كوبي- DNSSEC للجميع -- دليل المبتدئين
الأحد، الموافق 10 مارس/آذار 2019 من الساعة 03:15 م إلى 04:45 م بالتوقيت الرسمي لليابان
ICANN64 | كوبي، اليابان

ويس هارداكر: سوف نصلح ذلك في خلال ثانية واحدة. سوف يكون فيهم جميعًا الآن أيضًا. جيد.

حسنًا. لذلك، سنتحدث اليوم عن ماهية DNSSEC وكيف تحمي استخدامك للإنترنت واستخدام الجميع للإنترنت، وكيف تشارك ICANN فيه. أنا ويس هارداكر من معهد علوم المعلومات التابع لجامعة جنوب كاليفورنيا. لدينا مجموعة من الشخصيات الرائعة التي وراءنا سوف تنضم إلينا في غضون دقيقة، وسوف أقدمها في دقيقة واحدة.

في غضون ذلك، أود أن أحكي لكم قصة عن DNSSEC، كيف بدأ بالفعل. حسنًا، لقد بدأت منذ فترة طويلة جدًا منذ عام 5000 قبل الميلاد في عصر الديناصورات. وبدأ الأمر مع أوغوينا - هذه هي شخصيتنا الرئيسية لهذا اليوم. تعيش في كهف في أحد جوانب جراند كانيون. هذه أوغوينا (أوغ). وهي تعيش على الجانب الآخر من جراند كانيون، أيضًا في كهف. فهما بعيدان جدًا. جراند كانيون عميقة جدًا واسعة جدًا. لها طريق طويل، وليس لديهم فرصة للتحدث كثيرًا - فهم بعيدون جدًا.

في إحدى زياراتهم النادرة، عبروا القناة وهم يتحدثون مع بعضهم البعض، ولاحظوا أن هناك دخانًا ناتجًا عن نيران أوغوينا ويعتقدون أن هذا احتمال. فكروا أنهم يمكنهم التواصل باستخدام إشارات الدخان. وسرعان ما أصبحوا يتحدثون بانتظام، ويتحدثون ذهابًا وإيابًا باستخدام الدخان، وكل شيء يسير على ما يرام. حتى في يوم ما تحرك رجل الكهف المزعج، كامينسكي، في البيت المجاور وبدأ في إرسال إشارات الدخان في نفس الوقت.

والآن، نجد أن أوغوينا مرتبكة حقاً. هناك مجموعتان من إشارات الدخان تأتي من مختلف أنحاء الوادي وهي لا تعرف أيهما لأي شيء. وهكذا، انطلقت أوغوينا من الوادي محاولة بذلك تسوية الفوضى كلها. تشاور أوغوينا وأوغ مع كبار حكماء القرية. رجل الكهف، ديفي - الآن بعض الناس يعرفون على ما يبدو من هو ديفي. ديفيس هو كاتب تشفير مشهور ساعد في تطوير التكنولوجيا وراء DNSSEC وسنتطرق إلى ذلك. لكنه يركض

في الجزء الخلفي من كهف أوغ، حيث يجد بعض المسحوق الأزرق السحري. وهو ذو لون غريب، ويهرب إلى النار ويرميها على النار، ولأن النار الزرقاء السحرية تتحول إلى دخان أزرق، يمكن الآن لأوغوينا وأوغ الاستمرار في الدردشة بسعادة لأن عليها فقط أن تصدق الدخان الأزرق، لأن الغبار الأزرق موجود فقط في الجزء الخلفي من كهف أوغ.

لذا، تم كل شيء على أكمل وجه، صحيح. لقد انتهينا. كان هذا تمهيد لـ DNSSEC - فهمتوه بشكل رائع. لذا، سنشرحها بتفصيل أكبر ولكن المفاهيم الكامنة وراء ذلك، المفهوم الكامن وراء شيء سحري يحول شيء واحد تعرفه إلى شيء تعرف أنه جاء من المكان الصحيح، هو بالضبط ما يحدث في DNSSEC.

لذا، دعوني أعود إلى DNS قليلاً، وسنبدأ بمفهوم عالٍ من DNS نفسه. إذا نظرتم إلى DNS أو ذهبتم إلى DNS للدرس التعليمي للمبتدئين في وقت مبكر من اليوم وأوائل أمس، فمن المحتمل أنهم أظهروا لكم رسمًا تخطيطيًا مثل هذا - يبدأ DNS من الأعلى، ويبدأ من الجذر، والذي تمت مناقشته بشكل مكثف في ICANN، ثم أسفل جميع نطاقات المستوى الأعلى (TLD)، وأحيانًا هناك رموز بلد، وأحيانًا تكون هناك أشياء مثل com، ثم أسفل نطاقات المستوى الثاني مثل co.uk و bigbank.com و nic.ma. اليوم، سوف نركز على bigbank.com.

لذلك، الشيء المهم الذي يجب معرفته هو أن مزود خدمة الإنترنت لديه معالج، والمعالج يعرف مكان منطقة الجذر، وطالما يعرف مكان منطقة الجذر، يمكنه متابعة هذه السلسلة لأسفل لمعرفة مكان كل شيء آخر. لذلك، يجب أن تبدأ من الجذر، ثم تنخفض وتعرف، حسناً، أين com، ثم تنخفض وسنتعمق في ذلك بمثال هنا بعد دقيقة واحدة، ولكن بشكل أساسي، كل مستوى يشير إلى معالج المستوى التالي لأسفل. لذا، فإن الشيء الوحيد الذي يجب أن تعرفوه في البداية هو مجرد مكان الجذر. في النهاية يتم الإجابة على السؤال ثم يقوم المعالج بالفعل بتخزين تلك المعلومات مؤقتًا لفترة من الوقت للاستخدام في المستقبل.

وهنا تكمن المشكلة. لا يوجد أمن في DNS. عندما تم اختراعه، لا أعرف أي عام، منذ فترة طويلة - 84، لم يتم إضافة أي أمان إليه. كان الجميع جيدون في ذلك الوقت، ولم

يكن هناك شر، وكانت الأسماء مخادعة بسهولة في وقت لاحق، وأدرك الناس أن بإمكانهم العمل في جميع أنحاء النظام وإعطائك إجابة سيئة، ويتم تسميم ذاكرات التخزين المؤقت بسهولة، وبالتالي فإن المعالج قد يتذكر ليس مجرد الإجابة الجيدة لفترة طويلة، ولكن سوف يتذكر إجابة سيئة لفترة طويلة كذلك.

لذا، لتوضيح ذلك بشكل أفضل، أود إبراز مجموعة من الشخصيات التي لدي هنا في هذه القمصان البيضاء، وهكذا، سوف يسيرون معك في مثال يوضح بالضبط ما يفعله معالجك وما يفعله مزود خدمة الإنترنت، وسنبدأ مع المستخدم جو هنا على اليسار. سيتعين عليه القيام ببعض الأعمال المصرفية اليوم على bigbank.com، لذلك، سوف يبدأ في القيام ببعض الأعمال المصرفية وسنرى كيف يقوده DNS إلى الإجابة الصحيحة كما نأمل.

شخص غير محدد: إنهم يريدونك أن تراني.

روس موندي: مرحبا، مزود خدمة الإنترنت.

ويس هارداكر: نعم.

روس موندي: أود الحديث إلى bigbank.com. هذا هو اسم الفتى.

ويس هارداكر: لا أعرف أين يوجد www.bigbank.com. اسمحوا لي أن أكتشف ذلك لكم، سوف أعود سريعًا.

مرحبًا أيها الجذر، أود الوصول إلى www.bigbank.com. هل يمكن أن تخبرني أين هو؟

شخص غير محدد: مرحبًا، أنا خادم منطقة الجذر، وأنا أعلم بنطاقات المستوى الأعلى، لذا، فأنت تبحث عن com.؟ لماذا لا تذهب إلى خادم com. على 1.1.1؟

ويس هارداكر: حسنًا بالتأكيد، اسمحوا لي بالذهاب إلى ذلك. مرحبًا com. أنا أبحث عن www.bigbank.com. من فضلك أخبرني، أين يمكن أن أجده؟

شخص غير محدد: لا أعرف أين يوجد www ولكن يمكن أن أخبرك أين bigbank.com. إنه على 2.2.2.2.

ويس هارداكر: مرحبًا، أنا أحاول الوصول إلى www.bigbank.com. من فضلكم أخبروني، أين يمكن أن أجده؟

روس موندي: نعم، يمكنني، أنا bigbank.com وأعرف أين يوجد www.bigbank.com. إنه على 2.2.2.3.

ويس هارداكر: رائع. دعوني أرجع لأخبر المستخدمين لدي.

روس موندي: وربما يريد بعضًا من أمواله.

ويس هارداكر: مرحبًا، بالتأكيد أنت متصل بـ 2.2.2.3. هذا هو المكان الذي يوجد به www.bigbank.com.

شخص غير محدد: شكرًا لك، bigbank.com.

ويس هارداكر: أجل. حسنًا. شكرًا لكم، لاعبين سخفاء من العرض التعليمي لـDNSSEC. إننا نقدر ذلك. سوف نعود إليكم خلال ثانية. نعم، من فضلكم امنحوهم حصة تصفيقات. ولكن انتظروا، سوف تسير الأمور نحو الأفضل. حسنًا، الشريحة التالية من فضلكم.

لذلك، كانت هذا المسرحية الكاملة مشابةً جدًا لكيفية قيام أوغوينا بالدردشة مع أوغ، من خلال المُحلِّل، والحصول على الإشارة قبل ظهور الشر. لذا، فإن السؤال هو ماذا حدث مع الشر الذي جاء به كامينسكي وقدم إشارة دخان بديلة؟ لذا، فكيف يؤثر هذا على نطاقات DNS؟ كيف يتم اختراق نطاقات DNS؟ وكيف يمكن أن تصل المشكلات؟

لذلك، سوف نمر على نفس المسرحية الهزلية الدقيقة مرة أخرى - ستكون هي نفسها تمامًا - أعدكم بذلك.

روس موندي: مرحبًا مزود خدمة الإنترنت.

ويس هارداكر: مرحبًا.

روس موندي: يجب علي تسجيل وديعة مع bigbank.com. هل يمكنك العثور على هذا الشخص؟

ويس هارداكر: بالتأكيد، لا تقلقي www.bigbank.com. سأذهب مباشرة وأسأل الجذر.

مرحبًا أيها الجذر، أحد مستخدمي يود الوصول إلى www.bigbank.com. هل يمكن أن تخبرني أين هو؟

شخص غير محدد: يمكني أن أخبرك أن تذهب إلى خادم com. على 1.1.1.1؟

ويس هارداكر: جيد، أعتقد أنني سوف أذهب وأسأله. مرحبًا، خادم com. أحد مستخدمي يود الوصول إلى www.bigbank.com. أين يوجد ذلك، رجاءً؟

شخص غير محدد: لا أعرف أين يوجد www ولكن يمكن أن أخبرك أين bigbank.com. على 2.2.2.2.

ويس هارداكر: رائع. سأذهب مباشرة وأسأل هناك. مرحبًا، أحد مستخدمي يود الوصول إلىwww.bigbank.com. هل يمكن أن تخبرني أين هو؟

شخص غير محدد: بالتأكيد. ولا توجد أي مشكلة.

ويس هارداكر: رائع.

شخص غير محدد: www.bigbank.comيوجد في 6.6.6.6.

ويس هارداكر: بالتأكيد، شكرًا لك. مرحبًا، أيها المستخدم، يجب أن تذهب إلى 6.6.6.6. هذا هو المكان الذي يوجد به www.bigbank.com.

روس موندي: يبدو ذلك جيدًا. أو أيًا كان. إذًا الآن كنت سأذهب إلى-

شخص غير محدد: سآخذ هذه الوديعة يا سيدي. شكرًا جزيلاً.

ويس هارداكر: حسنًا. إذًا يمكنكم رؤية المشكلة، أليس كذلك؟ المستخدم جو المسكين لا يعرف أي إجابة يجب عليه أن يصدقها. هو يعتقد أن الأولى هي ما يحصل عليه. وهكذا، هذه هي مشكلة إشارات الدخان، مثلما حدث من قبل، حيث يوجد في الواقع إشارتان ويميل المستخدم إلى تصديق أحدهما، ويتعين عليه الاختيار العشوائي، وفي هذه الحالة، لا تعرف أوغوينا حقًا أي مجموعة من إشارات الدخان يجب عليها أن تصدقها.

لذا، لنعود إلى معتقدنا عال-المستوى لنطاقات DNS. تحدثنا في وقت سابق قليلاً عن الجذور في الأعلى و com تحتها، ثم bigbank.com، وإذا كان المعالج لدى موفر خدمة الإنترنت الخاص بك يتحدث إلى نظام خاطئ، فقد يحصل على إجابة جيدة، الزرقاء، أو ربما يحصل على إجابة سيئة، الحمراء.

لذلك، يقوم DNSSEC بإصلاح هذا، وهذا هو سبب وجودكم هنا اليوم. يضيف DNSSEC الأمان إلى DNS حيث لم يكن موجودًا من قبل، ويقوم بذلك باستخدام التواقيع الرقمية. إنه يقوم بأمرين مهمين. تقول أن المعلومات لم يتم التلاعب بها في أي وقت على أي من عمليات النقل، وتقول إنها نشأت من المكان الصحيح. يمكنك أن تضمن أنها جاءت من الموقع الأصلي الصحيح، حتى لو تم تخزينها في أسفل الحذاء أو شيء من هذا القبيل. لقد تم توقيعها وهي سارية للأبد. يتم تخزين المفاتيح في التواقيع في DNS نفسه مما يجعلها جميلة بالفعل، لأنه من أجل معرفة ما إذا كانت آمنة أم لا، يمكنك بالفعل استخدام DNS نفسه لإجراء عمليات البحث هذه ومعرفة المفاتيح التي تحتاجها، ونحن سنرى مثال على ذلك في ثانية.

يجب على المُعالج أن... تمامًا مثل المُعالج قبل أن يعرف فقط من أين تبدأ خوادم الجذر معها ومن ثم يمكنهم التسلسل طوال الطريق، DNSSEC يعمل بنفس الطريقة. يجب على المعالج معرفة مكان خوادم الجذر وعليهم أن يعرفوا أن مفتاح جذر واحد، ومن ثم يمكنهم بناء سلسلة من الثقة أدناه، لأن كل مستوى يوقع مفتاح المستوى التالي حتى تكتمل السلسلة. لذلك، طالما أنك تتبع سلسلة التشفير هذه على طول الطريق، فأنت تعلم أنك تحصل على الإجابات الصحيحة.

لذلك، الميزة الآن هي، سابقًا عندما كان لدينا هذا المخطط السابق، لم يكن المستخدم جو يعرف أيهما ينبغي عليه أن يصدق. لم يعرف أيهما يصدق الأزرق أم الأحمر. الآن يمكننا التحقق من الصحة وإظار أن الأحمر لن يتطابق. لن ينجح الأمر.

لذلك، دعونا نصلح هذا الأمر في لعبتنا وسنرى ما إذا كان - هل يمكنكم يا رفاق أن تقوموا بذلك بالمزيد من الخير وشر أقل؟

شخص غير محدد: هذا رائع.

روس موندي: مرحبًا، مزود خدمة الإنترنت ISP، أحتاج إلى التحدث إلى bigbank.com، وأريد أن أعرف أنها إجابة صحيحة.

ويس هارداكر: حسنًا، هذا منصف بما يكفي. دعوني أبين ذلك لكم. مرحبًا أيها الجذر، أحد مستخدمي يود الوصول إلىwww.bigbank.com. هل يمكن أن تخبرني أين هو؟

شخص غير محدد: يمكنني إخبارك بمكان com.، إنه 1.1.1.1 وإليكم الشهادة التي توضح أن هذه المعلومات صحيحة.

ويس هارداكر: حسنًا، رائع، سوف أثق بذلك. دعوني أستمر واسأل خوادم com.

مرحبًا، خمّنوا ماذا؟ أحد مستخدمي يود التكلم مع www.bigbank.com. هل يمكن أن تخبرني أين هو؟ وسوف أتحقق من توقيعك عندما تقوم بذلك.

شخص غير محدد: بالتأكيد، يبدو أنك تطلب ذلك كثيرًا. لا يممكن إخبارك أين www.bigbank.com ولكن يمكن أن أخبرك أين bigbank. على 2.2.2.2 وهاهو التوقيع.

ويس هارداكر: رائع. سأذهب مباشرة وأسأل. مرحبًا أيها الجذر، أريد العنوان الخاص بـwww.bigbank.com. هل يمكن أن تخبرني من فضلك؟

شخص غير محدد: يوجد Bigbank.com في 6.6.6.6.

ويس هارداكر: حسنًا، انتظروا دقيقة. أين التوقيع؟

شخص غير محدد: ليس لدي شيء من هذا القبيل. آه، حسنًا!

ويس هارداكر: سوف أسأل شخص آخر- أنا لا أثق بك، متأنق حقير.

مرحبًا، هل يمكن أن تخبرني أين www.bigbank.com؟

روس موندي: حسنًا، أنا لا أعرف www.bigbank.com على 2.2.3 وهذا هو التوقيع.

ويس هارداكر: يبدو هذا صحيحًا. مرحبًا سيدي المستخدم bigbank.com على 2.2.2.3 وقد فحصت التوقيع ويمكنك الاعتماد على ذلك.

روس موندي: وأنا أرى التوقيع هنا، وأشكرك على ذلك. لذا، شكرًا لك Big Bank. أرسل المال.

ويس هارداكر: حسنًا، شكرًا جزيلاً لك. هل يمكن أن تصفقوا بحرارة على آدائنا من فضلكم؟ فهم يقومون بعمل رائع. إذا كنتم اجتماعات ICANN المستقبلية فنحن نقوم بهذا كل مرة. هل شاهد أحد هذه المسرحية من قبل؟ بضعة أشخاص، نعم.

شخص غير محدد: [غير مسموع]

ويس هارداكر: لذا، هذا مساو للدخان الأزرق. حسنا. تمكنت أوغوينا أخيرًا من رؤية الدخان الأزرق لأنه تم توقيعه، وفي هذه الحالة، في المسرحية، استخدمنا الميداليات الصغيرة حول رقبة شخص ما، لكن ذلك أشار إلى المفاتيح المستخدمة للتوقيع على كل مستوى من شجرة DNS.

لذا، سأنتقل بعد ذلك إلى شريكي في هذه الجريمة [غير مسموع]، روس موندي، الذي سيتحدث عن أمثلة لماذا تحتاج إلى DNSSEC وبعض الأدلة البسيطة لنشرها بالفعل.

روس موندي: شكرًا لك، ويس. أنا روس موندي من بارسونز، والجزء الذي أنا هنا لمحاولة مساعدتكم على فهمه بشكل أفضل هو كيف يمكنكم نشره وما هي بعض الأشياء التي تحتاج إلى دراستها والتفكير بها خلال هذه العملية.

لذلك، فإن أحد الجوانب المهمة لنظام DNS والتي لا يفكر فيها الأشخاص في كثير من الأحيان هي أن يتم استخدام DNS من قبل كل تطبيق على الإنترنت اليوم، وبالتالي عندما لا تحصل على الأشياء الصحيحة مع DNS الخاص بك أو يتم تغييره أو لسبب ما، حدوث مشكلة، أو عطل أو شيء ما، إنها التطبيقات التي تتأثر بالفعل، والتي تنتهي بمشكلة بالفعل. لا يمكنك الحصول على اتصال. في حالة مسرحيتنا، لا يمكن للمستخدم جو التحدث للبنك الخاص به. لذلك، هذه هي المشكلة الأساسية والواسعة في كل شيء حول ما هو DNS وماذا يفعل DNS.

لذا، كما هو ضروري لجعل جميع التطبيقات تعمل جيدًا، فلماذا يواصل الناس مهاجمة DNS؟ حسنًا، كنت أتابع أنشطة أمان DNS و DNS لسنوات أكثر مما أرغب، وبصراحة لم يسبق لي أن رأيت أو سمعت عن مثال يهاجم فيه الناس DNS لأنهم يرغبون في تغيير DNS والخروج من هناك ولا يقومون بشيء آخر. وليس هذا ما يريدونه.

ما يريدون القيام به هو أنهم يريدون الوصول إلى المعلومات الموجودة في بعض التطبيقات التي يتم تشغيلها بعد حدوث استعلامات DNS. ربما يرغبون فقط في إنشاء نسخة من جميع رسائل البريد الإلكتروني الواردة من مكان معين، لذلك فإنهم، بالنسبة لجميع الوجهات التي قد يرسلها خادم البريد الإلكتروني، يمكنهم الجلوس هناك وإعطاء عنوان الرجل المزيف في خادم البريد الإلكتروني من النوع الأوسط وتلقي جميع رسائل البريد الإلكتروني التي تأتي من هذا الجهاز المحدد، ومن ثم بالمناسبة، من المحتمل أن يتم إرساله إلى حيث ينوي الذهاب والأشخاص الذين يتلقونه لا يعرفون الفرق مطلقًا. لذا فهو نوع من الرجال في وسط الهجوم.

الآن، منذ عامين، ولحسن الحظ، عدت إلى الوراء ونظرت ما إذا كان بإمكاني العثور على الدورات التدريبية مرة أخرى، وهي على الأقل لا تبدو أنها خارج على الإنترنت كما كانت لفترة من الوقت، كان هناك بالفعل واحد أو اثنين من الدورات التدريبية حيث كان المدربون في المنهج الدراسي يشترطون على الطلاب أن يكتبوا اختطاف نظام أسماء النطاقات. وفي المنهج الدراسي، لم يكن هناك شيء أستطيع أن أرى أنه يقول إن هذا شيء سيء، وهذا خطأ. ولكن كانت هناك أيضًا حزم برامج تتيح لك القيام بنفس الشيء. لذلك، من السهل جدًا تحديد أدوات المساعدة أو البرامج الموجودة بالفعل في العالم. إذن، ما الذي يساعد فيه DNSSEC؟

حسنًا، يمكنكم حينئذٍ، كما رأيتم في المسرحية الهزلية، أن السؤال الذي طرحه المستخدم مر بعملية للتحقق من صحة أصل المعلومات وصحة تفاصيل المحتوى التي لم يتم تغييرها في رحلة في مكان ما على طول الطريق.

لذا، هذا مثال للطريقة التي تعمل بها بعض عمليات الخطف. إنه مثال مبسط إلى حد ما، وليس مبسطًا تمامًا مثل المسرحية الهزلية الخاصة بنا، لذلك دعونا نمضي قدمًا واضغطوا على... يمكنكم أن تروا أن هذا هو الاستعلام الأول، هذا الخط المنقوط الذي يأتي من المستخدم جو، ثم يتقدم للحصول على الخادم الموثوق، ثم يعود إلى الخادم المتكرر بالإجابة، ثم يعود إلى المستخدم، ثم أخيرًا، بعد كل هذا، ينتقل الاستعلام بالفعل إلى خادم الويب. لذلك، يمكنكم أن تروا أن هناك مجموعة كبيرة من حركة مرور الشبكة التي يحدث

أن معظم الناس لا يفكرون فيها - تلك هي حركة مرور DNS التي تحدث قبل حركة مرور خادم الويب أو حركة البريد الإلكتروني أو فيس بوك، أو ما تفعله هناك.

لذا، ما فعلناه قبل عامين، أنشأنا موقعًا مخصصًا يتحقق في الواقع من أن الاستعلامات تأتي وتم التحقق من صحة DNSSEC وفحص التحقق من صحة DNSSEC، وما فعلناه هو وجود علامة X صغيرة، علامة اختيار صغيرة، وكان ذلك مجرد شيء تم تنفيذه بشكل مخصص لهذا الموقع المحدد، ثم إذا أتيت وقمت بنفس الاستعلام ولم تكن تقوم بتشغيل DNSSEC، فيمكنك أن ترى من خلال المحتوى الموجود في الصفحة أنه في الحقيقة لم يتم التحقق من DNSSEC.

ما فعلناه بعد ذلك كان عملية خطف DNS التي من شأنها أن تظهر ما يمكن أن يحدث عندما يحدث هذا. لذلك، امضي قدماً واضغط على أول ما يظهر لك، ثم انقر فوق التالي. الدكتور "شرير"، مساعدنا الرائع هنا من الجانب الذي يحمل الرأس الأسود الكبير، دخل في الرد وقدم إجابة، وهذه الإجابة أدت إلى خروج المستخدم جو من الموقع الإلكتروني المعاد توجيهه، واستمر الاستعلام والإجابة التي كانت شرعية من خلال النظام، ولكن لم يحصل عليها المستخدم جو وآلته مطلقًا، لأن الإجابة الأولى التي تلقاها، الإجابة من الخاطف الشرير، قد وصلت بالفعل إلى جهازه وقال الجهاز، "حسنًا، حصلت على إجابة، لن أقلق بشأن أي شيء آخر."

لذلك، مع DNSSEC، تحصل على نفس مجموعة تدفقات الحزمة التي يمكنك رؤيتها هنا، والفرق هو أن التحقق من الصحة يتحقق من الحزم التي تأتي وإجابة DNS التي تأتي من الخاطف الشرير لا تقبلها آلة المستخدم جو. آمل أن يكون هناك عدد قليل من [الأخطاء]، ولكن على أي حال، نعم، هذه هي الحزم التي تستمر في التدفق في طريقها إلى هناك.

الآن، كيف تبدو صفحة الويب المخصصة؟ حسنًا، تبدو صفحة الويب المخصصة هذه كما كانت تمامًا عندما عرضتها عليكم من قبل، والآن الصفحة التالية. لقد قمنا بالاختطاف وفي هذه الحالة، كان هذا في الواقع عندما كان ستيف كروكر رئيسًا لمجلس إدارة ICANN، ولهذا السبب نحن - وشارك ستيف مع DNSSEC لفترة طويلة، لذلك وضعنا

رابطًا فكاهيًا على موقع آخر يملأ فعليًا جزءًا من الشاشة التي شاهدها المستخدم إذا أتوا إلى هذا الموقع دون القيام بالتحقق من DNSSEC. لذلك، كنا في الواقع نختطف معلوماتنا الخاصة، في هذه الحالة، فقط لإظهار ما يمكن أن يحدث إذا كان هناك هجوم على صفحة من هذا القبيل.

الآن، يكون هذا عندما تبدأ بحل فارغ ومستعرض فارغ وتذهب إلى cnn.com قبل حوالي 10 سنوات. لقد كان بهذا السمك. واليوم، إنه أكثر سمكًا. يبدو الأمر كذلك. لذا،هذا فقط لملئ صفحة ويب واحدة. التالي.

الشيء المهم حقًا في كل هذا، والسبب وراء DNSSEC، هو التأكد من أن بيانات منطقة DNS، ومحتوى المنطقة نفسها، صحيحة وتبقى صحيحة أثناء تدفقها عبر الإنترنت.

لذلك، مثال آخر بسيط للغاية، هذه منطقة غير موقعة، وتقوم بالاستعلام وتقوم بالإجابة... لذا، فهي عبارة عن عدد صغير من الخطوات وتعمل بسرعة كبيرة في الخلفية. ثم عند تشغيل DNSSEC، سواء كنت تقوم بتشغيل المعالج أو تقوم بالتحقق من الصحة، سواء كان مزود خدمة الإنترنت أو مؤسسة محلية، وما إذا كنت تقوم بعملية تشغيل خادم أسماء كبيرة، فربما تقوم بتشغيل مسجل وتوفر الكثير من خوادم الأسماء. ثم إذا كنت قادرًا بالفعل على تشغيل أنظمة DNS الخاصة بك، فيجب أن يكون دمج DNSSEC في هذه الأنظمة واضحًا نسبيًا. التحدي الأكبر كان دعم البرنامج مع مرور الوقت لدمج قدرات DNSSEC، وقد تحسن هذا كثيرًا في السنوات الأخيرة، لذلك يمكنكم الحصول على DNSSEC في معظم الوقت. إذا كنت تقوم بتشغيل خوادم الأسماء الخاصة بك، فأنت فقط تضع البرنامج الصحيح.

الآن، إذا كنت تقوم بعملية كبيرة بالفعل، مثل TLD أو مؤسسة كبيرة جدًا، فمن المحتمل أنك تريد القيام بذلك بنفسك بدلاً من الاستعانة بمصادر خارجية في مكان ما. لذلك، مرة أخرى، إنها امتداد للقدرة التي تمتلكها منظمتك بالفعل.

الآن، إذا كنت مستخدمًا نهائيًا، فأنت بصفتك فردًا يجلس في هذه الغرفة، يمكنك أن تكون الشخص الذي يطلب الحصول على نموذج التحقق من صحة DNSSEC من مزود

الخدمة، سواء كان مؤسسة، أو كان مزود خدمة إنترنت. في هذه الحالة، من المحتمل ألا تقوم بتشغيل خوادم الأسماء الخاصة بك - على الرغم من قيام عدد قليل من الأشخاص بعمل ذلك - لكن في معظم الوقت يقوم شخص آخر بتشغيله لأجله، وهؤلاء المشغلون هم الذين يحتاجون إلى أن يطلبوا القيام بالتحقق من صحة DNSSEC لمنع الدكتور "شرير" من الدخول وسرقة معلومات DNS الخاصة بك.

وكما قلت من قبل، فإن التركيز الأكبر لـ DNSSEC هو التأكد من أن بيانات المنطقة التي يتم إدخالها، في البداية من خلال النشاط سواء كانت bigbank أو com، أو ما إذا كانت شركة أخرى، محتفظ بها في النظام ويتم تسليمها بواسطة نظام DNS قيد التشغيل للمستخدمين النهائيين ولا يتم تعديلها في المنتصف.

لذلك، فالمهم حقًا هو محتوى المنطقة، وهذا ما تحتاجه حقًا للتركيز عليه - الوصول إلى محتوى المنطقة إلى المكان المناسب - وهذا له نفس أهمية أي شيء آخر... في مرحلة ما كان هناك الكثير من الأشخاص الذين كانوا يركزون كثيرًا بالفعل - أوه، يستخدم DNSSEC التشفير، هذا التشفير، وهذه أشياء خاصة حقًا، علينا أن نفعل أشياء خاصة حقًا. تحتاج إلى التأكد من أن تشفيرك يتم إدارته بشكل صحيح وأن مفاتيحك تدار بشكل صحيح، لكن معظم البرامج الحديثة تقوم بذلك. يجب أن يتذكر الناس أنك تحتاج أيضًا إلى إدارة المحتوى الخاص بك بشكل صحيح - إدخاله وعدم تعديله على طول الطريق حتى يصبح في خوادم الأسماء وبعد ذلك بمجرد أن يصبح في خوادم الأسماء، باستخدام DNSSEC للتحقق من صحته للوصول إلى النهاية.

لذا، الآن، من الصور السابقة، لا يوجد فرق كبير عن الرسم التخطيطي الأخير. يمكنكم أن تروا أنه من الناحية المفاهيمية، فإن مجرد إضافة بعض أنواع السجلات الإضافية هو ما يسمونه في نظام DNS، والذي يتم تضمينه من إنشاء المنطقة الموجودة في خادم الاسم الموثوق، ومن ثم يقوم الخادم المتكرر بالتحقق من الصحة بالتحقق من صحة هذه المعلومات، و كان هذا للتحقق من الميداليات لأنها استمرت مع تقدم مزود خدمة الإنترنت، من الجذر إلى com إلى bigbank.

لذا، عمومًا، فيما يتعلق بنشر الأشياء مع DNSSEC، فإن الشيء المهم الذي يجب النظر إليه هو مقدار المشاركة التي تتمتع بها مؤسستك أو كيانك الخاص في تشغيل DNS الحالي الخاص بك؟ إذا كنت تقوم بتشغيل DNS الحالي الخاص بك في جميع خوادم الأسماء وتقوم بتشغيلها بنفسك، فمن المحتمل أن تكون قادرًا على القيام بهذه الوظائف الإضافية اللازمة لتوفير توقيع DNSSEC والتحقق منه في المواقع المناسبة. إذا كنت لا تقوم بتشغيله بنفسك - على سبيل المثال، فإن العديد من الشركات الكبيرة ستقدم قدرات DNS إلى مؤسساتهم، ويمكن أن تكون parsons.com، ويستخدم كمزود خارجي كهذا. حسنًا، أحد الأسباب الرئيسية التي اختاروا لأجلها مقدم الخدمة الخارجي هي أن هذا الموفر الخارجي يقوم بـ DNSSEC.

لذا، إذا كنت تستخدم موفرًا خارجيًا، فربما تريد أن تطلب من ذلك الموفر الخارجي القيام بـ DNSSEC نيابةً عنك، ولا تخاف من الانتقال إلى مزود آخر إذا كان الموفر الأول يقول، أو موفرك الحالي يقول، "أوه، أنا آسف، لم أكن أعرف أنك تريد DNSSEC؛ لا يمكنني القيام بذلك. " أعثر على الموفر الذي يقوم بذلك. هناك عدد قليل يقوم بذلك.

لذلك، يتم استضافة هذا النشاط بالاشتراك مع ICANN واللجنة الاستشارية للأمن والاستقرار. لقد كان لدينا أيضًا بعض الأعضاء من اللجنة الاستشارية لنظام خادم الجذر لمساعدتنا اليوم، وهو أمر رائع، وبرنامج Internet Society Deploy360، لذلك هذا الذي دعمنا لأجله هذه الأنشطة لفترة طويلة، وأعتقد أن هذه هي الشريحة الأخيرة بالنسبة لنا هنا. والآن لقد حان وقت الأسئلة.

ويس هارداكر: حسنًا، شكراً جزيلاً لك، روس. سنجعل الدكتور "شرير" يركض هناك بينكم جميعًا باستخدام ميكروفون، لذا إذا كان لدى أي شخص أسئلة حول كيفية عمل DNSSEC أو شيء لم تروه في المعلومات من قبل، أو ما زالت لديكم أسئلة، فالرجاء رفع أيديكم و أندرو سوف يتجول - آسف، سوف يتجول الدكتور "شرير" ويتيح لكم التحدث على الميكروفون.

أنجيلا: مرحبًا، اسمي أنجيلا. وأنا من هيئة تنظيم الاتصالات في بوتسوانا. في حالة القول بأن المفتاح العمومي مختطف من قبل مختطف، هل هناك أي آليات تم وضعها لقول، حسنًا، في حالة اختطاف المفتاح، كيف يمكنني التحقق أيضًا مما إذا كان هذا هو الرد الصحيح؟

ويس هارداكر: كان هذا سؤالًا جيدًا جدًا. لست معتادًا على الأسئلة الجيدة. شكرًا لك على ذلك. لذا هذا سؤال رائع. لذا ما الذي سيحدث إذا تم اختراق المفتاح الخاص بك؟

هناك أمران، وهناك بالفعل الكثير من الخبراء الآخرين في الغرف. لا تترددوا في رفع أيديكم إذا أردتم الإجابة.

يوجد بالفعل مفتاحان مشتركان، وقد قمنا بتبسيطه كثيرًا، ولكن يوجد بالفعل مفتاح عام ومفتاح خاص. لقد ذكرتم المفتاح العام. المفتاح العام الذي يمكن إعطاؤه لأي أحد. إنه شيء آمن للقيام به. الغرض من المفاتيح العامة هو أنه يمكنك توزيعها على نطاق واسع. إنه المفتاح الخاص الذي تحتاج إلى حمايته. إذا أصبح ذلك مخترقًا، يقوم شخص ما باختراق نظامك وسرقة المفتاح الخاص، نعم، يجب عليك إخبار والديك على الفور. لذلك، إذا كنت bigbank.com، فعليك أن تخبر والديك، "لدي مفتاح جديد، يرجى تبديل هذه السلسلة."

هل تتذكرون كيف تم فحص الميدليات طوال الوقت؟ في الأساس، يمكنك تغيير إحدى هذه الميداليات، كما تعلمون، بتعليقها على com. وتقول: "لدي ميدالية جديدة لك، ولدي مفتاح جديد سأستخدمه. مفتاحي الخاص يختلف الآن." وهكذا، يمكنك جعل هذا يتغير بسرعة.وبهذا. هناك الكثير من التعقيدات التي تتوافق مع 1. هناك وقت لتعيش فيه القيم والتخزين المؤقت وجميع أنواع الأشياء الأخرى التي تلعب دورًا أساسيًا، ولكن هذا هو ما يجب عليك فعله. أخبر والديك، "لدي مفتاح جديد. أحتاج منك أن تقوم بتبديله على الفور، وهذا يجعلك آمنًا إلى حد ما بسرعة كبيرة.

هل من أسئلة أخرى؟ سؤال جيد، شكرًا لك.

سافيو فينيكيوس دي موريس: مرحبًا. أنا سافيو من البرازيل، NextGen. سؤالي حول ما هو التحدي الأكبر الذي تواجهه لـ DNSSEC كلما زاد استخدامه في الإنترنت؟

ويس هارداكر: إذًا، فإن السؤال هو: ما هو التحدي الأكبر في وجود المزيد من المستخدمين يستخدمونه؟ هل يريد أحد الرد على ذلك؟ يمكنني المحاولة، ولكن روس؟

روس موندي: حسنًا، لقد كان هذا جهدًا مستمرًا من حيث التعليم، والتشجيع من خلال العديد من المنتديات مثل هذا، والعمل الذي أنجزته عدد من الأنشطة لتشجيع بائعي البرامج على التأكد من أنهم يتمتعون بجميع البنية والقدرات الصحيحة في برامجهم، والعمل مع بائعي التطبيقات لتشجيعهم على دعمه أيضًا.

أعتقد أن أحد أكبر المساهمات في جعل المزيد من الأشخاص يستخدمونه يأتي بالضبط من المستخدمين سواء كانوا مستخدمين كفرد أو مستخدمين يمثلون جزءًا من مؤسسة تقول "أريد أن أفعل DNSSEC" بعض وظائف المسجل في الشركات لا تفعل DNSSEC فقط مما يجعل من الصعب الحصول على DNSSEC إذا كنت تستخدم هذه الشركة. جميع مشغلي السجل تقريبًا يتعاملون الآن بشكل صحيح، لكن فيما يتعلق بالمستخدمين النهائيين، يمكن للمستخدمين النهائيين أيضًا أن يطلبوا من بائعي البرامج استخدامه وزيادة الطلب وزيادة حجم الطلب على DNSSEC في هذه المرحلة، ربما يكون الدافع الأكبر الذي يحتاج الناس إلى سماعه لأنه بمرور الوقت حيث أن البرامج المختلفة قد تناولت هذه الأنشطة مباشرة، كانت الإجابة في معظم الأوقات أن عملائنا لا يطلبون ذلك، وهذا هو أحد الأسباب وراء قيامنا بجلسات مثل هذه، لمساعدة الناس ليس فقط على فهم ما هذا، ولكن لتفهم أنك كمستخدم نهائي لديك دور، وأن تطلب ذلك.

شخص غير محدد: أود أن أضيف شيئا لما قاله روس. بعض الشرائح قبل النهاية، كان هناك رسم بياني ذكر التحقق من صحة المعالج. عندما نقيس نجاح DNSSEC، فإن أحد المقاييس التي نستخدمها هو عدد المناطق التي تم توقيعها، ولكن الذي له نفس هذه الأهمية هو من الذي يتحقق؟ لا يصح ذلك إذا كان لديك جميع النطاقات في العالم موقعة إذا لم تكن التطبيقات، وإذا لم تتحقق المعالجات المتكررة من صحة ما تحصل عليه. ثم كان هناك شيء آخر لدي لما قلته لكن لا يمكنني تذكره، لذلك سأغلق الميكروفون.

ويس هارداكر: حسنًا. لذا، سؤال جيد، ونحن نحاول باستمرار جمع الإحصاءات وتتبع الاستخدام ومعرفة ما إذا كان DNSSEC لا يزال ينمو، وإذا نظرت إلى النشر مع مرور الوقت، فإن DNSSEC نفسه ما زال ينمو. إنه لا ينمو بالسرعة التي نريدها لأنه لا يمكنه ذلك. بالسرعة التي نريدها تعني تعيين كل شيء اليوم.

هذه صفحة وضعتها معًا. إنها تسمى stats.dnssec-tools.org. البيانات تأتي من شخص ما، فيكتور دوتشوفني، وهو خبير في ربط DNSSEC بالبريد. كما ترون، كانت هناك مجموعة من القفزات الكبيرة مؤخرًا - في الآونة الأخيرة في الواقع، خلال الشهرين الماضيين - والتي تتبعت ما إذا كانت خوادم البريد الإلكتروني تستخدم بالفعل سجلات البريد الإلكتروني الموقعة من DNSSEC. بعض هذه القفزات الكبيرة جاءت في الواقع من الشركات الحديثة التي بدأت تشغيل كل شيء، وجميع خوادم البريد الخاصة بهم. تعمل هذه الأجهزة على تشغيل أكثر من نطاق واحد لخوادم البريد، وقد قامت بتشغيلها جميعًا مرة واحدة، وهذا هو سبب وجود قفزات كبيرة.

لذا، فإن الخبر السار هو أننا نحصل على المزيد والمزيد من الاستخدام، ولكن الكثير من كلماته المتصاعدة، والكثير منها هو أنشطة مثل هذه والأنشطة التي تقوم بها ISOC لترويجه. لا يزال هناك الكثير من العمل الذي يتعين القيام به، على الرغم من أننا حصلنا على أكثر من 10 ملايين نطاق موقعة أو شيء من هذا القبيل. الحقيقة هي أن com.

لديها الكثير والكثير والكثير أكثر من ذلك، لذلك نحن نحاول النمو باستمرار. هل من أسئلة أخرى؟

[كوفي]: اسمي [كوفي]، من سجل اسم النطاق في غانا، ولدي سؤالان سريعان. الأول يدور حول السؤال الأول وهو: هل من الممارسات المعتادة تغيير المفاتيح الخاصة بشكل منتظم أو الانتظار حتى يتم اختراقها قبل التغيير؟ والثاني هو: هل DNSSEC مطلب للحصول على اعتماد ICANN بأي طريقة أو شكل أو نموذج للمسجلين وأشياء من هذا القبيل؟

ويس هارداكر: إنه سؤال جيد. للإجابة على سؤالك الأول، توجد مدرستان فكريتان في هذا الصدد. يعتقد بعض الأشخاص أنك لست بحاجة إلى تدوير المفاتيح حتى يتم اختراقها [المفاتيح]. في هذه الأيام، إذا قمت بإعداد مفاتيح قوية بما فيه الكفاية - لأنه يمكنك عمل مفاتيح ضعيفة للغاية، ولكن إذا قمت بإنشاء مفاتيح قوية بما فيه الكفاية، فلست بحاجة حقًا إلى تدويرها كثيرًا. سوف أخبرك أنني لا أدير مفاتيحي بشكل متكرر.

التوجيه العام هو أنه إذا لم تفعل ذلك، فلن تعرف كيف. لذلك، من الناحية التشغيلية، إذا قمت بذلك بشكل منتظم، فيمكنك التأكد من أن لديك المهارات التي تحتاجها من أجل القيام بذلك إذا كنت بحاجة إلى ذلك بسرعة، لذلك يقوم الكثير من الأشخاص بتدوير مفاتيحهم بشكل منتظم، مرة واحدة كل سنة أو شيء من هذا القبيل من أجل القيام بذلك.

السؤال الثاني هو أن ICANN لديها متطلبات لبعض الهيئات التي تتعاقد معها. على سبيل المثال، على جميع نطاقات gTLD الجديدة دعم DNSSEC. لا أعرف الإجابة على سؤال المسجلين. هل على المسجلين الجدد [غير مسموع] دعم DNSSEC؟

روس موندي: لست متأكدًا، لكنني لا أعتقد أن هذا المطلب موجود في متطلبات المسجل حتى الآن.

ويس هارداكر: إنه سؤال جيد. شكرًا. أسئلة أخرى، كان هناك سؤال واحد هنا، وهناك سؤالان في الخلف أندرو عندما تنتهي منهم.

[كوري]: أنا [كوري] من الولايات المتحدة. كان لدي سؤال يتعلق على وجه التحديد بـ- كان DNSSEC موجود منذ عدة سنوات كما أفهمه، ولكن في الآونة الأخيرة كان هناك حديث حول DNS عبر HTTPS أو TLS، فكيف يعمل هذا العامل مع DNSSEC؟ هل هم متكاملون، هل هم متنافسون، كيف يرتبطون ببعضهم البعض؟

ويس هارداكر: إنه سؤال جيد. أنتم يا رفاق، مطلعون جيدًا. أنها منبهر. لذا هناك بعض الأشياء، وهم ليسوا متنافسين. إنهم تكميليون في الكثير من الأشياء. تقوم DNSSEC بتوقيع البيانات، لذلك لا يهم حقًا كيفية نقلها أو مكان تخزينها، بل هي علامة حتى تعرفوا أن السجل لم يتم تغييره. يوجد DNSSEC عبر TLS وهو أحد المواصفات الحديثة التي تقوم بتشفير وتصديق حركة المرور بين جهازين. ويقوم DNS عبر HTTPS بنفس الشيء، ولكنه يرسله عبر HTTPS والميزة الأساسية لذلك هي أنه لا يمكن حظره بواسطة جدران الحماية التي تتيح المرور العادي عبر الويب.

لذلك، هناك أسباب مختلفة لاختيار كل واحدة من تلك التقنيات، لكن الفرق الأكثر أهمية بين DNSSEC والآخران هو أن DNSSEC يوقعها لذا لا يهم من أين تحصل عليها فأنت تعرف أنها أصلية. أنتم تعلمون، أنها محمية من جهة السلامة. إذا استخدمت DNSSEC عبر TLS أو عبر HTTPS، فأنت تعلم أن هذه المعاملة الفردية جيدة ولكن ليس لديك تاريخ لكيفية حصولهم على هذه البيانات.

لذا، يميل DNS إلى استخدام الكثير من القفزات المتعددة، والكثير من الحالات - مثل إذا كنت تستخدم DNS عبر HTTPS للتحدث إلى أحد مقدمي الخدمات الذين يفعلون ذلك،

فأنت لا تعلم أنهم خرجوا بالفعل من وراء الكواليس وحصلوا على البيانات الصحيحة ومن ثم التحقق من ذلك. لا تقوم الخوادم الموثوقة باستخدام DNS عبر TLS أو HTTPS حتى الآن.

روس موندي: مدونة واحدة سريعة لورشة عمل الأربعاء. هناك ورشة عمل DNSSEC يوم الأربعاء، وهناك عرض تقديمي محدد في ورشة العمل حول هذا الموضوع بالتحديد.

ويس هارداكر: الأربعاء يوم رائع. وإذا أردتم المزيد من DNSSEC, فيوم الأربعاء يوم مناسب.

روس موندي: واسمحوا لي أن أقدم ملخصًا سريعًا لما قلته، أن DNSSEC موجود لحماية البيانات. يوجد DNS على البروتوكول المشفر لحماية خصوصية استفسارك، وهما شيئان مختلفان.

ويس هارداكر: نعم. وراءك أندرو. عودة إلى الخلف، التالي، حسنًا.

[بولجيشنر]: مرحبًا أنا [بولجيشنر] من نيبال. يعمل DNSSEC على حماية المستخدم النهائي، أليس كذلك؟ لذلك، هل هناك أي صعوبة في جعل DNSSEC غير إلزامي، أو ربما يمكنكم تحديد التاريخ النهائي ويحتاج الجميع إلى الانتقال إلى DNSSEC - هل هناك أي صعوبة؟

ويس هارداكر: هذا صعب، لأن العالم عالم حر ويمكن للناس اختيار استخدامه أم لا. هناك عبارة شائعة: لا يوجد شرطة إنترنت. لا يوجد أحد يفرض الخير على الشر في الإنترنت، لذلك عليك

اختيار التقنيات التي تعمل من أجلك والتأكد من أنك تستخدم مواقع في العالم قد تحتوي عليها أو أشياء من هذا القبيل، لسوء الحظ، لا، لا يوجد طريقة لإجبار الجميع على التحول إلى استخدامه. سوف يكون هذا أكثر سهولة أليس كذلك، لكن لا.

روس موندي: أحد التعليقات هو أن بعض المؤسسات قد اختارت وضع سياسات أمنية تملي استخدام بعض تقنيات الأمان. لذلك، اختارت بعض المنظمات القيام بذلك ولكن لا توجد إجابة واحدة لكل شيء.

ويس هارداكر: هذه نقطة صحيحة للغاية وهناك بعض الحكومات التي اختارت أن تستخدم جميع البنية التحتية الحكومية DNSSEC كمثال جيد. شكرًا هذه نقطة جيدة للغاية.

شخص غير محدد: مرحبًا، أنا [غير مسموع] من سريلانكا. ليس لدي سؤال سريع. لذا، فإن DNSSEC يعيق التدفق العادي لـ DNS. لذا، عندما يحدث هذا، هل يوجد أي تباطؤ في شبكة الإنترنت، وإذا كان الأمر كذلك، فما نوع التباطؤ الموجود هناك؟

ويس هارداكر: حسنًا، لذلك إذا فهمتك بشكل صحيح، فأنت قلق بشأن السرعة التي يتكبدها DNSSEC من أجل القيام بهذا التحقق. سؤال رائع. هناك بعض النقاط. أولاً، DNSSEC أبطأ قليلاً لأنه يتطلب في الواقع عددًا أزيد من الطلبات، وهناك الكثير من الدراسات. يمكنكم فعلا العثور على دراسات قام بها الأشخاص بالفعل بقياس ذلك.

وهذا هو الجزء الأكثر أهمية. يتم تخزين بيانات DNS مؤقتًا، وقد ذكرت ذلك مرة واحدة في الشريحة لكننا لم نتحدث عنها كثيرًا. يتم تخزين جوانب الأمان في ذاكرة التخزين المؤقت أيضًا، لذلك بمجرد البحث عن bigbank.com، تحتوي جميع هذه السجلات

على روابط زمنية مرتبطة بالفترة التي يفترض أن تتذكرها بها. لا يتم إعادة التحقق من الصحة في كل مرة. بمجرد التحقق من صحتها، يضعوها في ذاكرة التخزين المؤقت الخاصة بهم، ووضع علامة عليها بأنها آمنة، وبعد ذلك تتاح لفترة طويلة من الزمن. هذه إحدى الميزات الرائعة حول نظام أسماء النطاقات DNS هي أن أول شخص يخرج ربما في بداية اليوم قد يكون لديه استجابة أبطأ قليلاً وقابلة للقياس بالكاد، لكن الجميع بعد ذلك يحصلون على البيانات المخزنة مؤقتًا بسرعة كبيرة. إنه سؤال جيد.

[كريستيان]: مرحبًا، اسمي [كريستيان] من ساحل العاج. أود أن أعرف شيئًا - أنا لست تقنية جدًا، لذا قد يبدو سؤالي غبيًا بعض الشيء.

ويس هارداكر: لا، لا بأس بذلك، تفضلي.

[كريستيان]: لكن أود أن أعرف، في حالة احتمال اختطاف DNS، هل هناك أي نوع من الإجراءات لـ DNSSEC لحل المشكلة، وهل هناك حالات قد تضطر فيها إلى انتهاك تلك الحالات وربما تتصرف بشكل مباشر؟

ويس هارداكر: لذلك، واجهت مشكلة صعبة حقًا أعتقد أن العديد من ميزات الأمان في العديد من البروتوكولات وحتى العديد من الأنظمة المادية. لا يقوم الناس بحماية أنظمتهم إلا بعد فوات الأمان.

إذاً، ما تسأل عنه أساسًا هو ما إن يتم اقتحام منزلك وسرقة أموالك، هل يمكنك فعل أي شيء حيال ذلك، حيال هذا الواقع؟ لا يمكنك ذلك. يجب عليك وضع أقفال أفضل على أنظمتك مسبقًا لحمايتها قبل حدوث شيء ما. لذلك، لا يمكن لـ DNSSEC إصلاح الأشياء

بمجرد قيام DNS باختراقها. والخبر السار هو أنه بنفس الطريقة التي ستنتهي بها ذاكرة التخزين المؤقت في نهاية المطاف، ستختفي المعلومات السيئة في النهاية، ونأمل أن يبدأ المستخدمون في الحصول على المعلومات الجيدة، ولكن الواقع هو إذا كنت ترغب في حماية بيانات DNS الخاصة بك اليوم، فأنت يجب عليك نشر DNSSEC قبل أن تتعرض لتلك المشكلات. هل يبدو ذلك منطقيًا؟ شكرًا.

أبراهام: انا اسمي أبراهام من نيجيريا. سؤالي هو أنه في تطبيق DNSSEC، هل نحن بحاجة إلى زيادة متطلبات الأجهزة للنظام، أم أننا بحاجة إلى الحفاظ على ما لدينا قبل البدء في تنفيذه؟ شكرًا.

ويس هارداكر: لذلك، أعتقد إذا سمعت ذلك بشكل صحيح - لدي الكثير من الصدى، لذلك أقف هنا بجوار هذه الشاشة. أنت تتساءل عما إذا كان هناك زيادة في متطلبات الأجهزة لنشر DNSSEC. هل هذا صحيح؟ حسنًا، مثل المزيد من وحدة المعالجة المركزية والمزيد من الذاكرة، وهذا النوع من الأشياء؟ نعم، حسنًا، جيد.

روس موندي: حسنًا، كان هناك تحليلان مختلفان تم إجراؤهما في هذا الشأن ومعظمهما تم إجراؤه من قبل أشخاص يركزون على TLD أو مستوى الجذر، وكان الاستنتاج السريع هو النمو الطبيعي ودورة استبدال الأجهزة التي نتابعها حاليًا كافية بالفعل.

ومع ذلك، فما هي الأرقام؟ كما أتذكر ما هي، هناك تأثير في الأجهزة ربما يتراوح بين 3 و 8% على توقيعك، لكن هذا ليس في الوقت الحقيقي. لم يتم في ... يمكنكم التوقيع قبل تحميل المنطقة. للتحقق من الصحة، يكون في نفس المستوى تقريباً، وربما يصل إلى 10%، لكنه ليس له تأثير كبير ولكنه شيء يجب أن يؤخذ في الاعتبار عند النظر في برنامج ترقية الأجهزة المستمر لبنية DNS الأساسية لديك.

ويس هارداكر: شكرًا. والشيء الآخر الذي يجب ملاحظته هو أن هناك زيادة في الذاكرة لأن هناك المزيد من السجلات وأشياء من هذا القبيل. تحتاج إلى المزيد من الذاكرة بعض الشيء. لذلك، على سبيل المثال، أنا أخدم على ما أعتقد 20 منطقة أو أكثر - لم أشتر قط أجهزة جديدة لنشر DNSSEC في أي من الأشياء التي قمت بها. إذا كنت TLD رئيسيًا يحتوي على الكثير والكثير من المدخلات، فربما يتعين عليك التفكير في ذلك ولكن في الواقع ربما لا يكون الأمر كذلك بالنسبة لمعظم الأشخاص، أنه سيتم تشغيله على أجهزتك الحالية دون مشكلة.

[بول]: مرحبًا، أنا [بول] من المملكة المتحدة. هل هناك أي آليات تم وضعها من خلال السياسة لتتبع ورصد خروقات DNS التي يتم إجراؤها على نطاقات TLD أو السجلات؟

ويس هارداكر: الرصد لأي غرض؟ نحن هنا حول DNSSEC اليوم. هل تعني مراقبة أداء الأمان لديهم أو البيانات التي يوزعونها؟

[بول]: لبناء قاعدة بيانات من الانتهاكات من أجل، بهدف طرد الأشرار؟

ويس هارداكر: حسنًا، من الصعب جدًا مراقبة ما إذا كانت هناك أشياء يتم إساءة استخدامها لأن الواقع ينتهي بك الأمر إلى مراقبة العالم بأسره. يمكنني أن أراقب بجوار TLD وأستطيع التحقق، مهلاً، إنهم يوزعون المعلومات الصحيحة دائمًا ولكن هذا لا يحدث عادةً في الهجمات. تحدث الهجمات [بالنسبة إلى المستخدمين النهائيين] وأشياء من هذا القبيل، وبالتالي ستضطر إلى مراقبة كل مزود خدمة إنترنت في العالم. هذا سؤال معقد للغاية. لا تتردد

في العودة إلي بعد ذلك أيضًا إذا كنت ترغب في التحدث حوله أكثر من ذلك، لأنها مشكلة صعبة وإذا كان لدينا إجابة على ذلك فمن المؤكد أننا قد ألقينا القبض على جميع الأشرار الآن.

شخص غير محدد: شكرًا. لإضافة وجيزة إلى الإجابة السابقة حول متطلبات الأجهزة لـ DNSSEC، ينشر nic.cz مركز معلومات الشبكة في جمهورية التشيك معايير قياسية منتظمة على خوادم DNS و DNSSEC. اعثر عليّ بعد ذلك. سأريك الرابط، وبالتالي فإن التأثير على الجهاز لا يكاد يذكر، إنه قليل، لكنك لن تلاحظ أي شيء إلا إذا كنت تتعامل مع حوالي مليون استفسار في الثانية على الجهاز الواحد.

ويس هارداكر: حسنًا، شكراً جزيلاً لك. أندرو، تعال هنا.

[برونوين]: مرحبًا أنا [برونوين] من أستراليا. سؤالي هو، إذن، في المسرحية الهزلية الخاصة بكم سابقًا، كان لديكم المعالج الذي يقوم بعملية التحقق من صحة الشهادة على كل مستوى من مستويات النطاق، فهل هناك أي تحديثات أو تغييرات مطلوبة للبرامج على مستوى المعالج لدعم هذا التحقق من الصحة في الواقع لأن المعالج سيقوم، على ما أفترض، بقرارات لكل من نطاقات DNSSEC الممكنة وغير الممكنة.

ويس هارداكر: سؤال جيد جدًا. لذا، فإن الخبر السار هو أن معظم برامج المعالج الحديثة تدعم DNSSEC بالفعل، مثل BIND و unbound هما الأكبر على الأرجح. لا أتذكر نسخة unbound، لكنهما يدعمان جميع ميزات DNSSEC المنشورة الأكثر أهمية لمدة 5 أو 10 سنوات على الأقل. لذا، إذا كنت تسحب أي شيء مؤخرًا أو حتى تقوم بتوزيعها مع أي نظام أساسي لخادم مزود خدمة الإنترنت مثل نظام التشغيل، يمكنني أن أضمن تقريبًا

قيام معالج Windows بفعل ذلك أيضًا في هذه المرحلة، لذا إذا كان لديك أي شيء حديث فهو ليس مشكلة. لقدكان متوفرًا لمدة طويلة.

[كريجان]: مرحبًا، وشكرًا. أنا اسمي [كريجان] من ناورو. أظن أن هذا يشبه DNSSEC لـ Dummies، لذا إليك سؤال وهمي. من منظور مزود خدمة الإنترنت، هل هناك أي مؤشرات أو إشارات حمراء يجب اعتبارها تشير إلى أن DNSSEC مطلوب؟

ويس هارداكر: هذا سؤال جيد للغاية. حسنًا، مزودو خدمة الإنترنت هم الذين يحتاجون إلى نشر مدقق، يحتاجون إلى النشر - لقد رأيت صديقي، وارن، يتجول من شخص لآخر في المسرحية. يجب عليهم القيام بمعظم العمل. يجب عليهم الانتقال إلى الجذر، وعليهم التحدث إلى TLD، وعليهم التحدث إلى الخوادم لكل شيء، وعليهم التأكد من أن برامجهم قادرة على التعامل مع عمليات البحث الآمنة وغير الآمنة لأن الواقع هو أنه لا يمكن إجبار DNSSEC على البقاء حتى يصبح العالم آمنًا.

تجدر الإشارة إلى أننا لم نتحدث عن ذلك خلال الشرائح وأثناء المسرحية، لكن DNSSEC نفسها ستخبرك بإجابة، "أنا آمن. هذا الخادم الآخر الذي تطلبه غير آمن، ويمكنني أن أحقق لك أنه ليس كذلك فأنت وحدك في هذه المرحلة. " لذلك، هناك بالفعل تقنيات مضمّنة للقيام بأمان جزئي ومن ثم يمكنك معرفة متى يمكنك الوصول إلى الأمان أو أنك غير آمن.

ما يجب على مزودي خدمة الإنترنت القيام به هو بالتأكيد مراقبة سجلاتهم والتأكد من ذلك، خاصة إذا بدأوا في رؤية فشل التحقق من الصحة، ربما تعرض شيء ما للهجوم أو ربما توجد مشكلة على الإنترنت. يعتبر النظر في السجلات أمرًا مهمًا في الواقع بغض النظر عما إذا كنت تحاول نشر تقنيات أمن أم لا.

[ألفيفا]: مرحبًا، [ألفيفا] من بنجلاديش. لستُ متأكدة مما إذا كنت الشخص الصحيح لطرح هذا السؤال.

ويس هارداكر: إذا لم أكن، فسيكون هو كذلك.

[ألفيفا]: كان السؤال هو ما إذا كنت قد واجهت أي حادث كبير بعد مرور KSK وكيف تعاملت مع ذلك؟

ويس هارداكر: إنه سؤال جيد. حسنًا، فإن السؤال، لأنه سوف يؤدي إلى ورشة عمل DNSSEC لك، هل كانت هناك أي مشاكل بعد مرور KSK، وماذا فعلت حيال ذلك وأشياء من هذا القبيل؟

روس موندي: شكرًا. عذرًا، لم أسمع بوضوح. الصوتيات هنا صعبة بعض الشيء. على أي حال، كان حدث التمرير في KSK حسب تقدير الكثير من الناس لا يعد حدثًا، وكانت هناك بعض الاختلافات الملحوظة في مقدار حركة المرور بمجرد إبطال المفتاح القديم، لكننا سننظم جلسة عمل حول ذلك و سيكون هناك بعض المعلومات المقدمة حول هذا الموضوع، وفي الواقع من منظور تشغيلي، لم يكن هناك أي تأثير ملحوظ على لفة KSK على الإطلاق. لذلك، كان بكل المقاييس نجاحًا تشغيليًا. لقدكان نجاحًا كبيرًا.

ويس هارداكر: هناك الكثير من العروض التقديمية التي يمكنك الرجوع إليها في ورش عمل DNSSEC السابقة حول سبب تأخر لفة KSK لمدة عام، ما هي بعض الأشياء التي تم العثور عليها. نظرًا لأنني قدمت عروضًا متعددة، قد قدمها الكثير من الأشخاص الآخرين. ويوم الأربعاء، ربما من المحتمل أن يكون هناك آخر مجموعة من العروض التقديمية حول

هذا الموضوع، لأن البت الذي تم إبطاله تم تعيينه في 11 يناير، وكانت تلك هي الخطوة الأخيرة في تدوير المفتاح وهناك بعض البيانات المثيرة للاهتمام التي نتجت عن ذلك، هذا يستحق النظر فيه. تعال إليَّ لاحقًا إذا كنت تريدين بالفعل قائمة بعناوين URL. يمكنني إرسال مقاطع فيديو إليك لمشاهدتها لاحقًا إذا كنت تشعرين بالملل حقًا، لكنها جيدة. هل من أسئلة أخرى؟ لدينا القليل من الوقت متبق.

حسنًا. لا أرى أي أيادٍ أخرى، لذا أشكركم جميعًا على مثل هذه الأسئلة المتفكرة. كنتم بالفعل أحد أكثر الجماهير استنارة الذين أعتقد أننا لم نحظى بهم من قبل. جميع الأسئلة كانت تقنية للغاية وتُظهر أنكم يا رفاق قد قمتم بأداء واجبكم في وقت مبكر. فليست هناك أسئلة حمقاء. لا تترددوا في المجيء اسألوني لاحقًا إذا كنتم تريدون ذلك. كل هذه التكنولوجيا تستغرق وقتًا طويلاً لتتعلمها ونعملها منذ 10 أو 20 عامًا، وبالتالي لا يوجد شيء اسمه سؤال غبي. هناك فقط أسئلة تتعلمها ولديكم الكثير لتتعرفوا عليه.

الكثير منا سوف يكون هنا بعد ذلك. لا تترددوا في المجيء والتحدث معنا. في الوقت الحالي، يرجى الاستمتاع ببقية ICANN والرجاء الحضور خلال ورشة عمل DNSSEC يوم الأربعاء إذا كان ذلك ممكنًا، لأنه مكان عظيم آخر لتعلم الأشياء، وكذلك يوم التكنولوجيا غالبًا ما يكون يوم الاثنين أيضًا. شكرًا جزيلاً.

**[نهاية النص المدون]**