Characteristic Analysis and Investigation Strategy of Computer Network Crime

Liangyan Tang
Sichuan Judicial and Police Officers Professional College DeYang, Sichuan, China 618000
2014326215@dlvtc.edu.cn

Abstract—This article analyzes the basic characteristics of computer network crime, including diversity, concealment, severity. The research content of this article combines the key points of application of electronic forensics technology, network investigation technology, and network tracking investigation technology. The author studied how to determine the investigative strategy, implement temptation investigation, and do a good job of monitoring and tracking coping strategies. The purpose of this article is to speed up the investigation of computer network crimes and improve the efficiency of solving cases.

1. INTRODUCTION
Computer network technology has made a huge and non-negligible contribution to improving China's comprehensive national strength and liberating and developing China's productivity. The tremendous benefits brought by computer network technology also brought a new form of crime that cannot be ignored, namely cyber crime. Computer cybercrime refers to the use of Internet technology, the use of programming, software instructions, encryption and decoding and other means to illegally invade the computer system of others, steal information or spread destructive codes, and then commit crimes such as theft, fraud, embezzlement, or theft of state secrets and commercial secrets and other behaviors. When we face cybercrime, we should first realize that this is an unavoidable problem brought about by the development of technology. At the same time, we should also realize that with the further expansion and integration of the Internet, cybercrime problems will become increasingly frequent and complex. In the face of the continuous spread of cybercrime, how to prevent and solve cybercrime problems has become a hot issue of general concern at home and abroad.

2. ANALYSIS OF CHARACTERISTICS OF COMPUTER NETWORK CRIME

2.1. The Diversity of Criminal Subjects
In the 1980s, computer network crimes began to appear in our country. At this time, most of the criminal subjects were highly intelligent individuals with certain computer resources. However, with the widespread use of computer equipment in China and the popularization of computer technology education, computer cybercrime is no longer the patent of highly intelligent people. In particular, the emergence of a variety of easy-to-operate Trojan horse programs, and their simplicity and ease of operation have created the diversity of computer cyber criminals. Among the criminal subjects, a group of people develops particularly rapidly, that is, minors, that is, young people. According to relevant survey reports, there are currently 230 million young Internet users in China, accounting for 25% of the total number of Internet users in China. Minors are often keen to master computer technology. However,
they do not have the ability to distinguish false information on the Internet. They are immature and are extremely vulnerable to bad temptations. They often commit crimes without knowing it is a crime.

2.2 Concealment of Crime
Compared with traditional crimes, computer network crimes often have strong concealment. Computer crimes that occur in a virtual state do not require a fixed crime location. Criminals can invade computer systems without the victim's awareness, intercept, tamper with, or delete computer stored data or information. The duration of the crime is generally relatively short. Moreover, some criminals have a high level of anti-investigation awareness, and they can erase traces of crime in a very short period of time, including virtual identities and forged IP addresses. Once the common Trojan horse virus enters the computer system, it can quickly destroy the system. In a short time, it will cause the system to be paralyzed, and the information and data in it will be stolen or lost. If the computer returns to normal after anti-virus, it is difficult for ordinary people to discover the fact that the data has been stolen, which leads to the concealment of crimes.

2.3 The Severity of the Consequences of the Crime
Except to the characteristics mentioned above, the types of computer network crimes are also diverse. Moreover, the motives of cybercrime are also diverse, the crime spreads to a wide range, and the severity of the consequences is more prominent. Judging from the current development situation, online payment methods are becoming popular, and more and more netizens tend to store their assets in virtual banks. If the perpetrator masters the relevant network technology to steal the passwords of netizens, it will directly cause huge economic losses to the users. For example, some hackers will gain more illegal benefits by attacking financial institutions and securities systems. Just as the information leakage caused by the Melissa virus at that time directly caused hundreds of millions of dollars in losses to some giant companies.

3. Analysis of Computer Network Crime Investigation Technology

3.1 Electronic Forensics Technology

3.1.1 Search and Seizure
Search and seizure are methods of investigation that are often used. In the specific application process, in order to collect the electronic evidence of cybercriminals, the investigative agency can search the computer system of the criminal suspect. In this way, the storage area of the original record of the data in the computer can be found. According to the requirements of relevant laws and regulations, investigative agencies can directly seize these electronic materials, and at the same time, based on existing resource information, they can conduct investigations on other potential sites and directly extract and seize their related application data. In the course of this activity, we can use computer engineers and program operators to complete these complex operations. In this way, scientific methods can be used to complete the search and processing of corresponding target electronic information. Meanwhile, recording electromagnetics as electronic information that can be read smoothly can increase the use value of analytical content.

3.1.2 Withhold Electronic Information
Computer network crimes are random and time-consuming, so we need to do a good job in the interception of electronic information while seizing the contents of the discovered materials. Judging from the current application situation, this method has a good ability to intercept some new types of computer network crimes. At this stage, computer networks have been widely used in many countries. Currently, the relevant laws drawn up by China affirm the value of the interception of electronic information. Moreover, the computer system can also use this method to assist the corresponding work when allowing investigative agencies to track cybercrime cases. However, the interception of electronic
information can invade the privacy of some people. Therefore, we need to go through a very strict approval process before using this method. Judging from the current practice, we need to do the following two things when intercepting electronic information. Firstly, the investigative agency can intercept information with the consent of the sender or recipient of the information. Secondly, the investigative agency can intercept the information without the consent of the sender or recipient, and select appropriate processing methods based on specific circumstances, thereby improving the reliability of the processing results.

3.1.3 Unit Provides Electronic Information
Judging from the current big data analysis, more than 70% of cyber crimes are launched against units. Hence, when we are investigating computer crimes, relevant units also need to actively cooperate to provide investigative agencies with reliable electronic information such as basic information, transaction records, and data. This will help investigative agencies to complete the collection of cybercrime data, and use this to complete the content of the case one by one. Moreover, this content is clearly stipulated in the "Criminal Procedure Law" promulgated by China. It requires units or individuals to actively cooperate with investigative agencies to speed up the detection of some criminal cases and maintain the security of the network environment. In addition, relevant units also need to keep some original records in their daily work, so as to lay the foundation for the smooth progress of various tasks.

3.2 Network Investigation Technology

3.2.1 Web Server Program Technology
In the network investigation technology, some network server applications will be used to assist the investigation work. Take the Ping Pro program as an example. In a network environment, the program can timely determine the opening ports in the network where Microsoft is located. Moreover, the program can also quickly identify the service protocol and service port in the remote running state during the application process. For example, UDP137 is often chosen to assist the smooth operation of the system during the operation of the Microsoft network. The other network scanning tools used in the use process will also dynamically monitor the UNIX application network, so as to achieve the expected investigation purpose. Ping Pro program can only be used in some specific networks in actual applications. For networks with high complexity, other tools are also needed to complete the processing, so as to obtain reliable application data to meet specific application requirements.

3.2.2 Stack Fingerprint Technology
Stack fingerprint technology is a commonly used application technology. In the actual application process, the technology will use the TCP/IP protocol to complete the processing work of the application service of the operating system. In most cases, the system administrator will also block and mark the leaked data. In this way, we can use the stack fingerprint to complete the necessary content identification processing. This is also very necessary for the application processing of the system. From the perspective of actual application, there are some differences in the TCP/IP protocol used by different units or individuals, and these basic conditions cannot be changed. Based on this situation, the system can record the differences during protocol application. Simultaneously, we can use the system to build a stack fingerprint table and comprehensively process the fingerprint content. This helps to improve the reliability and effectiveness of the data processing results.

3.2.3 NMAP Network Detection Software
Among the types of reconnaissance technologies, NMAP has strong application functions, and its reserved interfaces can be continuously upgraded and improved. The common options in the application of this network are shown in Figure 1, which has high efficiency of detection. In practical applications, the technology has a flexible TCP/IP stack fingerprint engine. During use, it can
continuously optimize and upgrade the system according to the specific requirements of the producer. In this way, the obtained engine system can obtain more required application content, thereby satisfying the basic requirements of system application development. Besides, in the process of technology application, fragment scanning technology will be used to complete the hidden FIN packets in the network. It can split the package into several fragments by means of segmentation, so that it can smoothly bypass the firewall structure to meet specific application requirements.

| Options | Explanation                  |
|---------|------------------------------|
| -T      | Timing Options               |
| -p      | Port Scan Sequence           |
| -sS     | TCP SYN Scan                 |
| -sT     | TCP Connection Scanning      |
| -sU     | UDP Scan                     |
| -sN, -sF, -sX | Covert Scan          |
| -sA     | TCP ACK Scan                 |
| -sW     | TCP Window Scan              |
| -sM     | TCP Mainmon Scan             |
| -scanflags | Custom TCP Scan          |
| -sI     | Idle Scan                    |
| -sO     | IP Protocol Scanning         |
| -b      | FTP Bounce Scan              |

Figure 1. Common Options for NMAP Networks

3.2.4. Shared Scanning Software
Except to the application technologies mentioned above, sharing scanning software is also a more commonly used investigation method. This technology can optimize the scanning of the application content in the network during the application process, and thereby ensure the sharing of the system application process. In the specific application process of scanning technology, it can share and process related data in the Windows network. However, this technology does not perform intrusion sharing processing on the collected data information, thereby ensuring the reliability of the processing results. For example, Microsoft Network will use TCP139 port to complete the construction of the sharing system in the application process. It will use some advanced detection software such as Red Button to complete the analysis of the corresponding data information. It can use this to complete the comprehensive application of data information and improve the use value of the software itself.

3.3. Network Tracking and Investigation Technology

3.3.1. Packet Sniffing
In the application process of this technology, its main application principle is to use packet sniffer to collect some specific data information. Subsequently, it will pass such data to the system for further application processing. However, the system cannot independently complete the investigation and processing of data information. In most cases, it will be used in combination with other assistive technologies. Moreover, in the analysis process, the technology also requires direct cooperation with operators. Otherwise, during use, the technology not only needs to ensure the reliability of the interface conditions of the communication data itself, but also needs to refer to the corresponding processing technology to meet the application processing requirements of the technology. In this way, some
potentially risky data packets can be intercepted. Its recognition rate is above 89%. This is also the technical content that will be used in many fields [1].

3.3.2. Wireless LAN Monitoring
In the application process of this technology, its main application principle lies in the monitoring technology. It can intercept some data packets during the communication period without affecting the communication between the monitoring target and other personnel. Subsequently, it can pass such data to the system for further application processing as evidence of illegality by the criminal suspect. In the specific use process, the application field of this technology is quite extensive. Users can use Wi-Fi as a monitoring channel to meet technical application requirements. Judging from the current development situation, in actual application processing, Wi-Fi used in many areas is relatively open and has not been encrypted. At this point, there will be an application gap in the system. In this case, there is a more than 90% probability that the information intrusion can be completed to meet specific usage requirements [2].

3.3.3. Email Monitoring
In the application process of this technology, its main application principle is the investigation activities carried out with the electronic agreement as the starting point on the basis of not affecting the monitoring target and other personnel to complete the normal e-mail communication. In a specific application process, the content it can intercept includes data packets, mail data, etc. It can then process such data in the system. In this way, comprehensive processing of information and data is realized. In practical applications, this technology is similar to a monitor of the running status of an email portal, and it can collect the required data correspondingly. Judging from the current development situation, many organizations still use mail for processing. The staff can also make suspicious access to the server when using network investigation technology to deal with it. In this way, the staff can directly complete the processing of dangerous data in the process of mail screening, so as to complete the smooth filtering of various dangerous mails [3].

3.3.4. Social Network Monitoring
In addition to the above-mentioned application technologies, social network surveillance technologies are also important investigative technologies. In the application process of this technology, its main application principle is to use monitoring technology to sort out the social network content on the network without affecting the normal communication of network information. Moreover, in the analysis process, it can choose to use the trajectory of the criminal suspect in the network as the investigation basis, sort out the application traces in the network, and find valuable network information from it. In practical applications, this technology is similar to a monitor of network operation status, and it can collect the required data correspondingly. Subsequently, it can complete the comprehensive processing of the data as required. Moreover, the technology can use software to smoothly complete the dangerous data or sorting work in the application process. This is conducive to the accumulation of reliable data and information, laying the foundation for the lock-in of criminal suspects [4].

4. Investigation Strategy of Computer Network Crime

4.1. Determine Detection Strategy
Determining the investigative strategy is conducive to the orderly conduct of investigations and speeds up the detection of cases. In the specific application process, relevant staff need to analyze the nature of the case and choose different investigative strategies based on the results of the nature analysis. This helps to improve the practical value of the data analysis results. For example, in the case of the misappropriation of network information, the original information system can be simulated based on the relevant information obtained and used as a bait to attract criminals into the trap. If the criminal wants to steal information again at this time, the relevant staff can use this method to complete the
information deception and introduce it into the simulation system, thereby speeding up the locking speed of the suspect [5].

4.2. Conduct Temptation Investigations when Necessary
The concealment of computer network crimes is often easy for criminals to get lucky after committing criminal acts. They tend to commit crimes again after hiding for a period of time and waiting for the calm. As a result, when formulating investigative strategies, relevant staff can often take advantage of the frequent and repetitive nature of computer network crimes to wait for criminals to commit crimes again by simulating or restoring crime scenes. The first task in temptation investigation is to copy the original crime scene and keep it highly consistent with the original scene. In this way, in the case that the criminal cannot detect that the scene is a trap, he can smoothly enter the trapping circle under the gradual induction, thereby speeding up the arrest of the criminal. It should be noted that during the scene construction process, relevant staff need to protect important data. At the same time, this also requires relevant staff to maintain sufficient patience, so as not to alarm criminals and increase the difficulty of investigation [6].

4.3. Do A Good Job of Monitoring and Tracking
Good monitoring and tracking can track the trace of the suspect. Combined with the actual surveillance technology, more sufficient criminal evidence can be accumulated. In the specific analysis process, relevant staff can initially locate the criminal suspect based on the attack software used by the criminal suspect, the specific attack time, the attack location, and the attack frequency. Subsequently, the relevant staff can monitor and track it to determine the specific information of the criminal suspect, and when the time is ripe, they can be directly arrested [7].

5. CONCLUSION
In summary, determining the investigation strategy is conducive to the orderly conduct of investigation work. Implementing temptation investigation when necessary can improve the efficiency of solving cases. Good monitoring and tracking can track the trace of the suspect. Reasonable application of computer network crime investigation technology can not only optimize the network operating environment, but also play a positive role in effectively combating network crimes. Criminals can use high technology to commit computer cyber crimes. Investigators can also use the technology brought about by high-tech to carry out criminal investigations, formulate thorough investigation measures and strategies to achieve the purpose of combating and punishing crimes, and create a safe, harmonious and stable network environment.

REFERENCES
[1] Bao Xue. Computer cybercrime investigation technology and countermeasures[J]. Computer Knowledge and Technology, 2017, 13(09): 50-51+53.
[2] Yu Li. Computer network crime investigation technology and countermeasures[J]. Communication World, 2016(19):3-4.
[3] Wu Yue. Computer network crime investigation and legal supervision [D]. East China University of Political Science and Law, 2016.
[4] Zhao Zhiwei, Li Cuicui. Overview of foreign computer network crime investigation techniques [J]. China Security, 2016(03): 95-103.
[5] Chen Yongsheng. The Challenges of Computer Network Crimes to Criminal Procedures and System Responses[J]. Science of Law (Journal of Northwest University of Political Science and Law), 2016, 32(03): 140-153.
[6] Zhang Yuexian. Research on IP location tracking technology for cybercrime investigation[J]. Information Network Security, 2016(06):72-74.
[7] Yin Qixin, Jia Xueming, Chen Yu. Research on Computer Network Crime Investigation Technology and Strategy[J]. Computer Security, 2016(04): 50-53.