UDC 343.9

ANALYSIS OF HIGH-TECH METHODS OF ILLIGAL REMOTE COMPUTER DATA ACCESS

V.V. Polyakov, S.M. Slobodyan

*Altay State University, Barnaul city
Tomsk State University of Control Systems and Radio Electronics
E-mail: polyakovvv@rambler.ru

The analysis of high-tech methods of committing crimes in the sphere of computer information has been performed. The crimes were practically committed from remote computers. Virtual traces left at realisation of such methods are revealed. Specific proposals in investigation and prevention of the given type computer entry are developed.

During last years the escalating tendency of development of illegal ways, from the point of view of the Russian Federation legislation, and administratively unauthorized access to the computer information with use of the network technologies based on users' removed access to the information or information databases is precisely traced. One of the major factors promoting this process, is [1] the presence in computer information circulation sphere of the new hardware-software means possessing wide high-technological abilities, development and application of which allows plotters to find non-standard decisions for realization of illegal access. In such situations illegal access is very specific, and virtual traces for law enforcement bodies remain hidden, especially in connection with the amplified counteraction to investigation from computer criminals. The given circumstances in the serious way affect crime latency in sphere of the computer information which reaches 90 %. We shall emphasize that in modern criminalistics traces of realization of such kind of crimes practically are not studied [2]. Thus, an actual problem is studying the pattern of the display of the mechanism «practice» of preparation, commission and concealment of crimes in the sphere of computer information.

Most professionally skilled infringers operate so that traces of computer penetration have been as much as possible hidden or authentically did not specify the person who left them, or the customers or heads of criminal group, when it was available [3]. Moreover, in these cases such ways of penetration are frequently used that logic ways of investigation, first of all, have led to innocent persons, which is in an even greater degree complicates work of law enforcement bodies. The problem is explained by an insufficient level of special knowledge of computer technics and information technologies by employees of law enforcement bodies investigating these crimes. In such conditions at carrying out the investigation precise representations about what virtual traces remain at hi-tech ways of illegal access in the sphere of computer information should render considerable aid. In this subject domain especially complex and important infringements are those based on hi-tech ways of unauthorized access to the computer information and accomplished by use of an information network from remote located PCs.

It is necessary to note that for the illegal remote access the finding of traces in different places simultaneously and at great distances is characteristic. So, they can be left not only on a workplace, but also in a place of storage or reservation of the information [4.] Traces also can be found on a place of preparation for access (for example, where programs for illegal access were developed or tested), a place of tooluse, devices and tools intended for operations of illegal access, and also in a place of information use [5.] The specified circumstances demand checking all prospective places where virtual traces can exist. It is important to note that only received and issued with compliance of criminal-procedure legislation the given traces can be attached to a criminal case and begin to be considered as evidence.

Let us consider some main features of hi-tech ways of illegal access to the computer information.

1. Use of somebody else's registration addresses in the local network that has Internet connection

The computers connected to a local network with Internet connection, as a rule, have two addresses: the logic address of a network level (IP-address) and the physical address of a network interface map (MAC-address). At sending packages out of a local network limits these addresses will be detected, hence, it would be possible to find the PC from which illegal access has been accomplished, which in the future will allow us to find corresponding traditional and virtual traces. However, the persons possessing special knowledge can independently register somebody else's IP-address to confuse an investigation. In case, when there are bases to believe that there was such situation, it is necessary to pay attention to the MAC-address of a network card. As a rule, all network cards have unique number which is complex for changing or destroying. Given number can be also detected during network connection. Thus, as a proof that the infringer used somebody else's IP-address, would serve discrepancy of the MAC-address of a computer network card to that MAC-address which has been specified during connection. For investigation of similar infringements the negative role is rendered by the circumstance, that there are the network cards on sale, allowing changing MAC-addresses by program method. In that case it is possible to use easily not only somebody else's IP-address, but also the MAC-address. If investigation will establish that during illegal access, behind a computer which specify registered by criminal IP and MAC-addresses, the specific person had worked the suspicion will fall on him. Moreover, the situation when stolen in-

formation or any other traces will be thrown on the given computer is quite possible. Similar actions are extremely dangerous, as at not skilful enough investigatory work the innocent person can be convicted.

More often, on provider's server the registration data of its clients can be stored. The majority of these data at their correct registration are used by law enforcement bodies as evidence of crime commission from a specific computer. At the same time the analysis shows that the control specifying on the person who worked on a computer during commission from it of illegal access, practically does not happen [7]. For example, we shall consider a situation when access was made from a house computer. The person, to whom it belongs, can declare in the indications, that during commission of access at his place there were people, and they approached computer. If in a similar situation the suspect will agree with someone of them to confirm the given circumstances, to establish who has made the access will be extremely difficult.

2. Use of wireless (Wi-Fi) connections

For unauthorized access a lap top, cellular telephone or other portable device near the point giving access to the Internet by wireless technology, for example, in «Internet-cafe» can be used. In such situation on provider's server the following virtual traces will be left:

- registration data of the infringer, for example, login and password;
- settings which the infringer used, in particular his IP-address, allocated for a certain communication session;
- information about packages which have been sent or received on client's address, in particular time of sending/receiving, size, type, IP-address of the addressee or the sender, etc.;
- in some cases data about plotter computer configuration.

At the same time the investigation, even having these data, is not able to allocate specific person and the device from which illegal access has been done. An uncertain circle of people, by whom the signal for that moment could be caught when the access has been accomplished, can be under suspicion. For example, it can be people with lap tops, being in cafe or in parked cars, the inhabitants of nearby houses using special devices catching a weak signal. Operative actions on a search of the listed people with the purpose of detection and inspection of their computers are represented improbable from the point of view of authorization of the given actions and their efficiency.

3. Use of somebody else's telephone number

Bodies of investigation during criminal search, as a rule, start with the data received from provider's firm, first of all concerning telephone number from which illegal access at use of modem connection had been done [8]. The analysis of some criminal cases has shown that proving commission of penetration is constructed on the basis of the main proof – telephone number from which there was a connection with provider's server [9]. It is represented that the similar circumstance cannot be considered as the universal proof. It proves to be true that telephone cables practically have an open access, technical failures on an automatic telephone exchange (ATE) are widespread, and also partnership of ATE workers in commission of illegal access is possible. All this creates a good situation for plotters to take advantage of the described variants. In such way, by means of a lap top it is possible to connect to a line of a telephone system in an apartment house and by that to carry out access to the Internet network from somebody else's telephone number, including use of an access card to the Internet. To prove the fact of connection of the infringer to somebody else's telephone cable is extremely difficult. We shall note that cases of use of somebody else's telephone communication lines for realization of long distance calls the modern Russian practice knows enough. The given circumstance testifies to potentially possible growth of commission of the actions connected with illegal access under the similar scheme. For prevention of an investigatory mistake and accusation of innocent it is necessary to take advantage of the specialists' or experts' help, whose objective would be the establishment of possession of penetration from other computer [10]. Revealing of the given circumstance is possible by research of hardware-software maintenance of that computer and data comparison available in it, with the information given by the provider.

4. Use of somebody else's computer as illegal access tool by short-term remote connection with it

For illegal access such way as the short-term remote connection with somebody else's computer can be used, in case when connection to a victim's telecommunication line is absent. For example connection to somebody else's computer by remote way with use of the virus type program «Trojan horse» is widespread. To establish such program is possible by means of E-mail, Wi-Fi connections or by illegal connection, since computer protection at the majority of users is very low. In such situation on the infected computer there will be information about illegal connection, and the suspicion will lay on the owner of that computer.

During investigation of such method of possession of access it is possible to offer following recommendations on detection of virtual traces. In case of self-liquidation of the nocuous program it is possible to analyze the system register on presence of characteristic commands and their requisites and to find out the data, allowing us to assume that there was a similar virus on a computer. For the proof of virus presence it is possible to try to use standard programs on restoration of the removed data. Such operation will not be successful, if in the memory cells reserved for a virus, the other information was entered after that. Besides in many cases access to the Internet is carried out with use of proxy-server which fixes the information, concerning network connections [11]. According to proxy-server it is possible to establish the fact of computer connection from which the crime was presumably made, to plotter computer.

5. Use of provider services not fixing data about its users

Now there is an increasing quantity of providers who do not fix users' information. It is done with the purpose of increase of anonymity, so it would not be known, what sites are visited by provider's clients. With use of such services on provider's server there will be no virtual traces of access, which will considerably complicate investigation. Besides, for illegal access the so-called anonymous proxies-servers, accessible in Internet network, can be used.

6. Possible ways of illegal access attempts prevention

Necessity of measure complex perfection on protection of computer systems and information databases, in particular, the automated means of control of special information use in various spheres of human activity, exists for a long time. The need in protection of the information from illegal access is caused by computerization of many economic and political branches of the state structures functioning as means of efficiency increase of information processing for acceleration of decision-making and management.

The computerization has sharply increased volume of information stream and capacity of databases. Moreover, the professional standard of qualified professionals in the field of computer means and the rate and intensity of these means use continuously increases. It leads to, following from here, logic necessity of development realization, creation of new and perfection of existing computer systems and means, and not only for protection, but also for an estimation of protection reliability and preservation of the computer information from the unauthorized to it access. There are also a number of factors of economic, political, social, psychophysiologic, medical, geopolitic, etc. character (their analysis is beyond this article object of research) which lead now to growth of attempts of unauthorized access to the computer information, including the increased practice of penetration through network structures in information databases from the removed PCs. Such practice of unauthorized penetration into databases from remote PCs is based on use of developing network technologies and improvements of means of reception and transfer of the computer information.

Most simple and effective enough way is introduction of some protection threshold of the information and preservation of inviolability of databases consists in aprioristic acceptance of measures consisting, for example, in installation into a computer of known software, intended for restriction of the easy access, prevention and warning of illegal use attempts of the given computer and stored in it computer information [6]. Such means provide maintenance of the minimal level of protection measures of the information in computer means of collective using. Established in them system makes protection of the information against unauthorized access so that the right and an opportunity of use, stored in computers informational data, realizations with them operations on their modification were received only by the user individually distinguished by the given system.

The similar variant of protection ensuring of the information from illegal to it of access can be executed by use of the standard software stipulated by library of Microsoft Access package. Application of Microsoft Access does not allow several users to correct or to change the same details simultaneously, i.e. enters ranging on access to the information based on priorities which are established by the system manager. At the same time, Microsoft Access automatically provides protection of data against their simultaneous change by different users (diversity by time and priorities of access to informational data).

In Microsoft Access measures of data integrity protection by division of access to the information by ranks and priorities are stipulated reliable, from the point of view of requirements satisfaction of bottom level protection of users' broad audience. At that, if to users with the highest priority the right of access to the main informational and software means is given, then to others, not included in the list by the manager, work with duplicates of the allocated fragments of the information or frames of the database only is permitted. It enables to create an additional threshold of access, besides stipulated in the Microsoft Access package, to logic rules of information protection and ensuring increase of databases protection reliability from attempts of illegal access.

Certainly, the user professionally mastered the Microsoft Access software product, can find ways of detour of protective barriers of access to information resources and database. But, in the latter case, he gets access only to fragments of the duplicate, instead of the main resources. Other logic rules of access barriers establishment are also essentially possible. For example, complicating the identification attributes order, reflecting authenticity of the user, on granting to him access right even to the duplicate or to the system from the remote terminal.

Another measure of protection is the account of the factor, that inclusion of highly professional experts in process of use of high technologies inevitably demands an establishment of corresponding to this factor and control measures. It is necessary as well as an estimation of maintenance order «transparency», established by the legislation or instructive materials, rules and requirements during use, permitted to the given user, those fragments of information and high computer technologies which, to some extent, touch the sphere of company safety, organization, the state or personal and other citizens' rights. Other principles, based on person's identification, of ranging access priorities and estimation of necessary level of informational safety of access to the given user to informational resources, are also possible.

7. Conclusion

In such a way, having done the analysis and generalization of above stated, it is possible to come to the following conclusions:

1. Development of measures, program and hardware means of counteraction of unauthorized access attempts to computer information should be closely coordinated with studying methods, approaches to

the decision and principles of high technologies of realization in practice of such attempts. The analysis of existing «practices» of illegal access to computer information is important for understanding of essence and formation in the following problem solution, which can basically prevent from such actions. It is more preferable to prevent them at a stage of planning and preparation of attempt of such opportunity realization, i.e. it is important to show an impracticability of doing illegal actions, meaning a goal of the penetration purpose achievement. Within the limits of mass inspection, for quite clear reasons, caused by certain motivation of such «users» and closeness of such information, the analysis and research of similar «practices» is inconvenient to carry out, more likely impossible.

2. Development of measures of illegal access to computer information prevention on the basis of generalization and the analysis, taken place in the practice, really considered or subjects to thorough and detailed studying, different aspects of approach ways and motivation of activity realization on illegal, including remote, access to computer information is actual. It is necessary to recognize that acceptance and development of forecast decisions on the basis of analysis of considered real «practices» of illegal penetration to computer information, and also their generalization are extremely complicated. Really, in such cases the researcher has «business» with multialternative motivation of a special sort of «user». Received at that actual material for research represents itself as a small dimensional extracts with attributes characteristic for juridical, sociological, psychological and legal practices.
3. In a considered subject domain it is important to investigate motivational aspects and technological ways of such sort «practices» realization. It is necessary to study the phenomenon pattern statistics. In other words, to reveal all possible directions of such activity; to define where and how unauthorized computer connections are established; to investigate the facts of any illegal access; to estimate, what promotes and what interferes illegal access, including access from remote PCs.

Conclusions

In the present work, though limited, the analysis of in the fact realized methods and ways, of hi-tech illegal, under the current legislation of the Russian Federation, actions by unauthorized access to computer information from remote terminals.

Features of criminal virtual traces connected with application by plotters of hi-tech ways of illegal access to computer information are analyzed, and ways of revealing of these traces are offered. Results of the research led in the present work, testify that in a view of the amplified counteraction from criminals, the further studying of patterns and mechanisms of preparation, commitment and concealment of a considered kind of hi-tech crimes is required from modern criminalistics.

In our opinion, only all-round studying of all aspects of the available problem will enable to find the optimum decision for formation of the occurrence of similar situations forecast and definitions of possible directions of their realization. On the basis of the found decisions during the analysis it is possible to generate a direction of actions on prevention of the illegal attempts of hi-tech penetration into computer systems preparation.

The brief description of the stated above real facts of illegal access allow specialists to state latent logic patterns of formation of illegal action «virtual» traces in an investigated subject domain. Logic patterns are essential for knowledge base construction about methods of illegal access, formation of which will demand input of new concepts and judgment of many knowledge fragments in the given area.

The considered approaches, ways and methods of revealing of «virtual» traces of «breaking in» – illegal access to computer information can be supplemented or replaced with other methods of search for the latent laws of formation of «virtual» traces of unauthorized access realization. It will demand revision of procedure of the real facts of access analysis or actions achieved in other way of penetration.

REFERENCES

1. Zegzshda D.P., Ivashko A.M. Fundamentals of information systems safety. – Moscow: Goryachaya liniya – Telecom, 2000. – 452 p.
2. Mesheryakov V.A. Crimes in sphere of computer information: legal and criminalistic analysis. – Voronezh: Voronezh State University, 2001. – 176 p.
3. Poleshchuk O.V., Shapovalova G.M.. Criminalistic research of traces during computer crimes investigation. – Vladivostok: Publishing house of Far-East University, 2006. – 157 p.
4. Gavrilov M., Ivanov A. Investigative inspection during crime investigation in sphere of computer information // Zakonnost. – 2001. – № 4. – P. 11–14.
5. Nikonov V., Panasyuk A. Non-traditional ways of collecting and securing evidence // Zakonnost. – 2001. – № 4. – P. 19–24.
6. Olifer V.G., Olifer N.A. Computer networks. Principles, technologies, reports. – Saint Pitersburg: Piter, 2006. – 960 p.
7. Gavlo V.K., Polyakov V.V. Some peculiarities of crimes investigation connected with illegal access to computer information // Izvestiya of the Altai State University. – 2006. – № 2. – P. 44–48.
8. Archive of October regional court of Barnaul city. Case № 1-705/04.
9. Archive of Industrial regional court of Barnaul city. Case № 1-51/05.
10. Rossinskaya E.R. Legal expertise in civil, arbitral, administrative and criminal procedure. – Moscow: Norma, 2005. – 656 p.
11. Archive of the Central regional court of Barnaul city. Case № 1-537/03.

Arrived on 26.10.2006