SOCIAL LINKS CASE STUDY: EXPOSING LINKS BETWEEN CRIMINAL ACTORS

Since 2015, Social Links has been proud to provide its partners with a way to view open-source data in a clear and comprehensible way. Our range of products including Social Links PRO for Maltego and IBM i2, Gamayun, and our integrated investigation hub SL BOX, have allowed our partners to enrich their investigations and achieve their goals, whether it be criminal investigations, lead generation, or due diligence. Besides offering the tools for such open-source investigations, our team of professionals is always willing to help our clients out with their real-world cases. In today's blog post, we will be exploring a real case that one of our partners shared with us.

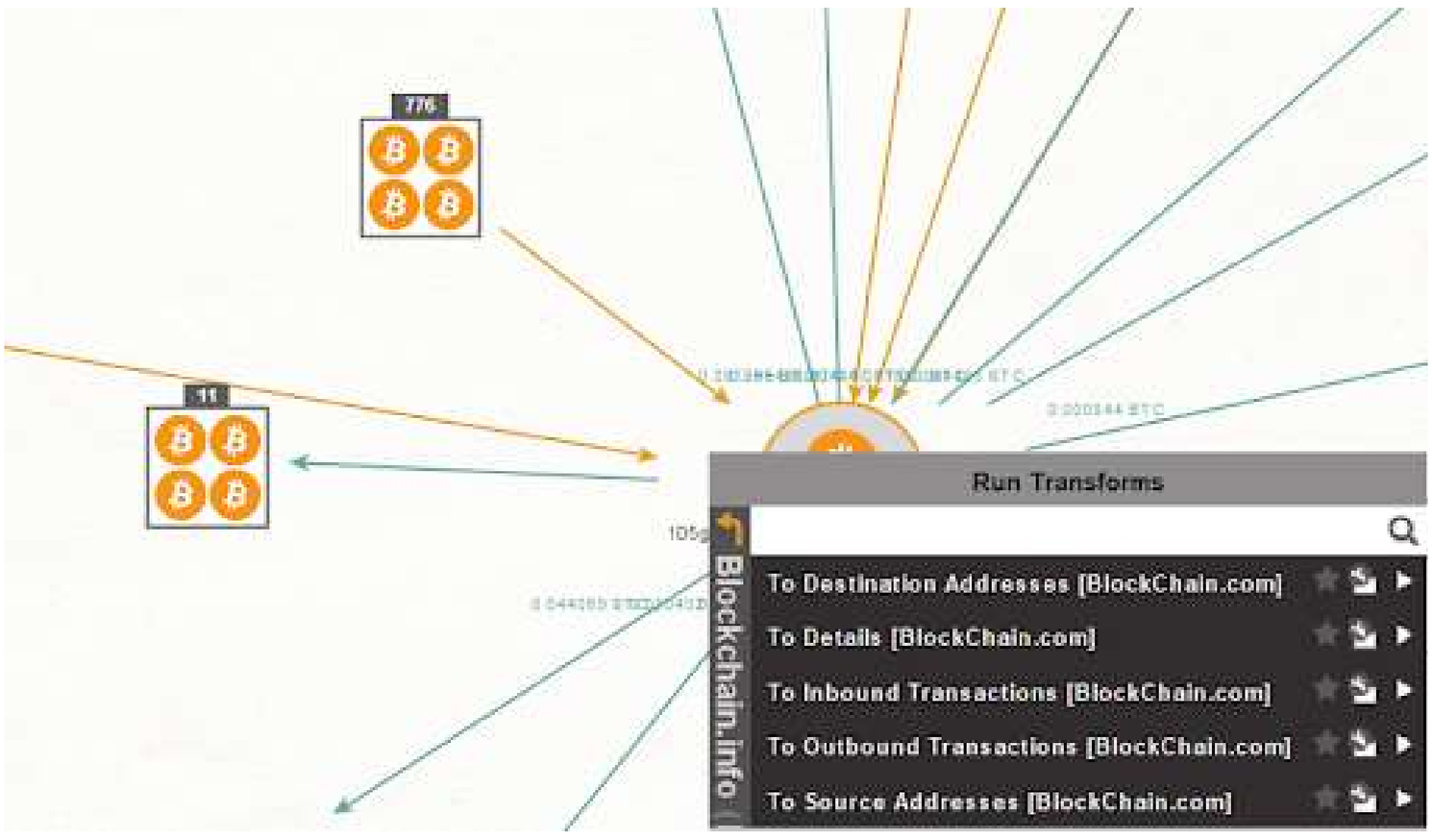
The partner in question had undertaken a case at the request of one of their clients (Country A), who had been the victims of criminal activity that they knew was originating from outside of their borders, with the suspicion that a neighbouring country was involved. Our partner started the investigation through traditional investigative methods and provided us with starting input data. They presented us with two cases, which we shall refer to as Case A and Case B respectively.

CASE A

01

The first case's goal was to discover who was behind the deanonymization of government employees of Country A, and the subsequent dissemination of that information through various channels on the internet. As with any investigation, we needed input data for our starting entities and Social Links were provided with various alias', VK profiles, Telegram channels, and the name of one particular individual. Using Pipl, a third-party world-leading provider of online identity information that can be integrated into Social Links, we discovered that the individual had ties to a bordering state of Country A.

Furthermore, our partner provided us with the address of a Bitcoin wallet, as they had already established that it was under the control of the criminal actors to receive payments for their activities. Utilizing our vast range of search methods that look at cryptocurrencies and those of Blockchain.com (that can be installed for free in the Maltego Transform Hub), we were able to see the ingoing and outgoing transfers and the wallets connected to these operations.

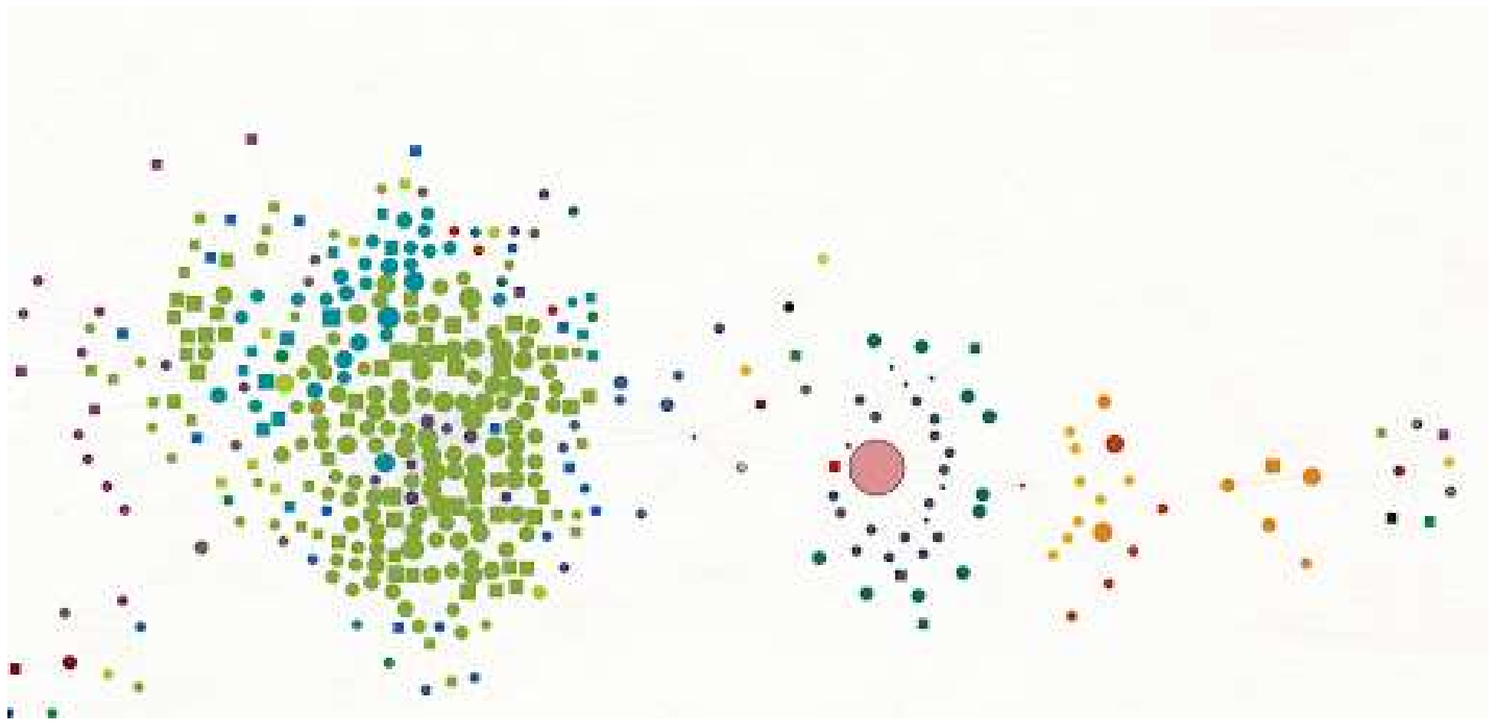


Pic. 1. Blockchain.com transforms allowing us to see the inbound and outbound transfers from the wallet.

CASE A

02

As the Dark Web is a hub for criminal activity, we decided to check whether any of these wallets had been mentioned on the darknet forums and marketplaces that Social Links constantly scrapes using the transform [Darknet: Search Bitcoin Wallet]. The search came back with a post on DreadForum, a dark web discussion forum similar to Reddit. From that post, we were able to retrieve an Alias that would allow us to delve even deeper.



Pic. 2. Interconnections between different entities as seen within Maltego: the red dot is the bitcoin wallet that the criminals used to receive payments. To the left are the social media entities linked to the criminal actor, and to the right of the wallet are the darknet posts related to it.

To our excitement, this alias was found in the SL ISE (Identity Search Engine with over 10TB of data) through the transform [SL ISE] Search and provided us with an IP address and a location. We validated the IP address through Shodan, a third-party platform that can be integrated into Social Links, to double-check the accuracy of this information. This service was able to find open ports, a location, an IP provider, and the domain of the IP provider. The results backed up the partner's hypothesis that the criminal actor was residing in a neighboring country of Country A.

CASE B

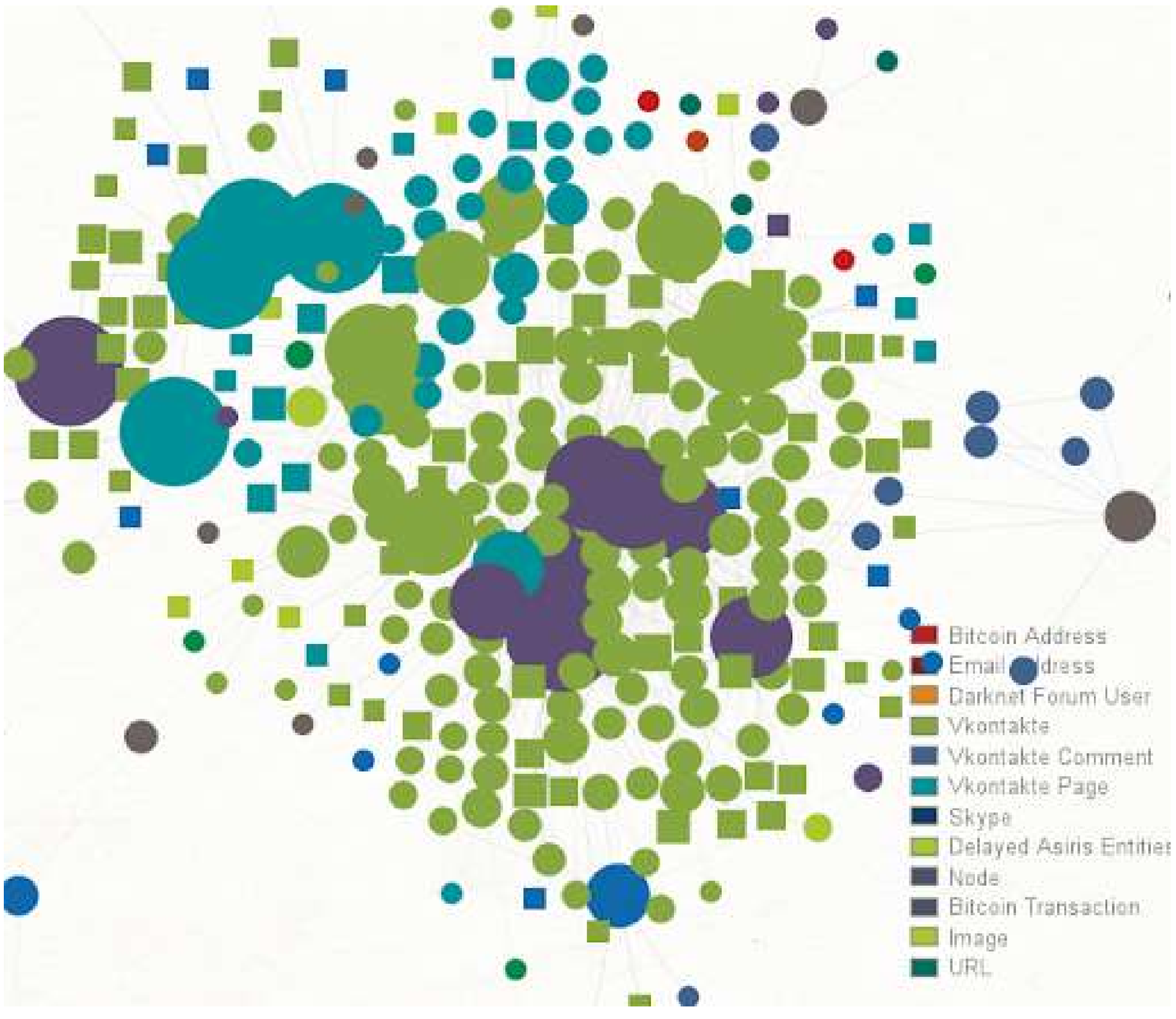
01

The second case was similar in nature to the first one but involved telephone swatting, a serious "prank" call that elicits a response from law enforcement. This can range from false bomb threats to claiming there is a hostage situation. Swatting leads to law enforcement potentially missing genuine incidents, wasting the taxpayers' money, and, in rare cases, to the death of individuals. As with Case A, our partner's client suspected that these activities were being coordinated by individuals from one of Country A's bordering countries. Our partner provided us with VKontakte profiles, the majority of which were fake profiles, Telegram accounts that stated the pricing set by the criminal actors, and an email address.

Using our Telegram search methods that we introduced in July, we could see that the Telegram profiles stating the pricing were not originally under the control of the criminal actors, but hacked accounts. From the VK profiles, our team used our range of transforms for this social media platform to enrich the graph. We saw a vast number of profiles and groups that were interconnected with each other, as well as the majority of groups all sharing common themes, and the profiles located in neighboring countries of Country A. Within these groups, we ran the transform [VK] Get Group Members. The results showed that many of the profiles in these groups had the same surname, and there was a common theme in the naming structures that shared this surname. This indicated that these profiles were under the control of a single actor, and the vast number of profiles made us believe that it must be under the control of a criminal organization.

CASE B

01



Pic. 3.
Running our vast range of VK search methods, we were able to build a network of profiles, groups, and pages, and see how they were interconnected.

The most fascinating part of this investigation was that our partner had once again provided us with a Bitcoin wallet that the criminal(s) used to accept payments. After running the same crypto search methods as in Case A to find ingoing/outgoing transfers, we exported the results of the two graphs to see if there were any common wallets. The results came back to us with the same Bitcoin wallet that had been provided to us in Case A! This was a surprise to our partner and our team, as, before this discovery, there was no hard evidence that these cases were linked to each other.

FINDINGS

OUR INVESTIGATION HAD PROVEN, WITHIN REASONABLE DOUBT, THAT:

A

The criminal activity was originating in a neighbouring country of Country A.

B

The two cases were linked to each other, and in all likelihood, the same criminal actor was behind each one.

Social Links was able to aid its partner in formulating the hypothesis that individuals from numerous bordering nations of Country A were using cryptocurrency to finance their criminal operations. There is an incontrovertible relationship indicating that the cases were linked via these wallets, and enrichment of VK, Telegram, and Darknet entities verified that these individuals were from neighbouring nations.
Our partner forwarded this material to its client in order for them to continue their investigation and establish whether or not this criminal behaviour is state-sponsored.

TO CONCLUDE

We hope you enjoyed this case study demonstrating Social Links' effective capabilities in finding links between different entities and making breakthroughs in investigations. Please contact us if you have similar cases underway so we can help you solve your investigations and show you the power of open-source data extraction and analysis!

ABOUT SOCIAL LINKS

Learn more at
sociallinks.io

Contact us for more information:
sales@sociallinks.io

Social Links is a Netherlands-based IT company providing OSINT solutions for law enforcement and customs divisions, cybersecurity operations, and major corporations, with more than 300 clients worldwide.