A REAL OSINT CASE: UNCOVERING A HACKER GROUP

OSINT investigations are like intricate puzzles that require meticulous research, often leading to a maze of different paths. While discussing the theory is helpful, the real treasure lies in experiencing an actual investigation unfold. That's why, at Social Links, we create case studies. These help experts learn from real situations and develop fresh ideas to solve tough cases.

In this article, we're embarking on a detailed journey through an investigation conducted by the Social Links Center of Excellence into a hacker group that steals and sells the personal information of ordinary people. We're going through the steps of how a Social Links investigator identified the malicious actors and created a complete digital footprint with SL Professional. So get ready for an up-close look into the inquiry process of a real case.

Let's check it out!

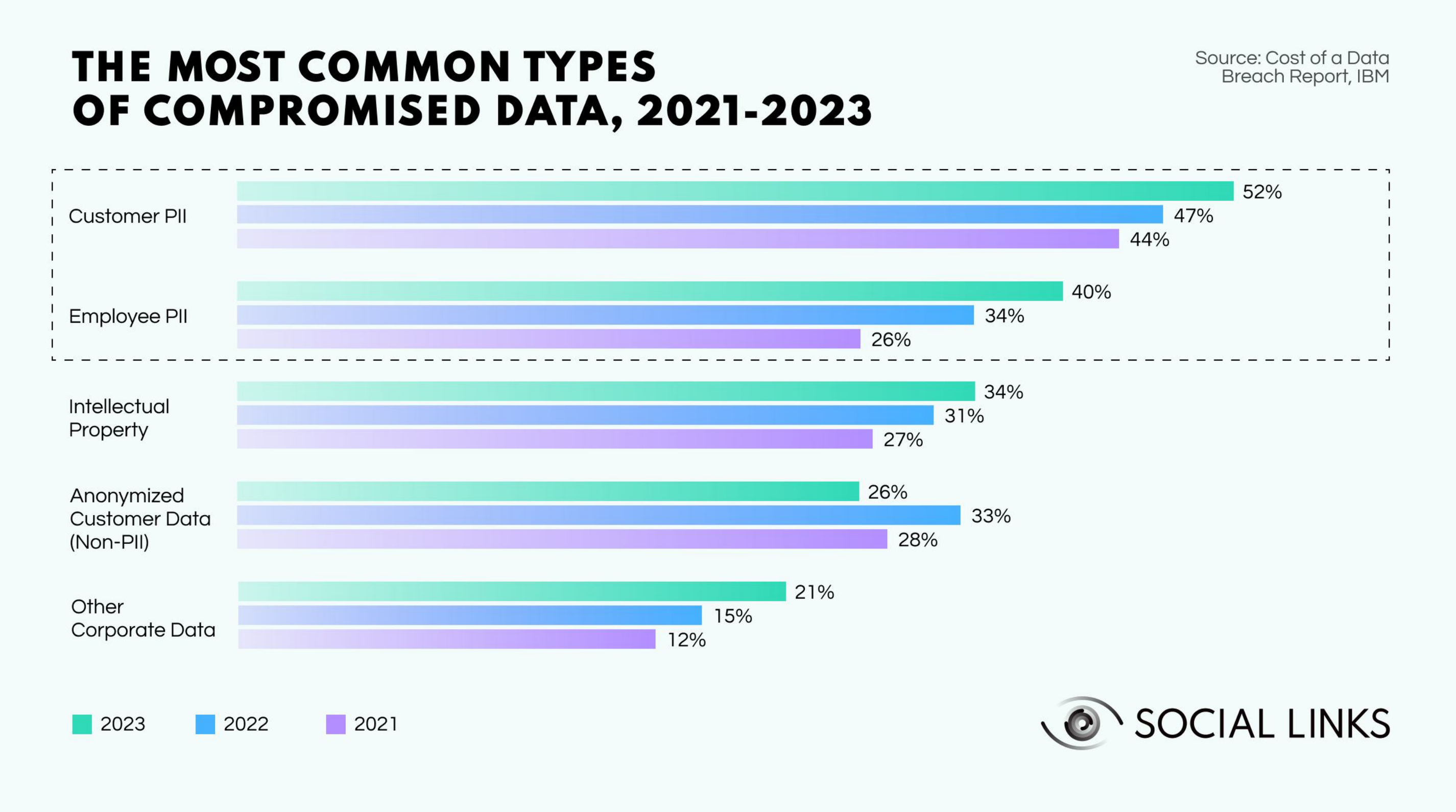
- The Challenge
- The Cast of the Investigation
- The Course of the OSINT Investigation
-
- Next Steps

THE CHALLENGE

Smaller criminal groups often prefer targeting ordinary people instead of businesses. These malicious actors use such tactics to conceal their operations from the public. Data brokering organizations stand out as a particularly menacing threat among these criminal entities. They specialize in the illicit act of stealing personal information, which eventually finds its way into the shady marketplaces of the Dark Web, fueling the ongoing cycle of cybercrime.

With this understanding in mind, let's turn our attention to an investigation centered around a loosely organized criminal group. This collective clearly understands the importance of maintaining anonymity while pursuing their unlawful activities. They are adept at avoiding easily traceable identifiers. However, even in the darkest situations, creative thinking can overcome challenges; this case study is a compelling example.

The main reason for such investigations is the widespread compromise of customer data in breaches. Personally identifiable information (PII) is a highly sought-after commodity for hackers. Dedicated Dark Web marketplaces exist to sell this data, and prices fluctuate widely. Some malicious actors are ready to pay up to $1k for complete documents containing IDs, social security numbers, etc. Threat actors use stolen personal data for fake documents and scams. In fact, recent reports suggest that a staggering 3.4B phishing emails are sent every day.



Customer and employee PII are the most costly and commonly compromised forms of data

THE CAST OF THE INVESTIGATION

Due to the sensitivity of the case, we've assigned aliases to all the individuals involved for privacy and legal compliance reasons. So, meet the cast:

- **Orion.** Social Links Investigator.
- **Apollo54.** The primary hacker and owner of the Illegal Data Brokering service.
- **NyxData.** Apollo54's right-hand man. Secondary hacker and Telegram admin.
- **InfoNest.** The name of the hacker group.

THE COURSE OF THE OSINT INVESTIGATION

Cybercriminals and investigators are locked in a constant game of cat and mouse, where threat actors break the rules and security experts bring them to justice. The following investigation is a prime example of how tiny decisions can snowball into a full-blown criminal inquiry.

PART 1. DISCOVERING THE HACKERS

> "A single spark can ignite a grand inferno..." - Orion

While most investigations start with an apparent victim, this one occurred by chance. One day, Orion, an investigator at Social Links, decided to examine an old email inbox he hadn't checked for a while. Curious about the contents of his spam folder, he decided to take a look. Amidst the usual flurry of scam offers like "Win a trip to Paradise!" and "Magic pills for all of your problems!" something different caught his attention—a phishing email.

Armed with Phishtool, a piece of software that analyzes emails using metadata and threat intelligence, Orion investigated further. He discovered that the email appeared to be from a hotdog vendor in Brazil. This got him interested. Orion decided to visit the company's website, only to be greeted by a bold message saying, "You've been pwned." Clearly, the website had been hacked and taken over.

In a cheeky move, the hackers had left their aliases (Apollo54 and NyxData) and the name of their group (InfoNest) on the front page of the compromised domain. Intrigued, our investigator conducted a Google dork and found more hacked websites associated with the same group. All of the sites had the same message, along with the same hacker names. Orion decided to delve deeper into the intruders' activities to better understand their actions' extent.

From a single email, the Social Links investigator found a whole group of cybercriminals

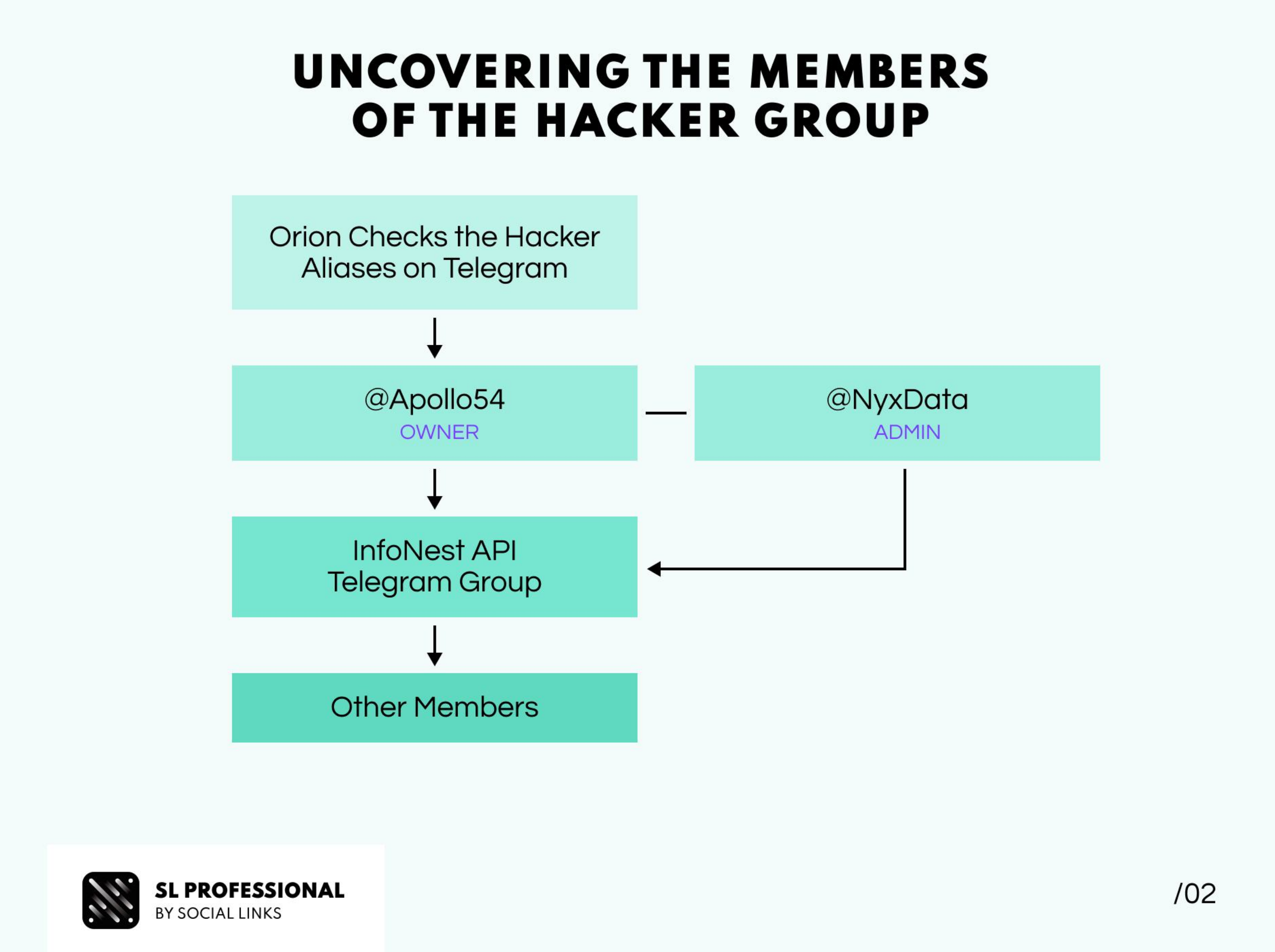
PART 2. DETECTING ILLEGAL DATA FOR SALE

> "A moment of inspiration uncovers an intricate investigation..." - Orion

With the investigation officially underway, Orion decided to check if the hackers were using any messengers to communicate with each other. Turns out they were—a Telegram group. To take his inquiry to the next level, our investigator enlisted the help of SL Professional's Telegram Pack (N.B. the extension is currently only available for government agencies). Armed with the right tool, Orion looked up Telegram's aliases, revealing that Apollo54 was the hacker group's owner, admin, and primary hacker. NyxData, on the other hand, was identified as his second-in-command. Impressively, the group boasted almost 200 members.

Their conversations revealed that this group was an eastern hacker group functioning as a data broker. Their modus operandi involved hacking and phishing to collect significant amounts of personal data. The group then bundled this ill-gotten information into an application programming interface (API), which they offered for sale. This API enabled buyers to conduct specific searches, including license plates, national ID numbers, birth dates, and more.

Orion's findings indicated that the group regularly updated its API interface, making it user-friendly for the paying customers of the hackers. Insights from the malicious actors' conversations revealed that core members took pride in their past clashes with Cyber Crime Agencies. Astonishingly, the threat actors even used the official insignias of LEAs as the group logo, making their involvement in criminal activities glaringly conspicuous.



With SL Professional's Telegram Pack, Orion was able to determine who controlled the illegal data brokering service and get leads on its wider member base

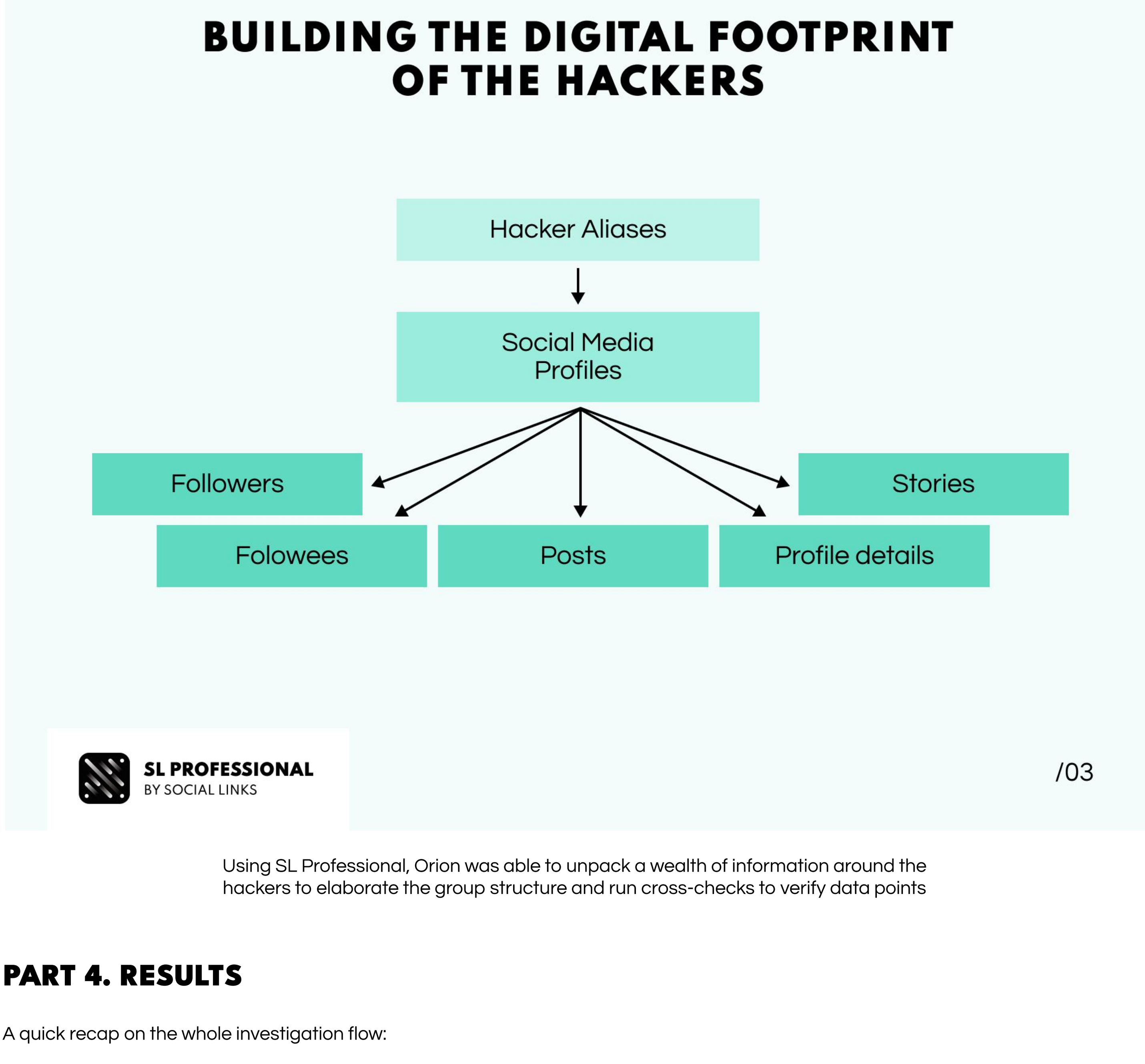
PART 3. BUILDING A WEB OF CONNECTIONS

> "A seemingly insignificant detail can sometimes unlock the truth..." - Orion

Armed with aliases and other distinct identifiers, Orion turned his attention to social media to extend his investigation. It became apparent that the threat actors employed the same aliases across their social media profiles and hijacked other users' accounts to promote their illicit API data brokering service. Utilizing SL Professional's powerful transforms, Orion discovered a noteworthy trend: the core members of the hacker group were interconnected through mutual followers lists and interactions (mentions, posts, stories, etc.) on Instagram.

Despite the hackers' cautious approach to concealing their identities, Orion ingeniously cross-referenced the available data using social media transforms that allowed getting aliases, followers, and followees, as well as profile details and story, to streamline the associations of these malicious actors' accounts across different platforms.

Following this comprehensive procedure, Orion amassed a collection of 31 Instagram, 2 TikTok, and 3 Twitter profiles. His astute fusion of messaging data with publicly accessible social media details effectively outlined the group's digital footprint. Through meticulous documentation of conversations, posts, and promotional content propagated via stories (showcasing the API and how the crimes were committed) by the criminal group, Orion established a compelling case for further investigation by Law Enforcement Agencies (LEAs).



Using SL Professional, Orion was able to unpack a wealth of information around the hackers to elaborate the group structure and run cross-checks to verify data points

PART 4. RESULTS

A quick recap on the whole investigation flow:

- Orion started with a phishing email, which he traced to hacked websites.
- Using the aliases the threat actors left behind, he pivoted the information and found the group's Telegram group chat and advertising channel.
- He searched the aliases the hackers were using on social media, cross-referenced the friend lists, and found out the malicious actors were following and interacting with each other on social platforms.
- The investigator proceeded to gather more evidence and, for now, finished the investigation.

NEXT STEPS

So, from this point on, there are a few paths the investigation can go.

FOLLOWING THE WEB. Since Orion already has plenty of evidence, he can further investigate and enrich his data on the hackers. With SL Professional, He can employ sentiment analysis and dive into public records to extract more information on the threat actors. By the end of the process, he would have their criminal history, real names, photos, and other acquaintances. However, this process would take a longer time and result in the case to grow further.

REPORTING TO LEAS. Orion can also forward all the evidence he gathered to the appropriate Cyber Crime divisions for them to pick up where he left off. Since the hackers are in the jurisdiction of government agencies, this could be a more effective strategy. Also, the threat actors were very open about their prior history with the authorities, which most likely means they have criminal files in the LEAs system. This could expedite the process significantly.

Orion can take one of two paths to conclude the investigation

---

Wrapping up our OSINT investigation case study, we hope you've gained an up-close insight into our experts' approach and found some inspiration for your own inquiries. Remember, with the open-source intelligence mindset, even the tiniest details can unveil entire information networks.