SAC 056

استشارة SSAC حول تأثيرات حجب المحتويات عن طريق نظام أسماء النطاقات

استشارة صادرة عن اللجنة الاستشارية
للحماية والاستقرار (SSAC)
التابعة لـ ICANN

09 أكتوبر 2012

تمهيد

هذه استشارة من من اللجنة الاستشارية للحماية والاستقرار (SSAC). تقدم SSAC المشورة إلى مجتمع ICANN ومجلس إدارتها حول المسائل المتعلقة بحماية وسلامة أنظمة تخصيص تسمية وعناوين الإنترنت. وهذا يتضمن الأمور التشغيلية (على سبيل المثال، الأمور المتعلقة بالتشغيل الصحيح والموثوق لنظام اسم الجذر)، والأمور الإدارية (على سبيل المثال، الأمور المتعلقة بتخصيص العناوين وتعيين أرقام الإنترنت)، وأمور التسجيل (على سبيل المثال، الأمور المتعلقة بخدمات السجل والمسجل). تشترك SSAC بشكل متواصل في تقييم التهديدات وتحليل مخاطر خدمات التسمية وتخصيص عناوين الإنترنت للوقوف على مكمن التهديد الرئيسي الذي يواجه الاستقرار والأمن، وتقدم توصياتها إلى مجتمع ICANN بناءً على ذلك. ولا تتمتع SSAC بالسلطة الرسمية للتنظيم أو التطبيق أو الحكم. إن هذه وظائف جهات أخرى، ويجب أن يتم تقييم المشورة المقدمة هنا بناءً على مزاياها.

ويمكن إيجاد المساهمين في هذه الاستشارة، ومرجع إلى السيرة الذاتية لأعضاء اللجنة وبيانات اهتماماتهم، واعتراضات أعضاء اللجنة على النتائج أو التوصيات في هذه الاستشارة، في نهايتها.

جدول المحتويات

1. ملخص تنفيذي

لقد أصبح استخدام حجب نظام أسماء النطاقات (DNS) لتقييد الدخول إلى الموارد على الإنترنت موضوع اهتمام في العديد من أوساط حوكمة الإنترنت. لقد نفذت عدة حكومات حول العالم حجب DNS عن طريق القوانين أو المعاهدات أو أوامر المحكمة أو الإجراءات القانونية أو إجراءات أو اتفاقيات أخرى، أو تفكر بجدية بفعل ذلك. ولكن بسبب هندسة الإنترنت التركيبية، يمكن للمستخدمين النهائيين تخطي حجب النطاق بسهولة، وبالتالي، من المحتمل أن يكون غير فعال على المدى الطويل ومليئاً بالعواقب غير المدروسة على المدى القصير. بالإضافة إلى ذلك، يمكن أن يؤدي حجب DNS إلى صراعات مع تبني امتدادت حماية DNS (أو DNSSEC)، وقد يروج لبلقنة الإنترنت بحسب نظرة كل دولة لمساحة أسماء الإنترنت.

تقتصر هذه الوثيقة على إمكانية استكشاف التأثيرات الفنية المرتبطة بحجب DNS، بما في ذلك:

- حجب النطاق عن طريق مايلي:
  - السجل أو المسجل،
  - مخدم مفوض،
  - في محلل دوري عن طريق إعادة التوجيه، أو اسم انطاق غير موجود أو رمز استجابة رفض الاستعلام أو رموز الاستجابة الأخرى أو عدم الاستجابة للاستعلام.
- حجب DNS في المحللات الدورية والصراعات مع DNSSEC،
- تكييف المستخدمين النهائيين نحو تشفير أكثر من الطرف للطرف،
- الحجب الزائد عن اللزوم،
- الأخطاء الطبوغرافية،
- توجيه حركة مرور DNS بعيداً عن دولة تفرض الحجب،
- تأثيرات محللات تحويل المستخدمين، و
- مخالفة التحويل المحلي لشبكة توزيع المحتويات (CDN) إذا قام المستخدمين بتحويل المحللات.

رغم أن ثمة مسائل غير فنية مثل القيود على حرية التعبير، لن تتم مناقشة هذه المسائل في هذه الوثيقة. ينبغي على مجتمع الإنترنت والحكومات وجهات أخرى ضمان أن تفهم وتأخذ بعين الاعتبار جميع المسائل المرتبطة بحجب DNS، من الناحيتين الفنية وغير الفنية.

2. مقدمة

هذه الوثيقة هي مبنية على "SAC050: حجب DNS: المزايا مقابل الأضرار – استشارة من لجنة الحماية والاستقرار الاستشارية"، والتي قد تثير اهتمام قراء هذه الوثيقة.[1]

[1] راجع "SAC050: حجب DNS: المزايا مقابل المساوىء – استشارة من لجنة الحماية والاستقرار الاستشارية" حول حجب أسماء نطاقات المستوى الأعلى على مستوى اسم النطاق"، هيئة الإنترنت لتعيين الأسماء والأرقام (ICANN)، لجنة الحماية والاستقرار الاستشارية http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf.

في عامي 2011 و2012، اقترحت عدة حكومات أو وضعت إرشادات رسمية أو قوانين أو أوامر محكمة أو إجراءات تطبيق قانون مرتبطة بحجب DNS أو فلترة DNS و/أو مصادرة اسم النطاق.[2] في بعض الحالات، كان الهدف من هذه الأنشطة هو وضع تشريعات جديدة تهدف إلى السيطرة على استخدام الإنترنت، بينما في حالات أخرى، اعتمدت المحاكم أو وكالات تطبيق القانون على حجب DNS أو مصادرة أسماء النطاقات كآلية لحجب الدخول إلى مواقع إلكترونية أو عناوين إنترنت معينة .[6,5,4,3]

تناقش هذه الوثيقة التأثيرات الفنية للأنواع المختلفة لحجب DNS التي تم تنفيذها أو اقتراحها. إن هدف هذه الوثيقة هو اطلاع مجتمع الإنترنت وصانعي السياسة ومسؤولي الحكومات وآخرين على التضمينات الفنية ذات المستوى العالي لاستخدام حجب DNS للسيطرة على الدخول إلى موارد الإنترنت.[7]

3. حجب DNS: المزايا مقابل الأضرار

الاستنتاجات الرئيسية لـ SAC050 هي:

> "قد تعتبر بعض المنظمات أن فلترة اسم النطاق أو عنوان بروتوكول الإنترنت (أو منع الدخول إليها مثل محتويات الإنترنت التي تنقل الفيروسات إلى الكمبيوترات أو تعتبر ذات استخدام غير لائق لموارد صاحب العمل) على أنها امتداد طبيعي للسياسات التاريخية التي تحجب الأشخاص ضمن هذه المنظمات من مراكمة الرسوم الهاتفية.
>
> بغض النظر عن الآلية المستخدمة، يجب أن تطبق المنظمات التي تنفذ الحجب المبادىء التالية:
>
> 1. تفرض المنظمة سياسة على الشبكة ومستخدميها تمارس من خلالها الضبط الإداري .(أي تصبح إداري نطاق السياسة)
> 2. تحدد المنظمة أن السياسة هي مفيدة لأهدافها ومصالح مستخدميها.
> 3. تنفذ المنظمة السياسة باستخدام أسلوب أقل تعطيلاً لعمليات شبكتها ومستخدميها، ما لم تحدد الأنظمة أساليب معينة.
> 4. تبذل المنظمة جهوداً مركزة لعدم التسبّب بأضرار على شبكاتها أو مستخدميها خارج نطاق سياستها كعواقب لتنفيذ السياسة.
>
> عندما لا يتم تطبيق هذه المبادىء، يمكن أن يسبّب حجب استخدام DNS أضراراً جانبية أكثر أو عواقب غير مقصودة بلا توفر حل للأطراف المتأثرة."

---

[2] راجع H.R. 3261 (قانون منع القرصنة عبر الإنترنت), مجلس الشيوخ الأمريكي، الكونغرس 112، الإصدار مؤرخ في 16 ديسمبر 2011، والقانون الإستوني المتعلق بحجب مواقع المقامرة غير القانونية، https://www.riigiteataja.ee/akt/125042012010.

[3] راجع مبادرة أوبين نيت, http://opennet.net/youtube-censored-a-recent-history.

[4] راجع http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/.

[5] راجع http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6] راجع http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

[7] لرؤية وصف لـ DNS، راجع http://queue.acm.org/detail.cfm?id=1242499.

للإضافة إلى استنتاجات SAC050، يتطلب كلاً من الرعاية الواجبة واستقرار الإنترنت الإجمالي أن يتم الكشف عن أية سياسة أو إجراء حجب DNS بشكل كامل للأطراف المتأثرة، بمن فيهم المستخدمين النهائيين ومزودي الخطمة ومصممي البرامج. إن حجب DNS بظل غياب مثل هذا الكشف سيؤدي إلى أنشطة حل مشكلات غير ضرورية، بالإضافة إلى أنشطة تجاوز تكيفية وربما غير مقصودة، من قبل مشغلي الشبكة والمستخدمين النهائيين .يجب أن يتضمن مثل هذا الكشف الدوافع والتأثيرات المقصودة والآثار الجانبية المتوقعة .بظل غياب مثل هذه الشفافية، يمكن إساءة تشخصي حجب DNS على أنه انقاطع أو هجمة خبيثة، مما قد يؤدي إلى استجابات من المستخدمين النهائيين وإداريي الشبكة ومزودي الخدمة وما إلى ذلك تحاول تخفيف الأضرار.

قد يؤدي احتمال سوء التشخيص هذا والبحث الحتمي عن أساليب الالتفاف إلى أضرار جانبية أو عواقب غير مقصودة. كما تمت المطالبة بمراجعة عامة مستقلة في تقرير مكتب المفوضية السامية للأمم المتحدة لحقوق الإنسان من المبعوث الخاص للترويج وحماية حق حرية الرأي والتعبير، الذي ينص على مايلي:

> "31. [...] ثالثاً، حتى عند تقديم تبريرات، تشكل إجراءات الحجب وسيلة غير ضرورية أو غير مناسبة لتحقيق الهدف المرجو، لأنها لا تكون مستهدفة بشكل كافٍ غالباً، وتمنع الوصول إلى مجموعة كبيرة من المحتويات لأكثر مما يتم اعتباره قانونياً. مؤخراً، غالباً ما يتم حجب المحتويات من دون تدخل أو إمكانية مراجعة هيئة قضائية أو مستقلة لها". [8]

إن استطلاع أنواع وتأثيرات حجب DNS هو موضوع بقية هذه الوثيقة.

4. حجب المحتويات ضمن سياق هندسة الإنترنت التركيبية

أحد المعتقدات الأساسية في هندسة الإنترنت التركيبية هو تجريدها "من طرف إلى طرف"، والذي يحد من الحاجة إلى الذكاء في صميم (وسط) الشبكة، ولكنه يعتنق الذكاء عند الطرف (عند المستضيف الفردي). لقد ساعدت هذه الهندسة التركيبية على تمكين مستوى وعمق هائلين للابتكار، مثل السماح للمبرمج عند أحد أطراف الشبكة بنشر برنامج جديد على المستضيف، بينما يقوم مستخدم نهائي على الطرف الآخر بتثبيت العميل المتوافق لتمكين أشكال جديدة من الاتصالات، من دون تطلب أي إذن أو ضوابط خاصة ضمن أي جزء آخر من الشبكة.

لقد تم تنفيذ حجب المحتويات عبر نظام أسماء النطاقات في "صميم" الإنترنت أحياناً وعند "طرف" الإنترنت في أحيان أخرى. إن الوصلات بين مزود الولوج وموارد حركته المرورية ومهابط الحركة المرورية تسمى "الطرف". بينما يسمى المشغلين الداخليين أو بينهما "الصميم". من الأمثلة على الحجب المبني على الطرف القوائم السوداء في متصفحات الإنترنت وفلترة حركة بروتوكول الإنترنت عند أحد أطراف الاتصال. إذا تم تطبيق الحجب ذو نمط الطرف على صميم الشبكة، يمكن للمستخدمين النهائيين المتأثرين تجاوز الحجب عن طريق تغيير مزودي DNS أو استخدام VPNs أو البروكسي أو القوابس. لن يكون الحجب المبني على الطرف فعالاً إلا بوجود الفلترة المبنية على السياسة في جميع المسارات الممكنة بين المستخدمين النهائيين المتأثرين وأية شبكات قد يتبادلون الباقات معها. من الأمثلة على مثل هذه الأنماط الهندسية الجدران النارية على مستوى الدولة والمؤسسات.

كأثر جانبي لهذه الهندسة التركيبية، من الممكن التحايل على جهود حجب الحركة المرورية، سواء بحسب اسم النطاق (مثل example.com) أو عنوان بروتوكول الإنترنت (مثل 192.0.2.117), في أية مرحلة من الشبكة عدا عن الطرف، عن طريق استخدام شبكة افتراضية خاصة (VPN) على سبيل

[8] فرانك لا ريو، "تقرير المبعوث الخاص للترويج وحماية حق حرية الرأي والتعبير," A.HRC.17.27.، http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

المثال.[9] تتوفر شبكات VPNs وأساليب مشابهة بجاهزية وسهولة لكي يتبناها حتى المستخدمين غير الفنيين نسبياً. حتى في الحالات التي تكون بها السيطرة الإدارية والتشغيلية الكاملة على شبكات الإنترنت ممكنة (مثل مزود خدمة الإنترنت (ISP) أو عند بعض نقاط تبادل المستخدمين[10])، يظلبوسع المستخدمين النهائيين الدخول إلى المحتويات المحظورة.[11]

إن الخصائص المشتركة للأنواع الأنجح من الفلترة هي أن يتفق المستخدم النهائي ومشغل شبكته بشكل صريح أو ضمني على ما ينبغي تنقيته وكيفية القيام بحجب المحتويات. في هذه الحالة، سيعتبر المستخدم النهائي أن حجب DNS هو خدمة قيمة.

5. أنواع حجب DNS الملحوظة أو المقترحة

لقد تم اقتراح أو تنفيذ أساليب متنوعة لحجب DNS في السنوات الأخيرة. وتثير بعض الأساليب مخاوف فنية أكثر من غيرها. تشتمل القائمة الجزئية على:

1. **مصادرة النطاق بواسطة السجل أو المسجل**: يزيل هذا الأسلوب بيانات DNS من مصدره عن طريق عمل سجل أو مسجل DNS كوكيل للسجل. السجل هو الهيئة المسؤولة عن إنشاء قاعدة بيانات مفوضة لبيانات DNS، بما في ذلك النطاقات التي يجب حجبها. أحد الأمثلة على هذا الأسلوب هو تنفيذ الحكومة لأمر "مصادرة" اسم نطاق لمسجل أو سجل يخضع قانونياً لمثل هذا الأمر. تتوقف استجابة السجل أو المسجل لمثل هذه المصادرة على مواصفات الأمر. تتضمن الخيارات إزالة اسم النطاق من المنطقة (التي تسمى "مصادرة النطاق" عند حفظ بيانات التسجيل لذلك النطاق)، وبالتالي، منع المستخدمين النهائيين من حل اسم النطاق المرتبط بموقع معين، أو توجيه اسم النطاق إلى مخدم اسم مرتبط سيقوم عندها بإعادة توجيه المستخدمين إلى صفحة إلكترونية تعرض معلومات إضافية مثل إشعارات تطبيق القانون للمصادرة. في موقف "مصادرة النطاق"، حالما تنتهي صلاحية إعدادات "فترة عمر" سجل DNS، على مدار بضعة ساعات أو أيام عادةً، يصبح النطاق غير قابل للحل عالمياً. هذا يعني أنه عندما يطبع مستخدم في اسم النطاق ذاك، سيحصل على استجابة "اسم النطاق غير موجود". إذا تمت مصادرة أسماء النطاقات الصحيحة، لن يكون ثمة تضمينات فنية سلبية متميزة بأسلوب "مصادرة النطاق". يمكن أن تتضمن التضمينات الفنية السلبية غير المباشرة حدوث عطل بالمخادم البعيدة إذا كان ثمة أسماء نطاقات تابعة لخدمة الاسم أو خدمة البريد الإلكتروني في موضوع النطاق لمثل هذه "المصادرة". في كلٍ من أسلوب تغيير "مصادرة الام" أو "مخدم الاسم"، ينبغي على السجل أو المسجل تحديث أو إزالة أية بيانات DNSSEC للنطاق المستهدف. إن عدم فعل ذلك سيؤدي إلى جعل البرامج المتوافقة مع DNSSEC كشف بيانات غير صالحة استجابة لاستعلامات DNS التي ستوقف جميع الاتصالات، حتى تلك التي تهدف إلى الشرح للمستخدمين سبب عدم وجود النطاق.
2. **حجب النطاق في مخدم مفوض: هذا النوع من الحجب**، الذي يتم تنفيذه من قبل مشغل مخادم الاسم المفوضة لاسم النطاق المتأثر، يتخطى السجل وكذلك المسجل على الأرجح، ويستهدف مباشرة الآلية التي يتم توفير اسم النطاق من خلالها عبر الإنترنت. حالما يحصل المشترك على اسم نطاق ويقوم بتهيئته بشكل صحيح، سيقوم السجل باستخراج بيانات DNS ونشرها إلى مجموعة من "المخادم المفوضة". يتولى المسجل تشغيل هذه المخادم المفوضة، ولكن هذا ليس أمراً متطلباً، ولا من المتطلب أن تكون جميع المخادم المفوضة من تشغيل الهيئة نفسها. بغض النظر عمن يتولى تشغيل المخادم المفوضة، فإن المخادم هي آلية نشر، وبالتالي، نقطة يمكن تنفيذ

[9] راجع http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html أو http://vpn-account.com/bypassblockedsites.html.

[10] راجع http://en.wikipedia.org/wiki/Internet_exchange_point.

[11] راجع http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter.

حجب DNS بها. أحد الأمثلة على هذا النوع من الحجب هو تنفيذ الحكومة لأمر مصادرة لمشغل مخدم DNS مفوض لاسم النطاق المستهدف. ثم سيقوم هذا المشغل بإزالة أو تعديل نسخته عن سجلات DNS المفوضة لاسم النطاق ذاك. على افتراض إرسال طلب المصادرة إلى جميع المخادم المفوضة للنطاق وتنفيذها له، سيصبح النطاق غير موثوق على الفور على أساس عالمي، وسيصبح غير قابل للحل في النهاية بعد انتهاء صلاحية فترة عمره. بالإضافة إلى الهيئات المختلفة التي تنفذ الحجب، يختلف هذا الأسلوب عن الحجب المبني على السجل/المسجل من ناحية أنه قد يؤدي إلى صعوبات إذا تم استخدام DNSSEC لأن مشغل المخدم المفوضلن يتمكن من الحفاظ على تواقيع DNSSEC المميزة للسجل عند تعديل محتويات نطاق السجل.

3. **حجب النطاق في محلل دوري**: المحللات الدورية هي مكان شائع لتنفيذ حجب DNS بعدد من الأدوات (مثل المصدر المفتوح والتجاري) الذي يسمح لمشغلي المحلل بتنفيذ الحجب بسهولة.[12] ولكن بسبب هندسة DNS التركيبية، فإن أسلوب الحجب في المحلل الدوري هو من بين أسهل الأساليب التي يمكن تجاوزها. تتم إدارة المحللات الدورية عادة من قبل مزودي الإنترنت للمستخدمين النهائيين، لإحضار بيانات DNS من المخادم المفوضة عند طلب المستخدمين النهائيين ذلك. عندما يرغب المستخدم النهائي بالاتصال مع موقع إلكتروني أوخدمة أخرى، سيترجم المحلل الدوري الذي يخدم ذلك المستخدم النهائي اسم نطاق ذلك الموقع أو الخدمة إلى عناوين بروتوكول إنترنت. يهدف حجب DNS عن طريق المحللات الدورية إلى فلترة أو تحرير أو حجب هذه الترجمة، ويمكن القيام بها بعدة وسائل:

   أ. **عن طريق إعادة التوجيه**: في هذا الشكل من الحجب عن طريق المحلل الدوري، يتم تعديل نموذج الاستجابة من لمخدم المفوض لاستبدال القيم المحددة من قبل سياسة حجب DNS. على سبيل المثال، بدلاً من إعادة عنوان بروتوكول الإنترنت لمخدم الموقع الإلكتروني المسيء، سيعيد المحلل الدوري عنوان بروتوكول الإنترنت لمخدم معالجة يعرض رسالة تشير إلى أنه قد تم حجب الموقع.[13]

   يتطلب هذا الشكل من الحجب مخدم معالجة لدعم أية بروتوكولات أوخدمات مدعومة من قبل المخادم الأصلية المستهدفة التي سيكون عرض راية إعادة توجيه عليها شبه مستحيل. أي، إذا كان المستهدف بالحجب يستخدم بروتوكول نقل الملف (FTP) لتوفير المحتويات، ينبغي أن يحتوي المخدم الذي يتم تحويل المستخدم إليه FTP أيضاً من أجل عرض الراية.[14] بسبب طريقة عمل بعض البروتوكولات، قد لا يكون هذا النوع من إعادة التوجيه مجدياً في جميع الحالات.[15] ولكن للبروتوكولات الشائعة مثل بروتوكول نقل النص الفوقي (HTTP)، وهو البروتوكول المحوري لشبكة الإنترنت العالمية)، يمكن تحقيق هذا النوع من إعادة التوجيه.

   ب. **عن طريق رمز استجابة اسم نطاق غير موجود (NXDOMAIN)**: كما هو الحال مع إعادة التوجيه، يقوم هذا النوع من الحجب بتعديل الاستجابة من المخدم المفوض،

---

[12] راجع http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ and http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/.

[13] راجع http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf.

[14] راجع "بروتوكول نقل الملفات" على http://en.wikipedia.org/wiki/File_Transfer_Protocol.

[15] راجع "إعادة التوجيه في نطاقي COM وNET (9 يوليو 2004)"، , اللجنة الاستشارية للحماية والاستقرار التابعة لـ ICANN على http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf.

ولكن بدلاً من إعادة عنوان بروتوكول الإنترنت، يتم تعديل الاستجابة للإشارة عدم وجود اسم النطاق المستهدف.

ج. **عن طريق رمز الاستعلام مرفوض**: يمتلك بروتوكول DNS رمز استجابة، مرفوض، وهو يهدف إلى الإشارة إلى أن النطاق غير قابل للحل لأسباب إدارية .يمكن تنفيذ حجب DNS عن طريق تغيير الاستجابة من مخدم مفوض إلى استجابة مرفوض للنطاقات المحجوبة .

أحد التفسيرات الصالحة والمنطقية تماماً لمواصفات بروتوكول DNS هو أن رموز استجابة مرفوض تشير إلى أنه ينبغي عدم استعلام مخدم الاسم على الإطلاق، مما قد يؤدي إلى إزالة نظام التشغيل لذلك المحلل الدوري من قائمته لمخادم الاسم .ويرجع السبب بهذا إلى أنه يتم تفسير استجابة مرفوض على أنها مشكلة بالسيطرة على الدخول للعميل ولجميع أسماء النطاقات المطلوبة من قبل ذلك العميل، بدلاً من رفض الاستجابة لاسم نطاق معين ما. مع عدد كافٍ من استعلامات المستخدم النهائي، قد يؤدي هذا النوع من الحجب إلى إزالة جميع مخادم الاسم المستخدمة من قبل المستخدم النهائي، مما يجعل كمبيوتر المستخدم النهائي عاجز .على استعلام أي اسم (أو غير قادر) بالتالي، من المرجح أن تؤدي المحللات التي تعيد استجابة مرفوض لاسم نطاق يتم حجبه إلى أضرار جانبية غير مقبولة.

د. **عن طريق رموز استجابة أخرى:** ثمة رموزاستجابة إضافية محددة في بروتوكول DNS يمكن استخدامها للإشارة إلى أن ذلك النطاق غير قابل للحل، مما يشير عادة إلى حدوث خطأ من نوع ما. تتضمن رموز الاستجابة هذه "فشل المخدم" (SERVFAIL)، و(NOTIMPL) "لم يتم التنفيذ"، و "خطأ تنسيق" (FORMERR).

كما هو الحال مع استجابة مرفوض، قد يؤدي الحجب عن طريق رموز الاستجابة هذه إلى إعلان نظام التشغيل أن المحلل الدوري غير عامل وإزالته من قائمة أسماء المخادم الدورية التي يستعلمها نظام التشغيل .لهذا السبب، لا تناسب أي من هذه الاستجابات البديلة حجب DNS.

ه. **عن طريق عدم استجابة الاستعلام**: في النهاية، ينبغي تهيئة المحلل الدوري لتجاهل الاستعلامات للنطاق المطلوب .قد يؤدي هذا إلى محاولة البرامج للاتصال مع الموقع المحجوب لإعادة محاولة الحل عن طريق تكرار الاستعلام المتعدد.

كما هو الحال مع استجابة مرفوض ورموز الاستجابة الأخرى، يمكن أن يزيل نظام التشغيل المحلل الدوري من قائمة أسماء المخادم الدورية التي يستعلمها نظام التشغيل. ولكن على عكس الحجب عن طريق رموز الاستجابة المبينة أعلاه، سيؤدي الحجب بعدم إعادة استجابة إلى تجربة مستخدم نهائي أسوأ كثيراً لأن على البرنامج انتظار انتهاء توقيت جميع عمليات البحث .قد يشجع هذا المستخدمين على التغيير إلى محللات دورية بديلة، وربما استخدام المخادم غير المغطاة بأمر المصادرة أو سياسة الحجب المرغوبة.

إن إعادة تهيئة المحللات الدورية هو تابع لنظام التشغيل، ولكنه عادة ما يتطلب عدداً صغيراً من النقرات في واجهة المستخدم الغرافية أنظمة التشغيل "برامج" نم ديدعلاو ،"تفضيلات النظام" تشغيل الأنالتي تقوم بظمة والأجهزة الذكية على حد سواء من هذه العملية عملية بنقرة واحدة. في معظم الحالات تقريباً، تكون إعادة التهيئة هذه ضمن قدرات الجميع ما عدا المستخدمين غير المطلعين على الأمور الفنية.

كما ذكرنا سابقاً، فإن الحجب عن طريق المحللات الدورية هو شكل شائع من أشكال حجب DNS المستخدمة اليوم، ولكن يمكن للمستخدمين النهائيين تجاوز هذا النوع من الحجب عن طريق استخدام محلل دوري لا ينفذ الحجب، مثل محلل "مفتوح" يقبل الاستعلامات من أي مصدر عنوان بروتوكول إنترنت [16] أو عن طريق تشغيل محللات دورية خاصة به.

بالإضافة إلى ذلك، بما أن المحلل الدوري المبني على حجب DNS يعيد صياغة أو يعدل استجابات DNS المستلمة من المخادم المفوضة، ستتم مخالفة نموذج سلسلة الثقة المستخدم من قبل DNSSEC مما سيؤدي إلى استخراج أخطاء مرتبطة بـ DNSSEC. قد تدفع هذه الأخطاء المستخدم النهائي إلى الاستنتاج بأن محلل DNS الدوري يعاني مشكلة أو يتعرض لهجوم. وسيكون هذا الاستنتاج ذومصداقية لأنه مع DNSSEC، لا يمكن تمييز استجابات DNS التي أعيدت كتابتها بموجب إلزام حكومي فنياً عما تتم ملاحظته أثناء تسميم الكاش الخبيث.

6. مقارنة حجب DNS بناءً على السجل أو المفوض مع حجب المحلل الدوري

بعض الدول, مثل اتخاذ المملكة المتحدة لإجراءات ضد أسماء في TLD لـ uk.[17] أواتخاذ الولايات المتحدة لإجراءات ضد أسماء في مستوى النطاق الأعلى (TLD) لـ com.[18] صادرت أسماء نطاقات يتم حفظها من قبل سجل عامل ضمن حدودها. في بعض الحالات، تم استبدال اسم النطاق في مصادرة السجل، وفي حالات أخرى، تم تعديل سجلات DNS لتوجيه الحركة المرورية إلى موقع إلكتروني خاضع لسيطرة الحكومة.

على افتراض أن أسماء النطاق المحجوبة هي قليلة العدد، ولن يكون إنشاء أسماء نطاق جديدة تخدم نفس الجمهور ونفس الغرض أمراً بسيطاً أو غير مكلف، يمكن أن تكون مصادرة أسماء النطاقات فعالة في حجب محتويات الإنترنت .بما أن الأجراءات المتخذة في TLD ستكون عند نقطة النشر، ستتم إزالة الأسماء المحجوبة من جميع محللات DNS الدورية عالمياً خلال فترة زمنية قصيرة، وخاصة خلال فترة عمر سجلات DNS التي يتم حجبها.

عند مصادرة النطاقات على مستوى السجل، يستمر DNSSEC[19] بالعمل بحسب ما هو مستهدف منه لأن هذا الإجراء هو تعديل لمحتويات DNS في مصدره، وبالتالي، على افتراض إعادة استخراج توقيعات DNSSEC المميزة بشكل صحيح، لن تتعرض سلسلة ثقة DNSSEC للمخالفة.

ولكن إذا كان السجل الذي يوفر الأسماء التي ينبغي حجبها يقع ضمن صلاحية قضائية مختلفة، قد يتطلب الأمر التعاون بين مسؤولي قوى تطبيق القانون في الحكومات ضمن الصلاحيات القضائية المختلفة. قد يشكل هذا مشكلة في بعض الحالات حين لا تكون قوانين الدولة الأخرى مطابقة، أو لا تمتلك منظمات تطبيق القانون معاهدات تعاون قانوني مشترك واضحة أو اتفاقيات تعاون أو تنسيق عن طريق الإنتربول مثلاً. بالتالي، تكون مصادرة النطاق على مستوى السجل عملياً أكثر ضمن الصلاحية القضائية الواحدة رغم حدوث تحسن ملحوظ مؤخراً بالتعاون والتنسيق بين وكالات تطبيق القانون. على سبيل المثال، يمكن تحقيق التعاون عن طريق مشاركة قوى تطبيق القانون في عملية ICANN متعددة المشاركين، وعن

---

[16] تتضمن أشهر المحللات المفتوحة (OpenDNS (http://www.opendns.com/ وDNS غوغيل العام (https://developers.google.com/speed/public-dns/).

[17] راجع http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/.

[18] راجع http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0.

[19] را جع http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

طريق تشكيل قوات مهمات خاصة ضمن منظمات مثل إنشاء مركز الجرائم الإلكترونية الأوروبي (E3C) ضمن يوروبول.[20]

يتطلب حجب DNS على مستوى المخدم المفوض أن يجري كل مشغل مخدم مفوض تغييرات على المنطقة التي تستلمها من السجل من دون التفويض من قبل السجل. قد يكون هذا أمراً صعباً في حالة تشغيل المخادم المفوضة من قبل أكثر من هيئة واحدإذا فشل مشغل مخدم مفوض أو أكثر بإجراء . التغييرات نفسها على نفس النسخةمن الجذر، قد يؤدي نفس الاستعلام إلى نتائج غير متسقة بحسب المحللات التي تم استعلامها، والمخادم المفوضة التي تم استعلامها من قبل المحللات، وموعدحدوث الاستعلامات وما إلى ذلكبالإضافة إلى ذلك، ما لم يصدف أن مشغل المخدم المفوض هو حامل مفتاح . (ZSK) توقيع المنطقة، فلن يتم توقيع التعديلات التي أجراها مشغل المخدم المفوض على المنطقة، مما سيؤدي إلى فشل سلسلة ثقة DNSSEC للمحللات التي تقوم بالتحقق من الصح. نتيجة لذلك، يميل هذا النوع من الحجب إلى كونه غير عملي.

إن استخدام حجب DNS المبني على المحلل الدوري يتجنب مثل مشكلات الصلاحية القضائية هذه لأنه يتم توجيه أوامر المصادرة إلى مزود خدمة الإنترنت أو مشغلي المحلل الآخرين ضمن نفس الصلاحية القضائية القانونية للجهة التي تطلب المصادرة. ولكن المشكلة بهذا أن مشغلي الشبكات المتنوعين من أنحاء العالم يشغلون محللات دورية، لذا من المستحيل ضمان التغطية الكاملة من دون مسار بيانات منسق وعالمي يقوم بالفلترة والتلاعب بالحمولة. بالإضافة إلى ذلك، سيخالف هذا التحقق من صحة DNSSEC على مستوى البرنامج من الطرف إلى الطرف، كما سنناقش في الجزء القادم. ولكن أثبتت دراسة واحدة على الأقل أنه بسبب ظاهرة تسمى "الفلترة العكسية"، وهي اتخاذ مزود الإنترنت لإجراءات في دولة لفلترة أو حجب المحتويات، قد يؤدي هذا إلى حجب المحتويات في دولة أخرى بسبب ترتيبات التوجيه بين مزودي خدمات الإنترنت.[21] إن العواقب غير المقصودة لهذا النوع من التأثير الحكومي الخارجي قد يظهر على شكل تكاليف تشغيل متزايدة واستقرار متزايد لجميع مشغلين ومستخدمي الإنترنت.

7. حجب DNS في المحللات الدورية يتضارب مع DNSSEC

كما ناقشنا في الأقسام السابقة، يمكن أن يكون لتنفيذ DNSSEC تأثيراً كبيراً على أنشطة حجب DNS. DNSSEC هي مجموعة من التعزيزات لبروتوكول DNS التي تم وضعها لمناقشة مسائل التحقق من الصحة ضمن DNS. رغم عدم انتشار البرامج التي تفعل DNSSEC بشكل واسع بعد، فإن الحاجة إلى مثل هذه البرامج هي دافع رئيسي لوضع ونشر DNSSEC. إن نشر DNSSEC من الطرف إلى الطرف هو متطلب لتفعيل دعم التحقق من الصحة الرمزي في البرامج الأمنية الحساسة الحالية والمستقبلية، والضرورية لحماية ثقة العامة في الإنترنت العالمي.

حجب DNS الفعال عن طريق المحللات الدورية يتضارب مع الغرض من DNSSEC. يرجع السبب بهذا إلى أنه قد تم تصميم DNSSEC لكي تكشف هذه التغييرات التي يهدف الحجب إلى القيام بها، رغم أن مصطلح "الحجب" يشير إلى إجراء التغييرات نفسها وفقاً للتشريعات و/أو القوانين الأخرى التي اتفقت عليها الأطراف المعنية. ن التغييرات التي يُحدثها الحجب هي غير قابلة للتميز عن التغييرات التي تجعلها DNSSEC قابلة للكشف، مثل إدخال المجرمين لاستجابات DNS زائفة حتى تتم إعادة توجيه الحركة المرورية إلى خدمات زائفة. أية تغييرات يتم إجراؤها على البيانات الموقعة من DNSSEC ستبدو مشابهة لمحاولات تسميم DNS الخبيثة بسبب عدم وجود ميزة أو إشارة ضمن DNSSEC لإعلام المستلم بتوقيع اسجابة معينة من قبل سلطة عدا عن حامل النطاق. وينطبق هذا على مصادرة النطاقات حيثما يكون الهدف هو مجرد حجب موقع إلكتروني، وكذلك لإعادة توجيه النطاقات حيثما يكون الغرض هو عرض إشعار اعتراض/مصادرة الحكومة مكان الموقع الإلكتروني

[20] راجع https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

[21] راجع https://citizenlab.org/2012/07/routing-gone-wild/.

عن طريق إعادة التوجيه. في كلتا الحالتين، سيتمكن المحلل الدوري للمستخدم النهائي عند التحقق من صحة الاستجابات الموقعة من DNSSEC من معرفة حدوث تلاعب، ولكنه لن يعرف سبب ذلك التلاعب. قد تتضمن أفعال محلل المستخدم النهائي الدوري عند اكتشاف هذا النوع من التلاعب استخدام أساليب الالتفاف، مثل تجاهل المحلل الدوري الذي يحل بشكل متكرر سلسلة الثقة بأكملها من الجذر إلى المخادم المفوضة نفسها.

يمكن أن يكون حجب DNS على مستوى المحلل الدوري مجدياً إذا كان لسد الفجوة بشكل مؤقت. على وجه الخصوص، إذا أراد أحدهم حجب أو فلترة DNS فقط عندما لا يستخدم حامل اسم النطاق أو المستخدم النهائي DNSSEC، ستظل عندها البيانات المعدلة مقبولة من قبل محللات المستخدم النهائي وستظل تستخدمها برامج مثل المتصفحات الإلكترونية. ولكن الأسلوب الالتفافي لحامل النطاق الذي لا يرغب بحجب اسم النطاق الخاص به سيكون توقيع بيانات DNS الخاصة به، والأسلوب الالتفافي للمستخدم النهائي الذي لا يرغب بحجب محتوياته سيكون تفعيل DNSSEC في محلل الجذل.[22] ومن هنا تأتي صفة "سد الفجوة بشكل مؤقت".

رغم الافتراض غالباً بأن لا يمكن أو ينبغي القيام بالتحقق من صحة DNSSEC إلا "داخل الشبكة"، فإن هذا يتجاهل احتياجات البرامج المرتبطة بـ DNSSEC. يمكن استخدام DNSSEC "داخل الشبكة" لحماية كاش DNS من البيانات المسمومة، وفي المراحل المبكرة من نشر DNSSEC، كان ذلك هو الاستخدام الوحيد الذي استطاعت صناعة الإنترنت الاستفادة من DNSSEC به. ولكن الرؤيا طويلة الأمد لـ DNSSEC هو إنشاء صنف جديد بالكامل من برامج المستخدم النهائي المرتبطة بـ DNSSEC باستخدام تقنيات مثل التحقق من صحة تسمية الهيئات (DANE) بناءً على DNS، وتبذل قوة مهمات هندسة الإنترنت (IETF) جهوداً في هذا المجال.[23] تعمل مجموعة عمل DANE على وضع آلية معيارية يتم من خلالها تعزيز هوية مخدم الويب الآمن وحماية الاتصال بين المتصفح والتي تحمي مخدم الويب عن طريق DNSSEC بدلاً من شبكة سلطة شهادة X.509 الأقدم والتي تميل إلى التسبّب بالمشاكل أكثر.[24]

نتيجة لجهود استخدام DNSSEC كبنية تحتية عامة سيتم بناء برامج آمنة، يمكن الافتراض أن حجب DNS في المحللات الدورية سيكون له تأثير سلبي على نشر DNSSEC أوسيصبح غير فعال حالما تشهد DNSSEC تنفيذاً أوسع. يمكن أن يحظى الاقتصاد العالمي إما بتسمية إنترنت آمنة وبالتالي برامج إنترنت آمنة، وإما حجب محتويات فعال عن طريق DNS الإنترنت،– ولكن ليس كليهما.

8. التضمينات الأخرى لحجب DNS

يتضمن حجب وفلترة DNS تضمينات خطيرة تتخطى ما تمت مناقشته في الأقسام السابقة. تتضمن بعض الإمكانيات الواضحة الحجب الزائد والتخطي/التحايل عن طريق توجيه حركة DNS المرورية بعيداً عن نقاط تطبيق الحجب.

[22] محللات الجذل هي محللات DNS دنيا تستخدم نمط الاستعلام الدوري لتفريغ معظم عمل حل DNS إلى مخدم اسم دوري. تحتوي معظم أجهزة الإنترنت على محلل الجذل، وتوفر معظم الشبكات مخدم اسم دوري لعملائها. راجع http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers.

[23] راجع https://datatracker.ietf.org/wg/dane/charter/.

[24] أحد الأمثلة على الصعوبات الأخيرة لـ X.509 هو تعرض Diginotar للاختراق (راجع http://en.wikipedia.org/wiki/DigiNotar) والاختراقات المتعددة لسلطات تسجيل Comodo (راجع http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/).

8.1 الحجب الزائد

على افتراض استخدام تقنيات حجب DNS، ثمة مخاطرة حدوث أخطاء في قائمة الهيئات التي ينبغي حجبها. ولا يرتبط ذلك بالقيام بالحجب عن طريق أسماء النطاقات أو المعرّفات الأخرى مثل عناوين بروتوكول الإنترنت أو محددات الموارد المحددة (URLs). بسبب هذه الحقيقة، ينبغي أن تكون العمليات المستخدمة لمراجعة البنود التي يجبإضافتها إلى قائمة معينة آمنة وجديرة بالثقة وتسمح بالتحقق الشامل. إن القوائم المستخدمة في أمثلة الحجب المبينة في هذا التقرير تشتق من موارد متعددة: الهيئات الخاصة، ووكالات تطبيق القانون المتعاونة والمحاكم أو الهيئات المشرّعة. لا تتخذ SSAC موقفاً معيناً حول العملية الأمثل، ولكنها توصي بعدة آليات للترويج للاستقرار الفني: قوانين واضحة حول ما ينبغي حجبه، وعملية اتخاذ قرارات ومراجعة جيدة التعريف.

بالإضافة إلى ذلك، من المهم الإقرار بأنه إذا تم القيام بحجب نطاق مثل *example.com*، فإن الحجب باستخدام نظام أسماء النطاقات سيحجب القدرة على البحث عن اسم النطاق عند الدخول إلى URL المحجوب، *http://example.com/bad-content.html*، وكذلك جميع URLs الأخرى التي تستخدم نفس اسم النطاق، مثل *http://abc.example.com/* أو *http://example.com/good-content.html*. كما سيؤدي حجب DNS إلى حجب البحث عن أسماء النطاقات لجميع الخدمات الأخرى مثل البريد الإلكتروني وإدارة الشبكات ونقل الملفات وغيرها من الخدمات التي تستخدم النطاق نفسه، وبالإضافة إلى ذلك، النطاقات التابعة لـ *example.com* (مثل *com.subdomain.example*).[25]

في النهاية، باستخدام أي نظام فلترة، سواء كان في DNS أو غيره، من المهم للغاية تجنب الأخطاء في استخراج الأهداف للحجب. على سبيل المثال، قد يؤدي خطأ طبوغرافي أثناء إدخال البيانات إلى فشل في حجب اسم النطاق المستهدف وحجب نطاق آخر غير مرتبط بالخطأ. ويمكن أن تشكل أسماء النطاقات الدولية (IDNs) مخاطر خاصة لأنه يمكن أن يظهر IDNs اثنين على أنهما متماثلين ولكن مميزين داخل DNS.

8.2 توجيه حركة مرور DNS بعيداً عن دولة تفرض الحجب

يمكن أن تشجع الإجراءات الحكومية التي تؤدي إلى حجب النطاق المستخدمين النهائيين على اتخاذ إجراءات لضمان توجيه حركة DNS المرورية عن طريق مخادم أسماء خارج البلاد، مثل استخدام VPNs أو محللات دورية معينة بدلاً من تلك التي تعمل عن طريق مزود الخدمة. هذا التوجيه "الخارجي" لاستعلامات اسم النطاق قد يحول ملاحظة DNS والسيطرة عليها إلى دول أخرى، مما سيحبط أنشطة مكافحة الجرائم الإلكتروني داخل البلاد التي تنفذ الحجب، و/أو ترعى أنشطة الجرائم الإلكترونية المتزايدة عن طريق الهيئات خارج البلاد. بالإضافة إلى التأخير الإضافي الذي قد يحدث، يمكن أن يكون لهذا التوجيه الخارجي لحركة DNS المرورية تأثير على أداء الإنترنت ضمن الدولة التي تحجبها لأن العديد من شبكات تسليم المحتويات تتخذ قرارات حول المعلومات التي ينبغي إعادتها عند استعلامات DNS بناءً على عنوان بروتوكول الإنترنت المصدر للمحلل الذي يقوم بالاستعلام. إن استخدام المخادم غير المحلية قد يؤدي إلى حركة مرورية غير متوقعة قد تعترض الروابط الدولية.

[25] راجع http://gigaom.com/europe/orange-censors-all-blogs/, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_s_elf_goal/ و http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

يمكن القيام بالتغيير إلى مخدم اسم آخر، سواء كان جزءاً من DNS من تنسيق ICANN أو نظام بديل، عن طريق إعادة الكتابة المباشرة لتهيئة الكمبيوتر، والتي يتم تسهيلها بشكل كبير بسبب وجود واجهات المستخدم الغرافية الودية في معظم أنظمة الكمبيوتر اليوم .حتى إذا لم يكن الشخص يتمتع بالمعرفة المتطلبة لتعديل إعدادات DNS على كمبيوتره قف ،(أو شبكته)د تم نشر نصوص وبرامج مخصصة تقوم بأتمتة تعديل DNS للتنزيل .أحد الأمثلة هو قابس MAFIAAFire الذي تم نشره بعد المراحل المبكرة من مبادرة التشغيل في مواقعنا الإلكترونية لقسم الهجرة والجمارك الأمريكي[26].

8.2.1 تأثيرات محللات تحويل المستخدمين

إن بيانات DNS تعطي مزودي خدمات الإنترنت صورة واضحة ودقيقة حول كلٍ من أنماط الحركة المرورية والتهديدات الأمنية على شبكاتهم. يمكن أن تسمح هذه المعلومات لمزودي خدمات الإنترنت بتحديد الزيادة والتحول في الحركة المرورية، مما سيؤدي إلى اتخاذ قرارات الأعمال عن اطلاع. والأهم من ذلك، فإن مراقبة بيانات DNS تدعم حماية الشبكات، وغالباً ما تساعد مزودي خدمات الإنترنت على تشخيص هجمات رفض الخدمة وتحدد المستضيف المصاب بالفيروسات والنطاقات المخترقة والمستخدمين الضعفاء.

مع تحول المستخدمين بشكل متزايد إلى مخادم DNS من غير تلك التي يوفرها مزودي خدمات الإنترنت، ستنخفض قدرة مزودي خدمات الإنترنت تلك على إدارة التهديدات الأمنية والحفاظ على عمليات الشبكة الفعالة. إن تخفيض استخدام المستهلك لمشغل شبكة محلي من الشركات، أو خدمة DNS من مزودي خدمات الإنترنت، سيعني أن تمر المزيد من الكمبيوترات المخترقة بلا تحديد أو تصحيح. بالإضافة إلى ذلك، ستكون مجموعة سمات تهيئة الإنترنت التي تحتاج إلى تقييم عندما يتصل العميل بمكتب المساعدة من المشغل لطلب الدعم أوسع كثيراً، وستزيد من كلٍ من التكلفة وتعقيد إصلاح العلل.

كما تشكل القضايا المذكورة أعلاه تحديات أمام حكومات الدول التي يقع بها مزودي خدمات الإنترنت .قد تفقد تلك الحكومات القدرة على جمع المعلومات الاستخبارية عن طريق ترتيبات مشاركة البيانات الممكنة مع مشغلي خدمة الإنترنت والشبكات، وكذلك عدم الحصول على معلومات قد تعتبر أدلة مهمة في تحقيقات قوى تطبيق القانون .على سبيل المثال، ربما ما كانت الحكومة الأمريكية ستحصل على أدلة كافية تتعلق بأمر بوتنيت وتراكيب السيطرة والكاش المسموم للتقدم بدعاوى قضائية مثل بوعد يهو ،"عملية نقر الشبح" DNSChanger ية مهمة أغلقت المخادم التي نشرت برمجياتقضاة الخبيثة [27].

ستكون مسائل تطبيق القانون خطيرة أكثر عندما يختار مستخدم مخدم DNS في دولة أخرى .ستتضاءل قدرة العمليات القانونية على مواجهة مشكلة ما عندما تكون المخادم خارج الصلاحية القضائية لوكالة تطبيق قانون معينة.

8.2.2 مخالفة التحويل المحلي لشبكة توزيع المحتويات (CDN) إذا قام المستخدمين بتحويل المحللات

كما سيؤثر تحويل حركة DNS المرورية بحيث لا تتطابق مع طبولوجيا الشبكة، مثلاً عن طريق مخادم DNS خارج دولة معينة، بشكل سلبي أيضاً على أداء الشبكة (ضمن الدولة، بحسب أوقات الرحلة الكاملة للنشر والتكتل) وزيادة التكاليف على مزودي خدمات الإنترنت. على سبيل المثال، إذا قام مستخدم بتحويل المحللات لتجنب الحجب، قد تكون النتيجة هي فشل التحول المحلي لشبكة توزيع المحتويات (CDN) بالعمل، وقد يتم توجيه المستخدم النهائي إلى محتويات من عقد شبكة توزيع محتويات تستضيفها مخادم خارج دولهم، بدلاً من تلك التي تقع ضمن شبكة ولوج المستخدم مع روابط متداخلة مباشرة.

---

[26] راجع https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ و http://en.wikipedia.org/wiki/MAFIAAFire_Redirector.

[27] راجع http://www.fbi.gov/news/stories/2011/november/malware_110911.

غالباً ما تقوم شبكات توزيع المحتويات بالتحويل المحلي للمحتويات عن طريق توزيع نفس المحتويات على نطاق المخادم على مجموعة واسعة من الشبكات عالمياً. سيخفض هذا التحويل المحلي من العبء على أي مخدم فردي ويحد من استهلاك موارد الشبكة والاختناق المروري عن طريق تسليم محتويات من مخادم قريبة من المستخدم قدر الإمكان. تستنتج العديد من شبكات توزيع المحتويات موقع المستخدم بناءً على عنوان بروتوكول الإنترنت لمحلل DNS الخاص بهم، مما يعني أن المستخدمين الذين يغيرون محللات DNS إلى خارج بلادهم سيظهرون على أنهم يتصفحون الإنترنت من خارج البلاد من منظور شبكات توزيع المحتويات. وستكون النتيجة هي التأثير السلبي على أداء واستقرار مستخدمي شبكات توزيع المحتويات، وزيادة التكاليف على مزودي خدمات الإنترنت الذين ينقلون الحركة المرورية المرتبطة.

9. الاستنتاجات والمزيد من المنشورات للاطلاع

مع انتشار حجب الولوج إلى المحتويات عن طريق DNS أكثر، من ناحية كونه موضوع للدراسة ومن ناحية تنفيذه، ثمة عدد من المسائل الفنية التي تصاحبه. إن الحجب على مستوى سجل DNS (سواء بشكل مباشر أو عن طريق مسجل) ذو أقل تضمينات فنية، ويمكنه العمل بنجاح مع DNSSEC، ولكنه قد يؤدي إلى مشكلات قضائية أو يسبّب بلقنة طويلة الأمد لاسم مساحة الإنترنت. إن الحجب على مستوى المخادم المفوضة يواجه نفس المشكلات القانونية، ولكن لا يمكنه العمل بنجاح مع DNSSEC في حالة عدم امتلاك مشغل المخدم المفوض القدرة على التوقيع الصحيح للمنطقة التي تحتوي على الاسم الذي ينبغي حجبه. في النهاية، رغم انتشار الحجب على مستوى المحلل اليوم، فإنه مثير للمشكلات في وجه DNSSEC بأحسن حالاته، وقد يعيق نشر DNSSEC بأسوأ حالاته.

ينبغي على الحكومات وجهات أخرى أخذ هذه المسائل بعين الاعتبار وفهم التضمينات الفنية بشكل كامل عند وضع السياسات التي تعتمد على DNS لحجب أو فلترة محتويات الإنترنت.

تتضمن المزيد من المنشورات المقترحة للاطلاع على هذا الموضوع المقالات التالية:

- Shutdowns, Suspensions, Seizures, Oh My!, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html.
- Preventing Access or Removing Content – Laser Scalpel or Saw?, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html.
- A Chainsaw is a Poor Choice for Surgery and for Blocking Content, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html.
- Alignment of Interests in DNS Blocking, P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/.

10. الإقرارات وبيانات المصلحة والاعتراضات والانسحابات

توفر هذه الأقسام للقارىء معلومات حول ثلاثة جوانب من عمليتنا. يبين قسم "الإقرارات" قائمة بالأعضاء الذين ساهموا في هذا المستند بعينه. يشير قسم بيانات المصلحة إلى السير الذاتية لأعضاء اللجنة وأي تضارب بالمصالح، سواء كان حقيقياً أو واضحاً أو محتملاً، قد يظهر في المواد في هذه الوثيقة. ويوفر قسم "الاعتراضات والانسحابات" مكانًا للأعضاء الفرديين للاعتراض على محتويات هذه الوثيقة أو عملية إعدادها.

10.1 الإقرارات

تود اللجنة شكر أعضاء اللجنة الاستشارية للحماية والاستقرار التالية أسماؤهم والمشاركين الآخرين نظير ما قدموه من وقت ومساهمات ومراجعة لوضع هذا التقرير.

آلين آلينا
جاب أكيرهوس
دون بلومينثيل
كي سي كلافي
ديفيد كونراد
باتريك فالتسروم
جيمس غالفين
وورين كوماري
جيسون ليفينغود
داني ماك فيرسون
رام موهان
بول فيكسي

10.2 بيانات المصلحة

تتوفر معلومات السيرة الذاتية وبيانات المصلحة لأعضاء SSAC على الموقع الإلكتروني:
http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

10.3 الاعتراضات والانسحابات

لم يكن ثمة أية اعتراضات أو انسحابات.