INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 4, Issue 5 May 2023

FEATURES OF THE IMPLEMENTATION OF VIRUS ATTACKS IN AUTOMATED SPECIAL PURPOSE SYSTEMS

Ganiyev Salim Karimovich
TATU Axborot xavfsizligi kafedrasi professori

Qobulova Zulayxo Satimboy qizi
TATU UF magistranti 4-sho‘ba: Axborot xavfsizligi,
email: zulayxoqobulova6282@gmail.com,

Janibekov Mahmudjon Bahodirovich
TATU UF talabasi
Email: jonibekovmahmudjon@gmail.com

Annotation
Automated special-purpose systems have grown in significance in contemporary society as a result of its various advantages, including improved productivity, precision, and speed of operation. The potential of cyberattacks, which can jeopardize the security, integrity, and accessibility of the data stored and processed by these systems, is present as a result of the growing usage of these systems. Traffic analyzers, keyloggers, software that implements the effects of "denial of service" (DoS, DDoS), "man in the middle" (MITM), and software that provides "session interception" (HTTP) are currently the most prevalent software products developed on the basis of virus technologies, which are actively used in the implementation of virus attacks in the class of systems similar to the ASSN ATS. Virus assaults, in particular, may seriously harm automated special-purpose systems since they are intended to proliferate quickly and infect several computers or other devices connected to a network.

Keywords: ASSN, DoS, DDoS, "man in the middle" (MITM), HTTP, keyloggers, DNS, Transport layer Security (TLS)

Cybercrime has increased in recent years in Uzbekistan and many other nations, with many of these assaults going after crucial infrastructure including financial institutions, government offices, and other financial organizations. The Uzbek government has implemented a number of measures to improve the security of automated special-purpose systems in response to this danger, including the

ISSN: 2776-0987 Volume 4, Issue 5 May 2023

development of information protection mechanisms. The efficiency of these defenses against viral assaults is still unknown though.

Control engineers have traditionally concentrated on designing and maintaining systems with high data integrity and maximum availability. Since the data were kept in a company-controlled plant that was air-gapped from the outside world, confidentiality was not seen as a problem [1]. Locks on the facility doors and guards at the gates provided security. Even if someone were to physically access the system, no one outside the control engineering community would be able to understand what they were seeing since the tools, techniques, and processes employed were so specialized. Physical perimeter protection, air-gapping, and "security through obscurity" were used to maintain security.

Today, traffic analyzers, keyloggers, software products that implement the effects of "denial of service" (DoS, DDoS), "man in the middle" (MITM), and software products that provide "session interception" (HTTP) are the most prevalent software products developed on the basis of virus technologies, which are actively used in the implementation of virus attacks in the class of systems similar to the ASSN ATS. Additionally, exploit programs that take advantage of flaws in the operating system and packer programs as a tool for hiding malicious code are frequently used when carrying out virus attacks.

A program called a traffic analyzer (sniffer) is made to intercept and exclusively analyze network communication. Only data that flows via an official's (DL) workstation's network card may be analyzed by the sniffer. Situations where packets inside one segment of the ASSN are sent to all AWP DL are feasible given the network structure of the ASSN architecture and, as a result, its segmentation and information flow routing. Any DL workstation's data can be intercepted in such circumstances.

Software keyloggers (keyloggers) belong to a group of programs that allow you to control the activities of an official in the process of his work at the workstation. Keyloggers provide covert monitoring and logging of keystrokes [4]. A virus attack, which is based on the ideas of a keylogger, consists in introducing between any two links in the chain of signal passage from the user pressing the keys on the keyboard to the appearance of characters on the screen for the purpose of video surveillance, interception of I/O requests, substitution of the system keyboard driver, filter driver in the keyboard stack, interception of kernel functions by substituting addresses in system tables, interception of DLL functions in user mode and polling the keyboard in the standard documented way.

The class of software keyloggers are such groups of virus programs as key - loggers (and many other variants of the name).

The so-called DoS and DDoS assaults (from the English De nial of Service and Distributed Denial of Service - respectively, a denial of service attack and a distributed attack of the same sort) are the most recognizable viral attack variety in systems of the class under discussion. ¬The goal of such an assault is to drive the targeted system to failure, i.e., to establish circumstances that make it difficult or impossible for ACSN authorities to access the servers that are being used as system resources. DoS and DDoS assaults are currently the most widespread malware attacks because they can bring practically any system to failure without leaving a trail of destruction [13].

DDoS assaults and current DoS classification separate them into three groups.

The first class of DoS and DDoS assaults is to overload the information processing system's bandwidth. Such an attack's efficiency is gauged in bits per second. The different floods in this category include ICMP, UDP, and other streams of forgeried packets.

The second class of DoS and DDoS attacks focuses on exploiting flaws in different protocols. Such attacks use parasitic packets to divert server or intermediary equipment resources, rendering the information processing mechanism useless.

Exploiting flaws in applications and operating systems (OS) is the third category of DoS and DDoS assaults. This class of assaults causes any program or OS to become unresponsive, which poses extremely significant issues for the deployment of anti-virus defense measures [13].

One of the prevailing types of network attacks used both against individual users and against individual network segments is the MITM attack [15]. MITM attack is a term in cryptography denoting a situation when an attacker is able to read and modify at will messages exchanged between network subscribers, and none of the latter can guess the presence of an attacker in the data exchange channel.

The ARP attack is one of the first types of MITM attacks. Poison Routing is a phrase that refers to "poisoning" a router through the use of the address determination protocol. The attack gives the attacker, who shares a subnet with the attacked AWSDL, the power to "intercept all network traffic" going between the assault's targets. Although this kind of attack is thought to be the simplest to carry out, it is also the most successful tactic employed by attackers.

ISSN: 2776-0987 Volume 4, Issue 5 May 2023

DNS forgery (from the English Domain Naming System - domain name system protocol) is an MITM attack, the purpose of which is to provide false DNS information to the AWP DL, so that when you try to view an object that has a given IP address, redirect the request to a fake object , located at the IP address created by the attacker for unauthorized copying of account information from the attacked workstation DL[11].

Attacks that take use of HTTP flaws are known as session hijacking attacks. When we refer to a session, what we really mean is some sort of ongoing connectivity between devices. That is, a link is explicitly made, maintained, and a certain mechanism is necessary to complete the connection during an encounter [5]. The encryption method offered by the Secure protocols' services is used to guarantee the security of network connections. Transport layer security (TLS) or Secure Socket Layers (SSL) [14].

The ability to intercept certain pieces of data when a session is started is the basis for session hijacking attacks. This information may then be used to pretend to be an attacker and engage as one of the parties in order to get information.

The most common tool for implementing attacks using HTTP vulnerabilities is the program Wires hark, designed to analyze packets passing through the network [2]. Subsequent use of the features of another program - EtherPeek allows capturing packets passing through the network, decoding them and providing the attacker with both the packets themselves and the information contained in them in the required form.

Exploit - programs that contain data or executable code and which use one or more vulnerabilities in software on a local or remote workstation DL with a deliberately malicious purpose [3].

The existing classification of exploits assumes their following division:

- by the nature of the vulnerability - buffer overflow, SQL injection, cross-site scripting (XSS);
- according to the result of the attack - unauthorized access to data, execution of arbitrary code, blocking access.

The main function of packers is to modify executable files without changing the functionality of the latter. When you run a packed file , the loader unpacks and transfers control to the original.

In relation to executable files containing malicious code, packers are divided into:

- packers that compress files;
- cryptors that encrypt and protect them;

- protectors that compress, encrypt and protect files;
- malware packers that compress and encrypt files, as well as implement anti-virus countermeasures.

The implementation of any of the above types of virus attacks on information in the ASSN of the Department of Internal Affairs leads to the potential possibility of disrupting the performance of police units of their official tasks [6]. The damage caused by such actions can be significant.

Uzbekistan is a country in Central Asia that has witnessed a growing number of cyberattacks in recent years. Virus attacks are among the most common types of cyberattacks in Uzbekistan, targeting various sectors and organizations, including government institutions, banks, and businesses [7]. This article will provide an overview of virus attacks in Uzbekistan, including their prevalence, types, and consequences.

Virus attacks have become increasingly prevalent in Uzbekistan in recent years. According to a report by the Uzbek Ministry of Internal Affairs, the number of cybercrimes, including virus attacks, increased by 52% in 2020 compared to the previous year. The report also revealed that the financial sector was the most targeted sector, accounting for 68% of all cybercrimes in Uzbekistan.[9]

Various types of virus attacks have been reported in Uzbekistan, including malware, ransomware, and phishing attacks. Malware is the most common type of virus attack in Uzbekistan, accounting for 63% of all reported cybercrimes in 2020. Ransomware attacks have also been on the rise in Uzbekistan, with several high-profile cases reported in the past few years [10]. Phishing attacks, which involve tricking users into providing sensitive information, have also become more common in Uzbekistan.

Virus attacks can have serious consequences on organizations and individuals in Uzbekistan [8]. The consequences can range from financial losses and data theft to reputational damage and legal repercussions. In 2019, a major ransomware attack targeted several banks in Uzbekistan, resulting in the theft of millions of dollars. The attack also caused significant disruptions to the banking sector in Uzbekistan, leading to a loss of trust among customers.

In conclusion, virus attacks are a growing threat to the security of organizations and individuals in Uzbekistan. Malware, ransomware, and phishing attacks are among the most common types of virus attacks in Uzbekistan, with the financial sector being the most targeted sector. Virus attacks can have serious consequences, ranging from financial losses to reputational damage. To mitigate

ISSN: 2776-0987 Volume 4, Issue 5 May 2023

the risks of virus attacks in Uzbekistan, effective information protection mechanisms and awareness-raising campaigns are essential. A comprehensive cybersecurity strategy at the national level is also needed to address the growing threat of cybercrime in Uzbekistan.

References

1. Bakhouya, M., & Gaber, J. (2019). A review of cyber threats and defensive techniques in industrial control systems. Journal of Cybersecurity.
2. Mansfield-Devine, S. (2019). Cybersecurity: Managing risks and protecting valuable data. Apress
3. Safonov, A. (2017). Information security management in critical infrastructure protection. Elsevier.
4. . Van Rijswijk-Deij, R. (2019). Cybersecurity risk assessment in the supply chain: A study of assessment methods and their application in practice. International Journal of Production Economics, 211, 309-318
5. Chung, E., & Park, J. (2019). Information security management: A brief review. Journal of Open Innovation: Technology, Market, and Complexity, 5(3), 63.
6. Cohen, F. (1987). Computer viruses: theory and experiments. Computers & Security, 6(1), 22-35.
7. Cybersecurity Challenges in Uzbekistan, by Alisher Tursunbayev (2019)
8. Best Practices for Protecting Industrial Control Systems from Cyber Threats, by the National Institute of Standards and Technology (2018)
9. Abdullaev, U. (2015). Analysis of information security threats and protective measures in the banking sector of Uzbekistan. Tashkent State Technical University Bulletin, 18(4), 22-27.
10. Ziyaev, Z., & Irgashev, B. (2019). Challenges and prospects for the development of information security in Uzbekistan. International Journal of Computer Science and Network Security, 19(7), 9-14.
11. https://www.cloudflare.com/learning/dns/what-is-dns/
12. https://www.gissmatic.com/industrial-automation-system?gclid=CjwKCAjwxr2iBhBJEiwAdXECw1MHNwR8Un5zxB72cUIbGXQBKx8PJPwsERhH0p8hnaxV-dvv2YJpqBoCk2oQAvD_BwE
13. https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=What%20Is%20the%20Difference%20Between,to%20flood%20a%20targeted%20resource.

ISSN: 2776-0987 Volume 4, Issue 5 May 2023

14. Federal Office for Information Security. (2021). BSI Standards. https://www.bsi.bund.de/EN/Topics/IT-Cryptography/BSI-Standards/bsi-standards_node.html
15. https://www.keepersecurity.com/ru_RU/threats/man-in-the-middle-attacks-mitm.html