Epidemic Model and Mathematical Study of Impact of Vaccination for the Control of Malware in Computer Network

Titus Ifeanyi Chinebu1*, Ikechukwu Valentine Udegbe2 and Adanma Cecilia Eberendu2

1Department of Physical Sciences, Federal College of Dental Technology and Therapy, P. M. B. 01473 Trans Ekulu Enugu, Nigeria.
2Department of Computer Science, Madonna University Nigeria, Elele, Nigeria.

Authors’ contributions
This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information
DOI: 10.9734/JAMCS/2021/v36i330348
Editor(s):
(1) Dr. Leo Willyanto Santoso, Petra Christian University, Indonesia.
Reviewers:
(1) Gamal Abdel Nassir Awad Ali Mohamed, University of Stirling, United Kingdom.
(2) A. Vanitha, Sona College of Technology, India.
(3) Putra Wanda, Respati University of Yogyakarta, Indonesia.
Complete Peer review History: http://www.sdiarticle4.com/review-history/66718

Received: 12 January 2021
Accepted: 21 March 2021
Published: 22 April 2021

Abstract
Malware remains a significant threat to computer network. In this paper, we considered the problem which computer malware cause to personal computers with its control by proposing a compartmental model SVEIRS (Susceptible Vaccinated-Exposed-infected-Recovered-Susceptible) for malware transmission in computer network using nonlinear ordinary differential equation. Through the analysis of the model, the basic reproduction number $R_0$ were obtained, and the malware free equilibrium was proved to be locally asymptotical stable if $R_0$ is less than unity and globally asymptotically stable if $R_0$ is less than some threshold using a Lyapunov function. Also, the unique endemic equilibrium exists under certain conditions and the model underwent backward bifurcation phenomenon. To illustrate our theoretical analysis, some numerical simulation of the system was performed with Runge-Kutta fourth order (KR4) method in Matlab. This was used in analyzing the behavior of different compartments of the model and the results showed that vaccination and treatment is very essential for malware control.

*Corresponding author: E-mail: titusifeanyi5432@gmail.com;
Keywords: Epidemic model; malware; vaccination; malicious software; computer network.

1 Introduction

Computer software, or simply software is a set of instruction that tell the computer what to do and collection of data that associated with the computer operations. In other words, computer software can be seen as a set of instructions, routines, and procedures together with data for the computer to perform a sequence of arithmetic or logical operations. Software is also embedded in electronic devices to interact with human. The computer software is made up of system software, which manages the resources of the system and application software (apps) is developed to perform specific task for the users. Software can be developed to replicate itself upon execution in order to cause damages to the computer system. Any software intentionally developed to cause damage to a computer, server, client, or computer network is a malicious software or malware [1].

However, any computer systems infected by malicious software (malware) perform unwanted or altered operations. Malware is an umbrella term used to represent any software purposefully developed for malicious attack such as virus, worms, trojans, adware, spyware [2]. The objectives of malware are to attack vulnerable computer systems thereby gaining admin control, corrupting system files, destroying data, stealing confidential information, or be a nuisance. Malware spreads through the use of infected removable media, downloads from the internet, opening infected e-mail attachments, viewing infected advertisement, visiting an infected website, or clicking executable files. Malware can replicate itself as soon as it enters into a computer system or remain dormant until triggered by user action [1].

Some malware attach itself to a program or a file and has the capability of executing itself to insert its own code thereby modifying other programs in a computing system. Malware propagates itself by infecting other applications on the host computer, inserting malicious code wherever it can (a resident virus does this to programs as they open, whereas, a nonresident virus can infect executable files even if they are not executing).

With the speedy growth of information technology, the development of malicious software thrives [1] from traditional computer viruses to current family of mobile viruses, internet worms, trojans, Adware, Spyware and so on. Malicious software operations can range from pop-up of malicious adverts, tricks that infiltrate a system, to spread itself from system to system without actions by the users, e.g. password theft, data damage and compromising device over networks [3].

According to Bushra and Ahmadi [4], malware growth has reached approximately 1.7 billion within the past decade. Actually, it is difficult to put an exact count on the number of malwares. Malware developers can use different tricks (polymorphic and metamorphic) to make their code appear as a new version.

A biological virus like HIV or HBV cannot reproduce on its own, rather it needs to hijack a cell before it can replicate. Similarly, malware is not a standalone program rather a code snippet that insert itself into other applications. When that application executes the malware code unknowingly, the results range from irritation to disastrous. As the infected application executes (usually at the request of the user), and the malware is loaded into the CPU memory before any of the legitimate executes. Computer Malware is not keen to alert their presence in a computer system. Just as biological virus wants to keep its host alive so that it will continue to use it as a vehicle to reproduce and spread, so too does computer malware attempt to do its damage in the background while the computer still limps along [2].

Under appropriate conditions, computer malware spreads to uninfected computers from the infected computer through many kinds of ways. It enters the computer and gets executed, thereby searching for other programs or storage media in line with the conditions of their infection and target to insert the code. This is to enable it to achieve the purpose of replication. Once the computer is infected and not promptly treated, the malware will spread speedily on the computer and maybe a large number of executable files will be infected.
These infected files become a new source of infection and when data are exchanged with other computers that are not vaccinated over the network, they will be infected. Computer malware can enter any computer through different means such as: an email attachment, file downloads from the internet, connection to a website, mobile hard disk. Since the network has no permanent immunity to the computer malware, they are prone to be infected.

Since 1990 when Tim Berners-Lee invented the World Wide Web (www), the internet has been growing at an exponential rate. The estimate showed that over 1 billion websites exist worldwide and the number of global internet users has exceeded 3 billion according to the online statistical estimates of international websites [5,6] and the number is still growing. Nowadays that the world wide web (www) is used in business activities like online banking and e-commerce, malware can scan the computer hard drive for banking credentials, log the key strokes to steal passwords, turn the computer into a zombie or even encrypt the data and demand a bit coin ransom to restore access [3]. Malware can thwart access to virtually anything; serve devices, services, networks, applications, and even specific transaction within applications [7]. Malware adds proxy server to alter Internet browser settings [2]. When the settings are altered, the malware redirects issues or completely block the Internet connection.

This paper develops a model to detect the problems malware cause to computers on the Internet. Malware vaccine is a software protection system that can inoculate virtually any computer against so called malicious programs.

2 Related Literatures

Computer virus can be associated with the biological virus, therefore formulating a compartmental epidemic model for prediction and control of malware in a computer network with vaccination and natural death is of great importance. Many authors have developed epidemic models on computer malware. These were based on the use of ordinary differential equations or on partial differential equations, which implies that such models are continuous in nature.

Sun [8] was inspired by the research of biological epidemic and he agreed that malware epidemiology aims to study the dynamic of malware over time [9] and analyzed the factors affecting its propagation process [10]. Much effort has also been done on the area of developing mathematical models for malware spread [11], and most existing models for malicious codes are based on deterministic epidemic models [12,9]. For instance, some earlier mathematical models were obtained by the compartmental approach such as epidemic SIS, SIR and SIRS models [13,14].

As stated in Martin del Rey [15], the first mathematical model studies aimed at predicting the behavior of an epidemic of were carried out in time Kephart and White [16,17,18]. Mishra and Saini [19] developed an SEIRS model of computer malware in which they assume that any computer in the network is susceptible to malware infection. their model was an extension of the SIR epidemic models of Diekmann and Heesterbeek [20]. Temporal immunity is considered in their model and it is obtained that the longer the exposed period the system has, the less the chance are that it will be epidemic.

Mishra and Jha [21], formulated an SEIQRS model that is defined with a system of differential equation where Q(t) represents the number of quarantined computers at time t. In their model the number of contacts is influence by the size of the quarantine class, and consequently, but the effective infectious period and the basic reproduction number decreases as the quarantine rate increases.

Mishra and Pandey [22] established an SEIRS model for studying the propagation of computer worms. The main characteristic of their model is the use of vertical transmission in which there is a constant period of temporary immunity of fixed length following by a temporary recovery period in lieu of exponentially distributed period of temporary immunity.
Zhu et al. [23] developed an SIR - type compartmental model in susceptible individuals and infectious individuals removed from the network are introduced. Their work provides an excellent start point for understanding the propagation of computer virus through the interactions between the computers and the external removable devices. Toutonji et al. [24] in their work formulated an SEIRS model which takes into consideration accurate positions for dysfunctional hosts and their replacements in state transmission.

Mishra and Ansari [25] in their e-SIRS epidemic model of virus and worm in a computer network considered latent period, immune period and time for self-replication. Their work also states that when a node is removed from infected class, it recovers temporary and acquire temporary immunity, or the node may vanish, but Yan and Lui [26] in their word considered the recovery from infected class acquiring permanent immunity.

Liu and Zhong [27] considered the features of web malware and formulated a new differential epidemic model to extend the traditional SIR model which added another delitescent compartment to deal with the distributing behavior of malicious sites over network. They finally showed numerically that the spreading of malware links can be managed effectively with proper control strategy.

Rao et al. [28], developed an e-SEIRS epidemic computer network model to study the transmission of malicious code in a computer network and derived the approximate threshold condition (basic reproduction number) to examine the equilibrium and stability of the model. Kumar et al. [29] formed an SEIQRS-V epidemic model of viruses in a computer network. Their model considered quarantine, vaccination and natural death in which they stated that a strong impact of vaccination in the computer network reduces rapidly the spreading behavior of worms and quarantine plays important role in the recovery of the infectious node.

The transformation of the dynamics of computer malware propagation into mathematical language is an effective methodology to understand and analyze the spreading behavior of malware [30]. Modification of these models generated guides for infection prevention by using the concept of epidemiological threshold [31,32].

3 Model Formulation

The total population of computers(nodes) at time $t$ denoted by $N(t)$ is split into five mutually exclusive compartments of susceptible $S(t)$ that can be infected $I(t)$ with an infectious malicious software. Most of these computers are provided with protective temporary immunity through vaccination (anti-virus software) $V(t)$. Once the malicious software enters into the network, the computer node becomes susceptible $S(t)$ and after a certain time delay it become infected $E(t)$ and get infectious $I(t)$. Immunity is obtained when antivirus software used in vaccinating the computer is run after a node gets affected by malware. However, this kind of immunity is usually temporary. Specifically, after running the antivirus software, the computer recovers $R(t)$. When a node is recovered from the infected class, it recovers temporarily, acquiring temporary immunity. Because of malware evolution or secure update failure, recovered computers will become susceptible to malicious infection again. Therefore, we have

$$N(t) = S(t) + V(t) + E(t) + I(t) + R(t)$$

(1)

Computer interaction in the population is modeled using a standard incidence function. For simplification, we assume that newly connected computers to the network are all malware free and are susceptible and is increased by recruitment of computers that are susceptible into the network (at a rate $\Lambda$) and recovered computers that become susceptible to malware attack again network (at a rate $\nu$). The susceptible population is decreased by malware attack (at a rate $\lambda$). Then the infection force of malware attack is given by

$$\lambda = \beta I(t)$$

(2)
and $\beta$ is the infection transmission rate. The susceptible population $S(t)$ is further decreased by the crashing of the nodes due to the reason other than the attack of malware (natural death rate) and is denoted by $\mu$. It is assumed that natural death rate occurs in all the compartments at this rate. $\alpha$ is the passage rate from susceptible class to vaccinated class and those that are not vaccinated is denoted by $(1-\alpha)$. So, we have

$$\frac{dS(t)}{dt} = \Lambda + R(t) - \delta S(t) - (1 - \delta)\lambda S(t) - \mu S(t)$$

the population of vaccinated computers is generated by computers that are vaccinated at rate $\delta$. It is diminished by natural death rate denoted $\mu$ and passage to exposed class due to loss of vaccine immunity (temporary protective immunity secure update failure) at rate $\epsilon$ and this gives

$$\frac{dV(t)}{dt} = \delta S(t) - \mu V(t) - \epsilon AV(t)$$

The population of exposed (delitescent) computers $E(t)$ is increased by the malware attack interaction that affect and subsequently succeed in accessing non vaccinated susceptible computers (at a rate $(1-\delta)\lambda$) and those that their temporary protective immunity wanes (at a rate $\epsilon$). This population is decreased by progression to infectious class (at a rate $\gamma$) and natural death (at a rate $\mu$). This gives

$$\frac{dE(t)}{dt} = (1 - \delta)\lambda S(t) + \epsilon AV(t) - (\mu + \gamma)E(t)$$

The population of infectious computers is generated by computers that progress from exposed class to infectious class at $\gamma$. It is diminished by natural death (at a rate $\mu$) and malware induced death rate (rate of crashing of the nodes due to the attack of viruses) and is denoted by $\alpha$. This is further reduced by computers that recover at rate $\phi$, due to the action of anti-malicious software (Treatment). Therefore, we have

$$\frac{dI(t)}{dt} = \gamma E(t) - (\mu + \phi + \alpha)I(t)$$

The population of recovered class is generated by computers that progressed from the infectious class to recovered class at rate $\phi$ due to the action of anti-malicious software. It is decreased by passage from recovered class to susceptible class at rate $\pi$ and natural death rate $\mu$. So we have

$$\frac{dR(t)}{dt} = \phi I(t) - (\pi + \mu)R(t)$$

Based on the above formulations and assumptions on viruses in nodes of computer network consists of non-linear (deterministic) differential equations

$$\frac{dS(t)}{dt} = \Lambda + \pi R(t) - \delta S(t) - (1 - \delta)\lambda S(t) - \mu S(t)$$

$$\frac{dV(t)}{dt} = \delta S(t) - \mu V(t) - \epsilon AV(t)$$

$$\frac{dE(t)}{dt} = (1 - \delta)\lambda S(t) + \epsilon AV(t) - (\mu + \gamma)E(t)$$

$$\frac{dI(t)}{dt} = \gamma E(t) - (\mu + \phi + \alpha)I(t)$$

(3)
\[
\frac{dR(t)}{dt} = \varphi I(t) - (\pi + \mu)R(t)
\]

With initial condition \(S(0) = S_1, V(0) = V_1, E(0) = E_1, I(0) = I_1, R(0) = R_1\)

Fig. 1. Schematic diagram of the compartmental model of the impact of vaccination for the control of malware in computer network

To formulate the above model, the following assumptions were made:

- we assume that we are dealing with an imperfect system where all attacked computers are secured. Hence, we make room for attack nodes that is likely to be recovered due to strong anti-malicious software.
- the death rate that is not caused by malicious software is constant and equal for any of the compartments of the model.
- vaccinated computers become exposed to malicious software due to loss of temporary immunity (lack of anti-malicious software update)
- when a computer is no longer infectious, it recovers, acquiring transient immunity.

Table 1. Description of variables

| Variables | Interpretation         |
|-----------|------------------------|
| \(S\)     | Susceptible Class       |
| \(V\)     | Vaccinated Class        |
| \(E\)     | Exposed Class           |
| \(I\)     | Infectious Class        |
| \(R\)     | Recovered Class         |

Though we modeled the spread of malicious software in computers and liken it to spread of disease in human population. We are able to do this due to proximity between the computers involved. This proximity between the computers is in network sharing which results in interaction between infected computers and uninfected ones, thus the uninfected computers can get infected by infected ones.

3.1 Basic properties

For model (3) to be meaningful, it is important to prove that all its state variables are non-negative for all time \(t\). In other words, the solution of model (3) with positive initial value will remain positive for all \(t \geq 0\).
Table 2. Description of parameters

| Parameters | Interpretation |
|------------|----------------|
| $\Lambda$  | Recruitment rate into susceptible class |
| $\beta$    | Contact rate |
| $\mu$      | Natural death rate (crashing of computers due to reasons other than the attack of malicious software) |
| $\alpha$   | Malware induced death rate (crashing of computers due to attack of malicious software) |
| $\delta$   | Vaccination rate of susceptible class |
| $\varepsilon$ | Progression rate from vaccinated class to exposed class |
| $\varphi$ | Progression rate from infectious class to recovered class |
| $\pi$      | Progression rate from recovered class to susceptible class |
| $\gamma$   | Progression rate from exposed class to infectious class |
| $\lambda$  | Force of infection |

3.1.1 Positivity of solution and well posedness of the model

Since model (3) monitors computer population in the network, all the state variables and parameters of the model are non-negative. Then we have that

**Theorem 1:** The biologically feasible region $D = \{ (S(t) + V(t) + E(t) + I(t) + R(t)) \in \mathbb{R}_+^5 : N \leq \frac{\Lambda}{\mu} \}$ is positively invariant and attracts all the solutions in $\mathbb{R}_+^5$.

**Proof:** By adding the equations in the model system (3), we have

$$N(t) \leq \Lambda - \mu N - \alpha I(t)$$

but at malware free Equilibrium (MFE), $\alpha I(t) = 0$ and this gives

$$N(t) \leq \Lambda - \mu N$$

The integrating factor is $IF = e^{\int \mu dt} = e^{\mu t}$

Integrating system (4) using the value of the integrating factor we have

$$N(t) \leq \frac{1}{e^{\mu t}} \left( \frac{\Lambda}{\mu} e^{\mu t} + c \right)$$

$$N(t) \leq \frac{\Lambda}{\mu} + ce^{-\mu t}$$

where $c$ is the constant of integration. Using the condition; when $t = 0, N(0) = N_s$, we obtain

$$N_s - \frac{\Lambda}{\mu} \leq c$$

$$N(t) \leq \frac{\Lambda}{\mu} + \left( N_s - \frac{\Lambda}{\mu} \right) e^{-\mu t}$$

Applying Birkhoff and Rota’s [33] theorem on the differential inequality, we have

$$0 \leq N \leq \frac{\Lambda}{\mu} \text{ as } t \to \infty.$$
Thus, D is the positive invariant set under the flow described by model (3), so that no solution path leaves through the boundary of region D. Hence, it is sufficient to consider the dynamic of model (3) in region D. Thus, in this region, the model can be considered as being epidemiologically and mathematically well posed.

3.2 Asymptotic stability of Malware Free Equilibrium (MFE)

At steady state (equilibrium point), each of the equations in (3) are equal to zero. This implies that malware free equilibrium of model (3) is given by

\[ R^*_0 = [S^*, V^*, E^*, I^*, R^*] = [S^*, V^*, 0, 0, 0] \]

Therefore, we have

\[
\begin{align*}
\Lambda &+ \pi R^*(t) - \delta S^*(t) - (1 - \delta) \lambda S^*(t) - \mu S^*(t) = 0 \\
\delta S^*(t) - \mu V^*(t) - \varepsilon A V^*(t) = 0 \\
(1 - \delta) \lambda S^*(t) + \varepsilon A V^*(t) - (\mu + \gamma) E^*(t) = 0 \\
\gamma E^*(t) - (\mu + \varphi + \alpha) I^*(t) = 0 \\
\varphi I^*(t) - (\pi + \mu) R^*(t) = 0 \\
\end{align*}
\]

At steady state where there is no malware (absence of malicious object) is called malware free equilibrium, that is, the point where \( E^* = 0, I^* = 0 \)

Therefore

\[ \varphi I^*(t) - (\pi + \mu) R^*(t) = 0 \implies R^* = 0 \]

Also,

\[ \Lambda + \pi R^*(t) - \delta S^*(t) - (1 - \delta) \lambda S^*(t) - \mu S^*(t) = 0 \implies S^*(t) = \frac{\Lambda}{\mu + \delta} \]

And

\[ \delta S^*(t) - \mu V^*(t) - \varepsilon A V^*(t) = 0 \implies V^* = \frac{\delta \Lambda}{\mu (\mu + \delta)} \]

Then we have that the malware free equilibrium point of the model

\[ H^*_0 = [S^*, V^*, 0, 0, 0] = \left[ \frac{\Lambda}{\mu + \delta}, \frac{\delta \Lambda}{\mu (\mu + \delta)}, 0, 0, 0 \right] \]

3.3 Basic reproduction number

The basic reproduction number \( R_0 \) is a threshold parameter for the linear stability of the malware free equilibrium and is related to the peak and final size of the malware spread. It is defined as the expected number of secondary cases of infection which would occur due to a primary case in a completely susceptible population. If \( R_0 < 1 \), then a few infected computers introduced into a completely susceptible nodes will on average fail to spread the malicious software, and the malware will not spread. On the other hand, when \( R_0 > 1 \), then the number of infected computers will increase and the malware will spread.

The linear stability of \( H^*_0 \) can be established using the next generation operator method on system (3) [31,34]. Using the notation in Van den Driessche and Watmough [34], it follows that \( F \) and \( V \) which stands for new infection and remaining transition terms respectively, then for the transmission part we have
\[ E = (1 - \delta)\beta I(t)S(t) + \epsilon\beta I(t)V(t) \]
\[ I = 0 \]
\[ R = 0 \]

\[ \Rightarrow E = \beta I(t)[(1 - \delta)S^*(t) + \epsilon\beta V^*(t)] \]

Then

\[ F = \beta[(1 - \delta)S^*(t) + \epsilon\beta V^*(t)] \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \]

Also, for the transition part we have

\[ E = (\mu + \gamma)E = AE \]
\[ I = -\gamma E + (\mu + \varphi + \alpha)I = -\gamma E + BI \]
\[ R = -\varphi I + (\pi + \mu)R = -\varphi I + G_iR \]
\[ V = \begin{bmatrix} A & 0 & 0 \\ -\gamma & B & 0 \\ -\varphi & 0 & C_1 \end{bmatrix} \]

\[ V^{-1} = \begin{bmatrix} 1 \\ \frac{\gamma}{AB} \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{B} & 0 & 0 \\ \frac{\varphi}{BC_1} & \frac{1}{C_1} & 0 \end{bmatrix} \]

\[ FV^{-1} = \beta \left[(1 - \delta)\frac{\Lambda}{\mu + \delta} + \epsilon\beta \frac{\delta\Lambda}{\mu(\mu + \delta)}\right] \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \frac{\gamma}{AB} \\ \frac{1}{B} \\ \frac{\varphi}{BC_1} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \]

The threshold quantity \( R_0 \) is the reproduction number for malicious software in computer network. Then we claim the following result:

\[ R_0 = \beta(1 - \delta)\frac{\Lambda}{\mu + \delta} + \epsilon\beta \frac{\delta\Lambda}{\mu(\mu + \delta)} \]
\[ R_0 = \beta\gamma\Lambda \left[\frac{\mu(1 - \delta) + \epsilon\delta}{\mu(\mu + \delta)(\mu + \gamma)(\mu + \varphi + \alpha)}\right] \]

Since the basic reproduction ratio is the dominant eigenvalue of the next generation matrix of \( FV^{-1} \) we have

\[ R_0 = \beta(1 - \delta)\frac{\Lambda}{\mu + \delta} + \epsilon\beta \frac{\delta\Lambda}{\mu(\mu + \delta)} \]
\[ R_0 = \beta\gamma\Lambda \left[\frac{\mu(1 - \delta) + \epsilon\delta}{\mu(\mu + \delta)(\mu + \gamma)(\mu + \varphi + \alpha)}\right] \]
Theorem 2: The malware free Equilibrium (MFE) D of the malicious software is locally asymptotically stable (LAS) if $R_0 < 1$ and unstable if $R_0 > 1$.

Proof: Biologically speaking, theorem implies that malicious software can be eliminated from the nodes (when $R_0 < 1$) if the initial size of the nodes of the model is in the basin of attraction of D. Now let us analyze the basic reproduction ratio $R_0$. The parameter $\delta$ is important for the prevalence of malware attack. It influences the dynamic of malicious software, in particular the equilibrium states, including the state of susceptible, infected and exposed. It is evident from system (7) that

$$\lim_{\delta \to 1} R_0 = \beta \gamma \Lambda \left[ \frac{\mathcal{E}}{\mu(\mu + 1)(\mu + \gamma)(\mu + \varphi + \alpha)} \right]$$

(8)

Thus, a sufficiently effective vaccination (anti-malicious software with constant update) can lead to effective malware control if it results in making the right-hand side of (8) less than unity, that is;

$$\beta \gamma \Lambda \left[ \mu(1 - \delta) + \varepsilon \delta \right] < \mu(\mu + \delta)(\mu + \gamma)(\mu + \varphi + \alpha)$$

$$\mathcal{E} < \frac{\mu(1 + \mu)(\mu + \gamma)(\mu + \varphi + \alpha)}{\beta \gamma \Lambda}$$

Further, sensitivity analysis on the vaccination parameter of the susceptible computers is carried out by computing the partial derivative of $R_0$ with respect to $\delta$ yielding

$$\frac{\partial R_0}{\partial \delta} = - \frac{\beta \gamma \Lambda}{\mu(\mu + \gamma)(\mu + \varphi + \alpha)} \left[ \delta^2 + \mu(1 - \mathcal{E}) \right]$$

(9)

Thus, increasing the vaccination parameter $\delta$ will have a positive impact in reducing the propagation of malware in computer population. To find better control strategies for malware attack, we would like to see what parameters can reduce the basic reproduction ratio $R_0$ given by (7).

3.4 Global stability of MFE of the model

Here we shall study the global stability of the MFE $H_0^*$ of system (3).

Theorem 3: The MFE of system (3) given by $H_0^*$ is globally asymptotically stable (GAS) in D if and only if $R_0 \leq 1$.

Proof: Considering the following LaSalle [35]Lyapunov candidate function as in [36], we have

$$\mathcal{L}(E, I) = a_1 E + a_2 I$$

(10)

where $a_1 = B$ and $a_2 = \beta [(1 - \delta)S + \varepsilon V]$. Its time derivatives along the trajectories of the system (3) satisfies

$$\mathcal{L}(E, I) = a_1 E + a_2 I$$

$$= a_1 \beta [(1 - \delta)S + \varepsilon V] - (\mu + \gamma)E + a_2 (\gamma E - BI)$$

(11)

Since the state variables of the model when the malware attack is endemic in the population do not exceed the state variable of the model in a population free of malware, one has that

$$(1 - \delta)S + \varepsilon V \leq (1 - \delta)S_1 + \varepsilon V_1$$
This gives
\[ \dot{L} \leq [a_1\beta((1 - \delta)S_1 + \varepsilon V_1) - a_2B]I - [a_1(\mu + \gamma) - a_2\gamma]E \] (12)

Now, plugging the positive constants \( a_1 \) and \( a_2 \) given in (12) we finally obtain
\[ \dot{L} \leq [B\beta((1 - \delta)S_1 + \varepsilon V_1) - B\beta((1 - \delta)S_1 + \varepsilon V_1)]I + [\gamma\beta((1 - \delta)S_1 + \varepsilon V_1) - AB]E \]
\[ \dot{L} \leq [\gamma\beta((1 - \delta)S_1 + \varepsilon V_1) - AB]E \]
\[ \leq [\gamma\beta\left(\frac{1 - \delta}{\mu + \delta} + \frac{\delta\Lambda}{\mu(\mu + \delta)}\right) - AB]E \]
\[ \leq AB\left[\gamma\beta\left(\frac{1 - \delta}{\mu(\mu + \delta)}\right) - 1\right]E \]
\[ \leq AB(R_0 - 1)E \]
\[ \dot{L} \leq (\mu + \gamma)(\mu + \varphi + \alpha)(R_0 - 1)E \] (13)

Thus, \( \dot{L} \leq 0 \) when \( R_0 \leq 1 \). By LaSalle [37] Lyapunov invariance principle, the largest invariant set in \( D \) contained in \( \{(S(t) + V(t) + E(t) + I(t) + R(t)) \in \mathbb{R}_+^5, \dot{L} = 0\} \) is reduced to the MFE. This proves the global asymptotic stability on \( D \) [38]. Since \( D \) is absorbing this proves the global asymptotic stability on the non negative orthant when \( R_0 \leq 0 \).

### 3.5 Existence and stability of Malware Endemic Equilibrium (MEE)

To establish the existence of the malware endemic equilibrium of the model (3), let \( H_0^* = [S^*, V^*, E^*, I^*, R^*] \) represent any arbitrary malware endemic equilibrium of the model (3). The equation in (3) are solved in terms of malware force of infection at steady state to give
\[ R^* = \frac{\phi I^*}{\pi + \mu} \] (14i)
\[ S^* = \frac{\Lambda(\pi + \mu) + \pi\phi I^*}{(\pi + \mu)((\delta + \mu) + (1 - \delta)\beta I^*)} \] (14ii)
\[ V^* = \frac{\delta(\Lambda(\pi + \mu) + \pi\phi I^*)}{(\mu + \varepsilon\beta I^*)(\pi + \mu)((\delta + \mu) + (1 - \delta)\beta I^*)} \] (14iii)
\[ E^* = \frac{1}{\mu + \gamma}\left[\beta(1 - \delta)\left(\frac{\Lambda(\pi + \mu) + \pi\phi I^*}{(\pi + \mu)((\delta + \mu) + (1 - \delta)\beta I^*)}\right)
+ \varepsilon\beta\left(\frac{\delta(\Lambda(\pi + \mu) + \pi\phi I^*)}{(\mu + \varepsilon\beta I^*)(\pi + \mu)((\delta + \mu) + (1 - \delta)\beta I^*)}\right)\right]I^* \] (14iv)
$$I^{**} = \frac{\gamma}{(\mu + \varphi + \alpha)} \left[ \frac{1}{\mu + \gamma} \left( \frac{\Lambda(\pi + \mu) + \pi \varphi^{**}}{(\pi + \mu)((\delta + \mu) + (1 - \delta)\beta^{**})} \right) \right] + \varepsilon \beta \left[ \frac{\delta(\Lambda(\pi + \mu) + \pi \varphi^{**})}{(\mu + \varepsilon \beta^{**})(\pi + \mu)((\delta + \mu) + (1 - \delta)\beta^{**})} \right] I^{**}$$  \hspace{1cm} (14v)

From sub equation (14v) we have

\[ \Rightarrow \varepsilon \beta^2(1 - \delta)[\gamma \pi \varphi - (\mu + \gamma)(\pi + \mu)(\mu + \varphi + \alpha)]I^{* - 2} \]

\[ + \frac{[\gamma(\Lambda \varepsilon \beta(1 - \delta)(\pi + \mu) + \varepsilon \beta \pi \varphi + \pi \varphi \mu(1 - \delta))] - (\mu + \gamma)(\pi + \mu)(\mu + \varphi + \alpha)(\mu(1 - \delta) + \varepsilon)(\delta + \mu)] \beta^{**} + (\pi + \mu)[\gamma \Lambda \beta(\mu(1 - \delta) + \varepsilon \delta) - \mu(\mu + \gamma)(\delta + \mu)](\mu + \varphi + \alpha)] \]

Therefore, \( I^{**} \) is the positive solution of the following equation:

\[ b_1 I^{**^2} + b_2 I^{**} + b_3 = 0 \]  \hspace{1cm} (15)

Where

\[ b_1 = \varepsilon \beta^2(1 - \delta)[\gamma \pi \varphi - (\mu + \gamma)(\pi + \mu)(\mu + \varphi + \alpha)] \]

\[ b_2 = \beta \gamma (\Lambda \varepsilon \beta(1 - \delta)(\pi + \mu) + \varepsilon \beta \pi \varphi + \pi \varphi \mu(1 - \delta)) - (\mu + \gamma)(\pi + \mu)(\mu + \varphi + \alpha)(\mu(1 - \delta) + \varepsilon)(\delta + \mu) \]

\[ b_3 = (\pi + \mu)(R_0 - 1) \]  \hspace{1cm} (16)

From system (16) it follows that \( b_3 > 0 \) whenever \( R_0 > 1 \). Thus, the number of positive real roots for (16) depends on the signs of \( b_1 \) and \( b_2 \). This can be analyzed using Descartes' rule of signs on quadratic function

\[ f(I^{**}) = b_1 I^{**^2} + b_2 I^{**} + b_3 \]

The different possibilities for the roots \( f(I^{**}) \) are tabulated in Table 3.

**Table 3. Number of possible positive real roots of \( f(I^{**}) \) for \( R_0 < 1 \) and \( R_0 > 1 \)**

| Cases | \( b_1 \) | \( b_2 \) | \( b_3 \) | \( R_0 \) | Number of sign changes | Number of positive real roots |
|-------|-----------|-----------|-----------|----------|------------------------|-----------------------------|
| 1     | +         | +         | +         | > 1      | 0                      | 0                           |
| 2     | +         | +         | -         | < 1      | 1                      | 1                           |
| 3     | +         | -         | +         | > 1      | 2                      | 2                           |
| 4     | +         | -         | -         | < 1      | 1                      | 1                           |
| 5     | -         | +         | +         | > 1      | 1                      | 1                           |
| 6     | -         | +         | -         | < 1      | 2                      | 2                           |
| 7     | -         | -         | +         | > 1      | 1                      | 1                           |
| 8     | -         | -         | -         | < 1      | 0                      | 0                           |

Hence, we have established the following result.

System (3) has a unique endemic equilibrium point where one of the cases 2, 4, 5 and 7 in Table 3 are satisfied. The existence of multiple endemic equilibrium point when \( R_0 < 1 \) is shown in Table 3 which suggests the possibility of backward bifurcation [39].
Theorem 4: Castillo-Chavez and Song [40] consider the following general system of differential equations with parameter \( \phi \).

\[
\frac{dx}{dt} = f(x, \phi), f: \mathbb{R}^n \times \mathbb{R} \rightarrow \mathbb{R} \text{ and } f \in C^2(\mathbb{R}^n, \mathbb{R})
\]  

(17)

Without loss of generality, it is assumed that 0 is an equilibrium for system (17) for all values of the parameter \( \phi \), that is \( f(0, \phi) \equiv 0 \).

Assume

1. \( Q = D_x f(0,0) = \frac{\partial f_i}{\partial x_j}(0,0) \) is the linearized matrix of system (17) around the equilibrium 0 with \( \phi \) evaluated at 0. Zero is a simple eigenvalue of \( Q \) and all other eigenvalues of \( Q \) have negative real parts;
2. Matrix \( Q \) has a nonnegative right eigenvalue \( w \) and left eigenvalue \( v \) corresponding to the zero eigenvalue. Let \( f_x \) be the \( k \)th component of \( f \) and

\[
a = \sum_{k, i, j = 1}^n v_k w_i w_j \frac{\partial^2 f_k}{\partial x_i \partial x_j}(0,0)
\]

\[
b = \sum_{k, i, j = 1}^n v_k w_i \frac{\partial^2 f_k}{\partial x_i \partial \phi}(0,0)
\]

(18)

The local dynamics of the system around the equilibrium point 0 is totally determined by the signs of \( a \) and \( b \).

1. \( a > 0, b > 0 \). When \( \phi < 0 \) with \( |\phi| \ll 1 \), 0 is locally asymptotically stable and there exists a positive unstable equilibrium; when \( 0 < \phi \ll 0 \), 0 is unstable and there exists a negative locally asymptotically stable equilibrium.
2. \( a < 0, b < 0 \). When \( \phi < 0 \) with \( |\phi| \ll 1 \), 0 is unstable; when \( 0 < \phi \ll 1 \), 0 is locally asymptotically stable equilibrium, and there exists a positive unstable equilibrium.
3. \( a > 0, b < 0 \). When \( \phi < 0 \) with \( |\phi| \ll 1 \), 0 is unstable and there exists a locally asymptotically stable negative equilibrium when \( 0 < \phi \ll 1 \), 0 is stable and a positive unstable equilibrium appears.
4. \( a > 0, b < 0 \). When \( \phi \) changes from negative to positive, 0 changes its stability from stable to unstable. Correspondingly a negative unstable equilibrium becomes positive and locally asymptotically stable.

to apply the above result, the following simplifications and changes of variables are made on system (3).

Let \( S(t) = x_1, V(t) = x_2, E(t) = x_3, I(t) = x_4, R(t) = x_5 \), moreover, by using vector notation \( x = (x_1, x_2, x_3, x_4, x_5) \), the system (3) can be written in the form \( \frac{dx}{dt} = (f_1, f_2, f_3, f_4, f_5)^T \) as follows.

\[
\frac{dx_1}{dt} = f_1 = \Lambda + \pi x_5 - \delta x_1 - (1 - \delta) \beta x_1 x_4 - \mu x_1
\]

\[
\frac{dx_2}{dt} = f_2 = \delta x_1 - \mu x_2 - \varepsilon \beta x_2 x_4
\]

\[
\frac{dx_3}{dt} = f_3 = (1 - \delta) \beta x_1 x_4 + \varepsilon \beta x_2 x_4 - (\mu + \gamma) x_3
\]

\[
\frac{dx_4}{dt} = f_4 = \gamma x_3 - (\mu + \varphi + \alpha) x_4
\]

(19)
choose $\beta = \beta^*$ as a bifurcation parameter. Solving for $\beta^*$ from $R_0 = 1$ gives

$$
\beta^* = \frac{\mu(\mu + \delta)(\mu + \gamma)(\mu + \varphi + \alpha)}{\beta \gamma \Lambda \mu(1 - \delta) + \varepsilon \delta}
$$

The Jacobian matrix of system (3) evaluated at the disease-free equilibrium $H_0^*$ with $\beta = \beta^*$ is given by

$$
J_{\beta} =
\begin{bmatrix}
-(\mu + \delta) & 0 & 0 & -\beta(1 - \delta) \left( \frac{\Lambda}{\mu + \delta} \right) & \pi \\
\delta & -\mu & 0 & -\varepsilon \beta \delta \Lambda & 0 \\
0 & 0 & -\beta(\mu + \gamma) & \beta \left( \frac{\Lambda(1 - \delta)}{\mu + \delta} + \varepsilon \delta \Lambda \right) & 0 \\
0 & 0 & \gamma & -\left( \mu + \varphi + \alpha \right) & 0 \\
0 & 0 & 0 & \varphi & \pi + \delta
\end{bmatrix}
$$

The Jacobian matrix $J_{\beta}$ of the linearized system has a single zero eigenvalue with all other eigenvalues having real part. For the case when $R_0 = 1$, using the technique in Castillo-Chavez and Song [40], it can be shown that the matrix $J_{\beta}$ has a right eigenvector (corresponding to the zero eigenvalue), given by $w = [w_1, w_2, w_3, w_4, w_5]^T$ and we obtain

$$
\begin{bmatrix}
-g & 0 & 0 & -C_1 & \pi \\
\delta & -\mu & 0 & -d & 0 \\
0 & 0 & -A & h & 0 \\
0 & 0 & \gamma & -B & 0 \\
0 & 0 & \varphi & -C_2
\end{bmatrix}
\begin{bmatrix}
w_1 \\
w_2 \\
w_3 \\
w_4 \\
w_5
\end{bmatrix} = \lambda \begin{bmatrix}
w_1 \\
w_2 \\
w_3 \\
w_4 \\
w_5
\end{bmatrix}
$$

Where

$$
g = (\delta + \mu), B = (\mu + \varphi + \alpha), d = \frac{\beta \Lambda \delta \varepsilon}{\mu(\mu + \delta)}, C_1 = \beta \Lambda(1 - \delta) \frac{1}{\mu + \delta}, \Lambda = \mu + \gamma,
$$

$$
h = \beta \left( \frac{\Lambda(1 - \delta)}{\mu + \delta} + \frac{\Lambda \delta \varepsilon}{\mu(\mu + \delta)} \right), C_2 = \pi + \mu
$$

Therefore, we obtain

$$
\begin{aligned}
w_1 &= \frac{[\pi \gamma C_1 C_2] w_3}{g B C_2} \\
w_2 &= \frac{[\delta \pi \gamma C_1 C_2 - \delta d C_2] w_3}{\mu g B C_2} \\
w_3 &= w_3 > 0 \\
w_4 &= \frac{\gamma w_2}{B} \\
w_5 &= \frac{\gamma w_4}{B C_2}
\end{aligned}
$$

(20)
Similarly, the component of the left eigenvector of $T$ (corresponding to the zero eigenvalue, denoted by $v = (v_1, v_2, v_3, v_4, v_5)$ are given by

$$
\begin{pmatrix}
v_1 & v_2 & v_3 & v_4 & v_5
\end{pmatrix}
\begin{pmatrix}
g & 0 & -C_1 & \pi \\
\delta -\mu & 0 & -d & 0 \\
0 & 0 & -A & h & 0 \\
0 & 0 & \gamma & -B & 0 \\
0 & 0 & 0 & \phi & -C_2
\end{pmatrix}
$$

Then we have

$$
\begin{cases}
v_1 = 0 \\
v_2 = 0 \\
v_3 = v_5 > 0 \\
v_4 = \frac{h}{\delta} v_3 \\
v_5 = 0
\end{cases}
$$

(21)

**Computation of $\alpha$**

By computing the second order non zero partial derivative of $f$ at malware free equilibrium (MFE) point, we have

$$
\frac{\partial^2 f_3}{\partial x_3 \partial x_j} = 0; j = 1, 2, 3, 5
$$

$$
\frac{\partial^2 f_3}{\partial x_2 \partial x_j} = 0; j = 1, 2, 3, 5
$$

$$
\frac{\partial^2 f_3}{\partial x_3 \partial x_j} = 0; j = 1, 2, 3, 4, 5
$$

$$
\frac{\partial^2 f_3}{\partial x_4 \partial x_j} = 0; j = 3, 4, 5
$$

$$
\frac{\partial^2 f_3}{\partial x_5 \partial x_j} = 0; j = 1, 2, 3, 4, 5
$$

Where as

$$
\frac{\partial^2 f_3}{\partial x_3 \partial x_4} = \frac{\partial^2 f_3}{\partial x_4 \partial x_1} = \beta(1 - \delta) \text{ and } \frac{\partial^2 f_3}{\partial x_3 \partial x_2} = \frac{\partial^2 f_3}{\partial x_4 \partial x_2} = \beta \varepsilon
$$

Similarly

$$
\frac{\partial^2 f_4}{\partial x_3 \partial x_j} = 0; j = 1, 2, 3, 4, 5
$$

$$
\frac{\partial^2 f_4}{\partial x_2 \partial x_j} = 0; j = 1, 2, 3, 4, 5
$$
\[
\frac{\partial^2 f_a}{\partial x_i \partial x_j} = 0; f = 1, 2, 3, 4, 5
\]
\[
\frac{\partial^2 f_a}{\partial x_i \partial x_j} = 0; f = 1, 2, 3, 4, 5
\]
\[
\frac{\partial^2 f_a}{\partial x_i \partial x_j} = 0; f = 1, 2, 3, 4, 5
\]

Then
\[
a = v_3 \sum_{i,j=1}^5 w_i w_j \frac{\partial^2 f_3}{\partial x_i \partial x_j} (0,0) + v_4 \sum_{i,j=1}^5 w_i w_j \frac{\partial^2 f_4}{\partial x_i \partial x_j} (0,0)
\]
\[
a = 2v_3 (w_1 w_4 \beta (1 - \delta) + w_2 w_4 \beta \varepsilon) + v_3 (0)
\]
\[
a = 2v_3 \left[ \frac{\pi \phi y - C_1 C_2 \gamma w_3 (\gamma w_3)}{gBC_2} \right] \frac{\beta (1 - \delta)}{B} + \left( \frac{\pi \phi y \delta - C_1 C_2 \gamma w_3}{gBC_2} \right) \frac{dy w_3}{B} \frac{\gamma w_3}{\mu B} \beta \varepsilon
\]
\[
= 2v_3 \left[ \frac{\pi \phi y - C_1 C_2 \gamma}{gBC_2} \right] \frac{\beta y}{B} (1 - \delta) + \left( \frac{\pi \phi y - C_1 C_2 \gamma}{gBC_2} \right) \frac{\beta y}{B} \frac{\beta \varepsilon}{\mu B} \frac{dy y}{B} \frac{w_3^2}{B}
\]
\[
= 2\beta y \left[ \frac{\pi \phi y - C_1 C_2 \gamma}{\mu gBC_2} \right] \left( \frac{\mu (1 - \delta) + \beta \varepsilon}{\mu + \varepsilon} \right) \frac{w_3^2}{B}
\]
\[
= 2\beta y \left[ \frac{\pi \phi y (\mu + \delta) - \left( \beta \Lambda (1 - \delta) \gamma \right)}{\mu (\mu + \delta)(\mu + \phi + \alpha)(\sigma + \mu)} \right] \left( \mu (1 - \delta) + \beta \varepsilon \right)
\]
\[
= 2\beta y \left[ \frac{\pi \phi y (\mu + \delta) - \left( \beta \Lambda (1 - \delta) \gamma \right)}{\mu (\mu + \delta)(\mu + \phi + \alpha)(\sigma + \mu)} \right] \frac{w_3^2}{B}
\]
\[
= 2\beta y \left[ \frac{\pi \phi y (\mu + \delta)}{\mu (\mu + \delta)(\mu + \phi + \alpha)(\sigma + \mu)} \right] \frac{w_3^2}{B}
\]
\[
= 2\beta y \left[ \frac{\pi \phi y (\mu + \delta)}{\mu (\mu + \delta)(\mu + \phi + \alpha)(\sigma + \mu)} \right] \frac{w_3^2}{B}
\]
\[
= 2\beta y \left[ \frac{\pi \phi y (\mu + \delta)}{\mu (\mu + \delta)(\mu + \phi + \alpha)(\sigma + \mu)} \right] \frac{w_3^2}{B}
\]

87
Computation of $b$

To compute $b$ we need to find the second order derivative of $f_3$ and $f_4$ with respect to $x_i$ and $\beta^*$ at the disease-free equilibrium point. Direct computation shows

\[
\frac{\partial^2 f_3}{\partial x_i \partial \beta} = 0; \quad j = 1, 2, 3, 5 \\
\frac{\partial^2 f_4}{\partial x_i \partial \beta} = 0; \quad j = 1, 2, 3, 4, 5 \\
\frac{\partial^2 f_3}{\partial x_i \partial \beta} = \frac{\Lambda(\mu(1 - \delta) + \varepsilon \delta)}{\mu(\mu + \delta)} \\
b = \sum_{i=1}^{5} v_3 w_4 \frac{\partial^2 f_3}{\partial x_i \partial \beta}(0,0) \\
b = v_3 w_3 \left[ \frac{\Lambda(\mu(1 - \delta) + \varepsilon \delta)}{\mu(\mu + \delta)} \right] \\
b = \frac{\Lambda(\mu(1 - \delta) + \varepsilon \delta)}{\mu(\mu + \delta)(\mu + \varphi + \alpha)} v_3 w_3 > 0
\]

Since $b$ is positive, it follows that the sign of $b$ determines the local dynamic around the malware free equilibrium for $\beta = \beta^*$. Based on theorem 4, system (3) will undergo backward bifurcation [41].

**Theorem 5:** The computer malware model system (3) exhibits backward bifurcation at $R_0 = 1$ whenever $a$ is positive.

![Backward bifurcation phenomenon](image)

**Fig. 2.** Backward bifurcation phenomenon

The following parameter values were used to simulate the bifurcation diagram: $\Lambda = 0.01$, $\beta = 0.09$, $\mu = 0.05$, $\alpha = 0.035$, $\delta = 0.65$, $\varepsilon = 0.55$, $\varphi = 0.35$, $\pi = 0.01$, $\gamma = 0.45$. Observe that $a > 0 \iff R_0 < T$, where
Moreover, \( T = 1 \) gives,
\[
\alpha = \sqrt{Z} - (\mu + \varphi) = \alpha^*
\]
Where
\[
Z = \frac{2\beta \gamma (\mu + \delta)[\mu \varphi \gamma (\mu + \delta) - \gamma \beta \Lambda \delta^2(\pi + \mu)]}{\mu^2(\mu + \delta)(\pi + \mu)(\mu + \varphi + \alpha)(1 - \delta)(\mu + \gamma)}
\]
Hence, if the malware attack induced death rate satisfies \( 0 \leq \alpha \leq \alpha^* \), then the malware attack can be eradicated provided \( R_0 < 1 \).

4 Discussion

In this section, we conducted numerical simulations to confirm the theoretical predictions discussed in the previous section using RungeKutta method of order four (RK4) in Matlab. The table below shows the set of parameter values which were used. In order to support the analytical results, graphical representations showing the graphs of different state variables are provided.

**Table 4. The Parameter values used for the numerical simulation of the control of malware in computer network**

| Parameters | Description                                                                 | Range of value  |
|------------|-----------------------------------------------------------------------------|-----------------|
| \( \Lambda \) | Recruitment rate into susceptible class                                      | 0.01 – 0.30     |
| \( \beta \)  | Contact rate                                                                | 0.09 – 0.30     |
| \( \mu \)   | Natural death rate (crashing of computers due to reasons other than the attack of malicious software) | 0.05 – 0.10     |
| \( \alpha \) | Malware induced death rate (crashing of computers due to attack of malicious software) | 0.035 – 0.20    |
| \( \delta \) | Vaccination rate of susceptible class                                       | 0.60 – 0.65     |
| \( \varepsilon \) | Progression rate from vaccinated class to exposed class                     | 0.20 – 1.20     |
| \( \varphi \) | Progression rate from infectious class to recovered class                   | 0.35 – 1.80     |
| \( \pi \)   | Progression rate from recovered class to susceptible class                  | 0.01 – 0.20     |
| \( \gamma \) | Progression rate from exposed class to infectious class                     | 0.30 – 0.45     |

**Fig. 3(a-c). Simulation of the basic reproduction number with control**
The following parameter values were used to simulate the basic reproduction number $R_0$ with different rate of $\delta$ and $\varphi$ where $\delta$ and $\varphi$ are represented with $a_5$ and $b_2$ respectively. It will be observed that vaccination (installation and constant updating of anti malware) and treatment (scanning) reduces the value of the $R_0$ effectively. Notice that integrated control works better than either of the control measures.

### Fig. 4. Simulation of the basic reproduction number without control

The following are parameter values used for the simulation of the basic reproduction number $R_0$ when there is loss of temporary immunity $\langle E \rangle$, where $E$ is represented with $b_1$. It will be seen that without control, $R_0$ will continuously increase and this simply means that the malware attack cannot be eliminated from the computers.

The initial values for the susceptible, vaccinated, exposed, infected and recovered were $S(0) = 30, V(0) = 5, E(0) = 3, I(0) = 0, R(0) = 2$ [21]. Also, we considered the initial values $S(0) = 65, V(0) = 20, E(0) = 10, I(0) = 0, R(0) = 5$ as in [42]. The behaviors of susceptible, vaccinated, exposed, infected and recovered compartments with respect to time as in Figs. 5, 7, 8, 9 and 10 with initial conditions from [42] and Fig. 6 with initial conditions from [21].

### Fig. 5(a-f). Simulation of the dynamic behavior of model system (3), generated in Matlab
Fig. 6. Simulation of the dynamic behavior of model system (3), generated in Matlab

Fig. 7. Simulation of the dynamic behavior of model system (3), generated in Matlab

Fig. 8. Simulation of the dynamic behavior of model system (3), generated in Matlab
From Fig. 5(a–f) and Fig. 7, we see that as the number of vaccinated computers increases, it reduces the infected compartment, thereby increasing the recovered compartment. High recovery rate from vaccinated compartment implies that more recently updated computers are present in the network. This simply means that updated antimalware gives immunization from malware attack and thus, to get immunization, users must update their antimalware regularly and on time. Fig. 6 shows the behaviors of V, E and I from which we observe that as the computers are strongly immunized with protective antimalware, the number of exposed and infected computers will be reduced and this helps to eradicate the attack from malware.

The effect of V, I and R is observed and depicted in Fig. 7 whereas, the effect of V, and R is depicted in Fig. 8. Vaccination and treatment play an important role for the protection from malicious objects and recovery of infected computers. When the computers are highly infected by different kind of malicious objects, treatment is the best option. The computers are treated with updated antimalware. Also, the effect of V and I
is observed and depicted in Fig. 9 and finally the effect of I and R is in Fig. 10. It was observed that the more we vaccinate the susceptible computers and update the vaccine regularly, the lesser they are infected with malicious objects. Therefore, vaccinated computers may become susceptible again due to lack of anti-malicious software with latest signature. In other words, to get the system, malware free (protected), we must update the antimalware regularly.

5 Conclusion

This model considers the incorporation of vaccination and treatment as the control measure and it also assume that every newly connected computer to the network is vaccinated. Through the analysis of the model, it was showed that there exists a domain in which the model is mathematically and epidemiologically well posed. The next generation operator was used to derive the basic reproduction number $R_0$ which is the average number of new cases that one infected computer will generate. The malware free equilibrium of the model was proved to be locally asymptotically stable whenever $0 < R_0 < 1$. It is also, showed that the malware free equilibrium is globally asymptotically stable provided that the basic reproduction number is less than some threshold. The unique endemic equilibrium point was shown to exist under certain conditions. It was shown that the model undergoes backward bifurcation phenomenon. Through the numerical analysis, it was observed that use of vaccine and treatment is very important in controlling the spread of malware in computer network. Thus, with effective vaccination (installation of anti-malicious software and constant updates) and treatment (scanning), the number of malware attack and its induced death rate will be reduced. As a future work, we look into applying optimal control with vaccination and treatment.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Vijayanand CD, Aninlal KS. Impact of malware in modern security. International Journal of Scientific Research and Engineering Development. 2019;2(3):593-600. ISSN: 2581-7175.

[2] Microsoft. Microsoft Security Intelligence Report. 2018;23. Available:https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf Accessed June 16, 2020.

[3] Weinberger S. Computer Security: Is this the Start of Cyber Warfare? Nature. 2011;474:142-145.

[4] Bushra IM, Ahmadi AIA. Mal Classifier. Malware Family Classification Using Network Flow Sequence Behavior; 2018. Available:http://ieeexplore.ieee.org/abstract/document/8376209

[5] Internet Live Stats; 2016. Available:www.internetlivestat.com.

[6] Murphy J, Roser M ; 2016. Internet Published Online at our world in data.org Available:http://ourworldindata.orginternet.
[7] Murphy J, Roser M. Internet; 2019. Published online at ourworldindata.org. Available: http://ourworldindata.org/internet

[8] Sun GO. Pattern Formation of Epidemic Model with Diffusion. Nonlinear Dyn. 2012;69:1097-1104.

[9] Liu W, Liu C, Yang Z, Liu X, Zhang Y, Wei Z. Modeling the propagation of Mobile Malware on Complex Network. Commun. Nonlinear Sci. 2016;37:249-264.

[10] Carter KM, Idika N, Streilein WW. Probabilistic threat propagation for network security. IEEE T. Inf. Foren. Sec. 2014;9(9):1394-1405.

[11] Gil S, Kott A, Barabasi AL. A genetic Epidemiology Approach to Cyber-security. Sci. Rep. 2014;4:56-59.

[12] Mishra AK, Verma M, Sharma A. Capturing the interplay between malware and antimalware in a computer network. Appl. Math. Comput. 2014;229:340-349.

[13] Li C, Van de Bovenkamp R, Van Mieghem P. Susceptible-infected-susceptible model: A comparison of N-intertwoned and heterogeneous mean-field approximations. Phys. Rev. E. 2012;86:026116.

[14] Parshani R, Carmi S, Harlin S. Epidemic Threshold for the Susceptible-Infected-Susceptible model on Random networks. Phys. Rev. Lett. 2010;104(250):258701.

[15] Martin del Rey A. Mathematical modeling of propagation of malware: A review security and communication Networks. Wiley Online Library. 2015;8:2561-2579. DOI: 10.1002/sec.1186

[16] Kephart JO, White SR. Directed-graph epidemiological models of computer virus prevalence. Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA. 1991;343-359.

[17] Kephart JO, White SR. Measuring and modeling computer virus prevalence. Proceedings of IEEE Symposium on Security and Privacy Oakland, CA. 1993;2-15.

[18] Kephart JO, White SR, Chess DM. Computers and Epidemiology. IEEE Spectrum. 1993;30:20-26.

[19] Mishra BK, Saini DK. SEIRS Epidemic model with Delay for Transmission of Malicious Object in computer Network. Applied Mathematics and Computation. 2007;188:1476-1482.

[20] Diekmann O, Heesterbeek JAP. Mathematical Epidemiology of Infectious Diseases. John Wiley and sons:Chichester, Wes Sussex, England ; 2000.

[21] Mishra BK, Jha N. SEIQS model for the transmission of malicious objects in computer network. Applied Mathematical Modeling . 2010;34:710-715.

[22] Mishra BK, Pandey SK. Dynamic model of worms with vertical transmission in computer network. Applied Mathematics and Computation. 2011;217:8438-8446.
[23] Zhu Q, Yang X, Ren J. Modeling and analysis of the spread of computer virus. Communication in Nonlinear Science. 2012;17:5117-5124.

[24] Toutonji OA, Yoo SM, Park M. Stability analysis of VEISV propagation model for network worm attack. Applied Mathematical Model. 2013;6:2751-2761.

[25] Mishra BK, Ansari GM. Differential epidemic model of virus and worms in computer network, International Journal of Network Security. 2012;14(1):88-94.

[26] Yan P and Liu S. SEIR Epidemic model with delay. The ANZIAM Journal. 2006;48:119-134.

[27] Liu W, Zhong S. Web Malware Spread Modelling and Optimal Control Strategies. Scientific Reports. 2017;7:42308. Available: www.nature.com/scientificreport DOI: 10.1038/rep42308

[28] Rao TS, Rauta AK, Haini HA, Panda CT. Mathematical model for Cyber Attack in Computer Network. International Journal of Business Data Communication and Network. 2017;13(1):58-59.

[29] Kumar M, Mishra BK, Panda TC. Effect of quarantine and vaccination on infectious nodes in computer network. International Journal of Computer Networks and Applications. 2015;2(2). ISSN: 2395-0455; 92-98.

[30] Ali J, Saeed M, Rafiq M, Igbal S. Numerical treatment of non linear model of virus propagation in computer networks: An innovation evolutionary pade approximation scheme. Advances in Mathematics, Springer Open Journal; 2018. Available: http://doi.org/10.1186/s1366-2018-1672-1

[31] Diekmann O, Heesterbeek JAP, Metz JAJ. On the definition and the computation of the basic reproduction ratio $R_0$ in models for infectious diseases in heterogeneous populations. J. Math Bwl. 1990;28:365-382.

[32] Li W, Liu X, Ciu S, Huang X. Modeling the spread of Malware with the influence of Heterogeneous Immunization. Appl. Math. Model. 2016;40(4):3141-3152.

[33] Birkhoff G, Rota GC. Ordinary Differential Equations, 4th Edition. New York: John Wiley and Sons, Inc.; Bowong S, Kurths J. (2010). Modelling Tuberculosis and Hepatitis B co-infection. Math. Model. Nat. Phenom. 1989;5(6):196-242.

[34] Van den Driessche P, Watmough J. Reproduction numbers and sub-threshold endemic equilibrium for compartmental models of disease transmission. Math. Bios. 2002;180:28-29.

[35] LaSalle JP. The Stability of dynamic Systems. Society for industrial and Applied Mathematics, Philadelphia, Pa; 1976.

[36] Bowong S, Kurths J. Modelling Tuberculosis and Hepatitis B co-infection. Math. Model. Nat. Phenom. 2010;5(6):196-242.
[37] LaSalle J P. Stability theory for ordinary differential equations. J. Differ. 1968;41:57-65.

[38] Bhatia NP, Szego GP. (n.d.). Stability theory of Dynamical systems. Springer Verlag; 1970.

[39] Gumel A. Causes of backward bifurcation in some epidemiological models. Journal of Mathematical Analysis and Applications. 2012;395(1):355-365.

[40] Castillo-Chavez C, Song B. Dynamic models of tuberculosis and their Applications. Math, Bios. Eng. 2004;1:361-404.

[41] Brauer F. Backward Bifurcation in Simple Vaccination Model. J. Math. Anal. Appl. 2004;298:418-431.
   Available:www.elsevier.com/locate/jmaa

[42] Cohen F. Computer Virus: Theory and Experiments. Computer and Security. 1987;6(1):22-35.

© 2021 Chinebu et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle4.com/review-history/66718