Redes Sociales: ¿Podemos detectar contenido malicioso?

Edith Rivero

Agenda

1. Introducción
2. Contenido malicioso
    - 2.1. Delitos informáticos
    - 2.2. En las redes sociales. Caso: Facebook
3. Machine Learning
    - 3.1.Data science - Data mining - Machine Learning
    - 3.2.ML: Aprendizaje supervisado
4. Aplicación
    - 4.1. Cuestionamiento
    - 4.2. Extracción y resultados
5. Consideraciones de seguridad
6. Conclusiones

"Todos podemos ser víctimas del cibercrimen, lo único que nos hace vulnerables es mantener una conexión a internet"

Los expertos.

Contenido malicioso

- Informe del Observatorio de Delitos Informáticos de Latinoamérica (**ODILA**): El acceso indebido a datos o sistemas, los fraudes y estafas son los más denunciados.

- Informe de **Symantec**: Incremento de ataques ramsonware, en su mayoría llegan a través mensajes de correo electrónico o durante la navegación en Internet.

Delitos Informáticos

Penalidades de acuerdo a:

- Valor de los datos
- Consecuencias de pérdida de privacidad, confidencialidad e integridad

Transgredir legislaciones - malware - spyware

Acceso ilícitos

Acceso a todo o parte de un sistema informático con vulneración de las medidas de seguridad.

Atentado a la integridad de los datos informáticos

Daño y toda alteración que hace inaccesibles los datos informáticos.

Atentado a la integridad de los sistemas informáticos

Cuando se inutiliza total o parcialmente un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios.

Proposiciones a niños, niñas y adolescentes con fines sexuales

A través de internet o medio análogo contacta con un menor de 14 años para obtener de éste, material pornográfico o para llevar a cabo actividades sexuales.

Tráfico ilegal de datos

El que crea, ingresa o utiliza indebidamente una base de datos para comercializar o traficar.

Interceptación de datos informáticos

El que intercepta datos y transmisiones no públicas incluidas las emisiones electromagnéticas

Fraude informático

Ilícitamente altera o clona datos o sistemas informáticos.

Suplantación de identidad

Mediante las TI suplanta la identidad de una persona natural o jurídica ocasionando algún perjuicio, material o moral.

Abuso de mecanismos y dispositivos informáticos

El que fabrica, distribuye u obtiene programas informáticos, códigos de acceso o cualquier dato para cometer delitos informáticos.

Discriminación (Código penal)

El que discrimina... "a través de internet u otro medio análogo".

Contenido malicioso en las redes sociales

Específicamente en las redes sociales en línea, el contenido malicioso pude ser fuente de:

- Fraude informático (phising, XSS)
- Atentado a la integridad de los datos y sistemas informáticos (exploitKits, virus, ejecución de scripts)
- Discriminación
- Proposiciones con fines sexuales a menores

Red social: Facebook

- Publicaciones
- Comentarios (incluidas las respuestas)
- Mensajes

Latin America Loves Facebook

By some measures, the social network's reach is highest in Argentina

March 2, 2016 | Social Media

SHARE EMAIL PRINT

Facebook is by far the top social site in Latin America, as in many markets around the world.

Facebook Users and Penetration in Latin America, by Country, 2014-2019

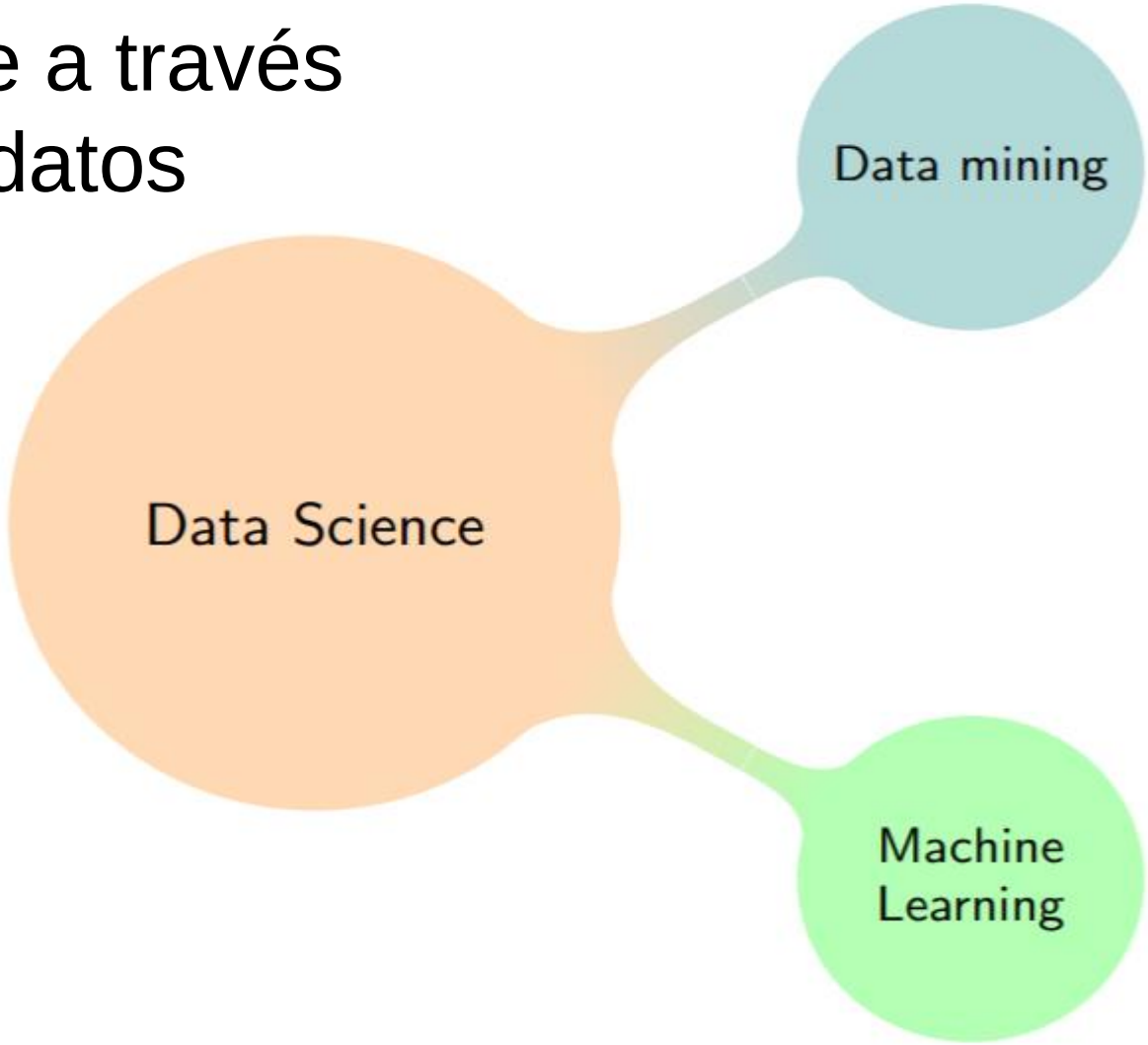
	2014	2015	2016	2017	2018	2019
Facebook users (millions)						
Brazil	72.0	79.0	87.0	92.5	94.8	97.0
Mexico	40.0	45.5	51.8	56.9	61.0	64.7
Argentina	18.2	19.7	20.9	21.7	22.4	23.0
Other	63.9	73.2	81.5	87.5	92.9	97.4
Latin America	**194.1**	**217.5**	**241.1**	**258.6**	**271.1**	**282.2**
Facebook user penetration (% of social network users)						
Argentina	94.8%	94.8%	96.3%	96.3%	96.4%	96.5%
Mexico	94.1%	94.5%	94.7%	94.8%	94.9%	95.0%
Brazil	92.2%	91.4%	93.3%	94.5%	94.2%	94.1%
Other	89.6%	88.4%	90.9%	91.1%	91.2%	91.1%
Latin America	**91.9%**	**91.3%**	**93.0%**	**93.5%**	**93.5%**	**93.4%**
Facebook user penetration (% of internet users)						
Mexico	67.3%	70.0%	73.3%	75.3%	75.8%	76.2%
Brazil	66.9%	69.5%	72.6%	75.0%	75.3%	75.5%
Argentina	67.0%	68.0%	70.0%	71.0%	72.0%	72.6%
Other	57.6%	61.0%	64.3%	66.0%	67.5%	68.6%
Latin America	**63.6%**	**66.4%**	**69.5%**	**71.4%**	**72.3%**	**72.9%**

eMarketer last estimated social media usage in Latin America in July 2015. Facebook is set to reach 39.0% of the total population of the region this year—equivalent to 69.5% of internet users and a dramatic 93.0% of social network users.

By some measures, Facebook's reach is highest in Argentina, where 96.3% of social network users and 47.6% of the total population will use the site this year.

Fuente: eMarketer, 2016

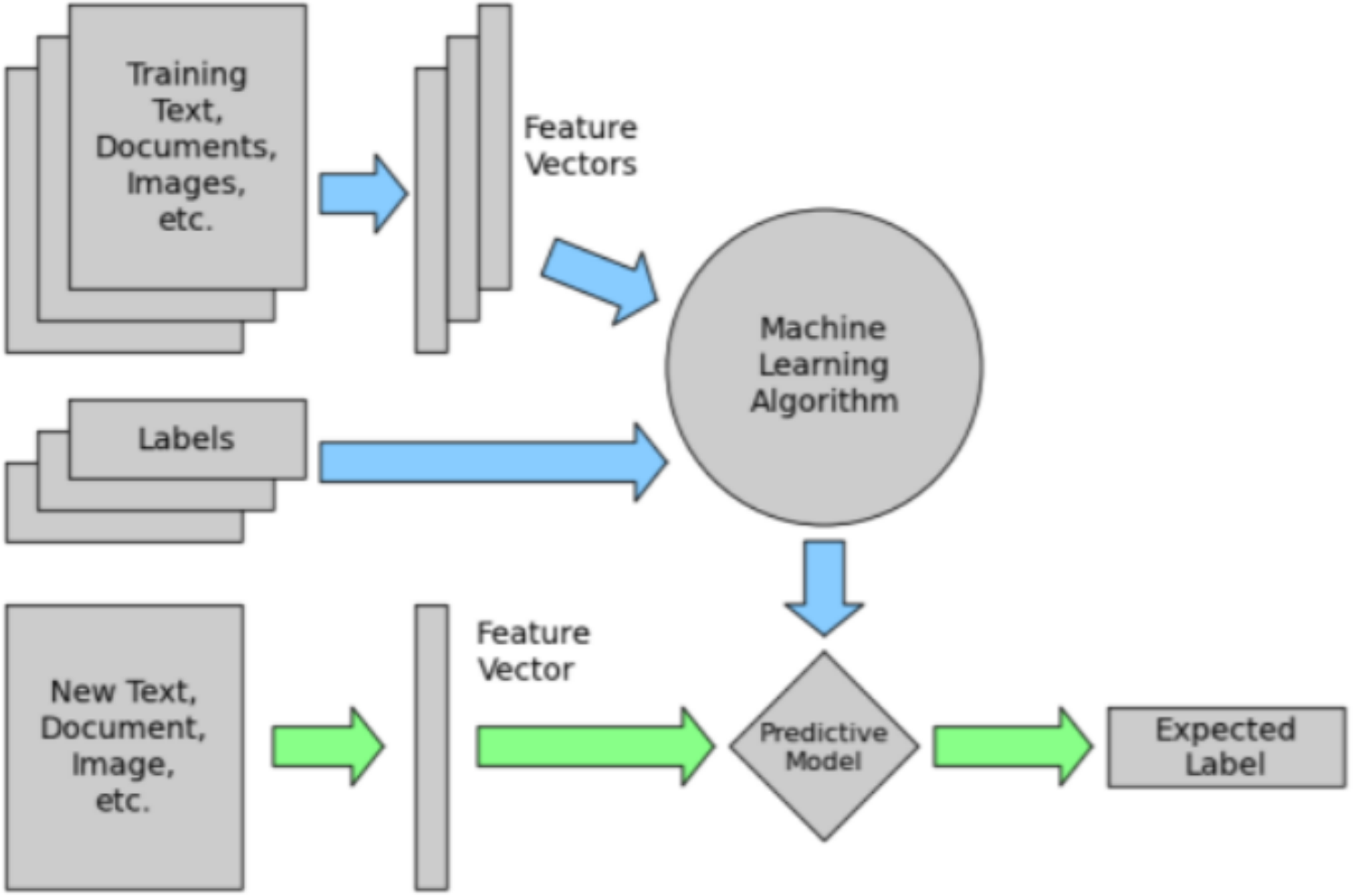
Aprendizaje a través de los datos



Aplicaciones de ML

- Detección de malware mediante las colección de firmas de **virus**.
- En los sistemas de detección de eventos de seguridad (Security and Event Management - **SIEM**)
- Mitigación de fraude en el **comercio electrónico**, mediante los patrones de compra de cada usuario.
- Detección de **spam en mail** utilizando (IP, asunto, longitud del mail, cantidad de imágenes, contenido de caracteres especiales, etc.)

ML: Supervisado



Fuente: http://blog.kaggle.com

ML: Supervisado

Para permitir que el algoritmo aprenda a transformar las entradas en sus respectivas salidas es necesario proporcionar instancias de entrenamiento **(training sets)** y cada instancia usualmente es representado por un conjunto de características **(features)**.

Conozcamos un poco del estado del arte…

Detecting Spam URLs in Social Media via Behavioral Analysis [Cao and Caverlee 2015]

La detección se hizo mediante: Links posteados en públicamente en tweets y mediante los patrones de clics obtenidos de **Bitly API** (permite obtener estadísticas de las URLs de ese servicio).

Discerning spam in social networking sites [Yadav 2016]

Se coleccionaron los datos de fanpages públicas buscando (p.e.: "reward", "bit.ly" y "share"). Se identificaron a los respectivos usuarios y de éstos se obtuvo información a través de su perfil público. Esto permitió clasificar el contenido entre spam y no spam y detectar posibles spammers.

COMPA: Detecting Compromised Accounts on Social Networks [Egele et al. 2013]

La base contiene datos entre (2007-2009) en ese momento Facebook permitía obtener información de las redes que compartían la ubicación geográfica (ahora deshabilitado por temas de privacidad). Se analizó el comportamiento de los usuarios para detectar cuentas maliciosas.

Facebook Immune System [Stein 2011]

Este sistema fue creado para evitar malware, phising, spam, cuentas falsas y creepers. Se alimenta del **feedback del usuario (explícito e implícito)** y **el conocimiento general**.

Cuestionamiento

- ¿Resulta conveniente experimentar con la colección de datos existentes?

- ¿Existirán nuevos patrones o estilos de publicación de contenido malicioso?

Herramientas

Web scrapping/web harvesting/data extraction

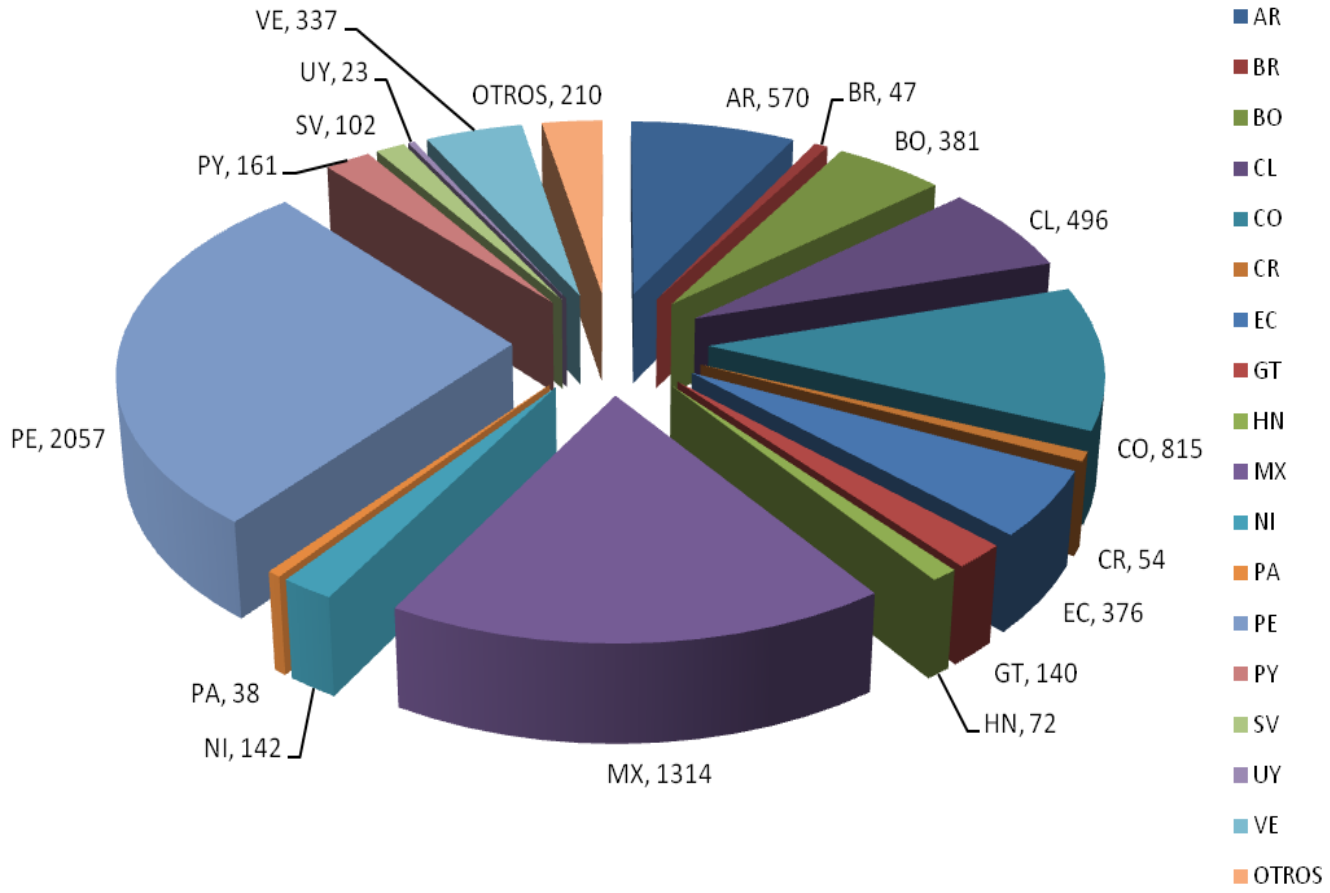
- Pyhton: Scrapy, Pyspider, Cola, Beautiful Soup
- Ruby: Upton, Wombat Javascript: Node Crawler, Simplecrawler
- PHP: Goutte
- Utilizar APIs (Facebook, Twitter, etc)
- Facebook Scrapper: Script para obtener publicaciones y comentarios.

Extracción

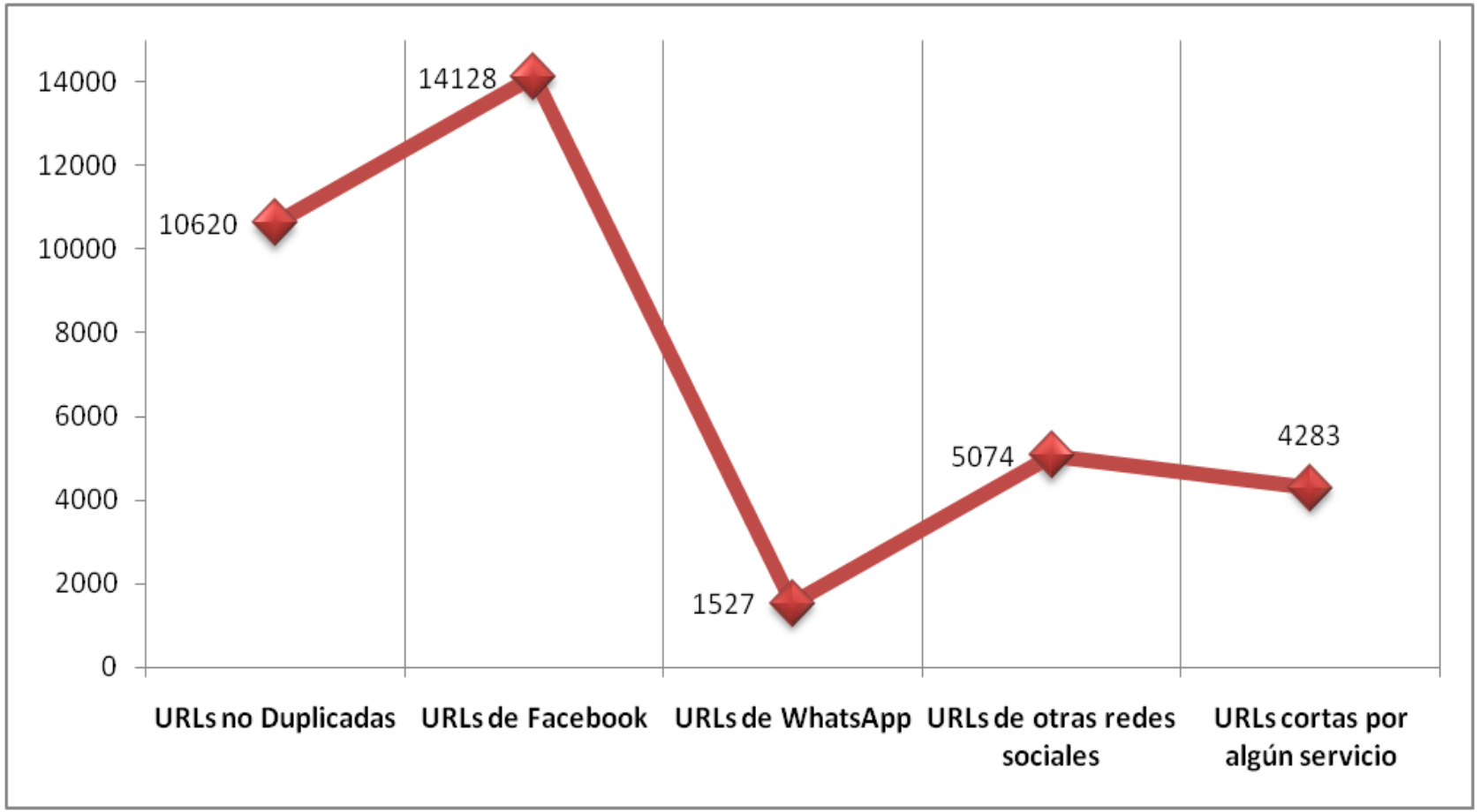
comment_id	status_id	parent_id	comment_message	comment_author	comment_published	comment_likes
1535376953161950	209184189114578_1535348389831478	1535373289828980	No me sale ðŸ˜	Carlos Hum	26/03/2017 07:33	0
1535386093161040	209184189114578_1535348389831478	1535373289828980	Dejaste espacio	Gustavo Ad	26/03/2017 07:38	0
1536842026348780	209184189114578_1536446303055020		No ..como asi ..	Isisdora Rui	27/03/2017 00:01	0
1537446369621680	209184189114578_1536446303055020		https://chat.whatsapp.com/D9i5sBUrvWT8DU	Jimenez Leo	27/03/2017 10:36	0
1537976512901990	209184189114578_1536446303055020		https://chat.whatsapp.com/28IrQE6ELmb1YA	Camilo Urru	27/03/2017 18:00	0
1530220627010920	209184189114578_1530195017013482		https://www.google.com.co/search?kgmid=/g	Alejandro Pi	23/03/2017 08:26	0
1530585700307740	209184189114578_1530195017013482		ALGO ASI https://www.youtube.com/watch	Jhon Robert	23/03/2017 13:22	0
1531241036908880	209184189114578_1530195017013482		https://youtu.be/g_w7GJBfiY	Yuli Andrea	23/03/2017 21:02	0
1531252180241090	209184189114578_1530195017013482		https://youtu.be/klIF0nhsxx	Yuli Andrea	23/03/2017 21:10	0
1531987650167550	209184189114578_1530195017013482		Hola damas y caballeros. Presento mi oferta de prestamo de dinero, pueden ponerse en contacto conmigo.	Cecile Dubo	24/03/2017 09:22	0
1537415809624730	209184189114578_1533342606698723		cuenta de Facebook, Ahora si chicos, esta aplicacion es Real, Funcional al 100% Solo son 3 pasos sencillos y listo Te invito a probarlo, no tienes nada que perder: Aca el lick de la aplicacion de Facebook :3 https://www.latina1005fm.com.ve/seguidore	Camilo Urru	27/03/2017 10:12	0

31 páginas y **36** grupos.
125283 URLs y **7336** números de teléfonos - 3 meses de recolección

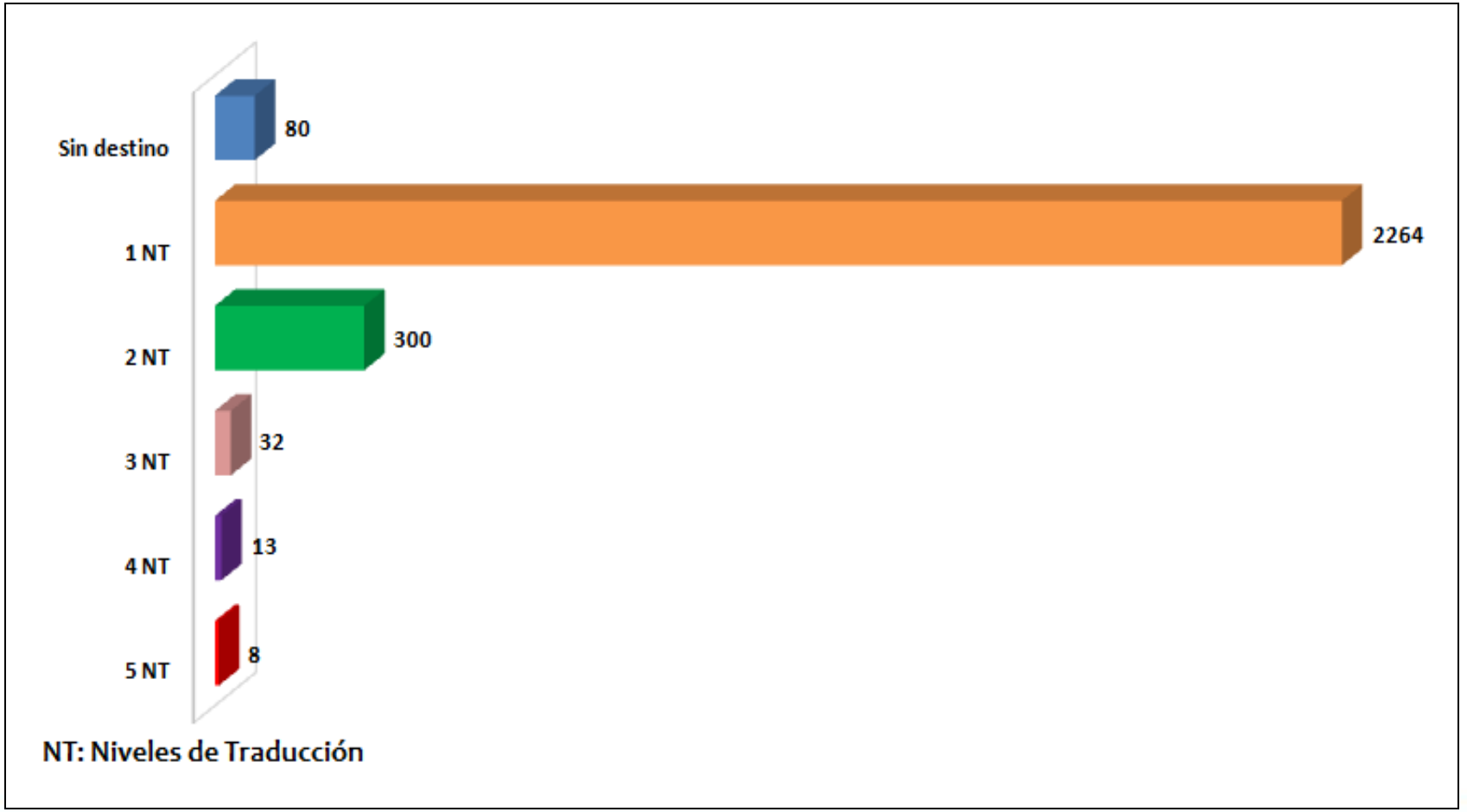
Números de teléfono por país



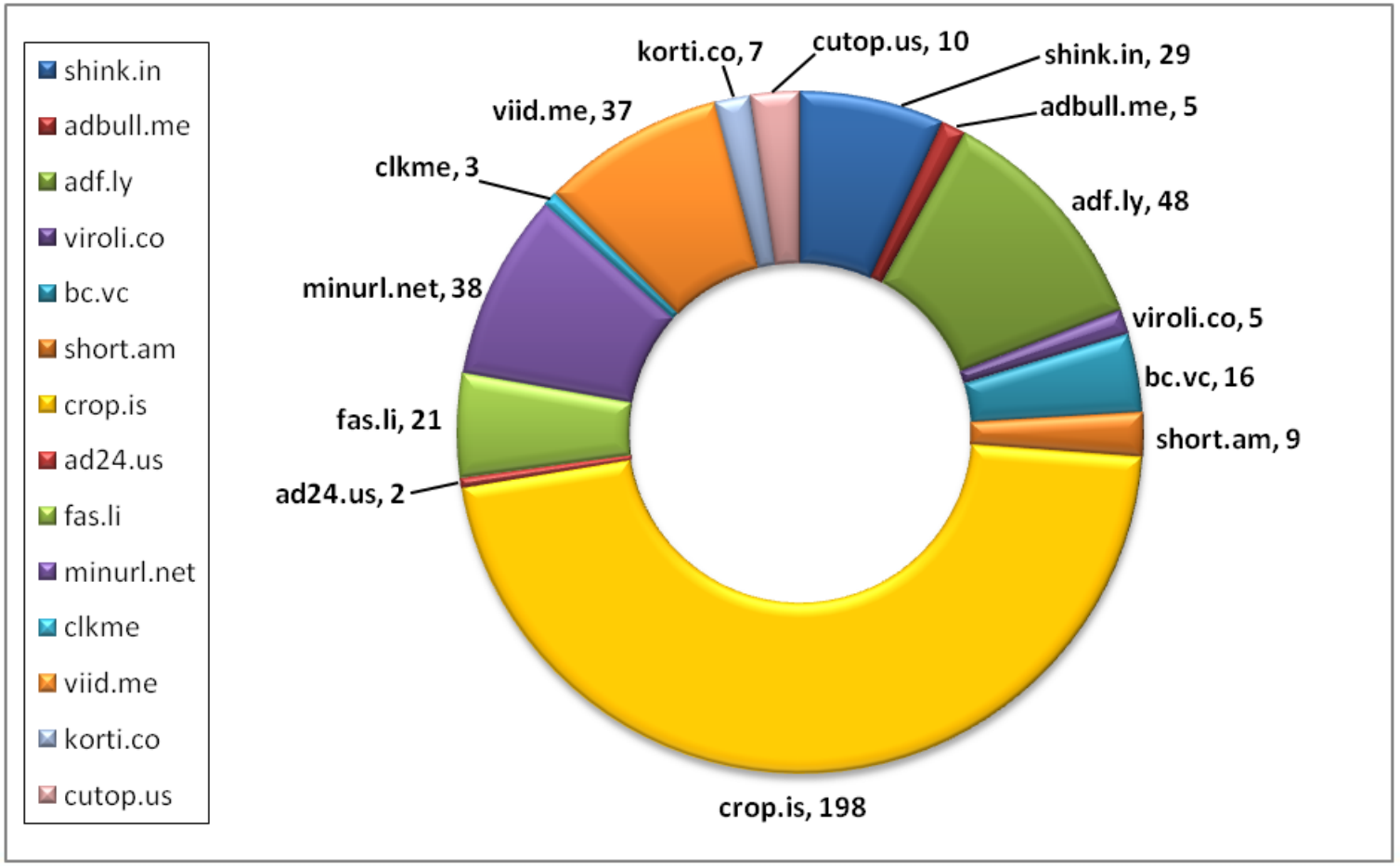
Clasificación de URLs recolectadas



Niveles de traducción de las URLs cortas



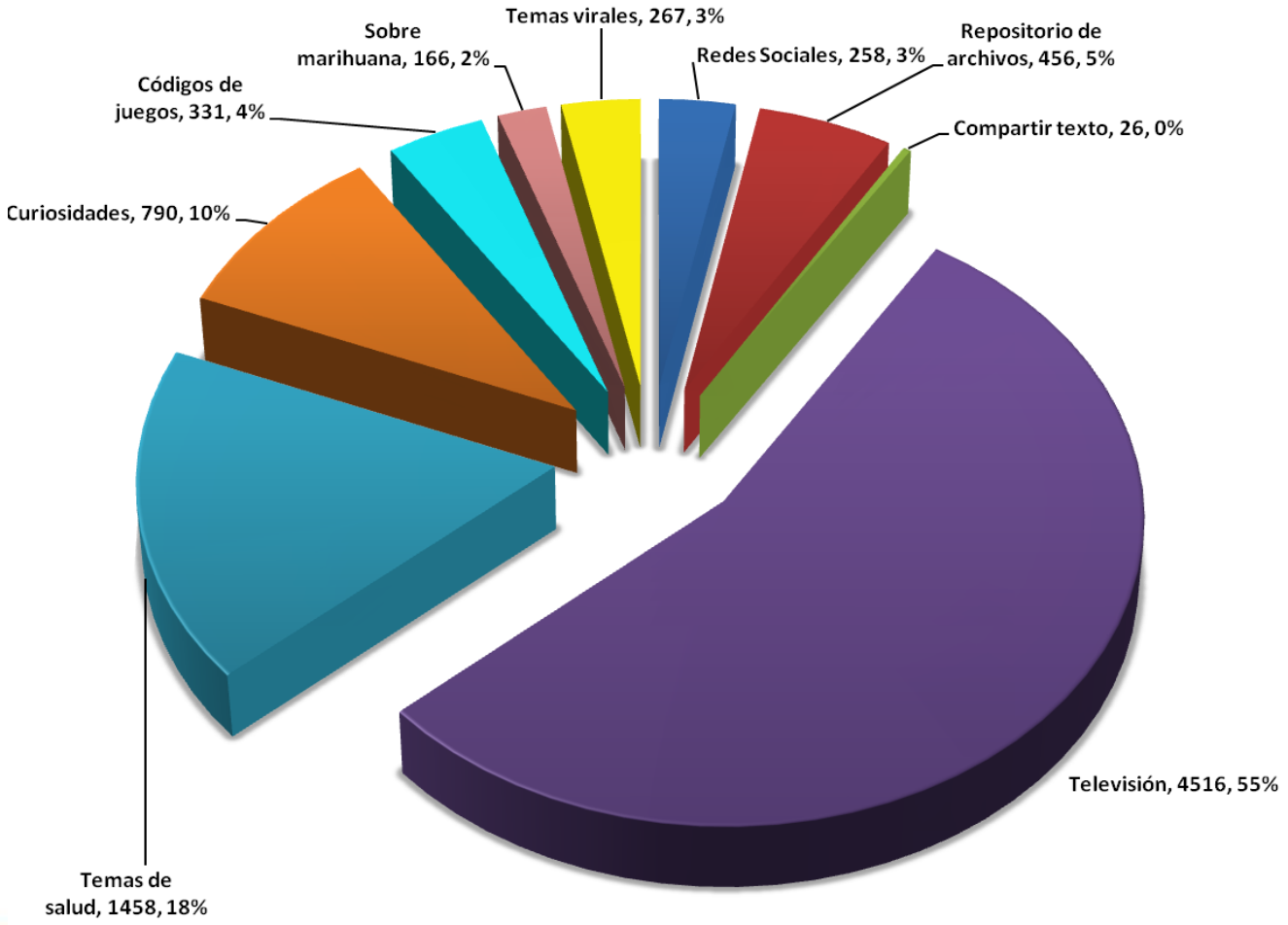
Servicios utilizados en los niveles de traducción de las URLs cortas



Resultados de URLs destino por Niveles de Traducción (NT)

URL destino	1 NT	2 NT	3 NT	4 NT	5 NT
mediafire.com	16	6	0	1	1
nolocreo.com	1	31	0	0	0
mega.nz	274	4	15	11	7
paste2.org	0	11	15	0	0
elfqrin.com	0	2	1	1	0
aldeaviral.com	3	28	0	0	0
viralymedio.com	1	20	0	0	0

Distribución de URLs agrupadas por tipo de contenido



Selección de características

Identidad del sitio

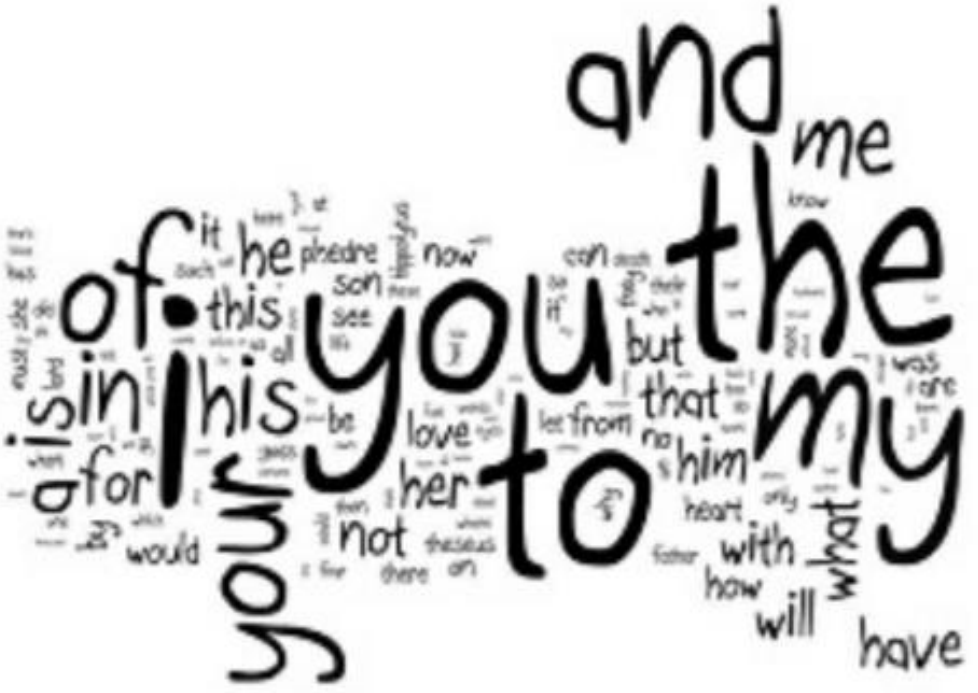
- (1)Domain
- (2)Title
- (3)Description
- (4)Http_Equivalent_Refresh
- (5)Script_Location_Redirect
- (6)Total_Cookies_Quantity
- (7)Own_Cookies_Quantity
- (8)Country
- (9)Email
- (10)Days_Exp_Creation

Referencia a URLs de sitios externos

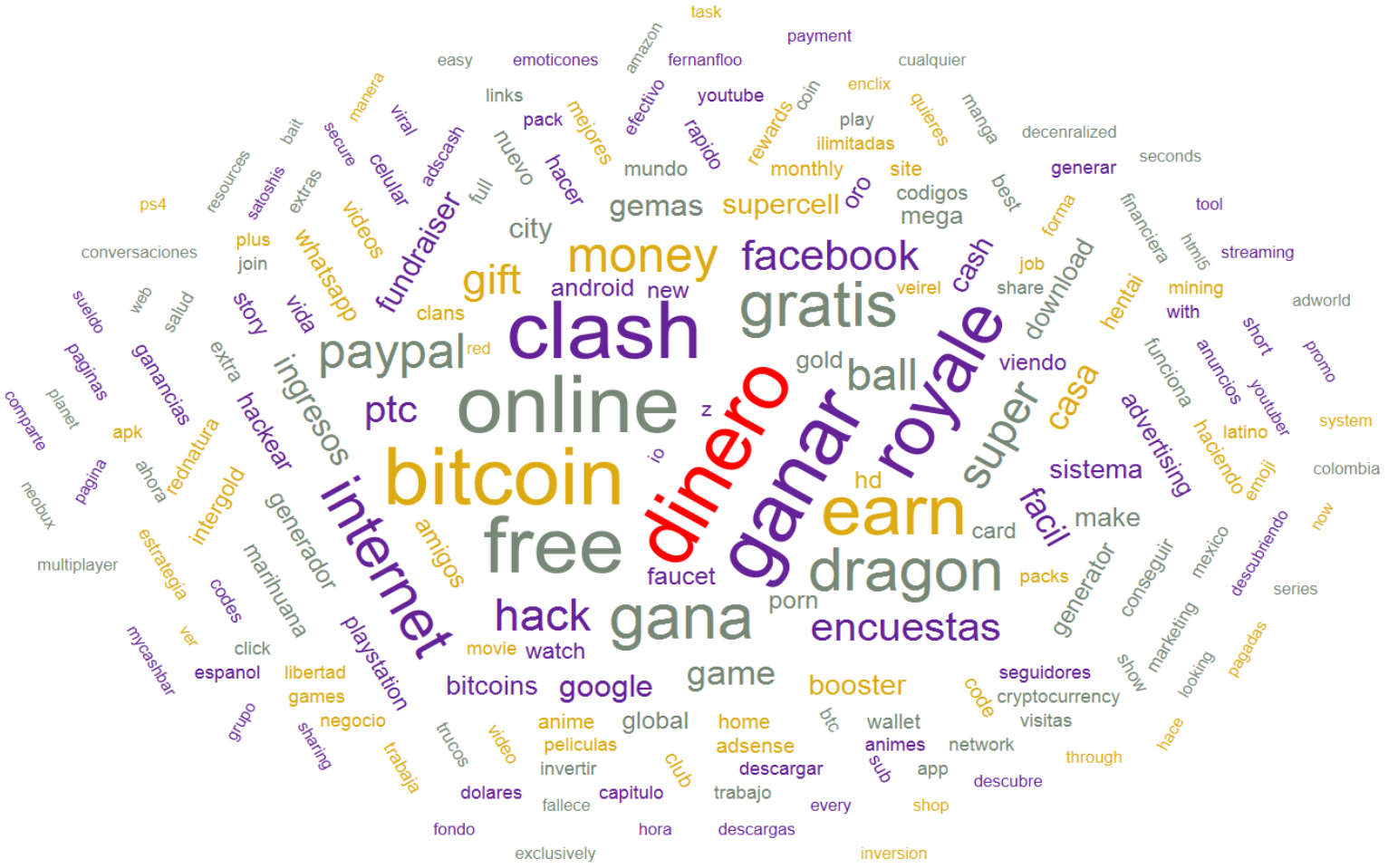
- (11)Days_Update_Creation
- (12)Days_Exp_Update
- (13)Days_Today_Creation
- (14)Total_Form_Action
- (15)Own_Form_Action
- (16)Total_Script_Source
- (17)Own_Script_Source
- (18)Total_A_References
- (19)Own_A_References - (20)Total_Img_Sources
- (21)Own_Img_Sources - (22)Quantity_iFrames

Pre procesamiento de datos

- Eliminar las stopwords.
- Stemming & lemmatization (reducir formas inflexionales de la palabra).
- Eliminar caracteres no reconocibles.
- Eliminar onomatopeyas.
- Eliminar comodines como [PHOTO], [STICKER].



Nube de palabras dentro de los títulos recolectados



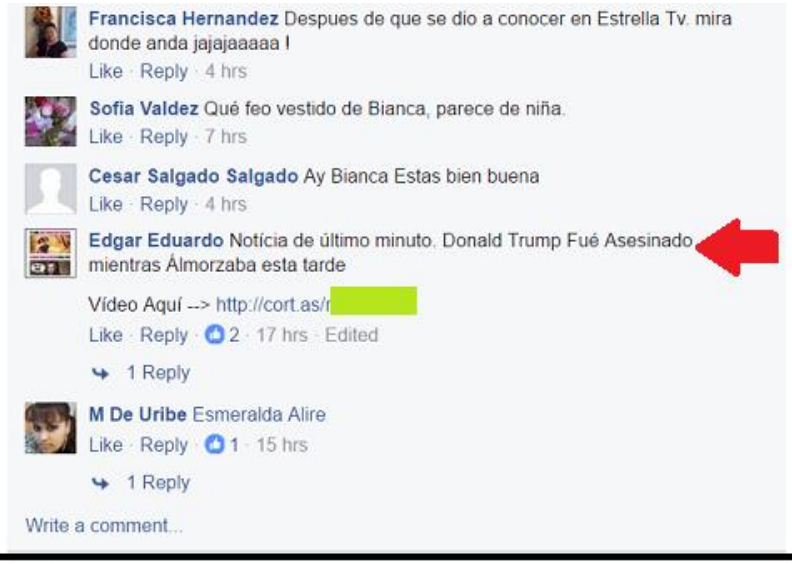
SITIOS DE BLOGS

1 y 2: Contenido sospechoso

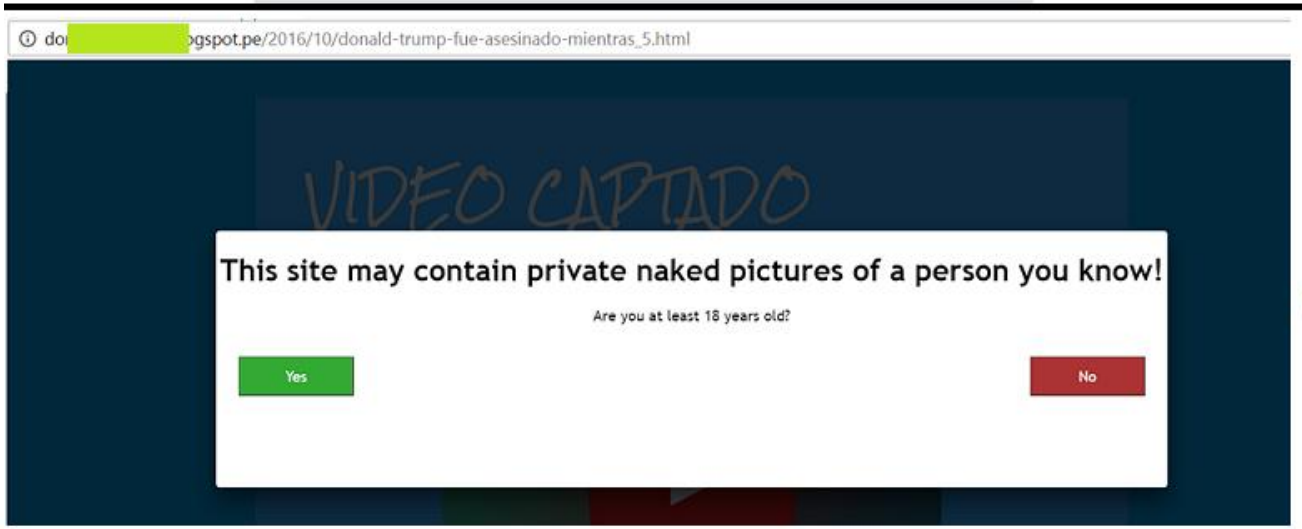
3: Contenido adulto


Yessenia Alejandra Hay un 9 en los P y la palabra encontrar
Like · Reply · 1 · May 17, 2015 at 1:57pm
Mauricio Sandoval hay 2
Like · Reply · June 30, 2015 at 3:02pm
Regina Huezo de Ledesma 9
Like · Reply · August 19, 2015 at 4:03am
Bryan Alvarado 9
Like · Reply · July 10, 2015 at 2:53pm
Richerd Rendiles en 1991 un niño llamado nick se tiro de un puente devido a problemas familiares
Like · Reply · December 31, 2016 at 12:43pm
Charly Elegante wow crea tu propia caricatura genial pruebalo Aqui esta Link de la aplicacion
Link ----> http://tes[redacted]o.com/caricatur3a/ <----
Like · Reply · October 24, 2016 at 8:47pm
Raul Ramos 9pendejo
Like · Reply · November 10, 2015 at 11:58am
Delmy Ortiz SI
Like · Reply · October 22, 2015 at 12:56am
Guillermo Sanchez Rios calidad
Like · Reply · October 20, 2015 at 11:11pm
Martha Andrade Guerrero Econtrar? O eNcontrar
Like · Reply · September 11, 2015 at 5:17pm
Jasser PG estaa en la ulrima fila
Like · Reply · August 29, 2015 at 7:57pm
Daniel Alvares yo tanvien
Like · Reply · August 29, 2015 at 4:18pm


te[redacted]m/caricatur3a/
Joana Ariana TK argentina.
WOW GENIAL esta aplicacion es genial lo recomiendo
HACE 13 minutes
Ariana Verano Alba PERU.
las caricaturas que hacen son buenas
HACE 15 minutes
Armando Santiago Sanca Ecuador.
EXITOS AMIGOS LA APK FUNCIONA
HACE 16 minutes
Angie Luna Rosales Colombia.
Saludos desde Colombia Gacias amigos. Gracias por la caricatura
div 540 × 28.67
Ver 164 comentarios mas
PodrÃƒÂ¡s comentar luego de usar nuestra increible herramienta!.
Status: ONLINE - Seguro
Actualizado: Hace 8 minutos
1 online
Copyright Â© 2016. All rights reserved. Terminos y Condiciones
…
<div style="
border-bottom: 1px #E2E2E2 solid;padding: 5px 0;">
<img src="http://pok[redacted]ee.com/ais/commentIcon.png">
Ver 164 comentarios mas == $0
<!--end -->


Francisca Hernandez Despues de que se dio a conocer en Estrella Tv. mira donde anda jajajaaaaa !
Like · Reply · 4 hrs
Sofia Valdez Qué feo vestido de Bianca, parece de niña.
Like · Reply · 7 hrs
Cesar Salgado Salgado Ay Bianca Estas bien buena
Like · Reply · 4 hrs
Edgar Eduardo Notícia de último minuto. Donald Trump Fué Asesinado mientras Álmorzaba esta tarde
Vídeo Aquí --> http://cort.as/r
Like · Reply · 2 · 17 hrs · Edited
1 Reply
M De Uribe Esmeralda Alire
Like · Reply · 1 · 15 hrs
1 Reply
Write a comment...

(a)

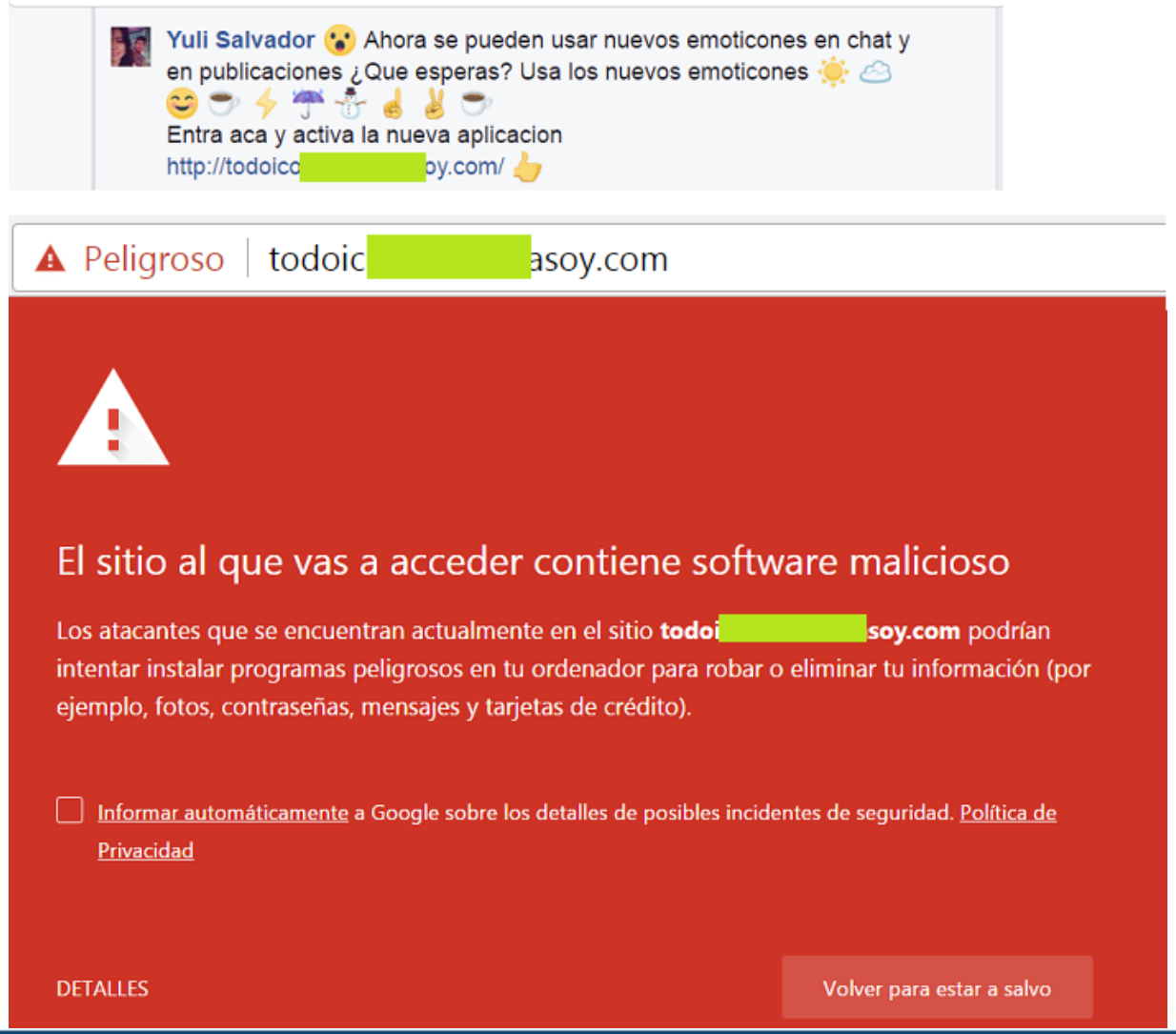

gspot.pe/2016/10/donald-trump-fue-asesinado-mientras_5.html
VIDEO CAPTADO
This site may contain private naked pictures of a person you know!
Are you at least 18 years old?
Yes
No

(b)


MIRA EL PRIMER COMENTARIO Y TE DIBUJO...
96
24 Comments
Like
Share
Sebastian Andres Gener Click aquí ---> https://goo.gl/j [redacted] <---- Entra aquí
Quieres convertir tu foto en caricatura?... ENTRA YA!
TUSWEB.SITE
Like · 1 · January 6 at 9:49pm
Yessibel Santamaria Siii
Like · January 6 at 10:05pm
Mari Diaz Diaz Eso es gracioso
Like · January 6 at 10:08pm
Gislaine Terán Yi
Like · January 6 at 10:12pm
Gislaine Terán Yo
Like · 1 · January 6 at 10:12pm
Ciber Ipanaque Yo
Like · January 6 at 10:15pm
David Denis yo
Like · January 6 at 10:47pm


checkshorturl.com/expand.php
Long URL
http://t [redacted] .site/dibujosebas/
Delay
0.34 second(s)
Short URL
https://goo.gl/j2egLp
t [redacted] .site/dibujosebas/
GENERA TU CARICATURA
Genera tu caricatura, sube tu foto ahora!
Seleccionar archivo
Ningún archivo seleccionado
Has click en Generar YA! y espere unos segundos
GENERAR YA!


ad a-descarga-peru.com/?aspid=c01c4ee3ecb81f4f52f61cf7b30c9b91&context=803f62e9-3d23-4a6d-a369-0b9808375974
Al Aceptar, quedara suscrito, Y recibirás cada semana 3 Contenidos. Cobro Recurrente S/.4.46 semanal.
¡Detectamos que es la primera vez que nos visitas!
¡Es muy fácil y sólo tienes que hacerlo una vez. Introduce aquí tu celular para poder verificar que es un número peruano y te enviaremos un código pin para que puedas confirmar que se trata de tu celular!
Claro
Recordar mi número de celular
Leí y acepto los términos y condiciones
CONTINUAR
14,181,439 downloads


Yuli Salvador 😮 Ahora se pueden usar nuevos emoticones en chat y en publicaciones ¿Que esperas? Usa los nuevos emoticones ☀️ ☁️ 😊 ☕ ⚡ ☔ ⛄ ☝️ ✌️ ☕
Entra aca y activa la nueva aplicacion
http://todoicc[redacted]oy.com/ 👍
Peligroso | todoic[redacted]asoy.com
El sitio al que vas a acceder contiene software malicioso
Los atacantes que se encuentran actualmente en el sitio todoi[redacted]soy.com podrían intentar instalar programas peligrosos en tu ordenador para robar o eliminar tu información (por ejemplo, fotos, contraseñas, mensajes y tarjetas de crédito).
Informar automáticamente a Google sobre los detalles de posibles incidentes de seguridad. Política de Privacidad
DETALLES
Volver para estar a salvo

Like · February 5 at 12:20pm

Santiago Ozuna 3952
Like · February 5 at 12:52pm

Melod Vitia Hi Clasher, come with the biggest tournament in the world, come join us, Gifts All you can get is :

1. [+] $ 250,000 + 100,000 Gems √
2. [+] $ 200,000 + 75,000 Gems √
3. [+] $ 175,000 + 50,000 Gems √

To Register You can Login to our website Link :
http://thetour[redacted]hofclans.zxc.pm/

*WARNING: the tournament can be Followed only for clasher Town hall 8-11
GOOD LUCK GUYS

SUPERCELL GIFT - TOURNAMENT 2017
Follow the tournament Clash of Clans and get the biggest prize in 2017.
THET[redacted]ANS.ZXC.PM

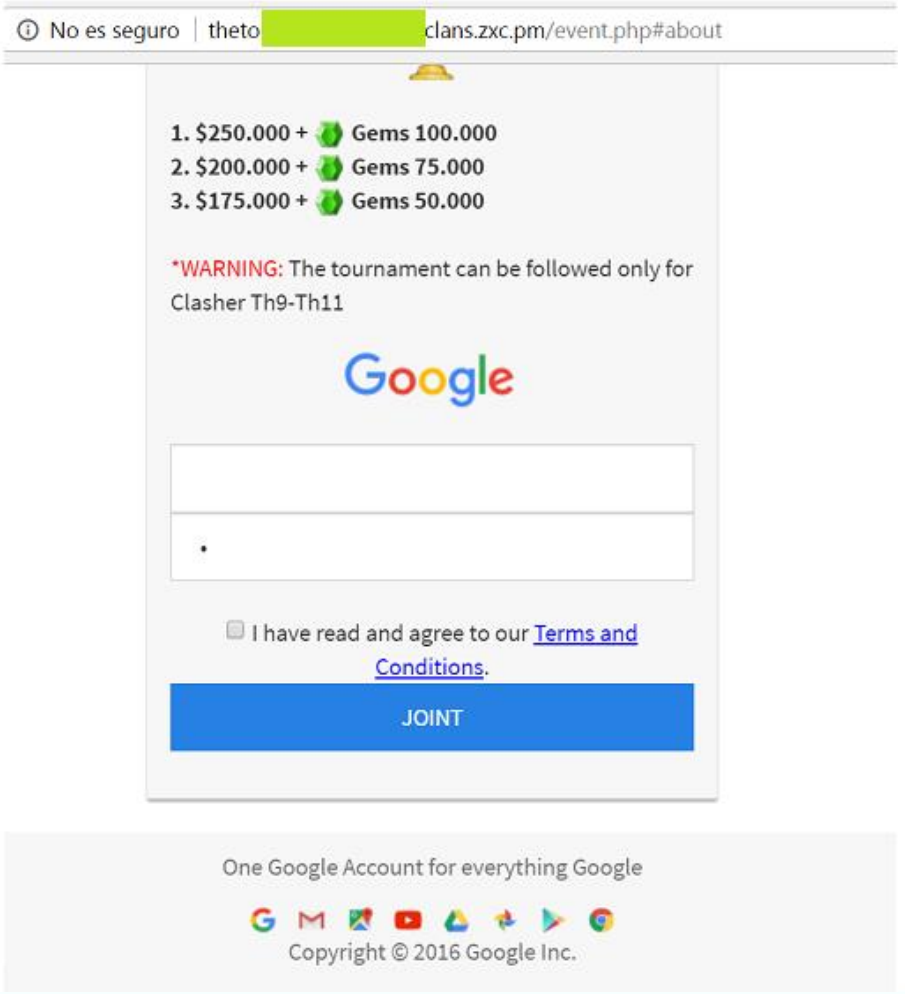
Like · February 5 at 12:53pm

Rodrigo Narvaez 2.610
Like · February 5 at 1:16pm

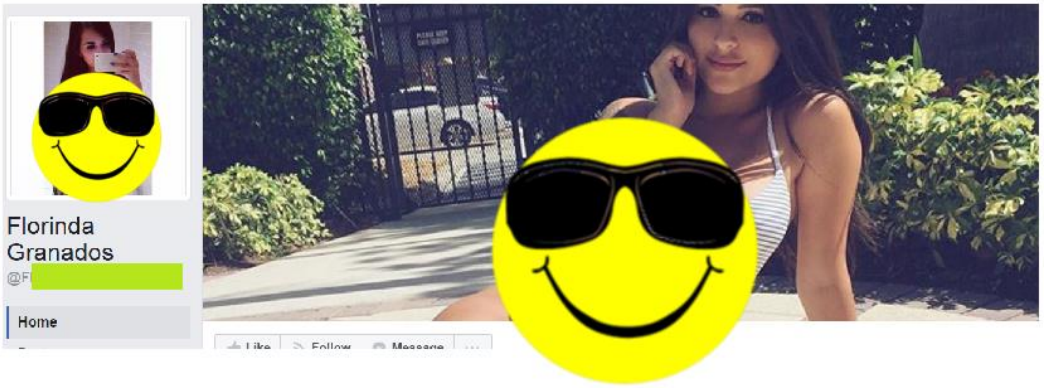
Bruno Martinéz 3400
Like · February 5 at 1:22pm

Juan Carlos Garcia Lopez 2789 copas
Like · February 5 at 1:31pm

Juanchi Cremonte 2800
Like · February 5 at 1:32pm




¿VES TU HERMOSA EDAD?
8,9,10,11,12,13,14,15,16,17,18
19,20,21,22,23,24,25,26,27
28,29,30,31,32,33,34,35,36
37,38,39,40,41,42,43,44,45
46,47,48,49,50,51,52,53,54
NO VEO MI EDAD
Comenta tu edad con el # & mira lo que pasa!
Like
Share
19K
View previous comments
57 of 5,434
Giuliana Hinostroa 12
Like · 2 hrs
Mateo Rufino #11
Like · 2 hrs
Viviana Arce 15
Like · 2 hrs
Fernanda Eulloqui #13
Like · 2 hrs
Cristian Moran 14
Like · 2 hrs
Alexander Panca Roque #11
Like · 2 hrs
Yudith Reyes #15
Like · 2 hrs
Florinda Granados Sigueme y Te Envio Add
Florinda Granados
Chat Caliente Si Quieres
Like · 2 hrs
Dean Jhony Payajo Caldas 11
Like · 2 hrs
Lenin Mero 9
Like · 2 hrs
Jose Francisco Viruete Garcia ########## 11
Like · 1 hr


Florinda Granados
Home


Yasmin Castro
2 de enero de 2016
COMENTA TU EDAD Y SI TIENES MAS DE 12 TE LLEGO AL CHAT Y TE ENVIO FOTOS MUY SEXIESS
SIGUEME Y TE SIGO MI AMORR
ENVIAM UN MENSAJIO Y TE RESPONDO

Consideraciones de seguridad

- Ejecutar consultas de contenido en un entorno sandboxing.
- Extender las URLs cortas y revisar su contenido.
- Utilizar servicios que muestren niveles de confianza de los sitios web. Ejm.: WebOfTrust.
- Explorar las páginas sospechosas:
  - El nombre de dominio. Ejm.: WHOIS-lookup.
  - Si tiene certificado de seguridad.
  - Si está dentro de las listas negras.
  - Si tiene deshabilitado entrar en modo desarrollador.

Conclusiones

1. El aprendizaje supervisado de ML permite detección de contenido malicioso, considerando una adecuada selección de características.
2. Una URL corta por servicios que pagan por cada enlace accedido, deben ser tratados como una posible amenaza.
3. Se observa la violación de los derechos de autor por la presencia de URLs que apuntaban a sitios de descarga de películas, música, videos, juegos, etc.
4. Se observa que las URLs con referencia a temas virales tienen incentivos por el negocio de la publicidad de los servicios de acortamiento.
5. La existencia de páginas para la minería de bitcoins también podría formar parte del contenido malicioso porque precisan la instalación de software de dudosa procedencia.

Edith Rivero

edith.rivero@unsaac.edu.pe