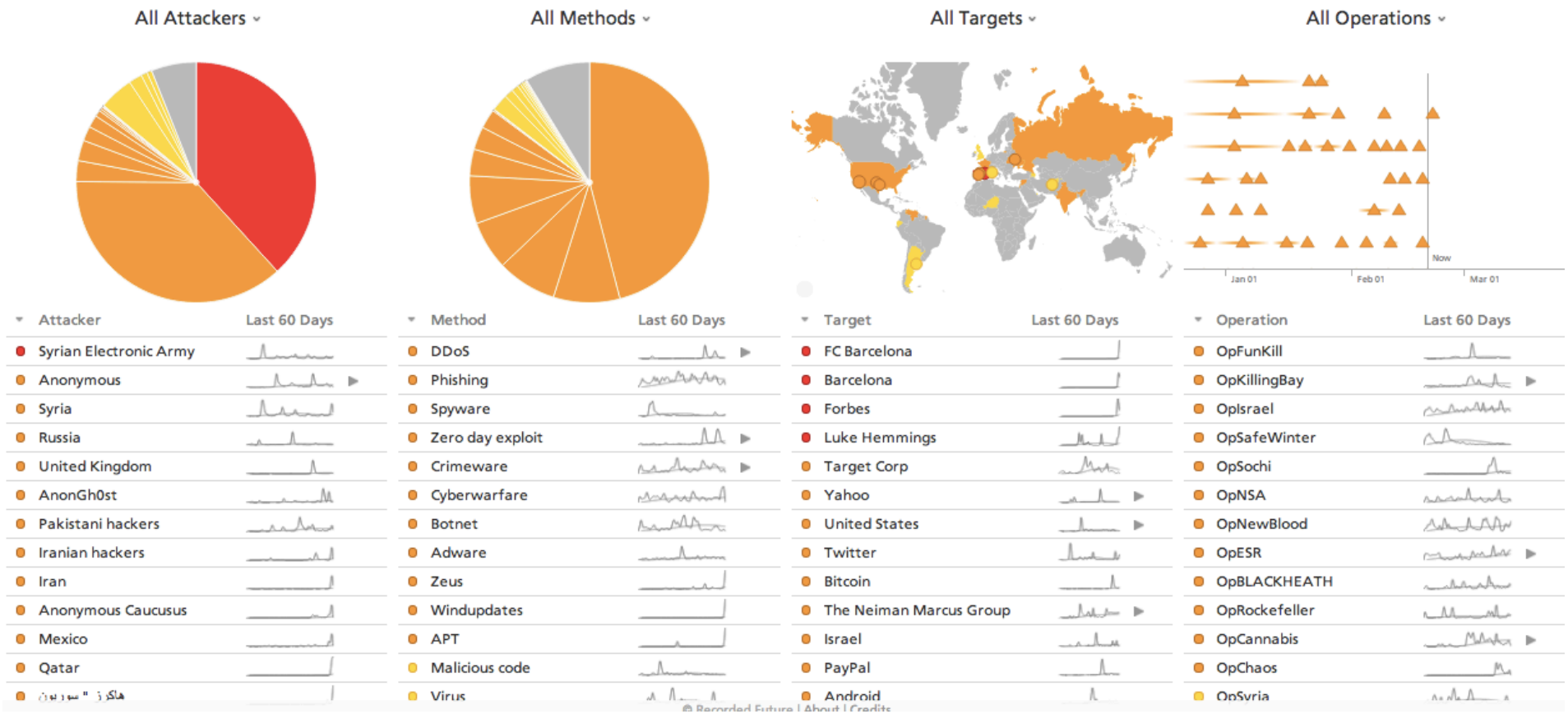
OPERATIONAL ••• STRATEGIC

Recorded Future

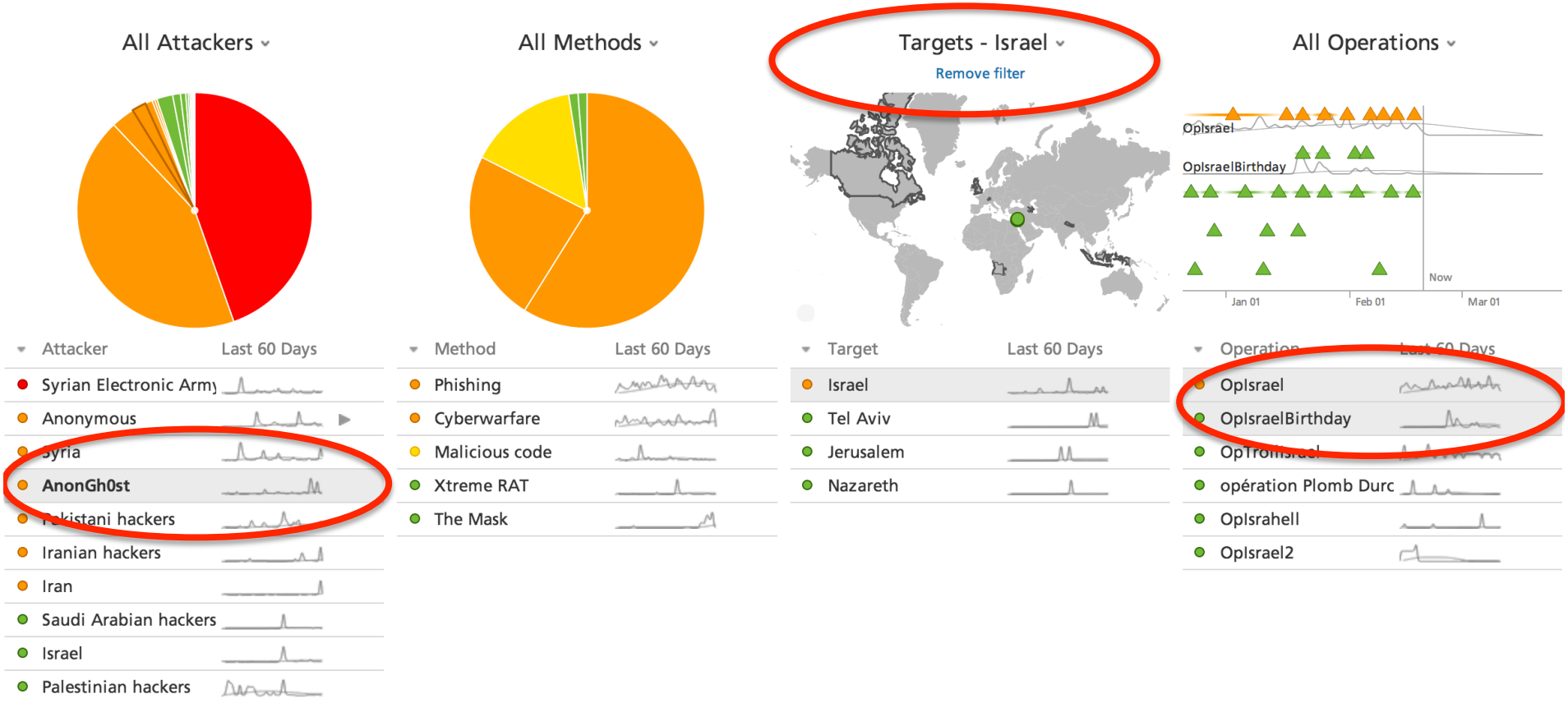
CREATING AN INSIGHTFUL WORLD

Example: Identifying and Understanding OpIsraelBirthday

Cyber Intelligence App

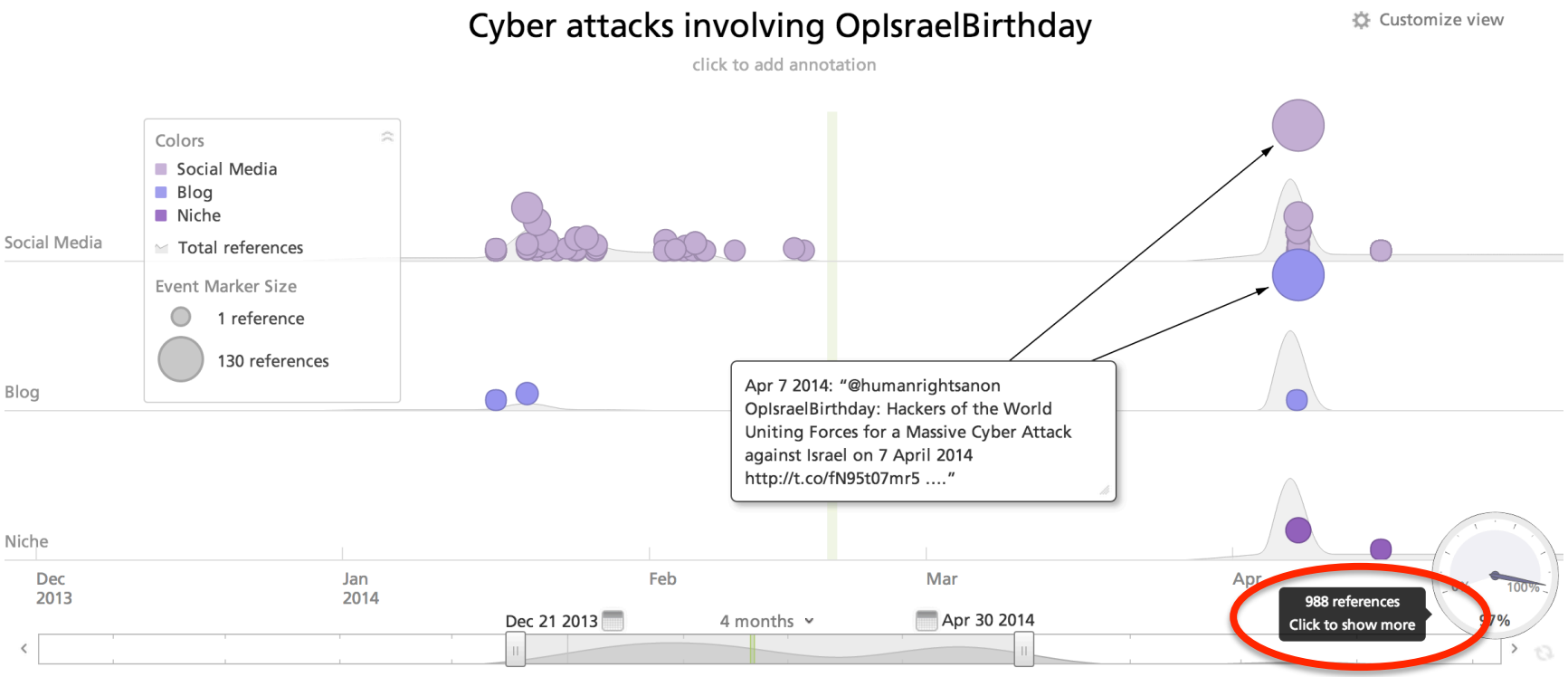


Situational Awareness – focused



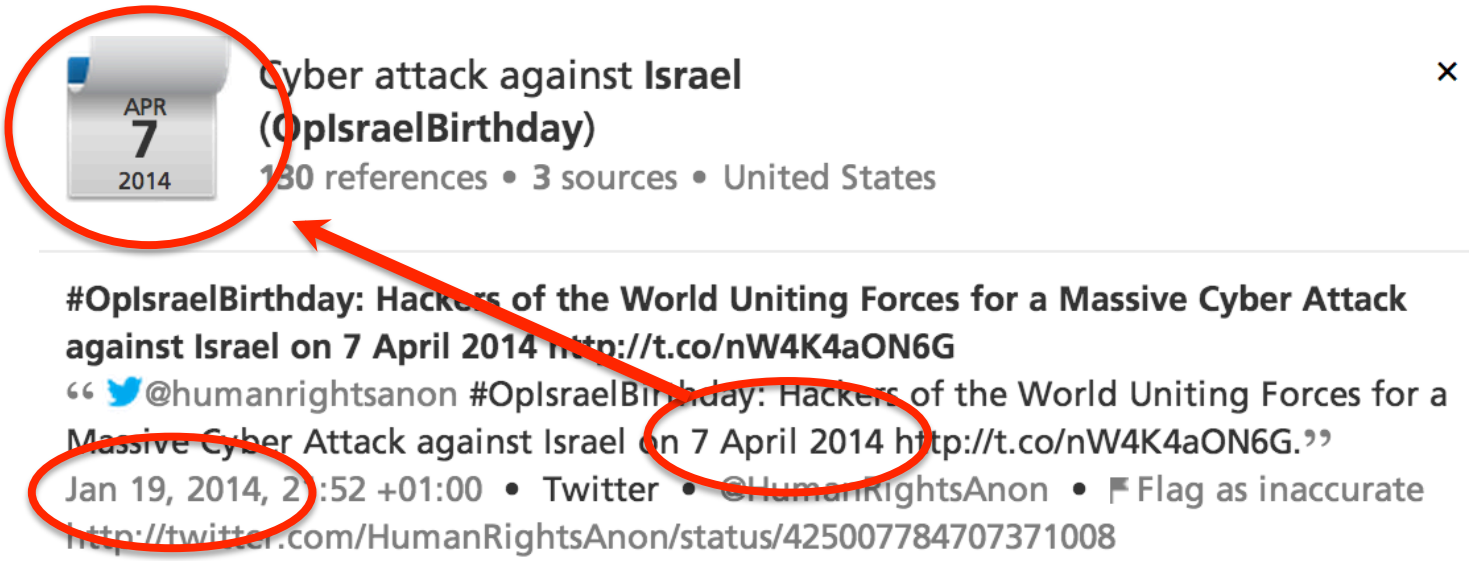
Understanding What's on the Horizon

Once the OpIsraelBirthday Threat is identified, analyzing the information with Recorded Future allows a user to quickly absorb nearly refences pulled from social media and niche open source publication.



How is the data organized?

Recorded Future's Temporal Analytics allows an analysts to see non-obvious future information.



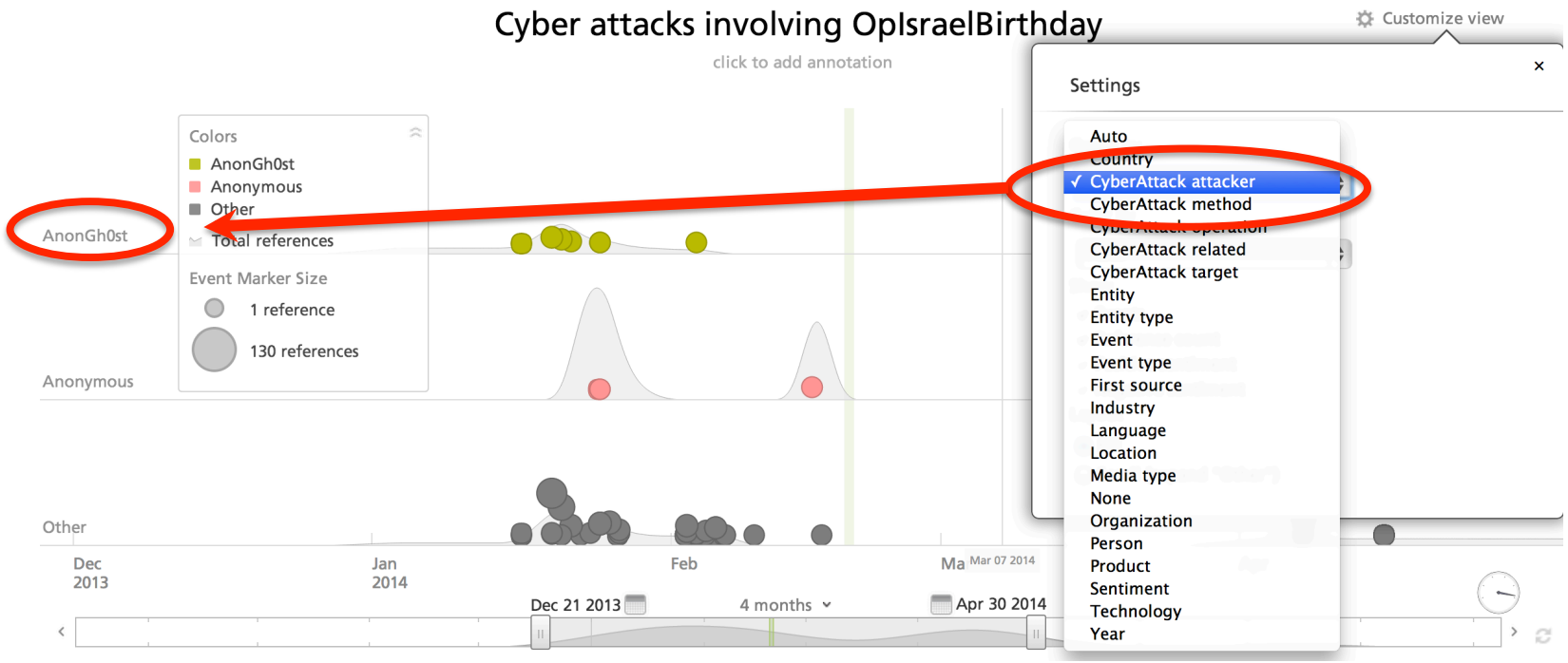
Organizing the Information Allows an Analyst to Unravel the Threat

AnonGhost Launch Op Israel Birthday 07/APRIL/2014

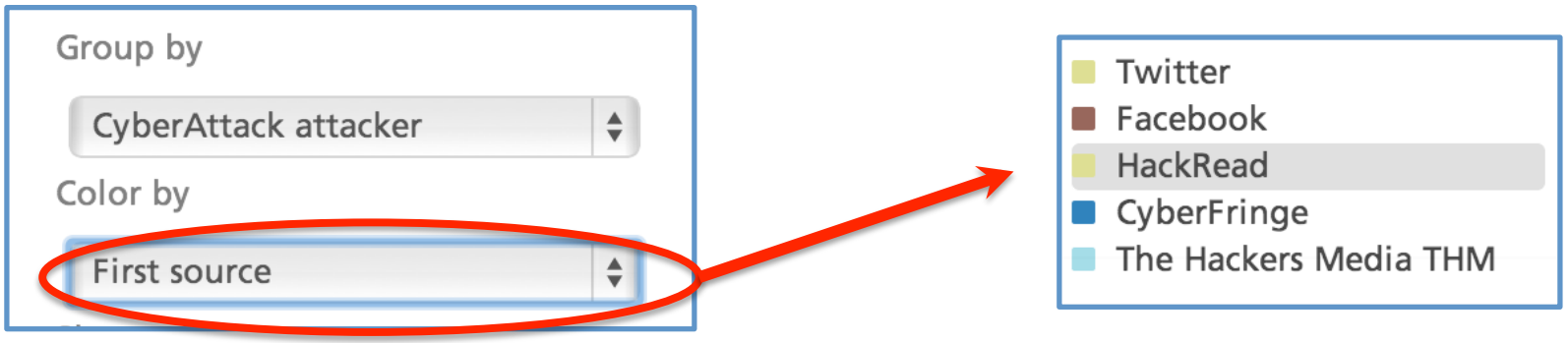
“One of AnonGhost's representative told us that this cyber attack will be conducted under the banner of #OpIsraelBirthday in which every possible Israeli website will be targeted in order to show their solidarity with #Palestine.”

Jan 20, 2014, 22:00 +01:00 • Facebook • Flag as inaccurate

http://www.facebook.com/172486642949943/posts/1397353373850929



Pulling Intelligence from the Information: Identifying OpIsraelBirthday participants.



Currently the teams involved in the operation are: Mauritania Attacker , Virusa Worm, Deto Beiber, Dr.SaM!M_008, M3GAFAB , Extazy007, PhObia_PhOneyz, Mr Domoz, Tak Dikenal, AnonxoxTN, Raka 3r00t, PirateX, Bl4ck Jorozz, Younes Lmaghribi, Indonesian r00t, BlackBase Hacker, CoderSec, h4shcr4ck, Mrlele, Donnazmi, TheGame Attacker, Man Rezpector, SaccaFrazi , Spec Tre, HusseiN98D, HolaKo, Mr.Ajword, Root Max, Egy Eagle, THE GREATEST, BiosTeRminat0r, Man Rezpector, Hani Xavi, Don Maverick, Psyco Hacker , Black Cracker, rummykhan, Root Max, VINUX, ARAFET, TITO_SFAXSIANO and SquiCk H4ck3r

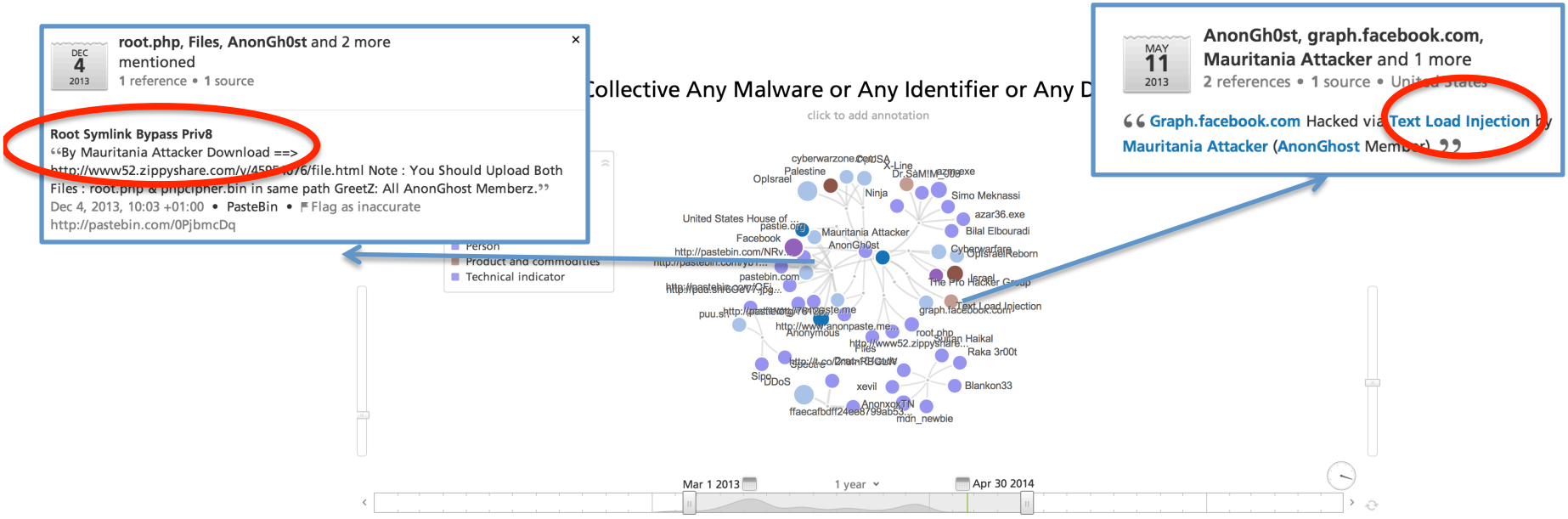
HackRead - Latest Cyber Crime - Information Security - Hacking News

Best Source for Latest Technology, Cyber Crime, Information Security & Hacking News

Identifying Actionable Intelligence

Members of the AnonGh0st collective have been associated with a wide-variety of attacks including **DDoS** and **Text Load Injections** (seen in the developer.facebook.com attack).

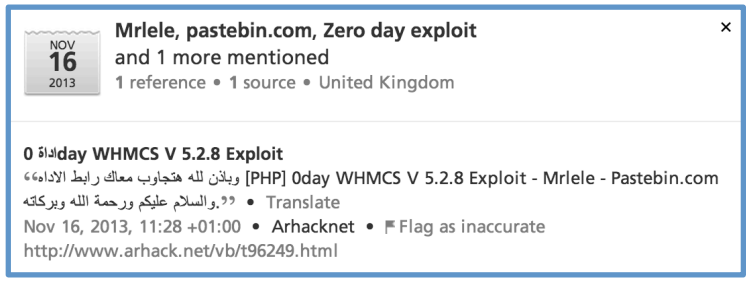
Of note, a tool to move a hacker from “website compromise” to “full root access” was linked to in Pastebin. (Root Symlink Bypass Priv8 By Mauritania Attacker)



Creating a list of OpIsraelBirthday Attackers (from the new HackRead information) allows for additional understanding of the threat.

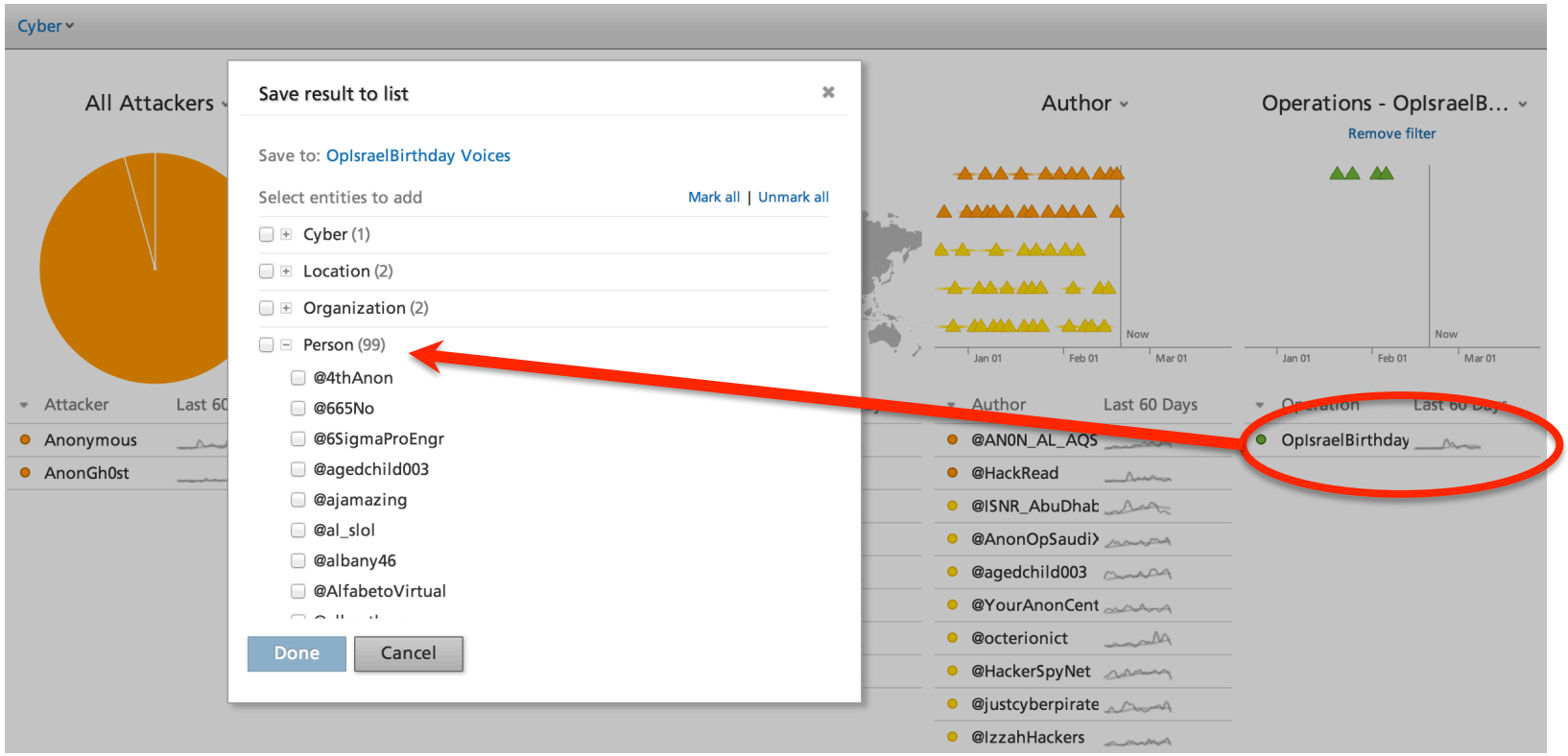
In late 2013, hacker Mrlele posted a 0-day and encouraged followers to use it.

The exploit uses Google dorking **to exploit a “submitticket.php” vulnerablity** on websites hosted by website.com.



Monitor the Threat

Recorded Future's Cyber Application allows a user to identify and monitor Twitter handles involved in the OpIsraelBirthday Discussion over a 90 day period (including 30 days forward into the future).



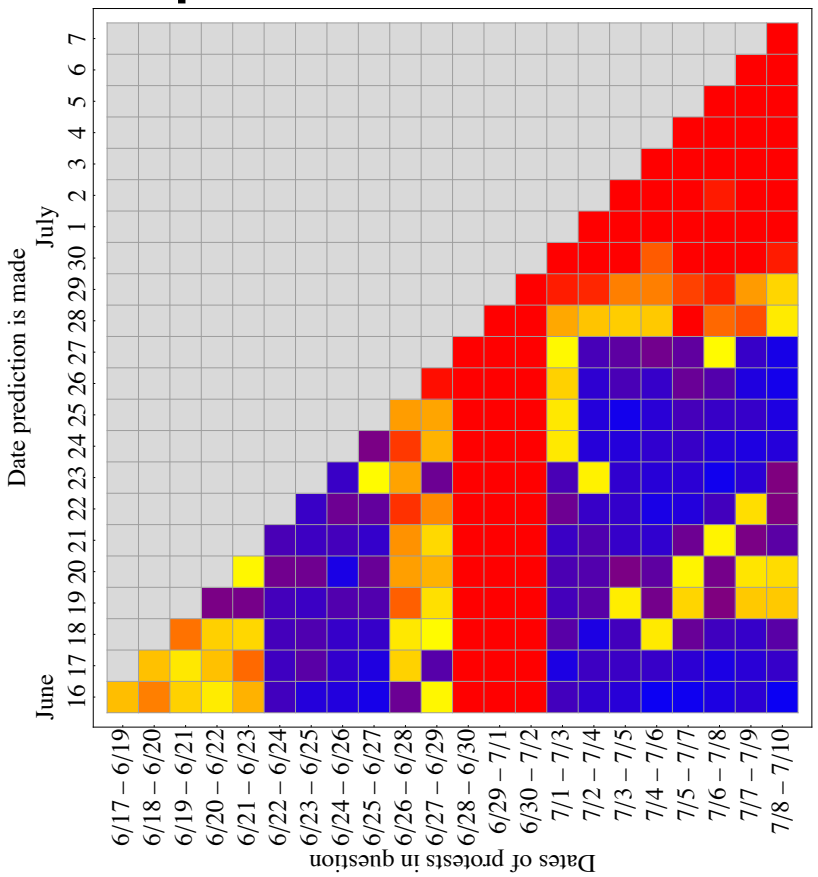
Recorded Future

CREATING AN INSIGHTFUL WORLD

Before that?

Under Attack!

In reality, predictions are probabilistic – like weather reports



truve@recordedfuture.com
www.recordedfuture.com
analysisintelligence.com

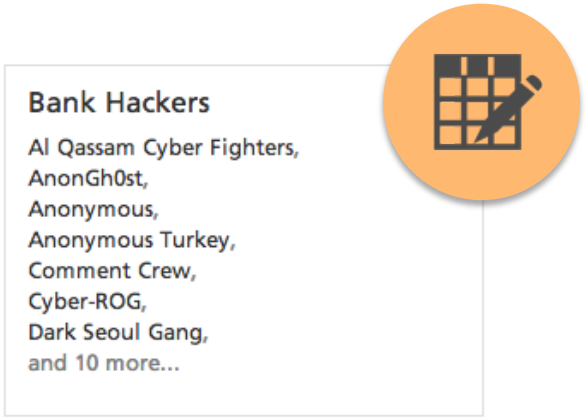
Recorded Future

CREATING AN INSIGHTFUL WORLD

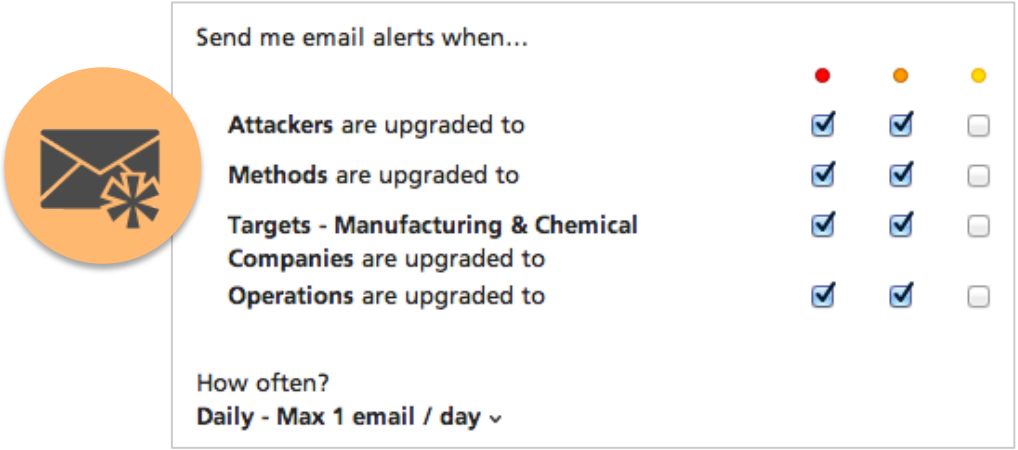
SPARE SLIDES

Situational Awareness

Monitoring + alerting
with real-time analytics



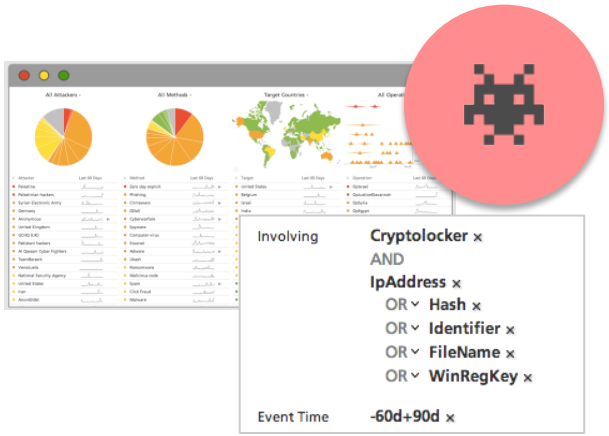
Build customized list of potential
targets, attackers, methods



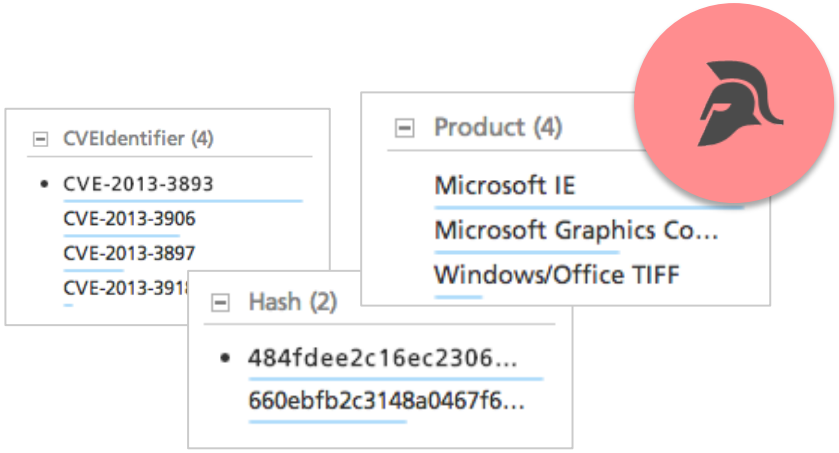
ACTIONABLE OUTCOME

Real-time alerts when
thresholds are crossed

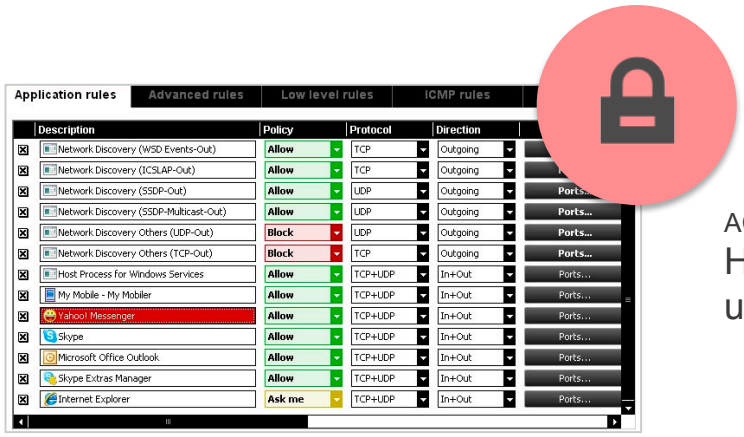
Investigate Vulnerabilities



Automatically surface trending methods of attack, or search for a known vulnerability



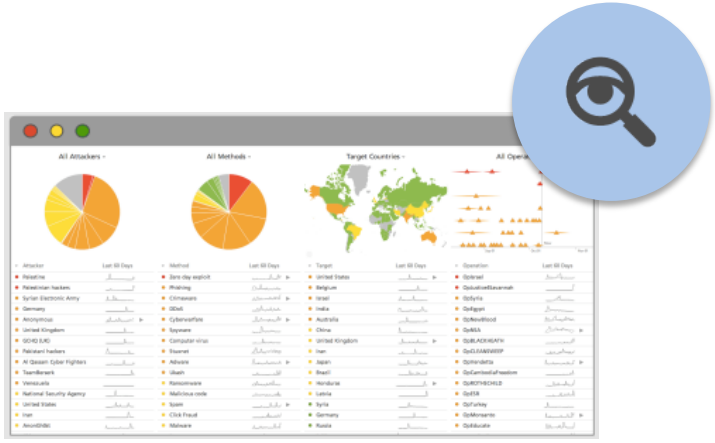
Quickly identify current technical indicators, affected products



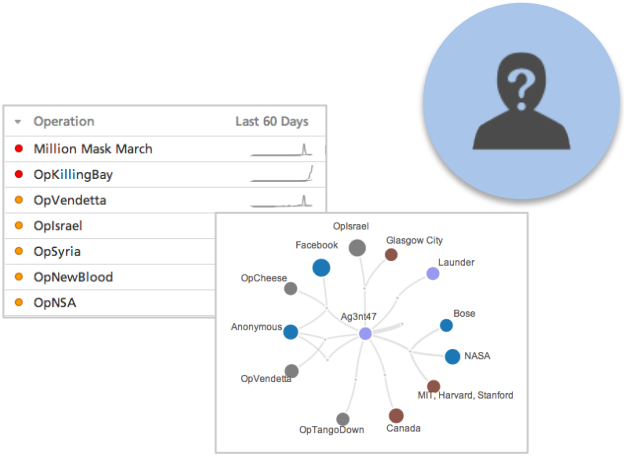
ACTIONABLE OUTCOME

Harden network defenses, update IPS rules

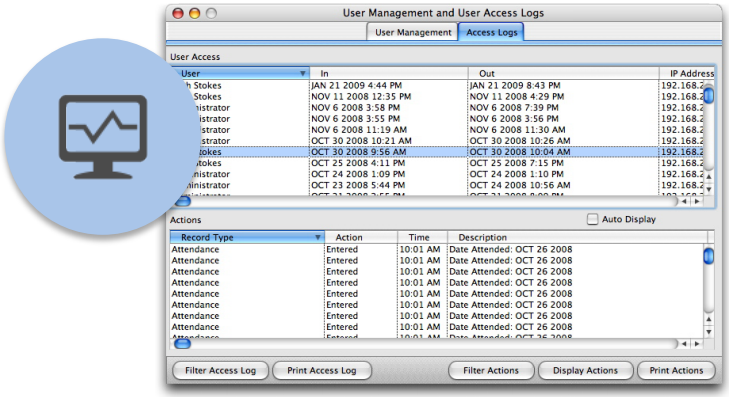
Research Actors, Methods, & Targets



Research and identify trends
across 5 yr archive, 7 languages



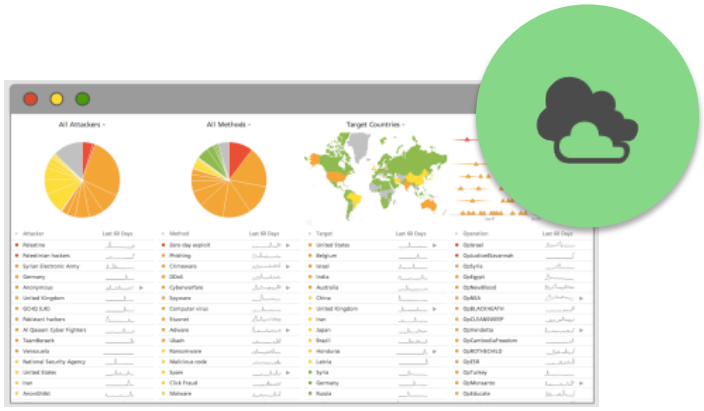
Early detection of campaigns against
industry, suppliers, partners



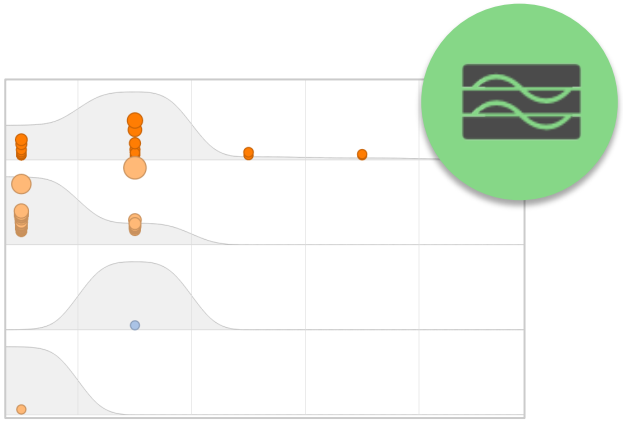
ACTIONABLE OUTCOME

Secure & monitor likely
target accounts

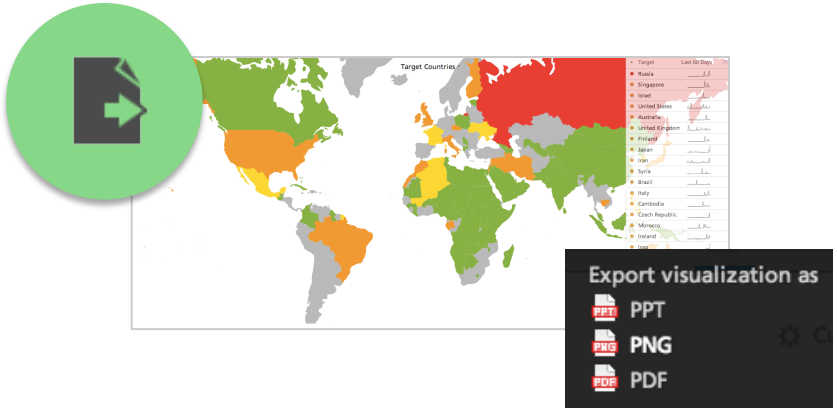
Update Threat Forecast



Identify upcoming events, both real-world and virtual



Correlate patterns and trends to current, upcoming, & past events



ACTIONABLE OUTCOME

Share outlook with CSO, management, peers, LOB execs

Developer Edition API

- Extensive server API
  - R, Python, Java, etc.
  - Palantir, i2, Maltego
  - Spotfire, Splunk
- Embed interactive views
  - Analytic dashboards
  - Portals

{JSON}