دليل إلى تعريف تضارب الأسماء والحد منه للمتخصصين في مجال تقنية المعلومات

1 أغسطس 2014
نسخة 1.1

جدول المحتويات

1. مقدمة

بعد إدخال اسم نطاق جديد من المستوى الأعلى في جذر DNS العالمي، قد ترى المؤسسات أن الاستعلامات المقدمة لحل بعض من الأسماء "الداخلية" والخاصة بشبكتهم تحيلهم إلى قيم مختلفة، مما يوفر للمستخدمين والبرامج نتائج مختلفة. وهناك مشكلتان أساسيتان: الأسماء "الداخلية" التي تتسرب داخل الإنترنت العالمي، ومساحات الأسماء الخاصة التي يتم تحديدها بشكل متضارب مع مساحة أسماء DNS العالمية.

والسبب في الوصول إلى هذه النتائج المختلفة هو أن أي استعلام DNS والذي اعتزم مدير شبكة حله على المستوى الداخلي باستخدام مساحة اسم داخلية، يجري الآن حله باستخدام بيانات نطاق جديد من المستوى الأعلى في نظام DNS العالمي. وبموجب هذه الظروف، فإن الاستعلامات التي لم يتوقع مطلقًا أن تغادر الشبكة الداخلية تحصل الآن على نتائج في نظام DNS العالمي، كما أن هذه النتائج مختلفة. وعلى أقل تقدير، فإن الأسماء المتسربة التي تؤدي إلى نتائج متباينة قد تكون مزعجة بالنسبة للمستخدمين (على سبيل المثال، قد تتسبب في تأخر الوصول إلى صفحات الويب). كما قد تمثل مشكلات بالنسبة للأمان (مثل إرسال البريد الإلكتروني إلى مستلمين غير معنيين).

تغطي هذه الوثيقة إستراتيجيات التخفيف والوقاية بالنسبة للأنواع الأكثر شيوعًا لمساحات الأسماء الخاصة التي تستخدمها المؤسسات. ويصف هذا المستند ما يمكن أن تصادفه المؤسسات عند تسرب الأسماء الداخلية إلى نظام DNS العالمي وتحدد ممارسات التخفيف الموصى بها. والوصف والنصيحة المقدمين هنا موجهين إلى متخصصين تقنية المعلومات (مديري الشبكات، ومديري الأنظمة، وفريق عمل تقنية المعلومات) الذين يفهمون بشكل عام كيفية عل نظام DNS وكيفية عمل نظم الأسماء الداخلية الخاصة بهم. تتم إحالة القراء الراغبين في مزيد من الخلفية إلى الوثائق في الملحق أ. أما القراء المعنيين بالأمان فيتم توجيههم على وجه الخصوص إلى التقارير الواردة من اللجنة الاستشارية للأمن والاستقرار (SSAC) التابعة لـICANN.

أما ICANN، تلك المنظمة التي تدير محتويات جذر نظام DNS العالمي، فقد أعدت هذه الوثيقة بالتشاور مع الخبراء المتخصصين في مساحة الأسماء من أجل مساعدة المؤسسات التي قد تكون مساحات الأسماء الخاصة بها متضاربة مع جذر DNS العالمي. وقد نشرت ICANN وثائق أخرى تصف كيفية تنظيم DNS العالمي، وكيفية إضافة الأسماء الجديدة في جذر DNS، وغير ذلك الكثير. ويسرد الملحق أ من هذه الوثيقة مراجع حول العديد من الموضوعات لإجراء مزيد من القراءة. بالإضافة إلى ذلك، بدأت ICANN مؤخرًا في مساعدة المنظمات التي تستخدم مساحات الأسماء في معرفة متى سوف يبدأ تصادم مساحات الأسماء، هذا موصوف في القسم 1.4 والقسم 6.

لاحظ أنه على الرغم من أن هذه الوثيقة تتناول إجراءات التخفيف لحالات تضارب الأسماء، فإنها تناقش فقط المكلات التي قد تصادفها تلك المؤسسات عند حل الأسماء. كما أنها تتناول المشكلات الأخرى ذات الصلة بتشغيل نظام DNS نفسه. على سبيل المثال، خوادم أسماء الجذر الخاصة بنظام DNS العالمي كانت دائمًا منغمرة بالاستعلامات التي لم يكن الغرض منها تناولها عن طريق نظام DNS (راجع SAC 045 في الملحق أ)، إلا أن خوادم اسم الجذر كانت تتوفر أيضًا بما يكفي لتتمكن من الرد على هذه الاستعلامات الزائدة. أما المشكلات ذات الصلة فيما يتعلق بخوادم أسماء الجذر فلم يتم تناولها في هذه الوثيقة. فهي تتناول فقط توابع الاستعلامات التي تتسرب بشكل غير متعمد إلى خوادم أسماء جذر DNS العالمية.

وقد وضعت ICANN صفحة ويب توفر مواد معلوماتية فيما يتعلق بتصادمات الأسماء المتوفرة على http://www.icann.org/en/help/name-collision. كما تحتوي الصفحة على عملية للإبلاغ بشكل واضح عن الضرر الفادح في أعقاب حالات تضارب الأسماء التي تحدث بسبب نطاق المستوى الأعلى العام الجديدة (gTLD).

1.1 حالات تضارب الأسماء

نظام DNS العالمي عبارة عن مساحة أسماء هرمية الشكل، كما أن الأسماء في نظام DNS تتألف من تسمية واحدة أو أكثر تمثل اسمًا كاملاً. وفي أعلى الرتيب الهرمي توجد منطقة جذر DNS والتي تحتوي على مجموعة من الأسماء مثل com، وru، وasia، وما إلى ذلك، وهذه هي نطاقاتTLD (نطاقات المستوى الأعلى)، والتي يشار إليها بشكل عام بلفظ "نطاقات TLD". وأحد الأمثلة على اسم نطاق كامل (والذي يطلق عليه في الغالب اسم النطاق المؤهل بالكامل أو FQDN) قد يكون www.ourcompany.com.

كما أن كافة مساحات الأسماء الخاصة تقريبًا تتميز بالترتيب الهرمي. وهناك ثلاثة أنواع رئيسية لمساحات الأسماء الخاصة:

- **مساحات الأسماء المشتقة من نظام DNS العالمي** أسماء النطاقات الخاصة المنبثقة عن نظام DNS العالمي متأصلة في اسم قابل للحل في نظام DNS العالمي، إلا أن هيكل الدليل تحت هذا الاسم يخضع للإدارة محليًا بأسماء لم ينو مديرو تقنية المعلومات أبدًا أن تُرى في نظام DNS العالمي. على سبيل المثال، نتناول مساحة اسم خاصة مندرجة في جذر winserve.ourcompany.com: الأسماء في مساحة الاسم الخاصة تلك (winserve) تدار من خلال خادم الاسم الخاص وهي مرئية في نظام DNS العالمي.

- **مساحات الاسم التي تستخدم الجذور الخاصة بها مع نطاقات TLD خاصة** جذر مساحة الاسم الخاصة عبارة عن تسمية فريدة وليست نطاقًا من نطاقات TLD العامة. وهيكل الدليل بالكامل، بالإضافة إلى هيئة TLD الخاص، يدار من خلال خوادم اسم خاصة لا تكون مرئية في نظام DNS العالمي. على سبيل المثال، إذا كانت مساحة الاسم الخاص متأصلة في ourcompany، تكون خوادم الاسم الخاصة مسئولة أيضًا عن www.ourcompany، و region1.ourcompany، و www.region1.ourcompany، وما إلى ذلك. وهناك العديد من الأنواع المختلفة من مساحات الأسماء التي تستخدم الجذور الخاصة بها مع نطاقات TLD الخاصة. وتشمل الأمثلة دليل مايكروسوفت النشط (في بعض التكوينات)، ونطاق DNS متعدد الإرسال (RFC 6762)، وخدمات دليل LAN القديمة التي لا تزال قيد الاستخدام في بعض جوانب الإنترنت.

- **مساحات الأسماء التي يتم إنشاؤها من خلال استخدام قوائم البحث** قائمة بحث عبارة عن ميزة في برنامج حل الأسماء المحلية (سواء لمساحة اسم خاصة أو برنامج حل متكرر لنظام DNS العالمي). قائمة بحث تسمح للمستخدم إدخال أسماء أقصر من أجل التسهيل، وأثناء عملية الحل يقوم خادم الاسم بإلحاق الأسماء المهيأة إلى يمين الاسم المقصود بالاستعلام. (ويطلق أيضًا على هذه الأسماء المهيأة لفظ اللواحق.)

ومساحات الأسماء التي تنبثق عن نظام DNS العالمي لا تسبب حدوث تضارب في الأسماء إلا عند دمجها بقوائم البحث. ولن يكون لأي استعلام يشتمل على اسم نطاق مؤهل بالكامل FQDN ويأتي من نظام DNS العالمي على الإطلاق حسب التعريف أي تضارب في الأسماء مع الأسماء المختلفة في نظام DNS العالمي. ويمكن لهذا الاستعلام أن يتسبب فقط في تضاربات الأسماء عند إنشاءه بإهمال من خلال استخدام قوائم البحث.

ويسبب مفهوم "مساحات الأسماء الخاصة" ارتباكاً للعديد من الأشخاص المعتادين بشكل كبير على الاستخدام النموذجي للإنترنت، أي الأشخاص الملمين فقط بأسماء DNS العالمية والذي قد يندهشوا من معرفة أن بعض الطلبات المقدمة لحل الأسماء لا تؤدي أو لا يجب أن تؤدي إلى استعلام في نظام DNS العالمي. وقد تصيبهم دهشة أكبر عند معرفة أن بعض الاستعلامات المقدمة للأسماء مقصودة عمدًا بحيث تبدأ في مساحة الأسماء الخاصة، ولكن ينتهي بها المطاف في نظام DNS العالمي. وأحد الأسباب وراء حدوث تضارب في الأسماء هو أن الاستعلامات الموجهة لخادم اسم في مساحة اسم خاصة يبدأ بشكل غير صحيح في نظام DNS العالمي بدلاً من ذلك.

1.2 حالات تضارب الأسماء بسبب نظام TLD الخاصة

تحدث حالات تضارب الأسماء نتيجة حدثين. الأول، وهو استعلام لاسم نطاق مؤهل بالكامل ومتأصل الجذر في نطاق TLD خاص يتسرب من شبكة خاصة إلى نظام DNS العالمي. الثاني، هو أن الاستعلام يضع في نظام DNS العام نفس الاسم تمامًا الموجود في الشبكة الخاصة تحت نطاق TLD الخاص.

وأحد الأسباب الشائعة وراء حدوث هذا التضارب في الأسماء هو أن استخدام أي اسم في نظام مثل الدليل النشط الخاص بشركة مايكروسوفت والذي لا يعد نطاق TLD في نظام DNS العام في الوقت الذي يجري فيه تهيئة النظام، ولكن يضاف فيما بعض إلى نظام DNS العام. وهذا النوع من تضارب الأسماء يحدث بالفعل عدة مرات قبل ذلك ومن المتوقع أن يستمر مع طرح نطاقات TLD الجديدة في نظام DNS العالمي (راجع مقدمة إلى برنامج gTLD الجديدة في الملحق أ).

1.3 حالات تضارب الأسماء بسبب قوائم البحث

هناك سبب آخر لحالات تضارب الأسماء وهو معالجة قوائم البحث. فإذا لم يكن الاستعلام اسم نطاق مؤهل بالكامل FQDN، فإنه يكون اسم قصير غير مؤهل. وتحتوي أي قائمة بحث على لاحقة واحدة أو أكثر. ويتم إلحاق هذه اللواحق بشكل متكرر على الجانب الأيمن من الاستعلامات. وعندما يتعذر على برنامج حل أن يحل اسم قصير غير مؤهل، يقوم بإلحاق لواحق من القائمة عند محاولته حل الاسم إلى أن يتم العثور على اسم مطابق. وقائمة البحث عبارة عن ميزة مفيدة، وعلى الرغم من ذلك، يناسب معالجة قوائم البحث استخدام الأسماء القصيرة غير المؤهلة التي لا تكون اسم نطاق مؤهل بالكامل FQDN ومن ثم يؤدي بدون قصد إلى إنشاء مساحات أسماء لا توجد الجذر الخاص بنظام DNS العالمي. وفي هذه الحالة، يحدث تضارب الأسماء متى ما اكتملت سلسلة يعتزم المستخدم استخدامها كاسم قصير غير مؤهل وذلك عن طريق قائمة البحث ويتم حله على أساس أنه اسم نطاق مؤهل بالكامل FQDN.

على سبيل المثال، هب أن برنامجًا لحل الأسماء يحتوي على قائمة بحث تتألف من اللاحقتين ourcompany.com و marketing.ourcompany.com. هب أيضًا أن مستخدمًا أدخل www في برنامج يستخدم هذا البرنامج الخاص بحل الأسماء. فقد يبحث برنامج الحل أولاً عن www، وإذا لم يحيل ذلك أي نتيجة فقد يبحث بعد ذلك عن www.ourcompany.com وعن www.marketing.ourcompany.com.

لاحظ استخدام كلمة "قد" في وصف هذا المثال. تتفاوت القواعد الخاصة بالكيفية التي سيتم تطبيق قوائم البحث بها عند القيام بحل الأسماء عبر مختلف نظم التشغيل أو التطبيقات. كما ستحاول بعض النظم حل أي اسم إما في مساحة الاسم الخاصة أو نظام DNS العالمي قبل تطبيق قائمة البحث. وعلى الرغم من ذلك، سوف تستخدم النظم الأخرى قائمة البحث أولاً إذا كانت السلسلة التي يجب البحث عنا لا تحتوي على حرف ".". ومع ذلك سوف تستخدم نظم أخرى قائمة البحث إذا كانت السلسلة بحرف ".". قامت بعض نظم التشغيل والتطبيقات (مثل برامج تصفح الويب) بتغيير قواعدها لقوائم البحث عدة مرات. ومن ثم من غير العملي التنبؤ بالوقت الذي سيتم فيه استخدام أو عدم استخدام قوائم البحث، وما هو الاسم القصير غير المؤهل أو غير ذلك، وأيضًا هل من المحتمل للأسماء القصيرة المؤهلة أن تتسرب إلى نظام DNS العالمي أم لا. راجع اهتمامات gTLD الجديدة: الأسماء الخالية من النقاط وتضارب الأسماء في الملحق أ للحصول على مزيد من التفاصيل حول تنوع التعامل مع قوائم البحث.

وقد يأتي هذا الوصف لقوائم البحث كمفاجأة بالنسبة لبعض الباحثين حيث إنه شائع جدًا في الأماكن التي لا تظهر من الوهلة الأولى أنها تنشئ "مساحات أسماء خاصة". وكل لاحقة في قائمة بحث تحدد مساحة اسم أخرى قد يتم الرجوع إليها أثناء عملية حل الأسماء. وهذا من شأنه إيجاد مساحة اسم خاصة لا تعمل بشكل موثوق إلا عند استعلام العميل عن برامج الحل لمساحة الاسم تلك. واعتمادًا على تنفيذ قائمة البحث، قد تجرب بعض برامج حل الأسماء الاسم القصير غير المؤهل الذي يقوم المستخدم بإدخاله أو تكوينه في البرنامج قبل إضافة أية أسماء في قائمة البحث. على سبيل المثال، قد يؤدي كتابة www.hr في موقع واحد على الإنترنت إلى تقديم نتيجة واحدة من برنامج حل DNS، إلا أن كتابته في موقع مختلف قد يؤدي إلى نتيجة مختلفة. وعند حدوث ذلك، فإن أحد مساحات الاسم تلك تكون "خاصة" بالتناسب مع للأخرى.

كما أن استخدام قوائم البحث بدلاً من حل أسماء النطاقات المؤهلة بالكامل FQDN عن طريق نظام DNS العالمي تساهم في عدم اليقين من حل الاسم. *من الصعب التنبؤ بحالات تضارب الأسماء التي تحدث بسبب قوائم البحث نظرًا لشيوع قوائم البحث للغاية. حيث إنها تعد جزءًا من برامج حل الأسماء في العديد من نظم التشغيل، وأجهزة الشبكات، والخوادم وأكثر من ذلك. وتعمل برمجيات الحل بشكل مختلف من نظام إلى آخر، وبين الإصدارات المختلفة لنفس نظام التشغيل، وحتى كوظيفة لنظرة نظام التشغيل أو التطبيق للمكان الذي يصدر منه الطلب على الشبكة. كما أن نشر خدمة حل الأسماء التي تقوم على حل الأسماء باستخدام نظام DNS العالمي هو أفضل تأكيد في مقابل هذا الشك والنتائج غير المتوقعة.

1.4 المساعدة في كشف تضارب الأسماء في gTLDs الجديدة

من 18 أغسطس 2014 فصاعدا، عندما تم تفويض نطاق gTLD من منطقة الجذر DNS، يتعين على نطاق gTLD إجراء خدمةالانقطاع الخاضع للرقابة لمدة 90 يوما. خلال فترة الانقطاع الخاضع للرقابة، يتم إرسال الإجابات التي يسهل التعرف عليها من خوادم الأسماء الرسمية لنطاقات gTLD الجديدة لمجموعة متنوعة من استفسارات DNS. والغرض من هذه الإجابات هو لتحذير المنظمات التي ستشهد تضارب الأسماء التي يحتاجونها لاتخاذ إجراءات فورية لمنع الضرر المحتمل بسبب الاستعلامات المسربة.

علاوة على ذلك، من نفس التاريخ، بعض نطاقات gTLD الموجودة بالفعل في منطقة الجذر مطلوبة لإجراء انقطاع الخدمة الخاضع للرقابة لمدة 90 يومًا قبل تفويض بعض أسماء المستوى الثاني في DNS العالمي. الغرض هنا هو نفسه على النحو الوارد أعلاه: لتحذير المنظمات التي تسرب الاستفسارات الخاصة التي يحتاجون إليها للتخفيف من الضرر المحتمل في أقرب وقت ممكن.

مع ملاحظة أن هذه القواعد لا تنطبق إلا على نطاقات gTLD، وليس نطاقات TLD التي هي لرموز الدولة (عادة ما تسمى "ccTLDs"). عند إضافة ccTLD إلى منطقة الجذر، يمكن لمشغلها أن يختار أن يكون له انقطاع خاضع للرقابة، ولكن لا يلتزم بذلك.

2. المشكلات التي تسببها حالات تضارب الأسماء

قد تكون لحوادث تضارب الأسماء المستندة إلى الاستعلامات المتسربة إلى نظام DNS العالمي من الشبكات الخاصة العديد من العواقب غير المقصودة. فعندما يحصل استعلام على رد إيجابي، لكنه رد يصدر من نظام DNS العالمي بدلاً من مساحة الاسم الخاصة المتوقعة، فسوف يحاول التطبيق الذي قدم الاستعلام الاتصال بنظام لا يكون جزءًا من الشبكة الخاصة، وقد ينجح في ذلك. وقد يمثل هذا الاتصال ضررًا (بالتسبب في حدوث تأخير أثناء حل الاسم). وقد يثبت أيضًا أنه مشكلة على الأمن، أي قد يؤدي إلى حدوث اختراق وضعف يمكن استغلاله لأغراض ضارة، وذلك استنادًا إلى ما يقوم به التطبيق بعد الاتصال.

2.1 التوجيه إلى مواقع الويب غير المتوقعة

هب أن مستخدمًا أدخل https://finance.ourcompany في متصفح الويب الخاص به أثناء الاتصال بشبكة خاصة، وأن هذه الشبكة لها مساحة اسم نطاق TLD الخاص بها هو ourcompany. وإذا قام استعلام المتصفح الخاص بالاسم finance.ourcompany بالحل كما هو متوقع، يحصل عنوان IP على خادم الويب الداخلي الخاص بالإدارة المالية. وتخيل رغم ذلك أن نطاق TLDourcompany هو جزء أيضًا من نظام DNS العالمي، وأن نطاق TLD هذا لديه اسم نطاق من المستوى الثاني (SLD) وهو finance. فإذا تسرب الاستعلام، فسوف يتم حله إلى عنوان IP مختلف عن ما قام به عند حل الاستعلام في مساحة الاسم الخاصة. والآن تخيل أن عنوان IP هذا المختلفة قد يستضيف خادم ويب. فسوف يحاول المتصفح الاتصال بخادم ويب على الإنترنت العامة، وليس على الشبكة الخاصة.

وكما أوضحنا في السابق، قد تحدث نفس المشكلة حتى في الشبكات التي ليس بها نطاقات TLD خاصة، ولكنها تستخدم قوائم البحث. هب أن برنامجًا للتصفح يستخدم في العادة على إحدى الشبكات التي يكون بها للمستخدم قوائم بحث وتحتوي على الاسم ourcompany.com، وقام المستخدم بإدخال الاسم www.finance من أجل الحصول على المضيف www.finance.ourcompany.com. والآن تخيل أن المتصفح يستخدمه الآن أحد الموظفين من جهاز محمول في أحد المقاهي. وإذا تسرب هذا الاستعلام إلى الإنترنت، وكان هناك نطاق TLD يسمى finance، فقد يتحول الاستعلام إلى عنوان IP مختلف، على سبيل المثال، مضيف مختلف بالكامل اسمه في نظام DNS هو www.finance. فسوف يؤدي هذا الاستعلام بالمتصفح إلى محاولة الاتصال بخادم ويب في جزء مختلف بالكامل من إنترنت عام بدلاً عن الجزء الخاص به إذا كان الاستعلام قد ذهب إلى برنامج الحل على الشبكة الخاصة.

والرد الشائع للمستخدمين على هذا السيناريو هو أن المستخدم سيدرك أن هذا كان موقع الويب الخطأ وسوف يغادر على الفور. وعلى الرغم من ذلك، قد يعرض المتصفح قدرًا كبيرًا من المعلومات على خادم ويب إذا "وثق" المتصفح في خادم الويب لأنه يحتوي على نفس اسم النطاق الذي قام المتصفح بزيارته في وقت سابق. وقد يقوم المتصفح تلقائيًا بإدخال بيانات تسجيل دخول أو بيانات أخرى حساسة، ومن ثم يعرض تلك المعلومات للاقتناص أو التحليل خارج المنظمة. وفي أحيان أخرى (على سبيل المثال؛ الهجوم المصاغ بعناية ضد المؤسسة)، قد يتصل المتصفح بموقع يستضيف شفرة ضارة تقوم بتنصيب برامج خطيرة على الكمبيوتر.

لاحظ أن استخدام TLS والشهادات الرقمية قد لا يساعد في الوقاية من الضرر الناجمة عن تضارب الأسماء، بل في حقيقة الأمر قد يزيد الأمر سوءًا بتقديم إحساس كاذب بالأمان للمستخدمين. كما أن العديد من جهات الاعتماد (CA) التي تقوم بإصدار شهادات للأسماء في نظام DNS العالمي تصدر أيضًا شهادات للأسماء القصيرة غير المؤهلة في مساحات الأسماء الخاصة، ومن ثم من المستحيل أن يظل مستخدم توجه بالخطأ إلى موقع مشاهدًا لشهادة صحيحة. راجع SAC 057 في الملحق أ للحصول على مزيد من التفاصيل حول الشهادات ذات الأسماء من مساحات الأسماء الخاصة.

2.2 التوجيه من البريد الإلكتروني إلى مرسل إليهم بالخطأ

لا تقتصر العواقب المحتملة التي تنشأ عن تضارب الأسماء على متصفحات الويب. يمكن إرسال البريد الإلكتروني المخصص لمستلم واحد إلى مستلم مختلف إذا كانت أسماء المضيف في عناوين المستلم متشابهة، على سبيل المثال، البريد الإلكتروني المرسل إلى chris@support.ourcompany قد يصل إلى حساب مستخدم مختلف تمامًا إذا أصبحت ourcompany نطاق TLD في نظام DNS العالمي. وحتى إن لم يتم تسليم الرسالة إلى مستخدم بريد إلكتروني محدد، قد تكون هناك محاولة لإرساله، وقد تعرض هذه المحالة محتويات البريد الإلكتروني للاقتناص أو التحليل خارج المنظمة.

ويمكن تكوين وتهيئة العديد من أجهزة الشبكات مثل جدران الحماية، وأجهزة التوجيه، وحتى الطابعات بحيث ترسل إشعارات أو بيانات سجل عن طريق البريد الإلكتروني. إذا كان اسم المستلم الذي تم إدخاله لإشعارات البريد الإلكتروني فيما بعد عرضة لتضارب الأسماء في نظام DNS العالمي، فقد يتم إرسال الإشعارات إلى مستلم غير مقصود تمامًا. كما أن بيانات الإجراءات أو بيانات السجل في نص الرسالة قد تكشف عن تكوين الشبكة وسلوك المضيف قد يتسرب إلى مستلم غير مقصود. وقد تتم مقاطعة أداء الشبكة الروتيني أو تحليل مرور البيانات عن طريق فريق عمل تقنية المعلومات إذا لم يتسلم مستلم هذه البيانات المقصود مطلقًا لبيانات السجل، أو أن الأحداث التي أدت إلى حدوث الإشعارات قد لا يتم التحري عنها أو الحد منها.

2.3 عمليات خفض الأمان

حالات تضارب الأسماء التي تترك دون حل قد تعرض النظم في الشبكات الخاصة لسلوك غير مقصود أو ضرر. والنظم التي تعتمد على حل الأسماء من أجل التشغيل الصحيح والتي تؤدي أيضًا وظائف أمان قد تعمل بشكل معتمد عند استخدام أسماء النطاقات المؤهلة بالكامل FQDN وحلها من نظام DNS العالمي.

على سبيل المثال، في جدران الحماية، تستند قواعد الأمان في الغالب إلى مصدر أو وجهة تدفق الحزم. ومصدر ووجهة الحزم هي عناوين IPv4 أو IPv6، إلا أن العديد من جدران الحماية تسمح بإدخالها كأسماء نطاقات أيضًا. وفي حالة استخدام الأسماء القصيرة غير المؤهلة وعدم إجراء حل للأسماء كما هو متوقع، فقد تعجز القواعد عن حجب أو السماح بمرور البيانات وفقًا لما يريد مدير الشبكة. وبالمثل، تستخدم سجلات جدران الحماية في الغالب أسماء النطاقات، واستخدام الأسماء القصيرة غير المؤهلة التي تحل بطرق غير متوقعة قد تتداخل مع مراقبة الحدث، أو التحليل أو الرد. وعلى سبيل المثال؛ قد يسيء فريق تنقية المعلومات الذي يقوم على مراجعة السجلات فهم تنوع حدث ما بسبب أن اسم قصير غير مؤهل في السجل قد يعرف مضيفين مختلفين استنادًا إلى المكان الذي تم إنشاء السجل فيه (أي أنه في السجل قد يبدو الاسم القصير المؤهل مرتبطًا بعنوانين IP أو أكثر مختلفين). وقد تتضاعف هذه المشكلة بسبب حقيقة أن غالبية جدران الحماية يمكنها العمل كبرامج حل DNS الخاصة بها أو السماح للمديرين باستخدام أو تكوين قوائم البحث.

2.4 النظم المتضررة من تضارب الأسماء

يجب التحقق من كافة النظم المتصلة بالشبكات لاستخدام الأسماء المضيفة والمقيدة في جذر نطاق TLD خاص أو أسماء مضيف مستندة إلى قوائم بحث. وسيتعين تحميل كل هذه الأمثلة على "الاستخدام" من أجل استخدام اسم نطاق مؤهل بالكامل FQDN من نظام DNS العالمي. تشمل قائمة غير شاملة بالنظم أو التطبيقات من أجل الفحص ما يلي:

- **برامج التصفح** تتيح برامج تصفح الويب للمستخدمين إمكاني تحديد موقع بروكسي HTTP، وغالبًا ما يكون هذا البروكسي على الشبكة الخاصة. تحقق مما إذا كان أحد المستخدمين أو فريق تقنية المعلومات قد حرر صفحات رئيسية مخصصة، أو إشارات مرجعية أو محركات بحث: فقد يكون لها روابط بخوادم على الشبكة الخاصة. كما تحتوي بعض برامج التصفح على خيارات تكوين للمكان الذي تحصل منه على معلومات الإلغاء على شهادات SSL/TLS التي قد تشير إلى أسماء مضيفة على الشبكة الخاصة.

- **خوادم الويب** تعرض خوادم الويب محتوي HTML يحتوي على روابط وبيانات كبيرة ذات أسماء مضيفة مضمنة. تحقق مما إذا كانت خوادم الويب على شبكة خاصة بها محتوي يضم أسماء قصيرة غير مؤهلة. تحقق مما إذا كانت ملفات التكوين لخادم الويب بها أسماء قصيرة غير مؤهلة أو خوادم أخرى على الشبكة الخاصة.

- **وكلاء مستخدم البريد الإلكتروني** وكلاء البريد الإلكتروني مثل Outlook وThunderbird تحتوي جميعها على خيارات تكوين لمكان استلام البريد الإلكتروني باستخدام بروتوكول POP أو IMAP، ومكان إرسال البريد الإلكتروني عن طريق بروتوكول SUBMIT؛ وقد يستخدم جميع هؤلاء الوكلاء أسماء مضيف على الشبكة الخاصة. تأكد مما إذا كانت هذه التطبيقات مهيأة للحصول على معلومات الرفض على شهادات SSL/TLS من المضيفين المحددة لهم أسماء قصيرة غير مؤهلة.

- **خوادم البريد الإلكتروني** تحقق مما إذا كانت خوادم البريد الإلكتروني بها تكوينات تسرد الأسماء القصيرة غير المؤهلة للمضيفين المحليين الآخرين، مثل بوابات البريد الإلكتروني الاحتياطية، وخوادم التخزين غير المتصلة، وما إلى ذلك.

- **الشهادات** تأكد مما إذا كانت التطبيقات التي تستخدم شهادات X.509، مثل الاتصال الهاتفي وبرامج المراسلة الفورية بها بيانات تهيئة تستخدم أسماء قصيرة غير مؤهلة من أجل تحديد مكان الحصول على معلومات الرفض على شهادات SSL/TLS أم لا.

- **البرامج الأخرى** قد تكون في التطبيقات المخصصة العديد من معلمات التهيئة التي يمكن تخرين أسماء المضيف فيها. وسوف تكون المساحة الأكثر وضوحًا هي ملفات التهيئة، إلا أن غالبية الأسماء قد تظهر في أنواع متعددة من بيانات التطبيقات، والروابط على الوسائط الاجتماعية أو مواقع ويكي، أو حتى الترميز الثابت في شفرة المصدر. تحقق من بيانات التهيئة تلك للتأكد من وجود أسماء قصيرة غير مؤهلة.

- **أجهزة الشبكة** تحقق من أجهزة البنية التحتية للشبكة أي جدران الحماية، ومعلومات الأمان ونظم إدارة الأحداث (SIEM)، وأجهزة التوجيه، والمحولات، وأجهزة مراقبة الشبكة، ونظم اكتشاف والحماية من التطفل، وخوادم VPN، وخوادم DNS، وخوادم DHCP، وخوادم السجل وذلك من أجل تحديد ما إذا كانت مهيأة باستخدام أسماء قصيرة غير مؤهلة لأجهزة أخرى على الشبكة الخاصة أم لا.

- **إدارة الوكيل** تأكد مما إذا كانت أدوات إدارة الوكيل المركزية مثل التي تقوم بتكوين محطات عمل المؤسسات وأجهزة الشبكة بها أسماء قصيرة غير مؤهلة أم لا في التكوينات (لاسيما قوائم البحث) التي تخضع للنظم من حيث التحكم وإعادة الضبط.

- **الأجهزة المحمولة** قد تحتوي أجهزة العملاء مثل الهواتف وأجهزة الكمبيوتر اللوحية على خيارات تكوين مشابهة مثل بعض التطبيقات المشار إليها أعلاه، ومن قد يكون بها خيارات تكوين ربما تحتوي على أسماء قصيرة غير مؤهلة من الشبكة المحلية.

ويجب التحقق من كافة هذه النظم للتعرف على بيانات التكوين التي تقوم بتخزين الأسماء القصيرة غير المؤهلة من أجل ضمان إمكانية تغيير هذه الأسماء عند تغير الجذر الخاصة بمساحة الاسم الخاصة أو عندما يتم الاستغناء عن استخدام قوائم البحث.

3. الوقت المناسب للحد من تضارب الأسماء

تتم إضافة الأسماء في بعض الأحيان إلى منطقة جذر DNS العالمية، على سبيل المثال عندما يتغير اسم بلد، أو عندما تقوم ICANN بتفويض نطاق TLD جديد. وتمت إضافة كلا نوعي نطاقات المستوى الأعلى كل عام تقريبًا على مدار ما يقرب من عقدين من الزمان. وتمت إضافة نطاقات TLD جديدة في عام 2013 و2014 ومن المؤكد أن يتم إضافة المزيد في الأعوام القادمة.

ويوضح التاريخ أن بعض حالات تضارب الأسماء قد حدثت عند إضافة نطاقات TLD إلى نظام DNS. كما يوضح التاريخ أن الأسماء من مساحات الأسماء الخاصة قد تسربت على مدار عدة أعوام، وفي بعض الحالات بتكرار عالي للغاية، راجعSAC 045 في الملحق أ للحصول على مزيد من التفاصيل. كما يوضح التاريخ أن مساحات الأسماء وحل الأسماء المخصص للشبكات الخاصة لم يتم فصلها أبدًا بنفس درجة الدقة التي يعتقدها مديرو الشبكات، وأن استعلامات الأسماء التي يعتزم مديرو الشبكات أن تحل من خلال خوادم الاسم الداخلية ترسل في بعض الأحيان عوضًا عن ذلك إلى برامج الحل في نظام DNS العالمي.

وفي بعض الأحيان يتخذ مديرو الشبكات خيارات للأسماء استنادًا إلى افتراضات بأن قائمة الأسماء في الجذر الخاص بنظام DNS العالمي ثابتة، إلا أن هذه القائمة في حقيقة الأمر قد تغيرت وسوف تتغير على مدار الوقت. على سبيل المثال، عندما تمت إضافة نطاق TLD باسم cs منذ ما يقرب من 25 سنة مضت لدولة تشيكوسلوفاكيا، كانت العديد من الجامعات تستخدم قوائم بحث أتاحت للمستخدمين إدخال اسم ينتهي بالحروف cs لقسم علوم الكمبيوتر المؤهلة بالكامل لاسم النطاق الخاص بالجامعة، وأدت هذه القرارات إلى عدم اليقين من حل الاسم عند إضافة نطاق TLD جديد إلى منطقة الجذر حيث إن الأسماء التي تنتهي بالحروف cs أصبحت الآن أسماء نطاقات مؤهلة بالكامل FQDN في نظام DNS العالمي. حتى عندما لا تتداخل في الغالب الأسماء الحالية لجذر DNS العالمي مع الأسماء الموجودة في مساحة اسم خاصة (سواء كان نطاق TLD خاص أو قائمة بحث)، ينسى مديرو الشبكات في الغالب الاطلاع على آخر مستجدات الأسماء في جذر DNS العالمي.

ويوصى أن يبدأ قسم تقنية المعلومات في جهود التخفيف بأسرع ما يمكن من الناحية العملية. كما أن اتخاذ موقف "تحسين عمليات جدران الحماية بشكل أفضل لدينا" قد يقلل من بعض حالات التصادم، لكنه لن يتخلص منها تمامًا. وبالمثل، فإن القول "بأننا سوف نجعل مستخدمينا متأكدين من استخدام خوادم الاسم الخاصة بنا" أو "سوف نجعل العمال عن بعد باستخدام شبكات VPN" من المحتمل أن يقلل من بعض حالات التضارب، لكن ذلك قد يجعل من الصعب تشخيص حالات التضارب الباقية.

فقد تحدث حالات التضارب بصرف النظر عن الأحرف المستخدمة في الاسم: وعلى الرغم من ذلك، فإن استخدام أحرف غير ASCII مثل ä و 中 و ﻯ في نطاقات TLD يضفي تعقيدًا على تحليل حالات التضارب. وقد ترسل برامج الحل استعلامات لهذه التضاربات بطرق يصعب التنبؤ بها، وقد لا تتوافق مع معايير الإنترنت، لذلك فإن تحديد الوقت الذي تحدث فيها حالات تضارب الأسماء يصبح صعبًا للغاية.

وعلى الرغم من أن جذر DNS العالمي سوف ينتهي به المطاف لأن يكون أكبر مما كانت عليه في الأعوام الأخيرة، فإن إضافة الأسماء إلى الجذر ليس أمرًا غير اعتيادي على الإطلاق. وبالنسبة لكل نطاق TLD جديد تتم إضافته، هناك فرصة بأن تحدث حالات تضارب في الأسماء مع مساحات الأسماء الخاصة التي تتسرب إلى الإنترنت بدون ملاحظة ذلك في الغالب. وقد دأبت المؤسسات على استخدام الأسماء وتحمل خطر التضارب في الأسماء على مدار أعوام.

لاحظ أيضًا أن إضافة أسماء جديدة إلى جذر DNS لم ولن يكون أبدًا مشكلة بالنسبة للمؤسسات التي تستخدم بالفعل أسماء النطاقات المؤهلة بالكامل FQDN من نظام DNS العالمي في الشبكة الخاصة بها. ولن ترى هذه المؤسسات أي فارق بالنسبة لاستخدامها لأسماء DNS، حيث لا توجد أية تضاربات في الأسماء. وتظهر المشكلات فقط بالنسبة للمؤسسات التي تستخدم نطاقات TLD الخاصة، أو المؤسسات التي تستخدم قوائم بحث تسمح بإدخال أسماء قصيرة غير مؤهلة بحيث إن الاسم المختصر نفسه قد يكون اسمًا صالحًا في نظام DNS العالمي.

3.1 تحديد احتماليات التضارب

لكي تتمكن من تحديد ما إذا كان هناك تضارب في الأسماء في مساحة الاسم الخاصة لشركتك أم لا، يتعين عليك تحديد وتصنيف كافة مساحات الأسماء الخاصة وقوائم بحث DNS التي تستخدمها مؤسستك، ثم بعد ذلك وضع قائمة بأسماء المستوى الأعلى في هذه المصادر. وبالنسبة لغالبية المؤسسات، هناك في الغالب مساحة اسم واحدة تحتوي على اسم واحد فقط من المستوى الأعلى، إلا أن بعض المؤسسات، لاسيما تلك المتوحدة مع مؤسسات أخرى والتي كانت تستخدم أيضًا مساحات أسماء خاصة (على سبيل المثال، نتيجة اندماج الشركات أو الاستحواذ عليها)، وتحتوي على العديد من الأسماء الخاصة من المستوى الأعلى.

بعد ذلك، يتعين عليك تحديد كل من المحتويات الحالية والمتوقعة لمنطقة DNS العالمية. ويمكن العثور على الأسماء في منطقة الجذر الحالية بالنسبة لنظام DNS العالمي على http://data.iana.org/TLD/tlds-alpha-by-domain.txt. ولتحديد ما إذا كان اسم من مساحة اسم خاصة يجري النظر فيه للتخصيص عبر برنامج gTLD الجديدة الحالي:

1. انتقل إلى https://gtldresult.icann.org/application-result/applicationstatus
2. انقر فوق العمود "String" (سلسلة)
3. قم بالتمرير عبر الصفحات إلى أن تجد النطاق الذي يحتوي على اسم مساحة الاسم الخاصة

وإذا كان هناك أي تداخل بين قائمة نطاقات TLD الخاصة التي قمت بإعدادها للتو وقائمة الأسماء في منطقة DNS، فثمة احتمال بأن هناك تضارب في الأسماء، ومن ثم يجب القيام بحله والحد منه الآن.

لاحظ أنه بعد دخول الجولة الحالية من نطاقات TLD الجديدة في منطقة الجذر، قد يتم اقتراح المزيد؛ وعلى وجه الخصوص، قد تتغير قائمة نطاقات TLD الجديدة وقد تحدث حالات تضارب الأسماء بين مساحات الأسماء الخاصة ونطاقات TLD الجديدة المستقبلية. بالإضافة إلى ذلك، فإن المؤسسات ذات نطاقات TLD الخاصة التي تتألف من حرفين (مثل ab) يجب أن تكون على وعي بأن أسماء نطاقات المستوى الأعلى ذات الحرفين محجوزة للاستخدام كشفرات للبلدان، وأن هذه الأسماء تضاف إلى منطقة الجذر من خلال إجراءات مختلفة كليًا.

3.2 نطاقات gTLD التابعة لـDNSالعالمية المؤجل تفويضها إلى أجل غير مسمى

ذكرت ICANN أنها ستؤجل إلى ما لا نهاية تفويض ثلاثة نطاقات TLD: corp. و home. و mail. لا تزال نطاقات gTLD تستعمل بشكل عام في مساحات الأسماء الخاصة، وبالتالي تشكل خطرًا للتضارب أعلى بكثير من غيرها من نطاقات TLD. والإحالة ليست مضمونة إلى الأبد، لذلك ينبغي علي أي منظمة تستخدم أحد تلك الأسماء باعتبارها مساحة اسم خاصة لا تزال تتبع الإرشادات الموجودة في القسم 4 أو القسم 5 للانتقال من مساحة الاسم الخاص. ومع ذلك، فهذه المنظمات لديها المزيد من الوقت لتنفيذ الانتقال من المنظمة التي استخدمت اسمًا مختلفًا قد يظهر في جذر DNS العالمي في المستقبل المنظور.

4. خطوات لتخفيف المشكلات المرتبطة بنطاق TLD خاص

ولم تتم التوصية باستخدام نطاقات TLD الخاصة باعتبارها ممارسة أفضل على مدار عقود. وفي حقيقة الأمر، فإن التعليمات التي تأتي مع منتجات الدليل النشط والخادم من مايكروسوفت قد أوصت بوضوح بعدم استخدام نطاقات TLD الخاصة على مدار عدة سنوات. والتخفيف الأكثر فاعلية لحالات تضارب الأسماء بسبب الأسماء التي تنتهي بنطاق TLD خاص يتسرب إلى نظام DNS العالمي يتمثل في التغيير من استخدام نطاق TLD خاص إلى نطاق له جذر في نظام DNS العالمي.

تنطبق الخطوات الواردة في هذا القسم على أي شبكة لها أسبابها الخاصة المحددة لاستخدام نطاق TLD خاص كجذر لها واستخدام قوائم البحث من أجل حل الأسماء القصيرة غير المؤهلة بدلاً من وضع مساحة الاسم الخاصة بها في الجذر في نظام DNS العالمي والاستعلام عن نظام DNS العالمي من أجل حل أسماء النطاقات المؤهلة بالكامل FQDN. وينطبق هذا القسم على أية مؤسسة تستخدم نطاق TLD خاص، وليس فقط المؤسسات التي تسرب بالفعل استعلامات أسماء في الإنترنت العالمي. إذا كانت المؤسسة الخاصة بك تستخدم ما ترى أنه نطاق TLD خاص "آمن"، أي اسم لم يتم تقديم طلب للحصول عليه حتى الآن أو اعتماده من أجل التفويض في جذر DNS العالمي، فيتوجب عليك النظر جديًا في إجراء تغيير على اسم متأصل في نظام DNS العالمي. وإذا كنت تعمل في مؤسسة كبرى بها أكثر من نطاق TLD خاص واحد (مثل الشركات التي اندمجت مع شركة أخرى ولم تقم بدمج مساحتي اسميها)، فيجب إجراء الخطوات الواردة في هذا القسم لكل نطاق TLD خاص.

وتتمثل الفرص في أنه عندما تختار المؤسسة استخدام نطاق TLD خاص، فإنها تقوم بذلك مع الأخذ في الاعتبار طريقة محددة للسمية. وقد تتعارض الخطوات الواردة هنا مع ذلك النموذج الأصلي. ومن أجل الحد بموثوقية من المشكلات المرتبطة بحالات تضارب الأسماء بسبب نطاقات TLD الخاصة، يتعين على كل من المستخدمين والنظم تغيير الطريقة التي يستخدمون بها أسماء النطاقات، ويتعين إعادة تكوين خوادم الاسم المحلية بطريقة قد يجدها بعض المستخدمين غير ملائمة. استخدم التفسيرات الخاصة بالعواقب غير المقصودة أو غير المرغوبة والتي قد تؤثر على مؤسستك من أجل رفع مستوى الوعي ودعم القبول بين مجتمع المستخدمين الخاص بك.

ملاحظة هامة: في نفس الوقت الذي تقوم فيه بإجراء الخطوات الواردة في هذا القسم، قد يتوجب عليك أيضًا الحد من حالات تضارب الأسماء التي تحدث بسبب قوائم البحث، والتي تمت تغطيتها في القسم 5. والعديد من الخطوات الموجودة في ذلك القسم هي نفس هذه الخطوات، ويمكن القيام بهام في نفس الوقت.

4.1. راقب الطلبات الواردة إلى خوادم الاسم المعتمدة

لكي يتم الحد من المشكلات التي تحدث في أي نطاق TLD خاص، أورد جميع أجهزة الكمبيوتر، وأجهزة الشبكة، وأي نظام آخر يستخدم نطاق TLD الخاص الحالي في أية طلبات. وعند تغيير الأسماء التي يجب استخدامها، يجب تحديث كافة الأجهزة التي تستخدم الأسماء الخاصة القديمة بطريقة تلقائية.

وفيما يلي ثلاث طرق شائعة لأداء هذه المراقبة وترقيم الأنظمة:

- خادم الاسم الرسمي (مثل الدليل النشط) قد تكون لها ميزة تسجيل. قم بتشغيل ميزة التسجيل من أجل جمع البيانات الخاصة بكافة الاستعلامات للأسماء الخاصة.

- كما يمكن أيضًا تكوين العديد من جدران الحماية الحديثة للتعرف على الاستعلامات عن الأسماء الخاصة وتسجيلها. وقد لا يكون ذلك بنفس فاعلية التسجيل من نظام التسمية نفسه، وذلك استنادًا إلى تقسيم شبكتك. على سبيل المثال، إذا لم يجتاز أي استعلام جدار حماية، فلا يمكن لجدار الحماية التعرف على الاستعلام، وسوف يتم تفويته على هذا النحو.

- وإذا تعذر استخدام أي مما سبق، فراقب واجمع مرور البيانات المقدمة إلى والمرسلة من خادم الاسم الرسمي باستخدام برنامج لالتقاط الحزم مثل برنامج Wireshark. وعلى الرغم من ذلك، تتطلب هذه الطريقة أن تتم معالجة البيانات المجمعة باستخدام برنامج وذلك من أجل العثور على الاستعلامات للأسماء الخاصة فقط.

وبعض المؤسسات سوف تختار (ويجب أن تختار) القيام بأكثر من خطوة من الخطوات السابقة من أجل زيادة فرص العثور على كافة الطلبات. لاحظ أن هذه الخطوة يمكن أن تؤدي إلى نتائج مربكة. وتحتوي أجهزة مثل أجهزة الكمبيوتر والهواتف على تطبيقات يقوم المستخدمون بكتابة أسماء فيها؛ وسوف تظهر هذه الأجهزة في الاستطلاع حتى وإن لم تكن هناك أية إصدارات مخزنة للأسماء الخاصة القديمة. وبالنسبة لهذه الخطوة، من الضروري فقط معرفة كافة الأماكن في الشبكة الخاصة بك حيث يجري تخزين الاسم الخاص القديم واستخدامها للتطبيقات.

4.2. قم بإنشاء قائمة لكل نظام يستخدم نطاق TLD الخاص بطريقة تلقائية

أنت بحاجة إلى ملخص بيانات السجل التي تم الحصول عليها من الخطوة السابقة. ويجب أن يكون هذا الملخص عبارة عن قائمة تضم كافة الأجهزة وكافة الأسماء التي يجري الاستعلام عنها وليس كل مثال على جهاز يجري استعلامًا. والسبب وراء حاجتك إلى كافة الأسماء التي يجري الاستعلام عنها هو أن بعض الأجهزة سوف يكون بها العديد من التطبيقات التي يتعين ضبط كل منها. وبذلك، يجب أن يحتوي الملخص على كافة الأنظمة وكافة التطبيقات على كل نظام تستخدم نطاق TLD الخاص. ويصبح هذا الملخص هو بيان الجرد للأجهزة التي يتعين تغييرها.

4.3. حدد المكان الذي تدار منه أسماء DNS العالمية الخاصة بك

من المحتمل أن يكون لديك بالفعل اسم نطاق DNS عالمي لمؤسستك وأنه يمكن استخدام اسم النطاق لجذر مساحة الاسم الخاصة لديك. ويتعين عليك تحديد من هو المسئول عن أسماء DNS الخاصة بك وما هي العمليات التي يستخدمها في إنشاء وتحديث الأسماء في نظام DNS. ويمكن القيام بذلك داخل إدارة تقنية المعلومات التابعة لك، أو يمكن القيام بها من خلال موفر خدمة (غالبًا ما تكون نفس الشركة التي تحصل منها على اتصال الإنترنت).

4.4. قم بتغيير جذر مساحة الاسم الخاصة لاستخدام اسم من نظام DNS العالمي

من الإستراتيجيات الشائعة في استخدام اسم DNS عالمي كجذر لمساحة الاسم الخاصة لديك هو الحصول على اسم قابل للوصول بشكل عام يتم تفويضه من نظام DNS العالمي لكن بعد ذلك استخدام خادم الاسم الرسمي الحالي لإدارة كافة الأسماء المندرجة تحت ذلك. على سبيل المثال، إذا كان لشركتك اسم النطاق العالمي ourcompany.com، فقد تختار ad1.ourcompany.com اسمًا للجذر.

وإذا كان لمؤسستك أكثر من اسم نطاق واحد في نظام DNS العالمي، فيتوجب عليك وضع الأسماء في الجذر تحت اسم يمكن التحكم فيه بسهولة كبيرة عن طريق فريق تقنية المعلومات في مؤسستك. وفي بعض الحالات، يتم التحكم في الأسماء الإضافية عن طريق كيانات أخرى، مثل إحدى إدارات التسويق. وإذا أمكن، من الأفضل وضع اسمك في الجذر تحت اسم تكون لمؤسسة تقنية المعلومات رقابة عليه بالفعل.

أما الخطوات الخاصة بإجراء هذا التغيير فتتوقف على طبيعة برنامج خادم الاسم الخاص الذي لديك، والإصدار الخاص بهذا البرنامج، والتقسيم الهرمي لخوادم الجذر على شبكتك الخاصة، والتكوين الحالي لخادم الاسم. وهذه التفاصيل خارجة عن نطاق هذه الوثيقة، ولكن يجب تغطيتها في التعليمات الواردة من موفر نظامك الحالي. بالإضافة إلى ذلك، يتطلب هذا التغيير في العديد من المؤسسات اعتمادًا من بعض المستويات الإدارية، لاسيما إذا كانت إدارة أسماء DNS العالمية مختلفة عن إدارة مساحة الاسم الخاصة.

وكجزء من هذه الخطوة، إذا كانت لديك شهادات لأي من المضيفين الذي يستخدمون الأسماء في مساحة الاسم الخاصة، يتعين عليك إنشاء شهادات لهؤلاء المضيفين باستخدام الأسماء الجديدة (المؤهلة بالكامل). وتعتمد الخطوات الخاصة بالحصول على هذه الشهادات على جهة الاعتماد CA الخاصة بك وهي أيضًا خارج نطاق هذه الوثيقة.

4.5. قم بتخصيص عناوين IP جديدة للمضيفين، إذا لزم ذلك

إذا كانت لديك شهادات TLS قائمة في اسم TLD الخاص والقديم لديك، سيتعين عليك الحصول على شهادات جديدة للأسماء الجديدة. إذا كان خادم الويب الخاص بك لا يدعم امتداد إظهار اسم الخادم (SNI) إلى TLS والذي يسمح بخدمة أكثر من اسم نطاق واحد بموجب TLS على نفس عنوان IP، فيتعين عليك إضافة عناوين IP إلى المضيفين بحيث يدعم المضيف الاسم الخاص القديم على عنوان IP الأصلي والاسم الجديد على عنوان IP الجديد. وعوضًا عن ذلك، يمكنك تحديث برنامج خادم الويب الخاص بك إلى إصدار يتناول امتدادات SNI بشكل صحيح.

4.6. قم بإنشاء نظام لمراقبة التكافؤ بين الأسماء الخاصة الجديد والقديمة

عندما تقوم بتغيير كافة الأسماء الخاصة لاستخدام جذر جديد، فسوف تواصل خدمة العناوين من أجل تسجيل الاستعلامات للأسماء الخاصة القديمة التابعة لك من أجل التعرف على الأنظمة غير الموجودة في قائمتك ولم يتم تحديثها لاستخدام الأسماء المدرجة في جذر DNS. وبسبب ذلك، يتعين عليك التأكد من أن الأسماء الخاصة الجديدة والقديمة لها نفس القيم لعناوين IP.

وبعض برامج مساحات الأسماء الخاصة تتيح لك الحفاظ على محورين متوازيين، لكن إذا كان لديك برنامج أقدم أو العديد من خوادم الاسم الرسمية، فقد يتوجب عليك مراقبة التكافؤ باستخدام أدوات مخصصة. ويتعين على هذه الأدوات المخصصة الاستعلام عن كافة الأسماء في كل من مساحة الاسم القديمة والاسم بشكل متكرر، وإشعارك في حالات عدم التطابق بحيث يمكنك تحديد النظام الذي تغير دون إجراء تغيير موازي في النظام الآخر.

وإذا احتجت إلى إضافة عناوين IP في الخطوة السابقة بسبب الحصول على شهادات SSL/TLS، فيجب إتاحة عدم التطابق عن طريق برنامج مراقبة التكافؤ.

4.7. درّب المستخدمين ومديري الأنظمة على استخدام الاسم الجديد

بالإضافة إلى تغيير النظم التي يتم إدخال الأسماء فيها في التكوينات، يتعين عليك تغيير الطرق التي يفكر بها المستخدمون لحملهم على التغيير من الأسماء الخاصة القديمة إلى الأسماء الخاصة الجديدة. ويجب إجراء هذا التغيير قبل تنفيذ الخطوات التالية بحيث تكون أمام المستخدمين الفرصة للاعتياد على الأسماء الجديدة، لكن يجب أن يوضح التدريب أن التغيير وارد وأنه يتعين عليهم البدء في التفكير من حيث الأسماء الجيدة في القريب العاجل. كما أن هذا توقيت مناسب لتدريب المستخدمين حول استخدام أسماء النطاقات المؤهلة بالكامل FQDN. استخدم التفسيرات الخاصة بالعواقب غير المقصودة أو غير المرغوبة والتي قد تؤثر على مؤسستك من أجل رفع مستوى الوعي ودعم القبول.

4.8. قم بتغيير كل نظام متضرر إلى الأسماء الجديدة

هذه هي النقطة التي يصبح فيها التحول من الأسماء الخاصة القديمة إلى الأسماء الجديدة واقعًا لكافة الأنظمة (أجهزة الكمبيوتر الشخصي، وأجهزة الشبكة، والطابعات، وما إلى ذلك) على الشبكة. وتُستبدل الأسماء الخاصة بأسماء DNS الجديدة على أساس كل نظام على حدة. وكل مثال على الاسم الخاص القديم موجود في كافة البرامج المستخدمة في النظام ويتم استبداله باسم DNS الجديد. وفي نفس الوقت، يتعين عليك الحد من استخدام الأسماء القصيرة غير المؤهلة في قوائم البحث.

كما أن المراقبة التي تم البدء فيها أعلاه ذات أهمية استثنائية في هذه الخطوة. ومن غير المتحمل أن تكون لك القدرة على تحديد كافة التطبيقات في كافة الأنظمة التي تحتوي على أسماء خاصة قديمة مضمنة فيها. وعوضًا عن ذلك، يجب الرجوع إلى نظام المراقبة بعد إجراء التغييرات على كل نظام للتعرف على ما إذا كان النظام لا يزال يصدر طلبات للأسماء الخاصة القديمة أم لا.

وتستخدم العديد من النظم بعض تطبيقات الاستهلال عند تشغيلها للمرة الأولى. وقد يكون لهذه التطبيقات أسماء نظام مضمنة فيها، كما أن العثور على كل هذا قد يكون صعبًا. وبعد تغيير كافة الأسماء في أي نظام من الأسماء الخاصة القديمة إلى أسماء DNS الجديد، أعد تشغيل النظام واستخدم برنامج المراقبة لمراقبة عمليات البحث عن الأسماء. فإذا كان النظام يبحث عن أي من الأسماء الخاصة القديمة، يتعين عليك تحديد البرنامج المتسبب في ذلك الطلب وتغييره لاستخدام الأسماء الجديدة. وقد تستغرق هذه العملية عدم مرات من إعادة تشغيل النظام من أجل إجراء تكوين كامل للنظام بشكل صحيح.

4.9. ابدأ المراقبة لاستخدام الأسماء الخاصة القديمة في خادم الاسم

يتعين عليك تكوين خادم الاسم الرسمي لديك بحيث يبدأ مراقبة كافة الطلبات للحصول على أسماء ذات جذر قديم. وحيث يتوجب على المستخدمين لديك عدم استخدام هذه الأسماء بعد ذلك، فإن السجل الناتج عن خطوة المراقبة هذه قد لا يكون كبيرًا للغاية، وإذا كان كذلك، فسيتعين عليك تكرار بعض الخطوات أعلاه لبعض الأنظمة العاملة على شبكتك.

4.10. قم بإعداد مراقبة طويلة الأجل بحدود خارجية لمراقبة الأسماء الخاصة القديمة

يجب أن تكون الخطوات السابقة قد عثرت على أغلبية كبيرة من الاستخدامات للأسماء الخاصة القديمة، ولكن بضعة أنظمة (ربما أساسية) قد لا تزال مستخدمة للأسماء الخاصة القديمة، لكن ربما يكون ذلك في النادر فقط. وأحد الطرق للتعرف على هذه الاستعلامات الخاصة بالاسم هو إضافة قواعد إلى كافة جدران الحماية عند حافة الشبكة الخاصة بك من أجل البحث عن أية طلبات تكون متسربة. ويجب أن تكون لهذه القواعد أولوية عالية مرتبطة بها ويجب تكوينها من أجل استخراج إشعارات بالأحداث بحيث يتم تنبيه فريق تقنية المعلومات على الفور. ويمكنك عوضًا عن ذلك العثور على هذه الأحداث في سجلات جدار الحماية، إلا أن القيام بذلك قد ينطوي على مخاطرة بفقدها. التنبيهات التي يتم إرسالها عند حدوث الطلب سوف تتيح لفريق العمل اكتشاف أن هذه الطلبات قد أصبح الآن نادرة. وبعض جدران الحماية تدعم فقط هذا النوع من القواعد عن طريق إضافة ميزات إضافية بتكلفة إضافية؛ فإذا كان هذا الأمر منطبقًا على جدار الحماية لديك، يتعين عليك تقييم ما إذا كانت فائدة العثور على طلبات مبعثرة يستحق التكلفة الإضافية أم لا.

4.11. قم بتغيير كافة الأسماء من الجذر القديم للإشارة إلى عنوان غير عامل

بعد إتمام المستخدمين لتدريبهم، فإن الطريق الأكثر فاعلية للتأكد من أنهم قد توقفوا عن استخدام الأسماء الخاصة القديم قبل التخلص منها هو جعل كافة الأسماء الخاصة القديمة تشير إلى خادم قمت أنت بتكوينه بحيث لا يستجيب لطلبات الخدمة من أي نوع. كما يساعد ذلك أيضًا في إخلاء وتنظيف أية أنظمة لا تزال تستخدم مساحة الاسم القديمة ولكن لم يتم التعرف عليها في الخطوات السابقة.

ويجب أن يكون العنوان المشار إليه خادمًا معتمدًا بعدم تشغيل أي خدمات. وبالقيام بذلك، لا توجد أي فرصة في حصول أي نظام يستخدم اسمًا خاصًا قديمًا على معلومات هائلة وهذه التطبيقات سوف تعلن عن الأخطاء القابلة للتعرف عليها بسهولة أو فهمها عن طريق المستخدمين؛ وكجزء

من تدريب الوعي، يمكنك التوصية بأن يبلغ المستخدمون عن كافة الأخطاء من هذا النوع إلى فريق تقنية المعلومات. ومع تنفيذ هذه الخطوة، فإن نظام المراقبة الذي يقوم على فحص التكافؤ بين الأسماء القديمة والجديدة (المشار إليها أعلاه) يجب تحديثها دومًا بالتغييرات.

ويجب تغيير الأسماء كلٌ على حدة، وربما يكون ذلك خلال بضعة ساعات على الأقل بين كل تغيير أو مجموعة من التغييرات. ومن المحتمل أن تتسبب هذه الخطوة في اتصالات بإدارة تقنية المعلومات، لذلك فإن تقسيم التغييرات على مراحل سوف يساعد على موازنة حمولة المكالمات مع بدء الأسماء التي لا تزال قيد الاستخدام في التوقف عن العمل.

4.12. إذا تم إصدار شهادات لأي مضيفين بموجب الأسماء الخاصة القديمة، فقم بإلغائها

إذا كانت المؤسسة الخاصة بك لديها شهادات SSL/TLS صادرة لأي من الخوادم في شبكتك باستخدام الأسماء الخاصة القديمة، فيجب إلغاء هذه الشهادات. وهذا من السهل القيام به إذا كان مؤسستك تعمل بصفتها جهة الترخيص الخاصة بها. وإذا استخدمت جهة ترخيص تجارية لإصدار الشهادات لمساحة اسم خاصة، فيتعين عليك تحديد عملية CA لإلغاء الطلبات؛ وقد يكون لدى جهات الترخيص CA الأخرى متطلبات مختلفة لهذه الطلبات.

4.13. عمليات التشغيل طويلة الأجل باستخدام الاسم الجديد

لاحظ أن الاسم الخاص القديم والنطاقات المندرجة تحته لا تزال تتلقى الخدمة، وسوف تواصل حصولها على الخدمة طالما أنك تقوم بتشغيل خادم الاسم. ولا يوجد أي سبب يدعو للتخلص منها، وفي العديد من الأنظمة مثل الدليل النشط، قد يكون من الصعب التخلص من الاسم الأول الذي تم تكوينه في النظام.

وهناك بالفعل سبب وجيه في ترك الاسم هناك: حيث يتيح لك ذلك إمكانية تحديد ما إذا كانت هناك أية آثار متبقية للاسم الخاص القديم في الأنظمة على الشبكة الخاصة بك. وطالما أن كافة العناوين المرتبطة بكافة الأسماء قيد نطاق TLD الخاص تشير إلى مضيف لا تعمل به خدمات، فيمكنك استخدام كل من السجلات من خادم الاسم (وللحصول على مزيد من الفائدة، نظام يقوم بتسجيل كافة مرور البيانات إلى ذلك الخادم) للوقوف على مدى دقتك في التخلص من الاسم الخاص القديم.

5. خطوات لتخفيف حالات تضارب الأسماء المرتبطة بقوائم البحث

للحد بموثوقية من المشكلات المرتبطة بحالات تضارب الأسماء بسبب قوائم البحث، يتعين على الأنظمة أن تغير الطرقة التي تستخدم بها أسماء النطاقات. وقد يكون من المفيد إعداد المستخدمين مقدمًا عن طريق تغيير الإشعارات، وبرامج التوعية والتدريب.

لاحظ أنه إذا كنت تقوم بعملية الإدارة المركزية بالفعل، فقد تكون هذه الإجراءات أقل صعوبة مما قد تتصور. والعديد من الأشخاص الذين يستخدمون في العادة قوائم البحث يعلمون أنه بإمكانهم كتابة الأسماء بالكامل إذا لزم الأمر (كما لو كانوا يدخلون على خادم من خارج الشبكة الخاصة بالمؤسسة)، وسوف يكونون بحاجة إلى تدريب أقل ممن يفهمون فقط الأسماء القصيرة المؤهلة.

5.1. راقب الطلبات الواردة إلى خادم الاسم

لكي يتم الحد من المشكلات التي تحدث بسبب قوائم البحث، يتعين عليك معرفة كافة أجهزة الكمبيوتر، ومعدات الشبكات، وأية أنظمة أخرى تستخدم قوائم البحث في أي طلب. وكافة الأجهزة التي تستخدم قوائم البحث بطريق تلقائية سوف تكون بحاجة إلى تحديث.

وفيما يلي ثلاث طرق شائعة لأداء هذه المراقبة وترقيم الأنظمة:

- خادم الاسم المتكرر (مثل الدليل النشط) قد يحتوي على ميزة تسجيل، ويمكنك تشغيل ميزة التشغيل للحصول على تفاصيل كافة الاستعلامات ذات الأسماء القصيرة غير المؤهلة.
- كما يمكن أيضًا تكوين العديد من جدران الحماية الحديثة للتعرف على الاستعلامات عن كافة الأسماء وتسجيلها. وقد لا يكون ذلك بنفس فاعلية التسجيل من نظام التسمية نفسه، وذلك استنادًا إلى تقسيم شبكتك. على سبيل المثال، إذا لم يجتاز أي استعلام جدار حماية، فلا يمكن لجدار الحماية التعرف على الاستعلام، وسوف يتم تفويته على هذا النحو.
- وإذا تعذر استخدام أي مما سبق، فيمكن مراقبة خادم الاسم باستخدام برنامج لالتقاط الحزم مثل برنامج Wireshark. وعلى الرغم من ذلك، تتطلب هذه الطريقة أن تتم معالجة البيانات المجمعة باستخدام برنامج وذلك من أجل العثور على الاستعلامات للأسماء القصيرة غير المؤهلة فقط.

لاحظ أن هذه الخطوة يمكن أن تؤدي إلى نتائج مربكة. وتحتوي أجهزة مثل أجهزة الكمبيوتر والهواتف على تطبيقات يقوم المستخدمون بكتابة أسماء فيها؛ وسوف تظهر هذه الأجهزة في الاستطلاع حتى وإن لم تكن هناك أية إصدارات مخزنة للأسماء القصيرة غير المؤهلة. وبالنسبة لهذه الخطوة، من الضروري فقط معرفة كافة الأماكن في الشبكة الخاصة بك حيث يجري تخزين الأسماء القصيرة غير المؤهلة أو استخدامها للتطبيقات.

5.2. قم بإنشاء قائمة لكل نظام يستخدم الأسماء القصيرة غير المؤهلة بطريقة تلقائية

أنت بحاجة إلى ملخص للسجلات من الخطوة السابقة. ويجب أن يكون هذا الملخص عبارة عن قائمة تضم كافة الأجهزة وكافة الأسماء القصيرة غير المؤهلة التي يجري الاستعلام عنها وليس كل مثال على جهاز يجري استعلامًا. والسبب وراء حاجتك إلى كافة الأسماء التي يجري الاستعلام عنها هو أن بعض الأجهزة سوف يكون بها العديد من التطبيقات التي يتعين ضبطها. ويصبح هذا الملخص هو بيان الجرد للأجهزة التي يتعين تغييرها.

5.3. درّب المستخدمين ومديري الأنظمة على استخدام أسماء النطاقات المؤهلة بالكامل FQDN

بالإضافة إلى تغيير الأنظمة التي يتم إدخال الأسماء القصيرة غير المؤهلة في أي تكوين (سواء كان تكوينًا على مستوى النظام أو تكوين لتطبيق فردي)، يتعين عليك تغيير الطرق التي يرى المستخدمون أنها تحملهم على التغيير من استخدام الأسماء المختصرة إلى الأسماء الكاملة. واستخدم التفسيرات الخاصة بالعواقب غير المقصودة أو غير المرغوبة والتي يمكن أن تؤثر على مؤسستك من أجل رفع مستوى الوعي ودعم مستوى القبول.

5.4. قم بتغيير كل نظام متضرر إلى استخدام أسماء النطاقات المؤهلة بالكامل FQDN

استبدل الأسماء القصيرة غير المؤهلة بأسماء النطاقات المؤهلة بالكامل FQDN المقابلة لها على أساس كل نظام على حدة. وكل مثال على الاسم القصير غير المؤهل الموجود في كافة البرامج المستخدمة في النظام يجب استبداله باسم النطاق الكامل.

كما أن المراقبة التي تم البدء فيها أعلاه ذات أهمية استثنائية في هذه الخطوة. ومن غير المتحمل أن تكون لك القدرة على تحديد كافة التطبيقات في كافة الأنظمة التي يجري تغييرها وتحتوي على أسماء قصيرة غير مؤهلة مضمنة فيها. وعوضًا عن ذلك، يجب الرجوع إلى نظام المراقبة بعد إجراء التغييرات على كل نظام للتعرف على ما إذا كان النظام لا يزال يصدر طلبات للأسماء القصيرة غير المؤهلة أم لا.

وتستخدم العديد من النظم بعض تطبيقات الاستهلال عند تشغيلها للمرة الأولى. وقد يكون لهذه التطبيقات أسماء نظام تعتمد على قوائم بحث مضمنة فيها، كما أن العثور على كل هذا قد يكون صعبًا. وبعد تغيير كافة الأسماء في أي نظام لاستخدام أسماء النطاقات المؤهلة بالكامل FQDN، أعد تشغيل النظام واستخدم برنامج المراقبة لمراقبة عمليات البحث عن الأسماء. فإذا كان النظام يبحث عن أي من الأسماء القصيرة غير المؤهلة، يتعين عليك تحديد البرنامج المتسبب في ذلك الطلب وتغييره لاستخدام أسماء النطاقات المؤهلة بالكامل FQDN. وقد تستغرق هذه العملية عدم مرات من إعادة تشغيل النظام من أجل إجراء تكوين كامل للنظام بشكل صحيح.

5.5. أوقف تشغيل قوائم البحث في برامج حل الأسماء المشتركة

هذه هي النقطة التي يصبح فيها التحول من الأسماء القصيرة غير المؤهلة واقعًا لكافة الأنظمة (أجهزة الكمبيوتر الشخصي، وأجهزة الشبكة، والطابعات، وما إلى ذلك) على الشبكة. وقد توجد قوائم البحث في أي من الأنظمة التي تقوم بحل الأسماء أو التي تخدم تكوينًا لأنظمة أخرى، مثل خادم DHCP. وغالبًا ما تكون هذه الأنظمة عبارة عن خوادم اسم قائمة بذاتها، لكن يمكن أن تكون أيضًا جدران حماية أو أجهزة شبكات أخرى. وبصرف النظر عن نوع النظام، يجب إيقاف تشغيل قوائم البحث على كل منها من أجل منع المستخدمين من محاولة استخدام الأسماء القصيرة غير المؤهلة داخل مساحة اسم محددة.

5.6. ابدأ المراقبة لاستخدام الأسماء القصيرة غير المؤهلة في خوادم الاسم

يتعين عليك تكوين خادم الاسم الخاص بك بحيث يبدأ مراقبة كافة الطلبات للحصول على الأسماء التي يجب أن تستخدم قوائم البحث. وإذا قمت بتقديم إشعار مسبق وتدريب، يتوجب على المستخدمين لديك عدم استخدام هذه الأسماء بعد ذلك، فإن السجل الناتج عن خطوة المراقبة هذه قد لا يكون كبيرًا للغاية، وإذا كان كذلك، فقد يتعين عليك تكرار بعض الخطوات أعلاه لبعض الأنظمة العاملة على شبكتك.

5.7. قم بإعداد مراقبة طويلة الأجل بحدود خارجية لمراقبة الأسماء القصيرة غير المؤهلة

يجب أن تكون الخطوات السابقة قد عثرت على أغلبية كبيرة من استخدامات الأسماء القصيرة غير المؤهلة، ولكن بضعة أنظمة (ربما أساسية) قد لا تزال مستخدمة للأسماء الخاصة القديمة، لكن ربما يكون ذلك في النادر فقط. وأفضل طريقة للتعرف على هذه الاستعلامات الخاصة بالاسم هو إضافة قواعد إلى كافة جدران الحماية عند حافة الشبكة الخاصة بك من أجل البحث عن أية طلبات تكون متسربة. ويجب أن تكون لهذه القواعد أولوية عالية مرتبطة بها ويجب تكوينها من أجل استخراج إشعارات بالأحداث بحيث يتم تنبيه فريق تقنية المعلومات على الفور. ويمكنك عوضًا عن ذلك العثور على هذه الأحداث في سجلات جدار الحماية، إلا أن القيام بذلك قد ينطوي على مخاطرة بفقدها. التنبيهات التي يتم إرسالها عند حدوث الطلب سوف تتيح لفريق العمل اكتشاف أن هذه الطلبات قد أصبح الآن نادرة. وبعض جدران الحماية تدعم فقط هذا النوع من القواعد عن طريق إضافة ميزات إضافية بتكلفة إضافية؛ فإذا كان هذا الأمر منطبقًا على جدار الحماية لديك، يتعين عليك تقييم ما إذا كانت فائدة العثور على طلبات مبعثرة يستحق التكلفة الإضافية أم لا.

6. الكشف عن تضارب الأسماء في نطاقات gTLD الجديدة

منذ 18 أغسطس 2014، تطلب ICANN أن تقوم نطاقات gTLD التي يتم تفويضها حديثًا في منطقة الجذر بمساعدة المنظمات للكشف عند تسريب الاستفسارات إلى DNS العالمية للأسماء التي تقع تحت نطاقات TLD الجديدة. هذه المساعدة سوف تستمر لمدة 90 يومًا، على الأرجح، في الأيام الأولى التي تكون فيها نطاقات gTLD الجديدة في منطقة الجذر. بعد ذلك، سوف تتصرف gTLD الجديدة مثل أي نطاقات TLD أخرى في منطقة الجذر. تقدم المساعدة من خلال خدمة "الانقطاع الخاضع للرقابة" الموضح في هذا القسم.

بوضوح، يجب على المنظمة التي تحتاج إلى تخفيف تضارب الأسماء بين مساحة الاسم الخاصة لديها ونطاقات DNS العالمية القيام بذلك قبل دخول نطاقات TLD المقابلة الجديدة لمنطقة الجذر: لا ينبغي الانتظار لفترة الـ90 يومًا هذه. (وهذا ينطبق بصفة خاصة على المنظمات التي تختار نطاقات TLD من حرفين لأسمائهم، لأن هذه الأسماء ليست مطلوبة لإجراء انقطاع خاضع للرقابة.) ويهدف الانقطاع الخاضع للرقابة ليكون التحذير الأخير للمنظمة بأنها تحتاج بسرعة إلى تنفيذ تخفيف قبل بدء نطاقات TLD في تقديم إجابات "حقيقية" للاستفسارات.

يصف هذا القسم كيف يتم تنفيذ الانقطاع الخاضع للرقابة على خادم الاسم المخول، وكيف يبدو في الإجابات على الاستفسارات. كما أنه يعطي المشورة للمنظمات التي لديها مساحات خاصة للأسماء لتحديد ما إذا كانت التغييرات التشغيلية التي يراقبونها هي نتيجة الانقطاع الخاضع للرقابة، وإذا كان الأمر كذلك، ما الذي يجب القيام به حيال هذه التغييرات.

6.1 وصف الانقطاع الخاضع للرقابة

خدمة الانقطاع الخاضع للتحكم التي تطلبها ICANN لنطاقات gTLDs الجديدة المضافة إلى منطقة الجذر بعد 18 أغسطس 2014 مصممة لتسبب انقطاع للأجهزة التي يتسرب طلبها لأسماء النطاقات في مساحات الأسماء الخاصة إلى DNS العالمي. حاليًا، عندما يتسرب طلب DNS هذا إلى DNS العالمي، ترسل خوادم اسم الجذر مرة أخرى ردًا مع رمز يشير إلى عدم وجود النطاق. (من الناحية الفنية، هذا حقل RCODE من عنوان الاستجابة المعين إلى قيمة 3، والمعرف لمساعدة الذاكرة ليكون رد "NXDOMAIN".)

خلال فترة خدمة النطاق الخاضعة للرقابة، بدلاً من الحصول على خطأ NXDOMAIN في الرد، لا يحتوي الرد على إشارة خطأ لأي خطأ، ولكن بدلاً من ذلك يحتوي على البيانات التي لديها أعلى فرصة لملاحظتها من قبل النظام الذي أرسل الطلب. فمن المستحيل تصميم الرد الذي سوف يكون ملاحظًا دائمًا لأن هناك العديد من الأنواع المختلفة من البرمجيات التي تصنع طلبات DNS. ومع ذلك، فإن الانقطاع الخاضع للرقابة بتكليف ICANN، سوف يكون ملاحظًا على الأنظمة مع التسجيل الكافي للأخطاء، وعلى الشبكات حيث حركة مرور DNS يمكن ملاحظتها من قبل مسؤولي الشبكة.

سوف تستجيب نطاقات gTLD العاملة في مجال الانقطاع الخاضع للمراقبة إلى مجموعة واسعة من استفسارات DNS بطريقة يمكن التنبؤ بها. يشرح القسم 6.2 كيفية مراقبة سلوكيات الأنظمة التي تحصل على ردود بالانقطاع الخاضع للمراقبة لاستفسارات انقطاع DNS.

- إلى حد بعيد فإن استعلام DNS الأكثر شيوعًا هو لسجلات ""A، وهو، لعناوين IPv4المصاحبة لاسم المجال. تأتي هذه الاستفسارات دائمًا مع عنوان IPv4 من 127.0.53.53. هذا العنوان هو عنوان الاسترجاع للمضيف الذي أرسل الاستعلام، بحيث إذا كان التطبيق يستخدم هذا العنوان لبدء أي نوع من الاتصال، سوف يرسل هذه الرسالة إلى نفسه. هذا، بطبيعة الحال، من المحتمل أن يفشل، لأن جميع البرامج التي تقوم بعمليات بحث DNS تقريبًا تنوي استخدام العنوان في الرد على اتصال ملقم آخر.

- استفسار آخر أكثر شيوعًا لـ DNS هو عن السجلات التي تحتوي على نص، والمعروف باسم "سجلات TXT". فيما يتعلق بخدمة الانقطاع الخاضع للرقابة، سيكون رد سجل TXT دائمًا نفس السلسلة "your-dns-needs-immediate-attention .أنظر https://icann.org/namecollision". إن النظام الذي يعرض سجلات النص هذه يعطي المشاهد معلومات بشأن تضارب الأسماء.

- للاستعلامات بشأن DNS الخاصة بخدمة البريد (من الناحية الفنية، لتبادل البريد أو سجلات (MX، فإن خدمة الانقطاع الخاضع للسيطرة سوف ترد باسم النطاق your-dns-needs-immediate-attention.. <TLD>، حيث "<TLD>" هي TLD في طلب DNS. قد يكون اسم النطاق هذا مشاهدًا في ردود الخطأ من عميل البريد أو خادم البريد. النظر في عناوين اسم النطاق your-dns-needs-immediate-attention.. <TLD>، سوف يعود 127.0.53.53.

- سوف ترد خدمة الانقطاع الخاضع للمراقبة على الاستفسارات لسجلات خدمة (SRV)مع اسم النطاق your-dns-needs-immediate-attention.. الاستفسارات عن سجلات SRV ليست شائعة مثل تلك لعناوين IPv4، وسجلات النص، وأسماء ملقم البريد، ولكن أصبحت أكثر شيوعًا لأحدث التطبيقات مثل الرسائل الفورية ونقل الصوت.

تمت إضافة gTLD إلى منطقة الجذر قبل 18 أغسطس 2014 وقد يكون لها أيضًا خدمة الانقطاع الخاضع للرقابة لمجموعة فرعية من نطاقات المستوى الثاني الممكنة في TLD. السجلات التي تم إرجاعها في الانقطاع الخاضع للرقابة لهذه الأسماء متطابق مع السجلات المذكورة أعلاه. طلبت ICANN أن يتم حظر بعضًا من SLD من TLD، وربما تصبح تلك الأسماء نشطة بعد انقطاع خاضع للرقابة لمدة 90 يومًا لـSLD.

6.2 ملاحظة الانقطاع الخاضع للرقابة

من المهم أن نلاحظ أنه لا يوجد هناك ما يضمن أن التطبيق الذي يتلقى استجابةمن الانقطاع الخاضع للرقابة سيعمل بوضوح بشكل مختلف عما كان عليه قبل الانقطاع الخاضع للرقابة. ومع ذلك، فمن المحتمل جدًا أن يتصرف التطبيق بشكل مختلف، وسوف يكون الفرق على الأرجح إخفاقًا، نأمل أن يكون للفشل رسائل الخطأ المرتبطة به وأن يقدم مستخدم التطبيقتقريرًا بذلك إلى مسؤول هذا النظام المكلف بالتعامل مع هذا.إذا كانت رسالة الخطأ تحتوي على عنوان IPv4127.0.53.53، فهذا مؤشر قوي جدًا على أن الخطأ يرجع إلى البرنامج الذي يستخدم الاسم من مساحة الاسم الخاص الذي تسرب إلى الإنترنت العام.

تظهر الأخطاء بسبب خدمة الانقطاع الخاضع للرقابة عندما يبدأ البرنامج الذي كان يحصل في وقت سابق على ردود NXDOMAIN على الاستفسارات، في الحصول على الردود الفعلية. وبطبيعة الحال، فإن هذه الأخطاء سوف تظهر في وقت لاحق عندما تستجيب gTLD الجديدة مع البيانات الحقيقية، ومن المرجح أن تستمر خدمة الانقطاع الخاضع للرقابة لمدة 90 يومًا فقط بتكليف من ICANN. خلال ذلك الوقت، فإن الأخطاء تكون أكثر وضوحًا بسبب رسائل الخطأ التي تحتوي على عنوان IPv4 من 127.0.53.53، النص "your-dns-needs-immediate-attention. أنظر "https://icann.org/namecollision"، أو اسم النطاق الذي يحتوي على "your-dns-needs-immediate-attention."

ويمكن ملاحظة الانقطاع الخاضع للرقابة في شبكة المؤسسة إذا قام مسؤول الشبكة بالبحث بنشاط عن رسائل DNS التي تحتوي على تلك الردود. يمكن أن يتم مثل هذا البحث من خلال تبويب للشبكة الصنبور في نقاط التسرب المناسبة، أو يمكن أن تتم على جدار الحماية. هذا النوع من المراقبة لا يعتمد على رؤية رسائل الخطأ في الكمبيوتر المصاب؛ بدلاً من ذلك، يمكن لمسؤول الشبكة تحديد أي كمبيوتر تتسرب طلباته للأسماء في مساحات الاسم الخاصة من شبكة المنظمة.

بغض النظر عن كيفية اكتشاف الانقطاع الخاضع للرقابة، يجب أن تكون النتيجة أن الكمبيوتر الذي يحصل على رد الانقطاع الخاضع للرقابة يجب أن تعاد تهيئته لتلبية لجعل استفسارات DNS على خادم اسم المنظمة، وليس على DNS العالمي. لا توجد طريقة قياسية لتحديد مثل هذا الإعداد، على الرغم من أن الإعداد هو عادة جزء من نظام التشغيل. إذا كان الكمبيوتر يحصل على إعدادات الشبكة من ملقم في شبكة المنظمة، تسمى عادة "خادم DHCP"، يحتاج ذلك الملقم إلى تغيير إعداداته لجعل استفسارات DNS تذهب إلى خادم اسم المنظمة، وليس إلى DNS العالمي.

أي ملاحظة من حصول الكمبيوتر على رد الانقطاع الخاضع للرقابة هو علامة على أن أجهزة الكمبيوتر الأخرى على شبكة هذه المنظمة تحصل عليه أيضًا. يجب على مسؤول النظام أن يفحص على الفور إعدادات DNS لكافة أجهزة الكمبيوتر على نفس الشبكة، حتى لو كانت تلك الحواسيب لا تظهر علامات يمكن ملاحظتها للحصول على إجابات الانقطاع الخاضع للرقابة. تذكر أن الانقطاع الخاضع للرقابة يدوم فقط 90 يومًا، لذلك، هناك وقت محدود لإيجاد أجهزة الكمبيوتر التي تحتوي على إعدادات DNS غير صحيحة.

بالطبع، القيام بمثل هذه التغييرات ليس سوى تخفيف مؤقت للمشكلة الكامنة وراء تضارب الاسم. القسمين 4 و5 من هذه الوثيقة يعطي تعليمات حول كيفية جعل التخفيف دائم.

7. موجز

لحالات تضارب الأسماء إمكانية إنشاء نتائج غير متوقعة بالنسبة للمؤسسات التي تستخدم مساحات الأسماء الخاصة. تتناول هذه الوثيقة بعضًا من تلك النتائج المحتملة وتحدد أفضل الممارسات لتغيير الطريقة التي تستخدم بها مساحات الأسماء الخاصة داخل المؤسسات.تصف الوثيقة أيضًا الانقطاع الخاضع للرقابة كوسيلة لتحديد أين يمكن أن يصبح تأثير تضارب الأسماء واضحًا.

بالنسبة لمساحات الأسماء التي استخدمت نطاق TLDخاص والتي تتحول (أو تحولت بالفعل) إلى TLD في نظام DNS العالمي، وأفضل تخفيف يأتي في صورة الحد من مساحة اسم غلى مساحة اسم متأصلة الجذر في نظام DNS العالمي. أما بالنسبة لمساحات الأسماء التي تستخدم اختصارات الأسماء مع قوائم البحث، يمكن أن يأتي التخفيف والحد فقط من خلال الحد من استخدام قوائم البحث. الخطوات الخاصة بتحقيق عمليات التخفيف هذه تشمل أيضًا المراقبة طويلة الأجل في الشبكة الخاصة للتحقق من أن كافة الأمثلة على الأسماء التي قد تسبب تضاربات لم تعد مستخدمة الآن. سيكون هناك وسائل للمنظمات للإخبار متى سيواجهون تضارب الأسماء حيث أن بعض نطاقات TLD الجديدة يتم تفويضها في منطقة الجذر.

وعملية التخلص الشاملة من مشكلات تضارب الأسماء تتمثل في استخدام أسماء النطاقات المؤهلة بالكامل FQDN في كافة الأماكن التي يجري فيها استخدام اسم نطاق. وفي الشبكات التي تستخدم بالفعل نظام DNS العالمي، فإن هذا يعني استخدام قوائم بحث. وفي الشبكات التي تستخدم مساحة اسم خاصة، فإن هذا يعني أن مساحة الاسم الخاصة يجب أن توضع في جذر نظام DNS العالمي، ويجب أن لا تستخدم قوائم البحث.

الملحق أ: لمزيد من القراءة

تم تقديم المستندات التالية بمعرفة العديد من المنظمات داخل ICANN. وتوفر مؤسسات أخرى مستندات قد تكون مفيدة أيضًا. والأكثر أهمية من ذلك، هو أن موفر برامج خادم الاسم و/أو الأجهزة قد تكون لديه معلومات قيّمة على موقع الدعم الفني الخاص به على الويب.

أ.1. مقدمة لبرنامج gTLD الجديدة

تصف هذه الصفحة تاريخ وتنفيذ وتقدم البرنامج لإضافة مئات من نطاقات gTLD الجديدة إلى نظام DNS العالمي.
http://newgtlds.icann.org/en/about/program

أ.2. تعارض الأسماء في DNS

أسندت ICANN إلى مجموعة Interisle Consulting Group, LLC مهمة وضع هذا التقرير المتعمق حول حالات تضارب الاسم المحتملة. وهي توفر نظرة عامة على حالات تضارب الأسماء، وتطرح بيانات حول نطاقات TLD غير الموجودة في الوقت الحالي والتي تم الاستعلام عنها في الوقت الحالي في خوادم الجذر، وتوفر قدر كبير من الخلفية حول المشكلات التي قد تسببها حالات تضارب الأسماء.
http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

أ.3. خطة إدارة حالات التضارب في gTLD الجديدة

هذه هي الخطة التي اعتمدتها ICANN حول كيفية إدارة حالات تضارب الأسماء بين نطاقات gTLD الجديدة ومساحات الأسماء الخاصة. وهي تشتمل أيضًا على العديد من المؤشرات للتعليقات الواردة من ICANN على المقترحات المبكرة ذات الصلة بحالات تضارب الأسماء في منطقة الجذر.
http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

أ.4. إطار إدارة وجود تضارب الأسماء

يحتوي هذا المستند على خطة لإدارة تضارب الأسماء في gTLD الجديدة. فهو يحدد خصوصيات خدمة الانقطاع الخاضع للرقابة لنطاقات gTLD التي يتم التفاوض بشأنها في منطقة جذر DNS بدءًا من 18 أغسطس 2014.
http://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

أ.5. اهتمامات gTLD الجديدة: الأسماء التي لا تحتوي على نقاط وحالات تضارب الأسماء

قد تقدم قوائم البحث على النظم المختلفة نتائج مختلفة جدًا وذلك استنادًا إلى ما هو موجود في الاسم القصير غير المؤهل والذي يجري الاستعلام عنه. تركز هذه المقالة على قوائم البحث حول النطاقات غير المحتوية على نقاط (نطاقات TLD ذات سجلات العناوين في قمتها)، إلا أن وصف معالجة قوائم البحث له قيمته في العديد من السياقات الأخرى أيضًا.
https://labs.ripe.net/Members/gih/dotless-names

أ.6. SAC 045: الاستعلامات غير الصالحة حول نطاقات في مستوى الجذر لنظام اسم النطاق

يصف هذا التقرير المقدم من SSAC التابعة لـ ICANN أنواع الاستعلامات عن نطاقات TLD التي تم البحث عنها في خوادم الجذر في زمن كتابة هذه الوثيقة.
http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

أ.7. SAC 057: استشارات SSAC لشهادات الاسم الداخلي

يصف هذا التقرير المقدم من لجنة SSAC التابعة لـ ICANN متضمنات الأمن والاستقرار للشهادات التي تحتوي على أسماء خاصة (داخلية). وهي تحدد ممارسة من هيئات التوثيق التي يمكن استغلالها من قبل المهاجمين ويمكن أن تمثل خطرًا كبيرًا على خصوصية ونزاهة اتصالات الإنترنت الآمن.
http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf