



**XIII
JORNADAS
STIC
CCN-CERT**



Vigilancia Digital en procesos electorales *Social Intelligence*

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT

Vigilancia Digital en procesos electorales *Social Intelligence*

Maite Moreno & Adrián Antón

CSIRT-CV, S2Grupo

csirtcv@gva.es



UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa



GENERALITAT
VALENCIANA



CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana



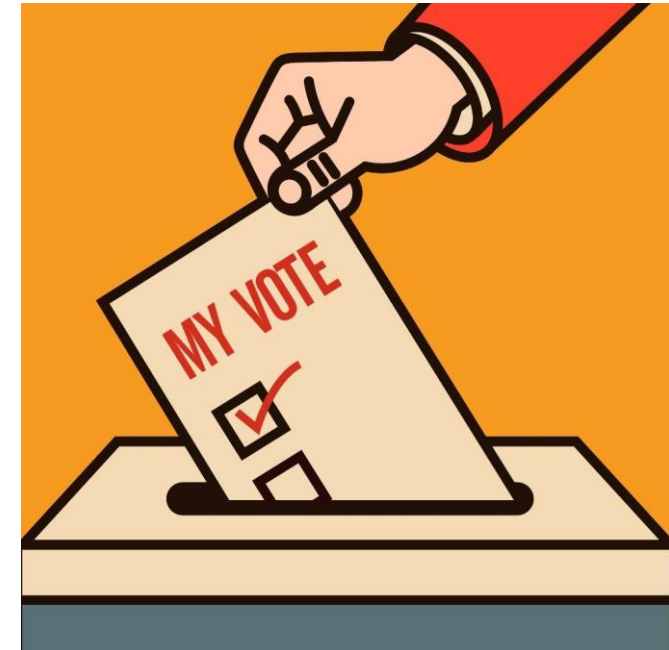
OPERATIVO ESPECIAL “ELECCIONES 2019”

Incremento de las capacidades de CSIRT-CV periodo pre y post electoral

- INTERNAL TELEMETRY
 - Monitorización infraestructuras
 - Auditorías aplicaciones y sistemas
 - Bastionado
- DIGITAL SURVEILLANCE
 - Orquestación de ciberataques
 - Leaks de información
 - Seguridad semántica, fraude
 - Desinformación

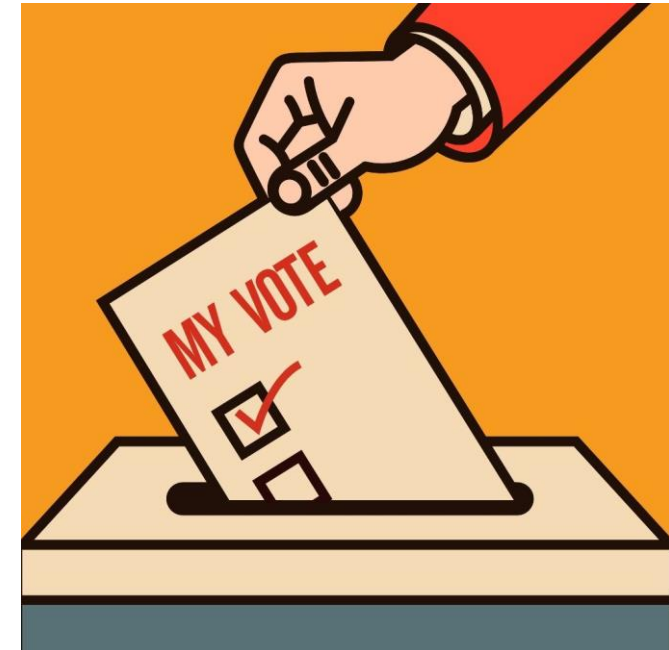
Índice

1. Amenazas híbridas
2. Obtención de datos
 1. Etapa de preparación
 1. Social Listening Tools
 2. Representación Big Data
 3. Recopilación y análisis de datos
3. Generación de inteligencia
 1. Prevención y respuesta ante ciberataques
 2. Datos estadísticos y tendencias
 3. Cuentas falsas y seguimiento de bots
4. Conclusiones



Índice

1. Amenazas híbridas
2. Obtención de datos
 1. Etapa de preparación
 1. Social Listening Tools
 2. Representación Big Data
 3. Recopilación y análisis de datos
3. Generación de inteligencia
 1. Prevención y respuesta ante ciberataques
 2. Datos estadísticos y tendencias
 3. Cuentas falsas y seguimiento de bots
4. Conclusiones



Amenazas Híbridas

Estrategia Nacional de Ciberseguridad 2019

“[...] una tendencia creciente de las denominadas amenazas híbridas [...] **acciones coordinadas y sincronizadas** dirigidas a **atacar** de manera deliberada las vulnerabilidades sistemáticas de los **estados democráticos y las instituciones**, a través de una amplia gama de medios, tales como acciones **militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica.** [...]”

Amenazas Híbridas en Procesos Electorales

Principales objetivos a vigilar

- Hacktivismo
- Ataques DDoS
- Defacement
- Leaks información
- Desinformación
- Cualquier otro tipo de ciberataque

 [#Anonymous](#) [#OpCatalunya](#) [#OpCatalonia](#) [#FreeCatalunya](#) [#OpSpain](#)

Spain Ministry of Justice [#Offline](#)

Site: [mjusticia.gob.es](https://www.mjusticia.gob.es)

Check website <https://www.mjusticia.gob.es/>

Permanent link to this check report | Share report: 

Location	Result	Time	Code
 Canada, Toronto	Connection timed out		
 France, Roubaix	Connection timed out		
 Germany, Dusseldorf	Connection timed out		
 Germany, Falkenstein	Connection timed out		
 Italy, Milan	Connection timed out		
 Latvia, Riga	Connection timed out		
 Lithuania, Vilnius	Connection timed out		
 Moldova, Chisinau	Connection timed out		
 Netherlands, Amsterdam	Connection timed out		
 Portugal, Oporto	Connection timed out		
 Russia, Moscow	Connection timed out		
 Russia, Moscow	Connection timed out		
 Sweden, Stockholm	Connection timed out		

Amenazas Híbridas en Procesos Electorales

Desinformación

- Fake news
- Amplificación de la información
- Posverdad (mentira emotiva)
- Ejemplos: Elecciones Brasil 2018, Brexit 2016



Amenazas Híbridas

Brexit 2016



Cartel a favor del Brexit con una afirmación falsa sobre la cuota de membresía de la Unión Europea, citado como un ejemplo de la política de la posverdad:

“Cada día enviamos a la UE 50 millones de libras esterlinas: mejor gastémoslos en nuestro sistema nacional de salud”

Amenazas Híbridas

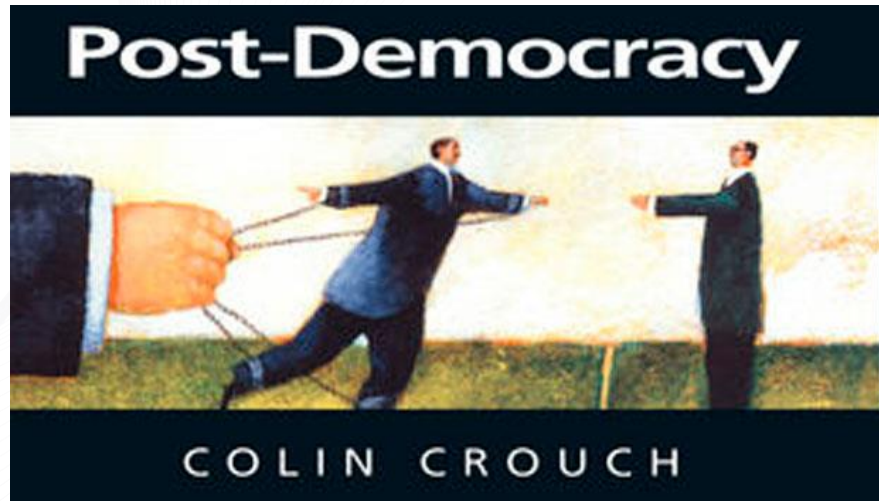
Brasil 2018



- Mas de 100.000 imágenes analizadas. Mas de la mitad contenía información engañosa o falsa
 - Fotografías y vídeos
 - Historias falsas sobre los candidatos
 - Teorías de conspiración
- Cuando se desmienten este tipo de comunicados, muchas veces la gente no confía

Amenazas Híbridas

Post-Democracy

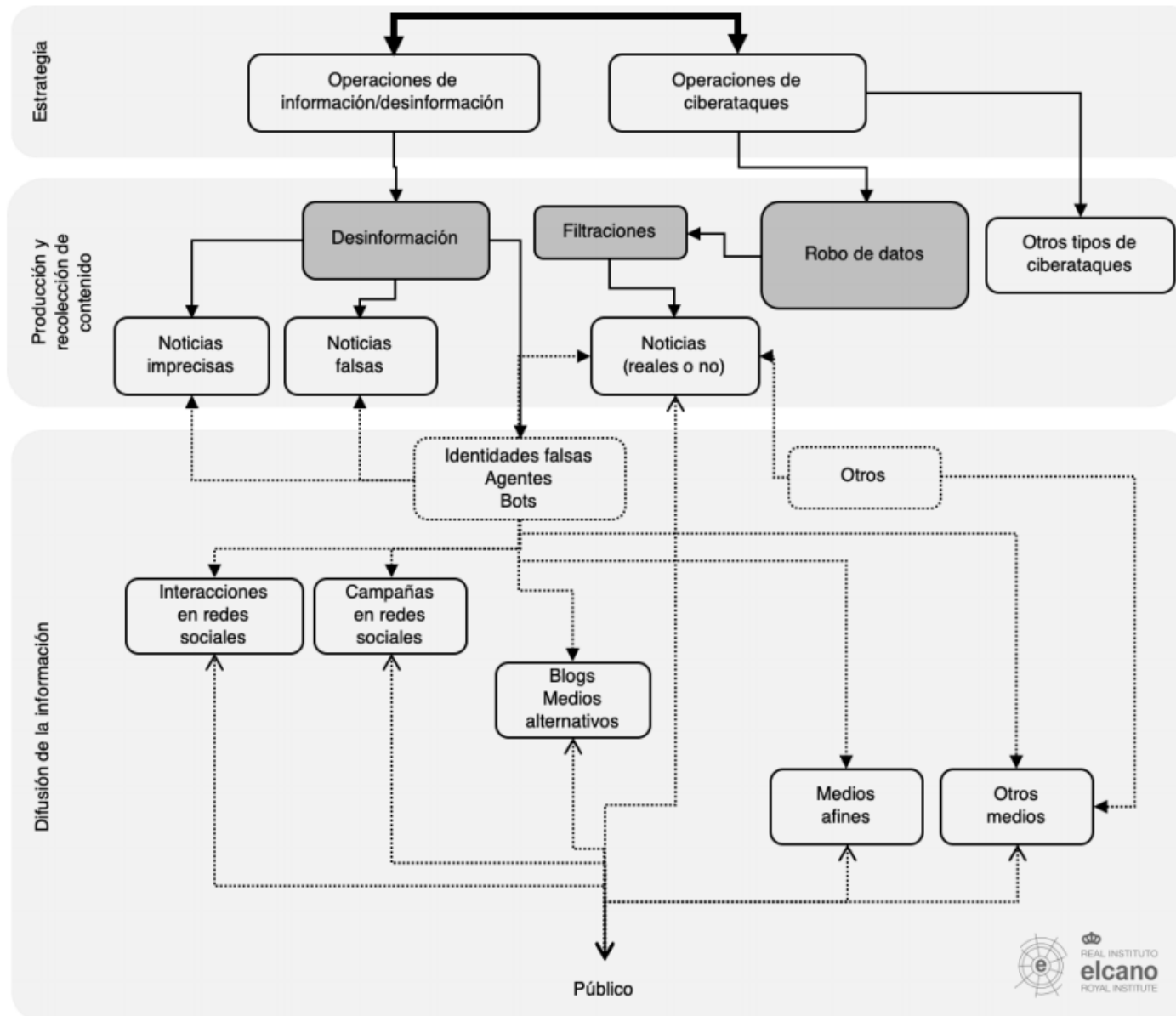


“[...] las elecciones ciertamente existen y pueden cambiar los gobiernos pero el debate electoral público es un espectáculo estrechamente controlado, gestionado por equipos rivales de profesionales expertos en técnicas de persuasión[...]»

- Erosionar la confianza de los ciudadanos en sus instituciones
- Generar desconfianza en el sistema democrático
- Convencer de la decadencia de un sistema
- Socavar la cohesión social o los modelos sociales de los Estados, de las comunidades políticas (como la UE) o de las organizaciones internacionales (la OTAN, por ejemplo)

<http://www.realinstitutoelcano.org>

Amenazas Híbridas: el modelo de la desinformación



**Ciberataques
+ Op. Desinformación**

Amenazas Híbridas en España

“Referéndum Cataluña”, “Sentencia Procés”

MB MALDITO BULO 
@malditobulo

No.

El Barça no ha felicitado a Puigdemont por la declaración de independencia.

Es un tuit de enero de 2016.

+ en t.me/malditobulo



NO, EL FCB NO HA FELICITADO A PUIGDEMONT POR LA DECLARACIÓN DE INDEPENDENCIA.

ES UN TUIT DE ENERO DE 2016, CUANDO PUIGDEMONT FUE INVESTIDO PRESIDENTE DE CATALUÑA.

FC Barcelona 
@FCBarcelona_es

Felicitades, president Puigdemont. Que el acierto os acompanyi en esta etapa històrica i apassionant que hem iniciat el nostre país.

698 16:08 - 27 oct. 2017



MB MALDITO BULO 
@malditobulo

No.

Gambia no ha reconocido Cataluña como Estado independiente.

Es una cuenta fake.

Nos lo confirma el Ministerio de Exteriores de Gambia

Foreign Ministry 
@Net_MFA

Congratulations, Catalonia. May your national flag fly high tonight.
[#CatalanIndependence](#)

 Traduce de inglés



21:08 - 27 oct. 2017

NO.

GAMBIA NO HA RECONOCIDO LA INDEPENDENCIA DE CATALUÑA.

@malditobulo

ES UNA CUENTA FALSA.

NOS LO DESMIENTE EL MINISTERIO DE EXTERIORES DE GAMBIA.

584 1:27 - 28 oct. 2017



Comunicado de Twitter

Junio 2019

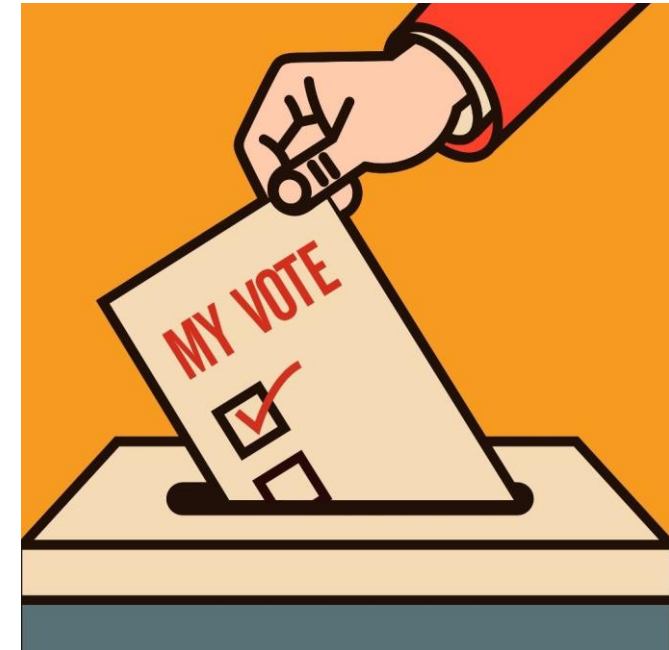
Spain (130 accounts)

Earlier this year, we suspended 130 fake accounts originating in Spain. These accounts were directly associated with the Catalan independence movement, specifically Esquerra Republicana de Catalunya. They were primarily engaged in spreading content about the Catalan Referendum. The network includes fake accounts which appear to have been created with the intent to inorganically influence the conversation in politically advantageous ways. Setting up fake accounts is a violation of the **Twitter Rules**, full stop.

https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

Índice

1. Amenazas híbridas
2. Obtención de datos
 1. Etapa de preparación
 1. Social Listening Tools
 2. Representación Big Data
 3. Recopilación y análisis de datos
3. Generación de inteligencia
 1. Prevención y respuesta ante ciberataques
 2. Datos estadísticos y tendencias
 3. Cuentas falsas y seguimiento de bots
4. Conclusiones



Etapa de Preparación

Fase de documentación

- Elegir y desplegar las herramientas más apropiadas
- Elegir el principal data feed
- Estudio de procesos electorales anteriores que sufrieron ciberincidentes. Ejemplos:
 - 2014. Elecciones generales Polonia. Ciberataque obligó a verificación manual para hacer el recuento votos
 - 2015. Elecciones europeas. Ataque DDoS que mantuvo inactivo el servicio Web de las autoridades búlgaras durante horas
 - 2017. Elecciones presidenciales Francia. Ciberataque contra la infraestructura del candidato Macron
 - 2017. Elecciones República Checa. Servicio electoral afectado por ataque DDoS

Etapa de Preparación

¿Qué queremos monitorizar?

- ESTRATEGIAS
 - Apoyos, ataques, cortinas de humo
- TARGETS
 - Individuos, movimientos, eventos
- OBJETIVOS
 - Activar y reforzar ideas

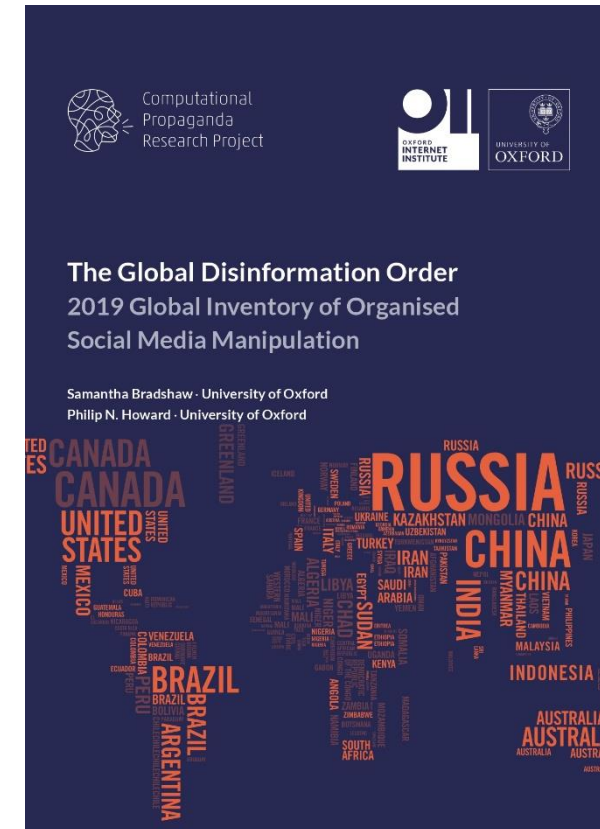


Table 2: Social Media Manipulation Strategies: Messaging and Valence

Country	Fake Account Type	Pro-Government or Party Messages	Attacks on the Opposition	Distracting or Neutral Messages	Trolling or Harassment
Angola					
Argentina					
Armenia					
Australia					
Austria					
Azerbaijan					
Bahrain					
Brazil					

Fuente: Oxford Internet Institute

Etapa de Preparación

¿Qué monitorizar?

- 200 dominios críticos
- Palabras clave
- Listado de dominios similares a los nuestros comprados en días previos (por si se usaran para phishing simulando web de Generalitat)
- Monitorización de sitios donde se detectan dominios de la Generalitat
- Fuentes OSINT: Sitios de “pastes”, Canales Telegram, Deep Web, Foros, Blogs...etc.

Etapa de Preparación

Principal Data Feed

- Twitter
- Necesidad de ampliar capacidades de monitorización y análisis para la información recopilada de Twitter
- Grandes volúmenes de datos
- Detección no solo de ciberataques, Leaks... sino también de Fake news

The screenshot shows the Twitter Help Center interface. At the top is an orange navigation bar with the Twitter logo, 'Centro de ayuda', 'Temas de ayuda', 'Guías', and a 'Comunicate con nosotros' button. Below this is a sidebar with categories: 'Uso de Twitter', 'Administrar tu cuenta', 'Seguridad y prevención', and 'Reglas y políticas'. The 'Reglas y políticas' section is expanded, showing links to 'Reglas y políticas de Twitter', 'Políticas y pautas generales', 'Pautas de aplicación de las normativas legales', and 'Investigación y experimentos'. The main content area shows the breadcrumb 'Centro de ayuda > Políticas y pautas generales > Política de integridad electoral' and the title 'Política de integridad electoral'. Under 'Descripción general', it states 'Abril de 2019' and provides a warning: 'No puedes utilizar los servicios de Twitter con el fin de manipular las elecciones o interferir en ellas. Esto incluye publicar o compartir contenido que pueda disuadir la participación de los votantes o engañar a las personas sobre cuándo, dónde o cómo votar.' It then explains that public conversation on Twitter is important and that the service's integrity is contrary to fundamental rights. Finally, it states Twitter's responsibility to protect the integrity of conversations from interference and manipulation, prohibiting attempts to use the service for manipulation or interruption.

Centro de ayuda > Políticas y pautas generales > Política de integridad electoral

Política de integridad electoral

Descripción general

Abril de 2019

No puedes utilizar los servicios de Twitter con el fin de manipular las elecciones o interferir en ellas. Esto incluye publicar o compartir contenido que pueda disuadir la participación de los votantes o engañar a las personas sobre cuándo, dónde o cómo votar.

La conversación pública que se produce en Twitter nunca es tan importante como durante el período de elecciones. Cualquier intento de socavar la integridad de nuestro servicio es contrario a nuestros derechos fundamentales y obstaculiza los principios esenciales de la libertad de expresión, el valor en el que se basa nuestra empresa.

Creemos que tenemos la responsabilidad de proteger la integridad de esas conversaciones de la interferencia y la manipulación. Por lo tanto, prohibimos los intentos de utilizar nuestros servicios para manipular o interrumpir las

Etapas de Preparación

Detección OSINT real time

- TERESA
 - Herramienta de S2Grupo
 - Monitorización Leaks, palabras clave etc. en diferentes fuentes públicas



TERESA
Tecnología Española
para la Recolección y
Explotación de
Sistemas Abiertos

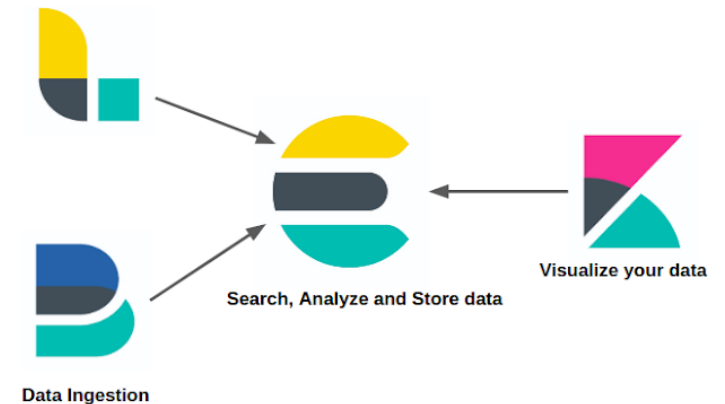
Evaluación herramientas Social Intelligence

- BRAND24
 - Herramienta de pago
 - Monitorización de marca
 - Análisis de sentimiento
 - Seguimiento de palabras clave
 - Exportación de datos

BRAND24
SOCIAL MEDIA MONITORING & ANALYTICS

Representación Big Data

- ELK STACK
 - Gratuita
 - Visualización de datos
 - Análisis grandes cantidades de datos



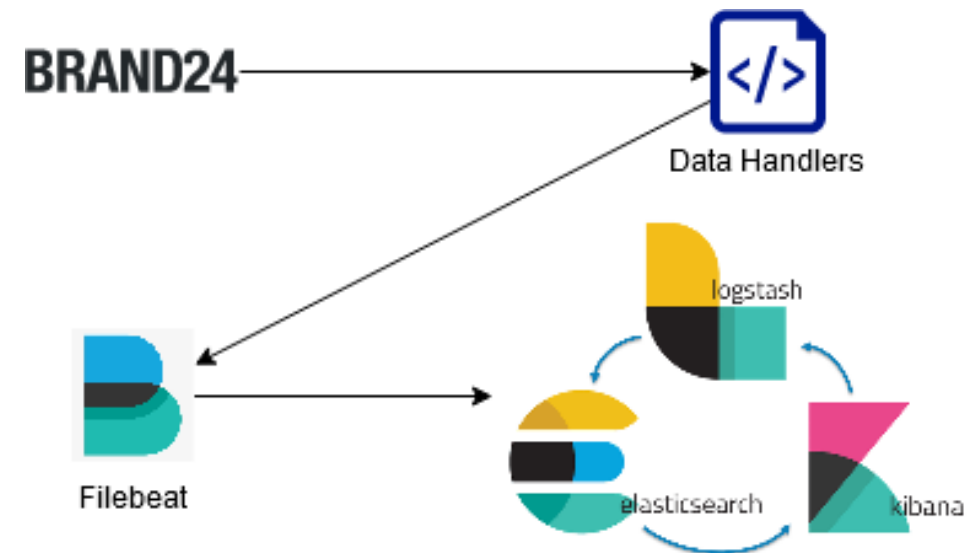
Etapas de Preparación

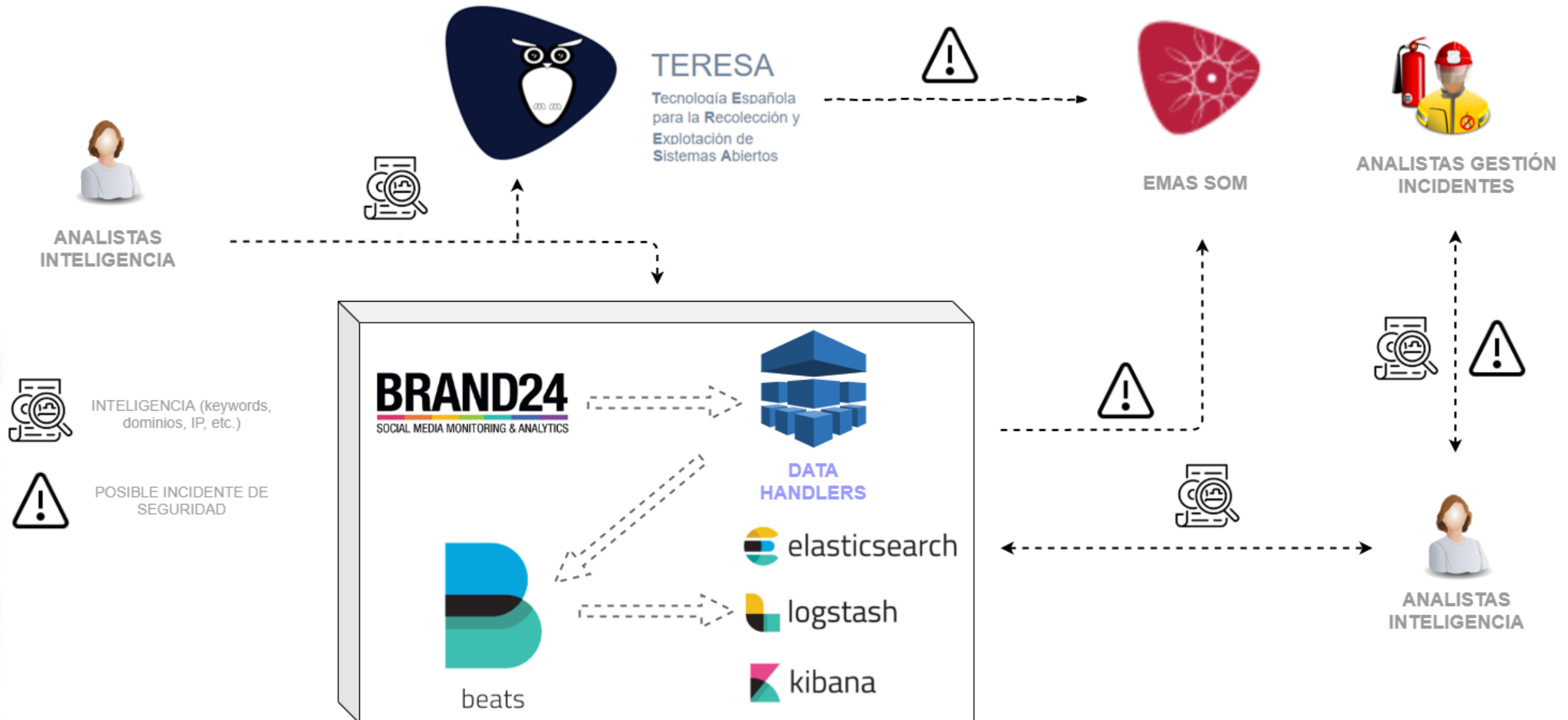
Obtención de datos

- Parametrización de BRAND24
- Menciones a dominios de Administración Pública de la Comunitat Valenciana
- Actualización constante de keywords
- Investigación de menciones relacionadas con posibles ataques

Tratamiento de los datos

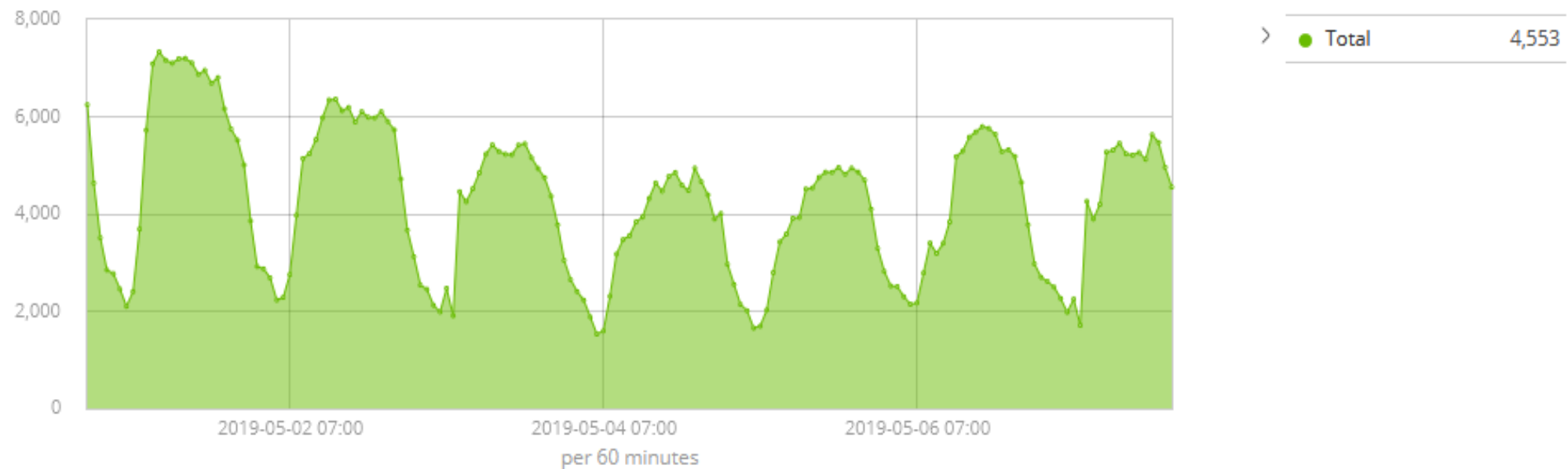
- Normalización de los datos
- Indexación de los datos en una pila ELK
- Visualización de los datos mediante dashboards





Etapa de Preparación

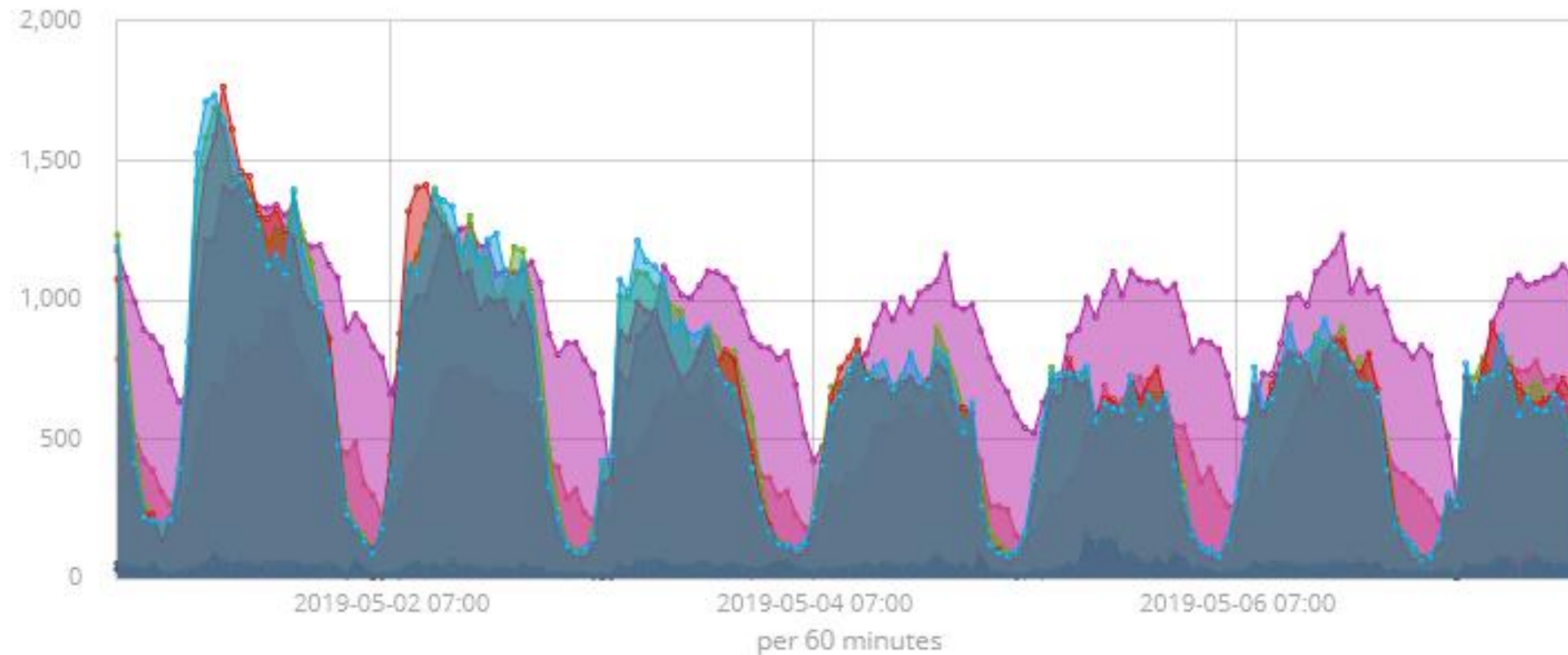
Representación Big Data



Menciones totales en tiempo real

Etapa de Preparación

Representación Big Data

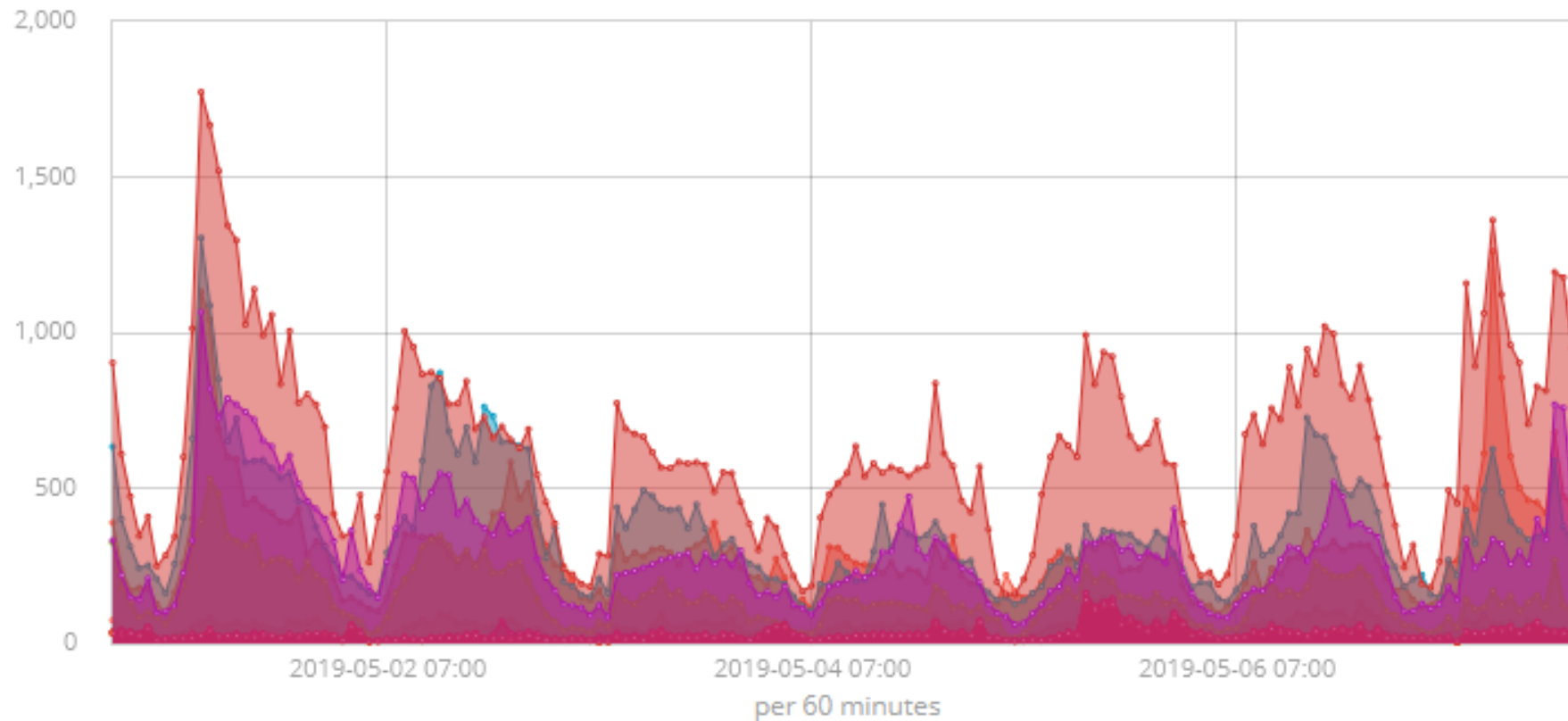


>	PP	490
	PSOE	496
	PNV	31
	Compromis	46
	PDeCat	27
	VOX	492
	PSPV	31
	Podemos	975
	Ciudadanos	562

Menciones a partidos políticos en tiempo real

Etapa de Preparación

Representación Big Data

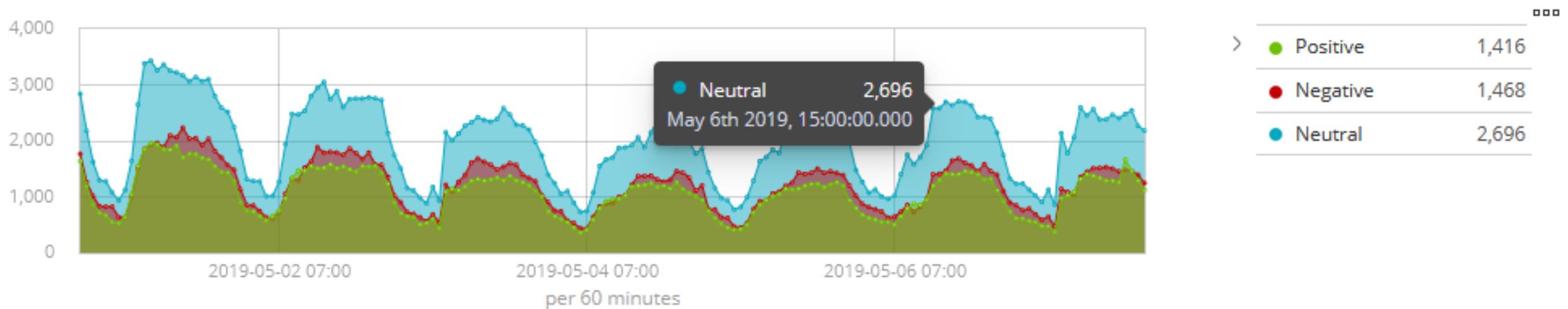


Menciones a individuos en tiempo real

>	Pablo Iglesias	388
	Mónica Oltra	27
	Pedro Sánchez	756
	Joan Ribó	29
	Ximo Puig	27
	Joan Baldoví	27
	Santiago Abascal	95
	Pablo Casado	324
	Albert Rivera	330
	Inés Arrimadas	38

Etapa de Preparación

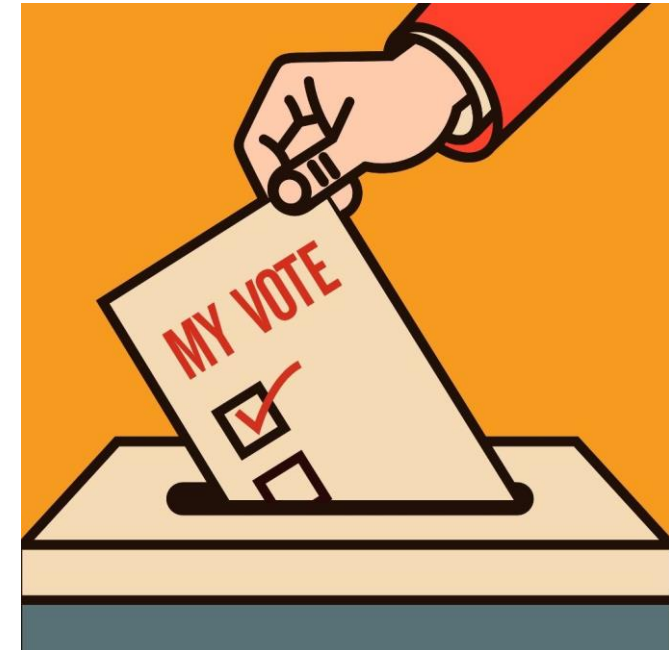
Representación Big Data



“Sentimiento” de las menciones totales en tiempo real

Índice

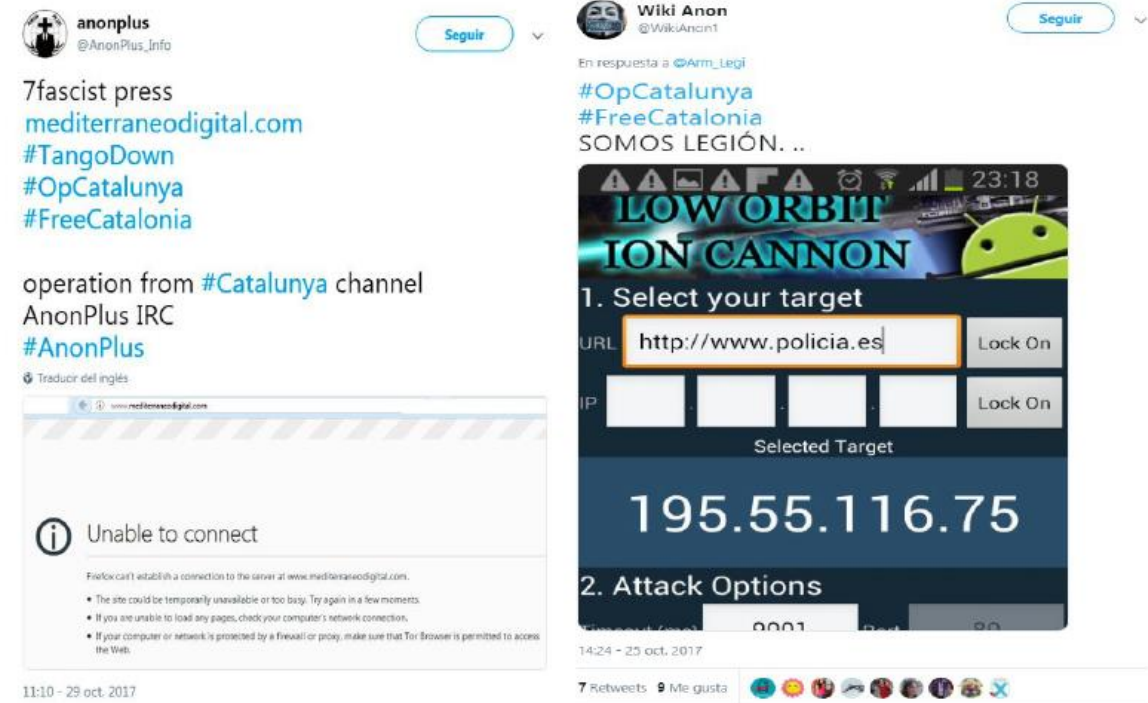
1. Amenazas híbridas
2. Obtención de datos
 1. Etapa de preparación
 1. Social Listening Tools
 2. Representación Big Data
 3. Recopilación y análisis de datos
3. Generación de inteligencia
 1. Prevención y respuesta ante ciberataques
 2. Datos estadísticos y tendencias
 3. Cuentas falsas y seguimiento de bots
4. Conclusiones



Generación de Inteligencia

Prevención y respuesta ante ciberataques

- Keywords relacionadas con ciberataques/ciberincidentes
- Correlación con dominios y keywords relacionadas con Administración Pública Comunitat Valenciana
- Gran cantidad de falsos positivos ☹️



Ejemplo orquestación ataque DDoS publicitado en Twitter

Generación de Inteligencia

Datos estadísticos y tendencias

- Fechas relevantes:

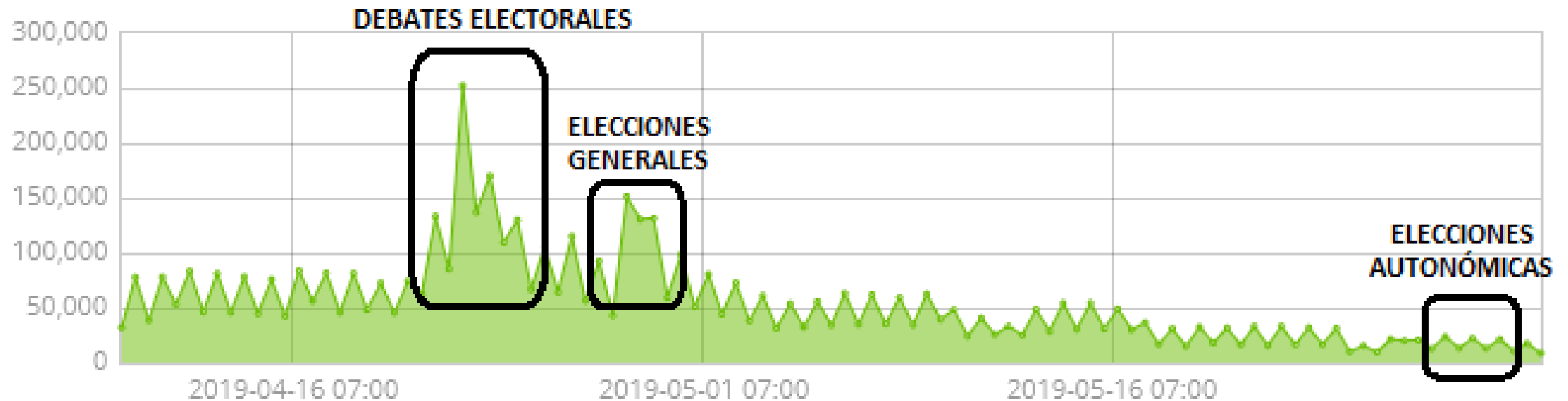
- 16 Abril: Debate a 6 en RTVE
- 22 Abril: Debate a 4 en RTVE
- 23 Abril: Debate Atresmedia
- 28 Abril: Elecciones generales y autonómicas de la Comunitat Valenciana
- 26 Mayo: Elecciones autonómicas

24 Febrero al 6 Junio

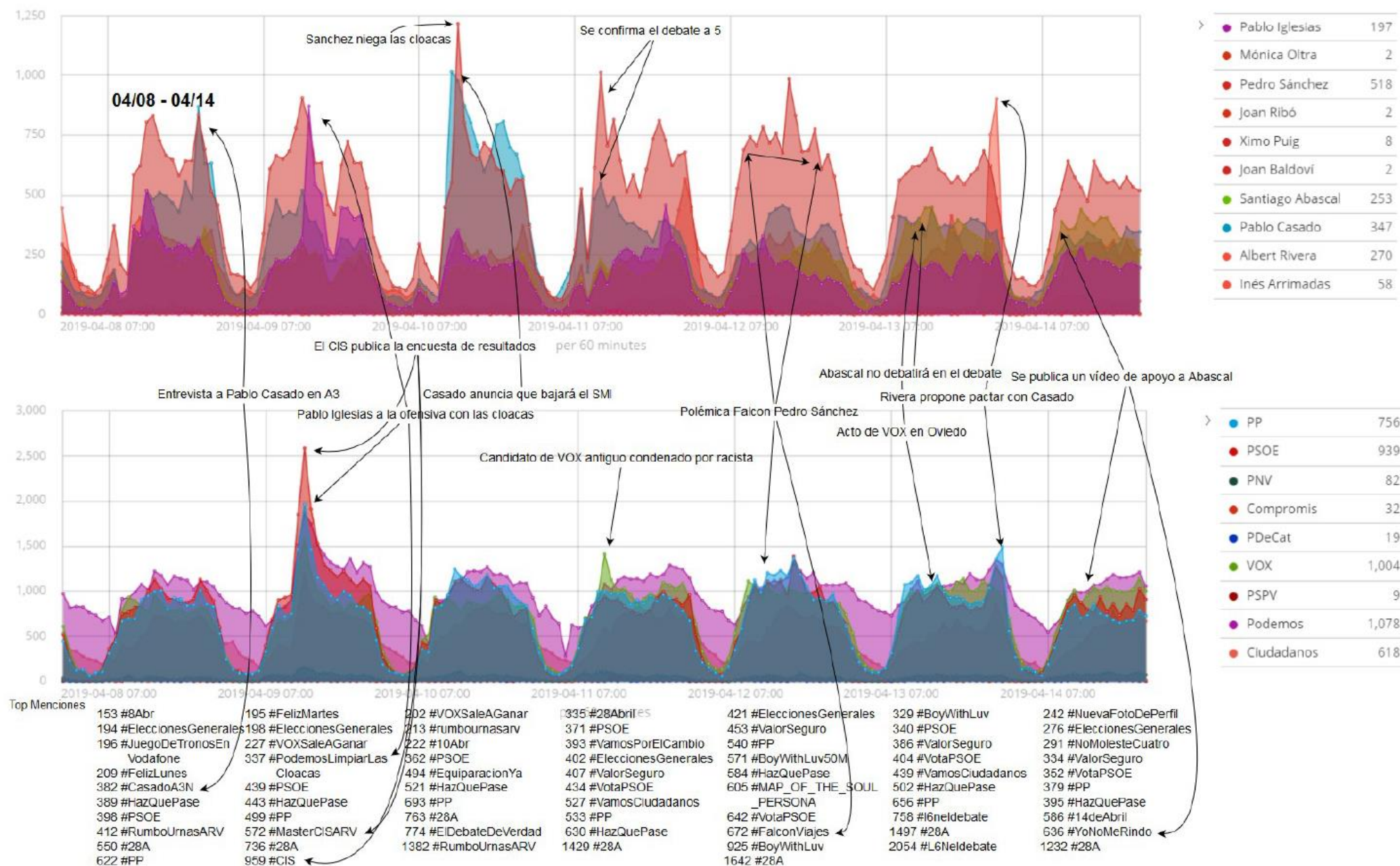
- 8 millones de menciones
- 1.5 millones usuarios
- 17.000 bots confirmados

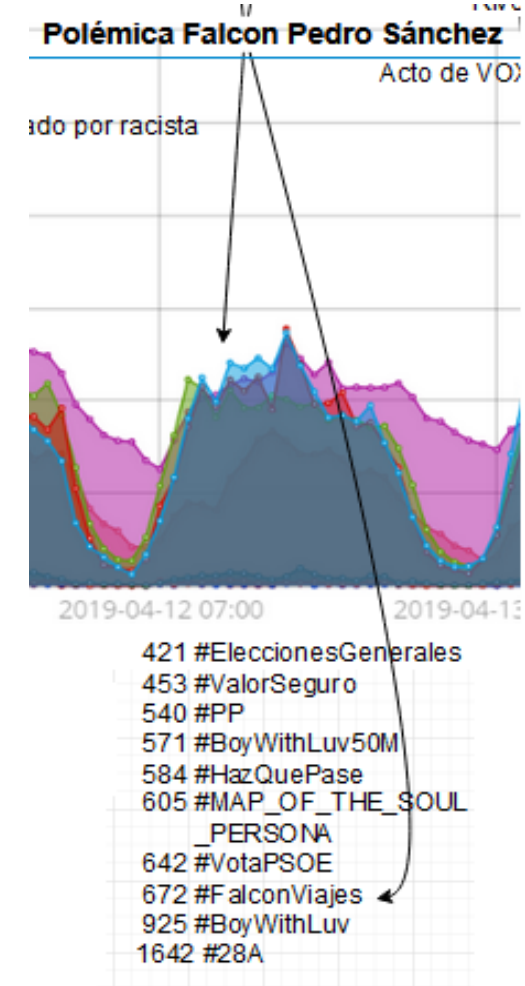
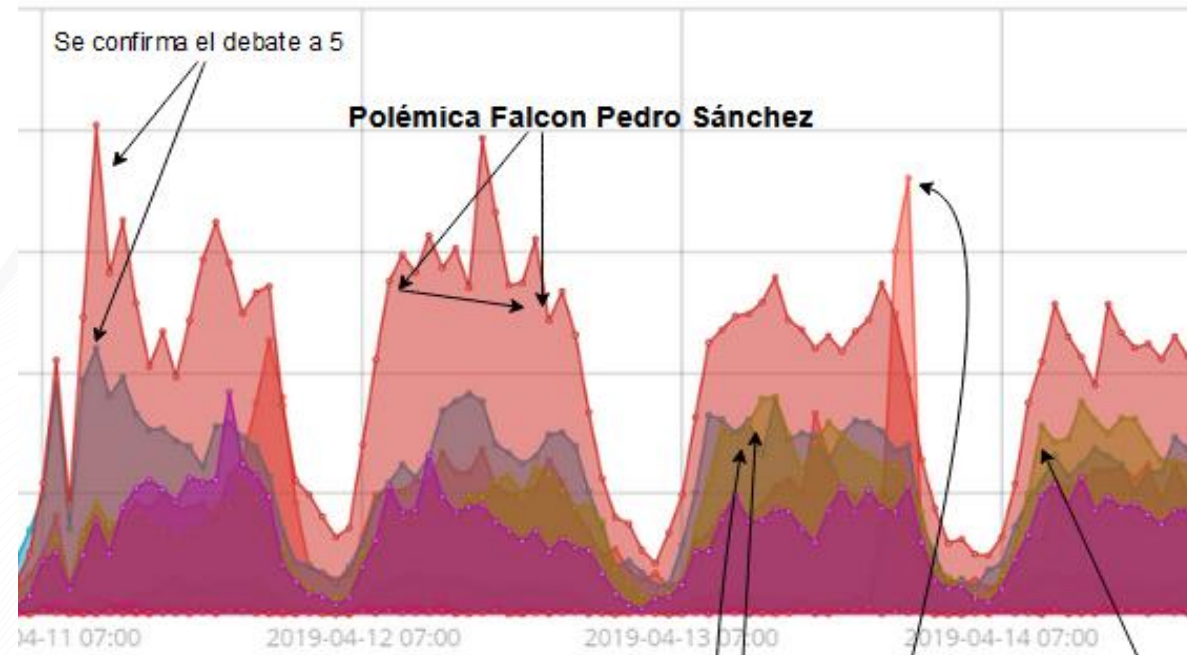
Generación de Inteligencia

Datos estadísticos y tendencias



Repercusión en las redes





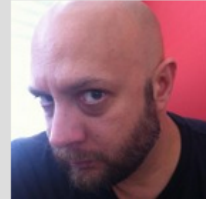
Generación de Inteligencia

Datos estadísticos y tendencias

- Análisis temático
- Automatización de detecciones
- “Analysis Of Brexit-Centric Twitter Activity” + análisis propio tras modelar comportamiento de bots y perfiles falsos

F-Secure NEWS FROM **THE LAB**

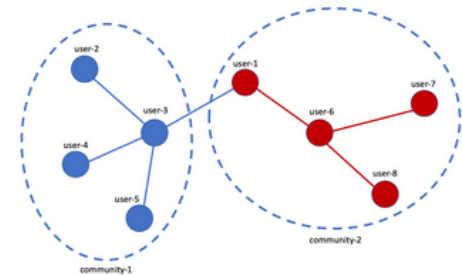
Analysis Of Brexit-Centric Twitter Activity
2019-03-12

Andy Patel

[Permalink](#)

present the results in an easily readable format. This analysis included:

- counts of how many times each user tweeted
- counts of how many times each user retweeted another user (amplifiers)
- counts of how many times each user was retweeted by another user (influencers)
- counts of hashtags seen
- counts of URLs shared
- counts of words seen in tweet text
- a map of interactions between users

By mapping the interactions between users (users interact when they retweet, mention, or reply to each other), a node-edge graph representation of observed conversations can be built. Here's a simple representation of what that looks like:



Generación de Inteligencia

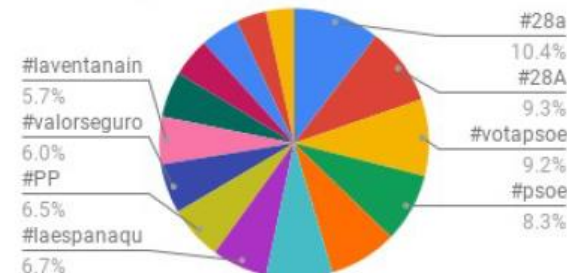
Modelado de comportamientos perfiles falsos y bots

- Cuantas veces tuitea un usuario
- Cuantas veces retuitea un usuario a otro (*amplifiers*)
- Cuantas veces un usuario es retuiteado (*influencers*)
- Cuantas URL se comparten
- Cuentas palabras contiene cada tweet analizado
- Fecha de creación de la cuenta
- Diferencia entre seguidores y seguidos
- Diferencia entre publicaciones propias y RT
- Mapa de interacciones entre usuarios
- Inmediatez en la actividad
- Biografía y fotos de perfil
- Diferencia entre “Nombre Real” y alias usado
- etc

Cuentas



Negativo



Generación de Inteligencia

Cálculo de amplificaciones

$$(\text{SA} + \text{DA}) * 20 + \text{MAX}(\text{PC} - 0.25, \text{NC} - 0.25, 0) * 12 + (\text{1MA} + \text{2MA} + \text{3MA}) * 20$$

The diagram illustrates the calculation of amplification using a formula with color-coded variables. Arrows point from the variables in the formula to their definitions:

- SA** (Suspended Accounts) is represented by a red arrow pointing to the first part of the formula.
- DA** (Deleted Accounts) is represented by a blue arrow pointing to the second part of the formula.
- PC** (Positive Comments) is represented by a green arrow pointing to the third part of the formula.
- NC** (Negative Comments) is represented by an orange arrow pointing to the fourth part of the formula.
- 1MA** (1 Month Accounts) is represented by a purple arrow pointing to the fifth part of the formula.
- 2MA** (2 Month Accounts) is represented by a light blue arrow pointing to the sixth part of the formula.
- 3MA** (3 Month Accounts) is represented by a grey arrow pointing to the seventh part of the formula.

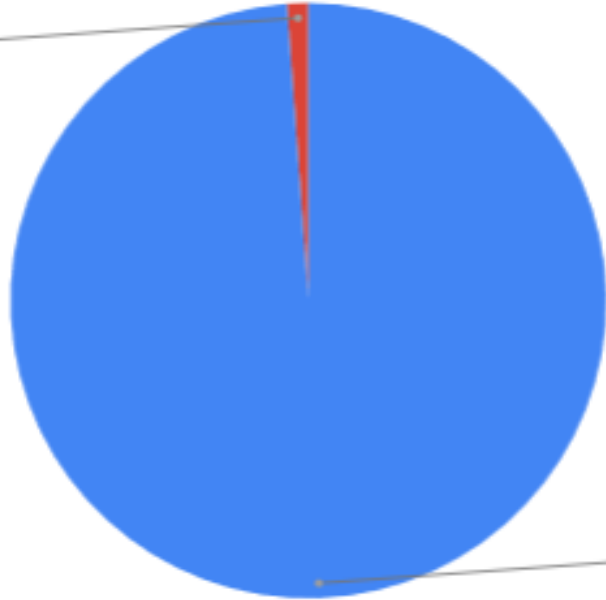
Generación de Inteligencia

Cuentas falsas y seguimiento de bots

Cada bot ha generado de media tres veces mas contenido falso que una cuenta legítima.

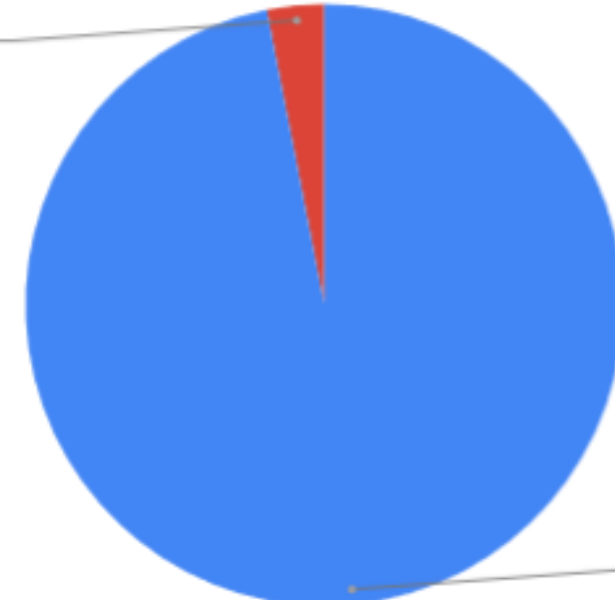
Cuentas

Bots
1.2%



Contenido

Bots
3.1%

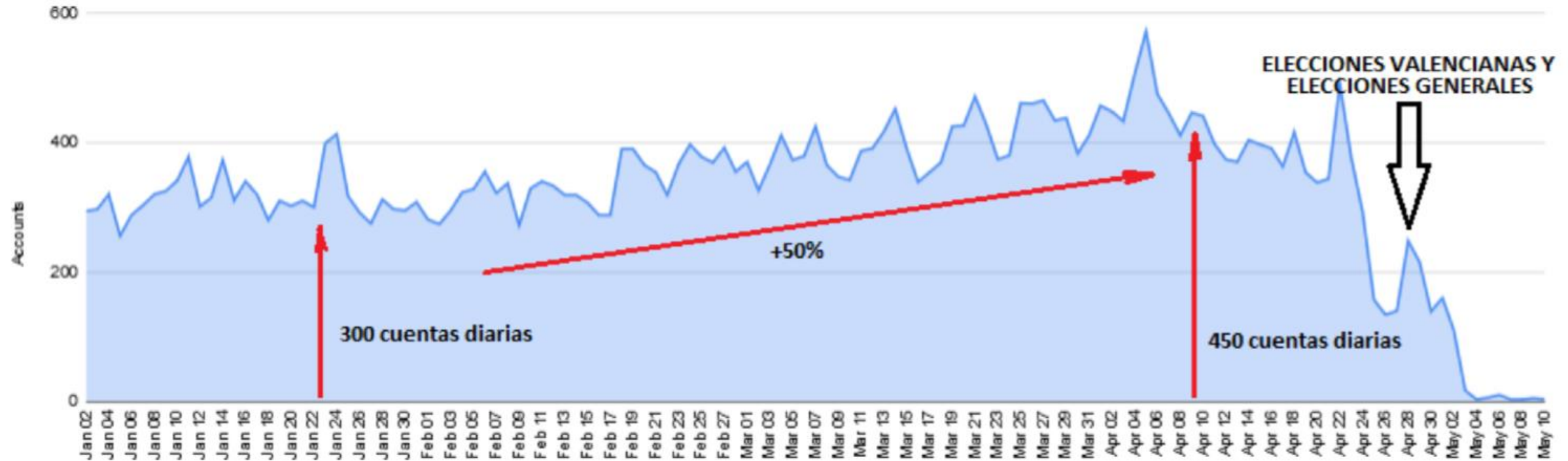


Cuentas falsas y contenido generado por bots

Generación de Inteligencia

Cuentas falsas y seguimiento de bots

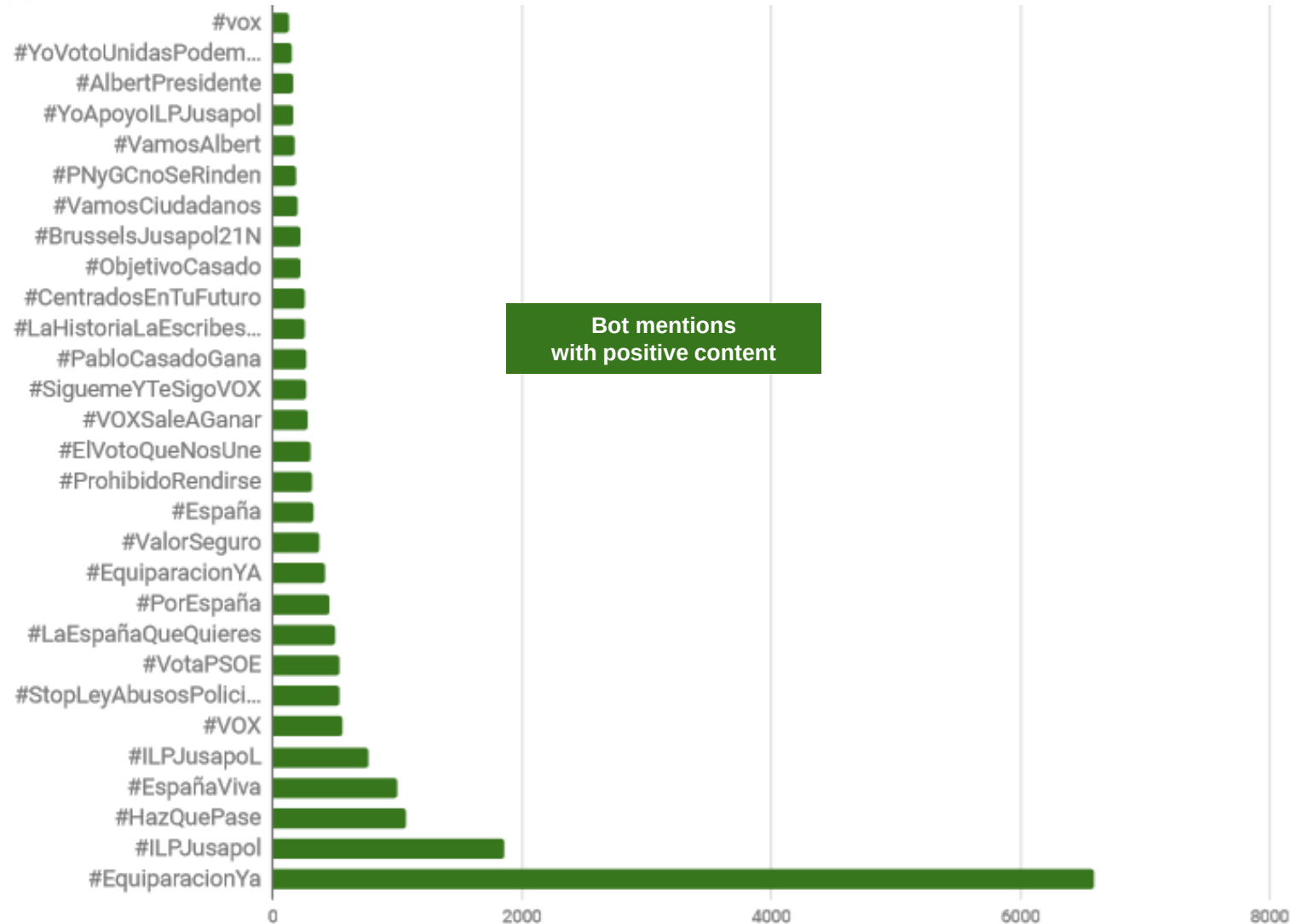
Accounts vs. Date



Cuentas creadas en el periodo preelectoral

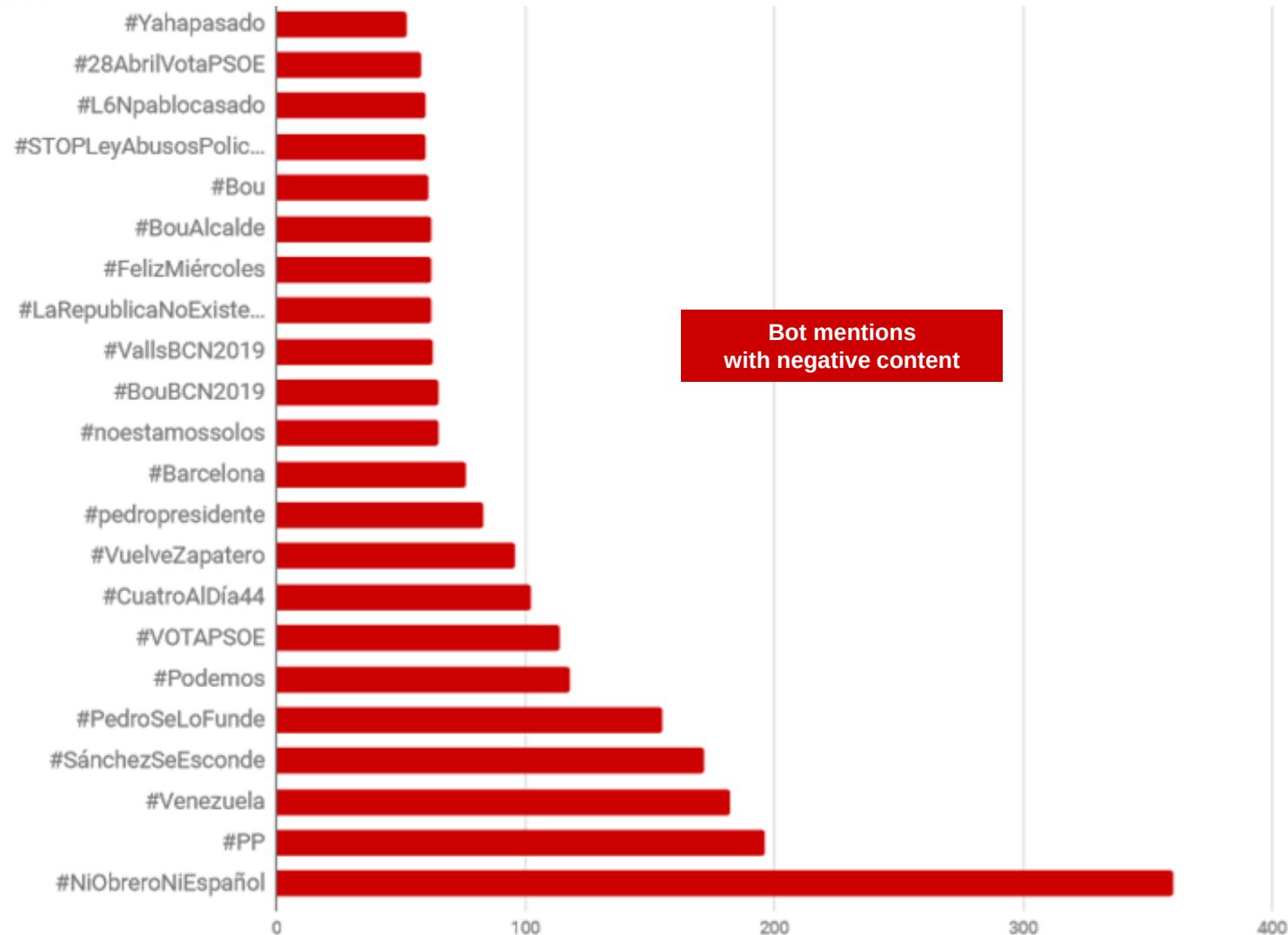
Generación de Inteligencia

Contenido generado por bots con sentimiento positivo



Generación de Inteligencia

Contenido generado por bots con sentimiento negativo



Imágenes generadas por IA

ThisPersonDoesNotExist.com



- Rostros falsos
- Imágenes falsas
- Vídeos falsos



Perfiles falsos

Periodo pre electoral



Perfiles falsos

Periodo pre electoral



FAKE

A large graphic featuring the text '10N' in a bold, sans-serif font. The '10' is white, and the 'N' is a medium blue. To the right of the 'N' is a white line-art icon of a laptop. The entire graphic is set against a dark blue background with a subtle circular pattern.

10N

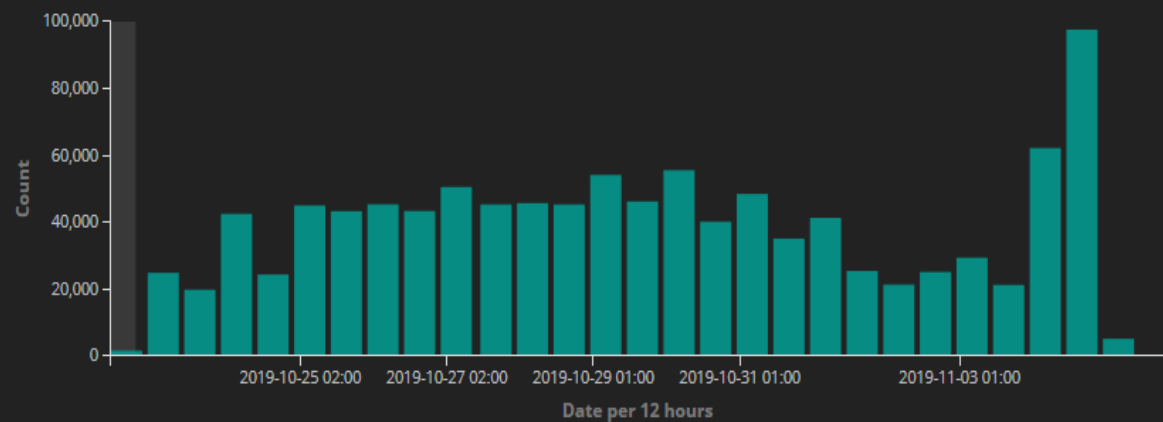
**ELECCIONES
GENERALES**

ELECCIONES 10N (EN PROCESO DE ANÁLISIS...)

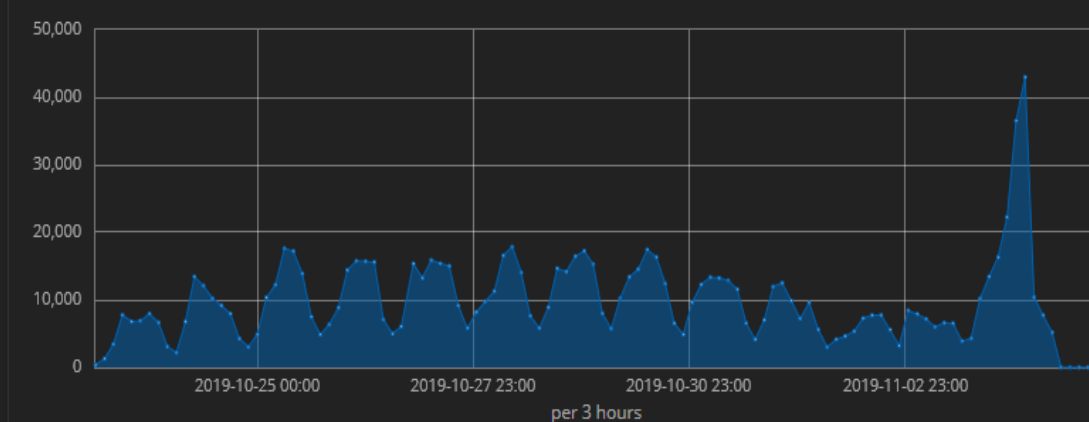
Novedades en el proceso de vigilancia

- Incorporación como Feeds Principales para el análisis de Fake News y perfiles falsos a mas fuentes:
 - Twitter
 - Youtube
 - Sitios de Noticias
 - Foros
 - Blogs
 - ...

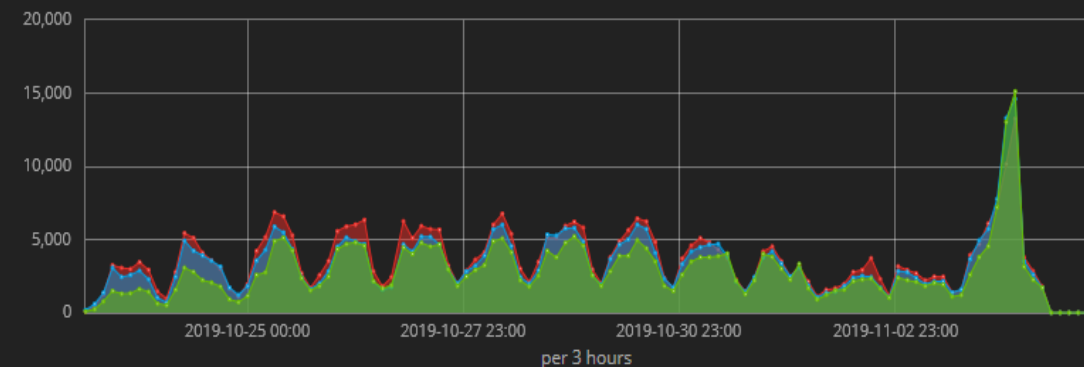
10N - Total



10N - Total Series



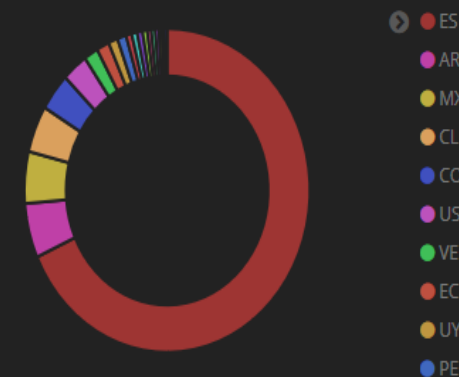
10N - Sentiment



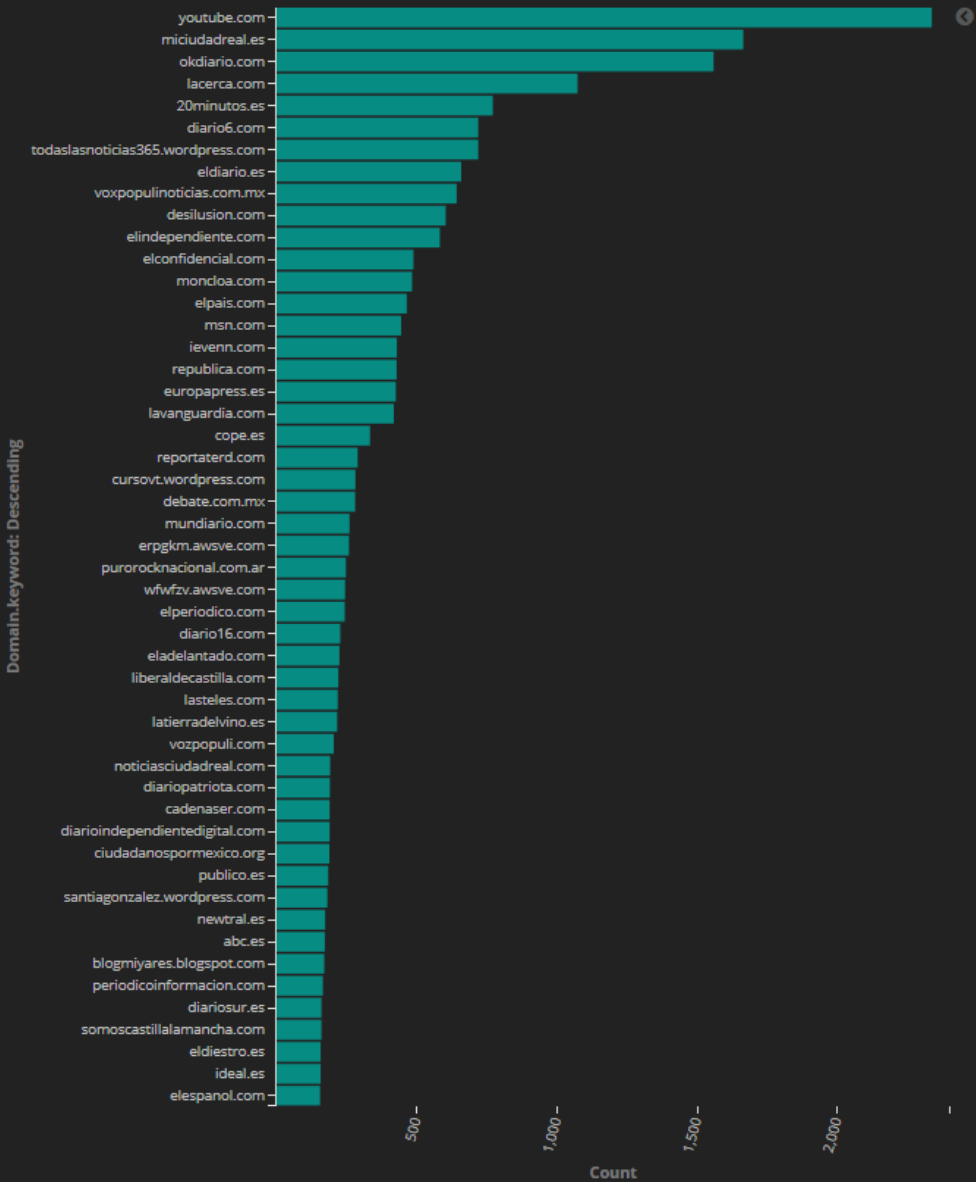
10N - Sentiment Gauge



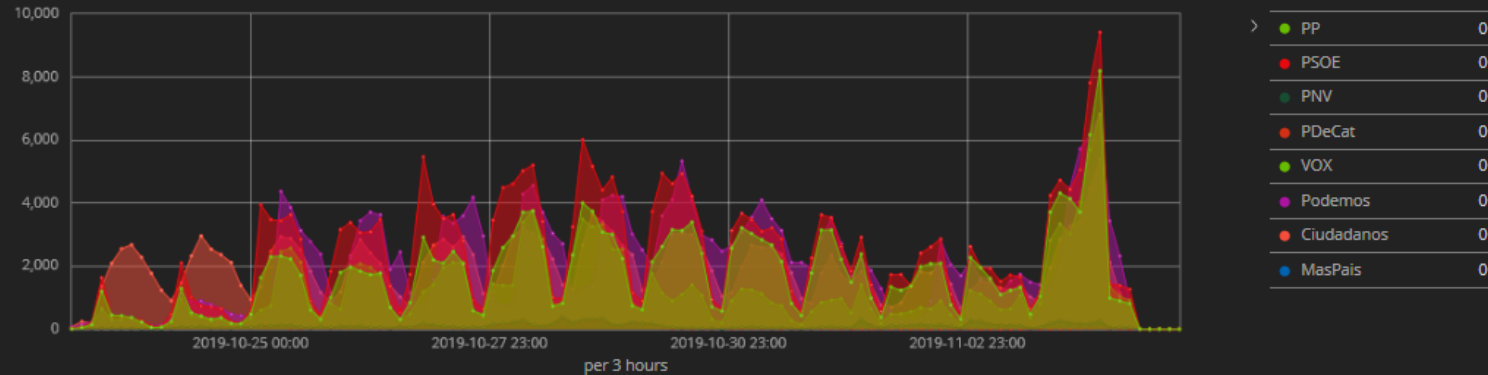
10N - Countries



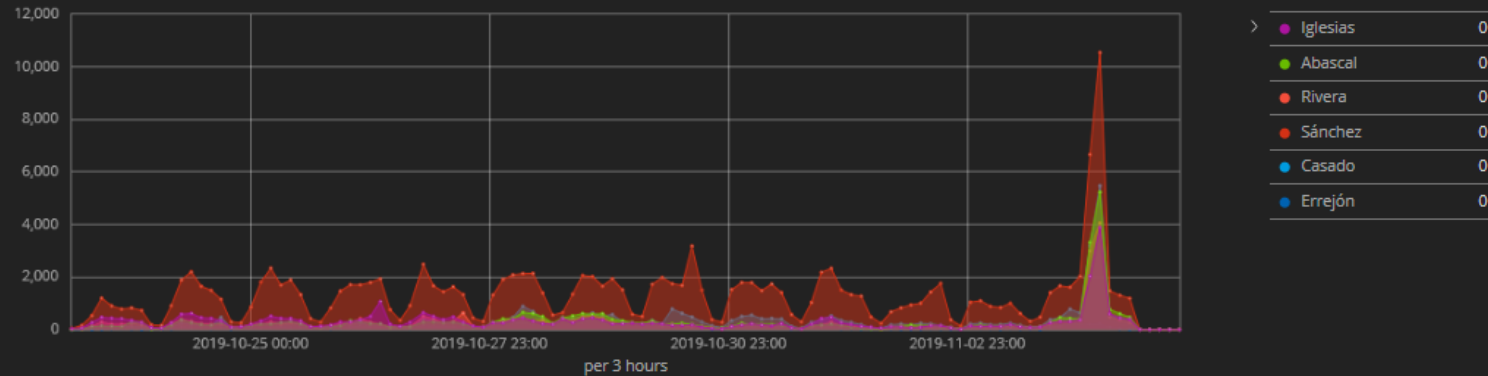
10N - Domains vertical



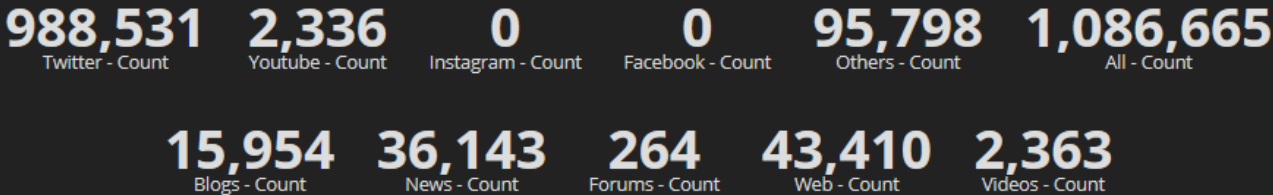
10N - Political Parties



10N - Candidate



10N - Sources



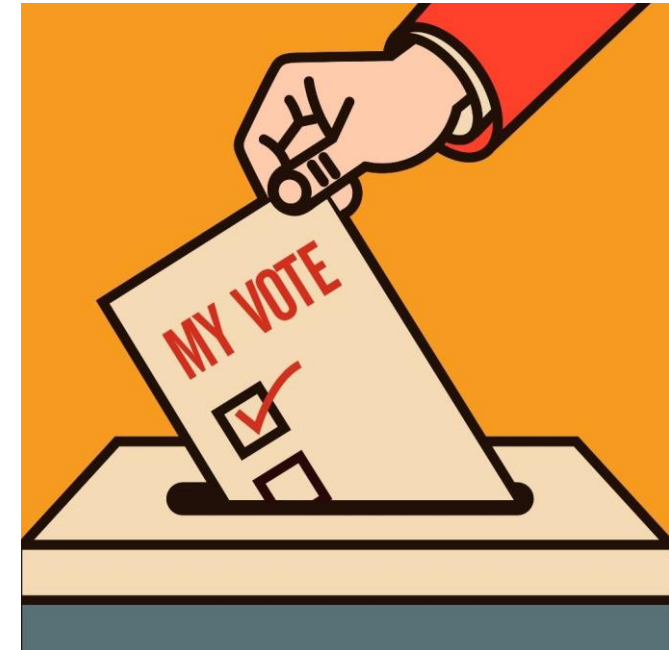
Comparativa

Elecciones 26 A vs 10 N

- El sentimiento de las menciones generadas en las Elecciones del 10N ha tendido mayoritariamente al sentimiento negativo, si lo comparemos con las elecciones anteriores.
- Se ha detectado un menor incremento de uso de bots
- **Análisis en proceso**

Índice

1. Amenazas híbridas
2. Obtención de datos
 1. Etapa de preparación
 1. Social Listening Tools
 2. Representación Big Data
 3. Recopilación y análisis de datos
3. Generación de inteligencia
 1. Prevención y respuesta ante ciberataques
 2. Datos estadísticos y tendencias
 3. Cuentas falsas y seguimiento de bots
4. Conclusiones



Conclusiones

- No se han identificado ciberataques significativos contra los activos TIC de Generalitat Valenciana que hubieran puesto en riesgo la seguridad de las elecciones
- No se ha identificado en fuentes públicas la organización de ciberataques contra los activos TIC de Generalitat Valenciana ni tampoco contra otros organismos públicos de la Comunitat Valenciana
- No se ha identificado en fuentes públicas la organización de ciberataques contra las empresas destinadas al escrutinio de las elecciones
- Se ha identificado el aumento de uso de perfiles falsos para realizar labores de amplificación de contenido y desinformación, conforme se acercaban las fechas de las elecciones. Estos perfiles falsos hacen uso de herramientas automáticas y han sido creados para dar a apoyo a diferentes partidos políticos
- Se ha identificado que muchos de los perfiles falsos detectados, poseían como imagen de perfil rostros humanos creados a través de algoritmos basados en inteligencia artificial, es decir, rostros de personas que no existen

Trabajos futuros

- Desarrollo herramienta propia para detección de perfiles falsos basada en Machine Learning
- Automatización tareas de análisis de la información
- Integración de todas las nuevas herramientas con nuestro SIEM, GLORIA (Emas SOM)

Vigilancia Digital en procesos electorales *Social Intelligence*

Maite Moreno & Adrián Antón

CSIRT-CV, S2Grupo

csirtcv@gva.es



UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa



GENERALITAT
VALENCIANA



CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional