Autoria: Silvio Ferreira

Finalidade: educativa e comunitária

(Extensão UniCV)

Essencial saber

Já fiz muita manutenção em computadores. Um dos grandes problemas que técnicos em manutenção enfrentam são os vírus. Não há lugar que não se ouve falar sobre vírus. A cada dia que passa vários ou centenas de novos vírus surgem, se espalhando através de diversos meios e afetando uma grande quantidade de computadores, celulares (entre outros), copiando ou apagando dados, alterando informações e por aí vai. E para tentar eliminar esses vírus surgem novos antivírus, e novas atualizações de vacinas.

Nos tempos atuais é exigido muito mais que um antivírus instalado no sistema. Por isso vamos aprender como evitar que vírus venham a causar problemas em computadores, celulares, tablets (entre outros), como eles surgem, como eles agem, como se multiplicam.

"Em muitas empresas, a base de dados contidas em seus servidores é o motivo delas existirem..."

Em muitas empresas, a base de dados contidas em seus servidores é o motivo delas existirem, e se a base de dados é destruída, a empresa pode até não ser destruída, mas pode ter um prejuízo enorme.

Quem trabalha com manutenção de redes e/ou computadores sabe que a missão de um técnico dos novos tempos não é só montar computadores ou prestar suporte técnico. Mas preservar para que os dados que lá estão tenham o máximo de segurança possível.

Ao final deste capítulo coloquei alguns exemplos de códigos de vírus apenas por motivos didáticos, para que todos possam compreender melhor o funcionamento de alguns tipos de vírus para que, dessa forma, saibam como combatê-los. Uma pessoa preparada saberá eliminar os vírus sem problemas, saberá que eles não são tão perigosos como muitos afirmam, como se eles fossem seres capazes de decidir por conta própria o que irão fazer com o computador

infectado. Não há mágica no que fazem, eles apenas se aproveitam de falhas na segurança do sistema operacional, falhas na segurança dos softwares usados no sistema e se aproveitam das piores falhas que existe: a humana.

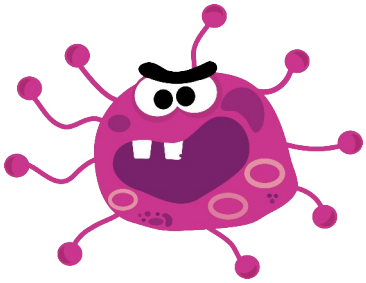
Se um HD de um computador é formatado, não foi porque criaram um vírus com “poderes” malignos, e sim que criaram um vírus capaz de enganar o homem, como os famosos trojans que exibem uma charge enquanto prepara o sistema para ser formatado na próxima vez que iniciar.

Um vírus pode ser feito usando o que há de mais tecnológico, porém só irá infectar o sistema da vítima se ela não estiver preparada.

Não somente os vírus são uma ameaça, mas também os criadores dos vírus, sejam eles hackers ou não.

Falar sobre hackers para muitos ainda é um tabu ou besteira, para outros, isso é pura indeliquência.

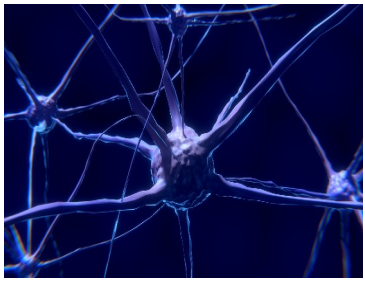
A grande verdade é que hacker é associado por muitos como aquele que invade sistemas, que faz vírus entre outras coisas. Se isso é ser hacker, então estamos condenados, porque qualquer criança de 12 anos pode ir na livraria/banca (ou através da internet) mais próxima e comprar um livro contendo um DVD demostrando como fazer vírus, invadir sistemas e trazem até todos os programas necessário e muita vezes códigos de vírus prontos.



É lógico que devemos nos prevenir (não podemos entrar em qualquer site que encontrar e digitar o número do meu cartão de crédito), mas também não há motivo para pânico.

Mais à frente, neste livro, ensino como saber se um site é seguro e quando é totalmente inseguro.

O que são os Vírus?



Vírus de computador são programas ou rotinas de programação dentro de outro programa, que ao infectar (se instalarem) um sistema irá alterar o seu funcionamento normal.

Essa alteração pode ser de incontáveis formas (dependerá único e exclusivamente da imaginação de seu criador), como sistema ficar mais lento, travar, reiniciar do nada, imprimir caracteres que não foram digitados, abrir milhares de janelas de forma descontrolada tendo como única alternativa resetar o computador, apagar arquivos, exibir mensagens na tela (mensagens que podem ser engraçadas ou até mesmos grosseiras, racistas, etc), alterar o setor de boot, formatar o HD, etc.

Os vírus são descritos como “pragas” destrutivas, que irá causar um evento negativo ao funcionamento sistema. Mas saiba que nem sempre um vírus é feito para destruir arquivos. Por exemplo: imagine um programa que esteja instalado em seu sistema, que monitora tudo que está sendo digitado no teclado e copia tudo que você digitar.

Mas vamos um pouco mais longe: imagine agora que ao invés desse programa copiar tudo que você digitar, ele copia apenas coisas relacionada com “senha”, “pass”, “password”, “key”, “nome”, “tel”, “telefone”, “end”, “endereço”, “CPF”, etc. Ele não destrói nada, mas é um vírus.

E quando por exemplo, você se conectar na internet, esse programa poderá enviar essas informações para algum e-mail pré-determinado, por exemplo.

Tudo isso é possível simplesmente porque o vírus nada mais é do que um "programinha", ou seja, um software que tem um código, e que pode fazer qualquer coisa que outros programas fazem, obviamente cada vírus só irá fazer aquilo que estiver programado em seu código.

Os vírus podem ser escritos utilizando variadas linguagens. Pode ser ser escritos, por exemplo, em Assembly, pois é a linguagem "nativa" do computador, o que gera menos códigos para executar alguma tarefa, além de ficarem com tamanhos pequenos (de 20 bytes até aproximadamente 2MB por exemplo).

Outras linguagens usadas podem ser o Pascal, C ou Basic. Alguns Pseudo Vírus são feitos usando comandos do DOS em arquivos de lot (BAT) ou até scripts (java scripts) em home pages.

Um grande mito é de os vírus poderiam danificar (quebrar) hardware, o que é mentira.

Hardware é a parte física, vírus é software, é parte lógica. Para danificar um hardware (literalmente) seria necessário provocar um super aquecimento, provocar um curto circuito, etc. Alguns vírus, como o *chernobyl,* conseguiu reescrever a gravação da BIOS em alguns modelos de placas-mãe (entenda isso, não são em todas), apagando-a. Nesse caso, o vírus conseguiu inutilizá-la temporariamente, mas não quebrá-la, ela pode ser recuperada usando técnicas apropriadas.

Essas “pragas” virtuais tem diversas classificações, diferentes nomes e tipos. Veja a seguir os mais conhecidos.

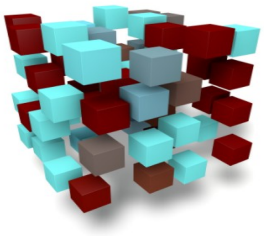
Malware

São softwares/códigos criados com a intenção de gerar algum dano ao sistema (e automaticamente aos usuários), redes ou servidores. Malware significa software malicioso.

Os malwares são uma denominação, uma forma de classificar. Spyware, Keylogger, Screenlogger, Adware, Backdoor, Cavalo de Tróia, e todos a seguir, todos são malwares.

E portanto, a forma de agir e as consequências dessas ações são variadas.

Vírus



Os vírus *precisam de um arquivo* (“hospedeiro”), de outro programa para que eles possam agir. Eles se ocultam em programas executáveis (com extensão .EXE, .COM por exemplo) ou bibliotecas

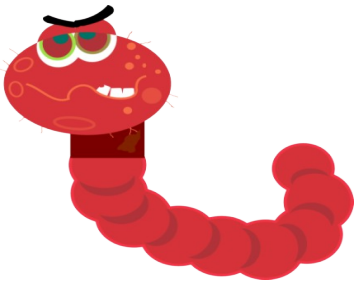
compartilhadas (com extensão .DLL). Por causa dessa característica, são capazes também de infectar outros arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão .SYS, .OVL, .OVY, .PRG, .MNU, .BIN ou .DRV.

São muito mais rápidos que os worms e atingem um grande número de dados rapidamente. O vírus de macro (um tipo de vírus) por exemplo, se espalham através de documentos Word ou Excel, que são os aplicativos mais usados em computadores.

Para que os vírus façam alguma coisa ao sistema, ele deve ser ativado pelo usuário. Isso é feito quando ativamos o programa que contém o código viral. Em outras palavras, o vírus é ativado quando abrimos o programa que o contém. Caso esse programa não seja ativado pelo usuário, o vírus não conseguirá fazer nada ao sistema, ele ficará apenas alojado.

Uma vez ativado, ou seja, o usuário executou o programa, o vírus passará a infectar outros arquivos. Aí começa a replicação: se o arquivo infectado for copiado para outro sistema "limpo", ele estará lá novamente esperando para ser ativado pelo usuário. Se o usuário ativar o arquivo, o sistema também será infectado.

Worms



Fazendo uma recapitulação sobre os vírus, dissemos anteriormente que eles (os vírus) precisam de um arquivo para agirem, ou seja, necessitam de um "hospedeiro".

No caso dos worms (ou vermes, em Português), eles *não precisam de um "hospedeiro"* para agirem, são independentes.

O código do worm não necessita de outro arquivo para executar as funções que lhes foram programadas.

O worm consegue se auto duplicar, fazer cópias de si mesmo, e isso é feito sem necessitar de interferência humana.

Outra característica do worm é a capacidade de enviar essas cópias através de e-mails (Vírus-mail).

Os worms também podem tentar desativar Anti-vírus e Firewall, gerar executáveis (muitas vezes pode ser trojans), gravar rotinas no registro, entre outras coisas.

Trojans

O Trojan horse (Cavalo de Tróia) também são programas que não necessitam de um "hospedeiro", sendo que eles tem uma particularidade: se disfarçam de um programa "inofensivo", mas que tem por trás um código malicioso.

Daí o seu nome ser Cavalo de Tróia, uma analogia com a mitologia grega do livro "A Odisseia", onde um grande cavalo de madeira é deixado nas portas de Troia. Os troianos imaginando que se tratava

de um presente, levaram o cavalo para o centro da cidade, mas, o que eles não imaginavam é que dentro desse cavalo haviam soldados gregos, que aproveitaram a situação e os atacaram.

Os Trojans horse não se duplicam, mas são eles que podem, por exemplo, copiar informações que são digitadas pelo usuário e incluir *backdoors* no computador da vítima.

Os backdoors são programas que garantirão que o hacker consiga retorno em um sistema que ele invadiu, ou seja, ele abre "uma porta dos fundos", como muitos dizem.

Os trojans podem chegar em um sistema através de inúmeros formas que os "disfarcem", fazendo os parecerem com programas benéficos. Exemplo: aplicativos muito requisitados, como aplicativos para retirar bugs do sistema, retirar senhas, que dizem acelerar o computador ou até mesmo jogos e protetores de tela. Alguns exibem algum tipo de animação ou se "disfarçam" de imagens BMP ou JPG por exemplo.

Um trojan que venha a se "disfarçar" de uma imagem, tipo jpg por exemplo, poderá ter o nome da seguinte forma: um_nome_qualquer.jpg.exe.

Uma configuração do Windows permite que não seja exibido as extensões dos arquivos (o que é sem dúvida uma falha), dessa forma o arquivo aparecerá como: um_nome_qualquer.jpg (a extensão EXE fica oculta), o que mais cedo ou mais tarde acaba pegando um desavisado.

Alguns trojans se disfarçam de jogos famosos. Só para citar como exemplo vou citar um caso real de trojan que infectou computadores

no passado: o trojan *Fintas.C*, que chegava por e-mail com um anexo chamado FF8.EXE e a mensagem: “the cool game about Final Fanstasy VIII :)”. O campo Assunto geralmente vem vazio.

Trata-se de um disfarce de uma prévia do famoso jogo Final Fantasy 8 de 1999. Quando o usuário executava o arquivo em anexo, ele substituia o AUTOEXEC.BAT incluindo comandos para que o Disco Rígido fosse formatado na próxima vez que o computador era iniciado.

Ele formatava não só o disco C:\, mas sim todos os discos do computador que ele encontrava , indo de C:\ à Z:\..

Para se espalhar pela internet ele usava a lista de e-mails do Outlook Express dos computadores contaminados.

Ransomware

Esse é um dos piores tipos de vírus a circular nos últimos anos. Após a contaminação, ele retem arquivos e bancos de dados e exigem o pagamento de algum valor, ou compra de algum produto, para a liberação do que foi sequestrado. E não há garantia dessa “liberação”.

Os ataques feitos por Ransomware são complexos. Envolvem um complexo ataque por engenharia social, no geral através de e-mails.

E-mails com iscas são enviados para uma empresa alvo. E para que eles consigam êxito nesse ataque é usado, geralmente, algum sistema corporativo (que pode inclusive ter sido invadido com antecedência) para dar veracidade ao conteúdo do e-mail. E o conteúdo do e-mail tem que incentivar o download de algum arquivo infectado.

Se o arquivo for aberto, o vírus entra no sistema. Ele faz uma varredura a procura de brechas, de falhas, que vão permitir sua entrada na base de dados do sistema e ao arquivos.

Assim que ele conclui essa etapa, todos os arquivos, banco de dados e tudo que for possível bloquear, são criptografadas. O acesso ao sistema é bloqueado.

A partir daí mensagens exigindo um pagamento para a liberação do sistema começa a aparecer, ou, os próprios cibercriminosos entram em contato com a empresa exigindo o pagamento. Esse pagamento geralmente é em bitcoin. E como já disse, não há garantia dessa "liberação" do sistema após o pagamento.

E se a empresa não fizer o pagamento? Caso a empresa tenha um backup seguro, desconectado do sistema invadido, ela pode simplesmente zerar toda a plataforma invadida. Formatar tudo, apagar todos os e-mails e todas as possibilidades de arquivos infectados. E fazer a restauração de todo o sistema, aplicando politicas fortes para impedir uma nova invasão. Mesmo assim é um processo arriscado porque os cibercriminosos podem acionar comandos no sistema invadido que podem apagar os arquivos permanentemente.

Portanto, esses ataques podem gerar grandes prejuízos financeiros e perda de dados críticos em uma empresa.

Autorun

Esse tipo de vírus tem como principal veículo de transmissão os pen drives, HDs externos, CDs e DVDs. O nome faz referência ao arquivo que irá ativar esse vírus: AutoRun.Inf.

O arquivo AutoRun.Inf é facilmente editável no bloco de notas. Ele não é o vírus em si, mas através dele é possível inserir comandos que irão abrir e ativar outros arquivos, que pode ser um vírus por exemplo.
Essa função AutoRun.Inf não foi criada com fins maléficos. Ela foi criada lá no Windows 95, para ser usada em CDs (e nos disquetes que ainda eram muitos usados na época) e tinha como objetivo facilitar a vida dos usuários.

Quando o CD era colocado na unidade leitora, os comandos que estavam no AutoRun.Inf eram automaticamente processados. E algum aplicativo que estava na linha de comando do AutoRun.Inf era executado.

Dessa forma passou a ser possível, por exemplo, ser aberta uma interface visual para apresentar todo o conteúdo do CD, ou, abrir automaticamente o programa de instalação de algum driver.

Mas é óbvio que cibercriminosos enxergaram uma brecha nisso aí. Se existe a possibilidade de abrir um programa automaticamente ao

colocar a mídia no computador, vírus também podem ser executados. Vírus são programas.

Isso facilitou inclusive o uso da engenharia social (mais à frente descrevo o que é isso).

Imagine a cena:

- V*ocê a caminho da sua empresa e ao chegar, encontra na calçada um DVD ou Pen drive escrito: "Nome da sua empresa" + "Lista de demissão" + Data mais atual (Exemplo: JK Veículos, Lista de Demissão Agosto de 2022).*

O que faria boa dos funcionários que encontrassem esse DVD ou pen drive? Correriam e colocariam ele em um computador o mais rápido possível para ver quais os nomes estão na tal lista. Sem saber que isso foi deixado ali por um cibercriminoso.

Kilim

São um tipo de vírus que causam problemas especificamente em redes sociais. Atualmente as redes sociais estão em enorme ascensão, por isso, é preciso ter cuidado ao perceber certos sintomas.

Dois dos principais sintomas de uma possível contaminação por esse tipo de vírus é a criação de posts indesejado e falsas curtidas. Eles se disfarçam de alguma extensão original, enganando o usuário que

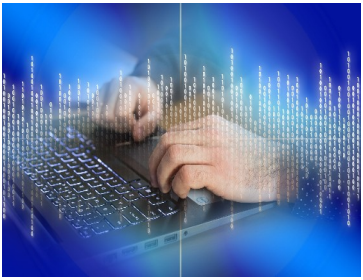
acaba o instalando no navegador. Uma vez instalado ele rouba informações de perfis em redes sociais e geram diversos problemas como os já citados.

Majava

O Majava é um tipo de vírus criado para infectar a plataforma Java. Esse vírus é um problema maior para que trabalha com programação e utiliza essa plataforma.

Ao infectar a plataforma ele consegue ter acesso aos dados da máquina e até dar acesso ao cibercriminoso ao sistema.

Keylogger



Keylogger significa Registrador de teclado. E a primeira coisa que você precisa saber é que ele por si só (e originalmente) não é um vírus. Mesmo que você leia em outro local ou veja algum vídeo dizendo o contrário.

Os “Keyloggers” são programas cuja finalidade é monitorar a atividade de uma pessoa em algum sistema. Por exemplo: um pai que

quer saber o que o filho anda "aprontando". Ele registra tudo que é digitado no teclado e pode registrar até o que for apontado/clicado com o mouse (apesar que essa função é do Screenlogger).

Você pode fazer o download de algum programa Keylogger na internet sem problema algum. Pesquise no Google e verá: download de Keylogger free.

É uma ferramenta extremamente útil que pode ser usada, por exemplo, por pais que querem e/ou precisam monitorar seus filhos (uma criança por exemplo). Imagine uma situação onde há a suspeita de um filho estar sofrendo algum tipo de abuso. Percebe como essa ferramenta pode ser útil para investigar e levantar provas?

O problema é que cibercriminosos perceberam a utilidade extremante poderosa dessa ferramenta. Afinal de contas ele registra tudo que é digitado, incluindo senhas, dados de cartão de crédito, etc. Tudo mesmo. E criam seus próprios Keyloggers que podem chegar até o sistema da vítima de várias formas, iscas digitais e podem ser instalados através de outros vírus (como o trojan por exemplo).

Screenlogger

É um Spyware que captura a posição do cursor do mouse quando ele é clicado. Cada vez que o usuário clica com o mouse ele captura uma imagem dessa região.

Spyware

Aproveito a oportunidade de ter explicado sobre os keyloggers e Screenlogger, trago-lhe agora informações sobre os spywares. Isso porque o keylogger e Screenlogger são spywares. Confuso? Calma que você entenderá agora.

Spywares são vírus espiões. Eles atacam computadores, e quaisquer outros dispositivos que eles consigam se instalar, para coletar informações sobre os usuários. Eles podem coletar praticamente qualquer tipo de informação: o que for digitado no teclado, o que for clicado com o mouse, históricos de navegação e por aí vai.

Existem tipos diferentes de spywares. Esses tipos são classificados de acordo com aquilo que ele consegue fazer:

- **Keyloggers/Screenlogger:** como já expliquei, eles capturam tudo que é digitado no teclado e captura de telas daquilo que foi clicado (e até captura de tela cheia) e enviam essas informações para seus criadores (os cibercriminosos). Mas, eles podem fazer muito mais: podem capturar toda a atividade do sistema, históricos de pesquisa, diálogos em chats, nomes de usuários e senhas;
- **Programas de Interceptação de senhas:** capturam senhas, nomes de usuários, inclusive as salvas em navegadores e outros sistemas;
- **Banking Trojans:** o alvo desses aqui são instituições financeiras, corretoras ou carteiras digitais;

- **Infostealers:** eles usas a funcionalidade de keylogger para roubar suas informações sigilosas, tais como número de cartões de crédito, senhas, etc.

Blended Threats

São conhecidos por Ameaças compostas. É um tipo de virus que possui uma combinação de vários códigos maliciosos. Isso permite que ele consiga agir como se fosse um grande conjunto de vírus.

Um Blended Threats é traduzido literalmente por Ameaças combinadas ou Ameaças compostas. Ele possui características de vários outros tipos de vírus. Ele pode, por exemplo, capturar dados dos usuários, fazer cópias de si mesmo, instalar outros vírus, etc.

Adware

São softwares maliciosos que, uma vez instalados, passam a exibir anúncios indesejados. Muitas vezes exibem uma grande quantidade de anúncios de todos os tipos, sem restrição. Podem exibir, inclusive, pornografias e demais nichos adultos.

Backdoor

Backdoor em português é Porta dos fundos. Isso porque se formos fazer uma analogia com uma casa, imagine que a entrada principal é a porta da frente, ou porta da sala, ou ainda, porta do saguão de entrada.

Todas as pessoas entram por essa porta principal. O Backdoor, no exemplo hipotético da casa, seria justamente a portas dos fundos. Ela é a porta "não oficial". É a porta que não é usada pela maioria, ela é usada somente pelos administradores do imóvel. Somente esses administradores é que sabem dessa porta.

Em um sistema de computação, Backdoor é uma porta usada somente pelos administradores do sistema. Somente eles podem acessar essa porta para fazer alguma manutenção, solucionar problemas, etc.

Esse Backdoor pode ser um programa à parte (que dá acesso ao programa principal), uma parte oculta do programa (que somente os administradores sabem como acessar) ou de sistemas operacionais.

Portanto, o Backdoor é um recurso que mantêm acesso aberto a um determinado sistema de computador. Originalmente é um recurso legítimo, porém, que pode ser explorado por cibercriminosos.

Cibercriminosos podem buscar, descobrir e explorar esses Backdoors e, muito além disso, podem criar seus próprios Backdoors em um sistema invadido. Dessa forma, eles podem entrar no sistema quando quiserem, de forma remota, podem modificar e excluir arquivos, executar programas, enviar e-mails a partir do seu computador, instalar outros programas e vírus.

Bots

Os bots (robôs) são programas criados para executar funções específicas automaticamente. Foram desenvolvidos com fins legítimos, mas, como sempre cibercriminosos perceberam neles mais uma possibilidade de invasão e criaram suas próprias versões, onde passam a ser um tipo de malware. Uma vez instalado em um sistema, ele passa a executar funções específicas. E isso sem o consentimento do usuário.

Um bot legítimo pode, por exemplo, ser criado para responder às dúvidas mais comuns de um usuário, como se fosse uma "pessoa de verdade", e até encaminhar ele para determinadas áreas de atendimento de acordo com as respostas dadas.

Um bot malware pode, por exemplo, infectar diversos computadores criando uma botnet (rede de robôs). A partir daí ele consegue

gerenciar essa botnet, ter acesso a dados sigilosos, distribuir spam, espionar as vítimas, iniciar ataques DDoS, e por aí vai.

DdoS são siglas de Denial of Service, que em português é ataque de negação de serviço. Não se trata de uma invasão, mas sim de provocar uma invalidação por sobrecarga. Veja um exemplo: uma Botnet pode ser usada para criar milhares de acesso simultâneos a um servidor, gerando sobrecarga. O resultado disso pode ser o servidor ficar muito lento, apresentar indisponibilidade de serviços e até ficar totalmente offline.

Outras classificações de vírus

Os vírus são classificados ainda quanto ao modo que eles operam, seu funcionamento e capacidades adicionais. São eles: vírus de boot, Vírus Multipartite/ Vírus Múltiplos, vírus de macro, vírus polifómicos, vírus stealth, vírus-mail e duas variações de não-vírus, que são eles: pseudos vírus e Hoax Vírus.

Vírus de arquivo

Como já explicamos, são aqueles que infectam arquivos do Disco Rígido em especial, arquivos executáveis (com extensão .EXE ou .COM por exemplo).

Vírus de boot

Conhecido também por vírus de MBR, eles se instalam no setor de inicialização do Disco Rígido. Na verdade eles conseguem se instalar em setores de inicialização de qualquer meio de armazenamento, como os disquetes e CDs. Disquetes de boot contaminados representam um grande risco, uma vez que inseridos podem contaminar o setor de boot do Disco Rígido. Caso a FAT seja corrompida, o acesso a arquivos e diretórios será perdido.

Vírus Multipartite / Vírus Múltiplos

São vírus capazes de infectar tanto o setor de boot (MBR) quanto arquivos de programas. São uma combinação do vírus de boot com os Vírus de arquivo, fazendo com que eles se propaguem com muito mais rapidez.

Vírus de macro

Os vírus de macro começaram a surgir por volta de 1995 e se espalharam a uma velocidade espantosa. Como dissemos no início desse capítulo, os vírus de macro se espalham rapidamente graças a popularidade dos programas Word e Excel da Microsoft.

Um dos primeiros vírus de macro que se tem notícia foi o CONCEPT, que infectaram documentos do Microsoft Word (versões 6.x, 7.x e 97), nas plataformas Windows e Macintosh. Surgiram mais tarde o Concept (F, G, J, L e M), todos baseados no Concept. Só para se ter uma idéia o Concept.F trocava as letras dos documentos do Word infectados, substituindo "." por ",", "a" por "e" e "and" por "not". Além disso os vírus Concept.F, G e J exibem no 16° dia de cada mês a seguinte mensagem na tela do monitor:

- / Parasite Virus 1.0 / X / Your computer is infected with the Parasite / Virus, version 1.0! / OK

Vírus Residente

Quando executados pelo usuário esse vírus é colocado na memória e a parti daí passa a infectar outros arquivos que forem abertos, ampliando cada vez mais a quantidade de arquivos contaminados.

Vírus polifómicos/ Vírus criptografados

São vírus com capacidade de enganar os antivírus. Esses vírus são conhecidos também por mutantes. Eles alteram o seu tamanho e formato de código, o que poderá dificultar (ou até impossibilitar) que o antivírus o detecte.

Para que o vírus seja polifórmico, o seu código deve ser randômico. Dessa forma, o vírus fará copias de si mesmo porém com formato de códigos diferentes, e como normalmente os antivírus usam como referencia pedaços do código virótico, ele será enganado.

Outra técnica usada é a criptografia do código viral com uma chave não constante com conjuntos aleatórios de comandos de descriptografia.

Geralmente, envolve um laço ("loop") no qual o vírus é encriptado ou desencriptado, toda a vez que é executado.

Os vírus polifórmicos foram divididos em seis níveis de acordo com o seu poliformismo:

Nível	Descrição
1	Compostos por descriptadores com código constante, que escolhe um deles durante a infecção. Conhecidos também por: "semipolimórficos" ou "oligomórficos".
2	Composto por descriptador com uma ou diversas instruções constantes e o restante pode ser modificado.
3	Compostos por um descriptador com funções não utilizadas como NOP, STI, etc.
4	Compostos por um descriptador que utiliza instruções intercambiáveis e modifica sua ordem, mantendo o algoritmo de descriptação inalterado.
5	Basicamente o algoritmo de descriptação é modificável e usa todas as técnicas mencionadas.
6	O código principal do vírus está sujeito a mudanças, é divido em blocos que são posicionados em ordem aleatória durante a infecção. Pode ser descriptografado.

Vírus Stealth

São os vírus “invisíveis”, são aqueles que usam algum tipo de técnica para se “esconder” dos antivírus e/ou do usuário. São portanto vírus difíceis de localizar tanto pelos antivírus quanto pelo usuário.

Os polifórmicos por exemplo mudam a sua forma e/ou usam criptografia. Os vírus de macros utilizam técnicas que impossibilitam que sejam encontrados como desabilitar ou redirecionar todos os comandos do Word ou excel (barra de ferramentas e menus) que possam exibir o seu código.

Vírus-mail

São vírus que se propagam anexados a E-mail. Geralmente são worms. Esse tipo de vírus funciona da seguinte forma: ao abrir o arquivo anexado ao E-mail, ele contaminará o PC fazendo com que todas as mensagens que forem enviadas pelo usuário, levarão junto o vírus anexado. O destinatário por receber um arquivo anexo de uma pessoa conhecida, muito provavelmente irá abrí-lo.

E para induzir a as vítimas a abrirem o arquivo anexo ao e-mail mais rapidamente, o vírus introduz no corpo do e-mail uma mensagem que faz parecer que o e-mail recebido é de alguém conhecido. Veja a seguir um exemplo de mensagem:

Olá, a quanto tempo! Eu me mudei dai para os Estados Unidos, e faz um tempo que perdemos o contato e consegui seu email através de uma amiga sua. Vamos fazer assim, eu vou lhe mandar meu álbum de fotos se você me reconhecer, me retorna o email. Quero ver se você ainda lembra de mim. :)

O vírus Worm.ExploreZip por exemplo envia a mensagem:

"Recebi seu e-mail e estarei respondendo assim que possível. Até lá, dê uma olhada no arquivo .zip atachado".

Se o arquivo anexo for aberto, o vírus modifica o arquivo WIN.INI e utiliza o programa de e-mail para se propagar. Além disso ele tenta apagar arquivos do Word, Excel e PowerPoint.

Pseudo vírus

Esse tipo de "não-vírus" causam na verdade um grande incômodo, perda de tempo e irritação. São feitos por pessoas com nenhum conhecimento em programação ou por pessoas que desejam apenas dar um susto em um amigo. Não se disseminam e nem contaminam outros arquivos, além disso só entram em ação quando são iniciados pelo usuário.

Só para exemplificar, técnicos mais antigos devem se lembrar de como era fácil criar arquivos no prompt de comando (ou no antigo MS-DOS) com comandos pré-definidos e em ordem exata de execução, linha a linha. Mais à frente você pode verificar um exemplo. Outra possibilidade é em java scripts.

Algumas páginas da internet tem o que seus criadores chamam de "ísca" ou "armadilha", que são links que desencadearão uma ação, que em alguns casos provocam uma desordem tamanha no sistema, que o que resta a fazer é resetar o PC. Colocaremos alguns exemplos de códigos de Pseudos vírus somente por motivos didáticos. Vejamos a seguir um exemplo de código que faz com que uma página da Internet seja aberta infinitamente:

```
<script language="Javascript">
Function ReloadBomb()
{
 history.go(0)
 window.setTimeout('ReloadBomb()',1)
}
</script>
```

Apesar desses tipos de códigos não necessariamente representarem um risco, parecerem muitas vezes até “bobos”, se uma pessoa entrar na página que contenha o código do exemplo 1, possivelmente terá que resetar o PC, não adiantando apertar a tecla ESC e muito menos tentar fechar as janelas que se abrem.

Existem diversos outros tipos de scripts que provocam os mais variados efeitos.

Já os “vírus” feitos com arquivos de lote do no prompt de comando (.BAT), como eu disse anteriormente, usam os comandos originados do MS-DOS, tais como:

- DEL
- FORMAT;
- DELTREE;
- COPY;
- Entre outros.

Em geral são feitos para uma finalidade bem específica e restrita, por exemplo: um arquivo .BAT com a linha C:\DEL *.exe.

Se esse arquivo for executado, ele apagará todos os arquivos com a extensão EXE que estiverem em C:\.

Apesar de parecerem inofensivos, podem formatar um Disco Rígido inteiro.

Vejamos no exemplo, um “vírus” feito em um arquivo BAT.

Exemplo 2: “Vírus” em arquivo BAT

```
:
@echo off
cls
echo Exemplo para o livro.
echo Responda a pergunta corretamente, ou seu HD sera formatado.
Echo O que significa a sigla T.U.J.F.D???
echo ----------------------------------------------------
Echo [1] Nao sei.
Echo [2] Eu desisto.
Echo [3] Nao tenho nada importante no HD mesmo!
choice /c123
echo ----------------------------------------------------
if errorlevel 3  dir
if errorlevel 2  cls
if errorlevel 1  vol
echo
echo
echo ----------------------------------------------------------
echo Isso e apenas um teste, seu HD nao foi formatado!
```

Esse “vírus” não faz nada a não ser fazer uma pergunta ao usuário. Ele não formata o Disco Rígido. Observe que há três alternativas de respostas:

- **Echo [1] Nao sei:** Escolhendo essa alternativa, o arquivo executa a linha “if errorlevel 1 vol”, ou seja, mostra o volume do Disco Rígido (através do comando vol);

- **Echo [2] Eu desisto.:** Escolhendo essa alternativa, o arquivo executa a linha “if errorlevel 2 cls”, ou seja, limpa a tela (através do comando CLS);

- **Echo [3] Nao tenho nada importante no HD mesmo!:** Escolhendo essa alternativa, o arquivo executa a linha "if errorlevel 3 dir", ou seja, mostra os diretórios do Disco Rígido (através do comando dir).

Nesse exemplo não é causado nada de grave. O problema começa quando pessoas mal intencionadas trocam os comandos *dir, cls e vol* por outros comandos como por exemplo o Deltree/Y, que exclui pastas e arquivos sem pedir confirmação do usuário. Esses sim podem ser perigosos e causarem sérios danos aos arquivos de um computador. Nem todo vírus feito com arquivos BAT será um Pseudos vírus.

Pode haver também a combinação de vírus perigosos como um worm, que instalam no computador da vítima comandos para formatar o Disco Rígido.

Hoax Vírus e Fake news

Na verdade não são vírus e sim boatos que se espalham pela Internet com o objetivo de provocar tumultos, desinformação, confusão ou fazer com que usuários menos experientes danifiquem os seus sistemas operacionais apagando arquivos importante.

Como realmente começaram a surgir no Brasil, se vieram de fora ou começaram por aqui mesmo é incerto dizer. Mas até alguns anos atrás isso era um problema típico nos EUA.

É importante entender, que apesar desse tipo se chamar Hoax Vírus (vírus boatos), ele não é um aplicativo, não é transportado por um "hospedeiro", não se multiplica automaticamente, portanto não são vírus.

Os Hoaxes e fake news se propagam através de sites, e-mails, redes sociais e aplicativos de mensagens instantâneas. Muitos podem fingir que são mensagens enviadas (inclusive com assinatura) por empresas oficiais (exemplo: IBM, Microsoft, Unicamp, etc).

Além disso, a cada dia, o número de Hoax aumenta, o que torna difícil distinguir o que é verdade do que é mentira.

Quer um exemplo clássico e que tenho certeza que você já ouviu falar? Sabe aqueles **quadrados coloridos que algumas caixas de leite possuem?** A um tempo atrás um **boato** se espalhou e deu milhares de views (e portanto, dinheiro) para criadores de conteúdo: segundo "fontes" dessas pessoas, aqueles quadradinhos coloridos significa que o leite foi reprocessado, ou seja, já entraram anteriormente no mercado, mas voltaram à indústria para serem tratados quimicamente e, então, foram devolvidos às prateleiras.

A loucura com esse boato foi tão grande, que diversas vezes eu presenciei no supermercado, bem ao meu lado, pessoas verificando caixa por caixa. Se tinha os quadradinhos coloridos, voltava para a prateleira.

Primeiro saiba que aqueles quadradinhos coloridos são simplesmente testes de cores para manter a qualidade da impressão da embalagem.

E segundo, e não menos importante, esses quadradinhos podem ser encontrados em outros tipos de embalagens (principalmente as cartonadas), e não somente em embalagem de leite.

Os criadores

Vírus não surgem do nada nos computadores, eles são escritos por alguém e colocados em circulação. O surgimento (a criação) de um vírus se dá de duas formas:

- **Intencional:** o criador desde o início queria fazer um vírus;
- **Acidental ou não- intencional:** apesar de parecer um absurdo que um vírus seja feito acidentalmente, imagine que um programador estava fazendo um aplicativo qualquer, descobre que ao inserir um determinado código ao seu aplicativo, este acabar reagindo de uma forma ao qual não era esperado, seja causando danos ao sistema ou não.

Mas quem pode fazer vírus? Ou melhor dizendo, quem consegue fazer vírus? Qualquer pessoa com um mínimo de tempo e uma grande disposição para aprender.

Essa reposta pode assustar em um primeiro momento, mas é a pura realidade. Com o avanço e a disseminação da Internet que temos atualmente, encontrar informações de como fazer não será o problema. Inclusive é possível encontrar livros ou revistas nas maioria das bancas ou livrarias com tudo que é necessário para uma pessoa sem experiência nenhuma fazer vírus. Ha vírus que são extremamente complexo de se fazer, outros são feitos com duas ou três linhas de comandos. Por isso a quantidade de vírus crescem aceleradamente.

Os motivos que podem levar uma pessoa a fazer um vírus são os mais variados possíveis. Pode ser por frustração, desejo de vingança, curiosidade, como forma de punir aqueles que usam programas de computadores sem pagar por direitos autorias, para roubar informações, crime, rebeldia (enquanto alguns picham muros, outros fazem vírus), etc.

É impossível determinar um motivo que justifiquem todos, mas algumas coisas são certas: praticar crimes, vandalismo e desejo de destruir. Muitos vírus foram feitos para simplesmente "aniquilarem" com o sistema operacional, formatando o Disco Rígido e junto com ele todas as informações que estavam guardadas.

A criação dos vírus são na maioria das vezes associadas aos Hackers, jovens com muito tempo livre e muita vontade de aprender mais e mais sobre computadores, em especial, a programação.

Hackers: mito ou realidade?

Mas o que são os Hackers, esses "seres" que ninguém vê, ou, quando vê é sendo presos acusados de crimes digitais.

A grande verdade é que um hacker de verdade nunca é preso, simplesmente porque ele não dá alarde de seus feitos e nem sai por aí dizendo que é um hacker (esse não é o objetivo dele).

O significado para o termo *Hacker de computadores* encontrado em qualquer livro sobre o assunto é um indivíduo que sabe muito sobre computadores, possui grande capacidade de análise, assimilação e compreensão. É hábil na programação e por isso não fica perdendo tempo tentando derrubar os outros da internet, o negócio dele é fazer programas novos, testar e corrigir falhas na segurança dos sistemas.

O que fica evidente é que foi criado uma espécie de “submundo”, de pessoas aficionadas por computadores, onde a palavra de ordem é o conhecimento.

Isso é levado tão a sério, que passam a levar uma rotina de vida quase que esotérica, estudando e aprendendo cada vez mais, principalmente novas linguagens de programação.

Algumas dessas pessoas acabam trabalhando para grandes empresas, na área de segurança, programação ou outra relacionada com informática. Esses são os verdadeiros hackers.

Mas outros acabam usando os seus conhecimentos para invadir sistemas, roubar senhas, desviar alguns centavos de contas bancárias, entre outras coisa erradas, e, muitos acabam, consequentemente atrás das grades. Esses são chamados de crakers.

Não há como fechar os olhos e fingir que eles não existem ou que isso é besteira. Realmente eles existem: pessoas que preferem trocar as “baladas” da noite por horas a fio em frente do computador.

E é preciso saber também que há um marketing exagerado sobre eles, atribuindo-lhes qualidades que muitas vezes não existem, como se eles tivesse controle de todos os computadores do mundo. Nem sempre um ataque hacker terá como ponto de partida um computador. Muitas vezes eles usam a engenharia social (leia o tópico a seguir).

Existe ainda uma divisão hierárquica que separa os indivíduos quanto ao seus conhecimentos. Somente com o objetivo de se fazer constar, vejamos o significado de alguns:

- **Hackers:** é um indivíduo que sabe muito sobre computadores, possui grande capacidade de análise, assimilação e compreensão. Prefere fazer novos programas, testar e corrigir falhas em sistemas;

- **Crakers:** Possui o mesmo conhecimento do hacker, com a diferença que para ele só invadir sistemas não basta. Eles precisam deixar um aviso que estiveram lá, através de mensagens ou até apagando arquivos;

- **Phreaker:** Fusão das palavras "freak, phone, free". É o especialista em telefonia

- **Lamer:** Novato. É aquele que aprendeu alguns truques, pegou algumas "receitas de bolo" (ferramentas que vão poupar-lhes seu trabalho intelectual, está relacionado com coisas prontas, já descobertas, algo fácil), e acha que é um hacker. Exatamente por saber pouco, corre o sério risco de ser preso.

Atualmente a palavra Hacker é usada de forma "genérica": quando você vê uma notícia sobre a prisão de um endivido relacionado com o que falamos aqui, são chamados pela mídia de hacker, e não cracker, phreaker ou lamer, sem distinção de Hacker ou Crakers, o que faz sentido, porque de forma resumida, Hacker de computador é aquele que é "fera" na informática, não importando se ele é o mocinho ou o vilão.

Engenharia social

Imagine a seguinte situação: você trabalha em uma grande empresa, e em um determinado dia, quando se encaminhava até a sua sala de trabalho encontrou dentro de um elevador um CD ou um DVD escrito "demonstrativo de salários da empresa", ou, "lista de demissão mês atual". São frases fortes não?!

Você mais que curioso correu para seu computador para ver quanto as pessoas estão ganhando ou quem será demitido. Será que seu nome está na lista?

Ao abrir o suposto documento é exibida a mensagem: "versão do sistema incompatível".

Ou você tentaria novamente em outro computador ou deixaria de lado.

Mas o que você não sabe é que este CD ou DVD foi deixado por um hacker (estou usando esse termo, agora, de forma genérica), e que ao executar o arquivo você instalou um vírus (um worm ou trojan por exemplo) que dará acesso ao hacker. Esse é só um exemplo de uma prática criminosa que pode acontecer.

Veja alguns exemplos que aconteceram: uma pessoa liga para você dizendo que é de alguma empresa (sempre muito conhecida) e que você acabou de ganhar um carro 0KM, uma quantia em dinheiro ou uma viagem.
Para retirar o prêmio será necessário você comprar três cartões de celulares pré-pagos e passar para eles as senhas dos créditos ou fazer deposito de alguma quantia em dinheiro.

Parece um absurdo mas isso acontece, e muitas pessoas desenformadas já caíram no golpe.

Veja mais um exemplo: alguém te liga e diz que é o "suporte técnico" do provedor e que a sua conexão está com problema. Para resolver o problema ele precisa de sua senha de conexão. Se você passar a senha para esse suposto "técnico", ele poderá usar a sua conta de acesso para práticas maliciosas.

Tudo isso são exemplos de engenharia social, onde o criminoso consegue informações (ou consegue convencê-la a fazer algo) de sua vítima aproveitando da falta de informação da mesma. Eles procuram induzir as suas vítimas a fazer alguma tarefa, e o sucesso do ataque dependerá exclusivamente da decisão do usuário.

Contaminação

A contaminação de um computador com qualquer tipo de vírus pode se dar de várias formas. A muitos anos atrás essa contaminação se dava basicamente através de disquetes, e mesmo assim eles conseguiam se espalhar. Com o advento da Internet, os vírus passaram a se alastrar via E-mail, programas de conversas instantâneas, etc. Veja a seguir as diversas maneiras de ocorrer uma contaminação:

- Abrir arquivos anexados aos e-mails;
- Abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- Instalar ou copiar arquivos de CDs de procedência duvidosa;
- Instalar ou copiar arquivos de DVD de procedência duvidosa;

- Instalar ou copiar arquivos de um pen drive de procedência duvidosa;
- Acessar sites inseguros;
- Clicar em links fraudulentos através de programas de comunicação instantânea, como o Whatsapp e Telegram;
- Clicar em links fraudulentos em redes sociais como, por exemplo, links enviados no direct do Instagram;
- Além de outros meios que eventualmente eu não coloquei aqui.

A contaminação pode ocorrer em qualquer sistema que permita que de alguma forma um arquivo contaminado seja executado. Isso quer dizer que novos meios de contaminação surgirão acompanhando o avanço tecnológico.

E como vimos nas páginas anteriores, alguns tipos de vírus podem contaminar um sistema e ficar "invisível" sem que seja percebido, uma vez que, nem todos os vírus são feitos com a intenção de apagar arquivos, travar o computador, entre outros danos.

Como os vírus atacam

Veremos agora um pouco sobre como alguns vírus atacam. Esperamos que desta forma, todos possam compreender melhor como eles chegam ao computador do usuário, como eles atacam e quais os reais riscos.

Worms

A principal especialidade do worm é fazer cópias de si mesmo e se propagar pela rede, sem necessitar da intervenção humana.

Por ter essa característica muitos são feito com o intuito de somente proliferarem o máximo possível.

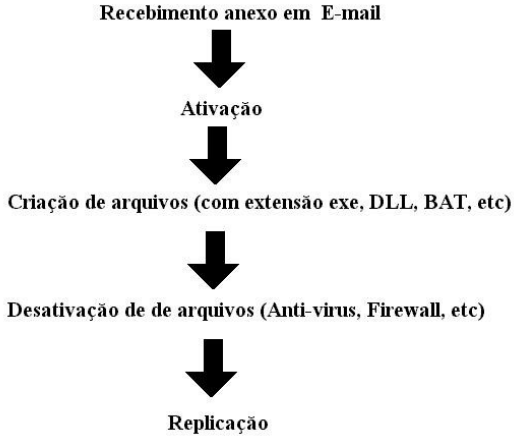
Isso faz deles uma grande ferramenta para os hackers, que podem usá-lo para espalharem outros tipos de vírus.

É o caso dos trojans, que podem chegar em um computador através de um Worm. Isso quer dizer, que se um antivírus detectar e eliminar um worm, não necessariamente o computador ficará “limpo”, talvez há um trojan instalado no sistema.

Vale lembrar que o worm pode ser programado para fazer diversas outras coisas além de se propagar.

Vamos usar como exemplo o worm W32/BugBear@mm: uma vez ativo em memória, esse worm tentará enviar uma cópia de si mesmo para todos os endereços de e-mail do sistema infectado.

Além disso, ele tentará desabilitar os programas antivírus e Firewall ativos e instalará um trojan no computador com o objetivo de capturar o que for digitado no teclado.



Exemplo de como um Worm pode agir

Trojans

Os trojans não se multiplicam e podem chegar ao computador da vítima anexo a E-mails ou podem ser instalados através de worms. O objetivo deles geralmente são dois: coletar informações e incluir backdoors, para garantir que um hacker tenha acesso ao computador.

Um trojan pode ser instalado manualmente pelo hacker ou pelo usuário. Para que ele seja instalado pelo usuário, o hacker tentará convencê-lo a executar o trojan, e isso é feito disfarçando-o de um aplicativo que pode ser jogos, charges, proteções de tela, etc.

Na época do “apagão” apareceu o Trojan "infectus" que exibia três tela fazendo uma alusão ao racionamento de energia.
A primeira tela vinha com a frase: "Com a onda do ‘Apagão’, o governo após vários estudos encontrou a tão esperada solução para os

problemas referentes ao racionamento de energia. Ela é totalmente segura e não requer gastos e verbas".

A Segunda tela: "O Ministério do ‘Apagão’ adverte: perder tempo com esse tipo de e-mail é desperdício de energia :-)".

E por fim a terceira: "Seu computador já pode ser desligado com segurança".

Apesar de parecer engraçado, o trojan por “trás”, se conectava a um site da Bélgica e baixava um programa que iria dar acesso ao computador da vítima ao hacker.

Vírus de Macro

Macro é um conjunto de comandos que são armazenados em alguns aplicativos, como o Word e Excel, que visam diminuir as tarefas repetitivas executadas pelo usuário como, por exemplo, substituir todos os "eh" por "é", em outras palavras, são rotinas personalizadas para serem feitas automaticamente pelo Word ou Excel ou qualquer programa que suporte scripts VBA (Visual Basic for Applications). O VBA é a linguagem das macros.

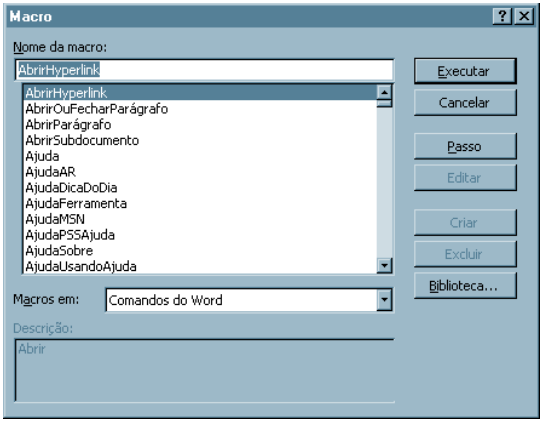
Utilizando macros é possível por exemplo acrescentar um cabeçalho automaticamente em um documento usando um conjunto de teclas, ou seja, é possível personalizar o processador de textos afim de otimizar o trabalho.

Todas essas facilidades chamaram a atenção de pessoas mal intencionadas que perceberam que podiam usar o scripts VBA para alterar o funcionamento normal dos aplicativos que suportem esses scripts, em especial o Word e Excel. Surgindo a parti daí os vírus de

Macro. Os vírus de macro só funcionam dentro dos programas aos quais estão ligados, dessa forma, atacam exclusivamente documentos do Microsoft Office.

Para que o vírus de macro contaminem outros documentos, este deve ser aberto. Geralmente o que o vírus de macro gostam de fazer é bagunçar os menus do Word. O grande problema é que isso pode ser feito de forma simples. Só para se ter uma idéia, você pode ver quais menus do Word podem ser modificados através de scripts VBA:

1. Abra o aplicativo Word;
2. Vá ao menu *Ferramentas* - *Macros* - *Macros* (ou pressione Alt+F8);
3. Na caixa *Listagem de macros* escolha Comandos do Word.



Comandos modificáveis do Word

Para modificar qualquer comando, bastará escolhê-lo na lista e mudar a categoria (na caixa de listagem) para o nome do documento em que será aplicada a macro e clicar em criar.

O editor do Visual Basic será aberto e com poucas linhas de códigos o comando pode ser mudado. Pode-se por exemplo redirecionar os comandos para exibir mensagens, em vez de executar a rotina padrão do software. Comandos importantes, como copiar texto ou formatar fonte (além de vários outros) podem ser mudados, e um detalhe é que os atalhos (Ctrl+C) também serão afetados.

A barra de ferramentas também pode ser mudada. Isso é conseguido através do número ID que identifica cada nome da barra de ferramentas, ou seja, cada nome (ou botão) que vemos na barra de ferramentas do Word tem um número que se trata da identificação "Visual Basic" correspondente.

Uma vez com posse desses números, é possível gerar instruções (macros) que podem por exemplo, desabilitar um determinado botão. E para conseguir essas IDs não é necessário fazer nenhuma "mágica" e basta, seguir os passos a seguir:

1. Abra o Word e acesse o Editor do Visual Basic (pressione Alt+F11);
2. À esquerda no editor haverá janela escrito *Project* (visualizador de projetos). Clique com o botão direito do mouse em uma área vazia dessa janela, e clique em *Inserir* - *Módulo*;
3. Um módulo em brando será aberto. Para prosseguir, digite os códigos a seguir:

```
Sub ExibeBarraDeFerramentas()
Dim i As Integer
Dim j As Integer
Word.Documents.Add
For i = 1 To Word.CommandBars.Count
Selection.TypeText Word.CommandBars(i).Name & vbCrLf
For j = 1 To Word.CommandBars(i).Controls.Count
Selection.TypeText " ID= " & Word.CommandBars(i).Controls(j).ID & "
--- " & " Texto = " _
& Word.CommandBars(i).Controls(j).Caption & vbCrLf
Next j
Selection.TypeParagraph
Selection.TypeParagraph
Next i
End Sub
```

4. Ao terminar clique no botão *Executar Sub/User/Form* do Editor. Será criado um novo documento do Word contendo uma lista com todas as barras de ferramentas e todos os botões do Word e seus respectivos IDs

Veja na lista a seguir alguns IDs que gerei:

Standard
ID= 2520 --- Texto = &Novo
ID= 23 --- Texto = &Abrir...
ID= 3 --- Texto = &Salvar
ID= 2521 --- Texto = &Imprimir
ID= 109 --- Texto = Visuali&zar impressão
ID= 2566 --- Texto = &Ortografia e gramática...
ID= 21 --- Texto = Recor&tar
ID= 19 --- Texto = &Copiar
ID= 22 --- Texto = C&olar

ID= 108 --- Texto = &Pincel
ID= 128 --- Texto = &Desfazer VBA-Selection.TypeText
ID= 129 --- Texto = Impossível &refazer
ID= 1576 --- Texto = &Hyperlink...
ID= 2934 --- Texto = Barra de ferramentas &Web
ID= 916 --- Texto = Barra de ferramentas &Tabelas e bordas
ID= 333 --- Texto = &Inserir tabela...
ID= 142 --- Texto = &Inserir planilha do Excel
ID= 9 --- Texto = Co&lunas...
ID= 204 --- Texto = &Desenho
ID= 1714 --- Texto = Estrutura do &documento
ID= 119 --- Texto = &Mostrar tudo
ID= 1733 --- Texto = &Zoom:
ID= 984 --- Texto = Aj&uda do Microsoft Word

Formatting
ID= 1732 --- Texto = &Estilo:
ID= 1728 --- Texto = &Fonte:
ID= 1731 --- Texto = &Tamanho da fonte:
ID= 113 --- Texto = &Negrito
ID= 114 --- Texto = &Itálico
ID= 115 --- Texto = &Sublinhado
ID= 120 --- Texto = &Alinhar à esquerda
ID= 122 --- Texto = &Centralizar
ID= 121 --- Texto = Alinhar à &direita
ID= 123 --- Texto = &Justificar
ID= 11 --- Texto = &Numeração
ID= 12 --- Texto = &Marcadores
ID= 3473 --- Texto = &Diminuir recuo
ID= 3472 --- Texto = &Aumentar recuo
ID= 203 --- Texto = &Bordas
ID= 340 --- Texto = &Realce
ID= 401 --- Texto = &Cor da fonte

Tables and Borders
ID= 2059 --- Texto = De&senhar tabela
ID= 2060 --- Texto = &Editar tabela
ID= 1724 --- Texto = &Espessura da borda
ID= 2622 --- Texto = &Largura da borda
ID= 2628 --- Texto = &Cor da borda
ID= 203 --- Texto = &Bordas
ID= 2947 --- Texto = &Cor do sombreamento
ID= 798 --- Texto = &Mesclar células
ID= 800 --- Texto = Dividir &células...

Qualquer pessoa com um pouco de experiência em criar macros, que conheça as linhas de códigos, e que tenha posse dos IDs, pode fazer coisas como alterar as funções dos botões e/ou menus, remover os menus da barra de tarefa, etc. Isso é conseguido usando o número do controle (exemplo: 798) e poucas linhas de código.

Exemplo:

```
Sub DeletaVBE()
    Word.CommandBars("Visual Basic").FindControl(, 798).Delete
End Sub
```

Essa macro usa o comando Delete para excluir o controle 798, removendo-o da barra de ferramentas.

Alguns vírus de macro usam exatamente essa técnica para se tornar invisível (stealth), onde eles apagam todos os menus da barra de ferramentas que poderiam exibir o seu código, como por exemplo

apagando o menu que abre o editor do Visual Basic. Isso pode complicar a vida de muitos, uma vez que alguns vírus de macro devem ser apagados manualmente de um computador contaminado.

Além disso, se o vírus for executado, ele poderá contaminar o arquivo modelos geral de arquivos do Word, e a partir desse ponto todos o outros arquivos que forem abertos passarão a ser contaminados.

Aí vem aquela dúvida: vírus de macro pode iniciar automaticamente, sem a intervenção do usuário? Sim. A resposta é tão direta que talvez até assunta. Os vírus de macro podem ser iniciados automaticamente graças as Automacros, que são macros que iniciam automaticamente em determinadas circunstâncias. As principais são:

- AutoExec: Executada quando iniciamos o Word;
- AutoNew: Executada quando criamos um documento no Word;
- AutoOpen: Executada quando abrimos um documento;
- AutoClose: Executada quando fechamos um documento;
- AutoExit: Executada quando saímos do Word.

Usando-se dessas automacros, surgem vírus que são ativados de várias formas, dependendo apenas das ações do usuário. Por isso que a simples abertura de um documento Word pode ativar o vírus de macro. Neste caso o vírus estaria usando por exemplo o módulo AutoOpen(), que abriria algum rotina.

Sintomas

Os sintomas de um PC com vírus de macro são típicos: a começar pela exibição de uma janela avisando sobre a presença de macros

sempre que iniciamos um arquivo (caso a proteção contra vírus de macro esteja ativada). Menus e botões faltando, imprimindo caracteres que não foram digitados, textos sendo apagados sem comando do usuário entre outros.

Palavras Finais

Tudo que expus aqui, principalmente os códigos, é apenas para fins didáticos. Não é para você, em hipótese alguma, tentar "colocar em prática" esses códigos. Tentar criar códigos ou até mesmo vírus. Não faça isso, não é o objetivo deste livro. O objetivo aqui é segurança, é entender como tudo funciona, quais os reais riscos e como se prevenir.