Vírus de email

Toda a verdade sobre essa mentira

É realmente surpreendente a resistência do ser humano em abandonar certas crenças. Tente argumentar com alguém que tem um adesivo com os dizeres "Eu acredito em duendes" sobre as implicações biológicas de um cérebro de 100 gramas... Minha missão é abalar, se possível destruir, a crença em uma dessas lendas.

Eu não vou falar sobre duendes, astrologia ou anjos. Falarei sobre vírus de email. Para começar, deixe-me esclarecer um detalhe: os vírus de email não existem. Eu repito, os vírus de email não existem.

Sim, eu sei, é difícil acreditar que uma verdade tão antiga possa ser declarada falsa assim, sem mais nem menos. Sim, eu me sinto um pouco como Copérnico em meio aos bárbaros. Mas, como ele, eu não tenho escolha senão opor a verdade fria às noções românticas sobre como funcionam o email e os vírus de computador.

A lenda dos vírus de email foi criada pela união de alguns milhões de usuários inexperientes a uma pequena horda de jornalistas desinformados.

Há apenas dez anos, uma mensagem sobre vírus de email só causaria irritação. Na época, o usuário típico da Internet era capaz de recitar os números IP (endereços de um computador na rede) dos vinte computadores que ele mais acessava.

Mas hoje, com o aparecimento da Web e a conseqüente massificação do uso da rede, uma mensagem dizendo "Não abra nenhum mail com o subject Good Times" causa uma corrente de pânico que se alastra rapidamente, atingindo os jornais, a televisão e, algumas vezes, até as revistas especializadas (felizmente não muitas).

> Subject: Goodtimes
>
> Seguem informações importantes. Cuidado com um arquivo chamado Goodtimes.
>
> Feliz Chanukah, pessoal, e cuidado por aí. Há um vírus na America Online circulando por e-Mail. Se você receber algo chamado "Good Times", NÃO leia ou descarregue. É um vírus que apagará seu disco rígido. Encaminhe este aviso a todos os seus amigos. Poderá ser de muita utilidade.

A triste realidade

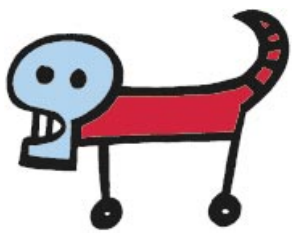
Para mostrar por que é impossível criar um vírus de email, eu terei que explicar um pouco da tecnologia que permite o envio e recebimento de mensagens através da Internet.

Um email simples tem duas partes. A primeira é o header (ou cabeçalho). O header contém todas as informações de identificação do remetente e do destinatário do email. São essas informações que permitem aos programas chamados de servidores de email enviar as mensagens para o destinatário certo (ou devolver ao remetente, caso o destinatário não exista). A segunda parte do email é a mensagem propriamente dita. Ambas as partes só podem conter texto. Nenhuma delas é executada como um programa em nenhum momento. Qualquer programa de computador colocado no header possivelmente impediria o processamento da mensagem pelo servidor de email.

Um programa de computador transcrito no corpo da mensagem possivelmente impediria que o cliente de email (o programa que roda na sua máquina) lesse aquela mensagem.

Agora, os vírus

Os vírus de computador são apenas programas, como o processador de texto ou o browser que você usa todos os dias. Eles têm certas características que os tornam especiais. Primeiro, eles são capazes de criar novas cópias de si mesmos. Em segundo lugar, eles em geral danificam os dados e programas dos discos onde se instalam. Mas, como todo programa, eles não conseguem se executar sozinhos.



> Subject: DEEYENDA
>
> A Internet está sendo novamente ameaçada por outro vírus de computador. Esse vírus, conhecido como Deeyenda Maddick, realiza uma varredura completa do seu computador em busca de dados valiosos como senhas de acesso, números de cartão de crédito, dados pessoais etc.

O usuário tem um papel ativo na instalação de um vírus, mesmo que esse papel seja tão inocente quanto examinar o conteúdo de um disquete infectado.

Note que, sendo um programa, um vírus é necessariamente criado para um determinado sistema operacional. É impossível executar um vírus de Windows em um Macintosh ou em uma máquina Unix.

Chegamos assim a um impasse. Os emails não podem ser executados como programas, eles são apenas lidos pelo programa de email e mostrados na tela do computador. Os vírus precisam ser executados para poder se instalar.

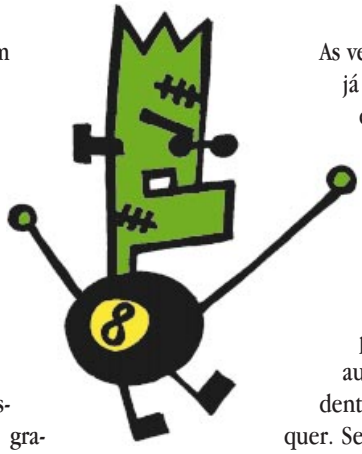
Então como seria possível pegar um vírus através do email? A resposta é aquela que já foi dada no início desta matéria. Não existem vírus de email!

Os attachments

Agora que você já sabe que ler um email não fará com que um vírus se aloje em sua máquina, vamos examinar alguns modos de utilizar o email para propagar um vírus pela Internet.

Note que nos casos que serão discutidos é sempre feito algo além da mera leitura da mensagem.

Além do header e do texto, um email pode conter outros arquivos. São os chamados attachments. Esses arquivos podem ter qualquer formato. Eles podem ser figuras, textos em formatos especiais, sons ou mesmo programas de computador.



Os servidores e clientes de email em geral ignoram esses arquivos. Eles apenas os transmitem junto com a mensagem, gravam os arquivos no disco do destinatário da mensagem e encerram sua participação. Existem aqui duas brechas que permitem a entrada de um vírus de computador: os programas executáveis e as macros do Word (ou melhor, de todos os aplicativos do Office).

É possível configurar alguns clientes de email para executar certas ações toda vez que um attachment é recebido. É possível, por exemplo, determinar que o programa de email deve abrir o programa que lê aquele tipo de arquivo. Assim, pode-se configurar o Netscape Mail para abrir o Word toda vez que for recebido um attachment com extensão ".doc".

Pode-se até configurar o Netscape Mail para executar qualquer attachment com extensão ".exe". Qualquer um é capaz de configurar seu cliente de email para executar programas recebidos junto com as mensagens, e possivelmente sabe dos riscos que corre.

Assim, não vou me alongar nessa discussão. Apenas não faça isso. Deixe pelo menos que seu programa anti-vírus dê uma olhada no programa antes de executá-lo (você tem um programa anti-vírus instalado, não é?). Os vírus de macro do Word são mais recentes e sutis. Quando você ler esta matéria já deverá estar disponível no site da Microsoft uma macro que impede a instalação desse tipo de vírus em sua biblioteca de macros do Office 95. Versões mais recentes do pacote já têm a correção.

As versões posteriores do Office já vêm com proteção contra esse tipo de vírus. Por motivos históricos e para incentivá-lo a fazer o download dessa macro "anti-vírus", vou descrever o mecanismo envolvido.

As macros são pequenos programas utilizados para automatizar certas operações dentro de um aplicativo qualquer. Se todas as semanas você tem que somar o resultado de várias planilhas de vendas, colocar os resultados em um relatório padrão e imprimir cinco cópias desse relatório, você pode fazer uma macro para executar todas essas operações. Desse modo, você pode ir tomar um café enquanto o Excel soma os números e passa para o Word, que então abre e atualiza o relatório e imprime as cópias.

A linguagem de macro atual do Office é suficientemente poderosa para permitir a criação de programas bastante sofisticados. É também poderosa o bastante para permitir a criação de programas nocivos, capazes até de apagar arquivos.

O problema surgiu por dois motivos. É natural que o cliente de email abra o Word toda vez que um arquivo com extensão ".doc" for recebido, especialmente se ele recebe esse tipo de arquivo com freqüência.

E, afinal, que mal haveria? Os arquivos de Word são aparentemente apenas textos (como os emails!).

Infelizmente, um arquivo de Word também pode conter macros (além de outras coisas, como sons, imagens etc.). Para piorar um pouco o problema, o Word, em sua configuração de fábrica, salvará para a biblioteca de macros qualquer macro nova presente em um documento. Não contente, o Word também não perguntará se você quer realmente salvar aquela macro (que você possivelmente nem sabe que está ali).

Eis aí o cenário ideal para alimentar a rede de desinformação sobre vírus de email. Para uma solução indolor para esse problema, vá até o site da Microsoft, faça o download e instale a macro "anti-vírus".

Não se assuste

Da próxima vez que você ouvir falar em um devastador vírus de email, ria.

Se você receber um aviso sobre um vírus de email, responda ao remetente do aviso que o verdadeiro vírus de email são as mensagens de aviso sobre vírus de email. Essas mensagens inúteis causam aumento de tráfego na rede, assustam usuários inocentes e tornam mais ricas algumas empresas espertas, que rapidamente lançam programas anti-vírus para email. Além de também darem mais uma oportunidade para a imprensa escrever outra matéria sobre os "perigos da Internet".

PAULO CANDIDO

PC não acredita em vírus de email, pero que los hay, hay.

"Subject: Novo virus

Se você receber um e-mail com o subject "WIN A HOLIDAY", NÃO O ABRA!!!!!!!!! Ele apagará tudo no disco rígido. Mande esta mensagem para quantas pessoas puder. Esse vírus é novo e não é muito conhecido. Essa informação foi anunciada ontem pela Microsoft, por favor compartilhe com todos que possam acessar a Internet. Também não abra ou mesmo olhe qualquer mail em que esteja escrito "RETURNED OR UNABLE TO DELIVER" (APENAS COM ESTA MENSAGEM) Esse vírus irá infectar os componentes do micro, tornando-os inúteis. Imediatamente delete qualquer mail que contenha essa mensagem. As informações da AOL dizem que ainda não há anti-vírus para este vírus. Por favor, pratique qualquer medida preventiva e novamente envie esse e-mail para todos os seus amigos."

Mais vírus de email em exposição e um contraponto metafísico: www.magnet.com.br/zero/virus