Instituto Superior de Engenharia do Porto

PROPAGAÇÃO DE VÍRUS INFORMÁTICOS BASEADA EM MODELOS BIOLÓGICOS

Rúben Manuel da Rocha Azevedo

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Arquitetura, Sistemas e Redes

Orientador: Doutora Carla Manuela Alves Pinto

Júri:

Presidente:

[Doutora Maria de Fátima Coutinho Rodrigues, Professora Coordenadora, ISEP]

Vogais:

[Doutor Nuno Alexandre Magalhães Pereira, Professor Adjunto, ISEP]

[Doutora Carla Manuela Alves Pinto, Professora Adjunta, ISEP]

Porto, [Julho] [2013]

Dedicatória

Dedico esta dissertação a todos aqueles que acreditaram em mim e fizeram parte de todo o processo de realização desta tese.

Resumo

A evolução digital proporcionou às sociedades uma facilidade extraordinária de comunicação. Com o número crescente de computadores e o aumento de acessos à internet, surgiu uma nova forma de criminologia, que cresceu em paralelo com o número de utilizadores. Desta forma, tornou-se comum a criação e difusão de vírus informáticos pelos chamados hackers.

Neste trabalho estudam-se modelos de transmissão de vírus informáticos, usando modelos epidemiológicos. Começa-se por fazer uma revisão dos modelos existentes na literatura, de seguida sugerem-se alterações a esses modelos de forma a conseguir uma melhor aproximação à dinâmica real de transmissão de vírus informáticos. As simulações numéricas dos modelos permitem-nos inferir de que uma forma de controlar a transmissão de vírus informáticos é a diminuição da taxa de infeção, isto é, da taxa de transmissão do vírus. No último capítulo enumeram-se as conclusões do trabalho efetuado e indicam-se direções de trabalho futuro.

Palavras-chave: vírus informáticos, transmissão, modelos biológicos.

Abstract

The digital evolution in the last decades has provided extraordinary communications facilities. With the increasing number of computers and internet access, a new form of criminology has emerged, which grew in parallel with the number of users. In this way, it became common the creation and dissemination of computer viruses by the so-called hackers.

This work studies models for computer viruses transmission, based on epidemiological models. We start by doing a review of the existing models in the literature, then suggest changes to these models, in order to get a better approximation to the real dynamics of transmission of computer viruses. The numerical simulations of the models allow us to infer that a way to control the transmission of computer viruses is to decrease the infection rate, i.e. the rate of transmission of the virus. In the last chapter, we list the findings of the work carried out and suggest directions of future work.

Keywords: computer virus, transmission, biological models.

Agradecimentos

Percorrendo todos os momentos vividos durante a elaboração desta dissertação, reconheço que é mais do que um trabalho individual, é o resultado da colaboração e contributos de várias pessoas, num processo que foi tudo, menos solitário. Por esta razão, quero expressar os meus sinceros agradecimentos:

Primeiramente, à Professora Doutora Carla Pinto, que sempre me incentivou e fez acreditar que era possível, com a sua sabedoria, capacidade de trabalho, organização e especialmente pela paciência e simpatia que sempre me recebeu.

À minha noiva Sílvia Tavares, por todo o incentivo, por sempre acreditar que eu seria capaz, por todo o amor, carinho e dedicação.

Aos meus pais, porque sempre foram pessoas fundamentais em todo o meu percurso de vida.

À minha irmã Andreia e ao Sérgio Oliveira, porque sempre me motivaram a fazer mais e sempre deram motivos para acreditar que seria possível.

Ao meu saudoso Tio Júlio Gomes, que onde quer que esteja, estará muito orgulhoso por ter-me levantado num momento tão difícil para a nossa família. Ele que será sempre recordado como sendo um exemplo e um lutador para mim.

À minha Tia Filomena Gomes e ao meu Primo Fábio Gomes, aos dois que mesmo no momento da perda, disponibilizaram um pouco das suas forças para me incentivar e encorajar.

E por fim, mas não menos importantes, a todos aqueles que directa ou indirectamente influenciaram de forma positiva a realização desta dissertação.

A todos o meu mais sincero obrigado!

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos e Símbolos

Lista de Acrónimos

SI	Modelo Suscetível – Infectado
SIS	Modelo Suscetível – Infectado-Suscetível
SIR	Modelo Suscetível – Infetado-Recuperado
MS-DOS	*Microsoft Disk Operating System*
EUA	Estados Unidos Da América
SIRS	Modelo Suscetível – Infetado-Recuperado - Suscetível

1 Introdução

O ser humano tem como uma das suas maiores necessidades a comunicação, esta torna-se produtiva para a sociedade quando é utilizada para objetivos comuns. O desenvolvimento dos métodos de comunicação foi essencial para suprimir as dificuldades causadas pela distância geográfica entre as pessoas, tornando a comunicação entre os povos uma necessidade e um desafio constante a ser superado.

A evolução digital proporcionou que as sociedades tivessem muito mais facilidade de acesso aos computadores, à internet e a outros novos meios tecnológicos que surgiram com o avanço das novas descobertas electrónicas. Esta evolução, originou uma nova forma de criminologia, que tem aumentado em paralelo com o aumento de acessos a este meio. Considera-se um crime, por exemplo, a difusão de vírus informáticos, o vandalismo eletrónico, o roubo ou fraude através de ataques a instituições bancárias ou posse ilegal de dados bancários de outro cidadão, sabotagem provocada nos meios informáticos, acesso indevido ou não autorizado a dados ou informações armazenadas, entre outros [Oliveira and Oliveira, 2005] [Colares, 2002].

Os *Hackers* são programadores mal-intencionados que causam danos a terceiros. Encontraram formas ainda mais eficazes de melhorar os seus programas tentando complicar ao máximo a cura para os seus vírus e desta forma aumentar o tempo para que seja descoberto o código antiviral, dando-lhe um comportamento idêntico aos vírus biológicos.

Como existe uma grande semelhança entre os vírus informáticos e os vírus biológicos, os modelos de transmissão de vírus de doenças epidemiológicas são utilizados usualmente para explicar o fenómeno de transmissão de vírus informáticos.

Neste trabalho estudamos alguns desses modelos epidemiológicos para explicar a propagação de vírus informáticos. Nomeadamente, selecionam-se três modelos propostos na literatura, exemplificativos da generalidade desses modelos. Estuda-se pormenorizadamente estes modelos salientando as suas constribiuções e as suas falhas no âmbito da propagação dos vírus informáticos. Propõem-se uma alteração ao terceiro modelo, acrescentando um atraso, o que se traduz num novo sistema de equações diferenciais ordinárias com atraso. Neste e no primeiro modelo, variou-se a taxa de infeção do vírus, estudo ausente das publicações existentes na literatura. Esta variação proporcionou a observação de uma bifurcação de Hopf, que não estava relatada na literatura para estes modelos.

Esta dissertação organiza-se da seguinte forma. No capítulo 2 apresenta-se o estado da arte relativamente aos *Hackers* e à transmissão de vírus informáticos. Descreve-se as motivações dos *Hackers* e posteriormente, apresentar-se a evolução das várias classificações, que foram criadas ao longo da história, para os mesmos. Neste mesmo capítulo, define-se um vírus informáticos, refere-se alguns dos vírus que marcaram a história e como deram origem à necessidade de criar uma forma de os detetar, neutralizar e remover dos sistemas informáticos com o auxílio de antivirus. No capítulo 3 aborda-se alguns dos modelos existentes na literatura para transmissão de vírus informáticos. No capítulo 4 apresentam-se as simulações de dois modelos de propagação de vírus. No último capítulo escreve-se as conclusões principais deste trabalho.

1.1 Contextualização

Para a sociedade, a evolução da comunicação foi importante na criação e desenvolvimento de meios de comunicação mais fiáveis e eficazes.

Na década de 80, os computadores sofreram alterações (tamanho, preço) que permitiram que os comerciantes, entidades empresariais e a população em geral, tivessem acesso a estes aparelhos. Até à data estes utilizadores não tinham possibilidade para adquiri-los devido aos seus custos de aquisição demasiado elevados. Esta nova geração de computadores, os que mais se notabilizaram no mercado pertenciam à *IBM*. O primeiro foi lançado no ano de 1982 e tinha como designação *IBM PC*. Outro modelo interessante era o *Apple Macintosh*, lançado no mercado no ano de 1984[Mentor, 1986].

O aumento do número de utilizadores originou um crescimento de oportunidades para os programadores mal intencionados, *hackers*, se aproveitarem das vulnerabilidades dos sistemas operativos e do desconhecimento e inexperiência destes novos utilizadores.

O aumento da pirataria está muito ligado à área económica, mas outro fator preponderante é o de ordem psicológica. Muitos *hackers* criam os vírus informáticos para terem sentimentos em tudo idênticos aos de rebeldia ou de simplesmente infringirem as leis, sentindo-se superiores em relação aos cidadãos que cumprem a lei.

Os programas que são especificamente desenvolvidos para executar ações nefastas nos computadores são designados por softwares maliciosos ou *malwares* e os mais conhecidos são os cavalos de troia (*trojan horse*), vermes (*worms*) e por fim os vírus.

Até ao ano de 2010, estima-se que o número de vírus de computador criados esteja situado entre 100.000 e 150.000, segundo Ivo Simões[Simões, 2010]. É praticamente impossível ser determinado um número exato porque muitos dos códigos virais não foram difundidos e/ou descobertos o que invalida a determinação de um número correto. Os vírus informáticos, quando são devidamente estruturados e pensados, podem provocar as mais diversas consequências devastadoras à economia e à sociedade provocando avolumados prejuízos monetários em danos. Segundo a empresa *mi2g*, o vírus *MyDoom* no ano de 2004, teve um impacto de 26,1 biliões de dólares, demonstrando claramente o seu impacto devastador [Zhu et al., 2012].

Os vírus informáticos são definidos como um programa de computador que tem a capacidade de se copiar e infectar outros computadores. Este tipo de programas herdaram o nome de vírus, porque compartilha algumas características dos vírus biológicos, isto, porque é possível o vírus propagar-se de um computador para o outro, tal como acontece com os vírus biológicos nos humanos. Vários autores compararam e encontraram diversas semelhanças entre os vírus biológicos e os vírus informáticos, desenvolvendo vários estudos para a propagação de vírus informáticos utilizando modelos de propagação de vírus biológicos.

Tem-se observado um progresso extraordinário na compreensão de diferentes cenários de transmissão de doenças e comportamentos de epidemias, na área da epidemiologia biológica. Um passo fundamental, foi a construção e análise de equações diferenciais, com e sem atraso de tempo [Blyuss and Kyrychko, 2010; Huang et al., 2010; Li et al., 2011, 2009; Song et al.,

2011]. Este sucesso, atraiu a atenção dos investigadores de vírus de computador, que após análise, verificaram que existem semelhanças entre a epidemiologia biológica e os vírus informáticos, possibilitando uma instrução teórica perfeita para controlar a prevalência de vírus de computador.

Em 1986, Cohen [Cohen, 1986], comprovou as semelhanças entre os vírus biológicos e os vírus informáticos. Um estudo de Kephart e White [Kephart and White, 1993, 1991] foi o primeiro passo para modelar devidamente o comportamento do vírus de computador durante a sua propagação. Zou *et al*. [Zou *et al.*, 2006, 2005, 2002] utilizou o modelo suscetível-infetado-suscetível (SI/SIS) e o modelo suscetível-infetado-recuperado (SIR) para analisar a propagação do vírus Red Code, porque pretendia investigar a propagação do vírus, dado que era afetado pelas características dos mesmos e pelas medidas de precaução do humano. Han e Tan[Han and Tan, 2010], demonstraram comportamentos dinâmicos mais complexos, como a bifurcação para trás e a bifurcação de Hopf, em dois modelos de propagação de vírus de computador. Estes estudos referidos anteriormente possibilitaram e forneceram uma compreensão mais abrangente e elucidativa das condições sob as quais os vírus de computador se propagam e porque alguns vírus têm uma capacidade superior de propagação em relação a outros. Mais tarde, outros autores sentiram a necessidade de considerar que os dispositivos externos (como por exemplo, PEN USB, discos externos entre outros) podiam ser atacados por vírus e posteriormente contaminarem também os computadores. Actualmente, os dispositivos externos são um dos principais meios de propagação de vírus a par das redes de computadores [Zhu *et al*., 2012].

Existem estudos em diferentes topologias de rede para a propagação de objectos maliciosos, como vírus e worms, em que se verifica que existem falhas. Deste modo, medidas de precaução que o utilizador pode aplicar para evitar a propagação de vírus informáticos, como por exemplo, realizar limpezas no sistema, aplicar as devidas actualizações e filtragens, entre outros, são muito importantes [De *et al.*, 2009; Garetto *et al*., 2003; Moreno *et al*., 2002]. Assim, Kephart e White [Kephart and White, 1993, 1991], concentraram a sua atenção sobre o efeito da estrutura topológica da rede na propagação de vírus, para com estes elementos tentar descobrir o mecanismo de propagação desses vírus.

1.2 Objetivos

No desenvolvimento deste trabalho, pretende-se estudar modelos epidemiológicos para a transmissão de vírus informáticos.

Apresentam-se detalhadamente três modelos demonstrativos da literatura que foi recolhida e analisada para a propagação de vírus informáticos.Salienta-se os pontos fortes e pontos fracos dos três modelos, sugerem-se alterações e varia-se a taxa de infeção dos vírus. Estes dois últimos itens constituem um valor acrescentado no estudo deste tipo de modelos.

1.3 Calendarização

Tabela 1 - Calendarização do projeto

		Out				Nov				Dez				Jan				Fev				Mar				Abr				Mai				Jun				Jul
ETAPA	**SEMANA**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**
Pesquisa	**4 S**																																					
Estudo do estado da arte de vírus e hackers	**6 S**																																					
Estudo dos modelos biológicos	**7 S**																																					
Simulação dos modelos biológicos	**12 S**																																					
Elaboração do Relatório Final	**8 S**																																					

2 Hackers e Vírus Informáticos

O computador em conjugação com a Internet tornou-se num dos maiores meios de comunicação para a sociadade atual. Este grande desenvolvimento potenciou pessoas mal intensionadas da sociedade a tirar partido das suas possíveis fragilidades.

Os programadores mal intencionados designados de *hackers*. O termo *hacker* é de origem inglesa, derivado do verbo *to hack*. Originalmente, este era apenas aplicado a fabricantes de móveis que recorriam a um machado [Vianna, 2005]. No meio informático, são programadores que se dedicam a obter soluções que ultrapassam os limites do funcionamento de um sistema previsto pelos seus criadores, obtendo acesso a certos dados e a controlos de sistemas que estão impedidos de controlar.

Na informática, um vírus é um software com intensões maliciosas desenvolvido por *hackers*. O vírus informático é programado com a característica de se reproduzir e ser transferido de um computador para outro, sem que o utilizador tenha a perceção de que o seu sistema foi contaminado por este. O processo de propagação e contaminação de um vírus informático pode ser equiparado à dinâmica de propagação dos vírus biológicos, pois "silenciosamente" infecta o sistema, realizando cópias de si mesmo e tenta propagar-se para outros computadores através dos mais diversos meios, como redes *peer-to-peer*, plataformas de intercâmbio de ficheiros online ou simples e-mails, entre outros.

Maioritariamente estes programas são idealizados para destruir ou ter acesso a dados, ou então imobilizar ou perturbar as operações do sistema.

2.1 Motivações dos Hackers

Existem várias razões que motivam os *hackers* a criar vírus informáticos. Eles são impulsionados pelas sensações de vandalismo e terrorismo. Reside na sua personalidade, uma essência destrutiva e maliciosa direcionando os seus conhecimentos e esforços para criar vírus que tenham consequências negativas para a restante população, com o único objectivo de alimentar o seu ego [Honório, 2003] .

Outro motivo, dado pela Psicologia, para este comportamento é a emoção sentida pelos *hackers* ao verem as coisas "explodirem", isto é, as consequências dos seus atos crescerem em cadeia e todas as suas consequências graves que podem provocar. Este sentimento é comparado ao dos terroristas, pelo fascínio que sentem pelas explosões e destruição em massa.

A terceira razão, envolve violar os direitos de propriedade, ou demonstrar vulnerabilidade do sistema atingindo o "impenetrável". Após descobrir uma falha de segurança num sistema, o programador tenta explorá-la de forma provocar falhas graves no sistema. Desta forma, o hacker sente que demonstrou a sua genialidade abrindo caminhos para outros programadores explorarem esta mesma falha.

Outra grande motivação dos hackers é a intenção de provocar perdas económicas através do roubo de informações, utilizando o método de disseminação de malware e assim ter proveitos próprios.

Por fim, o hacker pode ser movido pela crença religiosa ou cultural, como por exemplo os hackers islâmicos que atacam websites ocidentais que os façam sentir provocados ou contra os seus ideais [Nóbrega, J., 2009].

The Mentor em 1986, tornou-se lendário para a comunidade *Hacker* ao criar o manifesto *The Conscience of a Hacker.* Incentiva outros indivíduos a entrarem e experimentarem o "seu mundo". No texto abaixo pode verificar o manifesto na íntegra.

The Conscience of a Hacker [i]

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him? I am a hacker, enter my world... Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me... Damn underachiever. They're all alike…

… I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me... Or thinks I'm a smart ass...

And then it happened... a door opened to a world...

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals…

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike [Mentor, 1986].

A comunidade *cyberpunk* aderiu de forma massiva a este manifesto, aceitando as suas ideias e visões expressas pelo seu criador, *The Mentor*. Rapidamente se tornou no maior clássico deste comunidade e é praticamente impossível encontrar um *hacker* da velha guarda que não tenha conhecimento do mesmo e se deixa guiar e emocionar pela ideologia defendida pelo mesmo [Vianna, 2003].

2.1.1 Classificação dos Hackers

Existem vários autores que realizaram escalas para classificar os grupos de *hackers*. Landreth no ano de 1985 [Rogers, 2003], com os seus estudos, concluiu que os *hackers* podiam ser divididos por categorias distintas, tendo como elementos classificativos o grau de experiência

e a motivação. As categorias da classificação propostas por Landreth são cinco e designam-se, da menos grave para a mais grave, em termos de consequências danosas, de: *novice*, *student, tourist, crasher* e *thief* [Vianna, 2003].

Hollinger em 1988, com os dados que recolheu para o seu estudo, dos crimes informáticos sucedidos nas comunidades informáticas, deduziu que podia classificar os *hackers* através do nível técnico, nomeadamente em *pirates*, *browsers* e *crackers* [Rogers, 2003]. O trabalho de Hollinger contribui para diferenciar os violadores de direitos de autor sobre o software dos invasores de redes de computador, tendo esta escala como fator limitativo o facto de não ser mais detalhada [Vianna, 2003].

Em 1996, Chantler melhorou a classificação atribuída aos *hackers*, utilizando diversas variáveis como por exemplo, a atividade do *hacker*, as suas proezas, o conhecimento, as motivações e o tempo que dedica à atividade, dividindo-os em três categorias: elite *group*, *noephytes* e *losers* [Rogers, 2003] [Vianna, 2003]. Esta classificação não distingue completamente o nível técnico da motivação.

No ano de 1998, Power divide os *hackers* em três grupos, *os sport intruders, competitive inteligence* e os *foreing intelligence* [Rogers, 2003]. O ponto forte desta classificação é a divisão entre os *hackers* amadores e os profissionais. Por seu lado esta classificação peca por não fazer uma análise mais detalhada da categoria dos amadores tratando este grupo como um só [Vianna, 2003].

Também no ano de 1998, Parker sugere sete classes para identificar os vários tipos de *hackers*: os *pranksters, hacksters, malicius hackers, personal problema solvers, career criminals, extreme advocates* e os *malcontents* [Rogers, 2003]. Esta classificação é muito eficiente, apesar de ser um pouco confusa e bastante complexa por levar em conta o nível técnico do *hacker*.

Em 2003, Marc Rogers encontra uma nova classificação para os *hackers*, sendo que a sua classificação tem bastantes semelhanças com a de Parker. Esta não faz uma divisão concreta, porque utiliza critérios de ordem objetiva, a nível técnico, com elementos subjetivos como a motivação ou a intenção. Esta classificação está dividida em sete classes, *newbie/tool kit, cyberpunks, internals, coders, old guard hackers, professional criminals,* e *cyber-terrorists* [Rogers, 2003].

Recentemente estas categorias de hipóteses foram alvo de mais estudos, o que originou uma necessidade de testar ou pelo menos representá-los de uma forma visual para testes. O método tradicional até à data seria a utilização de dois eixos, em que o eixo principal seria a motivação e o outro eixo representativo do nível de habilidade e enredo de cada categoria sobre esses eixos [Rogers, 2003]. Este método utilizado é limitado porque não possibilita o estudo das interações entre os dois componentes principais, a habilidade e a motivação [Rogers, 2006].

Como alternativa, foi apresentado o método circumplexo que permite a representação de relações complexas cujas variáveis estão interligadas. Este método, tem flexibilidade para representar vários conceitos de comportamento, como por exemplo, as capacidades cognitivas, interpessoais, psicopatologia, entre outros. Mas neste caso em concreto, está vocacionado para orientar e vincular a taxonomia dos *hackers* com um modelo circumplexo circular modificado [Rogers, 2006].

2.2 Vírus Informáticos

O termo vírus deriva do latim vírus, que significa veneno ou toxina [Vianna, 2005][Simões, 2010]. Este termo foi aplicado à informática para programas maliciosos, mas, foi inicialmente utilizado apenas nas Ciências Biológicas para designar agentes infeciosos. Os *hackers* criaram os vírus informáticos com o mesmo conceito e funcionamento que os vírus biológicos [Simões, 2010], implementando como característica básica apresentar comportamentos similares aos dos vírus biológicos. Os vírus de computador são programados para criar cópias de si mesmos para, desta forma, conseguirem prolongar a sua presença e tempo de "vida" no(s) sistema(s) em que se alojaram.

Do mesmo modo, os vírus informáticos possuem a metodologia de preservação da própria espécie, tendo os requisitos mínimos para serem considerados formas de vida [Simões, 2010].

Os vírus informáticos necessitam de uma aplicação hospedeira para ter a possibilidade de replicar e infectar outros sistemas.

Os *Hackers* encontraram formas ainda mais eficazes de melhorar os seus programas, tentando complicar ao máximo a cura para o seu vírus e desta forma aumentar o tempo para que seja descoberto o código antiviral. Tentam, também, aumentar e dificultar o tempo necessário

para a detecção dos objetos infetados e manter o vírus ativo e fazer com que tenha as condições para se replicar pelo maior tempo possível. Por fim, restringem a aquisição do conhecimento viral por parte dos investigadores que colaboram com as empresas de antivírus[Simões, 2010].

O diagrama abaixo, sintetiza as grandes diferenças entres três tipos:

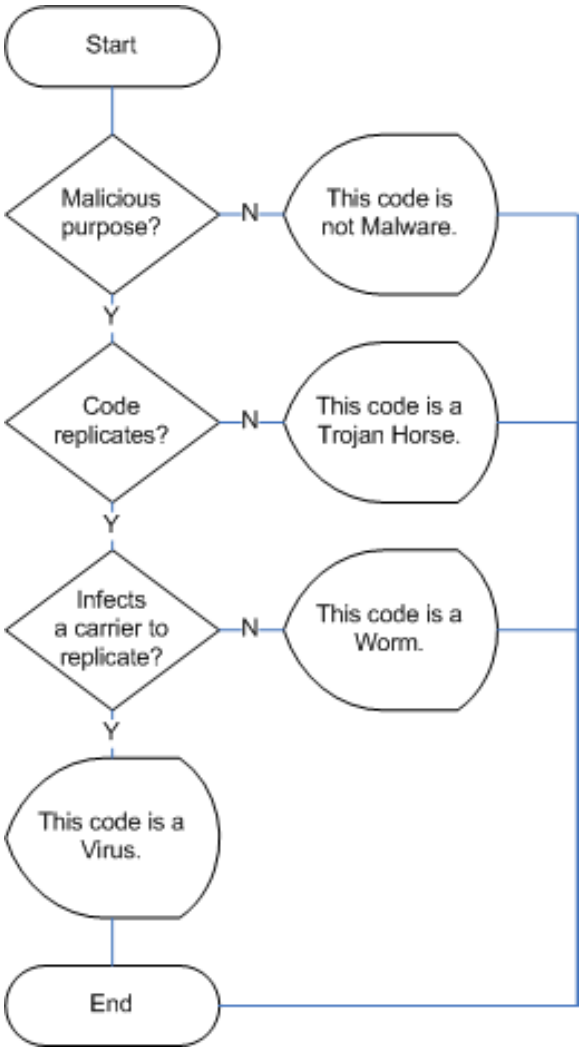

Figura 1 - Árvore de decisão de um código mal-intencionado [Gaspar, 2007].

Estas pragas a cada dia que passa, tornam-se cada vez melhores, mais complexas e mais difíceis de detectar, porque os seus criadores incutem mais capacidades de replicação e de "invisibilidade", tendo agora novos objetivos além dos danos que conseguem causar ao sistema, procurando o roubo de informações confidenciais entre outros aspetos igualmente graves e ilegais. Desta forma os desafios são cada vez maiores para a industria de segurança

que tem que melhorar e adaptar-se de uma forma ainda mais eficaz para todo o tipo de *malwares* que possam surgir.

2.2.1 Vírus Informáticos da História

Decorria o ano de 1982 quando Rich Skrenta, um estudante com apenas 15 anos, desenvolvia aquele que é considerado o primeiro vírus de computador pessoal para os computadores *Apple II* [Gaspar, 2007]. Este ataque deu-se devido à grande aderência dos utilizadores aos computadores *Apple II*, despertando a atenção dos criadores de vírus. O primeiro vírus de distribuição ampla conhecido, tem como designação, *The Cloner Elk* e tinha como finalidade propagar-se para outros computadores através da unidade de disquetes que se escrevia nas disquetes que fossem colocadas no sistema infetado. Então cada computador em que essa disquete infetada fosse colocada ia contaminar o sistema e posteriormente todas as disquetes inseridas nos computadores com o sistema contagiado iriam infetar as restantes disquetes. A cada cinquenta inicializações que o computador realizava aparecia um pequeno poema. O *Elk Cloner* não causava danos nos dados, ele apenas irritava os utilizadores e a pior consequência que o vírus podia ter, era o facto do disco que contivesse uma imagem que não fosse a de padrão do sistema porque o programa copia-se a si mesmo na mesma posição independentemente do conteúdo da disquete.

Em 1983, Fred Cohen no estudo "*Experiments with computer viruses*", relata e batiza os programas com objectivos maliciosos e nocivos para os computadores como "Vírus de computador" [Gaspar, 2007].

Neste mesmo ano, Len Eidelmen durante um seminário sobre segurança computacional, apresentou um programa auto-replicante a funcionar num sistema *VAX11/750* que consistia em instalar-se em vários locais do sistema.

Fred Cohen, em 1984, definiu os vírus de computador como sendo um programa que pode infetar outros programas modificando-os para incluir uma cópia possivelmente evoluída de si. Com a propriedade de infecção, o vírus pode espalhar-se por todo o sistema do computador ou rede utilizando as autorizações de cada utilizador usando-as para infetar os seus programas. Cada programa que é infetado pode também atuar como um vírus, e portanto a infecção aumenta [Cohen, 1984].

No ano de 1986 foi descoberto o *Brain*, o primeiro vírus de computador do *IBM PC* que utilizava o sistema operativo *MS-DOS* da *Microsoft* [Rohr, 2011].

O vírus *Brain*, pertence à classe de *boot* pois, apropriava-se de uma grande parte da memória infetando o setor de *boot* e teve a capacidade de se expandir por praticamente todo o mundo num pequeno espaço de meses.

A facilidade que este vírus teve para se propagar deveu-se à quase ausência total de consciência na comunidade de computação de como proteger os computadores.

O vírus *Brain* foi desenvolvido por dois irmãos paquistaneses que se chamavam Farooq Alvi Basit e Amjad e segundo eles, este vírus foi escrito com o intuito de medirem o nível de pirataria no seu país, só que perderam o controle sobre a sua propagação, isto porque eles tinham criado um software médico de monitorização cardíaca que tinham desenvolvido para a plataforma da *Apple*. Eles descobriram que o seu programa tinha sido copiado por um outro programador para o sistema operativo *MS-DOS* [Rohr, 2011][Toor, 2011].

O *Brain* incluía uma sequência de texto contendo nomes, o endereço e o número de telefone dos seus programadores.

Em 1987, é descoberto o vírus Vienna desenvolvido pelo estudante Rolf Burger. Este vírus, cada vez que é executado infeta os programas *.com do disco rígido, os programas eram alterados pelo vírus e aumentava o espaço ocupado de forma a forçar o sistema a reiniciar-se continuamente até que todos o programas fossem substituídos por cópias não contaminadas [MalwareWiki, 2013][McAfee, 2013a].

Dark Avenger, também conhecido como Eddie, era o pseudónimo de um programador de vírus de computador famoso da Bulgária. Este vírus foi lançado em 1989 e utilizava uma técnica nova para a data designada como *fast infector*, que contaminava os programas muito rapidamente e de forma muito eficaz mas os seus efeitos só surgiam muito lentamente [F-Secure, 2013a].

No ano de 1991 foi lançado o vírus Michelangelo descoberto na Nova Zelândia. Este vírus foi projetado para infetar o *MS-DOS* e está programado para ser executado apenas a 6 de março de cada ano, data de aniversário do artista renascentista. Este, infetava a informação do primeiro sector do disco rígido designado por *Master Boot Record*. Uma vez infetado,

qualquer disquete que era inserida no sistema ficava contagiada pelo vírus, mas como este vírus apenas era ativado a 6 Março de cada ano, este podia nunca ser descoberto pelo utilizador ou então demorar anos a ser descoberto [Schell, B. and Martin, C., 2010].

Em abril de 1994, um programador desempregado com 26 anos a residir em *Devon*, no Reino Unido chamado Christopher Pile, criou o vírus Pathogen que realizava upload de um arquivo infetado para um *pop-up* de aviso no computador, desta forma as vítimas iriam fazer o download de uma cópia do arquivo. Este vírus continha um segundo vírus, o *SMEG*, que tinha como função esconder o Pathogen dos softwares de antivírus. O autor deste vírus foi um dos poucos *hackers* que foram presos e condenados pelas consequências causadas pelo seu vírus [Standler, R., 2002].

Durante o ano de 1995, surgiu o vírus *Concept*, que trazia consigo uma nova abordagem para a disseminação de vírus nos computadores. O criador do *Concept* utilizou uma macro escrita no *Word* básico para o *Microsoft Word* em alternativa ao típico programa contaminado com vírus. Retirou as típicas restrições que um programa tinha, pois deixou de estar restrito a um sistema de computador específico, tendo assim a possibilidade de funcionar em qualquer um dos sistemas desenvolvidos até à altura. O único requisito era o sistema ter instalado o *Microsoft Word.* Este vírus foi criado para que sempre que um documento infetado fosse carregado pelo utilizador ele ficaria com o seu sistema infetado com o vírus. A forma como o vírus infetava o sistema era muito rápida e eficaz pois a macro do modelo copia o vírus para o modelo principal do sistema e assim todos os documentos do *Microsoft Word* depois de abertos, iriam ficar infetados com o *Concept*. O *Concept* foi um revolucionário pois, para iniciar uma infeção num sistema, deixou de ser necessário correr um pedaço de código, para simplemente um documento que tinha que ser aberto pelo utilizador [Forest, N., 2013].

O vírus *CIH* foi criado no ano de 1998, conseguindo limpar as memórias de centenas de milhares de computadores de todo mundo, mas as zonas mais afetadas foram os países asiáticos e do médio oriente. Este vírus foi programado para destruir sistematicamente cada parte do sistema infetado. Ele foi concebido para substituir a informação crítica em unidades do sistema infetado e corromper o sistema de entrada/saída básico (*BIOS*), tornando-se um dos vírus informáticos mais prejudiciais para os computadores. Este vírus foi responsável por destruir milhões de computadores em todo o mundo provocando prejuízos económico extremamente elevados [F-Secure, 2013c].

Posteriormente este vírus ganhou a designação *Chernobyl*, pois o seu criador Chen Ing Hau, nasceu na Tailandia no dia em que ocorreu o desastre nuclear de *Chernobyl*, decorrido na Ucrânia em 1986 [Beattie, A., 2012][Janssen, C., 2013].

No ano de 1999 surgiu o *Melissa* criado por David L. Smith, sendo este vírus baseado numa macro do *Microsoft*, utilizando como método de propagação as mensagens do email. Quando o utilizador abria um documento com uma mensagem "*Here is that document you asked for... don´t show anyone else ;-)*". Depois de o utilizador abrir o documento, o vírus está programado para realizar uma cópia de si mesmo e ser enviado para os primeiros cinquenta contatos da lista do utilizador contaminado [Standler, R., 2002].

A origem do nome do vírus *Melissa* inspirando-se no nome de uma dançarina exótica da Flórida e causou danos estimados entre os valores de US$300 milhões e os US$600 milhões [Strickland, J., 2013].

O vírus *I Love You teve* origem nas Filipinas a 5 de Maio de 2000 e foi atribuído como nome oficial *Love-letter-for-you.txt* mas foi abreviado para *I Love you*. O worm foi disseminado via email para se propagar de uma forma extremamente rápida e eficaz, tendo atingido inúmeros sistemas e de acordo com a *CCOMputer Economics*, mais de 45 milhões de computadores em todo o mundo foram infetados pelo vírus. Este vírus entrou para a história do mundo digital, pois segundo a empresa de consultoria *Computer Economics*, as perdas e os danos causados foram devastadores e até à data da sua criação as mais elevadas de sempre [Standler, R., 2002][Festa, P. and Wilcox, J., 2013].

O vírus *Nimda*, de trás para a frente lê-se "*admin*", foi um dos vírus de computador criado no ano de 2001. Foi o que mais rapidamente se propagou pela Web e tinha como grande objetivo tornar o trafego da internet muito mais lento. Na verdade, segundo o *TruSecure CTO* Peter Tippett, este vírus apenas necessitou de vinte e dois minutos desde o momento que atingiu a Internet até alcançar o topo da lista de relatos de ataques tendo como alvos principais os computadores pessoais e os servidores de *Internet* [Standler, R., 2002][Anthes, G., 2002].

O *Ninda* para se propagar, utiliza o email como meio de difusão com anexos designados como "*readme.exe*". Utilizava também sites pouco seguros como forma de chegar aos seus objetivos, porque consegue anexar-se aos navegadores dos utilizadores que visitavam estes sites [Subramanya, 2001].

Depois de entrar no sistema, o hacker ficava com acesso ao computador infetado com o mesmo nível de permissões que tinha a última conta que teve acesso ao computador agora infetado.

No ano de 2002 surgiu o primeiro vírus que infetava os arquivos Shockwave Flash designado por SWF/LFM-926. Este vírus quando era executado, exibia uma mensagem "Loading.Flash.Movie…". Utilizava o CMD.EXE para executar o programa DEBUG.EXE para criar um arquivo chamado V.COM na pasta em que foi executado, e assim infetar outros ficheiros SWF no mesmo directório [Hypponen, M., 2002] [Sophos, 2002].

Em 2004 o vírus Mydoom afetou computadores com o sistema operativo Microsoft Windows. Este Worm tornou-se até à data que foi difundido, aquele que mais rápidamente se propagou através do email, excedendo recordes de vírus anteriores como por exemplo do vírus I Love You [Strickland, J., 2004].

O Mydoom era acompanhado de uma mensagem que dizia, "andy: I´m just doing my job, nothing personal, sorry,". Esta mensagem levou várias pessoas a acreditar que o autor foi pago para o conceber, sendo que até aos dias de hoje ainda se desconhece quem foi o programador deste vírus [F-Secure, 2013c] [RecoveryLabs, 2004].

Também no ano de 2004, foi criado um trojan horse para o sistema MAC OS X, com a finalidade de comprovar que existia uma brecha de segurança. O MP3Concept passa a imagem de ser um arquivo de MP3 comum, mas quando o utilizador executa o arquivo, este exibe uma mensagem com o texto " this is an application (So what is your iTunes playing right now?)" [Schmudlach, M., 2004] [Symantec, 2007] [Wikimedia, 2010] .

W32.Sality, foi descoberto no ano 2007, este vírus tem como finalidade infetar arquivos com extensões: .EXE, .SCR e .PIF. O W32.Sality utiliza como uma das suas técnicas de infeção a geração polimórfica de código viral [Falliere, N., 2011].

Em 2009, surgiu o Waledac, também designado por Waled ou Waledpak [Microsoft, 2013]. Este, era um *trojan* que agrupava endereços de email que se encontravam no computador infetado e posteriormente difundia mensagens de email de spam. Este trojan teve uma taxa de infeção entre 70000 a 90000 computadores e tinha a capacidade de enviar cerca de 1,5

bilhões de mensagens de spam por dia, ou seja cerca de 1% do volume total de spam global [F-Secure, 2013b].

No ano de 2011 foi descoberto o ZeroAccess, que é um trojan horse que tem como finalidade atacar os sistemas operativos Microsoft Windows. Este tem como principal objectivo camuflar-se ou camuflar outras espécies de malware. O ZeroAccess tem a capacidade de eliminar processos reconhecidos de ferramentas de segurança para não ser detetado e/ou eliminado. Além desta capacidade o ZeroAccess pode atuar como botnet, recorrendo a um sistema P2P para dificultar a identificação e o impedimento da comunicação com o exterior e receber instruções precisas sobre o que deve realizar a cada momento [McAfee, 2013b] [Shearer, J., 2011].

2.3 Antivírus

Segundo o vice-presidente de vendas da *Trend Micro Inc*, uma empresa especializada em segurança de computadores só na Europa, foram mais de quinze mil companhias que foram contaminadas pelo *Nimda* e nos EUA, segundo o investigador da *Cooperative Association for Internet Data Analysis,* David Moore, este vírus infetou cerca de cento e trinta mil servidores e inúmeros computadores [Reuters, 2001].

Nos últimos anos as operações que são realizadas por empresas, bancos, governos, entre muitos outros, cresceram à medida que a ligação em rede dos computadores se tornou mais sofisticada. Desta forma os *hackers* e os "ciber-criminosos" aumentaram os seus esforços para tirarem partido deste rápido desenvolvimento e do grande aumento de utilizadores. Os *hackers* aperceberam-se das grandes vantagens que podiam tirar de muitas fragilidades existentes nos softwares desenvolvidos e fornecidos pelas empresas que os criam. Há a preocupação de proteger os utilizadores destes perigos e passar-lhes uma sensação de que podem gerir e usufruir destes sistemas com toda a segurança informática.

Apareceu uma pequena indústria, até ao final dos anos 90, que se dedicava a desenvolvimento de software com o objetivo de fornecer uma proteção antivírus aos utilizadores de computadores [Mota, 2010].

Atualmente, qualquer organização que desenvolva software para proteger os computadores de ataques informáticos tem um desafio diário de manter os computadores protegidos e

atualizados. O aumento de complexidade com que estes códigos maliciosos são desenvolvidos dificultam cada vez mais a sua deteção e mesmo depois de detetados exigem correções cada vez mais complexas.

Assim sendo, os antivírus foram criados com a finalidade de detetar vírus, neutralizar as suas acessões maliciosas e removê-los do sistema [Santos and Barros, 2005].

2.3.1 Funcionamento e Procedimentos

Para funcionar na sua plenitude, os antivírus devem ser atualizados com frequência para poderem ser eficazes na deteção de novos vírus que surgem diariamente. Os meios utilizados para realizar a deteção de vírus são quatro no total.

Cada vírus tem uma assinatura própria e o antivírus utiliza-a para o identificar. Este método é o mais utilizado pelos antivírus para detetar vírus, é designado por investigação de assinatura (*scanning*). Este método só é eficiente se a base do antivírus estiver atualizada, assim pode-se verificar que este método só é viável para identificar vírus conhecidos. Para contornar esta fácil identificação do programa de antivírus, os *hackers,* dotaram os seus programas com a capacidade de camuflagem, de forma a tornar a sua assinatura ainda mais complexa de detetar, podendo mesma ser indetetável. Quando os vírus são dotados desta capacidade são designados por vírus polimorfos. Estes vírus, até à data são os mais complexos, pois evitam a deteção criando uma mutação em si cada vez que infecta um novo programa. Todas as mutações criadas adquirem todas as suas capacidades anteriores para infetar os sistemas da mesma forma que o seu progenitor [Nachenberg, 1997].

Existe uma diferença de atuação entre os vírus de computador polimorfos e os vírus biológicos. Nos biológicos, podem verificar-se imensas mutações que podem não ter sucesso, no entanto, como ocorrem em grande número, alguns dos descendentes mutantes podem ter êxito. Por outro lado, os vírus de computador não têm a oportunidade de proceder dessa forma [Nachenberg, 1997].

Os vírus polimórficos informáticos não são mutados na sua totalidade, eles são desenhados por *mutation engines* que simulam o processo de mutação. Estes, não podem ser detetados com as chamadas máscaras de vírus, ou então são detetadas com grande dificuldade. É uma grande contrariedade para os analistas de segurança, porque cada amostra replicada é

significativamente diferente da antecessora e assim, tornam praticamente ineficazes os processos de assinaturas de antivírus criados para detetar vírus informáticos.

Esta nova metodologia, originou nas empresas produtoras de antivírus, a necessidade de encontrar uma forma eficaz para responder a esta forma de vírus, pelo que criaram uma solução criativa para tentar afastar este tipo de ameaças dos computadores dos utilizadores. Os programas de antivírus começaram a ser constituídos por uma técnica conhecida como *generic decryption* para detectar os vírus polimórficos mais complexos de uma forma rápida e com o mínimo de custos [Nachenberg, 1997].

Nos vírus polimórficos só a sua forma exterior e o modo como se apresenta muda. O seu código base não é reescrito.

Segundo vários investigadores, a fronteira existente entre o mundo digital e o mundo físico está a deixar de existir, porque atualmente são utilizados dispositivos eletrónicos no corpo humano, como por exemplo o *pacemaker*, estimuladores cerebrais e implantes cocleares. E desta forma, o corpo humano fica vulnerável a partir do momento que existe a necessidade de algum destes dispositivos tenham que comunicar com um equipamento externo, expondo-se desta forma a possíveis vírus informáticos [ComputerWorld, 2012].

Numa era de grande desenvolvimento tecnológico, em que um dos principais benificiários é o comércio electrónico, os vírus começaram a ser observados como ameaças irracionais à integridade do mercado emergente virtual em evolução.

Parte dos antivírus, para verificar se os ficheiros do utilizador foram alterados, recorrem a um controlador de integridade, que tem como características, construir uma base de dados que contém todas as informações relativamente aos ficheiros executáveis do sistema do seu utilizador. Assim, caso um ficheiro executável sofra alguma alteração que mude as suas características, o antivírus previne o seu utilizador.

Outro método de funcionamento dos antivírus, consiste em analisar o comportamento das aplicações para verificar se existe uma atividade ou um comportamento idêntico a algum dos vírus conhecidos. Este método designa-se como heurístico e possibilita que o antivírus tente impedir que a máquina fique contaminada com algum vírus, que ainda não esteja registado na sua base de dados. O software nocivo, é detetado pela estrutura característica do ficheiro ou das execuções típicas. Independentemente da mutação que o arquivo tenha tido, o antivírus

analisa e vai classificar a estirpe principal e tem a capacidade de identificar as suas mutações, as quais são designadas por variantes. Muitas vezes os vírus podem crescer em diferentes linhagens, na tentativa de se disfarçarem para evitarem a deteção segundo este método.

A parte negativa deste método é a quantidade de falsos alertas que o antivírus pode desencadear.

O método baseado em assinaturas que coleciona todas as assinaturas do vírus na base de dados de forma a fazer um rastreio aos programas, mas para funcionar o antivírus necessita de ser atualizado regularmente. O funcionamento deste método é muito simples ele compara a assinatura dos programas com as que tem armazenadas na base de dados, a partir do momento que e identificado o antivírus pode eliminar ou isolar o programa suspeito. Este método é considerado o método mais seguro para a proteção de antivírus.

Tem como lado negativo o facto de apenas detetar vírus conhecidos na sua base de dados [Symantec, 2013].

O utilizador está sempre exposto ao risco de contaminação, para tal tem que estar consciente dos riscos que corre perante as decisões que toma, pois mesmo o software "gratuito" ou de "domínio público" pode acarretar riscos, e desta forma cabe ao utilizador se quer mesmo viver e arriscar avançar com a situação [Mota, 2010]. O computador do utilizador pode ser infetado por um vírus informático, mas também está vulnerável a outros riscos, como por exemplo, *hackers* ou "ciber-criminosos" que tem como objetivo e finalidade encontrar e decifrar os pontos fracos no sistema informáticos dos computadores dos utilizadores para poderem ter acesso aos segredos mais íntimos, e assim violarem as "fronteiras" criadas pelos sistemas informáticos. Desta forma foram feitos esforços para fornecer ao computador o equivalente digital de um sistema imunitário imaginário, para que o corpo seja protegido como se de uma fortaleza sobre ameaça se tratasse [Mota, 2010].

Os antivírus, por analogia, tal como os anticorpos, tem como função eliminar infeções e vírus que surgem no corpo humano, e desta forma, são visto como os protetores do sistema informático.

A resposta por parte dos investigadores das empresas de antivírus tem que dar prioridade às virtudes de resposta flexíveis e adaptativas para conseguir assegurar o sistema informático e

protege-lo contra ataques de vírus informáticos. Esta noção de adaptabilidade tem sido abordada por vários autores, que afirmam ser necessária para melhorar a eficiência dos antivírus utilizando analogias relativas à evolução. Estes, sugerem que os sistemas operativos devem ser programados com maior capacidade de flexibilidade e desta forma aumentarem a sua eficiência de resposta perante os novos vírus que continuamente vão surgindo. Esta noção de adaptabilidade é vista como um factor essencial pelos peritos que procuram desenvolver defesas ainda mais eficazes contra os vírus informáticos, designados por vírus polimórficos [Mota, 2010].

Para ser manter a integridade dos sistemas dos computadores, os profissionais de segurança informática querem aliar a flexibilidade à estabilidade, na tentativa de encontrar um ponto de equilíbrio durante a era da especialização flexível [Helmreich, 2000].

Hackers, vírus informáticos e antivírus têm sofrido um grande desenvolvimento nos últimos anos, isto porque todos têm uma ligação direta. Os hackers criam os vírus informáticos e a com estes há a necessidade de criar os antivírus respectivos para os detetar, neutralizar e remover. Ao longo da história, *hackers,* vírus e antivírus desenvolveram-se consideravelmente. O hacker visualiza e idealiza os novos vírus informáticos, dotando-os com caraterísticas que os distingue dos vírus anteriores de forma a dificultarem o trabalho realizado pelos antivírus que são “obrigados” a acompanhar estas evoluções constantes.

3 Modelos Epidemiológicos de Transmissão de Vírus Informáticos

Tipicamente os vírus de computador simples consistem em pequenos programas criados com a finalidade de causar danos no computador infetado, podendo apagar dados, capturar informações privadas ou alterar o normal desempenho do sistema. Estes vírus, vêm preparados para ter um comportamento idêntico aos vírus biológicos, porque são desenvolvidos para enviar cópias de si mesmos, na tentativa de se espalharem para outros computadores.

Numa analogia em termos mais populares, os vírus informáticos são comparados aos vírus biológicos fazendo uma comparação dos computadores ao corpo humano, atribuindo uma visão mais humanizada ao computador como se tratasse de um corpo vulnerável a doenças virais. Segundo Sara Mota, "*nas últimas décadas, criaturas biológicas como os vírus ou as bactérias, parecem ter migrado dos seus habitats naturais para ecologias de silicone e eletricidade.*" [Mota, 2010].

Neste capítulo apresentam-se alguns modelos epidemiológicos de transmissão de vírus informáticos.

3.1 Modelo I

Xie Han e Qiolin Tan [Han and Tan, 2010] estudam um modelo de vírus de computador utilizando o modelo SIRS, para a transmissão de doenças infeciosas. Designa-se de Modelo I.

Neste artigo, alertam para os perigos e receios que os utilizadores sentem devido às consequências que os vírus informáticos podem provocar. São dados alguns exemplos de vírus informáticos que surgiram ao longo da história e quais as piores consequências que estes tiveram no quotidiano das pessoas que utilizam a rede de *internet*, enumerando alguns como o utilizador não poder enviar ou receber *email* ou ver o seu cartão de crédito ser usado para pagar por nada que não adquiriu.

Os autores revelam que um estudo realizado na China em 2007 sobre a taxa de infeção por vírus informáticos no país, revelou que se estima que a taxa de infeção seja superior a 90% [Goldberg et al., 1998].

3.1.1 Descrição do Modelo I

Assumindo que cada nó é indicado como um computador e o estado do computador saudável pode ser suscetível à infeção (S), os computadores infetados (I) que podem transmitir a doença a computadores saudáveis ou a computadores recuperados (R) que não podem ter a doença ou transmiti-la. Como resultado, o modelo apresentado pelos autores fica como se segue.

$$\begin{aligned} \frac{dS}{dt} &= (1-p)b - \mu S - \beta S(t-\tau_1)I(t-\tau_1) + \nu R(t-\tau_2) \\ \frac{dI}{dt} &= \beta S(t-\tau_1)I(t-\tau_1) - (\mu+\gamma+\alpha)I \\ \frac{dR}{dt} &= pb + \gamma I - \mu R - \nu R(t-\tau_2) \end{aligned} \qquad (1)$$

onde b é o número de computadores, p é a taxa de computadores imunes, β é a taxa de infeção de computadores infetados, μ é a taxa de mortalidade dos computadores, ν é a taxa de perda da imunidade dos computadores recuperados, γ é a taxa de computadores infetados recuperados e o α é a taxa de mortalidade devido a vírus. O τ_1 e τ_2 são respectivamente o período latente e temporário imunológico.

O modelo (1) necessita de ser analisado com as seguintes condições iniciais:

$$\begin{array}{ll} S(t) \geqslant 0, t \in [-\tau, 0], & S(0) > 0, \tau = \max\{\tau_1, \tau_2\} \\ I(t) \geqslant 0, t \in [-\tau_1, 0], & I(0) > 0 \\ R(t) \geqslant 0, t \in [-\tau_2, 0], & R(0) > 0 \end{array} \qquad (2)$$

Somando-se as três equações em (1) e denotar o número de população total por N, obtemos,

$$\frac{dN}{dt} = b - \mu N - \alpha I \qquad (3)$$

É fácil verificar que o cone positivo R_+^3 é positivamente invariante em respeito a (1) , onde $R_+^3 = \{(S, I, R) \in R^3 : S > 0, I > 0, R > 0\}$. Além disso, todas a soluções possíveis do sistema (1) são delimitadas e entram na região Λ, onde

$$\Lambda = \left\{(S, I, R) \in R^3 : S > 0, I > 0, R > 0, S + I + R \leqslant \frac{b}{\mu}\right\}.$$

O número de reprodução é dado por:

$$R_0 = \frac{\beta b[(1-p)\mu + \nu}{\mu(\mu+\nu)(\mu+\gamma+\alpha)}. \qquad (4)$$

Para o sistema (1), existe sempre o equilíbrio livre de doença $E_0 = \left(\frac{b[(1-p)\mu+\nu]}{\mu(\mu+\nu)}, 0, \frac{pb}{\mu+\nu}\right)$. Se $R_0 > 1$, também existe um equilíbrio endémico $E^* = (S^*, I^*, R^*)$, onde

$$S^* = \frac{\mu + \gamma + \alpha}{\beta}$$
$$I^* = \frac{\mu(\mu + \nu)(\mu + \gamma + \alpha)}{\beta[(\mu + \alpha)(\mu + \nu) + \mu\gamma]}(R_0 - 1)$$
$$R^* = \frac{pb + \gamma I^*}{\mu + \nu}$$

Equilibrio livre de doença:

Teorema

Se $R_0 \leqslant 1$, então a solução de (1), com respeito a Λ, satisfaz $\left(S(t), I(t), R(t)\right) \to \left(\frac{b[(1-p)\mu+\nu}{\mu(\mu+\nu)}\ 0, \frac{pb}{\mu+\nu}\right)$ como $t \to \infty$.

3.1.2 Simulações Numéricas do Modelo I

Nesta secção apresenta-se simulações numéricas do Modelo I. Na Figura 2 observa-se um comportamento dinâmico designado de equilíbrio endémico, em que a transmissão de vírus se faz de forma constante ao longo do tempo.

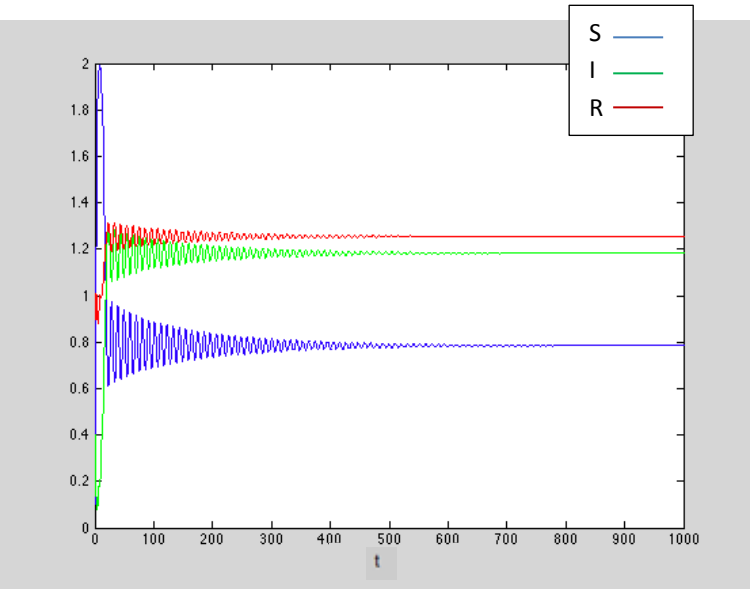

Figura 2 - Estado endémico estável do modelo I. Os parâmetros utilizados são: $p = 0.9$, $b = 1$, $\beta = 0.8$, $\mu = 0.3$, $\nu = 0.7$, $\gamma = 0.3$, $\alpha = 0.028$, $\tau_1 = 4$ e $\tau_2 = 2$. As condições iniciais são: $S(0) = 1.5$, $I(0) = 0.2$ e $R(0) = 0.5$.

Na Figura 3 verifica-se um comportamento dinâmico designado de órbita ou solução periódica, onde a propagação de vírus se realiza de forma periódica.

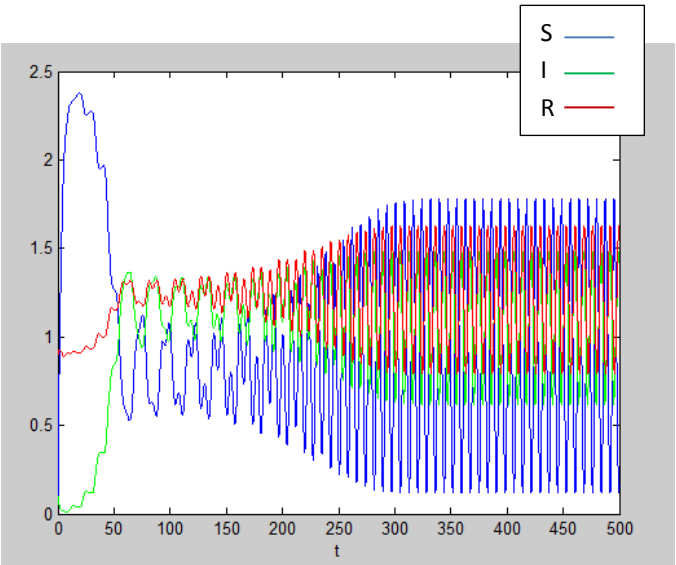

Figura 3 – Solução periódica estável do Modelo I. Os parâmetros utilizados são: $p = 0.9$, $b = 1$, $\beta = 0.8$, $\mu = 0.3$, $\nu = 0.7$, $\gamma = 0.3$, $\alpha = 0.028$, $\tau_1 = 10$ e $\tau_2 = 2$. As condições iniciais são: $S(0) = 0.1$, $I(0) = 0.1$ e $R(0) = 0.9$.

3.1.3 Conclusões do Modelo I

Os autores estudaram um modelo de vírus de computador, com períodos latentes e temporais imunes, baseado num modelo de epidemia. Descobriram que a dinâmica global é determinada pelo valor do número de reprodução R_0, pelo atraso no tempo. Mais especificamente, o equilíbrio livre de doença é globalmente assintoticamente estável se $R_0 < 1$. Os resultados numéricos mostram que o sistema tem uma solução periódica para determinados valores de τ_1, tempo de atraso.

Os autores concluem que uma boa estratégia para controlar e erradicar a transmissão de vírus é diminuir o valor do número de reprodução R_0.

3.2 Modelo II

Liping Feng, Xiaofeng Liao, Huaquing Li e Qi Han [Feng et al., 2011] apresentam um novo modelo de propagação de vírus de computador, com dois atrasos medidas antivírus multi-estados. Durante este estudo os autores utilizam teorias de estabilidade e de bifurcação de sistemas dinâmicos. Este modelo é doravante designado de Modelo II.

O desenvolvimento das redes de computadores, traduziu-se num aumento da sua interconectividade e interoperabilidade, aumentando a probabilidade dos vírus de

computadores se espalharem e causarem avolumados prejuízos para as organizações e clientes. A perda anual média, devido a infeções por vírus, segundo informações reunidas pelos autores, estima-se que seja superior a 0,2 milhões de dólares. Na China em 2009, a taxa de infeção por vírus chegou a 70,15% [Goldberg et al., 1998]. Estes fatores impulsionaram a necessidade de compreender de uma forma mais detalhada como os vírus de computador se propagam pelos sistemas.

3.2.1 Descrição do Modelo II

O estudo é baseado no modelo epidémico clássico de Kermack-McKendrick suscetível-infetado-recuperado (SIR) e foram considerados os três factos seguintes.

Alguns vírus passam por um período de latência antes de os anfitriões serem infetados;

Os utilizadores podem imunizar os seus anfitriões com medidas de precaução no estado S e no estado I;

Alguns anfitriões recuperados passam por uma imunidade temporária com probabilidade δ;

Estas medidas podem ser encaradas como estratégias antivírus multi-estados. Podem resultar nos caminhos de transição de estado seguintes:

S → R, utiliza medidas de precaução de imunização em tempo real;

I → R, vírus de limpeza após os anfitriões estarem infetados;

R→ S, uma parte dos hosts recuperados podem tornar-se suscetíveis novamente.

Como resultado dos parâmetros referidos anteriormente, o modelo SIRS fica formulados com as seguintes equações diferenciais com atraso:

$$\begin{cases} \frac{dS}{dt} = p\Lambda - \beta S(t-\tau_1)\, I(t-\tau_1) - (\mu + \Upsilon)\, S(t) + \delta R(t-\tau_2), \\ \frac{dI}{dt} = \beta S(t-\tau_1)\, I(t-\tau_1) - (\mu + \alpha) I(t), \\ \frac{dR}{dt} = (1-p)\Lambda + \gamma S(t) + \alpha I(t) - \delta R(t-\tau_2) - \mu R(t). \end{cases} \quad (1)$$

onde p é a proporção de novos *hosts* que são suscetíveis, os outros estão imunizados. E assim pertencem a classe R. Λ é o novo número de *hosts*, δ é a taxa de perda de imunidade dos

hosts recuperados, μ é a taxa de mortalidade dos *hosts*, β é a taxa constante de contato entre I e S, γ é a taxa de pré-imunidade devida aos antivírus, α é a taxa de *hosts* infetados recuperados, τ_1 e τ_2 é o período de latência e de imunidade, respetivamente. Os autores do estudo consideraram que os períodos de latência e imunidade temporária tem o mesmo valor.

O modelo proposto apresenta uma bifurcação *Hopf*, para variações dos períodos de latência e de imunidade (τ_2) , sendo estes considerados parâmetros de bifurcação. (faz-se $\tau_1 = \tau_2 = \tau$).

Os autores do estudo realizado para este modelo consideraram que a bifurcação *Hopf* do sistema é dado com atrasos tendo como parâmetros de bifurcação τ1, τ2 (τ1 = τ2 = τ).

3.2.2 Simulações Numéricas do Modelo II

Nesta secção apresenta-se simulações numéricas do Modelo II. Na Figura 4 observa-se um comportamento dinâmico designado de equilíbrio endémico, em que a transmissão de vírus se faz de forma constante ao longo do tempo.

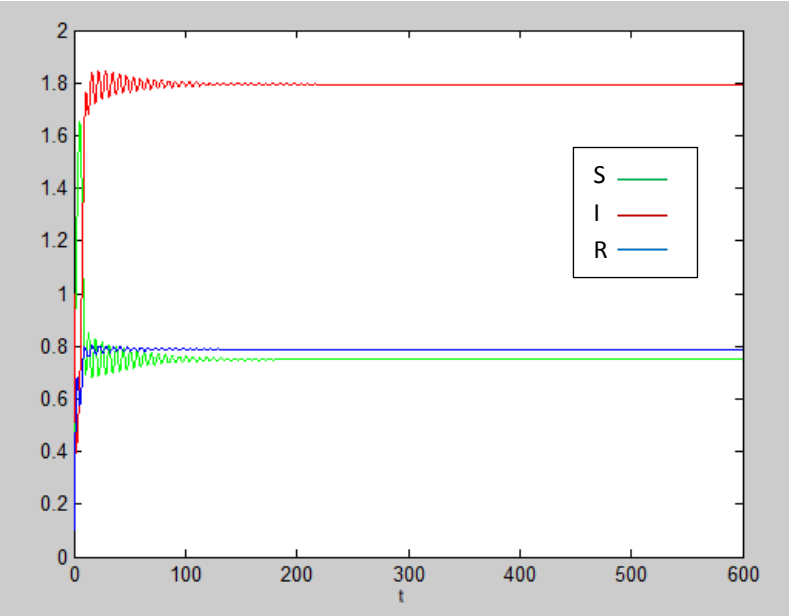

Figura 4 – Equilíbrio endémico do Modelo II. Os valores dos parâmetros usados são: $\Lambda = 1$, $\mu = 0.3$, $p = 0.9$, $\alpha = 0.3$, $\beta = 0.8$, $\gamma = 0.2$, $\delta = 0.7$ e $\tau_1 = 1.85$. As condições iniciais são: $S(0) = 0.1$, $I(0) = 1$ e $R(0) = 0.1$.

Na Figura 5 verifica-se um comportamento dinâmico designado de órbita ou solução periódica, onde a propagação de vírus se realiza de forma periódica.

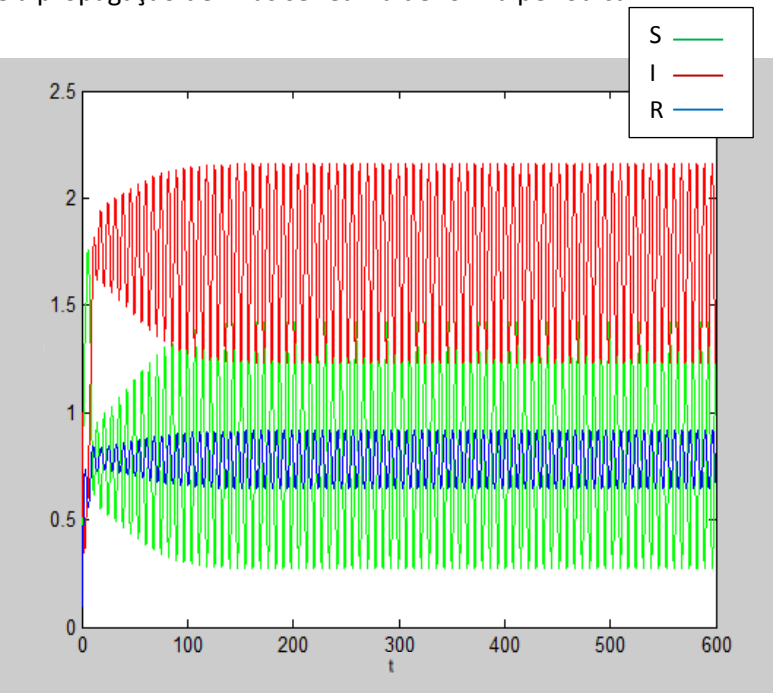

Figura 5 - Solução periódica estável do Modelo II. Os parâmetros utilizados são: $\Lambda = 1$, μ = 0.3, $p = 0.9$, $\alpha = 0.3$, $\beta = 0.8$, $\gamma = 0.2$, $\delta = 0.7$ e $\tau_1 = 2.2$. As condições iniciais são: $S(0) = 0.1$, $I(0) = 1$ e $R(0) = 0.1$.

3.2.3 Conclusões do Modelo II

Os autores propõem um modelo para a transmissão de vírus informáticos, usando dois tipos de atrasos e medidas antivírus multi-estados.

O modelo apresenta o fenómeno de bifurcação de *Hopf*, sendo o parâmetro de bifurcação os tempos de latência e de imunidade.

Os autores sugerem como estratégias de combate ao vírus o uso de estruturas topológicas de redes, entre outros.

3.3 Modelo III

Quingyi Zhu, Xiaofan Yang e Jianguo Ren [Zhu et al., 2012] propõem um modelo dinâmico para descrever a propagação de vírus no computador. Provam que (1) o equilíbrio livre de doença é globalmente assintoticamente estável se o número de reprodução R_0 for menor que um, demonstrando assim, neste caso, que o vírus acabaria por morrer e (2) o equilibrio endémico é globalmente assintoticamente estável, se o número de reprodução, R_0, for maior que um.

Os autores deste estudo observaram que os modelos anteriores, propostos para a transmissão de vírus, consideravam apenas a possibilidade de serem só os computadores a estarem expostos a uma infecção por vírus. Estes modelos ignoravam dispositivos externos, que podem ser igualmente contaminados, como por exemplo, Pen USB, discos externos entre outros. Na verdade a tendência é estes dispositivos externos serem atualmente um dos principais meios de propagação de vírus a par das redes de computadores. Desta forma, os autores consideraram que era importante estudarem a dinâmica de infeção da interação do computador com os dispositivos externos.

3.3.1 Descrição do Modelo III

O sistema de equações que descreve a dinâmica da transmissão de vírus informáticos é derivado da interacção entre os computadores e os dispositivos amovíveis. Neste modelo, todos os computadores presentes na rede estão divididos em três grupos: Suscetíveis (S), infeciosos (I) e recuperados (R). Quanto aos dispositivos removíveis são divididos em dois grupos: dispositivos suscetíveis (R_S) ou infeciosos (R_I).

No estudo, os autores criaram notações e hipóteses que tiveram que seguir.

Os autores para este modelo acrescentaram as seguintes anotações: $N(t)$ para o valor do número total de computadores presentes na rede no tempo t ($S(t) + I(t) + R(t) \equiv N(t)$), $R_N(t)$ para o número total de dispositivos removiveis no tempo t ($R_S(t) + R_I(t) \equiv R_N(t)$), o número de computadores e dispositivos removíveis recrutados estão representados respetivamente por λ_1 e λ_2, β_1 representa o contacto da força infeciosa entre computadores suscetíveis e infetantes, β_2 representa o contacto da força infeciosa entre computadores e dispositivos removíveis, as taxas de recuperação de computadores infeciosos e dispositivos removíveis, derivado ao efeito do software de antivírus estão identificadas respetivamente

por σ_1 e σ_2, μ_1 identifica a taxa dos computadores desligados da rede e o μ_2 representa o ritmo que os dispositivos removíveis avariam.

Os pressupostos que estiveram na base do Modelo III são: Na H1 são suscetiveis todos os computadores que sejam acedidos recentemente e todos os dispositivos externos, na H2 no tempo t, a força de infeção de computadores infeciosos para computadores suscetíveis é dada por $\beta_1 S(t)I(t)$, na H3, os dispositivos infeciosos têm a mesma capacidade infeciosa dos computadores infeciosos, o que implica que a capacidade de infeção de dispositivos infeciosos para computadores suscetíveis é dada por $\beta_2 S(t)\frac{R_I(t)}{R_N(t)}$, e a capacidade de infeção de computadores infeciosos para suspetíveis seja dada por $\beta_2 R_S(t)\frac{I(t)}{N(t)}$, na H4, a capacidade de recuperação dos dispositivos infeciosos é dada por $\sigma_2 R_1(t)\frac{R(t)}{N(t)}$ porque um dispositivo infecioso pode tornar-se suscetível se estiver ligado a um computadores recuperado e por fim a H5, o antivírus é suficientemente poderoso e eficaz para manter os computadores imunes a vírus.

Na Figura 6 representa-se o diagrama do Modelo III.

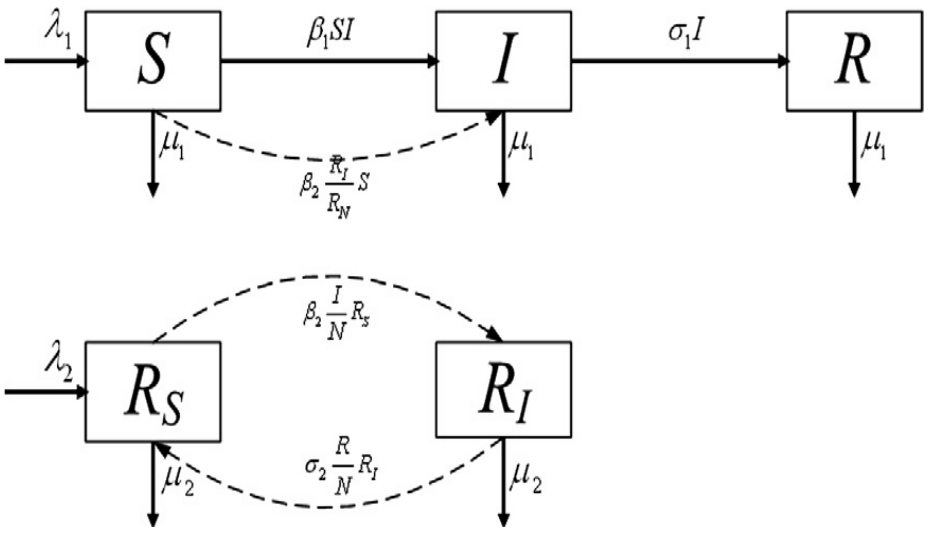

Figura 6 - Diagrama de transferência do Modelo III [Zhu et al., 2012].

O sistema de equações diferenciais para o Modelo III é:

$$\begin{cases} \dot{S} = \lambda_1 - \beta_1 SI - \beta_2 S\frac{R_I}{R_N} - \mu_1 S, \\ \dot{I} = \beta_1 SI + \beta_2 S\frac{R_I}{R_N} - (\mu_1 - \sigma_1), \\ \dot{R} = \sigma_1 I - \mu_1 R, \\ \dot{R}_S = \lambda_2 - \beta_2 R_S\frac{I}{N} + \sigma_2 R_I\frac{R}{N} - \mu_2 R_S, \\ \dot{R}_I = \beta_2 R_S\frac{I}{N} - \sigma_2 R_I\frac{R}{N} - \mu_2 R_I. \end{cases} \quad (1)$$

onde S, I, R, N, R_S, R_I e R_N são abreviações de $S(t)$, $I(t)$, $N(t)$, $R_S(t)$, $R_I(t)$ e $R_N(t)$, respetivamente. Do sistema anterior e do facto de $N = S + I + R$ e $R_N = R_S + R_I$, obtêm-se as equações para a variação de N e de R_N.

$$\begin{cases} \dot{N} = \lambda_1 - \mu_1 N, \\ \dot{R}_N = \lambda_2 - \mu_2 R_N. \end{cases} \quad (2)$$

3.3.2 Simulações Numéricas do Modelo III

Na Figura 7 observa-se um equilíbrio livre de doença para o número de computadores. Neste caso, o vírus acaba por desaparecer.

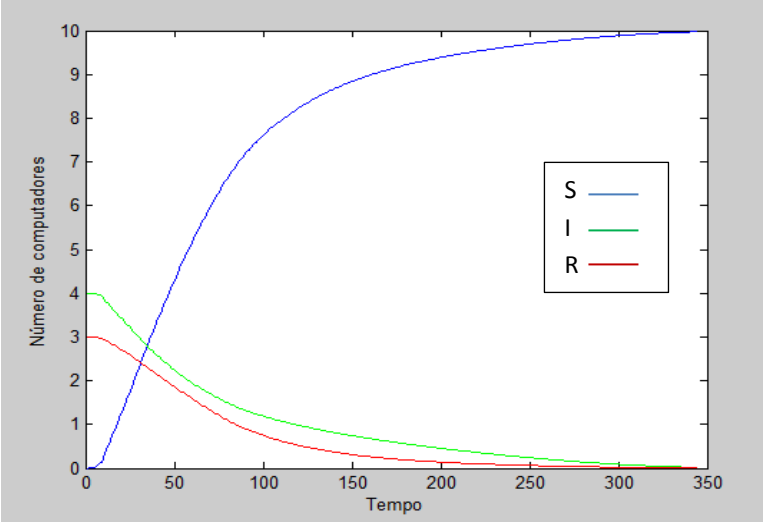

Figura 7 - Equilíbrio livre de doença do Modelo III para os computadores, para $R_0 < 1$. Os valores dos parâmetros usados são: $\lambda_1 = 1$, $\lambda_2 = 0.1$, $\beta_1 = 0.01$, $\beta_2 = 0.01$, $\mu_1 = 0.1$, $\mu_2 = 0.1$, $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $S(0) = 0$, $I(0) = 4$ e $R(0) = 3$.

Na Figura 8, verifica-se um equilíbrio livre de doença para o número de dispositivos externos. Também neste caso, o vírus acaba por desaparecer.

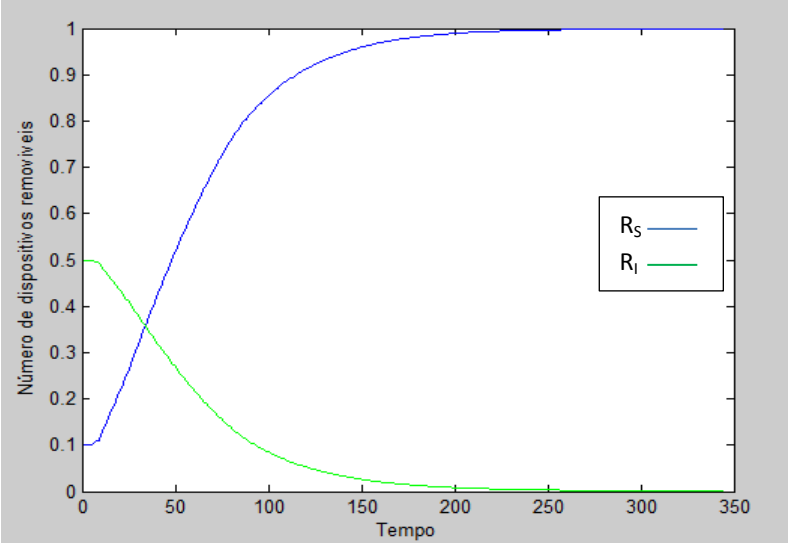

Figura 8 - Equilíbrio livre de doença do Modelo III para os dispositivos externos, para $R_0 < 1$. Os valores dos parâmetros usados são: $\lambda_1 = 1$, $\lambda_2 = 0.1$, $\beta_1 = 0.01$, $\beta_2 = 0.01$, $\mu_1 = 0.1$, $\mu_2 = 0.1$, $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $R_S(0) = 0.1$ e $R_I(0) = 0.5$.

Na Figura 9 observa-se um equilíbrio endémico para o número de computadores. Neste caso, o vírus acaba por estabilizar.

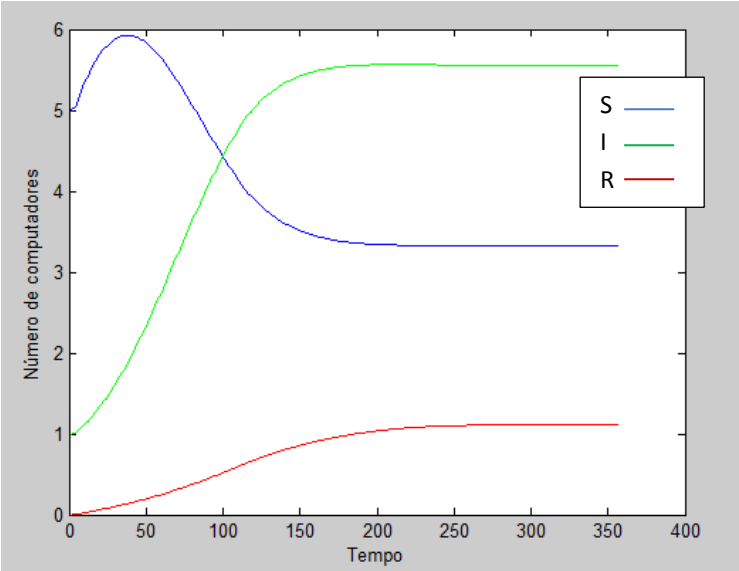

Figura 9 - Equilíbrio endémico do Modelo III para os computadores, para $R_0 > 1$. Os valores dos parâmetros usados são: $\lambda_1 = 1$, $\lambda_2 = 0.1$, $\beta_1 = 0.035$, $\beta_2 = 0.035$, $\mu_1 = 0.1$, $\mu_2 = 0.1$, $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $S(0) = 5$, $I(0) = 1$ e $R(0) = 0$.

Na Figura 10 observa-se um equilíbrio endémico para o número de dispositivos externos. Neste caso, o vírus também acaba por estabilizar.

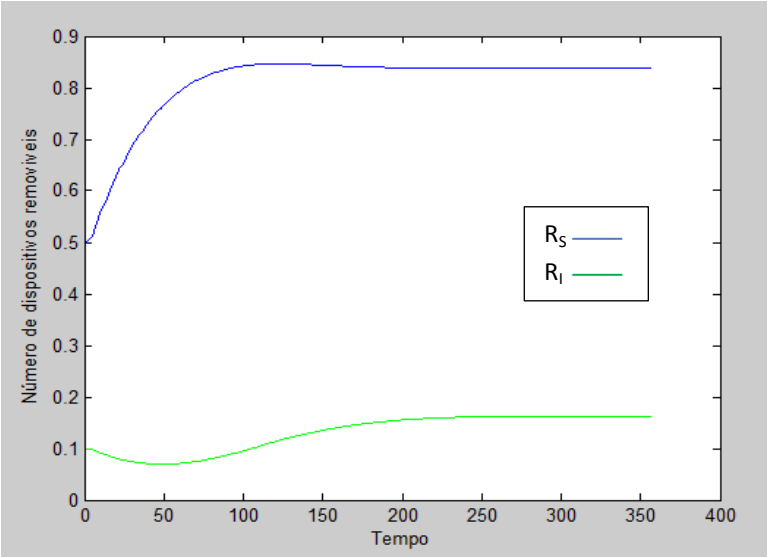

Figura 10 - Equilíbrio endémico do Modelo III para os dispositivos externos, para $R_0 > 1$. Os valores dos parâmetros usados são: $\lambda_1 = 1$, $\lambda_2 = 0.1$, $\beta_1 = 0.035$, $\beta_2 = 0.035$, $\mu_1 = 0.1$, $\mu_2 = 0.1$, $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $R_S(0) = 0.5$ e $R_I(0) = 0.1$.

3.3.3 Conclusões do Modelo III

Os autores deste estudo propuseram um modelo dinâmico para a propagação de vírus de computador e realizaram uma análise detalhada do mesmo, tendo em conta que através da reunião de vários estudos de outros autores, estes descobriram que existia uma possível falha por não considerarem a interação entre computadores e dispositivos removíveis externos.

O equilíbrio livre de infeção é globalmente assintoticamente estável se $R_0 < 1$ e o equilíbrio positivo é globalmente assintoticamente estável se o $R_0 > 1$. Através destes valores verifica-se que um meio eficaz para extinguir o vírus é encontrar as soluções para manter o R_0 num valor abaixo de 1.

Este modelo é apenas um ponto de partida para a compreensão da propagação de vírus de computador através das interações dos computadores com os dispositivos removíveis, apesar de se verificar que o padrão de interação realista entre eles seja muito mais complexo do que foi aqui abordado.

4 Simulações Numéricas

Neste capítulo estudam-se mais aprofundadamente os modelos epidemiológicos do capítulo anterior. Propõem-se uma alteração ao Modelo III, acrescentando um atraso, o que se traduz num novo sistema de equações diferenciais ordinárias com atraso. Neste e no Modelo I, variou-se a taxa de infeção do vírus, estudo ausente das publicações existentes na literatura. Esta variação proporcionou a observação de uma bifurcação de Hopf, que não estava relatada na literatura para estes modelos. No Modelo I, observa-se, para valores crescentes da taxa de infeção, o sistema passa de um equilíbrio endémico estável para uma órbita periódica estável. Deu-se, assim, um agravamento na propagação de vírus que passou a realizar-se de forma periódica. No Modelo III, observa-se que, para valores crescentes da taxa de infeção, o sistema passa de um estado de equilíbrio livre de doença (não há propagação de vírus) para uma solução periódica estável (há propagação periódica do vírus). Houve, novamente, um agravamento da dinâmica da propagação do vírus informático.

4.1 Modelo I

Neste modelo varia-se a taxa de infeção β, no intervalo [0.6, 0.9], neste caso.

Na Figura 11 observa-se e regista-se o comportamento dinâmico do modelo do sistema, um equilíbrio endémico, em que a transmissão de vírus se faz de forma constante ao longo do tempo, para $\beta = 0.6$.

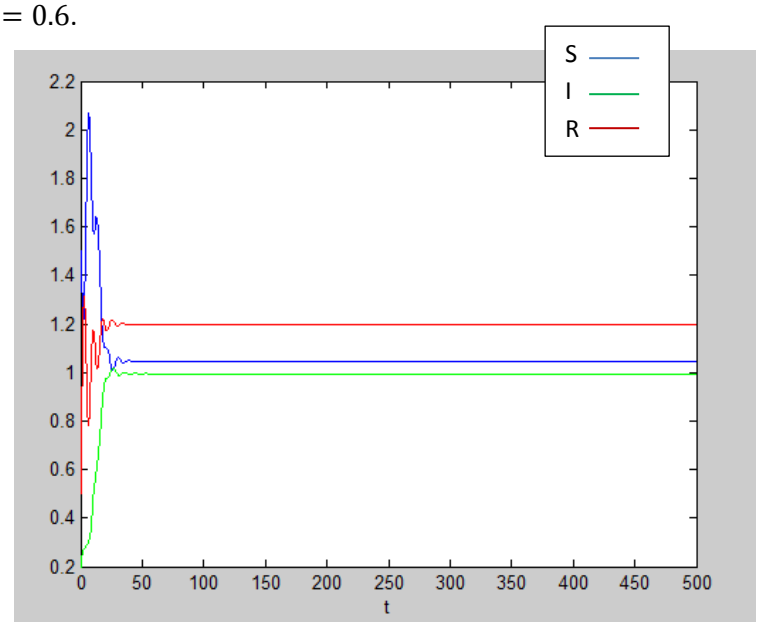

Figura 11 - Equilíbrio endémico estável do Modelo I para $\beta = 0.6$. Os parâmetros utilizados são: $p = 0.9$, $b = 1$, $\mu = 0.3$, $\nu = 0.7$, $\gamma = 0.3$, $\alpha = 0.028$, $\tau_1 = 4$ e $\tau_2 = 2$. As condições iniciais são: $S(0) = 1.5$, $I(0) = 0.2$ e $R(0) = 0.5$.

Na Figura 12 observa-se novamente um equilíbrio endémico estável, para $\beta = 0.83$.

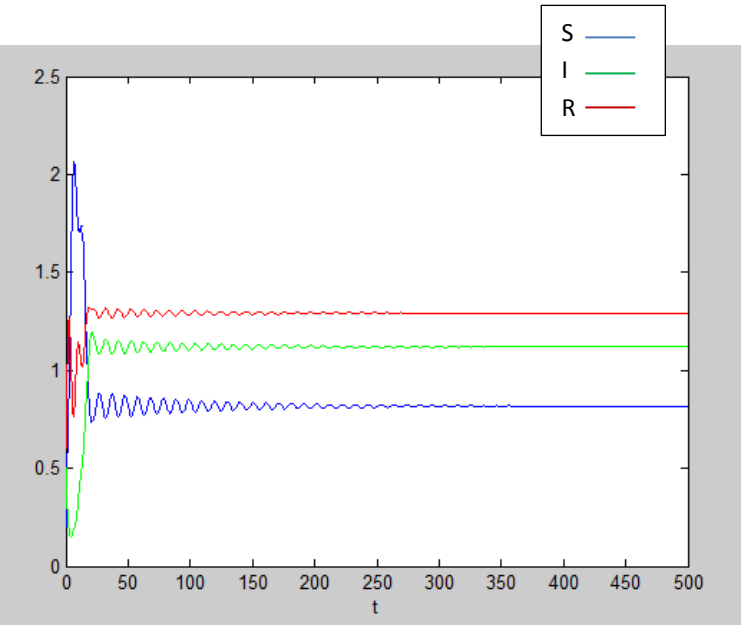

Figura 12 - Equilíbrio endémico estável do Modelo I para $\beta = 0.83$. Os parâmetros utilizados são: $p = 0.9$, $b = 1$, $\mu = 0.3$, $\nu = 0.7$, $\gamma = 0.3$, $\alpha = 0.028$, $\tau_1 = 4$ e $\tau_2 = 2$. As condições iniciais são: $S(0) = 1.5$, $I(0) = 0.2$ e $R(0) = 0.5$.

Na Figura 13 mostra uma alteração do comportamento dinâmico, pois este deixou de estar em equilíbrio endémico para passar a uma solução periódica estável, para $\beta = 0.85$. Neste caso, a propagação do vírus realiza-se de forma periódica.

Este comportamento do sistema não está descrito no artigo proposto por Han e Tan [Han and Tan, 2010], constituindo um complemento à análise aí efectuada.

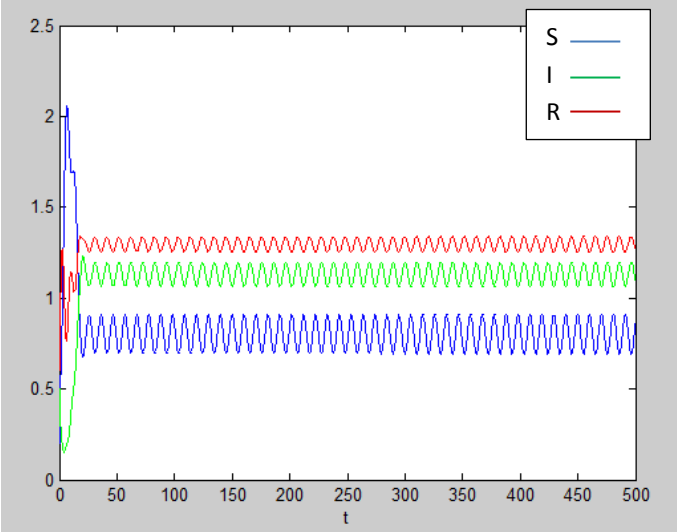

Figura 13 - Solução periódica estável do Modelo I para $\boldsymbol{\beta = 0.85}$. Os parâmetros utilizados são: $\boldsymbol{p = 0.9}$, $\boldsymbol{b = 1}$, $\boldsymbol{\mu = 0.3}$, $\boldsymbol{\nu = 0.7}$, $\boldsymbol{\gamma = 0.3}$, $\boldsymbol{\alpha = 0.028}$, $\boldsymbol{\tau_1 = 4}$ e $\boldsymbol{\tau_2 = 2}$. As condições iniciais são: $\boldsymbol{S(0) = 1.5}$, $\boldsymbol{I(0) = 0.2}$ e $\boldsymbol{R(0) = 0.5}$.

4.2 Modelo III Modificado

Nesta secção altera-se o Modelo III para incluir o período de latência τ_1, para além de variar-se a taxa de infeção β, no intervalo [0.01, 0.0825],

As equações do novo modelo são:

$$\begin{cases} \dot{S} = \lambda_1 - \beta_1 S(t-\tau_1)I(t-\tau_1) - \beta_2 S\frac{R_I}{R_N} - \mu_1 S, \\ \dot{I} = \beta_1 S(t-\tau_1)I(t-\tau_1) + \beta_2 S\frac{R_I}{R_N} - (\mu_1 - \sigma_1), \\ \dot{R} = \sigma_1 I - \mu_1 R, \\ \dot{R}_S = \lambda_2 - \beta_2 R_S\frac{I}{N} + \sigma_2 R_I\frac{R}{N} - \mu_2 R_S, \\ \dot{R}_I = \beta_2 R_S\frac{I}{N} - \sigma_2 R_I\frac{R}{N} - \mu_2 R_I. \end{cases} \quad (1)$$

$$\begin{cases} \dot{N} = \lambda_1 - \mu_1 N, \\ \dot{R}_N = \lambda_2 - \mu_2 R_N. \end{cases} \quad (2)$$

Na Figura 15 observa-se um equilibrio livre de doença para o número de computadores, para $\tau_1 = 4$.

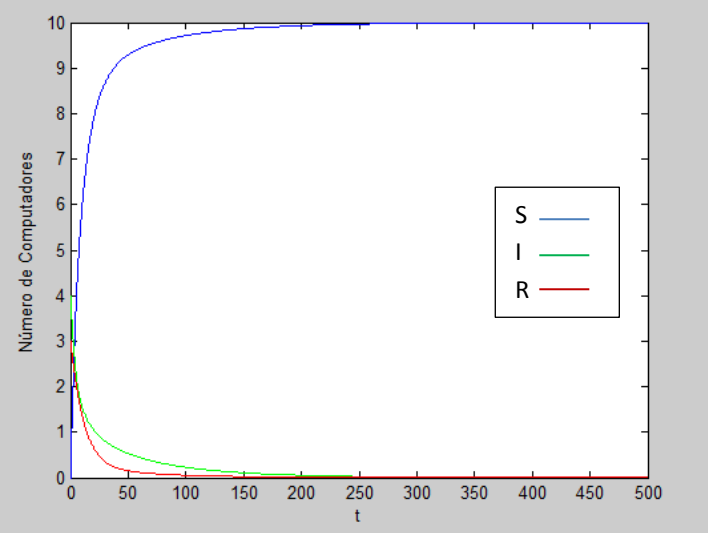

Figura 14 – Equilíbrio livre de doença do Modelo III para os computadores, para $\tau_1 = 4$. Os valores dos parâmetros usados são: $\lambda_1 = 1, \lambda_2 = 0.1, \beta_1 = 0.01, \beta_2 = 0.01, \mu_1 = 0.1, \mu_2 = 0.1,$ $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $S(0) = 0, I(0) = 4$ e $R(0) = 3$.

Na Figura 16 também observa-se um equilibrio livre de doença para o número de dispositívos externos, para $\tau_1 = 4$.

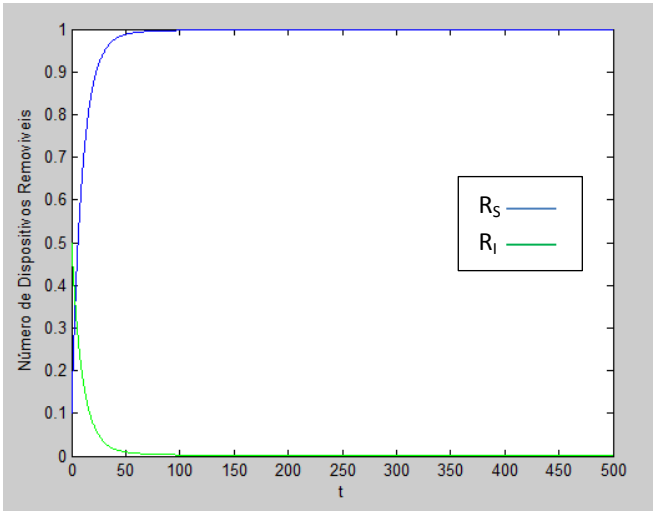

Figura 15 – Equilíbrio livre de doença do Modelo III para os dispositivos externos, no $\tau_1 = 4$. Os valores dos parâmetros usados são: $\lambda_1 = 1, \lambda_2 = 0.1, \beta_1 = 0.01, \beta_2 = 0.01, \mu_1 = 0.1, \mu_2 = 0.1,$ $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $R_S(0) = 0.1$ e $R_I(0) = 0.5$.

Na Figura 16 verifica-se uma alteração do comportamento dinâmico para os computadores, pois este deixou de estar em equilíbrio livre de doença para passar a uma solução periódica estável, para $\beta_1 = 0.0825$, $\beta_2 = 0.0825$ e $\tau_1 = 4$. Neste caso, a propagação do vírus passa a realiza-se de forma periódica.

Este comportamento do sistema não está descrito no artigo proposto por Zhu, Yang e Ren [Zhu et al., 2012], integrando um complemento à análise aí efetuada.

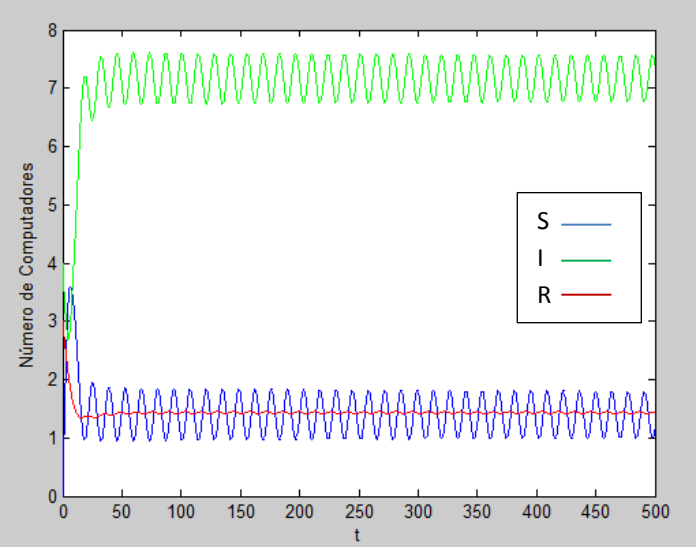

Figura 16 - Solução periódica estável do Modelo III para os computadores, para $\beta_1 = 0.0825$, $\beta_2 = 0.0825$ e $\tau_1 = 4$. Os valores dos parâmetros usados são: $\lambda_1 = 1$, $\lambda_2 = 0.1$, $\mu_1 = 0.1$, $\mu_2 = 0.1$, $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $S(0) = 0$, $I(0) = 4$ e $R(0) = 3$.

Na Figura 17 verifica-se também, uma alteração do comportamento dinâmico para os dispositivos externos, pois este deixou de estar em equilíbrio livre de doença para passar a uma solução periódica estável, para $\beta_1 = 0.0825$, $\beta_2 = 0.0825$ e $\tau_1 = 4$. Neste caso, tal como para os computadores, a propagação do vírus passa a realizar-se de forma periódica.

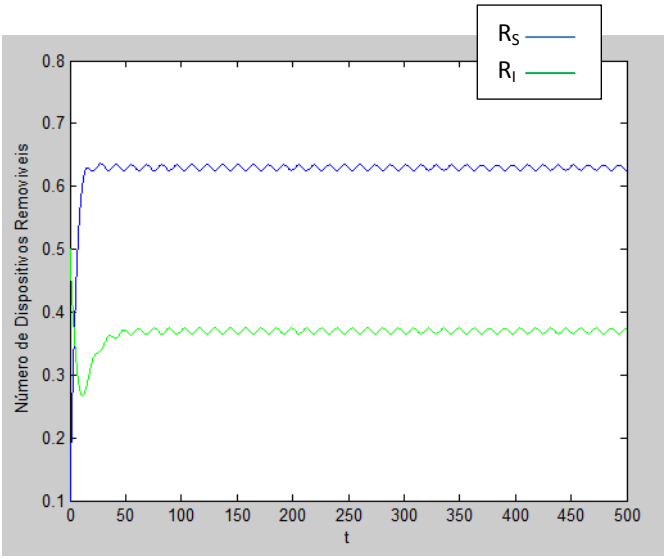

Figura 17 - Solução periódica estável do Modelo III para os dispositívos removíveis, para $\beta_1 = 0.0825$, $\beta_2 = 0.0825$ e $\tau_1 = 4$. Os valores dos parâmetros usados são: $\lambda_1 = 1$, $\lambda_2 = 0.1$, $\mu_1 = 0.1$, $\mu_2 = 0.1$, $\sigma_1 = 0.02$ e $\sigma_2 = 0.005$. As condições iniciais são: $R_S(0) = 0.1$ e $R_I(0) = 0.5$.

5 Conclusões

Neste trabalho estudam-se modelos de transmissão de vírus informáticos, baseados em modelos biológicos.

Começa-se por apresentar o estado da arte dos modelos conhecidos para a propagação de vírus informáticos. De seguida escolhem-se três modelos exemplificativos da generalidade de literatura sobre vírus informáticos. Descrevem-se os pontos fortes e os pontos fracos desdes modelos. Fazem-se simulações numéricas, no Matlab, complementares do Modelo I, variando-se a taxa de infeção, não explorada na literatura. Para valores crescentes dessa taxa, o sistema passa de um equilíbrio endémico estável para uma órbita periódica estável. Deu-se, assim, um agravamento na propagação de vírus que passou a realizar-se de forma periódica. Faz-se ainda uma alteração, não existente na literatura, ao Modelo III, acrescentando-se o período de latência, τ_1. O novo sistema passou a ser um sistema de equações diferenciais ordinárias com atraso. Estuda-se este novo modelo numericamente no Matlab. Observa-se que, para valores crescentes da taxa de infeção, o sistema passa de um estado de equilíbrio livre de doença (não há propagação de vírus) para uma solução periódica estável (há propagação periódica do vírus). Dá-se um agravamento na propagação do vírus que passa a efetuar-se de forma periódica.

Concluí-se assim que, para controlar ou erradicar a transmissão de vírus informáticos, se deve insistir na diminuição do valor da taxa de infecção.

Como trabalho futuro, pretende-se recriar, num ambiente controlado, a propagação de um vírus informático, criado para esse efeito. Posteriormente estudar-se-á os dados resultantes desta experiência, considerando especificamente o tempo de infeção e os danos causados no sistema.

Referências

[Anthes, G., 2002] Anthes, G., Experts Warn of a New Wave of Viruses, http://www.pcworld.com/article/92123/article.html, 2002 [último acesso: 16 Junho 2013]

[Beattie, A., 2012] Beattie, A. The Most Devastating Computer Viruses, http://www.techopedia.com/2/26178/security/the-most-devastating-computer-viruses, 2012 [último acesso: 4 Julho 2013]

[Blyuss and Kyrychko, 2010] Blyrychko, K. B., Kyrychko, Y. N. Stability and bifurcations in an epidemic model with varying immunity period. Bulletin of Mathematical Biology 72, p. 490-505, 2010.

[Cohen, 1984] Cohen, F. Computer Viruses – Theory and Experiments, 1984.

[Cohen, 1986] Cohen, F. Computer Viruses: Theory and Experiments. Computers and Security 6, p. 22-35,1986.

[Colares, 2002] Colares, R. G. Cybercrimes: os crimes na era da informática, 2002.

[ComputerWorld, 2012] ComputerWorld. Vírus informáticos podem saltar para o mundo biológico, http://www.computerworld.com.pt/2012/03/20/virus-informaticos-podem-saltar-para-o-mundo-biologico/, 2012 [último acesso: 4 Julho 2013]

[De et al, 2009] De, P., Liu, Y., Das, S. An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks. IEEE Transactions on Mobile Computing 8, p. 413-425, 2009.

[Falliere, N., 2011] Falliere, N. Sality: Story of a Peer-to-Peer Viral Network, Symantec, Security Response, 2012.

[Feng et al, 2012] Feng, L., Liau, X., Li, H., Han, Q. Hpf bifurcation analysis of a delayed viral infection model in a computer networks. Mathematical and Computer Modeling 56, p. 167-179, 2012.

[Festa, P. and Wilcox, J., 2013] Festa, P. and Wilcox, J., Experts estimate damages in the billions for bug, http://news.cnet.com/Experts-estimate-damages-in-the-billions-for-bug/2100-1001_3-240112.html, 2000 [último acesso: 16 Junho 2013]

[Forest, N., 2013] Forest, N. The Concept Virus, http://www.chebucto.ns.ca/~af380/ConceptMacro.html, 2013 [último acesso: 3 Junho 2013]

[F-Secure, 2013a] F-Secure. Dark Avenger, http://www.f-secure.com/v-descs/eddie.shtml, 2013 [último acesso: 4 Julho 2013]

[F-Secure, 2013b] F-Secure. Trojan:W32/Waledac.A, http://www.f-secure.com/v-descs/trojan_w32_waledac_a.shtml, 2013 [último acesso: 4 Julho 2013]

[F-Secure, 2013c] F-Secure. Virus:DOS/CIH, http://www.f-secure.com/v-descs/eddie.shtml, 2013 [último acesso: 4 Julho 2013]

[F-Secure, 2013d] F-Secure. Worm:W32/Mydoom, http://www.f-secure.com/v-descs/novarg.shtml, 2013 [último acesso: 4 Julho 2013]

[Garreto et al, 2003] Garetto, M., Gong, W.B., Towsley, D., Modeling malware spreading dynamics. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, p. 1869-1879, 2003.

[Gaspar, 2007] Gaspar, P., Pragas eletrônicas: ainda não estamos livres delas, 2007.
[Goldberg et al, 1998] Goldberg, L., Goldberg, P., Phillips, C., Sorkin, G., Constructing computer virus phylogenies. Journal of Algorithms 26, p. 188-208, 1998.
[Han and Tan, 2010] Han, X., Tan, Q., Dynamical behavior of computer virus on Internet, 2010.
[Helmreich, 2000] Helmreich, S. Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism. Science, Technology & Human Values, Vol. 25 (4), 2000.
[Huang et al, 2010] Huang, G., Takeuchi, Y., Ma, W.B., Wei, D.J., Global stability for delay SIR and SEIR epidemic models with nonlinear incidence rate. Bulletin of Mathematical Biology 72, p. 1192–1207, 2010.
[Hypponen, M., 2002] Hypponen, M. SWF.LFM.926, http://www.f-secure.com/v-descs/swflfm.shtml, 2002 [último acesso: 4 Julho 2013]
[Janssen, C., 2013] Janssen, C. Chernobyl Virus http://www.techopedia.com/definition/15796/chernobyl-virus, 2013 [último acesso: 4 Julho 2013]
[Kephart and White, 1991] Kephart, J., White, S., Directed-graph epidemiological models of computer viruses, 1991.
[Kephart and White, 1993] Kephart, J., White, S., Measuring and modeling computer virus prevalence. IEEE Symposium on Security and Privacy, p. 2-15, 1993.
[Li et al, 2011] Li, J.Q., Wang, Y.L., Yang, Y.L., Dynamical behaviors of an HBV infection model with logistic hepatocyte growth. Mathematical and Computer Modelling 5, p. 704-711, 2011.
[Li et al, 2009] Li, X.Z., Li, W.S., Ghosh, M., Stability and bifurcation of an SIS epidemic model with treatment. Chaos, Solitons and Fractals 42, p. 2822-2832, 2009.
[MalwareWiki, 2013] MalwareWiki. Vienna, http://malware.wikia.com/wiki/Vienna, 2013 [último acesso: 4 Julho 2013]
[McAfee, 2013a] McAfee. Vienna, http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=1337, 2013 [último acesso: 4 Julho 2013]
[McAfee, 2013b] McAfee, Virus Profile: ZeroAccess, http://home.mcafee.com/virusinfo/VirusProfile.aspx?key=579309, 2013 [último acesso: 4 Julho 2013]
[Microsoft, 2013] Microsoft. Trojan:Win32/Waledac, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan%3AWin32%2FWaledac , 2013 [último acesso: 4 Julho 2013]
[Mentor, 1986] Mentor, T. The Conscience of a Hacker, http://www.phrack.org/issues.html?issue=7&id=3&mode=txt, 1986 [último acesso: 3 Junho 2013]
[Moreno et al, 2002] Moreno, Y., Pastor-Satorras, R., Vespignani, A. Epidemic outbreaks in complex heterogeneous networks. European Physical Journal B 26, p. 521-529, 2002.
[Mota, 2010] Mota, S.P. Concepções Imunológicas na Era Virtual, 2010.
[Nachenberg, 1997] Nachenberg, C. Computer virus-antivirus coevolution, 1997.
[Nóbrega, J., 2009] Nóbrega, J. Vandalismo lidera motivações dos hackers, http://www.computerworld.com.pt/2009/03/25/vandalismo-lidera-motivaes-dos-hackers/, 2009 [último acesso: 4 Julho 2013]
[Oliveira and Oliveira, 2005] Oliveira, H., Oliveira, L. Pirataria Informática - A cópia e o Download ilegal, 2005.
[RecoveryLabs, 2004] RecoveryLabs. Vírus MyDoom, http://www.recoverylabs.pt/relatorios/Mydoom.pdf, 2004 [último acesso: 4 Julho 2013]

[Reuters, 2001] Reuters. Vírus Nimda se espalha pelo mundo, http://www.viaseg.com.br/noticia/382-virus_nimda_se_espalha_pelo_mundo.html, 2001 [último acesso: 16 Junho 2013]

[Rogers, 2003] Rogers, M. A New Hacker Taxonomy, 2003.

[Rogers, 2006] Rogers, M.K. A two-dimensional circumplex approach to the development of a hacker taxonomy, 2006.

[Rohr, 2011] Rohr, A. Primeiro vírus de PCs, 'Brain' completa 25 anos, http://g1.globo.com/tecnologia/noticia/2011/01/primeiro-virus-de-pcs-brain-completa-25-anos.html, 2011 [último acesso: 3 Junho 2013]

[Santos and Barros, 2005] Santos, A., Barros, O.O funcionamento interno dos softwares antivírus, 2005.

[Schell, B. and Martin, C., 2010] Schell, B. and Martin, C. Michelangelo virus - technical definition, http://computer.yourdictionary.com/michelangelo-virus, 2010 [último acesso: 3 Junho 2013]

[Schmudlach, M., 2004] Schmudlach, M. Spyware, viruses, & security forum: MP3Concept (trojan), http://forums.cnet.com/7723-6132_102-19126/mp3concept-trojan/, 2004 [último acesso: 4 Julho 2013]

[Shearer, J., 2011] Shearer, J. Trojan.Zeroaccess, http://www.symantec.com/security_response/writeup.jsp?docid=2011-071314-0410-99, 2011 [último acesso: 4 Julho 2013]

[Simões, 2010] Simões, I. Paradigmas da codificação dos vírus de computador – uma análise das estruturas arquiteturais internas, 2010.

[Song, 2011] Song, X., Wang, S., Dong, J. Stability properties and Hopf bifurcation of a delayed viral infection model with lytic immune response. Journal of Mathematical Analysis and Applications 373, p. 345-355, 2011.

[Sophos, 2002] Sophos. SWF/LFM-926, https://secure2.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/SWF~LFM-926/detailed-analysis.aspx, 2002 [último acesso: 4 Julho 2013]

[Standler, R., 2002] Standler, R. Examples of Malicious Computer Programs, http://www.rbs2.com/cvirus.htm#anchor111550, 2002 [último acesso: 3 Junho 2013]

[Strickland, J., 2013] Strickland, J. Os 10 piores vírus de computador de todos os tempos, http://informatica.hsw.uol.com.br/piores-virus-computador1.htm, 2013 [último acesso: 4 Julho 2013]

[Strickland, J., 2004] Strickland, J. Vírus MyDoom, http://informatica.hsw.uol.com.br/piores-virus-computador7.htm, 2004 [último acesso: 4 Julho 2013]

[Subramanya, 2001] Subramanya, S.R. Computer viroses, 2001.

[Symantec, 2013] Symantec. Assinatura de vírus, http://www.mediamarkt.pt/mp/article/Assinatura-de-v%C3%ADrus,933014.html, 2013 [último acesso: 4 Julho 2013]

[Symantec, 2007] Symantec. MP3Concept, http://www.symantec.com/security_response/writeup.jsp?docid=2004-040915-1449-99, 2007 [último acesso: 4 Julho 2013]

[Toor, 2011] Toor, A. The Brains Behind 'Brain' World's First PC Virus, http://www.switched.com/2011/03/14/pc-brain-virus-tracked-down-mikko-hypponen/, 2011 [último acesso: 3 Junho 2013]

[Wikimedia, 2010] Wikimedia. MP3Concept, http://en.academic.ru/dic.nsf/enwiki/5272650, 2010 [último acesso: 4 Julho 2013]

[Vianna, 2003] Vianna, T.L. HACKERS: um estudo criminológico da subcultura cyberpunk, 2003.

[Vianna, 2005] Vianna, T.L. Dos Crimes por Computador, 2005.

[Zou et al, 2002] Zou, C., Gong, W., Towsley, D. Code red worm propagation modeling and analysis, CCS'02, p. 18-22, 2002.

[Zou et al, 2005] Zou, C., Gong, W., Towsley, D., Gao, L. The monitoring and early detection of internet worms, 2005.

[Zou et al, 2006] Zou, C., Towsley, D., Gong, W. On the performance of Internet worm scanning strategies. Performance Evaluation 63, p.700–723, 2006.

[Zhu et al., 2012] Zhu, Q., Yang, X., Ren, J. Modeling and analysis of the spread of computer virus. Commun Nonlinear Sci Numer Simulat 17, p. 5117-5124, 2012.