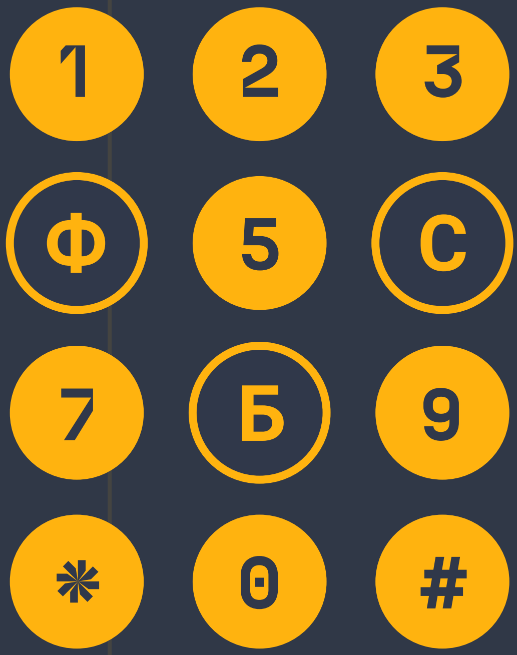
case study

Investigating the Alleged Leak of FSB Agents' Phone Numbers



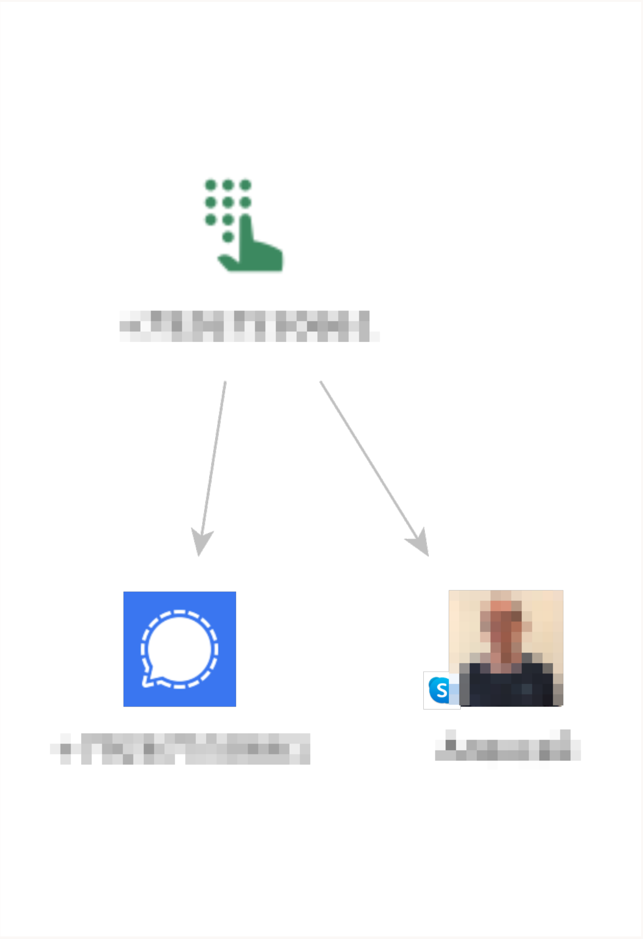
MALTEGO

Person of Interest: Investigating the Alleged Leak of FSB Agents' Phone Numbers

Oftentimes, investigators do not possess ample information to launch a person of interest (POI) investigation. They may have a name or an alias as a starting point, which is the most common scenario but not most optimal, as these types of data are not always strictly linked to a unique individual. While people may randomly share a name or an alias without being connected in any other way, a phone number of an email are data types that investigators may pivot off of with a much higher degree of confidence in the results. However, a phone number or an email might not yield as much information as a name or an alias.

To conduct a successful POI investigation, an investigator must combine the previously mentioned types of personal identifiers in order to harvest the maximum amount of information. We will demonstrate this in the following investigation.

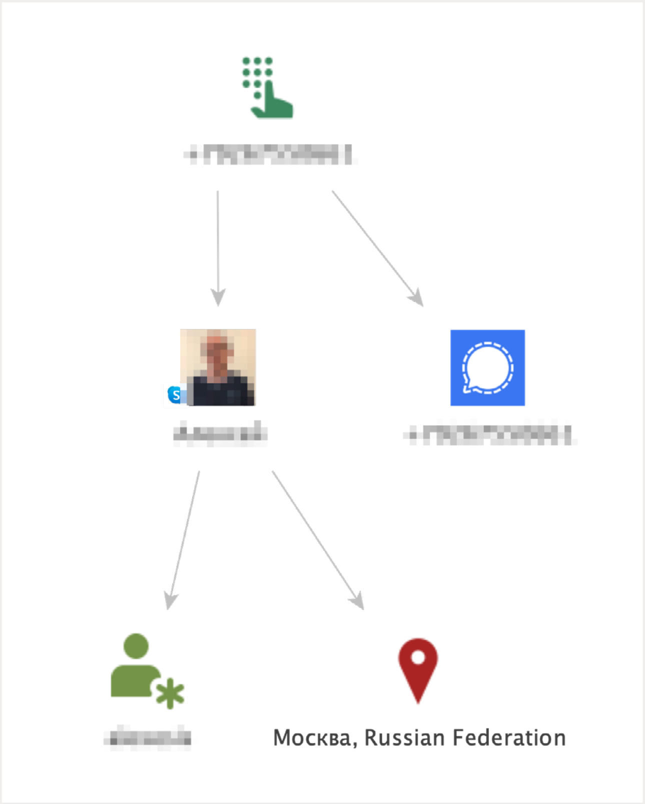
Recently, a list of phone numbers—supposedly belonging to employees of the FSB, one of the main Russian security agencies, was published by the Defense Intelligence of the Ministry of Defense of Ukraine. In this case study, we will investigate these phone numbers in an attempt to validate them.



To start our investigation, we will paste the phone number we want to investigate into Maltego. The first thing that one can do to investigate a phone number in Maltego, is to run the **SocialNet – Bulk Search** Transform. This ShadowDragon Transform will probe all social media platforms which allow their users to be searched by phone numbers. Two accounts come up: A Signal account and a Skype account. The Skype account displays a profile picture. We are also able to obtain an alias and a location using the **SocialNet – Extract Alias** and the **SocialNet – Extract Location** Transforms. In this situation, we have two things going for us:

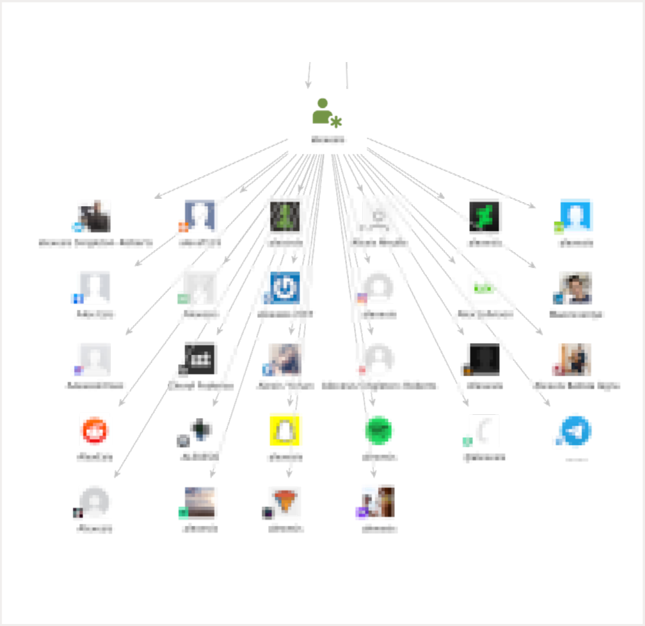
1. The resulting alias is not very common and therefore unlikely to be used by a lot of different people.

2. We have enough information to differentiate accounts linked to our Person of Interest (POI) from accounts operated by strangers who incidentally have the same username: We have two different pictures that include the face of our POI, a city, as well as a first name which is displayed in the Skype profile.



With this in mind, let's run the **SocialNet – Bulk Search** Transform on this alias.

Oftentimes, when performing a bulk search on an alias, several dozens of accounts may be brought into your graph. To find the needle in the haystack, we can start by searching for the location that we have: "Moscow" with the use of the search bar. We can also search for the name displayed in the Skype profile.



The point is to find commonalities between what we know of our POI and the profile returned by the bulk search.

Unfortunately, the search bar does not seem to be enough here.

Since this first approach did not work, let's begin reviewing the accounts one by one. Approaching this task logically can save us a tremendous amount of time: Since our POI is tied to Russia, we can start with profiles that belong to social media platforms that are more popular with this demographic. Mail.ru and VKontakte are great starting points.

> After several minutes of browsing different profiles on our graph, it is clear that none of the profiles we are exploring have information that matches what we know of our POI.

This could be the end of the investigation; however, there is still one card left to play: Pivoting off of the profile picture we obtained earlier. ShadowDragon SocialNet allows you to perform a reverse image search using 3 different search engines: Yandex, Sogou, and TinEye. Each of these engines cater to a different public. For example, the vast majority of Yandex's users are Russian.

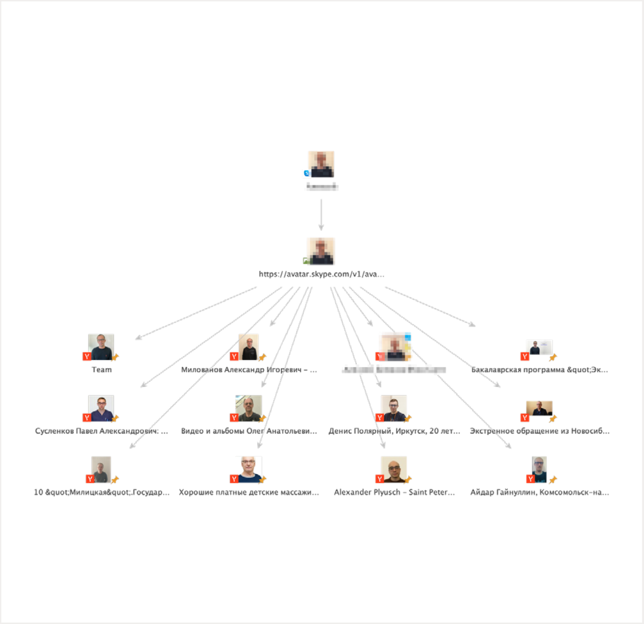
The consequence of this is that they will offer you different results and will perform better or worse depending on the image you are searching for. Suppose the image in this investigation was linked to a Chinese POI. Then maybe Sogou will do a better job than TinEye or Yandex.

To perform a reverse image search, we first need to add the Skype profile picture to our graph as a separate Entity. This can be done by running the **SocialNet – Extract Image** Transform. Next, let's use Yandex to search for similar pictures on the Internet. Before doing so, let's check our Result Slider: We have 4 different options: 12, 256, 4K, or 65K. It must be noted that this reverse image search is a fuzzy search, meaning the results will not always be exact copies of the image searched for.

So, after running the Transform, we will have to examine the results to find the images that are indeed the same as the one we started our search from. With this in mind, setting your slider results to 4K or higher will not be useful. After all, looking at, and manually comparing four thousand images is not something an investigator would have time to do. Let's set the slider at 12 for now and execute the **SocialNet – Search Yandex for Images** Transform.

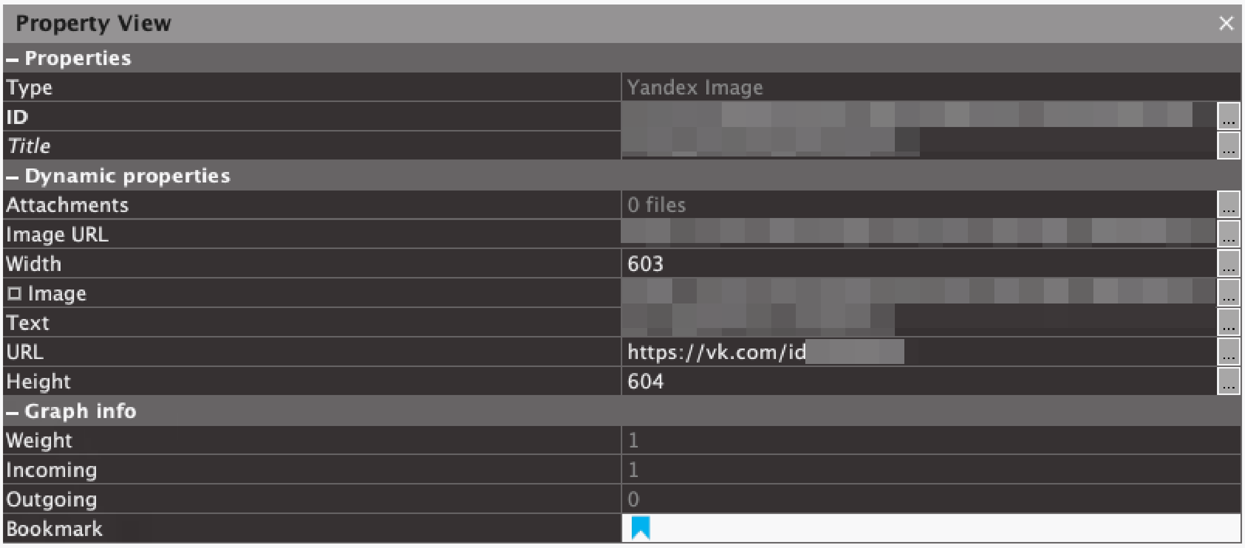
The results are mostly in the general vicinity of the POI profile's picture, but there is a particular one that is a perfect copy. Luckily for us, the URL is tied to a VK account.

When opening this VK account in our browser, it appears that it indeed belongs to our POI. The profile displays personal information, including workplace, name, and surname as well as hometown and current city of residence. We could harvest all of this information manually from this page, but it is easier to automate this collection process using SocialNet.


[redacted]
https://avatar.skype.com/v1/ava...
Team
Милованов Александр Игоревич – ...
[redacted]
Бакалаврская программа &quot;Эк...
Сусленков Павел Александрович: ...
Видео и альбомы Олег Анатольеви...
Денис Полярный, Иркутск, 20 лет...
Экстренное обращение из Новосиб...
10 &quot;Милицкая&quot;.Государ...
Хорошие платные детские массажи...
Alexander Plyusch – Saint Peter...
Айдар Гайнуллин, Комсомольск-на...

One small hurdle is left to overcome: Our usual workflow would be to start from a name using the **SocialNet – Search VK for Users** Transform. However here, we already have the profile, therefore there is no need to search for it. Also, if the name of our POI is common, this Transform could yield hundreds of profiles.

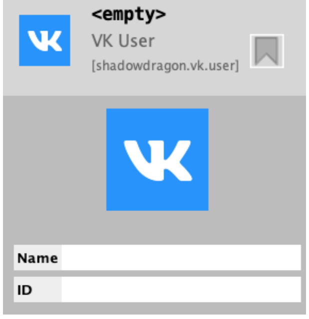
To spare some time, we load the right profile directly into Maltego: Grab a VK User Entity from the Entity Palette. After adding it to the graph, go to browser and look at the URL of the VK profile. It should be formatted like so:



Property View

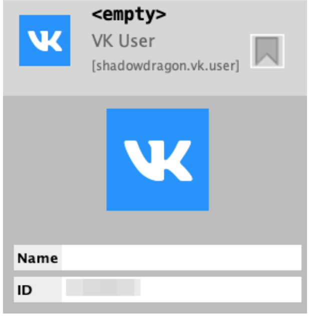
– Properties	
Type	Yandex Image
ID	[redacted]
Title	[redacted]
– Dynamic properties	
Attachments	0 files
Image URL	[redacted]
Width	603
□ Image	[redacted]
Text	[redacted]
URL	https://vk.com/id[redacted]
Height	604
– Graph info	
Weight	1
Incoming	1
Outgoing	0
Bookmark	

https://vk.com/id... with a list of digits trailing behind the "id" string. This list of digits is the ID of the VK profile. Replace the ID of the blank VK profile you added to your graph with the ID of the target profile.



<empty>
VK User
[shadowdragon.vk.user]

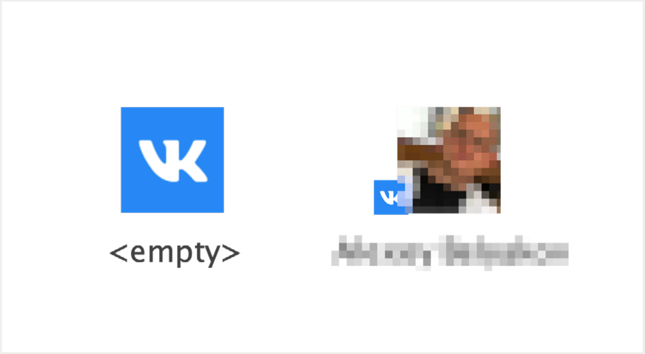
Name
ID



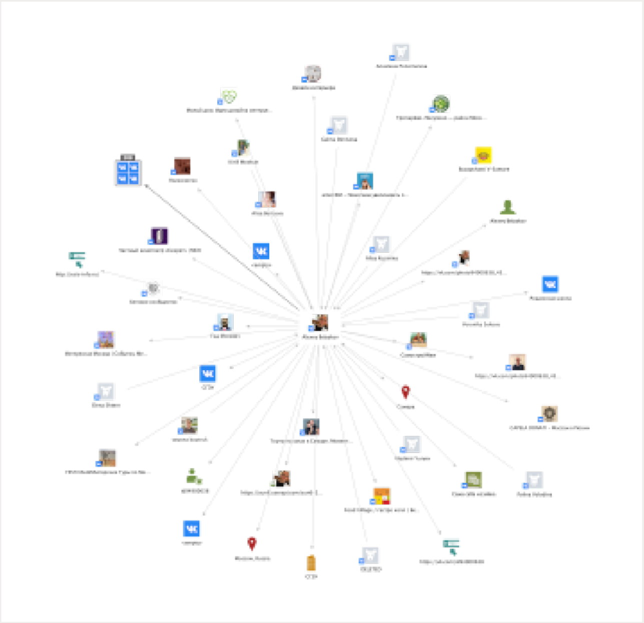
<empty>
VK User
[shadowdragon.vk.user]

Name
ID

After doing so, run the **SocialNet – Fill Extra Info** Transform. This will populate the VK profile with information that would normally get returned by the **SocialNet – Search VK for Users** Transform.



Then, to gather more information, one can simply run all the available SocialNet Transforms on this VK profile, populating the graph with our POI's hometown, his current job, friends, posts... Everything we would need to continue our investigation.



We hope you enjoyed this walk-through of how to use ShadowDragon SocialNet to conduct your person of interest investigations. Happy investigating!

About the Author

Mathieu Gaucheler is a subject matter expert at Maltego. His responsibilities include research-driven content development for blog posts, webinars, and talks. He started working in cybersecurity in Barcelona, focusing on malware analysis and sandbox development. He has previously presented his research at BotConf and RSA APJ.

For more information, please visit maltego.com

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

MINE • MERGE • MAP / DATA

Maltego Technologies GmbH
Address: Paul-Heyse-Strasse 29, 80336 Munich
Email: contact@maltego.com
Phone: +49-89-24418490

MALTEGO