The Current Situation of Internet Underground Industry Chain and Its Governance Model

Dade Tang, Guangxuan Chen*, Qiang Liu

Zhejiang Police College, Hangzhou, China

tangdade2022@163.com, chenguangxuan@zjjcxy.cn, liuqiang@zjjcxy.cn

Abstract. In the present internet era, the cyber crime has become the mainstream crime among the whole crime, which bringing huge losses to society and has become the focus of the social attention. The huge internet underground industry chain provides the crime method and crime tools for the criminals that seriously damaged our country's network ecological environment. With the continuous development of Internet technology, the internet underground industry is also constantly presenting new criminal characteristics. First of all, this paper introduces the background situation of the current cyber crime, internet underground industry, and analyzes the classification, form, industry chain and future development trend of the internet underground industry chain. Then it probes into the root causes of internet illegal production, and finally puts forward the strategies of strengthening the control of network resources to raise the cost of crime, improving the legal mechanism of network crime and constructing joint prevention and control system in order to purify the network environment and compress the living space of internet illegal production, so as to improve the governance ability of cyber space in our country.

Keywords: Internet underground industry chain; Cyber crime; Prevention and control system;

1 Introduction

In the current Internet era, people are enjoying the huge dividends brought by high digitalization, at the same time, netizens and enterprises are also encountering a variety of network security threats and personal information leaks. According to the "State of Security 2022", 49% of the more than 1200 security industry leaders said their businesses had suffered data breaches in the past two years, 79% said they had been attacked by ransomware, and 35% admitted that one or more attacks had prevented them from accessing data and systems. 59% of security teams said they had to devote significant time and resources to remediation [1]. Behind this large number of cyber crimes is an invisible network underground industry chain.

A. Holl et al. (Eds.): ICHESS 2022, ASSEHR 720, pp. 1008–1017, 2022.
https://doi.org/10.2991/978-2-494069-89-3_117

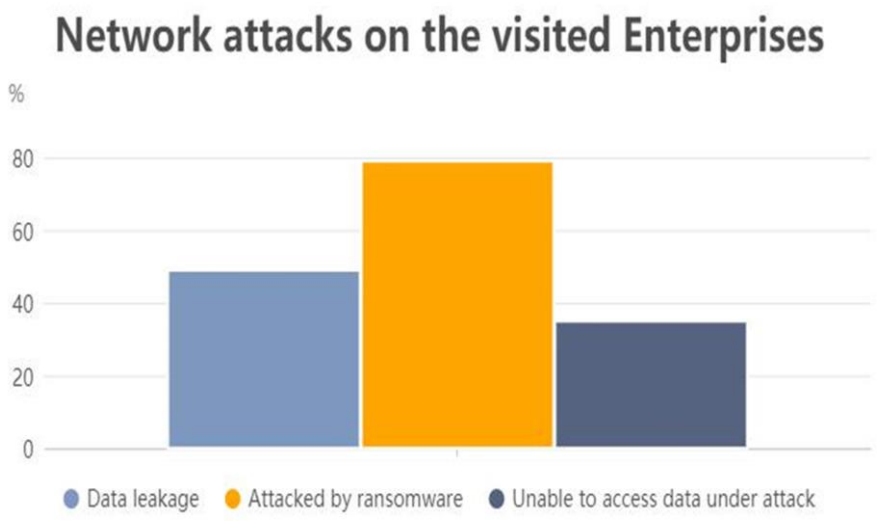

Fig. 1. Network attacks on the visited Enterprises

With the continuous development of the Internet, the internet underground industry is also constantly updated and iterated, forming a highly modular and market-oriented industry chain, in which the upstream, midstream and downstream of the industry chain have a clear division of labor and strict coordination, making cybercrime highly automated, thus forming a set of formulaic profit methods. It has seriously damaged the network ecological environment of our country and it has become a huge obstacle to the development of China's Internet industry. At present, China is faced with the severe situation, we need to strengthen the supervision of the Internet field and purify the internet market environment. Therefore, it is imperative to increase investment in the management of network underground production and crack down on cybercrime.

2 The current situation of the internet underground industry chain

2.1 Industry status of network underground production

Nowadays, the internet underground industry chain has developed into a huge interest chain with an annual output value of 100 billion yuan and more than 1.5 million employees [2]. It includes the grey industry which is not defined by law and the black industry which has violated the law. Because of the concealment, decentralization and cross-regional nature of the network, as well as the lack of relevant interpretation in the law, it is more difficult to deal with the problem of network underground production. The biggest characteristic of network underground production lies in its profit-driven

nature, and the shadow of network underground production can often be seen in places with high profits.

2.2 Classification of network internet underground industries

"Internet underground industry" can be defined as a social division of labor organization form that takes virtual cyberspace as the place, relies on neutral technology, seeks illegitimate interests as the motive, takes non-criminal technology or behavior as the appearance, and takes the implementation of illegal and criminal acts as the essence [3].

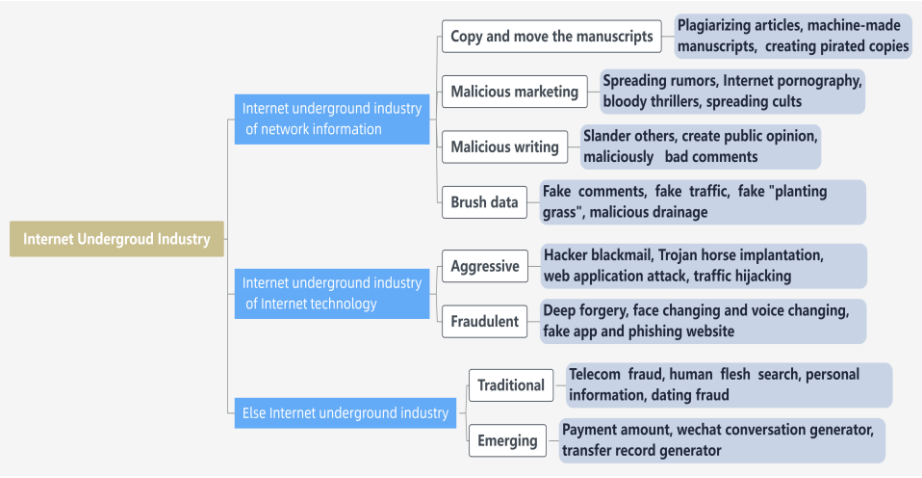

Fig. 2. Classification **o**f Internet underground Industry

According to the nature and content of internet underground industry, it can be divided into network information internet underground industry, Internet technology internet underground production and other types of internet underground production (Fig.2).

Internet underground industry of network information.

Network information internet underground industry includes copying manuscripts, malicious marketing, malicious writing, cheating promotion and so on. Copying manuscripts refers to the use of technical means to replace Synonyms, replace Synonyms, delete, and other ways to piece together the original article, and then apply it to the media account. Its cost is much lower than creating an original article. Malicious marketing refers to guiding public sentiment to gain public attention and gain benefits at a specific time. Brush flow refers to the illegal operation of machines and software to manipulate a large number of zombie users to brush data. This kind of internet underground industry is usually in the downstream of the industrial chain, involving a wide range of industries, causing great harm, and can make huge profits directly, which has a serious impact on the network environment.

Internet underground industry of Internet technology.

The internet underground products of Internet technology are divided into attack type and fraud type, including hacker blackmail, Trojan horse implantation, deep forgery, face-changing and voice-changing, etc. These internet underground products are highly technical, usually in the upper and middle reaches of the industrial chain, with stealing data as the core to make profits. Common technologies include hacker database collision technology, which collects leaked user information to log on to other websites in batches, and app to steal login user information; web crawler technology illegally collects a large number of users' personal sensitive information. Implant Trojan horse virus to control mobile phones Web sites to obtain personal information.

2.3 Industrial chain form of network internet underground industry

The network internet underground industry chain can be roughly divided into upstream, midstream and downstream. The upstream link is mainly responsible for software development and technical support, providing tools and means for cybercrime, including code receiving platform, code printing platform, black production software, various software account information, etc.; The midstream maintenance account is used to simulate the normal user behavior to avoid the regulatory measures of the platform, or manually add friends and other methods to identify target groups for downstream crimes [4], and improve account activity and value;, including collecting various accounts, card issuing platforms, etc., and selling the collected account resources to downstream enterprises. Downstream is to obtain huge illegal profits by realizing the resources obtained in the upper and middle reaches through certain methods, such as fraud, drainage, and so on. At present, in the network internet underground industry market, there have been a number of network black industry teams with professional quality and excellent technology, who use the network to carry out illegal activities and make huge profits, which poses a great threat to national network security.

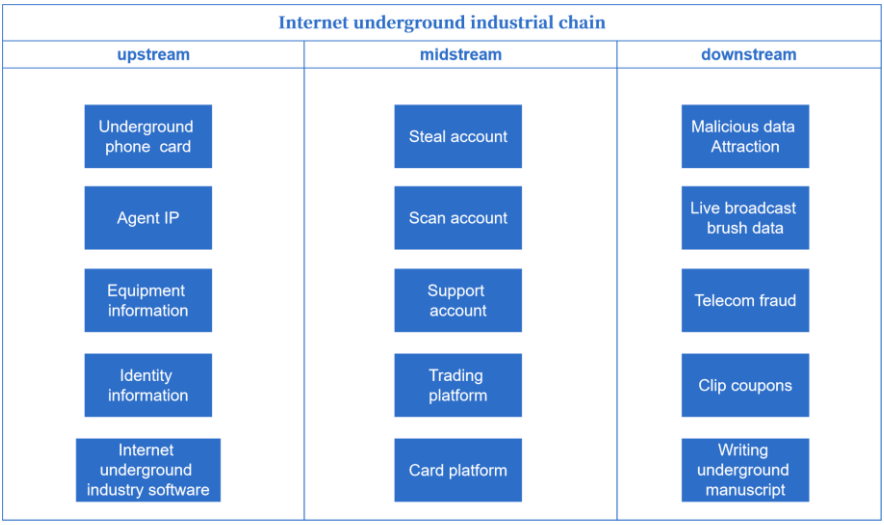

Fig. 3. Internet underground industrial chain

2.4 Development trend of network internet underground industry

(1) From machine cheating to real person cheating

In the past, internet underground products mostly used automated machines to forge real user behavior, however, due to the intensification of supervision, this way of committing crimes has greater risks, so they often changed to crowdsourcing and outsourcing. By giving users a part of the commission to attract ordinary users to participate and the ordinary users are using normal equipment, IP address, and so on. As the real person cheating is more difficult to identify, it makes the rectification work more difficult.

(2) Mobile phone black cards are transferred from domestic cards to foreign cards

Common mobile phone black cards mainly include virtual cards of virtual operators, IOT network cards, overseas cards and mobile phone cards registered by others [5]. As the law enforcement vigorously carries out the action of cutting off cards and severely cracks down on illegal trading of telephone cards, the number of telephone cards in China has declined and the cost has risen sharply. Therefore, illegal elements will introduce a large number of telephone cards from other countries to supplement the gap of domestic cards and reduce costs.

(3) The crime is more efficient and the form is more complex

In recent years, with the continuous development of artificial intelligence, bigdata, cloud computing and other new technologies, criminals can also use these technologies to make their criminal traces more concealed. For example, they can analyze the people

who are more easily deceived by means of bigdata, carry out more accurate fraud, reduce the number of times and improve the quality. Code printing platform and card issuing platform are built on cloud servers domestic and abroad, which greatly reduces the cost of crime, and provides automated API interfaces to achieve automation and improve the efficiency of crime. At the same time, the means of crime are constantly innovating and more diversified.

3 Analysis of the root causes of network internet underground industry

3.1 High profits and large demand.

In the era of traffic, data represents profits. The number of short video users in China has reached 934 million, and data such as traffic, clicks, likes and purchases are the basis for enterprises and individuals to make decisions. Under such underlying business logic, the internet underground industry of the network will naturally develop rapidly. According to the data, the unit price of high-quality SMS and SDK data traded in the current market can reach 0.6-1.5 yuan during its validity period. External hacker attacks penetrate the enterprise background, and the highest unit price of data obtained from the database can reach 15 yuan. Under the temptation of such huge profits, it naturally attracts a large number of teams and individuals to make profits.

3.2 Difficulties in the application of law

There are still big loopholes in the laws and regulations and the national regulatory system. For example, for the control of false traffic, there is no unified identification standard for false traffic, and there is no unified statement for the identification standard of false traffic [6]. It is difficult to collect and trace the relevant evidence. There are also big problems in the supervision and punishment of cyber violence. There is no clear legal definition for the subject of responsibility for cyber violence, and there is no clear boundary for the attribute and value of virtual property. On this basis, how to regulate this kind of behavior by improving laws and regulations has become one of the focuses of social concern.

3.3 Netizens' awareness of network security is weak

China has a large number of Internet users, and the overall awareness of Internet security is relatively weak. When conducting network activities, many netizens do not know whether to fill in personal information, what kind of security protection software should be used, which app is regular, and whether to give app permission [7]. Data show that 82.6% of Internet users have not received network security education, but have obtained this knowledge sporadically from various channels; 13.8% of Internet users use the same password for all accounts; 33.5% of netizens will install app directly and ignore the permissions they require. From this point of view, there are still a large number of

Internet users who lack knowledge and awareness of network security, and criminals will use the negligence to obtain a large amount of personal information.

3.4 Difficulties to effectively combat cybercrime

Cyber crime, especially the highly technical cyber crime, has a high degree of specialization, strong concealment and difficulty in obtaining evidence. Because the network has the characteristics of openness, uncertainty and transcending time and space, cybercrime has a very high degree of concealment, which increases the difficulty of detecting cybercrime cases [8]. However, the public security organs around the country are weak in the investigation of cybercrime and lack of professionals, which makes it difficult to improve the detection rate of cyber crime.

4 Strategies and Methods for Controlling Internet underground industry

4.1 Guiding enterprises to establish reasonable wind control strategies and deal with cybercrime reasonably

First of all, enterprises must understand the internet underground industry, understand the internet underground industry will be harmful to their own business, which business still has security risks, many enterprises do not pay enough attention to black ash production, unwilling to spend financial and human resources to prevent black ash production, resulting in greater losses. Enterprises can cultivate employees' risk awareness and enhance their risk awareness by carrying out relevant training.

Secondly, enterprises need to establish correct corporate values, attach importance to internet underground products, establish matching business security mechanisms in the process of business development, and have reasonable countermeasures and coping strategies after being invaded.

4.2 Strengthen the control of network internet underground industry demand resources and increase the cost of crime.

Owning to the biggest characteristic of network internet underground industry lies in its profit-driven nature, it is an effective way to reduce profits and increase the cost of crime. Strengthen the control of all kinds of resources needed by the whole industrial chain.

First, in view of the upstream and middle reaches, we should strengthen the management of mobile phone cards, severely crack down on illegal and prohibited items such as mobile phone black cards and cat pools, and increase penalties. Further strengthen the management obligations of application providers for false registration of accounts.

Secondly, for the downstream, we should strengthen traffic monitoring, standardize applications, forbit false propaganda and bundle downloads. And further establish the

identification mechanism of application providers for users to brush various bills, clarify the management obligations of application providers, improve the technical interception mechanism for internet underground industry's personnel to use group control software and malicious plug-in software to automatically follow, like and comment, and improve the freezing mechanism of illegal accounts.

4.3 improve the relevant legal mechanism and promote the sharing of intelligence resources.

Law is the basis and guarantee to govern the internet underground industrial chain of the network. Promote the establishment of fixed industry standards for self-media, formulate or improve Internet industry standards and self-discipline conventions [9], encourage the media to disseminate positive energy, and further standardize the registration and authentication of self-media users, content requirements, codes of conduct and punishment rules, so as to promote the healthy development of self-media. Strengthen government supervision, promptly stop and correct violations of laws and regulations, and intensify law enforcement efforts. Maintain a level playing field and market order in accordance with the law. Because of the cross-platform characteristics of network internet underground industry, it is necessary to further establish a multi-linkage supervision and cooperation mechanism, break the information obstacles of "network internet underground industry" among application platforms, co-govern network internet underground industry, and share a clear network environment.

4.4 Construct joint prevention and control system to counter technology with technology.

Firstly, we should establish an effective prevention and control system, which is led by the competent authorities to build a prevention and control system for major industries and enterprises, and monitor mobile phone numbers, IP addresses, bank cards, market prices of internet underground products and other important information, so as to improve the overall efficiency of prevention and control, strengthen cooperation between police and enterprises, and encourage operators to actively provide clues to public security organs. Create an "internet underground industry" governance ecosystem.

Secondly, we should fully mobilize the masses, give full play to the power of social supervision, encourage the broad masses of the people to participate in reporting. At the present stage, the effect of mass prevention and treatment is not obvious in the whole country. The public think that the government and public security organs are the main bodies of the prevention and control of cybercrime, and only a small part of the social forces actively participate in the prevention and control of cybercrime [10]. Therefore, we should fully mobilize the enthusiasm of netizens, and improve the complaint mechanism of internet underground products and the reporting mechanism of users. Enterprises also need to establish a normal review mechanism, timely discovery, timely processing, and actively cooperate with the work of relevant departments. Give timely feedback on the results and take the initiative to accept the supervision of the masses.

On this basis, a long-term mechanism should be formed to ensure the balance of interests between enterprises and consumers.

Thirdly, we should constantly develop technology and use new technology to counter the old routine. Network internet underground industry usually takes a fixed routine to make profits, combing out the defects of its fixed model and constantly innovating new measures can effectively counter the network internet underground industry. Innovative technological means to combat network internet underground industry is a sustainable management method, which can summarize and promote the experience of technology with remarkable effect.

Fourthly, we should strengthen the guidance of public opinion and create a good social atmosphere. Giving full play to the role of public opinion supervision of the news media, let more people know the harm of network internet underground industry and how to prevent and deal with network internet underground industry through various channels, and enhance the whole society's understanding of network internet underground industry behavior, so as to better provide strong support for curbing the development of Network Internet underground industry.

5 Conclusion

A large part of the reason why cybercrime is so rampant is that the network behind it is complete internet underground industry chain, can provide hacker extortion, network crawler and other criminal technology and network accounts, identity data and other criminal raw materials. Therefore, the fight against cybercrime must start from the internet underground industry chain. In the vast internet underground market, we should find precise entry points, attack the key nodes of the internet underground industry chain, especially its root causes, and strengthen cooperation and coordination with banks, operators, public security and other relevant departments, so as to achieve rapid, accurate and efficient governance of cyber internet underground industry, combat cybercrime and create a clean and clean cyber environment.

Acknowledgment

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

References

1. Sqlunk. State of Security 2022[EB/OL]. (2022-4-13) [2022-8-10]. https://www.splunk.com/zh_cn/newsroom/press-releases/2022/state-of-security-2022-report-reveals-increase-in-cyberattacks-while-security-talent-remains-scarce.html
2. Huangqinhong. Suggestions for operators to do a good job in digital intelligence prevention and control of "black ash production"[J]. Communication world, 2022(5):3.

3. Liuxiangquan. The criminal law regulation of the upstream crime of network black ash production[J]. Journal of the state prosecutor's College, 2021(1):15.
4. Yuhaisong. The pattern and regulation of the black gray industrial chain of cyber crime [J]. Journal of the state prosecutor's College, 2021(1):14.
5. Weichunliang, Guocong, Lixiaozhuang, et al. Research on account number regulation under the background of network black and grey production[J]. Information network security, 2021(S01):4.
6. Xinhuawang. To provide legal guarantee for cracking down on cyber black industry [EB/OL]. (2020-12-22) [2022-8-12]. http://www.xinhuanet.com/legal/2020-12/22/c_1126889443.htm
7. Shenlong, Quyuanming, Hushumeng. Analysis and Countermeasures of black gray industry chain of telecom network fraud[J]. Chinese Criminal Police, 2021(4):5.
8. Qinyan, Linyifei. Research on the economic crime by using illegal software[J]. 2021.
9. Zhangyuan. Research on the control of black ash production of network information content[J]. Network communication, 2021(12):86-89.
10. Liuxiaoyue, Censhijie, Hutiehan. Cyber crime in the era of digital Policing: current situation, trend and Governance[J]. Network security technology and Application, 2022(4):3.