



McAfee System Protection

Os invasores e suas ferramentas: Como o McAfee Enterscept protege os servidores

White Paper do McAfee Enterscept

Índice

I. A caixa de ferramentas do invasor	3
1. Worms	3
2. Ataques do tipo buffer overflow	3
3. Ataques do tipo elevação de privilégio	4
4. Cavalos de Tróia	4
5. Backdoors	4
6. Rootkits	5
7. Ataques a HTTP	5
II. O McAfee Enterecept protege seus servidores	5
1. McAfee Enterecept Standard Edition	6
2. McAfee Enterecept Web Server Edition	6
3. McAfee Enterecept Database Edition	7
III. Resumo: Como o McAfee Enterecept bloqueia as ferramentas dos invasores	8

Os invasores e suas ferramentas: Como o McAfee Enterecept protege os servidores

White Paper do McAfee Enterecept

Ataques contra servidores são responsáveis por bilhões de dólares em danos anualmente. Como estes ataques acontecem? O que as empresas podem fazer para evitá-los? Este documento pretende responder essas perguntas explicando os métodos mais comuns utilizados para comprometer os servidores e como o McAfee Enterecept[®] impede que tais ataques sejam bem-sucedidos.

I. A caixa de ferramentas do invasor

Atualmente, existem muitas ferramentas e métodos de ataque disponíveis para os invasores. Entre os ataques mais comuns a servidores, estão:

- Worms
- Ataques do tipo buffer overflow
- Ataques do tipo elevação de privilégios
- Cavalos de Tróia
- Rootkits
- Backdoors
- Ataques a HTTP

É essencial compreender cada um desses métodos de ataque para combatê-los.

1. Worms

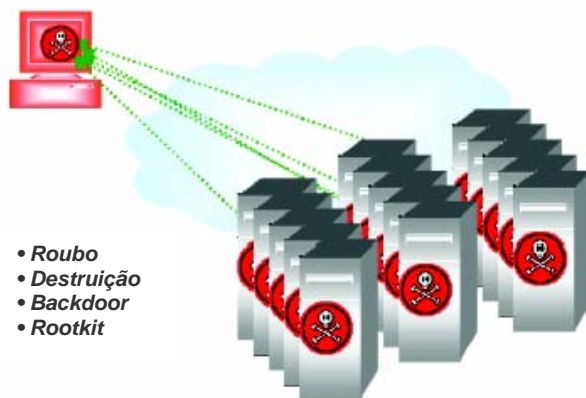
Worms são programas mal-intencionados que se espalham automaticamente, diferentemente dos vírus que precisam de intervenção humana para se propagar (por exemplo, inserir um disquete infectado no computador, clicar duas vezes em um anexo de email, etc.). Worms recentes como Code Red e Nimda causaram danos de bilhões de dólares, despesas com limpeza e perda de negócios. Os invasores agora estão usando os worms com muito mais frequência, pois eles também podem causar grandes danos rapidamente.

Os worms são muito perigosos por vários motivos. Em primeiro lugar, se espalham com muita rapidez. O Code Red infectou mais de 100.000 máquinas em 24 horas. Em segundo, se o worm conseguir obter privilégios suficientes geralmente pode executar qualquer atividade mal-intencionada que o invasor desejar. Em terceiro, estão mais fáceis de se desenvolverem, pois há programas de criação de worms disponíveis na Internet.

Um worm possui três partes principais:

- **Vulnerabilidade**—A “brecha” que o worm explora para obter acesso ao sistema
- **Mecanismo de propagação**—O método usado pelo worm para se comunicar com suas vítimas
- **Carga mal-intencionada**—O dano real causado pelo worm ao comprometer o sistema

Essas três partes variam de worm para worm, mas todos eles possuem esses três elementos.



2. Ataques do tipo buffer overflow

Atualmente, os ataques do tipo buffer overflow são um dos maiores problemas da segurança computacional. Todos os aplicativos possuem buffers contendo dados. Tais buffers têm um tamanho fixo. Se o invasor enviar dados demais para um desses buffers, este “estoura”. Então, o servidor executa os dados “estourados” como um programa. Esse programa pode realizar várias coisas: desde enviar senhas à Rússia até alterar arquivos do sistema; instalar backdoors, etc., dependendo de quais dados o invasor enviou ao buffer.

Os programadores podem impedir esse ataque verificando o volume dos dados enviados antes de armazená-los no buffer. Se houver um volume muito grande de dados é retornado um erro. Infelizmente vários programadores esquecem-se de verificar o volume dos dados antes de salvá-los em um buffer. Assim, os aplicativos contêm um grande número de “buffers não-verificados”, vulneráveis a ataques.

Os invasores e suas ferramentas: Como o McAfee Enterecept protege os servidores

White Paper do McAfee Enterecept

A Microsoft já publicou pelo menos cinco boletins nos últimos seis meses sobre buffers não-verificados existentes em seus produtos. Quando um fornecedor (Microsoft®, entre outros) lança um patch para impedir esses estouros de buffer potenciais, o patch simplesmente adiciona um código que verifica o volume dos dados antes de salvá-los no buffer. Dessa forma, se um patch estiver disponível impedirá o estouro do buffer.

“Em 2001 houve um aumento de 33% no número de empresas atingidas por ataques do tipo buffer overflow...”

Pesquisa de mercado realizada em 2001 pela revista Information Security

Os ataques do tipo buffer overflow são problemas sérios devido aos fatores a seguir:

- Eles são muito comuns. É sabido que centenas de buffers não-verificados podem ser aproveitados pelos hackers, sendo que, outros são descobertos a todo momento. Mais de 50% dos consultores da CERT lidam com ataques do tipo buffer overflow.
- Eles são fáceis de usar. Qualquer um (inclusive crianças de dez anos de idade e “Script Kiddies”) pode baixar um código para ataque de buffer overflow e seguir uma “receita” simples para executá-lo, ou seja, não há necessidade de conhecimento técnico avançado.
- Eles são muito potentes. Em vários casos, o código mal-intencionado executado para causar um buffer overflow tem privilégios de administrador, portanto pode fazer o que quiser no servidor.

3. Ataques do tipo elevação de privilégio

Os ataques do tipo elevação de privilégios concedem direitos de acesso de administrador ou no nível da raiz a usuários que antes não tinham tal privilégio. Por exemplo, há uma conta em todos os servidores Windows NT e 2000 chamada “Convidado”(guest). Por padrão, essa conta não exige senha. Qualquer um pode realizar logon no servidor utilizando a conta “Convidado” e usar uma exploração comum de elevação de privilégios chamada “GetAdmin” para conseguir direito de acesso de administrador ao sistema. Há vários ataques do tipo elevação de privilégio, como HackDLL. Elas são bastante úteis, pois permitem que quaisquer usuários com direito de acesso, de qualquer nível no sistema, eleve seus privilégios facilmente e realize qualquer atividade.

4. Cavalos de Tróia

Na conhecida história do cavalo de Tróia os invasores usaram algo que parecia inofensivo (um enorme cavalo de madeira) para atacar uma cidade protegida. Da mesma forma, os cavalos de Tróia do universo da segurança da informação parecem ser programas inofensivos, entretanto atacam o sistema dos computadores.

Normalmente, os invasores substituem arquivos essenciais ao sistema e/ou programas por versões mal-intencionadas. Quando esses programas são executados executam atividades destrutivas e os usuários não têm como evitá-las.

Por exemplo, um invasor pode substituir uma das DLLs (Dynamically Linked Library) do sistema operacional Windows® por uma versão mal-intencionada. As DLLs são arquivos de programa chamados pelo Windows para realizar várias tarefas. O invasor pode substituir uma dessas DLLs por um cavalo de Tróia que faz tudo o que a DLL normal faz e um pouco mais. Esse “um pouco mais” pode ser várias coisas, desde reformatar o disco rígido até roubar números de cartão de crédito, etc.

5. Backdoors

Quando um invasor consegue direitos de acesso no nível da raiz em um servidor (por exemplo, usando uma exploração de buffer overflow ou de elevação de privilégios), ele fará duas coisas:

1. Instalar um backdoor
2. Ocultar seus rastros

Os backdoors permitem que os invasores acessem remotamente um sistema no futuro. Por exemplo, o invasor pode ter aproveitado uma determinada falha na segurança para obter direitos de acesso no nível da raiz. No entanto, com o tempo, aquela falha de segurança pode ser sanada impedindo que o invasor acesse o sistema novamente. Para evitar serem barrados no futuro, os invasores instalam backdoors. Eles podem tomar diversas formas, mas todos permitem que o invasor acesse o servidor novamente sem ter que passar pelos procedimentos padrão de logon ou ter que repetir o mesmo ataque.

Os invasores e suas ferramentas: Como o McAfee Intercept protege os servidores

White Paper do McAfee Intercept

Vários worms instalam backdoors como parte de sua carga mal-intencionada. O Code Red II, por exemplo, instalou um backdoor que proporcionava acesso às unidades C e D do servidor da Web comprometido a partir de qualquer lugar na Internet. Outros backdoors comuns são o Netbus e o BackOrifice, os quais permitem que os invasores controlem remotamente um servidor comprometido.

6. Rootkits

Os rootkits são usados para ocultar os rastros do invasor. Se o invasor instala um backdoor ou outro programa mal-intencionado, o administrador do sistema pode perceber um novo programa e removê-lo, impedindo que o hacker acesse o sistema no futuro. O objetivo de um rootkit é disfarçar a existência de programas mal-intencionados em um sistema.

Ao substituir certos programas do sistema por versões modificadas, os rootkits mascaram a presença de backdoors ou de outros programas mal-intencionados. Por exemplo, o programa UNIX "ls" imprime uma lista de diretórios do sistema de arquivos. Normalmente, isso permitiria que o administrador do sistema visse os arquivos deixados pelo invasor. O rootkit instala uma versão modificada do "ls" que exibe todos os arquivos e programas no diretório, exceto o backdoor ou qualquer outro arquivo deixado pelo invasor. Isso oculta com eficiência as provas de que o sistema foi comprometido. Geralmente, os rootkits substituem o "ls" e vários outros programas do sistema operacional para ocultar rastros.

7. Ataques a HTTP

Os ataques a HTTP envolvem o uso de um aplicativo do servidor da Web para a execução de atividades mal-intencionadas. Tais ataques são muito comuns e estão crescendo em popularidade, pois, em geral, os firewalls bloqueiam a maior parte do tráfego da Internet para mantê-lo longe dos servidores corporativos. No entanto, o tráfego HTTP, utilizado para a navegação na Web quase sempre passa desimpedido pelos firewalls. Assim, os invasores têm uma linha direta com o servidor da Web. Se for possível fazer o servidor da Web executar atividades mal-intencionadas, recursos que, de outra maneira não estariam disponíveis, poderão ser acessados.

Novos ataques a HTTP aparecem com bastante frequência. Entre alguns deles estão as vulnerabilidades Unicode Directory Traversal Exploit e Double Hex Encoding Exploit. A primeira usa seqüências de caracteres como "../.." para acessar diretórios fora do diretório normal Webroot, no qual o conteúdo da Web é armazenado. Uma vez que a maioria dos servidores da Web bloqueia URLs contendo "../". Os invasores contornam essa proteção usando Unicode ou codificações hexadecimais para representar o padrão "../". Ao digitar em um navegador da Web uma seqüência de caracteres elaborada para realizar um ataque, os invasores podem acessar outros diretórios no servidor da Web. Esses outros diretórios podem conter informações confidenciais, senhas ou outros arquivos secretos.

Quando um ataque a HTTP é utilizado, os invasores podem acessar tais arquivos facilmente por meio de um navegador da Web padrão. Outros ataques a HTTP permitem que os invasores executem programas, alterem informações do sistema e chaves de registro de acesso e executem outras atividades mal-intencionadas.

II. O McAfee Intercept protege seus servidores

O McAfee Intercept protege os servidores contra os tipos de ataque mencionados acima e contra vários outros, inclusive novos ataques ainda não publicados. Uma análise da arquitetura e das várias camadas de proteção do McAfee Intercept mostra como o produto bloqueia tais ataques.

O McAfee Intercept está diretamente ligado ao sistema operacional interceptando chamadas do sistema antes de serem executadas. Se a chamada for classificada como um ataque, o McAfee Intercept a bloqueia, caso contrário, ela pode ser concluída normalmente.

O McAfee Intercept está disponível em três versões de agente: Standard Edition, Web Server Edition e Database Edition. As versões Web Server e Database Editions incluem todas as funcionalidades da versão Standard Edition juntamente com recursos adicionais específicos para impedir ataques contra servidores da Web ou servidores de banco de dados.

Os invasores e suas ferramentas: Como o McAfee Enterecept protege os servidores

White Paper do McAfee Enterecept

1. McAfee Enterecept Standard Edition

O McAfee Enterecept Standard Edition protege a parte mais importante de qualquer servidor: o sistema operacional. Todos os usuários e programas acessam o servidor pelo sistema operacional.

Protege recursos

A versão Standard Edition protege os recursos do sistema (bibliotecas, arquivos, diretórios, contas de usuário) impedindo que eles sejam alterados. Essa proteção é extremamente valiosa, uma vez que: cavalos de Tróia, rootkits e backdoors alteram os recursos do sistema para poderem instalar-se. Ao impedir a alteração desses recursos, o McAfee Enterecept Standard Edition evita a instalação dessas ferramentas de invasão.

Barra os ataques do tipo elevação de privilégio

A versão Standard Edition também impede que ataques do tipo elevação de privilégios sejam bem-sucedidos. Os ataques do tipo elevação de privilégios são bastante comuns, pois oferecem a usuários comuns direitos de acesso de usuário avançado (raiz ou administrador) no servidor. O McAfee Enterecept Standard Edition previne que tais ataques tenham êxito bloqueando o acesso a arquivos e recursos necessários para alterar os níveis de privilégio. Até mesmo elevações de privilégios novas, ainda não publicadas, podem ser barradas sem o conhecimento da exploração específica. Isso é possível porque todos os ataques do tipo elevação de privilégios alteram os privilégios dos usuários e o McAfee Enterecept os impede.

Previne contra ataques do tipo buffer overflow

Nos dias de hoje, os ataques do tipo buffer overflow são o método mais comum de atacar os servidores. Esses ataques podem ser baixados e executados facilmente por invasores com pouco conhecimento, também chamados de "Script Kiddies". Mais de 60% dos consultores da CERT lidam com ataques do tipo buffer overflow, portanto, impedir essas ataques comuns é essencial. O McAfee Enterecept Standard Edition é capaz de determinar se o código a ser executado pelo SO é proveniente de um aplicativo normal ou de um buffer overflow. Se for proveniente de um aplicativo comum, o McAfee Enterecept permitirá sua execução. Se for proveniente de um buffer overflow, será bloqueado, e a exploração não terá êxito.

Dessa maneira, o McAfee Enterecept impede que o servidor seja comprometido por um buffer overflow. Essa proteção é extremamente importante, pois evita os métodos mais comuns de ataque contra os servidores.

Ataques conhecidos

O mais importante é que o McAfee Enterecept pode impedir os ataques mencionados anteriormente utilizando a tecnologia de regras comportamentais, ao invés de depender apenas de assinaturas individuais. Essa tecnologia permite que o McAfee Enterecept barre ataques novos, ainda desconhecidos, sem a necessidade de atualizar as assinaturas do produto. Por exemplo, as regras do McAfee Enterecept para impedir o êxito dos ataques do tipo buffer overflow não estão ligadas a um aplicativo ou a uma assinatura específicos. Em vez disso, o McAfee Enterecept pode impedir essas ataques, independentemente do aplicativo ou buffer envolvido. Do mesmo modo, a proteção de recursos do McAfee Enterecept protege contra ataques novos e antigos, conhecidos ou não.

SecureSelect

O McAfee Enterecept oferece três modos de segurança:

SecureSelect™ Warning Mode, SecureSelect Protection Mode e SecureSelect Vault Mode. Cada modo oferece mais segurança que o anterior. Os clientes começam as implementações do McAfee Enterecept no Warning Mode, depois avançam para o Protection Mode e para o Vault Mode, conforme vão adaptando e refinando sua instalação do McAfee Enterecept.

2. McAfee Enterecept Web Server Edition

As camadas do WSE (McAfee Enterecept Web Server Edition) são:

Filtragem de HTTP

O McAfee Enterecept Web Server Edition inclui uma camada de filtragem de HTTP que intercepta solicitações HTTP depois de serem descriptografadas e decodificadas (não importa se foram criptografadas por SSL, Unicode ou hex), mas antes de o servidor da Web as executar. O McAfee Enterecept usa assinaturas nessa camada para detectar ataques contra o servidor da Web e outras vulnerabilidades. A importância dessa filtragem foi comprovada durante os recentes ataques dos worms Code Red e Nimda.

Os invasores e suas ferramentas: Como o McAfee Enterecept protege os servidores

White Paper do McAfee Enterecept

O McAfee Enterecept bloqueou ambos os worms na camada de HTTP, antes que se tomasse conhecimento deles. Não foi necessária nenhuma atualização de assinatura, pois a filtragem de HTTP do McAfee Enterecept protege contra as solicitações normais que os worms usaram para tentar penetrar no servidor da Web. Nem o Code Red nem o Nimda infectaram servidores protegidos pelo McAfee Enterecept Web Server Edition. Essa camada é o principal local para barrar ataques, uma vez que estes ataques são bloqueados muito antes do servidor executá-los.

Proteção de servidores da Web

O McAfee Enterecept também utiliza Proteção de Servidores da Web para impedir que ataques conhecidos e desconhecidos alterem o conteúdo da Web ou usem o servidor da Web como uma ferramenta de ataque. O McAfee Enterecept coloca o aplicativo do servidor da Web, seus arquivos e recursos em um recipiente altamente protegido. Se o servidor da Web tentar acessar quaisquer recursos fora do recipiente, o McAfee Enterecept bloqueia a tentativa. Do mesmo modo, se qualquer outro usuário ou processo tentar acessar ou alterar os arquivos ou recursos contidos no recipiente, o McAfee Enterecept bloqueia esse acesso também.

O McAfee Enterecept protege definindo um conjunto de regras de comportamento para o servidor da Web. Se o servidor da Web tentar fazer algo diferente do comportamento definido, a tentativa é bloqueada. Isso permite que o McAfee Enterecept proteja contra ataques desconhecidos, que ainda não foram publicados. Em vez de concentrar-se somente em abordagens que utilizam assinaturas, como os fornecedores de IDS tradicionais, o McAfee Enterecept usa regras comportamentais para identificar o comportamento conhecido e adequado. Quando um novo ataque é criado, ele viola, por definição, as regras do McAfee Enterecept que estabelecem o comportamento apropriado e será bloqueado.

Abordagens baseadas em assinatura concentram-se em como o ataque funciona, tentando detectar certas seqüências de caracteres ou outras informações de identificação. Essa abordagem funciona, até certo ponto, para ataques conhecidos. No entanto, se o invasor fizer alterações mínimas em como o ataque funciona, as assinaturas gravadas não o detectarão.

Ao contrário, o McAfee Enterecept concentra-se no que o ataque faz. Até mesmo se o invasor alterar a maneira como o ataque é realizado, o que ele faz não muda: o ataque realiza atividades mal-intencionadas.

A tecnologia de regras de comportamento do McAfee Enterecept identifica tentativas de executar atividades mal-intencionadas impedindo-as de obterem êxito. Essa abordagem protege os usuários contra ataques desconhecidos ainda não publicados.

Inclui camadas de proteção do McAfee Enterecept Standard Edition

O WSE inclui todos os recursos da Standard Edition, bem como níveis adicionais de proteção, criados especificamente para servidores da Web.

3. McAfee Enterecept Database Edition

As camadas do McAfee Enterecept Database Edition são:

Proteção contra injeção de SQL

Esse recurso do McAfee Enterecept Database Edition protege contra uma ameaça comum à segurança do banco de dados: as técnicas de inclusão de código SQL. Com a inserção de instruções SQL bem elaboradas em campos de dados de um aplicativo vulnerável, os invasores podem acessar dados restritos, como números de cartão de crédito, excluir dados particulares, alterar dados e até mesmo atacar outros computadores na rede do servidor de bancos de dados. O McAfee Enterecept Database Edition impede ataques do tipo injeção de SQL com a validação de consultas SQL antes de serem processadas pelo mecanismo do banco de dados. Assim, as tentativas mal-intencionadas de injeção de SQL são rejeitadas, e a integridade do banco de dados é preservada.

Prevenção contra ataques específicos

Esse recurso impede que os invasores prejudiquem o banco de dados. Sabe-se de dezenas de ataques criados para impedir o funcionamento de e/ou para comprometer servidores de bancos de dados. Com o uso da tecnologia de Interceptação de SQL, o McAfee Enterecept bloqueia tais ataques antes que eles possam causar qualquer dano ao banco de dados.

Proteção de banco de dados

Ela protege bancos de dados e dados contra acesso não autorizado. Essa proteção garante que qualquer processo além do próprio banco de dados não possa acessar o ambiente de execução, os dados ou as configurações do banco de dados. Além disso, o banco de dados fica impedido de acessar recursos que não dizem respeito a ele. Isso impede que os invasores usem o banco de dados para iniciar ataques contra outros alvos.

Os invasores e suas ferramentas: Como o McAfee Enterecept protege os servidores

White Paper do McAfee Enterecept

Portanto, a proteção de bancos de dados age como uma camada protetora para as operações evitando tanto a penetração externa quanto o uso mal-intencionado do servidor de banco de dados. O resultado disso é que: tanto os ataques conhecidos quanto os desconhecidos são bloqueados em tempo real, antes de atingir o servidor de banco de dados e causar danos. Invasores potenciais não conseguem acessar ou modificar parâmetros operacionais—mesmo que consigam privilégios de acesso ao servidor.

III. Resumo: Como o McAfee Enterecept bloqueia as ferramentas dos invasores

- **Worms**—O McAfee Enterecept impede que um worm infecte um servidor bloqueando sua tentativa de explorar vulnerabilidades no servidor.
- **Ataques do tipo buffer overflow**—O McAfee Enterecept bloqueia a execução de códigos provenientes de buffer overflow impedindo que o servidor seja comprometido.

- **Ataques do tipo elevação de privilégios**—O McAfee Enterecept barra os ataques do tipo elevação de privilégios utilizando a camada de Proteção de Recursos que impede a alteração de recursos do sistema.

- **Cavalos de Tróia, rootkits e backdoors**—O McAfee Enterecept impede que essas ferramentas de ataque comuns comprometam os servidores bloqueando a alteração de recursos do sistema. Uma vez que cavalos de Tróia, rootkits e backdoors são todas tentativas de modificar recursos do sistema, o McAfee Enterecept impede sua instalação.

- **Ataques a HTTP**—A camada de filtragem a HTTP do McAfee Enterecept impede que ataques a HTTP tenham êxito ao bloquear solicitações HTTP mal-intencionadas.



Todos os produtos da Network Associates® contam com o respaldo do nosso programa PrimeSupport® e dos Laboratórios da Network Associates. Projetados para se adequarem às necessidades da empresa, os serviços da PrimeSupport oferecem o conhecimento de produto e as soluções técnicas rápidas e confiáveis necessárias para mantê-lo em plena atividade. Os Laboratórios da Network Associates, líderes mundiais em sistemas de informação e segurança, são a garantia do desenvolvimento e refinamento contínuo de todas as nossas tecnologias.

Network Associates, McAfee, Enterecept e PrimeSupport são marcas comerciais, registradas ou não, da Network Associates, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Os produtos que levam a marca Sniffer® são produzidos apenas pela Network Associates, Inc. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente a seus respectivos proprietários. ©2003 Networks Associates Technology, Inc. Todos os direitos reservados. 6-avd-ent-tools-001-1003