5º CONGRESSO BRASILEIRO DE PESQUISA E DESENVOLVIMENTO EM PETRÓLEO E GÁS

TÍTULO DO TRABALHO:

Modelos Matemáticos para Ações Preventivas em Redes de Computadores da ANP

AUTORES:

Felipe Barbosa Cesar

INSTITUIÇÃO:

Escola Politécnica da Universidade de São Paulo

Abstract

Currently, computer systems and digital networks are the primary tools used in engineering planning, design, operation and control of all aspects of construction, transportation, machinery, maintenance and lifetime of devices. Consequently, computer viruses have become one of the most important sources of uncertainty, contributing to reduce the reliability of the systems activities. In addition, some viruses are able to acquire vital information, such as logins and passwords, which pose a major threat both to users of such systems for large corporations that manage them.

The aim of this work is to study possibilities for improvement in the struggle against computer viruses using the number of infections knowledge about one type of virus on the network and behavioral dynamics that it may have in this local network. In this case the specific network studied is from ANP. Some network manage actions are suggested and tested to improve the efficiency in the fight against virus spread.

Keywords: computer security, computer virus, mathematical modeling

Introdução

Há algumas décadas surgiram os vírus de computador, programas de códigos simples com o objetivo de prejudicar o bom funcionamento de uma máquina. No entanto, não havia grande número de vírus, eles causavam pequenos danos às máquinas e, além disso, sua propagação era muito lenta.

Com o passar dos anos, o desenvolvimento acelerado da tecnologia, tanto de softwares como de hardware, o surgimento e popularização da internet e a grande variedade de equipamentos que utilizam softwares e redes, os vírus se tornaram uma grande ameaça. Atualmente, esses programas possuem um código mais complexo, são capazes de produzir mutações de si próprios, dificultando sua detecção e remoção por programas de proteção contra vírus, seus objetivos vão muito mais além do que simplesmente danificar uma máquina. São capazes de adquirir dados pessoais de usuários de redes, como dados de conta bancária, e causar prejuízos milionários em grandes corporações.

Tendo em vista essas grandes preocupações, é importante entendermos melhor o funcionamento e a dinâmica de propagação de um vírus de computador. Para que haja segurança nos novos meios de comunicação é importante que sejamos capazes de reconhecer e combater de forma mais rápida e eficaz os vários tipos de vírus.

Esse trabalho tem como principal objetivo sugerir comportamentos que os gerenciadores de rede poderiam ter para melhorar a eficácia do combate a propagação de certos tipos de vírus em redes com topologias conhecidas.

Metodologia

Coleta de Dados

A coleta de dados foi realizada mediante entrevista com um gestor de redes da ANP e um estudo de casos foi gerado e está demonstrado nos resultados deste trabalho.

Modelos Epidemiológicos

Uma abordagem muito comum atualmente no estudo da dinâmica de propagação de vírus de computador é o uso de técnicas de modelagem de epidemiologia de vírus reais. Os motivos para o grande uso dessas técnicas estão enumerados em seguida:

- Tanto vírus reais quanto os de computador possuem códigos simples, genético ou computacional.
- Ambos necessitam de um hospedeiro para existirem.
- Ambos possuem grande poder de propagação para outros futuros infectados e mutação do código, o que dificulta a observação de um método eficiente de combate a essas ameaças.

A seguir, está uma descrição sucinta de um dos métodos que mais têm sido utilizados como base para os estudos recentes realizados nessa área.

Modelo SIR

Em 1927, W.O.Kermach e A.G.McKendric propuseram um modelo epidemiológico para estudar a disseminação de uma doença numa população.

Atualmente, esse modelo e inúmeras variações têm sido empregados, por exemplo, para se estimar o nível de vacinação necessário para erradicar uma doença contagiosa, como sarampo ou a poliomielite.

Nesse modelo, divide-se a população em três grupos: o grupo dos susceptíveis S, composto por indivíduos que podem contrair a doença através de contatos com os infectados; o grupo dos infectados, formado pelos indivíduos que já possuem a doença e são capazes de transmiti-la; e o grupo dos removidos R, que já possuíram a doença e não são mais nem susceptíveis nem infectados, de modo que eles morreram ou se recuperaram adquirindo imunidade. Esse modelo foi modificado em trabalhos posteriores que considera um grupo a mais no modelo, o grupo de “antidotais”, que se trata de indivíduos imunes de forma temporária ou permanente.

Simulações de Redes

Neste trabalho foi implementada a simulação da propagação de vírus em redes de diversas topologias. Para a simulação de uma rede local alguma das três principais topologias estrela, anel,

barramento ou uma combinação entre essas podem ser geradas. As simulações foram feitas com o uso da ferramenta MATLAB.

Três níveis de gerenciamento foram sugeridos e testados.

Gerenciamento nível I

Trata-se do gerenciamento que já é realizado atualmente nas redes em geral, principalmente em redes corporativas, em que cada host está equipado com programas antivírus e são realizadas varreduras periódicas assim como levantamento de dados por parte dos gestores da rede.

Gerenciamento nível II

Trata-se da tentativa de implementação física do modelo Kill-Signal, uma adaptação do modelo SIR. Nesse caso, a partir de certo nível de infecção da rede os hosts que detectarem malwares enviarão sinais para seus vizinhos realizarem varreduras, além das varreduras periódicas já realizadas.

Gerenciamento nível III

Atitude mais ostensiva no combate ao vírus. Quando um vírus reconhecidamente letal for detectado na rede, ou quando grande de hosts estiverem infectados com variados tipos de vírus, caracterizando uma epidemia, toda a rede será desconectada e serão realizadas varreduras em todos os hosts. Essa medida visa à erradicação imediata dos malwares.

Cada simulação corresponde a cem intervalos de tempo. As simulações foram realizadas cinqüenta vezes para cada nível de gerenciamento e gráficos mostrando os valores máximos, mínimos e médios de cada simulação, referentes a cada intervalo de tempo, foram feitos e estão expostos no próximo tópico.

Resultados e Discussão

Foram realizadas algumas perguntas para um gestor de redes da ANP com o objetivo de traçar o perfil de uma rede desse tipo e de checar a viabilidade de implementação das ações sugeridas neste trabalho. As informações mais relevantes estão apresentadas abaixo.

Estrutura Física

A rede possui aproximadamente 1500 equipamentos entre microcomputadores, notebooks e servidores distribuídos em 27 sub-redes. A rede é conectada internamente por redes LAN e WAN e conectada com o mundo externo por uma rede DMZ. As informações sobre as topologias específicas são sigilosas.

Solução de Segurança

A rede possui implantada uma solução específica, do fabricante McAfee, para controle e proteção contra códigos maliciosos. Os dados e informações de controle sobre os agentes do antivírus instalado em todo o ambiente computacional, bem como as incidências de códigos maliciosos no ambiente, são registrados e tratados de forma automática no sistema e no banco de dados desta solução. Esta ferramenta, bem como a situação do ambiente, é monitorada continuamente pela equipe técnica do Núcleo de Informática, principalmente no que diz respeito à atualização de vacinas e a picos de incidência em determinados ativos que requerem uma atuação imediata da equipe de Service Desk, para identificar as causas da incidência e evitar a proliferação da infecção.

São gerados ainda relatórios quinzenais sobre a incidência de códigos maliciosos em todo o ambiente computacional, separados por nome de equipamento e usuários.

Foram também habilitados alertas automáticos para notificar a equipe sempre que for identificado um grande número de incidências de códigos maliciosos em curto intervalo de tempo, para que sejam tratados pontualmente. Nestes casos, a equipe do Núcleo de Informática realiza uma atuação direta junto ao usuário e ao equipamento no intuito de identificar as causas da incidência (acesso a sites, mídias infectadas, spam recebido) possibilitando assim tanto a resolução pontual do problema, como a identificação de outras medidas de controle ou melhoria (filtro de spam, filtro de conteúdo web) para todo o ambiente computacional, além de aproveitar a oportunidade para conscientizar os usuários sobre boas práticas de segurança a serem adotadas.

Situações Críticas

Em um único dia já foram detectadas mais de 30.000 infecções. No entanto, o fator mais relevante quando se trata de um pico de infecção é um grande aumento do número de incidências em um curto espaço de tempo. Outra situação crítica ocorre quando algum código malicioso é detectado, mas não pode ser excluído.

Outras Informações Relevantes

Algumas vezes são observadas concentrações de infecção em uma sub-rede, embora isso não configure um padrão, essa característica poderia tornar o gerenciamento nível II muito eficiente, principalmente se as sub-redes tiverem topologia em barramento.

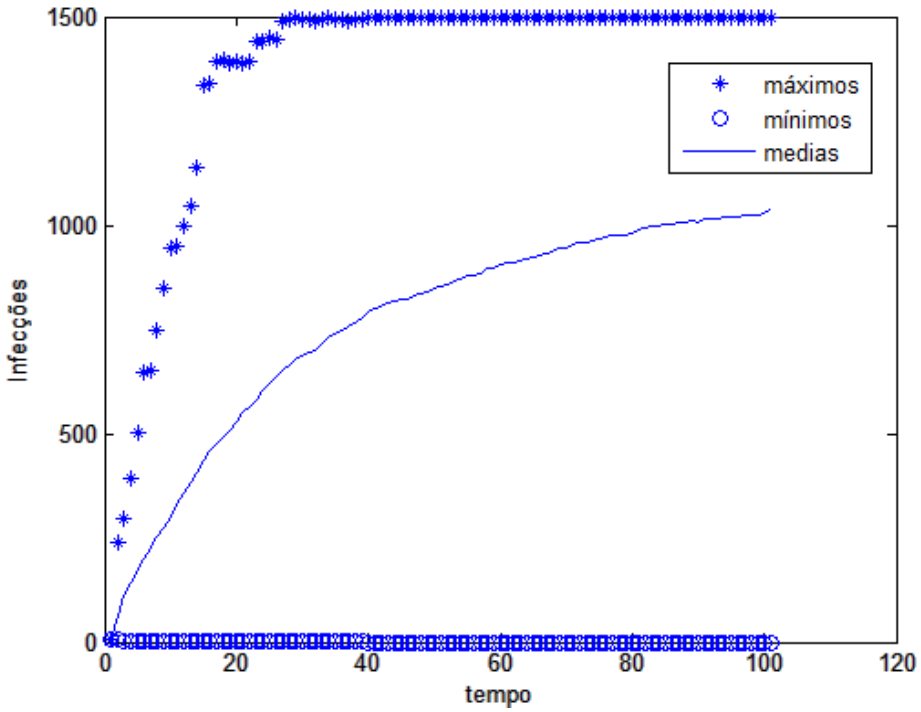
Já ocorreram situações em que a rede interna teve que ser desconectada da rede externa devido a infecções, esse fato, se acompanhado de varreduras nos micros da rede, configura um gerenciamento nível III, embora não automatizado.

Em seguida, estão mostrados alguns valores de um dos relatórios quinzenais que são gerados. Nessa quinzena foram detectadas, no total, em torno de 4800 infecções, um valor considerado baixo pelo gestor da rede.

Ameaças	Infecções Detectadas
W32/Conficker.worm!job	1,625
W32/Conficker.worm	1,603
W32/Sality.gen	557
Generic.dx!op	188
Artemis!3DB86DE852FB	53

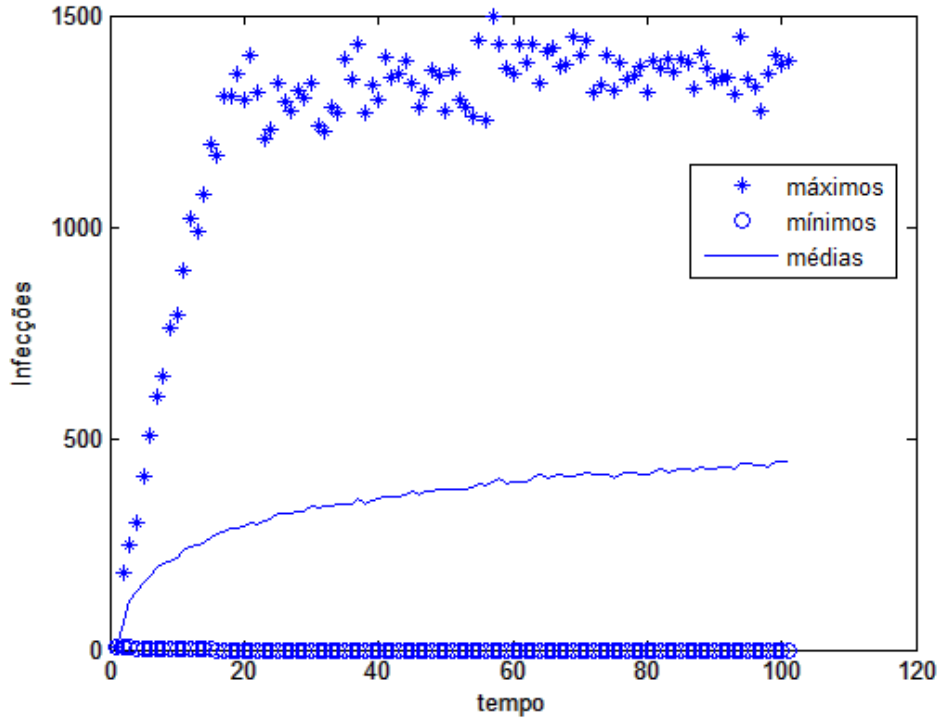
Uma rede virtual foi gerada para a realização de simulações dessa rede corporativa. Essa rede virtual é composta de 50 sub-redes com topologia em barramento, contendo 30 nós cada, e com servidores interligados em anel.

As simulações realizadas possuem vírus com baixo potencial de execução e baixo reconhecimento por parte dos programas antivírus. Essas características são comuns, por exemplo, em mutações de vírus enviados por email.



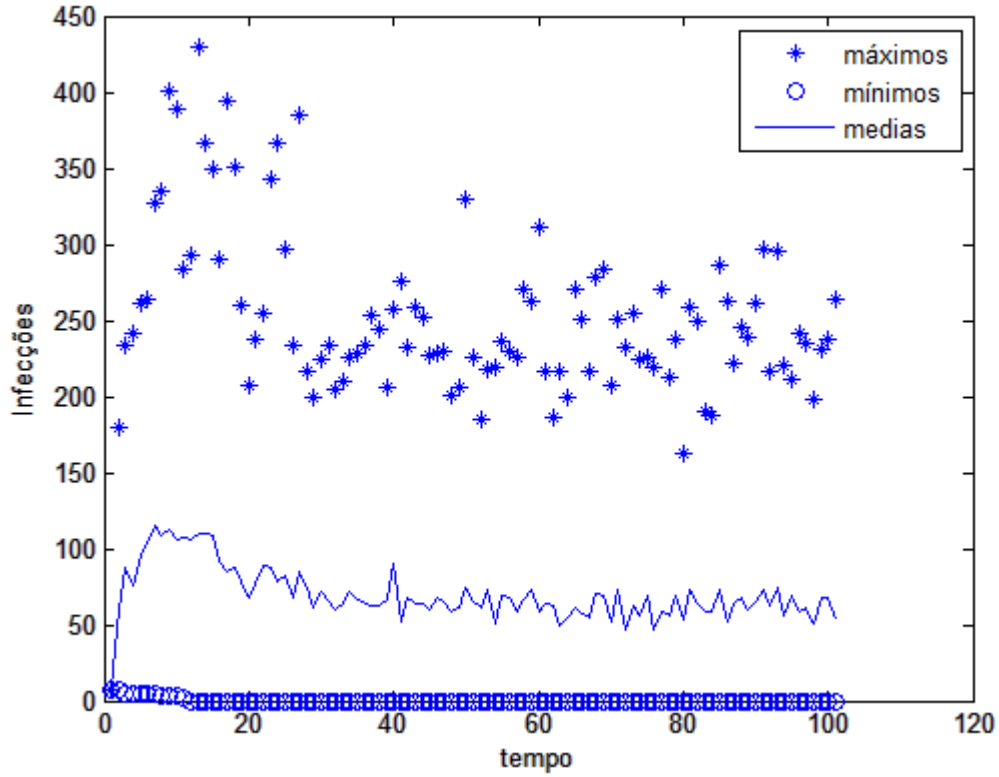
Em várias simulações, como se pode observar, houve epidemia na rede.

Em seguida, para a mesma rede e o mesmo tipo de vírus, foi empregado um gerenciamento nível II e o seguinte gráfico foi gerado.



Pode-se observar que o número de epidemias registradas diminuiu significativamente. Os valores médios das infecções ainda estão altos, porém reduziram para valores mais próximos dos aceitáveis. O custo operacional dessa medida é a redução do desempenho da rede, pois um grande número de micros realizará varredura ao mesmo tempo.

Em seguida, a ação será repetida, utilizando, dessa vez, gerenciamento nível III.



Pode-se observar dessa vez que todos os valores, até os mais críticos, estão dentro da faixa aceitável. No entanto, vale ressaltar que essa atitude é a mais custosa operacionalmente, pois além de reduzir o desempenho da rede com as varreduras é necessária, em algum momento, a perda da comunicação externa.

Conclusões

Neste trabalho foram aliados os modelos matemáticos utilizados em parte da bibliografia com a busca de soluções concretas do problema de propagação de ameaças virtuais em meios eletrônicos.

O objetivo do projeto era sugerir e testar melhorias que os gestores de redes poderiam implementar no combate as pragas virtuais.

Dentre as melhorias sugeridas e não testadas está o uso de previsão do comportamento futuro da rede para que medidas possam ser tomadas antes mesmo das situações críticas ocorrerem.

Um estudo de casos mostrou a viabilidade de políticas mais ostensivas de combate a propagação de malwares suas vantagens e limitações. Além disso, pôde-se observar que as políticas de gerenciamento sugeridas já são, em parte, empregadas, no entanto de uma forma não sistemática.

Agradecimentos

Agradeço aos meus pais e amigos por todos os dias da minha vida. Agradeço a ANP pelo apoio financeiro ao projeto, aos professores responsáveis Miguel e Fagá pela oportunidade dada e ao meu orientador Piqueira pelos ensinamentos, pela paciência e pela confiança.

Referências Bibliográficas

[1] Forrest S., Hofmayer, S.A. & Somayaj, A., "Computer Immunology", Communications of the ACM, 1997, 40(10), pp. 88-96.

[2] Piqueira J.R.C., Navarro B.F. & Monteiro, L.H.A., "Epidemiological Models Applied to Viruses in Computer Networks", Journal of Computer Science, 2005, 1(1), pp. 31-34.

[3] Kephart, J.O., Hogg, T. & Huberman, B.A., "Dynamics of computational ecosystems", Physical Review A, 1989, 40(1), pp. 404-421.

[4] Kephart, J.O., White, S.R. & Chess, D.M., "Computers and Epidemiology", IEEE Spectrum, 1993, pp. 20-26.

[5] Piqueira, J.R.C & Cesar, F.B., "Dynamical Models for Computer Viruses Propagation", Mathematical Problems in Engineering, ID 940526, 2008. (doi: 10.1155/2008/940526)

[6] Billings, L., Spears, W.M. & Schartz, I.B., "A unified prediction of computer virus spread in connected networks", Physics Letters A, 2002, 297, pp. 261-266.

[7] Mishra, B.K. & Saini, D., "Mathematical models on computer viruses", Applied Mathematics and Computation, 2007, 187(2), pp. 929-936.

[8] Olofsson, P. Probability, Statistics, and Stochastic Processes, Hoboken, N.J.: Wiley-Interscience, 2005.

[9] Aguirre, L.A. Introdução à identificação de sistemas, Belo Horizonte-MGBrazil: Editora UFMG, 2004.