Complexity

WILEY

RESEARCH ARTICLE OPEN ACCESS

Modeling and Simulation of Cyber Epidemics Using a Delayed Variable-Order Fractional Framework

Mohamed Khalil[1] | Anas Arafa[2] | Ahmad Almutlg[2] | Amaal Sayed[3]

[1]Department of Mathematics, Faculty of Engineering, October University for Modern Sciences and Arts (MSA), Giza, Egypt | [2]Department of Mathematics, College of Science, Qassim University, Buraydah, Saudi Arabia | [3]Department of Basic Science, Faculty of Engineering, May University in Cairo (MUC), 15 May City, Cairo, Egypt

Correspondence: Mohamed Khalil (mkibrahim@msa.edu.eg)

Received: 10 March 2026 | **Revised:** 11 May 2026 | **Accepted:** 11 June 2026

Academic Editor: Jesus Manuel Munoz-Pacheco

Keywords: cyber epidemics | fractional derivatives | local stability | malware propagation | numerical simulation | predictor–corrector method

ABSTRACT

In today's digital era, cyber epidemics are evolving rapidly. They pose a growing global threat. A cyber epidemic involves malware that spreads across connected networks. In this paper, we propose a delayed variable-order fractional model to study the spread of malware. The model incorporates time-varying memory effects through Caputo's variable-order fractional derivative. It also accounts for delayed antivirus response via a time-delay term. The system is solved numerically using a predictor–corrector scheme. To the best of our knowledge, this work presents the first delayed variable-order fractional cyber epidemic model that integrates both time-dependent memory and time-delay effects. The results indicate that as the fractional order decreases, the system dynamics become slower and more stable, with lower infection levels. In addition, the variable-order model provides a more flexible description of evolving memory effects in cyber epidemic systems.

1 | Introduction

A computer virus is a type of harmful software that has been created to steal data, delete files, or damage computer systems. It can replicate itself and move from a computer to another via networks or removable storage media. In the era of large-scale networks, such malicious software has become a serious global problem that threatens national security [1]. Moreover, these cyber threats have social and economic consequences [2]. Numerous cyberattack outbreaks have occurred in the form of malware, including ILOVEYOU, Mydoom, Conficker, Storm Worm, and Tinba. More recently, Zeus Gameover and Dyreza have become well-known examples of malware that have caused global disruption [3]. Controlling the propagation of such threats has become a global challenge. Mathematical models provide a deep understanding of malware diffusion and can predict its dynamics. In addition, these models support decision makers in developing strategies to control the spread of malware. Most of these models are integer-order models. Consequently, they often fail to capture memory effects [4]. This may limit their ability to provide an accurate description of the complex behavior of real-world networks. The spread of malware depends not only on the current state of the system but also on past interactions, user behavior, and system responses. To overcome these limitations, fractional calculus (FC) provides a powerful tool for incorporating memory effects into system dynamics [5]. In recent years, fractional-order models have been widely used in several fields, including ecological systems [6], infectious diseases [7], and control systems [8]. Furthermore, time-delay models can be employed to reflect delays in system responses. On the other hand, fractional-order delay models can capture both memory and time delays effects more effectively. Fractional-order models with delay have been used in several fields, including neural networks [9] and chaotic systems [10]. Moreover, fractional-order models have also been applied in fluid flow systems

[11], while neural network approaches are successfully used to analyze complex fractional-order dynamical systems [12].

Based on these advantages, fractional-order approaches have increasingly been adopted in cyber system modeling, offering a more realistic representation of malware propagation and network behavior.

In this section, we present some examples of the most recent studies on computer virus propagation. The authors in [13] developed a mathematical model to study the propagation of Stuxnet computer virus via networks. The impact of removable storage media on virus propagation has been considered in this work. A new compartmental SLBR model was proposed in [14] to study the spread of computer viruses over SCADA systems via USB drives and LANs. Such malware has a significant effect on industrial production and the global economy. A mathematical model was presented in [15] to investigate the spread of worms on mobile devices and to evaluate the effectiveness of the control strategies.

However, several fractional-order models have been proposed in recent years to provide a better understanding of malware spread. These models capture the system's history reflecting memory effects on the malware dynamics. This cannot be easily achieved using integer-order derivatives.

In other words, classical integer-order derivatives are used to describe the short memory of dynamical systems, whereas the fractional-order derivatives can characterize the long memory. An example of a fractional-order model was presented by Farman et al. [16], where a non-integer-order model was implemented using Caputo–Fabrizio and Atangana–Baleanu derivatives to study the spread of computer viruses. Another computer virus model based on Atangana–Baleanu fractional-order derivative was presented in [17] with optimal control analysis. Furthermore, the authors in [18] developed a non-integer-order computer virus model in the Caputo fractional derivative sense. They employed the residual power series method to obtain numerical solutions of the proposed model.

Despite the rapid progress in modeling cyber epidemics, several limitations still remain:

- Most existing models are based on integer-order derivatives; therefore, they do not capture memory effects in cyber systems.
- Constant fractional-order models fail to reflect the time-varying memory of cyber environments.
- Several studies do not consider time-delay effects associated with antivirus response.
- The integration of time-dependent memory and time-delay effects is often neglected in recent models.

To address these limitations, we propose a delayed variable-order fractional cyber epidemic model. The main motivation for implementing a fractional variable-order model with time delay is to better capture cyber epidemic dynamics. The variable-order fractional derivative reflects time-varying memory effects, while the time delay characterizes the antivirus response time. Hence, the proposed model provides a more realistic description of cyber epidemics.

The variable-order fractional derivative is an extension of the constant fractional-order derivative. It is a powerful tool to capture memory effects that evolve over time. In this work, we use the variable-order fractional derivative to describe the impact of the time-varying memory during the cyber epidemic outbreak [19].

The main contribution of this study is to investigate the impact of the variable memory on the malware dynamics. In addition, the proposed model includes a time delay to account for the antivirus response time. To the best of our knowledge, the proposed model is the first delay variable-order fractional cyber epidemic model for malware propagation presented in the literature. The combination of time-dependent memory and time-delay effects allows both memory effects and system responses to evolve over time. The obtained results demonstrate that this approach provides a more realistic description of malware dynamics compared with integer-order and constant fractional-order models. They also highlight the role of memory effects, interpreted here as antivirus updates, while capturing time-delay effects. These findings suggest that incorporating memory effects can help to develop more effective antivirus strategies for controlling malware spread.

This paper is organized as follows. Section 2 provides an overview of fractional calculus (FC). Section 3 presents the proposed model. Section 4 discusses the nonnegative solutions of the system. Section 5 examines the endemic equilibrium points, along with the existence and stability of the solutions. Sections 6 and 7 present the numerical results and the conclusions, respectively.

2 | FC

FC has become an important mathematical framework for studying numerous scientific and natural phenomena due to its nonlocal nature. It has been widely used to model complex dynamical systems, including infectious disease propagation [20], cancer treatment [21], cancer growth [22], and glucose–insulin interactions [23].

The variable-order fractional derivative is the natural generalization of the constant fractional-order derivative [24]. It captures memory effects that evolve over time in many complex systems [25]. In recent years, many variable-order fractional models have been proposed to describe processes in different scientific fields and to build a deep understanding of various natural phenomena [26].

Using fractional-order derivatives allows the proposed model to capture memory effects. Therefore, the system dynamics depend not only on the current state but also on the past states. Consequently, the fractional-order model exhibits slower transient responses and more persistent infection levels. Moreover, the variable-order derivative allows the memory effect to vary over time, providing a more flexible description of cyber epidemic dynamics.

Several definitions of variable-order fractional derivatives have been introduced in the literature. The Caputo derivative is widely used because it allows standard initial conditions of integer-order models to be applied to non-integer-order models [27]. It bridges the gap between theoretical FC and real-life applications. Its variable-order form enables the modeling of time-varying memory behavior, providing an accurate description of cyber epidemics dynamics. Other definitions, such as Riemann–Liouville, Caputo–Fabrizio, and Atangana–Baleanu, may involve less well-defined initial conditions.

Definition 1. Caputo variable-order fractional derivative [27]:

$$ {}_{a}^{C}D_{t}^{\alpha(t)}f(t) = \frac{1}{\Gamma(1-\alpha(t))}\int_{a}^{t}(t-s)^{-\alpha(t)}f'(s)ds, \alpha(t) \in (n-1, n). \quad (1)$$

For simplicity, the operator $D^{\alpha(t)}$ is used throughout the paper to represent the Caputo variable-order fractional derivative with lower limit a.

3 | Model Derivation

Here, a non-integer variable-order model of malware with time delay is developed based on the cyber epidemic model presented in [28, 29]. In [28], Yang et al. proposed the following cyber epidemic model for computer viruses:

$$\begin{cases} \frac{dS(t)}{dt} = \mu_1 - \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) + \gamma_1 L(t) + \gamma_2 B(t) - (\delta+\theta)S(t), \\ \frac{dL(t)}{dt} = \mu_2 + \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) - \left(\gamma_1 + q + \delta\right)L(t) + \theta S(t), \\ \frac{dB(t)}{dt} = qL(t) - \left(\gamma_2 + \delta\right)B(t). \end{cases} \quad (2)$$

In a computer network, computers are considered as nodes. A node is called infected if it contains viruses, while it is called external if it is connected to the internet. In system (2), the nodes are categorized into uninfected nodes ($S(t)$), latent nodes ($L(t)$), and breaking-out nodes ($B(t)$). When external nodes are connected to the internet, they are either latent or virus-free. External S-nodes and external L-nodes are connected to the internet at rates μ_1 and μ_2, respectively, while the probability that internal nodes are disconnected from the internet is δ. The impact of external removable storage media is considered in the proposed model. It is assumed that computer viruses can be transmitted to the S-nodes with probability θ through infected removable media. The probability that each S-node is infected by L-nodes at time t is $\beta_1 L(t)$. On the other hand, each S-node can be infected by B-nodes at time t with probability $\beta_2 B(t)$. L-nodes may break out with probability q. Furthermore, L-nodes and B-nodes are cleaned up from the virus with probabilities γ_1 and γ_2, respectively. All the parameters in this system are nonnegative.

Zhang et al. designed a delayed computer virus model based on system (2) as follows [29]:

$$\begin{cases} \frac{dS(t)}{dt} = \mu_1 - \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) + \gamma_1 L(t-\tau) + \gamma_2 B(t-\tau) - (\delta+\theta)S(t), \\ \frac{dL(t)}{dt} = \mu_2 + \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) - \gamma_1 L(t-\tau) - (q+\delta)L(t) + \theta S(t), \\ \frac{dB(t)}{dt} = qL(t) - \gamma_2 B(t-\tau) - (\delta)B(t). \end{cases} \quad (3)$$

Based on the above systems, we propose the following fractional variable-order model of computer virus with time delay:

$$\begin{cases} \frac{1}{\sigma^{1-\alpha(t)}}D^{\alpha(t)}(S(t)) = \mu_1 - \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) + \gamma_1 L(t-\tau) + \gamma_2 B(t-\tau) - (\delta+\theta)S(t), \\ \frac{1}{\sigma^{1-\alpha(t)}}D^{\alpha(t)}(L(t)) = \mu_2 + \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) - \gamma_1 L(t-\tau) - (q+\delta)L(t) + \theta S(t), \\ \frac{1}{\sigma^{1-\alpha(t)}}D^{\alpha(t)}(B(t)) = qL(t) - \gamma_2 B(t-\tau) - (\delta)B(t), \end{cases} \quad (4)$$

where $S(0) = S_0, L(0) = L_0, B(0) = B_0$ and $0 < \alpha(t) < 1$.

Model (4) is derived from model (3) by replacing the first-order derivative with the Caputo variable-order fractional derivative $D^{\alpha(t)}$, along with the scaling factor $1/\sigma^{1-\alpha(t)}$, where $0 < \alpha(t) < 1$.

The variable fractional order $\alpha(t)$ which is considered as the parameter of memory is a function of time. We use the parameter σ to maintain dimensional consistency in the variable-order fractional model [19]. The impact of the parameter of memory $\alpha(t)$ and the time delay τ on the dynamics of system (4) is investigated in this paper. The delay parameter τ represents the time lag associated with malware detection or antivirus response. The condition $0 < \alpha(t) < 1$ follows from the general fractional-order interval $m-1 < \alpha(t) < m$, where $m = 1$, which is consistent with first-order systems.

In other words, the time delay τ represents the lag in antivirus actions to remove malware, while $\alpha(t)$ reflects the evolving memory and updates of the antivirus.

Model (4) can overcome several flaws of several earlier models. These models missed the fact that any computer device will be infectious after getting infected. Secondly, previous models did not take into account the difference between latent and breaking-out devices. Additionally, earlier models do not consider that any computer may be susceptible to the malware again after recovery. Moreover, most of these models neglect the impact of removable storage devices on the propagation of malware. Besides, all of the previous models assumed that a computer is virus-free when it is connected to the internet, which is not always true. Finally, the previous cyber epidemic models considered that the number of computer devices connected to the internet is constant, which is inconsistent with reality.

4 | Nonnegative Solutions

Let $R_+^3 = \{x \in R^3 : x \geq 0\}$ and $x(t) = (S(t), L(t), B(t))^T$; then, we should prove the following lemma and corollary before proving Theorem 1 [30, 31].

Lemma 1 (generalized mean value theorem) [31]. *Suppose that $f(x) \in C[a, b]$, $D^{\alpha(t)}f(x) \in C(a, b]$, and $0 < \alpha(t) \leq 1$, where $\alpha(t)$ is a continuous function on $[a, b]$. Then,*

$$f(x) = f(a) + \frac{1}{\Gamma(\alpha)}\left(D^{\alpha(t)}f\right)(\xi)(x-a)^{\alpha(t)}, \tag{5}$$

where $a \leq \xi \leq x$, for all $x \in (a, b]$.

Corollary 1. *Suppose that $f(x) \in C[a, b]$, $D^{\alpha(t)}f(x) \in C(a, b]$, and $\alpha(t) \in C(a, b]$, for $0 < \alpha(t) \leq 1$. Then:*

- *If $D^{\alpha(t)}f(x) \geq 0, f(x)$ is a nondecreasing function for all $x \in [a, b]$.*
- *If $D^{\alpha(t)}f(x) \leq 0, f(x)$ is nonincreasing function for all $x \in [a, b]$.*

Proof 1. The result follows directly from Lemma 1, since the sign of the fractional derivative determines whether the function is increasing or decreasing. □

Theorem 1. *A unique solution $x(t) = (S(t), L(t), B(t))^T$ exists to system (4) on $[0, T]$, and this solution remains in $\mathbb{R}^3_+$ under the assumption that $\alpha(t) \in C[0, T]$.*

Proof 2. From Theorem 3.1 and Remark 3.2 in [32], it is clear that the solution of the proposed model (4) exists and is unique. Since $\alpha(t) \in C[0, T]$, the Caputo derivative is well-defined and the generalized mean value theorem is applicable. Hence, it follows that the solution of system (4) is nonnegative and therefore remains in $\mathbb{R}^3_+$. □

This can also be verified by evaluating the fractional derivatives at the boundary, as follows:

$$\begin{aligned} D^{\alpha(t)}(S(t))\big|_{S=0} &\geq 0, \\ D^{\alpha(t)}(L(t))\big|_{L=0} &\geq 0, \\ D^{\alpha(t)}(B(t))\big|_{B=0} &\geq 0, \end{aligned} \tag{6}$$

which shows that the solution remains in $\mathbb{R}^3_+$.

5 | Endemic Equilibrium Point and Existence of Uniformly Stable Solution

Model (4) can be presented as follows:

$$D^{\alpha(t)}(y_i(t)) = f(t, y_i(t), y_i(t-\tau)), \tag{7}$$

with initial conditions $y_i(0) \geq 0$,

$$0 \leq t \leq T, i = 1, 2, 3. \tag{8}$$

Where $y(t) = (S, L, B)^T, f = (f_1, f_2, f_3)^T$,

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} \sigma^{1-\alpha(t)}\left(\mu_1 - \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) + \gamma_1 L(t-\tau) + \gamma_2 B(t-\tau) - (\delta+\theta)S(t)\right) \\ \sigma^{1-\alpha(t)}\left(\mu_2 + \left(\beta_1 L(t) + \beta_2 B(t)\right)S(t) - \gamma_1 L(t-\tau) - (q+\delta)L(t) + \theta S(t)\right) \\ \sigma^{1-\alpha(t)}\left(qL(t) - \gamma_2 B(t-\tau) - (\delta)B(t)\right) \end{pmatrix}. \tag{9}$$

Then, $f(t, y(t), y(t-\tau))$ is globally Lipschitz continuous as Lipschitz conditions have been satisfied as follows:

$$||f(t, y_1(t), y_1(t-\tau)) - f(t, y_2(t), y_2(t-\tau))|| \leq K_1||y_1(t) - y_2(t)|| + K_1||y_1(t-\tau) - y_2(t-\tau)||, \tag{10}$$

where $K_1 > 0$ and $K_2 > 0$ are Lipschitz constants. So, the solution of the system $f(t, y_i(t), y_i(t-\tau))$ satisfies the existence and uniqueness conditions. In other words, the Lipschitz continuity of system (4) follows from the boundedness of the model functions and their partial derivatives. Since all model parameters are assumed to be bounded real constants and the state variables remain in a bounded domain, the right-hand side satisfies a global Lipschitz condition. Consequently, there exist positive constants K_1 and K_2 such that the Lipschitz condition holds. This ensures the existence and uniqueness of the solution.

Theorem 2. *System (4) has a unique endemic equilibrium point $E^*(S^*, L^*, B^*)$ where*

$$\begin{aligned} S^* &= \frac{\mu_1 + A_1 B^*}{A_2 + A_3 B^*}, \\ L^* &= \frac{\gamma_2 + \delta}{q} B^*, \end{aligned} \tag{11}$$

and B^* is the positive root of $m_2(B^*)^2 + m_1 B^* + m_0 = 0$ with

$$\begin{aligned} m_0 &= -q\left(\mu_1\theta + \mu_2\delta + \mu_2\theta\right), \\ m_1 &= q\delta A_1 + \delta\left(q + \gamma_2 + \delta\right)A_2 - q\left(\mu_1 + \mu_2\right)A_3, \\ m_2 &= \delta\left(q + \gamma_2 + \delta\right)A_3, \end{aligned} \tag{12}$$

where $A_1 = (\gamma_1(\gamma_2 + \delta)/q) + \gamma_2, A_2 = \delta + \theta, A_3 = (\beta_1(\gamma_2 + \delta)/q) + \beta_2$.

Proof 3. The endemic equilibrium point is obtained by setting the fractional derivatives in system (4) equal to zero, which leads to a system of algebraic equations.

$$\begin{aligned} D^{\alpha(t)}(S(t)) &= 0, \\ D^{\alpha(t)}(L(t)) &= 0, \\ D^{\alpha(t)}(B(t)) &= 0, \end{aligned} \tag{13}$$

so $S^* = (\mu_1 + A_1 B^*)/(A_2 + A_3 B^*), L^* = ((\gamma_2 + \delta)/q)B^*$.

Moreover, this equilibrium is endemic, i.e., $L^* + B^* > 0$.

The coefficients m_0, m_1, and m_2 represent the combined effects of infection rates, recovery processes, and external connections. They also describe the balance between malware propagation and control procedure at the equilibrium state. □

Lemma 2. *If $\tau = 0$, then the roots of the characteristic equation of system (4) have negative real parts, and the endemic point (S^*, L^*, B^*) of (4) is locally asymptotically stable. To investigate the local stability of the proposed system (4), the Lyapunov method is employed. The linearized form of system (7) can be written as follows:*

$$D^{\alpha(t)}(y_i(t)) = B_0 u_i + B_1 w_i, \tag{14}$$

where $u_i = y_i(t)$, $w_i = y_i(t-\tau)$, $B_0 = (\partial/(\partial u_i))f(t, u_i, w_i)$, and $B_1 = (\partial/(\partial w_i))f(t, u_i, w_i)$ are 3×3 matrices evaluated at the equilibrium point.

So, $f_1(t, u_i, w_i) = f(t, u_i, w_i) - B_0 u_i - B_1 w_i$ tends to zero when u_i and w_i tend to zero. The following conditions may be needed because of the nonuniform behavior of $f_1(t, u_i, w_i)$ when it approaches zero:

$$\lim_{\|u_i\| \longrightarrow 0} \sup_{t \geq 0} \frac{\|f_1(t, u_i, w_i)\|}{\|u_i\|} = 0, \tag{15}$$

$$\lim_{\|w_i\| \longrightarrow 0} \sup_{t \geq 0} \frac{\|f_1(t, u_i, w_i)\|}{\|w_i\|} = 0. \tag{16}$$

If the above conditions (15) and (16) have been satisfied, then system (14) exists, and it can be considered as the linearization of system (7). Consequently, the stability of the linearized system reflects the local stability of the original nonlinear system. Suppose that P^* is a uniformly asymptotically stable equilibrium point of system (14); then, P^* is also a locally uniformly asymptotically stable equilibrium point of system (7), provided that B_0 and B_1 are bounded.

The above stability analysis is derived for $\tau = 0$. When $\tau > 0$, the delay introduces a more complex characteristic equation, and analytical stability investigation becomes more difficult. Therefore, the effect of τ on system stability is investigated through numerical simulations, reflecting the effect of delayed antivirus response.

The nonnegative solutions of model (4) confirm the physical interpretation of $S(t)$, $L(t)$, and $B(t)$, while the local asymptotic stability of the equilibrium point describes the long-term behavior of malware in the network. These results form the basis for the numerical simulations presented in the next section.

6 | Numerical Simulations and Discussion

The main reason for using numerical methods to solve constant or variable-order fractional models is that exact solutions are difficult to obtain [33]. In this work, we use the Adams–Bashforth–Moulton predictor–corrector scheme, a well-established method for solving fractional-order differential equations [34], which can be extended to variable-order models with time-delay effects. This method offers a good balance of accuracy, stability, and simplicity. All numerical simulations were performed using MATLAB.

The proposed model (4) has been solved for different values of $\alpha(t)$ to study the memory effect on numerical results.

System (4) can be written in the general form as

$$\begin{aligned} D^{\alpha(t)}(S(t)) &= \sigma^{1-\alpha(t)} f_1(t_j, S_j, L_j, B_j), \\ D^{\alpha(t)}(L(t)) &= \sigma^{1-\alpha(t)} f_2(t_j, S_j, L_j, B_j), \\ D^{\alpha(t)}(B(t)) &= \sigma^{1-\alpha(t)} f_3(t_j, L_j, B_j). \end{aligned} \tag{17}$$

We consider the uniform grid $\{t_j = jh\colon j = 0, 1, \cdots, n\}$, with $n \in \mathbb{Z}$ such that $n = T/h$, $\alpha(t) \in (0, 1]$, $0 \leq t \leq T$, and $T \in \mathbb{R}^+$.

The predictors S^p_{n+1}, L^p_{n+1}, and B^p_{n+1} are given by

$$\begin{aligned} S^p_{n+1} &= S_0 + \frac{1}{\Gamma(\alpha(t_{n+1}))} \sum_{j=0}^{n} Q_{j,n+1} f_1(t_j, S_j, L_j, B_j), \\ L^p_{n+1} &= L_0 + \frac{1}{\Gamma(\alpha(t_{n+1}))} \sum_{j=0}^{n} Q_{j,n+1} f_2(t_j, S_j, L_j, B_j), \\ B^p_{n+1} &= B_0 + \frac{1}{\Gamma(\alpha(t_{n+1}))} \sum_{j=0}^{n} Q_{j,n+1} f_3(t_j, L_j, B_j), \end{aligned} \tag{18}$$

where $Q_{j,n+1} = (h^{\alpha(t_{n+1})}/\alpha(t_{n+1}))[(n-j+1)^{\alpha(t_{n+1})} - (n-j)^{\alpha(t_{n+1})}]$, $0 \leq j \leq n$.

The corrector approximations S_{n+1}, L_{n+1}, and B_{n+1} are given by

$$\begin{aligned} S_{n+1} &= S_0 + \frac{h^{\alpha(t_{n+1})}}{\Gamma(\alpha(t_{n+1})+2)} f_1(t_{n+1}, S^p_{n+1}, L^p_{n+1}, B^p_{n+1}) + \frac{h^{\alpha(t_{n+1})}}{\Gamma(\alpha(t_{n+1})+2)} \sum_{j=0}^{n} a_{j,n+1} f_1(t_j, S_j, L_j, B_j), \\ L_{n+1} &= L_0 + \frac{h^{\alpha(t_{n+1})}}{\Gamma(\alpha(t_{n+1})+2)} f_2(t_{n+1}, S^p_{n+1}, L^p_{n+1}, B^p_{n+1}) + \frac{h^{\alpha(t_{n+1})}}{\Gamma(\alpha(t_{n+1})+2)} \sum_{j=0}^{n} a_{j,n+1} f_2(t_j, S_j, L_j, B_j), \\ B_{n+1} &= B_0 + \frac{h^{\alpha(t_{n+1})}}{\Gamma(\alpha(t_{n+1})+2)} f_3(t_{n+1}, L^p_{n+1}, B^p_{n+1}) + \frac{h^{\alpha(t_{n+1})}}{\Gamma(\alpha(t_{n+1})+2)} \sum_{j=0}^{n} a_{j,n+1} f_3\Big(t_j, (L)_j, (B)_j\Big), \end{aligned} \tag{19}$$

where

$$a_{j,n+1} = \begin{cases} n^{\alpha(t_{n+1})+1} - [n - \alpha(t_{n+1})](n+1)^{\alpha(t_{n+1})}, & j = 0, \\ (n-j+2)^{\alpha(t_{n+1})+1} - 2(n-j+1)^{\alpha(t_{n+1})+1} + (n-j)^{\alpha(t_{n+1})+1}, & 1 \leq j \leq n, \\ 1, & j = n+1. \end{cases} \tag{20}$$

The parameters' values and the initial conditions are considered as follows:

$$\mu_1 = 4, \mu_2 = 2, q = 0.2, \beta_1 = 0.01, \beta_2 = 0.02, \gamma_1 = 0.1, \gamma_2 = 0.3, \delta = 0.1, \theta = 0.02, S(0) = 10, L(0) = 5, B(0) = 5. \tag{21}$$

As shown in Figures 1, 2, and 3, the system has been solved for $\alpha(t) = 1$ and $\alpha(t) = 0.9$. It is clear that, when $\alpha(t)$ tends to 1, the non-integer-order model reduces to the standard integer-order model when $\alpha(t) = 1$. Decreasing $\alpha(t)$ increases the memory effect on the numerical results. In other words, decreasing $\alpha(t)$ indicates stronger antivirus update effectiveness. Hence, number of uninfected computers increases while number of latent computers and breaking-out computers decreases as seen in Figures 1, 2, and 3.

The variable order $\alpha(t)$ describes the time-varying memory effect. When $\alpha(t)$ is periodic, the memory effect varies periodically, resulting in numerical solutions with periodic behavior as shown in Figures 4, 5, 6, 7, 8, and 9. If $\alpha(t)$ is a decreasing function, the memory effect becomes stronger. Consequently, the numerical results exhibit slower dynamics over time, as illustrated in Figures 10, 11, and 12.

The auxiliary parameter σ is taken close to unity ($\sigma = 0.99$) to maintain dimensional consistency. Unlike the classical model in [29], σ appears in the variable-order model as a scaling factor for dimensional consistency.

The main contributions of this work can be summarized as follows. The integer-order cyber epidemic model is improved by introducing the variable order $\alpha(t)$ into the integer-order system. The variable fractional order $\alpha(t)$ is an extra degree of freedom added to the system to capture the impact of the evolving memory of the antivirus. It is associated with regular updates which reflect the learning process of antivirus software to detect known or new malware.

To assess the effectiveness of the proposed fractional model, a comparison with the classical approach ($\alpha = 1, \tau = 0$) discussed in [28] is presented in Figures 13, 14, and 15. On the other hand, a comparison with the classical integer-order model proposed in [29] is conducted by considering $\alpha = 1$ and $\tau = 8$. Both the classical case ($\alpha = 1$) and the proposed fractional model for $\tau = 8$ are presented in Figures 1, 2, and 3.

When $\alpha(t)$ approaches zero, the model has a perfect memory. So, lower values of $\alpha(t)$ reflect a more effective and up-to-date antivirus system. From the obtained numerical results, it is clear that the number of infected nodes is decreasing with $\alpha(t) \longrightarrow 0$ (as shown in Figures 2, 3, 4, 5, 6, 7, 8, and 9) while the number of uninfected nodes is increasing (as shown in Figures 1, 4, and 7. The variable-order functions $\alpha = 0.96 - 0.01\cos^2(t)$ and $\alpha = 0.8 - 0.01\sin(\pi t)$ are chosen to simulate fluctuations in antivirus performance over time (see Figures 4, 5, 6, 7, 8, 9, and 10). We choose small amplitudes to ensure realistic memory variations while maintaining system stability. Numerical results in Figures 7, 8, and 9 show that the constant fractional order captures a fixed memory, while the variable order reflects memory that changes over time. In Figures 10, 11, and 12, the time interval is chosen so that $\alpha(t) = 0.9 - 0.0002t$ remains within the range $(0, 1]$, ensuring the model's validity. Figures 4, 5, 6, 7, 8, 9, 10, 11, and 12 illustrate the impact of fractional variable order and time delay on system behavior. These functions describe time-varying memory effects. These effects lead to smoother system dynamics and reduced infection levels. In addition, increasing the time delay τ introduces oscillations and may destabilize the system, while smaller delays promote faster stabilization (see Figure 16).

Figures 17 and 18 illustrate the dynamics of $S(t)$, $L(t)$, and $B(t)$ for $\tau = 8$ under constant and variable fractional orders. For $\alpha = 1$, the system displays sustained oscillations before gradually approaching equilibrium. However, the variable-order case $\alpha(t) = 0.9 - 0.0002t$ leads to smoother behavior and faster convergence. This behavior highlights the influence of time-varying memory, which enhances system stability.

The results in Figures 13, 14, and 15 show the effect of varying the fractional order on $S(t)$, $L(t)$, and $B(t)$ for $\tau = 0$. As α decreases, the system exhibits smoother dynamics with reduced transient oscillations. Also, the number of breaking-out computers $B(t)$ decreases as memory effects become stronger. In other words, lower fractional orders enhance the system's resistance to malware. Furthermore, the variable-order case produces slightly

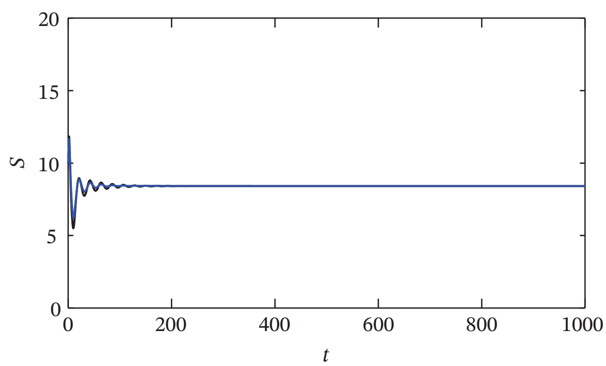

FIGURE 1 | Dynamics of uninfected computers $S(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$.

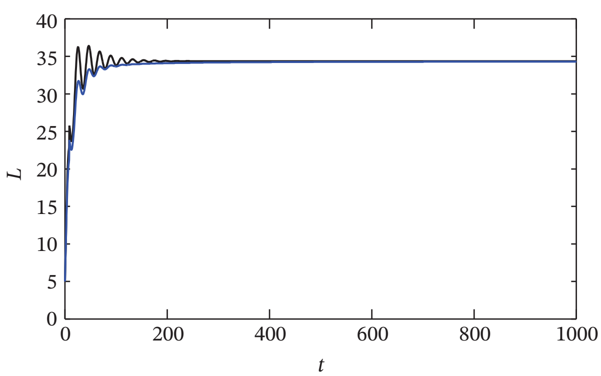

FIGURE 2 | Dynamics of latent computers $L(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$.

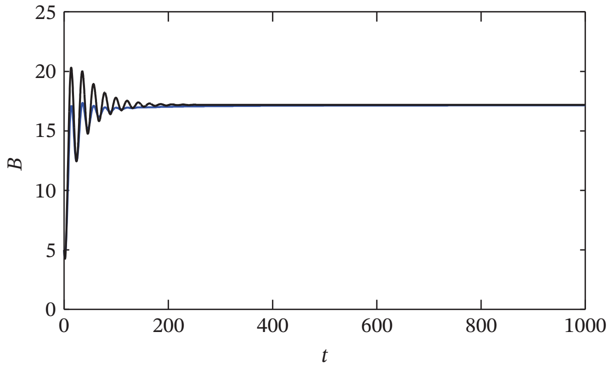

FIGURE 3 | Dynamics of breaking-out computers $B(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$.

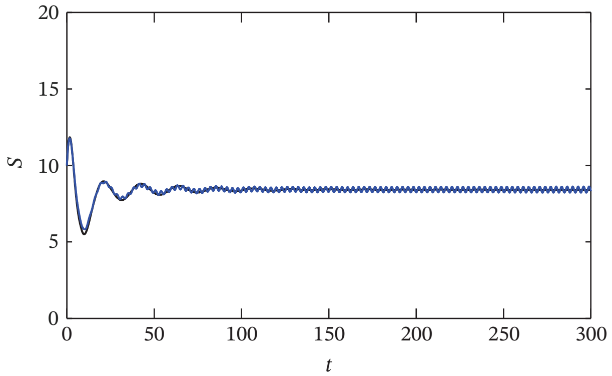

FIGURE 4 | Dynamics of uninfected computers $S(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.96 - 0.01\cos^2(t)$.

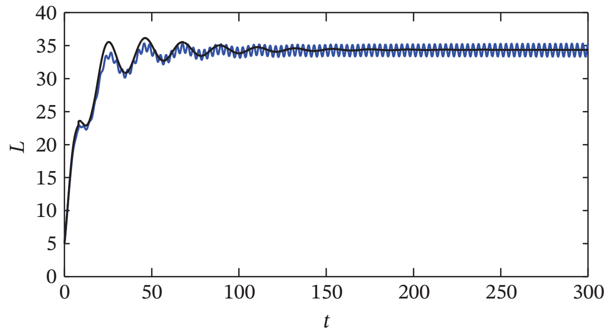

FIGURE 5 | Dynamics of latent computers $L(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.96 - 0.01\cos^2(t)$.

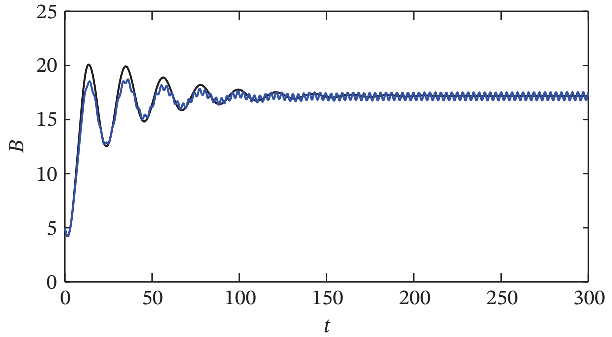

FIGURE 6 | Dynamics of breaking-out computers $B(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.96 - 0.01\cos^2(t)$.

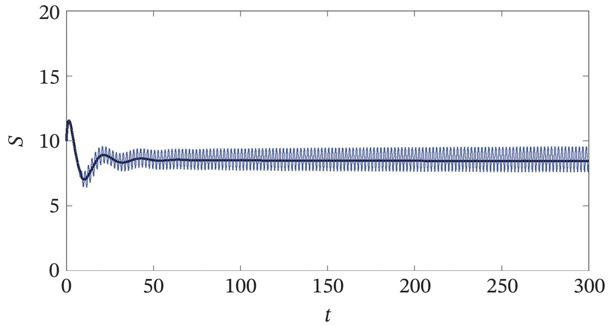

FIGURE 7 | Dynamics of uninfected computers $S(t)$ for $\tau = 8$. Black curve: $\alpha = 0.8$; blue curve: $\alpha = 0.8 - 0.01\sin(\pi t)$.

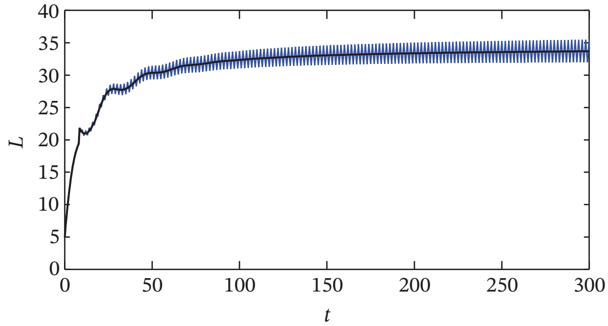

FIGURE 8 | Dynamics of latent computers $L(t)$ for $\tau = 8$. Black curve: $\alpha = 0.8$; blue curve: $\alpha = 0.8 - 0.01\sin(\pi t)$.

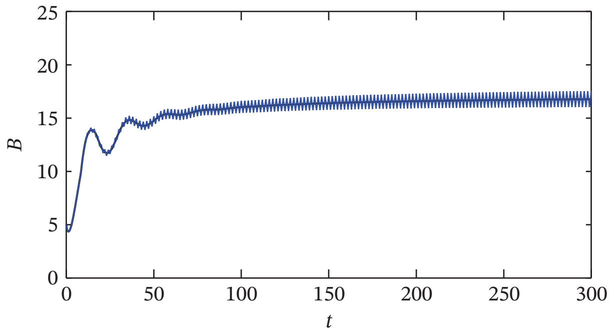

FIGURE 9 | Dynamics of breaking-out computers $B(t)$ for $\tau = 8$. Black curve: $\alpha = 0.8$; blue curve: $\alpha = 0.8 - 0.01\sin(\pi t)$.

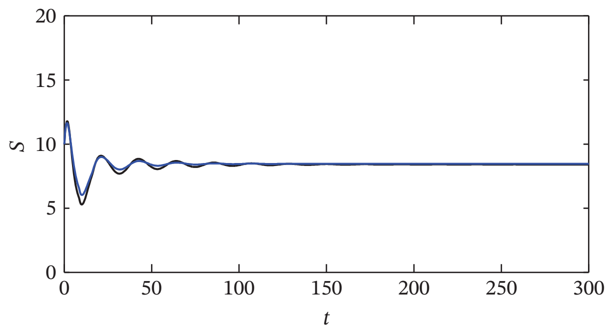

FIGURE 10 | Dynamics of uninfected computers $S(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9 - 0.0002t$.

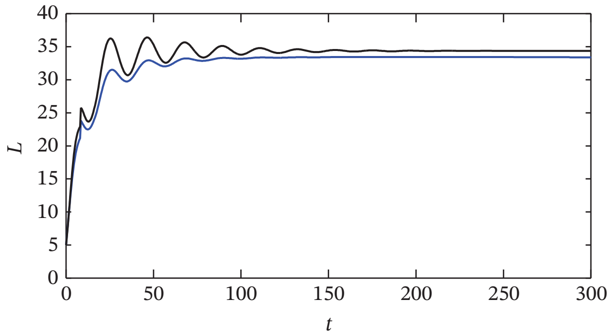

FIGURE 11 | Dynamics of latent computers $L(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9 - 0.0002t$.

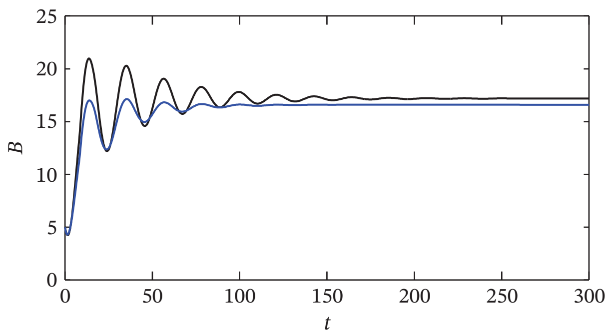

FIGURE 12 | Dynamics of breaking-out computers $B(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9 - 0.0002t$.

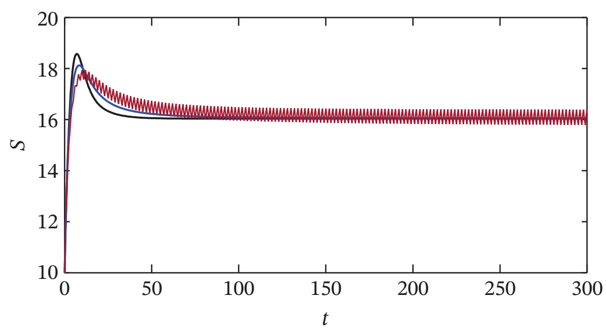

FIGURE 13 | Dynamics of uninfected computers $S(t)$ for $\tau = 0$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$; and red curve: $\alpha(t) = 0.8 - 0.01\sin(\pi t)$.

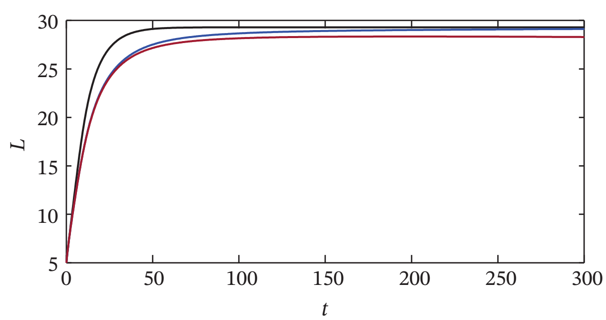

FIGURE 14 | Dynamics of latent computers $L(t)$ for $\tau = 0$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$; and red curve: $\alpha(t) = 0.9 - 0.0002t$.

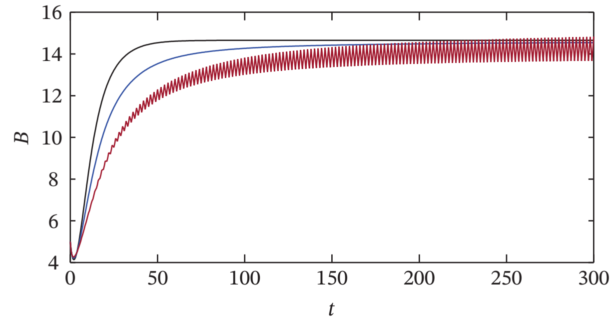

FIGURE 15 | Dynamics of breaking-out computers $B(t)$ for $\tau = 0$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$; and red curve: $\alpha(t) = 0.8 - 0.01\sin(\pi t)$.

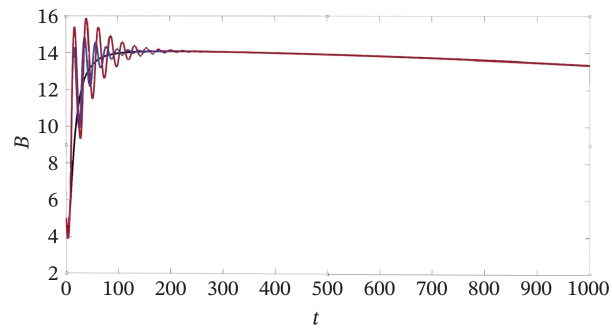

FIGURE 16 | Effect of time delay τ on the breaking-out computers $B(t)$ for $\alpha(t) = 0.9 - 0.0002t$. Black curve: $\tau = 0$; blue curve: $\tau = 7$; and red curve: $\tau = 8$.

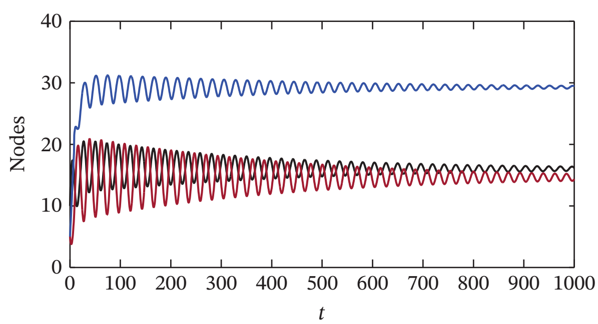

FIGURE 17 | Dynamics of uninfected $S(t)$, latent $L(t)$, and breaking-out $B(t)$ computers for $\tau = 8$ and $\alpha = 1$. Black curve: $S(t)$; blue curve: $L(t)$; and red curve: $B(t)$.

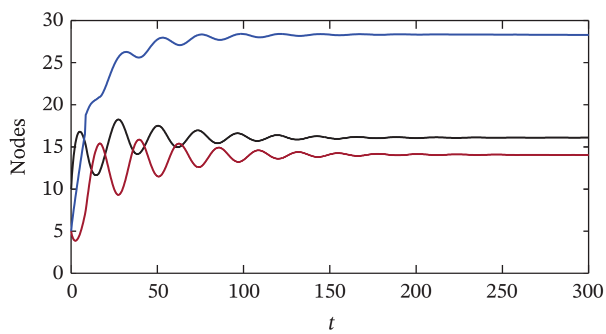

FIGURE 18 | Dynamics of uninfected $S(t)$, latent $L(t)$, and breaking-out $B(t)$ computers for $\tau = 8$ and $\alpha(t) = 0.9 - 0.0002t$. Black curve: $S(t)$; blue curve: $L(t)$; and red curve: $B(t)$.

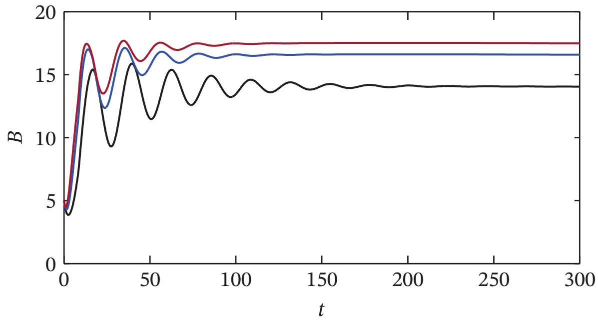

FIGURE 19 | Effect of the latent infection rate β_1 on the dynamics of breaking-out computers $B(t)$ for $\tau = 8$ and $\alpha(t) = 0.9 - 0.0002t$. Black curve: $\beta_1 = 0.01$; blue curve: $\beta_1 = 0.03$; and red curve: $\beta_1 = 0.05$.

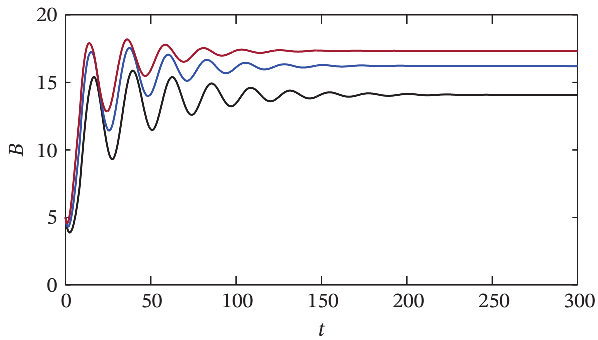

FIGURE 20 | Effect of the breaking-out infection rate β_2 on the dynamics of breaking-out computers $B(t)$ for $\tau = 8$ and $\alpha(t) = 0.9 - 0.0002t$. Black curve: $\beta_2 = 0.01$; blue curve: $\beta_2 = 0.05$; and red curve: $\beta_2 = 0.09$.

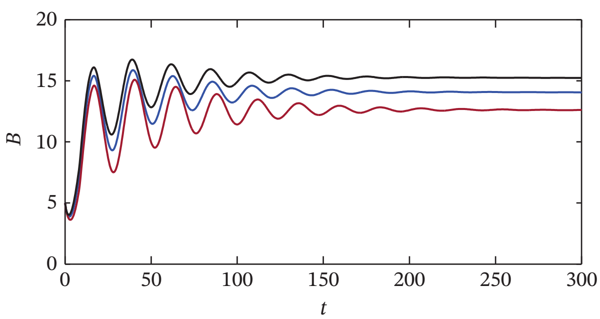

FIGURE 21 | Effect of the latent recovery rate γ_1 on the dynamics of breaking-out computers $B(t)$ for $\tau = 8$ and $\alpha(t) = 0.9 - 0.0002t$. Black curve: $\gamma_1 = 0.02$; blue curve: $\gamma_1 = 0.1$; and red curve: $\gamma_1 = 0.2$.

different dynamics compared to the constant fractional-order as shown in Figures 13, 14, and 15. This highlights the ability of the variable-order model to capture evolving memory effects.

The influence of the latent and breaking-out infection rates β_1 and β_2 on $B(t)$ is shown in Figures 19 and 20. Increasing these parameters leads to higher levels of infection and larger oscillation amplitudes. Figure 21 illustrates that increasing the latent recovery rate γ_1 reduces the number of breaking-out computers. This highlights the role of recovery mechanisms in controlling malware spread. On the other hand, Figure 22 illustrates the impact of the external infection rate θ, showing that increasing θ leads to higher infection levels.

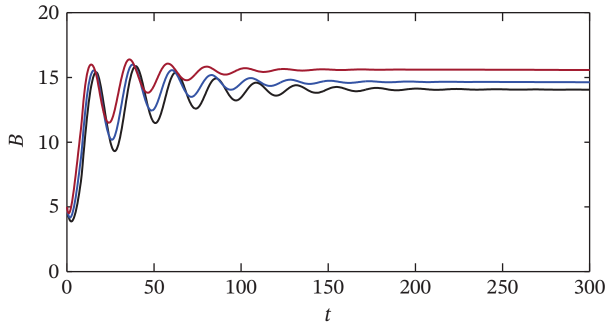

FIGURE 22 | Effect of the external infection rate θ on the dynamics of breaking-out computers $B(t)$ for $\tau = 8$ and $\alpha(t) = 0.9 - 0.0002t$. Black curve: $\theta = 0.02$; blue curve: $\theta = 0.2$; and red curve: $\theta = 0.3$.

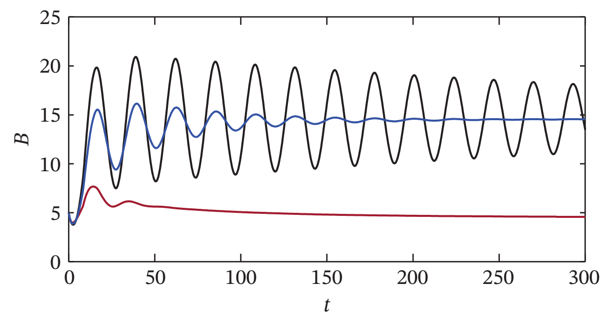

FIGURE 23 | Dynamics of breaking-out computers $B(t)$ for $\tau = 8$. Black curve: $\alpha = 1$; blue curve: $\alpha = 0.9$; and red curve: $\alpha(t) = 0.8/(1 + 0.02t)$.

As shown in Figure 23, decreasing the fractional order leads to a lower infection levels. Moreover, it is evident that as $\alpha(t)$ tends to zero, the memory effect becomes stronger. Consequently, the number of infected computers decreases, and the system becomes more stable.

Figure 16 shows that increasing the time delay τ leads to stronger oscillations in $B(t)$ during the early stages. This reflects the effect of delayed antivirus response on infected computers. All curves eventually converge nearly to the same steady state. This indicates that the delay primarily affects the transient behavior rather than the long-term dynamics.

The proposed model gives a better understanding of malware propagation under the memory effect. Therefore, a better understanding of computer virus propagation under the memory effect (regular antivirus updates) is provided by the proposed model. In addition, the influence of time delay due to the time taken by the antivirus to remove the virus from the infected devices is considered in the proposed mode. So, we hope that this study can help to develop antivirus software based on the proposed model.

Overall, the results show that variable-order memory and time delay provide a deeper understanding of cyber epidemic dynamics. They also highlight memory effects and delayed response on system behavior.

7 | Conclusion

In this work, a delayed cyber epidemic fractional model with variable order is proposed. Numerical simulations are executed to investigate the dynamics of the proposed model. The variable-order fractional derivative is employed to capture the time-dependent memory effect on the dynamics of the antivirus software. The time delay represents the time taken by the antivirus to detect and eliminate malware. We use the predictor–corrector method due to its efficiency in solving variable-order fractional dynamical systems. Furthermore, it is suitable for capturing the memory effects and provides stable numerical solutions for systems with time delay. We argue that studying memory effects can improve antivirus strategies and reduce malware spread. The results show that frequent antivirus updates (captured by variable memory effects) and reduced response delays play a significant role in improving antivirus performance. Future work will focus on validating the proposed model using real data and assessing its predictive capability.

Author Contributions

Mohamed Khalil: conceptualization and mathematical formulation, investigation, formal analysis, and writing–review and editing.

Anas Arafa: supervision, formal analysis, visualization of numerical results, validation, and writing–review and editing.

Ahmad Almutlg: supervision, methodology, formal analysis, and writing–review and editing.

Amaal Sayed: methodology, software implementation, numerical simulations, visualization, writing–original draft, and writing–review and editing.

Acknowledgments

The authors would like to acknowledge the Deanship of Graduate Studies and Scientific Research at Qassim University for its financial support (QU-APC-2026). The authors confirm that no AI tools were used in modeling and analysis in this study. ChatGPT was used only for minor language editing and grammar checking during the preparation of the manuscript.

Funding

The researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for its financial support (QU-APC-2026).

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

No datasets were generated or analyzed during this study.

References

1. D. Howard, K. Prince, and B. Schneier, *Security 2020: Reduce Security Risks This Decade* (John Wiley and Sons, 2010), https://doi.org/10.1002/9781118255803.

2. H. J. Highland, "A History of Computer viruses—Introduction," *Computers and Security* 16, no. 5 (1997): 412–415, https://doi.org/10.1016/S0167-4048(97)01002-8.

3. K. Thakur and A. S. K. Pathan, *Cybersecurity Fundamentals: A Real-World Perspective* (CRC Press, 2020), https://doi.org/10.1201/9780429283850.

4. L. Guo, Y. Wang, H. Liu, C. Li, J. Zhao, and H. Chu, "On Iterative Positive Solutions for a Class of Singular Infinite-Point *p*-Laplacian Fractional Differential Equation With Singular Source Terms," *Journal of Applied Analysis and Computation* 13, no. 5 (2023): 2827–2842, https://doi.org/10.11948/20230008.

5. H. A. A. El-Saka, A. A. M. Arafa, and M. I. Gouda, "Dynamical Analysis of a Fractional SIRS Model on Homogeneous Networks," *Advances in Difference Equations* 2019, no. 1 (2019): 144, https://doi.org/10.1186/s13662-019-2083-0.

6. V. K. Shukla, M. C. Joshi, J. E. N. Valdes, P. K. Mishra, and C. Xu, "Combination–Combination Synchronisation and Ultimate Bound of the Fractional-Order Ecological System," *Pramana—Journal of Physics* 100, no. 1 (2026): 34, https://doi.org/10.1007/s12043-025-03055-7.

7. P. A. Naik, M. Farman, K. Jamil, K. S. Nisar, M. A. Hashmi, and Z. Huang, "Modeling and Analysis Using Piecewise Hybrid Fractional Operator in Time Scale Measure for Ebola Virus Epidemics Under Mittag–Leffler Kernel," *Scientific Reports* 14, no. 1 (2024): 24963, https://doi.org/10.1038/s41598-024-75644-2.

8. Y. Yang, Q. Qi, J. Hu, J. Dai, and C. Yang, "Adaptive Fault-Tolerant Control for Consensus of Nonlinear Fractional-Order Multi-Agent Systems With Diffusion," *Fractal and Fractional* 7, no. 10 (2023): 760, https://doi.org/10.3390/fractalfract7100760.

9. T. Jia, X. Chen, L. He, F. Zhao, and J. Qiu, "Finite-Time Synchronization of Uncertain Fractional-Order Delayed Memristive Neural Networks via Adaptive Sliding Mode Control and Its Application," *Fractal and Fractional* 6, no. 9 (2022): 502, https://doi.org/10.3390/fractalfract6090502.

10. V. K. Shukla, M. C. Joshi, P. K. Mishra, and C. Xu, "Generalized Synchronization Between Coupled Integer, Fractional and Delay Chaotic Systems," *Evolving Systems* 16, no. 4 (2025): 132, https://doi.org/10.1007/s12530-025-09758-x.

11. M. Alwuthaynani, U. Ishtiaq, H. A. El-Wahed Khalifa, A. Alburaikan, R. Idress, and I. L. Popa, "Fractional-Order Modelling and Analytical Solutions for MHD Casson Fluid Flow in an Inclined Channel With Heat and Mass Transfer," *Scientific Reports* 15, no. 1 (2025): 39790, https://doi.org/10.1038/s41598-025-23478-x.

12. Y. Sokolovskyy, K. Drozd, T. Samotii, and I. Boretska, "Fractional-Order Modeling of Heat and Moisture Transfer in Anisotropic Materials Using a Physics-Informed Neural Network," *Materials* 17, no. 19 (2024): 4753, https://doi.org/10.3390/ma17194753.

13. Z. Masood, R. Samar, and M. A. Z. Raja, "Design of a Mathematical Model for the Stuxnet Virus in a Network of Critical Control Infrastructure," *Computers and Security* 87 (2019): 101565, https://doi.org/10.1016/j.cose.2019.101565.

14. Q. Zhu, G. Zhang, X. Luo, and C. Gan, "An Industrial Virus Propagation Model Based on SCADA System," *Information Sciences* 630 (2023): 546–566, https://doi.org/10.1016/j.ins.2023.02.030.

15. Q. Gao and J. Zhuang, "Stability Analysis and Control Strategies for Worm Attack in Mobile Networks via a VEIQS Propagation Model," *Applied Mathematics and Computation* 368 (2020): 124584, https://doi.org/10.1016/j.amc.2019.124584.

16. M. Farman, A. Akgül, A. Ahmad, M. U. Saleem, and M. O. Ahmad, "Modeling and Analysis of Computer Virus Fractional Order Model," *Methods of Mathematical Modeling* (2022): 137–157, https://doi.org/10.1016/B978-0-323-99888-8.00010-3.

17. C. Ravichandran, K. Logeswari, A. Khan, T. Abdeljawad, and J. F. Gomez-Aguilar, "An Epidemiological Model for Computer Virus With Atangana–Baleanu Fractional Derivative," *Results in Physics* 51 (2023): 106601, https://doi.org/10.1016/j.rinp.2023.106601.

18. A. Al-Jarrah, M. Alquran, A. Freihat, S. Al-Omari, and K. Nonlaopon, "A Fractional-Order Model for Computer Viruses and Associated Solutions via Residual Power Series Method," *Applied Mathematics in Science and Engineering* 31, no. 1 (2023): 2214301, https://doi.org/10.1080/27690911.2023.2214301.

19. N. Sweilam, S. M. Al-Mekhlafi, R. G. Salama, and T. A. Assiri, "Numerical Simulation for a Hybrid Variable-Order Multi-Vaccination COVID-19 Mathematical Model," *Symmetry Plus* 15, no. 4 (2023): 869, https://doi.org/10.3390/sym15040869.

20. W. Adel, H. Günerhan, K. S. Nisar, P. Agarwal, and A. El-Mesady, "Designing a Novel Fractional-Order Mathematical Model for COVID-19 Incorporating Lockdown Measures," *Scientific Reports* 14, no. 1 (2024): 2926, https://doi.org/10.1038/s41598-024-52926-0.

21. D. Amilo, B. Kaymakamzade, and E. Hincal, "A Fractional-Order Mathematical Model for Lung Cancer Incorporating Integrated Therapeutic Approaches," *Scientific Reports* 13, no. 1 (2023): 12426, https://doi.org/10.1038/s41598-023-39485-1.

22. Z. Huang, Q. Haider, Z. Sabir, M. Arshad, B. K. Siddiqui, and M. M. Alam, "A Neural Network Computational Structure for the Fractional Order Breast Cancer Model," *Scientific Reports* 13, no. 1 (2023): 22756, https://doi.org/10.1038/s41598-023-49872-2.

23. F. A. Rihan and K. Udhayakumar, "Optimal Control of Glucose–Insulin Dynamics via Delay Differential Model With Fractional Order," *Alexandria Engineering Journal* 114 (2025): 243–255, https://doi.org/10.1016/j.aej.2024.10.012.

24. S. Sawar, M. Ayaz, M. S. Aldhabani, M. Abd El-Rahman, S. Hussain, and S. Jebran, "Modeling Nonlinear Variable-Order Fractional Chaotic Systems Using the Caputo–Fabrizio Operator and Radial Basis Function Neural Networks," *Scientific Reports* 16, no. 1 (2026): 7912, https://doi.org/10.1038/s41598-026-39288-8.

25. N. H. Sweilam, S. M. Al-Mekhlafi, Z. N. Mohammed, and D. Baleanu, "Optimal Control for Variable-Order Fractional HIV/AIDS and Malaria Mathematical Models With Multi-Time Delay," *Alexandria Engineering Journal* 59, no. 5 (2020): 3149–3162, https://doi.org/10.1016/j.aej.2020.05.026.

26. N. H. Sweilam and S. M. Al-Mekhlafi, "Numerical Study for Multi-Strain Tuberculosis Model of Variable-Order Fractional Derivatives," *Journal of Advanced Research* 7, no. 2 (2016): 271–283, https://doi.org/10.1016/j.jare.2015.06.002.

27. A. A. M. Arafa, M. Khalil, and A. Sayed, "A Non-Integer Variable-Order Mathematical Model of HIV and Malaria Coinfection With Time Delay," *Complexity* 2019 (2019): 1–13, https://doi.org/10.1155/2019/4291017.

28. L. X. Yang and X. Yang, "A New Epidemic Model of Computer Viruses," *Communications in Nonlinear Science and Numerical Simulation* 19, no. 6 (2014): 1935–1944, https://doi.org/10.1016/j.cnsns.2013.09.038.

29. Z. Zhang, S. Kumari, and R. K. Upadhyay, "A Delayed e-Epidemic SLBS Model for Computer Virus," *Advances in Differential Equations* 2019 (2019): 1–24, https://doi.org/10.1186/s13662-019-2341-8.

30. N. H. Sweilam, S. M. Al-Mekhlafi, A. Almutairi, and D. Baleanu, "A Hybrid Fractional COVID-19 Model With General Population Mask Use: Numerical Treatments," *Alexandria Engineering Journal* 60, no. 3 (2021): 3219–3232, https://doi.org/10.1016/j.aej.2021.01.041.

31. Z. M. Odibat and N. T. Shawagfeh, "Generalized Taylor's Formula," *Applied Mathematics and Computation* 186, no. 1 (2007): 286–293, https://doi.org/10.1016/j.amc.2006.07.102.

32. W. Lin, "Global Existence Theory and Chaos Control of Fractional Differential Equations," *Journal of Mathematical Analysis and Applications* 332, no. 1 (2007): 709–726, https://doi.org/10.1016/j.jmaa.2006.10.040.

33. R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete* (American Mathematical Society, 2012), https://doi.org/10.1090/mbk/019.

34. K. Diethelm, N. J. Ford, and A. D. Freed, "A Predictor–Corrector Approach for the Numerical Solution of Fractional Differential Equations," *Nonlinear Dynamics* 29, no. 1–4 (2002): 3–22, https://doi.org/10.1023/A:1016592219341.