



III Jornada de Iniciação à Docência Aplicação de minicurso como ferramenta didático-pedagógica: Conceitualização e Aplicação dos Antivírus nas instituições Educacionais

Tiago Pani da Penha¹

Gilberto Gil Pedracini²

Resumo: O artigo apresentado tem por objetivo mostrar a importância da utilização dos antivírus a partir de dados coletados por meio de uma palestra explicativa oral. Dentre outros assuntos, que trataremos ao longo do artigo, o projeto enfatiza os principais tipos de antivírus e suas respectivas vantagens e desvantagens. Além disso, ainda relata o custo benefício de cada através de gráficos explicativos e os principais tipos de vírus.

Palavras-chave: Antivírus; palestra; vírus.

1. Introdução

A palestra ministrada no dia 04 de maio de 2012 na Escola Conde de Linhares na cidade de Colatina-ES para os alunos do Curso de Informática para Internet do período noturno. O objetivo maior da mencionada explanação foi expor os pontos falhos dos antivírus e como proteger o sistema operacional do computador de maneira eficaz.

2. Fundamentos Teóricos

A história da informática está intimamente ligada à história dos vírus de computador, que são programas executáveis com poder de replicação e estes quando executados passam ativos na memória do computador replicando seu código para dentro de unidades de armazenamentos. Com a finalidade de corromper ou destruir dados acondicionados em tais unidades.

Atualmente os vírus de computadores se destacam como um dos maiores desafios enfrentado por qualquer organização. Pois a disseminação de novos vírus com códigos cada vez mais difíceis de detectar e corrigir, implicam na elaboração de atualizações constantes nos softwares de antivírus por parte das empresas fornecedoras de soluções de segurança da informação. Um aspecto que pode ser constantemente melhorado é a obtenção de conhecimentos a respeito do manuseamento e manutenção desses programas de antivírus.

De acordo com o pesquisador Cohen (1983) Vírus é um tipo de programa. Existem suas diferenças na codificação, mas, no entanto é executado da mesma forma que um programa comum, a grande

¹ Licenciando em Informática/ PIBID-IFES/ tiagopani18@hotmail.com

² Licenciando em Informática/ PIBID-IFES/gilpedracini@gmail.com



III Jornada de Iniciação à Docência

diferença está no que o programa faz. O vírus tem seu código perigoso aos sistemas operacionais, aos drives, programas e documentos que poderão ser apagados ou danificados. Um vírus ou praga virtual é um código de máquina que se anexa a um programa ou arquivo para poder se espalhar entre os computadores da mesma rede, infectando-os à medida que se é executado. Ele infecta enquanto se vai para outros computadores ou arquivos. Os vírus podem danificar seu software, hardware e arquivos (MICROSOFT, 2009).

“Vírus, WORM s e cavalos de Tróia são programas mal-intencionados que podem causar danos ao seu computador e às informações armazenadas nele. Também podem deixar a Internet mais lenta e usar o seu computador para espalharem-se entre os seus amigos, familiares, colegas de trabalho e o restante da Web. A boa notícia é que, com prevenção e algum bom senso, você terá menos probabilidade de ser vítima dessas ameaças.” (Microsoft, 2009)

De acordo com Orrico (2004, p. 51) os códigos maliciosos são gerados como executáveis tanto em *pen drivers*, browsers e nos sistemas operacionais, podem ser replicados e executados. Depois de executados ficam na memória, procurando todas as unidades disponíveis tanto no computador, na rede ou internet para ser replicados e executados pelas possíveis vítimas.

3. Materiais e Métodos

O método de apresentação foi oral e participativo, com utilização de slides e projetor, à medida que iam aparecendo os assuntos abordados relacionados com a palestra, os alunos participavam com perguntas, sugestões e comparações dos aplicativos e programas utilizando sem casa e o que a instituição educacional utiliza.

4. Desenvolvimento

Durante a palestra expositiva, tanto os alunos quanto o professor e o palestrante procuraram demonstrar que o computador tornou-se um objeto de muito valor e muito usado não só em empresas, mas também em residências e até mesmo no celular. E diante de toda essa propagação dos meios tecnológicos e seu crescimento avançado também temos um grande perigo a nossa espreita que são os vírus (programas maliciosos) tão usualmente propagados para tentar roubar nossos dados pessoais como contas bancárias, e-mails e rotinas do computador.

Tendo em vista todas as exposições são de extrema importância o conhecimento e estudo dos tipos de vírus encontrados para que possamos nos precaver desse mal da tecnologia.

III Jornada de Iniciação à Docência

4.1 Tipos de Vírus mencionados

- Vírus de Arquivos: Infectam a máquina através de vírus com extensão “.com” ou “.exe.” e eles copiam os seus códigos fonte para dentro dos arquivos infectados, por consequência, os arquivos infectados ficam maiores enquanto outros acabam por multiplicarem-se de tal forma que ocupam todo espaço do disco.
- Vírus Polifórmicos: São aqueles que podem mudar seu próprio código-fonte e são também chamados de vírus mutantes.
- Vírus de *Boot*: São aqueles que iniciam junto com o sistema operacional e se instalam no setor de boot dos discos. São facilmente identificados pelos antivírus modernos.
- Vírus *Stealth*: Ele é semelhante ao vírus de arquivo, mas não podem aumentar o tamanho do arquivo infectado.
- Vírus de Macro: São programas maliciosos que usam as macros disponíveis para atacar o computador dos usuários
- Vírus de *Bios*: Atacam a *Bios* para danificar os discos rígidos.

A apresentação dos tipos de vírus é apresentada no minicurso, vide Figura 1.



Figura 1 - Apresentação dos tipos de vírus.

III Jornada de Iniciação à Docência

- **Piadas:** São softwares que danificam diretamente o host e advertem o usuário sobre perigos inexistentes, como mensagens que avisam sobre a formatação do disco rígido (embora isso não ocorra realmente) ou a detecção de vírus não infectados.
- **Rootkits:** São utilitários para disfarçar a atividade mal-intencionada e modificam funções básicas do SO do computador ocultando sua própria existência e as ações executadas pelo hacker no computador infectado.
- **Hoax:** Apesar de terem um comportamento de vírus eles não o são. Eles são histórias falsas e correntes que são transmitidas pelas pessoas e vão se multiplicando através do e-mail.
- **Spam:** São propagandas que as pessoas mandam para sua caixa de entrada no e-mail sem o seu consentimento e são enviadas em larga escala.

4.2 Precauções a serem tomadas:

Sabendo que um antivírus mesmo com toda sua potência pode conter erros e falhar em proteger o seu sistema operacional de invasões podemos nos prevenir tentando remediar a situação usando de artifícios como:

1. Não baixar arquivos de sites com conteúdo duvidoso.
2. Não aceitar disquetes, pen drive e cds de terceiros, pois pode conter algum vírus. Caso aceite passar o antivírus nos arquivos.
3. Fazer varredura no sistema operacional e nos arquivos de tempo em tempo.
4. Ao abrir e-mail de amigos verificar a presença de vírus.
5. Fazer varredura no sistema operacional e nos arquivos periodicamente.

5. Considerações Finais

O papel do antivírus é monitorar esses vírus e aplicar a vacina para tentar restaurar o arquivo como o original, mas para isso ele precisa ser periodicamente atualizado que pode facilmente ser feito através de atualizações automáticas que o próprio antivírus possui. Se ele não for atualizado novas versões deste vírus e outros novos vão surgindo e o antivírus não consegue identificá-los. Tendo em vista todo o conteúdo que foi exposto ficou claro que não basta apenas possuir um antivírus potente e sim uma boa cultura de prevenção, pois tomando os cuidados necessários uma invasão será mais difícil. Durante a palestra foram citados alguns termos técnicos que fazem parte do cotidiano dos vírus e do antivírus como quarentena, *removal tools*, falso positivo. Com isso, percebe-se que um vírus não pode destruir o seu computador e o dano maior que ele pode causar à máquina é apagar todos os dados do computador deixando o usuário perdido e propenso a golpes.

Os alunos participantes se mostraram muito atentos e participativos durante todo o evento ultrapassando o tempo estimado, e ao final dessa palestra pegar email do palestrante para tirar possíveis novas dúvidas, além de prestarem mais atenção as aulas e aos aplicativos instalados nos equipamentos educacionais.



III Jornada de Iniciação à Docência

6. Agradecimentos

Agradecemos primeiramente a Deus que nos dá força e capacidade para iniciarmos e concluirmos qualquer que seja a etapa de nossas vidas. Agradecemos também a EEEMT “Conde de Linhares”, ao professor Dayan Bissoli e aos alunos do Curso de Informática para Internet do período noturno, pois sem eles de nada teria valido tanto esforço.

7. Referências

COHEN, Fred. **Histórico: a evolução do vírus de computador.** Disponível em:<<http://www.fisicastronomorais.com/pdf/virusinfor.pdf>>

MICROSOFT. **O que são vírus, worms e cavalos de Tróia?** Disponível em:<<http://www.microsoft.com/brasil/athome/security/viruses/virus101.msp>>

ORRICO, J. H. **Pirataria de Software.** 1. ed. São Paulo: MM Livros, 2004. (Informática). ISBN 89788590424222.