C00 – Março de 1999

Cartilha dos Trojan Horses

O que são os Trojan Horses?
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, desejando a paz. Tal cavalo escondia no seu interior um grupo de soldados gregos, que abririam os portões da cidade para o exército grego, depois que os troianos levassem o cavalo para dentro da cidadela.

Trojan horses (Cavalo de Tróia, em português) são programas que ocultam os seus reais objetivos sob uma camuflagem de programas úteis ou inofensivos. Um exemplo hipotético de trojan horse seria um programa escrito, por exemplo, para formatar de forma incondicional o disco rígido, oferecido como um duplicador de disco ou PC game, por exemplo. A formatação poderia ocorrer imediatamente ao instalarmos ou executarmos o programa, ou o hipotético trojan poderia ser tão sofisticado na sua camuflagem que realmente funcionasse como duplicador ou videogame, ativando a formatação de acordo com algum evento específico (data, comandos específicos, etc).

Os objetivos
Os objetivos dos trojans horse, na realidade, podem ser os mais variados, de acordo com os desejos do seu produtor. Destruição de dados e quebra de segurança de sistemas são apenas alguns exemplos do que trojan horses costumam visar. De uma forma geral, ainda que alguns considerem os vírus um tipo particular de trojan, as seguintes diferenças são notadas entre trojan horses e vírus:

1. Não possuem instruções para auto-replicação;
2. São programas autônomos, não necessitam infectar outras entidades (programas, setores de boot) para serem executados;
3. Sempre possuem um payload, ativados por diversos tipos de gatilho como: diretamente pelo próprio usuário (executando ou abrindo uma trojan no PC), sequências lógicas de eventos (bombas lógicas) ou por uma data ou período de tempo (bombas de tempo), e
4. Não existe uma preocupação de auto-preservação, não objetivam a disseminação como os vírus.

A contaminação
Trojan horses não são comuns por causa da sua limitada capacidade de disseminação. Como não são feitos para se replicar, costumam permanecer indefinidamente no PC ou se auto-destruir juntamente com os dados que visa apagar ou corromper. A sua propagação se dá apenas por meio canais de distribuição como Internet e BBSs, normalmente colocados a disposição como um programa muito útil e até mesmo milagroso. São assim, voluntariamente downlodeados por usuários incautos, enganados quanto aos reais efeitos do programa, e a partir deles, eventualmente, para outros usuários.

Como atuam tecnicamente
O trojan para ambiente Windows, depois de executado pela primeira vez, adiciona linhas ao registro do sistema para ser executado automaticamente toda vez que o Windows for iniciado. Em tempo de execução, deixa aberta uma das inúmeras portas de comunicação do sistema operacional, o que a faz ficar à espera de uma conexão. Os dois trojans do momento fazem isso abrindo a porta 1234 (Netbus) e 31337 (Back Orifice) por default, esperando assim, por conexões de clientes (atacantes).

Tipos mais comuns

Trojan Horse	Tamanho executável (Kb)	Porta aberta por default
BackOrifice	122	31337
Netbus	461	12345, 12346 e 20034
De Troie	331	61802 e 61194
Winnuke	188	50505
Icqrev	322	12076
Ickiller	420	7789
Master Paradise	1234	561

Existem mais de 50 trojans conhecidos

O potencial
Uma vez instalado na máquina da vítima, o trojan permite que o cliente (atacante) tenha perigosas permissões como: executar e fechar programas, apagar, renomear, criar e copiar arquivos, tocar sons, encerrar a conexão, travar o teclado e o micro, abrir e fechar a porta do cdrom, capturar as senhas do usuário e até mesmo capturar telas e todas as teclas pressionadas. É importante dizer que em se tratando de programas dinâmicos e cheios de detalhes, todas as recomendações possuem mais de uma alternativa, seja de configuração, detecção ou remoção.

Detectando o Netbus
É possível detectar o NetBus sem um programa antivírus. Proceda da seguinte maneira:

1. No menu INICIAR, clique em PROGRAMAS e depois em PROMPT do MS-DOS.
2. Na janela do MS-DOS, digite netstat –an | find "12345"
3. Caso o NetBus esteja hospedado na sua máquina, pode aparecer uma linha de comando com as seguintes características:
   TCP 0.0.0.0:12345 0.0.0.0:0 LISTENING

Eliminando o Netbus
Existem programas escritos especialmente para removê-lo, mas ele também pode removido manualmente. Proceda da seguinte maneira :

1. Conecte-se (se necessário);
2. Em INICIAR, EXECUTAR, digite WINIPCFG;
3. Anote o endereço IP;
4. Em INICIAR, EXECUTAR, digite TELNET, seguido do endereço anotado mais 12345. (Exemplo: telnet 200.300.100.1 12345).
5. Digite Password;1; e tecle enter, e
6. Digite RemoveServer;1 e tecle enter.

Pronto, seu computador está livre do NetBus.

Detectando o Back Orifice
É possível detectar o Back Orifice (BO) sem um programa antivírus. Proceda da seguinte maneira:

1. No menu INICIAR, clique em PROGRAMAS e depois em PROMPT do MS-DOS.
2. Na janela do MS-DOS, digite netstat –an | find "31337"
3. Caso o Back Orifice esteja hospedado na sua máquina, pode aparecer uma linha de comando com as seguintes características:
   TCP 0.0.0.0:31337 0.0.0.0:0 LISTENING

Eliminando o Back Orifice

Existem programas escritos especialmente para removê-lo, mas ele também pode removido manualmente. Proceda da seguinte maneira :

1. Em INICIAR, EXECUTAR, digite REGEDIT;
2. Obs.: Cuidado no manuseio do registro, sua importância para o perfeito funcionamento do sistema é enorme. Se tiver dúvidas, procure esclarecimentos.
3. Abra o registro e vá entrando nas pastas indicadas abaixo com duplo clique "KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices" (clique duas vezes em HKEY_LOCAL_MACHINE, depois duas vezes em SOFTWARE, e assim por diante).
4. Na coluna da direita, deverá aparecer uma série de programas que são executados quando o Windows é inicializado. Apague a linha que contém o arquivo BOSERVER.EXE (normalmente ele recebe este nome). Para verificar, compare seu tamanho com o tamanho original do BOSERVER que é 122Kb.

5. Agora reinicie o Windows e finalmente apague o arquivo (BOSERVER.EXE) que você encontrou.

Pronto, seu computador está livre do Back Orifice.

Monitorando o ataque do Back Orifice
Existem vários programas que detectam o Back Orifice, mas nenhum destes pode avisá-lo quando alguém com o BO Client o está usando para invadir o seu computador. Por isso, o NOBO é imprescindível para quem quer descobrir o atacante que quer furar a segurança do seu sistema. O NOBO não impede que o BO se instale na sua máquina, nem é capaz de removê-lo caso ele já esteja instalado, mas permite descobrir o endereço IP da pessoa que está fazendo o ataque e ainda pode enviar uma mensagem personalizada como resposta à fracassada tentativa de invasão.

Tamanho: 67Kb
Status: Freeware
Download: http://web.cip.com.br/nobo/nobo.html

A prevenção
Antivírus normalmente detectam trojan horses e as precauções que tomamos para evitar vírus costumam ser suficientes para evitá-los. Entretanto, devemos estar cientes de que trojans não se limitam às características dos vírus - podem ser potencialmente mais perigosos e de payload imediato. Programas desconhecidos e de origem duvidosa, mesmo que passem pelo antivírus, devem ser executados com cautela, de preferência em computadores devidamente "backupeados" e, se possível, em um computador "cobaia", cujo disco rígido não possua nada indispensável. Cabe lembrar, que se for notada a presença de um trojan, o mesmo deve ser devidamente identificado para que se possa tomar as medidas corretivas próprias à cada tipo.

Em tempo, existem diversos programas desenvolvidos especificamente para monitorar e retirar os trojans, e por possuirem características diferentes, você deverá se armar de um anti-trojan para cada tipo.

As recomendações
Alguns procedimentos de prevenção são suficientes para fechar o cerco a um eventual primeiro contato com um trojan horses e estão descritos abaixo:

1. Jamais abra ou execute arquivos suspeitos ou de origem não confiável obtidos via Internet ou BBS. Jamais abra ou execute arquivos attachados em e-mails sem checagem contra vírus. Contudo, pode ficar relativamente tranqüilo quanto aos e-mails propriamente ditos, eles em si são inofensivos, ao contrário dos boatos comuns indicando o contrário.

2. Atualize constantemente seu antivírus. Usualmente são disponibilizados na Internet e em BBSs atualizações mensais que podem ser downlodeadas na forma de arquivos executáveis ou acessadas diretamente na forma de smart-updates pelo seu antivírus.

3. Lembra-se sempre de se proteger, mesmo que seus remetentes lhe pareçam confiáveis. Eles podem estar sendo vítimas passivas e simplesmente propagando inconscientemente um desses cavalos de tróia.

A realidade
Para lidarmos com os vírus, devemos ter uma idéia clara em mente: não existem computadores imunes à vírus. Um fato essencial não pode ser desprezado em nenhuma estratégia de prevenção contra vírus de PC e danos causados por eles, pois não existem programas que possam nos dar 100% de proteção. Novos vírus estão sempre surgindo, eles são projetados para burlar os antivírus. Arquivos que não são atualmente checados por antivírus, podem ser hospedeiros de vírus amanhã. Portanto, fazendo uma analogia ao automóvel: tenha sempre o seguro em dia.

Softwares antitrojans
Higienic Paper (339Kb) - http://members.xoom.com/tkover/faq/hpth_200.exe
Cleaner (144Kb) - http://members.xoom.com/tkover/faq/cleaner19c.zip
Detectam e eliminam do computador os trojans Netbus e Back Orifice simultaneamente.

BODetect - http://www.plugue.com.br/avisos.html
AntiGen – http:// http://www.geocities.com/siliconvalley/chip/5510/frames/antigen.zip
NOBO - http://web.cip.com.br/nobo/nobo.html
NetbusOff - http://www.geocities.com/siliconvalley/chip/5510/frames/netbusoff.zip
NetBuster - http://www.geocities.com/siliconvalley/chip/5510/frames/netbuster.zip

Softwares antivírus
Dr Solomon - http://www.drsolomon.com/index_new.cfm
Dr Solomon's Download – http://www.drsolomon.com/download/index.cfm
Symantec – http://www.symantec.com/region/br/
SARC Download Updates – http://www.symantec.com/avcenter/download.html
McAfee – http://www.mcafee.com.br/
Network Associates DATs Dnload –
http://www.mcafee.com.br/download/datafile/index.htm
ThunderBYTE – http://www.thunderbyte.com/
ThunderBYTE Anti-Virus Protection Utilities – http://209.95.212.70/antivirus/index.html
F-PROT – http://www.europe.datafellows.com/f-prot/

Parte desta cartilha foi resultado da compilação de informações disponíveis na Internet