Guia para a identificação e atenuação de colisão de nomes para profissionais de TI

1º de agosto de 2014
Versão 1.1

Índice

1. Introdução

Após a entrada de um novo nome de domínio de primeiro nível na raiz do DNS global, as organizações poderão observar que as consultas para resolver alguns nomes “internos” específicos de suas redes retornam valores diferentes, fornecendo resultados diferentes aos usuários e aos programas. Existem dois problemas básicos: nomes “internos” que estão vazando para a Internet global e espaços de nomes privados definidos como em conflito com o espaço de nome do DNS global.

A causa desses resultados diferentes é uma consulta de DNS que um administrador de rede pretendia resolver localmente, usando um espaço de nome interno, mas que está sendo resolvida usando os dados do novo domínio de primeiro nível no DNS global. Diante dessas circunstâncias, as consultas cuja saída da rede interna nunca havia sido prevista estão agora obtendo resultados no DNS global, e esses resultados são diferentes. Na pior das hipóteses, os nomes vazados que produzem resultados diferentes podem ser um transtorno para os usuários (por exemplo, eles podem retardar o acesso a páginas da Web). Eles também podem gerar problemas de segurança (como o envio de e-mail aos destinatários errados).

Este documento abrange estratégias de atenuação e prevenção para os tipos mais comuns de espaços de nomes privados usados por organizações. Este documento descreve o que as organizações podem enfrentar quando nomes internos vazam para o DNS global e especifica práticas de atenuação recomendadas. A descrição e os conselhos fornecidos são voltados a profissionais de TI (administradores de redes, administradores de sistemas e equipes de departamentos de TI) que entendem, em geral, como o DNS funciona e como seus próprios sistemas de nomes internos funcionam. Os leitores que desejarem obter mais informações básicas devem consultar os documentos contidos no anexo A. Os leitores preocupados com a segurança devem buscar, em especial, os relatórios do comitê consultivo de segurança e estabilidade (SSAC) da ICANN.

A ICANN, a organização que administra o conteúdo da raiz do DNS global, preparou este documento após consultar especialistas em espaços de nomes, para ajudar as organizações cujos espaços de nomes privados possam estar em conflito com a raiz do DNS global. A ICANN publicou outros documentos que descrevem como o DNS global está organizado, como novos nomes são adicionados à raiz do DNS e muito mais. O anexo A deste documento lista referências para obter mais informações sobre diversos tópicos. Além disso, a ICANN recentemente passou a ajudar as organizações que usam espaços de nomes privados a perceber quando esses espaços de nomes começarem a ter colisões; isso é descrito na Seção 1.4 e Seção 6.

Observe que, embora aborde medidas para a atenuação de colisões de nomes, este documento somente apresenta problemas que poderão ser enfrentados por organizações ao resolver nomes. Ele não aborda outras questões relacionadas à operação do DNS global em si. Por exemplo, os servidores de nome raiz do DNS global sempre foram inundados por consultas que não deveriam ser processadas pelo DNS global (consulte o *SAC 045* no anexo A), mas os servidores de nome raiz também sempre foram aprovisionados de maneira suficiente para abranger essas consultas excessivas. As questões relacionadas aos servidores de nomes raiz não são abordadas neste documento. Ele aborda somente as consequências das consultas que são vazadas inadvertidamente para os servidores de nome raiz do DNS global.

A ICANN desenvolveu uma página da Web que fornece materiais informativos sobre as colisões de nomes, disponíveis em http://www.icann.org/namecollision. A página também inclui um processo para relatar danos comprovadamente sérios resultantes de colisões de nomes causadas pelos novos domínios genéricos de primeiro nível (gTLDs).

1.1 Colisões de nomes

O DNS global é um espaço de nomes hierárquico, e os nomes no DNS são compostos por um ou mais rótulos que formam um nome completo. No topo da hierarquia está a zona raiz do DNS que contém um conjunto de nomes como `com`, `ru`, `asia` e assim por diante; esses são os TLD*s* (domínios de primeiro nível) globais, normalmente chamados apenas de "TLDs". Um exemplo de nome de domínio completo (geralmente chamado de *nome de domínio totalmente qualificado* ou *FQDN*) seria `www.nossaempresa.com`.

Quase todos os espaços de nomes privados também são hierárquicos. Existem três tipos principais de espaços de nomes privados:

- **Espaços de nomes que se ramificam do DNS global** – Os espaços de nomes privados que se ramificam do DNS global estão enraizados em um nome que é resolvido no DNS global, mas toda a estrutura de diretório abaixo desse nome é gerenciada localmente com nomes que o administrador de TI nunca pretendeu que fossem vistos no DNS global. Por exemplo, considere um espaço de nome privado enraizado em `winserve.nossaempresa.com`: os nomes nesse espaço de nome privado (`winserve`) são gerenciados pelo servidor de nomes privado e não estão visíveis no DNS global.

- **Espaços de nomes que usam suas próprias raízes com TLDs privados** – A raiz de um espaço de nome privado é um rótulo único que não é um TLD global. A estrutura completa do diretório, incluindo o TLD privado, é gerenciado por servidores de nomes privados que não são visíveis no DNS global. Por exemplo, se o espaço de nome privado estiver enraizado em `nossaempresa`, os servidores de nomes privados também serão responsáveis por `www.nossaempresa`, `regiao1.nossaempresa`, `www.regiao1.nossaempresa` e assim por diante. Existem muitos tipos diferentes de espaços de nomes que usam suas próprias raízes com TLDs privados. Alguns exemplos incluem o Active Directory da Microsoft (em algumas configurações), o multicast DNS (RFC 6762) e serviços antigos de diretório de LAN que ainda são usados em algumas partes da Internet.

- **Espaços de nomes criados pelo uso de listas de buscas** – Uma lista de busca é um recurso de um resolvedor de nomes local (tanto para um espaço de nome privado quanto para um resolvedor recursivo do DNS global). Uma lista de busca permite que um usuário insira nomes mais curtos por conveniência; durante a resolução, o servidor de nomes anexa nomes configurados à direita do nome em uma consulta. (Esses nomes configurados também são chamados de *sufixos*.)

Os espaços de nomes que se ramificam do DNS global somente causam colisões de nomes quando combinados a listas de busca. As consultas que envolverem um FQDN que está no DNS global, por definição, nunca terão uma colisão de nomes com um nome diferente no DNS global. Essas consultas somente causariam colisões de nomes se fossem inadvertidamente criadas com o uso de listas de busca.

O conceito de "espaços de nomes privados" confunde muitas pessoas que estão acostumadas com o uso típico da Internet, ou seja, pessoas que estão familiarizadas com a nomenclatura do DNS global e que podem surpreender-se ao descobrir que algumas solicitações de resolução de nomes não resultam ou não devem resultar em uma consulta ao DNS global. Elas podem surpreender-se ainda mais ao descobrir que algumas consultas de nomes devem propositadamente ter início no espaço de nome privado, mas terminar no DNS global. Um motivo pelo qual podem ocorrer colisões de nomes é que as consultas dirigidas a um servidor de nomes de um espaço de nome privado são, em vez disso, iniciadas incorretamente no DNS global.

1.2 Colisões de nomes devido a TLDs privados

As colisões de nomes ocorrem como resultado de dois eventos. Primeiro, uma consulta por um nome de domínio totalmente qualificado enraizado em um TLD privado vaza da rede privada para o DNS global. Segundo, a consulta localiza no DNS global um nome exatamente igual ao que existe na rede privada abaixo do TLD privado.

Uma causa comum para essas colisões de nomes é o uso de um nome em um sistema como o Active Directory da Microsoft que não seja um TLD no DNS global no momento em que o sistema é configurado, mas é posteriormente adicionado ao DNS global. Esse tipo de colisão de nomes já aconteceu muitas vezes antes e provavelmente continuará com a introdução de novos TLDs no DNS global (consulte *Introdução ao programa de novos gTLDs*, no anexo A).

1.3 Colisões de nomes devido a listas de buscas

Outra causa para as colisões de nomes é o processamento de uma lista de busca. Se uma consulta não for um FQDN, ela é um *nome curto não qualificado*. Uma lista de busca contém um ou mais sufixos. Eles são iterativamente anexados ao lado direito de uma consulta. Quando um resolvedor é incapaz de resolver um nome curto não qualificado, ele anexa sufixos da lista à medida que tenta resolver o nome até encontrar um nome correspondente. Uma lista de busca é um recurso útil; no entanto, o processamento de uma lista de busca acomoda o uso de nomes curtos não qualificados que não são FQDNs e, assim, inadvertidamente cria espaços de nomes que não são enraizados no DNS global. Nesse caso, a colisão de nomes ocorre quando uma cadeia de caracteres que o usuário pretende usar como um nome curto não qualificado é, em vez disso, concluída pela lista de busca e resolvida como um FQDN.

Por exemplo, suponhamos que um resolvedor de nomes tenha uma lista de busca que consiste nos sufixos `nossaempresa.com` e `marketing.nossaempresa.com`. Suponhamos também que um usuário digite `www` em um programa que usa esse resolvedor. O resolvedor poderia, primeiro, buscar `www` e, se isso não retornasse um resultado, ele poderia buscar `www.nossaempresa.com` e `www.marketing.nossaempresa.com`.

Observe o uso da palavra “poderia” na descrição desse exemplo. As regras que definirão como as listas de busca serão aplicadas ao realizar resoluções de nomes variam entre os sistemas operacionais ou os aplicativos. Alguns sistemas sempre tentarão resolver um nome no espaço de nome privado ou no DNS global antes de aplicar a lista de busca. No entanto, outros sistemas usarão a lista de busca primeiro, caso a cadeia de caracteres que está sendo pesquisada não contenha um caractere “`.`”. Ainda assim, há outros que usarão a lista de busca caso a cadeia de caracteres que está sendo pesquisada termine com um caractere “`.`”. Alguns sistemas operacionais e aplicativos (como navegadores da Web) alteraram suas regras para listas de busca várias vezes. Sendo assim, é impossível prever quando as listas de busca serão usadas ou não, o que é ou não um nome curto não qualificado e se é possível ou não que os nomes curtos não qualificados vazem para o DNS global. Consulte *Preocupações a respeito de novos gTLDs: nomes sem ponto e colisões de nomes*, no anexo A, para obter mais detalhes sobre a diversidade do processamento da lista de busca.

Essa descrição de listas de busca pode ser uma surpresa para alguns leitores, porque elas são muito comuns em lugares que, à primeira vista, não parecem criar “espaços de nomes privados”. Cada sufixo em uma lista de busca define outro espaço de nome que poderá ser consultado durante uma resolução de nome. Isso cria um espaço de nome privado que opera de maneira confiável somente quando o cliente envia uma consulta aos resolvedores desse espaço de nome. Dependendo da implementação da lista de busca, alguns resolvedores de nome até poderiam testar o nome curto não qualificado inserido pelo usuário ou configurado no software antes de anexar algum dos nomes à lista

de busca. Por exemplo, digitar `www.hr` em um local na Internet poderá produzir um resultado pelo resolvedor do DNS, mas digitar isso em um local diferente poderá produzir um resultado diferente. Quando isso ocorre, significa que um dos espaços de nome é “privado” em comparação com o outro.

Usar listas de busca em vez de resolver FQDNs pelo DNS global contribui para a incerteza da resolução de nomes. As colisões de nomes produzidas pelas listas de busca são difíceis de prever, porque as listas de busca são muito comuns. Elas fazem parte do software do resolvedor de nomes em muitos sistemas operacionais, equipamentos de rede, servidores, entre outros. O software do resolvedor age de maneira distinta de um sistema para outro, entre versões diferentes do mesmo sistema operacional e até mesmo como uma função da visão de sistemas operacionais ou aplicativos sobre o ponto de origem da solicitação na rede. A implementação de um serviço de resolução de nomes que resolva nomes usando apenas o DNS global é a melhor garantia contra esses resultados incertos e imprevisíveis.

1.4 Ajuda na detecção de colisões de nomes em novos gTLDs

A partir do dia 18 de agosto de 2014, quando um gTLD for delegado da zona raiz do DNS, esse gTLD deverá realizar um serviço de *interrupção controlada* por 90 dias. Durante o período de interrupção controlada, as respostas facilmente identificáveis são enviadas dos servidores de nome oficiais ao novo gTLD para várias consultas do DNS. O objetivo dessas respostas é advertir as organizações de que elas sofrerão colisões de nomes e deverão tomar medidas imediatas para evitar possíveis danos devido às consultas vazadas.

Além disso, a partir da mesma data, alguns gTLDs que já estão na zona raiz deverão realizar um serviço de interrupção controlada por 90 dias antes de delegar determinados nomes de segundo nível no DNS global. O objetivo aqui é o mesmo que o anterior: advertir as organizações de que há vazamentos de consultas privadas e que elas devem atenuar possíveis danos o mais rápido possível.

Observe que estas regras se aplicam apenas aos gTLDs, não aos TLDs para códigos de países (normalmente denominados “ccTLDs”). Quando um ccTLD é adicionado à zona raiz, seu operador pode escolher ter uma interrupção controlada, mas não é obrigado a fazê-lo.

2. Problemas causados por colisões de nomes

As colisões de nomes baseadas em consultas que vazam no DNS global de redes privadas podem ter várias consequências involuntárias. Quando uma consulta obtém uma resposta positiva, mas que venha do DNS global em vez do espaço de nome privado esperado, o aplicativo que está fazendo a consulta tentará conectar-se a um sistema que não faz parte da rede privada e poderá consegui-lo. Essa conexão pode ser um incômodo (gerando um atraso durante a resolução de nomes). Isso também pode constituir um problema de segurança, ou seja, pode gerar uma vulnerabilidade que poderia ser explorada para fins maliciosos, dependendo do que for realizado pelo aplicativo após a conexão.

2.1 Direcionamento a sites inesperados

Suponhamos que um usuário digite `https://financeiro.nossaempresa` em seu navegador da Web enquanto estiver em uma rede privada, e que essa rede tenha um espaço de nome cujo TLD privado é `nossaempresa`. Se a consulta do navegador pelo nome `financeiro.nossaempresa` for resolvida da maneira esperada, o navegador obterá um endereço IP para o servidor da Web interno do departamento financeiro. Imagine, no entanto, que o TLD `nossaempresa` também faz parte do DNS global e que esse TLD tem um nome de SLD (Second-Level Domain, domínio de segundo nível) `financeiro`. Se a consulta vazar, ela será resolvida para um endereço IP diferente de quando a consulta foi resolvida no espaço de nome privado. Agora imagine que esse endereço IP diferente poderia hospedar um servidor da Web. O navegador tentaria conectar-se a um servidor da Web na Internet pública, e não na rede privada.

Conforme mostrado anteriormente, o mesmo problema pode ocorrer também na redes que não têm TLDs privados, mas que usam listas de busca. Considere um navegador que seja normalmente usado em uma rede em que os usuários têm uma lista de busca com o mesmo nome `nossaempresa.com`, e o usuário digita o nome `www.financeiro` para acessar o host `www.financeiro.nossaempresa.com`. Agora imagine que o navegador esteja sendo usado por um funcionário a partir de um dispositivo móvel em uma cafeteria. Se essa consulta vazar para a Internet e houver um TLD chamado `financeiro`, a consulta poderia ser resolvida para um endereço IP diferente, por exemplo, um host totalmente diferente cujo nome no DNS global seja `www.financeiro`. Essa consulta faria o navegador tentar conectar-se a um servidor da Web em uma parte da Internet pública totalmente diferente daquela em que se conectaria caso a consulta fosse enviada ao resolvedor na rede privada.

A resposta de um usuário comum a essa situação é que o usuário reconheceria que não era o site correto e sairia imediatamente. Entretanto, um navegador pode expor um grande volume de informações a um servidor da Web se o navegador “confiar” no servidor da Web, porque ele tem o mesmo nome de domínio já visitado pelo navegador anteriormente. O navegador poderá inserir o login automaticamente ou outros dados confidenciais, expondo essas informações para captura ou análise fora da organização. Em outras circunstâncias (por exemplo, um ataque planejado cuidadosamente contra a organização), o navegador poderia conectar-se a um site com um código malicioso que instala programas perigosos no computador.

Observe que o uso de TLS e certificados digitais poderiam não ajudar a evitar os danos causados por colisões de nomes. Na realidade, isso poderia piorar a situação, dando aos usuários uma falsa sensação de segurança. Muitas das autoridades de certificação (CAs) que emitem certificados para nomes no DNS global também emitem certificados para nomes curtos não qualificados em espaços de endereço privados; portanto, é possível que um usuário que fosse encaminhado erroneamente a um

site ainda visse um certificado válido. Consulte o *SAC 057,* no anexo A, para obter mais detalhes sobre certificados com nomes de espaços de nomes privados.

2.2 Direcionamento de e-mail a destinatários errados

As possíveis consequências decorrentes de colisões de nomes não se limitam aos navegadores. Um e-mail dirigido a um destinatário pode ser enviado a um destinatário diferente se os nomes do host nos endereços do recipiente forem iguais; por exemplo, um e-mail para `chris@suporte.nossaempresa` poderia ser entregue a um usuário completamente diferente se `nossaempresa` se tornasse um TLD no DNS global. Mesmo que a mensagem não seja entregue a um determinado usuário de e-mail, é possível haver a tentativa de enviá-lo, e essas tentativas poderão expor o conteúdo do e-mail para captura ou análise fora da organização.

Muitos dispositivos de rede, como firewalls, roteadores e até mesmo impressoras, podem ser configurados para enviar notificações ou dados de registro por e-mail. Se o nome do destinatário informado para as notificações por e-mail for posteriormente o objeto de uma colisão de nomes no DNS global, a notificação poderá ser entregue de maneira totalmente involuntária a outro destinatário. Eventos ou dados de registro contidos no corpo da mensagem e que podem revelar a configuração de rede e o comportamento do host podem vazar a um destinatário não desejado. A análise de rotina do tráfego e do desempenho de rede pela equipe de TI pode ser interrompida se o destinatário desejado desses dados nunca receber os dados de registro, ou os eventos que acionam notificações podem não ser investigados ou atenuados.

2.3 Reduções de segurança

As ocorrências de colisões de nomes que não forem atenuadas poderão expor os sistemas nas redes privadas a comportamentos ou danos involuntários. Os sistemas que dependem da resolução de nomes para seu funcionamento correto e que também realizam funções de segurança *podem* ter um desempenho confiável se usarem FQDNs e executarem a resolução pelo DNS global.

Por exemplo, em firewalls, as regras de segurança geralmente se baseiam na origem ou no destino de um fluxo de pacote. A origem e o destino de pacotes são endereços IPv4 ou IPv6, mas muitos firewalls permitem que eles sejam inseridos como nomes de domínio também. Se nomes curtos não qualificados forem usados e a resolução de nomes não for executada da maneira esperada, as regras poderão não bloquear ou permitir o tráfego conforme desejado pelo administrador. Da mesma forma, os registros de firewall geralmente usam nomes de domínio, e o uso de nomes curtos não qualificados, cuja resolução é imprevisível, pode interferir no monitoramento de eventos, análise ou resposta. Durante a revisão dos registros, há o risco de a equipe de TI, por exemplo, interpretar erroneamente a gravidade de um evento, porque um nome curto não qualificado no registro pode identificar hosts diferentes, dependendo do local de criação do registro (ou seja, no registro, o mesmo nome curto não qualificado pode parecer estar associado a dois ou mais endereços IP diferentes). É possível também que esse problema seja agravado pelo fato de que a maioria dos firewalls pode agir como seu próprio resolvedor de DNS ou permitir que os administradores usem ou configurem listas de busca.

2.4 Sistemas afetados por colisões de nomes

Todos os sistemas conectados à rede devem ser verificados quanto ao uso de nomes de host enraizados em um TLD privado ou nomes de host baseados em listas de busca. Todas essas instâncias de “uso” deverão ser atualizadas para utilizar um FQDN do DNS global. Uma lista não exaustiva de exemplos de sistemas ou aplicativos que deverão ser verificados inclui:

- **Navegadores** – Os navegadores da Web permitem que os usuários especifiquem o local de procurações HTTP, e estas frequentemente estão na rede privada. Verifique se um usuário ou a equipe de TI adicionou páginas iniciais personalizadas, páginas nos favoritos ou mecanismos de busca: eles podem ter links para servidores na rede privada. Alguns navegadores também têm opções de configuração para onde obter informações de revogação sobre certificados de SSL/TLS que podem direcionar a nomes de host na rede privada.

- **Servidores da Web** – Os servidores da Web oferecem conteúdo em HTML que contém links e metadados com nomes de host incorporados. Verifique se os servidores da Web em uma rede privada têm conteúdo com nomes curtos não qualificados. Verifique se os arquivos de configuração do servidor da Web têm nomes curtos não qualificados de outros hosts na rede privada.

- **Agentes de usuários de e-mail –** Os clientes de e-mail, como o Outlook e o Thunderbird, todos têm opções de configuração para o local de recebimento de e-mails usando os protocolos POP ou IMAP, e para o local de envio de e-mails usando o protocolo SUBMIT; todos eles podem usar nomes de host na rede privada. Verifique se esses aplicativos estão configurados para obter informações de revogação sobre certificados de SSL/TLS de nomes curtos não qualificados atribuídos a hosts.

- **Servidores de e-mail** – Verifique se os servidores de e-mail têm configurações que listem os nomes curtos não qualificados de outros hosts locais, como gateways de e-mail de backup, servidores de armazenamento off-line e assim por diante.

- **Certificados** – Verifique se os aplicativos empregam certificados X.509, como programas de telefonia e mensagens instantâneas, têm dados de configuração que usam nomes curtos não qualificados para identificar onde obter informações de revogação sobre certificados de SSL/TLS.

- **Outros aplicativos** – Os aplicativos personalizados podem ter muitos parâmetros de configuração em que os nomes de host podem ser armazenados. O espaço mais óbvio seria nos arquivos de configuração, mas os nomes de host podem aparecer em muitos tipos de dados de aplicativos, links em mídias sociais ou sites wiki, ou até mesmo incorporados no código fonte. Verifique se esses dados de configuração contêm nomes curtos não qualificados.

- **Dispositivos de rede** – Verifique os dispositivos da infraestrutura de rede – firewalls, sistemas de SIEM (Security Information and Event Management,informações de segurança e gerenciamento de eventos), roteadores, comutadores, dispositivos de monitoramento de rede, sistemas de prevenção ou detecção de invasão, servidores VPN, servidores DNS, servidores DHCP, servidores de registro – para determinar se eles estão configurados com nomes curtos não qualificados de outros dispositivos na rede privada.

- **Administração de clientes** – Verifique se as ferramentas de administração de clientes centralizadas, como as que configuram as estações de trabalho e os dispositivos de rede de uma organização, têm nomes curtos não qualificados nas configurações (especialmente listas de busca) que são controladas e redefinidas pelos sistemas.

- **Dispositivos móveis** – Os dispositivos de consumo, como telefones e tablets, podem ter opções de configuração semelhantes às dos aplicativos listados acima e, portanto, possivelmente têm definições de configuração que podem conter nomes curtos não qualificados da rede local.

Todos esses sistemas devem ser verificados quanto aos dados de configuração que armazenam nomes curtos não qualificados, a fim de garantir que esses nomes possam ser alterados quando a raiz do espaço de nome privado for alterada ou quando as listas de busca não forem mais usadas.

3. Quando agir para atenuar as colisões de nomes

Às vezes, são adicionados nomes à zona raiz do DNS global, como quando um nome de país é alterado ou quando a ICANN delega novos TLDs. Esses dois tipos de domínios de primeiro nível têm sido adicionados praticamente todos os anos nos últimas duas décadas. Novos TLDs foram adicionados em 2013 e 2014 e, certamente, haverá mais adições nos próximos anos.

A história demonstra a ocorrência de algumas colisões de nomes no passado, quando TLDs foram adicionados ao DNS. A história também demonstra que ocorreram vazamentos de nomes de espaços de nomes privados durante muitos anos; consulte o *SAC 045*, no anexo A, para obter mais detalhes. A história demonstra ainda que os espaços de nomes e a resolução de nomes para redes privadas nunca estão tão perfeitamente separados quanto os administradores imaginam, e que as consultas de nomes, cuja resolução, de acordo com os administradores, deveria ser feita por servidores de nomes internos, são, às vezes, enviadas a resolvedores no DNS global.

Ocasionalmente os administradores de rede fazem escolhas de nomes com base na suposição de que a lista de nomes na raiz do DNS global é imutável. No entanto, essa lista tem mudado e continuará mudando com o tempo. Por exemplo, quando o TLD `cs` foi adicionado há quase 25 anos para a Tchecoslováquia, muitas universidades usavam listas de busca que permitiam a um usuário inserir um nome terminado por `cs` para o departamento de Ciências da Computação (Computer Science) que estaria totalmente qualificado com o nome de domínio da universidade, e essas decisões resultavam em incerteza na resolução de nomes quando o novo TLD era adicionado à zona raiz, porque os nomes terminados em `cs` eram agora FQDNs no DNS global. Mesmo quando os atuais nomes na raiz do DNS global não se sobrepõem a nomes em um espaço de nome privado (um TLD privado ou uma lista de busca), os administradores de rede geralmente se esquecem de manter-se atualizados sobre os nomes que estão na raiz do DNS global.

É recomendável que o departamento de TI inicie os processos de atenuação o mais rápido possível. Assumir uma postura como “vamos apenas melhorar nosso firewall” poderá reduzir algumas colisões, mas nunca eliminará todas. Da mesma maneira, dizer “vamos pedir que nossos usuários se certifiquem de usar nossos servidores de nomes” ou “faremos os funcionários remotos usarem VPNs” provavelmente reduzirá algumas colisões, mas essas atitudes também poderão dificultar o diagnóstico das colisões restantes.

As colisões de nomes podem ocorrer independentemente dos caracteres no nome. Contudo, o uso de caracteres que não são ASCII, como `ä`, `中` e `ӣ`, em TLDs privados dificulta a análise de colisões. Os resolvedores podem enviar consultas para esses caracteres de maneiras imprevisíveis e que podem não corresponder aos padrões da Internet; por isso, determinar quando ocorrerão as colisões de nomes se torna muito mais difícil.

Embora a raiz do DNS global fique maior do que tem sido nos últimos anos, a adição de nomes à raiz, na verdade, não é algo tão incomum. Para cada novo TLD adicionado, haverá uma chance de ocorrerem colisões de nomes com espaços de nomes privados que vazaram para a Internet, geralmente sem serem notados. As organizações têm usado nomes e assumido o risco de colisões há anos.

Observe que a adição de novos nomes à raiz do DNS não é, nem nunca será, um problema para organizações que já usam FQDNs do DNS global em sua rede. Essas organizações não perceberão uma diferença no seu próprio uso dos nomes no DNS, porque não há colisões. Os problemas só

aparecem para organizações que usam TLDs privados, ou organizações que usam listas de busca que permitem a entrada de nomes curtos não qualificados em que o nome curto em si pode ser um nome válido no DNS global.

3.1 Como determinar a possibilidade de colisões

Para determinar se haverá colisões de nomes no espaço de nome privado da sua organização, é necessário identificar e catalogar todos os espaços de nome privados e as listas de busca no DNS utilizados pela sua organização e, em seguida, fazer uma lista dos nomes de primeiro nível nessas origens. Na maioria das organizações há geralmente um espaço de nome com apenas um nome de primeiro nível. Entretanto, algumas organizações, particularmente aquelas que foram combinadas com outras organizações que também usavam espaços de nomes privados (por exemplo, como o resultado de uma fusão corporativa ou aquisição), têm vários nomes de primeiro nível privados.

Em seguida, é necessário determinar o conteúdo atual e o conteúdo esperado na zona do DNS global. Os nomes na atual zona raiz do DNS global podem ser encontrados em http://data.iana.org/TLD/tlds-alpha-by-domain.txt. Para determinar se o nome de um espaço de nome privado está sendo considerado para alocação pelo programa atual de novos gTLDs:

1. Acesse https://gtldresult.icann.org/application-result/applicationstatus
2. Clique na seta na coluna "String"
3. Avance pelas páginas até encontrar o intervalo que contém o nome do seu espaço de nome privado

Se houver alguma sobreposição entre a lista de TLDs privados que você acabou de fazer e a lista de nomes na raiz do DNS, há uma chance de ocorrerem colisões de nomes e, portanto, a atenuação é necessária agora.

Observe que após a entrada da atual rodada de novos TLDs na zona raiz, mais nomes poderão ser propostos; em particular, a lista de novos TLDs poderá ser alterada e as colisões de nomes entre os espaços de nomes privados e futuros novos TLDs poderão ocorrer. Além disso, as organizações com TLDs privados formados por duas letras (como `ab`) devem estar cientes de que nomes de domínio de primeiro nível com duas letras são reservados para uso como códigos de país, e eles são adicionados à zona raiz por meio de um procedimento totalmente diferente.

3.2 gTLDs do DNS global cuja delegação está adiada indefinidamente

A ICANN declarou que adiará indefinidamente a delegação de três TLDs: .corp, .home, e .mail. Esses gTLDs ainda estão em uso comum nos espaços de nomes privados e, portanto, oferecem um risco de colisões significativamente maior do que outros TLDs. Não é garantido que o adiamento seja para sempre; portanto, qualquer organização que use um desses nomes como espaço de nome privado ainda deverá seguir as instruções da Seção 4 ou Seção 5 para migrar do espaço de nome privado. No entanto, essas organizações têm mais tempo para realizar a migração do que uma organização que tenha utilizado um nome diferente que pode aparecer na raiz do DNS global no futuro imediato.

4. Etapas para atenuar os problemas associados a um TLD privado

O uso de TLDs privados não é indicado como uma prática recomendada há décadas. Na verdade, as instruções que acompanham os produtos Active Directory e Server da Microsoft explicitamente desaconselham o uso de TLDs privados há muitos anos. A atenuação mais eficiente para colisões de nomes decorrentes do vazamento de nomes de um TLD privado para o DNS global é deixar de usar um TLD privado e passar a usar um que esteja enraizado no DNS global.

As etapas nesta seção se aplicam a qualquer rede que tenha, por motivos próprios, optado por usar um TLD privado como sua raiz e usar listas de busca para resolver nomes curtos não qualificados, em vez de colocar seu espaço de nome na raiz do DNS global e fazer consultas no DNS global para a resolução de FQDNs. Esta seção se aplica a qualquer organização que use um TLD privado, e não apenas àquelas que já apresentam o vazamento de consultas de nomes na Internet global. Caso sua organização use o que parece ser um TLD privado “seguro”, ou seja, um nome que ainda não foi solicitado nem aprovado para ser delegado na raiz do DNS global, ainda assim, considere seriamente mudar para um nome enraizado no DNS global. Se você trabalha em uma grande organização com mais de um TLD privado (como uma empresa que se fundiu a outra e não fez a fusão de seus dois espaços de nomes), as etapas nesta seção deverão ser realizadas para cada TLD privado.

É possível que, quando a organização optou por usar um TLD privado, ela tivesse uma convenção de nomenclatura em mente. As etapas aqui podem estar em conflito com esse modelo original. Para atenuar de forma segura os problemas associados às colisões de nomes causadas pelos TLDs privados, os usuários e os sistemas devem alterar o modo como usam os nomes de domínio, e os servidores de nomes locais devem ser reconfigurados de uma maneira que alguns usuários podem achar inconveniente. Use as explicações das consequências involuntárias ou indesejadas que podem afetar sua organização para aumentar a conscientização e estimular a aceitação entre sua comunidade de usuários.

Observação importante: Ao mesmo tempo em que executar as etapas nesta seção, você provavelmente também deverá atenuar as colisões de nomes causadas por listas de busca, o que é abordado na Seção 5. Muitas das etapas dessa seção são iguais a estas e podem ser realizadas ao mesmo tempo.

4.1. Monitorar as solicitações que entram nos servidores de nomes oficiais

Para atenuar os problemas com um TLD privado, liste todos os computadores, equipamentos de rede e qualquer outro sistema que use o TLD privado atual em quaisquer solicitações. Quando você alterar os nomes que estão sendo usados, todos os dispositivos que usarem os nomes privados antigos de maneira automatizada deverão ser atualizados.

Existem três maneiras comuns de realizar esse monitoramento e a enumeração de sistemas:

- O servidor de nomes oficial (como o Active Directory) pode ter um recurso de geração de registros. Ative o recurso de geração de registros para coletar os detalhes de todas as consultas dos nomes privados.

- Muitos firewalls modernos também podem ser configurados para detectar e registrar consultas de nomes privados. Isso pode não ser tão eficiente quanto a geração de registros do sistema de nomenclatura em si, dependendo da topologia de sua rede. Por exemplo, se a consulta não passar por um firewall, o firewall não poderá ver a consulta e, assim, ela será ignorada.

- Se nenhuma das opções anteriores puder ser usada, monitore e colete o tráfego de entrada e de saída do servidor de nomes oficial usando um programa de captura de pacote, como o Wireshark. Contudo, esse método requer que os dados capturados sejam processados com um programa a fim de localizar as consultas somente para os nomes privados.

Algumas organizações optarão (o que é recomendado) por realizar mais de uma das etapas anteriores para aumentar as chances de localizar todas as solicitações. Observe que essa etapa pode produzir resultados confusos. Os dispositivos, como computadores e telefones, têm aplicativos nos quais os usuários digitam nomes; esses dispositivos aparecerão na pesquisa, embora possa não haver nenhuma versão armazenada dos nomes privados antigos. Para essa etapa, basta conhecer todos os locais na sua rede em que o nome privado antigo está sendo armazenado e usado em aplicativos.

4.2. Criar um inventário de cada sistema que usa o TLD privado de maneira automatizada

Você precisará de um resumo dos dados de registro obtidos na etapa anterior. Esse resumo deve ser uma lista de todos os dispositivos e de todos os nomes que estão sendo consultados, em vez de cada instância do dispositivo que está fazendo a consulta. O motivo pelo qual é necessário ter todos os nomes que estão sendo consultados é que alguns dispositivos terão vários aplicativos, e cada um deles deverá ser corrigido. Assim, o resumo deverá incluir todos os sistemas e todos os aplicativos em cada sistema que usarem o TLD privado. Esse resumo será o manifesto dos dispositivos que deverão ser alterados.

4.3. Determinar o local em que seus nomes no DNS global são administrados

É provável que você já tenha um nome no DNS global para sua organização e que o nome de domínio possa ser usado para a raiz do seu espaço de nome privado. Você deve determinar quem é o responsável pelos seus nomes no DNS e os processos que são usados para criar e atualizar os nomes no DNS. Isso pode ser feito pelo seu departamento de TI ou por meio de um provedor de serviço (geralmente a mesma empresa que fornece a sua conexão de Internet).

4.4. Alterar a raiz do seu espaço de nome privado para usar um nome do DNS global

Uma estratégia comum para usar um nome do DNS global como a raiz do seu espaço de nome privado é ter um nome acessível publicamente delegado pelo DNS global, mas usar o seu servidor de nomes oficial para administrar todos os nomes abaixo dele. Por exemplo, se a sua empresa tiver o nome de domínio global `nossaempresa.com`, você poderá escolher `ad1.nossaempresa.com` como o nome raiz.

Se a sua organização tiver mais de um nome de domínio no DNS global, você deverá colocar os seus nomes na raiz abaixo de um nome que possa ser controlado mais facilmente pela equipe de TI da organização. Em alguns casos, nomes adicionais são controlados por outras entidades, como um

departamento de marketing. Se possível, é melhor colocar o nome na raiz abaixo de um nome que já é controlado pelo departamento de TI.

As etapas para fazer essa alteração dependem do software do servidor de nomes privado que você utiliza, a versão específica desse software, a topologia dos servidores de nomes na sua rede privada e a configuração existente do servidor de nomes. Esses detalhes estão além do escopo deste documento, mas devem ser abordados nas instruções do fornecedor do seu sistema. Além disso, em muitas organizações, essa alteração exigirá a autorização de alguns níveis da gerência, particularmente se o gerenciamento dos nomes no DNS global for diferente do gerenciamento do espaço de nome privado.

Como parte desta etapa, se você tiver certificados para algum host que use nomes no espaço de nome privado, será necessário criar certificados para esses hosts usando os novos nomes (totalmente qualificados). As etapas para obter esses certificados dependem da sua CA e, portanto, também estão fora do escopo deste documento.

4.5. Alocar novos endereços IP para hosts, se necessário

Se você tiver certificados de TLS baseados no seu nome de TLD privado antigo, será necessário obter novos certificados para os novos nomes. Se o seu servidor da Web não for compatível com a extensão da SNI (Server Name Indication, indicação de nome de servidor) para o TLS que permite que mais de um nome de domínio seja atendido pelo TLS no mesmo endereço IP, será necessário adicionar endereços IP aos hosts, de modo que o host seja compatível com o nome privado no endereço IP original e o novo nome em um novo endereço IP. Como alternativa, você pode atualizar o software do seu servidor da Web para um versão que execute as extensões de SNI corretamente.

4.6. Criar um sistema para monitorar a equivalência entre os nomes privados novos e antigos

Quando alterar todos os nomes privados para usar a nova raiz, você continuará atendendo a endereços e registrando consultas para seus nomes privados antigos, a fim de verificar sistemas que não estejam em seu inventário e que não foram atualizados para usar os nomes na raiz do DNS. Por causa disso, você deve ter certeza de que os nomes privados novos e antigos tenham os mesmos valores para os endereços IP.

Alguns programas de software de espaço de nome privado permitem manter as duas árvores em paralelo, mas se você tiver um programa mais antigo ou vários servidores de nomes oficiais, provavelmente será necessário monitorar a equivalência usando ferramentas personalizadas. Essas ferramentas personalizadas precisam fazer consultas a todos os nomes com frequência, tanto nos espaços de nomes novos quanto nos antigos, e enviar um alerta, caso haja uma divergência, para que você possa determinar qual sistema foi alterado sem uma alteração paralela no outro sistema.

Se você precisou adicionar endereços IP na etapa anterior porque tem certificados de SSL/TLS, a divergência precisa ser permitida pelo software de monitoramento de equivalência.

4.7. Treinar usuários e administradores de sistema para que usem o novo nome

Além de alterar os sistemas em que os nomes são inseridos em configurações, você deve alterar as formas de pensar dos usuários para que eles mudem dos nomes privados antigos para os novos. Este treinamento deve ser feito antes de implementar as etapas a seguir, para que os usuários tenham uma

chance de acostumar-se aos novos nomes. No entanto, o treinamento deve deixar claro que a alteração é eminente e que, em breve, eles devem começar a pensar tendo em mente os novos nomes. Essa é também uma boa oportunidade para treinar usuários quanto ao uso de FQDNs. Use as explicações das consequências involuntárias ou indesejadas que podem afetar sua organização para aumentar a conscientização e estimular a aceitação.

4.8. Alterar todos os sistemas afetados para os novos nomes

É nesse momento que a migração dos nomes privados antigos para os nomes novos se torna realidade para todos os sistemas (PCs, dispositivos de rede, impressoras etc.) na rede. Os nomes privados são substituídos pelos novos nomes do DNS, sistema por sistema. Cada instância do nome privado antigo é encontrada em todos os programas no sistema e substituída pelo novo nome do DNS. Ao mesmo tempo, é necessário reprovar o uso de nomes curtos não qualificados em listas de busca.

O monitoramento iniciado acima é extremamente importante nesta etapa. É muito improvável que você consiga determinar todos os aplicativos em todos os sistemas que tenham os nomes privados antigos incorporados a eles. Em vez disso, o sistema de monitoramento deverá ser consultado após a alteração de cada sistema a fim de observar se o sistema ainda está fazendo solicitações pelos nomes privados antigos.

Muitos sistemas executam alguns aplicativos de inicialização quando são ligados. Esses aplicativos podem conter nomes de sistemas integrados a eles, e localizar todos eles pode ser uma tarefa difícil. Depois de alterar todos os nomes em um sistema dos nomes privados antigos para os novos nomes do DNS, reinicie o sistema e use o software de monitoramento para observar buscas por nomes. Se o sistema fizer buscas por algum dos nomes privados antigos, determine qual programa está gerando essa solicitação e altere-o para usar os novos nomes. Podem ser necessárias algumas reinicializações nesse processo para configurar todo o sistema corretamente.

4.9. Iniciar o monitoramento quanto ao uso de nomes privados antigos no servidor de nomes

Configure o seu servidor de nomes oficial para iniciar o monitoramento de todas as solicitações por nomes que tenham a raiz antiga. Como os seus usuários não devem mais estar usando esses nomes, o registro criado nessa etapa de monitoramento pode não ser muito grande; se for, será necessário repetir algumas das etapas acima em determinados sistemas na rede.

4.10. Configurar um monitoramento a longo prazo em perímetros para observar a ocorrência de nomes privados antigos

As etapas anteriores devem encontrar a grande maioria de usos de nomes privados antigos, mas alguns sistemas (possivelmente importantes) podem ainda estar usando nomes privados antigos, embora talvez apenas raramente. Uma forma de detectar essas consultas de nomes é adicionar regras a todos os firewalls na extremidade da rede para buscar as solicitações que estejam vazando. Essas regras devem ter uma alta prioridade associada a elas e ser configuradas para gerar notificações de eventos para que a equipe de TI seja alertada imediatamente. Opcionalmente, você pode encontrar esses eventos nos registros do firewall, mas isso aumenta as chances de eles serem ignorados. Os alertas acionados com a ocorrência de solicitações permitirão que a equipe os detectem, embora

esses eventos devam ser raros agora. Alguns firewalls são compatíveis com esse tipo de regra somente mediante a adição de recursos extra a um custo adicional; se esse for o caso de seu firewall, você deve avaliar se o benefício de encontrar solicitações restantes compensa o custo adicional.

4.11. Alterar todos os nomes da raiz antiga para direcionar a um endereço inoperante

Após o treinamento de todos os usuários, a maneira mais eficaz para garantir que eles parem de usar nomes privados antigos antes de removê-los é fazer com que todos os nomes privados antigos direcionem a um servidor configurado para não responder a solicitações de serviço de nenhum tipo. Isso também ajuda a eliminar os sistemas que ainda estão usando o espaço de nome antigo, mas que não foram detectados nas etapas anteriores.

O endereço de direcionamento deve ser um servidor que certamente não estará executando nenhum serviço. Ao fazer isso, não haverá chance de que nenhum sistema que esteja usando um nome privado antigo obtenha informações incorretas e de que os aplicativos relatem erros que deveriam ser facilmente detectados ou compreendidos pelos usuários; como parte do treinamento de conscientização, você pode recomendar que os usuários relatem todos os erros desse tipo à equipe de TI. Quando esta etapa for implementada, o sistema de monitoramento que verifica a equivalência entre os nomes antigos e novos (descrito acima) deverá ser mantido atualizado com as alterações.

Os nomes devem ser alterados um de cada vez, provavelmente com pelo menos algumas horas entre cada alteração ou lote de alterações. Esta etapa possivelmente resultará em chamadas para o departamento de TI; portanto, fazer as alterações em etapas ajudará a equilibrar o volume de chamadas, à medida que os nomes que ainda estejam sendo usados começarem a parar de funcionar.

4.12. Se forem emitidos certificados para algum host com os nomes privados antigos, revogue-os

Se a sua organização obteve certificados de SSL/TLS emitidos para qualquer servidor na rede usando os nomes privados antigos, esses certificados devem ser revogados. Essa revogação é muito simples se a sua organização atuar como sua própria CA. Se usou uma CA comercial para emitir certificados para espaços de nomes privados, você deve determinar o processo para a solicitação de revogação dessa CA; diferentes CAs podem ter diferentes requisitos para essas solicitações.

4.13. Operações a longo prazo com o novo nome

Observe que o antigo nome privado e os domínios abaixo dele ainda estão sendo atendidos, e continuarão sendo atendidos enquanto o servidor de nomes estiver em execução. Não há motivo para removê-los e, em muitos sistemas, como o Active Directory, pode ser difícil remover o primeiro nome que foi configurado no sistema.

Na realidade, há um bom motivo para deixar o nome onde está: isso permitirá que você veja se há resquícios do nome privado antigo nos sistemas da sua rede. Desde que todos os endereços associados a todos os nomes abaixo desse TLD privado direcionem a um host sem serviços em execução, você poderá usar os dois registros do servidor de nomes (e, para obter uma vantagem maior, um sistema que registre todo o tráfego para esse servidor) para determinar se você removeu completamente o nome privado antigo.

5. Etapas para atenuar as colisões de nomes associadas a listas de busca

Para atenuar de forma segura os problemas associados às colisões de nomes decorrentes de listas de busca, os usuários e os sistemas devem mudar sua forma de usar os nomes de domínio. Pode ser interessante preparar os usuários com antecedência com o envio de notificações sobre a alteração, programas de conscientização e treinamento.

Observe que, se você já estiver usando uma administração centralizada, essas ações serão provavelmente mais fáceis do que você imagina. Muitas pessoas que normalmente usam listas de busca sabem que também podem digitar nomes completos se necessário (como se estivessem acessando um servidor de fora da rede privada da organização), e essas pessoas precisarão de menos treinamento do que aquelas que apenas conhecem os nomes curtos não qualificados.

5.1. Monitorar as solicitações que entram no servidor de nomes

Para atenuar os problemas causados por listas de busca, você deve conhecer todos os computadores, equipamentos de rede e qualquer outro sistema que use listas de busca em qualquer solicitação. Todos os dispositivos que usarem listas de buscas de maneira automatizada deverão ser atualizados.

Existem três maneiras comuns de realizar esse monitoramento e a enumeração de sistemas:

- O servidor de nomes recursivo (como o Active Directory) pode ter um recurso de geração de registros. Você pode ativar esse recurso para obter detalhes de todas as consultas que contêm nomes curtos não qualificados.

- Muitos firewalls modernos também podem ser configurados para detectar e registrar consultas de todos os nomes. Isso pode não ser tão eficiente quanto a geração de registros do sistema de nomenclatura em si, dependendo da topologia de sua rede. Por exemplo, se a consulta não passar por um firewall, o firewall não poderá ver a consulta e, assim, ela será ignorada.

- Se nenhuma das opções anteriores puder ser usada, é possível monitorar o servidor de nomes usando um programa de captura de pacote, como o Wireshark. Contudo, esse método requer que os dados capturados sejam processados com um programa a fim de localizar as consultas somente para os nomes curtos não qualificados.

Observe que essa etapa pode produzir resultados confusos. Os dispositivos, como computadores e telefones, podem ter aplicativos nos quais os usuários digitam nomes; esses dispositivos aparecerão na pesquisa, embora possa não haver nenhuma versão armazenada dos nomes curtos não qualificados. Para essa etapa, basta conhecer todos os locais na sua rede em que o nome curto não qualificado está sendo armazenado ou usado em aplicativos.

5.2. Criar um inventário de todos os sistemas que usam nomes curtos não qualificados de maneira automatizada

Você precisará de um resumo dos registros da etapa anterior. Esse resumo deve ser uma lista de todos os dispositivos e de todos os nomes curtos não qualificados que estão sendo consultados, em

vez de cada instância do dispositivo que está fazendo a consulta. O motivo pelo qual é necessário ter todos os nomes que estão sendo consultados é que alguns dispositivos terão vários aplicativos que deverão ser corrigidos. Esse resumo será o manifesto dos dispositivos que deverão ser alterados.

5.3. Treinar usuários e administradores de sistema quanto ao uso de FQDNs

Além de alterar os sistemas em que os nomes curtos não qualificados são inseridos em qualquer configuração (seja ela uma configuração para todo o sistema ou para um aplicativo individual), você deve alterar as formas de pensar dos usuários para que eles passem a usar nomes completos, em vez de nomes curtos não qualificados. Use as explicações das consequências involuntárias ou indesejadas que podem afetar sua organização para aumentar a conscientização e estimular a aceitação.

5.4. Alterar todos os sistemas afetados para o uso de FQDNs

Substitua os nomes curtos não qualificados por seus FQDNs equivalentes, sistema por sistema. Cada instância de um nome curto não qualificado encontrada em todos os programas do sistema deve ser substituída pelo nome de domínio completo.

O monitoramento iniciado acima é extremamente importante nesta etapa. É muito improvável que você consiga determinar todos os aplicativos em todos os sistemas sendo alterados que tenham nomes curtos não qualificados incorporados a eles. Em vez disso, o sistema de monitoramento deverá ser consultado após a alteração de cada sistema a fim de observar se o sistema ainda está fazendo solicitações pelos nomes curtos não qualificados.

Muitos sistemas executam alguns aplicativos de inicialização quando são ligados. Esses aplicativos podem conter nomes de sistemas que dependem das listas de busca integrados a eles, e localizar todos eles pode ser uma tarefa difícil. Depois de alterar todos os nomes em um sistema para usar FQDNs, reinicie o sistema e use o software de monitoramento para observar buscas por nomes. Se o sistema fizer buscas por algum nome curto não qualificado, determine qual programa está gerando essa solicitação e altere-o para usar FQDNs. Podem ser necessárias algumas reinicializações nesse processo para configurar todo o sistema corretamente.

5.5. Desativar as listas de busca em resolvedores de nome compartilhados

É nesse momento que a migração para abandonar os nomes curtos não qualificados se torna realidade para todos os sistemas (PCs, dispositivos de rede, impressoras etc.) na rede. As listas de busca podem existir em qualquer sistema que execute a resolução de nomes ou que forneça configuração para outros sistemas, como um servidor DHCP. Esses sistemas são geralmente servidores de nomes independentes, mas eles também podem ser firewalls ou outros dispositivos de rede. Independentemente do tipo de sistema, as listas de busca precisam ser desativadas em cada um deles para evitar que os usuários tentem usar nomes curtos não qualificados em um determinado espaço de nome.

5.6. Iniciar o monitoramento quanto ao uso de nomes curtos não qualificados no servidor de nomes

Configure o seu servidor de nomes oficial para iniciar o monitoramento de todas as solicitações que precisam usar listas de busca. Se você fornecer notificação e treinamento com antecedência, seus usuários não devem mais estar usando esses nomes. Sendo assim, o registro criado nessa etapa de monitoramento pode não ser muito grande; se for, poderá ser necessário repetir algumas das etapas acima em determinados sistemas na rede.

5.7. Configurar um monitoramento a longo prazo em perímetros para observar a ocorrência de nomes curtos não qualificados

As etapas anteriores devem encontrar a grande maioria de usos de nomes privados antigos, mas alguns sistemas (possivelmente importantes) podem ainda estar usando nomes curtos não qualificados, embora talvez apenas raramente. A melhor maneira de detectar essas consultas de nomes é adicionar regras a todos os firewalls na extremidade da rede para buscar as solicitações que estejam vazando. Essas regras devem ter uma alta prioridade associada a elas e ser configuradas para gerar notificações de eventos para que a equipe de TI seja alertada imediatamente. Opcionalmente, você pode encontrar esses eventos nos registros do firewall, mas isso aumenta as chances de eles serem ignorados. Os alertas acionados com a ocorrência de solicitações permitirão que a equipe os detectem, embora esses eventos devam ser raros agora. Alguns firewalls são compatíveis com esse tipo de regra somente mediante a adição de recursos extra a um custo adicional; se esse for o caso de seu firewall, você deve avaliar se o benefício de encontrar solicitações restantes compensa o custo adicional.

6. Detecção de colisões de nomes nos novos gTLDs

Desde o dia 18 de agosto de 2014, a ICANN está exigindo que os gTLDs que forem delegados na zona raiz ajudem as organizações a detectar quando estiverem vazando consultas no DNS global para os nomes que entrem no novo TLD. Essa ajuda durará 90 dias, normalmente, os primeiros dias em que o novo gTLD estiver na zona raiz; após isso, o novo gTLD se comportará como qualquer outro TLD na zona raiz. A ajuda é fornecida por meio de um serviço de “interrupção controlada” descrito nesta seção.

Claramente, uma organização que precise atenuar colisões de nomes entre seu espaço de nome privado e o DNS global deve fazer isso antes que o novo TLD correspondente entre na zona raiz: ele não deve esperar esse período de 90 dias. (Isso é especialmente verdadeiro para organizações que escolhem um TLD de duas letras como seu nome, porque esses nomes não são necessários para realizar uma interrupção controlada.) As interrupções controladas são projetadas como um último aviso para uma organização que necessite realizar rapidamente a atenuação antes que o TLD comece a dar respostas “reais” às consultas.

Essa seção descreve como uma interrupção controlada é implementada em um servidor de nome oficial e como ela aparece nas respostas às consultas. Também oferece conselhos para que as organizações que têm espaços de nomes privados determinem se as alterações operacionais que estão observando se devem à interrupção controlada e, se for assim, o que fazer em relação a essas alterações.

6.1 Descrição das interrupções controladas

O serviço de interrupção controlada que está sendo solicitado pela ICANN para novos gTLDs adicionados à zona raiz após 18 de agosto de 2014 foi criado para causar uma interrupção dos dispositivos cujas solicitações de nomes de domínio em espaços de nomes privados vazam no DNS global. Atualmente, quando essa solicitação de DNS vaza no DNS global, os servidores de nomes raiz enviam de volta uma resposta com um código que indica que o domínio não existe. (Tecnicamente, esse é o campo RCODE do cabeçalho da resposta que está sendo definido em um valor de 3, definido de maneira mnemônica como uma resposta “NXDOMAIN”.)

Durante o período de serviço de domínios controlados, em vez de um erro de NXDOMAIN na resposta, a resposta não contém nenhuma indicação de erro, mas, em vez disso, contém dados com a maior possibilidade de serem observados pelo sistema que enviou a solicitação. É impossível desenhar uma resposta que sempre seja observada, porque há muitos tipos diferentes de programas de software que fazem solicitações de DNS; no entanto, a interrupção controlada determinada pela ICANN será observável nos sistemas com registros de erros adequados e em redes onde o tráfego do DNS pode ser observado pelos administradores da rede.

Os gTLDs que operam no modo de interrupção controlada responderão a uma ampla variedade de solicitações de DNS de maneira previsível. A Seção 6.2 explica como observar os comportamentos dos sistemas que obtêm respostas de interrupção controlada a essas solicitações de DNS.

- A consulta ao DNS mais comum é para os registros A, ou seja, para o(s) endereço(s) IPv4 associados a um nome de domínio. Essas consultas sempre voltarão com o endereço IPv4 de 127.0.53.53. Este é um endereço de retorno para o host que enviou a consulta, de maneira que se o aplicativo utilizar este endereço para iniciar qualquer tipo de contato, ele enviará a mensagem a si mesmo. O mais provável é que isso falhe, já que quase todos os programas

que fazem pesquisas no DNS tentam utilizar o endereço na resposta para contatar outro servidor.

- Outra consulta comum do DNS é de registros que contêm texto, conhecidos como “registros TXT”. No serviço de interrupção controlada, a resposta do registro TXT sempre será a cadeia de caracteres exata “Your DNS configuration needs immediate attention see https://icann.org/namecollision” (A configuração do seu DNS necessita de atenção imediata, consulte https://icann.org/namecollision). Um sistema que exibe esses registros de texto fornece ao observador informações sobre colisões de nomes.

- Nas consultas do DNS feitas para servidores de correio (tecnicamente, para intercâmbio de e-mail ou registros MX), o serviço de interrupção controlada responderá com o nome de domínio your-dns-needs-immediate-attention.<TLD>, onde “<TLD>“ é o TLD da solicitação do DNS. Este nome de domínio pode ser visível em respostas de erro do cliente de e-mail ou servidor de e-mail. A pesquisa pelo endereço do nome de domínio your-dns-needs-immediate-attention.<TLD> retornará 127.0.53.53.

- O serviço de interrupção controlada responderá às consultas de registros do serviço (SRV) com o nome de domínio your-dns-needs-immediate-attention.<TLD>. As consultas de registros SRV não são tão comuns como aquelas dos endereços IPv4, registros de texto e nomes de servidores de e-mail, mas estão tornando-se mais comuns para os aplicativos mais novos, como mensagens instantâneas e transmissão de voz.

Um gTLD adicionado à zona raiz antes de 18 de agosto de 2014 também pode ter um serviço de interrupção controlada para um subconjunto dos domínios de segundo nível possíveis no TLD. Os registros retornados na interrupção controlada para esses nomes são idênticos aos registros descritos acima. A ICANN exigiu que alguns SLDs sejam bloqueados do TLD e esses nomes podem tornar-se ativos em breve após uma interrupção controlada de 90 dias para os SLDs

6.2 Observando as interrupções controladas

É importante observar que não há garantia de que um aplicativo que receber uma resposta de interrupção controlada agirá de maneira visivelmente diferente do que antes da interrupção controlada. No entanto, muito provavelmente o aplicativo se comportará de maneira diferente e a diferença provavelmente será uma falha; espera-se que a falha tenha uma mensagem de erro associada a ela e o usuário do aplicativo relatará isso ao administrador do sistema que tem a tarefa de solucioná-lo. Se a mensagem de erro incluir o endereço IPv4 127.0.53.53, essa é uma indicação muito forte de que o erro se deve ao programa que está utilizando um nome de um espaço de nome privado que vazou para a Internet pública.

Os erros devidos ao serviço de interrupção controlada aparecem quando um programa que antes estava obtendo respostas NXDOMAIN às consultas começa a obter respostas reais. É claro que estes erros apareceriam mais tarde quando o novo gTLD estivesse respondendo com dados reais, e o serviço de interrupção controlada provavelmente durará apenas os 90 dias determinados pela ICANN. Durante esse tempo, os erros serão mais óbvios porque as mensagens de erro contêm o endereço IPv4 127.0.53.53, o texto “Your DNS configuration needs immediate attention see https://icann.org/namecollision” (a configuração do seu DNS necessita de atenção imediata, consulte https://icann.org/namecollision) ou um nome de domínio contendo “your-dns-needs-immediate-attention”.

As interrupções controladas também podem ser observadas na rede de uma organização se o administrador da rede estiver pesquisando ativamente mensagens de DNS que contenham essas respostas. Essa pesquisa pode ser feita por meio de uma exploração da rede em pontos de ingresso

apropriados, ou pode ser feita em um firewall. Este tipo de observação não depende de ver mensagens de erro no computador afetado; em vez disso, o administrador da rede pode determinar qual é o computador cujas solicitações de nomes em espaços de nomes privados estão vazando da rede da organização.

Independentemente de como a interrupção controlada for descoberta, o resultado seria que o computador que obtém a resposta da interrupção controlada deve ser reconfigurado para fazer apenas consultas do DNS no servidor de nomes da organização, não no DNS global. Não há uma forma padrão de especificar essa configuração, embora ela normalmente faça parte do sistema operacional. Se o computador obtiver suas configurações de rede de um servidor na rede da organização, normalmente denominado “servidor DHCP”, esse servidor deverá alterar suas configurações para que as consultas de DNS sejam enviadas para o servidor de nomes da organização, e não para o DNS global.

Qualquer observação sobre um computador que obtém uma resposta de interrupção controlada é um sinal de que outros computadores da rede dessa organização também as podem estar obtendo. Um administrador do sistema deve imediatamente verificar as configurações do DNS para todos os computadores da mesma rede, mesmo se esses computadores não estiverem mostrando sinais visíveis de obterem respostas de interrupção controlada. Lembre que a interrupção controlada dura apenas 90 dias; portanto, é limitado o tempo para encontrar os computadores que têm configurações de DNS incorretas.

É claro que fazer essas alterações é apenas uma atenuação temporária para o problema subjacente das colisões de nomes. As Seções 4 e 5 deste documento oferecem instruções sobre como fazer atenuações permanentes.

7. Resumo

As colisões de nomes podem gerar resultados inesperados para as organizações que usam espaços de nomes privados. Este documento lista alguns desses possíveis resultados e especifica as práticas recomendadas para alterar o modo como os espaços de nomes privados são utilizados nas organizações. O documento também descreve a interrupção controlada como um meio de identificar onde pode tornar-se aparente o efeito das colisões de nomes.

Para espaços de nomes que usavam um TLD privado que está transformando-se em (ou já é) um TLD no DNS global, o melhor processo de atenuação é a migração do espaço de nome para um espaço de nome que esteja na raiz do DNS global. Para espaços de nomes que usam encurtamento de nomes em listas de pesquisa, a atenuação somente pode ocorrer pela eliminação do uso de listas de pesquisa. As etapas para realizar essas atenuações também podem incluir o monitoramento a longo prazo da rede privada para garantir que todas as instâncias de nomes que possam causar colisões não estejam mais sendo usadas. Haverá meios para que as organizações digam quando vão sofrer colisões de nomes quando alguns novos TLDs forem delegados na zona raiz.

A atenuação abrangente dos problemas causados pelas colisões de nomes é usar FQDNs em todos os locais em que um nome de domínio é usado. Em uma rede que já use o DNS global, isso significa não usar listas de busca. Em uma rede que use um espaço de nome privado, isso significa que o espaço de nome privado deve estar na raiz do DNS global e não usar listas de busca.

Anexo A: Leituras complementares

Os documentos a seguir foram elaborados por várias organizações da ICANN. Outras organizações fornecem documentos que podem ser úteis também. É importante notar que o fornecedor do software e/ou hardware do seu servidor de nomes pode ter informações valiosas no respectivo site de suporte técnico.

A.1. Introdução ao programa de novos gTLDs

Esta página descreve a história, a implementação e o progresso do programa para adicionar centenas de novos gTLDs ao DNS global.
http://newgtlds.icann.org/en/about/program

A.2. Colisões de nomes no DNS

ICANN contratou o Interisle Consulting Group, LLC, para criar este relatório detalhado sobre possíveis colisões de nomes. Ele fornece uma visão geral sobre as colisões de nomes, apresenta dados sobre os atuais TLDs não existentes que são atualmente consultados nos servidores raiz e oferece muitas informações de histórico sobre os problemas que as colisões de nomes podem causar.
http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3. Plano de gestão de ocorrências de colisões de novos gTLDs

Este é o plano adotado pela ICANN sobre como gerenciar ocorrências de colisões de nomes entre novos gTLDs e espaços de nomes privados. Ele também inclui muitos indicadores para comentários recebidos pela ICANN para propostas anteriores referentes às colisões de nomes na zona raiz.
http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4. Estrutura para a gestão de ocorrências de colisões de nomes

Este documento é parte integrante do plano de gestão de ocorrências de colisões de novos gTLDs. Ele define as especificações do serviço de interrupção controlada para gTLDs que serão delegados na zona raiz do DNS a partir de 18 de agosto de 2014.
http://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

A.5. Preocupações a respeito de novos gTLDs: nomes sem ponto e colisões de nomes

As listas de busca em diferentes sistemas podem fornecer resultados muito diferentes dependendo do conteúdo do nome curto não qualificado que estiver sendo consultado. Este artigo aborda as listas de busca por domínios sem ponto (TLDs que contêm registros de endereço em seu ápice), mas a descrição do processamento da lista de busca é valiosa em muitos outros contextos também.
https://labs.ripe.net/Members/gih/dotless-names

A.6. SAC 045: consultas inválidas em domínio de primeiro nível no nível raiz do sistema de nomes de domínio

Este relatório do SSAC da ICANN descreve os tipos de consultas por TLDs que foram observadas por servidores raiz no momento da sua elaboração.
http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.7. SAC 057: conselho do SSAC sobre certificados de nomes internos

Este relatório do SSAC da ICANN descreve as implicações de segurança e estabilidade para certificados que contêm nomes privados (internos). Ele identifica uma prática de CAs que pode ser explorada por invasores e representar um risco significativo à privacidade e à integridade das comunicações seguras na Internet.
http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf