Guía para la Identificación y Mitigación de Colisión de Nombres destinada a Profesionales de IT

5 de diciembre de 2013
Versión 1.0

Tabla de Contenidos

1. Introducción 4
1.1 Colisiones de nombres 5
1.2 Colisiones de nombres debido a TLDs privados 6
1.3 Colisiones de nombres debido a listas de búsqueda 6

2. Problemas causados por las colisiones de nombres 8
2.1 Direccionamiento a sitios web inesperados 8
2.2 Correos electrónicos direccionados a destinatarios equivocados 9
2.3 Reducciones de seguridad 9
2.4 Sistemas afectados por las colisiones de nombres 10

3. Cuándo mitigar las colisiones de nombres 12
3.1 Determinación del potencial para colisiones 13

4. Pasos para mitigar los problemas asociados con los TLD privados 14
4.1. Monitorear las peticiones recibidas por los servidores de nombre autoritativos 14
4.2. Crear un inventario de cada sistema que utiliza el TLD privado en forma automatizada 15
4.3. Determinar si sus nombres del DNS global están siendo administrados 15
4.4. Cambiar la raíz de su espacio de nombre privado para utilizar un nombre del DNS global 15
4.5. Asignar nuevas direcciones IP para los hosts, si fuese necesario 16
4.6. Crear un sistema para monitorear la equivalencia entre los nombres privados nuevos y antiguos 16
4.7. Capacitar a usuarios y administradores de sistema para utilizar el nuevo nombre 17
4.8. Cambiar cada sistema afectado hacia los nuevos nombres 17
4.9. Comenzar a monitorear el uso de antiguos nombres privados en el servidor de nombres 17
4.10. Establecer el monitoreo a largo plazo en los perímetros para observar antiguos nombres privados 18
4.11. Cambiar todos los nombres de la antigua raíz que apunten a direcciones fuera de servicio 18
4.12. Si se emitieron certificados para cualquier host bajo los antiguos nombres privados, revocarlos 18
4.13. Operaciones a largo plazo con los nuevos nombres 19

5. Pasos para mitigar las colisiones de nombres asociadas a las listas de búsqueda 20
5.1. Monitorear las peticiones recibidas por el servidor de nombres 20
5.2. Crear un inventario de cada sistema utilizando nombres breves no cualificados en forma automatizada 21
5.3. Capacitar a los usuarios y administradores de sistema en el uso de FQDNs 21
5.4. Cambiar cada sistema afectado hacia el uso de FQDN 21
5.5. Desactivar las listas de búsqueda en los dispositivos de resolución de nombres compartidos 21
5.6. Comenzar a monitorear el uso de nombres breves no cualificados en el servidor de nombres 22
5.7. Establecer el monitoreo a largo plazo en los perímetros para observar nombres breves no cualificados 22

6. Resumen 23

Apéndice A: Para mayor información 24
A.1 Introducción al Programa de Nuevos gTLD 24
A.2 Colisión de nombres en el DNS 24
A.3 Plan para la gestión de colisiones de nuevos gTLD 24

A.4 Preocupaciones por los nuevos gTLD: nombres sin punto y colisiones de nombres 24
A.5 SAC 045: Consultas de TLD inválidas a nivel de la raíz del DNS 24
A.6 SAC 057: Asesoramiento del SSAC sobre los certificados de nombres internos..... 24

1. Introducción

Tras la entrada de un nuevo nombre de dominio de nivel superior en la raíz del DNS (Sistema de Nombres de Dominio) global, las organizaciones pueden ver que las consultas para resolver algunos de los nombres "internos" específicos a su red devuelven valores diferentes, ofreciendo diferentes resultados a los usuarios y programas. Existen dos problemas básicos: Los nombres "internos" que se filtran a la Internet global y espacios de nombres privados que se definen en conflicto con el espacio de nombres del DNS global.

La causa de estos resultados diferentes es que una consulta del DNS que un administrador de red previó resolver de manera local —utilizando un espacio de nombres interno—, ahora se está resolviendo mediante la utilización de datos de nuevos dominios de nivel superior en el DNS global. Bajo estas circunstancias, las consultas nunca previstas para salir de la red interna ahora están obteniendo resultados en el DNS global, y esos resultados son diferentes. Como mínimo, los nombres filtrados que producen diferentes resultados pueden ser molestos para los usuarios (por ejemplo, pueden causar retraso en el acceso a las páginas web). También pueden plantear problemas de seguridad (tal como que el correo electrónico se envíe a destinatarios equivocados).

El presente documento cubre las estrategias de mitigación y prevención de los tipos más comunes de espacios de nombres privados utilizados por las organizaciones. Este documento describe aquello que las organizaciones pueden encontrar cuando los nombres internos se filtran al DNS global y especifica las prácticas recomendadas de mitigación. Tanto la descripción como el asesoramiento que aquí se ofrecen están dirigidos a los profesionales de IT (Tecnología de la Información) —administradores de red, administradores de sistemas y personal del departamento de IT—, quienes en general entienden cómo funciona el DNS y cómo funcionan sus propios sistemas de nombres internos. Los lectores que deseen obtener más antecedentes, pueden referirse a los documentos enumerados en el Apéndice A en relación a la seguridad y dirigirse en particular a los informes del Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN (Corporación para la Asignación de Números y Nombres en Internet).

La ICANN —la organización que administra el contenido de la raíz del DNS global—, ha preparado este documento en consulta con expertos en materia del espacio de nombres, a fin de asistir a las organizaciones cuyos espacios de nombres privados pueden estar en conflicto con la raíz del DNS global. La ICANN ha publicado otros documentos que describen la manera en que el DNS global está organizado, cómo los nuevos nombres son incorporados a la raíz del DNS y más. El Apéndice A de este documento enumera referencias sobre diversos temas para una lectura ulterior.

Tenga en cuenta que si bien este documento se refiere a medidas de mitigación de colisiones de nombre, únicamente se analizan los problemas que las organizaciones pueden encontrar al resolver nombres. No se ocupa de otras cuestiones relacionadas con el funcionamiento del DNS global en sí mismo. Por ejemplo, los servidores de nombres de la raíz del DNS global siempre han sido inundados con consultas que nunca estuvieron previstas para ser procesadas por el DNS global (véase el documento SAC 045 en el Apéndice A), pero los servidores de nombres de la raíz también han contado siempre con el suficiente abastecimiento como para poder responder a este exceso de consultas. Este documento no aborda cuestiones relacionadas con los servidores de nombres de la raíz. Aborda sólo las consecuencias de las consultas que se filtren inadvertidamente a los servidores de nombres de la raíz pública del DNS.

La ICANN ha desarrollado una página web que ofrece materiales informativos relacionados con colisiones de nombres, la cual se encuentra disponible en http://www.icann.org/en/help/name-collision.

La página también incluye un proceso para informar daños severos demostrables, como consecuencia de la colisión de nombres causada por los nuevos dominios genéricos de nivel superior (gTLDs).

1.1 Colisiones de nombres

El DNS global es un espacio de nombres jerárquico, y los nombres en el DNS se componen de una o más etiquetas que crean un nombre completo. En la parte superior de la jerarquía está la zona raíz del DNS que contiene un conjunto de nombres, tales como `com`, `ru`, `asia` y demás; estos son los TLDs (dominios de nivel superior) globales, comúnmente conocidos simplemente como "los TLDs". Un ejemplo de un nombre de dominio completo (a menudo llamado un nombre de dominio plenamente cualificado o FQDN por sus siglas en inglés) podría ser `www.nuestraempresa.com`.

Casi todos los espacios de nombres privados también son jerárquicos. Hay tres tipos principales de espacios de nombres privados:

- **Espacios de nombres que se derivan del DNS global** - Los espacios de nombres privados que se derivan del DNS global tienen su raíz bajo un nombre que se puede resolver en el DNS global, aunque toda la estructura de directorio bajo ese nombre es administrada en forma local, con nombres que los administradores de IT nunca previeron ver en el DNS global. Por ejemplo, considere un espacio de nombres privado arraigado bajo `winserve.nuestraempresa.com`: los nombres en ese espacio de nombres privado (winserve) son administrados por el servidor de nombres privado y no son visibles en el DNS global.

- **Espacios de nombres que utilizan sus propias raíces con TLDs privados** - La raíz del espacio de nombres privado es una etiqueta única que no es un TLD global. La estructura completa del directorio —incluyendo la del TLD privado—, es administrada por servidores de nombre privados que no son visibles en el DNS global. Por ejemplo, si el espacio de nombres privado tiene su raíz en `nuestraempresa`, entonces los servidores de nombre privados también son responsables de `www.nuestraempresa`, `region1.nuestraempresa`, `www.region1.nuestraempresa`, y así sucesivamente. Existen diversos tipos de espacios de nombres diferentes, los cuales utilizan sus propias raíces con TLDs privados. Algunos ejemplos incluyen el *Active Directory* de Microsoft (en algunas configuraciones), el DNS multidifusión (RFC 6762) y servicios de directorio LAN más antiguos que aún se utilizan en algunos rincones de Internet.

- **Espacios de nombres que son creados mediante el uso de listas de búsqueda** - Una lista de búsqueda es una función de un dispositivo de resolución de nombres a nivel local (ya sea para un espacio de nombres privado o un dispositivo de resolución recursiva para el DNS global). Una lista de búsqueda permite al usuario introducir nombres abreviados para mayor comodidad; durante la resolución, el servidor de nombres agrega los nombres configurados a la derecha del nombre en una consulta. (Estos nombres configurados también se llaman *sufijos*.)

Los espacios de nombres que se derivan del DNS global sólo causan una colisión de nombres cuando se combinan con las listas de búsqueda. Cualquier consulta que implica un FQDN proveniente del DNS global, por definición, nunca generará una colisión de nombres con un nombre diferente en el DNS global. Esta consulta sólo podría causar colisiones de nombres cuando sean creados inadvertidamente a través de la utilización de listas de búsqueda.

El concepto de "espacios de nombres privados" confunde a muchas personas que están en gran medida acostumbrados al uso típico de Internet; es decir, las personas que sólo están familiarizadas con los nombres del DNS global y que pueden sorprenderse al saber que algunas consultas de resolución de nombres no resultan o no deben resultar en una consulta al DNS global. Ellos podrían

sorprenderse más aún al enterarse de que algunas consultas de nombres están intencionalmente destinadas a iniciarse en el espacio de nombres privado, pero terminan en el DNS global. Una de las razones por las cuales se pueden producir colisiones de nombres es que las consultas destinadas a un servidor de nombres de un espacio de nombres privado comiencen incorrectamente en el DNS global.

1.2 Colisiones de nombres debido a TLDs privados

Las colisiones de nombres se producen como resultado de dos eventos. En primer lugar, una consulta para un nombre de dominio completo que tiene raíz en un TLD privado se filtra desde la red privada al DNS global. En segundo lugar, la consulta localiza en el DNS global exactamente el mismo nombre que existe en la red privada bajo el TLD privado.

Una causa común de este tipo de colisiones de nombres es el uso de un nombre en un sistema como el *Active Directory* de Microsoft, el cual no constituye un TLD en el DNS global al momento en que el sistema es configurado, sino que es agregado más tarde al DNS global. Este tipo de colisión de nombres ya ha ocurrido muchas veces antes y se espera que continúe con la introducción de nuevos TLDs al DNS global (véase la Introducción al Programa de Nuevos gTLD en el Apéndice A).

1.3 Colisiones de nombres debido a listas de búsqueda

Otra causa de colisión de nombres es el procesamiento de las listas de búsqueda. Si una consulta no es un FQDN, es un *nombre breve no cualificado*. Una lista de búsqueda contiene uno o más sufijos. Los mismos se añaden en forma iterativa del lado derecho de una consulta. Cuando un dispositivo de resolución no puede resolver un nombre breve no cualificado, añade sufijos de la lista mientras intenta resolver el nombre hasta que un nombre coincidente es encontrado. Una lista de búsqueda es una función muy útil; sin embargo, el procesamiento de las listas de búsqueda se adapta al uso de nombres breves no cualificados que no son FQDN creando así, inadvertidamente, espacios de nombres que no tienen su raíz en el DNS global. En este caso, la colisión de nombres ocurre cuando una cadena de caracteres que el usuario prevé utilizar como un nombre breve no cualificado es en realidad completado por la lista de búsqueda y resuelto como un FQDN.

Por ejemplo, supongamos que un dispositivo de resolución de nombres tiene una lista de búsqueda que consiste en los sufijos `nuestraempresa.com` y `marketing.nuestraempresa.com`. Supongamos además que un usuario ingresa `www` en un programa que utiliza ese dispositivo de resolución. El dispositivo de resolución puede entonces consultar primero `www`, y si eso no arrojase resultado, luego podría consultar `www.nuestraempresa.com` y luego `www.marketing.nuestraempresa.com`.

Nótese el uso de la palabra "podría" en la descripción de este ejemplo. Las reglas para la forma en que las listas de búsqueda son aplicadas al realizar la resolución de nombres, varían según los sistemas operativos o aplicaciones. Algunos sistemas intentarán siempre resolver un nombre, ya sea en el espacio de nombres privado o en el DNS global, antes de aplicar la lista de búsqueda. Sin embargo, otros sistemas utilizarán la lista de búsqueda primero si la cadena de caracteres que se consulta no contiene un carácter "`.`" . Y otros utilizarán la lista de búsqueda si la cadena de caracteres que se consulta finaliza con un carácter "`.`". Algunos sistemas operativos y aplicaciones (tal como navegadores web) han modificado sus reglas de lista de búsqueda varias veces. De modo que resulta poco práctico predecir cuándo se utilizarán o no las listas de búsqueda, qué es o no es un nombre breve no cualificado y, por lo tanto, si es o no probable que los nombres breves no cualificados se filtren al DNS global. Véase *Preocupaciones por los Nuevos gTLD*: *Nombres sin punto y colisiones de nombres* en el Apéndice A, para más detalles acerca de la diversidad de procesamiento de las listas de búsqueda.

Esta descripción de las listas de búsqueda puede ser una sorpresa para algunos lectores, dado que son tan comunes en lugares que a primera vista no aparentan crear "espacios de nombres privados" . Cada sufijo de una lista de búsqueda define otro espacio de nombres que puede ser consultado durante la resolución de nombres. Esto crea un espacio de nombres privado, que funciona de manera confiable únicamente cuando el cliente consulta los dispositivos de resolución particulares para ese espacio de nombres. Dependiendo de la implementación de la lista de búsqueda, algunos dispositivos de resolución de nombres incluso podrían probar el nombre breve no cualificado ingresado por el usuario o configurado en el software, antes de añadir cualquiera de los nombres en la lista de búsqueda. Por ejemplo, el ingreso de `www.hr` en un lugar de Internet podría producir un resultado a partir de la resolución del DNS, mientras que al ingresarlo en un lugar diferente podría producir un resultado diferente. Cuando esto ocurre, uno de esos espacios de nombres "privados" está relacionado al otro.

El uso de listas de búsqueda en lugar de resolver los FQDNs a través del DNS mundial global, contribuye a la incertidumbre en la resolución de nombres. Las colisiones de nombres producidas por las listas de búsqueda son difíciles de predecir debido a lo comunes que son las listas de búsqueda. Las mismas son parte del software de resolución de nombres en muchos sistemas operativos, equipos de red, servidores y más. El software de los dispositivos de resolución actúa de manera diferente de un sistema a otro, entre diferentes versiones del mismo sistema operativo e incluso como una función de la visualización de un sistema o aplicación respecto a la procedencia de la solicitud en la red. La implementación de un servicio de resolución de nombres que resuelve nombres utilizando sólo el DNS global es la mejor garantía contra tal incertidumbre y resultados impredecibles.

2. Problemas causados por las colisiones de nombres

Las colisiones de nombres basadas en consultas que se filtran al DNS global a partir de redes privadas, pueden tener muchas consecuencias no deseadas. Cuando una consulta obtiene una respuesta positiva, pero con una respuesta que proviene del DNS global en lugar del espacio de nombres privado esperado, la aplicación que efectúa la consulta intentará conectarse a un sistema que no forma parte de la red privada, y podrá tener éxito. Tal conexión podría ser una molestia (al introducir un retraso durante la resolución de nombres). También podría llegar a constituir un problema de seguridad; es decir, puede crear una vulnerabilidad que podría ser explotada con fines maliciosos, dependiendo de lo que la aplicación haga después de conectarse.

2.1 Direccionamiento a sitios web inesperados

Supongamos que un usuario ingresa `https://finanzas.nuestraempresa` en su navegador web, estando en una red privada, y que la red dispone de un espacio de nombres cuyo TLD privado es `nuestraempresa`. Si la consulta del navegador para el nombre `finanzas.nuestraempresa` se resuelve como se esperaba, el navegador obtiene una dirección IP para el servidor web interno del departamento de finanzas. Sin embargo, imaginemos que el TLD `nuestraempresa` es también parte del DNS global, y que ese TLD tiene un dominio de segundo nivel (SLD) `finanzas`. Si la consulta se filtra, se resolverá a una dirección IP diferente de la cual lo hacía cuando resolvía en el espacio de nombres privado. Ahora imagine que esta dirección IP diferente pudiese alojar un servidor web. El navegador podría intentar conectarse a un servidor web en la Internet pública, no en la red privada.

Tal como se mostró anteriormente, el mismo problema puede ocurrir incluso en las redes que no tienen TLDs privados, pero que utilizan listas de búsqueda. Considere que un navegador que se utiliza normalmente en una red donde los usuarios tienen una lista de búsqueda que tiene el nombre `nuestraempresa.com`, y el usuario introduce el nombre `www.finanzas` con el fin de llegar al host `www.finance.ourcompany.com`. Ahora imagine que el navegador está siendo utilizado por un empleado desde un dispositivo móvil en una tienda de café. Si esa consulta se filtra a la Internet, y hay un TLD llamado `finanzas`, la consulta podría resolverse a una dirección IP diferente, por ejemplo, a un host totalmente diferente cuyo nombre en el DNS global sea `www.finance`. Esa consulta causaría que el navegador intente conectarse a un servidor web en una parte completamente diferente de la Internet pública respecto a la que tendría que conectarse si la consulta se resolviese a través del dispositivo de resolución de la red privada.

Una respuesta común del usuario ante este escenario es que reconozca que este era un sitio web equivocado y salga en forma inmediata. No obstante, un navegador puede exponer una gran cantidad de información a un servidor web si el navegador "confía" en dicho servidor web, dado que tiene el mismo nombre de dominio que uno que el navegador ha visitado antes. El navegador podría ingresar automáticamente información de acceso u otros datos sensibles, exponiendo así la información a que pueda ser capturada o analizada fuera de la organización. En otras circunstancias (por ejemplo, un ataque cuidadosamente formulado en contra de la organización), el navegador podría conectarse a un sitio que aloje un código malicioso para instalar programas peligrosos en la computadora.

Tenga en cuenta que el uso de TLS (Seguridad en la Capa de Transporte) y certificados digitales podrían no ayudar a prevenir los daños debido a las colisiones de nombres; de hecho, podrían empeorar las cosas, ofreciendo a los usuarios una falsa sensación de seguridad. Muchas de las autoridades de certificación (CAs) que emiten certificados para los nombres en el DNS global también

emiten certificados para nombres breves no cualificados en espacios de direcciones privadas, de modo que es posible que un usuario que sea mal dirigido a un sitio aún observe un certificado válido. Véase el documento SAC 057 en el Apéndice A para obtener más detalles sobre los certificados de nombres a partir de espacios de nombres privados.

2.2 Correos electrónicos direccionados a destinatarios equivocados

Las consecuencias posibles que surgen de las colisiones de nombres no se limitan a los navegadores web. Los correos electrónicos enviados a un destinatario pueden ser enviados a un destinatario diferente si los nombres de host son iguales en las direcciones de los destinatarios; por ejemplo, un correo electrónico a `chris@asistencia.nuestraempresa` se podría entregar a una cuenta de usuario completamente diferente si `nuestraempresa` se convierte en un TLD del DNS global. Incluso si el mensaje no se entrega a un usuario de correo electrónico en particular, podría haber un intento de enviarlo, y tales intentos podrían exponer el contenido del correo electrónico a ser capturado o analizado fuera de una organización.

Muchos dispositivos de red tales como firewalls (también llamados cortafuegos o programas de seguridad), enrutadores e incluso impresoras pueden estar configurados para enviar notificaciones o datos de acceso por correo electrónico. Si el nombre del destinatario que se ha especificado para las notificaciones de correo electrónico luego sufre una colisión de nombres en el DNS global, dichas notificaciones podrían ser entregadas a un destinatario completamente accidental. Un evento o un dato de acceso en el cuerpo del mensaje que puede revelar la configuración de la red y el comportamiento del host podrían filtrarse hacia un destinatario no deseado. El desempeño rutinario de la red o el análisis de tráfico por parte del personal de IT puede verse interrumpido si el destinatario de dichos datos nunca recibe los datos de acceso o los eventos que desencadenan notificaciones no pueden ser investigados o mitigados.

2.3 Reducciones de seguridad

Los incidentes de colisión de nombres que no son mitigados, pueden exponer a los sistemas de redes privadas a un comportamiento no deseado o perjuicio. Los sistemas que dependen de la resolución de nombres para su correcto funcionamiento y que también realizan funciones de seguridad *pueden* funcionar en forma confiable cuando se utilizan FQDNs y se resuelven a partir del DNS global.

Por ejemplo, en los firewalls, a menudo las reglas de seguridad están basadas en el origen o destino de un flujo de paquetes. El origen y el destino de los paquetes son direcciones IPv4 o IPv6, pero muchos firewalls permiten que también sean ingresados como nombres de dominio. Si se utilizan nombres breves no cualificados y la resolución de nombres no se realiza como se esperaba, las reglas pueden fallar para bloquear o permitir el tráfico del modo intencionado por el administrador. Del mismo modo, los accesos del firewall a menudo utilizan nombres de dominio, y el uso de nombres breves no cualificados que resuelven de manera impredecible puede interferir con la supervisión, el análisis o la respuesta a eventos. El personal de IT que revisa los accesos podría, por ejemplo, malinterpretar la gravedad de un evento debido a que un nombre breve no cualificado en el acceso podría identificar diferentes hosts en función de donde dicho acceso ha tomado lugar (es decir, en el registro, el mismo nombre breve no cualificado podría aparecer y ser asociado con dos o más direcciones IP diferentes). Este problema puede verse agravado por el hecho de que la mayoría de los firewalls pueden actuar como su propio dispositivo de resolución del DNS o permitir a los administradores utilizar o configurar las listas de búsqueda.

2.4 Sistemas afectados por las colisiones de nombres

Todos los sistemas conectados a la red deben ser revisados por el uso de nombres de host que estén en la raíz de un TLD o nombres de host que estén basados en listas de búsqueda. Todas estas instancias de "uso" tendrán que ser actualizadas para utilizar un FQDN del DNS global. Una lista no exhaustiva de los sistemas o aplicaciones a revisar, incluiría:

- **Navegadores** - los navegadores web permiten a los usuarios especificar la ubicación de los servidores proxy HTTP, y muy a menudo éstos se encuentran en la red privada. Comprobar si un usuario o personal de IT ha realizado páginas de inicio personalizadas, marcadores o motores de búsqueda: éstos pueden tener enlaces a servidores de la red privada. Algunos navegadores también tienen opciones de configuración para el lugar donde conseguir información de revocación de los certificados SSL/TLS, que podrían apuntar a nombres de host de la red privada.

- **Servidores web** - Los servidores web ofrecen contenido HTML que contiene enlaces y metadatos que han incorporado nombres de host. Compruebe si los servidores web en una red privada tienen contenido con nombres breves no cualificados. Compruebe si los archivos de configuración del servidor web tienen nombres breves no cualificados de otros hosts de la red privada.

- **Agentes de usuario de correo electrónico** - Los clientes de correo electrónico, como *Outlook* y *Thunderbird*, cuentan todos con opciones de configuración para el lugar donde recibir el correo electrónico utilizando el protocolo POP o IMAP, y donde enviar el correo electrónico a través del protocolo SUBMIT; todos ellos podrían usar nombres de host de la red privada. Compruebe si estas aplicaciones están configuradas para obtener información de revocación de los certificados SSL/TLS a partir de los nombres breves no cualificados asignados a los hosts.

- **Servidores de correo electrónico** - Compruebe si los servidores de correo electrónico tienen configuraciones que enumeran los nombres breves no cualificados de otros hosts locales, tal como las pasarelas de respaldo de correo electrónico, los servidores de almacenamiento fuera de línea y demás.

- **Certificados** - Compruebe si las aplicaciones que utilizan certificados X.509 , tal como los programas de telefonía y mensajería instantánea, tienen datos de configuración que utilizan nombres breves no cualificados para identificar el lugar donde obtener información de revocación de los certificados SSL/TLS.

- **Otras aplicaciones** - Las aplicaciones personalizadas pueden tener muchos parámetros de configuración del lugar donde los nombres de host podrían ser almacenados. El espacio más obvio sería en los archivos de configuración, pero los nombres de host podrían aparecer en muchos tipos de datos de la aplicación, enlaces en las redes sociales o sitios wiki, o incluso en programaciones permanentes del código fuente. Compruebe estos datos de configuración para los nombres breves no cualificados.

- **Dispositivos de red** - Comprobar los dispositivos de infraestructura de red: firewalls, sistemas de información y gestión de eventos (SIEM), enrutadores, interruptores, dispositivos de monitoreo de red, detección de intrusos o sistemas de prevención, servidores VPN, servidores del DNS, servidores DHCP, servidores de acceso; para determinar si éstos están configurados con nombres breves no cualificados de otros dispositivos de la red privada.

- **Administración de clientes** - Comprobar si las herramientas de administración de cliente centralizadas, como las que configuran las estaciones de trabajo y los dispositivos de red de una organización tienen nombres breves no cualificados en las configuraciones (especialmente las listas de búsqueda), que sean controlados y restablecidos por los sistemas.

- **Dispositivos móviles** - Los dispositivos del consumidor tal como los teléfonos y tabletas pueden tener opciones de configuración similares a algunas de las aplicaciones mencionadas anteriormente, y por lo tanto, posiblemente tengan opciones de configuración que podrían contener nombres breves no cualificados de la red local.

Todos estos sistemas deben ser revisados para comprobar cuáles datos de configuración almacenan nombres breves no cualificados a fin de garantizar que estos nombres se puedan cambiar cuando cambie la raíz del espacio de nombre privado o cuando las listas de búsqueda ya no sean utilizadas.

3. Cuándo mitigar las colisiones de nombres

A veces los nombres se agregan a la zona raíz del DNS global, tal como cuando cambia el nombre de un país o cuando la ICANN delega nuevos TLDs. Ambos tipos de dominios de nivel superior han sido añadidos casi todos los años, desde hace más de dos décadas. Este año (2013) se han añadido nuevos nombres y se espera que más sean añadidos en 2014 y más allá.

La historia muestra que se han producido algunas colisiones de nombres cuando los TLDs son añadidos al DNS. La historia también demuestra que los nombres de espacios de nombres privados se han filtrado desde hace muchos años, en algunos casos con una frecuencia muy alta; véase el documento SAC 045 en el Apéndice A para mayor información. La historia demuestra que los espacios de nombres y la resolución de nombres destinados a las redes privadas nunca están tan completamente segregados como los administradores piensan que están; y que las consultas de nombres que los administradores prevén que sean resueltas por los servidores de nombres internos, a veces son enviadas a dispositivos de resolución del DNS global.

A veces los administradores de red toman decisiones de nombres basados en suposiciones de que la lista de nombres en la raíz del DNS global es inmutable, pero de hecho esa lista tiene y tendrá cambios en el tiempo. Por ejemplo, cuando se añadió el TLD `cs` hace casi 25 años para el país de Checoslovaquia, muchas universidades utilizaban listas de búsqueda que permitían a un usuario introducir un nombre que terminaba con `cs` en alusión al departamento de Ciencias de la Computación ['cs' por sus siglas en inglés], que fuesen plenamente cualificados con el nombre de dominio de la universidad; y estas decisiones dieron lugar a incertidumbres en la resolución de nombres cuando el nuevo TLD fue añadido a la zona raíz, debido a que los nombres que terminaban con `cs` pasaron a ser FQDNs en el DNS global. Incluso cuando los nombres actuales de raíz del DNS global a menudo no se superponen con los de un espacio de nombre privado (ya sea un TLD privado o una lista de búsqueda), los administradores de red a menudo olvidan mantenerse al día respecto a qué nombres están en la raíz del DNS global.

Se recomienda que un departamento de IT comience los esfuerzos de mitigación lo más pronto posible. El adoptar una postura de "simplemente mejoraremos nuestro firewall" puede reducir algunas colisiones, pero nunca vamos a erradicarlas a todas. Del mismo modo, es probable que diciendo "haremos que nuestros usuarios se aseguren de utilizar nuestros servidores de nombres " o " haremos que los trabajadores remotos utilicen VPNs" se reduzcan algunas colisiones, aunque ello también dificultaría diagnosticar las colisiones restantes.

Las colisiones de nombres pueden ocurrir independientemente de los caracteres en el nombre; sin embargo, el uso de caracteres no ASCII, tal como `ä` y `中` y `ѝ` en TLDs privados complica el análisis de las colisiones. Los dispositivos de resolución pueden enviar consultas para éstos en formas que son difíciles de predecir y pueden no coincidir con los estándares de Internet; de modo que la determinación de cuándo ocurrirán colisiones de nombres se vuelve mucho más difícil.

Aunque la raíz del DNS global acabará más grande de lo que ha sido en años anteriores, la incorporación de nombres a la raíz en realidad no es tan inusual. Por cada nuevo TLD añadido hay una posibilidad de que no haya colisiones de nombres con los espacios de nombres privados que se han ido filtrando a Internet, en forma mayormente desapercibida. Por años las organizaciones han estado utilizando nombres y asumiendo el riesgo de colisiones.

Téngase en cuenta que la incorporación de nuevos nombres a la raíz del DNS no es —y nunca será—, un problema para las organizaciones que ya utilizan FQDNs del DNS global en su red. Estas organizaciones no verán ninguna diferencia en su propio uso de nombres del DNS, dado que no existe

ninguna colisión de nombres. Los problemas únicamente aparecen para las organizaciones que utilizan TLDs privados u organizaciones que utilizan listas de búsqueda que permiten ingresar nombres breves no cualificados, donde el nombre abreviado en sí mismo podría constituir un nombre válido en el DNS global.

3.1 Determinación del potencial para colisiones

Para que usted pueda determinar si habrá o no colisiones de nombres con el espacio de nombre privado de su organización, es necesario identificar y catalogar todos los espacios de nombres privados y las listas de búsqueda del DNS que utiliza su organización, y luego compilar una lista de los nombres de nivel superior en estas fuentes. Para la mayoría de las organizaciones, generalmente hay sólo un espacio de nombre con un único nombre de nivel superior, pero algunas organizaciones —en particular las que se han combinado con otras organizaciones que también estaban utilizando espacios de nombres privados (por ejemplo, como resultado de una fusión o adquisición de negocios)— tienen múltiples nombres privados de nivel superior.

Luego, es necesario determinar tanto los contenidos actuales como los esperados en la zona del DNS global. Los nombres de la actual zona raíz del DNS global se pueden encontrar en http://data.iana.org/TLD/tlds-alpha-by-domain.txt. Para determinar si un nombre de un espacio de nombre privado está siendo considerado para asignarse a través del Programa de Nuevos gTLD que está activo en el año 2013:

1. Refiérase a https://gtldresult.icann.org/application-result/applicationstatus
2. Presione sobre la flecha de la columna "String" (cadena de caracteres)
3. Desplácese por las páginas hasta encontrar el rango que contiene el nombre de su espacio de nombres privado.

Si hay alguna superposición entre la lista de TLDs privados que acaba de realizar y la lista de nombres en la zona del DNS, existe la posibilidad de que haya una colisión de nombres, y por lo tanto es necesario que ahora se tomen medidas de mitigación.

Nótese que posteriormente a que la actual ronda de nuevos TLDs se introduzcan en la zona raíz, podrían proponerse más de ellos; en particular, la lista de nuevos TLDs puede cambiar y se pueden producir colisiones de nombres entre los espacios de nombres privados y los futuros nuevos TLD. Además, las organizaciones con TLDs privados que constan de dos letras (tal como `ab`) deben ser conscientes de que los nombres de dominio de nivel superior de dos letras están reservados para ser utilizados como códigos de país, y los mismos se añaden a la zona raíz a través de un procedimiento completamente diferente.

4. Pasos para mitigar los problemas asociados con los TLD privados

Durante décadas, el uso de TLDs privados no ha sido recomendado como una mejor práctica recomendada. De hecho, durante muchos años, las instrucciones que vienen con los productos *Active Directory* y *Server* de Microsoft han desalentado explícitamente el uso de los TLDs privados. La mitigación más eficaz para las colisiones de nombres, planteadas por nombres que terminan en un TLD privado filtrándose al DNS global, es cambiar el uso desde un TLD privado a uno que tenga su raíz en el DNS global.

Los pasos de esta sección se aplican a cualquier red que, por sus propias razones, ha optado por utilizar un TLD privado como su raíz y utilizar listas de búsqueda para resolver los nombres breves no cualificados, en lugar de colocar la raíz de su espacio de nombres en el DNS global y consultar al DNS global para la resolución de FQDNs. Esta sección se aplica a cualquier organización que utiliza un TLD privado, no únicamente a aquellas que ya tienen consultas de nombres filtrándose a la Internet global. Si su organización está utilizando lo que se percibe como un TLD privado "seguro" —es decir, un nombre que aún no ha sido solicitado o autorizado para delegar en la raíz del DNS global—, usted debe considerar seriamente la posibilidad de cambiar a un nombre con raíz en el DNS global. Si usted trabaja en una gran organización con más de un TLD privado (tal como una empresa que se ha fusionado con otra empresa y no ha fusionado sus dos espacios de nombres), debe realizar los pasos de esta sección para cada TLD privado.

Lo más probable es que cuando la organización optó por utilizar un TLD privado, lo hubiese hecho con una convención particular de nombres en mente. Los pasos del presente documento pueden estar en conflicto con ese modelo original. Con el fin de mitigar los problemas asociados con la colisión de nombres debido a los TLDs privados en forma confiable, los usuarios y los sistemas ambos necesitan cambiar la forma en que utilizan los nombres de dominio y los servidores de nombres locales deben ser reconfigurados de una manera que algunos usuarios pueden encontrar inconveniente. Utilice las explicaciones de las consecuencias no previstas o no deseadas que pueden afectar a su organización, con el fin de crear conciencia y fomentar la aceptación entre su comunidad de usuarios.

Nota importante: Al mismo tiempo que está llevando a cabo los pasos de esta sección, es probable que también deba mitigar las colisiones de nombres causadas por las listas de búsqueda, lo cual se trata en la Sección 5. Muchos de los pasos en esa sección son los mismos que los aquí presentados, se puede realizar al mismo tiempo.

4.1. Monitorear las peticiones recibidas por los servidores de nombre autoritativos

Con el fin de mitigar los problemas con un TLD privado, realice una lista de todas las computadoras, equipos de red y cualquier otro sistema que utilice el actual TLD privado en cualquier petición. Cuando cambie los nombres que se utilizan, todos los dispositivos que utilizan los antiguos nombres privados en forma automatizada deben ser actualizados.

Hay tres formas comunes de realizar este monitoreo y enumeración de los sistemas:

- El servidor de nombres autoritativo (por ejemplo, *Active Directory*) puede tener una función de registro. Active la función de registro para recopilar los datos de todas las consultas para los nombres privados.

- Muchos firewalls modernos también pueden ser configurados para detectar y registrar las consultas de nombres privados. Dependiendo de la topología de la red, esto puede no ser tan eficaz como acceder desde el sistema de nombres en sí mismo. Por ejemplo, si una consulta no pasa a través de un firewall, éste no puede ver la consulta y por lo tanto se perderá.

- De no poder utilizarse nada de lo anterior, supervise y recopile el tráfico entregado a y emitido por el servidor de nombres autoritativo, utilizando un programa de captura de paquetes, como *Wireshark*. No obstante, este método requiere que los datos capturados sean procesados con un programa, con el fin de encontrar las consultas únicamente para los nombres privados.

Algunas organizaciones elegirán (y deben hacerlo) tomar más de una de las acciones anteriores, con el fin de aumentar las posibilidades de encontrar todas las solicitudes. Tenga en cuenta que este paso puede producir resultados confusos. Los dispositivos tales como computadoras y teléfonos tienen aplicaciones en las cuales los usuarios ingresan nombres; esos dispositivos se mostrarán en el sondeo incluso cuando podría no existir ninguna versión almacenada de los antiguos nombres privados. Para este paso, sólo es necesario conocer todos los lugares en su red donde los antiguos nombres privados están siendo almacenados y utilizados para las aplicaciones.

4.2. Crear un inventario de cada sistema que utiliza el TLD privado en forma automatizada

Usted necesita un resumen de los registros obtenidos en el paso anterior. Dicho resumen debe ser una lista de todos los dispositivos y todos los nombres que son consultados, en lugar de todas las instancias en que el dispositivo hace una consulta. La razón por la cual usted necesita todos los nombres que están siendo consultados, es que algunos dispositivos cuentan con múltiples aplicaciones que deberán arreglarse en forma individual. Por lo tanto, el resumen debe incluir tanto a todos los sistemas como a todas las aplicaciones en cada sistema que utilice el TLD privado. Este resumen se convierte en el listado de los dispositivos que necesitan cambiarse.

4.3. Determinar si sus nombres del DNS global están siendo administrados

Es probable que usted ya cuente con un nombre del DNS global para su organización, y que el nombre de dominio pueda ser utilizado para la raíz de su espacio de nombres privado. Es necesario determinar quién está a cargo de sus nombres del DNS y qué procesos utilizan para crear y actualizar los nombres en el DNS. Esto se puede hacer dentro de su departamento de IT o puede hacerse a través de un proveedor de servicios (a menudo la misma empresa que le ofrece conectividad a Internet).

4.4. Cambiar la raíz de su espacio de nombre privado para utilizar un nombre del DNS global

Una estrategia común para el uso de un nombre del DNS global como la raíz de su espacio de nombres privado, es contar con un nombre de acceso público delegado a partir del DNS global, pero luego utilizar su servidor de nombres autoritativo existente para administrar todos los nombres debajo de él. Por ejemplo, si su empresa tiene el nombre de dominio global `nuestraempresa.com`, usted podría elegir `ad1.ourcompany.com` como el nombre de la raíz.

Si su organización cuenta con más de un nombre de dominio en el DNS global, todos sus nombres deben estar en la raíz bajo uno que pueda ser fácilmente controlado por el personal de IT de su organización. En algunos casos, los nombres adicionales son controlados por otras entidades, tal

como un departamento de marketing. De ser posible, lo mejor es colocar su nombre en la raíz bajo un nombre que la organización de IT ya controle.

Los pasos para realizar este cambio dependen del software del servidor de nombres privado que usted tenga, la versión específica de ese software, la topología de los servidores de nombres en su red privada y la configuración existente del servidor de nombres. Estos detalles están más allá del alcance del presente documento, aunque deben estar incluidos en las instrucciones de su proveedor para su sistema actual. Además, en muchas organizaciones, este cambio requerirá la autorización por parte de algunos niveles de dirección, sobre todo si la administración de los nombres del DNS global es diferente de la administración del espacio de nombres privado.

Si usted tiene certificados para cualquier host que utilice nombres en el espacio de nombres privado es necesario, como parte de este paso, que genere certificados para esos hosts utilizando los nuevos nombres (completos/plenamente cualificados). Los pasos a seguir para la obtención de estos certificados dependen de su CA, por lo cual también están más allá del alcance del presente documento.

4.5. Asignar nuevas direcciones IP para los hosts, si fuese necesario

Si usted tiene certificados TLS basados en su antiguo nombre de TLD privado, tendrá que obtener nuevos certificados para los nuevos nombres. Si su servidor web no respalda la extensión de Indicación de Nombre del Servidor (SNI) hacia TLS que permita a más de un nombre de dominio ser atendido bajo la TLS en la misma dirección IP, tendrá que agregar direcciones IP a los hosts, de manera que los hosts respalden al antiguo nombre privado en la dirección IP original y al nuevo nombre en una dirección IP nueva. En forma alternativa, usted puede actualizar su software del servidor web a una versión que maneje extensiones SNI en forma correcta.

4.6. Crear un sistema para monitorear la equivalencia entre los nombres privados nuevos y antiguos

Al cambiar todos los nombres privados para utilizar la nueva raíz, usted continuará atendiendo direcciones y accediendo a consultas para sus antiguos nombres privados, con el fin de comprobar si los sistemas que no están en su inventario y que no fueron actualizados, utilizan los nombres con raíz en el DNS. Debido a esto, usted necesita garantizar que los nombres privados nuevos y antiguos tengan los mismos valores para las direcciones IP.

Algunos programas del espacio de nombres privado le permitirán mantener los dos árboles en paralelo, pero si usted tiene un software más antiguo o múltiples servidores de nombres autoritativos, es probable que tenga que monitorear la equivalencia utilizando herramientas personalizadas. Estas herramientas personalizadas deben consultar a menudo todos los nombres —tanto del espacio de nombres nuevo como del antiguo— y avisarle si se produce una falta de coincidencia, para que usted pueda determinar qué sistema ha cambiado sin un cambio paralelo en el otro sistema.

Si usted necesita añadir direcciones IP en el paso anterior, debido a contar con los certificados SSL/TLS, la falta de coincidencia debe ser permitida por el software de monitoreo de equivalencias.

4.7. Capacitar a usuarios y administradores de sistema para utilizar el nuevo nombre

Además de cambiar los sistemas en los cuales se introducen nombres en las configuraciones, es necesario cambiar la manera de pensar de los usuarios, con el fin de conseguir que cambien de los nombres privados antiguos a los nuevos. Esta capacitación debe hacerse antes de implementar las siguientes medidas, de modo que los usuarios cuenten con la oportunidad de acostumbrarse a los nuevos nombres; aunque la formación debe dejar claro que el cambio está llegando y que a la brevedad, deberán comenzar a pensar en términos de los nuevos nombres. Este es también un buen momento para formar a los usuarios sobre el uso de los FQDNs. Utilice las explicaciones de las consecuencias no previstas o no deseadas que pueden afectar a su organización, con el fin de crear conciencia y fomentar la aceptación.

4.8. Cambiar cada sistema afectado hacia los nuevos nombres

Este es el punto en el que la migración desde los antiguos nombres privados hacia los nuevos nombres privados se vuelve real para todos los sistemas en la red (computadoras, dispositivos de red, impresoras, etc.). Los nombres privados son reemplazados por los nuevos nombres del DNS sobre una base de sistema por sistema. Cada instancia del antiguo nombre privado es encontrada en todo el software del sistema y es reemplazada con el nuevo nombre del DNS. Al mismo tiempo se debe desvalorizar el uso de nombres breves no cualificados en las listas de búsqueda.

El seguimiento iniciado anteriormente, resulta excepcionalmente importante en este paso. Es improbable que usted logre determinar todas las aplicaciones en todos los sistemas que tienen incrustados los antiguos nombres privados. En lugar de ello, el sistema de monitoreo debe ser consultado después de que cada sistema sea cambiado, con el fin de observar si ese sistema continúa generando peticiones para los antiguos nombres privados.

Muchos sistemas ejecutan algunas aplicaciones de inicialización cuando se encienden por primera vez. Estas aplicaciones pueden tener nombres de sistemas incrustados en ellos, y el encontrarlos todos puede ser difícil. Luego de cambiar todos los nombres en un sistema, desde los antiguos nombres privados hacia los nuevos nombres del DNS, reinicie el sistema y utilice el software de monitoreo para observar las búsquedas de nombre. Si el sistema busca cualquiera de los antiguos nombres privados, es necesario determinar qué software está causando esa petición y cambiarlo para que utilice los nuevos nombres. Este proceso podría requerir de algunos reinicios, con el fin de configurar un sistema en forma correcta y completa.

4.9. Comenzar a monitorear el uso de antiguos nombres privados en el servidor de nombres

Usted debe configurar su servidor de nombres autoritativo para que inicie el monitoreo de todas las peticiones de nombres que tengan la antigua raíz. Debido a que los usuarios ya no deberían utilizar más estos nombres, el registro creado por este paso de monitoreo no puede ser muy grande; y si lo es, tendrá que repetir algunos de los pasos anteriores para sistemas específicos de su red.

4.10. Establecer el monitoreo a largo plazo en los perímetros para observar antiguos nombres privados

Los pasos anteriores deberían haber encontrado la gran mayoría de usos de los antiguos nombres privados, pero algunos sistemas (posiblemente clave) pueden seguir usando los antiguos nombres privados, aunque tal vez sólo en raras ocasiones. Una forma de detectar estas consultas de nombre es agregar reglas a todos los firewalls, en la periferia de su red, para buscar cualquier petición que se esté filtrando. Estas reglas deben tener una alta prioridad asociada a ellas y deben configurarse para generar notificaciones de eventos, con el fin de que el personal de IT sea prontamente alertado. En lugar de ello, usted podría encontrar estos eventos en los registros del firewall, pero el hacer esto conlleva a una mayor probabilidad de no detectarlos. Las alertas que se desencadenan cuando se producen las peticiones, permitirán al personal detectar estos eventos, esperados ahora en rara ocasión. Algunos firewalls únicamente admiten este tipo de regla mediante el agregado de características adicionales a un costo adicional; si esto es lo que sucede con su firewall, deberá evaluar si el beneficio de encontrar dichas peticiones justifica el costo adicional.

4.11. Cambiar todos los nombres de la antigua raíz que apunten a direcciones fuera de servicio

Tras capacitar a los usuarios, la forma más eficaz para garantizar que dejen de utilizar los antiguos nombres privados antes de eliminarlos, es hacer que todos los antiguos nombres privados apunten a un servidor que se haya configurado para no responder a las peticiones de servicio de ningún tipo. Esto también ayuda a erradicar cualquier sistema que todavía utilice el antiguo espacio de nombres y que no hubiese sido detectado en los pasos anteriores.

La dirección apuntada debe ser un servidor con garantía de no ejecutar ningún servicio. Al hacer esto, no existe ninguna posibilidad de que algún sistema que utilice un antiguo nombre privado obtenga información errónea y las aplicaciones informarán errores que deben ser fácilmente detectables o entendidos por los usuarios; como parte de la capacitación para la toma de conciencia, se puede recomendar que los usuarios informen todos los errores de este tipo al personal de IT. Al implementar este paso, el sistema de monitoreo que está comprobando la equivalencia entre los nombres antiguos y los nuevos (descripto anteriormente) debe mantenerse actualizado con los cambios.

Los nombres se deben cambiar de uno por vez, probablemente con al menos unas horas entre cada cambio o lote de cambios. Es probable que este paso provoque llamadas al departamento de IT, por lo cual organizar los cambios le ayudará a equilibrar la carga de llamadas a medida que los nombres que se encontraban en uso comiencen a dejar de funcionar.

4.12. Si se emitieron certificados para cualquier host bajo los antiguos nombres privados, revocarlos

Si su organización contaba con certificados SSL/TLS emitidos por cualquier servidor de su red, utilizando los antiguos nombres privados, dichos certificados deben ser revocados. Esto es bastante fácil de hacer si su organización actúa como su propia CA. Si ha utilizado una CA comercial para emitir certificados para el espacio de nombres privado, es necesario determinar ese proceso del CA para solicitar la revocación; diferentes CAs pueden tener diferentes requisitos para tales solicitudes.

4.13. Operaciones a largo plazo con los nuevos nombres

Tenga en cuenta que el antiguo nombre privado y dominios debajo de él aún están siendo atendidos y continuarán siendo atendidos por el tiempo que usted opere el servidor de nombres. No hay ninguna razón para eliminarlos, y en muchos sistemas tales como *Active Directory,* puede ser difícil eliminar el primer nombre que ha sido configurado en el sistema.

En realidad hay una buena razón para dejar el nombre allí: esto le permite ver si hay vestigios residuales del antiguo nombre privado en los sistemas de su red. Mientras todas las direcciones asociadas con todos los nombres bajo ese TLD apunten a un host que no ejecute servicios, se pueden utilizar ambos accesos a partir del servidor de nombres (y, para el beneficio adicional, un sistema de acceso para todo el tráfico a ese servidor) para determinar qué tan minucioso fue al eliminar el antiguo nombre privado.

5. Pasos para mitigar las colisiones de nombres asociadas a las listas de búsqueda

Con el fin de mitigar de manera fiable los problemas asociados con las colisiones de nombres debido a las listas de búsqueda, los usuarios y los sistemas tienen que cambiar la forma en que utilizan los nombres de dominio. Puede resultar útil preparar a los usuarios con antelación, a través de notificaciones de cambio, programas de sensibilización y capacitación.

Tenga en cuenta que si usted ya cuenta con una administración centralizada, estas acciones probablemente sean menos difíciles de lo que podría pensar. Muchas personas que normalmente utilizan las listas de búsqueda saben que, de ser necesario, también pueden ingresar los nombres completos (por ejemplo, si están accediendo a un servidor desde fuera de la red privada de la organización) y necesitarán menos capacitación que aquellos que sólo entienden los nombres breves no cualificados.

5.1. Monitorear las peticiones recibidas por el servidor de nombres

Con el fin de mitigar los problemas causados por las listas de búsqueda, es necesario conocer todas las computadoras, equipos de red y cualquier otro sistema que utilice las listas de búsqueda en cualquier petición. Todos los dispositivos que utilizan las listas de búsqueda en forma automatizada tendrán que ser actualizados.

Hay tres formas comunes de realizar este monitoreo y enumerar los sistemas:

- El servidor de nombres recursivo (tal como *Active Directory*) puede tener una función de registro, y dicha función puede ser activada para obtener los detalles de todas las consultas que tienen nombres breves no cualificados.

- Muchos firewalls modernos también pueden ser configurados para detectar y registrar las consultas de nombres privados. Dependiendo de la topología de la red, esto puede no ser tan eficaz como acceder desde el sistema de nombres en sí mismo. Por ejemplo, si una consulta no pasa a través de un firewall, éste no puede ver la consulta y por lo tanto se perderá.

- De no poder utilizarse nada de lo anterior, el servidor de nombres puede ser monitoreado utilizando un programa de captura de paquetes, como *Wireshark*. No obstante, este método requiere que los datos capturados sean procesados con un programa, con el fin de encontrar las consultas únicamente para los nombres breves no cualificados.

Tenga en cuenta que este paso puede producir resultados confusos. Los dispositivos tales como computadoras y teléfonos pueden tener aplicaciones en las cuales los usuarios ingresan nombres; esos dispositivos se mostrarán en el sondeo incluso cuando podría no existir ninguna versión almacenada de los nombres breves no cualificados. Para este paso, sólo es necesario conocer todos los lugares de su red donde un nombre breve no cualificado está siendo almacenado o utilizado para las aplicaciones.

5.2. Crear un inventario de cada sistema utilizando nombres breves no cualificados en forma automatizada

Usted necesita un resumen de los registros obtenidos en el paso anterior. Dicho resumen debe ser una lista de todos los dispositivos y todos los nombres breves no cualificados que son consultados, en lugar de todas las instancias en que el dispositivo hace una consulta. La razón por la cual usted necesita todos los nombres que están siendo consultados, es que algunos dispositivos cuentan con múltiples aplicaciones que deberán ser arregladas. Este resumen se convierte en el listado de los dispositivos que necesitan cambiarse.

5.3. Capacitar a los usuarios y administradores de sistema en el uso de FQDNs

Además de cambiar los sistemas donde los nombres breves no cualificados son ingresados en cualquier configuración (ya sea una configuración de todo el sistema o la configuración de una aplicación individual), es necesario cambiar la forma en que los usuarios piensan para que cambien el uso de los nombres abreviados por nombres completos. Utilice las explicaciones de las consecuencias no previstas o no deseadas que pueden afectar a su organización, con el fin de crear conciencia y fomentar la aceptación.

5.4. Cambiar cada sistema afectado hacia el uso de FQDN

Reemplace los nombres breves no cualificados con FQDNs equivalentes, sobre una base de sistema por sistema. Cada instancia de un nombre breve no cualificado que es encontrada en todo el software del sistema debe ser reemplazada con el nombre de dominio completo.

El seguimiento iniciado anteriormente, resulta excepcionalmente importante en este paso. Es improbable que usted logre determinar todas las aplicaciones en todos los sistemas que están siendo cambiados que tienen incrustados los nombres breves no cualificados. En lugar de ello, el sistema de monitoreo debe ser consultado después de que cada sistema sea cambiado, con el fin de observar si ese sistema continúa generando peticiones para los nombres breves no cualificados.

Muchos sistemas ejecutan algunas aplicaciones de inicialización cuando se encienden por primera vez. Estas aplicaciones pueden tener nombres de sistemas que dependen de las listas de búsqueda incrustados en ellos, y el encontrarlos todos puede ser difícil. Luego de cambiar todos los nombres en un sistema para utilizar FQDNs, reinicie el sistema y utilice el software de monitoreo para observar las búsquedas de nombre. Si el sistema busca cualquiera de los nombres breves no cualificados, es necesario determinar qué software está causando esa petición y cambiarlo para que utilice los FQDNs. Este proceso podría requerir de algunos reinicios, con el fin de configurar un sistema en forma correcta y completa.

5.5. Desactivar las listas de búsqueda en los dispositivos de resolución de nombres compartidos

Este es el punto en que la migración desde los nombres breves no cualificados se convierte en realidad para todos los sistemas en la red (computadoras, dispositivos de red, impresoras, etc.). Las listas de búsqueda pueden existir en cualquier sistema que procese la resolución de nombres o que sirva de configuración para otros sistemas, como por ejemplo un servidor de DHCP (Protocolo de Configuración Dinámica de Host). A menudo estos sistemas son servidores de nombres

independientes, pero también pueden ser servidores de firewalls o de otros dispositivos de la red. Independientemente del tipo de sistema, las listas de búsqueda deben desactivarse en cada uno de ellos, con el fin de evitar que los usuarios intenten utilizar los nombres breves no cualificados dentro de un espacio de nombres determinado.

5.6. Comenzar a monitorear el uso de nombres breves no cualificados en el servidor de nombres

Usted debe configurar su servidor de nombres para que inicie el monitoreo de todas las peticiones de nombres que necesitan utilizar las listas de búsqueda. Si usted ofrece notificación y capacitación anticipada, los usuarios no deberían utilizar estos nombres nunca más, de modo que el registro creado por este paso de monitoreo no puede no ser muy grande; y si lo es, tendrá que repetir algunos de los pasos anteriores para sistemas específicos de su red.

5.7. Establecer el monitoreo a largo plazo en los perímetros para observar nombres breves no cualificados

Los pasos anteriores deberían haber encontrado la gran mayoría de usos de los nombres breves no cualificados, pero algunos sistemas (posiblemente clave) pueden seguir usando dichos nombres, aunque tal vez sólo en raras ocasiones. La mejor forma de detectar estas consultas de nombre es agregar reglas a todos los firewalls, en la periferia de su red, para buscar cualquier petición que se esté filtrando. Estas reglas deben tener una alta prioridad asociada a ellas y deben configurarse para generar notificaciones de eventos, con el fin de que el personal de IT sea prontamente alertado. En lugar de ello, usted podría encontrar estos eventos en los registros del firewall, pero el hacer esto conlleva a una mayor probabilidad de no detectarlos. Las alertas que se desencadenan cuando se producen las peticiones, permitirán al personal detectar estos eventos, esperados ahora en rara ocasión. Algunos firewalls únicamente admiten este tipo de regla mediante el agregado de funciones adicionales a un costo adicional; si esto es lo que sucede con su firewall, deberá evaluar si el beneficio de encontrar dichas peticiones justifica el costo adicional.

6. Resumen

Las colisiones de nombres tienen el potencial de crear resultados inesperados para las organizaciones que utilizan los espacios de nombres privados. El presente documento enumera algunos de esos posibles resultados y especifica las mejores prácticas recomendadas para cambiar la forma en que los espacios de nombres privados son utilizados dentro de las organizaciones.

Para los espacios de nombres que utilizaban un TLD privado que se está volviendo (o ya es) un TLD en el DNS global, la mejor mitigación proviene en la forma de migrar el espacio de nombres a un espacio de nombres que tenga raíz en el DNS global. Para los espacios de nombres que utilizan el nombre abreviado con listas de búsqueda, la mitigación puede provenir sólo por la eliminación del uso de tales listas de búsqueda. Los pasos para lograr estas acciones de mitigación, incluyen también el monitoreo de la red privada a largo plazo, para garantizar que todas las instancias de los nombres que pudiesen causar colisiones ya no estén siendo utilizadas.

La mitigación exhaustiva de los problemas de colisiones de nombres consiste en utilizar FQDNs en todos los lugares donde se utilizaba un nombre de dominio. En una red que ya está utilizando el DNS global, esto significa no utilizar listas de búsqueda. En una red que utiliza un espacio de nombres privado, esto significa que el espacio de nombres privado debe tener su raíz en el DNS global, y no debe utilizar listas de búsqueda.

Apéndice A: Para mayor información

Los siguientes documentos fueron producidos por varias organizaciones dentro de la ICANN. Otras organizaciones brindan documentos que también podrían serle útiles. Cabe destacar que el proveedor del software y/o hardware de su servidor de nombres puede tener información valiosa en el área de soporte técnico de su sitio web.

A.1 Introducción al Programa de Nuevos gTLD

Esta página describe la historia, la implementación y la progresión del programa para introducir cientos de nuevos gTLDs al DNS global.
http://newgtlds.icann.org/en/about/program

A.2 Colisión de nombres en el DNS

La ICANN encargó a *Interisle Consulting Group, LLC* la creación de este informe detallado sobre las posibles colisiones de nombres. Dicho documento ofrece una visión general de las colisiones de nombres, presenta datos sobre TLDs actualmente inexistentes que en la actualidad son consultados en los servidores de raíz, y brinda una gran cantidad de antecedentes sobre los problemas que las colisiones de nombres podrían presentar.
http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3 Plan para la gestión de colisiones de nuevos gTLD

Este es el plan adoptado por la ICANN en relación a cómo manejar los incidentes de colisión de nombres entre los nuevos gTLDs y los espacios de nombres privados. También incluye muchas referencias a comentarios recibidos por la ICANN en relación a las propuestas anteriores referidas a las colisiones de nombres en la zona raíz.
http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4 Preocupaciones por los nuevos gTLD: nombres sin punto y colisiones de nombres

Las listas de búsqueda en diferentes sistemas pueden entregar resultados muy diferentes dependiendo de aquello que figura en el nombre breve no cualificado que se está consultando. Este artículo se enfoca en las listas de búsqueda de dominios sin punto (TLDs que tienen registros de dirección en su ápice), pero la descripción del procesamiento de las listas de búsqueda es valiosa en muchos otros contextos.
https://labs.ripe.net/Members/gih/dotless-names

A.5 SAC 045: Consultas de TLD inválidas a nivel de la raíz del DNS

Este informe del SSAC de la ICANN describe los tipos de consultas de TLDs que fueron vistos por los servidores de raíz al momento de escribirse.
http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.6 SAC 057: Asesoramiento del SSAC sobre los certificados de nombres internos

Este informe del SSAC de la ICANN describe las implicaciones de seguridad y estabilidad para los certificados que contienen nombres privados (internos).

El mismo identifica una práctica por parte de los CAs, que puede ser explotada por atacantes y que podría suponer un riesgo importante para la privacidad y la integridad de las comunicaciones seguras en Internet.
http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf