



#Tinfoleak: analizando nuestras pautas y comportamientos a través del análisis de la exposición pública en Twitter

Vicente Aguilera Díaz
@VAguileraDiaz
06/12/2014
Madrid.

www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
SPANISH NATIONAL
CYBERSECURITY INSTITUTE





Sobre mí

Socio y Director de Auditoría de Internet Security Auditors

OWASP Spain Chapter Leader

Miembro del Consejo Técnico Asesor de RedSeguridad

Miembro del Jurado de los Trofeos de Seguridad TIC

CISA, CISSP, CSSLP, ITILF, PCI ASV, CEH, ECSP, OPSA, OPST

Colaborador en diversos proyectos open-source

Vicente Aguilera Díaz

@VAguileraDiaz

vaguilera@isecauditors.com

www.vicenteaguileradiaz.com



www.isecauditors.com



Agenda

- I. Predecir el comportamiento humano
- II. Tinfoleak: bondades y limitaciones
- III. Próximos pasos
- IV. Referencias

Predecir el comportamiento humano



Tinfoleak: bondades y limitaciones





Tinfoleak: bondades y limitaciones

Sobre Tinfoleak...

- Script desarrollado en Python
- #Twitter #OSINT #stalker #privacy #security #socialengineering
- Requerimientos:
 - Tweepy
 - Jinja2
 - OAuth access token
- Puede ser ejecutado en dispositivos móviles
- Incorporado en la distro CAINE 6.0
- Descarga:
www.vicenteaguileradiaz.com/tools

Tinfoleak: bondades y limitaciones

Sobre Tinfoleak...

- De interés en diversos ámbitos:
 - Ingeniería social
 - Pentesting
 - Vigilancia digital





Tinfoleak: bondades y limitaciones

Sobre Tinfoleak...

- Existe alguna herramienta similar...
 - Creepy
 - TIGEO (basada en Tinfoleak)
 - MyPrivacyAudit.com
 - Geostalker
 - Geofeedia

... pero sin la potencia ni flexibilidad de Tinfoleak! 😊



Tinfoleak: bondades y limitaciones

A partir de un @usuario:

- Extracción de información básica
- Identificación de dispositivos, sistemas operativos, aplicaciones y redes sociales utilizadas
- Temáticas sobre las que opina el usuario
- Franjas horarias de mayor actividad
- Contactos del usuario y relaciones entre ellos
- Opinión del usuario sobre temáticas específicas
- Descarga de imágenes publicadas
- Geolocalización de tweets (incluyendo fotografías)



Tinfoleak: bondades y limitaciones

A partir de un @usuario:

- Identificación de residencia habitual, lugar de trabajo y otras ubicaciones relevantes
- Predicción de ubicaciones futuras
- Análisis de metadatos
- Temáticas relacionadas con una palabra clave
- Búsquedas avanzadas
- Informe de resultados en formato HTML

Tinfoleak: bondades y limitaciones





Tinfoleak: bondades y limitaciones

#Tinfoleak: Limitaciones

- Sólo analiza la red social Twitter
- Existen restricciones en el uso de la API
- La geolocalización puede ser deshabilitada por el usuario



Próximos pasos

¿Y AHORA QUÉ?



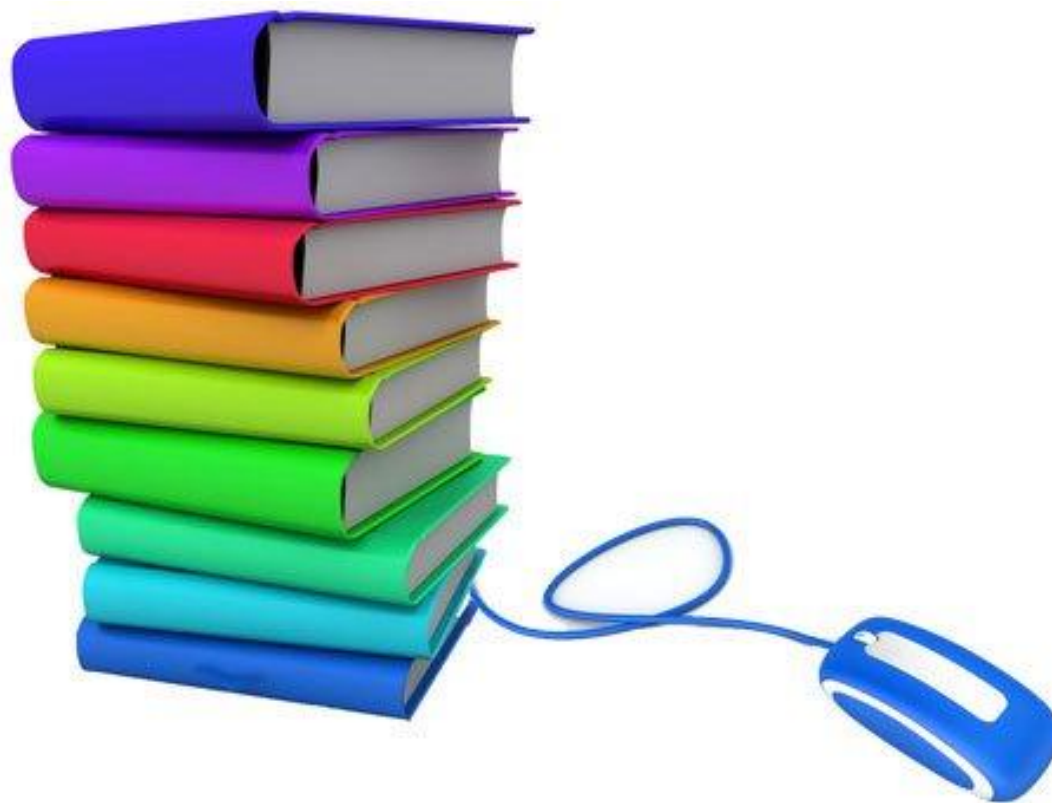
Próximos pasos

En futuras versiones de Tinfoleak:

- Explotar nuevas características implementadas en Twitter
- Análisis de otras redes sociales
- Interfaz gráfica
- Mejorar operativas actuales
- Exportación de resultados en otros formatos
- Mayor velocidad de ejecución
- ???

Se aceptan ideas ;-)

Referencias





Referencias

Tweepy – Python library for accessing the Twitter API

<http://www.tweepy.org/>

Jinja2 – Python template engine

<http://jinja.pocoo.org/>

OAuth – Authorization framework

<http://oauth.net/>

CAINE – Computer Forensics Linux Live Distro

<http://www.caine-live.net/>



Referencias

Creepy – Geolocation OSINT tool

<http://ilektrojohn.github.io/creepy/>

TIGEO – Geolocalización basada en tweets

<http://www.tigeostalk.tk>

@MyPrivacyAudit

<http://www.miprivacyaudit.com>

Geostalker

<https://github.com/milo2012/osintstalker>



Referencias

Geofeedia – Location-based social media monitoring

<http://www.geofeedia.com>

Artículo: “La predicción de la conducta a través de los constructos que integran la teoría de acción planeada”

<http://reme.uji.es/articulos/abreva7191302101/texto.html>

Artículo: “La actividad en redes sociales permite predecir el comportamiento laboral”

<http://www.infobae.com/2014/04/23/1559282-la-actividad-redes-sociales-permite-predecir-el-comportamiento-laboral>



Referencias

Artículo: “Monitorizar la información compartida en Twitter para predecir grandes acontecimientos”

<http://blogthinkbig.com/predecir-grandes-acontecimientos-twitter>

