
WILSON OLIVEIRA
TÉCNICAS
PARA
HACKERS
soluções para
segurança

Sobre esta Obra

Esta obra tem por objectivo desmistificar as técnicas utilizadas pelos *Hackers* para invadir sistemas computacionais, bem como fornecer as melhores soluções para impedir essas invasões.

Esta obra tem uma finalidade puramente didáctica, sendo de grande utilidade para responsáveis por redes de computadores, fornecedores de serviços de Internet e administradores de Intranets, e também estudantes para terem conhecimentos das técnicas que são mais utilizadas pelos *Hackers* e as principais técnicas utilizadas para prevenir essas invasões.

Lembrando:
"*Hacker* não é aquele que faz um *flood* num canal de IRC, nem aquele que manda *mail-bombs* e muito menos aquele que cria vírus ou que tem prazer em prejudicar os outros utilizadores"; *Hacker* é aquele que ama o seu computador a ponto de transformar um XT inerte num instrumento de desencriptação ou que conhece o terreno que pisa, conhece o TCP/IP em detalhe, sabe todos os comandos do UNIX e os seus parâmetros na ponta da língua e anda sempre em contacto pleno com as novidades do seu mundo.

1. Introdução

Este livro foi escrito pois o assunto desperta grande curiosidade em todas as pessoas, e não existem muitas publicações no mercado mundial sobre esta temática.

Este livro visa mostrar os pontos fracos na segurança dos sistemas computacionais, visando que o programador encontre métodos para se defender.

Em primeiro lugar vamos identificar o termo *Hacker*:
Hacker, originalmente, designava qualquer pessoa que fosse extremamente especializada numa determinada área. Qualquer "barra" em qualquer assunto poderia ser considerado um *Hacker*. Somente com a ajuda do cinema americano é que o termo *Hacker de Computador* passou a ser utilizado largamente, mas nem por isso perdeu a sua identidade. Quem não se lembra do filme *War Games*, onde um míudo, brincando com o seu *modem*, acede (por "acidente") ao NORAD, simplesmente o computador responsável pela segurança de guerra dos Estados Unidos da América. Evidentemente, as pesquisas e técnicas realizadas pelo míudo para descobrir a palavra-chave do suposto jogo (ele não sabia no que estava a "mexer") é digna de um *Hacker*. Pelo menos dos *Hackers* daquela época.

Isso não quer dizer que este filme foi a base de lançamento de atitudes *Hacker* por todo o mundo, mas foi um dos responsáveis pela dilatação desses pensamentos. Já antes disso existiam *Hackers*. Eram pessoas que trabalhavam em projectos informáticos e eram técnicos altamente especializados. Mas também existiam aqueles míudos, que após descobrirem que invadir um sistema ou lançar um míssil não era tão fácil quanto ver um filme ou ler um livro, insistiram e estudaram muito (as maiores virtudes dos *Hackers* são a força de vontade e a dedicação aos estudos), conseguiram muitas proezas e hoje, grande parte trabalha na área de segurança de computadores. O resto está preso (espero que você faça a opção para trabalhar em segurança de computadores, pois ser preso não é muito aconselhável).

A grande maioria dos *Hackers* é jovem. Dizem que é uma fase da vida de cada utilizador avançado de computadores. E além do mais os jovens têm muito mais tempo para estudar e aprender. Depois de crescerem precisam de se preocupar com a vida e passar a trabalhar (geralmente com compu-

tadores), deixando de invadir sistemas ou fazer coisas piores. Os poucos que continuam a praticar actos de *Hacker* são espiões industriais ou especialistas em segurança, e passam a fazer um trabalho extremamente profissional, onde vão tentar deter, agora a sério, os invasores perigosos, ou protegerem-se do risco de invadir sistemas.

Quase todos os *Hackers* depois da fase da adolescência possuem habilitações literárias universitárias. O *Hacker* que aprendeu sozinho é sempre considerado (pelo menos para os outros *Hackers*) como mais motivado, e pode ser mais respeitado que o seu equivalente com o canudo. As áreas incluem (além da óbvia ciência da computação e engenharia eléctrica e electrónica) física, matemática, línguas e filosofia.

Definições

Hacker:
Uma pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes com um computador. Ele sabe perfeitamente (como todos nós sabemos) que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando as técnicas mais variadas.

Cracker:
Possui tanto conhecimento quanto os *Hackers*, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar códigos, e descobrir falhas. Eles precisam deixar um aviso de que estiveram lá, geralmente com recados malcriados, algumas vezes destruindo partes do sistema, e até destruindo o que encontram. Também são atribuídos aos *Crackers* programas que retiram controlos contra cópia em software, bem como os que alteram as suas características, adicionando ou modificando opções, muitas vezes relacionadas com pirataria.

Phreaker:
É especializado em telefonia. Faz parte das suas principais actividades as ligações gratuitas (tanto locais como interurbanas e internacionais), reprogramação de centrais telefónicas, instalação de escutas (não aquelas colocadas em postes telefónicos, mas imagine algo no sentido de, a cada vez que o seu telefone tocar, o dele também o fará, e ele poderá ouvir as suas conversas), etc. O conhecimento de um *Phreaker* é essencial para se procurar informações que seriam muito úteis nas mãos de mal-intencionados. Além de permitir que um possível ataque a um sistema tenha como ponto de partida fornecedores de acessos noutros países, as suas técnicas permitem, não somente ficar invisível diante de um provável rastreamento, como também forjar o culpado da ligação fraudulenta, fazendo com que o coitado pague o pato (e a conta).

Guru:
O supra-sumo dos *Hackers*.

Agora, fora desses grupos acima, temos inúmeras categorias de "não-*Hackers*", onde se enquadram a maioria dos pretendentes a *Hacker*, e a cada dia, surgem novos termos para designá-los. Temos como principais:

Lamers:
Lamer é aquele que deseja aprender sobre *Hackers*, e está sempre a fazer perguntas a toda a gente. Os *Hackers*, ou qualquer outra categoria, não gostam disso, e passam a insultá-los chamando-os *Lamer*. Ou seja, novato.

Wannabe:
É o principiante que aprendeu a usar algumas receitas de bolo (programas já prontos para descobrir códigos ou invadir sistemas).

Larva:
Este já está quase a tornar-se um *Hacker*. Já consegue desenvolver as suas próprias técnicas de como invadir sistemas.

Arackers:
Estes são os piores! Os "*Hackers*-de-araque" são a maioria absoluta no submundo cibernético. Algo em torno de 99,9%. Fingem ser os mais ousados e espertos utilizadores informáticos, planeiam ataques, fazem reuniões durante as madrugadas (ou pelo menos até à hora em que a mãe manda dormir), contam casos absurdamente fantasiosos, mas no final de contas não fazem mais do que fazer *download*s do *site* da Playboy ou jogar algum desses "killerware", resultando na mais engraçada espécie: a "odonto-*Hackers*" - "o *Hacker* da boca para fora".

Um outro detalhe que vale a pena lembrar é que: os "pseudo-*Hackers*" fazem questão de escrever de forma absolutamente ilegível, trocando letras por caracteres especiais que, segundo eles, são similares. Além disso, muitas palavras podem ser substituídas por outras com grafia um pouco diferente. Os *Lamers*, por exemplo, podem perfeitamente transformar-se em *Lamerz*, *Lammerz*, *Lamah*, e por aí fora...

Por incrível que pareça, a maioria das pessoas que acha que é *Hacker*, não é. E uma minoria, que obviamente jura não ter nenhum envolvimento com o *underground* da computação, são *Hackers* muito experientes mas raramente perigosos. Os *Hackers* perigosos ficam entre estes dois grupos, pois são experientes mas gostam de aparecer, o que dá a impressão de que são muitos, mas na verdade, muitos mesmo são só os artifícios utilizados por eles para descobrir novas maneiras de pendurar uma melancia no pescoço.

8. Vírus

O que é um Vírus?

Um Vírus é um programinha, com uma série de instruções "maldosas" para o seu computador executar. Em geral, ficam escondidos dentro da série de comandos de um programa maior. Mas eles não surgem do nada!

Os vírus ocultam-se em ficheiros executáveis, ou seja, em programascom as extensões *.EXE* ou *.COM*, ou de bibliotecas partilhadas, de extensão *.DLL* .

Quanto a ficheiros de dados, você pode abri-los sem medo! Assim, pode abrir tranquilamente os seus ficheiros de som (*.WAV*, *.MID*), imagem (*.BMP*, *.PCX*, *.GIF*, *.JPG*), vídeo (*.AVI*, *.MOV*) e os de texto que não contenham macros (*.TXT*, *.WRI*).

Para que o vírus faça alguma coisa, não basta você tê-lo no seu computador. Para que ele seja activado, passando a infectar o PC, é preciso executar o programa que o contém. E isto você só faz se quiser, mesmo que não seja de propósito. Ou seja, o vírus só é activado se você der a ordem para que o programa seja aberto, por ignorar o que ele traz de mal... Se eles não forem "abertos", ou seja, "executados", o vírus simplesmente fica inactivo, alojado, aguardando ser executado para infectar o computador.

Após infectar o computador, eles passam a atacar outros ficheiros. Se um destes ficheiros infectados for transferido para outro computador, este também vai passar a ter um vírus alojado, esperando o momento para infectá-lo, ou seja, quando for também executado. Daí o nome de vírus, pela sua capacidade de auto-replicação, parecida com a de um ser vivo.

Como é que os Vírus trabalham?

Vírus de disco

Os vírus de disco infectam o *BOOT-SECTOR*. Esta é a parte do disco responsável pela manutenção dos ficheiros. Da mesma forma que uma biblioteca precisa de um índice para saber onde se encontram os livros, um disco precisa ter uma tabela com o endereço dos dados armazenados. Qualquer operação de entrada e saída (carregamento ou gravação de um ficheiro, por exemplo), precisaria do uso dessa tabela. Gravar ou carregar um ficheiro numa disquete infectada possibilitaria a activação do vírus, que poderia infectar outras disquetes e o disco rígido.

Vírus de Ficheiro

Este infectam ficheiros executáveis ou de extensão *.SYS*, *.OVL*, *.MNU*, etc. Estes vírus copiam-se para o início ou fim do ficheiro. Dessa forma, ao chamar o programa X, o vírus activa-se, executa ou não outras tarefas e depois activa o verdadeiro programa.

Vírus Multi-partite

Infectam tanto a disquete quanto os ficheiros executáveis. São extremamente sofisticados.

Vírus Tipo DIR-II

Alteram a tabela de ficheiros de forma a serem chamados antes do ficheiro programa. Nem são propriamente FILE-INFECTORS nem são realmente BOOT-INFECTORS e muito menos *multi-partites*.

Outras características e um pouco de história:

Porque é que os Vírus são escritos?

O chamado vírus de computador é um software que capta a atenção e estimula a curiosidade. Esta pergunta foi feita na convenção de *Hackers* e fabricantes de vírus na Argentina. A primeira resposta foi:

- *Because it's fun* (por diversão, entretenimento).

- Para estudar as possibilidades relativas ao estudo de vida artificial (de acordo com a frase de Stephen Hawkind "*Os vírus de computador são a primeira forma de vida feita pelo homem*"). Esta proposta é seguida por vários cientistas, incluindo um que pôs à disposição um vírus seu (inofensivo) para aqueles que estivessem interessados. Existe uma revista electrónica dedicada a isto, chamada Artificial Life e vários livros sobre o assunto.

- Para descobrir se são capazes de fazer isso ou para mostrarem para os colegas do que são capazes de fazer com um computador. Para testar os seus conhecimentos de computação.

- Por frustração ou desejo de vingança. Muitos autores de vírus são adolescentes.

- Curiosidade. Algo muito forte, mesmo para aqueles que têm poucos conhecimentos de informática. Uma das melhores formas de se aprender sobre vírus é "criando" um.

- Para punir aqueles que copiam programas de computador sem pagar direitos de autor.

- Para conseguir fama.

- Fins militares. Falou-se sobre isso na guerra do golfo, para esconder o uso de uma outra arma de "atrapalhamento" do sistema de computadores do inimigo. Ainda assim, os vírus para uso militar são uma possibilidade.

O que é um Vírus de Macro?

Recentemente, vem-se espalhando uma nova espécie de vírus, que hoje já corresponde a mais de 50% do total das infecções. São os famosos "vírus de macro".

Uma Macro é uma série de rotinas personalizadas para serem feitas automaticamente no Word, ou no Excel, ou qualquer outro programa que suporte VBA (Visual Basic for Applications), a linguagem usada nas macros. Os vírus de macro mais comuns são os do Word, por ser o programa mais difundido.

Você pode criar uma macro pra acrescentar um cabeçalho automaticamente assim que clica num botão da barra de ferramentas, ou para abrir o Painel de Controlo apenas com uma combinação de teclas, ou ainda para retirar todas as cedilhas, acentos, etc. de um texto. A macro é quase um programa, interno a outro programa.

O vírus de macro é um vírus feito na linguagem das macros, para funcionar dentro do programa ao qual está ligado. Ao abrir um documento de Word (*.DOC*) infectado com um vírus de macro, o vírus é activado, gravando sobre o ficheiro *NORMAL.DOT* (modelo geral dos ficheiros do Word) e criando macros que substituem boa parte dos comandos normais do Word.

A partir daí, quando você estiver a usar o Word vai começar a verificar os sintomas mais diversos, dependendo do vírus que tiver apanhado. Se verificar algum dos abaixo referidos, provavelmente o seu computador já estará infectado:

- quando tenta guardar um ficheiro, ele guarda com a extensão *.DOT* em vez de *.DOC*;

- todos os ficheiros do Word são gravados assim que você o fecha, como *Doc1.doc*, ou *Doc2.doc*, e assim por diante, sem sequer perguntar se quer guardá-los ou não;

- uma mensagenzinha fica a correr pelo rodapé da janela do Word;

- aparecem palavras sem que você as digite e imediatamente desaparecem;

- a impressora pára sem explicação;

- o computador fica a "trabalhar" (ampulheta) sem que você peça para ele fazer algo;

- retira dos menus todas as menções a macro, de forma que você fica impedido de manipular as macros para retirar o vírus;

- todas as macros personalizadas que você tenha criado antes são perdidas.

Uma vez infectado o ficheiro *NORMAL.DOT*, todos os outros ficheiros que forem abertos no Word a partir de então serão infectados. Se você enviar um ficheiro infectado para alguém, por disquete ou e-mail, ele pode infectar o computador do destinatário, se ele o receber e o abrir no Word, e o ciclo recomeça.

Os vírus de macro não estão escondidos na forma de um ficheiro executável (*.EXE*, *.COM*, *.DLL*), mas em inocentes documentos do Word (*.DOC*) ou numa folha do Excel (*.XLS*). Trata-se de uma verdadeira revolução dos vírus. E aí está a causa da facilidade com que eles se propagam.

As macros transformaram-se em verdadeiras armas postas à disposição de quem quer fazer um vírus. Ninguém imagina que um texto que a namorada escreveu ou uma folha de cálculo que um colega de trabalho mandou possa estar infectado. E a pessoa que lhe enviou o ficheiro com o vírus pode nem saber (e geralmente não sabe) da infecção...

Ainda assim é bom frisar: mesmo os vírus de macro só infectam o seu computador se você abrir o ficheiro que o contém. Não basta receber o ficheiro infectado, seja por que meio for - é necessário abri-lo para que o vírus seja activado.

Como criar um Vírus de Macro?

Enquanto que criadores de vírus concentraram-se em código que funcionasse ao nível de sistema operativo, eles, no entanto, negligenciaram as aplicações. Muitas aplicações de negócios, tais como folhas de cálculo, processadores de texto e bases de dados vêm com poderosas linguagens de macro. Muitas aplicações têm a habilidade de auto-executar macros. Essa combinação fornece um sério perigo para utilizadores de computadores que pensavam que ficheiros de dados não criavam problemas ao seu sistema. Quando nos refererimos a um vírus de macro

utilizaremos a sua sigla DMV (*document macro vírus*) para descrever esse tipo de código. Algumas características de um DMV incluem:

- Um DMV é escrito na linguagem macro de uma aplicação. Ele explora a habilidade da aplicação para automaticamente executar a macro em algum evento, tal como a abertura ou fecho de um documento. Uma vez que esse evento ocorre num documento que possui o DMV, o vírus espalha-se (ou algum tipo de cavalo de tróia é executado). A menos que um vírus convencional ou cavalo de tróia esteja no código executável, o DMV usa a sua aplicação criadora como agente para executar o código.

- Os DMVs são extremamente simples de criar. Muitas linguagens macros são uma modificação do BASIC, o qual é muito mais fácil de programar do que em linguagem Assembly preferida por muitos escritores de vírus. Como muito macros suportam a capacidade de chamar rotinas externas (tal como funções em ficheiros *.DLL*), a linguagem de macro pode facilmente se estender para criar vírus sofisticados.

- De uma forma simplificada, os DMVs tendem a ser feitos para uma aplicação somente da sua natureza. Isso significa que o vírus apenas infecta documentos com o mesmo tipo de dado, por exemplo, todos os documentos para o Microsoft Word for Windows. Muitas linguagens de macro não são compatíveis na passagem de uma aplicação para outra (por exemplo, um documento Word DMV que foi importado pelo Ami Pro, pode não passar o vírus). Uma excepção pode ser a linguagem Microsoft's Common Macro, Visual Basic for Applications. É um DMV avançado que pode ser escrito com VBA que se pode mover de uma aplicação para outra.

- Uma vez que um DMV é específico para cada aplicação, é teoricamente possível que um documento possa passar de uma plataforma para outra (i.e., sistemas baseados em Intel com Windows, para Motorola/Power PC em sistemas Macintosh). Isso faz com que os DMVs sejam diferentes dos vírus normais, que tendem a ser específicos para uma dada plataforma devido à natureza da sua codificação.

- Obviamente, existe uma numerosa quantidade de riscos de segurança e privacidade que o utilizador corre quando sem saber usa um documento que possui um DMV. Esses são limitados apenas pela imaginação da pessoa que criou o DMV. Algumas acções maliciosas que são relativamente fáceis de implementar incluem:

1. Infectar o seu computador com um vírus (obviamente).
2. Apagar ficheiros de seu disco rígido.
3. Renomear ficheiros existentes.

4. Copiar ficheiros pessoais do seu disco rígido para um local da rede onde eles podem ser recuperados mais tarde por outra pessoa.
5. Enviar ficheiros sensíveis do seu disco rígido para um endereço de e-mail via MAPI (Windows).

É importante notar que esses riscos não são exclusivos do Word for Windows. Qualquer aplicação que suporta macros automáticos é um perigo potencial.

Tipos de Vírus de Macro

O Word possui um ficheiro chamado "*normal.dot*" onde estão todas as configurações por defeito do Word. Se por algum motivo este ficheiro for eliminado, o Word cria automaticamente outro quando for inicializado.

Níveis de vírus de macro:

Nível 1 - Apenas uma brincadeira;
Nível 2 - Apenas uma brincadeira de mau gosto;
Nível 3 - Não é apenas uma brincadeira.

Primeiro você precisa criar uma macro. Siga os seguintes passos:

Entre no Word, feche a janela do documento, não deixe nenhum documento aberto (activo), clique em Ficheiro (File) e depois Macro, coloque no nome da macro "AutoExec" (obrigatório). Esta macro será inicializada todas as vezes que o Word for iniciado. Depois clique em 'Criar', elimine as duas linhas que tiver lá (Sub MAIN e End Sub) e copie a rotina que tem abaixo.

ps: existem outras formas/meios para criar uma macro, mas esta é mais simples.

Nível 1

O nível 1 serve para você mostrar que sabe muito de Word.

Cada vez que o utilizador inicia o Word receberá uma mensagem, de alerta ou de qualquer outra coisa que sair da sua cabeça. Veja o exemplo a seguir.