## Contas atraentes para roubo de credenciais

Os ataques de roubo de credenciais são aqueles em que um invasor recebe inicialmente o acesso mais alto (raiz, administrador ou sistema, dependendo do sistema operacional em uso), a um computador em uma rede e, em seguida, usa as ferramentas disponíveis gratuitamente para extrair as credenciais das sessões de outras contas conectadas. Dependendo da configuração do sistema, essas credenciais podem ser extraídas na forma de hashes, tíquetes ou até mesmo senhas de texto sem formatação. Se qualquer uma das credenciais coletadas for para contas locais que provavelmente existem em outros computadores na rede (por exemplo, contas de administrador no Windows ou contas raiz no OSX, UNIX ou Linux), o invasor apresentará as credenciais para outros computadores na rede para propagar o comprometimento para computadores adicionais e tentar obter as credenciais de dois tipos específicos de contas :

Contas de domínio privilegiadas com privilégios amplos e profundos (ou seja, contas que têm privilégios de nível de administrador em vários computadores e em Active Directory). Essas contas podem não ser membros de nenhum dos grupos de privilégio mais alto no Active Directory, mas podem ter recebido privilégios de nível de administrador em vários servidores e estações de trabalho no domínio ou floresta, o que os torna efetivamente tão poderosos quanto os membros de grupos com privilégios no Active Directory. Na maioria dos casos, as contas que receberam altos níveis de privilégio em faixas amplas da infraestrutura do Windows são contas de serviço, de modo que as contas de serviço sempre devem ser avaliadas quanto à amplitude e à profundidade do privilégio.

Contas de domínio de "pessoa muito importante" (VIP). No contexto deste documento, uma conta VIP é qualquer conta que tenha acesso às informações que um invasor desejar (propriedade intelectual e outras informações confidenciais) ou qualquer conta que possa ser usada para conceder ao invasor acesso a essas informações. Exemplos dessas contas de usuário incluem:

Executivos cujas contas têm acesso a informações corporativas confidenciais

Contas para a equipe de suporte técnico responsável por manter os computadores e aplicativos usados pelos executivos

Contas para a equipe jurídica que têm acesso aos documentos de ofertas e contratos de uma organização, sejam eles para sua própria organização ou organizações de clientes

Planejadores de produtos que têm acesso a planos e especificações de produtos no pipeline de desenvolvimento de uma empresa, independentemente dos tipos de produtos que a empresa faz

Pesquisadores cujas contas são usadas para acessar dados de estudo, formulações de produtos ou qualquer outra pesquisa de interesse de um invasor

Como contas altamente privilegiadas no Active Directory podem ser usadas para propagar o comprometimento e para manipular contas VIP ou os dados que eles podem acessar, as contas mais úteis para ataques de roubo de credenciais são contas que são membros de grupos Administradores de

empresa, administradores de domínio e administradores no Active Directory.

Como os controladores de domínio são os repositórios para o banco de dados de AD DS e os controladores de domínio têm acesso total a todas as informações em Active Directory, os controladores de domínio também são destinados a comprometimento, seja em paralelo com ataques de roubo de credenciais ou após uma ou mais contas de Active Directory altamente privilegiadas terem sido comprometidas. Embora várias publicações (e muitos invasores) se concentrem nas associações do grupo Admins. do domínio ao descrever os ataques Pass-the-hash e outros roubos de credenciais (como é descrito em reduzindo a superfície de ataque Active Directory), uma conta que seja membro de qualquer um dos grupos listados aqui pode ser usada para comprometer toda a instalação do AD DS.

Observação

Para obter informações abrangentes sobre o Pass-the-hash e outros ataques de roubo de credenciais, consulte o White Paper atenuando ataques de Pass-the-hash (PTH) e outras técnicas de roubo de credenciais listadas no Apêndice M: links de documentos e leitura recomendada. Para obter mais informações sobre ataques por determinados adversários, que às vezes são chamados de "ameaças persistentes avançadas" (APTs), consulte determinados adversários e ataques direcionados.

Atividades que aumentam a probabilidade de comprometimento

Como o destino do roubo de credenciais é geralmente contas de domínio altamente privilegiadas e contas VIP, é importante que os administradores estejam preocupados com as atividades que aumentam a probabilidade de sucesso de um ataque de roubo de credencial. Embora os invasores também tenham como alvo contas VIP, se VIPs não forem dadas altos níveis de privilégio em sistemas ou no domínio, o roubo de suas credenciais exigirá outros tipos de ataques, como a engenharia social do VIP para fornecer informações secretas. Ou o invasor deve primeiro obter acesso privilegiado a um sistema no qual as credenciais VIP são armazenadas em cache. Por isso, as atividades que aumentam a probabilidade de roubo de credenciais descritas aqui se concentram principalmente em impedir a aquisição de credenciais administrativas altamente privilegiadas. Essas atividades são mecanismos comuns pelos quais os invasores podem comprometer os sistemas para obter credenciais privilegiadas.

Fazendo logon em computadores não seguros com contas com privilégios

A vulnerabilidade principal que permite que os ataques de roubo de credenciais seja bem sucedido é o ato de fazer logon em computadores que não são seguros com contas que são amplamente e profundamente privilegiadas em todo o ambiente. Esses logons podem ser o resultado de várias configurações incorretas descritas aqui.

Não manter credenciais administrativas separadas

Embora isso seja relativamente incomum, na avaliação de várias instalações de AD DS, descobrimos que os funcionários usam uma única conta para todo o seu trabalho. A conta é membro de pelo menos um dos grupos com mais privilégios no Active Directory e é a mesma conta que os funcionários usam para fazer logon em suas estações de trabalho na manhã, verificar seu email, navegar em sites da Internet e baixar conteúdo para

seus computadores. Quando os usuários são executados com contas que recebem direitos e permissões de administrador local, eles expõem o computador local para concluir o comprometimento. Quando essas contas também são membros dos grupos mais privilegiados no Active Directory, elas expõem toda a floresta para comprometimento, tornando fácil para um invasor obter controle total do ambiente Active Directory e do Windows.

Da mesma forma, em alguns ambientes, descobrimos que os mesmos nomes de usuário e senhas são usados para contas raiz em computadores não Windows, como são usados no ambiente do Windows, o que permite aos invasores estender o comprometimento de sistemas UNIX ou Linux para sistemas Windows e vice-versa.

Logons para estações de trabalho comprometidas ou servidores membro com contas privilegiadas

Quando uma conta de domínio altamente privilegiado é usada para fazer logon interativamente em um servidor de estação de trabalho ou membro comprometido, esse computador comprometido pode coletar credenciais de qualquer conta que fizer logon no sistema.

Estações de trabalho administrativas não seguras

Em muitas organizações, a equipe de ti usa várias contas. Uma conta é usada para fazer logon na estação de trabalho do funcionário, e como elas são a equipe de ti, elas geralmente têm direitos de administrador local em suas estações de trabalho. Em alguns casos, o UAC é deixado habilitado para que o usuário receba pelo menos um token de acesso de divisão no logon e seja necessário elevar quando os privilégios forem necessários. Quando esses usuários estão executando atividades de manutenção, normalmente usam as ferramentas de gerenciamento instaladas localmente e fornecem as credenciais para suas contas com privilégios de domínio, selecionando a opção Executar como administrador ou fornecendo as credenciais quando solicitado. Embora essa configuração possa parecer apropriada, ela expõe o ambiente a ser comprometido porque:

A conta de usuário "regular" que o funcionário usa para fazer logon em sua estação de trabalho tem direitos de administrador local, o computador está vulnerável a drive-by download ataques nos quais o usuário está convencido a instalar malware.

O malware é instalado no contexto de uma conta administrativa, o computador agora pode ser usado para capturar pressionamentos de teclas, conteúdo da área de transferência, capturas de tela e credenciais residentes na memória, o que pode resultar na exposição das credenciais de uma conta de domínio avançada.

Os problemas neste cenário são duplos. Primeiro, embora contas separadas sejam usadas para administração local e de domínio, o computador não é seguro e não protege as contas contra roubo. Em segundo lugar, a conta de usuário normal e a conta administrativa receberam direitos e permissões excessivas.

Navegando pela Internet com uma conta altamente privilegiada

Os usuários que fazem logon em computadores com contas que são membros do grupo Administradores local no computador, ou membros de grupos com privilégios no Active Directory, e que navegam pela Internet (ou uma

intranet comprometida) expõem o computador local e o diretório a ser comprometido.

O acesso a um site mal-intencionado criado com um navegador em execução com privilégios administrativos pode permitir que um invasor deposite código mal-intencionado no computador local no contexto do usuário privilegiado. Se o usuário tiver direitos de administrador local no computador, os invasores poderão induzir o usuário a baixar código mal-intencionado ou abrir anexos de email que aproveitam as vulnerabilidades do aplicativo e aproveitar os privilégios do usuário para extrair as credenciais armazenadas em cache localmente para todos os usuários ativos no computador. Se o usuário tiver direitos administrativos no diretório por associação nos grupos administradores corporativos, administradores de domínio ou administradores no Active Directory, o invasor poderá extrair as credenciais de domínio e usá-las para comprometer todo o domínio AD DS ou a floresta, sem a necessidade de comprometer qualquer outro computador na floresta.

Configurando contas com privilégios locais com as mesmas credenciais entre sistemas

Configurar o mesmo nome de conta de administrador local e a senha em muitos ou todos os computadores permite que as credenciais roubadas do banco de dados SAM em um computador sejam usadas para comprometer todos os outros computadores que usam as mesmas credenciais. No mínimo, você deve usar senhas diferentes para contas de administrador local em cada sistema ingressado no domínio. As contas de administrador local também podem ser nomeadas exclusivamente, mas usar senhas diferentes para as contas locais privilegiadas de cada sistema é suficiente para garantir que as credenciais não possam ser usadas em outros sistemas.

Sobrepopulação e uso excessivo de grupos de domínio com privilégios

A concessão de associação nos grupos EA, DA ou BA em um domínio cria um destino para os invasores. Quanto maior o número de membros desses grupos, maior a probabilidade de que um usuário com privilégios possa inadvertidamente aproveitar as credenciais e expô-las a ataques de roubo de credenciais. Cada estação de trabalho ou servidor no qual um usuário de domínio com privilégios faz logon apresenta um possível mecanismo pelo qual as credenciais do usuário privilegiado podem ser coletadas e usadas para comprometer o domínio AD DS e a floresta.

Controladores de domínio mal protegidos

Controladores de domínio hospedam uma réplica do banco de dados AD DS de um domínio. No caso de
controladores de domínio somente leitura, a réplica local do banco de dados contém as credenciais
para apenas um subconjunto das contas no diretório, nenhuma das quais são contas de domínio privilegiadas
por padrão. Em controladores de domínio de leitura-gravação, cada controlador de domínio mantém uma réplica
completa do banco de dados AD DS, incluindo credenciais não apenas para usuários privilegiados como administradores
de domínio, mas contas com privilégios, como contas de controlador de domínio ou a conta krbtgt do domínio, que é a
conta associada ao serviço KDC em controladores de domínio. Se os aplicativos adicionais que não são necessários para

a funcionalidade do controlador de domínio estiverem instalados em controladores de domínio ou se os controladores de domínio não forem rigorosamente corrigidos e protegidos, os invasores poderão comprometa-los por meio de vulnerabilidades sem patch ou poderão aproveitar outros vetores de ataque para instalar software mal-intencionado diretamente neles.

Elevação de privilégio e propagação

Independentemente dos métodos de ataque usados, Active Directory é sempre direcionada quando um ambiente do Windows é atacado, pois ele finalmente controla o acesso a qualquer coisa que os invasores desejarem. No entanto, isso não significa que todo o diretório é direcionado. Contas, servidores e componentes de infraestrutura específicos geralmente são os principais destinos de ataques contra Active Directory. Essas contas são descritas a seguir.

Contas com privilégios permanentes

Como a introdução do Active Directory, foi possível usar contas altamente privilegiadas para criar a floresta de Active Directory e, em seguida, delegar direitos e permissões necessários para executar a administração diária para contas com menos privilégios. A associação nos grupos administradores corporativos, administradores de domínio ou administradores no Active Directory é necessária apenas temporariamente e raramente em um ambiente que implementa abordagens de privilégios mínimos para administração diária.

Contas com privilégios permanentes são contas que foram colocadas em grupos privilegiados e deixadas lá a partir do dia a dia. Se sua organização colocar cinco contas no grupo Admins. do domínio para um domínio, essas cinco contas poderão ser direcionadas 24 horas por dia, sete dias por semana. No entanto, a necessidade real de usar contas com privilégios de admins. do domínio normalmente é apenas para uma configuração específica em todo o domínio e por curtos períodos de tempo.

Contas VIP

Um destino frequentemente ignorado em violações de Active Directory é a conta de "pessoas muito importantes" (ou VIPs) em uma organização. Contas com privilégios são direcionadas porque essas contas podem conceder acesso a invasores, o que permite comprometer ou até mesmo destruir sistemas de destino, conforme descrito anteriormente nesta seção.

Contas de Active Directory "anexadas por privilégio"

Contas de Active Directory "anexadas por privilégio" são contas de domínio que não se tornaram membros de nenhum dos grupos que têm os níveis mais altos de privilégio em Active Directory, mas, em vez disso,

receberam altos níveis de privilégio em vários servidores e estações de trabalho no ambiente. Essas contas
geralmente são contas baseadas em domínio que são configuradas para executar serviços em sistemas ingressados
no domínio, normalmente para aplicativos executados em grandes seções da infraestrutura. Embora essas contas
não tenham privilégios em Active Directory, se elas recebem alto privilégio em um grande número de sistemas,
elas podem ser usadas para comprometer ou até mesmo destruir grandes segmentos da infraestrutura, atingindo o
mesmo efeito que o comprometimento de uma conta de Active Directory privilegiada