MALWARE, O VÍRUS QUE OCULTA ARQUIVOS: como recuperar arquivos afetados por esse vírus de computador[1]

Fellipe Borges de Oliveira*

Resumo

Este trabalho trata sobre o funcionamento do vírus *Malware* mostrando suas ações em discos rígidos e discos removíveis. O objetivo deste estudo é mostrar como recuperar os arquivos afetados pelo vírus e quais programas e métodos usados na identificação das ações desse vírus. Mostra-se neste artigo algumas das funções do software de compactação de arquivos Winrar, da ferramenta "opções de pastas e pesquisa" e o comando "Executar" do Sistema Operacional Windows. A metodologia usada dar-se através da aplicação das ferramentas citadas acima para recuperar os arquivos infectados pelo *Malware*. Conhecer e dominar uma quantidade significante do uso das tecnologias e suas ferramentas é de suma importância para o profissional da informação, pois as mesmas são de fundamental importância no mundo em que estamos inseridos e estar aptos a essas tecnologias e seus funcionamentos são essenciais para o novo perfil do bibliotecário, cuja função é ser gestor da informação.

Palavras-Chave: Vírus *Malware*. Recuperação de informação. Recuperação de arquivos digitais.

[1] Comunicação Oral apresentada ao GT 06 (Tema Livre)

*Universidade Federal do Pará. Graduando em Biblioteconomia. Email. borges.fellipe@hotmail.com.

1 INTRODUÇÃO

Este estudo aborda assuntos referentes ao funcionamento de alguns Softwares Maliciosos (*Malware*) que são criados por *crackers* com a finalidade que vai desde causar algum dano em sistemas operacionais ou discos removíveis e rígidos; até o roubo de informações dos usuários dessas plataformas de interação com a máquina. Frequentemente computadores e outros suportes eletrônicos vêm sendo infectados pelo *Malware,* processo esse vivenciado principalmente no cotidiano de alunos de Biblioteconomia, Documentação, Ciência e Gestão da Informação, e profissionais dessas áreas, uma vez que a informação é principal objeto de trabalho desse ramo do conhecimento.

Com base nestes fatos, o objetivo deste estudo é esclarecer de forma muito sucinta alguns desses problemas, mais especificamente em *pendrives* e cartões de memória, e como recuperar estes arquivos através de ferramentas básicas do sistema operacional Windows, como a "opções de pasta e pesquisa", "Executar", "Winrar" e um programa denominado "FixPolicies".

Almeja-se também conscientizar os indivíduos dos ramos do conhecimento supracitados a utilizar antivírus e suas respectivas atualizações, para que seus documentos eletrônicos possam ter um pouco mais de segurança, uma vez que corrompidas estas informações tem-se a possibilidade de perda total das mesmas, o que, em certos casos, nem mesmos programas específicos poderão recuperá-las.

2 FUNDAMENTAÇÃO TEÓRICA

Para que possamos entender mais sobre os *Malware* precisamos conhecer a origem desta palavra. *Malware* é uma abreviação de *Malicious Software* que adaptado para o português significa códigos maliciosos. Segundo Goertzel e Winograd (2009) também podemos utilizar os termos "badware" e "harmware" para designá-lo.

Os autores citados acima em seus estudos denominados "Malware" apresentam uma tabela com os diversos tipos desses códigos maliciosos, porém serão listados aqui apenas alguns deles que se alinham ao objetivo deste trabalho, para isso veja o quadro 1.

Quadro 1 – Tipos de *Malware*

CATEGORIAS	**TIPOS DAS CATEGORIAS**	**SUBTIPOS DAS CATEGORIAS**
VÍRUS Código malicioso que cria cópias de arquivos host, documentos e entre outros, sendo executados assim que estes programas afetados também iniciarem.	VÍRUS DE ARQUIVOS Utiliza arquivos dos Operating System (OS)[2] para se propagarem.	VÍRUS DE SCRIPT Subconjuntos de vírus de arquivos escritos em diversas linguagens de informáticas como Visual Basic, Scripts, JavaScript, PHP, e outros.
	VÍRUS DO SETOR DO BOOT Estes vírus instalam-se nos setores de boot ou no master boot impedindo que o mesmo carregue a memória do computador. Uma vez instalado no boot, o vírus impede que o OS se carreguem através do boot.	
	VÍRUS DE MACRO Estes vírus se instalam nos scripts de macro de processadores de textos, planilhas e outros, executando arquivos infectados a partir das macros.	
CAVALO DE TRÓIA OU TROJAN Os Trojans são softwares maliciosos que camuflam os programas originais assumindo a forma dos mesmos. Suas origens de infecções ocorrem através de anexos de e-mail que contenham o vírus, link de web e entre outros.	BACKDOOR TROJAN São trojans que se infiltram no computador infectado dando ao seu controlador acesso remoto a máquina por meio de um host.	DENIAL OF SERVICE (DoS) TROJAN Se uma máquina estiver com um estado crítico de infecção desde trojan, ele pode causar um ataque de criação de Distributed Denial of Service (DDoS)[3].
MALWARE CONSTRUCTOR Ferramenta que possibilita a criação de novos *malware*.	CRYPTOGRAPHIC OBFUSCATORS Ferramenta de criptografia de programas de códigos maliciosos, impossibilitando-os de serem descobertos por software anti-*malware*.	

Fonte: Goertzel e Winograd, 2009, adaptado pelo autor desta pesquisa.

[2] Sistemas Operacionais
[3] Negação Distribuída de Serviços.

O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (2006) conceitua *malware* como programas que são exclusivamente desenvolvidos com o objetivos de atuar de forma prejudicial ao sistema de um computador.

A partir das denominações mencionada anteriormente, podemos inferir que *malware* são códigos maliciosos, usados por *crackers* tendo como finalidades corromper o computador, discos rígidos e removíveis etc, de um usuário recolhendo informações dos mesmos, tais como: senhas de computador, senhas de cartões de créditos, Cadastro de Pessoas Físicas (CPF), arquivos confidenciais e diversos tipos de informações, substituindo arquivos do system32, ocultando pastas/documentos de *pendrive* criando *trojans* no lugar dos mesmos e outras funcionalidades que comprometam o desenvolvimento do OS.

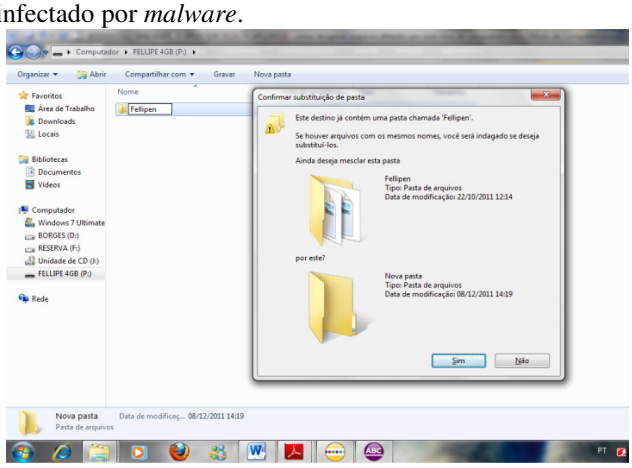
3 METODOLOGIA E RESULTADOS

Muitos usuários do sistema operacional Windows já se depararam com a situação em que ao colocar seu pendrive no computador suas pastas e/ou documentos não estavam visíveis, o que lhes causou a impressão de que um vírus tinha infectado seu disco removível apagando seus arquivos e ao tentar copiar novos documentos para o mesmo acabaram se deparando com os seguintes informes: “Não há espaço suficiente em seu disco” ou alguma informação similar, variando de sistemas para sistemas, como demonstra a figura, 1 ou “Este destino já contém uma pasta/arquivo chamado”, como mostra a figura 2.

Figura 1 – Copiar pasta para um *pendrive* infectado por *malware*.

Fonte: Do autor.

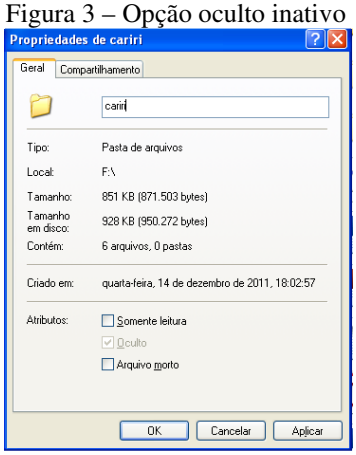
Figura 2 – Criando nova pasta dentro de um *pendrive* infectado por *malware*.



Fonte: Do autor.

Isso acontece devido ao fato de os arquivos originais estarem ocultos mesmo após a execução de um antivírus excluindo os *malware*. Essas pastas, de acordo com a pesquisa realizada, não podem ficar visíveis novamente, pois a opção de marcar/desmarcar oculto permanece inativa como é demonstrado na figura 3, o mesmo vale para os documentos originais infectados.

Figura 3 – Opção oculto inativo



Fonte: Do autor

Porém, existe uma possibilidade de recuperar esses arquivos, através do uso, em conjunto, de ferramentas básicas de sistemas operacionais. Vale ressaltar que o método utilizado neste trabalho dá-se por meio do uso do Windows OS – nas versões do XP e Seven, ressaltando que a não utilização de métodos para a plataforma Linux dá-se ao fato do mesmo

permitir a visualização das pastas infectadas possibilitando ao usuário recuperar seus arquivos.

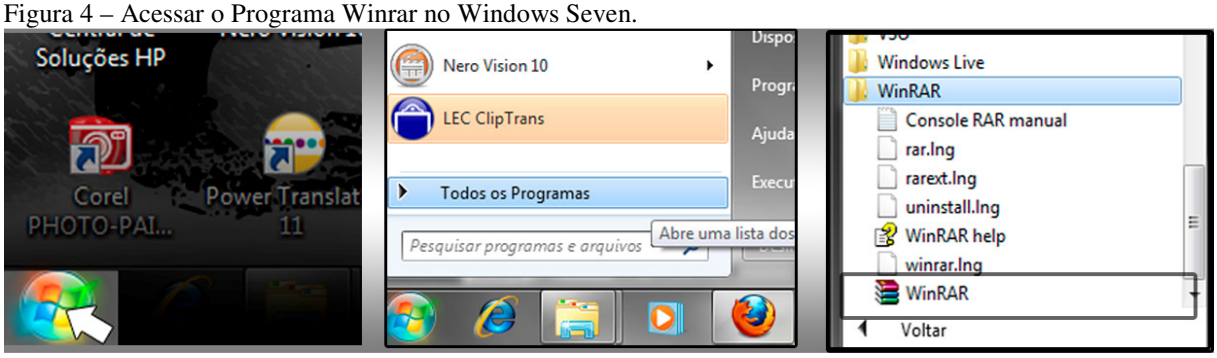
3.1 RECUPERANDO ARQUIVOS INFECTADOS POR *MALWARE* ATRAVÉS DO COMANDO EXECUTAR E DO PROGRAMA WINRAR

Antes de partimos para esse método temos que compreender o que é o comando "Executar" e o que é o programa Winrar. O comando “Executar” encontra-se no menu iniciar tanto no Windows Seven quanto no Windows XP e tem como função executar caminhos de pastas, documentos, programas e comandos de atalhos que configuram o sistema operacional. Já o Winrar, segundo a Winrar Brasil (20--?), é um programa capaz de compactar diversos tipos de formatos eletrônicos e que suporta várias extensão de arquivos compactados com: .rar, .zip, .cab, .arj, .lzh, .ace, .tar, .gzip, .uue, .iso, bzip2, z e 7-zip e oferece uma interface possibilitando uma melhor organização dos documentos compactados.

A partir do conhecimento sobre suas funcionalidades dá-se início ao método de recuperação de informação desses arquivos em discos removíveis.

- Primeiro é necessário o computador conter um antivírus atualizado.
- Depois escanerizar com o antivírus a unidade inserida para eliminar os *malware*.
- Após isso, verifique se sua unidade ainda contém seus documentos, se eles não aparecerem certifique que existem arquivos a partir das propriedades da unidade, acessada através do clique com o botão direito do mouse no disco inserido e propriedades. Se contiver alguma informação de preenchimento do disco adote os procedimentos a seguir.
- Abra o programa Winrar que fica no “Menu iniciar” – Todos os Programas – Winrar – Winrar. Veja a figura 4.

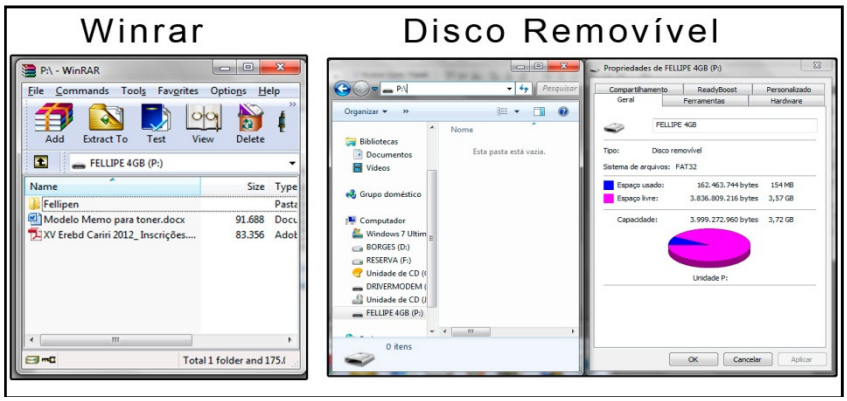
Figura 4 – Acessar o Programa Winrar no Windows Seven.



Fonte: Do autor.

- Com o Winrar aberto navegue através da barra de endereço até a sua unidade removível perceba que ele mostra seus arquivos que estão ocultos como mostra a figura 5.

Figura 5 – Quadro comparativo do Winrar e unidade removível afetada com *malware*



Fonte: Do autor.

- Os arquivos das pastas ocultas pelo *malware* não são ocultados, por isso a utilização do Winrar para conhecer o nome das pastas ocultas, como foi descrito acima para usar o comando "Executar" temos que conhecer o caminho em que as pastas/arquivos se encontram e seus respectivos nomes, pois sem isto não poderemos acessá-los.
- Agora podemos abrir o comando "Executar" no "menu iniciar" – "Executar" ou pressionado as teclas "logotipo do Windows" mais "R". Digita o caminho das pastas, copia os arquivos e mova para uma pasta no computador. Após ter concluído esses processo formate o seu disco removível.

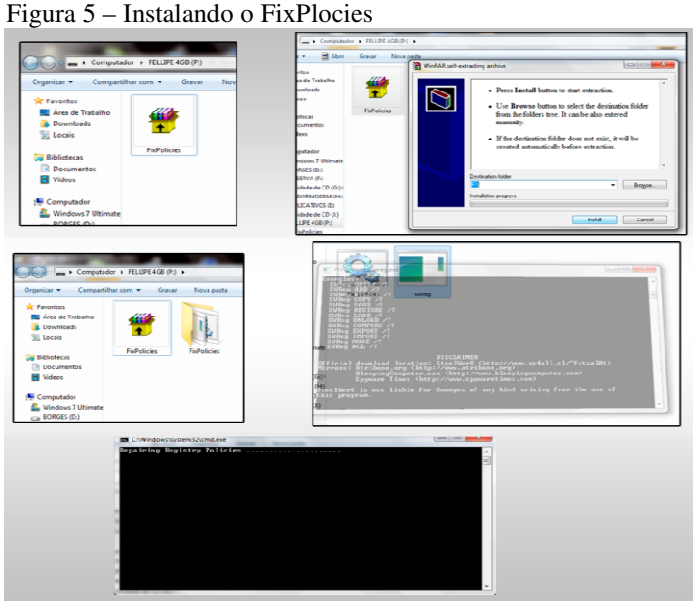
3.2 RECUPERAÇÃO DE ARQUIVOS INFECTADOS PELO *MALWARE* POR MEIO DO PROGRAMA FIXPOLICIES E DA FERRAMENTA "OPÇÕES DE PASTA E ARQUIVOS" DO EXPLORER DO WINDOWS

Neste método de recuperação dos documentos, será utilizada a ferramenta "opções de pasta e arquivos" do *Explorer* do Windows; que possibilita o usuário configurar as pastas de sua máquina da forma desejada, com um ou dois cliques para abrir pastas/documentos, mostrar/não mostrar arquivos ocultos, ou restaurar as configurações padrões de seu sistema operacional. Juntamente com essa ferramenta é aplicado um software livre denominado FixPolicies que tem como finalidade mostrar todos os arquivos e pastas ocultas no computador que possivelmente estejam corrompidos e que não possam ser visualizadas apenas com a ferramenta descrita acima.

Para a recuperação de arquivos através desse método deve-se seguir os passos abaixo.

- Primeiro baixe o FixPolicies através do link "http://downloads.malwareremoval.com/BillCastner/FixPolicies.exe" e salve no seu pendrive.
- Abra seu pendrive instale o software dando dois cliques nele e clicando em instalar sem modificar nada.
- Abra a pasta que será criada e dê dois cliques primeiramente em "swreg.exe" e depois em "Fix_policies.cmd". Aparecerá uma janela do comando DOS e fechará logo em seguida em ambos os arquivos, procedimento este normal.

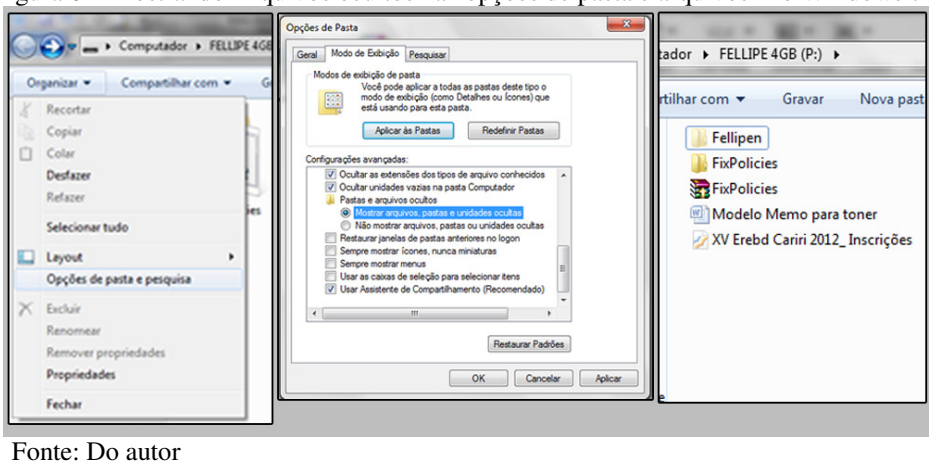
Figura 5 – Instalando o FixPlocies



Fonte: Do autor

- Perceba que se a opção de mostrar arquivos ocultos não estiver marcada, seus arquivos ainda não serão visualizados. Para ativar essa opção no Windows 7 clique na ferramenta "Organizar", depois em "opções de pastas e arquivos" ou no Windows XP no Menu Ferramentas e em seguida "opções de pastas e arquivos". Aparecerá uma nova janela, clique na aba "Modo de exibição" e nas configurações avançadas navegue até a "Mostrar arquivos, pastas e unidades ocultas" e dê "OK". Veja a figura 6.

Figura 6 – Mostrando Arquivos ocultos na "opções de pasta e arquivos" no Windows 7



Fonte: Do autor

A partir desse momento as pastas e arquivos estão prontos para serem copiados para seu computador e sua unidade removível deverá ser formatada para que possa ser utilizada normalmente. Ressalta-se que estes métodos também são válidos para os discos rígidos. Os documentos que foram corrompidos podem ser abertos, porém para ficarem visíveis novamente deve-se salva-los com a opção "salvar como" e atribuir um novo nome para o mesmo. Para diminuir o tempo de processo de recuperação dessas informações recomenda-se que o usuário crie uma pasta como o nome que desejar e salve os arquivos dentro dessas pastas, pois como foi mencionado acima, apenas os arquivos das primeiras pastas são ocultos e os documentos que estão dentro da mesma podem ser visualizados assim que ela for aberta.

4 CONSIDERAÇÕES FINAIS

Conhecer e dominar uma quantidade significante do uso das tecnologias e suas ferramentas é precípuo ao profissional da informação, pois as mesmas são de fundamental importância no mundo em que estamos inseridos. Estar apto a essas tecnologias e seus funcionamentos são essenciais para o novo perfil do bibliotecário, cuja função é ser gestor da informação.

Gerir uma unidade de informação é semelhante ao processo de um sistema operacional, se um dos componentes estiver danificado ou não respondendo, isso gera um mau funcionamento do sistema, deixando-o mais lento comprometendo a qualidade de seus serviços. Para evitar esses fatores que afetam os processos de disseminação e recuperação da informação tanto no espaço físico como no virtual e eletrônico é imperativo que o bibliotecário esteja atualizado quanto aos métodos existentes que permitam solucionar problemas de ordem tecnológica que afetam a sua práxis biblioteconômica.

MALWARE, THE VIRUS THAT HIDES FILES: how to recover affected files for that computer virus

ABSTRACT

This work treats on the operation of the virus Malware showing its actions in hard disks and removable disks. The objective of this study is to show as recovering the affected files for the virus and which program and methods used in the identification of the actions of that virus. It is shown in this article some of the functions of the Winrar, a software that to compact files, as well as of the tool "options of pastes and it researches" and the command "Execute" of the operating system Windows. The methodology used was the application of the tools mentioned above to recover the files infected by Malware. To know and to dominate a significant amount of the use of the technologies and its tools is of highest importance for the professional of the information, because the same ones are of fundamental importance in the world in that are inserted and to be able to use those technologies and its operations are essential for the librarian's new profile, whose function is to be manager of the information.

Keywords: Malware Virus. Information retrieval. Digital files recovery.

REFERÊNCIAS

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Parte VIII:** códigos maliciosos. 2006. Disponível em: <http://cartilha.cert.br/download/cartilha-08-*malware*.pdf>. Acesso em: 22 out. 2011.

GOERTZEL, Karen Mercedes; WIMOGRAD, Theodore. *Malware*. **Information Assurance Tools Report.** Herdon, VA: IATAC, 17 set. 2009. Disponível em: <http://iac.dtic.mil/iatac/download/*malware*.pdf>. Acesso em: 10 out. 2011.

WINRAR BRASIL. **Conheça o Winrar.** [S.l]: SILICONACTION, [20--?]. Disponível em: <http://www.winrarbrasil.com.br/winrar/info.mv>. Acesso em: 1 nov. 2011.