باللغة العربية

SAC 032

تقرير تمهيدي حول تعديل استجابة DNS

ملاحظة حول الترجمات

كُتبت النسخة الأصلية لهذه الوثيقة باللغة الإنجليزية، وهي متاحة على http://www.icann.org/committees/security/sac032.pdf. وأينما وجد اختلاف في المعنى أو ما يوهم أنه اختلاف في المعنى بين هذه الوثيقة والنص الأصلي، فسيكون النص الأصلي هو السائد.

تقرير استشاري صادر عن
اللجنة الاستشارية للأمان والاستقرار (SSAC)
التابعة لـ ICANN
يونيو 2008

مقدمة

يقدم مجال رمز الاستجابة (RCODE) الخاص ببروتوكول DNS وسائلاً لخادم الاسم للإشارة إلى المشاكل التي يواجهها عند محاولة الاستجابة لاستفسار من عميل (المحلل) ووصف هذه المشاكل. وسيقوم خادم الاسم المعتمد بإعادة مجموعة من رموز الاستجابة (RCODE) إلى القيمة *خطأ في الاسم* للإشارة إلى عدم وجود اسم النطاق الموجود في الاستفسار. كما تستخدم معايير الإنترنت أيضًا المصطلحات *نطاق غير موجود* أو *استجابة NXDomain* لوصف خطأ الاستجابة هذا[2].

وتكون قيمة خطأ في الاسم ذات معنى فقط في الاستجابات القادمة من خادم الاسم المعتمد. وفي بعض الحالات، يعهد مسجّلو النطاقات الخاصة بالنطاق بخدمة الاسم المعتمد الخاصة بهم إلى موظفين داخليين، بينما في حالات أخرى، يعهدون بها إلى منظمة خارجية لإدارة DNS الخاص بهم. وتطلق SSAC على هؤلاء اسم الوكلاء المفوضون لخدمة الاسم أو ببساطة الوكلاء المفوضون. ولا يقوم عملاء DNS عادةً بتقديم استفسار لخوادم الاسم المعتمد مباشرةً. وعلى العكس، يتم تحليل غالبية استفسارات DNS بواسطة نظم وسيطة تعرف *بالمحللين التكراريين*. وقد يتم تشغيل المحللين التكراريين بشكل خاص بواسطة أية منظمة. كما يتم تشغيلها علنًا أيضًا بواسطة مزودي الخدمة الذين يقومون باستضافة خدمات الاسم نيابةً عن العملاء أو يقومون بتوفير خدمة تحليل الاسم للمشاركين. ونظرًا لأنه يكون لدى مسجّلو النطاق عادةً عمل تجاري وعلاقة ثقة مع الوكلاء المفوضين، غير أنهم لا يتمتعون بشكل عام بهذه العلاقات مع جميع مشغلي المحللين التكراريين. وهكذا، فإننا نستخدم مصطلح –في هذا التقرير- *الطرف الآخر* عند التحدث عن هذه الفئة من مزودي خدمة الاسم.

وفي هذا التقرير التمهيدي، نقوم بوصف ممارسة تعديل استجابة DNS بواسطة الوكلاء المفوضون أو الأطراف الأخرى. وفي الحالة الأولى، يتلقى الوكيل المفوض استفسار DNS من أحد الأسماء. ويقوم الوكيل المفوض بتقرير أن الاسم الموجود في الاستفسار غير موجود في ملف المنطقة الذي يقوم باستضافته لمسجّل النطاق، ولكن بدلاً من إعادة استجابة DNS تشير إلى *اسم غير موجود*، يقوم الوكيل المفوض بإعادة استجابة تشير إلى وجود الاسم وإحتوائه على توجيه عنوان بروتوكول إنترنت (IP) للاسم صاحب الاستفسار الخاص باختيار الوكيل. وفي الحالة الثانية، يتلقى طرف آخر يقوم بتشغيل محلل تكراري استجابات NXDomain التي يتم إنشاؤها بواسطة خادم اسم معتمد ويقوم في هدوء بتعديل المحتويات مما يؤدي إلى تغيير الاستجابة *اسم غير موجود* إلى أخرى تشير إلى *الاسم موجود* وإدراج توجيه عنوان بروتوكول إنترنت (IP) للاسم صاحب الاستفسار الخاص باختيار الطرف الآخر.

ويتم التعرف على هذا السلوك بواسطة العديد من العناوين: إعادة توجيه النطاق الفرعي وإعادة توجيه NXDomain وتنقيح NXDomain والاستيلاء على NXDomain والاستيلاء على النطاق الفرعي وتحليل الخطأ وخطأ في التسويق. وتوضح هذه العناوين أن الممارسة لها أهمية تجارية ومثيرة للجدل.

---

[1] انظر RFC 1035، تنفيذ نظام اسم النطاق والمواصفات، http://rfc.net/rfc1035.html ومزود امتداد IANA http://www.iana.org/assignments/dns-parameters

[2] RFC 2308, NXDomain, http://rfc.net/rfc2308.html

والهدف من هذا التقرير هو وصف تأثيرات تعديل استجابة DNS على مسجّلي نطاقات اسم النطاق ومشغلي DNS ومستخدمي الإنترنت واستكشاف عمليات الاستغلال المحتملة للممارسة من قِبل الوكلاء السيئين. ويركز هذا التقرير المبدئي على توضيح آثار النتائج غير المطلوبة على المستخدمين ومسجّلي النطاقات وأولئك الذين يعتمدون على استجابات عدم وجود النطاق في تقديم تقارير بالخطأ ولأهداف إدارية.

ما المقصود بتعديل استجابة DNS؟

تعديل استجابة DNS هو عبارة عن عملية يقوم مزود خادم الاسم من خلالها بإعادة رسالة استجابة DNS تشير إلى أن *الاسم موجود* بدلاً من رسالة تشير إلى اسمٍ غير موجود عند الاستفسار عن اسم معين ولكن هذا الاسم لم يتم نشره في معلومات منطقة مسجّل النطاق. وفي بعض الحالات، يستغل الوكيل المفوض لمسجّل النطاق الفرصة التي وُجدت عند عدم وجود اسم داخل أحد النطاقات (على سبيل المثال، خطأ في الكتابة مثل ww.example.com بدلاً من www.example.com) ليعيد *استجابة مركبة*، على سبيل المثال، توجيه عنوان بروتوكول الإنترنت (IP) للاسم المستفسر عنه من اختياره. وقد يستخدم الوكيل المفوض توجيه عنوان بروتوكول إنترنت (IP) مشترك أو افتراضي لجميع الأسماء المستفسر عنها والتي لم يتم نشرها في ملف المنطقة: وتسمى هذه العملية *بتركيب الرمز العشوائي*.

وفي حالات أخرى، سيقوم محلل تكراري يتم تشغيله بواسطة طرف آخر بفحص استجابات DNS للاستفسارات التي حاول حلها نيابة عن عملائه. وعند اكتشاف أن استجابة DNS تحتوي على رمز استجابة تم تعيينه على القيمة *خطأ في الاسم*، يقوم الطرف الآخر بتهيئة المحلل التكراري لتغيير المحتويات الخاصة باستجابة DNS هذا بشكل صامت قبل إرسال الرسالة إلى العميل الذي قدم الاستفسار. وبشكل خاص، يقوم المحلل التكراري بتغيير رمز الاستجابة من الاستجابة التي تشير إلى عدم وجود الاسم إلى استجابة تشير إلى وجود هذا الاسم. وبالإضافة إلى ذلك يقوم المزود بتهيئة المحلل لتعديل محتويات الاستجابة من خلال إدخال توجيه عنوان بروتوكول الإنترنت (IP) للاسم المستفسَر عنه، وبوجه خاص، لا يتم نشر هذا التوجيه في ملف منطقة مسجّل النطاق ولكن هذا التوجيه هو من اختيار الطرف الآخر.

إعادة التوجيه في مستوى مزود امتداد DNS

قامت كل من SSAC ومجلس إدارة هندسة الإنترنت (IAB) في فترة سابقة بالتعليق على إعادة التوجيه وتركيب DNS في مستوى مزود امتداد DNS [4, 5, 6]. ولا تضيف SSAC أية تعليقات أو توصيات إضافية في هذا التقرير. ومع ذلك، وفي محاولة الوصول إلى الاكتمال، نوضح التدفق الأساسي *للاستجابة المركبة من مُشغل* TLD هنا:

1) يقوم العميل بإرسال استفسار DNS لتحليل اسم نطاق example.tld إلى عنوان بروتوكول الإنترنت (IP) إلى محلل تكراري A.
2) يقوم المحلل التكراري A ببدء عملية التحليل من خلال إرسال الاستفسار إلى أحد خوادم اسم الجذر.
3) يقوم خادم اسم الجذر بإعادة قائمة بخوادم الاسم التي تستطيع تحليل عناوين *tld*.
4) يقوم المحلل التكراري *A* بإرسال الاستفسار لتحليل example.tld إلى أحد خوادم الاسم الخاصة بـ tld التي حددها خادم اسم الجذر.

---

[3] نحن نصف هذا السلوك *كتغيير صامت* نظرًا لأن المحلل البديل لا يوفر أية معلومات بروتوكول واضحة للإشارة إلى أنه تم تغيير المحتويات إلى العميل أو إلى الاسم المعتمد.

[4] SAC 006، إعادة التوجيه في نطاقي COM وNET (9 يوليو 2004)
http://www.icann.org/committees/security/ssac-report-09jul04.pdf

[5] SAC 015، سبب عدم استخدام نطاقات المستوى الأعلى لسجلات مورد الرمز العشوائي (10 نوفمبر 2006)
http://www.icann.org/committees/security/sac015.htm

[6] SAC 013، استجابة SSAC لخطاب ICANN، الرد: خدمة مزود الامتداد الجديد المقترَح من Tralliance،
http://www.icann.org/committees/security/sac013.htm

5) يقوم خادم الاسم الخاص بـ *tld* بتحديد أن العنوان *example* لا يتطابق مع عنوان محدد في ملف منطقة *tld*. وبدلاً من إعادة رسالة استجابة DNS برمز استجابة معين على القيمة *خطأ في الاسم*، يقوم خادم الاسم الخاص بـ tld بتكوين رسالة استجابة DNS تقوم بتحليل *example.tld* إلى عنوان بروتوكول الإنترنت (IP) يختاره ويعيدها إلى المحلل التكراري A.

6) يقوم المحلل التكراري A بإرسال رسالة الاستجابة الإيجابية إلى العميل الذي قام بتقديم الطلب (وقد يحفظ هذه الاستجابة في الذاكرة المؤقتة بشكل اختياري).

استجابات DNS المركبة من الوكلاء المفوضين

في هذا المثال، نوضح كيف يتمكن المفوض من تركيب استجابة DNS من نطاق *example.tld*:

1) يقوم العميل بإرسال استفسار DNS لتحليل اسم نطاق *service.example.tld* إلى عنوان بروتوكول الإنترنت (IP) إلى محلل تكراري A.

2) يقوم المحلل التكراري A ببدء عملية التحليل من خلال إرسال الاستفسار إلى أحد خوادم اسم الجذر.

3) يقوم خادم اسم الجذر بإعادة قائمة بخوادم الاسم التي تستطيع تحليل عناوين tld.

4) يقوم المحلل التكراري A بإرسال الاستفسار لتحليل *service.example.tld* إلى أحد خوادم الاسم الخاصة بـ tld التي حددها خادم اسم الجذر.

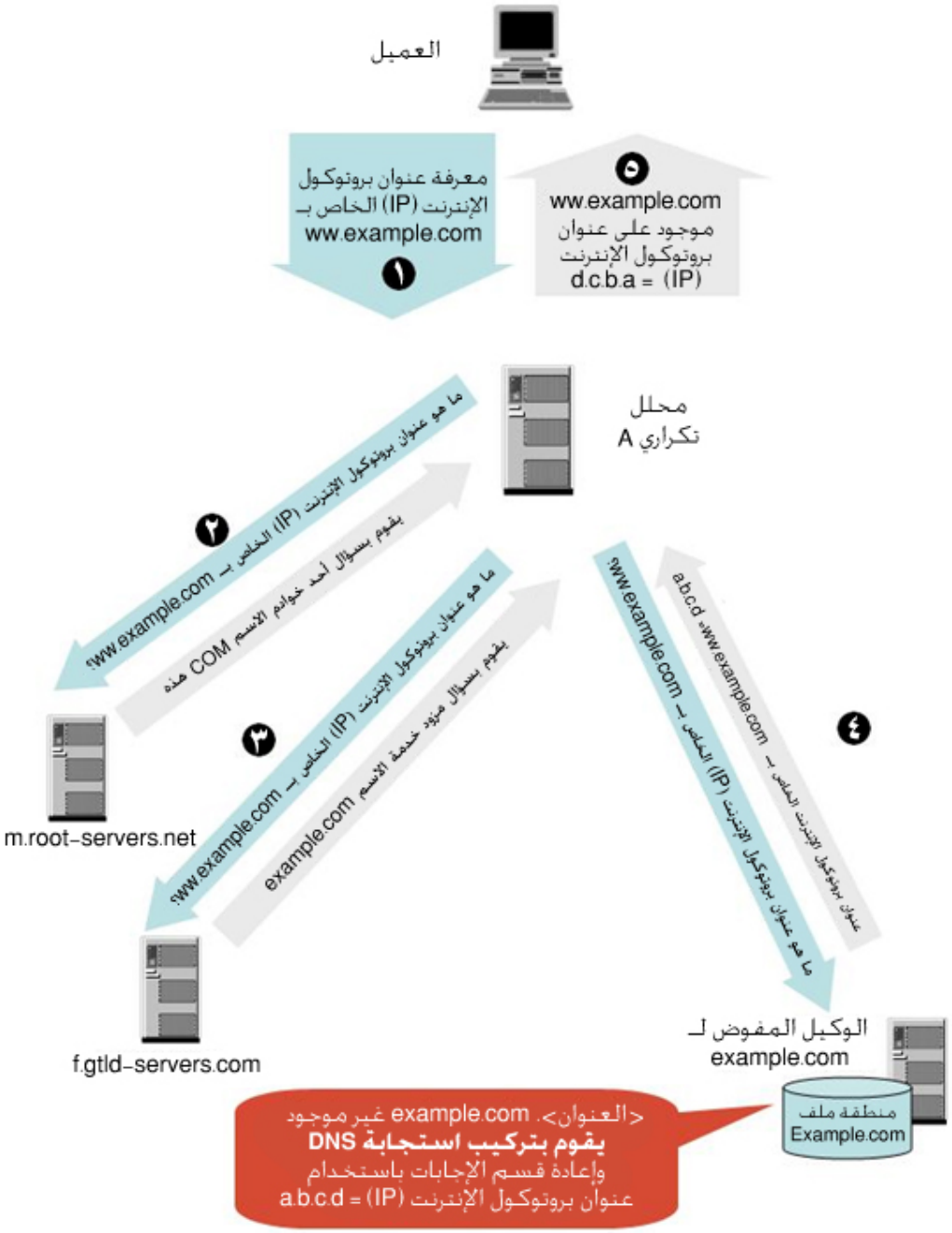
5) يقوم خادم الاسم الخاص بـ *tld* بإعادة قائمة بخوادم الاسم التي تستطيع تحليل عناوين *example.tld*.

6) يقوم المحلل التكراري A بمتابعة عملية التحليل من خلال إصدار استفسار لتحليل *service.example.tld* إلى أحد خوادم الاسم الخاصة بـ *example.tld* التي حددها خادم الاسم الخاص بـ tld.

7) يقوم خادم الاسم الخاص بـ *example.tld* بتحديد أن العنوان *service* لا يتطابق تحديداً مع عنوان موجود في ملف منطقة *example.tld*. فيقوم خادم الاسم الخاص بـ *example.tld* بتكوين رسالة استجابة DNS تقوم بتحليل *service.example.tld* إلى عنوان بروتوكول إنترنت (IP) افتراضي محدد في ملف المنطقة ويعيدها إلى المحلل التكراري A.

8) يقوم المحلل التكراري A بإرسال رسالة الاستجابة الإيجابية إلى العميل الذي قام بتقديم الطلب (وقد يحفظ هذه الاستجابة في الذاكرة المؤقتة بشكل اختياري).

يوضح الشكل 1 هذا النموذج الخاص بتعديل استجابة DNS:



الشكل 1. استجابة NXDomain التي تم تعديلها بواسطة الوكيل المفوض

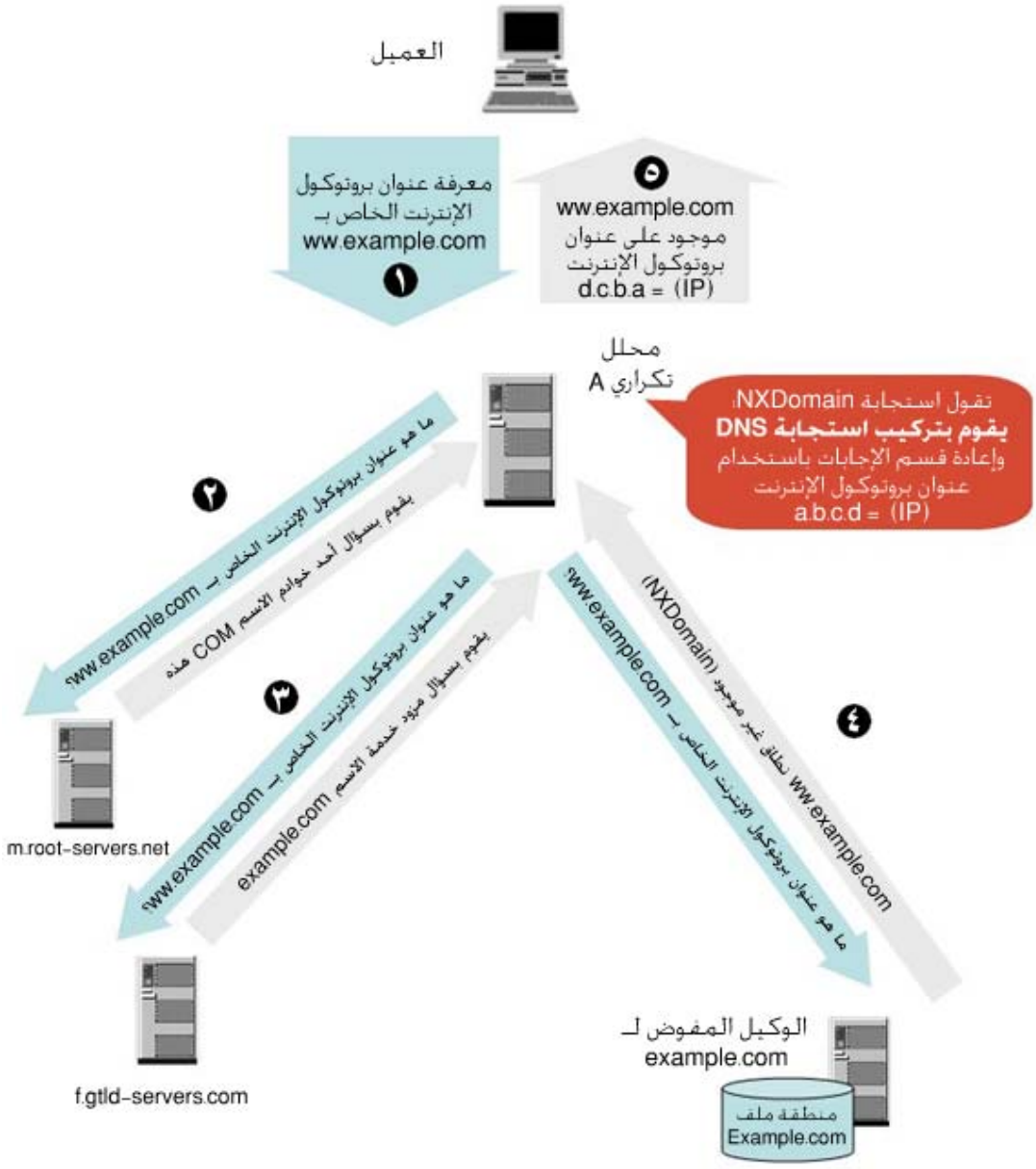
تعديل استجابة NXDomain بواسطة مزودي NS للطرف الآخر

يستطيع أي مُشغل لخادم الاسم الخاص بطرف آخر في أي محلل تكراري مشترك في عملية تحليل اسم محددة تنفيذ تعديل استجابة NXDomain. على سبيل المثال:

1) يقوم العميل بإرسال استفسار DNS لتحليل اسم نطاق service.example.tld إلى عنوان بروتوكول الإنترنت (IP) إلى محلل تكراري A.
2) يقوم المحلل التكراري A ببدء عملية التحليل من خلال إرسال الاستفسار إلى أحد خوادم اسم الجذر.
3) يقوم خادم اسم الجذر بإعادة قائمة بخوادم الاسم التي تستطيع تحليل عناوين tld.
4) يقوم المحلل التكراري A بإرسال الاستفسار لتحليل service.example.tld إلى أحد خوادم الاسم الخاصة بـ tld التي حددها خادم اسم الجذر.
5) يقوم خادم الاسم الخاص بـ tld بإعادة قائمة بخوادم الاسم التي تستطيع تحليل عناوين example.tld.
6) يقوم المحلل التكراري A بمتابعة عملية التحليل من خلال إصدار استفسار لتحليل service.example.tld إلى أحد خوادم الاسم الخاصة بـ example.tld التي حددها خادم الاسم الخاص بـ tld.
7) يقوم خادم الاسم الخاص بـ Example.tld بتحديد أن العنوان service غير موجود في ملف منطقة example.tld ويقوم بإعادة رسالة استجابة DNS برمز استجابة معين على القيمة *خطأ في الاسم*، إلى المحلل التكراري A.
8) يلاحظ المحلل التكراري A أن خادم الاسم الخاص بـ example.tld قام بإعادة رسالة استجابة تشير إلى أن الاسم غير موجود. وبدلاً من نقل رسالة الاستجابة هذه إلى العميل، يقوم المحلل التكراري A بتغيير رمز الاستجابة (RCODE) بشكل صامت في رسالة استجابة DNS إلى RCODE يشير إلى *الاسم موجود* ويقوم بإدخال إجابة للاستفسار بحيث تقوم بتوجيه service.example.tld إلى عنوان IP يختاره مشغل خادم الاسم الخاص بطرف آخر قبل إرسال الاستجابة إلى العميل.

ومن المهم أن نلاحظ -من الناحية العملية- أن أي طرف مشترك في عملية التحليل يستطيع تنفيذ إعادة توجيه NXDOMAIN لأي اسم قام بتحديده على أنه غير موجود أو تم إعلامه بذلك، بغض النظر عما إذا كان هناك خادم معتمد يقدم NXDOMAIN أو لا.

يوضح الشكل 2 هذا النموذج الخاص بتعديل استجابة DNS:



الشكل 1. استجابة NXDomain التي تم تعديلها بواسطة الوكيل المفوض

من الذي يستطيع تعديل رسائل استجابة DNS؟

تحدد الأمثلة المذكورة في القسم السابق مجموعة من الأطراف التي يمكنها إعادة توجيه رسائل استجابة NXDomain. وتتضمن القائمة الوكلاء المفوضين وأطراف الأخرى.

الوكلاء المفوضون. يحق للموظفين الداخليين لمسجّل النطاق العمل كطرف مفوض وإدارة معلومات منطقة مسجّل النطاق. كما يحق للمُسجل الراعي لاسم النطاق أو مزود خدمة إنترنت أو مزودي DNS بالاستعانة بمصادر خارجية (الشركات التي تقوم باستضافة DNS الخاص بإحدى المنظمات مقابل رسوم) العمل كطرف مفوض واستضافة معلومات منطقة مسجّل النطاق.

الأطراف الأخرى. يتمتع أي مشغل DNS خاص بمحلل تكراري يشارك في عملية التحليل استفسار DNS محدد بإمكانية معالجة رسائل استجابة DNS من خادم الاسم المعتمد إلى مقدم الاستفسار بما في ذلك:

- مزودو خدمة DNS العامة، الذين يحققون إيرادات بواسطة
  - جمع تحاليل حركة DNS وبيعها أو
  - بيع فرص الإعلان في الصفحات التي تتم استضافتها على العناوين التي يقومون بإدراجها في استجابات DNS التي يقومون بتغييرها،
- ISPs أو وكلاء ISP (الشركات التي تقوم بتشغيل DNS لـ ISPs مقابل رسوم) الذين يقدمون تحليل الاسم للمشتركين أو -بشكل عام- إلى أي طرف يوفر استخدام خدمة اسم ISP.
- مزودو الخدمة، الذين يقدمون تحليل الاسم وفقًا لخدمات البروكسي على الويب.

وقد يقوم **المعتدون** أيضًا بتعديل استجابات DNS لدعم البرامج الضارة أو الأنشطة الإجرامية.

وتوضح هذه القائمة أيضًا أن هناك العديد من الدوافع لتعديل استجابات DNS. وقد قمنا بمراعاتها في القسم التالي.

لماذا يتم تعديل رسائل استجابة NXDomain؟

تم توضيح العديد من الأسباب التي تدفع الأطراف المختلفة إلى اختيار تعديل استجابات DNS وتحديدها بواسطة SSAC. على سبيل المثال، بدلاً من تقديم استجابة NXDomain التي أصدرها خادم الاسم المعتمد، يستطيع أي طرف آخر وقف هذه العملية وتغيير محتويات استجابة DNS بشكل صامت حتى تحتوي على عنوان بروتوكول الإنترنت (IP) لصفحة ويب مقصود منها:

- **تحقيق إيرادات.** حيث تقوم الصفحة المقصودة باستضافة إعلانات أو محتويات أخرى تؤدي إلى تحقيق إيرادات على نطاق ما ونطاقات فرعية خاصة بالنطاقات المُسجَّلة.
- **تحسين تجربة الويب الخاصة بالمستخدم.** حيث تقوم الصفحة المقصودة بإخبار المستخدم (العميل المحتمل) أن اسم النطاق الذي قام بالاستفسار عنه غير متوفر وتقوم بتزويد المستخدم بطريقة لتحليل نتيجة خطأ، على سبيل المثال، قد يكون يستطيع المستخدم حل الخطأ باستخدام صيغة بحث (مدعومة) يتم الوصول إليها عبر الصفحة المقصودة.
- **تفعيل سياسة.** حيث تقوم الصفحة المقصودة بإخبار المستخدم أن محتوى الصفحات الموجودة في النطاق الذي يحاول الوصول إليه ينتهك إحدى سياسات الاستخدام المقبول. وقد تقوم الصفحة المقصودة بتحديد نوع المحتوى المحدد أو قد تقدم نسخة من سياسة الاستخدام المقبول (AUP) للمستخدم ليقوم بمراجعتها.
- **تقديم تعليم علاجي.** حيث تقوم الصفحة المقصودة بإخبار المستخدم أنه قد حاول الوصول إلى نطاق تم تحديده كنطاق خادع وتم تعليق الموقع. ويتم منح المستخدم فرصة للتعلم من "نجاته" هذه بمراجعة المواد التعليمية لمكافحة الخداع المنشورة على صفحة الويب.
- **التحريض على الأنشطة المحظورة أو الإجرامية.** حيث تستضيف الصفحة المقصودة محتوى ضار قابل للتنزيل باسم موجود في النطاق ولكنه لم يتم تمثيله بواسطة مسجّل النطاق لتسهيل أنشطة إجرامية (الخداع، سرقة الهوية، الاحتيال، إلخ.).

هل يُمثِّل تعديل استجابة DNS مشكلة في الأمان والاستقرار؟

يستحق العديد من سمات تعديل استجابة DNS الانتباه. وتلاحظ SSAC السلوكيات التالية للوكلاء المفوضين والأطراف الأخرى الذين اشتركوا في تعديل استجابة DNS.

1) من المفترض أن يقوم الوكلاء المفوضون بعملية التشغيل بالنيابة عن مسجّل النطاق. ومن المنظور التشغيلي، يتم السماح بالتغييرات التي يقوم بها الوكيل المفوض داخل نموذج بيانات DNS. كما أن تحديد السماح للوكيل المفوض بإنشاء استجابة مركبة أمر يمكن حله بين الوكيل ومسجّل النطاق. ويستطيع مسجّل النطاق اختيار استضافة منطقته بواسطة وكيل مختلف في حالة تحديد أن الوكيل المفوض ليس أهلاً للثقة.

2) ونظرًا لطبيعة DNS المجردة، فإن أي طرف آخر يقوم بتقديم محلل تكراري يشارك في عملية التحليل هو عبارة عن رجل محتمل في منصب متوسط ولديه القدرة على تعديل الرسائل التي يتلقاها من خادم اسم معتمد قبل إرسالها إلى العميل. وقد تكون التعديلات التي يتم إجراؤها على استجابات NXDomain بواسطة أطراف أخرى في أي مرحلة على امتداد مسار عملية التحليل خارج أية علاقة تجارية تتضمن مسجّل النطاق.

3) تستطيع الأطراف الأخرى التي تقوم بتغيير دلالات ومحتوى استجابة DNS القيام بذلك لمصلحتهم الشخصية بدون إخطار وموافقة مسجّل النطاق أو المستخدم الذي قدم الاستفسار.

4) توفر الأطراف الأخرى التي تقوم بتعديل رسائل استجابة NXDomain معلومات حول النطاق تختلف عن المعلومات التي يهدف مسجّل النطاق إلى توزيعها بطرق عديدة هادفة. وتؤكد الاستجابة على أن العنوان (النطاق الفرعي) قد تم تمثيله داخل نطاق ما وتم توجيهه إلى عنوان بروتوكول إنترنت (IP)

معين. ومن منظور مسجّل النطاق، فهذا الاسم غير موجود في منطقته. ومثل هذه الاستجابة تكون غير صحيحة وتحرف أهداف مسجّل النطاق.

5) تؤثر الأطراف الأخرى على الإجراءات التالية للمستخدم الذي قام بصياغة الاستفسار من خلال تضمين ارتباط مع مسجّل النطاق. وإذا كان هدف الطرف الآخر هو الاستفادة من تضمين علاقة بين الطرف الآخر ومسجّل النطاق، فإن هذا قد يكون احتيالاً أو خداعًا أو استخدامًا محظورًا لماركة أو علامة تجارية.

6) يمكن أن تؤثر تعديلات استجابة DNS على تطبيقات أخرى خلاف الويب وبوجه خاص، يمكنها تعطيل البريد الإلكتروني وهاتف الإنترنت وخدمات الإنترنت الأخرى.

7) يمكن أن تؤدي تعديلات استجابة DNS إلى إنشاء استجابات غير متوقعة (مشكلة استقرار اسمية، ولكن قد تتسبب في أسوأ الحالات في هجمات الحرمان من الخدمات).

ونستكشف فيما يلي كيفية تأثير نواحي الأمان والاستقرار هذه على مسجّلي النطاق.

كيف يؤثر تعديل استجابة DNS *على مسجّلي النطاق؟*

في الحالات التي يتم فيها تعديل استجابات NXDomain دون إعلام مسجّل النطاق بوضوح والحصول على موافقته موافقته، لا تعكس رسالة الاستجابة بدقة حالة تشغيل النطاق التي أرادها مسجّل النطاق:

1) ينبغي تقديم تقرير إلى العميل صاحب الاستفسار بعدم وجود اسم ما في ملف منطقة. وبشكل خاص، ينبغي إعادة استجابة تحتوي على رمز الاستجابة *خطأ في الاسم* بواسطة الوكيل المفوض أو الطرف الآخر الذي يقوم بتغيير الرسالة إلى العميل بشكل صامت، ولكنه لا يفعل.
2) تتم كتابة نوع سجلات المورد A في قسم الإجابات الخاص برسالة الاستجابة. ولا يوجد توجيه الاسم إلى العنوان الموضح في سجل المورد هذا في ملف المنطقة المنشور لمسجّل النطاق.

وعند فحص ذلك عن كثب، فهذه ليست مجرد طريقة بديلة لمعالجة حالة خطأ ولكنها تبديل للمحتوى. وعندما يقوم الوكيل المفوض لمسجّل النطاق بإنشاء رسالة استجابة DNS، بغض النظر عن الاستجابة، ينبغي أن يكون لدى الوكيل ومسجّل النطاق كل الأسباب ليتوقعوا أن الوسطاء سيحاولون تقديم المحتوى دون تغيير. فإذا ثبتت صحة هذا الافتراض، قد يتأثر مسجّل النطاق بأي من هذه الطرق المتعددة:

عدم استمرار نقل الاستجابة للمعلومات المقصودة. لن يعمل أي تطبيق أو نشاط إداري يعتمد على استجابات NXDomain للحصول على تشغيل أو تدخل صحيح بعد الآن لجميع العناوين داخل النطاق التي تتم إعادة توجيهها.

تدمير الاستجابة لنموذج التقليدي لثقة النطاق. تقوم المنظمات عادةً باتخاذ قرارات أمنية بناءً على نموذج ثقة ضمني: يثق النطاق الأصل بالنطاقات الفرعية داخل النطاق. تنشأ هذه الثقة الضمنية من افتراض أنه تتم إدارة المضيفين المحددين داخل نطاق منظمة ما بواسطة موظفي تكنولوجيا معلومات النطاق أو وكلائه المخصصين والموثوق بهم. وتوجه استجابة NXDomain التي تم تعديلها المستخدمين إلى خدمات يتم تشغيلها على مضيف يتم تشغيله خارج دائرة التحكم الإداري ونطاق أمان مسجّل النطاق.

تأثير الاستجابة بشكل عكسي على اختبار التوافق والتدقيق. يجب أن تراعي أية منظمة تقوم بإجراء تدقيقات على الأمان -وخاصة المنظمات المطلوب منها ذلك لإثبات التوافق التنظيمي- أن الطرف الآخر قد يضيف على نحو تعسفي مضيف يبدو أنه مسمى بنطاقه ولكن هذا المضيف لن يقع تحت دائرة التحكم الإداري الخاصة به ولن يتم نشر الاسم في منطقته.

إمكانية حدوث حالات عدم استقرار تشغيل DNS نتيجة للاستجابة. ستؤدي عملية تحليل الاسم التي يتم تنفيذها مباشرة إلى خادم الاسم المعتمد الخاص بالنطاق أو من خلال محلل تكراري لا يقوم بتغيير استجابات NXDomain إلى إعادة الاستجابة التي يستهدفها مسجّل النطاق، ولكن قد يعيد الاستفسار نفسه استجابات مختلفة بناءً على ما إذا كان قد تمت معالجته بواسطة طرف آخر يقوم بتعديل استجابات NXDomain أو من خلال أي محلل تكراري أو عقب يقوم بحفظ الاستجابة المعدلة في ذاكرة مؤقتة. قد تنشأ هذه الحالة بعينها في حالة استخدم مسجّل النطاق وكيلين مفوضين لاستضافة ملف المنطقة الخاصة به. فقد يقوم أحد الوكيلين المفوضين بنشر ملف منطقة مسجّل النطاق باستخدام قيد الرمز العشوائي بينما قد يقوم الوكيل الآخر بنشر ملف المنطقة الأصلي (الذي لم يتغير).

زيادة إمكانية تعارض توجيه العناوين. قد يقوم مسجّل النطاق بإضافة نوع سجل مورد A لاسم ما (ww.example.com) إلى ملف منطقته فقط لاكتشاف أن طرف آخر (أو ربما عدة أطراف) قد وجه بالفعل عنوان بروتوكول الإنترنت (IP) إلى هذا الاسم. [ملاحظة: وسيكون هذا صحيحًا بوجه عام بالنسبة لأي نوع سجل يطلبه العميل].

تعرُّض المضيفون في النطاق لأي إصابة ناتجة عن هجوم قد يُستغل من قبل مضيف إعادة التوجيه أو من خلاله. حتى في الحالات التي يكون فيها المضيف المحدد في استجابة NXDomain التي تم تعديلها قد تم تشغيله بواسطة أعمال شرعية (على سبيل المثال، للإعلانات أو لترويج خدمات)، قد يكون هذا المضيف عرضة للهجمات على خادم الويب وتطبيقات الويب أو برمجة عبر الموقع أو عمليات استغلال نظام التشغيل، وبشكل خاص خاص، يستطيع المعتدون إدخال محتوى في أحد نظم مسجّل النطاق من خلال المضيف المحدد في استجابة NXDomain التي تم تعديلها. وهذه الهجمات ليست نظرية. فقد أثبت باحثو الأمان للجمهور أنه من الممكن إدخال لغات برمجة في النطاق الأصل من خلال المضيفين المحددين في استجابات NXDomain التي تم تعديلها (خوادم إدخال الإعلانات).

إضافة الاستجابة مضيفين إلى النطاق ولا يتمكن مشرف مسجّل النطاق من ممارسة التحكم في محتوى هذه المواقع. يستفيد المضيفون المحددون في استجابات NXDomain التي تم تعديلها بواسطة طرف آخر من الاسم التجاري لمسجّل النطاق وسمعته وشيوع الموقع والرابط واتفاقيات الرابط المدعومة مع محركات البحث. ولا يحصل مسجّل النطاق على أية استفادة من هذا النشاط، وفي حالات معينة قد يتضرر أو يعاني منه. على سبيل المثال،

- يمكن أن يقوم طرف آخر بنشر إعلانات على مضيف يحدده في استجابة NXDomain تم تعديلها. وقد تقوم هذه الإعلانات بالترويج لخدمات أو سلع خاصة بمنافسي مسجّل نطاق اسم النطاق.
- تستفيد الشركات التي تم نشر إعلاناتها على مضيف حدده طرف آخر في استجابة NXDomain تم تعديلها من الروابط المدعومة المرتبطة باسم النطاق ومحركات البحث بالكلمات الرئيسية المرتبطة بأعمال مسجّل النطاق.
- يمكن أن يحصل مسجّل النطاق على علاقاته الإعلانية الخاصة به وقد تعمل خدمات الإعلانات المنشورة على مضيف حدده طرف آخر في استجابة NXDomain التي تم تعديلها على إضعاف أو منافسة الإعلانات التي يقوم مسجّل النطاق بنشرها على مضيفي الويب الخاصين به. ويؤثر ذلك على مسجّل النطاق، الذي حيث يتعرض اندماجه مع خدمة إعلانات شريكه للخطر، وشريك الإعلانات، الذي تم الاستيلاء على فرص تحقيقه للإيرادات.
- يمكن أن يقوم المضيف الذي حدده طرف آخر في استجابة NXDomain التي تم تعديلها بنشر حملات إعلانية سلبية أو نشر معلومات غير دقيقة أو مضللة تهدف إحداث أضرار في سمعة مسجّل النطاق.

استجابات NXDomain المعدَّلة ليست مقصورة على سجلات مورد A. وليس مقصوراً على طرف آخر تعديل استجابات NXDomain التي ستساعد على تحليل ما يُفترض أن يكون أسماء مضيف لاستخدامها في اتصالات HTTP؛ حيث يمكن اتصال استجابة NXDomain بطلب لأي سجل مورد من أي تطبيق-يرى محلل DNS جميع ذلك كاسم ونوع سجل في طلب. ويمكن لطرف آخر –نظرياً- تعديل استجابات NXDomain لأية استفسارات بصفة عامة (MX، SRV، NAPTR)، على سبيل المثال، يمكن -نظرياً- إعادة توجيه استفسارات DNS المستخدَمة في البحث عن رقم الإرسال الهاتفي لعنوان بروتوكول الإنترنت (IP) (مثل الطلبات التي تعرض سجل مورد NAPTR) إلى خادم مكالمات خاص باختيار الطرف الآخر.

وتؤدي الاستجابة إلى توفير فرص لإساءة الاستخدام والهجمات. وتتضمن الهجمات التي يمكن القيام بها باستخدام استجابات زائفة:

---

[7] h0h0h0h0 بواسطة دان كامينسكي، على http://www.doxpara.com/DMK_Neut_toor.ppt

[8] صفحات أخطاء ISP للقرصنة، بروس شينير، على الموقع http://www.schneier.com/blog/archives/2008/04/hacking_isp_err.html

- الخداع عبر **إدخال موقع مضلل في نطاقات فرعية مخادعة.** وقد يتمكن المعتدون من استغلال الأبجديات التي يجدونها على المضيف المحدد في استجابات NXDomain المعدَّلة ومهاجمة نظم مسجّلي النطاقات عبر هذه الأبجديات. فعلى سبيل المثال، قد يجد المهاجم أبجدية تقبل الإدخال ولكنه يفشل في تصحيح إدخال معاملات معينة من الأبجدية. ومن خلال إدخال شفرة التنفيذ الخاصة به في هذا المعامل القابل للاستغلال، يستطيع المعتدي خداع زائري الموقع بتنفيذ إصدار مزيف لعملية دفع أو نموذج تسجيل دخول إلى هذا الموقع. ويستطيع المعتدون تطبيق تقنيات مشابهة على نشر إعلانات لافتات تدعو المستخدمين إلى تنزيل برامج ضارة، أو نوافذ منبثقة تدعو المستخدمين إلى تحديث برامج التطبيقات أو برامج نظم التشغيل ولكن هذه التحديثات عبارة عن برامج ضارة وليست نسخًا قانونية.
- **استخلاص البيانات**. يستطيع مضيف إعادة التوجيه مراقبة الحركة وجمع إحصائيات ويب بالزائرين الذين تمت إعادة توجيههم بنفس الطريقة التي قد تتبعها شركة تتبع الإعلانات.
- **استرجاع ملفات تعريف الارتباط بشكل تعسفي.** يستطيع مضيف إعادة التوجيه إيقاف ملفات تعريف الارتباط التي قرر خادم ويب مسجّل النطاق إرسالها إلى العميل ونسخها. وقد يؤدي ذلك إلى كشف معلومات شخصية أو بيانات اعتماد بطاقة ائتمان أو حساب.
- **الهجمات التي تستهدف الماركات.** يقوم الكثير من مسجّلي نطاق اسم النطاق بحماية الماركات والعلامات التجارية من خلال تسجيل الأسماء وقائيًا ضمن TLDs مشابهة بشكل هجومي أو عدواني ومخادع أو مشابهة هجائيًا. ويستطيع المعتدي الذي يقوم باستخدام إدخال الرمز العشوائي إثبات أن العلامات نفسها هي نطاقات فرعية. وبدلاً من كافة استفسارات الاسم هذه والتي تعرض نطاق غير موجود، يمكن توجيه هذه الاستفسارات إلى صفحة ويب مشوهة أو محل دعوى.

وإضافة إلى تأثيرات التشغيل والأمان هذه، ترى SSAC أن إعادة توجيه النطاقات الفرعية قد تثير مشاكل تتعلق بالملكية الفكرية والعلامات التجارية. وتستحق هذه المشاكل –التي تقع خارج نطاق خبرة SSAC- المناقشة من جانب الأطراف المؤهلة حيث ينبغي دراسة هذا الموضوع بشكل إضافي.

[9] تحليل هجوم البرمجة عبر الموقع (XSS): استغلال التأثير والاستجابة، روس ماكري، صحيفة ISSA، يونيو 2008 الصفحة من 12 إلى 14.

المراجعات المتنافسة

يعد تعديل استجابة DNS نفسه موضوعًا يحتاج إلى تعديل. وقد تمت الإشارة إلى هذه الظاهرة *بالمراجعات المتنافسة* ويمكن تلخيصها كما يلي:

1) يقوم مستخدم -شادي مثلاً- بتسجيل النطاق example.tld عبر المُسجل س.

2) يستخدم مسجّل النطاق example.tld خدمة DNS التي يقدمها المُسجل س، لاستضافة ملف المنطقة example.tld.

3) يستخدم الكمبيوتر الخاص بشادي NS1.mylocalisp.tld كخادم الاسم الافتراضي لديه.

4) يقوم شادي بفتح إطار متصفح من كمبيوتر 1 ويحاول الاتصال بـ ww.example.tld. وقد أخطأ خطئًا هجائيًا في كتابة www.example.tld، الذي يعد اسم المضيف الذي استخدمه مسجّل النطاق للعنوان المستخدم في توصيل خادم الويب الخاص به ببروتوكول HTTP.

5) يقوم NS1.mylocalisp.tld بإجراء عملية تحليل لتحليل ww.example.tld؛ حيث يقوم أولاً بالاستفسار عن خادم اسم جذر للامتداد tld، ثم الاستفسار عن خادم الاسم لـ example.tld، وأخيرًا الاستفسار عن خادم اسم المُسجل س لـ ww.example.tld.

6) يعرض خادم اسم المُسجل س استجابة DNS إيجابية بدلاً من استجابة NXDomain لـ ww.example.tld. وتحتوي هذه الاستجابة على سجل A في تخطيط قسم الإجابة ww.example.tld لـ a.b.c.d.

7) يعمل NS1.mylocalisp.tld على إيقاف استجابة DNS للمُسجل س، ويتعرف على إعادة توجيه العنوان a.b.c.d كصفحة إعلانية من تحليل سابق لحركة مرور DNS.

8) يحل NS1.mylocalisp.tld محل معلومات إعادة التوجيه الخاصة به ويُظهر استجابة DNS إيجابية تحتوي على سجل A في تخطيط قسم الإجابة ww.example.tld لـ a.x.y.z.

9) يقوم شادي بفتح إطار متصفح من كمبيوتر 1 ويحاول الاتصال بـ ww.example.tld على a.x.y.z.

نتائج تمهيدية

تقدم SSAC النتائج والملاحظات التمهيدية التالية، فيما يتعلق بممارسة تعديل استجابة DNS.

1) قد يقوم مزودو طرف آخر بتعديل استجابات NXDomain على أي محلل تكراري، على مدى المسار بين عميل وخادم الاسم المعتمد لأحد النطاقات. وقد يقوم الوكلاء المفوضون بتضمين قيود الرمز العشوائي في ملف منطقة خاص بمسجّل نطاق، وعرض توجيه هذا العنوان بدلاً من عرض *خطأ في الاسم*.

2) تعمل إعادة توجيه تعديل استجابة NXDomain الخاصة بطرف آخر، على إحداث مشاكل تشغيل وأمان لمسجّلي النطاق والتي لا يمكن حلها بسهولة حتى من خلال استضافة خدمة اسم أحدهم.

3) يمكن أن يؤدي تعديل استجابة NXDomain والاستجابات المركبة إلى حدوث مشاكل أمان لمسجّلي النطاق. وبخاصة، لا يمكن الوثوق بعلاقة الثقة بين نطاق رئيسي والنطاق الفرعي التابع له. وقد ينتج عن تدهور علاقات الثقة تأثير ضار على مراجعة الأمان واختبار التوافق.

4) يمكن أن يؤدي تعديل استجابة NXDomain والاستجابات المركبة إلى توفير فرص للهجمات الضارة ضد مسجّل النطاق وفرص للمعتدين لاستغلال أصول نطاق مسجّل النطاق للأغراض الضارة أو الإجرامية.

5) يكون تعديل استجابة NXDomain والاستجابات المركبة معرضة للتعديل بواسطة أطراف أخرى تقوم بتعديل استجابات NXDomain التي تتلقاها.

6) يعد الوكلاء المفوضون الذين يقومون بتركيب الاستجابات والأطراف الأخرى التي تقوم بتعديل NXDomain معروفون ومتشابهين لا متناقضين. تمارس أطراف أخرى معينة تعديل استجابة NXDomain مباشرة أو من خلال *شركاء تحليل الخطأ*.

7) لا يجوز للوكلاء المفوضين والأطراف الأخرى كشف حقيقة أنهم يمارسون تعديل استجابة DNS بطريقة واضحة وجلية، وعندما يقومون بكشف الممارسة، لا يجوز لهم كشف التأثيرات الضارة المحتملة التي قد تكون لهذه الممارسة على مصالح مسجّل النطاق. ويقوم مزودون محددون بإرسال إخطار بأنهم سيقومون بممارسة حقهم في إجراء تحليل خطأ أو إعادة توجيه؛ كشرط تنص عليه اتفاقية الخدمة ولا تكون هناك فرصة لاستثناء مسجّل نطاق إلا أن يختار مزودًا آخر.

8) لا تشير استجابات NXDomain فقط إلى حالة خطأ من مسجّل النطاق، ولكنها تنقل المحتوى، وفقًا للقيود الموجودة في ملف منطقة. ويجب عدم التمييز في معاملة هذا المحتوى عن أي محتوى تطبيق آخر.

9) تصل آثار تعديل الاستجابة لأبعد من تطبيقات الويب. وبشكل خاص، تمثل عمليات الاستبدال والإدخال التي تتم في البريد الإلكتروني والصوتي عبر خدمات الإنترنت أرضًا خصبة لعمليات الاستغلال المشابهة.

قد يثير تعديل استجابة DNS مشاكل تتعلق بالملكية الفكرية والعلامات التجارية.

[10] يُحدد مشاركون محددون في هذا النشاط سوق أخطاء عالمي سنوي يصل إلى ما يزيد عن 1 بليون دولار، http://barefruit.com/services.htm

توصيات تمهيدية

تضع SSAC التوصيات التمهيدية التالية.

1) أوصت SSAC مرارًا وتكرارًا بعدم تركيب استجابات DNS على مستوى TLD. ولا يجب ممارسة إجراءات مشابهة على مستويات النطاق الفرعي.

2) يستطيع مسجّلو النطاق التحكم في كيفية إجابة وكيل مفوض على استفسار لاسم غير موجود في ملف المنطقة الخاص به، عبر علاقة ثقة وعمل. وبشكل أكثر تحديداً، ينبغي أن يوضح مسجّل النطاق ما إذا كانت خوادم الاسم المعتمدة لديه تعرض أخطاء اسم أم استجابات مركبة.

3) ينبغي أن يستفسر مسجّلو النطاق عن كيفية معاملة الوكلاء المفوضين لنطاقاتهم الفرعية غير المسجّلة. تتفق SSAC مع IAB وتوصي بضرورة عدم استخدام الوكلاء المفوضين للرموز العشوائية الخاصة بـ DNS في منطقة بدون إعلام مسجّل النطاق بالمخاطر المحددة في هذا التقرير وفي مكان آخر، وأنه ينبغي على الوكلاء المفوضين عدم إنشاء الرمز العشوائي واستجابات مركبة بدون موافقة مطلعة من مسجّل النطاق، وأنه ينبغي على الوكلاء المفوضين تقديم آليات اختيار تسمح للعملاء باستلام إجابات DNS الأصلية على استفساراتهم.

4) ينبغي على الأطراف الأخرى إعلان أنهم يقومون بممارسة تعديل استجابة NXDomain وتوفير فرص للعملاء للاختيار.

5) ينبغي أن تقوم المنظمات التي تعتمد على تقارير NXDomain الدقيقة لاستقرار التشغيل باختيار وكيل مفوض، يؤكد أنها لن تقوم بتعديل استجابات DNS في شروط الخدمة الخاصة بها.

6) ينبغي أن يقوم مسجّلو النطاق بدراسة طرق تقديم دليل معتمد من طرف لطرف للنطاقات الفرعية غير الموجودة، مثل امتدادات أمان DNSSEC[11]. كما ينبغي أن تحاول المنظمات بشكل أكبر تقليل مستوى التعرُّض لتعديل استجابة NXDomain باختيار أطراف موثوق بها لتوفير محللين تكراريين حتى لا يتم تخطيط الاستفسارات من عملاء المنظمة عبر مزودي تحليل اسم عشوائي الذين قد يقومون بإعادة توجيه نطاق فرعي.

.

[11] RFC 4033، مقدمة أمان DNS والمتطلبات، http://rfc.net/rfc4033.html

[12] RFC 4034، سجلات مورد امتدادات أمان DNS، http://rfc.net/rfc4034.html

[13] RFC 4035، تعديلات بروتوكول امتدادات أمان DNS، http://rfc.net/rfc4035.html

[14] RFC 5155، أمان DNS (DNSSEC)، رفض التواجد المعتمد المبعثر، http://rfc.net/rfc5155.html

العمل المستقبلي

تستحق الآثار التجارية والاقتصادية والأمنية والتشغيلية الخاصة بإعادة توجيه النطاق الفرعي مزيدًا من الاهتمام. ويبدو من خلال معرفتنا أن تعديل استجابة DNS مقصور بشكل كبير على التطبيقات التي تعتمد على الويب، كما أن مشكلة معرفة مدى تأثيره على الخدمات التي تعتمد على بروتوكول الإنترنت (IP) تستحق مزيدًا من الدراسة. وتشجع SSAC المجتمع على التفكير في التداعيات الكبيرة لتغيير الاستجابات السلبية إلى فرص كسب إيرادات دون التفكير في نتائج التشغيل ودون التفكير في رغبات كل من مسجّلي النطاق أو العملاء الخاصة ببيانات DNS. وبشكل أساسي، تعمل بعض الممارسات مثل تحليل الخطأ و"أسواق الخطأ" على تمكين مجموعة من الإجراءات التي تثير بعض القلق من خلال تقديم الغموض والتغير في النماذج التقليدية لإدارة الخطأ والثقة. ولا يتضح ما إذا كانت ستمتد آثار هذه الممارسات لتصل إلى خدمات البريد الإلكتروني والصوتي والخدمات المساعدة، أو حتى العناوين والتوجيه وعمليات تشغيل الإنترنت الأساسية الأخرى، وبالمثل ليس واضحًا مدى خطورة تأثير هذه الأنشطة على الاتصالات التي تعتمد على بروتوكول الإنترنت (IP).