BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **22**, No 3
Sofia • 2022 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2022-0026

Mathematical Modelling of Malware Intrusion in Computer Networks

Andon D. Lazarov[1,2]

[1]*Information Technology Department, Nikola Vaptsarov Naval Academy, 9000 Varna, Bulgaria*
[2]*Faculty of Aerospace Engineering, K.N. Toosi University of Technology, Tehran, Iran*
E-mail: a.lazarov@naval-acad.bg

Abstract: *Malware attacks cause great harms in the contemporary information systems and that requires analysis of computer networks reaction in case of malware impact. The focus of the present study is on the analysis of the computer network's states and reactions in case of malware attacks defined by the susceptibility, exposition, infection and recoverability of computer nodes. Two scenarios are considered – equilibrium without secure software and not equilibrium with secure software in the computer network. The behavior of the computer network under a malware attack is described by a system of nonhomogeneous differential equations. The system of the nonhomogeneous differential equations is solved, and analytical expressions are derived to analyze network characteristics in case of susceptibility, exposition, infection and recoverability of computer nodes during malware attack. The analytical expressions derived are illustrated with results of numerical experiments. The conception developed in this work can be applied to control, prevent and protect computer networks from malware intrusions.*

Keywords: *Cybersecurity, malware attack modelling, network differential equation.*

1. Introduction

Computer networks are software-based, which determines their vulnerability to malware. Computer malware is software with the ability to multiply, i.e., make multiple copies of itself to defeat multiple computers. Malware damages are on the network components and functionality, which results in an increase in network traffic and a significant delay in the transmission of data on it. The structure of modern computer malware and the common strategies used by this software to defeat the computer networks in which they reproduce themselves is discussed in [1, 2]. A classic Susceptible-Infective-Recovery (SIR) model is applied in [3] to describe the impact of malware on the Internet. Mathematical modelling the processes of malware exposure, infection, and recovery with a graphical illustration of differential equations' solutions is presented in [4, 5].

A dynamic model based on epidemic processes in the spread of bacteria and viruses with theoretical analysis and digital simulation of the epidemic process is presented in [6]. A mathematical model to study propagation of computer worms in a network is suggested in [7]. A network infection model of malware attack described by a differential equation is proposed in [8]. Computer malware does not affect physically the computer systems through which they pass. However, for example, the known malware of Morris and Mydoom can cause serious interference by increasing network traffic and causing other side effects.

Slammer malware has exploited a vulnerability in Microsoft's SQL database software and caused cascading effects on computer infrastructure, airline reservation systems and ATMs. Various concepts related to the impact of malware and the classification of existing worms into Internet, e-mail, Point-to-Point, and Instant Messaging (IM) worms have been discussed in [9], with an emphasis on the detection and counteraction strategy of email and IM striking programs.

Computer malware is regarded as a type of computer virus, but there are several characteristics that distinguish computer malware from virus software. The main difference is that the virus software is distributed through the activity of the operator (user) (program start, file opening, etc.), while the computer malware has the ability to multiply and distribute automatically without human intervention.

In addition to being able to distribute without operator intervention, computer malware has the ability to self-replicate. That is, this software creates multiple copies of itself to smash other computers. This is accomplished by sending mass emails to email addresses of malware infected computers on the web.

Examples of computer malware are Stuxnet, Duqu, and Flame, which continue to make new copies of their primary cyber-malware copies. The ability of malware to spread and multiply at high speeds, overcoming defence mechanisms, makes them a major threat to the security of distributed computer systems. In [10] a software sensor complex for the automatic detection of potential vectors (directions) for network infection and counteraction is presented. A common feature of various types of malware, viruses and bots (automatic generation of data that floods IP addresses on the network) and methods of influencing applications and network devices and countermeasures are presented in [11].

The Internet is the main medium used to commit computer crimes. Malware attacks are identified as the highest security risk on the computer network. This software is designed to be distributed without notice or interaction with users. It causes an increase in traffic requests, which in turn ensures a cyberattack. An assessment and topological analysis of network vulnerabilities, as well as cyber-attack prevention algorithms for unauthorized access to data, and a robotic program completely to neutralize malware are presented in [12]. Modern information and communication systems are becoming more diverse and sophisticated, making them a privileged target for network and computer attacks.

An attack model called Attack Identification and Defence AIDD is presented in [13]. A complete description of the processes for detecting and preventing malware attacks in modern computer networks is given in [14]. Knowledge of its source code is essential to counteract malware effectively. The characteristics and descriptions of

some major source codes with malicious effects on applications and network components are presented in [15]. A detailed description of the Stuxnet Worm malware has been made in [16]. Pass-the-Hash, one of the most prevalent yet underrated attacks for credentials theft and reuse is presented in [17]. Time correlation between security and risk assessments and individual environment compliance framework is analysed in [18]. Observing, measuring and collecting HDD performance metrics on a physical machine during ransomware attack is discussed in [19]. Big data analytics in the e-Learning space, data pre-processing, and classification for traffic anomaly intrusion detection using NSL-KDD dataset are presented in [20, 21].

Mathematical modelling of the computer network behaviour and the dynamics of its nodes, which are malware exposed, infected and recovered by protected software after malware attack is in the focus of the present work. It includes a definition of basic differential equations describing the state of the network, i.e., determining the number of nodes in the computer network that are prone to attack, susceptible, exposed, infected, and recovered from impact. The purpose of this study is to suggest a solution of the differential equations describing the behaviour of the computer network under a malware attack.

The rest of the article is organized as follows. Section 2 presents a mathematical model of cyberattack. Section 3 presents the solution of the system of differential equations at equilibrium state of a computer network. Section 4 determines the optimal (extreme) values of the characteristics of a computer network for malware attack at system equilibrium. Section 5 presents the solution of the system of differential equations in the no equilibrium state of the computer system. Section 6 draws conclusion remarks.

2. Mathematical model of cyber malware attack

In the area of the cyber security, an epidemic Susceptible-Exposed-Infectious-Recovered (SEIR) model is applied to evaluate transmission of malware in computer networks. The variables *S*, *E*, *I*, *R* are introduced, where: *S* is the class of susceptible nodes (those able to contact the malware); *E* is the class of exposed nodes (those who have been infected but are not yet infectious); *I* is the class of the infective nodes (those capable of transmitting the malware); *R* is the class of recovered nodes (those which have become immune by antivirus software). The following rates and periods are introduced in the analysis:

$\mu = 1/T_\mu$ is the mortality rate, T_μ is the mortality period due to malware attack;

$\beta = 1/T_\beta$ is the rate of the infectious contact, i.e., data exchange between susceptible and infected nodes, T_β is the period of the infectious contact or the latent period;

$\delta = 1/T_\delta$ is the rate of node failure, T_δ is the period of node failure in the network because of infection;

$\tau = 1/T_\tau$ is the infection rate of the exposed class, T_τ is the infection latent period;

$\rho = 1/T_\rho$ is the rate of recovery from infection, T_ρ is the recovery period;

$r = 1/T_r$ is the inherent susceptible growth rate, T_r is the inherent susceptible growth period.

The susceptible class is characterized by a competition carrying capacity $k > 0$ of logistic growth, and maximal susceptible growth rate $r > 0$. The logistic growth is equal to the sum all classes' initial cardinalities, i.e., $k = S_0 + E_0 + I_0 + R_0$. The carrying capacity k is a constant if the rate of recovery and failure are equal, in general k is a variable. The effectiveness of the antivirus software on a network is limited due to the time interval for updating antivirus software and cost efficiency.

In case β is the effective contact rate, as many as $\beta.I.S/k$ susceptible nodes will be exposed. In case new nodes in the computer network are categorized as susceptible, the number of susceptible nodes increases to $\delta.S$ nodes. The transmission malware infection can occur through direct data exchange between susceptible and infected nodes. The dynamics of the nodes in the susceptible S class is defined by the differential equation

$$\frac{dS}{dt} = r.S\left(1 - \frac{S}{k}\right) - \frac{\beta.I.S}{k} - \delta.S, \quad (1)$$

where $r.S\left(1 - \frac{S}{k}\right)$ relates the growth rate of the susceptible class, dS/dt, to the current size S of the susceptible class, incorporating the effect of the two constant parameters r, the inherent susceptible growth rate, and k, the carrying capacity k of logistic growth.

The number of infected nodes increases to τE, due to the existence of exposed and infected nodes. In case that τ is the rate, at which the exposed nodes become infective up to τE of exposed nodes will be infected. The number of exposed nodes increases up to $\beta.I.S/k$ nodes. The transmission malware infection can occur through direct data exchange between susceptible and infected nodes. The dynamics of the nodes in the exposed E class is defined by the differential equation

$$\frac{dE}{dt} = \frac{\beta.I.S}{k} - (\tau + \delta).E. \quad (2)$$

The number of infected nodes increases up to τE due to existence of exposed nodes that have been infected. The number of infected nodes decreases to $(\mu + \delta).I$ and Rec(I) due to mortal and failure nodes and recovery of infected nodes.

The dynamics of nodes in the infected I class is defined by the differential equation

$$\frac{dI}{dt} = \tau.E - (\mu + \delta).I - \mathrm{Rec}(I). \quad (3)$$

In case that ρ is the recovery rate, the number of recovered nodes based on the protected software is defined by the expression [3]

$$\mathrm{Rec}(I) = \begin{cases} \rho I, & 0 \le I \le I_{\min}, \\ m, & I \ge I_{\min}, \end{cases} \quad (4)$$

where ρ is the recovery rate of *I* nodes when the antivirus program is not fully used, i.e., $0 \le I \le I_{\min}$, $m = \rho.I_{\min}$ if $I \ge I_{\min}$, where $I_{\min}$ is the minimum number of infected nodes, after that the antivirus program is activated.

The number of recovered nodes increases up to $\rho.I$, due to recovery of infected nodes. The number of recovered nodes also increases to $\mathrm{Rec}(I)$ due recovery of infected nodes, and decreases to $\delta.R$, due to failure of recovered nodes. The dynamics of recovered nodes in class *R*, i.e., the instantaneous rate of recoverability is defined by the differential equation

$$\frac{dR}{dt} = \mathrm{Rec}(I) - \delta R \,. \tag{5}$$

The system of differential equations describing the behaviour of a computer system attacked by malware and dynamics of classes *S*, *E*, *I*, and *R* in the computer network can be written as

$$\begin{cases} \dfrac{dS}{dt} = r.S - (r.S).\left(\dfrac{S}{k}\right) - \dfrac{\beta.I.S}{k} - \delta.S, \\ \dfrac{dE}{dt} = \dfrac{\beta.I.S}{k} - (\tau + \delta).E, \\ \dfrac{dI}{dt} = \tau.E - (\mu + \delta).I - \mathrm{Rec}(I), \\ \dfrac{dR}{dt} = \mathrm{Rec}(I) - \delta R. \end{cases} \tag{6}$$

The first three equations are independent of the recovery class *R*, which allows the system of equations to be reduced to three linear differential equations, i.e.,

$$\begin{cases} \dfrac{dS}{dt} = r.S - (r.S).\left(\dfrac{S}{k}\right) - \dfrac{\beta.I.S}{k} - \delta.S, \\ \dfrac{dE}{dt} = (\beta.I).S - (\tau + \delta).E, \\ \dfrac{dI}{dt} = \tau.E - (\mu + \delta).I - \mathrm{Rec}(I). \end{cases} \tag{7}$$

3. Solution of the differential equations' system at equilibrium state of a computer network

In equilibrium state of a computer network, the variables *S*, *E*, *I* defining the susceptible, exposed and infected classes of nodes are constant in time, i.e.,

$$\frac{dS}{dt} = 0 \,,\ \frac{dE}{dt} = 0 \,,\ \frac{dI}{dt} = 0 \,. \tag{8}$$

Taking into account the above conditions, the system of algebraic equations defining the equilibrium state of the computer network is written as:

a) In case $0 \le I \le I_{\min}$

$$\begin{cases} r.S - (r.S).\left(\frac{S}{k}\right) - \frac{\beta.I.S}{k} - \delta.S = 0, \\ \frac{\beta.I.S}{k} - (\tau + \delta).E = 0, \\ \tau.E - (\mu + \delta + \rho)I = 0; \end{cases} \tag{9}$$

b) In case $I > I_{\min}$

$$\begin{cases} r.S - (r.S).\left(\frac{S}{k}\right) - \frac{\beta.I.S}{k} - \delta.S = 0, \\ \frac{\beta.I.S}{k} - (\tau + \delta).E = 0, \\ \tau.E - (\mu + \delta).I - m = 0, \end{cases} \tag{10}$$

where $m = \rho.I_{\min}$.

The solution of the system (9) in the presence of susceptible computers, but in absence of exposed and infected nodes, i.e., $E = 0$, $I = 0$, is written as

$$S = \frac{k(r-\delta)}{r}. \tag{11}$$

In endemic equilibrium, i.e., $S \neq 0$, E, I are constant, the system of the algebraic equations (9) is rewritten as

$$\begin{cases} r - \frac{r.S}{k} - \frac{\beta.I}{k} - \delta. = 0, \\ \frac{\beta.I.S}{k} - (\tau + \delta).E = 0, \\ \tau.E - (\mu + \delta + \rho)I = 0. \end{cases} \tag{12}$$

The solutions of algebraic system (12) are as follows:

$$\begin{cases} S' = \frac{k.a(\tau + \delta)}{\beta.\tau}, \\ E' = a.\frac{k.\beta\tau(r-\delta) - r.k.a(\tau + \delta)}{\beta^2.\tau^2}, \\ I' = \frac{k.\beta\tau(r-\delta) - r.k.a(\tau + \delta)}{\beta^2.\tau}, \end{cases} \tag{13}$$

where $a = \rho + \mu + \delta$.

In endemic equilibrium, i.e., $S \neq 0$, E, I are constant, the system of the algebraic equations (10) is rewritten as

$$\begin{cases} r - S.\left(\frac{r}{k}\right) - \frac{\beta I}{k} - \delta = 0, \\ \frac{\beta.I.S}{k} - (\tau + \delta).E = 0, \\ \tau.E - (\mu + \delta).I - m = 0. \end{cases} \quad (14)$$

The solution of the system (14) in endemic equilibrium is as follows. From the first equation the number of nodes in the susceptible class S is determined

$$S = \frac{k(r-\delta) - \beta.I}{r}. \quad (15)$$

From the third equation the number of nodes in the exposed class E is determined

$$E = \frac{(\mu + \delta).I + m}{\tau}. \quad (16)$$

Substitute (15) and (16) into the second equation of (14). The following quadratic equation is obtained for the infected nodes I in the network at endemic equilibrium

$$\beta^2 \tau I^2 - [\beta\tau k(r-\delta) - k.r(\tau+\delta)(\mu+\delta)].I + k.m.r.(\tau+\delta) = 0. \quad (17)$$

The solution for the number of infected nodes I can be written as

$$I_{1,2} = \frac{b \pm \sqrt{t}}{2.\tau.\beta^2}, \quad (18)$$

where $b = \beta\tau k(r-\delta) - k.r(\tau+\delta)(\mu+\delta)$, $t = b^2 - 4.\beta^2.\tau.k.m.r.(\tau+\delta)$.

Substitute the expression (16) in the expressions (15) and (16) for determining the susceptible S and exposed E nodes in the network at endemic equilibrium

$$S_{1,2} = \frac{k.(r-\delta) - \beta I_{1,2}}{r}, \quad (19)$$

$$E_{1,2} = \frac{(\mu+\delta).I_{1,2} + m}{\tau}. \quad (20)$$

In endemic equilibrium and antivirus software on, i.e., $I_{1,2} > I_{\min}$, the number of infected nodes is defined by

$$I_{1,2} = \frac{b \pm \sqrt{t}}{2.\tau.\beta^2} \geq I_{\min}. \quad (21)$$

Hence, in case of positive value of the radical, the condition of endemic equilibrium with the antivirus program on is defined by the inequality

$$\sqrt{t} \geq I_{\min}.2.\tau.k\beta^2 - b. \quad (22)$$

4. Determination of the extreme values of the computer network's characteristics against malware attack at system equilibrium

To determine the extreme values of the computer network's characteristics against malware attack at endemic equilibrium, the Jacobian matrices of the systems (9) and (10) and their eigenvalues are calculated. Based on the left-hand sides of the equations (9), the following vectors are defined

$$(23)\qquad \begin{cases} A = r.S - (r.S).\left(\dfrac{S}{k}\right) - \dfrac{\beta.I.S}{k} - \delta.S, \\ B = (\beta.I).S - (\tau + \delta).E, \\ C = \tau.E - (\mu + \delta).I - \rho I. \end{cases}$$

From the left-hand sides of the equations from the system of Equations (10), the following vectors are defined:

$$(24)\qquad \begin{cases} A = r.S - (r.S).\left(\dfrac{S}{k}\right) - \dfrac{\beta.I.S}{k} - \delta.S, \\ B = (\beta.I).S - (\tau + \delta).E, \\ C' = \tau.E - (\mu + \delta).I - m. \end{cases}$$

In case $0 \le I \le I_{\min}$ the Jacobian matrix of the system (9) can be written as

$$(25)\qquad J_1 = \begin{bmatrix} \dfrac{\partial A}{\partial S} & \dfrac{\partial A}{\partial E} & \dfrac{\partial A}{\partial I} \\ \dfrac{\partial B}{\partial S} & \dfrac{\partial B}{\partial E} & \dfrac{\partial B}{\partial I} \\ \dfrac{\partial C}{\partial S} & \dfrac{\partial C}{\partial E} & \dfrac{\partial C}{\partial I} \end{bmatrix} = \begin{bmatrix} r - 2.r.\left(\dfrac{S}{k}\right) - \dfrac{\beta.I}{k} - \delta & 0 & -\dfrac{\beta S}{k} \\ \dfrac{\beta.I}{k} & -(\tau + \delta) & \dfrac{\beta.S}{k} \\ 0 & \tau & -(\mu + \delta + \rho) \end{bmatrix}.$$

In case $I > I_{\min}$ the Jacobian matrix of the system (10) can be written as

$$(26)\qquad J_2 = \begin{bmatrix} \dfrac{\partial A}{\partial S} & \dfrac{\partial A}{\partial E} & \dfrac{\partial A}{\partial I} \\ \dfrac{\partial B}{\partial S} & \dfrac{\partial B}{\partial E} & \dfrac{\partial B}{\partial I} \\ \dfrac{\partial C'}{\partial S} & \dfrac{\partial C'}{\partial E} & \dfrac{\partial C'}{\partial I} \end{bmatrix} = \begin{bmatrix} r - 2.r.\left(\dfrac{S}{k}\right) - \dfrac{\beta.I}{k} - \delta & 0 & -\dfrac{\beta S}{k} \\ \dfrac{\beta.I}{k} & -(\tau + \delta) & \dfrac{\beta S}{k} \\ 0 & \tau & -(\mu + \delta) \end{bmatrix}.$$

In case of complete equilibrium in the computer network, $S = 0$, $E = 0$, $I = 0$, i.e., in absence of susceptible, exposed and infected nodes, the eigenvalues of the matrix J_1 are elements of the rectangular diagonal matrix $\hat{J}_1$ from the singular decomposition of J_1

(27) $$\hat{J}_1 = \begin{bmatrix} r-\delta & 0 & 0 \\ 0 & -(\tau+\delta) & 0 \\ 0 & 0 & -(\mu+\delta+\rho) \end{bmatrix}.$$

In order to achieve asymptotic equilibrium and global stability in a computer network over time in case $0 \le I \le I_{\min}$ the eigenvalues should be negative, which sets the condition $r < \delta$. In the case of complete equilibrium of the computer network, i.e., $S = 0$, $E = 0$, $I = 0$ (in absence of susceptibility, exposure to infection and infection of nodes) the eigenvalues of the matrix J_2 are elements of the rectangular diagonal matrix $\hat{J}_2$ from the singular decomposition of J_2.

(28) $$\hat{J}_2 = \begin{bmatrix} r-\delta & 0 & 0 \\ 0 & -(\tau+\delta) & 0 \\ 0 & 0 & -(\mu+\delta) \end{bmatrix}.$$

In order to achieve asymptotic equilibrium and global stability in the computer network in case $I > I_{\min}$ over time, the eigenvalues must be negative, which again poses a condition $r < \delta$. In presence of a susceptibility of the computer network under a time condition $t \ge t_0$, where t_0 determines the moment of asymptotic constant susceptibility S and the absence of exposed and infected nodes in the network, i.e.,

(29) $$S = \frac{k(r-\delta)}{r},\ E = 0,\ I = 0.$$

The Jacobian matrix

(30) $$J_3 = \begin{bmatrix} r - 2.r.\left(\frac{S}{k}\right) - \delta & 0 & -\frac{\beta S}{k} \\ 0 & -(\tau+\delta) & \frac{\beta S}{k} \\ 0 & \tau & -(\mu+\delta) \end{bmatrix},$$

can be rewritten as

(31) $$J_3 = \begin{bmatrix} -(\delta-r) & 0 & -\beta\frac{(r-\delta)}{r} \\ 0 & -(\tau+\delta) & \beta.\frac{(r-\delta)}{r} \\ 0 & \tau & -(\mu+\delta) \end{bmatrix}.$$

The eigenvalues of the matrix J_3 are elements of the rectangular diagonal matrix $\hat{J}_3$ from the singular decomposition of J_3

(32) $$\hat{J}_3 = \begin{bmatrix} -(\delta - r) & 0 & 0 \\ 0 & \dfrac{-f - \sqrt{g^2 - 4f}}{2} & 0 \\ 0 & 0 & \dfrac{-f + \sqrt{g^2 - 4f}}{2} \end{bmatrix},$$

where $f = 2\delta + \mu + \tau$, $g = (\delta + \tau)(\mu + \delta) - \dfrac{\beta.\tau.(r - \delta)}{r}$.

The eigenvalues of the matrix J_3 are negative, which means $r < \delta$ and $\dfrac{-f + \sqrt{g^2 - 4f}}{2} < 0$. In the presence of a fixed susceptibility of the computer network to malware attack asymptotically defined by the expression $S = \dfrac{k(r - \delta)}{r}$ in case $t \geq t_0$ and dynamics of exposed and infected nodes in the network, i.e., $E = \text{var} \neq 0$, $I = \text{var} \neq 0$, the system of differential equations for *E* and *I* is rewritten as

(33) $$\begin{cases} \dfrac{dE}{dt} = -(\tau + \delta).E + \beta.\dfrac{(r - \delta)}{r}.I, \\ \dfrac{dI}{dt} = \tau.E - (\mu + \delta + \rho).I. \end{cases}$$

The matrix of coefficients of the system (33) is written as

(34) $$\begin{bmatrix} -(\tau + \delta) & \beta.\dfrac{k.(r - \delta)}{r} \\ \tau & -(\mu + \delta + \rho) \end{bmatrix}.$$

Eigenvalues λ of the matrix (34) are calculated from the following equation

(35) $$\det \begin{bmatrix} -(\tau + \delta) - \lambda & \beta.\dfrac{(r - \delta)}{r} \\ \tau & -(\mu + \delta + \rho) - \lambda \end{bmatrix} = 0.$$

Based on (35), the following quadratic equation in respect of the eigenvalues λ of the matrix (34) is written

(36) $$\lambda^2 + (\tau + 2\delta + \mu + \rho)\lambda + (\tau + \delta)(\mu + \delta + \rho) - \frac{\tau.\beta(r - \delta)}{r} = 0.$$

To obtain asymptotically decreasing number of nodes in classes *E* and *I*, the eigenvalues should have real negative values, which is achieved if $r < \delta$, and $(\tau + \delta)(\mu + \delta + \rho) \geq \dfrac{\tau.\beta(r - \delta)}{r}$ if $r > \delta$. The latter can be expressed as

(37) $$\frac{\tau.\beta.(r - \delta)}{r.(\tau + \delta)(\mu + \delta + \rho)} \leq 1.$$

The left-hand side of inequality (37) is the baseline reproductive number of new infected nodes caused by infection of the susceptible nodes in the network, which is denoted as

(38) $$R_0 = \frac{\tau.k(r-\delta)}{r.(\tau+\delta)(\mu+\delta+\rho)}.$$

In case $R_0 < 1$, the malware cannot affect a network that remains asymptotically locally stable. If $R_0 > 1$, the malware attacks the computer network, which becomes unstable.

The solution of the quadratic equation (36) can be written as

(39) $$\lambda_{1,2} = \frac{-(\tau+2\delta+\mu+\rho) \pm \sqrt{(\tau+2\delta+\mu+\rho)^2 - 4\left[(\tau+\delta)(\mu+\delta+\rho) - \frac{\tau.\beta(r-\delta)}{r}\right]}}{2}.$$

The maximal eigenvalues of the singular matrix decomposition (34) determine the dynamics of classes *E* and *I*. In case, $t = t_0$ a maximum in the class *E* exposed to malware is registered. In case, $t = t_1 > t_0$ a maximum in class *I* of malware infection is registered.

5. Solution of the differential equations' system in the no equilibrium state of the computer system

The behavior of a computer network attacked by malware is represented by dynamics of susceptible *S*, exposed *E*, infected *I*, and recovered *R* classes and is expressed as

(40) $$\frac{dS}{dt} \neq 0\,,\ \frac{dE}{dt} \neq 0\,,\ \frac{dI}{dt} \neq 0\,.$$

Based on the time dependence of classes *S*, *E*, *I*, *R* the following complete system of differential equations can be written

(41) $$\begin{cases} \frac{dS}{dt} = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S, \\ \frac{dE}{dt} = \frac{\beta.I.S}{k} - (\tau+\delta).E, \\ \frac{dI}{dt} = \tau.E - (\mu+\delta).I - \rho.I, \\ \frac{dR}{dt} = \mathrm{Rec}(I) - \delta R. \end{cases}$$

In case $0 \le I \le I_{\min}$ the system of differential equations (41) is rewritten as

(42) $$\begin{cases} \frac{dS}{dt} = r.S - (r.S).\left(\frac{S}{k}\right) - \frac{\beta.I.S}{k} - \delta.S, \\ \frac{dE}{dt} = \frac{\beta.I.S}{k} - (\tau+\delta).E, \\ \frac{dI}{dt} = \tau.E - (\mu+\delta).I - \rho I, \\ \frac{dR}{dt} = \rho.I - \delta.R. \end{cases}$$

In case $I > I_{\min}$ the system of differential equations (41) is written as

$$(43)\quad \begin{cases} \dfrac{dS}{dt} = r.S - (r.S).\left(\dfrac{S}{k}\right) - \dfrac{\beta.I.S}{k} - \delta.S, \\ \dfrac{dE}{dt} = \dfrac{\beta.I.S}{k} - (\tau + \delta).E, \\ \dfrac{dI}{dt} = \tau.E - (\mu + \delta).I - m, \\ \dfrac{dR}{dt} = m - \delta.R. \end{cases}$$

In case $I = I_{\min}$, the systems of equations (42) and (43) can be combined provided that $m = \rho.I_{\min}$. The first differential equation rewritten in the form

$$(44)\quad \frac{dS}{dt} = \left(r - \frac{\beta.I_{\min}}{k} - \delta\right).S - \frac{r}{k}.S^2,$$

can be interpreted and solved as a Bernoulli differential equation.

The following substitution is made

$$(45)\quad a = \left(r - \frac{\beta.I_{\min}}{k} - \delta\right),\ b = \left(-\frac{r}{k}\right).$$

Then equation (44) is rewritten as

$$(46)\quad \frac{dS}{dt} = S' = a.S + b.S^2.$$

Assume $S \neq 0$, then the left and right parts of (44) are divided by S^2, i.e.,

$$(47)\quad \frac{S'}{S^2} - \frac{a}{S} = b.$$

A new function is being introduced $z = z(t)$ and its first derivative $z' = z'(t)$ is determined, i.e.,

$$(48)\quad z = z(t) = \frac{1}{S} = S^{-1},\ z' = z'(t) = \frac{dz(t)}{dt} = -\frac{S'}{S^2}.$$

Equation (47) can be written as

$$(49)\quad z' + a.z = -b.$$

The solution of (49) is written as

$$(50)\quad z = \exp\left(\int a.dt\right)\left(C + \int b.\exp\left(\int a.dt\right)dt\right).$$

Based on substitution $S = z^{-1}$, the solution of the differential equation (47) for *S* is

$$(51)\quad S(t) = \frac{\exp\left(-\int a.dt\right)}{\left(C + \int b.\exp\left(\int a.dt\right)dt\right)}.$$

Given that *a* and *b* are constant quantities, the expression (51) can be rewritten as

$$(52)\quad S(t) = \frac{\exp(-a.t)}{C + (b/a).\exp(a.t)}.$$

In case $t = 0$, $S(t_0) = S_0$. Then, the integration constant is $C = (S_0)^{-1}$.

The following expression is derived for the susceptible class

(53) $$S(t) = \frac{E_0.e^{-a.t}}{1 + E_0.(b/a).e^{a.t}}, \text{ or } S(t) = \frac{e^{-a.t}}{\frac{1}{S_0} + \frac{b}{a}\left(1 - .e^{a.t}\right)},$$

where $a = (r - \beta.I_{\min} - \delta)$, $b = \left(-\frac{r}{k}\right)$.

The fourth differential nonhomogeneous equation from the system of differential Equations (6) is rewritten in the form

(54) $$\frac{dR(t)}{dt} + \delta.R = m.$$

The equation (54) is a first-order nonhomogeneous differential equation with a constant term $m \neq 0$. The solution of (54) is the sum of the general solution $R_0(t)$ of the homogeneous differential equation $\frac{dR_0(t)}{dt} + \delta.R(t) = 0$ and a particular solution of a nonhomogeneous equation R_c, i. e.,

(55) $$R(t) = R_0(t) + R_c.$$

The homogeneous differential equation for the component $R_0(t)$ is written as

(56) $$\frac{dR_0(t)}{dt} + \delta.R_0(t) = 0, \text{ i.e., } \frac{dR_0(t)}{R_0} = -\delta.dt.$$

After integration, it can be written

(57) $$\ln R_0(t) = -\delta.t + C, \text{ i.e., } R_0(t) = C.e^{-\delta.t},$$

where C is the integration constant.

Let R_c be a particular solution of the differential Equation (54),

(58) $$\frac{dR_c}{dt} + \delta.R_c = m.$$

The term m of the differential equation is a constant, and then the particular solution R_c is a constant. Hence, it can be written

(59) $$R_c = \frac{m}{\delta}.$$

The expressions (57) and (59) are substituted in (55), i.e.,

(60) $$R(t) = C.e^{-\delta.t} + \frac{m}{\delta}.$$

In case $t = 0$, $R(0) = 0$, and $C = -\frac{m}{\delta}$, then the general solution of the nonhomogeneous differential equation can be written as

(61) $$R(t) = \frac{m}{\delta}\left(1 - e^{-\delta.t}\right).$$

Equation (61) describes the dynamics of recovered computer network's nodes. In case $t \to \infty$, the maximum number of recovered computer nodes in the class R is

m/δ. Taking into account the time dependent *S*, defined by (53), the second and third differential equations in (42) are written as

(62) $$\frac{dE}{dt} = \dot{E} = -(\tau+\delta).E + \frac{E_0.e^{-a.t}}{1+E_0.b.e^{a.t}}.\beta.I\ ,$$

(63) $$\frac{dI}{dt} = \dot{I} = \tau.E - (\mu+\delta+\rho).I\ .$$

From equation (63) E and $\dot{E}$ are defined as follows:

(64) $$E = \frac{\dot{I}+(\mu+\delta+\rho).I}{\tau}\ ,\ \dot{E} = \frac{\ddot{I}+(\mu+\delta+\rho).\dot{I}}{\tau}\ .$$

Substitute expressions (64) in (62), which yields

(65) $$\ddot{I} + (\tau+\mu+2.\delta+\rho).\dot{I} + \left[(\tau+\delta)(\mu+\delta+\rho) - \frac{\tau.\beta.E_0.e^{-a.t}}{1+E_0.(b/a).e^{a.t}}\right].I = 0\ .$$

The characteristic equation of the differential (65) is written as

(66) $$\omega^2 + (\tau+\mu+2.\delta+\rho).\omega + \left[(\tau+\delta)(\mu+\delta+\rho) - \frac{\tau.\beta.E_0.e^{-a.t}}{1+E_0.(b/a).e^{a.t}}\right] = 0\ .$$

To obtain solutions for *E* and *I* asymptotically decreasing in case $t \to \infty$ the following condition should be satisfied

(67) $$(\tau+\delta)(\mu+\delta+\rho) \geq \frac{\tau.\beta.E_0.e^{-a.t}}{1+E_0.(b/a).e^{a.t}}\ .$$

The solution of quadratic equation (66) is written as

(68) $$\omega_{1,2} = \frac{-(\tau+2\delta+\mu+\rho) \pm \sqrt{(\tau+2\delta+\mu+\rho)^2 - 4\left[(\tau+\delta)(\mu+\delta+\rho) - \frac{\tau.\beta.E_0.e^{-a.t}}{1+E_0.(b/a).e^{a.t}}\right]}}{2}.$$

The root of the greater absolute value, denoted by $(-\omega)$ is chosen. Then, the solution of the differential equation (60) is written as

(69) $$I = C.e^{-\omega.t}\ .$$

The integration constant is determined by the condition $C = I(0) = I_0 = I_{\min}$ in case $t = 0$, i.e., it can be written $I = I_0.e^{-\omega.t}$.

Replace $I = C.e^{-\omega.t}$ in $E = \frac{\dot{I}+(\mu+\delta+\rho).I}{\tau}$, then

(70) $$E = \frac{(\mu+\delta+\rho-\omega).C.e^{-\omega.t}}{\tau}\ .$$

The integration constant *C* in (70) is determined by condition $E = E(0) = E_0$, in case $t = 0$, i.e., it can be written

(71) $$C = \frac{E_0.\tau}{\mu+\delta+\rho-\omega}\ .$$

The expression (70) is rewritten as

(72) $$E = E_0.e^{-\omega.t}\ .$$

The analytical expressions determining the dynamics of susceptible, exposed, infected and recovered computer nodes in case of a malware attack could be used to

simulate the behaviour of nodes in computer networks, and to develop defensive counter-strategies.

6. Numerical experiment

Based on the solution of the system of the differential equations in respect of susceptible, exposed, infected and recovered nodes of the computer network in state of endemic equilibrium and not endemic equilibrium, i.e., in the state of activated secure software, the numerical experiment has been carried out at the following initial values of the main parameters:

Initial number of susceptible nodes $S_0 = 150$.
Initial number of exposure nodes $E_0 = 15$.
Initial number of infectious nodes $I_0 = 2$.
Initial number of recovered nodes $R_0 = 0$.
Rate of contact infection $\beta = 0.05$.
Natural death rate of nodes $\delta = 0.02$.
Infection rate $\tau = 0.04$.
Penetration intrinsic growth rate $r = 0.2$.
Carrying capacity $k = 167$.
Recovery rate $\rho_0 = 0.04$.
Death (destruction) rate due to the attack $\mu = 0.01$.

The results of the experiment are shown in the following figures.

The dependence of the susceptible class on time at endemic no equilibrium, i.e., under the action of security software is presented in Fig. 1. The curve illustrates very steep decreasing of the malware susceptibility in the computer network due to the activation of the protected software.

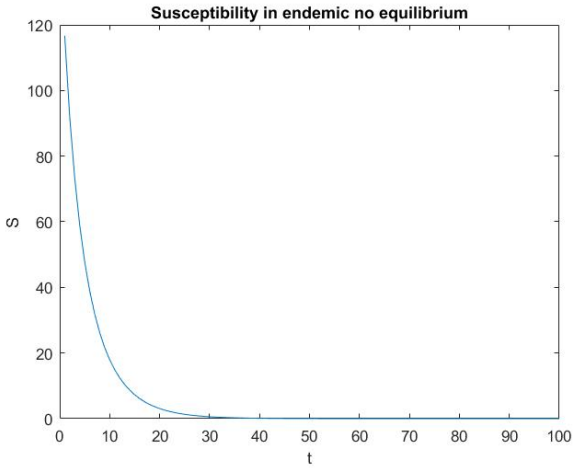

Fig. 1. Dependence of the susceptibility on time at endemic no equilibrium, i.e., under the action of security software

The dependence of the computer nodes' exposure on the time at endemic no equilibrium, i.e., under the action of security software, is shown in Fig. 2. At the beginning, the exposure of the computers to the infection increases to the point $t_0 = 9$ of the extremal exposure, where the curve of the susceptibility alters its steep, i.e. the steep of the susceptibility decreases. After that point, the exposure decreases and asymptotically strives to zero.

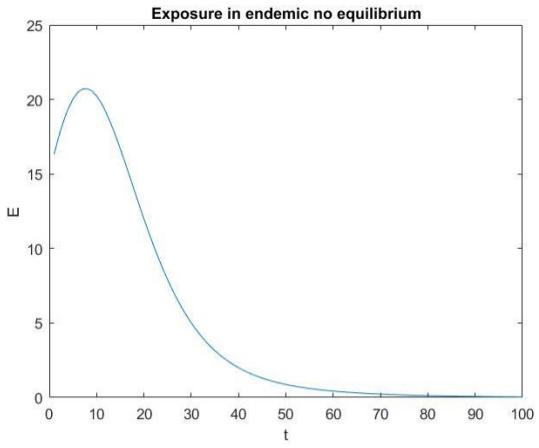

Fig. 2. Dependence of the exposure on time at endemic no equilibrium, i.e., under the action of security software

The dependence of the computer nodes' infection on time at endemic no equilibrium, i.e., under the action of security software is shown in Fig. 3. At the beginning, the infection of the computers steeply increases to point of the extremal infection, $t_1 = 15$. After the extremal point, the infection asymptotically decreases to zero.

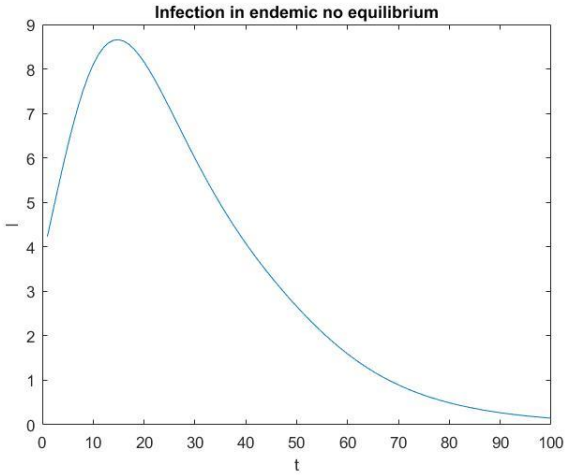

Fig. 3. Dependence of infection on time at endemic no equilibrium, i.e., under the action of security software

The dependence of computer nodes' recoverability on time at endemic no equilibrium, i.e., under the action of security software is shown in Fig. 4. The recoverability of computers in the network exponentially increases.

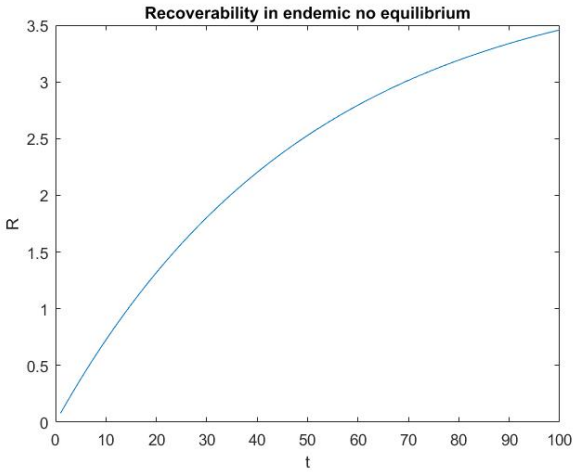

Fig. 4. Dependence of recoverability on time at endemic no equilibrium in case $\rho 0 = 0.04$, i.e., under the action of security software

In case the initial recovery rate is $\rho_0 = 0.04$, the behavioural curve of the network recoverability is shown in Fig. 3. In case $t \to \infty$, the recoverability strives asymptotically to $R = 4$.

7. Conclusion

The dynamic states of the computer network's nodes exposed to malware impact has been defined by a linear system of differential equations. Solutions of differential equations in case of endemic equilibrium and no equilibrium in case the protected software is activated in the computer nodes from *S*, *E*, *R*, and *I* classes, have been derived. The methodology being developed for evaluating the behaviour of a computer network can be further expanded and applied in case of different stochastic distributions of malware attacks.

References

1. Widyaninsih, P., D. R. S. Saputro, A. W. Nugroho. Susceptible Exposed Infected Recovery (SEIR) Model with Immigration: Equilibria Points and Its Application. – In: Proc. of ICSAS, 2018, AIP Conf. 2014, 020165-1-020165-7. **https://doi.org/10.1063/1.5054569**, **https://aip.scitation.org/doi/pdf/10.1063/1.5054569**
2. Chen, Z. Modeling and Defending against Internet Worm Attacks. Doctor of Philosophy Thesis, School of Electrical and Computer Engineering, Georgia Institute of Technology, May 2007.
3. Mishra, B. K., A. Prajapati. Cyber Warfare: Worms' Transmission Model. – International Journal of Advanced Science and Technology, Vol. **63**, 2014, pp. 83-94. **http://dx.doi.org/10.14257/ijast.2014.63.08**

4. Joseph, A. F., S. E Adewumi, Ih. Olalekan, K. Sunday. Computer Viruses: A Framework for Modeling Infection Susceptibility of Workstations. – Advances in Computer Science and Engineering, Vol. **14**, 2015, No 2 pp. 97-109. DOI: 10.17654/ACSEMay2015_097_109.
5. Vetrivelan, P., M. Jagannath, T. S. Pradeep Kumar. Network Intrusion Detection and Prevention Systems on Flooding and Worm Attacks. Combating Security Breaches and Criminal Activity in the Digital Sphere Chapter: Network Intrusion Detection and Prevention Systems on Flooding and Worm Attacks, Publisher: IGI Global. Y. Asnath Victy Phamila, S. Geetha, Eds. June 2016. DOI: 10.4018/978-1-5225-0193-0.
6. Liu, L., R. K. L. Ko, G. Ren, X. Xu. Malware Propagation and Prevention Model for Time-Varying Community Networks within Software Defined Networks. – Security and Communication Networks, Vol. **2017**, Article ID 2910310. 8 p. **https://doi.org/10.1155/2017/2910310**
7. Gowtham, K., N. Sricharan, R. Kisore. Mathematical Model to Study Propagation of Computer Worm in a Network. – In: Proc. of IEEE International Advance Computing Conference (IACC'15), June 2015, pp. 12-13. DOI: 10.1109/IADCC.2015.7154812.
8. Bradley, J. T., S. Gilamore. Analyzing Distributed Internet Worm Attacks Using Continuous State-Space Approximation of Process Algebra Models. – Journal of Computer and System Sciences, Vol. **74**, 2008, pp. 1013-1032.
9. Tang, Y., J. Luo, B. Xiao, G. Vei. Concept, Characteristics and Defending Mechanism of Worms, Special Section on Information and Communication System Security. – IEICE Trans. Inf. & Syst., Vol. **E92–D**, 2009, No 5. **http://www4.comp.polyu.edu.hk/~csbxiao/paper/2009/IEICE-2009-worm.pdf**
10. Sidiroglou, St., A. D. Keromytis. A Network Worm Vaccine Architecture. – In: Proc. of 12th International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE'03, June 2003. **https://dl.acm.org/doi/10.5555/938984.939795**
11. Kamal, S. U. M., R. J. A. Ali, H. K. Alani, E. S. Abdulmajed. Survey and Brief History on Malware in Network Security Case Study: Viruses, Worms, and Bots. – ARPN Journal of Engineering and Applied Sciences, Vol. **11**, 2016, No 1, pp. 683-698.
12. Masthan, M., R. Ravi. Detection and Prevention of Unknown Vulnerabilities on Enterprise IP Networks. – International Journal of Computer Science and Mobile Computing, Vol. **4**, 2015, No 10, pp. 343-352.
13. Souissi, S., A. Serhrouchni. AIDD: A Novel Generic Attack Modeling Approach. – In: Proc. of International Conference on High Performance Computing, Simulation (HPCS'14), July 2014, Bologne, Italy, 2014. ⟨10.1109/HPCSim.2014.6903738⟩. ⟨hal01205824⟩.
14. Chapter 16 Attack Detection and Prevention. National Security Telecommunications Advisory Committee (NSTAC) Intrusion Detection Subgroup, [NetSec], WS 2006/2007. **http://www.ccs-labs.org/~dressler/teaching/netzwerksicherheit-ws0607/16_AttackDetection-v2.pdf**
15. Bajaj, P., A. G. Roy. Source Code Analysis of Worms. **http://www.micsymposium.org/mics_2004/Bajaj.pdf**
16. Mueller, P., B. Yadegari. The Stuxnet Worm. **https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf**
17. Dimov, D., Y. Tzonev. Pass-the-Hash: One of the Most Prevalent Yet Underrated Attacks for Credentials Theft and Reuse. – In: Proc. of ACM International Conference Proceeding Series, Part F132086, 2017, pp. 149-154. ISBN 978-145035234-5. DOI:10.1145/3134302.3134338.
18. Dimov, D., Y. Tzonev. Result Oriented Time Correlation between Security and Risk Assessments, and Individual Environment Compliance Framework. – In: Proc. of International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning Smart Innovation, Systems and Technologies, 2019, pp. 373-383. ISBN 978-3-030-03576-1. DOI:10.1007/978-3-030-03577-8_42.

19. D i m o v, D., Y. T z o n e v. Observing, Measuring and Collecting HDD Performance Metrics on a Physical Machine during Ransomware Attack. – Information & Security: An International Journal, Vol. **47**, 2020, No 3, pp. 317-327. ISSN 0861-5160. DOI:10.11610/isij.4723.
20. P o p c h e v, I., D. O r o z o v a. Towards Big Data Analytics in the e-Learning Space. – Cybernetics and Information Technologies, Vol. **19**, 2019, No 3, pp. 16-24.
21. G n a n a p r a s a n a m b i k a i, L., N. M u n u s a m y. Towards Big Data Analytics Data Pre-Processing and Classification for Traffic Anomaly Intrusion Detection Using NSLKDD Dataset. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 3, pp. 111-119.

Received: 28.12.2021; Second Version: 19.03.2022; Third Version: 17.04.2022; Accepted: 29.04.2022