Journal of Politics and Law; Vol. 17, No. 2; 2024
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Research on Identification Standard and Judicial Determination of Destructive Procedure - Based on Technical Specifications and Legal Provisions

Chaojie Ma[1] & Xiaoyu Yu[2]

[1] Law, College of Humanities and Law, South China Agricultural University, Guangzhou, China,

[2] Art and Design, School of Art and Design, Shenzhen University, Shenzhen, China

Correspondence: Chaojie Ma, Law, College of Humanities and Law, South China Agricultural University, Guangzhou 510642, China. E-mail: 1793094137@qq.com

Received: February 18, 2024 Accepted: March 30, 2024 Online Published: April 2, 2024

doi:10.5539/jpl.v17n2p36 URL: https://doi.org/10.5539/jpl.v17n2p36

Abstract

With the rapid development of Internet technology, the identification of destructive procedures has a dilemma that the legislative purpose is inconsistent with the practice at the judicial level. The traditional identification is generally based on technical specifications, but the legal positioning of the procedure is often ignored in computer network crimes. In order to establish the identification standard of destructive procedures as soon as possible and reduce the judicial problems caused by the identification of procedures, this paper, based on the computer network crime, through the combination of technical specifications and legal provisions, through in-depth analysis of the computer technical parameters and typical cases of crimes of destructive procedures, expounds the technical level to follow the destructive procedure inspection operation specification, at the legal level to subjective malice and serious harm two aspects of the judgment method. The results of the study revealed that the double identification of destructive procedures through technical specifications and legal provisions is not only more practical than ever, but also saves judicial resources and improves litigation efficiency.

Keywords: destructive programs, ideal of perfection, technical specification, subjective malice, severe harm

1. Introduction

1.1 Research Background

The report of the 20th National Congress of the Communist Party of China pointed out that the problem is the voice of the times, and answering and guiding the problem-solving is the fundamental task of the theory. With the rapid development of computer network technology, the number and types of computer destructive programs are also increasing. We should pay close attention to and effectively deal with the ensuing problems. The act of destroying the computer information system not only has a serious impact on the normal operation of the computer system and the integrity of the data, but also poses a threat to the public interest. In the era of big data, through the powerful editing ability of artificial intelligence, destructive programs have become an important tool for destroying computer systems. They can help people obtain corresponding malicious programs in a short period of time, and obtain, delete, add, modify, interfere with and destroy the functions of computer information systems or the data stored, processed or transmitted in computer information systems without authorization. Harsh behaviors such as interference and destruction pollute the network security environment. For now, the regulatory and governance crackdown is far less than the pace of technological updates. Therefore, the identification of destructive procedures needs to start from two aspects of technical standards and legal provisions, strengthen the legal crackdown and social education of the crime of information system of computer destructive procedures, and ensure the security of computer systems and social stability.

1.2 Literature Review

As of March 2024, a total of 574 referee documents were retrieved through the Peking University Magic Web site on the condition that the full text contains 'destructive procedures'. Through the statistics and analysis of these cases, it is found that the number of judicial cases related to 'destructive procedures' is increasing year by year, reaching its peak in 2019 and 2020, with 124 and 138 cases respectively. Up to 80 % of the cases are basically

solved at the grass-roots level. However, through the full-text accurate retrieval of CNKI containing 'destructive program' characters, it is found that there are only 161 documents, and most of them focus on computer network crime cases, rogue software or computer viruses, of which less than 10 have been studied in the past five years; however, there are only two guiding cases through the full text of the People's Court Case Library to accurately retrieve the characters containing 'destructive procedures'. In summary, the current research on 'destructive procedures' is extremely small, and it is not enough to support the identification task of destructive procedures at the judicial level.

1.3 Problem Statement and Objectives

At present, most of the theoretical and practical circles define the destructive procedure by summarizing the commonness through individuality, and there is no unified identification model. For example, based on the study of the No.104 guiding case of the Supreme People's Court, Xiaoqin Ye et al.divided the destructive behavior into two types according to the essential characteristics, one is the deletion, modification, addition and interference behavior, and the other is the production and dissemination of destructive program behavior, and pointed out that the destructive program is a computer program that can damage data, programs or destroy computer systems. For example, Chong Yu, a scholar, analyzes the current situation and harmfulness of rogue software. He believes that although rogue software is between virus program and legal program, its harmfulness is enough to be summarized as destructive program. It is necessary to sanction rogue software on the basis of expanding the interpretation of computer virus program. Although both of them systematically discuss destructive procedures, they are only separated from technical performance or legal provisions to identify destructive procedures. Furthermore, through the analysis of two guiding cases included in the case database of the people's court, it is found that only the trojan horse program control application program should be regarded as a destructive program, and there is no other discussion. In a word, the identification of destructive procedures is relatively vague at present, and it is difficult to be qualitative and quantitative. Therefore, only by further standardizing the identification operation and optimizing the technical methods at the technical level, and accurately describing the individuality and commonality of destructive procedures at the legal level, can we effectively judge destructive procedures and sanction computer network crimes.

2. The Problem of the Identification of Destructive Procedures: The Complexity of Technical Identification and the General Legal Provisions

2.1 Technical Level: Behavior Concealment and Means of Professional

First of all, the crime of destroying computer information systems often has a high degree of concealment, which means that destructive programs have certain hidden functions. Criminal suspects may use encryption, compression, dynamic debugging and other technologies to cover their malicious behavior, and use social software, fishing and other means to deceive users to further cover up their criminal behavior. Taking destructive programs such as computer viruses as an example, they hide their abilities in the computer system to achieve the purpose of not being detected and cleared by the system.They usually have anti-reconnaissance and latency, so that they can be active in the computer system for a long time and continue to develop and upgrade themselves.

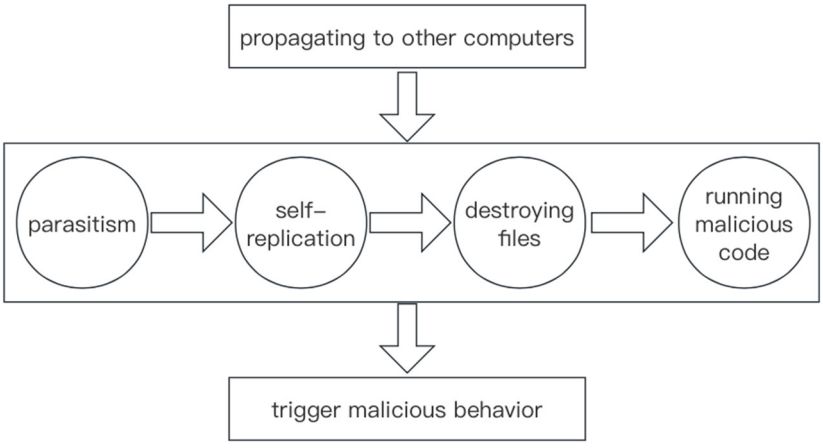

Figure 1. Computer virus boot process

Secondly, according to the provisions of China's current 'criminal law' on the subject of the crime of destroying computer information system, all natural persons and units who have reached the age of 16 and have criminal responsibility can constitute this crime. Because the means of destroying computer information systems often have certain technical content, in judicial practice, natural persons using destructive programs are usually professionals who are proficient in computer information technology and engaged in computer information technology-related industries. It has a good understanding of the working principle of the computer system, that is, the four steps of input, processing, output and storage.

Furthermore, the use of destructive programs may involve multiple links, including computer systems, the Internet, mobile devices, etc., and criminal suspects may exploit loopholes between these links to commit criminal acts. In particular, network security vulnerabilities, in systems such as computers, networks, or security devices, there are always unauthorized or unsecured vulnerabilities, which will indirectly lead to security problems such as hacker intrusion, data leakage, and network service interruption. Avoiding network security vulnerabilities requires comprehensive security measures, including updating the operating system and software, maintaining password strength, limiting access, installing firewalls, backing up important data, etc. These require professional technicians to manipulate and grasp.

Finally, the crime of destroying computer information systems may be intertwined with other crimes, such as phishing, hacking, extortion, etc. In handling such cases, it is necessary to have compound talents who are proficient in both legal and technical aspects. Therefore, it is determined that the destructive procedure has certain complex dilemmas at the technical level.

2.2 The Legal Level: The Essence of 'Ambiguity' and the Judgment of 'Pocket'

With regard to the legal provisions on the identification of destructive procedures, Article 28 of the "Regulations on the Protection of Computer Information System Security" and Article 5 of the Supreme People's Court and the Supreme People's Procuratorate's "Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Endangering the Security of Computer Information Systems" (hereinafter referred to as "Interpretation") are relatively complete. The destructive program stipulated by the former is mainly computer virus program, and it is considered that the destructive program has the characteristics of replication and infectivity. The latter stipulates that destructive procedures should be fast-spreading, difficult to control, difficult to obtain evidence, and potentially destructive and specially designed. Although the two explain the legislative intent through the combination of enumeration and generalization, the destructive programs have different forms and the technical means to achieve the purpose are different. The objects are mainly data and applications stored in the computer, which can often be destroyed in a moment, and the termination of criminal behavior is immediately submerged in the dynamic data. Therefore, the identification of destructive procedures in judicial cases is often abstract and unspecific, and even skips the identification of destructive procedures and directly identifies the crime of destroying computer, showing the trend of "pocketing" the crime of destroying computer information system.

3. Technical Identification Based on Destructive Procedure Test Operation Specification

3.1 Computer Destructive Program Testing Steps and Special Cases

The process of computer inspection is not complicated. Mastering and analyzing is the necessary process. In the whole process, it is necessary to carefully observe the suspicious clues in the system to ensure the safety and stability of the whole system.

The first is to test the attributes, determine the type of destructive program that needs to be tested and the scope of its possible influence, so as to facilitate the determination of the identification results and enhance the accuracy of the test results. The second is to determine the inspection environment. Establish a test environment similar to the actual crime environment, including the interface to interact with actual users and devices, secure and insecure network access, malicious files, etc. The purpose is to detect whether the computer system is attacked by destructive programs, and to evaluate the security performance of the computer system. For example, determine whether adequate security measures are in place to protect computer systems from destructive programs. In addition, the testing environment of destructive programs can also be used to test the resilience of computer systems to determine that the computer can return to normal after being attacked by destructive programs. The third is to select inspection tools, select tools that can effectively test destructive programs, such as code audit platforms; the fourth is to configure the test environment, configure the variables of the test environment, such as the path of the program to be tested, the port to be checked, the user list, etc.; the fifth is to run the inspection tool, to test the specified environment, to find potential security vulnerabilities and destructive code; the sixth is to analyze the test results, confirm the existence of destructive procedures, and explain and determine the test results; finally, the vulnerability is repaired, and the vulnerabilities and security problems found are repaired according to

the test results to ensure the safe and normal operation of the test environment.

It should be noted that some destructive programs are latent at the time of destruction, usually hidden in the normal system. For example, in the case of "logical bomb" in the United States, the programmer of the company's management payroll placed a "logical bomb" in the file, and the bomb destroyed the entire file library three months after he was dismissed by the company. Although sometimes the delivery technology of logical bombs is the same as that of computers infected with viruses or other malware, in most cases, they are implanted by insiders with privileged access to the attacked system, so they are difficult to detect. The best way to identify a logical bomb is to focus on the behavior of the computer, understand its system from beginning to end, and investigate anything abnormal. If unfortunately, it is necessary to make full use of the advanced malware removal tools in the market and contact relevant security experts to assist in handling. Therefore, after understanding the basic steps of destructive program inspection, it is still necessary to be careful of the hidden malicious programs or codes, otherwise the consequences will be unimaginable.

3.2 Test Results at the Technical Level

The results can be identified by static analysis, dynamic analysis, code analysis and other methods, and the similarity can be judged by comparing with the real computer destructive program. In judging whether a program is a computer destructive program, the following aspects need to be considered: the ability to destroy the computer system, that is, the computer destructive program should have the ability to destroy the computer system, such as destroying files, deleting files, destroying databases, etc.; self-replication ability, that is, computer destructive programs should have the ability to replicate themselves so that they can continue to spread after infecting other computers. The ability to destroy applications, that is, computer destructive programs should have the ability to destroy data and applications, such as deleting files, destroying databases, destroying network connections, etc. Breach behavior, that is, computer destructive programs should have malicious behavior, such as spreading malware, stealing. The test results need to be considered in many aspects, and the test results cannot be determined alone.

3.3 Security Methods and Software

The first is to select the vulnerability scanning algorithm. According to the type and requirements of the application, select the appropriate vulnerability scanning algorithm, collect data, collect system configuration files, applications, networks and services and other related information for analysis of application vulnerabilities. After that, vulnerability scanning is performed to identify possible vulnerabilities. Complete the above steps and then perform vulnerability assessment, repair comments, scan result reports, and regular updates. It should be noted that no malicious activity or destructive behavior should be carried out when building a destructive program testing environment.

Secondly, you can choose the computer nanny Trojan Ender. Trojan Ender is a security software that can fully block hacker programs. The software also has a variety of practical aids. After the software is installed, it will automatically run Registry Protector and QQ Protector. Many malicious programs will destroy some important registry entries of the host to achieve the purpose of automatic infection or activation. The registry protector can monitor the relevant key values of the registry in real time to prevent illegal modification. QQ protection master is to provide real-time protection for the current Riched20.dll buffer overflow vulnerability in QQ. In addition, it also has the functions of process management, system optimization, IE repair and so on. Its unique "view the Trojan hide area" function can effectively deal with the destruction of the most difficult to remove the file associated Trojan, and comprehensively maintain the system security.

4. The Legal Standard of Destructive Procedure: Subjective Malice and Serious Harm

4.1 The Subjective Malice of the Crime Is the Primary Criterion for Determining the Destructive Procedure

At present, in the choice of the mode of crime constitution in China, although the four elements are generally used to determine, the three classes are highly respected because of their logical rigor and clear positioning. For objective and subjective priority, most scholars tend to be objective than subjective. Professor Hong Li advocates that subjective elements can only be considered at the level of responsibility, and emphasizes that the occurrence of infringement results requires understanding or foreseeing conditions. Professor Mingkai Zhang also believes that'we must first discuss the objective wrongfulness of the act, and then examine the responsibility of the actor'. Therefore, as stipulated in Article 5 of the "Interpretation," the original intention and purpose of the producer should be scrutinized first. On the one hand, although some programs have the function of modifying the computer, they are intended to improve the performance of the computer, such as 360 security guards, 2345 cleaning king, and provide system optimization services for network users; on the other hand, some programs, such as Chameleon

malware, are created to destroy computers for personal gain. The software can impersonate the Australian government agency CoinSpot cryptocurrency exchange and IKO bank, distribute through damaged websites, Discord attachments and Bitbucket hosting services, and launch cyberattacks on victim users. Chameleon also steals user credentials through overlay injection and key records, cookies, and text messages from infected devices. In order to avoid being discovered, the software has a strong ability to evade security checks at the beginning of the factory. Once it is launched, it will immediately perform various 'checks'. At the same time, it will give itself more permissions to evade the detection of security software. It can be seen that for the identification of destructive procedures, its functional malicious effect is a necessary condition. Secondly, different from the manufacturer's idea, the user's subjective malice is often the key to judging the destructive program. The harmful results caused by direct intent, indirect intent, negligence and accidents are not comparable. In terms of the specific legal interests infringed by the use of destructive procedures in some cases, "those who are single-minded in dealing with it are obviously more terrible than those who accidentally bump into it through its side". If the user expects the occurrence of dangerous results before using a program, it means that he at least knows that the program can achieve his personal illegal purpose and harm the legitimate rights and interests of others, and indirectly derives the harm of the program to the computer. However, it cannot be inferred solely on the basis of subjective malice, and on the contrary, there is a suspicion of 'subjective imputation'. It is undeniable that the program used by most malicious users has the nature of destroying or interfering with the computer, but there may be a situation of "inviolability," that is, on the basis of full use of the program, all harmful results can not occur under any circumstances, and the program itself cannot be considered as a destructive program. For such programs, some functions cannot be implemented because of the disorder of the program itself, and some of its subjects do not have destructive functions. But in any case, if there is no subjective malice, destructive programs can not have an effect or even do not exist.

4.2 The Serious Harm of the Results Is an Important Criterion for Determining the Destructive Procedure

As we all know, China's four elements theory takes the concept of social harmfulness to lead the overall situation, and advocates that social harmfulness is the most basic feature of crime. For the division of computer programs, it can be generally divided into destructive programs and 'neutral programs'. The former is mainly used to invade, interfere with and destroy the computer system. Its production and use usually have illegal circumstances such as citizen information leakage and damage to legal property, and the possibility of causing serious harm is much greater than the latter, such as the Supreme People's Procuratorate Guiding Case 69. The defendant used trojan software to manipulate the control server and launched high-frequency service requests to three game companies, resulting in the inability of the three game companies 'cloud servers to operate. In order to reduce losses, it was forced to organize personnel to carry out emergency repairs and generate more than 40,000 yuan of losses. In case No.103, the defendant used the 'GPS jammer' to modify and interfere with the GPS information service system, resulting in the failure of the system function, the inability to remotely lock the vehicle and monitor the vehicle in real time, and the criminals were able to take the opportunity to collect improper benefits. Whether it is trojan software or 'GPS jammer', although they are not similar in the scope, quantity and degree of infringement, they all have the characteristics of endangering social public order, and are predictable in causing losses, in line with the 'destructive' characteristics. In addition, focusing on the relevant provisions of the "destructive program inspection operation specification," it can be seen that the destructive program is an application program, and the application program refers to a computer program that completes one or more specific tasks. According to Article 3 of the Regulations on the Protection of Computer Software (2013Revision), computer programs refer to a sequence of coded instructions that can be executed by devices with information processing capabilities such as computers in order to obtain certain results, or can be automatically converted into a sequence of coded instructions. Symbolic instruction sequence or symbolic statement sequence. Therefore, it is necessary to make it clear that only serious harm results cannot be identified as destructive procedures, such as Supreme Law Guidance Case 102. The two defendants modified the DNS settings of Internet user routers through malicious code and committed 'traffic robbery'. It not only causes damage to the computer system of network users, but also increases the risk of personal privacy exposure of citizens. However, malicious code is not a program, and the code is only the basic unit of the program. Even if the malicious code conforms to the 'destructive' feature, it cannot be identified as a destructive program. Furthermore, the harmful results caused by the suspected destructive procedure should be objectively and accurately determined as a whole. It is not possible to determine whether it meets the objective requirements of the destructive procedure only based on the amount of illegal proceeds of crime or the economic losses caused. Although the amount of crime in some cases is small, some of them affect the normal Internet access of Internet users on a large scale, some cause bad social impact, and some even endanger personal safety. Therefore, it is necessary to further judge the destructive procedure through the harmful results from many aspects.

5. Conclusions

From the computer era to the Internet era, human society has been inseparable from the computer, and software programs have never so comprehensively and profoundly affected the production methods and living habits of human society. However, the rapid development of science and technology has spawned strong vicious economic benefits, and constantly encourage the iterative upgrading of destructive procedures. Among them, the new malware represented by Chameleon seriously damages the legitimate rights and interests of citizens. On the issue of protecting user security and mobile Internet security in accordance with the law, the identification technology of traditional destructive procedures is scarce, the content is thin, the traditional legislative concept is lagging behind, and it is unable to meet the upcoming era of artificial intelligence. The problem of computer network security will be a wake-up call. In view of this, the identification mode of destructive procedures is upgraded from technical parameters and legal norms, and the identification standards are reconstructed with a new concept. We should not only make rational use of the legitimate functions of software programs, but also highlight the protection of citizens 'legitimate rights; we should not only pay attention to the development trend of artificial intelligence, but also further formulate the identification countermeasures of destructive procedures. At present, in view of the particularity of destructive procedures in the new form, we should take the constitution as the fundamental basis, expand and modify the necessary legislation on the damage objects, types of harmful behavior regulation, protection of legal interests and other aspects of destructive procedures, and improve the relevant identification methods, so as to meet the actual needs of computer information security and safeguard the necessary legitimate interests of citizens.

References

Hu, H. Y. Y. (2022) Judicial determination of non-computer virus destructive procedures. *People's Justice,* (20), 27-30.

Li, H. (2008). The development of the theory of result without value. *Legal Studies,* (05), 109-128.

Li, J. J., & Jiang, H. (2022). information security strategy analysis of computer network. *Electronic Technology,* (07), 236-237.

Liu, J. J. (2023). Path selection of fault imputation: from traditional review mode to behavior imputation theory. *Journal of Zhejiang University* (Humanities and Social Sciences Edition) (05), 79-93.

Sun, D. C. (2015). Characterized the behavior of implanting destructive programs into mobile phones and illegally profiting. *Chinese prosecutors,* (14), 45-47.

Sun, Q. (2007). Thoughts on the Crime of Creating and Disseminating Disruptive Programs such as Computer Viruses. Master's degree thesis, Jilin University.

Xu, H. B. (2003). Computer babysitter. *Software guide,* (05), 29.

Xu, Y. X. (2005). *Contemporary criminal law thought.* China Democracy and Legal Publishing House. Beijing.

Ye, X. Q., & Gao, C. Y. (2020). criminal law determination of the act of destroying computer information system-based on the development of the No.104 guiding case of the Supreme People's Court. *Applicable law,* (14), 3-14.

Yu, C. (2015). The criminal law evaluation of rogue software and its criminalization. *Journal of Yunnan University (Law),* (02), 53-60.

Yu, H. S. (2011). Understanding and application of'Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Endangering the Security of Computer Information Systems'. *People's Justice,* (19), 24-32.

Zhang, M. K. (2016). *Criminal Law* (I). Law Publishing House. Beijing

Zhang, M. K. (2017). Judicial application of class theory. *Tsinghua Jurisprudence,* (05), 20-39.

Zhao, H. (2023). Analysis of computer network security protection countermeasures based on Internet of Things. *Integrated Circuit Applications,* (12), 50-51.

Acknowledgments

Thanks for my family’s support, without whom I would not be able to publish my article.

Thank my good friends Minghan Fang, Saicheng Fang, Minghui Wu, Jianming He for their support, so that my paper can be published smoothly.

At the same time, I also thank my friend Xiaoyu Yu who wrote this paper together and gave me a lot of help.

Authors contributions

Chaojie Ma is responsible for the research and analysis of the whole paper, drafting and revising the contents of the first, second, fourth and fifth parts, and Xiaoyu Yu drafting the third part.

Funding

Not applicable

Competing interests

Not applicable

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.