



Apresentação Web Intelligence

Ferramenta de busca, investigação e monitoramento da internet aberta, mídias sociais e deep e dark web

Agosto de 2020

Webint – suíte completa e robusta para busca e investigação

The screenshot displays the Webint software interface, which is designed for social media monitoring and investigation. The interface is divided into several key sections:

- Top Navigation Bar:** Includes links for Help, Settings, Alerts, Account, Support, and a dropdown for "Choose Live Settings: [Region]". On the right, it shows "Police Department: [Name]" and a "Log Out" button.
- Map View:** The central area features a map of New York City, specifically the area around Chambers Street and Murray Street. A social media post is overlaid on the map, showing a tweet from "Kristen Carol-Jeane" with a location pin and a "Classified as High Risk" warning.
- Left Sidebar:** A dark sidebar contains navigation options: "Live Monitoring", "People", "POI", "Flags", and "Time Machine".
- Right Sidebar:** Contains monitoring tools: two gauges labeled "Risk" and "Shot", a "Keywords" section with a list of terms (shot, gun, police, blood, hurt) and a "Load More Keywords" button.
- Bottom Section:** Shows pagination controls ("First", "Next") and a status message: "Current Page 1 - 2,864 posts in this query". Below this is a copyright notice: "2014-2016 © Social Navigator Inc. Terms Privacy".

Contra a Criminalidade & Violência

+ Superfície WEB
Investigação dos Crimes



+ DEEP WEB
Organização Criminosa / Incitação à violência



+ WEB Privada
Comunicação Interna dos criminosos



+ DARK WEB
Comércio de Armas / Drogas / Documentos falsos



Suíte Web Intelligence



WEB INTELLIGENCE CENTER

Mestre em Investigação Web em grande escala



PROFILER

Identidade web
Instantânea



WEBALERT

Consciência Situacional
Geo-localizada



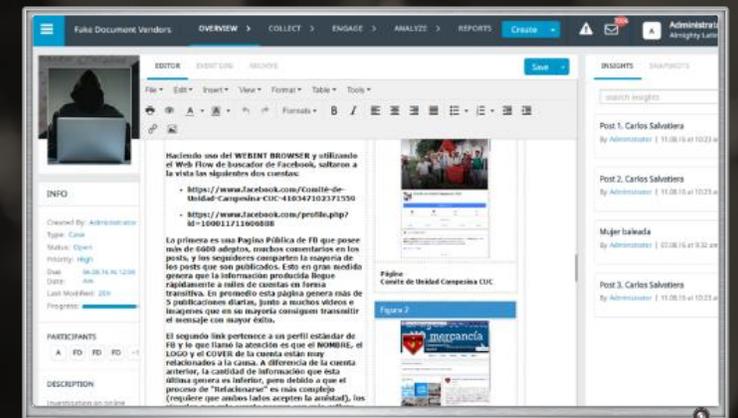
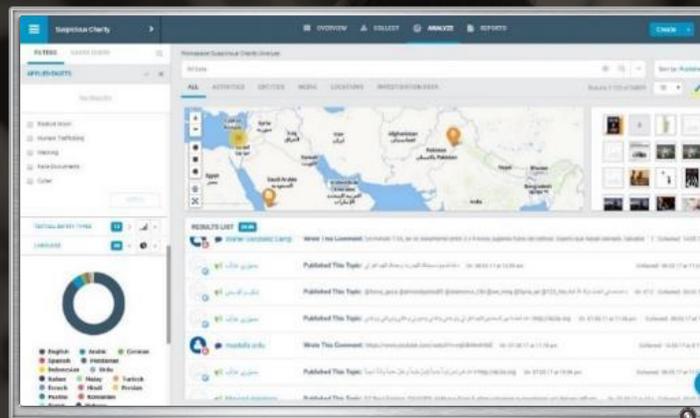
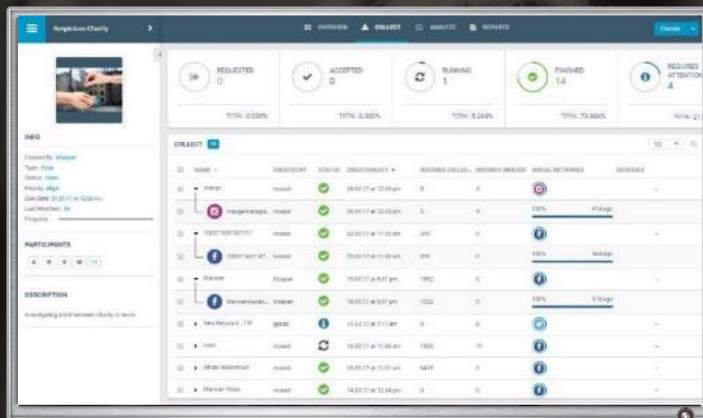
DARKALERT

Google na
Dark Web

Sei mais de investigação
Especialistas no Assunto



Fluxo Guiado de Investigação



Colete



Pesquisa



Análise



Aja

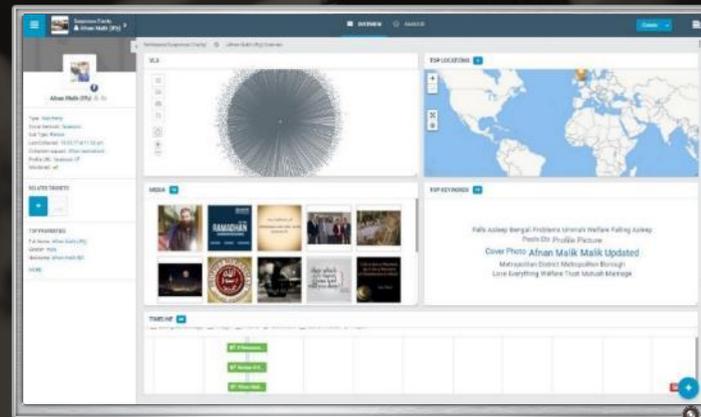


Relatório

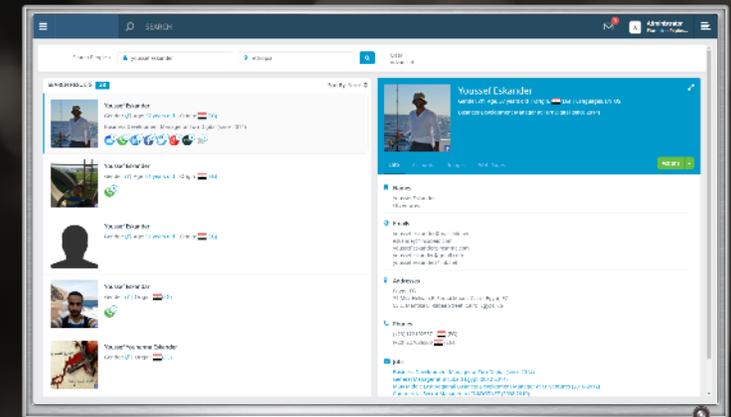
Mapeamento ativo de uma Entidade



Revele Conexões Suspeitas /
mapeie Quadrilhas
completas



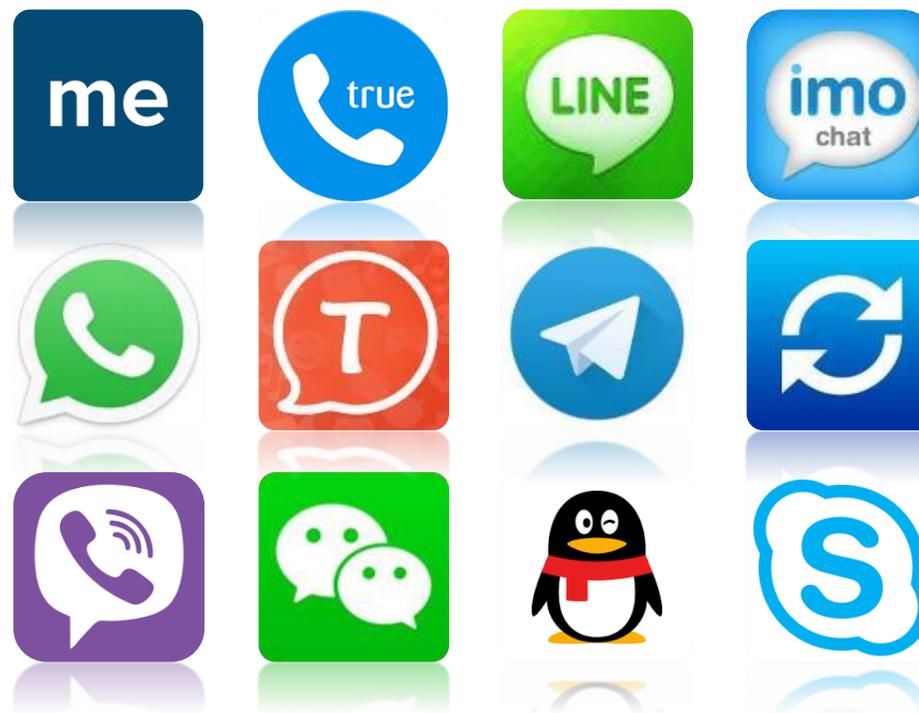
Widgets voltados ao
monitoramento de alvos



Identificação multi-source
Instantânea do Alvo

Profiler – Perfil Web Instantâneo

- + Dados Coletados:
- + Telefones e emails
- + Nomes e relacionamentos
- + Interesses e eventos
- + Status no IMs (last seen timestamp)
- + Localizações, fotos e mídia
- + Educação e carreira
- + Citações na Web



WebAlert

Solução para monitoramento de mídias sociais que permite georreferencia, mapas de vínculos, filtros, nuvem de palavras, identificação de autores mais relevantes, relatórios, filtros nos dados recebidos, busca histórica (busca no passado), entre outras funcionalidades.

The screenshot displays the WebAlert interface with a search query 'Radical Islam activities in Nigeria'. The interface includes a sidebar with navigation options like 'Live Monitoring', 'Queries', 'Posts', 'Subjects', 'Recently Deleted', 'Social Search', 'Social Graph', 'Tags', and 'Alerts'. The main content area shows search results with a status of 'Stopped' and 'Posts Today: 0'. A specific post is highlighted, mentioning 'Boko Haram' and 'EFCC'. Overlaid on the screenshot are five yellow circular callouts, each describing a key feature of the tool:

- TRACK**
Online conversations by applying geo-fence and/or keywords
- REAL TIME ALERTS**
Via varies channels including emails and SMS
- LOCATION INSIGHTS**
View the location of threats using street map view
- REVEAL SOURCES**
Find person behind virtual identity by analyzing his profile activity
- BACK IN TIME**
Find what happened in a specific area and range of dates

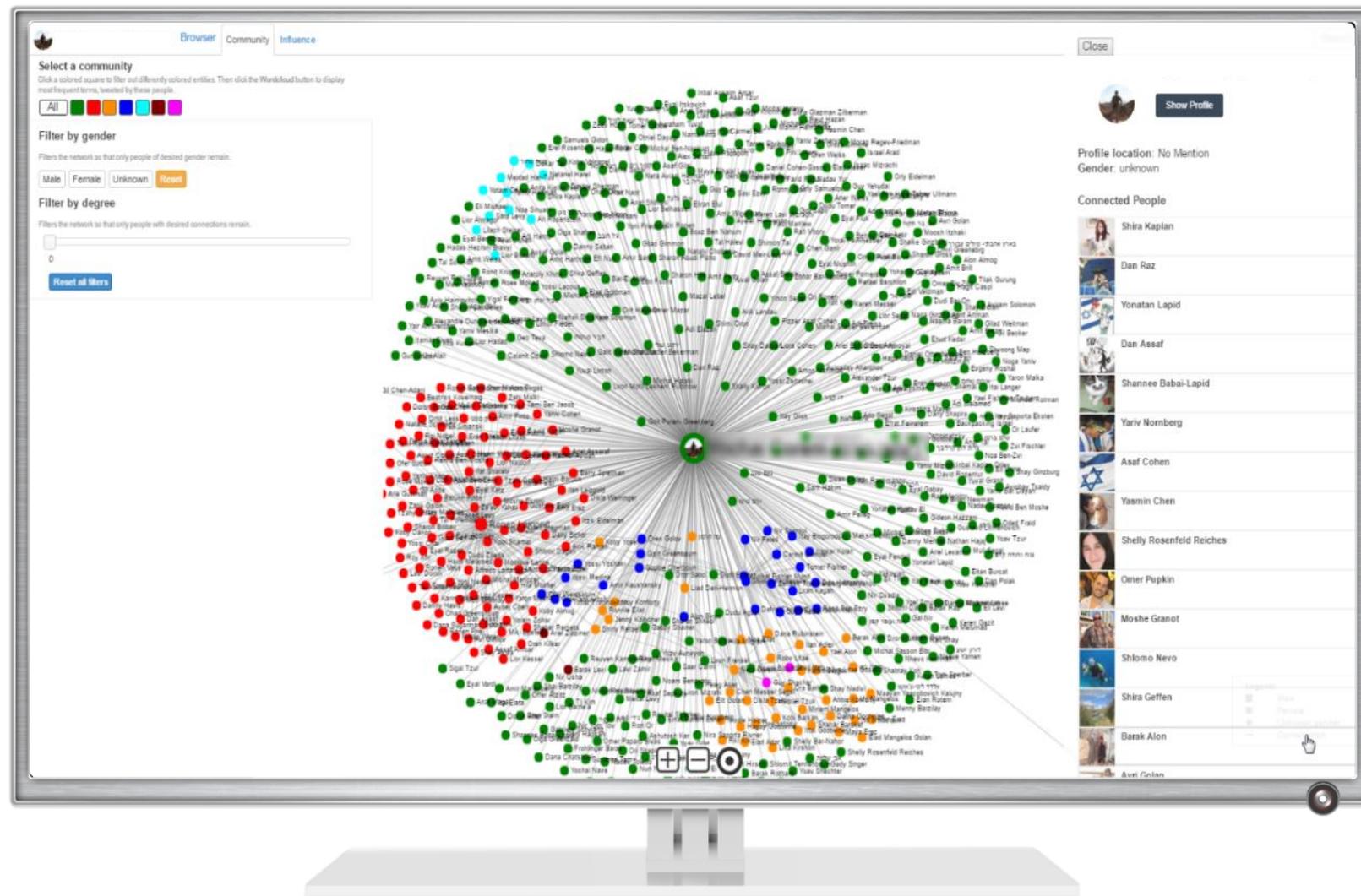
WebAlert - Monitoramento georreferenciado de palavras-chave

- + Vigilância em uma área pré-determinada
- + Monitoramento em tempo real
- + Alertas para atividades suspeitas

The screenshot displays a 'WebAlert' interface with a dark sidebar on the left containing navigation options: Live Monitoring, Queries, Peek, Subjects, Historic Search, Social Search, Social Graph, Reports, and Tags. The main area shows a grid of social media posts, primarily from Twitter, all related to the search query 'Euro 2016: Russian hooligans took MMA gloves and gum shields to assault'. The posts include text, images of fans, and links to news articles. A large, semi-transparent image of a man with a bloody face is overlaid on the center of the grid. The interface also features a search bar at the top and a user profile icon in the top right corner.

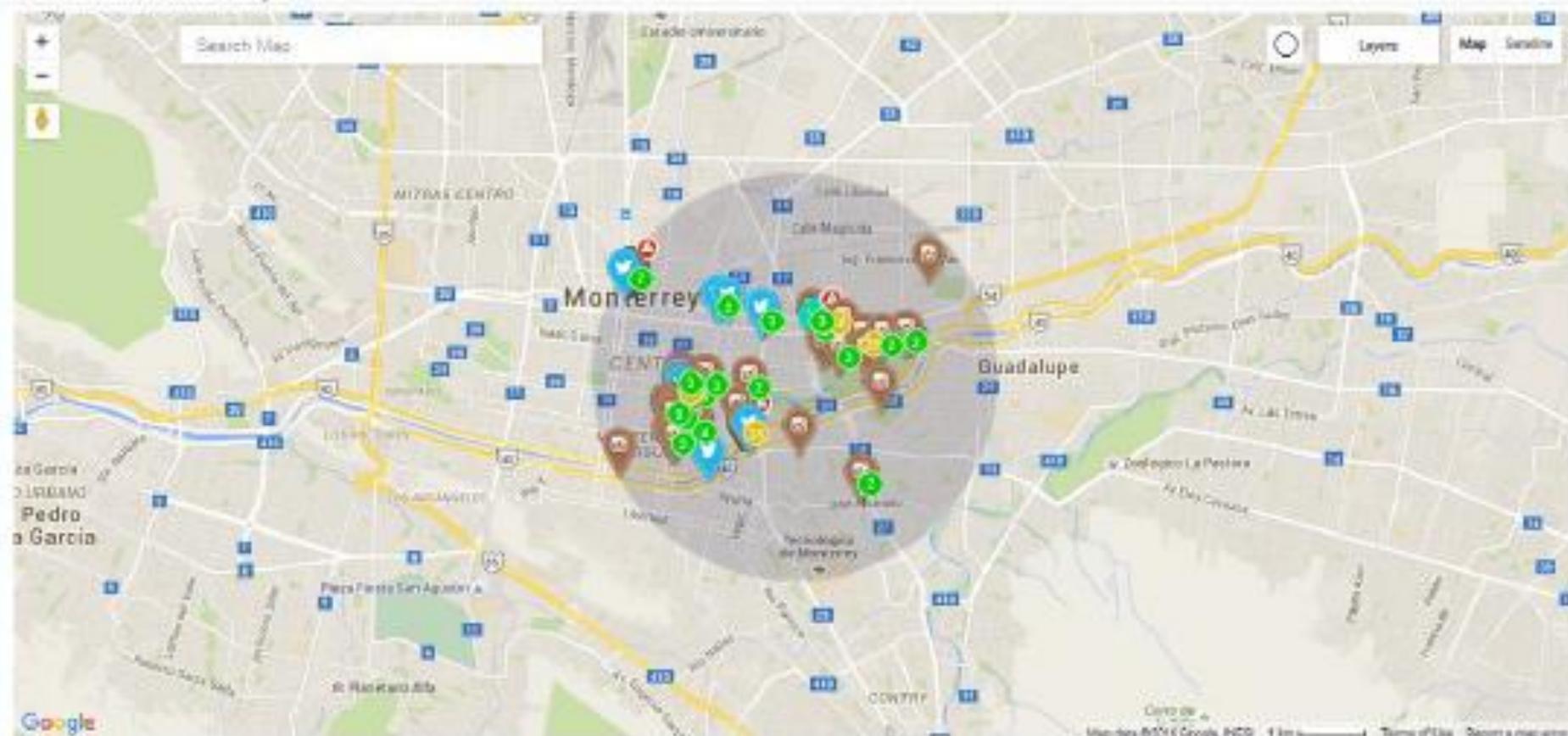
Monitoramento de Pessoas de Interesse

- + Construa rastreamento ao vivo
- + Aprenda os padrões de vida do alvo
- + Monitore a localização do alvo
- + Alerta sobre ameaças emergentes
- + Descubra as relações sociais do alvo



Auto Refresh:

Status: Active Posts Today: 5



Page 1 of 1 | 153 posts

Live Query:

Top Keywords:

- #NL
- #BRONCO
- #BRONCO
- #GOBERNADOR
- #JAME

 Any All

Filter By Type:





craigpumfrey

Visit Twitter profile

Select graph type

Click a button to display different graphs. Each graph shows a different view of relationships & content.

Community **Influencer** Location

Tweets on map

Clicking on a tweet will show it on a map.

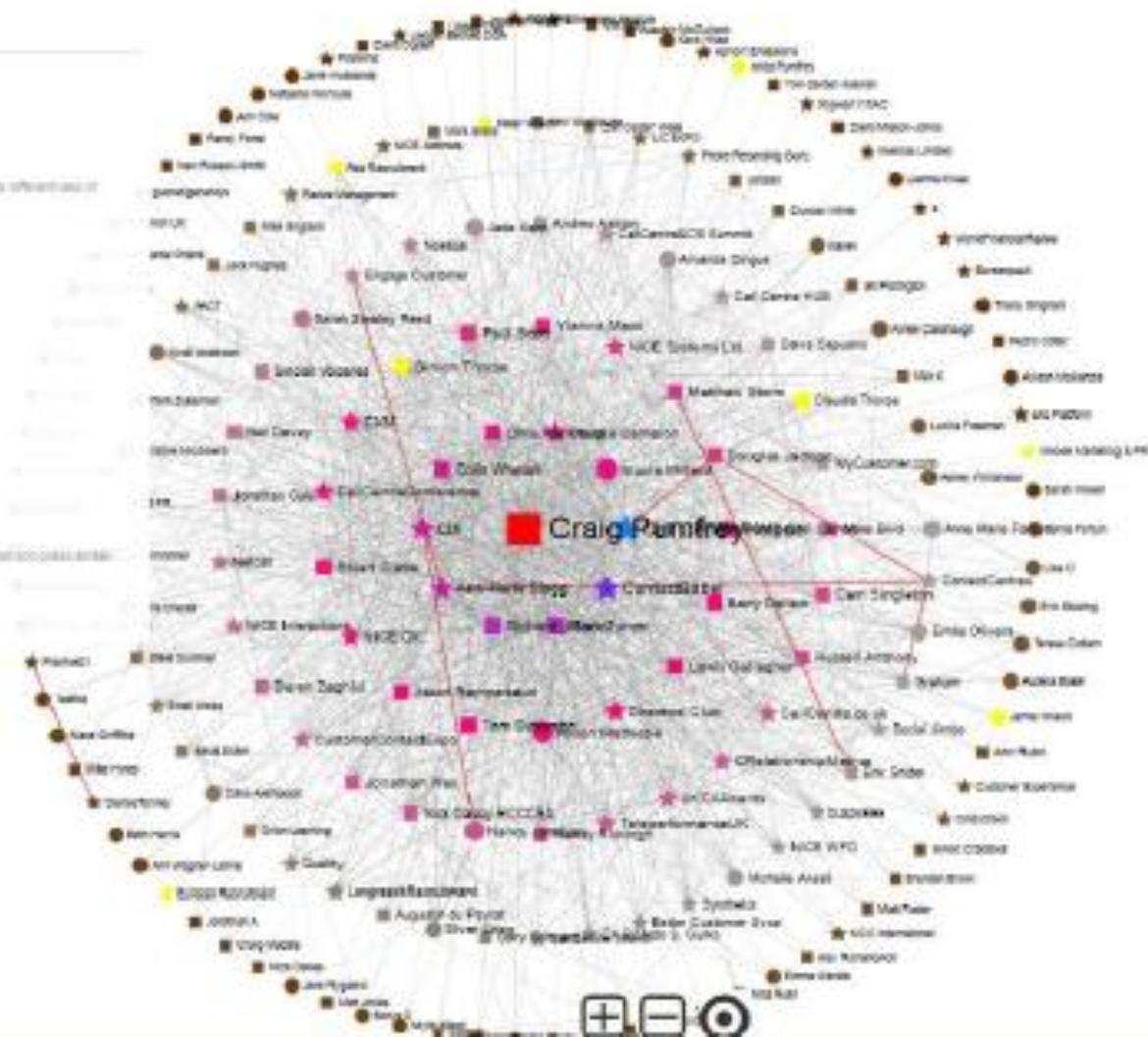
Show tweet map

Legend:

- male
- female
- ★ unknown gender
- conversation

Search users and tweets

Start typing a username in the box that would appear at a network node to search users, just type your query, and press enter.



Web Alert™

Live Monitoring > Bronco

Status: Active Posts Today: 0

7a. Zona

7a. Zona

7a. Zona

Google

Page 1 of 1 | 153 posts

Live Query: Bronco
 Top Keywords:
 #L
 #BRONCO
 #BRONCO
 #GOSHWADOT
 #JMS
 Author Name:
 Username:
 Search Terms:
 Any All
 From Date: To Date:
 Choose Language:
 Filter By Type:

Tarunjit Singh (TarunjitsBanny)

Sunday, October 25th 2015, 6:51:41 am +02:00 New Delhi, DELHI

[#Gulzar supports writers protest](#)
[#BJPdividingIndia](#)
[@IYC](#)
[@INCIndia](#)
[@OfficeOfRG](#)
[@DelhiPCC](#)
[@khushsundar](#)
[@PraveenaLeo](#)
<https://t.co/dDuXnxuGbb>

⚠ Classified as High Risk based on account settings

Address: RAGHUVVEER PURA ROAD, Rajgarh, New Delhi, Delhi, 110032, India

Web Alert™

- Live Monitoring
- Queue
- Peak
- Subjects
- Address Search
- Social Search
- Social Graph
- Tags
- Alerts

Peak

Map View Live View

Brooklyn, Manhattan, United States

Google

Web Alert Systems Inc.



Kristen Carol-Jeane



Tuesday, May 12th 2015, 10:00:52 am EDT

New York City, NY

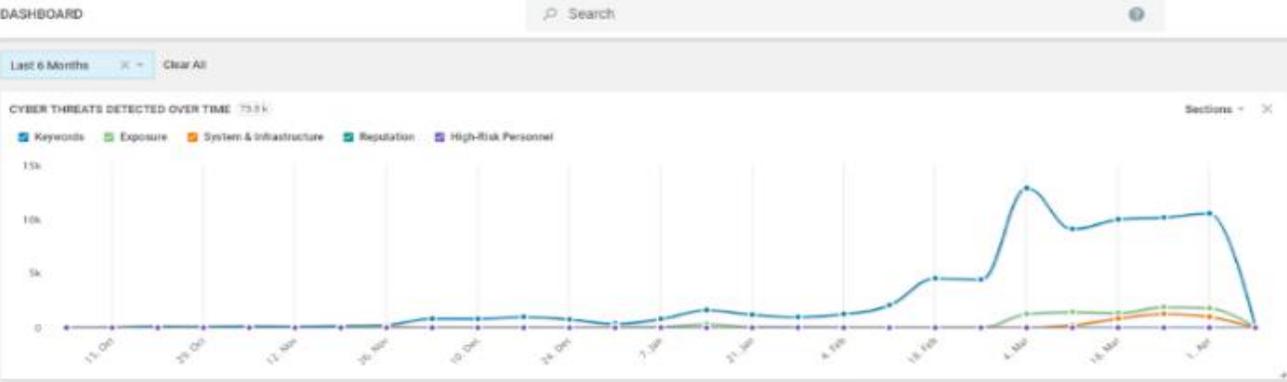
Hot, sunny days... #nyc #hot #sunshine #rooftops #billyrood #nym #shooting #models
#blackandwhite 🖱️☀️🖱️☀️

⚠️ Classified as High Risk based on account settings.

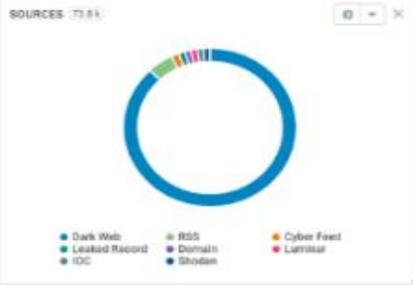
Address: 270 Broadway, New York City, NY 10007, US

Luminar (Dark Alert)

- Solução de proteção cibernética que monitora a Deep e Dark Web
- Ótima solução para análise de riscos, identificação de hackers e pessoas planejando ações contra a organização
 - Também é utilizada para identificar se dados da organização estão sendo compartilhados pela DarkWeb, identificar se nomes, e-mails e informações ligadas a empresa estão sendo vendidos em Blackmarkets...
- Inclui relatórios customizados de inteligência, que chegam mensalmente e são integrados dentro da solução



- ### DAILY CYBER FEED 1.1k
- Bayer Fallen a Victim of a Cyber-Attack**
The leading German chemicals producer Bayer was hit by a ma...
02/04/19
 - Suspect Arrested at Mar-a-Lago with Suspicious USB Drive**
The U.S. authorities have arrested a Chinese tourist, who attempt...
02/04/19
 - Reaming Mantis Campaign Continues to Evolve**
Security researchers have revealed that threat actors behind the ...
02/04/19
 - Bashlite IoT Malware Upgrade Lets it Target WeMo Home ...**
Security researchers have discovered a new version of Bashlite I...
02/04/19
 - Georgia Tech Breach Hits Up to 1.3 Million People**
The Georgia Institute of Technology has suffered a massive data...
02/04/19
 - Dozens of Credit Card Info-Skimming Scripts Infect Thous...**
Security researchers have uncovered 38 unique families of malic...
02/04/19
 - Indian Govt Agency Left Details of Millions of Pregnant Wo...**
An Indian government healthcare agency has suffered a serious ...
01/04/19
 - WordPress iOS App Leaked Authentication Tokens**
Security researchers have identified a vulnerability affecting the ...
01/04/19

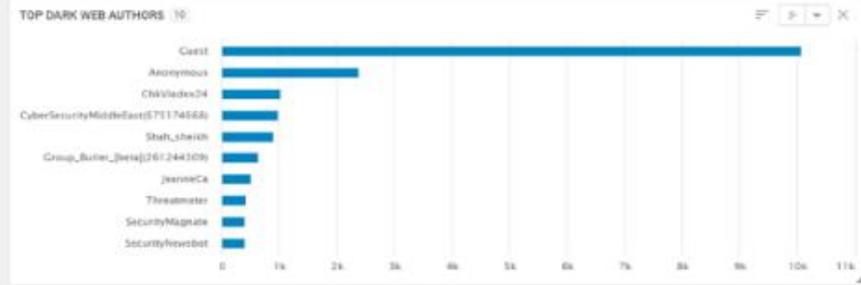


HIGH-RISK PERSONNEL 14

IBD	~10k
IPF	~8k
RP	~6k
SV	~4k
JC	~2k



- ### THREAT INTELLIGENCE HUB 27
- Major Data Leaks in 2018**
In the course of 2018, data breaches and data leaks have been a prominent vector in cyber-attacks. W...
04/04/19
 - Technical CTI Overview Equation on Group Leak**
On August 13, 2016, a group of hackers dubbed the Shadow Brokers aploaded a post to Pastebin claim...
18/03/19
 - Avoiding a BEC Attack**
31/12/18
 - List of Websites for SQL Injection**
25/11/18
 - XSS Vulnerability in Reports Addon for CUBA Platform**
07/01/19
 - Support for old PHP Versions to Cease by the End of the Year**
The company that develops the PHP language announced it is going to stop supporting its old versions...
01/11/18
 - The North Korean Group APT38 Targets Financial Institutions**
Recently, a new report was published, shedding light on the north Korean state-sponsored group, APT3...
01/11/18
 - Marriott Leak**
16/12/18
 - New Variant of the Olympic Destroyer Malware Presents New Capabilities**
During the past month, security researchers published a new report regarding the malware dubbed Olym...
18/12/18
 - Rise in Mobile Banking Trojan Campaigns; Brazil Among the Targets**
Multiple cyber campaigns distributing various mobile banking Trojans were recently reported by secur...
12/11/18
 - The North Korean Group, APT38, Targets Financial Institutions**
Recently, a new report was published, shedding light on the North Korean state-sponsored group, APT3...
01/11/18
 - New Malware Attributed to the Cyberespionage Group, Tick Group; GreyEnergy APT Group Targets the Energy a...**
Security researchers have recently identified the activity of a new attack group, related to the not...
12/11/18
 - Opicarus 2018**
20/12/18





Publish Date



ADD WIDGETS

THREAT INTELLIGENCE HUB 242



	Major Data Leaks in 2018 In the course of 2018, data breaches and data leaks have been a prominent vector in cyber-attacks. W		04/04/19
	A New Attack Campaign Uses Fileless Malware to Infect Organizations On February 8, 2017, cyber security researchers reported a new attack campaign that uses legitimate	2	01/03/17
	Phishing Attacks Target the French Tax Authority We have detected multiple phishing attempts targeting the website of the French tax authorities (www	2	03/04/17
	New Darknet Marketplace Offers Dozens of Attack Tools and Services We identified a new marketplace on the Darknet called "Scylla Hacking Store," which sells different		19/12/17
	Shadow Brokers Release Windows Hacking Tools The Shadow Brokers hacking group released of another batch of Equation Group (EQGP) files from their	3	03/05/17
	Technical CTI Overview Equation Group Leak On August 13, 2016, a group of hackers dubbed the Shadow Brokers uploaded a post to Pastebin claimin		18/03/19
	Sharp Rise in Mining Related Malware on the Russian speaking Underground Replacing the Development of Banking Malware Our monitoring has revealed a sharp rise in mining malware traded on underground sources in recent m		27/02/18
	Bangladesh Central Bank Hack Between March 4 and March 5, 2016, cyber criminals stole approximately \$80 million from the Banglade	2	18/05/16
	New Darknet Marketplace Offers Dozens of Attack Tools and Various Services We identified a new marketplace on the Darknet called "Scylla Hacking Store," which sells different		04/01/18
	Tokyo Botnet for Sale on a Dark Web Forum		09/07/18

DAILY CYBER FEED 4.5k



	Telegram Says DDoS Attack Launched Mostly from China Telegram instant messaging service has fallen a victim of a pow...		13/06/19
	TAS05 Group Uses HTML, RATs and Other Techniques in T... Security researchers have analyzed the latest campaigns launch...		12/06/19
	Ransomware Halts Production for Days at Major Airplane ... The major supplier of airplane parts ASCO has fallen victim of a ...		12/06/19
	AgentTesla Keylogger and Binary Options Scam Security researchers have uncovered a new AgentTesla campaig...		12/06/19
	Flaw in SymCrypt Can Trigger DDoS The SymCrypt cryptographic library on Windows OS is affected b...		12/06/19
	Fishwrap Campaign Sways Social Media Users with Old Ne...		
	Hide 'N Seek Botnet Updates Arsenal with Exploits Against... The Hide 'N Seek botnet adds new capabilities to its arsenal. Th...		

DARKALERT - LUMINAR

Principais Funcionalidades

- + Pesquisa na dark Web
- + Resultados Instantâneos
- + Dados indexados
- + Análise de Alvos
- + Notificações
- + Monitoramento
- + Relatórios

