O que são Cavalos de Tróia (trojans)?

Uma das formas mais antigas e potencialmente mal compreendidas de malware é o Cavalo de Tróia. Simplificando, um Cavalo de Tróia (Trojan) é um aplicativo de software que é projetado para fornecer acesso secreto ao sistema de uma vítima. O código malicioso é empacotado de tal forma que parece inofensivo e, assim, fica escondido tanto do usuário e do antivírus ou outras aplicações que estão à procura de malwares. Uma vez em um sistema, seus objetivos são semelhantes aos de um vírus ou worm: obter e manter o controle do sistema ou executar alguma outra tarefa.

Uma infecção troiana pode ser indicada por alguns dos seguintes comportamentos:

- A gaveta de CD de um computador abre e fecha, sem motivo aparente;
- A tela do computador muda, movendo ou invertendo;
- As configurações de tela mudam por si mesmas;
- Impressão de documentos sem explicação;
- O navegador é redirecionado para uma página da Web estranha ou desconhecida;
- As configurações de cores do Windows são alteradas;
- As configurações da proteção de tela mudam;
- Os botões direito e esquerdo do mouse invertem suas funções;
- O ponteiro do mouse desaparece;
- O ponteiro do mouse se move de maneiras inexplicáveis;
- O botão Iniciar desaparece;
- As caixas de chat aparecem;
- O provedor de serviços de Internet (ISP) informa que o computador da vítima está executando scan em portas;
- As pessoas que conversam com você parecem saber informações pessoais detalhadas sobre você;

- O sistema é desligado sozinho;
- A barra de tarefas desaparece;
- Senhas de conta são alteradas;
- As contas legítimas são acessadas sem autorização;
- Declarações de compra desconhecidas aparecem em contas de cartão de crédito;
- Os modems ligam e se conectam à Internet por si mesmos;
- Ctrl + Alt + Del para de funcionar;
- Quando o computador é reinicializado, uma mensagem informa que outros usuários ainda estão conectados;

As operações que podem ser realizadas por um hacker em um sistema de computador alvo incluem:

- Roubo de dados;
- Instalação de software;
- Faz o download ou o upload de arquivos;
- Modifica arquivos;
- Instalação de keyloggers;
- Visualiza a tela do usuário do sistema;
- Consumindo espaço de armazenamento do computador;
- Causa um crash no sistema da vítima.

Antes de continuar no assunto dos Trojans, você precisa saber sobre *covert channel* e *overt channel*. Um cavalo de Tróia confia nestes itens:

- Um overt channel (canal aberto) é um caminho de comunicação ou canal que é usado para enviar informações ou executar outras ações. HTTP e TCP/IP são exemplos de mecanismos de comunicação que podem e enviam informações legitimamente;
- Um covert channel (canal secreto) é um caminho que é usado para transmitir informações, mas o faz de uma forma que é ilegítimo ou supostamente impossível, mas é capaz de contornar a segurança. O covert channel viola a política de segurança em um sistema.

Por que um invasor usa um cavalo de Tróia em vez de um vírus?

A razão é porque um Trojan é mais furtivo e ainda abre um canal secreto que pode ser usado para transmitir informações. Os dados transmitidos podem ser um número de itens, incluindo informações de identidade.

Tipos de Trojans

Trojans de Acesso Remoto (Remote Access Trojans – RATs) – Projetados para fornecer um controle remoto do sistema da vítima. Dois membros bem conhecidos desta classe são o programa SubSeven e seu primo, Back Orifice, embora ambos sejam exemplos bem antigos.

Envio de dados – Para se enquadrar nesta categoria, um cavalo de Tróia deve capturar algum tipo de dados do sistema da vítima, incluindo arquivos e o que foi digitado. Uma vez capturados, estes dados são transmitidos por e-mail ou outros meios se o cavalo de Tróia estiver habilitado. Os keyloggers são trojans comuns desse tipo.

Destrutivo – Este tipo de Trojan procura corromper, apagar ou destruir dados do sistema. Em casos mais extremos, o cavalo de Tróia pode afetar o hardware de tal forma que ele se torna inutilizável.

Proxy – Malware desse tipo faz com que um sistema seja usado como um proxy pelo atacante. O atacante usa o sistema da vítima para escanear ou acessar outro sistema ou local. O resultado é que o atacante real fica difícil de ser encontrado.

FTP – Software nesta categoria é projetado para configurar o sistema infectado como um servidor FTP. Um sistema infectado se torna um servidor hospedando todos os tipos de informações, que podem incluir conteúdo ilegal de todos os tipos.

Desativadores de software de segurança – Um cavalo de Tróia pode ser usado como o primeiro passo em novos ataques se for

usado para desabilitar o software de segurança.

Detectando Trojans e Vírus

Um trojan pode ser detectado de várias maneiras. Um escaneamento de portas pode ser bem efetivo se vocês souber o que está procurando.

Como um cavalo de Tróia é usado para permitir acesso através de backdoors ou canais secretos, a porta deve ser aberta para permitir essa comunicação. Uma varredura de porta usando uma ferramenta como o Nmap revela essas portas e permite que você investigue ainda mais. As seguintes portas são usadas para Trojans clássicos:

- Back Orifice—UDP 31337 ou 31338
- Back Orifice 2000—TCP/UDP 54320/54321
- Beast—TCP 6666
- Citrix ICA—TCP/UDP 1494
- Deep Throat—UDP 2140 e 3150
- Desktop Control—UDP NA
- Loki—Internet Control Message Protocol (ICMP)
- NetBus—TCP 12345 e 12346
- Netcat—TCP/UDP (qualquer porta)
- NetMeeting Remote—TCP 49608/49609
- pcAnywhere—TCP 5631/5632/65301
- Reachout—TCP 43188
- Remotely Anywhere—TCP 2000/2001
- Remote—TCP/UDP 135-1139
- Whack-a-Mole—TCP 12361 e 12362
- NetBus 2 Pro—TCP 20034
- GirlFriend—TCP 21544
- Masters Paradise—TCP 3129, 40421, 40422, 40423 e 40426
- Timbuktu—TCP/UDP 407
- VNC—TCP/UDP 5800/5801

Usando o Netstat para detectar portas abertas

Outra ferramenta que auxilia na detecção de Trojans é o **netstat**. Esta ferramenta pode listar as portas abertas e de escuta por conexões no sistema. Para usar netstat, siga estas etapas no Windows:

1. Abra um prompt de comando (cmd);
2. Na linha de comando, insira **netstat -an** (observe que o comando é caso sensível).
3. Observe os resultados.

Você deve ver que várias portas estão abertas e ouvindo. Você pode não reconhecer todos os números, mas isso não significa que eles são maliciosos. Você pode pesquisar pelas portas abertas (elas variam de sistema para sistema) para ver com o que cada um se relaciona.

Note que embora as portas aqui se refiram a alguns exemplos clássicos de Trojans, há muitos novos. Não podemos listá-los todos, porque eles estão sempre evoluindo e as portas mudam.

Usando o TCPView para rastrear o uso da porta

Netstat é uma ferramenta poderosa, mas uma das suas deficiências é o fato de que não é tempo real. Se você deseja controlar o uso da porta em tempo real, você pode usar ferramentas como TCPView. Se você ainda não tiver TCPView, você pode baixá-lo de www.microsoft.com. Para usar TCPView, siga estas etapas:

1. No Windows, execute o executável tcpview.exe
2. Observe os resultados nainterface;
3. Com o TCPView ainda em execução, abra um navegador da Web e abra o site www.google.com.br.

4. No TCPView, repare os resultados e adicione novas entradas.
5. No navegador, vá para www.youtube.com (ou outro site que transmite vídeo ou áudio), e reproduza um vídeo ou um pedaço de conteúdo.
6. No TCPView, observe como as entradas mudam à medida que as portas são abertas e fechadas. Observe por um minuto ou dois e observe como o visor é atualizado.
7. Feche o navegador da Web.
8. No TCPView, observe como o monitor é atualizado como algumas conexões e aplicativos são removidos.

O que é realmente conveniente sobre o TCPView é que ele codifica os resultados em cores: Vermelho – Significa que uma conexão será fechada em breve, e verde significa que uma conexão foi aberta.

Ao usar TCPView, você pode salvar momentos do conteúdo da tela em um arquivo TXT. Este recurso é extremamente útil para investigação e posterior análise de informações e potencialmente para fins de gerenciamento de incidentes mais tarde.

Ferramentas para criar cavalos de Tróia

Existe uma ampla gama de ferramentas que são usadas para assumir o controle do sistema de uma vítima e deixar para trás um presente na forma de um backdoor. Esta não é uma lista exaustiva, e versões mais recentes de muitos destes são lançados regularmente:

Let Me Rule – Um Trojan de acesso remoto criado inteiramente em Delphi. Ele usa a porta TCP 26097 por padrão.

Remote Encrypted Callback Unix Backdoor (RECUB) – Tem o seu nome do mundo Unix. Ele possui criptografia RC4, injeção de

código e solicitações de comunicação ICMP criptografadas. Demonstra um traço chave do Trojan – de tamanho pequeno – já que seu tamanho tem menos de 6 KB.

Phatbot – Capaz de roubar informações pessoais, incluindo endereços de e-mail, números de cartões de crédito e códigos de licenciamento de software. Ele retorna essas informações para o invasor ou solicitante usando uma rede P2P. Phatbot também pode encerrar muitos antivírus e produtos de firewall baseados em software, deixando a vítima aberta a ataques secundários.

Amitis – Abre a porta TCP 27551 para dar ao hacker controle completo sobre o computador da vítima.

Zombam.B – Permite que o invasor use um navegador da Web para infectar um computador. Ele usa a porta 80 por padrão e é criado com uma ferramenta de geração de cavalos de Tróia conhecida como HTTPRat. Assim como o Phatbot, ele também tenta encerrar diversos processos antivírus e de firewall.

Beast – Usa uma técnica conhecida como injeção de Data Definition Language (DDL) para se injetar em um processo existente, escondendo-se efetivamente dos visualizadores de processo.

Hard-Disk Killer – Um Trojan escrito para destruir o disco rígido de um sistema. Quando executado, ele ataca o disco rígido de um sistema e limpa-o em apenas alguns segundos.

Uma ferramenta que deve ser mencionada é Back Orifice, que é uma das ferramentas de criação de cavalos de Tróia mais antigas. A maioria, se não todos, dos aplicativos antivírus em uso hoje deve ser capaz de detectar e remover este software.
Eu pensei que seria interessante olhar para o texto que o fabricante usa para descrever o seu toolkit. Observe que isso

soa muito parecido com a maneira como um aplicativo de software normal de um grande fornecedor seria descrito. O fabricante do Back Orifice diz isso sobre Back Orifice 2000 (BO2K):

> *Construído sobre o sucesso fenomenal de Back Orifice lançado em agosto de 98, BO2K coloca administradores de rede solidamente de volta no controle. No controle do sistema, rede, registro, senhas, sistema de arquivos e processos. BO2K é muito parecido com outros grandes pacotes de sincronização de arquivos e controle remoto que estão no mercado como produtos comerciais. Exceto que BO2K é menor, mais rápido, livre e muito, muito extensível. Com a ajuda da comunidade de desenvolvimento open-source, BO2K vai crescer ainda mais poderoso. Com novos plug-ins e recursos sendo adicionados o tempo todo, BO2K é uma escolha óbvia para o administrador da rede.*

Um olhar em profundidade no BO2K

Se você o considera um Trojan ou uma ferramenta remota do administrador, os recursos de BO2K são razoavelmente extensivos para algo deste tipo. Esta lista de características é adaptada do site do fabricante:

- Lista de servidores do catálogo de endereços
- Funcionalidade que pode ser estendida através do uso de plug-ins
- Várias conexões de servidor simultâneas
- Capacidade de registro de sessão
- Suporte ao servidor nativo
- Capacidade de keylogging
- Navegação e transferência do sistema de arquivos do Hypertext Transfer Protocol (HTTP)
- Compartilhamento de arquivos de rede da Microsoft
- Edição remota do registro
- Navegação, transferência e gerenciamento de arquivos

- Extensibilidade do plug-in
- Atualização remota, instalação e desinstalação
- Redirecionamento de rede de conexões TCP / IP (protocolo de controle de transferência / protocolo Internet)
- Capacidade de acessar programas de console, como shells de comando por meio do Telnet
- Suporte multimídia para captura de áudio / vídeo e reprodução de áudio
- Windows NT senhas de registro e proteção de tela Win9x senha de proteção
- Controle de processo, início, parada e lista
- Várias conexões de cliente em qualquer meio
- Mensagens da GUI

O BO2K é uma ferramenta de última geração que foi projetada para aceitar plug-ins personalizados, especialmente projetados. É uma ferramenta perigosa nas mãos erradas. Com a capacidade do software para ser configurado para realizar um conjunto diverso de tarefas a pedido do atacante, pode ser uma ferramenta devastadora.

O BO2K consiste de dois componentes de software: um cliente e um servidor. Para usar o servidor BO2K, a configuração é a seguinte:

1. Inicie o Wizard do BO2K e clique em Avançar quando a tela inicial do assistente for exibida.
2. Quando solicitado pelo assistente, digite o executável do servidor a ser editado.
3. Escolha o protocolo sobre o qual executar a comunicação do servidor. A escolha típica é para usar TCP como o protocolo, devido à sua robustez inerente. UDP normalmente é usado se um firewall ou outra arquitetura de segurança precisa ser percorrida.
4. A tela seguinte pergunta qual número de porta será usado. A porta 80 é geralmente aberta, e por isso é mais usado, mas você pode usar qualquer porta aberta.
5. Na próxima tela, digite uma senha que será usada para

acessar o servidor. Note que as senhas podem ser usadas, mas você também pode escolher a autenticação aberta – isso significa que qualquer pessoa pode obter acesso sem ter que fornecer credenciais de qualquer tipo.
6. Quando o assistente terminar, a ferramenta de configuração do servidor é fornecida com as informações inseridas.
7. O servidor pode ser configurado para iniciar quando o sistema é iniciado. Isso permite que o programa seja reiniciado sempre que o sistema for reinicializado, impedindo que o programa fique indisponível.
8. Clique em Salvar servidor para salvar as alterações e confirmá-las ao servidor.

Uma vez que o servidor está configurado, ele está pronto para ser instalado no sistema da vítima.

Não importa como a instalação deve ocorrer, o único aplicativo que precisa ser executado no sistema de destino é o executável do BO2K. Após a execução deste aplicativo, a porta configurada anteriormente está aberta no sistema da vítima e pronta para aceitar a entrada do invasor.

O aplicativo também executa um arquivo executável chamado Umgr32.exe e coloca-lo na pasta Windows system32. Além disso, se você configurar o executável BO2K para executar no modo furtivo, ele não aparecerá no Gerenciador de tarefas – ele modifica um processo em execução existente para atuar como sua capa. Se o modo stealth não foi configurado, o aplicativo aparece como um serviço de administração remota.

O atacante agora tem um ponto de apoio no sistema da vítima.

Distribuição de cavalos de Tróia

Uma vez que um cavalo de Tróia foi criado, você deve abordar como entrar no sistema de uma vítima. Para esta etapa, muitas opções estão disponíveis, incluindo ferramentas conhecidas

como wrappers.

Usando Wrappers para instalar Trojans

Usando wrappers, os atacantes podem pegar sua carga útil e fundi-la com um executável inofensivo para criar um único executável a partir dos dois. Alguns programas de estilo wrapper mais avançados podem até mesmo vincular vários aplicativos em vez de apenas dois. Neste ponto, o novo executável pode ser lançado em um local onde provavelmente será baixado.

Considere uma situação em que um possível atacante baixe um aplicativo autêntico do site de um fornecedor e usa wrappers para mesclar um cavalo de Tróia (BO2K) no aplicativo antes de publicá-lo em um grupo de notícias ou em outro local. O que parece inofensivo para o downloader é realmente uma bomba à espera de ir para fora no sistema. Quando a vítima executa o software infectado, o infector instala e assume o sistema.

Alguns dos programas wrapper mais conhecidos são os seguintes:

- **EliteWrap** é uma das ferramentas de envolvimento mais populares, devido ao seu rico conjunto de recursos que inclui a capacidade de executar verificações de redundância em arquivos mesclados para garantir que o processo foi corretamente e a capacidade de verificar se o software será instalado conforme o esperado. O software pode ser configurado até o ponto de permitir que o invasor escolha um diretório de instalação para a carga. Software embrulhado com EliteWrap pode ser configurado para instalar silenciosamente sem qualquer interação do usuário.
- **Saran Wrap** é projetado especificamente para trabalhar com e ocultar o Back Orifice. Ele pode agrupar Back Orifice com um programa existente no que parece ser um programa padrão usando o Install Shield.
- O **Trojan Man** funde programas e pode criptografar o novo

pacote para esconder-se dos programas antivírus.

- **Teflon Oil Patch** é projetado para ligar Trojans a um arquivo especificado a fim de desligar aplicações detectoras de Trojan.
- **Restorator** foi projetado com as melhores intenções, mas agora é usado para fins menos do que honorável. Ele pode adicionar uma carga em, por exemplo, um protetor de tela aparentemente inofensivo, antes de ser encaminhado para a vítima.
- **Firekiller 2000** foi projetado para ser usado com outras aplicações quando embrulhado. Este aplicativo desativa o firewall e o software antivírus. Programas como o Norton Antivirus e o McAfee VirusScan eram alvos vulneráveis ??antes de serem corrigidos.

Kits de construção de Trojan

Assim como para vírus e worms, vários kits de construção estão disponíveis que permitem a rápida criação e implantação de Trojans. A disponibilidade desses kits tornou a criação e implantação de malware mais fácil do que nunca:

Trojan Construction Kit – Um dos melhores exemplos de uma ferramenta relativamente fácil de usar, mas potencialmente destrutiva. Este kit é baseado em linha de comando, o que pode torná-lo um pouco menos acessível para a pessoa comum, mas ainda assim é muito eficaz nas mãos certas. Com um pouco de esforço, é possível construir um cavalo de Tróia que pode se envolver em comportamento destrutivo, como destruir tabelas de partição, registros de inicialização mestre (MBRs) e discos rígidos.

Senna Spy – Outro kit de criação de cavalos de Tróia que oferece opções personalizadas, como transferência de arquivos, execução de comandos DOS, controle de teclado e processos de lista e controle.

Stealth Tool – Um programa usado para não criar cavalos de

Tróia mas para ajudá-los a se esconder. Na prática, essa ferramenta é usada para alterar o arquivo de destino movendo bytes, alterando cabeçalhos, dividindo arquivos e combinando arquivos.

Backdoors

Muitos atacantes ganham acesso ao seu sistema de destino através de um backdoor. O proprietário de um sistema comprometido desta forma pode não ter nenhuma indicação de que outra pessoa está usando o sistema.

Quando implementado, um backdoor tipicamente atinge um ou mais dos seguintes objetivos principais:

1. Permite que um invasor acesse um sistema mais tarde ignorando quaisquer contra medidas que o proprietário do sistema possa ter colocado.
2. Fornece a capacidade de obter acesso a um sistema, mantendo um perfil baixo. Isso permite que um invasor acesse um sistema e evite o registro e outros métodos de detecção.
3. Fornece a capacidade de acessar um sistema com o mínimo esforço no menor período de tempo. Sob as condições certas, um backdoor permite que um invasor obtenha acesso a um sistema sem ter que recapturar.

Alguns backdoors comuns que são colocados em um sistema são dos seguintes tipos e propósitos:

1. **Password-cracking backdoor** – Backdoors deste tipo permite um invasor descobrir e explorar senhas fracas que foram configurados pelo proprietário do sistema.
2. **Processo de esconder-backdoor** – Um atacante que quer ficar indetectável pelo maior tempo possível, normalmente escolhe ir a etapa extra de esconder o software que eles estão executando. Programas como um serviço comprometido, um cracker de senhas, sniffers e rootkits são itens que um invasor irá configurar para

evitar a detecção e remoção. As técnicas incluem renomear um pacote para o nome de um programa legítimo e alterar outros arquivos em um sistema para impedir que sejam detectados e executados.

Uma vez que um backdoor está no lugar, um atacante pode acessar e manipular o sistema à vontade.

Sugestões de livros: