Vírus de Macro

22/01/2021

Autor: Pedro Luis Kantek Garcia Navarro

O WORD tem, há umas 2 versões, uma linguagem de programação chamada WordBasic, que permite escrever programas dentro dos arquivos .DOT (modelos). Neste contexto tais programas são chamadas macros, e são escritos, depurados e executados sob o comando Utilitários - Macros do WORD.

Existem alguns nomes de macros especiais que servem a propósitos especiais: (AutoOpen, FileExit, etc., e aquele que mais nos interessa que é o AutoExec). Quando houver macros definidas com estes nomes, elas serão chamadas automaticamente pelo WORD, nos diversos eventos associados. AutoExec é chamada e executada automaticamente quando o arquivo que a contém é aberto. O usuário não é avisado de nada.
Aqui estão presentes todas as condições necessárias e suficientes para o alastramento da virose, senão vejamos:

1. Uma linguagem de programação poderosa (wordbasic);

2. Um evento que chama um programa automaticamente (a macro autoexec);

3. Vetores de transmissão e disseminação (arquivos .DOT que se intercambiam entre máquinas e redes).

As macros só residem em arquivos DOT, mas aqui têm uma sutileza infernal: Eu

posso gravar um arquivo como MODELO (isto é, com a habilidade de carregar macros consigo) e dar a ela o nome de fulano.DOC. Nessa hora eu tenho um arquivo DOC que não é um arquivo DOC e sim DOT, só que é quase impossível descobrir isso. Quando um usuário desavisado abrir o arquivo DOC, ele na verdade vai estar abrindo um DOT.

Outra possibilidade é usar o NORMAL.DOT que sempre existe associado a qualquer WORD. O DOC não carrega macros consigo, a menos que seja um doc de mentirinha (um dot vestido de doc).

Ontem, em visita a um Cliente, deparei-me com um vírus, que hoje vim a descobrir ser o vírus Nuclear. O sintoma que me levou a desconfiar da existência de vírus foi o desaparecimento de alguns comandos na estrutura de menus do Word. Na tentativa de retornar ao "status quo" anterior, com os comandos completos, percebi que o comando que permite restaurar os comandos desaparecidos havia desaparecido. Ou seja, sentiu-se o inconfundível cheiro de sacanagem da grossa no ar.

O texto fazia coisas enlouquecidas (via macros de nomes automáticos) e eu nem sequer podia ver as macros, pois o comando Utilitários Macros, havia sido excluído da árvore de menu.

Fiz a pressuposição de que o vírus estava no arquivo NORMAL.DOT que, como se sabe, descreve características (tais como macros, ou supressão de comandos) dos arquivos .DOC.

Saí do programa e procurei onde estava o NORMAL.DOT. Mudei o nome dele para Vírus.DOT e carreguei o mesmo texto. Voi-lá, os comandos haviam voltado ao normal.

Chamei Utilitários - Macro, e lá estava a prova do crime. Havia 9 macros (de nomes autoexec, utoopen, dropsuriv, fileexit, fileprint, fileprintdefault, filesaveas, insertpayload, payload). Eis a prova do crime. Só que o comando que permite editar macros, havia sido desabilitado.

Seria necessário passar algumas horas sobre o help do wordbasic (ÚNICO local onde esta linguagem maluca está descrita), para desativar o vírus. Achei melhor pedir socorro pra Elaine -DISAT que me enviou um disquete com anti-vírus e ... final feliz.

Hoje fui navegar na Internet na busca de mais informações, e um resumo do que descobri foi:

Conhecem-se 3 vírus de macros:

CONCEPT: Não provoca nenhum dano, exceto que transforma o seu arquivo .DOC em .DOT, ainda que com o nome .DOC (autêntico samba do crioulo doido). Com isso ele carrega a macro consigo. Quando este documento (na verdade estilo) for reaberto pela primeira vez, aparecerá uma caixa de diálogo escrito "1", e o botão OK.

Ele é detectado pela presença das macros AAAZAO e AAAZFS no Utlitários Macro.

NUCLEAR: Tem uma lista interminável de sacanagens. Entre elas:

a. Se você imprimir um arquivo infectado entre um décimo quinto e um décimo sexto segundo, (por exemplo às 20:15:20), a última frase do relatório será uma mensagem pedindo a interrupção dos testes atômicos franceses no pacífico.
b. Se abrir um arquivo infectado entre 17 e 18 horas, o NUCLEAR vai tentar instalar o programa residente PH33R na memória (outro vírus, este agora convencional, daqueles que infectam arquivos executáveis, através do ensanduichamento de uma interrupção qualquer do PC).
c. Se abrir um arquivo infectado no dia 5 de abril, o vírus zera os arquivos Msdos.sys e Io.sys do seu diretório raiz, além de excluir o arquivo Command.com do mesmo diretório. Em outras palavras, seu micro vai para o espaço, e o sistema operacional precisa ser reinstalado.

DMV: Igual ao NUCLEAR, mas sem a lista de baixarias.

Proteção:

O SCAN, a partir da versão 300, alega proteger os arquivos. Não conferi o resultado.

No site da Microsoft tem um arquivo .dot (scanprot.dot) que é um anti-viral que usa o mesmo princípio dos vírus de macro para atuar.

Maiores informações:

http://www.microsoft.com/brasil

pedir base de dados, programa word e palavra de pesquisa Vírus.

Observação final: pelo jeitão do dito cujo, é possível (e, conseqüentemente, esperado) que essa mesma praga comece a aparecer via arquivos Excel, Access e Powerpoint, já que estes 4 compartilham a linguagem wordbasic.