separately. This can be done by building IS models. Following this strategy, one should always proceed from the fact in which subject area and to what extent information is adequately collected in the IS.

So, while studying IS, one should stress the indisputable fact that the information accumulated in it is a model of some area of the real world. The main requirement for any IS is to ensure the adequacy of this model. The main tools for increasing the efficiency of complex information systems are: operational analysis of the situation, drawing up an operational calendar work plan, modeling management processes. Modeling is understood as the replacement of one object (original) with another object, called a model, and the study of the properties of the original is carried out by examining the properties of the model. The need to use models arises when obtaining solutions on a real object is expensive, difficult or even impossible. The model simplifies, reduces the cost and speeds up the process of studying the original.

REFERENCES

1. https://s3.amazonaws.com/s3.documentcloud.org/documents/555334/1-11-cr-10260-nmg.pdf)
2. Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States Catherine D. Marcum1 Georgia Southern University, USA George E. Higgins2 Richard Tewksbury3 University of Louisville, USA (www.cybercrimejournal.com/marcumetal2011julyijcc.pdf

M. Shevchenko, V. Makedon, O. Bovkunova

POSSIBILITIES OF RESEARCH OF INFORMATION CARRIERS WHILE UNAUTHORIZED ACCESS TO EDS KEYS

The main application of EDS keys was found in the financial sector – while working with trading platforms on the Internet and in systems of remote banking service (hereinafter referred to as RBS) – what gave rise to high interest in these keys from attackers. Crimes related to unauthorized access to systems RBS have

some features that affect the capabilities production of computer and computer-technical expertise and research media.

There are several stages of NSD, each of which leaves traces in the computer system:

1) Primary penetration. It is implemented through the implementation malware of the Downloader or Backdoor class on the computer, for example, through programs of the Exploit class.

2) Fixing their positions on the infected computer. Installation of specialized Trojan programs that copy keys EDS from a removable storage medium (USB disk or floppy disk), keyloggers to copy the password to access these keys (for the purpose of further money transfer from a computer intruder). In order not to lose control over the infected computer, modified package of utilities for remote administration (R-Admin, TeamViewer, WinVNC, etc.), can be installed additionally as well as daily updating versions of installed malware to avoid detection of old versions by antivirus programs. There are cases when Trojan programs are made in a single copy for each specific organization being hacked, which guarantees the absence of malware signatures in anti-virus databases.

3) Collection of information about the RBS system. Copying EDS keys, interception of entered passwords, making screenshots during work of the user with protected resources. As a rule, money transfer funds from a hacked account are not carried out on the first day after infection of a computer. Intruders are trained to work in a specific Internet banking system, they check account statements, study the features of payments being made.

4) Waiting for the receipt of money on the account. If the frequency of funds to the hacked banking account is fixed, then attackers will regularly check the status of the account, hoping for new transfers to the account.

5) Transfer of funds. It is implemented directly from infected computer using a USB-connected key or from the attacker's computer using copied access details.

6) "Sweeping" traces. After an unauthorized payment, the attackers must promptly either cash out the money, or transfer them to other accounts along

the chain, possibly splitting stolen money in smaller amounts. So that the account owner does not detect the loss and can not apply to the bank with a request to block money on the account, attackers try to block or make it difficult for the user to work with his account. For this special malware programs that interfere into the user's work is installed on the infected computer (blocking or slowing down the user's work), deleting some files of operating system or destroying the entire file system on computer disks completely.

An expert or a specialist must find such traces of UA on the hard drive of an infected computer: 1) date and time of the initial infection of the computer, source infection; 2) type, characteristics, settings of malware, used for unauthorized access, reports and logs of their work; 3) information that personalizes the author of malicious programs; 4) the actions carried out by the attacker in the system, and addresses from which the attacker performed the remote computer administration; 5) information on the preparation of payment orders (drafts).

So, it is important to stress that establishing the type of malware detected on the computer programs is an important stage of an expert research, since the expert must determine whether it was possible using detected malicious programs to carry out unauthorized access to the RBS system, or they are not related to this computer crime. Investigation of undetectable malware is possible with the use of debuggers or in a virtual machine environment. It should be noted that modern malware has the definite algorithms for detecting and counteracting debuggers and virtual machines in its arsenal.

REFERENCES

3. Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States Catherine D. Marcum1 Georgia Southern University, USA George E. Higgins2 Richard Tewksbury3 University of Louisville, USA (www.cybercrimejournal.com/marcumetal2011julyijcc.pdf
4. Jurnal Ilmiah KURSOR Vol. 6, No. 3, Januari 2012, hlm.159-166
5. Deepesh Jain. Superresolution using Papoulis-Gerchberg Algorithm Digital Video Processing Stanford University, Stanford, CA.

.