Spid3r

“ We bring the unknown to light. “

Case studies

1.Competitive Intelligence Research for a Multi-National Corporate

A multi-national medical device company wished to understand its key competitor's pricing and external funding sources, after learning that the competitor was selling a similar product at a significantly reduced price in several countries.

Using open sources and personal interviews, there was discovered that the competitor received vast sums in subsidies from several sources, including a European Union research and development program and local scientific funds. The competitor also collaborated with local centers of excellence and universities that conducted R&D work for the company using government allocated funds. Total funding and savings amounted to over €65M, which gave the competitor the power to undercut market prices.

This understanding of the competitor's sources of funding, as well as the vitality of its pricing strategy, allowed our client to develop a plan to restructure its own R&D funding to generate major savings and improve its competitive position.

2. Identification of Bribery During Multi-Billion-Euro Arbitration

The client was a multi-billion-dollar American firm that entered the investigated market with the assistance of a local partner. The relationship between the two started deteriorating with time, leading to a series of lawsuits whereby the client now former partner sought damage refunds for over two billion Euros.

The arbitrators appointed to the case adopted several unbalanced resolutions that raised the client's suspicion. The research and operations conducted by the teams disclosed pre-existing relationships between some of the individuals involved in the case, uncovering that the client ex-partner had bribed the chief arbitrator. There was obtained a statement by the latter bragging about his ability to guarantee a favorable outcome to a given party.

This evidence drastically changed the balance of forces in the case. From a position of disadvantage, the client was able to file several lawsuits against both the ex-partner and the chief arbitrator, forcing the ex-partner to reach a compromise with the client .

3.Investigating into Detrimental Financial Campaign

UK, France, Spain, Germany, Brazil, Israel

Following a harsh negative campaign in the financial industry that eventually led to a down-grade by international credit rating agencies, approached by the client to locate and investigate the sources and motivations behind the campaign. The client had gathered testimony from several of its investors regarding details passed around the market making strong allegations in regards to the financial behavior of the client, with precise recommendations not to invest in the company. Using these initial findings to reach further into the industry and extract the intelligence regarding those behind the negative campaign.

Performing an in-depth open source research and analysis of the client's financial history within the market, in order to gain a full understanding of the relevant industry and key players. Then the case itself was detailed and organized into a comprehensive timeline in order to best interpret its context and pinpoint relevant individuals. We then mapped potential links to the campaign across the financial market, including the client's investors, investment bankers, the credit agencies, the financial media and even companies the client had partnered with on joint ventures.

Each of the individuals pinpointed by the research team was thoroughly profiled, using personal and professional history, connections, and behavioral patterns. Potential sources were contacted using long established and reliable web identities and advanced social engineering capabilities. The intelligence provided by these sources strengthened the understanding of the

case. Additionally, their connections within the industry were used to further establish a network of reliable sources.

Using gathered intelligence together with extensive open source research, the team was able to diagnose the nature and significance of large scale procedures within the financial market. Additionally, the intelligence gathered from the sources proved invaluable to solving the case, with details provided in regards to exact dates, conversations, motives and internal dealings and consequences that pointed directly at those responsible for the campaign. The team identified two specific individuals who had acted separately but in tandem in regards to the attack on the client. It was also shown that both of these key individuals continued to harbor negative opinions in regards to the client's financial dealings, and both remained in key positions of influence within the financial industry. All findings were provided to the client with insight regarding the way his financial dealings were being perceived by the public and the market, allowing him to carefully consider his actions.

4.Proving Misrepresentation in Arbitration Proceedings

Israel, Georgia, Chile

The client faced a large-scaled arbitration proceedings, initiated against him on grounds of an alleged breach of a signed contract for conducting an infrastructure project between the plaintiffs and the client. The client vehemently denied the mere existence of the contract, let alone signing it, and needed to gather evidence to prove that the contract was never signed and the business relations subject of the contract have never occurred. The client, who is a large and well-established player in the market, argued that the plaintiffs misrepresented their size and essence and claimed that it is unlikely that it would get involved in a significant infrastructure contract with companies of such size, as suggested by the alleged contract.

There have been successes in gathering relevant intelligence that demonstrated that there is a considerable doubt in regards to the existence of any business activity of the plaintiffs, and thus undermined the representations submitted by the plaintiffs in regards to the scope and volume of their business.

A thorough investigation which included researching both open sources and typically inaccessible sources, as well as actively approaching relevant individuals, has proved that the plaintiff presented a false picture of his conduct. It showed that there were no employees in any of the plaintiffs companies in the past or present, that a person who was mentioned by the plaintiffs as one

of their employees does not exist, that the plaintiffs did not reside in their alleged, official addresses and that all the phone numbers allocated to them were disconnected.

Furthermore, there was performed a comprehensive research regarding several contracts signed by the plaintiffs, which were disclosed in the arbitration. It has been managed to reach the signatory of each contract, and managed to get the majority of them to confirm that they do not know and have not conducted any business neither with the plaintiffs nor with its director, despite of the fact that they have allegedly signed these contracts. Some other signatories did know the plaintiffs, but have positively refute any business relationship with them, emphasizing that they only had a friendly relationship with the plaintiffs' director.

There was submitted all findings as an expert opinion, as part of the arbitration proceedings.

5.Identification of Fraud

China, Ukraine, Kazakhstan

The client had noticed several anomalies in a large acquisition by a significant technology company in China. The belief was that the acquisition was a related party transaction, and that the basis of the deal was fraudulent, even though no such relationships had been declared by either party prior to the acquisition. Project was retained to identify any fraud in the transaction and/or any previously undeclared relationships.

'The Great Firewall of China' has made internet-based communication in China difficult, but has had the unintended effect of creating a vibrant community of political dissidents, watchdogs, activists, and journalists in the deep web, who communicate via hidden dark nets. This community, unique in its size in China, possesses a wealth of information and knowledge, but is notoriously difficult to penetrate.

In order to overcome this obstacle, it began with a comprehensive open source investigation, including a search of all relevant company databases in the People's Republic of China. The investigation also looked into limited access databases that on-the ground associates and contacts in China were able to access, in order to identify the basic structure of the target company and the key players in the company's operations.

From this, it was able to map all of the key players' associations, and to reveal hidden relationships and indicators of undeclared motivations, particularly on the part of the primary shareholder of the acquiring company, who had many undisclosed ties to the

acquired company. Furthermore, there were several indicators of fraud on the part of the acquiring company's primary shareholder.

Using long-established deep web identities and advanced social engineering capabilities, challenge was accomplished to reach, recruit and verify several well-placed sources, who claimed to hold relevant information in this case. Two of these sources were able to return verifiable information regarding the fraudulent activity in the target company - including legally obtained company documents which showed that the aforementioned shareholder was using the acquired company as a 'personal bank account'. The documents also showed that there was a pattern of abuse of employees of a subsidiary company operating in Eastern Europe, and withholding of wages led by the shareholder, as well as evidence of tax evasion, and evidence that the major shareholder was hiding company holdings under the names of family members and close associates.

6.Asset Tracing

Panama , Central America, EU

The case was in possession of a very significant judgment against an individual and a target company (both Panama), and needed to identify any tangible and recoverable assets, including bank accounts, and understand their value. Due to the nature of the enforcement orders, the areas of focus for the client's recovery efforts were physical assets Panama, and financial products and bank accounts in Central America and Europe. A thorough search of limited access databases quickly revealed several firms (Panamian plantations) of significant value, along with several other tangible assets of value, including real estate in Europe. Following this, there was performed an initial mapping of all

relevant entities and companies, and identified several new companies within the subject's company structure.

Created a short-list of companies that the subject was believed to hold significant numbers of shares in, but that do not release any information regarding shareholders. Furthermore, it was identified several individuals that were well positioned to provide information on the subject's financial holdings. Using proprietary combination of deep-web intelligence collection, human intelligence, and social engineering techniques, There was discovered that the subject held significant numbers of shares in two previously unknown companies with value in the tens of millions.

Using the previously created map of key players, and intelligence gained from the individuals identified as having knowledge of the subject's financial holdings, There was constructed an intelligence dossier sufficient to obtain Intermediary Bank Discovery subpoenas against 17 target companies. Managed the discovery process from beginning to end, processing and analyzing all data received – which was well over 1,100 separate bank transactions. As a result, over 24 new bank accounts were discovered, and the movement of over 600M USD was tracked.

Further to this, several new companies that were eligible for recovery efforts were identified. As well revealed fraudulent transactions that provided the basis for piercing the corporate veil in US courts, allowing for the addition of further defendants to the judgment.

7.Employee Data Leakage

UK, USA

We were contracted to investigate recent data leakage by the client's employees.

After identifying potential sources of leaks amongst the client's employees and categorizing them into expanding 'circles of risk', we proactively engaged in areas with a high likelihood of leaking information.

Furthermore, our operators also monitored a broad range of sources and media; such as social media discussions, forums and news article talkbacks, in order to create a picture of employee satisfaction and identify potential leakers.

Our efforts not only identified those company employees who leaked the critical information, thus helping the client mitigate the risk as far as possible, but also discovered employee criticism of management, information that the client found very useful in planning its managerial strategy. We were using cyber tools , tracking locations , monitoring tools , social engineering and human intelligence.

8.Negative political campaign

Africa, USA ,Russia

We were hired to investigate a non stop negative campaign against a high rank politician in Africa. Our special team created avatars that through special tools and by cyber intelligence monitored the IT department who tried to conceal their operation and location. We obtained all their phones and accurate location and identification. The police has arrested the guys and through the investigation we have discovered who are behind this operation , the affair was published in the media and the politic party that was under attack became 10 times stronger , attack was stopped obviously .

9. Deffence and protection

UA , USA ,Guatemala

A well known multi billionaire was under cyber attack as a part of international espionage . We have tracked the attackers locations, phones , real identity . They were arrested.We have a special Scada department to protect critical infrastructures (energy / transportation / aviation / assets)

Type of clients

Finance institutions / Banks

Multi national corporations

Public Sector – Gov institutions

Critical infrastructures –

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
- agriculture, food production and distribution;
- heating (e.g. natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- financial services (banking, clearing);
- security services (police, military).

Private sector (VIPS)

Any client who has a unique and sophisticate affair and need a special solution .