أبوظبي - ورشة عمل DNSSEC - الجزء 2
الأربعاء، 1 تشرين الثان (نوفمبر) 2017 - 10:30 حتي 12:00 بالتوقيت الرسمي الخليجي
اجتماع ICANN رقم 60 | أبوظبي، الإمارات العربية المتحدة

سيدة غير معروفة: الأول من تشرين الثاني (نوفمبر)، 2017، القاعة ""A، القسم BC، ورشة عمل DNSSEC الجزء 2، 10:30 - ظهرًا.

شخص غير محدد: حسنًا. هل يجب أن نبدأ؟

شخص غير محدد: هل أنت بصدد الإشراف على هذه الجلسة؟

شخص غير محدد: حسنًا، روس هو.

شخص غير محدد: أريد فقط أن أعرف كم من الوقت لدي.

روس موندي: حسنًا. نحن على وشك إعادة التشغيل مرة أخرى من خلال عرض الجدول التالي. سنقوم بإجراء تغيير طفيف على النظام عم هو على البرنامج - هل هذا لك، [باري]؟ - و - عفوًا. اعتقدت أني رأيت - أوه، دوان هناك. نعم، لماذا لا تأتي إلى هنا؟ اظهر قليلاً. نعم. حسنًا.

ترتيبنا المنقح: دوان ويسلز يبدأ أولاً، يليه جاب آكرهويس وكريستيان هيسلمان، وجيف هوستون، ثم روي أريندز مع ICANN.

أعتقد أن لدينا الوقت الكافي هنا، ولكني سوف أحاول أن أحمس الناس طوال الوقت إذا تعثرنا في نقطة ما حتى نتمكن من تجاوزها ويكون لدينا ما يكفي من الوقت للأسئلة والأجوبة على كل من العروض التقديمية. لذلك سنأخذ بعض الأسئلة مع كل عرض تقديمي. وأعتقد، مع ذلك، سنقوم بإعطاء الكلمة إلى دوان. تفضل الآن، رجاءً.

دوان ويسلز: شكرًا لك، روس. سألت روس عما إذا كان باستطاعتي البدء أولاً لأن هذا نوع من المعلومات العامة للمقدمين من بعدي، كما أعتقد.

هذا العرض التقديمي حول بيانات إشارة مرتكز الثقة RFC 8145. كان اهتمامي في هذا باعتباري مؤلف مشارك لـ RFC وكذلك كشخص يتلقى بعض البيانات على حد سواء. وهذه بمثابة نسخة أقصر من حديث أعطيته قبل شهر في مركز عمليات وتحليلات وأبحاث نظام اسم النطاق لهذا نذكر أجزاء جيدة هنا في العنوان.

ويحدد RFC هذا العملية التي يمكن من خلالها للمصادقين أن يشيروا إلى معرفة مرتكز الثقة الخاص بهم. سأشرح بإيجاز كيف يعمل هذا. تتخذ الإشارة شكل علامة رئيسية، وهي رقم صحيح 16 بت الذي يحدد المفاتيح والتوقيعات وأشياء من هذا القبيل.

هناك نوعان من قيم العلامات الرئيسية ذات الصلة بالمناقشة اليوم. 19036 هي العلامة الرئيسية لما نسميه KSK-2010، و20326 لـ KSK-2017. يتم الإبلاغ عن هذه الإشارات لتصل إلى "خوادم الأسماء الموثوقة" في المناطق، والتي تكون في هذه الحالة منطقة الجذر. وعلى المصادقين إرسالها مرة واحدة كل TTL أو نحو ذلك.

ويحدد طلب تقديم التعقيبات شكلين لإرسال الإشارة الأساسية. أحدها يتمثل في خيار EDNS0. في الممارسة العملية، لا يتم تنفيذ هذا من قبل أي شخص، لذلك، تأتي جميع البيانات بالفعل في شكل الصيغة الثانية، وهو استفسار عن العلامة الأساسية. فهو مجرد استعلام العادي حيث يتم ترميز بيانات علامة المفتاح في اسم الاستعلام ويتم ترميز قيم علامة المفتاح في ست عشري. قد يكون من المفيد أن نعرف أن 19036 هو 4-alpha-5-charlie، و20326 هو foxtrot-66-4 في ست عشري.

يعرض هذا الجدول جدولاً زمنيا لكيفية تنفيذ الأمور. وكان أول مشروع للإنترنت في كانون الأول (ديسمبر) 2015. بحلول عام 2016، كان هناك أول تنفيذ لبرامجيات بيركلي لنظام اسم النطاق على الإنترنت. ثم كان هناك مشروع الإنترنت في وقت لاحق، والذي أصبح RFC8145 في (نيسان) أبريل. وفي نفس الوقت، تم تنفيذه في وضع غير محدد. يعتبر أيار (مايو) هو الوقت الذي تم فيه البدء في النظر في البيانات.

في برامجيات بيركلي لنظام اسم النطاق على الإنترنت، تم تمكين هذه الميزة افتراضيًا. في الوضع "غير محدد"، لم يتم تمكينه في البداية بشكل افتراضي، ولكنه تغير إلى الوضع الافتراضي في أوائل تشرين الأول (أكتوبر).

بعض البيانات. كما ذكرت، يتم إرسال بيانات الإشارة إلى خوادم اسم منطقة الجذر. تأتي البيانات التي يجب النظر إليها من اثنين من منها - من A-root وJ-root. أريد أن أكون واضحًا بشأن أن هذه البيانات تأتي من التطبيقات الأخيرة فقط لبرنامج اسم الخادم، لذلك فإن الأشخاص الذين تمت ترقيتهم مؤخرًا فقط هم من يقدمون هذه البيانات.

توضح هذه الشريحة ما تبدو عليه البيانات الأولية. يمكنك رؤية هذه الأعمدة هنا في الأسفل. هناك طابع زمني UNIX ، [إنه] يحمل اسم الاستعلام، حيث ترى underscore-TA-hyphen ثم الأرقام العشرية، ثم عنوان المصدر وعنوان الوجهة والسنة والشهر والتاريخ.

تم أخذ هذه العينة من وقت سابق في المجموعة. معظم الأعمدة التي تظهر هنا فقط مرتكز ثقة القديمة، وهو alpha-5-charlie-4. تحتوي معظم هذه الخطوط على ذلك فقط. يحتوي بعضها على كلا القيمتين، مشيرًا إلى أن هذه تعتبر المصادر التي تم الحصول على KSK الجديدة بالفعل.

يوضح هذا الرسم البياني عدد من عناوين بروتوكول الإنترنت التي تقدم البيانات يوميًا خلال الفترة الزمنية، بدءًا من أيار (مايو) وحتى وقت قريب جدًا. يمثل الخط الرأسي الأول على اليسار الوقت الذي تم فيه نشر KSK-2017 لأول مرة في منطقة الجذر. يشير الخط الرأسي الثاني على اليمين إلى الوقت الذي ينتهي فيه الموقت المؤقت للتركيب

RFC5011. ووفقًا لهذا البروتوكول، يكون هذا عندما يمكن للمصادقين إضافة مفتاح جديد إلى مخزن مرتكز الثقة الخاص بهم.

في البداية، كان لدينا شيء مثل 500 مصدر يوميًا. وفي الآونة الأخيرة جدًا، وصلنا إلى 2500 في اليوم الواحد.

يوضح هذا الرسم البياني الإشارات التي ترسلها هذه المصادر. مرة أخرى، هذا في اليوم الواحد. الأحمر هنا، النقطة في اليسار، هو إشارات تشير فقط إلى مرتكز ثقة لعام 2010 فقط. الأخضر الكبير على اليمين هو المصادر الخاصة بكل من مفاتيح 2010 و2017 في مجموعة مرتكز الثقة الخاصة بها.

قد يكون من الصعب قليلاً أن نراها، ولكنها بين الأحمر والأخضر، هناك تبعثر للبكسل الأصفر هنا. وهي تمثل عناوين مصدر بروتوكول الإنترنت المصدر التي، على مدار اليوم، أرسلت إشارات مختلطة. في بعض الأحيان، قالوا إنه ليس لديهم سوى المفتاح القديم، وقالوا أحيانًا أخرى أن لديهم كل من المفتاح القديم والجديد. ولكن هذه نسبة صغيرة نسبيًا.

والشيء الذي كان يتعلق بالتمديد حقًا هو أنه بعد انتهاء الموقت المعلق، ظل الخط الأحمر ثابتًا ولم ينزل.

حسنًا. شكرًا لك، [جاب]. ستلاحظ على اليسار بعيدًا جدًا هذا الخط الأحمر. ونرى ارتفاعًا آخر. سوف أتحدث قليلا عن ذلك هنا.

هذه في الحقيقة البيانات نفسها، ولكنها تمثل كنسبة مئوية بدلاً من العد. يمكنك رؤية ذلك، بعد انتهاء مؤقت الانتظار باستمرار، كان هناك هذا الالتقاء الكبير الذي أشار إليها الكثير من المصادقين إلى أنها قبلت مرتكز الثقة الجديدة وتحويله.

ليس لدي نقطة، أو لا أعتقد، ولكن إذا نظرتم إلى أسفل مرة أخرى في تلك الزاوية اليمنى السفلى، نحو هذا الارتفاع في نهاية تشرين الأول (أكتوبر). المؤشرات الأولية هي تلك التي تعود إليها البرامج غير المحددة. أصدرت النسخة المحدودة نسخة في 10 تشرين الأول (أكتوبر) مما مكن من الإبلاغ عن بيانات مرتكز الثقة بشكل افتراضي. يبدو أن

السكان الذين يستخدمون النسخة غير المحددة - ربما عدد كبير منهم لم يكن لديهم مفتاح جديد.

شكرًا لك، [جاك].

هناك شيء آخر اعتقدت أنه من المثير للاهتمام أن ننظر إليه وهو عدد المرات التي نرى فيها بيانات علامة مفتاح غير متوقعة أو غير IANA في هذا. فمنذ بدء المجموعة، رأيت حوالي 29 علامة رئيسية بخلاف الاثنتين نتوقعهما كمرتكزي ثقة IANA. عندما قدمت هذا العرض التقديمي في مركز عمليات وتحليلات وأبحاث نظام اسم النطاق قبل شهر، كان هناك 19. لذلك تطرقت قليلاً منذ ذلك الحين. وبالمثل، في ذلك الوقت كان هناك فقط حوالي 12 عنوان مصدر بروتوكول الإنترنت للمسافة في اليوم، ولكنها الآن تصل إلى 100.

فيما يلي رسم بياني يعرض إرسال الاشارة الأساسية غير المتوقعة في اليوم. مرة أخرى، أسفل في أسفل اليمين هناك نرى هذا الارتفاع. مرة أخرى، تخميني عند هذه النقطة يتمثل في تقديم هذه البرامج غير المحدودة. ولكن السبب في أن الخط الأزرق ارتفع كثيرًا لأنه يبدو أن بعض السكان مناسبين من حيث من حيث الحجم - ربما في أنظمة تشغيل معينة أو شيء من هذا القبيل - فعلوا شيئًا أعتبره سخيفا. وأضافوا منطقة الجذر ZSK، مفتاح الدخول لمنطقة الجذر، إلى مجموعة مرتكز الثقة، والتي كانت غير ضارة. ولكنه يؤدي إلى هذا الارتفاع هنا. يعتبر هذا محيرًا قليلاً في سبب حدوث ذلك، ولكن هذا أفضل تخمين.

استنتاجي من هذا هو أن هذه البيانات ذات نوعية جيدة إلى حد معقول. ولم أرى أي دليل على العبث أو أي شيء من هذا القبيل. يجعل كلا من NATs واسم الخوادم الذي تم إعادة توجيهها إلى اسم خادم آخر وعنوان IPs ديناميكي وكذلك وجود رؤية لاثنين فقط من خوادم الجذر التحليل معقدًا. للحصول على صورة أفضل، من الأفضل أن يكون لديك المزيد من خوادم الجذر. أعتقد أن روي سوف يتحدث عن ذلك لاحقًا.

لقد سبق أن ذكرت عن [الغرابة] بحلول 10 من تشرين الأول (أكتوبر)، والتي، مرة أخرى، وأعتقد أنه يرجع إلى البيانات الواردة من المستخدمين غير المقدين.

أود أن أشكر ISC على تنفيذ هذا وتحويله بشكل افتراضي، وأيضا NLnet Labs عن نفس الشيء: لتنفيذه وتحويله إلى وضع غير مقيد. وأود أن أشجع موردي البرامج الآخرين على توفير هذه البيانات في المستقبل.

إذن فهذا هو نهاية العرض. هل نطرح الأسئلة الآن أم لاحقًا؟

روس موندي: أجل. لدينا الوقت لسؤالين سريعين إذا كان هناك أي منها في هذه المرحلة.

دوان ويسلز: حسنًا.

روس موندي: نعم؟

دوان ويسلز: اوندريج؟ عذرًا.

ستيفن باري: ستيفن باري من كندا. لقد عزيت اثنين من الفروق في ارتفاع الإرسال إلى التطبيقات في الوضع غير المقيد. ربما فوت ذلك، ولكن هل تعرف الأرقام النسبية للوضع غير المقيد مقابل تطبيقات برامجيات بيركلي لنظام اسم النطاق على الإنترنت التي هي إشارات؟

دوان ويسلز: لم يكن لدي الوقت لإدراج هذا، ولكن في مركز عمليات وتحليلات وأبحاث نظام اسم النطاق، هناك بعض الشرائح التي تظهر كيف نعرف هذا. تعتبر الطريقة الأفضل هي أن برامجيات بيركلي لنظام اسم النطاق على الإنترنت نوفر إشارات في فترات منتظمة جدًا، على مدار 24 ساعة. غير المقيد - لقد تطرقت إليها على حد سواء في المنزل ونظرت

إليها - قدمت البيانات على فترات أقل اعتيادية وأقصر. يمكننا أن نرى ذلك في هذه البيانات، وهذا يعتبر أحد الأسباب التي أعزو هذه الإشارات الأخيرة إلى الوضع غير المقيد.

أما بالنسبة إلى النسبة المئوية، فليس لدي رقم دقيق. وقد نكون في نطاق 5-10٪ أو شيء من هذا القبيل.

اوندريج؟

أوندريج سوري: شكرًا لكم على العرض. فقط لإظهار أن طلبك كان صعبًا، قمنا بتنفيذ هذه الميزة أمس. في الأساس، سوف نذهب إلى الإصدار التالي، وكذلك محلل KNOT لدعم هذه الوظيفة في الإصدار التالي.

دوان ويسلز: ممتاز. شكرًا جزيلًا لك.

روي آريندس: سؤال سريع، أوندريج، عند جدولة هذا الإصدار التالي؟

أوندريج سوري: بصراحة لا. معذرة. تم ترميزها أمس فقط. وهي لم تمر من خلال مراجعة الرمز والاختبار وكل شيء. وذلك سوف يستغرق بعض الوقت. لا يمكننا إصدار شيء لم تختبر، للأسف. ولكن سنحاول تسريعها قدر الإمكان. سوف ادفع المطورين لتنفيذه بسرعة.

روس موندي: تفضل.

روي آريندس: دوان، توضيح واحد. أعلم أننا تحدثنا عن ذلك بالأمس، ولكنك تقول علامات رئيسية بخلاف 4a5c و4f66. ولكن أعتقد أن ما رأيناه هو إضافة علامة رئيسية إلى 4a5c و4f66. وهذا يعني أن الإشارة التي شاهدناها لها مفتاحين ومفتاح آخر. هل هذا صحيح؟

دوان ويسلز: نعم، هذا صحيح. مرة أخرى، هذا الارتفاع هناك - تلك لديها المفاتيح المتوقعة بالإضافة إلى مفتاح غير متوقع. وبالتالي فإن الخط الأزرق هناك يشير إلى الإشارات التي توفر المفاتيح المتوقعة والمفاتيح غير متوقعة. ويكون الخط الأحمر، الذي هو الأسفل بشكل ثابت في الجزء السفلي، قيم العلامات الرئيسية غير المتوقعة فقط من تلك المصادر. لذلك هذه تجارب أخرى أو شيء ما آخر.

روس موندي: حسنًا. أعتقد أننا بحاجة إلى الانتقال إلى العرض التقديمي التالي. شكرًا جزيلا لك، دوان.

التالي هو جاب أكيرهويس.

جاب أكيرهويس: جاب أكرهويس، NLnet Labs، والقيام بالوضع غير المقيد أيضًا، من بين أمور أخرى. أعتقد أن الحديث [غير مسموع]. هذا أمر مثير جدًا. ويظهر أيضا أن الإشارة التي تحصل عليها من الصعب جدًا تفسيرها. أنت لا تعرف ماذا يحدث. قد يكون ذلك أيضًا هروب أساسية [غير مسموع].

على أي حال، قبل ذلك، سوف أتحدث قليلاً عن الوضع غير المقيد و5011 وكيف يحدث هذا إذا كنت البائع الذي يقوم بتنفيذ الاشياء التي كنت لا تعرف ما هي عليه. لذا هذه بعض المعلومات.

بشكل عام، تظهر ميزات جديدة في نظام أسماء النطاقات. السياسة تتمثل في أننا متحفظون في وضع التعليمات البرمجية. أساسًا ما نقوم به هو، كلما بدأ الإنترنت [غير مسموع]، ونحن نعتقد أن الهوية سوف تظل على قيد الحياة بالفعل ولن تموت الموت الرهيب، إذا

كان هناك ما يكفي من الوقت، سيكون لدينا في الواقع قاعدة تعليمات برمجية أو في القانون الداخلي بعض إصدارات الحصول على الاشياء القيام به، وربما التعليق على ميزة جديدة، أم لا كان ذلك ممكنًا والقيام بأي شيء من هذا القبيل. وبمجرد الحصول على مواصفات أكثر استقرارًا قليلاً، سيتم إصدارها في الإصدار [القياسي]، ولكن فقط كخيار [الوقت] المجمع. لذلك سيعرف الناس حقًا ما يجب القيام به، والناس الذين يعرفون ما يفعلونه في الواقع قد تكونوا قادرين على تجربة هذا، ولكن لديهم ما يقومون به ببعض العمل الإضافي من أجل [غير مسموع].

ثم هناك فترة تبلغ 48 ساعة في IETF. هذا عندما يكون المشروع مستقرًا و يتم وضع تعليقات على توافه الأمور فقط. حسنًا، قد يستغرق الأمر 48 ساعة إلى بضعة أشهر من حيث شروط IETF . لذلك بناءً على المدة التي قد تستغرق 48 ساعة، سوف يضع بالفعل في [فيما يتعلق] بالإصدار عن خيار وقت التشغيل. لذلك يتم إيقاف تشغيل الافتراضي للقمة العالمية لمجتمع المعلومات. لذ يصبح خيار وقت التشغيل. الناس الذين يريدون بالفعل أن يكونوا يعيشون على حافة العالم يمكنهم بالفعل التبديل ما إذا كانوا يعرفون ما يفعلون أم لا.

كلما تحققت المعايير حقًا، كما هو الحال في RFCs، ذهبنا إلى فترة 48 ساعة. إننا أساسا نقلع عما هو موصى به في RFC ونضعه في الإعداد الافتراضي. قد ننتظر في بعض الأحيان، عندما يكون هناك تغيير كبير حقيقي، حتى لا لا يتم الإصدار التالي ولكن تحدث عثرة كبيرة في الإصدار [تأتي من] ثانية لأنه في الواقع ميزة جديدة للوظيفة. إننا نحاول الحفاظ على ذلك تلقائيًا. هذه هي السياسة القياسية. ويفعل البعض الآخر ذلك أيضًا. [أخذت المحلل من] [غير مسموع].

كيف حدث ذلك مع 5011؟ حسنا، 5011 هو في الواقع عبارة عن برنامج منفصل. وهو يسمى مرتكز غير مقيد، وهو مختلف تمامًا عما هو عليه الآن. لذا ظل منفصلاً حتى تمكن الناس من تشغيله. كان في الواقع [رمزًا غير ملموسًا] على الإطلاق. ولكن عندما ذهبت إلى فترة 48 ساعة، انتقلنا إلى قاعدة التعليمات البرمجية الرئيسية. لقد أدرجنا في الإصدار 1.4.0 غير المقيد في 2009 بالفعل، لذلك حتى قبل تنفيذ DNSSEC في الجذر. ولكن كان هناك. هذا [يتعذر تمييز الصوت].

المشكلة هي انه بروتوكول غريب. في الواقع، 5011 ليس بروتوكول. فهو مجرد وثائق تغييرات الحالة. فهي لا تخبركم ما يجب القيام به، بل يخبرك فقط كيفية القيام الاشياء. هذا يجعل الاختبار يبدو إلى حد ما [صعب]. قاعدة التعليمات البرمجية هي ما كنا نسميه بالفعل لسنوات اختبار موحد لـ [غير مسموع]. يمكننا اختبار الوظائف المنفصلة، وتشغيلها دائمًا قبل أن نصدر أي شيء كبير.

لإجراء 5011، أنشأنا في الواقع - على الأقل [فولكر] قام بمعظم العمل - أدوات الاختبار - حدث شيء لإملائه هناك. على أي حال، هذا ما تحصل عليه عند إجراء الشرائح في اللحظة الأخيرة. تعتبر أدوات الاختبار اختبار موحد من شأنه أن يسرع في الواقع الوقت، حتى تتمكن من التظاهر بأن الأمور حدثت بسرعة أكبر. وهذا يأتي [حتى] مع فترة زمنية تبلغ 30 يومًا، والتي ذكرت في 5011.

في الواقع، لقد اخذت فكرة إجراء دورات الاختبار بالكامل من الرجال في cz.nic، وبلورتها أكثر قليلاً. لقد أصدروها بالفعل كنقطة منفصلة من البرمجيات.

وبعد عام 2009، حدثت بعض التغييرات الإضافية، مثل إصلاحات الشوائب، لأنه، إذا تم تنفيذ ميزات أخرى، فقد تتطلب تغييرات في كيفية تعامل التعليمات البرمجية مع 5011. ولكن لا شيء تغيير بشكل أساسي.

لذلك كان [الكذب هناك]، ونحن في الواقع فكرنا في القيام دعم T-shirts من أجل 5011 منذ عام 2009، ولكن لم نفعل ذلك قط.

على أي حال، ثم بسبب تسارع منصة الاختبار - يعتبر هذا Rick-Roll التي أنشأها ريك لامب والاستبدال الرئيسي من قبل وارن كوماري، التي قامت بالفعل بالاستبدالات طوال الوقت. لقد نسيت كم مرة في اليوم يفعل ريك ذلك. يفعل وارن ذلك كل 90 دقيقة، وأعتقد، وهو نوع من سريع، أن هذا يتوقف على 30 يومًا.

لاختبار ذلك، كان علينا تغيير التعليمات البرمجية إلى وضع غير مقيد لاتباع هذا البروتوكول الوهمي في الواقع. ما حدث هناك كان - وهذا في الواقع ليس لطيفًا حقا لأنك ستكون بالتأكيد رمزًا إضافيًا [يمر] في التعليمات البرمجية الخاصة بك والتي لن يتم

استخدامها أبدًا في أي عمل. ولن يتم اختبار [مرور] الرمز حقيقي على الاطلاق. لدى كل [الأسرة] ذلك.

بسبب التوقيت السريع، لقد فوتنا بالفعل حالة الزاوية. حالة الزاوية - ثابتة الآن مرة أخرى - هي - كلما بدأت إجراء DNSSEC و5011 في فترة تكون في الواقع أقصر من 30 يومًا المطلوبة في البروتوكول، وكنت لا تعرف ماذا تفعل، فسوف تكون صارمة جدا - في الواقع [غير متعمد] غير مفيد للبروتوكول لهذا الأخير. لذ [غير مسموع] لم يلاحظ إلا كلما مرت مدة 30 يومًا.

تقول برامجيات بيركلي لنظام اسم النطاق على الإنترنت في الواقع بشكل أعمى، "حسنًا. حسنًا. هذا هو الاستبدال. دعونا نهرب لمدة 30 يومًا". لدينا طريقة أكثر توهمًا قليلاً لفحص هذه الأشياء، ولكن في هذه الحالة، لاحظنا حدوث هذا. يعتبر هذا هو البروتوكول[غير مسموع] غير محدد [غير مسموع] ، لذلك نقوم بذلك. أي شخص لديه وضع غير مقيد أقدم من ذلك - فإن هناك الكثير جدًا منها في كل مكان لأن الكثير من الناس مثل [غير مسموع] - لا تتبع حقا أحدث إصدار التعليمات البرمجية، ولكنهم الاشياء الامنية للحمل العكسي في جميع الإصدارات. لذلك قد أو قد لا تنفذ 5011، وهي مشكلة أخرى، مع محاولة للعثور عليه.

إذا كنت تنفذ DNSSEC في الوقت قبل 30 يومًا، فإنك على ما يرام. إذا كنت في هذا الوضع سيئ الحظ، فالشيء الوحيد الذي عليك القيام به هو مجرد إزالة المرتكز القديم وإعادة تشغيل الوضع غير المقيد، وسوف تكون الأمور على ما يرام أيضًا. لذلك ليس صفقة كبيرة. على أي حال، أحدث إصدار من الوضع غير المقيد الآن يدرك هذا. هذا هو ما أقوله هنا. إذا تخلصت بالفعل [غير مسموع] من KSK القديم وإعادة تشغيل الخادم. سوف تكون سعيدًا.

ما يظهره لك في الواقع هو أنه لا أحد ينظر حقًا إلى [غير مسموع] من هذا البروتوكول الجديد لما سيحدث. تجد فقط أنه وافعي.

على أي حال، فإن الإنترنت هو مجرد تجربة كبيرة، لذلك لا يمكننا بالفعل أن يحل محله بشيء آخر.

روس موندي: حسنًا. شكرًا لك، جاب. سيكون لدينا الوقت لبعض الأسئلة السريعة لجاب إذا كان هناك أي منها. ربما لدينا بضع دقائق إذا كان هناك بضعة أسئلة سريعة.

أنا لا أرى أي أسئلة. هل هناك أي شيء عبر الإنترنت؟

حسنًا. في هذه الحالة، شكرًا جزيلاً لك، جاب. إننا نقدر ذلك.

التالي هو كريستيان هيسلمان على مشروع كاناري الجذر.

كريستيان هاسلمان: 23 دقيقة. لن أحتاج إلى الكثير من الوقت. حسنًا.

أنا في انتظار سحب الشرائح.

سوف أتحدث بإيجاز عن مشروع كناري الجذر، وهو جهد مشترك من عدة أطراف، كما ترون في هذه الشريحة. أنا مع سيدن، وهو الحشد الموجود على اليسار مع ما نسميه [شعار]، ولكن هذا ينطوي أيضًا على مختبرات NLnet، جامعتين، سورفنيت، وأيضًا ICANN وRIPE.

الشريحة التالية، من فضلك - نعم، لدي ضاغط في مكان ما.

شكرًا. يعرف مشروع كناري الجذر أيضًا باسم الكناري في منجم الفحم الفعلي. كما تعلمون، في الماضي، كان الناس الذين عملوا في مناجم الفحم في كاناري معهم للحصول على مؤشر على ما إذا كان هناك أي شيء يحدث مع أول أكسيد الكربون في منجم للفحم. سوف يمر الكناري ببساطة أو يموت عندما يحدث ذلك. وهذا في الواقع مماثلاً.

بالنسبة للاستبدال الأساسي KSK، فإن ما نريد القيام به هو تتبع الأثر التشغيلي للاستبدال الأساسي KSK وكذلك الحصول على إشارات تحذير في حالة حدوث شيء خطأ هناك. وفي الوقت نفسه، نود أيضًا قياس عملية التحقق من صحة الاستبدال الأساسي KSK من منظور عالمي لتتعلم بشكل أساسي من هذا النوع من الأحداث.

لذا فإن هذين هما الهدفين الرئيسيين للمشروع.

وهو أساسًا منهجية قياس نقوم بتطويرها هنا، وهي تستخدم منظورين مختلفين. أهم اثنين هما RIPE Atlas وLuminati RIPE Atlas هو شبكة استشعار معروفة ربما سمعت عنها. بها حوالي 9000 عقدة تنتشر في جميع أنحاء الكوكب، ومعظمها مدمن متصل بشبكات من الناس في المنزل، على سبيل المثال. إننا نستخدم أيضا شبكة Luminati، وهي شبكة وكيل يستخدمها الأشخاص لإخفاء عناوين بروتوكول الإنترنت الخاصة بهم. إننا نتحدث إلى APNIC وربما أيضًا نستخدم قياساتها في منهجنا.

وأخيرًا، إننا نفكر أيضًا في استخدام ما كان يسمى هنا وجهة نظر غير متصل، والقيام بقياسات حركة مرور خادم الجذر بطريقة غير متصلة بالإنترنت بعد أن يتم الاستبدال.

لذلك في جوهرها، هذا في الأساس مشروع قياس.

أيضا، على منهجية القياس، وقعنا العديد من أسماء النطاقات، سواءً بطريقة صحيحة وطريقة وهمية، إذا جاز التعبير. ما نحاول الحصول عليه من هذه المعلومات هو عدد من المحللين التي تحقق بشكل صحيح، أوليك الذين يحققون بشكل غير صحيح التي تنتج SERVFAIL، والمحللين الذين لا يحققون. وكآثار جانبية للمشروع، فإننا نقوم أيضًا بقياس أي من المصادقين يدعمون أنواع الخوارزميات.

شبكة Luminati التي تحدثت عنها هي خدمة وكيل https . ما يعتبر مهمًا هنا هو أنه يوفر وجهة نظر مختلفة تمامًا على شبكة الإنترنت مما يفعله من أجل RIPE Atlas. وهذا يغطي 15000 نظام مستقل، ولكن 14,000 من تلك لا تغطيها RIPE Atlas لأن RIPE Atlas عادة ما يتم تشغيله من قبل الناس الذين لديهم خلفية عن الشبكات وكذلك القياسات، على سبيل المثال. تعتبر هذه العقد في الواقع إعدادًا في شبكات المستهلكين العادية، لذلك قد تكون في الواقع أكثر تمثيلاً لكيفية القيام بالأشياء مما نراه من شبكة RIPE Atlas.

أجرينا بضعة قياسات بحلول 19 أيلول (سبتمبر)، وهو عندما زاد حجم سجلات DNSKEY. كما ترون هنا، لم يحدث شيء خاص حقًا. هذه هي الردود الفاشلة - SERVFAILs. حسنا، ليس هناك شيء يتغير كثيرًا في هذه الفترة.

شخص غير محدد: إذن KSK هو [غير مسموع].

كريستيان هاسلمان: أجل. يجب أن يقول KSK، بالمناسبة. هذا خطأ مطبعي أسفل هناك.

شخص غير محدد: ما الفرق بين الأحمر والأزرق [غير مسموع]؟

كريستيان هاسلمان: تاريخها، نعم. يبين هذا الرسم البياني المماثل استخدام TCP وUDP خلال تلك الفترة. إذا كان هناك شيء غريب قد يحدث، فقد تتوقع أن المحللين قد تحولوا إلى TCP بسبب زيادة حجم الرسالة. كما ترون هنا، فإنه لم يحدث حقًا، بحيث تبدو مستقرة للغاية، أيضًا.

هذا هو بت التجزئة. ليس هناك الكثير من التغييرات في التجزؤ، أيًا كان. لذلك لا شيء حدث حقًا بعد لأنه، بالطبع، تم تمديد استبدال أساسي KSK. لذلك هذا نوعًا ما ممل.

على أي حال، نريد تعميم هذه المنهجية التي أنشأناها الآن لقياس المقاييس الرئيسية على مستوى TLD، على سبيل المثال. لذا، فنحن نرغب في تطبيق ذلك بشكل أكثر عمومية، وكذلك الحصول علي المزيد من المعلومات حول كيفية تصرف المحللين في خوارزميات DNSSEC، علي سبيل المثال، ولكن أيضًا أنواع عمليات التحليل. ولكن كما قلت أولاً، نحن بحاجة إلى التوصل إلى الصفقة الحقيقية هناك.

إذا كنتم في قياسات الشبكة وكنتم تقومون بتشغيل الآلات الخاصة بك، فإننا نقدر تعاونكم في هذا الجهد من خلال تشغيل النص الصغير الذي كتبناه. ويستخدم المحللين الافتراضيين أساسًا للاستعلام عن خوادم الجذر كل ساعة. إذا كنت مهتما بالانضمام إلى هذا الجهد، فإنه يرجى المجيء والاتصال بي بعد ذلك.

وهنا حفنة من المؤشرات لمزيد من المعلومات حول مشروع كناري الجذر.

كانت هذه أخر شريحة. روس؟

روس موندي: شكرًا لك، كريستيان. هل لدينا جولة لطيفة من التصفيق؟ شكرًا. دعونا نتأكد من الجميع مستيقظا وتغيير ترتيب الأشياء قليلاً هنا.

هل لدينا أسئلة لكريستيان بشأن كناري الجذر؟

روي؟

روي آريندس: مرحبًا، كريستيان. معكم روي أريندز. كيف حالكم يا أصدقاء؟

كريستيان هاسلمان: مرحبًا، روي.

روي آريندس: لقد ذكرت ثم قمت بتصحيح ذلك، ولكنني لم أسمع ما قلت. أعتقد في الواقع أن ZSK الجديد يأتي في 19 أيلول (سبتمبر). هل هذا صحيح؟ لأنني أعتقد أنك تقيس الزيادة في -

كريستيان هاسلمان: نعم، الزيادة في الرسالة.

روي آريندس: أجل. هذا عندما يكون فيريسين، شريك إدارة منطقة الجذر، هو استبدال ZSK القياسي. وهم يفعلون ذلك كل ثلاثة أشهر. و[لقد فعلوا ذلك لمدة] سنوات. لذلك أعتقد ZSK صحيحًا.

كريستيان هاسلمان: حسنًا. ثم حدث خطأ.

روس موندي: حسنًا. هل نحن - أوه. نعم؟

شخص غير محدد: مرحبًا، كريستيان. [يورام] تشنيك. فيما يتعلق باحتمالية فحص الخوارزمية في كناري الجذر، هل لديك بعض البيانات من هذا؟ ربما بشكل خاص لكل بلد - كيف يتم دعم بعض الخوارزميات، شيء بديل لما يفعله جيوف.

كريستيان هاسلمان: أجل. في الواقع، لدينا القليل جدًا من البيانات على ذلك، ولكن لم أدرجها في الشرائح. ولكنها على موقع كناري الجذر، rootcanary.org. وهناك رسوم بيانية تفاعلية يمكنك التحقق منها.

شخص غير محدد: حسنًا. سأتأكد. شكرًا.

كريستيان هاسلمان: بالتأكيد.

جاب أكيرهويس: يمكنك أن ترى في الواقع القياسات تحدث في الوقت الحقيقي. فهي يستغرق الكثير من وقت الحوسبة، لذلك لا تفعل ذلك أيضًا [خفيف].

شخص غير محدد: أرى على الموقع هناك قياسات RIPE Atlas. هل يشمل أيضًا بيانات Luminati؟

كريستيان هاسلمان: إنه سؤال جيد. لست متأكدًا، بصراحة. أنا بحاجة للتحقق من ذلك. يجب، ولكن اسمحوا لي أن اتحقق من ذلك.

روس موندي: حسنًا. لا أكثر - أوه. آه، نعم. جاب [غير مسموع].

جاب أكيرهويس: بالنسبة للأشخاص الذين يريدون تشغيل تحقيقات أطلس الخاص بهم، هناك خمسة [معي]. لذا تعال وانظرني وأنا قد أحصل على أحدها. نحن حقًا بحاجة إلى بعض تحقيقات أطلس في هذه المنطقة، لذلك قد يكون لطيفًا.

روس موندي: حسنًا. شكرًا جزيلاً لك، كريستيان. عرضنا التقديمي التالي هو من جيف هوستون. هل لدينا ضاغط، من فضلك؟

شخص غير محدد: انقر، انقر.

روس موندي: انقر، انقر. ها نحن ذا. الكلمة لك، جيوف.

جيف هوستن: شكرًا لك، وصباح الخير لجميع الزملاء. أنا في انتظار الشريحة الأولى. شريحة غير صحيحة.

شخص غير محدد: هذا أنا.

جيف هوستن: هذا هو أنتم. هذا ليس أنا.

جاب أكيرهويس: أنت لست روي؟

جيف هوستن: أنا لست روي. الآن، أنا أرسلت هذه في وقت ما، وقد يكون تعفن الآن.

حسنًا. شكرًا. لدينا قليلاً من لقطة مستمرة، ولكن نأمل انها لن تؤثر على أشياء أكثر من اللازم. هل تم التحكم الآن؟ نعم. حسنًا. قليلاً إلى اليسار. شكرًا.

السؤال العام لـ ICANN في إدارة ملف KSK الجذر - تتمثل المشكلة الحقيقية في: ما عدد المستخدمين المعرضين للخطر؟ ونحن نعلم جيدًا أن حوالي 11-12٪ من المستخدمين تقريبًا، في هذه الأيام، يقومون بالتحقق من صحة DNSSEC ولن يحلوا اسما صالحًا. وبعبارة أخرى، فإنهم لا يقومون فقط بالتحقق من صحة DNSSEC، ولكن هذا كل ما يفعلونه. فليس لديهم سجلات خاصة بمحلل غير مصادق عليه. لذلك قد يتأثر عدد كبير من المستخدمين بنسبة 11-12٪، من لفة KSK كانت خطأ بشكل ما. لذلك هذا هو الحد الأعلى. هذا ما كنا قادرين على قياسه.

الآن، هناك نوعان من عناصر الخطر في هذه الدورة. الأول هو أن هذه هي المرة الأولى عندما تكون الاستجابة كبيرة نسبيًا جزءًا لا يتجزأ من إنشاء محلل التحقق من الصحة لأنه، عند هذه النقطة، تكون أكبر استجابة نحصل عليها في هذه المرحلة من الدور الرئيسي هي 1440 octets.

والخبر السار هو أن هذا النوع أقل من 1500، وهو حجم MTU الفعلي للإنترنت IPv4. والأخبار السيئة لن يختار V6 فقط عددًا تعسفيًا من 1280 - إذا كنت تسأل لماذا 1،280 (السؤال الغريب بشدة)، فإن الجواب هو: هذا هو 1024 بالإضافة إلى 256. فماذا يعني ذلك؟ لا شيء.

على أي حال، هذا العدد أكبر من 1،280. هناك العدد V6 الذي - غريبة بما فيه الكفاية، يصر على 1280، وهو أمر غريب. ولكنهم يفعلون ذلك. هذا أكبر. لذلك هناك مشكلة في التعامل مع التجزئة في V6 الذي يدخل الغرفة في هذه المرحلة.

الشيء الثاني الذي سمعته للتو هو هذه المسألة برمتها حول RFC 5011. لا يمكننا اختبار الإنتاج. يمكننا الاختبار، إذا كنت في بيئات ألعاب. الطريقة الوحيدة التي يمكنك اختبار نظام الإنتاج هو مع الشيء الحقيقي. لا توجد طريقة أخرى لاختباره على بيئة الإنتاج لديك.

الآن، إذا فشلت، فسوف تفشل [داك]. نتائج المحلل مماثلة. إذا لم تتمكن من الحصول على مفاتيح الثقة، فلا يمكنك القيام بأي شيء. وسوف تفقد الخدمة. انها ليست فقط حيث كنت تقدم منطقة لم يتم التوقيع فيها وأنت توافق. لا. لن يخدم المحلل بعد الآن. لذلك إذا كان المستخدم يمرر الاستعلامات فقط لهؤلاء المحللين، فسوف يعاني من فقدان الخدمة، والتي، كما قلت، تكون بنسبة 11-12٪ تقريبًا من جميع المستخدمين. هذه هي الإمكانات.

لقد سمعنا حتى الآن عن قياس المحللين. هذا هو السؤال. المستخدمون - وما سمعته هو المحللون. الطريقة التي يعمل بها هو أن المحللين التي تدعم آلية إشارة ترسل في إشارة. دوان أوضح هذا.

ولكن دعونا نتطرق إلى هذا أكثر من ذلك بقليل. اعتادت خوادم الجذر فقط على رؤية تلك الإشارة ويعيد بعض المحللين توجيها بشكل متكرر. لا أحد آخر. لذلك هذه إشارة إلى أنني لن أقشي سرا ولكن من الصعب جدًا التوصل إليه إلا إذا قمت بتشغيل خادم الجذر والبحث.

ثانيًا، هذا استعلام بدون إسناد. إذا كنت معيد التوجيه الخاص بي، فإن الأمر كما لو كنت التقارير، وليس لي، لأنني الآن غير مرئيًا. لذلك كل هؤلاء المحللين الذين يستخدمون وكلاء الشحن غير مرئيين هنا. فهم يرتبكون بين إسناد تلك الإشارة.

الآن، لقد سمعت للتو أن الإشارة هي إشارة، ولكن في عالم DNS، فإن بعض المحللين أكثر أهمية بكثير من غيرهم. توفر خدمة DNS العامة من Google نظام أسماء النطاقات لنحو 14-15٪ من سكان العالم. يعتبر المحللون مهمين للغاية. يوفر المحلل الخاص بي في المنزل الإجابات لي. وأود أن أتردد في القول أنه غير مهم. إنني أحب ذلك، ولكن بقيتكم لا يهتمون حقًا، ولا ينبغي لك. لذلك حاولوا فهم أن بعض الإشارات مهمة حقًا والبعض الآخر ليس مهمًا لأن عدد المستخدمين غير واضح في تلك البيانات.

أيضًا، ما هو غير واضح هو أنه إذا فشل محللا ما، فإن معظم الناس في [غير مسموع] يأتون إلى أدوات حل متعددة. لذلك حتى لو حصلت [داك] من A، فقد تحصل على إجابة من B. لذلك فإنه ليس سيئًا كما يبدو. إذا كانت هناك وسيلة، فسوف يجد المستخدمون ذلك. 8145 لا يمكن أن أقول لكم ذلك.

لذا، فإن هذه المسألة برمتها، باعتبار مقياسين للحلول كغاية في حد ذاتها، ليست مفيدة في هذا الصدد. إجابة خاطئة. ما تريده فعلا هو إجابة تخبرنا بالبيانات التي تحاول الحصول عليها. ما نوع الاستعلام الذي سيكشف عن حالة مفاتيح المحللين التي يستخدمونها - وهذا الجمع - يعود إلى المستخدم؟

هل يمكنني معرفة ما إذا كنت سأكون ضحية لخدمة DNS؟ هل سيبقى جميع المحللين الذين أعول عليهم حاليًا أسودًا، أم سيبقى سيحافظ أحدهم على العمل؟ لأنني بحاجة فقط وأنا بخير.

فهل يمكننا استنباط مثل هذا الاستعلام الذي يمكن أن يكشف ذلك؟ لا، نحن لا نستطيع. الآن، إذا قال أحدهم: "أنت مخطئ، جيف. لدي طريقة، والحمد لله. أحبكم كثيرًا. دعنا نبدأ في القيام بذلك. ولكن حتى الآن، هناك الكثير من الاكتشافات. ولا يمكننا القيام بها.

يجب تغيير شيء ما. إما أن تقوم بإنشاء نطاق ذهبي داخل DNS يتم حله بشكل مختلف، أو تقوم بتغيير سلوك المحلل. علينا القيام بشيء ما.

ماذا لو تمكنا من تغيير سلوك المحلل؟ تذهب، "لا يمكنك القيام بذلك." لقد فعلنا فقط. RFC8145 غير سلوك المحلل. لذلك نحن نرى الآن أن باعة المحلل - شكرًا لك، cz.nic، شكرًا لك، ISC، شكرًا لك، غير مقيد - عرضة لتغيير التعليمات البرمجية مع الفكرة الصحيحة.

ماذا لو استطعنا ذلك؟ هذا هو جوهر الفكرة. هل يمكنني وضع تسمية سحرية؟ انها ليست اسم النطاق. انها مجرد تسمية. إذا كنت ترى هذه البطاقة في اسم نطاق وكنت محلل تتحقق من الصحة، فقد ترغب في تغيير من جيد إلى سيئ في إجابتك إذا - الآن الحالة الأولى هي: "هل هذا المفتاح علامة مفتاح TA موثوقة؟" إذا لم يكن ذلك، سوف ترسل

الإجابة مرة أخرى. واجعلها SERVFAIL; RCODE3, كما أسميها. وبعبارة أخرى، إرسال فشل مرة أخرى إذا كنت لا تثق هذا المفتاح.

لأننا بحاجة للكشف - وسترى لماذا - الفرق بين المحللين التي تدعم آليته وتلك التي لا تفعل ذلك، يمكنك أيضًا القيام بالعكسية المنطقية: "هل هذا ليس مفتاحًا موثوقًا به؟" إرسال مرة أخرى جيدة إذا لم يكن موثوقًا به. إرسال مرة أخرى SERVFAIL إذا كان موثوقًا به.

ثلاث استعلامات. أنت النطاق المفضل - لأنه يمكنك إجراء هذا الاستعلام وكذلك أي شخص آخر، يمكنك إجراء الاستعلام حتى كمستخدم. Label.some.signeddomain. لا يهم ما هو النطاق الموقع. أيضًا، لأنه مهم نوعًا ما ، لإعداد التسمية التي تم توقيعها عن قصد بشكل سيء. أنا متأكد من أنك عندما تقوم بإعداد DNSSEC كنت قد أنتجته لكومة كاملة من تلك لأنه من السهل حقًا إعداد واحدة وتوقيع بشكل سيئ.

إذا نظرتم إلى نوع الإجابات التي تحصلون عليها، فهناك أربعة أنواع من سلوكيات المحللين التي نهتم بها، يدعم المحلل الآلية الجديدة وقد حمل KSK الجديد. سأحصل على السجل A لطلب البحث الأول، SERVFAIL للثانية، وSERVFAIL للثالث. ويدعم المحلل الآلية ولكنه لم يحمل المفتاح بعد. سيتم تبديل استعلاميي الأولين. SERVFAIL و A سوف يأتيان في اثنين [باعتبارهما] حالتين مختلفتين. إذا لم يتعلم المحلل عن هذه الآلية الجديدة، فسوف أحصل على نمط مختلف: السجل A، السجل A SERVFAIL ،. وإذا لم يتم التحقق من المحلل، فسوف أعيد جميع سجلات A لأنه لا يتم التحقق من صحتها. لذلك سوف تعمل دائمًا. حتى أستطيع التمييز بين الحالات الأربع التي اهتم بها فعليًا.

ولكن ليس لديك مجرد محلل واحد. أنت تميل إلى امتلاك المال، وهم يميلون إلى أن يكونوا وكلاء، الخ، أصبح الوضع أكثر تعقيدًا. ولكن الغريب أن تحليل النتائج مماثل جدًا. إذا استطعت الحصول على إجابة من جميع المحللين المتكررين عن الاستعلام الأول، فلا بأس. إذا حصلت على SERVFAIL للثانية - SERVFAIL، SERVFAIL، A

يقول أنك جيد. SERVFAIL, A, SERVFAIL يقول أنك في مكان سيء. ولن تكون مجدية لك.

يذكر النوعان الآخران من الإجابات، في كل من المحللين التي تستخدمها، وبعضهم لا يدعم هذه الآلية [و]لا يمكن معرفة ما سيكون الجواب. هذا اثنتين من النتائج حيث كنت قد حصلت على نتيجة غير معروف. بطبيعة الحال، إذا كنت قد حصلت على كل ما، مهما كانت الإجابة، فهذا جيد لأن واحد على الأقل من المحللين الخاص بك لا يتحقق من الصحة.

لذلك ضعه في صفحة ويب. افعلها بنفسك. اختبرها نفسك. أو، إذا كنت تعرف حملة إعلانية عبر الإنترنت - وأفعلها - ضعها في نص جافا البرمجي أو HTMLLM5 في حملة إعلانية وقس بضع مئات من ملايين المستخدمين لأن هذه التقنية لن تظهر في الواقع حالة تغيير المفتاح فقط ولكن أيضًا حالة مدخول الآلية نفسها لكل مستخدم. لذلك فمن الممكن فعلاً في حملة إعلانية عبر الإنترنت التتبع الفعلي ليس فقط لمدى تشغيل هذه الآلية ولكن ما يكشف عن حالة المفاتيح الموثوق بها بينما يحدث هذا.

نقوم بتشغيل DNS، لذلك فمن الضروري التأكيد للتفكير في الخصوصية والأمن. هذا لا يكشف عن هويات المستخدم النهائي. بل فقط المحللين، وليس المستخدمين النهائيين. وهي لا تحتوي على أي معلومات تعريف المستخدم النهائي. لا يلزم ذلك لأن المجموعة هي التي تنشئها، لذا فإن ما تفعله هو نشاطك التجاري. ليس عليك تحديد المستخدمين.

لا تغيير أبدا غير الآمنة لتأمينه. هذه فكرة سيئة حقًا، وهذا لا يفعل ذلك. فكل ما يفعله هو تغيير مصدق على انعدام الأمن في ظل حالات معينة جدًا اعتمادًا على حالة مفتاح الثقة. لذلك أنا أحول أساسا الجيد إلى سيئ، بحيث يبدو أكثر أمنًا قليلاً من التحويل سيئ إلى جيد.

أي شخص يمكنه القيام بذلك. فهذا ليست حصريًا لخوادم الجذر أو أي شخص يمكن القيام به. يمكن لأي شخص أن يفعل ذلك إذا كان تريد، وتحصل على البيانات مرة أخرى بنفسك. لا أحد آخر. لذا فإن النتائج تعود إليك كجواب على استعلامات DNS. إنها طريقة أكثر ديمقراطية للقيام بهذا الاختبار وبالتأكيد أكثر انفتاحًا. يمكن لمزودي خدمة

الإنترنت اختبار أنفسهم. ويمكن للمستخدمين اختبار مزودي خدمة الإنترنت. إن الأمر متروك لكم. إنها طريقة أوضح بكثير للقيام بذلك.

هناك مشروع هناك. كالمعتاد مع المسودات، في هذه المرحلة تكون الفكرة حديثة نسبيًا. أعتقد أنه قبل حوالي أسبوعين. إذا كان DNS اللعبة الخاصة بك - وأود أن نقدر بالتأكيد أي ردود فعل، وحتى المؤلفين المشاركين معي جو أداماس و وارين كوماري. نحن مهتمون جدًا بالتعليقات التي قد تكون لديكم حول جدوى هذا النهج لأنني أؤمن به، على عكس الآخر، حيث تأخذ إشارة RFC 8145، وتفسر ما تسمعه من حيث الإسناد، ومن ثم فهم بطريقة أو بأخرى أهمية هذه الإشارة مقابل عدد المستخدمين، وهذا نهج مختلف تمامًا يحاول أن ينظر إلى حالة المفاتيح موثوقة للمستخدمين وبيئة DNS شاملة بنفسه. ولن يكشف عن قدرة المحلل الفردي بشكل عام لأن DNS ليس مثله. وسوف تكشف عما إذا كان المستخدم هو في مكان جيد أو مكان سيء حول دورة المفتاح.

أعتقد أنني الآن في الوقت الضائع، ولكن هناك 46 ثانية للأسئلة. شكرًا.

روبرت مارتن ليجين: مرحبًا. هذا هو روبرت مارتن ليجين من PCH. إنني دائمًا أحب العروض التقديمية. هل فكرت في النظر في شيء مثل خيار إDNS [غير مسموع] لهذه [crows] ضرب خوادم الاسم لمعرفة ما إذا كان الوكيل في الأمام يضع تلك أم لا؟

أيضًا، شيء واحد يمكن أن يكون قد تم الكشف عنه، إذا كان هناك وكيل يُستخدم، وإذا كان RFC قد شمل شيء مثل وضع في خيار EDNS التي لن تحصل على توجيه من قبل معيد التوجيه.

جيف هوستن: لقد انقلبت كل هذه الحجة على عقبها. فلا علاقة لها مع الاستعلام وتقوم بكل شيء للإجابة. هذا هو، إذا كنت سوف، الجزء الأساسي. تقريبا أي معلومات تأتي إلى خادم اسم موثوق، والتخزين المؤقت تكون غير مهمة. إعادة توجيه غير مهم. ما كنت بعد كمستخدم واحد من تلك الأنماط من ثلاثة استعلامات.. لذا، فإن الإجابات التي تعود إليك مهمة.

ومن الغريب أن يتم تجاهل خوادم الأسماء الموثوقة في الجذور. بالتأكيد، أنهم يعرفون الحالة الرئيسية الخاصة بهم، ولكنهم لا يعرفون المحللين لديك. أنت فقط من تعرف. هذا الاختبار لك، وليس لهم.

غريبًا، لروي أكثر من هنا، في مكتب CTO - روي كان ينظر بعد دورة المفتاح - انها حقًا بعد حيث ستحدث العناوين في الصحيفة. هذه مشكلة المستخدم، وليست مشكلة محلل. لذا أحاول أن أركز هذا على المحللين. لذلك، فإن الإجابات هي المهمة، وليس الاستعلامات.

روبرت مارتن ليجين: أجل. يتمثل المخصص في التركيز الخاص بك، ولكن الإنترنت ليس فقط المستخدمين. اليوم، هناك الكثير من الأنظمة الآلية. إذا كان هناك شيء ينكسر ولا تلاحظ الناس لمدة شهرين أو أيا كان، فإنه من المرجح جدًا أن يحدث في الأنظمة الآلية لأن العديد من النظم لا تنتج أي نوع من الأخطاء المرئية إلى أي شخص. أمي، إذا كان جهاز الكمبيوتر الخاص به لا يعمل، فاتصلي لاستدعاء شخص ما. فهي لن يموت لأن الإنترنت لديها لا يعمل. إنها أمور مختلفة تحتاج إلى قياس.

جيف هوستن: ما هو هذا العرضة، إذا كنت قد حصلت عليه هنا في مكان ما، إنه في الواقع كمية كبيرة من الاستعلامات - حيث وضعت حول الحملة الإعلانية؟ إذا قمنا بهذا بشكل صحيح، فإنه يمكننا إجراء كميات كبيرة من العينات. ولن نختبر المستخدم من أي وقت مضى. أنا لست متأكدا من أنه يمكننا القيام بذلك. ولن نختار كل جهاز. أنا لست متأكدا من أنه يمكننا القيام بذلك. ولكن من خلال نفس الآلية التي تخبرنا أن حوالي 11-12٪ من المستخدمين يستخدمون فقط التحقق من DNSSEC، يمكننا أن نخرج بنفس الإجابات هنا ونفس مستوى الثقة حول ما إذا كانت دورة KSK ستعمل أم لا. هذا هو القصد الكامل هنا.

روي آريندس: هل يمكنني الرد على ذلك؟ أريد فقط أن أشير إلى أن الأنظمة الآلية - الناس الذين يبنوها، والناس الذين يعملون عليها - يمكن أيضًا أن تستخدم هذه التقنية.

روس موندي: أعتقد أننا بحاجة إلى التحرك الآن. نحن نريد أن نعطي روي ما يكفي من الوقت لتغطية عرضه وتقديم الأسئلة والأجوبة بشأن استبدال مفتاح الجذر نفسه. الكلمة لك، روي.

روي آريندس: هذه هي المرة السابعة لي هذا الأسبوع التي أقدم فيها نفس العرض التقديمي، لذلك أود أن أرى أيدي الذين لم ير هذا العرض التقديمي من قبل.

هذا يكفيني. وسوف أستمر. اسمي روي أريندز. أعمل في مكتب CTO. أنا باحث. تمهيد صغير - لست متأكدًا مما إذا كان هذا ضروري هنا أم لا. إذا كنت تقوم بالتحقق من DNSSEC، فإنك بحاجة إلى مرتكز الثقة. ومرتكز الثقة هو مفتاح عام. ويجب ألا يعيش المفتاح العام إلى الأبد، لذا يجب تجديده. في DNSSEC، نسمى ذلك بتداول المفتاح. يمكنك القيام بذلك أوتوماتيكيًا أو يدويًا، ولكن ليس هناك طريقة بالنسبة لنا - زملائي هنا المذكورة بالفعل - للتحقق مما إذا كان لديك المفتاح المكون بشكل صحيح أم لا.

عندما قمنا بتصميم هذا قبل بضع سنوات، كان هناك فريق تصميم مناسب مع [كتل] توعية، الخ وضعنا معًا الخطط. تحدثنا إلى البائعين. تحدثنا إلى الحكومات، وما إلى ذلك، وكان 11 تشرين الأول (أكتوبر) 2017موعدًا هامًا. وذلك لأننا في الواقع لم نعرف من كان يتحقق أو لا، أو من كان لديه المفتاح ذو التكوين الصحيح.

وبطبيعة الحال، لدينا عملية لذلك. في 11 تموز (يوليو) 2017، قدمنا KSK الجديد، ومن ثم قمنا بمراقبته بحثًا عن أية تغييرات جوهرية في حركة مرور خادم الجذر. صديقي دوان يعمل لدى فيريسين، شريك إدارة منطقة الجذر. وكان بإمكانه الوصول إلى حركة المرور في منطقة الجذر A وJ. لقد وصلنا إلى حركة المرور منطقة الجذر Bو D وF، وL

أحتاج لبعض الماء.

شخص غير محدد: [غير مسموع] بعض الماء.

روي آريندس: لا، لقد حصلت على الماء. حصلنا توصلنا إلى حركة المرور للجذر Bو D وF، وL وفي نهاية المطاف حصلنا على جميع خوادم الجذر لتوفير [غير مسموع] لنا، وهو شيء آخر في التحقق من عدد المرات التي يتم إرسال استعلامات DNSKEY إليه غالبًا. تعرفون جميعًا أنه إذا كان [لا يمكن] التحقق من صحة المحلل، فسوف تحدث عدوانية كبيرة. وسوف تتطرق فقط للسؤال.

قبل بضع سنوات، جيف وأنا قمنا ببعض البحوث حول الاستبدال والموت يمكننا تسميتها بالاستبدال وكوماتوس، أليس كذلك؟ لأن التأثير المماثل لا يزال ساريًا. المحللون المصادقون سوف يمضون في طريقهم للحصول على DNSKEY. ولكن لا شيء يحدث. لدينا احصائيات جميلة بشأن ذلك، والرسوم البيانية الجميلة، لكنها تظهر فقط شيئًا ما خط مسطح في 11 تموز (يوليو).

وبعد 30 يومًا - كانت هذه فترة تعليق لمدة 30 يومًا. كان دوان الرسم البياني جميل هناك، حيث يمكنك أن ترى مبادلة رائعة - وكان لا يزال هناك [غير مسموع] حركة مرور. لا يمكنك رؤية شيء آخر. لذلك واصلنا.

19 أيلول (سبتمبر). هذا ما أشرت إليه في وقت سابق: عندما قدم شريكنا في إدارة منطقة الجذر، فيريسين، شكل ZSK جديدًا. هذا شيء خاص. وهم يفعلون ذلك كل ثلاثة أشهر. هذا استبدال ZSK قياسي. انهم يفعلون ذلك كل ثلاثة أشهر منذ 2010. والاستثناء الوحيد هنا هو أن هذه هي المرة الأولى التي زاد فيها الحجم. أعتقد أن الاستجابة [زائدة]. تحدثنا عن ذلك أيضًا، سوف أواصل.

لقد شاهدت هذه الشريحة. إنه من العرض [غير مسموع]. حتى وقت قريب، لم يكن لدينا معرفة عن من كان لديه مرتكز الثقة المكونة. تحدثنا بالفعل عن RFC 8145. وتحدثنا بالفعل عن BIND9 وغير مقيد، لذلك سوف اتخطي ذلك.

أنها تقول هنا "لا يُعرف تنفيذ آخر". تعلمت للتو من [أندريه فيليب] أن KNOT سوف يكون في المستقبل القريب نسخة مع [غير مسموع] في مكان، لذلك هذا جيد. أنا لا أعرف عن PowerDNS recurser. إذا كان لديهم ذلك، فأنا لا أعرف. ولكن Microsoft - recurser

لدي رقم هنا. حوالي 4.2 مليون عنوان فريد من نوعه لإرسال الاستعلامات إلى خوادم الجذر. هذا رقم قديم من خوادم الجذر B انسى هذا الرقم، إذا استطعت. وربما يكون أعلى بكثير إذا قمت بدمج كل خوادم الجذر معا. إذا قمت بإجراء دراسة طولية حول عدد من العناوين الفريدة من نوعها، فسوف يرتفع العدد بطبيعة الحال. لذل 4.2 مليون هو أقل.

الأرقام التي حصلنا عليها بالفعل مع بيانات RFC 8145 منخفضة للغاية. سوف أتطرق لها في غضون ثانية.

ها نحن. هذه هي الإحصاءات لدينا. انها حتى 24 تشرين الأول (أكتوبر) من 1 أيلول (سبتمبر). هذا هو عندما كان على السفر لحضور اجتماع RIPE. لدينا حوالي 27,000 من بيانات تقارير أولئك 4.2 مليون. ويبلغ العدد الإجمالي لـ KSK-2010 فقط 1.631. وهذا يشكّل 6%.

الآن، لم أكن أتطلع إلى ما إذا كان هؤلاء المحللين في الواقع يتحققون من الصحة، لذلك قد لا يكون [مجموعة DO bits]. قد يكون لديهم [RD bits]، شخص ما التحقق أساسًا مما إذا كان إرسال الاشارة الأساسية هذا يعمل بالفعل أم لا. إذا قمت بذلك، فإن العدد ينخفض قليلاً، ولكن ليس بشكل كبير.

وقد أشار أصدقائي بالفعل إلى ذلك. التحليل معقد. أنا فعلا أحب اقتراح جيف هوستون. أتمنى لو كان ذلك قبل عامين. أنا حقا أحب ذلك - أوه، قبل أن أقول شيئا خاطئاً، هذا رأيي الشخصي. أنا لا أتحدث عن ICANN. ولكنني حقا أحب الاقتراح.

نحن نعرف بعض الأسباب وراء الإبلاغ عن KSK-2010 وليس KSK-2017. أحدث نسخة برامجيات بيركلي لنظام اسم النطاق على الإنترنت تبلغ عن مرتكز الثقة، على الرغم من انهم لا يتحققون من صحتها، وهو أمر مزعج لأن الآن لديك إشارة كاذبة. أنت لا تقوم بالتحقق من الصحة. لقد تمت تهيئة هذا المفتاح وربما لن يتم تحديثه نظرًا لأنك لا تقوم بالتحقق من بالصحة.

في الأصل، قبل 5011، كان هناك هذا التكوين القديم [غير مسموع] في برامجيات بيركلي لنظام اسم النطاق على الإنترنت التي تذكر مفاتيح موثوقة. وقد وضعت مرتكز الثقة الخاص بكم، الأمر الذي يجعله منطقيًا. ولكن بعد ذلك وصلنا RFC5011، وتحتاج إلى تكوين مختلف إلى [غير مسموع] الآن والتأكد من أن بعض المفاتيح يمكن تحديثها مع 5011. يتم تكوين الآخرين يدويًا. لذلك تستخدم برامجيات بيركلي لنظام اسم النطاق على الإنترنت مفاتيح مدارة للقيام بالمفاتيح المدارة 5011. بعض الناس مشوشة حول ذلك.

سوف اتخطي هذا. توج مشكلات عديدة. هناك الكثير جدًا للإبلاغ عنه هنا.

عودة إلى الخطة والعملية، قلت بالفعل أنه في 19 أيلول (سبتمبر)، لم يكن هناك شيء يحدث هنا. في هذا الوقت تقريبًا - يعتبر هذا صحيحًا قبل اجتماع DNS-OARC - حيث حصلنا على تقرير فيريسين، وأيدنا هذه البيانات الخاصة بنا.

ولا يمكننا أن نقرر فقط الأمور المخصصة، لذلك استشرنا الخطة التشغيلية - وهي خطة عمرها بضع سنوات؛ وقد صدق المجتمع عليها - وهو يقول إن شركاء إدارة منطقة الجذر، فيريسين وICANN، قد يقومون أيضاً بتمديد المرحلة الجديدة لأرباع إضافية. على سبيل المثال، إذا أشارت معلومات جديدة إلى أن المرحلة التالية قد تؤدي إلى مضاعفات، فإن المرحلة الحالية ستكون مطولة. ويشار إلى ذلك على أنه سيناريو موسع. في 27 أيلول (سبتمبر)، بدأ سيناريو تمديد، حين قررناها وجعلناها علنية.

لقد سمعت بعض التقارير بأن بعض القوائم البريدية حصلت على هذه المعلومات في وقت أقرب من غيرها، ولكن ذلك لأن فريق الاتصالات لدينا ليس على جميع القوائم البريدية DNSSEC. لذلك كان علينا أن نحيل تلك المعلومات بسرعة.

كما ذكرت من قبل، نحن لا نعرف كيف تمثل مجموعة من المصححين الذين يبلغون عن ماهية بيانات العلامة الرئيسية. ذكر جيوف من قبل أن المصادقة ليست هي نفسها للمستخدمين النهائيين. وأنا أخطط للعمل بشكل وثيق مع جيوف. يمكننا أن نشارك بعض البيانات، جيف وأنا، وبالتالي فإن الأرقام التي تبلغ عن علامات مفتاح المصادقة يمكن أن تفيد بالفعل، إذا كان هذا يجعله منطقيًا.

عدد المستخدمين وراء ذلك؟ سمعت عددا في يوم آخر أنه 750 مليون حاليًا وراء التحقق من صحة المحللين. هل هذا صحيح؟

جيف هوستن: Google.

روي آريندس: وراء Google. عذرًا. حسنًا. التخفيف صعبًا. كانت لدينا بالفعل حملة أخرى سنوية للوصول إلى المشغلين. لا تجعل هذه المشاكل الخاصة بالتنفيذ التي ذكرتها للتو من قبل المشكلة أسهل. لقد كتبنا جميع البرامج في الماضي. ونحن نعلم جميعا الأخطاء الحالية. لا يمكننا إلا تجزئتها لهم عند القيام بذلك في الواقع. كما قال جيوف من قبل، يمكنك القيام فقط بهذه الدورة التشغيلية. لا يمكننا اختبار هذا في بيئة المختبر.

لقد أجلنا دورة المفتاح حتى نحصل على مزيد من المعلومات وفهم الوضع بشكل أفضل. وسوف تكون ربعية على الأقل. بالنسبة لأولئك الذين لديهم أسئلة حول ذلك، فهذا يعني ربع أو أكثر من رفع. انها دائمًا موازية لربع. والسبب في ذلك هو أن الاحتفالات الرئيسية التي تنظمها ICANN كل ثلاثة أشهر. لم نحدد بعد عدد الأرباع المؤجلة.

سنقوم على الأقل بالتخفيف جزئيًا. لقد استأجرت شخصًا، وهو مقاول، لتتبع 500 الأولي التي رأيناها في أيلول (سبتمبر). كان هذا قبل إصدار النسخة غير المقيد مع إرسال الاشارة الأساسية افتراضيًا.

يستمر جمع البيانات. أريد فقط أن أذكر شيئًا عن النسخة غير المقيدة. وذكر دوان أنه تم إصدار النسخة غير المقيدة في 10 أو 11 تشرين الأول (أكتوبر)، وأن ذلك تزامن مع إشارة. ليس هناك يوم يتزامن مع تلك الإشارة. ان يوم 10 تشرين الأول (أكتوبر) أيضًا في اليوم الأخير الذي تم استخدام ZSK-q3. وكان جزء من الارتفاع هو أن ZSK-q3 تمت إضافتها إلى الإشارة.

أيضًا، إن مجرد إرسال النسخة غير المقيدة لهذا الاستعلام لا يعني في الواقع أن النسخة غير المقيدة خاضعة للتحقق. قد يكون fowarder أمام -

جاب أكيرهويس: لا تعطي سوى إشارة عند التحقق من صحتها. انها مختلفة عن برامجيات بيركلي لنظام اسم النطاق على الإنترنت.

روي آريندس: حسنًا. إذا سألت عن النسخة غير المقيدة، فإن الاستعلام سيستخدم علامة المفاتيح، وهو نطاق المستوى الأعلى، في الأساس، سوف يذهب إلى الجذر ويسأله عنه؟ فهو يحل العلامة الرئيسية.

جاب أكيرهويس: ذلك يعتمد حقًا على كيفية التكوين لإكمال سلسلة DNS. انها محلل التخزين المؤقت. إذا كان المستخدم قد وضع بطريقة ما على [غير مسموع] وكلاء الشحن - فسوف يقوم الناس بالأشياء الغريبة، مثل وضع في وكلاء. يمكن لبعضهم بالفعل-

روي آريندس: عذرًا. كنت أكل في وقتي. دعونا نأخذ هذا في دقيقة واحدة. سأعرض لكم بعض البيانات لاحقًا. كانت مجرد مساعدة تسمعونها عن أن النسخة غير المقيدة ليست دائمًا مشكلة.

على أي حال، آخر شيء أريد أن أقوله عن هذا الجزء هو: أنه يرجى عدم إزالة KSK-2017. ما حدث عندما أعلنا أننا أخرنا الدورة هو أن بعض الناس قررت عدم تكوين أو إزالة KSK 2017 من تكوينها. لا تفعل ذلك.

لقد وصلت على شريحة الأخرى سريعة حقًا. إنها حول تردد دورة KSK للجذر. كان هذا عرضًا الذي كان من المفترض أن أقدمه لفريق الخبراء التقنيين، ولكن حصلت على ثلاث دقائق لذلك. الآن ألقي نظرة على الساعة ولدي دقيقة ونصف فقط لهذا.

سريعًا حقًا، هذه مناقشة صغيرة حول تكرار دورة KSK. بدأنا استخدام المفتاح القديم في عام 2010. نخطط الآن لبدء استخدام مفتاح الدخول الرئيسي KSK الجديد في عام 2018 إذا لم يحدث أي شيء آخر. بعض الناس يصرون على تكوين مرتكز الثقة الجديدة يدوياً. تعتمد بعض الناس على 5011m، والبعض يستخدم اشياء التحديث التلقائي غير 5011. قد تكون للمصادقة بعض المشكلات في التكوين: أقسام للقراءة فقط أو باستخدام مواضع تهيئة غير صحيحة. ونحن نعلم أن الخطأ وارد. يعتبر قياس مرتكز الثقة أبعد ما يكون عن الأمثل.

ويعتقد أن هناك مدرستان. متكرر التغيير. وهذا غير معني في كثير من الأحيان. أنا بحاجة إلى جعل ذلك واضحاً تكرار التغيير لا يعني التغيير بصورة أكبر. تكرار التغيير يعني فترة زمنية محددة. تكرار التغيير يعني، "مهلا، لم يتم الكسر. لم يحدث شيء، فلماذا يجب التغيير؟ " لذلك ليس له فاصل زمني محدد.

تطرق المجتمع التقني DNSSEC منذ بضع سنوات إلى نوع من التغيير في كثير من الأحيان، والتي كانت خمس سنوات. وأنا أعلم أننا الآن [غير مسموع] ذلك.

قررت أن وضعت هنا بعض نطاق التردد. نطاق التردد هو التردد المنخفض والتردد العلوي. التردد العلوي سهل. دعونا نستغرق خمس سنوات من الآن. الحد الأدنى المطلق هو ثلاثة أشهر بسبب مراسم التوقيع الرئيسية التي لدينا. إذا كنا نريد تغيير المفتاح لعد

أكثر من ثلاثة أشهر - وأنا أعلم أنكم قد تجدون هذا مثيرًا للسخرية - فقد سمعت الناس يقولون علينا أن نفعل هذا كل أسبوع. هذا هو السبب في أنني وضعت هذا هناك. الحد الأدنى للنسخة المقيدة، وهو أعلى تردد، هو ثلاثة أشهر. أي شيء أكبر يحتاج إلى كمية كبيرة من العمل.

ما هو تأثير القيام بذلك كل ثلاثة أشهر؟ لدينا ثلاث مراحل التي تتعامل مع إدخال هذه المفاتيح. إذا قمتم بذلك كل ثلاثة أشهر، يمكنك طي ثلاث مراحل في واحدة. يمكنكم إدخال مفتاح جديد، يمكنكم بدء التوقيع مع المفتاح الحالي، وإلغاء المفتاح القديم. هذه مشكلة كبيرة. سوف أتخطي السطر الثاني. وبطبيعة الحال يحتاج إلى إعادة تصميم - الخطة التشغيلية بأكملها - ولكن الحد الأدنى بحجم استجابة DNSKEY هو 1,986 بت. هذا نوع من عدم التطرق.

شخص غير محدد: [غير مسموع]

روي آريندس: أجل. كما يجب تحديث عمليات النشر اليدوية أو شبه التلقائية كل ثلاثة أشهر. لذلك وضعت فقط هذا هناك. هذا ليس رأيا. هذا ما سيحدث.

عندما تفعل ذلك ستة أشهر، فلن تكون هناك مشكلة في حجم الاستجابة لأنه ليس عليك للقيام بهذا التداخل الكامل. لا تزال تدخل مرحلتين في مرحلة. المرحلة واحدة هي أن تقوم بإدخال المفتاح الجديد والمرحلة الثانية هي أن تبطل المفتاح القديم وتستخدم المفتاح الجديد.

هناك مشكلة صغيرة هناك. إذا أدخلت هاتين المرحلتين في واحدة، فلن يمكنك التراجع. لذلك نحن بحاجة إلى إعادة تصميم العملية برمتها. وأعتقد أنها في الواقع فكرة جيدة أن يكون هناك خيارًا للتراجع.

آثار التغيير كل تسعة أشهر: تزيل مشكلة حجم الاستجابة، ويمكنك استخدام التصميم الحالي لخطة التغيير، ولا يحدث التردد الأعلى تغييرات جوهرية على التصميم. هذا من الرجال الذين يرون تغيير المفاتيح. لاحظت آراء مختلفة من المجتمع التشغيلي، ولكن هذا من وجهة نظرنا.

ومع ذلك، قد يكون هذا الأمر محرجًا فيما يتعلق بالتوقيت. كل عام، تتحرك فتحة الوقت إلى الأمام موسمًا. كل أربع سنوات، سيكون لدينا مرتين في سنة واحدة. هذا ليس الأمثل أو مشغلي بسبب عدم القدرة على التنبؤ. هذا رأيي.

آثار التغيير كل تسعة أشهر: تزيل مشكلة حجم الاستجابة، يمكنك استخدام التصميم الحالي لخطة التغيير، ويكون التردد أعلى بحيث لا تحدث تغييرات جوهرية على التصميم.

آثار المتداول بعد أكثر من سنة واحدة: ليس هنا فرق كبير في القيام بذلك كل عام. انها نوع من يوم Groundhog إذا كنت تفعل هذا كل عام أو كل N سنوات في نفس الوقت بالضبط.

أستطيع أن أتخيل أننا إذا فعلنا ذلك بشكل متكرر - وهذا لا يعني في كثير من الأحيان. وهو ما يعني بفاصل زمني محدد؛ ونحن نفعل ذلك ليس أسرع من سنة واحدة ولدينا الحد الأعلى البالغ خمس سنوات.

تحدثت إلى جاب أمس، وطرح نقطة جيدة للغاية. أنا لا أريد أن سرقة السؤال منك، ولكن كان لدى جاب نقطة جيدة للغاية. نظر لي وقال: "يجب علينا أولاً القيام بالتغيير رئيسية قبل أن نتخذ أي قرار؟" انه على حق تمامًا. وعدت أن أقوم بهذا العرض التقديمي. فأجبرني. لذا أعتقد أنه لا يزال بإمكاننا إجراء هذه المناقشة. ولكن، نعم، فإنه من السابق لأوانه بسبب أننا لم ننفذ التغيير حتى الآن. شكرًا.

روس موندي: شكرًا لك، روي. دوان، تفضل.

دوان ويسلز: روي، هل يمكنك العودة إلى الشريحة مدة ستة أشهر لثانية؟ هل يمكنك توضيح ذلك؟ قلت لا توجد وسيلة للتراجع، ولكن ماذا عن التمديد؟ هل تتراجع وتوسع نفس الشيء في هذه الحالة؟

روي آريندس: لا، انها ليست نفس الشيء. إذا قمت بإلغاء المفتاح القديم في اللحظة التي تبدأ فيها باستخدام المفتاح الجديد، فلن تتمكن من التراجع. ولكن إذا أخرت إلغاء المفتاح القديم لمدة موسم، فسوف تظل بإمكانك التراجع.

دوان ويسلز: حسنًا، أنا أفكر في الوضع الحالي، حيث قمنا بتمديد - فترة ما قبل النشر، في الأساس. لقد مددنا ولم نذهب إلى الخطوة التالية. ربما من الصعب جدًا معرفة ذلك في الوقت الحالي، ولكن يجب أن نتحدث لاحقًا.

روي آريندس: أجل.

روس موندي: أجل. أعتقد أنني قد تطرقت إلى بعض الأمور الهامة للغاية. أحد الأمور تتمثل في أنه نظرا لأننا مجموعة مرتبطة بلجنة SSAC، تعاملت SSAC63 مع الكثير من هذه القضايا منذ عدة سنوات. وكان أحد الأشياء الهامة التي لوحظت هو أننا يجب أن نحاول أن نتعلم بقدر ما نستطيع من هذا التغيير بحيث يمكن استخدامها في التغييرات في المستقبل. وأعتقد أن هذا هو بالضبط ما بدأناه هنا. لذلك هذا ممتاز.

هل لدينا أي أسئلة سريعة أخرى لروي؟ الغداء ينتظر بالنسبة لأولئك الذين ينضمون إلينا لتناول الغداء.

روبرت؟

روبرت مارتن ليجين: نعم، لا يمكنك أن تبقيني منتظرًا. شيء واحد يمكن النظر إليه من حيث كل هذا - ما يجدي وما لا يجدي - ماذا سيكون، دعونا نقول - سوف تفكر في أنني مجنون - نصف بيانات توريد الجذر الموقعة مع المفتاح القديم ووقع النصف الآخر مع المفتاح الجديد. إذا كنت ترى من الذي سيظل يسأل - توقف عن قول لا. لن تتمكن من رفض الخدمة، في الواقع، بالنسبة للمستخدم، ولكنك سترى من سيستخدم المفتاح.

روي آريندس: هذه الفكرة ليست فكرة سيئة في حد ذاتها، ولكن تم ذكرها مرتين، وقد نظرنا في هذا. وتتمثل الفكرة أساسًا أن تكون مجموعة من خوادم الجذر تخدم منطقة الجذر بالمفتاح الحالي وليس مفتاحًا جديدًا. وتتمثل الفكرة بعد ذلك في مشاهدة هذا التقدم الطبيعي لكل من محققين مرتكز الثقة المكون نحو هذا الجديد - وهذا يصعب قياسه بشكل لا يصدق. فهي حقًا لا تساعد لأن ما نريد حقا القيام به هو، في مرحلة ما، على الجميع الحصول على أكثر من KSK 2017. ثم لديك سؤال: متى سنقوم بتبديل ذلك؟ حتى لا يساعد. فهو لا يعطينا أي معلومات جديدة. نحن نعرف بالفعل من هم. هذا ما يمكننا أن نراه هنا، على افتراض أن هذا عينة مناسبة. لذا أمعائي الغريزية تقول لا.

روبرت مارتن ليجين: أنا لا أعتقد فعلا أنه ينبغي القيام به، ولكن يمكن القيام به. أنا أفهم جيدا لماذا لا ترغب ICANN في السير بهذا الاتجاه.

روي آريندس: نعم. هناك العديد من الأشياء التي يمكن القيام بها ونريد القيام بها.

روس موندي: أعتقد أننا نريد شكر روي على تقديم هذا العرض للمرة السابعة. شكرًا لك، روي.

والآن، جاك - أين أنت؟

سيدة غير معروفة: ذهب إلى الحمام. وقال أنه سيعود على الفور.

روس موندي: آه. مسابقة DNS العظمى. ما أعتقد أننا سنفعله، لأننا قد انتهى -

سيدة غير معروفة: لدينا الوقت، روس. الغداء ليس حتى الساعة 12:15.

روس موندي: أوه، انها ليست حتى 12:15؟

سيدة غير معروفة: نعم. لدينا مخزن مؤقت هنا، لذلك لدينا الوقت.

روس موندي: هذا جيد.

جيف هوستن: هل يمكنني تقديم القليل من ...

روس موندي: أجل. تفضل، جيوف.

جيف هوستن: جزء من سبب عدم وجود إجابة واضحة حقًا، روبرت - وانه لا يستمع حتى - هو أنه عندما يكون لديك مفتاحين مدرجين في سجلات DNSKEY المصادر التي وقعتها بالمفتاح القديم، التي تسمح لك ضمنًا بالثقة في المواد الموقعة بالمفتاح الجديد لأنك تثق بالمفتاح القديم. حتى لو ذهبت إلى خادم جذر مختلف، لأنك لا تزال حصلت على الشيء القديم في ذاكرة التخزين المؤقت، سوف تثق في كل شيء يعدله خادم الجذر لأنك تثق في المفتاح القديم. و المفتاح القديم موقع عبر المفتاح الجديد.

لذا، فإن هذه المسألة كلها معقدة بسبب أن المفتاح القديم - يوقع - المفتاح - الجديد. وهذا يعني أنك تثق بالمفتاح الجديد طالما أنه في ذاكرة التخزين المؤقت التي وقعتها المفتاح القديم. هذا هو السبب في فصله داخل الجذر مع أسماء النطاقات المتميزة التي لديها سلوك DNSSEC مختلف - "وهنا الاسم الذي يمكن التحقق من صحته بالمفتاح الجديد فقط إذا كنت تثق فيه" - يتطلب العمل في الجذر، والعمل على بروتوكول التحقق من الصحة، والعمل في المحللين. ربما تكون أصعب طريقة للقيام بذلك، وأنا لست متأكدًا من أن البيانات ستكون مفيدة لأنه، كما قلت الآن في المقدمة، انها لا تحل ما يدعو للقلق إذا غيرت المفتاح. إنه الضرر الذي ستفعله للمستخدمين. كنت حقًا بحاجة إلى هيكل القياس للبعد عن التركيز على كيفية عمل المحللين وإعادة التركيز على المستخدمين.

دخل جاك الغرفة، لذلك أنا بحاجة إلى عدم تضييع المزيد من الوقت. شكرًا.

جاك لاتور: هل من أسئلة أخرى؟

شخص غير محدد: إنه دورك.

جاك لاتور: حسنًا. حسنًا، لست متأكدا كيف أصبحت رئيس المسابقة. ذلك لأن شخصًا ما توقف عن فعل ذلك، أليس كذلك؟

شخص غير محدد: [غير مسموع]

جاك لاتور: لا؟ هه. حسنًا. هذا صحيح. مرحبًا بك في مسابقة DNS الكبرى واختبار DNSSEC لـ ICANN60. أمامك مسابقة من عشرة أسئلة للرد عليها. لذلك ستحصل على ورقة. إذا لم يكن لديك أي منها، ويمكنك انتزاع البعض من المناضد الأمامية. يجب أن يكون لدى الجميع قلم أو نحو ذلك.

حسنًا. وهنا قاعدة تعلمتها من روي: أنا على حق. نعم، يمكن أن أكون مخطئًا، ولكن لا يهم. أنا على حق. لذلك هذا هو المكان حيث أكود خادم رئيسي المسابقة الرسمي.

إنها إجابة جيدة لكل سؤال. هناك نقطة واحدة لكل إجابة جيدة. الأمر في غاية البساطة. لديك عشرة أسئلة والحد الأقصى عشر نقاط. لا توجد طريقة يمكنك الذهاب إلى -17 أو -19 أو -20.

شخص غير محدد: [غير مسموع]

جاك لاتور: كان ذلك جيدا. لنبدأ. السؤال 1: ما هو التاريخ الذي كان من المفترض أن يحدث فيه استبدال KSK الجذري؟ يتم استخدام KSK لتخصيص مجموعة مفتاح منطقة الجذر. متى كان من المفترض أن يحدث؟ أ) 11 تشرين الأول (أكتوبر) 2014، ب) 15، ج) 16، د) 17، أو هـ) كان من المفترض أن يحدث في العام الماضي ولكن قررنا عدم القيام بذلك؟

ثلاثة ... اثنان ... واحد ... صفر.

السؤال 2 - هذا سؤال مختلف، إيه؟ - ما هي تغذية Twitter التي تتتبع تغيير منطقة الجذر؟ @therootchange، @changeroot، @diffroot، – @root Jessica, انتقل إلى أعلى قليلاً لأن النص ... وهذا مزعج. أو @IAmGroot?

التالي (غير مسموع) السؤال 3. ما القائمة البريدية التي يجب الاشتراك فيها؟ ما هو الأفضل لعرض التقرير المتعلق بالقضايا الخاصة بـ DNS بشكل عام؟
DNSoperation@list.DNS-OARC، أو
IAmGroot@list.DNS.DNS-OARC، أو
DNSSECcord@elist.ISOC.org, DNSop@IETF.org, أو
HelpWithDNS@ICANN.org?

تذكر، أنا دائما على حق، لذلك كل ما أراه جيدًا هو الجواب الصحيح.

ثلاثة .....اثنان .....واحد.

السؤال 4: في مشروع IETF homenet.14، ما هو النطاق المخصص لعدم الاستخدام في الشبكات المنزلية السكنية ويعين هذا النطاق كنطاق استخدام خاص؟ أ) .المنزل، ب). [ربو] / المنزل، ج). المنزل. [.mezo.kaza.mezo] – أعتقد أن هذه صينية - المنزل. [rpo] أوmezo.؟

السؤال 5: أي ccTLD تم توقيعه مؤخرًا مع الجذر [DSN]؟ أ) .ax - لا أستطيع أن أقول ذلك -. [ألين إسلاند] - gw. [غير مسموع] - bm. (برمودا)، أو sa. (المملكة العربية السعودية)؟ تم التوقيع عليها مؤخرًا. وقد تحدثنا عن ذلك صباحاً.

ثلاثة .....اثنان .....واحد.

وهنا واحد خاص. ويبدأ مع آسف لأنني كندي. أي مما يلي يصف أفضل بروتوكول المصادقة المستندة على نظام اسم النطاق للكيانات المسماة (DANE) لقيمة استخدام شهادة 2 # TLSA؟ أ) غير معين، ب) PKXDA-CA - المترجم سيء؛ لابد أنه يمر بوقت عصير الآن - ج) DANE-TA، د) DANE-EE، أو ه) PKIX-EE؟

هذا واضح جدا، أليس كذلك؟ نعم؟ [غير مسموع] نعم.

حسنًا. التالي. السؤال 7: ما النسبة المئوية لجميع نطاقات المستوى الأعلى (TLD) في الجذر الموقعة مع [تفويض ثاني] APS في الجذر؟ كانت لدينا هذه الشريحة في هذا الصباح عندما كان الجميع نائمون وقلت: "أوه، هذا مهم".

مهلا، أنا أحب هذا. أي ورقتين كتبها بول موكابتريس نشرت في تشرين الثاني (نوفمبر) - تحتاج إلى التمرير هناك قليلاً - 1983 علامة بداية DNS؟ إذن أي ورقتين؟ أ) BCP16 وBCP17. هل هي ب) BCP42 وBCP78؟ ج) RFC882 وRFC883, أو د) RFC1034 وRFC1035؟

كان ذلك بحث Google الفوري.

ثلاثة .....اثنان .....واحد.

السؤال 9: ما هي طريقة معالجة الشبكة وطريقة توجيه والتوجه فيها [داتا غرام] من مرسل واحد إلى أي من الوجهات المتعددة المختارة على أساس أقرب وأقل تكلفة [LTS] مع أقل الطرق ازدحامًا أو مقياس بعيد آخر؟ هل هو Multicast أم Anycast أم Unicast أم Star Trek Subspacecast, أم [Flurrycast]؟

أوه، هذا جيد. ثلاثة .....اثنان .....واحد.

ما الذي ترمز إليه DNS ؟ هل هو خادم اسم النطاق أو نظام أسماء النطاقات أو برامج أسماء النطاقات أو خدمة اسم النطاق أو مساحة اسم النطاق؟

السبب الذي وضعت من أجله السؤال هنا لأنني لست متأكدا من الإجابة.

شخص غير محدد: [إذا كيف يمكن] أن تكون صحيحا؟

جاك لاتور: سأختار واحدة وأنا على حق. وهذا ما أردت توضيحه. لست متأكدًا من أننا سنجري نقاشا حول الغداء.

DNS - أوه، نعم، نعم، نعم. كان هذا أسرع.

حسنًا. لذلك التصحيحات. مرر الورقة إلى رقمك. سهلة للغاية. إنها إجابة واحدة لكل سؤال. انها نقطة واحدة وبحد أقصى عشر نقاط. نحن بصدد معرفة ما إذا كنت مخطئًا، أليس كذلك؟

السؤال 1. الجواب هو د. كان من المفترض أن يحدث 11 تشرين الأول (أكتوبر) 2017.

شخص غير محدد: [غير مسموع]

جاك لاتور: هل كل شيء على ما يرام؟

شخص غير محدد: لا بأس بنا.

جاك لاتور: حتى الآن جيدة جدًا؟ كان هذا [gimme]. تحتاج إلى نقطة واحدة على الأقل للحصول على تذكرة الغداء. هذا هو دورنا الجديد للرعاية، أليس كذلك، كريستيان؟ أجل. إذا كانت نتيجتك صفر، لا تذهب لتناول طعام الغداء. سيء جداً.

السؤال 2. الجواب هو IAmGroot .@diffroot – أحب هذه الإجابة.

السؤال 3. أ. قائمة عمليات DNS هي على الأرجح أفضل مكان إذا كان لديك مشاكل مع DNS. إذا لم تكن مدرجا في هذه القائمة، يمكنك الذهاب إلى Google والانضمام إليها والمشاركة فيها. انه مورد جيد. هل رأيت؟ أنا أقوم بالقليل من التسويق هنا.

السؤال 4. الجواب هو د. أحب ج. يجب أن يكون لدينا هذا النطاق الضخم مع جميع الأسماء وجميع اللغات، .home. انها تُجدي.

السؤال 5. gw. (غينا بيساو) تم اضافته في تشرين الأول (أكتوبر) 2017. وكانت هذه آخر إضافة.

السؤال 6. الجواب هو ج. هل حصلت عليه الآن؟ أجل. كان ذلك فقط لأجلك. مرتكز الثقة [بالتأكيد] هو الجواب الصحيح من أجل DANE.

السؤال 7: (ج) عددهم هو: يتم توقيع 90٪ من TLDs بالضبط.

السؤال 8: كان ذلك RFC882 و883 التي كتبت في 83 بوصة. هل هناك علاقة بين 883 و83؟ لا.

السؤال 9: Anycast. في نهاية المطاف الإصدار التالي هو Subspacecasting. سنبدأ العمل على هذا المنظر الجميل. [Flurrycast] هو ما كنا نرسله في كل مكان، وهي كلها تستجيب و[نأمل]. أنا أؤيد هذا الاقتراح.

السؤال 10. لم أكن أعرف حقًا ما كان الجواب، لذلك ذهبت إلى "ب".

حسنًا. الآن نحن بصدد معرفة من هو معلم DNS العظيم. عد النتيجة. ارفع يدك إذا كان لديك خمسة أو أكثر واستمر في رفع يدك.

ستة وأكثر. سبعة وأكثر. ثمانية وأكثر. تسعة وأكثر.

شخص غير محدد: [غير مسموع]

جاك لاتور: أوه. وعشرة؟ لذلك نحن في حضرتك معلم DNS العظيم. وو-هوو!

أعتقد أن معنا نجم -

روس موندي: ما تحصل عليه بالتأكيد هو وجبة غداء مجانية.

جاك لاتور: أجل. لذا ستحصل على الغداء مجانًا. تسعة من عشرة؟ عظيم جدًا. ممتاز. الغداء هو -

سيدة غير معروفة: الغداء في قاعة 4. إذا أردت الذهاب حالاً للتسجيل، فخذ اليمين. إنها الغرفة الكبيرة الضخمة. فقط للعلم، ليس عليكم المرور عبر أجهزة الكشف عن المعادن. فقط أدخل إلى اليمين، وتذكر فقط أنه يجي أن يكون لديكم تذاكركم الخاصة.

روس موندي: حسنًا، أيها الحضور. رجاءً الذهاب.

[نهاية النص المدون]