

fwhibbit.es

Maltego II (o cómo conejear a un conejo)

10-13 minutos

Saludos conejiles!!

Hoy continuamos con la segunda entrega sobre Maltego, la fantástica herramienta de [Paterva](#) usada primordialmente para temas de OSINT y forense. Podéis leer la entrada anterior en el siguiente [enlace](#), en el que nos adentramos en lo más básico de esta herramienta.

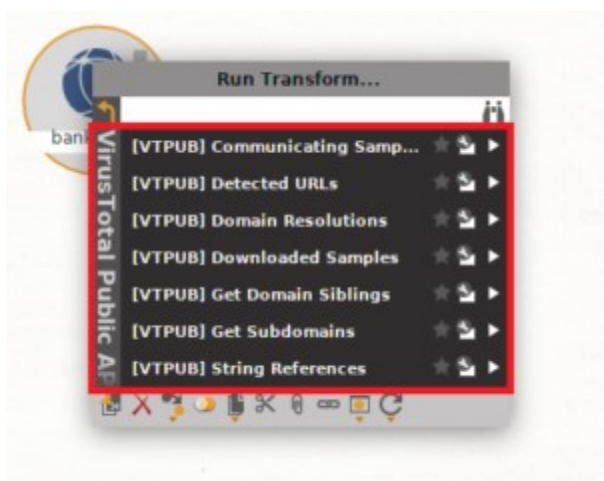
Sin más, vamos a darle un poco de chicha.

Integración con Virus total

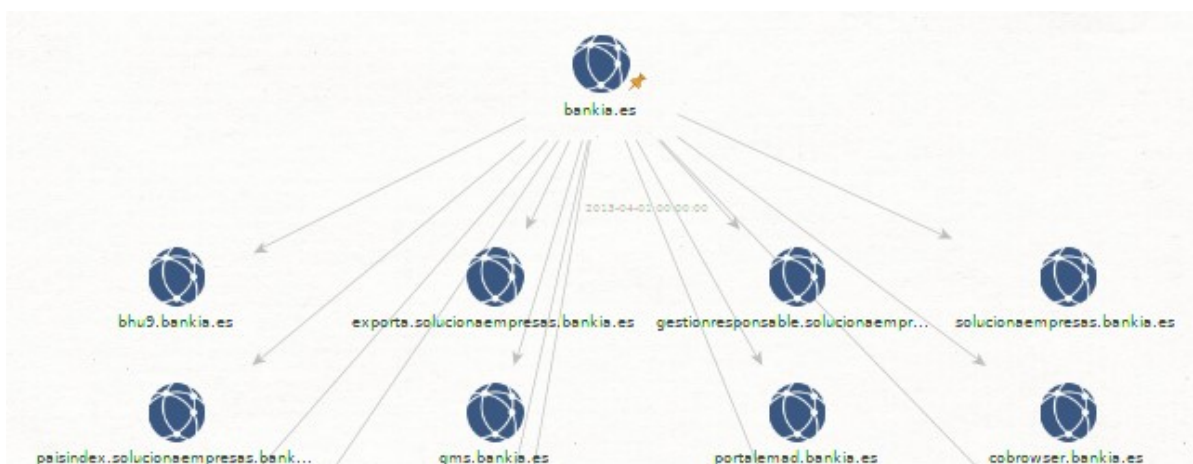
Continuando con lo visto en la entrada anterior referente a la búsqueda e investigación de dominios, y si hemos configurado la transformada de [Virus Total](#) con una **API Key**, Maltego comprobará si en el dominio objetivo se encuentra algún tipo de información al respecto.

Virus Total, además de proporcionar y realizar informes de escaneos de archivos con multitud de antivirus, analiza los dominios y devuelve un listado de subdominios, muestra un histórico de las IPs del objetivo, y lista archivos relacionados al dominio, como es el caso de referencias a «strings». En este caso

vamos a ejecutar la transformada entera de Virus Total para nuestro objetivo (un importante banco español):




Como podemos ver en este caso, al ejecutar la transformada de Virus Total, se nos muestran dominios (hasta 12 al usar la versión no comercial de prueba), la IP de nuestro objetivo, y una entidad de tipo hash:





Detail View [X]

 Hash
maltego.Hash
`b3746b5c57bc382b9ac4ad272f1277adc32151`

- Relationships

- Incoming
[bankia.es](#)

- Generator detail

Source	bankia.es	(Domain)
Transform	[VTPUB] String References	
Gen. date	2018-01-22 11:40:07.194 +0100	

Property View [X] **Hub Transform Inputs**

- Properties

Type	Hash
Hash	<code>b3746b5c57bc382b9ac4a...</code> [...]
Hash Type	[...]
Owner	[...]
Before	
After	
Included Media Types	[...]
Excluded Media Types	[...]

- Dynamic properties

Positives	18	[...]
-----------	----	-------

- Graph info

Weight	100
Incoming	1
Outgoing	0
Bookmark	[Bookmark icon]

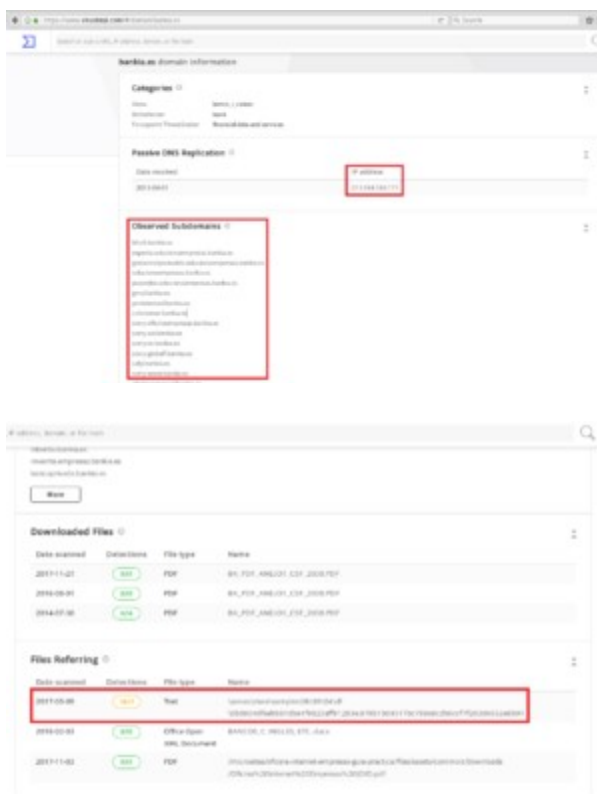
1 of 15 entities

Detalles de la entidad tipo Hash

Si comprobamos que tipo de información se obtiene desde la propia página de Virus Total, en este caso obtenemos información



Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.



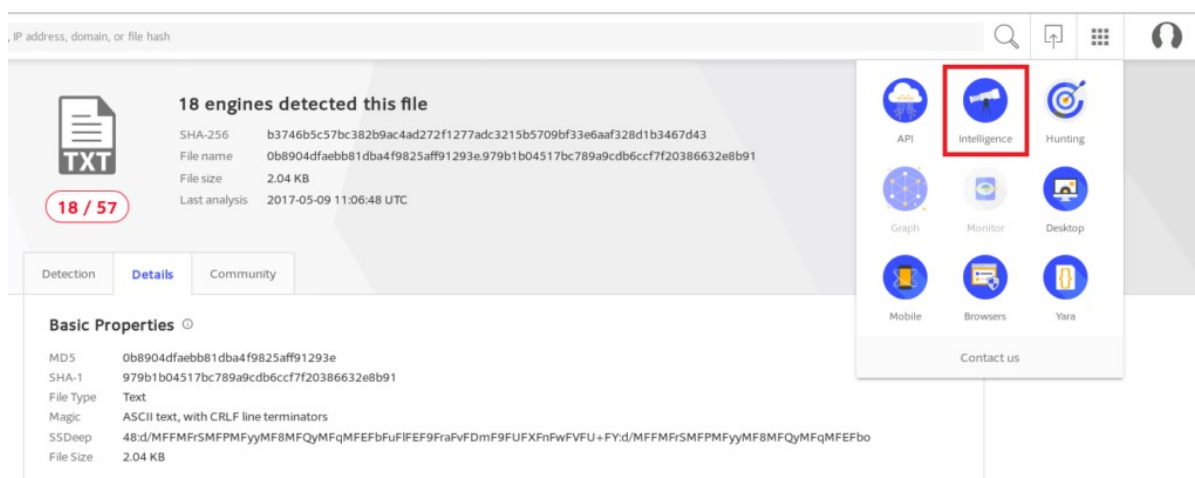


18 engines detected this file

SHA-256: b3746b5c57bc382b9ac4ad272f1277adc3215b5709bf33e6aaf328d1b3467d43
 File name: 0b8904dfaebb81dba4f9825aff91293e979b1b04517bc789a9cdbc6cf7f20386632e8b91
 File size: 2.04 KB
 Last analysis: 2017-05-09 11:06:48 UTC

Detection	Details	Community
Agility40	Trig-Spyder-Security	Agility40
Avast	Avast-Mobile	Avast-Mobile
Comodo	Trig-Spyder-Security	Comodo
ESB-MSD32	Trig-Spyder-Security	ESB-MSD32
Fortinet	Trig-Spyder-Security	Fortinet
Microsoft	Trig-Spyder-Security	Microsoft
QIPSO-DBS	Trig-Spyder-Security	QIPSO-DBS
Symantec	Trig-Spyder-Security	Symantec
VirusShare	Trig-Spyder-Security	VirusShare
Ad-Aware	Ad-Aware	Ad-Aware
Avast	Avast	Avast

Si disponemos de cuenta en Virus Total, podremos investigar más sobre el hash en cuestión. Para ello, deberemos acceder al módulo de inteligencia (Intelligence), e ingresar el hash anterior. Este hash ha sido identificado como 'string referenciado', por lo que en la sección *Strings* de *Content*, debería aparecer el nombre de nuestro objetivo:



IP address, domain, or file hash

18 engines detected this file

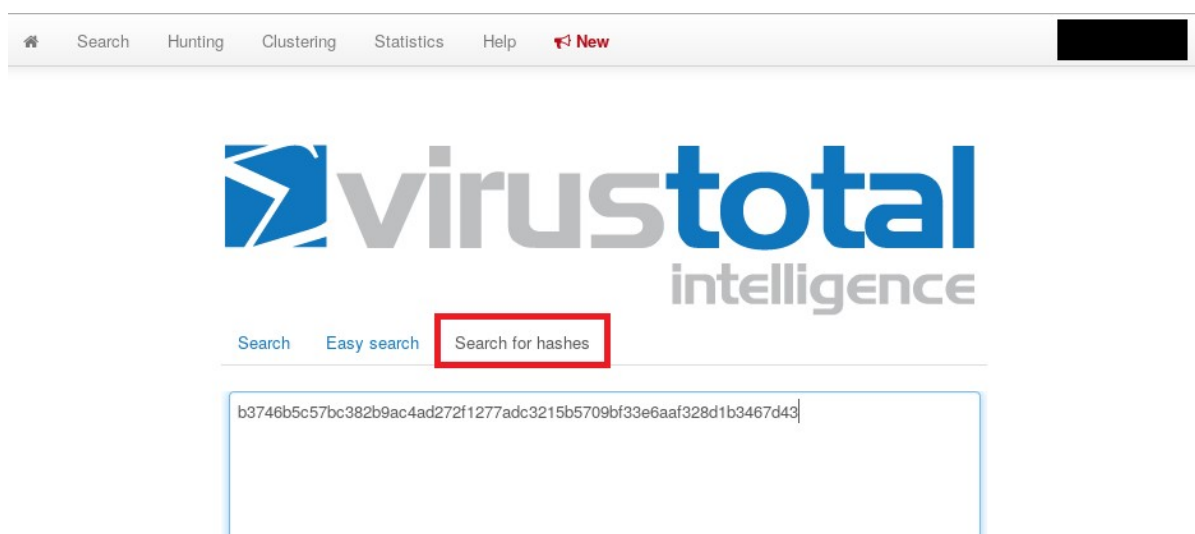
SHA-256: b3746b5c57bc382b9ac4ad272f1277adc3215b5709bf33e6aaf328d1b3467d43
 File name: 0b8904dfaebb81dba4f9825aff91293e979b1b04517bc789a9cdbc6cf7f20386632e8b91
 File size: 2.04 KB
 Last analysis: 2017-05-09 11:06:48 UTC

Basic Properties

MD5: 0b8904dfaebb81dba4f9825aff91293e
 SHA-1: 979b1b04517bc789a9cdbc6cf7f20386632e8b91
 File Type: Text
 Magic: ASCII text, with CRLF line terminators
 SSDeep: 48:d/MFFMFySMFPMFyyMF8MFQyMFqMFEFbFuFIFE9FraFvFDmF9FUFxFnFwFVFU+FY:d/MFFMFySMFPMFyyMF8MFQyMFqMFEFbo
 File Size: 2.04 KB

Intelligence

Acceso al área de Inteligencia en Virus Total



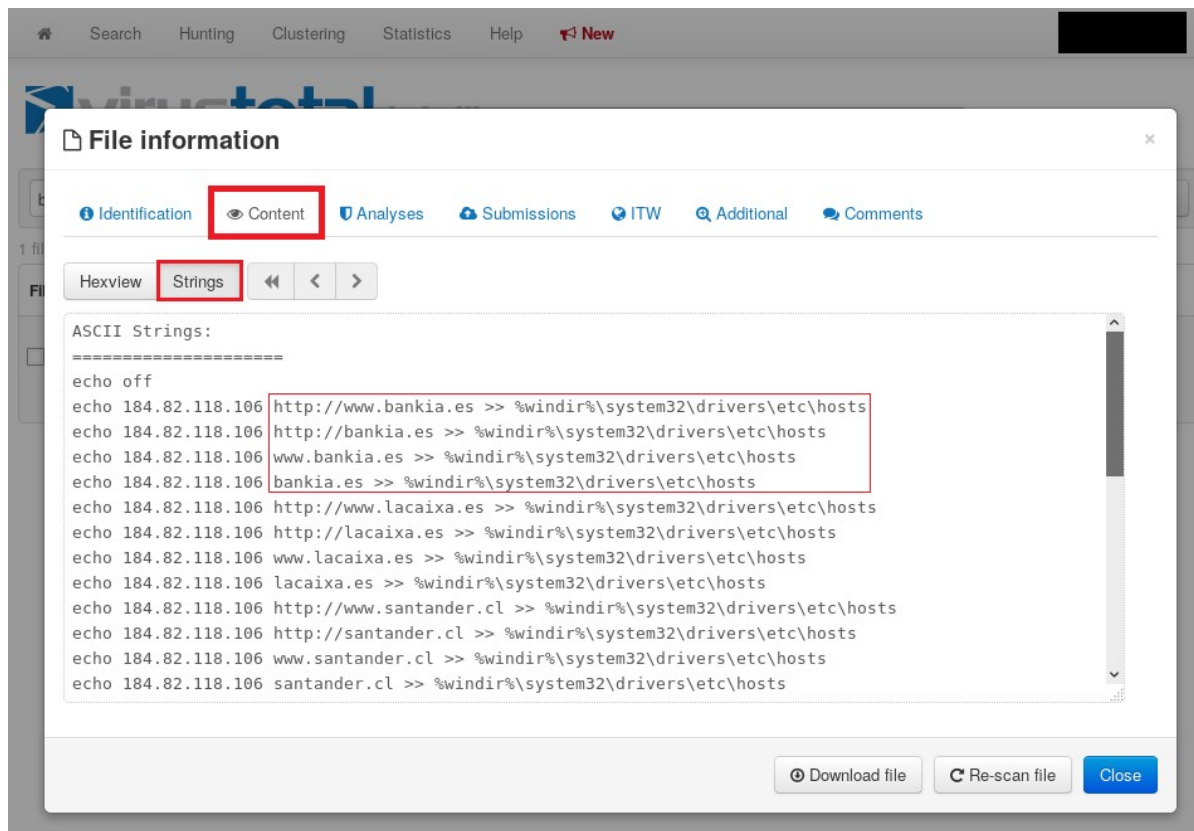
Search Hunting Clustering Statistics Help New

Search Easy search Search for hashes

b3746b5c57bc382b9ac4ad272f1277adc3215b5709bf33e6aaf328d1b3467d43

Search

Búsqueda del hash



Ejemplo de la indexación del objetivo en los Strings del fichero

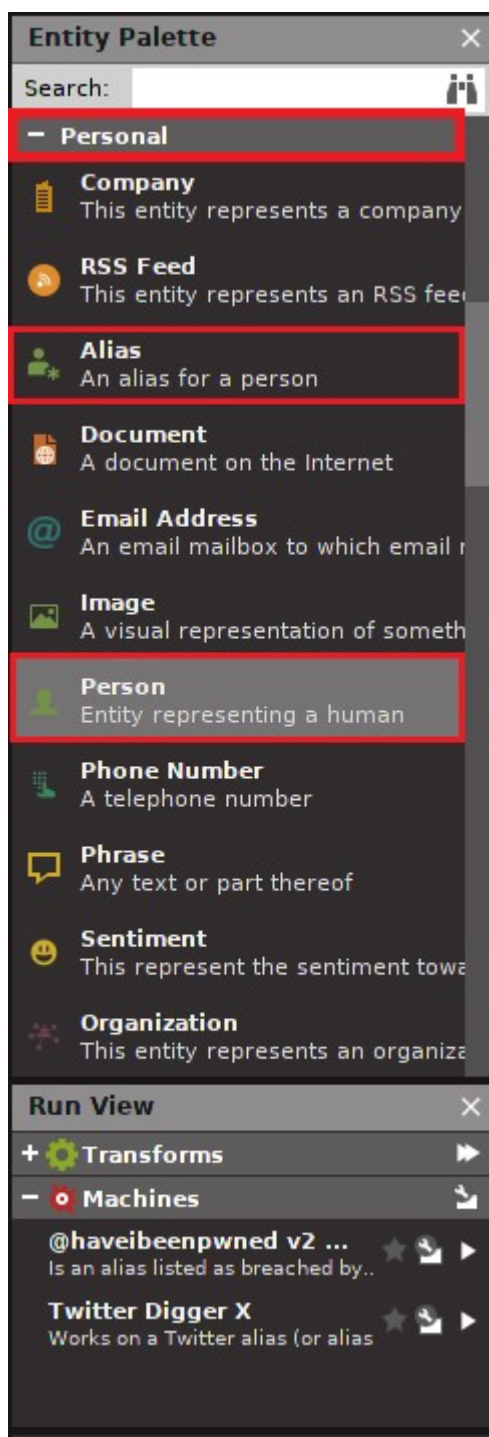
Podemos concluir entonces, que Maltego está bien para recopilar los hashes, ya que si ejecutamos las transformadas de la entidad hash, no se suele obtener información al respecto. Si quisiésemos más información al respecto de dicho hash, deberemos buscar la información directamente en Virus Total.

Investigación sobre perfiles

Otra de las funcionalidades de Maltego, es la búsqueda de información pública de una persona; para qué se use, es ya decisión de cada uno. Desde FWHIBBIT recomendamos un uso

responsable. En caso de duda, acuda a su farmacéutico.

En este caso, vamos a realizar una prueba para ver el funcionamiento con un personaje público (bastante conejo él). Dentro de la paleta de entidades, tenemos una sección dedicada a perfiles llamada *Personal*. Dentro de ella, podemos seleccionar entidades como direcciones de correo, nombre de compañía, documentación, imagen, teléfono, alias, o persona:



Paleta de entidades, sección para personas física o compañías

Para empezar el descubrimiento, estas dos últimas entidades son las más representativas: *Alias* y *Person*. Entendemos como alias el «nickname» (esto suena un poco años 80 xD), por lo que arrastramos las dos entidades y las rellenamos con el nombre de nuestro objetivo. En este caso, ya que nuestro objetivo tiene un nombre artístico, arrastraré dos entidades de persona, una con el nombre real y otra con el artístico:

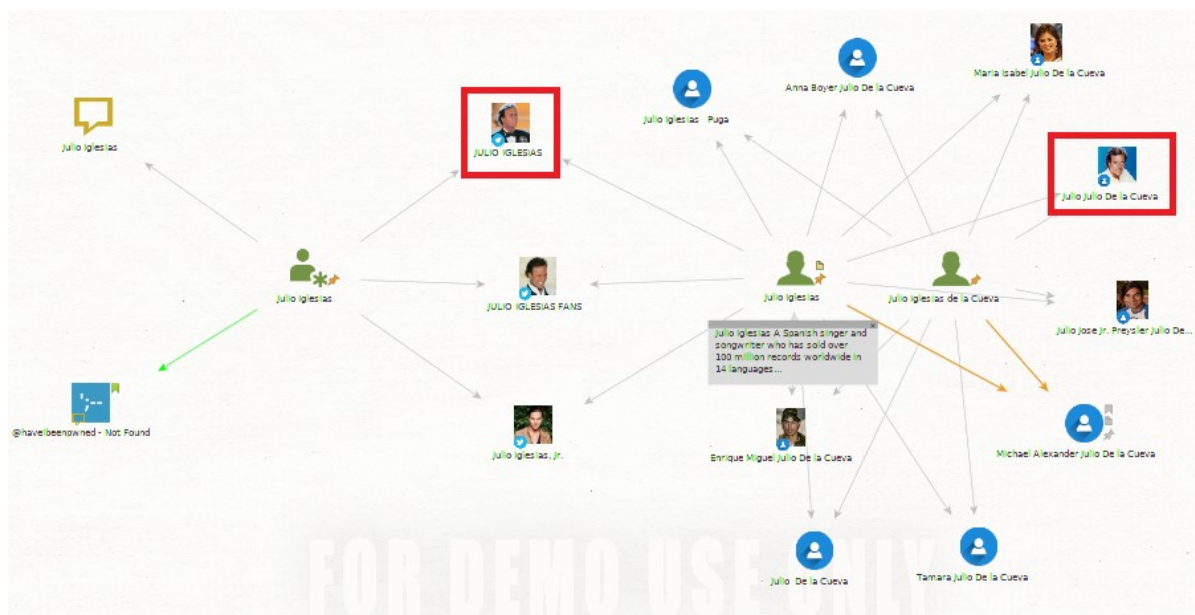


Tras ejecutar todas las transformadas, podemos ver que existen una gran cantidad de falsos positivos. Cuanto más específicos seamos al poner el nombre en la entidad, menos falsos positivos tendremos, pero también cabe la opción de que al ingresar por ejemplo tan sólo un apellido del objetivo estemos perdiendo información. Por mi experiencia, prefiero crear varias entidades para abarcar más posibilidades y obtener el máximo número de resultados, para luego aplicarle un análisis e ir borrando los falsos positivos. En este caso, suprimo los falsos positivos para poder ver la información de una manera más sintetizada, sino, saldría algo como este grafo:





Grafo resultante sin borrar falsos positivos



Grafo tratado sobre el objetivo. Entidades nuevas significativas marcadas

Como podemos ver, se nos han interrelacionado los perfiles del objetivo, ya que las entidades que hemos creado comparten otras entidades transformadas. Es significativo que nos aparezcan miembros de la familia del objetivo, como son su padre, sus hijos, y su exmujer (y los hijos previos a su relación). En este caso vamos a volver a eliminar a sus familiares, para poder quedarnos con los datos del objetivo. Es interesante tener instalada la transformada de *haveibeenpwned* ya que nos analizará si existen datos al respecto de los alias introducidos. En este caso, borraremos también esta entidad ya que no muestra información alguna.

Como podemos ver, Maltego incluso te puede dar una referencia histórica del objetivo:





Si queremos saber de dónde viene uno de los datos encontrados, podremos hacerlo seleccionando la entidad y viendo sus propiedades, o bien haciendo doble click sobre la entidad, y después en la sección *Properties*:

FOR DEMO USE ONLY

Property View

Affiliation - Twitter
maltego.affiliation.Twitter
JULIO IGLESIAS

Relationships

Incoming
Julio Iglesias, Julio Iglesias

Details

Generator detail

Source: Julio Iglesias (Alias)
Transform: To Twitter Affiliation [Search Twitter]
Gen. date: 2018-01-22 16:00:57.513 +0100

Property View

Properties

Type	Affiliation - Twitter
Name	JULIO IGLESIAS
Network	Twitter
UID	julioiglesias
Profile URL	https://twitter.com/julioigl...
Twitter ID	51325856
Screen Name	julioiglesias
Friend Count	38
Real Name	JULIO IGLESIAS

Dynamic properties

Image	https://pbs.twimg.com/profil...
Location	Miami, FL
Follower Count	81555

Graph info

Weight	81555
Incoming	2
Outgoing	0
Bookmark	

```
erify common] done (from 2_entities)
ned)) returned with 0 entities (from entity "Julio Iglesias")
ned)) done (from 2_entities)
```

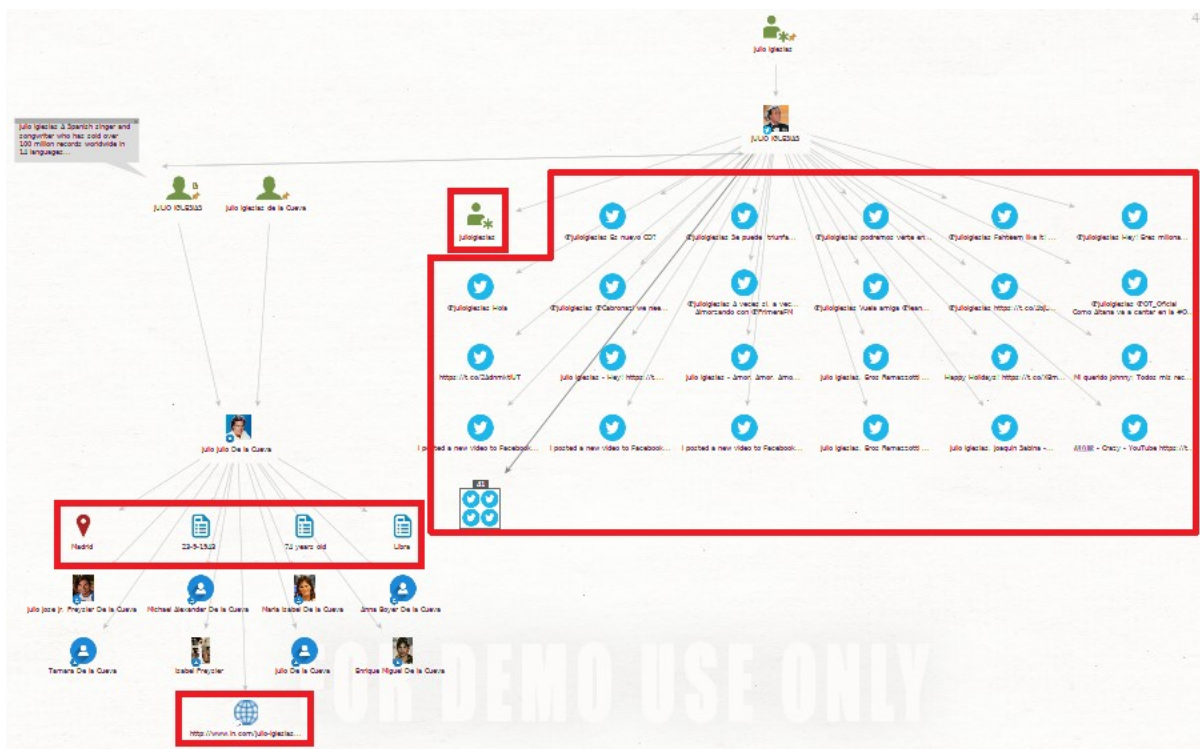
Details

Summary Attachments (0) Notes **Properties (11)**

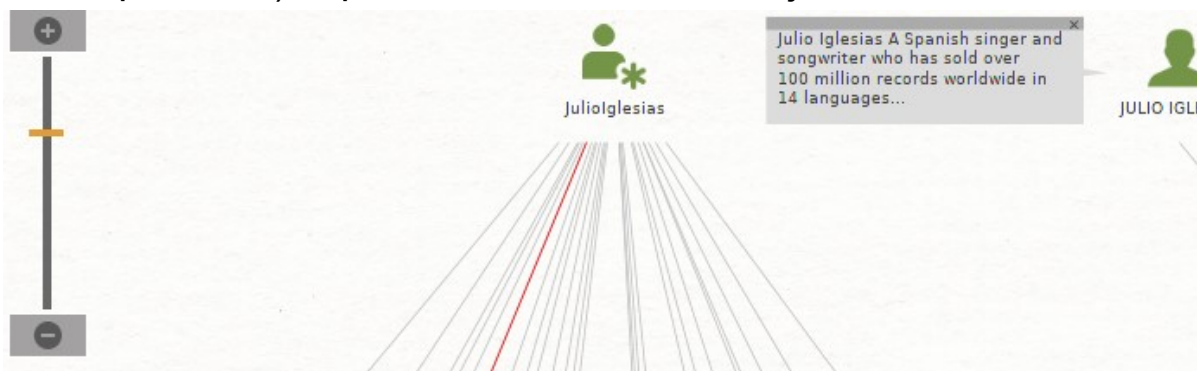
Name	JULIO IGLESIAS
Network	Twitter
UID	julioiglesias
Profile URL	https://twitter.com/julioiglesias
Twitter ID	51325856
Screen Name	julioiglesias
Friend Count	38
Real Name	JULIO IGLESIAS
Image	https://pbs.twimg.com/profile_images/664146719245000704/EEQI7K44_normal.jpg
Location	Miami, FL
Follower Count	81555

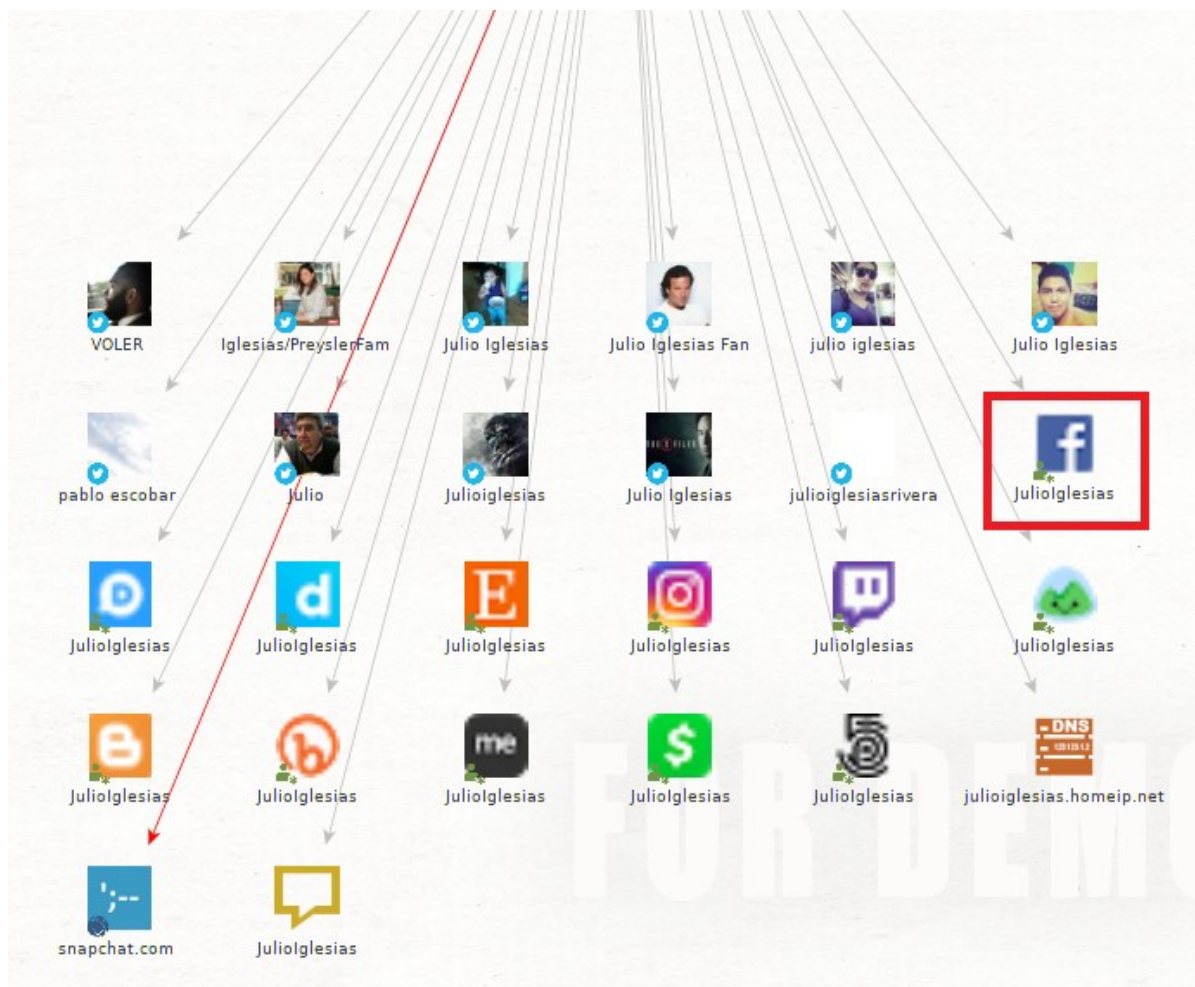
Tendremos que seguir tirando un poco del hilo... por lo que

Al realizar las transformadas de un perfil de Twitter, nos muestra tanto un nuevo alias, como una gran cantidad de tuits referentes al perfil público de nuestro objetivo. Por otra parte, y gracias a la entidad de PeopleMon, nos vuelve a salir información de sus familiares, así como su fecha de cumpleaños, los años que tiene, el símbolo del zodiaco, la ubicación de nacimiento (reside en Miami, tal y como indica su Twitter), así como una página de noticias americana, que dispone de un perfil de nuestro objetivo:

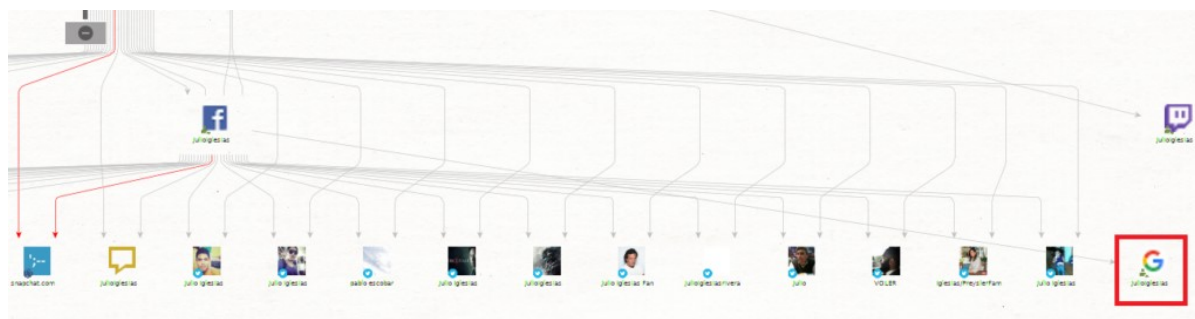


A continuación, podemos ejecutar las transformadas del alias que se generó anteriormente, lo que nos trae (además de muchos falsos positivos) el perfil de Facebook del objetivo:





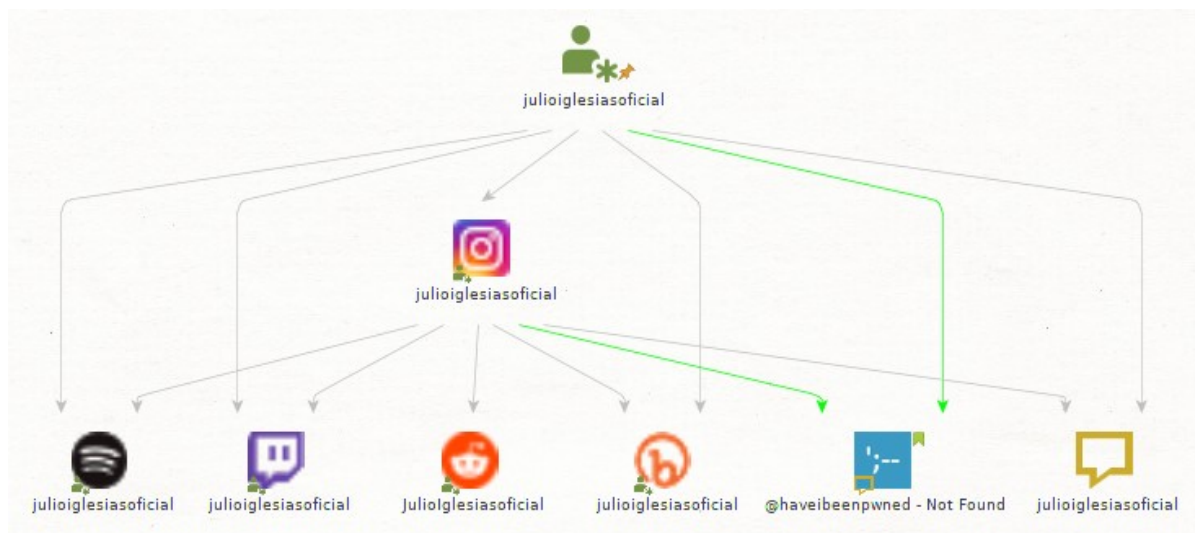
Del perfil de Facebook, hemos podido conseguir su perfil de Google+:



Y de su perfil de Google+, volvemos a obtener los falsos positivos anteriores, por lo que podríamos dar por finalizada nuestra investigación.

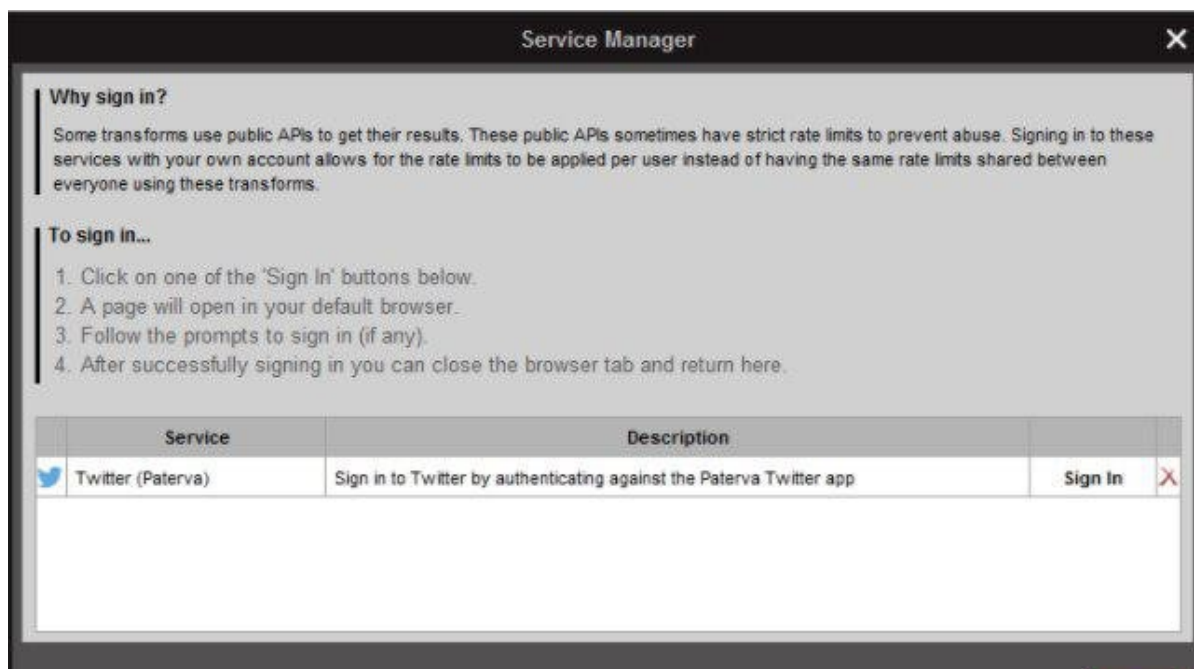
Como análisis en general del perfil público de una persona, no está nada mal, pero por ejemplo no se ha llegado a relacionar su cuenta oficial de Instagram, por lo que recomiendo que siempre que se

quiera realizar una investigación sobre un objetivo, primero se intente obtener los perfiles más importantes mediante buscadores (o al menos sus Alias), para así no perder información por el camino:





Twitter

Normalmente, en toda herramienta que usa Twitter se suele necesitar crear una aplicación para poder tener acceso a la API. En el caso de Maltego, tan sólo nos hará falta registrarnos con una cuenta y autorizar a la aplicación de Maltego el uso de Twitter:



Close



**¿Autorizas a
MaltegoIntegrationApplication a
utilizar tu cuenta?**

Autorizar la aplicación


Cancelar

Esta aplicación podrá:

- Leer Tweets de tu cronología.
- Ver a quién sigues.

No podrá:

- Sigue a nuevas personas.
- Actualizar tu perfil.
- Publicar Tweets por ti.
- Acceder a tus mensajes directos.
- Ver tu dirección de correo electrónico.
- Ver tu contraseña de Twitter.



MaltegoIntegrationApplication
Por Paterva
www.paterva.com/
Application used for the integration with
twitter within Maltego.

Puedes revocar el acceso a cualquier aplicación en cualquier momento desde la [pestaña de Aplicaciones](#) de tu página de Configuración.

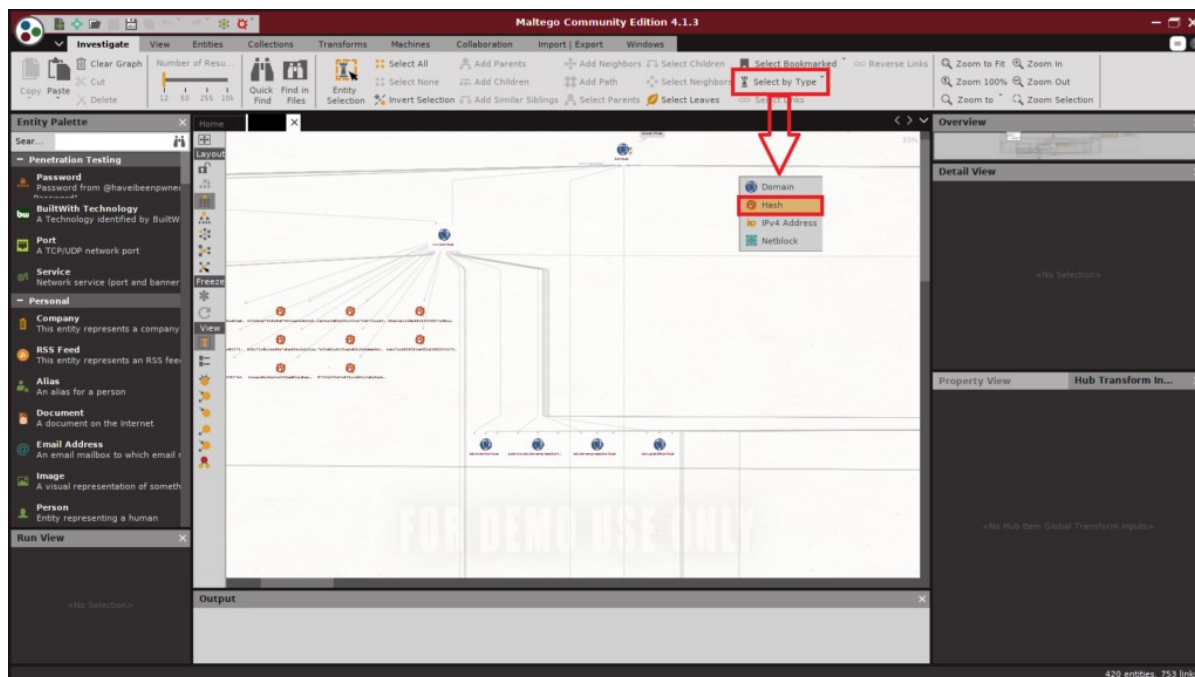
Al autorizar una aplicación, continuarás operando bajo las [Condiciones de Servicio de Twitter](#). En concreto, algunos datos de uso serán compartidos con Twitter. Para más información, mira nuestra [Política de Privacidad](#).

Tips útiles

Selección de entidades por tipo

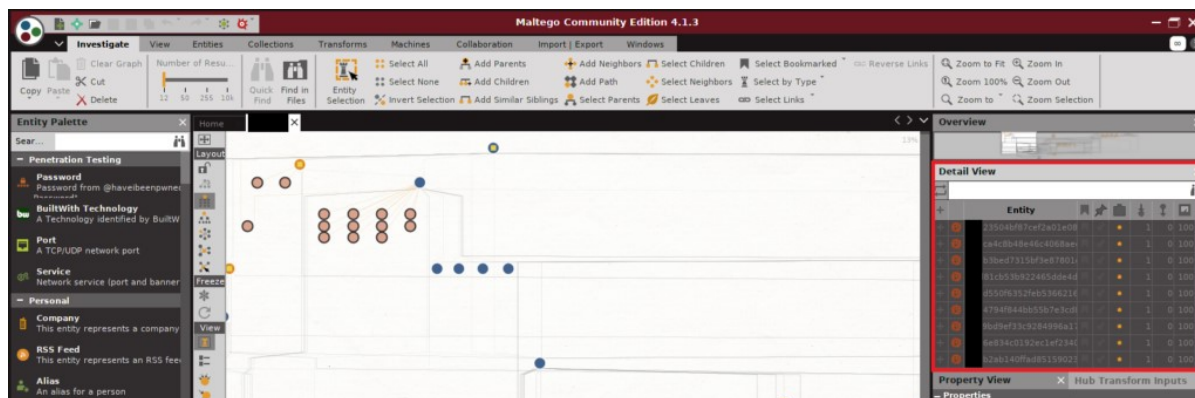
En muchas ocasiones, querremos por ejemplo recoger los datos que ha arrojado Maltego para nuestros «informes». Imaginemos por ejemplo que estamos buscando Malware de un objetivo. Tras varias ejecuciones de las transformadas para los dominios principales y los generados desde sus transformadas, podemos

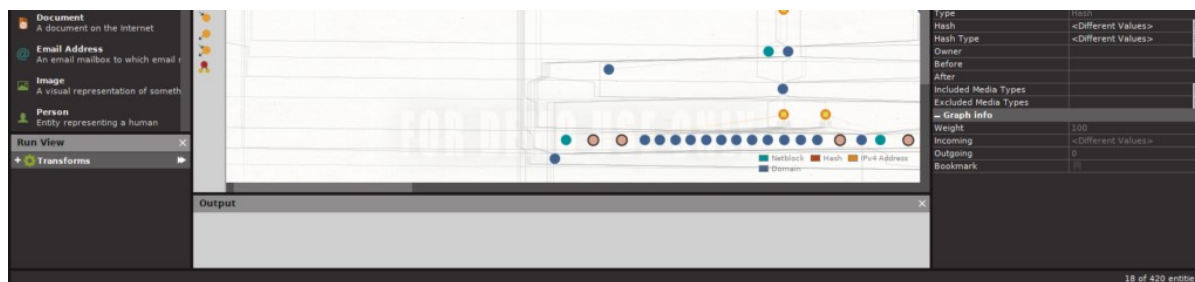
hacer uso de la funcionalidad *Select by Type* del panel de opciones superior para seleccionar todas las entidades del mismo tipo. En este caso, seleccionamos *Hash*:



Copiar bloques de información resultante

En este momento, se nos seleccionarán todas las entidades de tipo hash, lo que podemos ver tanto en el grafo (se realizará un zoom para abarcar todas las entidades), y se nos mostrará su información en el panel derecho de *Detail View*. Precisamente en este panel, podremos seleccionar todos los hashes (seleccionando el primero y arrastrando o pulsando *ctrl+a*), y copiar los resultados a nuestro editor de texto favorito (*ctrl+c* y *ctrl+v*):





1	Type,Entity,Bookmark,Pinned,Collected,Incoming Links,Outgoing Links,Weight
2	maltego.Hash, 574fc33db2ea517ec2a1, -1,no,no,1,0,100
3	maltego.Hash, dece35a2ba16019d86c2, -1,no,no,1,0,100
4	maltego.Hash, e99215418484a0feedd1, -1,no,no,1,0,100
5	maltego.Hash, 379e3f0eb5d1fecc7cb1, -1,no,no,1,0,100
6	maltego.Hash, 323739eea065d116d5bd, -1,no,no,1,0,100
7	maltego.Hash, 36e87398139ed3f8f5c6, -1,no,no,1,0,100
8	maltego.Hash, 64e18c85b246641bcd5, -1,no,no,1,0,100
9	maltego.Hash, 2a0d7bc750b69deedb4, -1,no,no,1,0,100
10	maltego.Hash, 73db1cab26c17f37e783, -1,no,no,1,0,100
11	maltego.Hash, 84ed74b4a15eae94f4e, -1,no,no,1,0,100
12	maltego.Hash, fb394713dc3080faf84c, -1,no,no,2,0,100
13	maltego.Hash, 2754285a9e92fe11b191, -1,no,no,1,0,100
14	maltego.Hash, 33e6aaf328d1b3467d43, -1,no,no,2,0,100
15	maltego.Hash, d85be3f44e3f23726f34, -1,no,no,1,0,100
16	maltego.Hash, 22f9903e9e01df6ae01d, -1,no,no,1,0,100
17	maltego.Hash, 7e2c961e4ecc607d57aa, -1,no,no,1,0,100
18	maltego.Hash, 72586fa56ceb3c5ca48f, -1,no,no,1,0,100
19	

Tipos de servidores

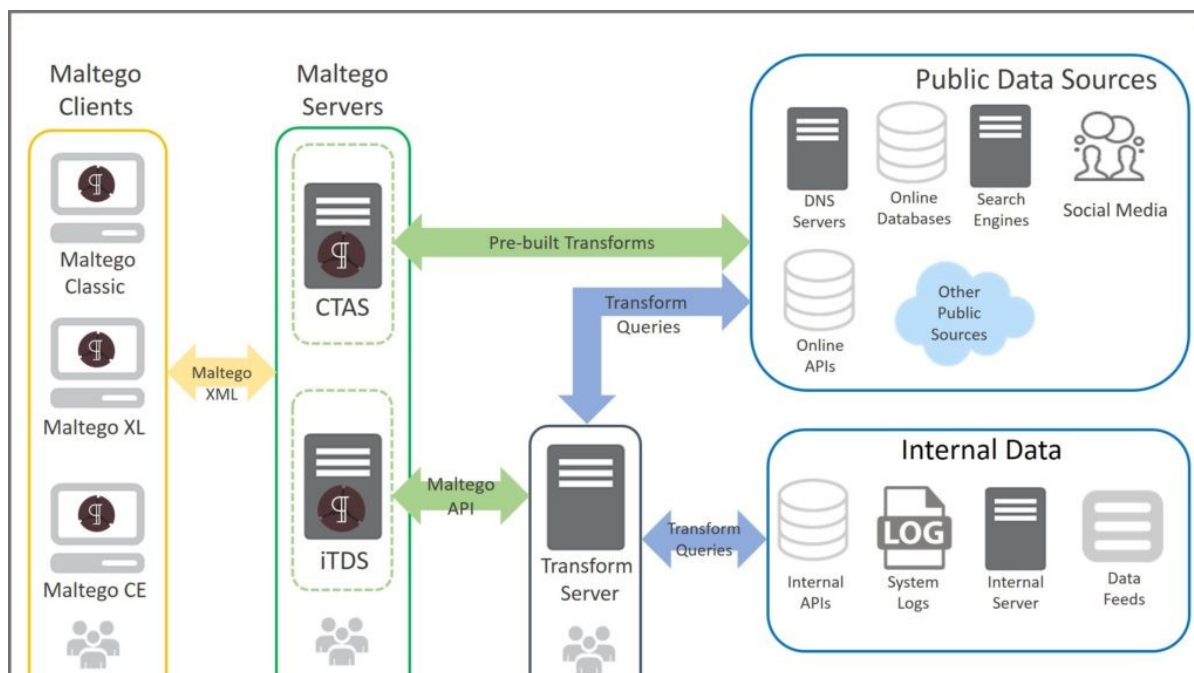
Como hemos podido ver, Maltego es una poderosa herramienta que es usada a menudo por delincuentes analistas individuos para recopilar información sobre personas y empresas. Este uso no comercial, y limitado en cuando a los resultados de las búsquedas, es suficiente para hacernos a la idea de un objetivo y tener un vistazo rápido.

Sin embargo, uno de los grandes inconvenientes de Maltego es cuando se usa de manera comercial en empresas dedicadas a ciberseguridad (Maltego XL y Maltego Classic). Por lo general, la política de las empresas del sector es de no compartir ni la información que se está buscando, ni la información obtenida. Es bien sabido que aplicaciones de este estilo, recopilan la información de las IPs que la están usando, y de los resultados que obtienen, para así retroalimentar su propia base de datos.

Para evitar esto, Maltego nos ofrece tres alternativas a consultar la información al servidor público:

- CTAS: servidor privado con todas las ventajas de utilizar una infraestructura propia donde alojarlo, y con acceso a las fuentes de información pública.
- iTDS: servidor de distribución donde las transformadas personalizadas pueden ser administradas, compartidas y distribuidas por una organización y sus integrantes, y con acceso a las fuentes de información pública, así como a fuentes de información propias de la organización.
- Comms: servidor privado que permite compartir grafos en distintas sesiones.

Tened esto bien en cuenta, ya que si usáis Maltego con la licencia gratuita en una empresa, y os hacen una auditoria podríais tener problemas; y si usáis una licencia comercial y las políticas de vuestra empresa especifican que no se debe compartir la información de los objetivos, tendríais que contratar uno de estos servidores dependiendo de vuestras necesidades.



End Users

Server Admins/
Developers

Developers

Descripción general de los servidores

Y nada más por hoy!! Al final me ha salido una entrada un poco grande..., espero que terminéis de leerla y os pueda aportar algo para mejorar vuestra labor «juankeriana». Cualquier duda será bien recibida y atendida (por comentario, telegram, ...), y si queréis que se escriba sobre algo más relacionado con Maltego no tenéis más que comentarlo!!

En la próxima entrada sobre Maltego contaré con la colaboración de un gran compañero de trabajo, y hablaremos de cómo automatizarlo: a todos nos apetece de vez en cuando tener una aplicación de botón gordo e ir a desayunar...

Y si queréis leer más entradas relacionadas con OSINT, os dejamos por aquí una entrada muy interesante de nuestro compañero Marcos sobre [OSRFramework](#).

Gonx0