A model of a DDoS attack scenario on elements of specialized information technology and methods of combating cybercriminals

Mykola Stetsyuk[1,*,†], Viktor Cheshun[1,†] ,Yuriy Stetsyuk[1,†] , Oleksandr Kozelskiy[1,†],and Abdel-Badeeh M. Salem [2, †]

[1] Khmelnytskyi National University, 11 Institutska Street, Khmelnytskyi, 29000, Ukraine
[2] Ain Shams University, Egypt

Abstract

In this article, we present a scenario model of a DDoS attack on elements of specialized information technology. The proposed model ensures the finding of initial data for a comprehensive assessment of the stability of the functioning of a specialized information system operating under the conditions of the action of malicious software on its network elements.

The approbation of the model and the simulation of the DDoS attack process in the environment of the MathCAD application program allowed us to conclude that the proposed model allows adequately, with a sufficient level of detail and flexibility, to display the simulated process, is sensitive to changes in input data, and allows obtaining consistent simulation results. as well as identify appropriate directions for ensuring the viability of specialized information systems. The resulting model allows you to estimate not only the potential capabilities of malicious software, but also the time it takes to implement a DDoS attack on network elements of information systems.

The work also provides practical advice regarding the inclusion in the architectures of developed specialized information systems of hardware to prevent malware attacks.

Keywords

cybersecurity, malware, DDoS attack, attack scenario, stochastic network, software vulnerability

Introduction

Ensuring information security is an important aspect of the development of modern society. Due to the fact that confidential and secret information is processed and stored in information systems, this problem is relevant in the design and operation of specialized information systems [1].

The difficulty of ensuring stable operation of modern specialized information systems (IS) has recently been constantly increasing due to more frequent cases of attacks implemented by malicious software [2,3]. These attacks are accompanied, as a rule, by information influences on IS elements. Information influences are carried out by the offender using computer attacks, which aim to make the functions implemented by specialized IS unavailable or difficult to access. The result of the influence of malicious software is the blocking of commands, work failures or the complete impossibility of IS operation [2].

IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.
† These authors contributed equally.
mykola.stetsiuk@khmnu.edu.ua(M. Stetsiuk); cheshunvn@khmnu.edu.ua(V.Cheshun); yuriy.stetsuk@khmnu.edu.ua(Y.Stetsiuk); oleksandr.kozelskiy@khmnu.edu.ua(O. Kozelskiy); abmsalem@yahoo.com (Abdel-Badeeh M. Salem);
0000-0003-3875-0416 (M. Stetsiuk); 0000-0002-3935-2068 (V.Cheshun); 0000-0001-9880-2666 (Y.Stetsiuk) ; 0000-0002-4104-745X (O. Kozelskiy); 0000-0003-0268-6539 (Abdel-Badeeh M. Salem)

In works [1, 4 - 7], the most famous types of computer attacks are given, where DDoS attacks (Distributed Denial of Service) occupy a special place. The prevalence of this type of attacks is due to the simplicity of their implementation and the serious consequences of their implementation.

DDoS attacks can be implemented at almost any level of the ISO/OSI network protocol stack model used by computer systems for communication [8 - 12].

DDoS attacks on levels 3-4 and 7 of the ISO/OSI model are the most popular among criminals [11, 13]. This is explained by the following reasons.

At the 3rd and 4th levels of the ISO/OSI model, the object of attack is the elements of the network infrastructure, such as routers and others. A DDoS attack at the third level aims at the transmission of a large volume of data (flood). The attack at the fourth level is carried out with the aim of slowing down, and with the maximum effect - blocking the operation of the web server. Loading the access channels of the web server will eventually lead to the blocking of access of the client's automated workplaces to the resources provided by the specialized IS.

Even more dangerous is a DDoS attack at the 7th level of the ISO/OSI model [11]. The reason is that it is directed to the application server, which causes it to become overloaded and, to a large extent, makes the functions of the specialized IS unavailable for its automated workplaces. This type of attack is particularly difficult to implement and is characterized by high transparency for anti-virus software due to their similarity to useful traffic.

According to the National Cyber Security Coordination Center of Ukraine [1], in 2023, every fifth Ukrainian company or state organization experienced a DDoS attack. At the same time, attacks most often targeted large banks (27%), medium and small businesses (15%). DDoS attacks were aimed at creating problems in the operation of the main pages of the websites of both state institutions (including educational institutions - the authors of the article directly observed and investigated the actions of attackers on the electronic resources of the Khmelnytskyi National University), and businesses (39% of attacks), output failure of communication services, mail, communication, as well as functions that allow the user to enter the IS (19%).

Experts of the National Cyber Security Coordination Center note that last year Ukraine took the leading place in the world in terms of the number of DDoS attacks on its specialized systems for various purposes.

Thus, the task of assessing the capabilities of malicious software to carry out DDoS attacks on specialized IS is, along with others, one of the most pressing scientific tasks today.

One of the most difficult and important tasks for evaluating capabilities, detecting and countering the effects of malicious software is the selection of a mathematical model adequate for the purposes [14,15]. Today, a large number of cyber security models are used in information security tasks: models of a legitimate user and violator [12, 20], models of attacks [3] and their detection [14], adaptive models of intrusion detection and countermeasures systems using methods of intelligent data analysis (multilayer direct propagation networks, radial base networks, recurrent networks and self-organizing maps, etc.) [15 - 17].

This work is devoted to the construction and consideration of a model of the process of a computer attack of the type "Distributed Denial of Service" on the elements of a specialized information system. The resulting model allows you to estimate not only the potential capabilities of malicious software, but also the time it takes to implement a DDoS attack on network elements of information systems.

2. A problem to be solved

Today, one of the most convenient technologies for building computer networks of organizations and companies is the MPLS network technology [18, 19]. It combines the technique of virtual channels with the functionality of the TCP/IP stack. This network property is achieved by having the same LSR (Label Switch Router) network device act as both an IP router and a virtual circuit switch. This makes it possible to combine territorially separated

parts of information systems of companies into single local networks, which is extremely convenient. That is why the MPLS technology is chosen as the basic one when creating a mathematical model of a DDoS attack.

We conduct research for the MPLS network, which consists of routers, switches, servers and client automated workstations of some specialized IS, which functions under the influence of DDoS attacks.

A DDoS attack is preceded by some preparatory actions. To a large extent, the success of the attack depends on the number of computers that make up the Bot network. Unfortunately, today, such networks not only exist, but are also provided by criminals for rent. Therefore, today the attacker has the opportunity to immediately focus directly on the object of the attack.

As a rule, an attacker needs to conduct reconnaissance of the network of the information system chosen for the attack by performing a number of steps. For this, he needs to determine its active elements, type and versions of operating systems, as well as network services. We denote the average time spent on this as $t_{def.elem}$,$t_{def.OS}$ and $t_{def.of.serv}$ with distribution functions M(t), D(t), L(t), respectively. The attacker successfully implements these actions with probabilities$P_{def.elem.}$, $P_{def.OS.}$ and $P_{def.of.serv}$. The calculation of these probabilities can be carried out according to the method proposed in the description of the mathematical model of the information security violator [20].

If the attacker failed to set at least one of the network parameters, then his attempts will be repeated with probabilities $1 - P_{def.elem}$, $1 - P_{def.OS}$ and $1 - P_{def.of.serv}$, respectively, where $t_{aver.repet}$ is the average repetition time with the distribution function Z(t).

In the next step, the attacker analyzes the received data and determines the vulnerabilities of the elements of the attacked network in the spent average time $t_{ident.vul}$ with the time distribution function K(t) and determines the connection requests to the server - attack targets in the average time $t_{request}$ with the time distribution function Y(t) and the probability connecting to the target server $P_{connect.}$, and receiving a response about its status after time $t_{get.status}$ with a distribution function U(t). If access is not obtained, the attacker sends a second request in the average time $t_{rep.reg}$ with the distribution function V(t).

To launch a DDoS attack, the offender activates the Bot network , indicates the object of the attack (Fig. 1). Each bot computer starts sending service requests to the attack object with an average time $t_{seg.reg.}$ with a time distribution function W(t).

In the case of successful implementation of all steps, the attacker sends a large number of anonymous false connection requests through the Bot-network controlled by him, which lead to the overflow of the server's RAM. Server overload, in turn, blocks the access of legitimate client automated jobs of the attacked specialized IS. Such blocking of IS servers is carried out during the average time $t_{lock.}$ with the distribution function N(t).

The average time $T_{impl.aver.}$ and the distribution function F(t) of the time of implementation by the offender of the DDoS attack are to be determined. At the same time, we will assume that the implementation time of all stages is random and characterized by an exponential distribution, and all probabilities take the same values.

3. DDoS attack scenario model

Let us present the process of organizing a DDoS attack in the form of a stochastic network (Fig. 2).

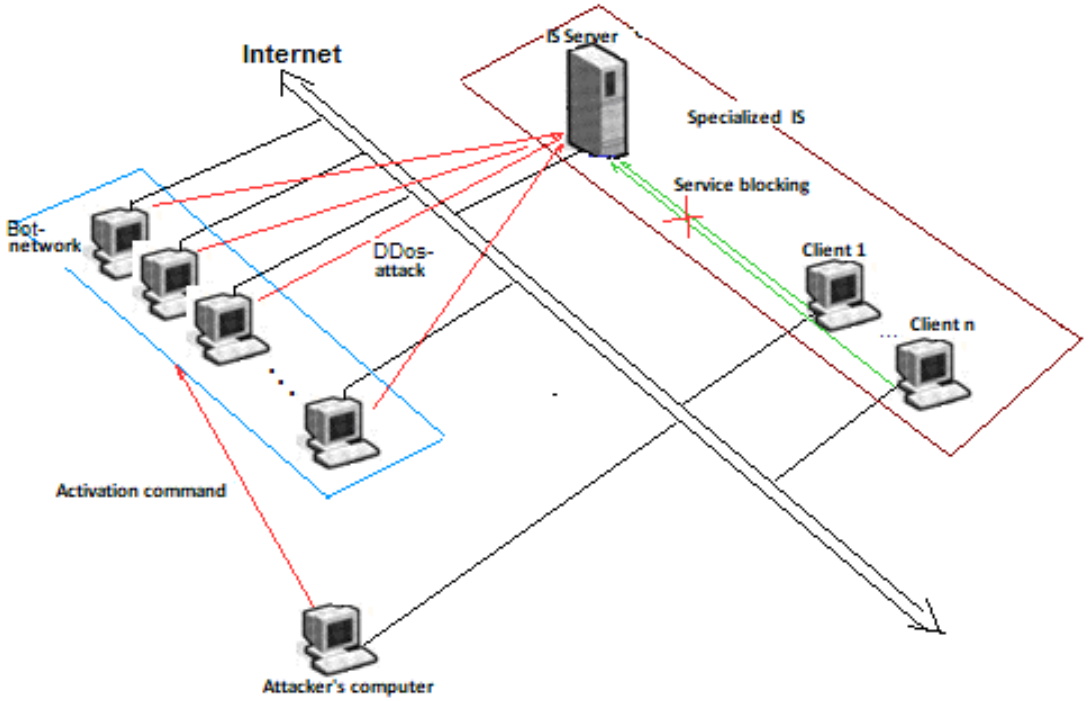

Figure 1: The principle of organizing and running a DDoS attack.

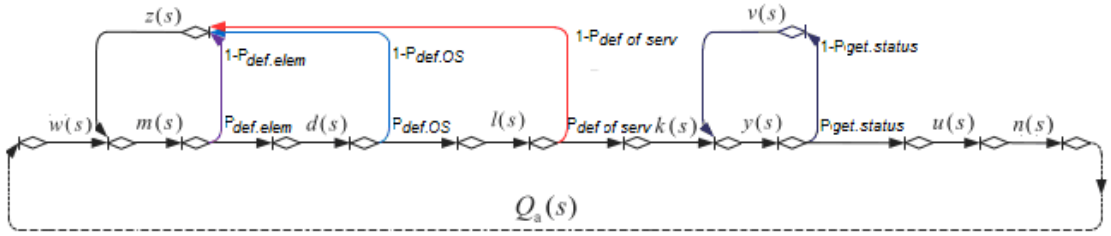

Figure 2: Stochastic network of a computer DDos attack.

The DDOS attack scenario may include a parcel in a special non-correal request server for an average time $t_{inv.reg}$ with probability $1 - P_{inv.reg.}$.

This scenario is carried out under the hypothesis that the attacked server contains configuration errors or vulnerabilities known to the attacker. Successful implementation of the attack script can cause the server to "hang" due to a buffer overflow, for example.

Taking into account the given scenario of a DDoS attack, its stochastic network will take the form shown in Fig. 3.

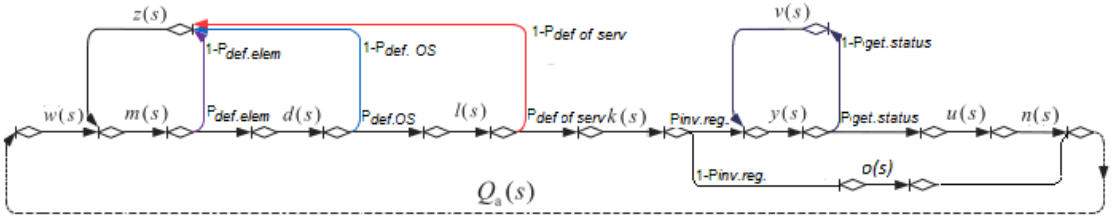

Figure 3: Stochastic network of a computer DDos attack with an incorrect request.

Note that here: *w(s), m(s), z(s), d(s), l(s), k(s), y(s), v(s), u(s), n(s)* and *o(s)* are the Laplace-Stiltjes transformations of the corresponding distribution functions specified in the problem statement and defined as:

$$ri(S) = \int_0^{\infty} e^{-st} d[Ri(t)] = \frac{ri}{ri + s} \quad (1)$$

where:

ri - the equivalent transformation function of the ith distribution function W(t), M(t),..., O(t);

Ri(t) is the i-th distribution function of the average time t for the i-th stage of a Ddos attack;

s is the change defined on the complex plane S, where the transformation $ri(S)$ exists.

To determine the equivalent function, we close the input and output of the stochastic network (Fig. 2 and Fig. 3) with a fictitious branch $Qa(s) = \frac{1}{Q(s)}$ where:

Q(s) is the equivalent function of the real resulting branch of the stochastic network (Fig. 2)

In our further steps, we will adhere to the DDoS attack scenario presented in the form of a stochastic network in Fig. 2.

Let's define loops of the first and second orders in the stochastic network model with the assumption that the values of all probabilities $P_{def.elem.}$, $P_{def.OS}$, $P_{def.serv.}$, $P_{state.defin}$ are equal and equal to some value P_n.

Then the loops of the first order Lk.n, where k = 1, n = 1 - 4 will be defined as:

$$L1.1 = m(s) \cdot (1 - P_n) \cdot z(s);$$

$$L1.2 = m(s) \cdot d(s) \cdot P_n \cdot (1 - P_n) \cdot z(s);$$

$$L1.3 = m(s) \cdot d(s) \cdot l(s) \cdot P_n^2 \cdot (1 - P_n) \cdot z(s);$$

$$L1.4 = y(s) \cdot (1 - P_n).$$

Accordingly, loops of the second order *Lk.n*, where *k*=2, *n*=1 - 3:

$$L2.1 = m(s) \cdot (1 - P_n^2) \cdot z(s) \cdot y(s) \cdot v(s);$$

$$L2.2 = m(s) \cdot d(s) \cdot P_n \cdot (1 - P_n^2) \cdot z(s) \cdot y(s) \cdot v(s);$$

$$L2.3 = m(s) \cdot d(s) \cdot l(s) \cdot P_n^2 \cdot (1 - P_n^2) \cdot z(s) \cdot y(s) \cdot v(s).$$

Using Mason's equation:

$$H = 1 + \sum_{i=1}^{k} (-1)^k \cdot Q_k(s) = 0 \quad (2)$$

where $Q_k(s)$ are the equivalent functions of loops of the kth order, we get the equivalent function of the stochastic network:

$$Q(s,P_n)=\frac{w(s)\cdot m(s)\cdot d(s)\cdot l(s)\cdot k(s)\cdot y(s)\cdot u(s)\cdot n(s)\cdot P_n^4}{1-m(s)\cdot(1-P_n)\cdot z(s)\cdot\left[1+d(s)\cdot P_n+d(s)\cdot l(s)\cdot P^2\right]-y(s)\cdot\left(1-P_n\right)}\cdot \frac{1}{v(s)\cdot\left[1+d(s)\cdot P_n+d(s)\cdot l(s)\cdot P_n^2\right]} \quad (3)$$

By definition, this is a characteristic function, so its differentiation will allow finding the first and second initial moments of the random time of the implementation of a DDos attack:

$$M_1(s,P_n)=-\frac{d}{ds}\left[\frac{Q(s,P_n)}{Q(s=0,P_n)}\right]s=0, \quad (4)$$

$$M_2(s,P_n)=-\frac{d^2}{ds^2}\left[\frac{Q(s,P_n)}{Q(s=0,P_n)}\right]s=0. \quad (5)$$

From expressions (4) and (5), we get the formula for determining the average time of DDoS attack implementation:

$$\bar{t}_p(P_n)=-\frac{d}{ds}\left[\frac{Q(s,P_n)}{Q(s=0,P_n)}\right]s=0. \quad (6)$$

The variance of DDoS attack implementation time $D(t_{impl.})$, which is defined as the second central moment, is represented by the expression:

$$D(\bar{t}_p)=-\frac{d^2}{ds^2}\left[\frac{Q(s,P_n)}{Q(s=0,P_n)}\right]s=0-\left\{-\frac{d}{ds}\left[\frac{Q(s,P_n)}{Q(s=0,P_n)}\right]s=0\right\}^2. \quad (7)$$

The calculation of mathematical expectation and dispersion allows to determine the time distribution function of the successful implementation of a DDoS attack as an incomplete gamma function with sufficient accuracy for engineering calculations [21]:

$$F(t)=\begin{cases}0,\_if\_t<0\\ \int_0^t\frac{\mu^\alpha}{\Gamma(\alpha)}\cdot t^{\alpha-1}\cdot e^{-\mu\cdot t}dt,\_if\_t>0\end{cases}, \quad (8)$$

where $\alpha=\frac{[\bar{t}_p(P_n)]^2}{D(\bar{t}_p)}$ is the shape parameter and $\mu==\frac{\bar{t}_p(P_n)}{D(\bar{t}_p)}$ is the scale parameter $\Gamma(\alpha)$.

4. Approbation of the model

Calculations were made using formula (8) in the environment of the MathCAD application program package, the results of which are presented in the graphs (Fig. 4). The values of the average time taken by the attacker to implement the steps of the DDoS attack are shown in Table 1 as the initial data.

The values of all of the probabilities are assumed to be equal to $P_{def.elem.}$, $P_{def.OS.}$, $P_{def.serv}$, $P_{conect.}$ Therefore, in the future we will replace them with the notation Pn and, in the calculation, we will take its value equal to 0.75 - 0.9.

In turn, the average implementation time $T_{impl.aver}$ of a DDoS attack at different values of the probability Pn is:

at Pn=0,75 $T_{impl.aver}$ = 64, 332 min;
Pn=0,85 $T_{impl.aver}$ = 50,197 min;
Pn= 0,9 $T_{impl.aver}$ = 41,129 min.

Table 1.
Time parameters of DDos attack simulation.

Step time	Parameter designation	Time, min
Average time to determine active network elements	$t_{def.elem}$	7
Average time to determine OS type and versions of server and client automated workstations	$t_{def.OS}$	5
Average time to determine services	$t_{def.of.serv}$	6
Average service request time	$t_{serv.reg.}$	2
Average time to identify vulnerabilities	$t_{ident.vul}$	7
The average time to repeat the definition of network elements	$t_{rep.reg}$	4
Average time to receive a response about the server status	$t_{get.status.}$	1
Average retry time of server connection requests	$t_{rep.reg}$	4
Average server lock time	$t_{lock.}$	3

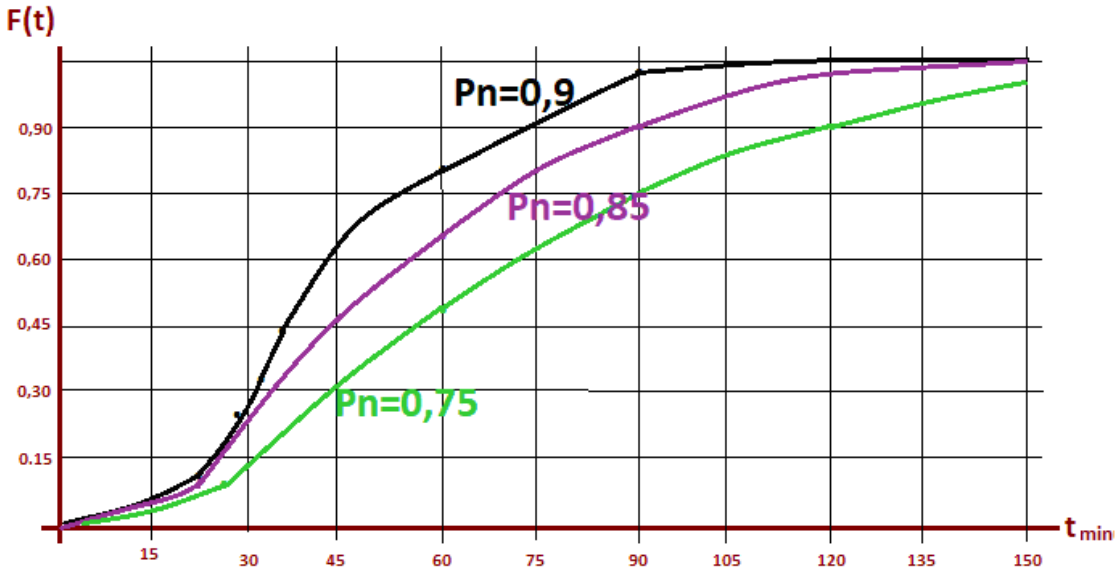

Figure 4: Dependence of the integral function of probability distribution on the time of implementation of a DDoS attack when it is successfully implemented with probability Pn.

Conclusions

The analysis of the obtained results shows that the developed model of the scenario of the implementation of a DDoS attack by an attacker on the elements of a specialized information system is sufficiently sensitive to changes in the initial data, allows obtaining consistent results, adequately reflects the course of the computer attack and makes it possible to determine the probability-time characteristics of the attacker's cyber influence system.

The simulation results show that the main influence on the success of the offender's implementation of a DDoS attack on IS elements is carried out through the parameters that can become available to him as a result of intelligence of the IS network, through knowledge of methods of identification and authentication of legitimate users.

To increase the security of IS against the cyber influence of the violator, it is advisable to implement the organizational and technical measures outlined in [21,23 - 26].

As can be seen from the analysis, today the main threat to information stored in IS comes from the global computer network.

Therefore, the structure of the computer network, on which the operation of the IS will be based, should provide for its division into local segments with access restrictions to them.

In such protected segments with controlled access, the server part of the IS and its client locations, which provide the basic functionality of the system, are placed.

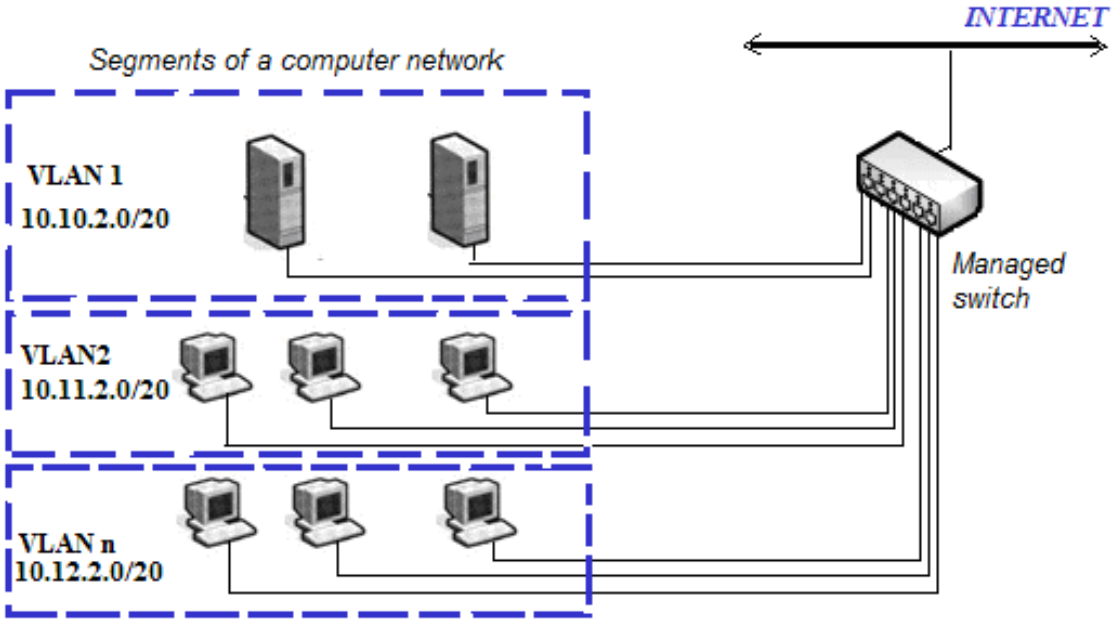

Figure 5 : Simplified topology of a segmented computer network of a specialized IS.

The use of managed switches with the function of creating virtual computer networks (VLAN) made it difficult for the attacker to explore the network he chose for the attack, increasing the probability of its negative termination $1 - P_{def.elem.}$, $1 - P_{def.OS}$, $1 - P_{def.of.serv}$, $1 - P_{connect}$ and at the same time allowed:

1. Protect the network from outside interference. A managed network switch port will be able to ignore and drop packets coming from other subnets, regardless of the originating IP address.
2. Flexibly manage the separation of computers by virtual subnets, ensuring isolation from each other, while their topology does not depend on where the network components are physically located.

3. Ensuring the reduction of broadcasting traffic in the network. Each virtual subnet created is a separate broadcast domain whose broadcast traffic will not be broadcast between different subnets, reducing the load on network equipment.
4. The division of the network into virtual subnets allowed us to apply our own security rules for each of them, which reduces the likelihood of a DDoS attack.

It is clear that it is almost impossible to get rid of the destructive influence of malicious software, but it is possible to significantly reduce its level using advanced countermeasures. As an example, the company "NVisionGroup" offers a comprehensive solution for protection against DDoS attacks based on Cisco Clean Pipes technology, which provides a quick response to DDoS attacks, is easily scalable, has high reliability and speed. Cisco Clean Pipes technology involves the use of Cisco Anomaly Detector and Cisco Guard modules, as well as various systems for statistical analysis of network traffic based on data received from routers using the Cisco Netflow protocol. At the same time, Anomaly Detector and statistical traffic analysis systems act as DDoS attack detection systems, and Cisco Guard as a means of countering an already detected attack.

Along with using the functionality of the latest network hardware, one should not ignore a fairly effective countermeasure, which is the elimination of software vulnerabilities at all levels. This leads to a sharp increase in the average time to find $t_{ident.vul.}$ vulnerabilities and, accordingly, a decrease in the probability of successful completion of $P_{ident.vul.}$. This approach is especially effective when used in conjunction with network monitoring.

References

[1] M. N. Alenezi, H.K. Alabdulrazzaq, A.A. Alshaher, M.M. Alkharang. Evolution of Malware Threats and Techniques: a Review. International Journal of Communication Networks and Information Security (IJCNIS). 12, 3 (Apr. 2022). pp. 326-337. URL: https://doi.org/10.17762/ijcnis.v12i3.4723.

[2] A. Zimba. A. Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks. International Journal of Computer Network and Information Security, 2022, Volume 14, Issue 1. pp. 25-39. DOI: https://doi.org/10.5815/ijcnis.2022.01.03

[3] Y. Li, Q. Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 2021, Vol. 7.pp. 8176–8186. DOI: https://doi.org/10.1016/j.egyr.2021.08.126

[4] Ö. Aslan, S.S. Aktug, M. Ozkan-Okay, A.A. Yilmaz, E. Akin. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 2023, Volume 12, Issue 6, pp. 1333. DOI: https://doi.org/10.3390/electronics12061333

[5] J. M. Biju, N. Gopal, A.J. Prakash. Cyber attacks and its different types. International Research Journal of Engineering and Technology (IRJET), 2019, Volume 06, Issue 03, pp. 4849-4852. URL: https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf

[6] Forbes Ukraine. "Monobank repels powerful DDoS attack" - Horokhovskyi. URL: https://forbes.ua/ru/news/monobank-zaznav-potuzhnoi-ddos-ataki-gorokhovskiy-12122023-17834.

[7] Enisa threat Landscape for DOS Attacks / Eurpean Union Agency for Cybersecurity, November, 2023. 34 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks

[8] J. Chahal, A. Bhandari, S. Behal. Distributed Denial of Service Attacks: A Threat or Challenge. New Review of Information Networking, 2019, 24. pp. 31-103. URL: https://doi.org/10.1080/13614576.2019.1611468

[9] S. Kotey, E.T. Tchao, D. Gadze. On Distributed Denial of Service Current Defense Schemes. Technologies, 2019, 7(1), 19. pp. 1-24. URL: https://doi.org/10.3390/technologies7010019

[10] M. Khambatta. Comparative Analysis Based on Survey of DDOS Attacks: Detection Techniques at Transport, Network, and Application Layers. Culminating Projects in Information Assurance, 2019, 91. 80 p. URL: https://repository.stcloudstate.edu/msia_etds/91

[11] A. Boyarchuk, N. Petliak, Y. Klots, V. Titova, V. Cheshun. Signature-based Approach to Detecting Malicious Outgoing Traffic. CEUR Workshop Proceedings, 2023, 3373. pp. 486–506. URL: https://ceur-ws.org/Vol-3373/paper33.pdf

[12] H. Alameen, A. Esamaddin. DoS and DDoS Attacks at OSI Layers. International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 2, Issue 8, 2020. pp. 1-9. URL: https://doi.org/10.5281/zenodo.3610833

[13] I. Dzhalladova, S. Škapa, V. Novotná, A. Babynyuk. Design and analysis of a model for detection of information attacks in computer networks. Economic Computation and Economic Cybernetics Studies and Research, 2019, Issue 3; Vol. 53.pp. 95-112.

[14] Y. Klots, V. Titova, N. Petliak, V. Cheshun, A. Salem. Research of the Neural Network Module for Detecting Anomalies in Network Traffic. CEUR Workshop Proceedings, 3156, 2022. pp. 378–389.

[15] D. Alomari, F. Anis, M. Alabdullatif, H. Aljamaan. A Survey on Botnets Attack Detection Utilizing Machine and Deep Learning Models. EASE '23: Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering, June 2023. pp. 493-498.

[16] N. Ahuja, G. Singal, D. Mukhopadhyay, N. Kumar. Automated DDOS attack detection in software defined networking. Journal of Network and Computer Applications, Volume 187, 1 August 2021. pp. 103-108. URL: https://doi.org/10.1016/j.jnca.2021.103108

[17] M. Soneja, C.V. Ravi Kumar. Analyzing the Performance of Various Corporate Networks using Multi-Protocol Label Switching Technology, International journal of engineering research & technology (IJERT), Volume 09, Issue 06 (June 2020). pp. 1338-1343.

[18] M.A. Ridwan, N.A. Mohamed Radzi, W.S.H.M. Wan Ahmad, F. Abdullah, M.Z. Jamaludin, M.N. Zakaria. Recent trends in MPLS networks: technologies, applications and challenges. IET Commun., 2020, Vol. 14 Iss. 2.pp. 177-185. URL: https://doi.org/10.1049/iet-com.2018.6129

[19] Y.M. Shcheblanin, D.I. Rabchun. Mathematical model of an information security violator / Cybersecurity: education, science, technology, No. 1, 2018, pp. 63-72.

[20] N.O. Virchenko. Basic properties of generalized gamma functions. / National Technical University of Ukraine "KPI", Scientific News of NTUU "KPI", No. 4, 2016. - Kyiv p. 20-26.

[21] M. Stetsyuk, L. Bedratyuk, B. Savenko, V. Stetsyuk, O. Savenko. Providing the Resilience and Survivability of Specialize d Information Technology Across Corporate Computer Networks. 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. Khmelnytskyi, Ukraine, June 10-12, 2020; CEUR Workshop Proceedings, 2020; vol 2623, pp 219-238.

[22] L. Yang, A. Obeidat, R. Yaqbeh. Smart Approach for Botnet Detection Based on Network Traffic Analysis. Journal of Electrical and Computer Engineering, Volume 2022, 2022. URL: https://doi.org/10.1155/2022/3073932

[23] J. Velasco-Mata, V. González-Castro, E. Fidalgo et al. Real-time botnet detection on large network bandwidths using machine learning. Scientific Reports 13, 4282 (2023). URL: https://doi.org/10.1038/s41598-023-31260-0

[24] R.S. Skandha Moorthy, N. Nathiya. Botnet Detection Using Artificial Intelligence. Procedia Computer Science Volume 218, 2023. pp. 1405-1413. URL: https://doi.org/10.1016/j.procs.2023.01.119.