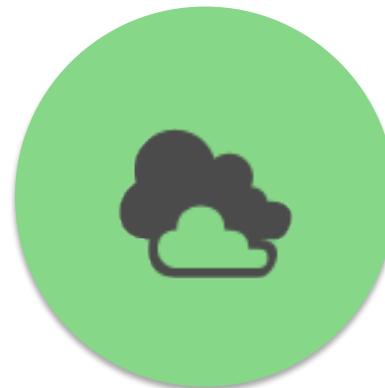
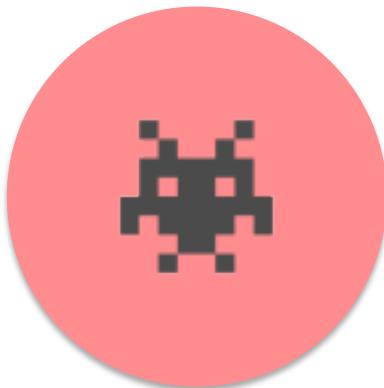




# Cyber Threat Intelligence

“Cloudy, with a risk of cyber attacks”

Staffan Truvé, PhD  
Co-founder / CTO  
[truve@recordedfuture.com](mailto: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



Cyber Monitoring



Executive Monitoring



Organization Monitoring



# #7

## The 15 Biggest Excesses in Google History

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

8+1 1

Like 4

Tweet 41

10 OF 16



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

COMPANY CONFIDENTIAL



# #1

## The 15 Biggest Excesses in Google History

BY BRENDEN GALLAGHER | FEB 19,

8+1 1 Like 4 Tweet



Image via Grand Youth

### Predicting the Future

The investment team at Google's X division is a company that attempts to create the future. It has paid off, as Recorded Future is now a major part of Google's base. From what we can tell,

## The 15 Biggest Excesses in Google History

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

8+1 1 Like 4 Tweet 41

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.

COMPANY CONFIDENTIAL

# Why am I here?

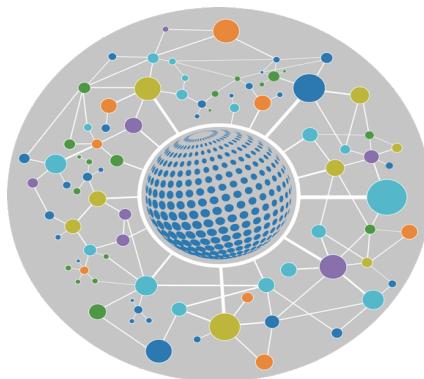
*“In cyber security the web balances being the platform to create attacks and being the source of information to prevent attacks”*

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

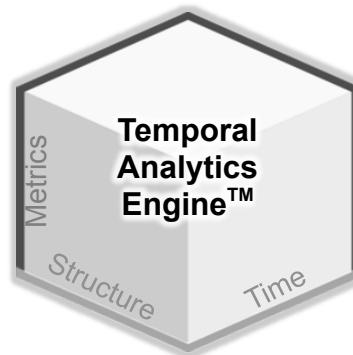


# Web Intelligence

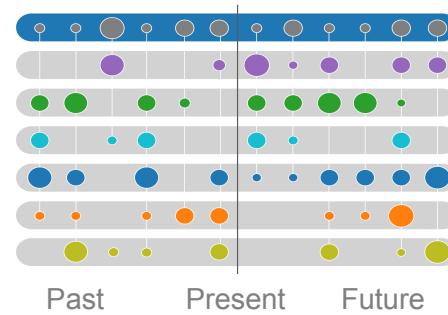
UNSTRUCTURED  
TEXT



ORGANIZED FOR  
ANALYSIS



YIELDS NEW  
INSIGHTS



APPLICATIONS



API

COMPANY CONFIDENTIAL

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 (OplsraelReborn)  
52 references • 2 sources • United States

“ Hackers joining venture for #OplsraelReborn, 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

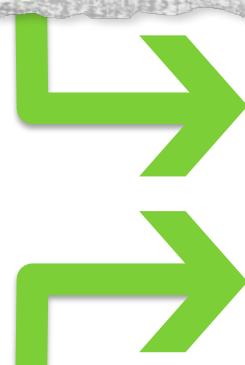
“ Congo's U.N. mission, MONUSCO, said two mortar bombs fired by M23 struck the Ndosho neighborhood of Goma - a city of 1 million people - on Saturday morning, killing three civilians ”

# 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, Intentions, 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

COMPANY CONFIDENTIAL



# 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**

" @thamilnatdell 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?

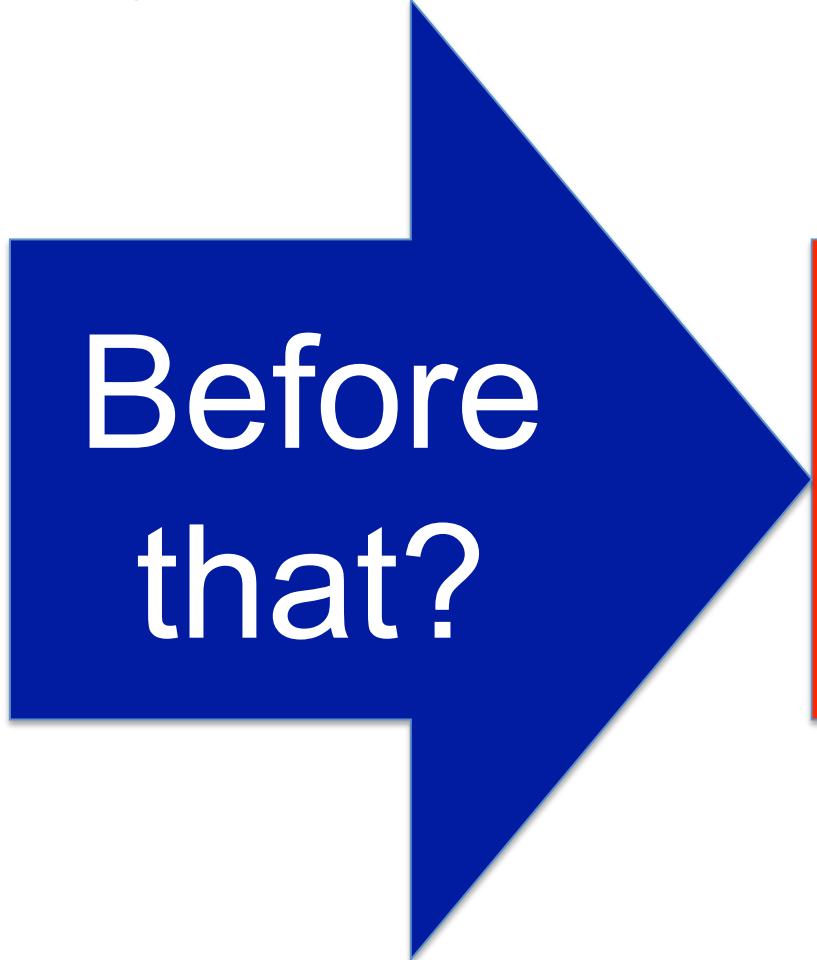


Under  
Attack!

COMPANY CONFIDENTIAL



# Why am I here?



Before  
that?



Under  
Attack!

COMPANY CONFIDENTIAL



# Why am I here?

Protests against me

Before  
that:

Attacks against  
others like me

Exposed vulnerabilities  
in my infrastructure

Under  
Attack!



# 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



Twitter and 1 more reported about

## Cyber attack against India on Aug 14, 2013

“ [@thamilonatdell](#) 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

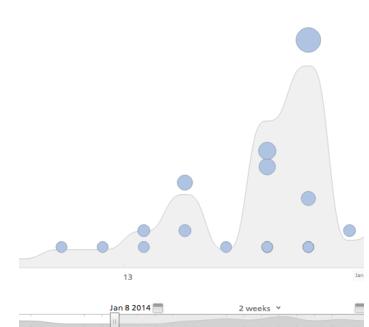
“ Pakistani Hackers Threaten to Attack India on August 14. ”

Jul 17, 2013 12:08 Team Cymru Internet Security News

Flag as inaccurate

Cyber "POS"

click to add annotation



▼ Target

Last 60 Days

Vodafone



Nokia



Sprint Nextel Corp



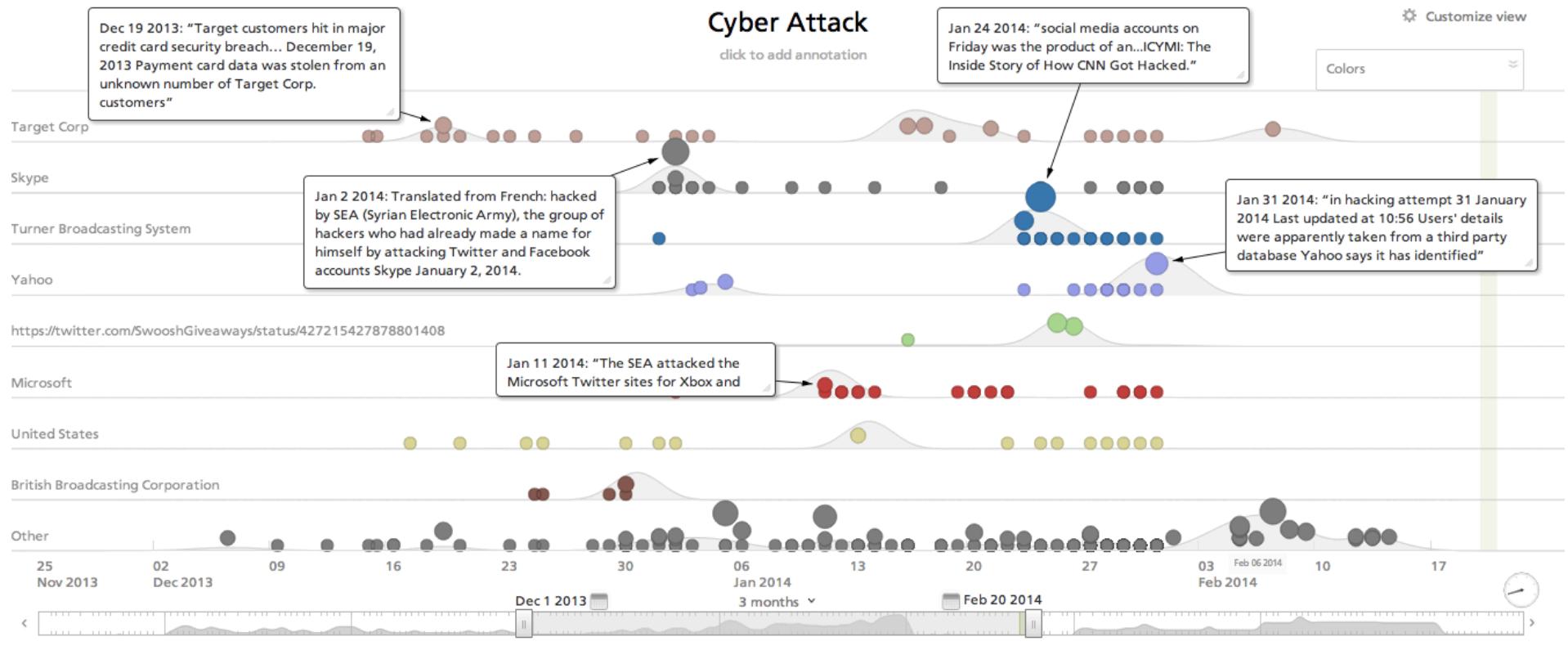
AT&T



BlackBerry



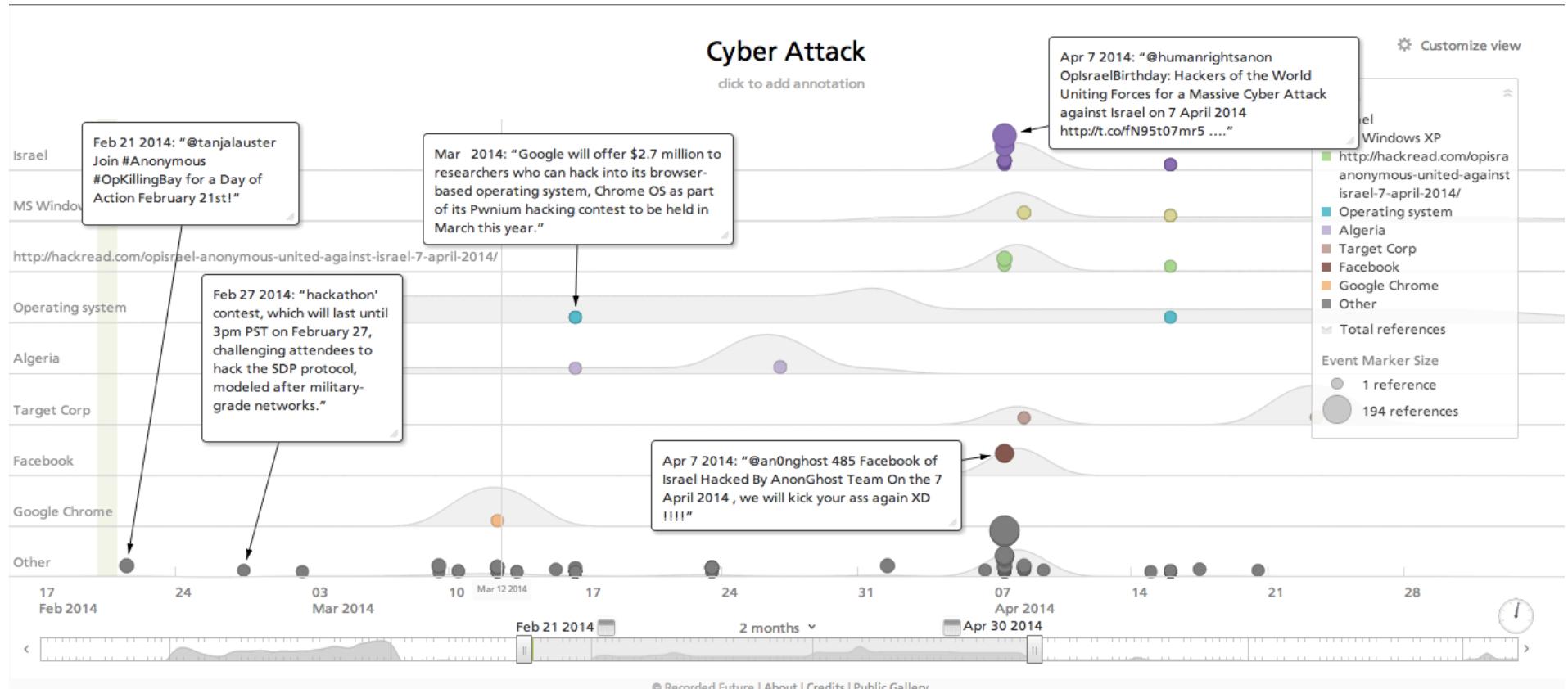
# Rear mirror



COMPANY CONFIDENTIAL



# Future?



COMPANY CONFIDENTIAL

## 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

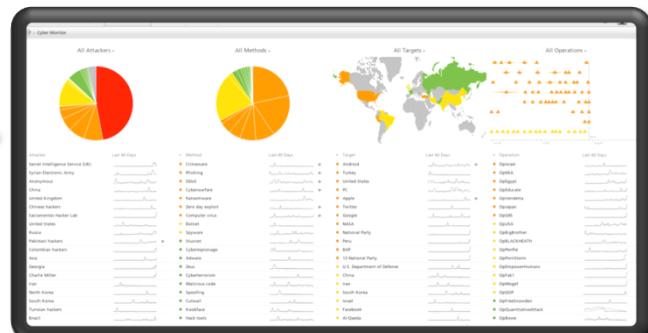
Security firms: RSA, McAfee, Verisign, Symantec, Cisco  
Exploits & metadata: Spamhaus, Malwr.com, ShodanHQ

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



Palantir  
ArcSight

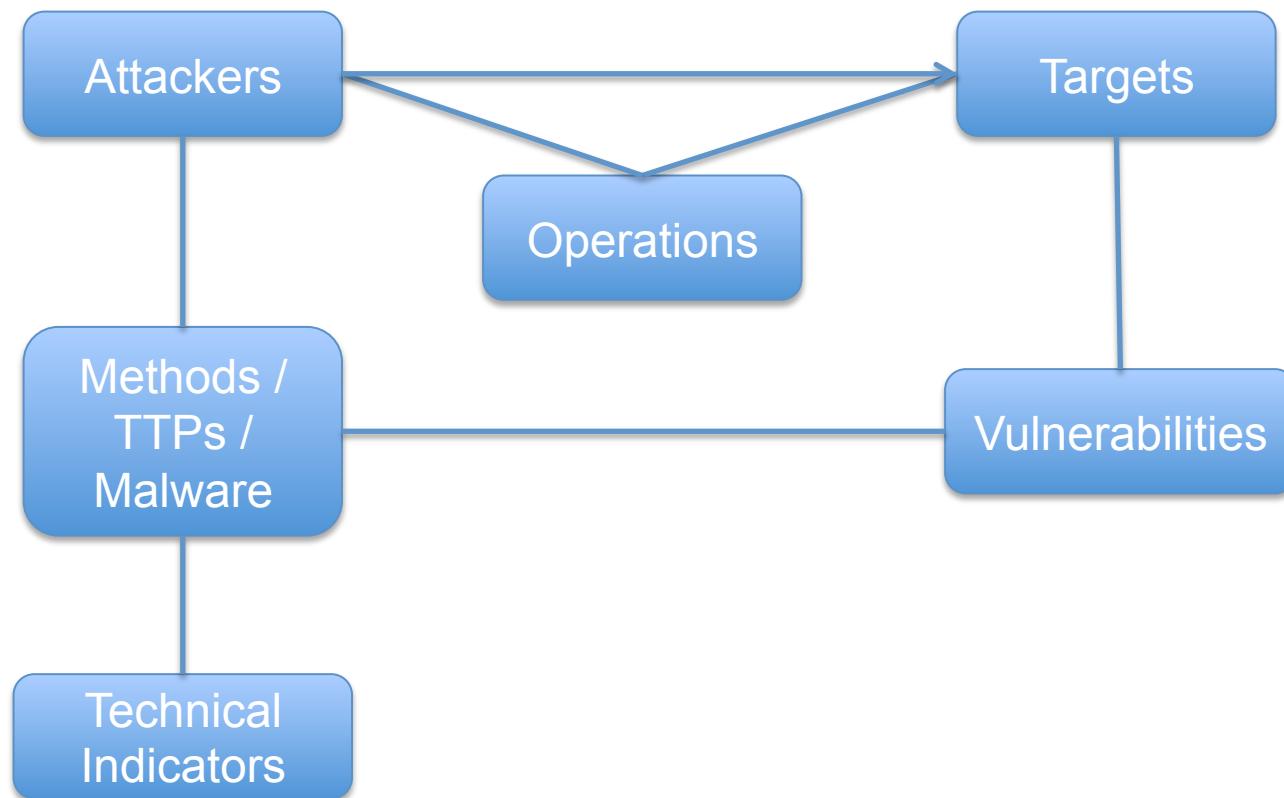
MALTEGO

splunk>  
R Spotfire®

COMPANY CONFIDENTIAL

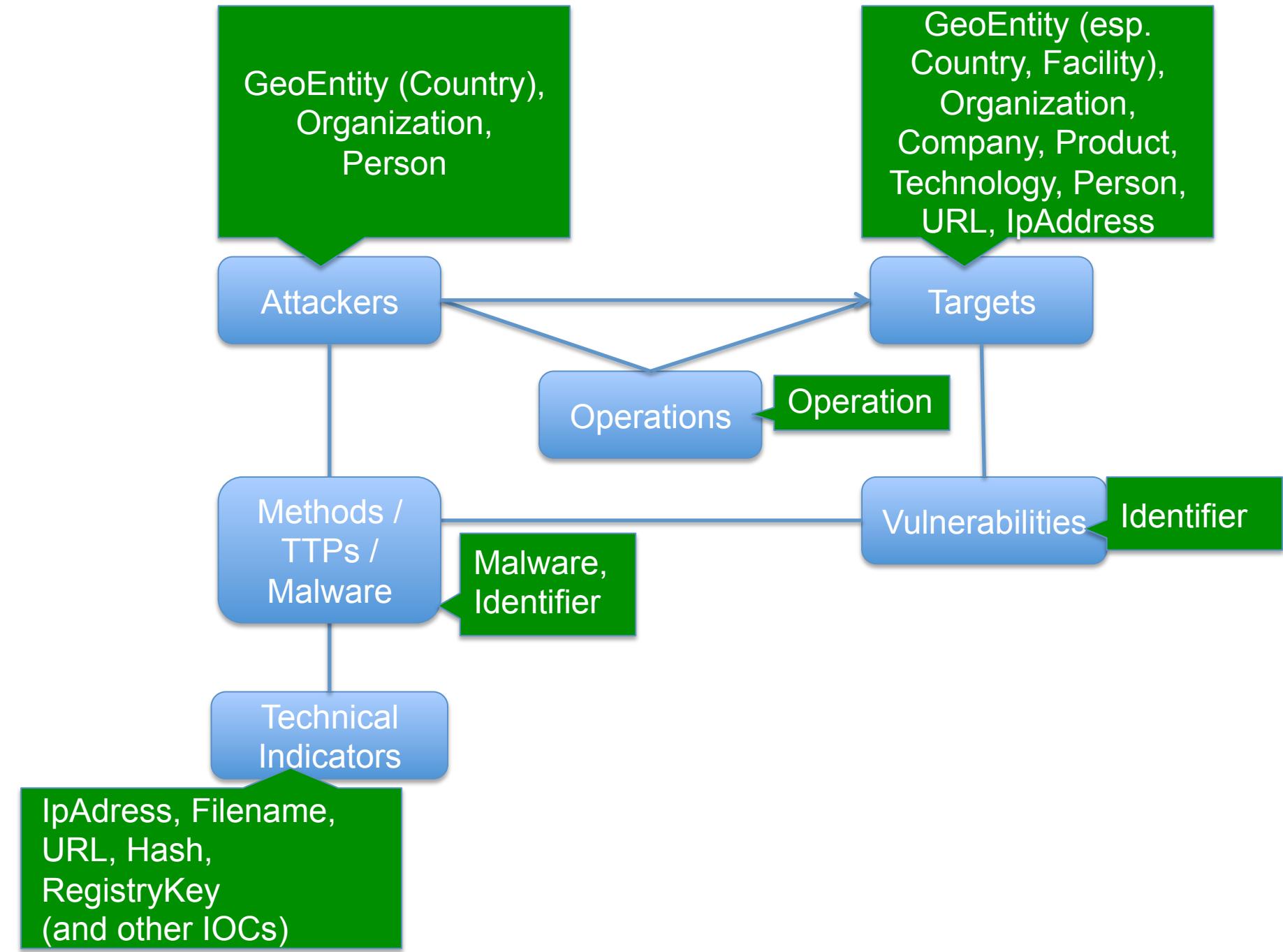


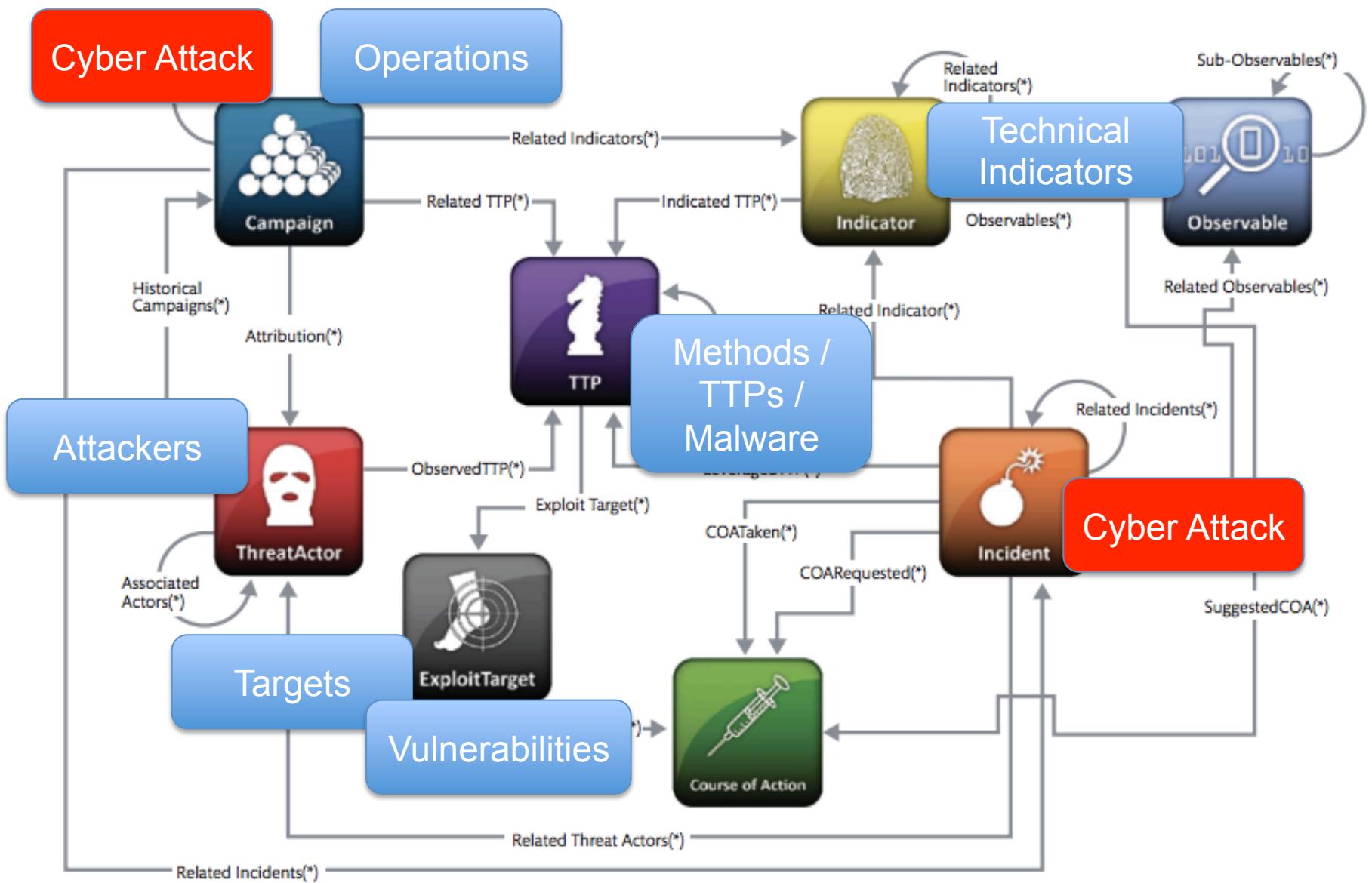
# Anatomy of a Cyber Attack



COMPANY CONFIDENTIAL







STIX Architecture





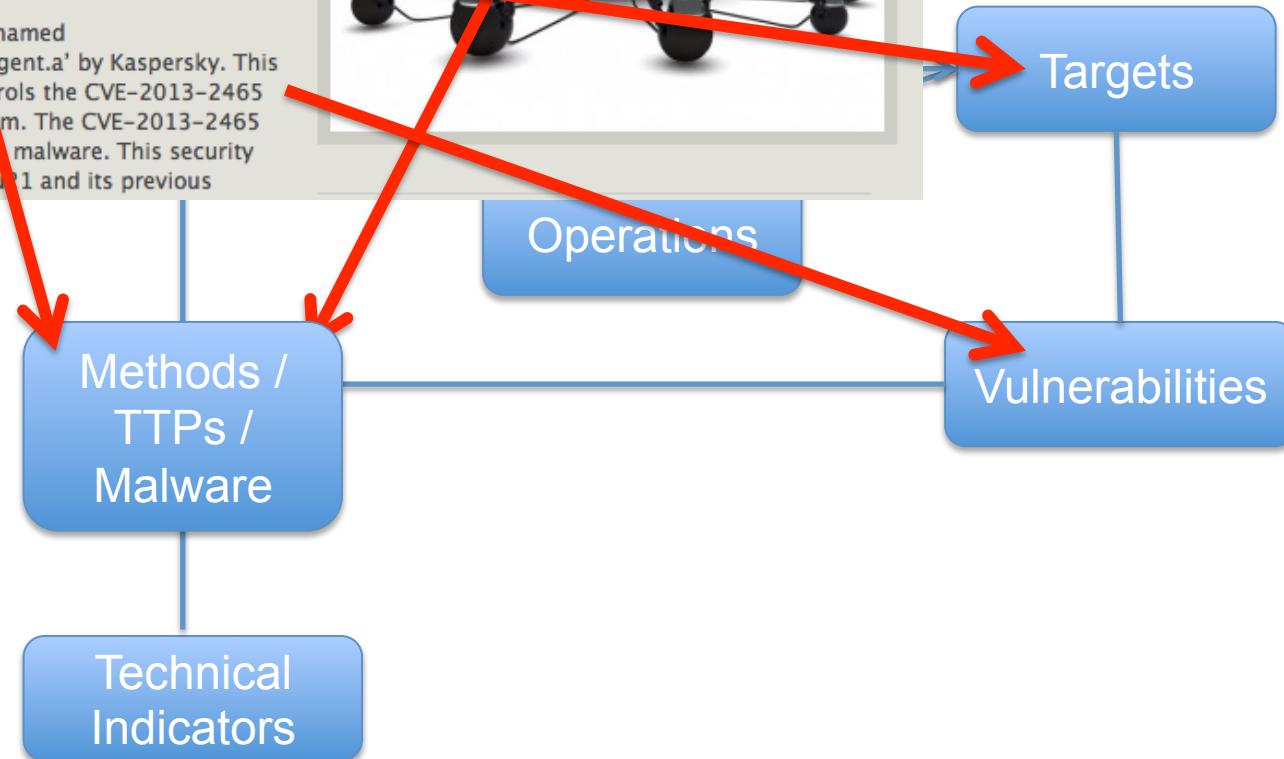
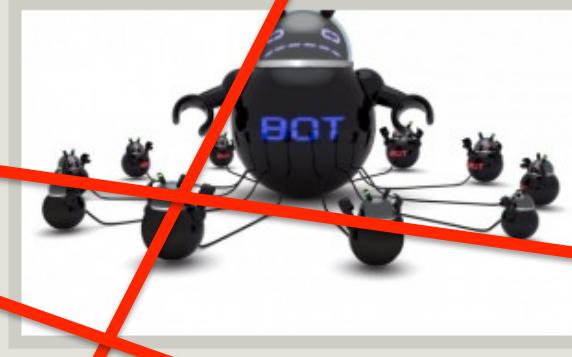
# Kaspersky identifies lethal cross platform Java DDoS botnet

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.

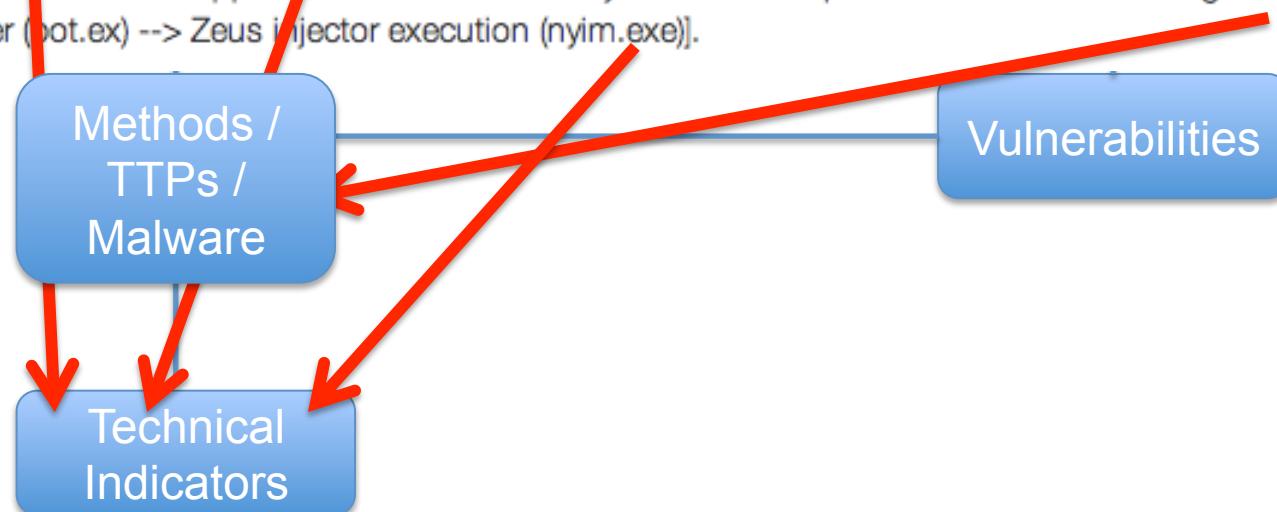
This cross platform is named 'HEUR:Backdoor.Java.Agent.a' by Kaspersky. This malware basically controls the CVE-2013-2465 and damages the system. The CVE-2013-2465 is quite exposed to this malware. This security glitch is found in Java v11 and its previous



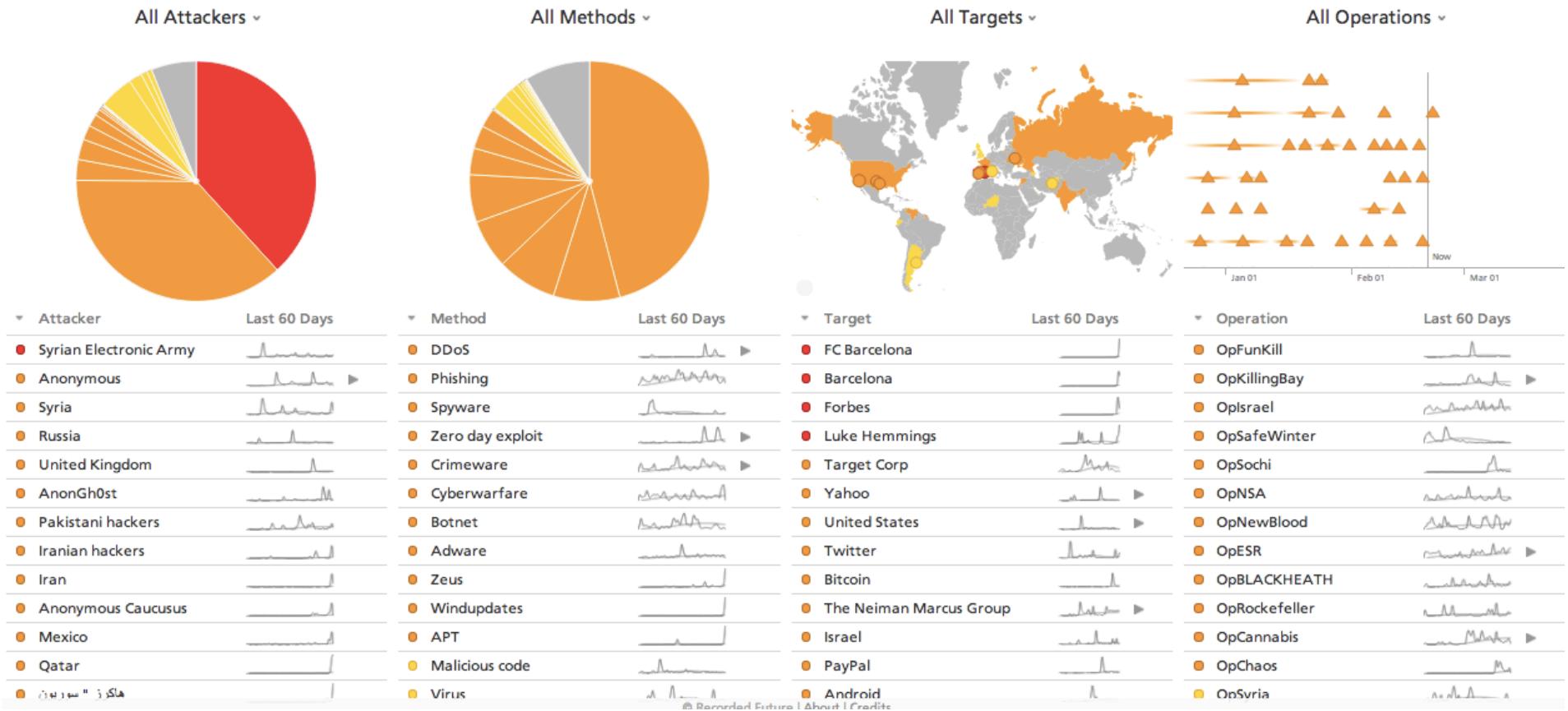
Based on the MFT timeline data we can see that at 2012-11-27 23:05:27 the standard info access time of nyim.exe was updated matching the start time of our suspicious process from pslist. Working backwards from that point we quickly can identify several interesting items from the MFT timeline data:

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.exe) --> Zeus injector execution (nyim.exe)].



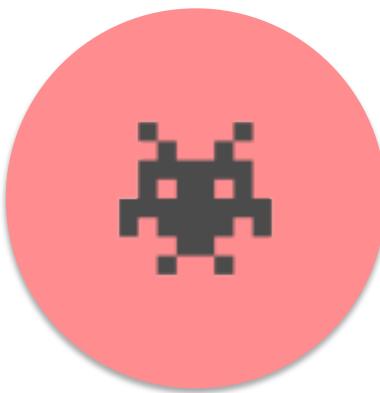
# Cyber Intelligence App



# Cyber Threat Intelligence Use Cases



Situational  
Awareness



Investigate  
Vulnerabilities



Research  
Actor/Method/Target



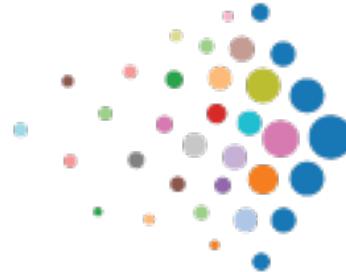
Update  
Threat Forecast

OPERATIONAL



STRATEGIC





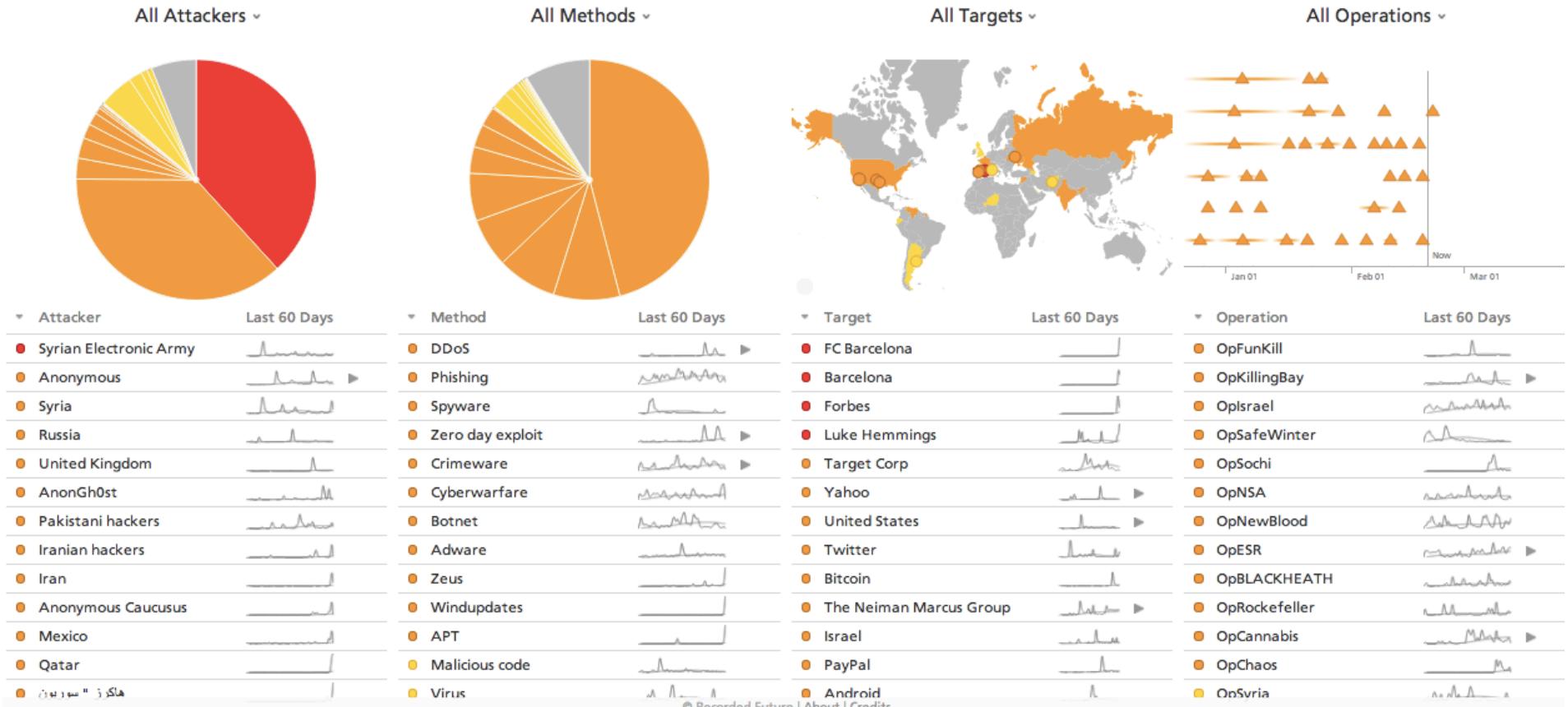
**Recorded Future**  
CREATING AN INSIGHTFUL WORLD



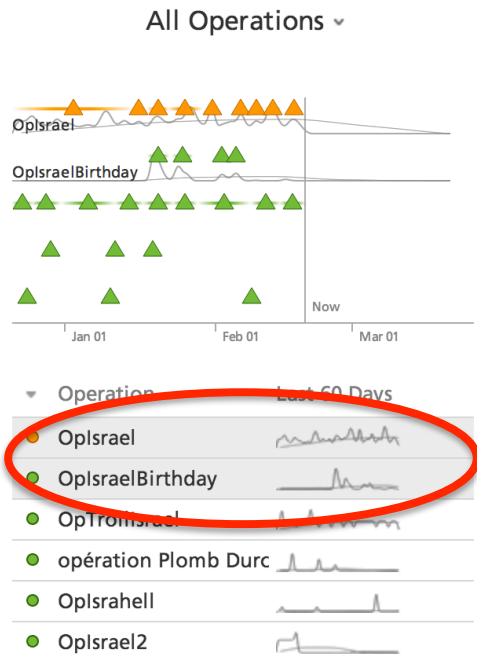
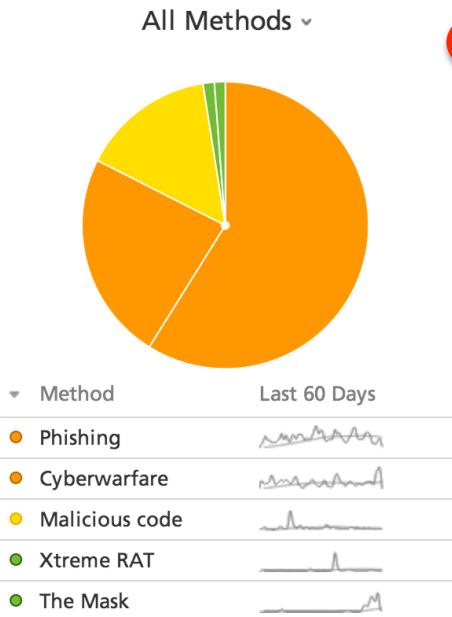
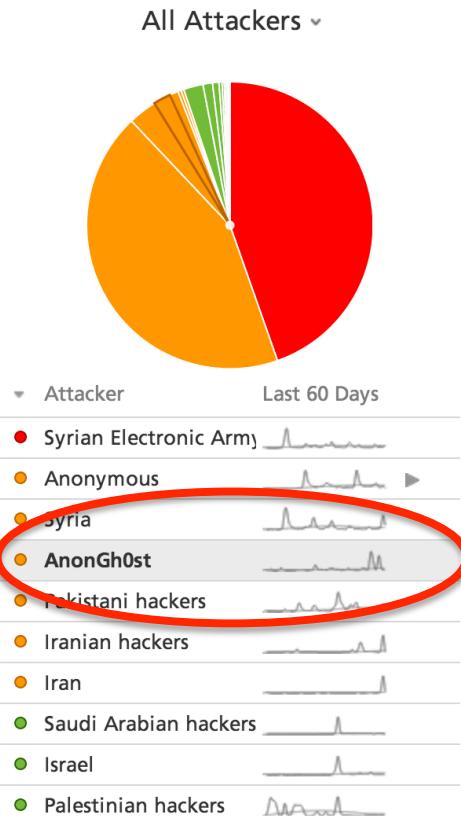
Example: Identifying and  
Understanding OplsraelBirthday



# Cyber Intelligence App

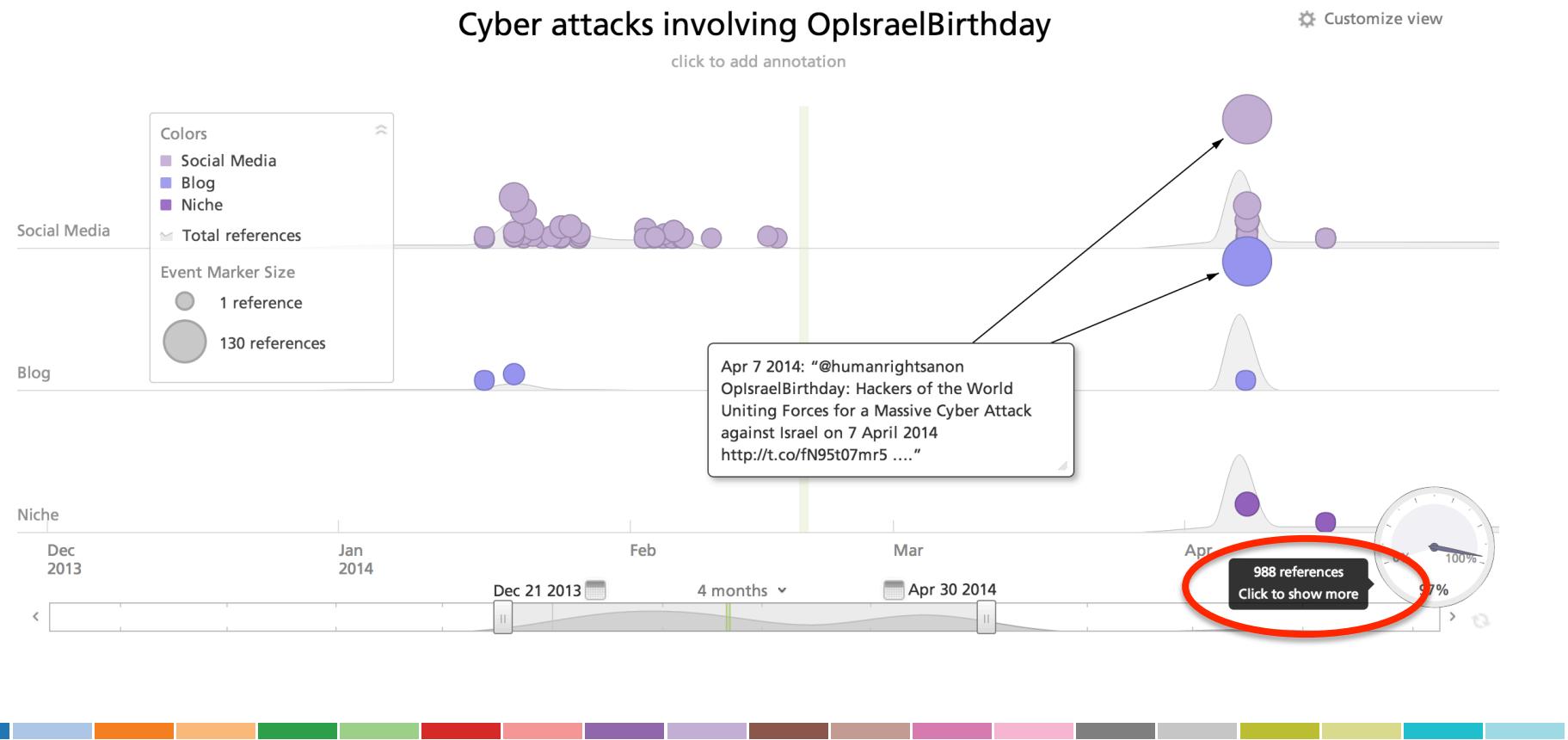


# Situational Awareness – focused



# Understanding What's on the Horizon

Once the OplsraelBirthday Threat is identified, analyzing the information with Recorded Future allows a user to quickly absorb nearly references 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.

The screenshot shows a timeline entry for a cyber attack. A red circle highlights the date 'APR 7 2014' on a calendar icon. A red arrow points from this circle to the text below. The text reads: 'Cyber attack against Israel (OplsraelBirthday) 130 references • 3 sources • United States'. Below this, another red circle highlights the date 'Jan 19, 2014, 21:52 +01:00' in a tweet from '@humanrightsanon'. The tweet content is also circled in red: '#OplsraelBirthday: Hackers of the World Uniting Forces for a Massive Cyber Attack against Israel on 7 April 2014 http://t.co/nW4K4aON6G'. The URL 'http://t.co/nW4K4aON6G' is also circled in red.

Cyber attack against Israel  
(OplsraelBirthday)  
130 references • 3 sources • United States

#OplsraelBirthday: Hackers of the World Uniting Forces for a Massive Cyber Attack  
against Israel on 7 April 2014 http://t.co/nW4K4aON6G

“@humanrightsanon #OplsraelBirthday: Hackers of the World Uniting Forces for a  
Massive Cyber Attack against Israel on 7 April 2014 http://t.co/nW4K4aON6G.”

Jan 19, 2014, 21:52 +01:00 • Twitter • @HumanRightsAnon • Flag as inaccurate  
<http://twitter.com/HumanRightsAnon/status/425007784707371008>



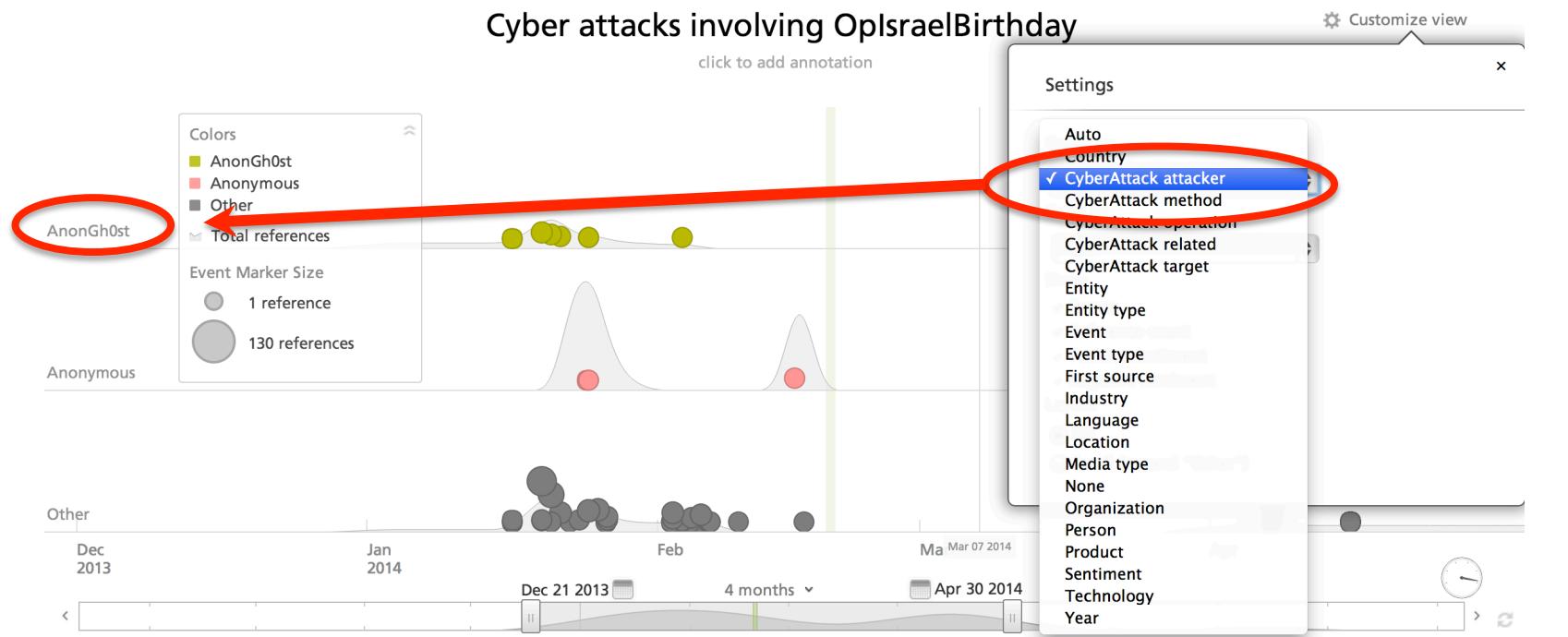
# Organizing the Information Allows an Analyst to Unravel the Threat

## 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 #OplsraelBirthday 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 OplsraelBirthday participants.

The screenshot shows a user interface for pulling intelligence from information. On the left, there are two dropdown menus: "Group by" set to "CyberAttack attacker" and "Color by" set to "First source". A red arrow points from the "Color by" dropdown to a legend on the right. The legend lists five sources with corresponding color swatches: Twitter (light yellow), Facebook (brown), HackRead (light green), CyberFringe (dark blue), and The Hackers Media THM (teal). Below the legend is a large text box containing a list of participant names, which is also circled in red. The text box reads:

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

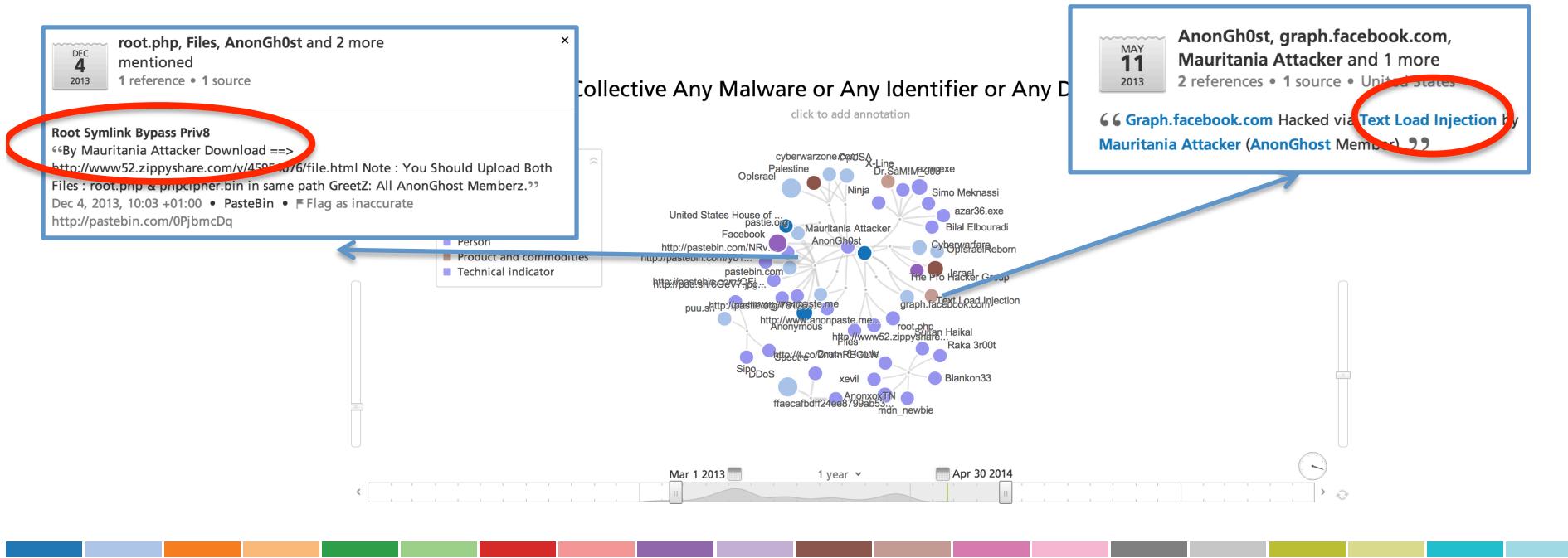


# Identifying Actionable Intelligence

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 OplsraelBirthday 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” vulnerability** on websites hosted by website.com.

Mrlele, pastebin.com, Zero day exploit  
and 1 more mentioned  
1 reference • 1 source • United Kingdom

Nov 16 2013

0day WHMCS V 5.2.8 Exploit  
[PHP] ويذن لله هتجاوب معاك رابط الاداء  
• Translate  
Nov 16, 2013, 11:28 +01:00 • Arhacknet • Flag as inaccurate  
<http://www.arhack.net/vb/t96249.html>



WHMCS Auto Xploiter (0day)  
[For WHMCS ver. <= 5.2.8]

Google Dork: `inurl:submitticket.php` Xploit!

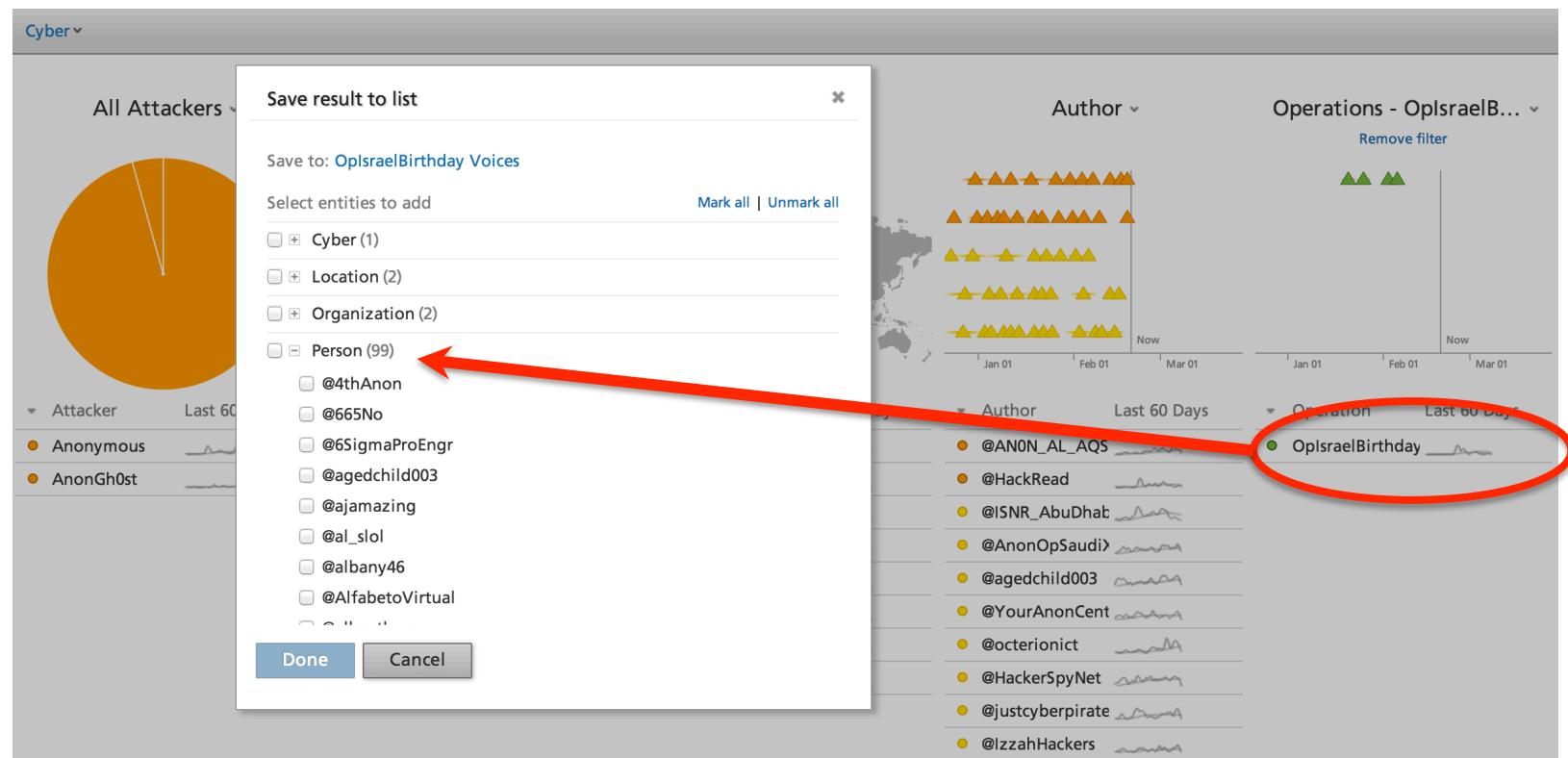
Coded by: g00n | Skype: t3hg00n

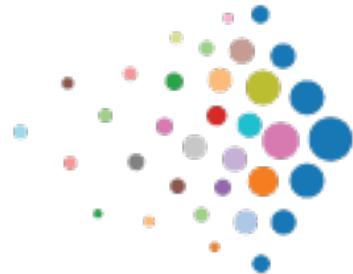
For more tools/scripts/exploits/etc.  
visit [www.Xploiter.net](http://www.Xploiter.net)



# Monitor the Threat

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





**Recorded Future**  
CREATING AN INSIGHTFUL WORLD

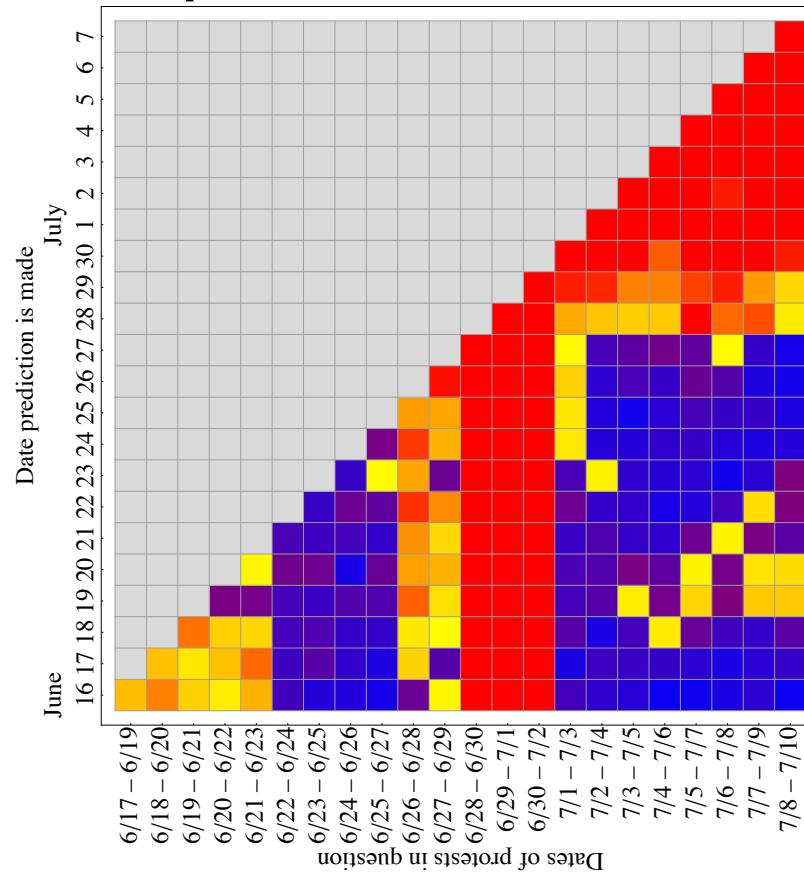
Before  
that?

Under  
Attack!

COMPANY CONFIDENTIAL



# In reality, predictions are probabilistic – like weather reports



[truve@recordedfuture.com](mailto:truve@recordedfuture.com)

[www.recordedfuture.com](http://www.recordedfuture.com)

[analysisintelligence.com](http://analysisintelligence.com)

COMPANY CONFIDENTIAL





# SPARE SLIDES



# Situational Awareness



Monitoring + alerting  
with real-time analytics



## Bank Hackers

AI Qassam Cyber Fighters,  
AnonGh0st,  
Anonymous,  
Anonymous Turkey,  
Comment Crew,  
Cyber-ROG,  
Dark Seoul Gang,  
and 10 more...



Build customized list of potential  
targets, attackers, methods



Send me email alerts when...

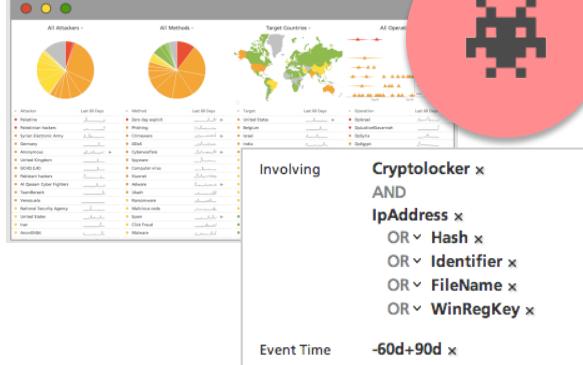
**Attackers** are upgraded to     
**Methods** are upgraded to     
**Targets - Manufacturing & Chemical**     
**Companies** are upgraded to     
**Operations** are upgraded to

How often?  
Daily - Max 1 email / day ▾

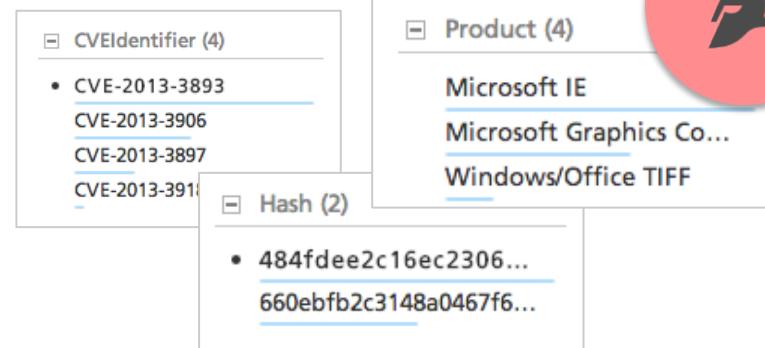


ACTIONABLE OUTCOME  
Real-time alerts when  
thresholds are crossed

# Investigate Vulnerabilities



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



Quickly identify current technical indicators, affected products

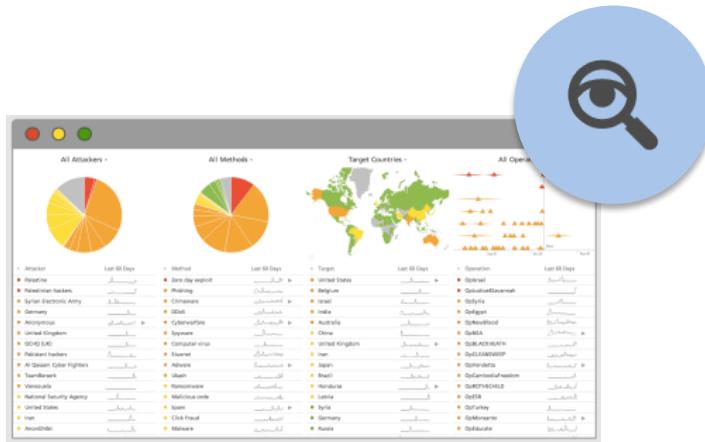
A screenshot of a network policy configuration interface. It shows a table with four columns: 'Description', 'Policy', 'Protocol', and 'Direction'. The 'Description' column lists various applications and services. The 'Policy' column includes 'Allow', 'Block', and 'Ask me' options. The 'Protocol' column specifies TCP, UDP, or both. The 'Direction' column indicates Outgoing or In+Out traffic. A red circle highlights the 'Yahoo! Messenger' row, which has a 'Block' policy and is listed under the 'Advanced rules' tab.

Description	Policy	Protocol	Direction
Network Discovery (WSD Events-Out)	Allow	TCP	Outgoing
Network Discovery (ICSLAP-Out)	Allow	TCP	Outgoing
Network Discovery (SSDP-Out)	Allow	UDP	Outgoing
Network Discovery (SSDP-Multicast-Out)	Allow	UDP	Outgoing
Network Discovery Others (UDP-Out)	Block	UDP	Outgoing
Network Discovery Others (TCP-Out)	Block	TCP	Outgoing
Host Process for Windows Services	Allow	TCP+UDP	In+Out
My Mobile - My Mobiler	Allow	TCP+UDP	In+Out
Yahoo! Messenger	Block	TCP+UDP	In+Out
Skype	Allow	TCP+UDP	In+Out
Microsoft Office Outlook	Allow	TCP+UDP	In+Out
Skype Extras Manager	Allow	TCP+UDP	In+Out
Internet Explorer	Ask me	TCP+UDP	In+Out

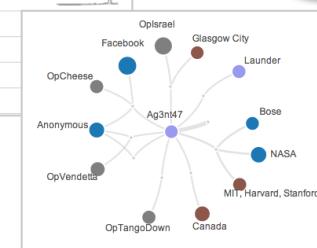
ACTIONABLE OUTCOME  
Harden network defenses,  
update IPS rules



# Research Actors, Methods, & Targets



- Operation Last 60 Days
- Million Mask March
  - OpKillingBay
  - OpVendetta
  - Oplsrael
  - OpSyria
  - OpNewBlood
  - OpNSA



Research and identify trends  
across 5 yr archive, 7 languages

Early detection of campaigns against  
industry, suppliers, partners

The screenshot shows a software interface titled "User Management and User Access Logs". It has two tabs: "User Management" and "Access Logs".

**User Access Log:**

User	In	Out	IP Address
John Stokes	JAN 21 2009 4:44 PM	JAN 21 2009 8:43 PM	192.168.2.1
Administrator	NOV 6 2008 1:25 PM	NOV 6 2008 1:26 PM	192.168.2.1
Administrator	NOV 6 2008 3:58 PM	NOV 6 2008 7:39 PM	192.168.2.1
Administrator	NOV 6 2008 3:55 PM	NOV 6 2008 3:56 PM	192.168.2.1
Administrator	NOV 6 2008 11:19 AM	NOV 6 2008 11:30 AM	192.168.2.1
Administrator	OCT 30 2008 10:41 AM	OCT 30 2008 10:26 AM	192.168.2.1
Administrator	OCT 25 2008 9:56 AM	OCT 25 2008 10:00 AM	192.168.2.1
John Stokes	OCT 25 2008 4:11 PM	OCT 25 2008 7:15 PM	192.168.2.1
Administrator	OCT 24 2008 1:09 PM	OCT 24 2008 1:10 PM	192.168.2.1
Administrator	OCT 23 2008 5:44 PM	OCT 24 2008 10:56 AM	192.168.2.1
Administrator	OCT 21 2008 3:55 PM	OCT 21 2008 3:56 PM	192.168.2.1

**Actions Log:**

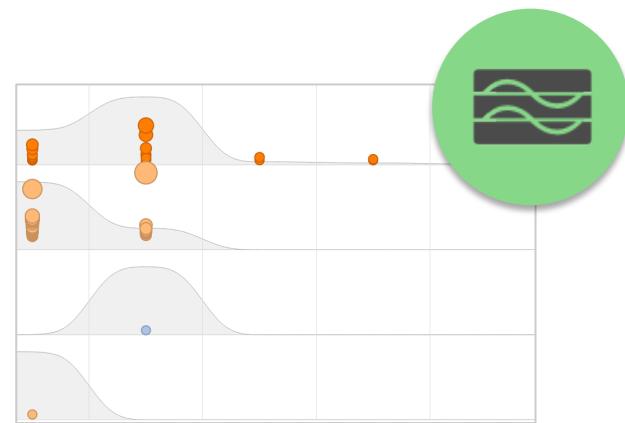
Record Type	Action	Time	Description
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008
Attendance	Entered	10:01 AM	Date Attended: OCT 26 2008

**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 }

```
  "Instance":{  
    "start_time": "2011-11-28T00:00:00.000Z",  
    "stop_time": "2012-10-31T23:59:59.000Z",  
    "attributes": [  
      {  
        "type": "Entity",  
        "entity": {  
          "id": [  
            34622742  
          ]  
        }  
      }  
    ]  
  }
```



Created by C

13

Visible to Recorded Future



**Recorded Future**  
CREATING AN INSIGHTFUL WORLD

**splunk®**



COMPANY CONFIDENTIAL

OSINT threat actor feeds  
OSINT events w/ telltales

Correlations w/ OSINT  
enrich threat scoring

Logs and network data  
Technical threat feeds

Threat actor intelligence

Threat intel  
investigation



Defensive package  
to IT Security

