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 study, 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, \( R_M \), was identified to discover the threshold values for the dynamics of malware infections to become both prevalent or

*Corresponding author: E-mail: Aprillya.Rosidian@asu.edu;
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 [1, 2, 3, 4]. 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 [5]. 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 [6].

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, etc.) [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 4, 21, 22, 23]. Many of these models were 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 [5].

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 assumed that the incoming rate of new mobile devices is constant and denoted by $\Lambda$. 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 $\beta$; this is the rate where malware virus is successfully transmitted to a susceptible mobile device. The rates at which mobile devices are infected with hostile and malicious malware are $\sigma$ and $\gamma$, 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 $\alpha$. Some mobile devices in $I_2$ are quarantined at a rate of $\nu$. The quarantine process may fail at a rate of $\eta$ and these mobile devices are assumed to return to $I_2$ class at a rate of $\eta$. The successful quarantine will produced recovered mobile devices at a rate of $\psi$. The model is described by the following system of equations

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

where

\[ X_1 = \sigma + \gamma + \mu, \quad X_2 = \rho + \alpha + \mu, \]
\[ X_3 = \nu + \alpha + \mu, \quad X_4 = \eta + \psi + \mu, \]
\[ X_5 = \omega + \mu. \]

In system (2.1), $\lambda_M$ is the force of infection and is defined by,

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

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

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

3.1 Basic properties

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

\[ S(0) = S^0 > 0, \quad I_1(0) = I_1^0 > 0, \quad Q(0) = Q^0 > 0, \]
\[ E(0) = E^0 > 0, \quad I_2(0) = I_2^0 > 0, \quad R(0) = R^0 > 0. \]

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

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

The region \( \mathcal{D} \) is positively invariant with respect to system (2.1) and all solutions of system (2.1) with \( (S^0, E^0, I_1^0, I_2^0, Q^0, R^0) \in \mathbb{R}_+^6 \) remain in \( \mathcal{D} \) 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

\[ \mathcal{M}^0 : (S^0, E^0, I_1^0, I_2^0, Q^0, R^0) = \left( \frac{\Lambda}{\mu}, 0, 0, 0, 0, 0 \right). \]
The linear stability of $M^0$ can be determined following a method by van den Driessche and Watmough [24]. 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, $M^0$,

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

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 $R_M = \rho(FV^{-1})$. Then,

\[
R_M = \frac{\beta \xi}{X_1} \frac{1}{X_2} + \frac{\gamma}{X_1} \frac{X_4}{X_3X_4 - \eta \nu}.
\]

It is noted that $M^0$ is locally asymptotically stable whenever $R_M < 1$ and unstable when $R_M > 1$.

### 3.2.2 Interpretation of Reproduction Number

The system’s malware reproduction number, $R_M$, 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 $R_M$ 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 $M^0$ is globally asymptotically stable in $\mathcal{D}$ if $R_M < 1$.

**Proof.** Consider the Lyapunov function

\[
V = aE + bI_1 + cI_2 + dQ,
\]

where

\[
a = (X_3X_4 - \eta \nu)X_2, \quad b = \beta \xi (X_3X_4 - \eta \nu), \quad c = \beta X_3X_4, \quad d = \beta \eta X_2.
\]

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

\[
\frac{dV}{dt} = (X_3X_4 - \eta \nu)X_2(\beta S_{\lambda M} - X_1E) + \beta \xi (X_3X_4 - \eta \nu)(\sigma E - X_2I_1) + \beta X_3X_4(\gamma E + \eta Q - X_3I_2) + \beta \eta X_2(\nu I_2 - X_3Q),
\]

\[
\leq (X_3X_4 - \eta \nu)(\beta \xi \sigma - X_2X_3) + \beta \gamma X_2X_4)E, = X_1X_2(X_3X_4 - \eta \nu)(R_M - 1)E.
\]
Thus, $\frac{dV}{dt} < 0$, when $R_M < 1$, and $\frac{dV}{dt} = 0$, when $E(t) = 0$. By the LaSalle’s Invariant Principle [25], every solution of (2.1) with initial conditions in $D$ approaches $M_0$ as $t \to \infty$.

### 3.2.4 Existence of Malware-Persistent Equilibrium

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

We identify $M = I_1 + I_2$ as the force of infection at the steady state $M$. The elements of $M$ are solved in terms of $I_1$ as follows,

$$S^* = \frac{X_1X_2}{\beta\sigma \lambda_M I_1^*}, \quad E^* = \frac{X_2}{\sigma I_1^*},$$

$$I_2^* = \frac{\gamma X_2 X_4}{\sigma(X_3 X_4 - \eta \nu)} I_1^*, \quad Q^* = \frac{\nu \gamma X_2}{\sigma(X_3 X_4 - \eta \nu)} I_1^*,$$

$$R^* = \frac{\rho \sigma (X_3 X_4 - \eta \nu) + \psi \nu \gamma X_2}{X_5(X_3 X_4 - \eta \nu)} I_1^*.$$  

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

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

where

$$a_1 = \beta [(X_3 X_4 - \eta \nu)(X_2 X_5 + \sigma X_5 + \rho \sigma) + \gamma X_2 (X_4 X_5 + \nu X_5 + \psi \nu)],$$

$$a_0 = X_1 X_2 X_5(X_3 X_4 - \eta \nu)(1 - R_M).$$

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 $R_M > 1$.

### 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. The observations are summarized in table 2.

Figures 2 show the trajectories of the number of infected mobile devices when the parameter values reflect $R_M < 1$ and $R_M > 1$ with various initial conditions. These simulations show that when $R_M < 1$, the number of infected mobile devices reaches the malware-free equilibrium, while when $R_M > 1$, 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.

Figures 3 show the trajectories of the number of infected mobile devices when $R_M > 1$ with varying $\sigma$, the infected rate of hostile malware, and $\gamma$, the infected rate of malicious malware. As $\sigma$ decreases, $R_M$ decreases. Figure 3(a) shows as $\sigma$ decreases, the peak of the trajectory also decreases. It also shows that decreasing $\sigma$ delays the occurrence of the epidemic. In Figure 3(b), the peak of the trajectory decreases as $\gamma$ increases.
Table 1. Description of parameters and estimated values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Estimated value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Lambda$</td>
<td>Recruitment rate</td>
<td>350</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Effective contact rate</td>
<td>0.085</td>
</tr>
<tr>
<td>$\xi$</td>
<td>Relative infectious factor of hostile malware</td>
<td>0.8</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>Infected rate of hostile malware</td>
<td>0.083</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>Infected rate of malicious malware</td>
<td>0.05</td>
</tr>
<tr>
<td>$\rho$</td>
<td>Recovery rate from hostile malware</td>
<td>0.038</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Malware-related exit rate</td>
<td>0.001</td>
</tr>
<tr>
<td>$\nu$</td>
<td>Isolation rate from malicious malware</td>
<td>0.083</td>
</tr>
<tr>
<td>$\eta$</td>
<td>Re-infection rate from isolation</td>
<td>0.00083</td>
</tr>
<tr>
<td>$\psi$</td>
<td>Recovery rate from isolation</td>
<td>0.017</td>
</tr>
<tr>
<td>$\omega$</td>
<td>Temporary immunity rate</td>
<td>0.00069</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Non-malware related exit rate</td>
<td>0.000057</td>
</tr>
</tbody>
</table>

Fig. 2. Trajectories of infected classes for (a) $R_M < 1$ and (b) $R_M > 1$ with various initial conditions.

Fig. 3. Trajectories of infected classes when $R_M > 1$ with (a) varying $\sigma$ and (b) varying $\gamma$. 
Figures 4 show the trajectories of the number of infected mobile devices when $R_M > 1$ with varying $\omega$, the temporary immunity rate from the recovered class, and $\psi$, the recovery rate from the isolation class. The trajectories in Figure 4(a) show a decreasing pattern of the peaks when $\omega$ increases. Figure 4(a) also shows a noticeable delay in the epidemic as $\omega$ increases. Lastly, as $\psi$ increases in Figure 4(b), the peaks of the epidemic also increases.

![Graph showing trajectories of infected devices](image)

(a) Varying $\omega$.  
(b) Varying $\psi$.

**Fig. 4. Trajectories of infected classes when $R_M > 1$ with (a) varying $\omega$ and (b) varying $\psi$.**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma$</td>
<td>epidemic peak increases, multiple endemic peaks occur</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>epidemic peak decreases, multiple endemic peaks disappear</td>
</tr>
<tr>
<td>$\omega$</td>
<td>epidemic peak increases, multiple endemic peaks disappear</td>
</tr>
<tr>
<td>$\psi$</td>
<td>epidemic peak increases, multiple endemic peaks occur</td>
</tr>
</tbody>
</table>

### Table 2. Summary of simulation results

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, $R_M$, 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 $\sigma$ increases, the malware reproduction number, $R_M$, also increases. The trajectories in Figure 3(a) show a shorter period of epidemic as $R_M$ increases. Interestingly, as $\gamma$ increases, $R_M$ decreases. The largest value of $R_M$ used in the simulation generates the trajectory with the highest peak in Figure 3(b). When $\omega$ increases, there is a threshold where a cycle of...
epidemic occurs generating more malware infections in the network. In Figure 4(a), the trajectory with the largest $\mathcal{R}_M$ appears on the bottom, showing multiple epidemic peaks. Finally, in Figure 4(b), the trajectories show a pattern that as $\psi$ increases, $\mathcal{R}_M$ decreases, resulting in increasing peaks.

From the different simulations with varying parameter values, we observe their effects on $\mathcal{R}_M$. 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.

Acknowledgement

The authors would like to thank the School for Engineering of Matter, Transport and Energy at Arizona State University (ASU) for allowing us to use their resources and facilities. The authors would also like to acknowledge the support provided by the National Science Foundation HBCU-UP Research Initiation Award (grant 074754805). Furthermore, the authors would also like to express gratitude to the reviewers for their valuable time and input.

Competing Interests

The corresponding author confirms on behalf of all authors that there have been no involvements that might raise the question of bias in the work reported or in the conclusions, implications, or opinions stated.

References


