EUROPEAN MULTIDISCIPLINARY JOURNAL OF MODERN SCIENCE
ISSN 2750-6274 https://emjms.academicjournal.io Volume: 26 | Jan-2024

Cyber Security and its Fundamentals

Axmetov Rustam Dilshotovich
Academy of the Armed Forces, Department of Internal Affairs, engineering and technical production cycle, lieutenant colonel

Annotation: Ransomware typically targets large commercial targets. However, random victims who are unable to repel a cyber attack also fall under their attacks. This article will talk about how malware can harm the life of an entire city, and even a country. This article provides information on cyber security, a summary of its worldwide research status and implications, and statistical sources.

Keywords: cyber security, information security, security, information, cyber attacks, organization security.

More and more often in modern everyday life you can hear the term “cyber attacks”. A cyber attack, in the narrow sense, is an attack on the computer security of an information system.

In a broad sense, a cyber attack is considered as a search for solutions, methods, the ultimate goal of which is to gain control over a remote system in order to destabilize it.

The state of information security in the field of state and public security is characterized by a constant increase in complexity, increasing scale and increasing coordination of computer attacks on critical information infrastructure facilities, increasing intelligence activities of foreign and domestic states in relation to the Republic of Uzbekistan, as well as increasing threats the use of information technologies in order to damage the sovereignty, territorial integrity, political and social stability of the Republic of Uzbekistan.

What is cyber defense? cyber defense is one of the new concepts that has come in recently and has various definitions given to it. In particular, he defined cyber defense as follows: cyber defense is a computationally based field of knowledge that combines technology, people, information and process to ensure actions in the presence of attackers. It includes the creation, implementation, analysis and testing of secure computer systems. Cyber defense is an interdisciplinary field of study that includes legal aspects, policy, human factors, ethics, and risk management. Fundamentals of cyber defense.

The Cyber Security Center named the main reasons for successful hacker attacks and the countries from which the majority of malicious activity originates.

In 2021, the Cyber Security Center identified more than 17 million cases of malicious and suspicious network activity in the national segment, emanating from the address space of the national segment of the Internet. The majority of this activity (76%) consists of participants in botnets, as follows from the Center’s Report.

According to the document, last year 100,015 domains were registered in the national segment of “Uzbekistan.uz”, of which about 38,000 are active. Of the active domains, only 14,014 are secure, that is, they have an SSL security certificate. In other cases, the certificate is either expired (613) or missing.

It is noted that the bulk of malicious and suspicious network activity came from users of

National operators and providers.

Using the Center's web application protection system, more than 1.3 million cyberattacks committed against national segment websites were identified and repelled. The largest number of cyber attacks were carried out from the territory of Uzbekistan, Russia, Germany, Great Britain and the USA.

As part of the secure operation of websites of government agencies (24-hour monitoring of events and security incidents), 636 security events were identified in 2021, which amounts to more than 1 million minutes of unavailability (downtime) of websites of government and economic management bodies, local government authorities and others organizations.

Based on the results of monitoring cybersecurity incidents committed against websites of the ".uz" domain zone, 444 incidents were recorded, of which the largest number were unauthorized downloads of content – 341 and unauthorized changes to the main page (Deface) – 89.

In addition, based on the results of the investigation of cybersecurity incidents, the main causes and methods of successful hacker attacks were identified:

- the presence of vulnerabilities in web applications, in particular due to their untimely updating (72%);
- use of weak passwords (25%).

Moreover, in 97% of cases, the sources of illegal activity are address spaces of foreign countries. In particular, the largest number of cases of unlawful activity are associated with the United States, Indonesia, the Netherlands, Romania, Algeria and Tunisia.

The damage from hacker attacks committed around the world in recent years ranged from $300 billion to $1 trillion. In 2017, Russia took second place in the number of cyber attacks - 10% of all global cyber attacks occurred. The data presented clearly demonstrates the scale and reality of the threat.

In Kazakhstan, the number of attacks using such programs from July to September 2022 reached almost 600 thousand. The average damage from a cyber attack for SMB is $105 thousand, for Enterprise - $1 million. 71% of attacks were financially motivated

Computer forensics is involved in the development of recommendations for the prevention and investigation of cybersecurity incidents, actively analyzing their content, developing response measures and ways to prevent them.

If previously the traditional understanding of cyber attacks included DOS and DDOS attacks1, today cybercriminals have radically changed their content.

Recent years have seen a steady increase in the adoption of digital technologies and online activity around the world. Digitalization is becoming an integral part of public life, new digital formats of interaction are emerging, the expert writes. - The number of Internet users has more than doubled over the past 10 years, rising from 2.18 billion at the beginning of 2012 to 5 billion in July 2022 (63.1% of the world's population). Research shows that on average each user spends almost 7 hours a day on the Internet.

Wide Internet coverage and digitalization provide a synergistic and multiplier effect to the development of the digital economy.

According to estimates by the United Nations Industrial Development Organization (UNIDO), in 2021 the share of the digital economy in global GDP was about 15.5%. It is predicted that in the medium term the level of digitalization of the global economy will exceed 40%. Already today, almost 60% of Internet users of working age make purchases online every week.

Global revenues associated with online purchases of “consumer goods,” including food, clothing, electronics and other household items, increased by more than half a trillion dollars during 2021, reaching a total of $3.85 trillion.

However, the rapid digitalization of the life of society, business and the state gives rise to a number of objective problems in the field of cybersecurity. According to experts, in 2021 the number of cyber attacks in the world increased by 50% compared to 2020. Damage from cybercrime in 2021 exceeded $6 trillion, up from $3 trillion in 2015.

In 2021, among the most attacked industries in the world, the education and research sector took first place - 1605 (75% increase in attacks compared to 2020). There were 1,136 attacks against government and defense organizations (+47%); communications sector – 1079 (+51%); healthcare – 830 (+71%).

The topic of international information security (IIS) entered the Shanghai Cooperation Organization (SCO) agenda over 15 years ago and has since become one of the most visible and significant areas in the organization’s activities.

The document also laid down a common terminological and conceptual framework for the SCO, which recorded a common understanding of such basic concepts as “the development and use of information weapons, the preparation and conduct of information warfare,” “information terrorism,” “information crime” and others.

At the same time, “information security” in the SCO is defined as “the state of protection of the individual, society and state and their interests from threats, destructive and other negative influences in the information space.”

The adoption of the above documents and a unified approach allowed the SCO to lead international efforts to develop universal rules for the responsible behavior of states in the information space and to prevent the use of ICT for illegal purposes.

Thus, in 2011, four SCO member countries (Russia, China, Uzbekistan, Tajikistan) presented to the UN their vision of problems related to ensuring information security in the Rules of Conduct of States in the field of ensuring information security, developed and sent to the UN Secretary General in a letter.

Although a regulatory document regulating the interaction of states in ensuring information security has not yet been adopted at the UN level, the vision of problems in this area sent by the SCO member countries is used in the activities of the UN Open Working Group on Advances in the Field of Information and Telecommunications in the context of international security.

Over the past 10 years, a number of conceptual documents on international investment security have also been approved within the SCO. Following the results of the summit of the heads of the SCO member states, held under the chairmanship of Russia in November 2020, an important document was adopted - the Joint Statement of the Heads of the SCO member states on cooperation in the field of ensuring international security.

This document is intended to focus the attention of the world community on the inadmissibility of using modern ICTs for purposes incompatible with the tasks of maintaining international peace, security and stability.

In 2021, following the anniversary summit in Dushanbe, 30 documents were signed. Among them is the Plan of interaction between the SCO countries on issues of ensuring international information security for 2022-2023, developed at the initiative of Uzbekistan and Russia.

Information security is becoming increasingly important in the overall system of national security of Uzbekistan and regional stability. At the same time, the cross-border nature of challenges and threats in this area requires the constant development of joint actions at the bilateral, regional and international levels.

In this regard, President Shavkat Mirziyoyev, speaking at a meeting of the SCO Council of Heads of State in Dushanbe, put forward an initiative to hold the first SCO expert forum on information security.

In order to prevent the active recruitment of citizens of SCO member states into zones of terrorist activity, 6 transportation channels have been blocked, the bank accounts of more than 5 thousand individuals and 24 terrorist financing channels have been blocked.

In this regard, the organization of an expert forum will contribute to the practical implementation of the SCO Plan for interaction in the field of international information security and the use of scientific potential in countering common threats and challenges in this direction.

Today, preparations for this forum, which is organized by the Institute of Strategic and Interregional Studies under the President of the Republic of Uzbekistan with the support of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan, as well as the Executive Committee of the SCO Regional Anti-Terrorism Structure, are being completed.

The relevance of this topic is confirmed by the representative composition of the participants. The forum is scheduled to include SCO Secretary General Zhang Ming, Director of the SCO RATS Executive Committee Rustam Mirzayev, as well as leading experts from relevant ministries and departments, scientific, academic and analytical circles of the SCO member states.

The event involves discussing a wide range of issues, including cooperation in the fight against threats in the information space, ensuring human rights in the fight against cyber threats, expanding the role of the SCO and strengthening interaction between states in this area.

It should be noted that the SCO member states have significant potential in ensuring information security. Thus, according to the Global Cybersecurity Index for 2021, Russia and India are in the top ten, while China and Kazakhstan are among 40 countries. The index takes into account legal, technical and organizational measures, as well as development potential and cooperation with other countries.

In our opinion, the expert forum will allow us to take coordinated and complementary measures in the field of information security, which will significantly increase the effectiveness of the work carried out in this area within the SCO states.

However, one cannot fail to note the role of computer system users in preventing cyber attacks, because many computer security incidents become possible precisely through their fault (use of outdated software, switching to unknown external resources, etc.). To minimize the risk of cyber attacks on the security of a computer system, the user must follow basic cybersecurity rules. These rules represent a set of forensic preventive knowledge formed based on the analysis of modern cyberattack incidents:

It is necessary to use only licensed software with the possibility of timely updating. Even large companies often use pirated versions of software. It would seem that this is a savings item in the organization’s budget. However, it is necessary soberly assess risks. The damage that can be caused by a cyber attack is disproportionate to the money saved on licensed software;

It is necessary to ensure that antivirus programs are up to date;

You cannot follow external links received from unknown users;

It is recommended to delete suspicious emails from unknown users unread. Having opened it, do not follow the links to unknown resources indicated in it, do not open or download attachments;

The main rule of corporate security: one computer - only for working with the bank serving the organization and for nothing else;

Electronic storage media should not be used in unknown devices and vice versa;

It is advisable to regularly backup files to an external storage device that is not permanently connected to the computer system. If attackers attack the system data, you can always continue working with the backup copy;

It is recommended not to use the same password for different applications, and also not to use personal data as a password;

If the computer system is nevertheless attacked, do not rush to transfer funds to the attackers, since there is no guarantee that the malicious software will be permanently removed from the computer and the extortion will not happen again, and also do not hide the computer security incident that has occurred, as from management, and from law enforcement agencies, do not try to reinstall the system yourself. It is necessary to immediately notify law enforcement agencies and take all measures to preserve and record traces of the cyber attack.

Compliance with the presented rules will protect the computer system of a particular user, will have a significant role in strengthening the information security of the Republic of Uzbekistan as a whole, and will also help in recording traces and in investigating such incidents.

Despite the scale of cyber threats, with coordinated actions, it is possible to successfully counter them. If the state is fighting cybercriminals through legislative and organizational measures, then each user has the power to make an invaluable contribution to the common cause – to know and follow the basic rules of cybersecurity, promptly and competently responding to problems in the operation of the computer system.

List of used literature

1. Кибератака-URL:http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E0%F2%E0%EA%E0/
(Дата обращения 5 мая 2017 г.).
2. https://securitymedia.org/tags/Kiberataki.
3. https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0.