Assessment of methods online forensics in alleviation of the consequences of the attacks of extortioners

F B Tebuyeva, M G Ogur, M M Gasparyan, A I Bliznetsova
1North-Caucasus Federal University, Stavropol, Pushkin str., 1, 355017, Russia

E-mail mogur@ncfu.ru

Abstract This article is devoted to disclosure of essence of a concept online forensics. On the basis of the analysis of practical activities and works of domestic and foreign experts in article the author's concept characterizing estimated judgment of methods in an issue of alleviation of the consequences of the attacks of extortioners reveals.

Keywords: forensic; criminalistics; forensic methods.

1. Introduction
There is no secret, that with development of new technologies also the illegal actions posing in themselves potential threat not only narrow-minded but also world scale actively progress. The amount of information grows in a geometrical progression that inevitably conducts to a compromise of a classical triad of information security: confidentiality, integrity and availability.

In a type of complication of the process of development and deployment of any given IT product the criminalistic examination accepts ambiguous character: not only the equipment and ways of investigation, but also a possibility of malefactors are improved. From there is an urgent need in assessment of the standard methods of a forensic for the purpose of ease of consequences of the attacks of extortioners.

2. Problem research:
The historical semantic origin of a forensic originates in Ancient Rome when one of favorite processes the people had judicial debate and performances which are characterized by the word "foren" that means "the speech to a forum".

However, emergence of this term in Russian is caused by loan from English: the concept "forensic science", or the "judicial science" understood in our country as criminalistics began to be used in a short form thanks to what got narrower circle of application and from the category of the general criminalistics passed into the category computer [1].

Taking into account a modern variety of the executed functions, there is no uniform comprehensive concept of a forensic, the number of interpretations is high, but the essence is invariable, we will consider a little from them.

Owing to the fact that the forensic as applied activity received the popularity in our country relatively recently, we will dilute a Russian-speaking segment of definitions English-speaking.

Michael A. Kaloyannides understands set of the methods and tools used for search of the data in the computer which can be used to the detriment of its user [1] as forensics. Addressing Henry B. Vulfi's
works, it is possible to claim that the forensic is a methodical number of receptions and procedures of collecting proofs, since computer facilities and various memory devices and finishing with digital data carriers which can be presented in court in a coherent and substantial format [2].

It is necessary to mention also one of the fullest and popular Russian-speaking sources "Forensic - computer criminalistics" N.N. Fedotov.

Relying on this author, one may say, that the forensic (computer criminalistics) is applied science about disclosure and investigation of the crimes connected with computer information about methods of receiving and a research of the proofs having the form of computer information (so-called digital proofs) about the technical means used for this purpose [3].

In spite of the fact that many things described in this work are outdated, Fedotov's interpretation is used in works of various level to this day.

Generalizing the above, it is possible to draw a conclusion that the forensic, in a generalized view, is the fundamental and most volume section of digital criminalistics comprising set of methods and means on identification, investigation and prevention of computer crimes.

3. Methods of computer criminalistics

At the moment the mankind only begins to plunge into an era of high technologies, but already now it is possible to notice how digitalization influences tenor of life habitual to us: personal computers, laptops, smartphones, etc. became an integral part of our life, separately in itself they are less subject to any given threats, but at connection to network and the Internet everything cardinally changes and this situation does us is significantly more vulnerable at any given attacks on devices [4].

Overwhelming part of information is on electronic media, from there is a certain risk of hit of all information base to the third parties.

As it was already told, the forensic comprises methods on identification and investigation already happened or planned cyber-attacks, then it is worth allocating two main methods of examination: static analysis (static analysis) and dynamic analysis (live analysis). Let's consider them in more detail.

3.1. Static analysis

This method is traditionally directed to creation of dumps (molds) and a research of copies of a disk that then to take contents of cells of memory. Remote files, Web browser history, files and fragments of open access, network connections and so on can be an example of that.

They are taken in order that it was possible to create the accurate schedule and statistics with the periods of time giving to the criminalist an idea of use of the device to restore the course of early events, that is the essence of a method consists in creation of the copy partial or a summary of any activity executed in the device of the victim before its reset or blackout.

The relevance of this method comes to the forefront only when there is an opportunity in due time to react to identification of an incident.

For direct unloading of data in the static analysis different types of instruments of program and technical support are used, presence or absence at malicious software of protection against removal of molds of the contents can serve as an important factor.

Data for a forensic are collected on various types of external stores, such as USB, external hard drive or CD/DVD carriers and then data are sent to specialized crime lab for carrying out by the investigator or expert of all necessary procedures for the analysis of evidentiary data.

As advantages of this method, it is possible to allocate that chances of modification of data are insignificant also an opportunity for extraction of dangerous materials small. Among shortcomings there is a work directly with cryptographic ways, dangerous data of the software, gigabytes of data for the analysis, the lack of the standardized procedures, practical and lawful restriction, proofs can easily pass into a condition of inaccessible.

3.2. Dynamic analysis

The sense of this analysis is revealed already in the name: if literally to translate "Live analysis", then
we will receive "the live analysis". That is work, unlike the static analysis, happens directly on the device of the victim without further power off [5].

It turns out that collecting, the analysis, generation in reports of necessary information happens at that time, the system so far compromised remains functional.

The tools which are used at this method of the analysis can provide a clear picture of dumps of memory, the started processes, open network connections and unencrypted versions of the encrypted files. As when using the static analysis, the contents of memory cannot be received properly fully, the dynamic analysis provides coherence and integrity of criminalistic data. Information collected by such method can be used in various ways for obtaining proofs necessary for investigation or idea of suspicious activity and operations performed directly by the user or existence of remote access to the compromised system [6].

Advantages of this method are search of harmful information and that fact that collected information is limited to relevant. Also, it should be noted shortcomings: modification of information in real time, indistinct images, limited volume of collected information, each computer installation is unique and bears in itself difficulties in work with it, it becomes more difficult to prove authenticity and reliability, the tool kit does not correspond to criminalistic.

4. Assessment of methods in alleviation of the consequences of the attacks of extortioners

The ideal system capable to fully protect any given device from various threats, does not exist therefore at stages of prevention and detection of the attacks most often attacks of criminals are crowned with success that forces users to liquidate their consequences [7].

One of the most topical issues of this subject are programs extortioners - a kind of malicious software which at hit on the device blocks to the owner partial or full access to its data, demanding to pay a certain sum for receiving the decoder.

Often such programs get on the device in several ways: harmful spam and advertising with use of technologies of social engineering, external foreign stores, phishing letters and so on.

Today this phenomenon gets new ways and tricks: if earlier extortioners asked repayment for the encrypted data, then now they replaced a business model with more flexible - threats of violation not only availability, but also integrity and confidentiality of the infected data are added to standard requirements. The specified scheme of succession of events nonpluses the victim and it does not have other choice how to pay, swindlers have access to the stolen information and can vary dexterously the sums and terms of transaction.

If after all program of this sort appeared on the device, then first of all it is worth isolating it from other devices if those are available, in order to avoid loss of full access to all database. Understanding and acceptance of that fact that it is impossible to go on similar transactions at all has to be the following step and to try to redeem access or data, it, on the contrary, will only aggravate a situation. When the swindler understands that you already on a hook, he will make sure that you and other users can be manipulated quietly, and it will lead to even big losses not only with yours, but also the foreign country.

The attempt of restoring access to some encrypted files by means of free programs decoders can become the following step, but because of use by criminals of difficult algorithms of enciphering not for all families of programs extortioners it is possible to find the decoder. But unintentionally not to aggravate the already deplorable state with the incorrect decoder and once again to encrypt the data, it is the best of all to address experts in the sphere of cyber security or information technologies [8].

Here we also approached consideration of the above-stated methods of a forensic.

Let's begin with traditional - static. As it was already told, this method will be the most effective at rapid response to intervention of the stranger ON. As the dump (mold) is created and the device is switched-off, the probability that not all files will be subject to infection increases. On the isolated platform there is a possibility of a research of the program extortioner of this type and selection of the corresponding decoder, and existence of backup copies of cells of memory guarantees safety of the encrypted file systems. Further at selection of the decoder it will be possible to carry out this operation several times and not to be afraid for additional encoding of files. Act as essential minuses of this method
need in cryptographic methods of interpretation and volumes of data of a dump, quite large for the analysis. But, despite this, the probability that you will go to the transaction with criminals, and this unconditional advantage over the essence of programs extortioners is reduced [9]. Speaking about a dynamic method of a forensic it is worth specifying first of all that the most part of files is saved and gives wider picture of the event as work happens directly in the infected functioning system. Availability of the relevant information but which is not written down final will be indisputable advantage that is an opportunity to trace in real time the center of distribution and according to its consequence is given. On the other hand, this method is characterized by a number of powerful shortcomings: in real time the risk of modification of all data on the device is high that leads to expansion of a zone of defeat by the program extortioner and strengthening of influence of swindlers on the victim; the device in itself is unique and there is not always an opportunity to competently process a flow of harmful information [10].

5. Conclusion

Accumulating information stated above it is possible to draw the following conclusions:

1. The efficiency of any given method, in the solution of a question of programs extortioners, cannot be hundred percentage: each of them has a number of advantages and shortcomings, but it does not cancel existence both a human factor on both sides of crime, and refinement of swindlers;

2. Decoding of important data independently or with the expert cannot bring fruitful results, and the stolen information can become object of blackmail (violations of confidentiality and dissemination of data to the fourth persons) there are two options of an outcome of events: either to pay, or to find the criminal;

3. To prevent hit of similar programs on the device it is worth following some simple actions:
   - Installation of the reliable antivirus software,
   - Timely SOFTWARE updating and other components of a system,
   - Creation reserve or backup copies of data,
   - the Attentive relation to advertising mailings, letters from unknown senders,
   - Use of safe VPN connection at connection through public WI-FI.

References
[1] Caloyannides M.A. 2004 Privacy Protection and Computer Forensics (Second Edition). (Artech House Publishers)
[2] Irfan Shakeel 2015 Introduction to Computer Forensics and Digital Investigation (INFOSEC INSTITUTE)
[3] N.N. Fedotov 2007 Forensic - computer criminalistics (M.: Legal world,. - 360 pages of ISBN 5-91159-013-1)
[4] Henry B. Wolfe 2001 An Introduction to Computer Forensics: Gathering Evidence in a Computing Environment (Informing Science, Special Series: Expanding the Focus vol 4 No 2) pp 47-52
[5] Mamoon Rafique, M.N.A.Khan 2013 Exploring Static and Live Digital Forensics: Methods, Practices and Tools (International Journal of Scientific & Engineering Research vol 4, Issue 10) pp 1048-1056
[6] D.N. Shevchenko 2018 Methods of digital criminalistics and a computer forensic for
investigation of incidents of information security

[7] Kalber, S.; Dewald, A.; Freiling, F.C. 2013 Forensic application-fingerprinting based on file system metadata (Proceedings of the Seventh International Conference on IT Security Incident Management and IT Forensics, Nuremberg, Germany) pp. 98-112

[8] Bang, J.; Yoo, B.; Kim, J.; Lee, S. 2009 Analysis of time information for digital investigation (Proceedings of the Fifth International Joint Conference on INC, IMS and IDC, Seoul, Korea, 25-27 August 2009) pp. 1858-1864.

[9] Chabot, Y.; Bertaux, A.; Nicolle, C.; Kechadi, M.T. 2014 A complete formalized knowledge representation model for advanced digital forensics timeline analysis (Digit. Investig. 2014, 11, 95-105)

[10] Carrier, B. 2019 Open Source Digital Forensics Tools