Analysis of Internet Black Market in New Types of Cyber-related Crime – Taking Personal Information Transaction as an Example

Guangxuan Chen[1], Anan Huang[1*], Bo Hu[1], and Guangxiao Chen[2]

[1]Zhejiang Police College, 310053 Hangzhou, China

[2]Wenzhou Public Security Bureau, 325000 Wenzhou, China

Abstract. With the rapid development of information technology such as cloud computing, big data, artificial intelligence and mobile internet, while bringing people many conveniences such as information interaction and online shopping, it has also gradually become a hotbed of new crimes. Traditional crimes are increasingly migrating to the Internet, and new types of cyber crimes are increasingly prominent. At the same time, the illegal crime chain that provides financial supply, technology, promotion, settlement and other assistance for cyber crime has been developing and extending, forming a tangled and complex illegal industrial chain. This paper reveals the current situation of the Internet black market in the new types of cyber-related crimes, explores the characteristics of the Internet black market, analyzes the industrial chain from the perspective of information flow, technology flow and capital flow, takes the information leakage industrial chain as an example, expounds the operation mode of the Internet black market in detail and judges its development trend, and then puts forward the comprehensive governance suggestions, providing reference for relevant departments.

1 Introduction

With the advent of the era of big data, the network has become irreplaceable in human society. According to the 50th Statistical Report on the Development of Internet in China released by the China Internet Network Information Center (CNNIC), as of June 2022, the number of Internet users in China was 1.051 billion, 19.19 million more than that in December 2021, and the Internet penetration rate reached 74.4%. The average Internet user spends 29.5 hours on the Internet every week, and the proportion of Internet users using mobile phones is 99.6%. However, when the Internet has provided great convenience for our lives nowadays, illegal and criminal activities are also spreading in cyberspace. China's 2020 Research Report on the Governance of Internet black market pointed out that by 2021, the market benefits of Internet black market will be the third largest economy in the world, and cyber crime will be one of the most noticeable risks in the world in the next decade. At the same time, Internet black market related crime is about to enter the AI era, and AI security will also become a key issue that cannot be ignored in all walks of life. Tencent released the Research Report on the Governance of Telecom Network Fraud in 2022, in which it analyzed and studied the current situation of telecom network fraud in 2022, and found that domestic telecom cyber crime was still operating at a high level, technology and methods were constantly updated iteratively, and the situation of network fraud crime was not optimistic. It can be seen that cyber crime is increasingly rampant in the information age, and the Internet black market is expanding, which has seriously threatened the information security and property security of citizens. It is difficult to fundamentally control the Internet black market only by traditional means, and more effective means of combating and governance are urgently needed.Use a two-column format, and set the spacing between the columns at 8 mm. Do not add any page numbers.

This paper attempts to reveal and analyze the new mode, industrial chain and capital operation mode of Internet black market and related crimes, and its new form in the current new cyber crime, as well as its crime scale, influencing factors and future development trend, and excavate its root cause and the dilemma of legal supervision, and enhance the academic attention to the Internet black market in the new cyber crime model. Finally, combined with the current laws, regulations and technical means, put forward countermeasures and suggestions for comprehensive treatment of Internet black market across departments, increase the sanctions on iInternet black market practitioners, and create a pure and healthy network environment.

* Corresponding author: huanganan@zjjcxy.cn

2 Related Work

2.1. International research on Internet black market

Internationally, the research on Internet black market can focus on the rise of cyber crimes such as network fraud, blackmail virus, malware, and the change and impact of cyber crimes.

The first hot spot is the research on the prevalence of online fraud. European scholars Steven Kemp, Fernando Miró-Linares, Asier Moneva and others conducted research on fraud in the Spanish and European context, and the results showed that online fraud has gradually become the most important property crime in Europe[1]. By comparing the criminal data of recent years in Kazakhstan, the scholars has found that network fraud has doubled in Kazakhstan in the past three years. Internet telephony technology has been widely used in business and personal communications, improving the way people communicate in their daily life and work [2]. However, criminals also focus on this media and use false advertising, marketing products, fake identity and other means to bombard end users by network telephone. The fraudster uses personal information such as credit card number and personal identification code obtained by fraud for financial fraud, which seriously damages the interests of the state and citizens. Muahammad Ajmal Azad, Mamoun Alazab and other scholars put forward a spam detection framework for the telephone network, which uses the social behavior characteristics of users in the network to identify malicious callers and protect citizens' information security and property security [3].

The second is the investigation and research on the use of blackmail virus, malicious software and other means to commit crimes. Through research and analysis, scholar Ford Eric W believes that the healthcare industry is the main target of ransomware attacks, and the health sector is particularly vulnerable to phishing attacks. Malware is a serious threat to people's use of intelligent technology. It has been used to attack mobile devices since its birth. According to scholars such as Moutaz Alazab and Andrii Shalaginov, mobile applications with malicious attacks can be divided into two categories: fraudulent applications and malicious injection applications [4]. After establishing an effective classification model and formulating an efficient API grouping strategy, they found that these mobile applications with malicious attacks frequently request dangerous permissions to access sensitive data than ordinary mobile applications.

The third hot spot is the research on the situation change and impact of cyber crime. During the outbreak of COVID-19, the number of property loss cases caused by cyber crime increased significantly. The gradual reduction of people's use of cash and the improvement of the degree of convenience of computer technology have exacerbated the rising trend of the crime of network property infringement that integrating new network means. Choi Kyung shick used logical analysis, comprehensive induction and other research methods to classify cyber crime that aiming to property, and found that fraud cyber crime has become the mainstream crime during the epidemic, and the massive use of information technology is the key factor for the success of crime [5]. In an annual report released by Europol on October 5, 2020, it was mentioned that during the COVID-19 epidemic, the number of online fraud cases and child pornography cases in Europe surged, and the life cycle of the dark network market shortened. Many criminals have begun to use other decentralized market platforms to sell their illegal products.

2.2. Research on Internet black market in China

In China, where new types of crimes such as telecommunication network fraud are rampant, the study of Internet black market mainly focuses on the following points.

First, research on the formation and expansion of the Internet black market chain. Wang Xin, from a sociological point of view, believes that the reason for the expansion of the Internet black market group is that the current legislation lags behind and needs to be improved. The lack of laws in the field of Internet black market provides a rare hotbed for the breeding and rapid spread of the network transmission virus; The digital forensics is difficult, and the security technology precautions for anonymous network behaviors are not sound enough; It is difficult to convict, lack of deterrence, and the cost of criminals' crimes is getting lower and lower. Virus programs and hacker tools used to commit crimes can be easily purchased online. In addition, existing laws and regulations lack specific binding standards for these acts, resulting in the spread of Trojan viruses; It is difficult to define and needs to be strengthened. Relevant laws and regulations only clarify that it is illegal to develop and spread viruses, but there is no clear definition of hacker programs, trojans, etc. The judicial department lacks unified standards for the value of virtual assets in reality.

Ren Yanjun analyzed the formation mechanism of hacker industry chain from the perspective of economics, and believed that the core motivation of crime was huge economic interests [6]. Because there is a perfect capital chain behind the hacker industry chain, and each chain has unlimited profit space. For example, hackers put a Trojan horse virus used to steal user information on the website in advance, and ordinary end users are attacked by the virus when browsing the website, resulting in user information such as credit card information, game accounts, passwords, etc. being obtained by hackers.

The second hot spot is the research on the current situation of the Internet black market chain. Chen Mingqi divided the network Internet black market chain into four categories. The first category is the hacker training industrial chain. After the hacker training, the personnel who did not have relevant professional skills can also participate in the network criminal activities. The second category is the spam industry chain, which uses e-mail to spread network viruses, or adds malicious

information such as fraud, pornography, extortion, etc. to the e-mail content, affecting the health of Internet users' online environment. The third category is the malicious code industry chain. Hackers use professional and targeted Trojan horse viruses to make hacker tools, invade network equipment and build botnet, and bring losses to the virtual property and financial property of Internet users. The fourth category is the industrial chain of online phishing and network fraud, which is mainly to build fake electronic trading sites on the Internet, such as banking sites and e-commerce trading sites, to lure users to visit fake sites through malicious links, and to defraud users of account information, passwords and identity credentials. Criminal gangs often conduct fraud in combination with current social hot spots. After analyzing the profit model of China's Internet information security underground industrial chain, Zhuge Jianwei further refined the structure of the specific underground industrial chain and divided the underground industrial chain into real asset theft and virtual asset theft. Du Yong studied the main active Internet Internet black market chain at present, and found that the rapid development of the Internet fraud industrial chain and the gradual expansion of the scope of influence are the top priority in the fight against Internet black market.

The third hot spot is the research on the characteristics and trends of the Internet black market chain. The network Internet black market chain has the characteristics of low age of criminals, division of labor in group organizations, and profit-oriented motivation. The development of the network Internet black market generally shows a trend of scale. Xu Hong and Zhao Yue believe that the network Internet black market has obvious chain characteristics, and the upstream of the industry chain provides technology and hacker tools to build a platform; The midstream set up a customer service team and chat group to attract netizens to participate in gambling or swiping activities on the platform and collect personal information of citizens; Downstream uses the information provided by the upper level to put all their money illegally obtained in cash. Zhao Lili, Ma Ke and Ma Minhu discussed the problems exposed in the evolution of black ash production from the perspective of legal norms. The profit-seeking nature of the network black industry has promoted the upgrading of hacker technology, the updating of criminal models, and the expansion of the industry has impacted the existing governance rules and legal norms. In judicial practice, law enforcement agencies are faced with the problems of digital forensics and difficult to convict the evidence. The "crime of helping information network crime", "crime of infringing on civil personal information", "crime of destroying and invading computer systems" and other crimes are inadequately applied.

3 Concept Analysis, Characteristics and Classification of Black Market

3.1. Concept analysis

The "network related" in this concept refers to the criminal behavior closely related to the network, or the behavior of the perpetrator is related to the network crime. The Internet black market usually refer to the acts of using the network to carry out illegal crimes, such as telecommunications fraud, phishing websites, Trojan horse viruses, and blackmail, and so on. With the rapid development of the Internet, crimes using the Internet as a medium have frequently occurred, and the traditional Internet black market chain has evolved and upgraded under this trend, resulting in the Internet black market in the new type of crimes involving the Internet.

3.2. Characteristics analysis

The traditional Internet black market includes extortion, online game coin earning, online theft, spam, etc. These industries are characterized by high professionalism and high technology. The industrial chain forms are both independent and interdependent, forming a complete upstream, middle and downstream Internet black market chain. For example, criminals first take part in hacker training to learn relevant skills, then use technical means to infiltrate into the network server to steal secret data, and finally sell it on the black market by people downstream of the industrial chain.

The black-and-gray industry in the new network-related crime has included telecommunications fraud into the key research category in the black-and-gray industry field, making the research on black-and-gray industry further improved and supplemented, and adapting to the current trend of nationwide anti-fraud. In addition, the traditional Internet black market has also been updated with the improvement of the level of science and technology, the means of crime has been upgraded, and the operation structure has been iterated. The analysis and research of Internet black market in the new type of crimes related to the Internet also put the evolution mode, new changes and development trend of these traditional industries into the research focus, and provide effective governance countermeasures for the fight against Internet black market.

At present, there have been structural changes in criminal activities, traditional crimes have accelerated to breed and spread to the network, and new types of crimes related to the network have become the mainstream. The core resources that Internet black market practitioners compete for have shifted from network traffic to personal information, usually including citizens' personal information such as ID card, bank card, mobile phone card and U-shield. Now it has expanded to voice print, fingerprint, iris and other biological information. Criminals use AI technology to synthesize 3D "fake faces" and cheat the authentication of the network platform, thus carrying out illegal acts such as best-deal-hunting, fraud and false registration. In

the payment process, criminals targeted ordinary citizens' mobile payment accounts, built fraudulent "scoring platforms", and induced scoring members to submit collection QR codes such as Alipay and WeChat for money laundering. The number of aggregation payment platforms increased, and the payment interface of merchants was illegally misappropriated from time to time.

3.3. Classification of black market

According to the different professions involved, the Internet black market related to the Internet can be divided into three categories: technical, social engineering and porn-related. Technical Internet black market refers to the malicious activities such as network theft, network monitoring, illegal control and so on by using the security vulnerabilities of computers and networks to invade the system services of the victims by means of hacker technology. The technology related Internet black market is not only the highest technology content in the complex network related Internet black market, but also the basis of the network crime chain. By providing network technology, the practitioners in the technical Internet black market make the network crime continue to spread, with clear levels and three-dimensional diversity, covering development, sales, publicity and other links.

The common technical black ash production related to the network includes the following categories:

(1) Trojan horse virus industry chain

Trojan horse viruses are usually based on computer networks and are communication and monitoring programs between clients and servers. The Trojan horse virus steals information from the user's computer or mobile terminal, such as identity information, network account password, chat records, credit card information, virtual assets in the game, by hiding in the normal program of the server and obeying the remote control command of the hacker.

(2) Dark link industry chain

"Dark link" is a link that is invisible to the naked eye or easily ignored, but can only be seen in the source code. Hackers set up dark links in their important pages after stealing the management rights of high-weight websites, so that they can gain more display volume and attract more users' attention. Dark link websites are mostly online pornography and online gambling websites. Hackers convert the number of visitors to dark link websites into corresponding fees in proportion.

(3) Traffic hijacks industrial chain

The so-called "traffic hijacking" is simply to force network users to visit a preset site. The implementation methods are mostly to set up a pop-up window on the web page, malicious software to modify the browser home page and other hacker technologies, so that users' traffic is forced to flow to a specific web page. Practitioners provide hijacking technology to share part of the flow profits.

(4) Phishing industry chain

Phishing is one of the most common types of Internet black market crimes. The criminals make fake web pages, emails and short messages with fraudulent links or two-dimensional codes, which are forwarded in large numbers to make the victims "hooked", and cheat and steal their ID number numbers, online banking account passwords, etc. Compared with social engineering, the phishing industry chain is more technical.

(5) Online pornography industry chain

Online pornography trading is realized through online means, online or offline. Nowadays, online pornographic websites tend to make profits by advertising or traffic promotion. Every time the promotion link on the website is clicked, practitioners can get a certain return.

(6) DDoS industrial chain

Attackers use network technologies such as Dos (denial of service), DDoS (distributed denial-of-service attack) to block the target network or system, and the server cannot receive, process and respond to user requests in a timely manner, thus making the target lose the ability to provide normal services to legitimate users.

(7) Private game service industry chain

"Private server" refers to the unauthorized construction of an unofficially recognized network server after obtaining the server-side installation program without the authorization of the copyright owner to divert the profits of the original operator. It is a typical network piracy. The strong demand of the game market and the low threshold of pirated technology have led to the fate of many well-known games being infringed.

There are still many types of cyber crime in technology, and with the development of computer network technology and economic level, there will be other criminal means in the future.

4 Analysis of Typical Internet Black Market

In order to better analyze the characteristics and operating principles of the Internet black market chain, the information disclosure industrial chain, a typical Internet black market chain, is analyzed here.

Information leakage in Internet black market generally refers to the outflow of personal information through hackers' technical means, and internal personnel taking advantage of their position to steal. If the security vulnerability is to find the entrance to the treasure house, then the data is the real "treasure" in the treasure house, and of all the data, the personal information of citizens is undoubtedly the most valuable. The purpose of hackers to search for vulnerabilities has changed from the initial showing off their skills to the acquisition of valuable

data. After obtaining personal information, these data will be reprocessed and finally flow into the black market, which will be used by many downstream companies. Real estate agents and advertising salesmen will use citizens' personal information to push spam ads and make harassing calls, and the higher risk is that the data being used in telecommunication fraud and network fraud.

4.1. Current situation of information disclosure industry chain

According to the statistics of the China Academy of Information and Communications, 152000 reports from telecom users were accepted in 2020, of which 64000 reported online fraud, up 14% from the previous month; There were 85000 fraud phone calls, up 88.9% month-on-month. It can be seen that the proportion of citizens' personal information used for telephone and online fraud is increasing, and information disclosure has become the "booster" of criminals' "accurate" fraud. The information disclosure industry chain is a Internet black market chain with complete elements. The citizen information in the upstream of the industry chain is illegally stolen by illegal elements by various means, the data in the middle of the industry chain is packaged and sold on the black market trading platform, and the private data in the downstream of the industry chain is used to implement network fraud and network extortion, which seriously disturbs the network environment and endangers the security of individuals, enterprises and countries.

(1) Rampant personal information transactions

The disclosure of citizens' personal information has become common. The most common transaction information on the black market is citizens' mobile phone number, ID card information and residential address information. In the era of the Internet, while citizens' information is being continuously developed and used, it also needs effective supervision and management, especially in the enterprise departments that have a large amount of personal information of citizens. According to the 49th Statistical Report on the Development of Internet in China by the China Internet Network Information Center, 22.1% of Internet users had suffered personal information leakage by December 2021. In the case of Shunfeng employees selling customer information in 2018, the police caught a group of criminal gangs illegally obtaining and reselling express sheets. According to the police, these criminal gangs intended to enter the express company through recruitment in order to obtain the information and data of citizens. During the work process, they used the interval of sorting out express delivery to secretly take delivery order information, and then packaged and sent it to the buyer after work.

With higher technical means, cameras will be installed on the express scanner. A computer can remotely control the camera to take photos and text recognition, so that a large amount of citizen information is illegally exported. The price of a express sheet photo varies from 2 yuan to 10 yuan. As long as you take it for one hour continuously, you can easily obtain several hundred yuan of income. The total amount of the crime in this case reached more than 2 million yuan, and more than 20 social groups were found to have illegally trafficked personal information. Information disclosure in the express industry is only the tip of the iceberg in the information disclosure industry chain. Illegal information transactions are widespread in fields from online shopping to medical care and education, which is one of the reasons why "precision fraud" and "precision marketing" are so overbearing at present.

(2) The competition for information is becoming increasingly fierce

The improvement of the Internet level has led to the explosive growth of the amount of network information. The network content is extremely rich, and the network application has penetrated into various fields. The development of science and technology has brought profound changes to people's activities, but also made it easier for criminals to obtain sensitive information from citizens. The theft of information is distributed in the upstream of the Internet black market chain. Professional hackers use SQL injection, XSS (cross site script attack), CSRF (cross site domain request forgery attack), phishing and other attack methods to invade the background and download the information of the database on the websites by exploring the vulnerabilities of the website.

After obtaining a large amount of database data, hackers use data analysis technology to clean and analyze all data, and screen out data that are valuable for crime, especially the user's real identity information. After getting the packaged data, the marketing personnel at the downstream of the industry chain release the sales information on the Internet black market and gain profits through illegal transactions. After "cleaning the database", hackers can also use the user accounts and passwords they have obtained to log in to other websites on the network platform in batches. This process is called "database collision". After many times of "database stealing" and "database collision", the amount of sensitive information obtained by hackers is as large as "snowball", gradually forming a huge "social work database", which contains a large number of common account names and passwords, identity information, occupational status, online records and other data information, which are urgently needed by Internet black market.

4.2. Analysis of personal information disclosure and transaction process

Information leakage is the upstream link of the whole information leakage Internet black market chain, the midstream is the processing and sale of information, and the downstream is the implementation of criminal activities such as network theft and network fraud. So how is personal information leaked out? Through the data, we found that the main ways of citizens' personal

information disclosure are hacking, insider disclosure and reselling, and the platform's failure to store and use data as agreed. Figure 1 shows a typical personal information trading industry chain.

Hackers use skills to attack database servers and steal their internal information is the main source of data leakage. Hackers mainly have two ways: penetration attack and hacker social engineering attack. Infiltration attack aims at a large number of websites and servers with potential security risks on the Internet, and steals data from the background database through information collection, vulnerability scanning, and the use of vulnerabilities to improve permissions. Hacker social engineering takes advantage of human weakness and combines hacker technology such as viruses and trojans in interpersonal communication activities to induce the other party to fall into the set "trap", such as mall advertisements with malicious links, counterfeit third-party payment platforms, phishing emails, etc.

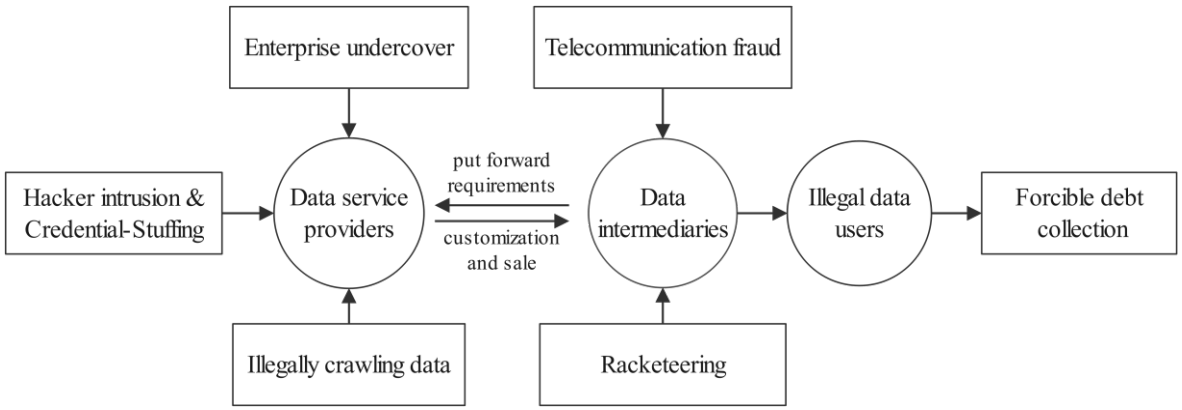

Fig. 1. Typical personal information trading industry chain

In the information age, data is increasing in value, and "insider" theft is also one of the main channels of personal information disclosure. This kind of method has almost no technical requirements. Usually, employees in the department collude with employees in the Internet black market driven by interests and other factors, and use their positions to facilitate the flow of user's personal information for resale. The Internet black market employees mainly select those who have certain authority in the department and have more resources as the "counter" targets, such as the middle-level leaders in the enterprise, the technicians responsible for the installation and maintenance of the computer information system, and the investigators responsible for collecting data. Through sorting out the uncovered cases of infringement of citizens' personal information, it is found that most of the suspect arrested are from the insiders of real estate development, sales and intermediaries.

In addition to the protection against hackers' technical attacks and "insider" data leakage, relevant departments should also strengthen the management of institutions that store massive amounts of citizens' data, and improve the laws and regulations on personal information protection as soon as possible. With the increase of third-party network platforms in the market, citizens' personal information is collected by various network platforms, but whether the platform stores and uses data as agreed is still a difficult point for the supervision of relevant departments. Many users have had the experience of filling in information online to apply for cash loans. Even if they fail, they will soon receive sales calls from other cash loan platforms or loan intermediaries. Whether it is commodity shopping, financial investment or application for counseling institutions, when users submit personal information required by the platform on the network, they will always receive mobile phone messages, sales calls and advertising push of relevant content from time to time. Some Internet platforms and big data companies have not only failed to perform their duties as stipulated in the Internet convention, but have even cooperated with the Internet mafia to purchase user data from illegal channels for their own use. These cyberspace chaos needs to be improved and regulated by relevant departments.

5 Conclusion

This paper reveals the current situation of the Internet Internet black market behind the rampant new types of cyber related crimes. Taking the typical Internet black market of personal information transaction as an example, this paper analyzes the characteristics of Internet black market, its operation process, upstream, middle and downstream roles and task division. At the same time, in view of how to effectively combat the Internet Internet black market, this paper believes that it is necessary to clarify the ecological chain, industrial chain, and interest chain of Internet black market. While taking platform governance as the starting point, it is also necessary to form linkage governance and effective co-governance, so as to protect citizens' privacy and property security and maintain social stability.

Acknowledgements

This work was supported by the National Social Science Foundation of China under Grant No. 21BSH051.

References

1. L.A. Temirzhanova, N.K. Imangaliec, B.Z. Sagymbekov, J. Advanced Res. L. & Econ **10**, 21(2019)
2. M.A. Azad, M. Alazab, F. Riaz, Fut. Gen. Computer. Sys, **105** (2020)
3. M. Alazab, M. Alazab, A. Shalaginov A, Fut. Gen. Computer. Sys, **107** (2020)
4. E.W. Ford, J. Healthcare. Mangement, **66**, 4(2021)
5. K. Choi, J. Contemporary Criminal Justice, **37**, 3(2021)
6. Y.J. Reng, Crime Investigation, **1**(2018)