70
REVISTA
TECNOLOGIA
FORTALEZA
Nº 20
P. 70-83
DEZ. 1999

VÍRUS DE INTERNET: PREVENÇÃO E SEGURANÇA NA REDE

RESUMO

Quando os futuros historiadores olharem para a segunda metade do 20º Século, eles estarão revendo o que seguramente será conhecido como a Revolução da Informação. O gênero humano progrediu mais nos últimos 50 anos do que em qualquer outro período de história. Uma das razões principais para este aumento da corrida em tecnologia é o computador. Capacidades tecnológicas e avanços aumentaram a um passo extremamente acelerado. Isto faz com que sistemas de computadores maiores e mais sofisticados sejam criados, permitindo funções mais importantes e críticas serem assimiladas por estes.

Este artigo técnico faz uma tentativa de informar e alertar, em boa parte, como evitar e fazer conhecer falsas mensagens de prováveis ataques de vírus através de e-mails ou Web Sites, as chamadas viroses da INTERNET. Um exemplo disto são as Pesquisas do Instituto para investigação, "Irregular Internet Phenomena", onde se chegou a conclusão que muitos usuários de Internet estão continuamente sendo infectados por um novo vírus, que os faz acreditar, sem questionar, sobre toda uma história infundada, lenda, e advertência de cuidados, mostrados em seu "inbox" ou em seu "browser". O Vírus de Gullibility, como é chamado, aparentemente faz com que as pessoas acreditem no tipo de mensagem recebida e remeta cópias das mesmas a outros, tais como brincadeiras tolas relativo a receitas de biscoito milionárias, vírus de e-mail, impostos em modem, esquemas de pirâmides entre outros tipos de mensagens de caráter psicológico.

José Paulo Narciso da Rocha Júnior

Arquiteto e Urbanista, Universidade Gama Filho – R.J.

Eng. Estrutural, Especialização Universidade de Fortaleza – CE

ABSTRACT

When future historians look back at the second half of the 20th Century, they will be reviewing what is sure to be known as the Information Revolution. Mankind has progressed further in the last 50 years than in any other period of history. One of the main reasons for this rapid increase in technology is the computer. Technological capabilities and advancements have increased at an extremely accelerated pace. This allows for the

larger and more sophisticated computer systems to be created and allowing for more and more important and critical functions to be assigned to them.

This article, explain about of search of "The Institute for the Investigation" of "Irregular Internet Phenomena" that many Internet users are becoming infected by a new virus that causes them to believe without question every groundless story, legend, and dire warning that shows up in their inbox or on their browser. The Gullibility Virus, as it is called, apparently makes people believe and forward copies of silly hoaxes relating to cookie recipes, email viruses, taxes on modems, get-rich-quick schemes, among other types of messages of psychological character.

INTRODUÇÃO

This message is so important, we're sending it anonymously! Forward it to all your friends right away! Don't think about it! This is not a chain letter! This story is true! Don't check it out! This story is so timely, there is no date on it! This story is so important, we're using lots of exclamation points! Lots!! For every message you forward to some unsuspecting person, the Home for the Hopelessly Gullible will donate ten cents to itself. (If you wonder how the Home will know you are forwarding these messages all over creation, you're obviously thinking too much.) ACT NOW! DON'T DELAY! LIMITED TIME ONLY! NOT SOLD IN ANY STORE! Estes são possíveis subjects que voce poderá receber com características do vírus Gullibitliy. - http://www.symantec.com/avcenter/index.html -, a verdade precisa ser dita e divulgada antes que uma caixa de correio eletrônico fique lotada de mentiras.

As mensagens eletrônicas que circulam por todo o mundo sob a forma de "correntes" são todas falsas. A maioria dos vírus sobre os quais as mensagens alertam não existe, e os que existem não contaminarão o computador a menos que "abra" os arquivos. Os pedidos de ajuda para crianças com câncer, além de não serem reais, causam transtornos para a Sociedade Americana de Câncer e ainda traem nossa confiança e boa intenção, nos fazendo de idiotas.

O e-mail sobre um menino que tem pouco tempo de vida, cujo último desejo é uma mensagem que circule o mundo eternamente, não tem fundamento. Esta história é comprovadamente tão velha que o menino hoje, se existisse e vivesse, seria um senhor de idade avançada.

A lenda da receita de um biscoito de chocolate, um cookie, circula há mais de 60 anos. Passar fatos inverídicos adiante, custa muitas horas de conexão, congestiona a Rede, difama instituições sérias e perpetua a estupidez nossa de cada dia.

A previsão do instituto americano de pesquisas IDC - International Database Corporation - é de que em 2005, haverá mais 1 bilhão de pessoas conectadas à Internet. Somos, atualmente, 147 milhões no mundo e, no Brasil, menos de 2,7 milhões. Por isso mesmo, devemos aproveitar enquanto ainda somos poucos e, de certa forma, pioneiros, para evitar o mau uso das mensagens de e-mail, como no caso da prática de spam.

Spam é o uso abusivo do correio eletrônico para mandar mensagens não-solicitadas para uma grande quantidade de usuários, como malas diretas, pirâmides de enriquecimento fácil, abaixo-assinados e as amaldiçoadas "correntes". Quando se tem a infelicidade de estar numa dessas grandes listas, perde-se tempo e paciência. As mensagens chegam de todas as partes do mundo e, infelizmente, são traduzidas por algum infeliz que teve a incrível idéia de importar uma idiotice qualquer. Em certos casos, o usuário pode ter entrado em algum site e permitido o envio de notícias ou novidades por e-mail, mas, em geral, seu Endereço Eletrônico foi incluído sem sua permissão.

No Brasil existe uma associação de combate a essas mensagens indesejadas, o Movimento Brasileiro Anti-SPAM, onde pode-se fazer denúncias e consultar listas-negras de spammers, entre outras coisas. Entre as mensagens indesejadas, existem casos clássicos, como histórias que já circulavam antes mesmo da invenção do e-mail e as notícias alarmantes de contaminação por vírus ou produtos cancerígenos. Alguns estudiosos

pesquisam a fundo para descobrir a veracidade dessas histórias, chamadas na INTERNET de "Lendas Urbanas". Até hoje, nenhuma foi confirmada. Nos e-mails de spam mais comuns pode-se observar como a ingenuidade de muitos nutre a má intenção de alguns poucos.

Pequenos e-mails, grandes bobagens. Cuidado com o vírus! É a cellula-mater de todos os boatos. Primeiro porque um vírus não pode infectar o computador via e-mail. O vírus pode, sim, infectar o computador se ele vier através de um arquivo anexado a um e-mail, como o Happy99.exe, que vem junto à mensagem sem que a pessoa que mandou perceba. Receber um e-mail com um arquivo em "attach" com esse nome, "Happy99.exe", basta não executar, não abrir o arquivo, que nada acontecerá. Por isso mesmo, nunca habilite o programa de correio para abrir automaticamente os programas anexos. Se preferir executá-lo, habilite a varredura automática do anti vírus atualizado para todos arquivos, subpastas e arquivos compactados com extensões específicas de forma que verifique todos arquivos.

Entre os vírus que não existem, sempre mencionados nesses e-mails, estão os seguintes:

A.I.D.S. Computer Virus, AOL4FREE virus, Budwiser Frog virus, Join The Crew virus, Penpal Greetings virus, "Win A Holiday" virus, Ajude uma criança doente entre outros.

A história da criança que tem câncer e precisa do seu e-mail é uma das correntes mais antigas, talvez porque as pessoas bem-intencionadas acreditem que realmente poderão ajudá-la. Não é verdade. A corrente nunca será transformada em dinheiro para ajudar ninguém e o endereço eletrônico não é da Sociedade Americana de Câncer (The American Cancer Society's). Não dê um forward para esse tipo de mensagem. Se você realmente quiser ajudar uma criança, procure uma instituição de caridade real, por exemplo. Há outras versões desta corrente, para um garoto que tem pouco tempo de vida e quer que um e-mail seja perpetuado para manter sua memória viva. Não são mensagens reais e que tentam a todo custo confundir o usuário. Esses fatos podem ser confirmados visitando-se alguns Web Sites. Acredite, não são reais.

A receita do cookie: Esta história é mais velha que a nossa avó e já circulava com outras versões, como a da receita de bolo do hotel Waldorf Astoria em Nova York, cuja corrente tem mais de 60 anos. O e-mail conta o caso de uma pessoa que pediu a receita de um biscoito que comeu num restaurante, um cookie de chocolate, e acabou lhe sendo cobrada em seu cartão de crédito a quantia de 250 dólares pela receita. Numa suposta vingança, a senhora passaria a receita de graça para o planeta inteiro. Trata-se de um "mito urbano" estudado e pesquisado. Não passe o e-mail adiante. É uma bobagem e, ainda por cima, uma bobagem americana. Quem já fez a receita, porém, garante que o biscoito é delicioso. Troque seu Nike velho: Esta lenda diz que seu par de tênis usado poderá ser doado para reciclagem. Em troca, por sua boa ação, você receberá um par de tênis novinho. Mais uma história pé-de-chinelo. Verifique a reação da empresa em Nike's reaction ou na história de The Mining Company para confirmar mais essa loucura. Perigo no shampoo, filtro solar, existem certas verdades que não podemos negar, se você comer todo o conteúdo do seu filtro solar e tomar todo o shampoo é provável que você adoeça. Os e-mails que circulam avisando sobre substâncias tóxicas e cancerígenas não foram comprovados. Guiness Book of World Records e o Totem da Sorte, não caia nessas. Para entrar no Guiness é preciso muito mais do que dar um "forward" num e-mail. E o Totem da Sorte, supostamente do Havaí, além de muito feio, nunca fez ninguém ficar rico. As grandes empresas não passam correntes. Se você realmente quiser doar seus órgãos para transplante, um gesto nobre e humano, registre-se como doador aqui mesmo no Brasil. Porque, passando e-mails, você não vai fazer com que alguém em Nova Orleans receba um rim ou um fígado.

Mas, se você não consegue controlar seu desejo de encaminhar uma mensagem para seus amigos, ou futuros ex-amigos, pedimos que ao menos siga algumas regras básicas de convivência, como estas:

- Se você usa o Outlook Express ou o Netscape, não habilite o HTML para formatação de mensagens (ferramentas/Opções/Enviar). As pessoas que usam plataformas Unix, por exemplo, não vão conseguir ler nada. Nem a receita do biscoito.

- Caso sua vontade de encaminhar ("forward") a mensagem seja incontrolável, pelo menos não envie dois quilômetros de usuários. Apague-os manualmente ou, se a versão do seu Outlook Express permitir, desabilite a função (Ferramentas/Opções/Enviar/Formato para envio de Mensagens, Sem formatação - Configurações) e desabilite o recuo .

Agora, se mesmo assim você não tem coragem de interromper uma corrente, porque tem medo de que o céu caia sobre sua cabeça, porque a plantação de repolho de um agricultor no Texas que quebrou a corrente foi devorada por gafanhotos, ou porque uma senhora na Transilvânia não copiou o e-mail e o seu periquito de estimação teve um ataque de caspa e morreu, saiba que, para cada corrente que você manda, e quanto mais correntes você passar, mais rápido você irá receber uma superlotação (spam) de e-mails em seu inbox.

Seu Micro Foi Invadido? Ele está se comportando de maneira estranha, quando conectado à INTERNET ?

Eu te disse! Mas eu te disse! Eu te disse!!! –"Nunca, jamais, NEVER! execute um arquivo, do qual você não sabe a procedência, nem tampouco tem certeza de que o fornecedor deste arquivo não quer lhe fazer mal". Mas nada adianta... Quando comecei a ouvir falar de Back Orifice, e agora do Back Orifice 2000, NetBus e alguns outros menos famosos, imaginei que os internautas não seriam ingênuos, o suficiente para executar estes arquivos. Na realidade, eles são ingênuos.

Marque 1 ponto para cada resposta "SIM" que der no questionário abaixo, e veja sua classificação:

1. Você executou, recentemente, algum arquivo o qual não produziu efeito nenhum e além disso sumiu de onde você o tinha gravado? ( ) Sim ( ) Não

2. Você tem reparado o aparecimento de diretórios estranhos do seu computador, ou o sumiço de alguns diretórios ou arquivos? ( ) Sim ( ) Não

3. O seu micro tem sido desligado ou reiniciado enquanto você usa a Internet? ( ) Sim ( ) Não

4. Você tem recebido mensagens estranhas ou ameaçadoras do computador, enquanto usa a Internet? ( ) Sim ( ) Não

5. Pessoas têm lhe abordado com informações pessoais, as quais só são encontradas no seu computador, e em mais nenhum lugar? ( ) Sim ( ) Não

6. O seu CD-ROM abre e fecha sozinho? ( ) Sim ( ) Não

7. Pessoas descobrem com quem você está conversando na Internet, e o que você digita no seu computador? ( ) Sim ( ) Não

Classificação:

0 ponto: Você provavelmente nunca sofreu o "ataque da moda", o que não exclui a possibilidade de estar vulnerável.

1 ponto: Você provavelmente conseguiu passar todo esse tempo imune aos hackers .

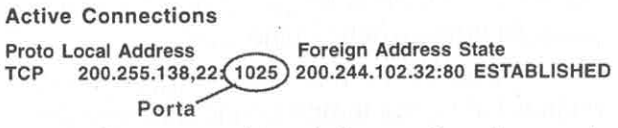
2 ou mais pontos: Se você fez 2 pontos marcando apenas algumas das questões, você simplesmente ainda não PERCEBEU os sintomas descritos nas outras questões! Se você marcou mais de 2 pontos, você já foi alvo de hacker.

Os programas aos quais estou me referindo chamam-se Back Orifice (também conhecido como BO) e NetBUS (também conhecido como NetBUS;-). Eles não são vírus (motivo pelo qual, provavelmente o anti-vírus não o detectou!). Nem mesmo são "Cavalos de Tróia", eles na verdade são aplicativos que, após executados, não lhe dão a opção de desativa-los. E o que estes aplicativos fazem? Eles disponibilizam, no seu computador, portas de conexão as quais podem ser acionadas para que outras pessoas tenham acesso a ele, sem que você precise dar nenhuma autorização. Já percebeu o perigo? Muitas pessoas já executaram estes programas, provavelmente enviados por terceiros pela Internet, e agora não tem mais controle sobre os próprios computadores. Obviamente, estes programas não deixam muitos rastros de que estão lá, e um usuário desatento pode passar a vida inteira pensando que seu computador está possuído por um Poltergeist... E então você me perguntaria: "Você disse que não deixa muitos rastros, o que quer dizer que algum rastro ele deixa. Onde posso encontrá-los?" Faça o seguinte: desconecte-se (?!) da Internet, reinicie seu computador, abra uma janela DOS e

execute "netstat -an". Este comando lhe mostrará as portas de conexão abertas em seu micro. Caso encontre alguma porta de número 31337 ou 12345, você está infectado.

Na verdade, suspeite de qualquer porta aberta nestas circunstâncias, pois não estando você conectado na Internet, não há motivos para ter portas abertas, a não ser o caso de firewalls ou monitoradores, principalmente porque as portas abertas podem ser configuráveis, e as 31337 e 12345 são apenas as portas default - veja o exemplo abaixo. Neste caso, feche todos os programas, inclusive o ICQ, e repita o teste.

Active Connections



De posse desta informação, aja o mais rápido possível, provavelmente alguém invadiu ou poderá invadir o micro. Deixando os detalhes técnicos para outra oportunidade passamos a resolver este problema. Baixe este programa... Higienic Paper - 339Kb - hpth_200.exe ou o anti - vírus mais recente McAfeeScan ...e o execute. Clique em "Detectar, Limpar e Vacinar". Se tudo correr conforme o esperado, ele informará que o micro agora encontra-se livre, tanto do BO quanto do NetBUS. Em seguida feche o programa. Que tal ficar de olho nas tentativas de invasão do seu computador através do BO? Para isto, baixe o programa NoBo, de autoria do veterano Flávio Veloso, que fica "escutando" a porta 31337 (isto é configurável), e então veremos as inúmeras tentativas. Na verdade, qualquer monitorador de portas faria o mesmo serviço. A minha recomendação se dá pela possibilidade de, através do NoBo, enviarmos uma mensagem (que não precisa ser necessariamente educada) para o agressor, de modo que ele saiba exatamente com quem está falando.

PREVENÇÕES BÁSICAS

Antivírus

Ter um excelente antivírus atualizado significa visitar pelo menos mensalmente a Home Page do fabricante e fazer o update ou seja, copiar um arquivo de atualização (geralmente com extensão DAT) que acrescentará os novos vírus que o programa poderá detectar. Mas, cuidado: copie e use o update específico para a sua versão do antivírus, senão, certamente, não funcionará. Veja no Help / About do seu antivírus a versão e procure copiar o update exato para a *sua* versão, no site do fabricante.

Update e upgrade

Update é uma atualização do conjunto de vírus que o antivírus ficará apto a detectar. Upgrade é a atualização de versão do próprio antivírus, ou seja se, por exemplo, você tem um qualquer 3.0 e já existe uma nova versão 4.0. Note que fazer o upgrade não dispensa de fazer o update cerca de um mês depois e a cada mês seguinte.

Recomendações

Nunca abra um arquivo anexado por duplo clique (ou procedimento correspondente) sobre o ícone do anexo (clips), no momento em que recebe a mensagem. Clique com o botão direito do mouse sobre ele (ou procedimento correspondente) e o "salve" no seu HD (ou outra mídia qualquer, como disquetes).

Após salvá-lo, antes de submetê-lo a um bom e atualizado antivírus, "não o abra". Use um bom visualizador de arquivos! Recomendo o WordView que é um freeware da Microsoft, (que vem no CD das ultimas versões do Microsoft Office, mas que também pode ser copiado a partir do site da Microsoft). Ele é muito bom, permite que se visualize todo o documento, com toda a sua formatação sem precisar abri-lo e até imprimi-lo. Quando for feita a instalação, surgirá mais uma opção - WordView - no menu de contexto que aparece quando se clica com o botão direito do mouse sobre o nome do arquivo, dentro do Windows explorer.

Tenha sempre um antivírus bom e atualizado instalado no seu micro e residente na memória. Antes de abrir qualquer arquivo recebido, comande o antivírus para escanear o arquivo. Um antivírus muito utilizado e disponibilizado é o Viruscan da McAfee. (Baseado em mail de Max Stocker).

GLOSSÁRIO TÉCNICO

Backdoors

Backdoors são programas que instalam um ambiente de serviço na máquina, tornando-a acessível a distância, permitindo o controle remoto de um computador sem que o usuário saiba.

Assim, a máquina poderá ser totalmente controlada de longe - por outra pessoa, em outro pc - dando a possibilidade de execução de todos os processos que o usuário possa executar.

É possível, portanto, para o invasor, logar todas as teclas digitadas da máquina para um arquivo (comprometendo acessos a sites seguros - cartão de crédito, homebanking etc.), ver seus arquivos, ler seus e-mails, ver todas suas senhas, apagar seus arquivos, dar boot em sua máquina, conectar via rede a outras máquinas as quais você tenha acesso, executar programas em seu computador, tais como inocentes jogos ou, até, formatar seu disco. Dois famosos programas desse tipo são o Back Oriffice e o Netbus.

Evidentemente, um grande problema é que invadir computadores hoje em dia não é coisa apenas para "hackers". Os backdoors tornaram possível que qualquer pessoa não especializada possa invadir um computador sem dificuldade.

Remoção de backdoors com o uso de programas

Backdoor Protection System

http://members.xoom.com/bpsystem/

O BPS 2.00, a partir da atualização do DAT, para 0003 consegue detectar 246 backdoors diferentes, incluindo key loggers e sniffers mais perigosos.

Back Oriffice (BO)

O Back Orifice (BO) é um pequeno programa - o BO Server - feito por um grupo denominado "Cult Of The Dead Cow" (cDc) e lançado em 21/08/98. Ele praticamente abre toda a segurança de um computador, possibilitando que um usuário conectado à Internet tenha acesso total aos recursos de uma outra máquina. Uma vez instalado, involuntariamente, em um computador, permite que qualquer usuário de posse do programa BO Client possa invadir aquela máquina sem que o proprietário saiba, enquanto estiver conectado à net, e executar qualquer comando que o proprietário também o possa fazer localmente.

O BO é uma aplicação "legal". Tecnicamente, seria um ótimo programa de monitoração remota, se não fosse pelo detalhe de não conter seqüência normal de instalação (avisos de que ele está sendo instalado), de não avisar quando está rodando e de não exigir senha para que aconteça o monitoramento remoto, deixando a máquina aberta para qualquer um, que possua o BO Client. Assim, quando conectado à Internet, o invasor pode enviar um pedido (por exemplo, del c:*.*) e abre uma conexão com um servidor BO. O Bo original se distribuía apenas por uma porta (a 31.337). Entretanto, isso pode ser alterado.

É um trojan e não um vírus, pois é necessário executá-lo para que ele se instale, mas o usuário o executa enganado, pensando que faz alguma outra ação.

Principais características

* tem entre 20 a 24 kb
* se autodeleta após a execução
* o ícone do BO é vazio

O BO não é o único, nem o primeiro, nem o mais perigoso, nem o mais fácil de usar dentre os programas deste tipo. Há dezenas de programas, para os mesmos perigosos fins. O BO é apenas o mais popular destes programas, os quais são conhecidos genericamente como backdoors (programas para monitoração remota sem a autorização do usuário).

Remoção do BO com o uso de programas

BPS

Copie o Backdoor Protection System, que consegue eliminar 246 tipos de backdoors. (Vá em: Remoção de back doors com o uso de programas)

Antigen

Se quiser testar se o computador está ou não infectado com o Back-Orifice, utilize um detetor. Um deles é o ANTIGEN que pode detectar e remover o Back Orifice de seu micro.

Antes de executar o ANTIGEN, certifique-se de desabilitar todos os programas detetores de acesso de BO, como o NoBo e outros antivírus. Caso contrário, o ANTIGEN pode acusar uma falsa infecção.

NOBO

O NOBO não elimina o Back Orifice, somente identifica quem (o IP) está mandando pacotes de Back Orifice e apenas se o programa não tiver sido alterado, em relação à porta utilizada.

Onde obter mais informação

http://lazaro.merchant.com.br/icq99/

http://ccc.unisinos.tche.br/users/c/charles/bo.htm

http://web.cip.com.br/nobo/

http://travel.to/psycho

Cavalo de Tróia (trojan horse)

A lenda do "Cavalo de Tróia" diz que um grande cavalo de madeira foi presenteado pelos gregos aos troianos, como sinal de que estavam desistindo da guerra. Mas, o cavalo escondia no seu interior um grupo de soldados gregos, que esperaram a noite e abririam os portões da cidade para o exército grego que invadiu e dominou a cidade. Assim, um trojan horse é um programa que oculta o seu objetivo sob uma camuflagem de programa útil ou inofensivo. É um programa que diz que faz uma coisa mas também faz outra e essa segunda atividade pode danificar seriamente o pc.

Diferenças principais entre trojan horses e vírus:

Não possuem instruções para auto-replicação

São programas autônomos, não necessitam infectar outras entidades (programas, setores de boot) para serem executados

Em geral, são ativados por diversos tipos de gatilho como: pelo próprio usuário (executando ou abrindo um trojan no PC), seqüências lógicas de eventos (bombas lógicas) ou por uma data ou período de tempo (bombas de tempo).

Não existe uma preocupação de auto-preservação, não objetivam a própria disseminação como os vírus.

Como não são feitos para se replicar, costumam permanecer indefinidamente no PC ou se autodestruir junto com os dados que visa apagar ou corromper.

A sua propagação acontece especialmente por meio de canais de distribuição (como Internet e BBSs), onde são colocados e oferecidos como programas úteis. São assim, voluntariamente copiados por usuários incautos, enganados quanto aos reais efeitos do programa.

Entretanto, inicialmente, os trojans horses não se replicavam, mas em janeiro de 1999 surgiu um trojan com capacidade de auto-distribuição, o happy99.exe.

Como os trojans não se limitam às características dos vírus são potencialmente mais perigosos. Assim, programas desconhecidos ou de origem duvidosa, mesmo que passem pelo antivírus, devem ser executados com cautela, de preferência em computadores devidamente "back-upeados" e, se possível, em um computador "cobaia", cujo disco rígido não possua nada indispensável. Atualmente há uma grande preocupação com trojans, pois vários backdoors são cavalos de Tróia.

Netbus

É um Trojan (ou seja, ele vem "escondido" em algum programa que se copia na Rede, inclusive os cartões animados que vem anexados -*.exe ou attach a uma mensagem de e-mail) que gerencia remotamente um computador, não sendo, portanto, um vírus.

O Netbus não é o único dentre os programas deste tipo. Há dezenas deles. São conhecidos genericamente como backdoors (programas para monitoração remota sem a autorização do usuário).

O NetBus surgiu antes do BO e é semelhante a ele, mas é maior, tendo cerca de 513 Kb.

Permite que o invasor possa monitorar a distância o computador da vítima. O invasor pode executar e encerrar programas, fazer download, ativar arquivos de sons, controlar os movimentos do mouse e abrir a bandeja de CD-ROM e, até mesmo, apagar arquivos e formatar o sistema, ou seja, pode fazer qualquer ação.

Ataca as versões 95, 98 e NT do Windows. Através do protocolo TCP/IP, o NetBus cria uma porta de conexões e fica esperando conexões nessa porta para, através dela, dar acesso a quase todos os controles da máquina a quem o acessar.

A máquina infectada fica com o NetBus Server cujo arquivo, por default, utiliza o nome de Patch.exe. O invasor, ou seja a pessoa que irá acessar essa máquina remotamente e que provavelmente implantou o NetBus no sistema, utiliza o NetBus Cliente, denominado NetBus.exe.

Há processos de remoção manual do Netbus, mas são complicados para usuários comuns.

Entretanto, se houver interesse estão descritos em:

http://www.brasirc.net/seguranca/netbus.html

http://www.antivirus.com/cgi-bin/vinfo.pl

Remoção do netbus com o uso de programas

BPS

Copie o Backdoor Protection System, que consegue eliminar 246 tipos de backdoors. (Veja o

item: Remoção de back doors com o uso de programas)

Corrente, Hoax e Spam

Corrente é aquele tipo de correspondência em que se envia a mesma mensagem para muitas pessoas. É facilmente identificável pois, em geral, consiste de :

• uma isca, para fazer o leitor ler a mensagem até o fim,

• uma ameaça para assustar ou penalizar o leitor e

• um pedido para o leitor repassar o material inútil para um certo número de pessoas, ou para quantas for possível.

A mensagem que estiver dentro deste padrão é uma corrente. No caso da Internet, seu único objetivo é entupir o correio eletrônico das redes de comunicação.

As pessoas reproduzem a mensagem achando que estão fazendo o bem, quando, na verdade, estão prejudicando o sistema, pois, independente da procedência e dos objetivos (sejam eles humanitários, de protesto ou de apoio) o que acontece é prejuízo para pessoas e organizações mundo afora, pois o envio indiscriminado de dezenas, centenas e até milhares de mensagens gera um tráfego absurdo, inútil e desnecessário na Internet e demonstra a desinformação dos Internautas. Redistribuindo mensagens, estamos cooperando para multiplicar geometricamente esse tráfego. Assim, a resposta dos servidores é cada vez mais lenta. Há perda de tempo útil, de produtividade, degradação do tempo de resposta do ambiente de correio das redes de comunicação etc. Ou seja, onde poderia passar comunicação de valor, passa lixo. Não há correntes bem intencionadas. Os "brincalhões" que as inventam usam temas dignos de credibilidade, tirados da realidade, que mexem com a sensibilidade das pessoas, mas, na verdade, só objetivam causar transtornos, perda de tempo, consumir recursos de crédulos e ingênuos destinatários ou, simplesmente, ver até onde sua brincadeira vai chegar.

Portanto, parar de usar tecla Encaminhar - Forward em mensagens alarmistas é um excelente procedimento. Confirmar antes de enviar é absolutamente necessário.

O The Hunger Site, um website que estaria canalizando doações para salvar pessoas que passam fome do Terceiro Mundo, se transformou, nas últimas semanas, em um dos assuntos mais comentados por internautas. A informação chegou por e-mail para muitos usuários e revela um dado assustador: a cada 3,6 segundos morre uma pessoa de fome no mundo. A mensagem diz que um clique salvaria uma vida. Basta escolher o país onde a fome é crítica e apertar o botão. Dessa maneira, a região receberia uma refeição e a empresa responsável pela doação apareceria no site. No entanto, alguns indícios apontam que isso pode ser uma fraude.

Segundo um e-mail enviado pelo "Informando", o patrocinador que se apresenta no site com mais freqüência, um laboratório que fabrica um derivado de aspirina chamado Heart-Trex, não existe na Internet. O próprio remédio não tem registro no FDA (órgão regulamentador dos medicamentos nos EUA).

O dono do "The Hunger Site" seria Otis Clapp, cujo e-mail seria, segundo a Network Solutions, jbooh@yahoo.com, com domínio gratuito, o que é bastante estranho.

Spam e Hoax

Spam é o ato de enviar mensagens não solicitadas a muitos destinatários. Normalmente, o conteúdo dessas mensagens é comercial. A classificação Hoax é usada quando o conteúdo é "alarmante", como os famosos vírus por mail. A definição mais real sobre spam é que é um vírus social, que utiliza a boa fé das pessoas para se reproduzir, sendo esse o seu único objetivo.

O que mais impressiona é o credito que os "spamers" (criadores de spam) recebem. Eles montam uma mensagem qualquer, apresentam fatos que a tornam quase verídica, indicam pessoas e seus endereços eletrônicos, distribuem em todas as listas que conhecem e, pronto, pessoas bem intencionadas, os "laranjas" fazem o resto, preocupadíssimos com a segurança do computador alheio, espalham a mensagem para todos que conhecem, pois querem evitar que o amigo seja prejudicado ou, então, mostrar que conhecem as novidades da net, pois descobriram antes que os outros o novo "vírus". De um modo geral:

Spam é e-mail não solicitado, como propaganda por exemplo.

Hoax é como uma espécie de lenda: estórias mentirosas, vírus por e-mail.

E-mail vírus:

Não existem. Quando se fala em vírus deve-se lembrar que:

• Um vírus é específico de um sistema operacional. Vírus para o DOS não afetam MacIntosh, assim como não afetam computadores Amiga.

• Um vírus, por definição, não funciona por si só. Deve infectar um arquivo executável ou arquivos que utilizam macros.

Para transmitir um vírus por e-mail, alguém deve infectar um programa e mandá-lo anexado (attach) a uma mensagem de e-mail. Para ativar o vírus, o destinatário deve executar o programa infectado que foi enviado, após copiá-lo do servidor decodificá-lo.

Neste caso, a mensagem de e-mail é apenas o meio de enviar um arquivo infectado, não sendo o vírus em si. Portanto:

• É impossível pegar vírus apenas pela leitura da mensagem.

• É impossível pegar vírus em anexos ou mensagens do tipo DADOS, que não executam nada no computador. Ou seja: que são apenas informação para uso de outro software, tais como txt, html simples, mid, gif, jpg, wav, bmp, mp3 etc.

• É possível pegar vírus e cavalos de Tróia pela execução de arquivos anexos nas mensagens, desde que os mesmos sejam do tipo executável (com, bat, exe) ou arquivos de algum tipo de aplicação que execute macros ou lotes (word, excel, powerpoint).

Um cuidado a ser tomado com a configuração de antivírus :

Existem alguns programas de e-mail que podem, automaticamente decodificar e executar um arquivo anexado. Nesse caso, deve-se desabilitar a opção que rode automaticamente um arquivo executável anexado.

Ser bastante cuidadoso com qualquer arquivo anexado que um estranho tenha mandado. Mais importante, deve-se checar qualquer arquivo recebido com programas antivírus, por medida de garantia.

Um cuidado que pode ser tomado, antes de espalhar textos alarmantes, especialmente em listas, é tentar verificar sua autenticidade na Internet. O endereço a seguir é mantido pelos fabricantes do Norton AntiVírus. Tem informações sobre falsos vírus e hoax:

http://www.symantec.com/avcenter/hoax.html

Antes de retransmitir qualquer aviso deste tipo, é importante verificar. Eles ficam sabendo dos novos vírus e os alarmes falsos rapidamente e o Web Site é atualizado sempre.

Outros endereços onde se pode obter mais informações sobre o assunto:

http://www.virtualand.net/icq/

http://ciac.llnl.gov/ciac/CIACHoaxes.html

http://afcert.csap.af.mil/hoaxes.html

http://www.unisinos.tche.br/ajuda/goodtime.htm

http://www.datafellows.com/news/hoax/

Worm

Nos anos 70, foram desenvolvidos os "worms" (vermes). Eles são programas projetados para duplicação e possuem as seguintes características:

• Se replicam;

• São entidades autônomas, não necessitando se anexar a um programa ou arquivo "hospedeiro", ao contrário dos vírus

• Residem, circulam e se multiplicam em sistemas multitarefa;

Apesar do caráter pejorativo do nome, os primeiros worms desenvolvidos para rede eram usados como mecanismos legítimos para o gerenciamento e execução de tarefas em sistemas de recursos distribuídos.

A Internet é a grande distribuidora desse tipo de programa.

Vírus

O que comumente chamamos de "vírus de computador" são programas que possuem algumas características em comum com os vírus biológicos:

• são pequenos;

• um vírus, por definição, não funciona por si só. Deve infectar um arquivo executável ou arquivos que utilizam macros, ou seja , em geral fica escondido dentro da série de comandos de um programa maior;

• contém instruções para parasitar e criar cópias de si mesmo de forma autônoma e sem autorização específica (e, em geral, sem o conhecimento) do usuário para isso - eles são, portanto, auto-replicantes;

Há várias manifestações visíveis da atividade dos vírus: mostrar mensagens, alterar ou deletar determinados tipos de arquivos, corromper a tabela de alocação, diminuir a performance do sistema ou até formatar o disco rígido.

Muitas vezes a ação de um vírus só se inicia a partir de eventos ou condições que seu criador pré-estipulou: atingir uma certa data, um número de vezes que um programa é rodado, um comando específico ser executado, etc.

Um vírus pode atingir um computador a partir de diferentes "vetores": documentos, programas, disquetes, arquivos de sistema, etc.

Após infectar o computador, eles podem passar a atacar outros arquivos. Se um destes arquivos infectados for transferido para outro computador, o vírus vai junto e, quando for executado irá contaminar o segundo pc.

Arquivos de dados, som (.wav, .mid), imagem (.bmp, .pcx, .gif, .jpg), vídeo (.avi, .mov) e os de texto que não contenham macros (.txt, .wri) podem ser abertos sem medo.

Tipos

Vírus de Boot (Master Boot Record / Boot Sector Viruses)

Todo drive lógico, seja o disco rígido ou um disquete, contém um setor de inicialização (boot) que possui informações relacionadas à formatação do disco, das pastas e dos arquivos nele armazenados (registro mestre do Sistema, o Master Boot Record - MBR dos discos rígidos ou a área de boot - Boot Sector dos disquetes). Como essas áreas são executadas antes de qualquer outro programa (incluindo qualquer programa Anti-Vírus), tais vírus são os mais comuns e os mais bem sucedidos do mundo. Para esse sucesso também contribui o fato da infecção poder ocorrer por meio de um ato simples do usuário: esquecer um disquete contaminado dentro do drive A.

Como todos os discos possuem também um pequeno programa de boot (responsável pela inicialização do sistema), que carrega os arquivos do sistema operacional (o DOS, por exemplo) os vírus de boot podem se "esconder" em qualquer disco ou disquete.

A contaminação ocorre quando um boot é feito através de um disquete contaminado. O setor de boot do disquete possui o código para determinar se um disquete é "bootável" ou para mostrar a mensagem: "Disquete Sem Sistema ou Erro de Disco". É este código, gravado no setor de boot que, ao ser contaminado, assume o controle do micro. Assim que o vírus é executado ele toma conta da memória do micro e infecciona o MBR do disco rígido.

A disseminação é fácil: cada disquete não contaminado, ao ser colocado no drive e ser lido pode passar a ter uma cópia do código e, nesse caso, é contaminado e passa a ser um "vetor".

Vírus de Programa (File Infecting Viruses)

Os vírus de programa infectam - normalmente - os arquivos com extensão .exe e .com (alguns contaminam arquivos com outras

extensões, como os .dll, as bibliotecas compartilhadas e os .ovl). Alguns deles se replicam, contaminando outros arquivos, de maneira silenciosa, sem interferir com a execução dos programas que estão contaminados. Assim sendo, pode não haver sinais perceptíveis do que está acontecendo no micro.

Alguns dos vírus de Programa vão se reproduzindo até que uma determinada data, ou conjunto de fatores, seja alcançado. Somente aí é que começa a sua ação. A infecção se dá pela execução de um arquivo já infectado no computador. Há diversas origens possíveis para o arquivo infectado: Internet, Rede Local, BBS, um disquete.

O vírus Melissa o Dominatrix é essencialmente uma simples seqüência macro do Word, que é um roteiro para tarefas automáticas dentro de documentos. Ele se espalha quando o usuário abre um documento infectado do Word 8 ou do Word 9, seja no Office 97 ou no 2000, e executa um roteiro de macro. Em alguns casos, no entanto, o vírus pode também se espalhar automaticamente entre aqueles usuários que configuraram os seus sistemas de maneira a não serem notificados quando a seqüência macro é executada.

O aspecto mais tortuoso do Melissa é como ele infecta. A macro induz o programa de e-mail do Outlook a enviar um documento para os 50 primeiros endereços no catálogo de endereços dos usuários, onde na linha do assunto está escrito: "Mensagem importante de" e então o nome do usuário. No texto da mensagem está escrito: "Aqui está aquele documento que você pediu" e o texto dentro da mensagem pede: "Não mostre a mais ninguém".

Mesmo as pessoas que não utilizam o Outlook estão sujeitas ao risco, contanto que o Outlook tenha sido usado para enviar o correio, e assim o documento infectado poderá ser enviado. Além disso, o modelo padrão do Word, .doc, que age como base de qualquer documento criado pelo usuário, fica infectado com o código virulento. Consequentemente os documentos do Word criados pelo usuário também irão conter o vírus.

Parece que o vírus foi originalmente espalhado através de um grupo de discussão do alt.sex, que publicou um anúncio com uma lista de senhas para vários sites pornográficos, aliás sites pornográficos dominam somente 1% do mercado em relação a soma de todos os outros sites existentes. O fato de site pornográfico possuir fama de domínio majoritário na net se deve a mídia que faz com que eles se tornem populares.

Apesar de o vírus se espalhar de forma extremamente rápida, ele causa pouco dano para os arquivos dos usuários. Além das ações tomadas para replicar a si próprio, a outra única modificação provocada pelo Melissa ocorre quando a data atual se iguala à data do documento. Por exemplo, às 2:27 da tarde do dia 27 de março, o vírus irá copiar a seguinte frase de Bart Simpson no documento atual: "Vinte e dois pontos, mais pontuação tripla de palavras, mais cinqüenta pontos por usar todas as minhas letras. O jogo acabou. Estou fora".

O dano mais severo que observamos é que ele pode parar os servidores de correio eletrônico de uma organização, essencialmente impedindo o seu funcionamento.

Vírus Multipartite

São uma mistura dos tipos de boot e de programa, podendo infectar ambos: arquivos de programas e setores de boot. São mais eficazes na tarefa de se espalhar, contaminando outros arquivos e/ou discos e são mais difíceis de serem detectados e removidos.

Outras capacidades

Entretanto, para tentar impedir a detecção pelos antivírus algumas capacidades foram dadas a qualquer um dos tipos de vírus acima. Assim, cada um desses três tipos de vírus pode ter outras características, podendo ser:

Polimorfismo (onde o código do vírus se altera constantemente): têm como principal característica o fato de estar sempre em mutação, ou seja, esse vírus muda ao criar cópias dele mesmo , alterando seu código. Mas, os clones são tão funcionais quanto seu original, ou mais. O objetivo da mudança é tentar dificultar a ação dos antivírus, criando uma mutação diferente daquilo que a vacina procura.

Invisibilidade (Stealth, onde o código do vírus é removido da memória): têm a capacidade de, entre outras coisas, temporariamente se auto-remover da memória, para escapar da ação dos programas antivírus.

Encriptação (onde o código do vírus é encriptado): É muito difícil a ação da vacina.

Vírus de macro

A partir de 1995 a classificação acima ficou insuficiente para abranger todos os vírus pois nesse ano surgiu uma nova tecnologia de construção desses programas. Alguns deles passaram a usar um conjunto de macros (comandos de programação interna) que é executado dentro de documentos de certos programas de processamento de texto (Word) e planilhas de cálculo (Excel). A simples abertura do documento pode ativar o vírus.

Assim, ao contrário dos vírus até então existentes, que se limitavam a arquivos executáveis ou afins e áreas de boot, os macrovírus infectam e se disseminam por arquivos de dados.

A disseminação desse tipo de vírus é muito mais acentuada pois documentos são muito móveis e passam de máquina em máquina (entre colegas de trabalho, estudantes, amigos e outras pessoas). Ao escrever, editar ou, simplesmente, ler arquivos vindos de computadores infectados a contaminação ocorre. Assim, verdadeiras "epidemias" podem acontecer dentro de poucas horas.

Além disso, os macrovírus constituem a primeira categoria de vírus multiplataforma, ou seja, não se limitam aos computadores pessoais, podendo infectar também outras plataformas que usem o mesmo programa, como o Macintosh, por exemplo.

Quando a macro é ativada (por exemplo, a macro AutoOpen do Word) os comandos nela existente se autocopiam, juntamente com qualquer outra macro que o vírus necessite. Assim, quando abrimos um documento infectado, automaticamente executamos o código virótico. Esse código altera o ambiente interno do Word de forma que todos os futuros documentos salvos utilizando a função "Auto open" sejam infectados com o código virótico. O destino dessas cópias é a memória o Modelo global do Word ou o arquivo Normal.dot, de onde o vírus contaminará qualquer novo documento que for criado ou, mesmo, qualquer documento que for aberto.

Um outro agravante em relação a esses vírus é a facilidade de lidar com as linguagens de macro, no que diz respeito à edição e criação, dispensando que o criador seja um especialista em programação, ao contrário do assembly, nem um pouco amigável e altamente abstrato. Isso acarretou no desenvolvimento de muitos vírus e inúmeras variantes e vírus de macro, num período curto de tempo.

Cuidados

Deve-se instalar e atualizar freqüentemente um bom antivírus, como o Viruscan da McAfee. Onde obter mais informação :

http://www.splitnet.com/index1.html

http://users.sti.com.br/helpdesk/

ANTIVÍRUS

Atualização

Instalar um antivírus é uma boa estratégia, mas não é suficiente. O programa deve ser atualizado freqüentemente, o que vai permitir o reconhecimento dos novos vírus. Para atualizar basta copiar e "deszipar" os arquivos DAT da McAffee sobre os já existentes, na pasta onde ele esteja instalado em seu computador. (Não esqueça de agendar uma atualização mensal do seu antivírus). Outras informações podem ser conseguidas em: http://download.mcafee.com/updates/3x.asp.

Instalação

Copie, dissipe e dê duplo clique no arquivo setup.exe para iniciar a instalação. Siga as instruções que forem aparecendo na tela, concordando ou não com a pasta onde será instalado o programa no seu computador.

Na janela "setup.exe" clique em "custom"; Desmarque a primeira e a última funções "command line..." "screen scan..." Deixe o processo terminar. Reinicialize o seu computador.

EPÍLOGO

Qual seria a região com a maior produção de vírus no mundo? Se você respondeu Estados Unidos, errou. De acordo com Fernando Silva, engenheiro de sistemas da Symantec, a Europa produz a maior parte dos vírus conhecidos atualmente. A explicação? O frio, que mantém as pessoas, leia-se hackers, em casa, em frente aos computadores.

Para driblar a imaginação fértil dos hackers, a Network Associates possui um laboratório, o Avert (Anti-Virus Emergency Response Team), que conta com 30 profissionais somente nos EUA, além de uma equipe de emergência espalhada por todo o mundo. Essa equipe é responsável pelo reconhecimento de arquivos suspeitos, que são enviados ao laboratório central ou analisados localmente.

Fernando Fontão, engenheiro de sistemas da Network Associates e membro do Avert, explica que o laboratório recebe os arquivos por meio de um e-mail robotizado, que compila as novas assinaturas (partes essenciais do vírus) dentro de uma nova DAT, que é atualizada a cada hora.

A produção de uma vacina contra um novo vírus pode consumir vários dias de trabalho.

Se, por um lado, a Internet ampliou significativamente a disseminação de vírus entre os computadores, por outro, abriga várias opções de softwares antivírus para download, alguns deles gratuitos, que podem auxiliar os internautas no combate aos invasores.

A grande novidade nesse segmento é o scanner on-line, que utiliza recursos de ActiveX e Java para rastrear o desktop, transmitindo a aplicação do servidor do site para a janela do browser de navegação. É o caso do antivírus PC-cillin House Call, disponível no site http://housecall.antivirus.com. Para ter acesso ao serviço, o internauta deve possuir os navegadores Microsoft Internet Explorer 3.0 ou Netscape Navigator 3.01, ou versões superiores, e baixar o plug-in, disponível na home page. Vale destacar que o antivírus on-line não garante proteção em tempo integral, como acontece com os melhores aplicativos do mercado.

O antivírus on-line, no entanto, leva algumas vantagens, ainda que relativas, sobre o antivírus full time: não reside na memória do computador e possui uma base de dados sempre atualizada. A Trend Micro, por sua vez, garante que o sistema é seguro, pois não envia à home page nenhuma informação sobre o desktop avaliado.

Outra empresa que possui um antivírus on-line é a Network Associates, que produz o aplicativo McAfee. O endereço http://clinic.mcafee.com abriga o VirusScan on-line, que permite utilização ilimitada. No site da McAfee (www.mcafee.com.br), por sua vez, pode-se fazer o download do soft de avaliação VirusScan 4.04. O shareware pode ser utilizado por 30 dias e não dá direito a suporte técnico. A Symantec abriga em seu site (www.symantec.com) diversos updates para o aplicativo Norton AntiVirus.

Durante o primeiro ano após a aquisição do produto, o serviço é gratuito. Depois, a assinatura anual custa US$ 3,95. O internauta poderá encontrar na Web outras opções de antivírus, como Thunder Byte, disponível no endereço www.thunderbyte.com. O download do aplicativo, considerado um dos melhores antivírus do mercado, dá direito a 30 dias de avaliação.

REFERÊNCIAS BIBLIOGRÁFICAS

BUCKLAND, John. **Combating Computer Crime:** Prevention, Detection, Investigation. McGraw-Hill: New York, 1992.

"The Central Intelligence Agency."; http://www.odci.gov/cia/

"Computer Crime - Legal Enforcement in the age of the Internet."; http://usit.oit.unc.edu/hoffmang/jomc191/paper.html

"Computer Crime, Security and Computer Viruses."; http://jaring.nmhu.edu/notes/security.htm

"Cybercrime on the Internet."; http://www.digitalcentury.com/encyclo/update/crime.html

FBI. ;"Federal Bureau of Investigation - National Computer Crime Squad."; http://www.fbi.gov/programs/nccs/compcrim.htm

FRASER, Bruce T.;

"Computer Crime Research Resources: Bibliography: Books." http://mailer.fsu.edu/~btf1553/ccrr/books.htm

"International review of criminal policy – ; United Nations Manual on the prevention and control of computer-related crime." http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html

KANE, Patrick.;
"Hacking the Hackers - Implementing a Cyberspace Hacker Assault Team."
http://www.trincoll.edu/~tj/tj12.02.93/articles/Article4.html
"The Lost World.";
http://www.lost-world.com
MORRIS, Gary S. ;
"Computer Security and the Law."
http://bilbo.isu.edu/security/isl/cslaw.html
"PCWebopaedia.";
http://www.pcwebopaedia.com/
POOLE, Gary A.;
"Hack Attack,"
Forbes June 3, 1996. pp. 97-110.
ROUSH, Wade.;
"Hackers: Taking a Byte out of Computer Crime,"
Technology Review April 1995. pp 32-41.
VENZKE, Ben N.;
"Economic/Industrial Espionage."
http://www.infowar.com/class_2/class2_2.html-ssi