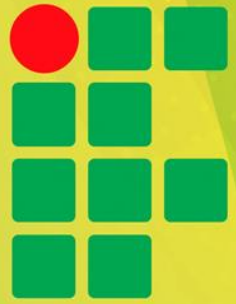
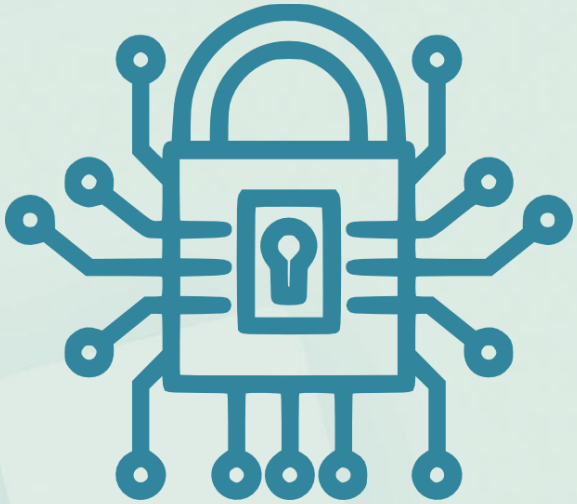


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Códigos Maliciosos

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

Backdoor

- Backdoor é um programa que **permite o retorno de um invasor** a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

Backdoor

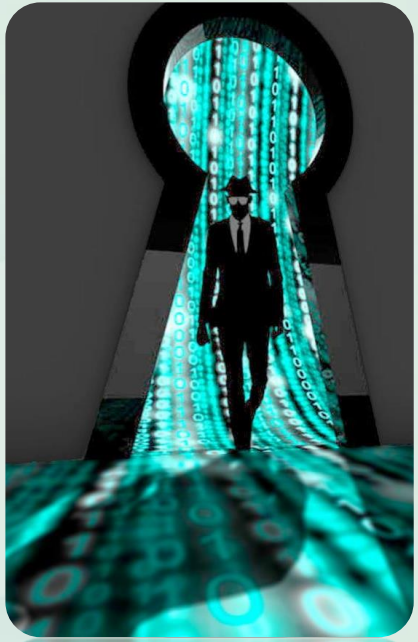
- Pode ser **incluído pela ação de outros códigos maliciosos**, que tenham previamente infectado o computador, **ou por atacantes**, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Backdoor

- Após incluído, o backdoor é usado para **assegurar o acesso futuro** ao computador comprometido, permitindo que ele seja acessado remotamente.

Backdoor

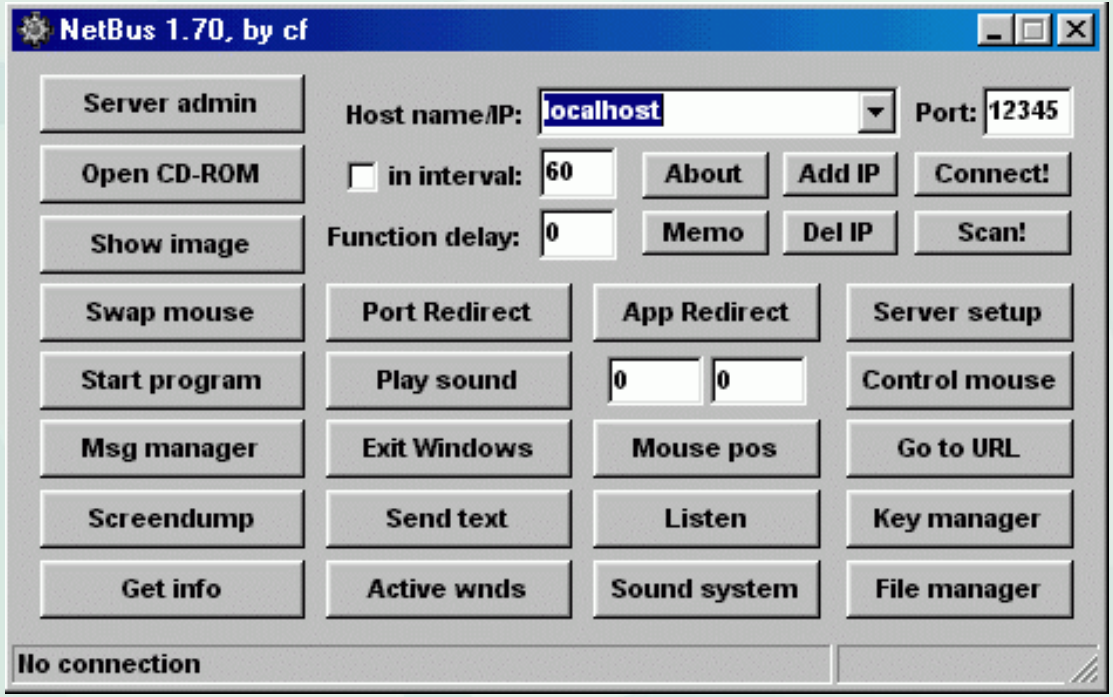
- A forma usual de inclusão de um backdoor consiste na **disponibilização de um novo serviço** ou na **substituição de um determinado serviço** por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto.



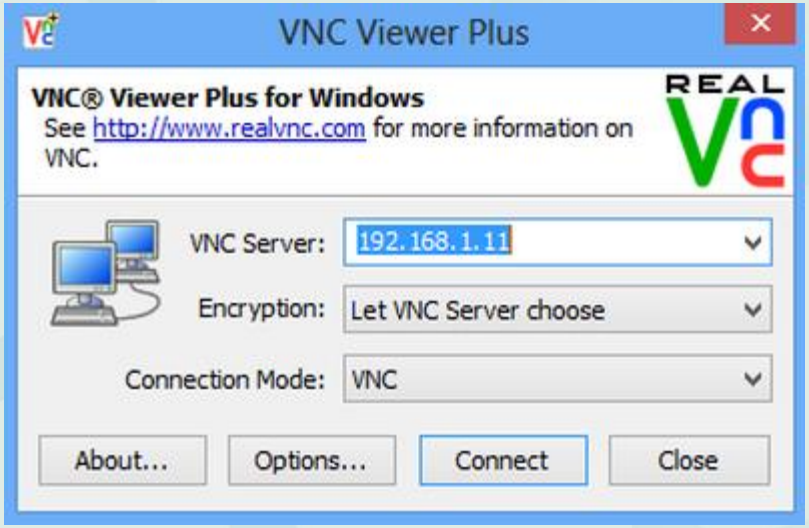
Backdoor

- Alguns programas de administração remota, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors.

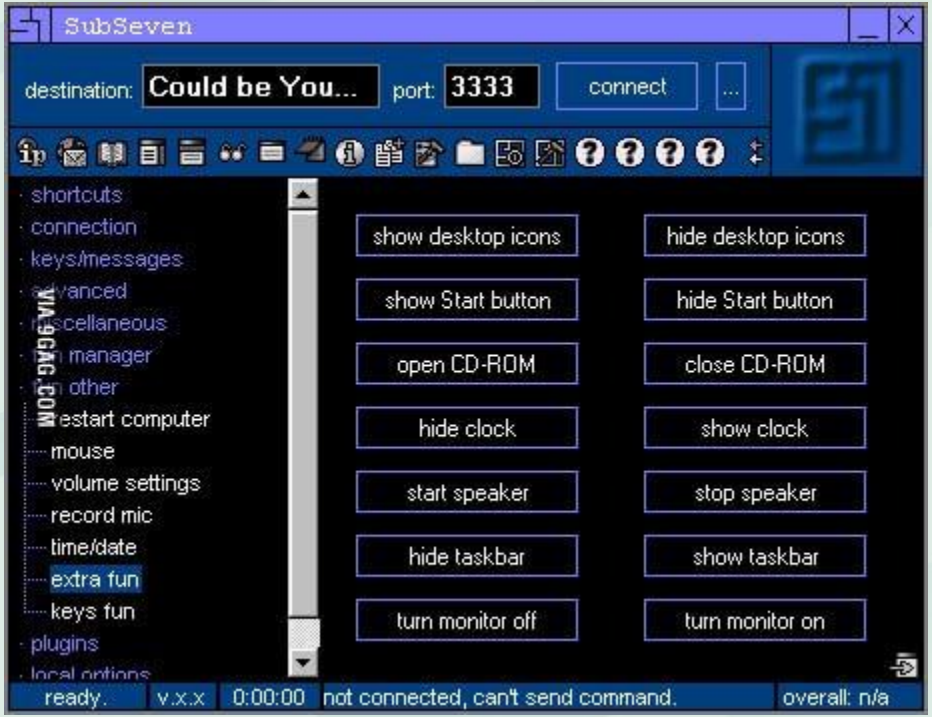
Backdoor: Netbus



Backdoor: VNC

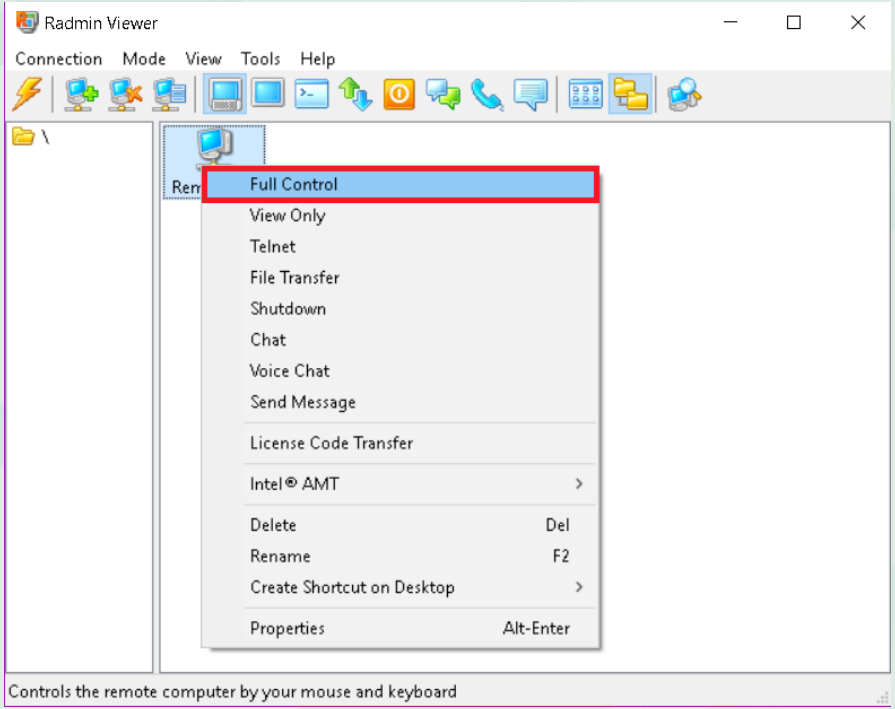


Backdoor: Subseven



INSTITUTO FEDERAL
Sertão Pernambucano

Backdoor: Radmin



Backdoor

- Há casos de backdoors **incluídos propositalmente por fabricantes** de programas, sob alegação de necessidades administrativas.

Backdoor

INSTITUTO FEDERAL
Sertão Pernambucano

Backdoor

Uma análise realizada pelos pesquisadores de segurança Mantas Sasnauskas, do site *cybernews*, James Clee e Roni Carta revelou um fato preocupante: roteadores Wi-Fi da marca chinesa JetStream, vendidos nos EUA exclusivamente pelo Walmart, vem de fábrica com uma backdoor que permite a execução remota de código e controle dos dispositivos conectados à rede.

A mesma pesquisa revelou que roteadores de baixo custo de outra marca chinesa, a Wavlink, vendidos na Amazon e eBay contém a mesma backdoor. De fato, Jetstream e Wavlink parecem ser subsidiárias de uma mesma empresa, a chinesa Winstars Technology Ltd.

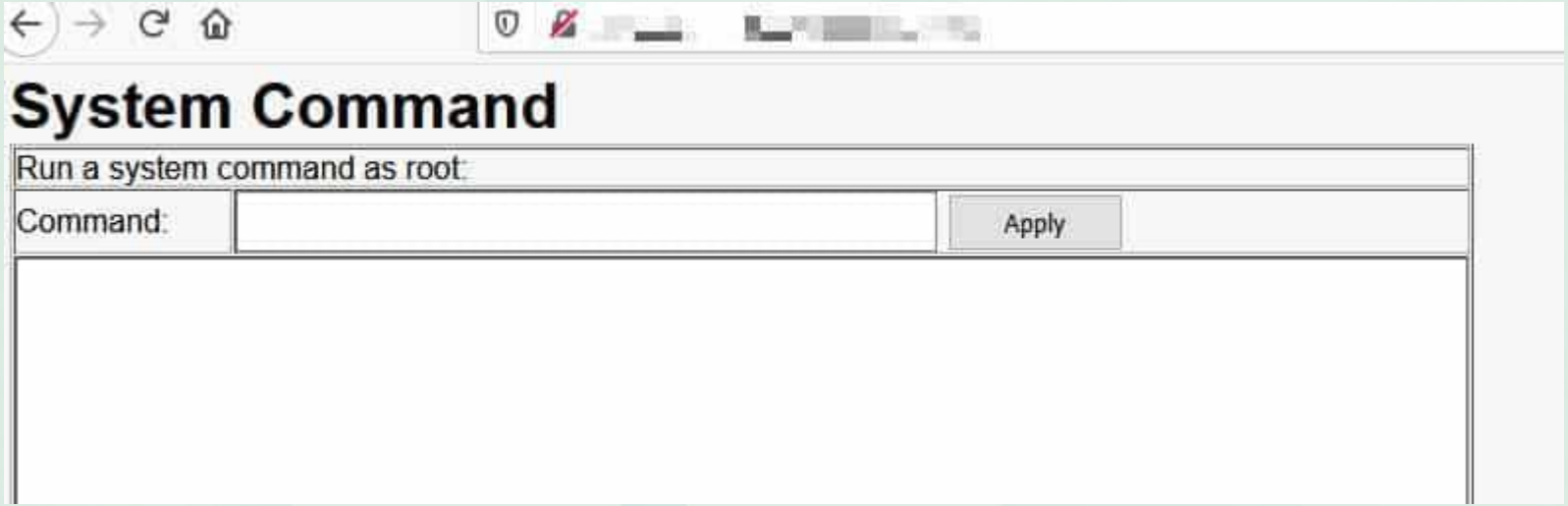
Backdoor

Backdoor

Roteadores Jetstream, como este modelo "gamer" da imagem, chamam a atenção pelo baixo custo e podem ser encontrados por apenas US$ 40 em lojas e no site do Walmart nos EUA.

A backdoor não parece ter sido resultado de um erro de configuração no firmware dos roteadores. Pelo contrário, tem todas as características de ser algo proposital com uma interface web que permite a qualquer um enviar e executar comandos no roteador.

Backdoor



Backdoor

O mais preocupante é que a botnet Mirai que em 2016 deixou quase 1 milhão de pessoas sem acesso à internet na Alemanha, está ativamente explorando a backdoor e infectando os roteadores. Segundo os pesquisadores, imediatamente após conectar um dos aparelhos à internet uma tentativa de conexão foi feita, usando a backdoor para transferir um arquivo com o malware responsável por converter o roteador em um "bot" a serviço da rede.

Backdoor

Os roteadores também tem um script para vasculhar as redes Wi-Fi da vizinhança e tentar se conectar a elas. “Isso levanta várias questões. Porque uma empresa precisaria criar e deixar este script na máquina? Com ele, um agressor poderia comprometer não só o roteador e sua rede, mas também as redes vizinhas. Isto não é e não deveria ser uma prática comum, não neste contexto”, diz Sasnauskas.

Backdoor

Não há muito que o proprietário de um roteador afetado possa fazer. Como a backdoor é integrada ao firmware, boas práticas de segurança como mudar a senha do administrador são ineficazes. O melhor a fazer é parar de usar os equipamentos da Wavlink e Jetstream, e substituí-los por aparelhos de marcas mais tradicionais e confiáveis.

Backdoor

- Diversos recursos podem ser empregados para evitar este problema. O uso de Firewall nos dispositivos e na rede é importante.
- No entanto, um firewall mal configurando pode ser uma brecha que permite a abertura de novas portas.

Cavalo de troia (Trojan)

- Cavalo de troia, trojan ou trojan-horse, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também **executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário**.

Cavalo de troia (Trojan)

- Exemplos de trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros.

Cavalo de troia (Trojan)

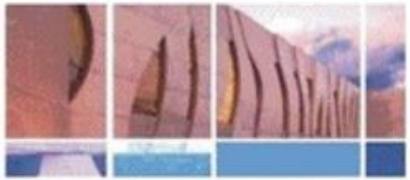
- Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Cavalo de troia (Trojan)

- Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, executem ações maliciosas.

INSTITUTO FEDERAL
Sertão Pernambucano

Tribunal de Justiça



Superior Tribunal de Justiça | O Tribunal da Cidadania

Brasília 17/02/2006

O Superior Tribunal de Justica informa:

De acordo com a lei 1745692-BR foi movido contra você o processo de número 005869/1973 (danos morais) ,o processo entrou em vigor dia 15/02/2006 na segunda vara penal.Para ver mais detalhes do processo veja relatório que dará todas informações neçessárias para realização do julgamento, e cancelamento de processo por erros do sistema. Caso não compareça no lugar especificado no relatório poderá implicar em chamada de segunda estância e/ou recolhimento da sociedade.

Ministro Edson Vidigal - Presidente do Superior Tribunal de Justiça

Tribunal Superior Eleitoral

Bem-vindo ao
TRIBUNAL SUPERIOR ELEITORAL

Brasília, 05 de Fevereiro de 2006

Informamos que seu titulo eleitoral teve um **Cancelamento provisório**.

O motivo do cancelamento foi uma irregularidade em seu Cadastro de Pessoa Física (CPF) a qual motivou o cancelamento do mesmo, e também de seu titulo eleitoral.

E-ma

Para saber mais detalhes sobre esta irregularidade, e quais providências tomar, leia o regulamento clicando no link abaixo.

Após clicar no link, será exibida uma janela, onde a opção "Abrir" deve ser clicada.

CLIQUE AQUI PARA ABRIR O REGULAMENTO

ou se não conseguir Clique Aqui

INFOWESTER.COM

Todos os direitos reservados ao Tribunal Superior Eleitoral

Cavalo de troia (Trojan)

- **Trojan Downloader:** instala outros códigos maliciosos, obtidos de sites na Internet.

- **Trojan Dropper:** instala outros códigos maliciosos, embutidos no próprio código do trojan.

Cavalo de troia (Trojan)

- **Trojan Backdoor:** inclui backdoors, possibilitando o acesso remoto do atacante ao computador.

- **Trojan DoS:** instala ferramentas de negação de serviço e as utiliza para desferir ataques.

Cavalo de troia (Trojan)

- **Trojan Destrutivo:** altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
- **Trojan Clicker:** redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.

Cavalo de troia (Trojan)

- **Trojan Proxy**: instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.
- **Trojan Spy:** instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

Cavalo de troia (Trojan)

- **Trojan Banker ou Bancos:** coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy porém com objetivos mais especéficos.


Buscar
techtudo DOWNLOADS
Segurança
Novo Trojan grava tela do PC enquanto usuário acessa site pornô
Ameaça tem como alvo funcionários de empresa na França e pode ser usada em golpes de sextorsão
Por Ana Letícia Loubak, para o TechTudo
10/08/2019 06h00 · Atualizado há 2 anos

Rootkit

- Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Rootkit

- Quando um rootkit assume o controle, **seu sistema age como se fosse um computador zumbi**, e o cibercriminoso pode exercer **controle absoluto no dispositivo** por acesso remoto. Essa parte da definição de rootkit é o que o torna tão poderoso.

Rootkit

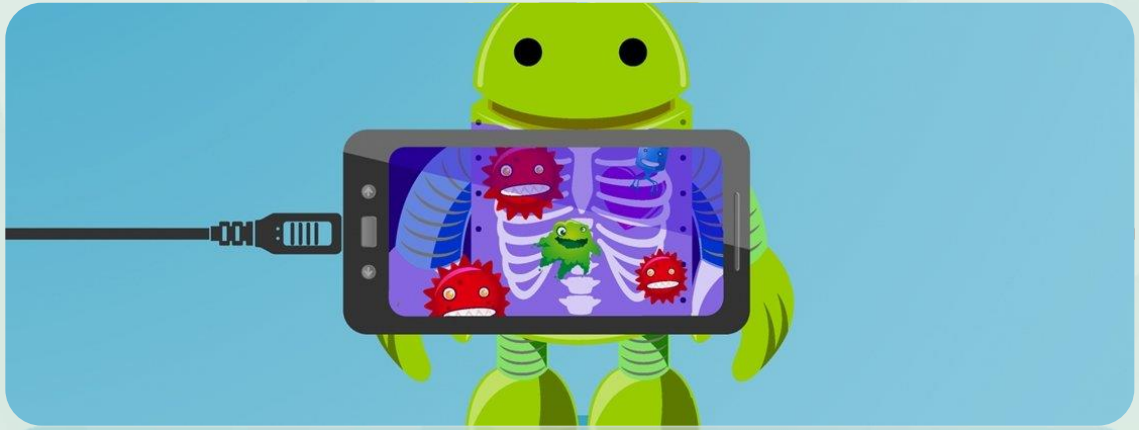
- Rootkits fazem o computador mentir para você e, às vezes, para o software antivírus e de segurança também.

Rootkit

- **O que um rootkit modifica?**
- Como a finalidade de um rootkit é obter acesso privilegiado de administrador ao sistema de computador, um rootkit **pode modificar tudo que um administrador pode**. Veja uma lista curta do que um rootkit pode fazer ou modificar.

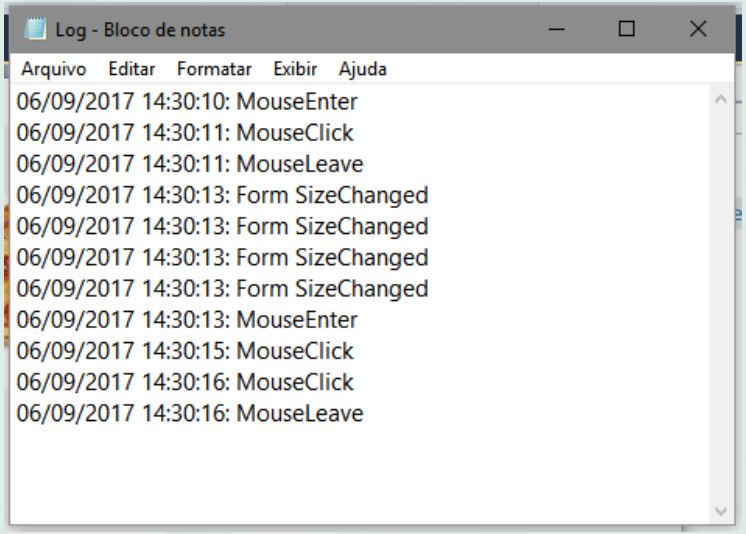
Rootkit

- **Ocultar malware:** rootkits ocultam outros tipos de malware no seu dispositivo e dificulta a remoção deles.



Rootkit

- **Remover evidências em arquivos de logs.**



Rootkit

- **Obter acesso remoto:** rootkits oferecem acesso remoto ao sistema operacional enquanto evitam serem detectados. Instalações de rootkit estão cada vez mais associadas com golpes de acesso remoto.

Rootkit

- **Violam ou desativam programas de segurança:** alguns rootkits podem se esconder dos programas de segurança do computador ou desativá-los completamente, dificultando a detecção e a remoção de malware.

Rootkit

- **Roubar dados:** na maioria das vezes, os cibercriminosos usam rootkits para roubar dados.
- Alguns cibercriminosos atacam indivíduos e coletam dados pessoais para roubo de identidade ou fraude. Outros perseguem alvos corporativos para cometer espionagem ou crimes financeiros.

Rootkit

- **Criar um “backdoor” permanente:** alguns rootkits podem criar um “backdoor” de segurança cibernética no sistema, que permanece aberto para que o cibercriminoso possa retornar posteriormente.

Rootkit

- **Espionar suas atividades:** rootkits podem ser usados como ferramentas de monitoramento, o que permite espionagem por parte de cibercriminosos
- **Invadir sua privacidade:** com um rootkit, um cibercriminoso pode interceptar o tráfego da internet, acompanhar as teclas digitadas e até ler e-mails.

Rootkit

- **Espionar suas atividades:** rootkits podem ser usados como ferramentas de monitoramento, o que permite espionagem por parte de cibercriminosos
- **Invadir sua privacidade:** com um rootkit, um cibercriminoso pode interceptar o tráfego da internet, acompanhar as teclas digitadas e até ler e-mails.

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano