An epidemic model of malware virus with quarantine

Original Research Article

Abstract

In March of 2018, about 500,000 desktop computers were infected with cryptocurrency mining malware in less than 24 hours. In addition to attacking desktop computers, malware also attacks laptops, tablets, mobile phones. That is, any device connected via the Internet, or a network is at risk of being attacked. In recent years, mobile phones have become extremely popular that places them as a big target of malware infections. In this presentation, the effectiveness of treatment for infected mobile devices is examined using compartmental modeling. Many studies have considered malware infections which also include treatment effectiveness. However, in this study we examine the treatment effectiveness of mobile devices based on the type of malware infections accrued (hostile or malicious malware). This model considers six classes of mobile devices based on their epidemiological status: susceptible, exposed, infected by hostile malware, infected by malicious malware, quarantined, and recovered. The malware reproduction number, $\mathscr{R}_w$, was identified to discover the threshold values for the dynamics of malware infections to become both prevalent or absent among mobile devices. Numerical simulations of the model give insights of various strategies that can be implemented to control malware epidemic in a mobile network.

Keywords: epidemiology, malware, computer virus, reproductive generation number

2010 Mathematics Subject Classification: 92D30, 92Bxx, 35A24

1 Introduction

From the transfer of funds to or from one's financial institutions, utilities provider, home-security devices, and devices in the home, the proliferation in the use of mobile applications has enabled

and enhanced everyday life across the globe. This has also spurred the rapid evolution of malicious software (or malware) that range from pop-up advertisements to vicious encroachment of individual's, businesses' and government's cyber security systems (Weinberger (2011); Gan *et al.* (2013); Yang and Yang (2014); Yang *et al.* (2013)). The Merriam-Webster defines malware as a software designed to interfere with a computer's normal functioning. As the capabilities and use of mobile application use increase, the risk for breach of cyber security systems increases as well.

In March of 2018, about 500,000 desktop computers were infected with a malicious cryptocurrency mining software in less than 24 hours (Liu and Zhong (2017)). In addition to attacking desktop computers, malware also attacks laptops, tablets, mobile phones. This act reveals the financial incentive that drives the development of a new generation malware for the encroachment host-sites or devices through susceptible webpages. Once in the host-site or device, the malicious software and deceptively gleans confidential information. The consequence can result in compromised passwords, browsing history, financial information, and *etc*.

In recent years, mobile phones have become extremely popular; thus, making them primary targets of malware attacks. Hence, there is ever growing necessity to understand how the malware infections propagates through the web, especially through social media. For example, Facebook is the common venue for encroachment vectors and followed by spam links on social media websites (Marchal *et al.* (2014)).

Given the common characteristic spread of biological viruses and computer viruses, malware epidemiology used the mathematical techniques developed in the epidemiology of infectious diseases to describe the encroachment and propagation of malware viruses. Earlier models described the use of electronic mails or removable storage devices as vectors that allow malware to encroach computer systems and execute malicious act. [7,8] Many of these earlier mathematical models were achieved using a compartmental approach (such as $SIRS, SIRA, SEIQR$, *et al.*) (Batistela and Piqueira (2018); Gan *et al.* (2014, 2013); Gan and Tan (2010); Piqueira *et al.* (2008, 2005); Ren *et al.* (2012); Yang and Yang (2012); Yang *et al.* (2013); Zhu *et al.* (2012)) . Many of these models were only able to describe migration of the viruses and treatment effects; however, they did not consider the inclusion of isolation period of those objects penetrated by malware (Liu and Zhong (2017)).

In this paper, we propose a malware transmission model in a network of mobile devices by considering the treatment effectiveness based on the type of malware infections accrued (hostile malware or malicious malware). The proposed model considers six classes of mobile devices based on their epidemiological status: susceptible, exposed, infected by hostile malware, infected by malicious malware, quarantined, and recovered. Quarantine in this case implies an isolation of the device from the network while going through a treatment process to remove the malware. It is also assumed that once the malware is removed, mobile devices employ temporary immunity which allow them to become susceptible again to the infection.

2 Model formulation

In this model, we consider the population as a network of mobile devices. The total population is divided into six classes: susceptible $S(t)$, exposed $E(t)$, devices containing hostile malware $I_1(t)$, devices containing malicious malware $I_2(t)$, devices in quarantine $Q(t)$, and devices recovered from malware $R(t)$. Thus, the total population at a given time t is

$$N(t) = S(t) + E(t) + I_1(t) + I_2(t) + Q(t) + R(t).$$

It is assume that the incoming rate of new mobile devices is constant and denoted by Λ. Mobile devices will be exposed to malware virus by *effective contacts* via electronic communications with other devices containing malware virus. This *effective contact* rate is denoted by β. The rates at which mobile devices are infected with hostile malware and malicious malware are σ and γ, respectively. It is assumed that mobile devices with hostile virus are recovered at a rate of rho. It is also assumed

that, while in class I_1 or I_2, mobile devices may become nonfunctional at a rate of α. Some mobile devices in I_2 are quarantined at a rate of ν. The quarantine process may fail at a rate of η and these mobile devices are assumed to return to I_2 class at a rate of η. The successful quarantine will produced recovered mobile devices at a rate of ψ. The model is described by the following system of equations

$$\begin{aligned}
\frac{dS}{dt} &= \Lambda - \beta S\lambda_M + \omega R - \mu S,\\
\frac{dE}{dt} &= \beta S\lambda_M - X_1 E,\\
\frac{dI_1}{dt} &= \sigma E - X_2 I_1,\\
\frac{dI_2}{dt} &= \gamma E + \eta Q - X_3 I_2,\\
\frac{dQ}{dt} &= \nu I_2 - X_4 Q,\\
\frac{dR}{dt} &= \rho I_1 + \psi Q - X_5 R,
\end{aligned} \tag{2.1}$$

where

$$\begin{aligned}
X_1 &= \sigma + \gamma + \mu, \qquad & X_2 &= \rho + \alpha + \mu,\\
X_3 &= \nu + \alpha + \mu, \qquad & X_4 &= \eta + \psi + \mu,\\
X_5 &= \omega + \mu.
\end{aligned}$$

In system (2.1), λ_M is the force of infection and is defined by,

$$\lambda_M = \frac{\xi I_1 + I_2}{N},$$

where ξ is the relative infection ability of hostile virus when compared to malicious virus. The values of ξ ranges from 0 to 1.

The system of nonlinear differential equations model (2.1) is represented by

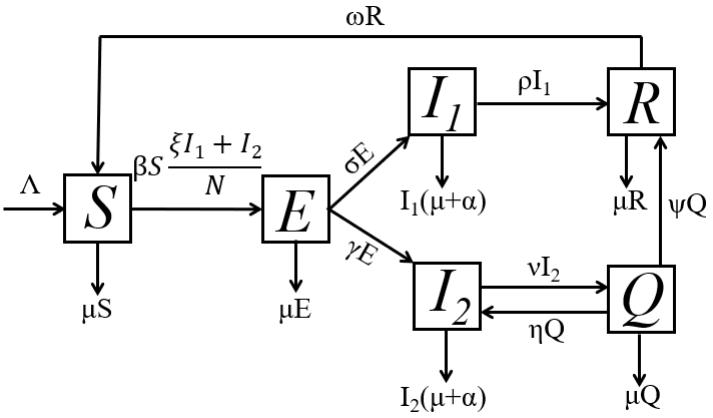


Figure 1: Systematic diagram of the malware transmission.

3 Model Analysis

3.1 Basic properties

It is assumed that all parameters and variables are greater than zero so that,

$$\begin{aligned} S(0) = S^0 > 0, \quad & I_1(0) = I_1^0 > 0, \quad & Q(0) = Q^0 > 0, \\ E(0) = E^0 > 0, \quad & I_2(0) = I_2^0 > 0, \quad & R(0) = R^0 > 0. \end{aligned}$$

It should be noted that

$$\frac{dN}{dt} = \Lambda - \alpha(I_1 + I_2) - \mu N < \Lambda - \mu N.$$

Thus, $N(t) < N(0)e^{-\mu t} + (\Lambda/\mu)(1 - e^{-\mu t})$ and $\sup_{t\to\infty} N(t) \leq \Lambda/\mu$. We can then study the system (2.1) in the feasible region

$$\mathscr{D} = \left\{ (S(t), E(t), I_1(t), I_2(t), Q(t), R(t)) \in \mathbb{R}_+^6 \mid 0 \leq N(t) \leq \frac{\Lambda}{\mu} \right\}.$$

The region $\mathscr{D}$ is positively invariant with respect to system (2.1) and all solutions of system (2.1) with $\left(S^0, E^0, I_1^0, I_2^0, Q^0, R^0\right) \in \mathbb{R}_+^6$ remain in $\mathscr{D}$ for all $t > 0$.

3.2 Model equilibria and stability analysis

3.2.1 Local stability of malware-free equilibrium

The malware free equilibrium (MFE) of system (2.1) is a state where there is no malware virus present in the network and is represented by the point

$$\mathscr{M}^0 : (S^0, E^0, I_1^0, I_2^0, Q^0, R^0) = \left(\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0\right).$$

The linear stability of $\mathscr{M}^0$ can be determined following a method by van den Driessche and Watmough [Driessche (2002)]. Using the next generation operator method (NGO), we employ the next generation matrices, F and V, where F is the Jacobian of the malware-generating terms and V is the Jacobian of the remaining transition terms. Both F and V are evaluated at the MFE, $\mathscr{M}^0$,

$$F = \begin{bmatrix} 0 & \beta\xi & \beta & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad V = \begin{bmatrix} X_1 & 0 & 0 & 0 \\ -\sigma & X_2 & 0 & 0 \\ -\gamma & 0 & X_3 & -\eta \\ 0 & 0 & -\nu & X_4 \end{bmatrix}.$$

Local stability of MFE, based on NGO, is determined by whether $\rho(FV^{-1}) < 1$. Here, $\rho(FV^{-1})$ is the spectral radius of the matrix FV^{-1}. MFE is locally asymptotically stable given that the linearized version of system (2.1) have eigenvalues with negative real parts.

We define the malware reproduction number $\mathscr{R}_w = \rho(FV^{-1})$. Then,

$$\mathscr{R}_w = \beta\xi \cdot \frac{\sigma}{X_1} \cdot \frac{1}{X_2} + \beta \cdot \frac{\gamma}{X_1} \cdot \frac{X_4}{X_3 X_4 - \eta\nu}.$$

It is noted that $\mathscr{R}_w$ is locally asymptotically stable whenever $\mathscr{R}_w < 1$ and unstable when $\mathscr{R}_w > 1$.

3.2.2 Interpretation of reproduction number

The system's malware reproduction number, $\mathscr{R}_w$, calculates the expected number of new malware infected mobile devices generated by an infected mobile device in a completely susceptible network during its duration of infection. The expression of $\mathscr{R}_w$ for system (2.1) consists of two terms. The first term represents the malware infections by hostile malware in class I_1 and the second term by malicious malware in class I_2.

3.2.3 Stability of Malware-Free Equilibrium

The global stability of MFE is established in the following theorem.

Theorem 3.1. *The MFE of the system (2.1) given by $\mathscr{M}^0$ is globally asymptotically stable in $\mathscr{D}$ if $\mathscr{R}_w < 1$.*

Proof. Consider the Lyapunov function

$$V = aE + bI_1 + cI_2 + dQ,$$

where

$$\begin{aligned} a &= (X_3X_4 - \eta\nu)X_2, \\ b &= \beta\xi(X_3X_4 - \eta\nu), \\ c &= \beta X_2X_4, \\ d &= \beta\eta X_2. \end{aligned}$$

Taking the derivative of V with respect to time, t, yields

$$\begin{aligned} V' &= (X_3X_4 - \eta\nu)X_2(\beta S\lambda_M - X_1E) + \beta\xi(X_3X_4 - \eta\nu)(\sigma E - X_2I_1) \\ &\quad + \beta X_2X_4(\gamma E + \eta Q - X_3I_2) + \beta\eta X_2(\nu I_2 - X_5Q), \\ &\leq \{(X_3X_4 - \eta\nu)(\beta\xi\sigma - X_1X_2) + \beta\gamma X_2X_4\}\, E, \\ &= X_1X_2(X_3X_4 - \eta\nu)(\mathscr{R}_w - 1)E. \end{aligned}$$

Thus, $\frac{dV}{dt} < 0$, when $\mathscr{R}_w < 1$, and $\frac{dV}{dt} = 0$, when $E(t) = 0$. By the LaSalle's Invariant Principle [Hale (1969)], every solution of (2.1) with initial conditions in $\mathscr{D}$ approaches $\mathscr{M}^0$ as $t \to \infty$.

□

3.2.4 Existence of Malware-Presistent Equilibrium

The malware-persistent equilibrium (MPE) is identified by setting the equations in (2.1) to zero. MPE is represented by

$$\mathscr{M}^{**} : (S^{**}, E^{**}, I_1^{**}, I_2^{**}, Q^{**}, R^{**}).$$

We identify

$$\lambda_M^* = \frac{\xi I_1 + I_2}{N} \tag{3.1}$$

as the force of infection at the steady state $\mathscr{M}^{**}$. The elements of $\mathscr{M}^{**}$ are solved in terms of I_1 as follows,

$$\begin{aligned} S^{**} &= \frac{X_1X_2}{\beta\sigma\lambda_M^*}I_1^{**}, & E^{**} &= \frac{X_2}{\sigma}I_1^{**}, \\ I_2^{**} &= \frac{\gamma X_2X_4}{\sigma(X_3X_4 - \eta\nu)}I_1^{**}, & Q^{**} &= \frac{\nu\gamma X_2}{\sigma(X_3X_4 - \eta\nu)}I_1^{**}, \\ R^{**} &= \frac{\rho\sigma(X_3X_4 - \eta\nu) + \psi\nu\gamma X_2}{X_5(X_3X_4 - \eta\nu)}I_1^{**}. \end{aligned} \tag{3.2}$$

Substituting (3.2) into (3.1) with some algebraic manipulation, we obtain the following quadratic polynomial in terms of λ_M^*,

$$\lambda_M^*(a_1\lambda_M^* + a_0) = 0,$$

where

$$a_1 = \beta\left[(X_3X_4 - \eta\nu)(X_2X_5 + \sigma X_5 + \rho\sigma) + \gamma X_2(X_4X_5 + \nu X_5 + \psi\nu)\right],$$
$$a_0 = X_1X_2X_5(X_3X_4 - \eta\nu)(1 - \mathscr{R}_w).$$

Thus, the polynomial yields $\lambda_M^* = 0$, which is the malware-free equilibrium, and $\lambda_M^* = -a_0/a_1$, which gives a unique malware-persistent equilibrium when $\mathscr{R}_w > 1$.

4 Numerical Analysis and Results

Several numerical simulations were performed using MATLAB 2019A to illustrate the dynamics of the hostile and malicious malware virus in a mobile network. The parameter values used in the simulations were estimated and listed in table 1. We assessed the effects of the duration of being exposed to a virus and being quarantined.

Table 1: Description of parameters and estimated values

Parameter	Description	Estimated value
Λ	Recruitment rate	350
β	Effective contact rate	0.085
ξ	Relative infectious factor of hostile malware	0.8
σ	Infected rate of hostile malware	0.083
γ	Infected rate of malicious malware	0.05
ρ	Recovery rate from hostile malware	0.038
α	Malware-related exit rate	0.001
ν	Isolation rate from malicious malware	0.083
η	Re-infection rate from isolation	0.00083
ψ	Recovery rate from isolation	0.017
ω	Temporary immunity rate	0.00069
μ	Non-malware related exit rate	0.000057

Figures (2) show the trajectories of the number of infected mobile devices when the parameter values reflect $\mathscr{R}_w < 1$ and $\mathscr{R}_w > 1$ with various initial conditions. These simulations show that when $\mathscr{R}_w < 1$, the number of infected mobile devices reaches the malware-free equilibrium, while when $\mathscr{R}_w > 1$, there exists a non-zero malware-persistent equilibrium. Furthermore, increasing the number of mobile devices exposed to malware virus reduces the time when the epidemic occurs.

Figure (3) shows the trajectories of the number of infected mobile devices when $\mathscr{R}_w > 1$ with varying σ, the infected rate of hostile malware, and γ, the infected rate of malicious malware. As σ decreases, $\mathscr{R}_w$ decreases. Figure (3a) shows as σ decreases, the peak of the trajectory also decreases. It also shows that decreasing σ delays the occurrence of the epidemic. In Figure (3b), the peak of the trajectory decreases as σ increases.

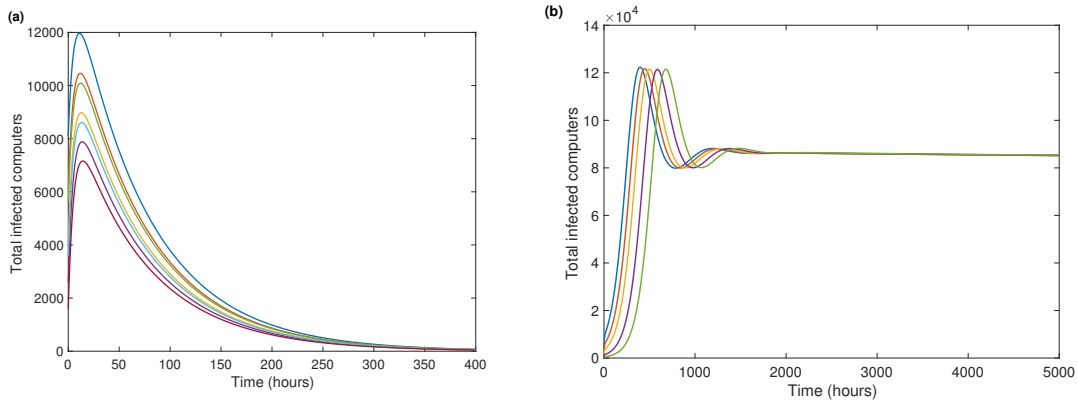
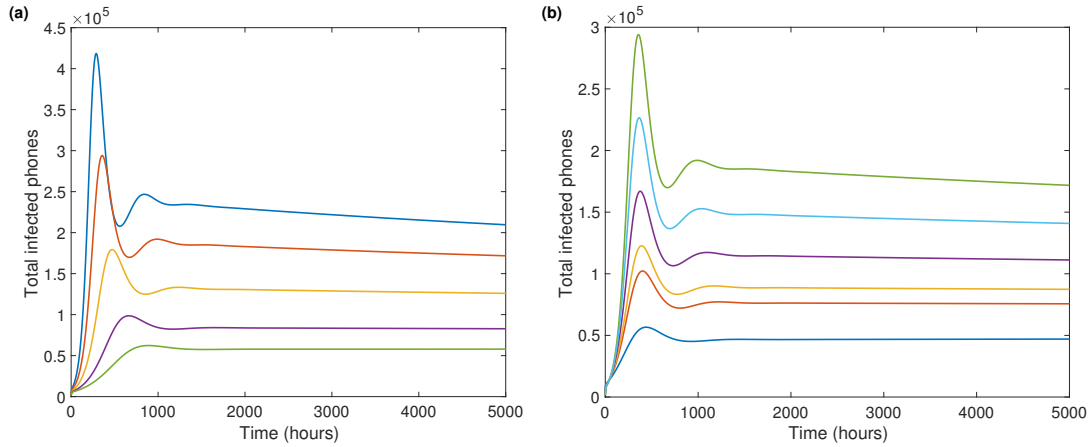


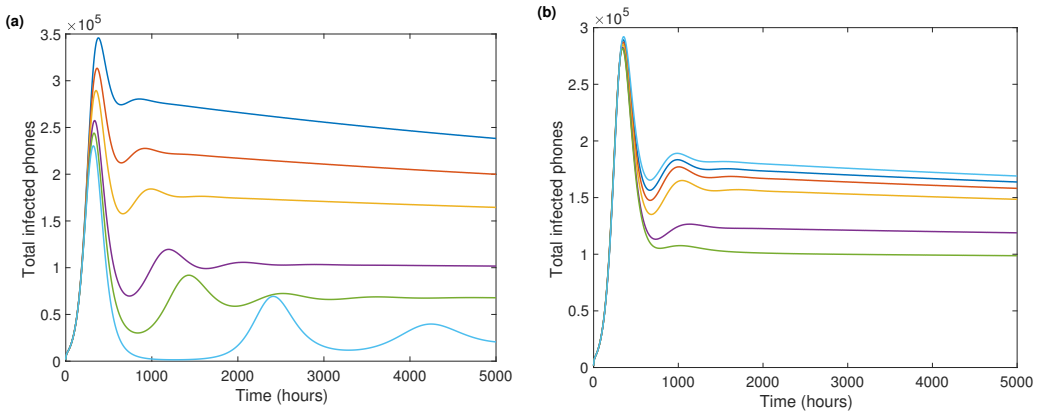
Figure 2: Trajectories of infected classes for (a) $\mathscr{R}_w < 1$ and (b) $\mathscr{R}_w > 1$ with various initial conditions.



(a) Varying σ. (b) Varying γ.

Figure 3: Trajectories of infected classes when $\mathscr{R}_w > 1$ with (a) varying σ and (b) varying γ.

Figure (4) shows the trajectories of the number of infected mobile devices when $\mathscr{R}_w > 1$ with varying ω, the temporary immunity rate from the recovered class, and ψ, the recovery rate from the isolation class. The trajectories in Figure (4a) show a decreasing pattern of the peaks when ω increases. Figure (4a) also shows a delay in the epidemic as ω increases. Lastly, as ψ increases in Figure (4b), the peaks of the epidemic also increases.



(a) Varying ω. (b) Varying ψ.

Figure 4: Trajectories of infected classes when $\mathscr{R}_w > 1$ with (a) varying ω and (b) varying ψ.

5 CONCLUSIONS

In this study, we investigated the transmission dynamics of malware virus in a network of mobile devices. Within this dynamics, we considered classifying malware virus types as hostile and malicious. We also considered the isolation of mobile devices infected with malicious malware in a quarantine. We demonstrated the existence of malware-free equilibrium and malware-persistent equilibrium both analytically and numerically. Furthermore, we obtained the malware reproduction number, $\mathscr{R}_w$, which determines the threshold value of the epidemic.

The numerical simulations of the system (2.1) show how the parameter values affect the occurrence of the malware epidemic. As σ increases, the malware reproduction number, $\mathscr{R}_w$, also increases. The trajectories in (3a) show a shorter period of epidemic as $\mathscr{R}_w$ increases. Interestingly, as γ increases, $\mathscr{R}_w$, decreases. The largest value of $\mathscr{R}_w$ used in the simulation generates the trajectory with the highest peak in Figure (3b). When ω increases, there is a threshold where a cycle of epidemic occurs generating more malware infections in the network. In Figure (4a), the trajectory with the largest $\mathscr{R}_w$ appears on the bottom, showing multiple epidemic peaks. Finally, in Figure (4b), the trajectories show a pattern that as ψ increases, $\mathscr{R}_w$ decreases, resulting in increasing peaks.

From the different simulations with varying parameter values, we observe their effects on $\mathscr{R}_w$. Numerous strategies can be implemented in order to prevent or control a malware epidemic. For example, longer duration in isolation for those mobile devices infected with malicious malware helps minimize the duration time of the epidemic.

References

Batistela, C. M., and Piqueira, J. R. C. (2018). SIRA Computer Viruses Propagation Model: Mortality and Robustness. International Journal of Applied and Computational Mathematics. 4(5), 128.

Gan, C., *et al.*. (2013). The spread of computer virus under the effect of external computers. Nonlinear Dyn. 73, 1615?1620, DOI 10.1007/s11071-013-0889-5.

Gan, C., *et al.* (2014). A propagation model of computer virus with nonlinear vaccination probability. Communications in Nonlinear Science and Numerical Simulation. 19(1), 92-100.

Gan, C., *et al.* (2013). An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate. Applied Mathematics and Computation. 222, 265-274.

Hale, J.K. (1969). Ordinary Differential Equations. Jon Wiley and Sons, New York.

Han, X., and Tan, Q. (2010). Dynamical behavior of computer virus on Internet. Applied Mathematics and Computation, 217(6), 2520-2526.

Liu, W. and Zhong, S. (2017) Web malware spread modelling and optimal control strategies. Scientific Reports. 7, 42308.

Marchal, S., *et al.* (2014). Phishstorm: detecting phishing with streaming analytics. IEEE Transactions on Network and Service Management.11(4), 458?471.

Mishra, B.K. and Jha, N. (2010) SEIQRS model for the transmission of malicious objects in computer network. Applied Mathematical Modeling. 34, 710?715.

Piqueira, J. R. C., and Araujo, V. O. (2009). A modified epidemiological model for computer viruses. Applied Mathematics and Computation. 213(2), 355-360.

Piqueira, J. R. C., *et al.* (2008). Dynamic models for computer viruses. computers & security, 27(7-8), 355-359.

Piqueira, J. R. C., *et al.* (2005). Epidemiological models applied to viruses in computer networks. Journal of Computer Science. 1(1), 31-34.

Ren, J., *et al.* (2012). A novel computer virus model and its dynamics. Nonlinear Analysis: Real World Applications. 13(1), 376-384.

Van den Driessche, P and Watmough, J. (2002). Reproduction numbers and subthreshold endemic equilibria for compartmental models of disease transmission. Math Biosci. 180, 29-48. http://dx.doi.org/10.1016/ S0025-5564(02)00108-6

Weinberger, S. (2011). Computer security: Is this the start of cyberwarfare? Nature 474, 142?145.

Yang, L-X. and Yang, X. (2014) A new epidemic model of computer viruses, Commun Nonlinear Sci. Numer. Simulat. 19, 1935?1944.

Yang, L.-X. and Yang, X. (2012). The spread of computer viruses under the influence of removable storage devices. Applied Mathematics and Computation. 219, 3914?3922.

Yang, X., and Yang, L. X. (2012). Towards the epidemiological modeling of computer viruses. Discrete Dynamics in Nature and Society.

Yang, X., *et al.* (2013) An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate. Applied Mathematics and Computation. 222, 265?274

Zhu, Q., *et al.* (2012). Modeling and analysis of the spread of computer virus. Communications in Nonlinear Science and Numerical Simulation, 17(12), 5117-5124.