ISSN NO: 2770-0003
Date of Publication: 22-10-2022

Analysis of Computer Crime Incidents

Radjabova Madina Shavkatovna
Teacher-intern of the "Cybersecurity and Criminalistics" department of Tashkent University of Information Technologies
Yusupova Surayo Muyasar's Qizi
Mehmonkhozhaev Azizbek Shukhratjon O'g'li
Information security students

Abstract: "Algorithms for predicting measures to ensure information security based on the analysis of computer crime incidents", computer crime, its types and reasons for committing were analyzed. In Maskur's article, a network traffic analysis algorithm generated several time series between different sets of infrastructure as a result of short-term forecasting and monitoring. If each observed value does not exist within the confidence interval, such information is called a risk, that is, an incident.

Keywords: Computer crime, use of banking services, DoS attack, hacking

Decree of the President of the Republic of Uzbekistan 2022

According to the Decree No. PF-60 dated January 28, preparation of information and analytical comments on the results of the implementation of the State Program in the new Development Strategy of Uzbekistan for 2022-2026, their publication in foreign languages and provision of wide distribution, Information and Mass Communications Agency, National Television and Radio Company of Uzbekistan and It is envisaged that the National Information Agency of Uzbekistan, together with the mass media, will regularly discuss the goals and objectives of the development strategy and the State Program in the mass media, including the Internet and social networks, and explain its content to the public.

Information protection should ensure prevention of damage caused by voluntary loss of information (theft, tampering, forgery). Information protection measures should be organized on the basis of current laws and regulations on information security and in the interests of information users. In order to ensure a high level of information protection, it is necessary to regularly solve complex scientific and technical tasks and improve protection tools. One of the most important problems in the modern world is the problem of the development of computer crime.

Computer crime is an illegal activity related to information resources, in which a computer is considered an object of crime or a subject of crime.

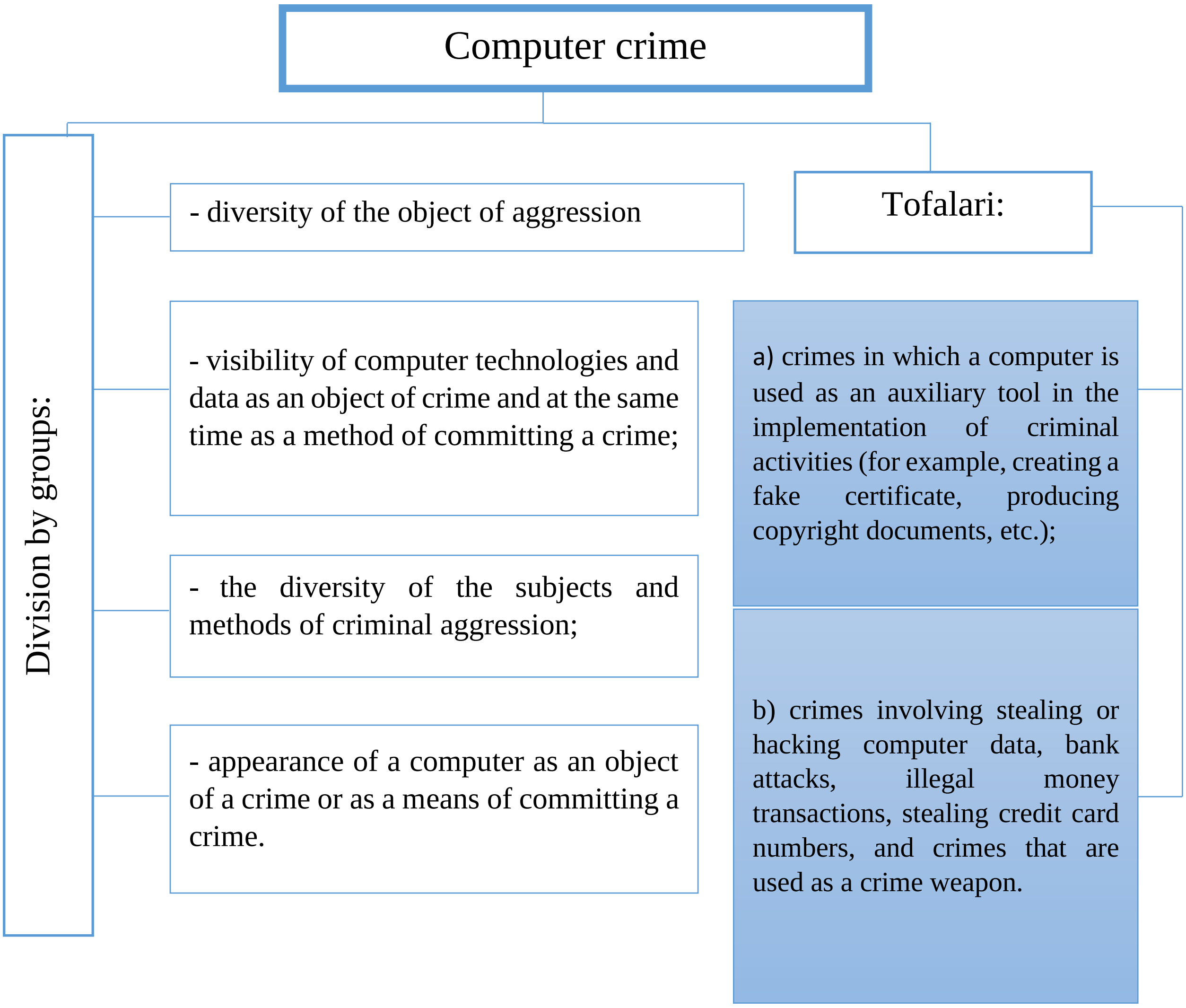
The main feature of computer crimes is the complexity of creating the composition of the crime and solving the problem of starting a criminal case. A computer is able to quickly change the form of data. As a result, it is difficult to identify the original source and the subject of the crime.

Using banking services over the Internet poses a great risk: the possibility of free transfer of funds to the attacker's account. Therefore, you should be especially careful about the security of the software you use and use only trusted sites and programs, while periodically fighting against computer attacks and preventing their occurrence.

1.2 Types of computer crime incidents and the essence of their methods

Because information resources are ubiquitous, and because businesses rely on digital media for confidential information, computer criminals know many ways to use computers to commit illegal activities. The cost and difficulty of identification attract buyers on the black market. Every year, companies that manufacture electronic components suffer multi-million dollar losses from the actions of cybercriminals. Software is also a target of crime. In fact, this type of computer crime is illegal if it is not provided with an appropriate license confirming the right to use it. Computer crime is classified as follows [Figure 1.2.1].

ISSN NO: 2770-0003
Date of Publication: 22-10-2022



Computer crime

Division by groups:

- diversity of the object of aggression

- visibility of computer technologies and data as an object of crime and at the same time as a method of committing a crime;

- the diversity of the subjects and methods of criminal aggression;

- appearance of a computer as an object of a crime or as a means of committing a crime.

Tofalari:

a) crimes in which a computer is used as an auxiliary tool in the implementation of criminal activities (for example, creating a fake certificate, producing copyright documents, etc.);

b) crimes involving stealing or hacking computer data, bank attacks, illegal money transactions, stealing credit card numbers, and crimes that are used as a crime weapon.

Figure 1.2.1. Classification of computer crime

Due to the large number of computer crimes, it is impossible to investigate them all. When investigating a crime, law enforcement and security agencies focus on the following facts:

- Type and degree of damage. Undoubtedly, violent computer crimes (compared to crimes involving only material damage) are more socially dangerous. Crimes that violate the rights of minors and other less protected subjects are also a priority.

- Spread. It is well known that the detection of a crime and the punishment of the criminal also have some effect on potential offenders. Therefore, it is more important to identify the types of crimes that occur more frequently than the types of crimes that occur less frequently.

- Number and qualifications of employees. Depending on how many employees there are and how skilled they are, certain computer crimes are expected to be investigated. A very complicated plan for starting an investigation will not always work.

- Jurisdiction. Investigating crimes that do not require the involvement of foreign law enforcement agencies is preferred. The fastest results are obtained from the investigation of localized crimes.

- Politics. Depending on the current political situation, certain types of computer crimes may be prioritized. Not because they are more socially dangerous, but because their disclosure leads to more PR exposure or more approval from the authorities. Only elements specific to the type of computer crime under consideration are described.

Online fraud can be seen in the example of some online store. It was found that this crime is widely used among businessmen for a number of reasons. In particular, it is characterized by low costs for the organization of trade. The cost of a website with a proper BACK-office is much lower than the cost of maintaining an actual retail space. In addition to fake online stores, fraudsters also use other excuses to receive payments:

- fake fundraising websites of charities, religious organizations, political parties and movements;
- spam mailing lists and websites asking for financial assistance based on a compelling story about a poor orphan, war victim, hostage, etc.;
- fraudulent online "banks" and "investment funds" promising interest on deposits;
- mailing lists and websites about alleged vulnerabilities and scams in payment systems that allow you to increase your money by transferring it to a special account (including, based on the fact that the victim thinks that he is being scammed, the other party becomes a victim of fraud);
- fake sites and mailing lists that offer remote work (which often refers to those who avoid the network) and demand some kind of "entry fee" under this pretext. All such crimes have the same forensic features and are associated with posting information on the Internet, communicating anonymously with the victim and receiving money from him, and then disappearing from the Internet.

Defamation, defamation and extremist activities on the Internet is a form of crime that consists in posting offensive, defamatory or extremist material on a public, usually popular, Internet resource. Resources can be: web forums and bulletin boards, web pages, newsgroup messages.

In some cases, the attacker is limited to one or two sources. Maybe it's because they're not professional or they can't judge the audience properly. Multiple sources cover many users at the same time. In other cases, information is placed on many resources at the same time, and its placement is repeated from time to time, as the advertising theory states. An attacker can independently implement a single location of data. For mass posting, he will need to hire professional spammers or find, prepare and operate suitable software for mass sending or spamming. Personal honor, dignity, business reputation, national and religious feelings are the subject of aggression. In some cases, the purpose of such a company may be to falsely accuse another person of defamation, insult, extremism, but this is rare.

A DoS attack or denial of service attack is one of the types of unauthorized access that leads to blocking of data and disruption of computers and their networks. Other types of unauthorized access (data copying, data destruction), as well as the use of malicious software, can be stages of a DoS attack. Such attacks are generally divided into two types, attacks that exploit any vulnerability in the attacked system and attacks that do not exploit vulnerabilities. In the second case, the specific "harmful factor" of the attack is the overloading of the resources of the attacked system - processor, RAM, disk, channel bandwidth.

Harassment is a crime in which the aggressor in one way or another is the victim

related to changing the appearance of a website, often its UI page. Technically, this can be done by getting write access to the directory where the web server data is stored. Hacking is often done by exploiting a vulnerability in the web server itself or in one of its CGI scripts. This happens when an attacker modifies a web page using a simple function under the account of one of the legitimate users. Hacking should be distinguished from attacking a DNS or spoofing a website by changing the DNS record for the victim's website. This is a different path, although the target of the attack may be the same. This phenomenon is very common. Thousands of such incidents are reported every month.

The reasons for the violation include:

- the desire to demonstrate one's skills in public;
- political, religious, other ideological motives;
- personal enmity, personal conflict with the victim or his employees;
- the desire to discredit the owner of the website, to damage his business reputation for the purpose of competition, to influence his capitalization for the purpose of stock speculation;
- showing the existence of a weakness in the software, the desire to draw attention to it. A potential criminal fits the model of a "hacker" or, more rarely, an "insider".

Malware analysts note a clear trend in the commercialization of malware.

ISSN NO: 2770-0003
Date of Publication: 22-10-2022

Even 5-7 years ago, almost all viruses and worms were created without an obvious mercenary purpose, they thought, because of bully intentions or ambitions. And today's malware is mostly for-profit. Their main types (according to their purpose) are as follows:

- Trojans to create zombie networks, which are then used to send spam, DoS attacks, organize phishing sites, etc.; often they are equipped with a self-reproduction mechanism;
- spyware, that is, worms and trojans designed to steal personal information - passwords and keys of payment systems, bank card details and other information that can be used for fraud or theft;
- so-called adware, that is, malicious programs that sneak into a personal computer and display unauthorized advertisements to the user (sometimes there is also a class of "law-abiding" adware, which is not only malicious, but also displays advertisements with the user's knowledge).
- rootkits that serve to increase user rights and hide their actions on a "broken" computer;
- logical bombs, which are designed to automatically destroy all sensitive information on a computer at a certain time or when certain conditions are met (if not met);
- so-called "ransomware" is a subtype of Trojan programs that sneak into a victim's computer and encrypt files.

List Of References:

1. Decree of the President of the Republic of Uzbekistan on the new development strategy of Uzbekistan for 2022-2026 2022
2. On the basis of the following article "Computer crime is becoming a real source of danger in our country" - Qilichev.U.V, the operative representative of the department for combating crimes in the field of information technologies, lieutenant colonel. 23.12.2019;
3. Fedotov N.N. DoSataki v Sethi. Introduction, tekushchaya practice and prognosis // magazine "Dokumentalnaya elektrosvyaz". 2015, No. 13 (http://www.rtcomm.ru/about/press/pa/?id=429).
4. Phishing Exposed. "Syngress Publishing",