Copyright by: Ricardo C. Zímmerl' - Todos os direitos reservados
A cópia de todo ou parte deste artigo só é permitida com a citação expressa do autor e fonte.
www.itabra.com

Esteganografia
A Ciência do Oculto

Há muitos milhares de anos o homem procura mandar mensagens cifradas ou ocultas por diversas razões. Algumas vezes para que somente iniciados em determinada crença possam entendê-las, outras, para fins militares, outras, como subterfúgio a que possíveis interessados não possam ter acesso às mesmas, somente quem seja autorizado e possua a chave para decodificação.

Seja qual for o motivo, as técnicas para ocultar mensagens são inúmeras, inclusive àquelas que visam embutir mensagens em "mídias" diferentes da própria mensagem em si, como, por exemplo, a ESTEGANOGRAFIA (steganos - Oculto, Graphein - Escrever), a escrita oculta.

Oculta onde? No caso de informática é uma escrita (texto) que pode estar oculta em qualquer coisa, um arquivo de imagem, som (incluindo um MP3), vídeo, áreas ocultas do sistema, enfim, em muitos lugares ou mídias.

Mas uma mensagem "esteganografada" não necessariamente estará criptografada, esteganografia é a "arte" de ocultar uma mensagem em outra mídia, essa mensagem pode ser criptografada para aumentar a segurança de seu conteúdo também.

Durante a Segunda Guerra Mundial muitas fotos continham mensagens esteganografadas, era um jeito prático de enviar mensagens sem despertar suspeitas, o que remonta à Roma e Grécia antigas, onde as mensagens eram escritas em cera ou suco sobre os escritos convencionais. Hoje teme-se que criminosos possam utilizar-se da esteganografia para envio de mensagens cifradas pela Internet sem que seja possível detectá-las.

Os alemães, ainda durante a 2ª Guerra Mundial, criaram o "microponto", um jeito de imprimir fotografias inteiras em um tamanho tão pequeno quanto um ponto escrito à máquina, o que passava despercebido em envelopes e textos de forma geral, e podia transmitir uma enorme quantidade de informações.

Porém a maneira mais simples de esteganografar mensagens de texto é usar uma das letras de cada palavra para montar a frase oculta.

Manipulando Bits

Mas como se consegue esconder um texto, criptografado ou não, em um outro arquivo?

A resposta é realmente muito simples. Todos os tipos de arquivo são formados por Bytes (cadeias de 8 bits), esses bytes são agrupados de modo a gerar o resultado que esperamos: uma figura, num arquivo de imagem, som, num arquivo de áudio, etc. Esses agrupamentos não são aleatórios, são montados de forma a recriar ou produzir o resultado desejado, por exemplo, em uma figura de Bitmap (.bmp) cada pixel (pontinho) da imagem é dividido em três bytes, cada um desses bytes contém o valor correspondente a uma das três cores óticas primárias (verde - vermelho e azul). Para esteganografar um texto nessa imagem o que fazemos é distribuir o valor do byte correspondente a uma letra em um ou mais dos bytes da imagem. É claro que isso altera um pouco a luminosidade ou cor do ponto da imagem, mas, normalmente, isso é imperceptível a um olhar desatento. Por outro lado fica evidente que os textos a serem esteganografados não podem ser muito extensos. O ocultamento em formatos como MP3, JPG, MPG, etc. também são possíveis seguindo técnica similar. Claro que isso poderá sempre gerar algum "ruído", de modo que a esteganografia não é uma técnica absolutamente perfeita, por outro lado, é uma técnica bem efetiva, principalmente se o texto esteganografado também estiver criptografado, aí será quase sempre impossível saber se realmente trata-se de um texto oculto ou se não é apenas "ruído" no arquivo. Há outras formas de ocultamento em alguns casos e que não geram interferência. Todos os tipos de arquivo exceto os de texto simples (.TXT) possuem um cabeçalho que identifica o tipo de arquivo e pode trazer detalhes sobre o CODEC usado (em caso de áudio ou vídeo) dimensões de imagem, etc. seguido pela parte de dados. Figuras JPG, por exemplo, aceitam que entre este cabeçalho e a parte dos dados da imagem seja inserida qualquer coisa (até programas), essa característica e uma falha no interpretador de arquivos .JPG do Windows foi explorada recentemente para disseminação de vírus. Em meu site pode

ser encontrado um programa gratuito que limpa os arquivos .JPG (de imagem) de dados "supérfluos" que possam estar neles contidos e, assim, pelo menos, não desperdiçamos espaço de armazenamento com inutilidades potencialmente perigosas.

Esteganografia, agente do mal?

Como quase todas as coisas pouco compreendidas, principalmente quando são ocultas, secretas, logo são associadas a usos escusos, maléficos, mas a esteganografia tem amplo uso na indústria não só digital. Ela é usada para, por exemplo, certificar e autenticar arquivos por meio de "marcas d'água" digitais ou "fingerprints" (impressões digitais) garantido maior proteção a direitos do autor e maior segurança relacionada a origem do arquivo. Pode proteger um documento contra edição, por exemplo, já que em havendo edição, os bytes que contém os valores esteganografados serão alterados, invalidando a mensagem oculta e, portanto, a garantia de autenticidade.

Também, como vimos, há usos que podem ser maléficos, usados por criminosos, terroristas, o que for, com propósito de passar mensagens não rastreáveis, mas, não é a técnica a culpada pelo uso que dela se faz.

Seria possível proteger-se contra a esteganografia criminosa?

Isso depende de como a mensagem foi ocultada mas, via de regra, não há uma proteção ou algo do que se proteger. Por exemplo: é possível que nesses emails tipo "corrente" haja mensagens ocultas? É possível. Mas, e daí? Há diversos arquivos em nosso computador, imagens, MP3, planilhas, etc., vamos escanear uma a uma, reeditar cada uma delas para nos livrar desses potenciais arquivos ocultos?

Seria algo meio paranóico e sem nenhuma utilidade prática, uma vez que só a pessoa que conhece o "segredo" e possui a ferramenta para extrair a mensagem escondida poderá fazê-lo, se ela não tiver acesso ao seu computador, a mensagem permanecerá perdida.

Mas e se você quiser achar essas mensagens ocultas?

Aí a história é diferente. Na verdade, se a mensagem for criptografada será uma busca praticamente inútil por que, mesmo que a recupere, ela não significará nada. Mas pode-se conseguir os programas de esteganografia mais comuns do mercado, a maioria é gratuito, e testar arquivos suspeitos para ver se obtém algo.

Também, para os mais dispostos, quando ler uma mensagem meio perdida e sem muito sentido, procure observar as frases que se formariam ao colocarmos cada uma das segundas ou terceiras letras de cada palavra juntas e, quem sabe, encontrará alguma mensagem oculta ;-)

Ricardo C. Zimmerl
www.itabra.com