سان خوان – الجلسة اليومية للزمالة
الإثنين الموافق 12 آذار (مارس) 2018 – من الساعة 12:00 م إلى الساعة 01:30 م بتوقيت الأطلنطي القياسي
ICANN61 | سان خوان، بورتوريكو

شخص غير محدد: طاب صباحكم. ICANN 61، 12 آذار (مارس) الجلسة اليومية للزمالة.

سيرانوش فاردانيان: لدينا اليوم جلسة خاصة وافق خبراء التكنولوجيا على عقدها لكم. لدي شركة رائعة هنا، وأود أن أعطي الكلمة لراتشيل أولا، ثم أنتم يا رفاق لتقديم أنفسكم للزملاء لمعرفة من يقوم بتقديم العروض.

يرجى تناول الغداء، تعال والعودة للجلوس والانتباه. هذه حقا جلسة ممتعة للغاية، ومتأكد أنكم ستعجبون بها. راتشيل؟

راتشيل رييس: مرحبا. طاب مساءكم، جميعا. مرحبا بكم في جلسة أساسيات نظام أسماء النطاقات DNS. تستغرق هذه الجلسة ساعة ونصف الساعة. ونستغرق 15-30 دقيقة لأسئلتكم والإجابة عنها في نهاية العرض التقديمي.

معكم راتشيل رييس. من الدعم الفني لمؤسسة ICANN. ويساعدني جون كرين هنا الذي يجلس على يميني في جلسة الأسئلة والأجوبة في وقت لاحق.

جون كرين: معكم جون كرين. أنا المسؤول الرئيس للأمن والاستقرار والمرونة في ICANN. وشاركت أيضا في تشغيل خوادم الجذر وخدمات DNS الأخرى خلال العشرين 20 أو الثلاثين 30 سنة الماضية.

ويختبئ في الركن هناك على الهاتف السيد/ مات لارسون، المعروف أيضا باسم مستر DNS. وقضى أيضا في صناعة DNS على الأرجح مدة أطول مما قضيت.

وبذلك أعود مرة أخرى إلى راتشيل.

راتشيل ريبس: حسنا، أتمنى أن أحصل على انتباهكم أثناء تناولكم لطعام الغداء. لذلك دعونا نبدأ.

إن عناوين IP سهلة الاستخدام على الآلة، لكن من الصحيح أيضا أنه من السهل علينا أن نتذكر الأسماء، لكن من الصعب علينا أن نتذكر الأرقام.

لنأخذ على سبيل المثال، بعضنا – على الأقل عن نفسي – من الصعب جدا أن أتذكر أرقام هواتف عائلتي أو حتى أصدقائي، لكن من السهل تذكرهم حسب الاسم، وهو الشيء نفسه لتذكر الأسماء والأرقام في نظام DNS.

في الأيام الأولى للإنترنت، كانت الأسماء بسيطة للغاية. ولم يكن هناك أي أسماء نطاقات في ذلك الحين. أسماء بعلامات مفردة من 24 حرفا يشار إليها باسم أسماء المضيفين.

دقة الاسم هي تعيين عنوان بروتوكول الإنترنت IP إلى أسماء. في الأيام الأولى لأسماء ملفات مضيفي الإنترنت HOST.TXT، وهذا ما نقوم بتحديثه ويقوم على صيانته مركزيا مركز معلومات الشبكة أو ما نسميه NIC في معهد أبحاث ستانفورد. يقومون يدويا بتحديث الملف عبر البريد الإلكتروني، ويتم إصداره مرة واحدة في الأسبوع ويمكن تنزيله بواسطة FTP. كان ذلك في الأيام الأولى للإنترنت.

المشكلة في هذا النظام هي أن كل شيء يتم تحريره يدويا، لذا فهو عرضة للخطأ فعلا وغير فعال للغاية لأنه يجب عليك إرسال بريد إلكتروني أولا قبل أن يتمكنوا من تحديثه بالفعل. ويتطلب ذلك أيضا عرض نطاق ترددي كبير عند محاولة رفع الملف أو تنزيله. ولم يتغير ذلك لمدة طويلة.

لهذا السبب بدأ الناس حوارا في الثمانينات حول كيفية استبدال النظام الحالي. وتوصلوا إلى مفهوم DNS أو نظام أسماء النطاقات الحالي حيث سيعملون على توسيع نطاق

مشكلة نظام HOST.TXT الحالي وكذلك تبسيط توجيه البريد الإلكتروني. ويمكنكم العثور على وثائق أكثر حول المتطلبات الواردة في طلبات التعليقات RFC المقدمة هنا. سوف يخبركم كل من RFC 799 وRFC 819 بالمزيد عن المتطلبات أو تلك المناقشة المتعلقة بمفهوم DNS.

DNS باختصار. سنناقش هنا أولا المصطلحات التي نستخدمها في نظام DNS. لدينا DNS، بيانات DNS، محللون، خوادم الأسماء، التخزين المؤقت، والتكرار.

سأناقش ذلك بالتفصيل باستخدام المخطط هنا. لدينا المحلل الجذري كأحد المصطلحات التي سنناقشها. وخادم الاسم المتكرر، وهو الذي يسل الاستعلامات إلى خوادم الأسماء لدينا. لذا فإن خوادم الأسماء هي تلك الموجودة على يساري، والتي تقع على يمينكم. ثم خوادم الأسماء التي تقدم إجابات محددة على الاستعلامات التي يتم طرحها من الخادم المتكرر. ولدينا فقاعة صغيرة جدا هنا تقول "ذاكرة مؤقتة." يتم استخدام الذاكرة المؤقتة في نظام DNS لجعلها أكثر كفاءة وقابلية للتوسع. وسنقوم بالتعمق في هذا في جزء لاحق من العرض.

فضاء الأسماء هو بنية قاعدة بيانات DNS في شكل شجرة مقلوبة. وعادة طريقة قراءة بنية بيانات الشجرة هي من أعلى إلى أسفل، ولكن في عالم DNS لدينا نقرأها من الأسفل إلى الأعلى.

لنأخذ هذا المخطط على سبيل المثال. لا نقرأه على أنه ".com.example.www" ولكن بدلا من ذلك، نقرأه على أنه ".."www.example.com""، وهو ما يطلق عليه اسم النطاق المؤهل كليا.

في فضاء السماء، الأول هو الجذر. والثاني هنا هو ما نسميه عقد المستوى الأعلى، تليها عقد المستوى الثاني، ثم عقد المستوى الثالث.

لكل عقدة من هذه العقد رمز. تتكون الرموز أو الأحرف القانونية التي يمكنك استخدامها للرموز، وهي ليست سوى حروف، أرقام، واصلات أو ما نسميه حرف، رقم، واصلة LDH.

الحد الأقصى للطول الذي يمكننا استخدامه لرمز هو 63 حرفا. وليست حساسة في الواقع لحالة الأحرف، لذلك يمكنك كتابة com. بشكل أساسي مثل "com" أو "cOm". ولا يهم الأمر حقا.

كل عقدة لديها اسم نطاق. وفي مثالنا، سنستخدم هنا هذه الشجرة. اسم النطاق المحدد هو "www.example.com".. ويتم فصلها كلها بالنقاط.

كما ذكرت سابقا، ينتهي اسم النطاق المؤهل كليا أو FQDN بنقطة دوت. في معظم الأوقات التي نبحث فيها عن اسم نطاق، لا نستخدم النقطة في النهاية ولكننا نكتب "example.com" أو "www.example.com" فقط.

النطاق هو عقدة وكل شيء تحته. في مثالنا هنا، يعد com. هو أعلى عقدة لنطاقنا وأي شيء تحته هو إقليم com. أو اسم النطاق com.

المناطق هي الإدارة الإدارية، وكل منطقة DNS تقوم على حد السلطة ويتم تفويضها إلى كيان. يمكن أن تحتوي منطقة DNS على نطاق واحد أو العديد من النطاقات أو النطاقات الفرعية. ويخلق التفويض المناطق. منطقة التفويض هو ما نسميه الأصل والمنطقة التي تم إنشاؤها هو ما نسميه الفرع.

هنا قام الأصل، وهو منطقة الجذر، بتفويض هذه المعلومات إلى الفرع com.، uk.، coffee. وقام com. بتفويضه إلى هذا الفرع وهو foo. وbar. وexample.

خوادم الأسماء، كما ذكرت سابقا، هي التي تجيب على الاستفسارات التي يتم طرحها من الخوادم المتكررة. ولخوادم الأسماء الرسمية لمنطقة ما معرفة كاملة بتلك المنطقة. وفي الأساس، عندما تقومون بإرسال استعلام، إذا كان خادم اسم متكرر فارغ، فإنه ينتقل مباشرة إلى المنطقة لأن هذا هو حيث يجب عليكم الانتقال لأنها تحتوي على الرد المحدد على الاستعلامات. وللمناطق خوادم رسمية متعددة. وهذا لأنه يريد تحقيق الكفاءة واستخدام التكرار.

كيف يمكنكم الاحتفاظ ببيانات منطقة في حالة تزامن عبر خوادم رسمية متعددة؟ لدينا بروتوكول DNS الحالي المضمن في الخادم الذي يقوم بتكرار المنطقة. يحدث ذلك باستخدام الخوادم الأساسية والثانوية.

يحتوي الخادم الأساسي على بيانات المنطقة المحددة. إذا أردتم إجراء تغييرات على منطقة ما، فيجب أن تكون على الخادم الأساسي. من ناحية أخرى، الخادم الثانوي أو ما نسميه خادم تابع هو الخادم الذي يقوم باسترجاع بيانات المنطقة من خادم رسمي آخر. والعملية هي ما نسميها نقل المنطقة. نقل المنطقة هو في الواقع الاتصال بين خادم DNS وخادم رسمي آخر.

خادم آخر علينا مناقشته هنا هو الخادم الرئيسي حيث ينشأ ملف المنطقة. لكن ضعوا في اعتباركم أن الخادم الرئيسي لا يحتاج إلى أن يكون خادمكم الأساسي. يمكن أن يقوم خادمكم الثانوي بعمل الخادم [الرئيسي] أيضا.

يبدأ نقل المنطقة من خلال الخادم الثانوي. يمكنكم أن تجدوا تحت RFC 1996 الحالي أنه يحتوي على تفاصيل لكيفية إجراء هذا النقل للمنطقة أو كيفية إجراء تغييرات على ملف المنطقة.

ننتقل الآن إلى سجلات بيانات DNS. سجلات بيانات نظام أسماء النطاقات DNS هي ما نسميه كثيرا للأشخاص باسم سجلات بيانات DNS. إذا استطعت أن تتذكر ما ذكرته سابقا، فإن كل عقدة لها اسم نطاق. ويحتوي اسم النطاق على أنواع مختلفة للبيانات المرتبطة به، ويتم تخزين هذه البيانات في اسم النطاق فعليا في سجلات بيانات DNS.

لدينا أنواع مختلفة من سجلات بيانات DNS، لكننا لن نناقش سوى عدد قليل منها. ننتقل إلى تنسيق سجلات بيانات DNS. تحتوي سجلات بيانات DNS على خمسة حقول: المالك، فترة بقاء البيانات فعالة أو TTL، الفئة، النوع، ثم RDATA. المالك هو اسم النطاق المرتبط بسجل بيانات DNS. فترة بقاء البيانات فعالة هي الوقت الذي يمكن فيه تخزين السجل مؤقتا في خادمك. الفئة هي آلية لقابلية الامتداد غير مستخدمة إلى حد كبير، والتي غالبا ما نراها IN في هذا للفئة. النوع هو نوع البيانات التي يخزنها السجل. وRDATA هي البيانات التي يحملها السجل.

أعتقد أنكم أكثر دراية إذا نظرتم إلى هذا الأمر، أو يمكنني توضيحه لكم. هذه المعلومات هي ما نسميه سجلات بيانات DNS. وأعتقد أن معظمكم إذا كنتم على دراية بالشبكات، فسوف تكونوا قادرين على فهم ما كنت أقوله سابقا.

[كما ذكرت هنا]، يظهر النوع وRDATA دائما وهما ضروريان. هذه هي أنواع سجلات بيانات DNS الأكثر استخداما: ترمز بيانات A إلى بروتوكول الإنترنت – الإصدار الرابع IPv4. وترمز AAAA إلى بروتوكول الإنترنت – الإصدار السادس IPv6. NS هو خادم الاسم الرسمي. تظهر دائما SOA أو بداية السلطة في قمة المنطقة. وفي مثالنا السابق، يمكنكم العثور على معلومات SOA في com. CNAME أو الاسم المتعارف عليه هو الاسم المستعار لنطاق آخر. يرمز MX إلى خادم مبادل البريد. وPTR هو المؤشر أو يستخدم لرسم الخرائط العكسي.

كما قلت، هناك العديد من أنواع سجلات بيانات DNS الأخرى هناك. واعتبارا من كانون الأول (ديسمبر) 2017، هناك 84 بالفعل. يمكنكم الانتقال إلى موقع الويب هذا للعثور على المزيد من أنواع سجلات بيانات DNS هذه. إذا انتقلتم إلى تلك الصفحة، فهذا ما ستحصلون عليه.

دعنا ننتقل مع سجلات A وAAAA. كما ذكرت سابقا، هذه هي الطريقة التي يبدو بها سجل A. سوف يعطيكم عنوان IPv4، ثم سوف يعطيكم AAAA عنوان IPv6.

يحدد خادم الأسماء (NS) خادم الاسم الرسمي لمنطقة ما. ويظهر في مكانين، الأصل والفرع، وهلم جرا. في هذا المثال، يكون الجانب الأيسر هو منطقة الاسم، ثم الجانب الأيمن هو خادم الأسماء، وليس عنوان بروتوكول الإنترنت IP.

هذه هي الطريقة التي يميز بها سجل خادم الأسماء التفويض من الأصل إلى الفرع. تحتوي com. على 13 خادم أسماء. أساسا، هذه هي مناطق الجذر الـ 13. ويظهر هنا من الجذر على طول الطريق إلى com.

أثناء التفويض، نضمن أيضا عنوان بروتوكول الإنترنت المرتبط بالسجل. ما هو عنوان بروتوكول الإنترنت المرتبط بالسجل؟ عنوان بروتوكول الإنترنت المرتبط بالسجل هو

إما سجل بيانات DNS لعنوان IPv4 أو IPv6. تم تضمينه في سجل الأصل كجزء من التفويض. السبب وراء حاجتنا إلى وجود عنوان بروتوكول الإنترنت المرتبط بالسجل هو أنه إذا افترضنا أنكم تستفسرون عن عنوان IP لـ www.example.com، فستنتقلون مباشرة إلى منطقة الجذر. وسوف يعطيكم الجذر عنوان IP لخادم الأسماء. ثم تسأل مرة أخرى خادم الاسم، "ما هو عنوان IP لـ www.example.com؟" وسيدخل في حلقة حتى لا تتمكن من العثور على إجابتك لأنهم ليس لديهم عنوان IP حتى الآن. هذا هو السبب في أننا بحاجة إلى الحصول على عنوان بروتوكول الإنترنت المرتبط بالسجل.

تقع بداية السلطة في قمة المنطقة. هنا، هذا هو مثال للطريقة التي تبدو عليها SOA. يوجد فيها نطاقكم، خادم الاسم الخاص بكم. Hostmaster.example.com هو المسؤول عن المنطقة. ثم الرقم التسلسلي للإصدار الحالي من الملف.

يمثل الإنعاش عدد الثواني التي يجب أن ينتظرها خادم الأسماء الثانوي قبل التحقق من وجود تحديثات. ثم ترمز إعادة المحاولة إلى عدد الثواني التي يجب أن ينتظرها خادم الأسماء الثانوي قبل إعادة محاولة نقل منطقة فاشلة. وتشير انتهاء مدة الصلاحية للحد الأقصى لعدد الثواني التي يمكن لخادم الأسماء الثانوي استخدام البيانات قبل الإنعاش أو انتهاء الصلاحية. وبعد ذلك الحد الأدنى هو فترة بقاء البيانات فعالة TTL.

ينشئ CNAME أو سجل الاسم المتعارف عليه اسما مستعارا من اسم نطاق إلى آخر. على جانبي الأيمن، ربما على جانبكم الأيسر، يوجد CNAME، ثم الجانب الأيمن هو الاسم المتعارف عليه وهدف الاسم المستعار. تذكروا أن CNAME ينشئ اسما مستعارا ويشير إلى اسم متعارف عليه، لكن يرجى مراعاة عدم الإفراط في استخدامه. لا تقوموا بإنشاء سلاسل أو حلقات. ولا يبدو الأمر مفيدا على بياناتكم أيضا.

نوع سجل مبادل البريد. يحدد MX خادم بريد والتفضيل لوجهة البريد. يوضح مثالنا هنا example.com MX 10 mail.example.com. الأرقام المتوافقة، 10 و20، هي كيفية حدوث البريد الإلكتروني أو ترتيب الأولويات. كلما كان الرقم أقل، كان ذلك أفضل. هذه هي طريقتنا المفضلة [غير مسموع] لتوجيه البريد.

عكس الخرائط. في معظم الأوقات، نبحث دائما عن عنوان IP لاسم النطاق، لكن هناك أوقات نبحث فيها عن فضاء اسم بدلا من عنوان IP. هذا هو حيث سجل بيانات DNS لـ PTR يكون مفيدا للغاية. لا نستخدمه في كل الأوقات، ولكن على الجانب الشبكي، فإنه يوجد دائما في البيانات. هذا ما يبدو عليه الأمر الآن.

اسمحوا لي أن أسأل جون كرين لماذا لدينا in-addr.arpa.

جون كرين: in-addr.arpa، كما نشير إليه، هو عكس العناوين. تتحقق بعض البروتوكولات فعليا من ذلك للتأكد من أن الاسم والرقم يرسمان الاتجاهين.

راتشيل رييس: حسنا، هذه هي أنواع سجلات بيانات DNS أخرى متوفرة لدينا، لكنني نادرا ما أراها حقا، باستثناء الموقع الجديد للتفويض CDS وCDNSKEY اللذان يعدان جزءا من الامتدادات الأمنية لنظام اسم النطاق DNSSEC.

هذا مثال على ملف منطقة ما لـ example.com. يحتوي على SOA وخادم الأسماء وIPv6 وIPv4 وسجل مبادل البريد MX وCNAME أيضا. ثم في الجزء الأخير يوجد عنوان بروتوكول الإنترنت المرتبط بالسجل. لذلك يذكر بالفعل عنوان IP، الذي ذكرته سابقا. بدون هذا، فإنه سوف يستمر فقط في حلقة.

الآن ننتقل إلى عملية التحليل. كما ذكرت سابقا، لدينا محللون جذريون، خوادم أسماء متكررة، وخوادم أسماء رسمية. تتعاون هذه الخوادم للبحث عن بيانات DNS في فضاء الاسم.

المحللون الجذريون محليون جدا لعميلكم. يمكن أن يكون في هاتفكم أو يمكن أن يكون على جهاز الكمبيوتر المحمول الخاص بكم. ثم خوادم الأسماء المتكررة، مرة أخرى، هذه هي التي ترسل الاستعلامات إلى خادم الأسماء الرسمي. خوادم الأسماء [الرسمية] هي التي ترسل الإجابات على هذا الاستعلام.

يتألف استعلام DNS دائما من ثلاثة معلمات، وهي اسم النطاق والفئة والنوع، وهو ما لدينا هنا في مثالنا.

نوعان من الاستعلامات. يقوم المحللون الجذريون بإرسال استعلامات متكررة، ثم ترسل خوادم الأسماء المتكررة استعلامات غير متكررة أو تكرارية أو ما نسميه الإحالة. سنناقش هذا في وقت لاحق.

أعتقد أنني سأتخطى هذا.

هذا ما يجب أن أناقشه لأننا لنفترض أنكم تبدؤون عملية تحليل حيث يكون الخادم المتكرر فارغا أو تم تشغيله للتو. ليس لديك أي خيار هنا إلا الانتقال مباشرة إلى خوادم اسم الجذر لأن ملفات منطقة الجذر موجودة في ذلك.

كيف يمكن لخادم اسم العثور على خوادم اسم الجذر؟ يجب أن يتم تكوينهم. يتم تكوين هذا بواسطة مسؤول الخادم، وليس هناك طريقة لاكتشافهم.

هذه هي قائمة خوادم أسماء الجذر وملف تلميحات الجذر. NS هي خوادم الأسماء. A عنوان IP لـ AAAA. IPv4 هي IPv6.

إدارة منطقة الجذر معقدة للغاية، لذلك لا ينبغي لنا مناقشة ذلك. يجب تبسيط الأمر. إذا كنتم تريدون معرفة المزيد عن ذلك، ربما يمكنكم الرجوع إلى مات لارسون و إم بينتس وسيكون لديه المزيد من الوقت لمناقشة ذلك. لكننا لن نتحدث عن ذلك هنا.

هناك منظمتان تتعاونان لإدارة محتويات المنطقة، بشكل أساسي ICANN، ثم Verisign. هناك 12 منظمة تعمل في تشغيل خوادم الأسماء الرسمية. ربما تتسألون لماذا 12 حيث لدينا في الواقع 13 خوادم جذرية. ذلك لأن Verisign لديها اثنين: الخادم A والخادم J. لماذا لديهم اثنين؟ مرة أخرى، سيكون لدى جون كرين ومات لارسون إجابات لكم، لكن على الأرجح لن يناقشاها هنا. ربما في الخارج ما لم يكن لدى جون الوقت للحديث؟

جون كرين: لا، إنه مجرد عامل تاريخي. تم توزيع خوادم الأسماء آخر مرة في التسعينيات عندما تمت إضافة خوادم أسماء جديدة، ولم يتم وضعهم جميعا في مؤسسات جديدة ولم يكن لاثنين منهم صفحات رئيسية. انتقل أحدهم للساحل الشرقي إلى Verisign الذي كان له علاقة قوية مع Jon Postel وISA وبقي الآخر في ISA الذي له الحرف L. عندما تشكلت ICANN، جاء ذلك الحرف إلى ICANN وبالطبع، بقى J مع Verisign. لذا فهو مجرد عامل تاريخي لكيفية توزيعهم.

راتشيل رييس: ها نحن ذا. إذا أردتم معرفة خوادم الجذر في بلد ما، يمكنكم الانتقال إلى هذا الموقع الإلكتروني: root-servers.org. يمكنني أن أريها لكم بالفعل. لنفترض أنكم تبحثون عن خوادم الجذر المتوفرة في بورتوريكو. يتوفر L وJ في بورتوريكو حاليا. لذا يمكنك المجيء إلى هذا الموقع إذا كنتم تودون معرفة هذه المعلومات.

أيضا، لدينا Anycast التي تستخدم الآن أمثال لهذه الخوادم الجذرية التي سوف تساعدكم على البحث عن أقرب DNS أو خوادم جذر في موقعكم. كما أنه يساعد عند قيامك بعملية بحث. وهي أكثر فعالية إذا كان لديكم أمثال في موقعكم.

عملية تغيير منطقة الجذر. كما ذكرت في هذه الشريحة، هذا إصدار مبسط. هناك المزيد من العمليات وراء ذلك في الواقع. لن نناقشها، لكننا نقدم لكم فقط نظرة عامة حول كيفية تغيير ملف منطقة الجذر.

بشكل أساسي، يبدأ الأمر بمدير نطاق المستوى الأعلى TLD الذي يقدم تغييرا إلى هيئة الإنترنت للأرقام المخصصة IANA. ثم تقوم IANA بتنفيذ هذا الطلب من خلال، أولا، تحديث قاعدة بيانات منطقة الجذر، ثم إنشاء ملف منطقة جذر وتهيئة منطقة الجذر لجميع خوادم الجذر.

ننتقل الآن لعملية التحليل. هذا هو في الواقع ما يحدث إذا كنتم تقومون بإجراء استعلام أيضا على هاتفكم. لا يجب أن يكون هاتفكم فقط. يمكن أن يكون الكمبيوتر المحمول

الخاص بكم أو يمكن أن يكون عميلا آخر. كل عميل من عملائكم – كمبيوتر محمول، هاتف – يحتوي على محلل جذري وهو محلي لعميلكم.

بعد ذلك، سيطرح سؤال: "ما عنوان IP لـ www.example.com؟" ينتقل هذا السؤال إلى خادمكم المتكرر مع عنوان IP لـ 4.2.2.2، ويسأل على هذا النحو: "ما هو عنوان IP لـ www.example.com؟" سيجيب خادم الاسم المتكرر لديكم على هذا النحو: "لا أعرف، لكن ربما يحتوي خادم الجذر على هذه المعلومات."

لماذا لا يحتوي خادم الاسم المتكرر الخاص بكم على هذه المعلومات حتى الآن لأنه خادم أسماء متكرر جديد تماما. كما ذكرنا سابقا، لا يحتوي خادم متكرر جديد تماما أو فارغ على جميع معلومات ذاكرة التخزين المؤقت حتى الآن، لذلك سينتقل مباشرة إلى خادم الجذر ليطلب من عنوان IP الانتقال إلى خادم الجذر لأن خادم الجذر يحتوي على ملف منطقة الجذر.

بعد ذلك، يعيد خادم الجذر إحالة: "لا أعرف العنوان، لكنني أعرف عنوان com." لذلك، سينتقل خادم الاسم المتكرر إلى خوادم com. وسيسأل: "ما هو عنوان IP لـ www.example.com؟" بعد ذلك، سيجيب خادم أسماء com.: "لا أعرف، لكنني أعرف عنوان IP لخادم الأسماء وns1.example.com".

لذا سيأتي خادمكم المتكرر الآن إلى خادم الأسماء ns1.example.com، ثم يقوم خادم الأسماء هذا بنشر عنوان IP أو العودة بإجابة محددة على استعلامكم. ثم يقوم خادم الأسماء المتكرر الآن بإعادة عنوان IP إلى محللكم الجذري.

يحدث هذا في ثوان. ولا يحدث في دقائق. هذا هو الحال تماما كما لو كنت تطلق تطبيقا من هاتفك أو من الكمبيوتر المحمول. في بعض الأحيان يستغرق تحميل الصفحة أو فتح التطبيق بعض الوقت. ولكن إذا كنت تحاول إعادة تحميلها مرة أخرى، فسيكون الأمر أسرع. لماذا؟ ذلك لأن المعلومات مخزنة مؤقتا بالفعل لعميلكم.

لنفكر في هذا مرة أخرى. يعمل التخزين المؤقت على تسريع عملية التحليل لأنه يعرف الآن اسم وعنوان IP لمنطقة الجذر الخاصة بكم وخوادم الأسماء الخاصة بكم. إذا حاولتم

الوصول أو إذا حاولتم طلب: "ما هو عنوان IP لـ ftp.example.com؟" منذ فترة طلبنا عنوان IP لـ www.example.com.

الآن نسأل ما هو عنوان IP لـ ftp.example.com. إذا سينتقل Safari أو المحلل الجذري إلى خادم الأسماء المتكرر مرة أخرى، لكن هذه المرة لن يعود إلى منطقة الجذر، ولكنه سيذهب مباشرة إلى خادم الأسماء لأنه يحتوي على معلومات ذاكرة التخزين المؤقت بالفعل. يجعل استخدام ذاكرة التخزين المؤقت العملية بأكملها فعالة وأسرع. هذه هي الطريقة التي تعمل بها عملية التحليل.

لدينا شريحة من صفحة واحدة هنا بشأن الامتدادات الأمنية لنظام اسم النطاق DNSSEC. إذا رغبتم في الدخول إلى مناقشة عميقة بشأن DNSSEC، فهناك بعض الجلسات المتاحة. هل لدينا جلسة متاحة لهذا الأسبوع حول DNSSEC يمكنهم حضورها؟

جون كرين: سأبحث عنها، لكن لدينا بالفعل جلسة DNSSEC قادمة. أعتقد أنها يوم الأربعاء، لكنني سأبحث عنها قبل نهاية الجلسة.

شخص غير محدد: كان هناك أيضا برنامج تعليمي بالأمس.

راتشيل رييس: حسنا، عظيم. إذن، هذه فقط أساسيات DNSSEC. وسوف أقرأها عليكم فقط. من خلال DNSSEC، يمكن توقيع بيانات DNS رقميا للمصادقة. تحتوي كل منطقة على مفتاح عام أو خاص للاقتران وتشغيل DNSSEC.

هناك عدة سجلات في DNSSEC هي DNSKEY وهي المفتاح العام لمنطقة أو RRSIG أو التوقيع الرقمي. NSEC أو NSEC3 هو المؤشر إلى الاسم التالي في منطقة، وDS هو موقع للتفويض.

مرة أخرى، إذا رغبتم في معرفة المزيد عن DNSSEC، فيمكنكم حضور إحدى جلسات DNSSEC التي لدينا هنا.

هذا ما تبدو عليه منظومة اسم النطاق. لدينا السجل الذي يحتوي على قاعدة بيانات لأسماء النطاقات والمشتركين، يليها أمين السجل الذي يعد الوكيل الأساسي بين المشترك والسجل، والمشترك هو صاحب تسجيل اسم النطاق.

هذه هي طريقة تسجيل اسم النطاق، لكننا لن نناقش العملية بأكملها. ما أحاول إخباركم به هو أن ما ناقشناه جزء من سجل أسماء النطاقات الكامل. وما ناقشناه موجود هنا تحت خوادم الأسماء الرسمية، خادم الأسماء المتكرر ومستخدم الإنترنت.

هذا كل ما لدي لجلسة اليوم إذا كان لدى أي شخص سؤال.

جون كرين: قبل أن ننتقل إلى الأسئلة، سأقوم فقط بإعطاء بيانات عن DNSSEC. يوم الأربعاء من الساعة 9:00 ص حتى الساعة 3:00 م، يوم كامل على DNSSEC. أكثر مما يحتاج أي شخص.

راتشيل رييس: حسنا.

سيرانوش فاردانيان: نعم، يمكننا الآن البدء في جزء الأسئلة والإجابات. نعم، تفضل.

نيكولاس فيوميارليلي: مرحبا. نيكولاس فيوماريلي من أوروجواي. لقد ذكرت أن DNS ليس حساسا لحالة الأحرف، لكن ماذا يحدث في حالة أسماء النطاقات المدولة؟

راتشيل رييس: مات يمكنه أن يجيب على هذا السؤال.

مات لارسون: DNS نفسه بالتأكيد ليس حساسا لحالة الأحرف. تشبه أسماء النطاقات المدولة طبقة فوق DNS. هل يمكنني أن أطلب منك يا راتشيل الرجوع إلى إحدى شرائح فضاء الأسماء في البداية. واصلي من فضلك. هذا جيد. شكرا.

إذا نظرتم إلى الشريحة، فيجب أن أقول العقدة في أعلى اليسار، وهي التي تبدأ بـ xn-- ، الطريقة التي قررنا بها عمل أسماء النطاقات المدولة كانت كما قلت لتنفيذها كطبقة في القمة.

من وجهة نظر المستخدم، إذا كان أحد التطبيقات ممكنا بواسطة اسم النطاق المدول IDN، فإن الاستخدام يتفاعل معه ويرى أسماء النطاقات بأحرف مدولة. لكن يجب أن يقوم هذا التطبيق بتحويلها إلى صيغة LDH – الحروف، الأرقام، الواصلة – التي يعرفها DNS.

لذا من منظور DNS، فهي تبدو كأنها رموز عادية، وإن كانت نوعا ما مضحكة. يمكنكم رؤية xn-- رمز يعني أن بقية هذا الرمز هو IDN مرمز. يوجد في الواقع ترميز خاص يسمى Punycode وهو نوع من التحويل لـ Unicode المصمم خصيصا لترميز أحرف Unicode للرموز في DNS.

نيكولاس فيوميارييلي: شكرا.

مات لارسون: أجل. فقط لإعطاء خلفية أكثر قليلا بشأن ذلك، عندما كنا نفعل ذلك، كان هناك بعض الأشخاص الذين قالوا: "حسنا، لماذا نحتاج هذه الطبقة فوق DNS؟ لماذا لا نضع فقط UTF-8 مباشرة في DNS؟ لنضع رموز UTF-8 في DNS."

كان هناك قلق واضح من أن نظام DNS لن يتوقع ذلك لأن هذا ليس ما تم تصميمه للقيام به. لذلك يتعين علينا ترقية البنية الأساسية لنظام أسماء النطاقات DNS بالكامل، ولا يزال يتعين علينا ترقية جميع العملاء لوضع UTF-8 في الرموز.

لذلك كان التفكير وراء الطريقة التي فعلنا بها أسماء النطاقات المدولة: "حسنا، لا يزال يتعين علينا ترقية كافة العملاء، لكن على الأقل لم يكن علينا المساس بما تبقى من البنية الأساسية لـ DNS." إذن، المسألة مدى ما تريد معالجته. هل تريدون معالجة كل شيء أم التطبيقات أم البنية الأساسية لنظام أسماء النطاقات DNS أم التطبيقات فقط؟

سيرانوش فاردانيان: حسنا. أعتقد أن لدينا سؤال هنا. رجاء.

عبدالكريم أولويد: شكرا. أريد أولا طرح سؤال متابعة. قلت أن هناك طبقة فوق DNS. في نفس الوقت من وجهة نظري يعني أنه إذا قمت بإرسال استعلام إلى خادم DNS، فأنت ترسل كل شيء إلى خادم DNS. إذن كيف لديكم الآن هذه الطبقة فوق DNS؟ هذا مجرد سؤال متابعة قبل أن أطرح سؤالي.

مات لارسون: بالتأكيد. ما أعنيه بطبقة فوق DNS هو من الناحية المفاهيمية، لكنه موجود بالفعل داخل أي تطبيق يفهم أسماء النطاقات المدولة IDN.

على سبيل المثال، في متصفح ويب حديث يفهم IDN، قد تكتب بعض الأحرف غير اللاتينية وسيحوله إلى شيء يشبه رمز xn--. قد يكون xn--.، xn-- شيء. وهي على رمز بأساس الرمز الذي يتم تدويله. لذا، فإن متصفح الويب هذا يرسل الاستعلام، يستدعي المحلل الجذري، ويقوم المحلل الجذري بإرسال الاستعلام إلى خادم الأسماء وهذا الاستعلام يحتوي على xn-- فقط في الرموز.

إذن، ما أعنيه بالطبقة فوق DNS هو أنه يتم في التطبيق، وليس في خوادم DNS والمحللين.

عبدالكريم أولويد: شكرا. الآن أنتقل إلى سؤالي. لدي سؤالان. أولهما، عندما كنت تقدم العرض، لا أعلم. ربما فاتني جزء ما عندما كنت آكل أو كان التقديم سريع قليلا. إنه عن خوادم المنطقة. قلت أنها معقدة بعض الشيء. كنت مرتبكا قليلا بشأن خوادم المنطقة. ماذا تقصد بخوادم المنطقة؟ خصوصا عندما كنت تتحدث عن خوادم المنطقة الأساسية، خوادم المنطقة الثانوية، ثم كنت تتحدث عن بعض خوادم هذه المنطقة مثل التابعة والرئيسية. هل يمكنك فقط شرح ذلك الجزء مرة أخرى؟

ثم الجزء الآخر من سؤالي هو 4.2.2.2 هل يعني أنه إذا قمت بإرسال أي استعلام، فهل هو مثل الخادم المتكرر الافتراضي لجميع الاستعلامات؟

جون كرين: إذا كنت تتحدث عن الأنواع المختلفة لخوادم الأسماء، فإننا لا نشير إليها بصفة عامة على أنها خوادم منطقة، وهناك ثلاثة أنواع من الخوادم بشكل أساسي. هناك الجذر الموجود على الكمبيوتر المحمول، على سبيل المثال، أو على الهاتف ويمكن أن يوجد في نظام التشغيل أو قد يوجد في التطبيق نفسه كما هو الحال في المتصفح. وتجيب تلك فقط عن الأسئلة.

ثم لديك الخوادم المتكررة التي عادة ما تكون إما في مزود خدمة الإنترنت أو أنها قد تكون على جهاز التوجيه المنزلي في المنزل. وتمر تلك على الأسئلة، إذا أردت. وتلك هي التي تخرج إلى الخوادم الرسمية. وهؤلاء هم الذين لديهم بالفعل الإجابات. ولهذا السبب نسميهم الخوادم الرسمية. كما أن لديهم القدرة على إعطاء الإجابة. وهذه هي بالفعل وظيفة ملفات المنطقة، الخوادم الرسمية.

على الخادم المتكرر، لديك محرك استعلام الذي ينتقل ويستعلم. والبيانات الوحيدة المخزنة بالفعل هي في ذاكرة التخزين المؤقت. لذلك لديه ذاكرة تتذكر إجاباته. وربما يكون لدى المحلل الجذري. لذلك لديك مسار من جهازك باستمرار.

الآن كان هناك تعليق آخر أعتقد أن راتشيل قدمته حول تعقيد كيفية توفير منطقة الجذر. لا أعلم إذا كنتم تشيرون إلى ذلك. وهذا شيء مختلف تماما. هذا نظام توفير كامل وليس نظام خادم أسماء. سأترك مات يتحدث عن هذا إذا أراد ذلك لأنه عمل على بعض تلك الأشياء من الجانب الآخر.

فيما يتعلق بالخادم المتكرر الذي تستخدمه، عادة ما يتم تحديده عند إعداد الكمبيوتر المحمول أو الشبكة. عند الاتصال من خلال شبكة، لنفرض هنا، نستخدم شيئا يسمى بروتوكول تكوين المضيف الديناميكي أو DHCP. فهذا ما يرسل إليك عنوان IP الذي تستخدمه، ولكنه قد يرسل إليك أيضا أسماء النطاقات، الخوادم المتكررة. يمكنك الحصول على اثنين لأولئك. يمكنك الحصول على أحدهم. يمكنك الحصول على أربعة لأولئك. يجب أن تنتقل جميع استعلاماتك إلى تلك التي تمت تهيئتها.

سيرانوش فاردانيان: هناك سؤال أو تعليق من أحد المشاركين عن بعد. حسنا، يرجى الانتهاء من هذا.

مات لارسون: على وجه التحديد سألت عن 4.2.2.2. هذا هو خادم الذي يتم تشغيله من قبل Level 3 Communications، مزود خدمة إنترنت. وهذا ما يسمى بخادم متكرر مفتوح. عادة، في أي مكان لديك مجموعة من العملاء – لذلك أي شبكة، إما مزود خدمة إنترنت لعملاء النطاق العريض أو في هذا المبنى على شبكة ICANN – أينما كان هناك مجموعة من العملاء الذين لديهم محللين جذريين (لذا أسفل اليسار) تحتاج إلى وجود خادم متكرر في الجزء العلوي.

وكما قال جون، فإن مشغل الشبكة مسؤول عن توفير الخادم المتكرر، وعندما تقوم بالاتصال بالشبكة، يحصل جهازك على عنوان IP لهذا الخادم المتكرر لتكوين نفسه.

ومع ذلك، لا يلزم استخدام هذا الخادم المتكرر. يمكنك استخدام آخرين. هناك بعض الخوادم المتكررة المفتوحة المعروفة جدا، مما يعني أنها تقبل الاستعلامات من أي شخص. يمكنك استدعاء هذه الخوادم المتكررة التابعة لجهات خارجية، الخوادم المتكررة العامة. ربما الأكثر شعبية لأنه يحتوي على عنوان سهل التذكر هو Google Public DNS الذي هو 8.8.8.8. لذلك يمكنك تكوين المحلل الجذري على هاتفك إذا أردت. ويمكنك تغيير تكوينه للانتقال إلى 8.8.8.8 بدلا مما يمنحه لك مزود خدمة الإنترنت.

وغيره من الخوادم المعروفة، كان Open DNS موجودا لفترة طويلة. كانوا من أول الأشخاص الذين قالوا دعونا نضع الخوادم المتكررة خارج شبكتك، وسنقدم هذه الخدمة. ولدى Verisign ذلك. ولدى PCH شيء يسمى Qaud9, 9.9.9.9. لذلك هناك العديد من الخوادم العامة، و4.2.2.2 هو أحدهم من المستوى 3 الذي كان موجودا لفترة طويلة.

سيرانوش فاردانيان: شكرا. هناك سؤال من مشارك عن بعد، [غير مسموع] من إفريقيا. يبدو أن إفريقيا تتطور تدريجيا وهناك حاجة إلى زيادة قدرتها. وبصرف النظر عن برنامج الزمالة الذي يملأ الفجوة في البلدان النامية، فما الذي تقوم به ICANN أو من أجل ذلك الأمر DNSSEC لزيادة قدرتها؟ وماذا يتعين علينا القيام به في أفريقيا من حيث السياسة؟"

جون كرين: بناء القدرات، نتحدث عن DNS، لذلك سأتحدث عن القدرة حول DNS. ونعمل بشكل عام مع المجتمع. ومجموعتي على وجه التحديد، نقوم بالكثير من بناء القدرات، الكثير من التدريب. ولكن في إفريقيا بالتحديد، من المرجح أن ترى منظمات مثل المركز الأفريقي لمعلومات الشبكة AfriNIC أو إذا ذهبت إلى المجموعة الأفريقية لمشغلي الشبكة AFNOG أو منظمة نطاق المستوى الأعلى في أفريقيا AfTLD (كما هو الحال في نطاق المستوى الأعلى (AF، فمن المرجح أن تراهم في الواقع يوفرون هذه الأنواع من التدريبات. ونحن نعمل معهم وندعمهم.

هناك منظمة أخرى تسمى "مركز موارد بدء التشغيل الشبكي" وهي أيضا نشطة بشكل كبير في إفريقيا وهي تعلم DNS وغيرها من قضايا البنية الأساسية.

بشأن DNSSEC على وجه التحديد، قمنا بإجراء تدريبات متعددة في المنطقة الأفريقية مع كل من AFNOG وجميع AF بشكل أساسي، والمنظمات الأفريقية الموجودة هناك. لست متأكدا من حيث التدريب المقرر القادم، ولكن أعتقد أن هناك تدريبين لـ DNSSEC عمليين مقرران لأفريقيا في أيار (مايو)/حزيران (يونيو).

لذلك فنحن نشطون بالفعل هناك، لكننا نعتمد على الخبرة المحلية. إذا كنت تحاول تدريب العالم، وهو مكان كبير، فهذه ليست مهمة ICANN. وICANN بالطبع مؤسسة صغيرة. يعتقد بعض الأشخاص أنها كبيرة للغاية، لكنها لا تزال مؤسسة صغيرة. لذلك نتواصل حقا مع المجتمعات التقنية المحلية ونساعدهم إما عن طريق تزويدهم بالمواد أو العمل على موادهم معهم. وذلك أفضل بكثير من أمور أخرى عديدة.

كما أننا نعمل أيضا على بعض منصات التعلم عبر الإنترنت التي ستمكننا من توفير قدرات التعلم الإلكتروني، كما ستمكننا من ترجمتها بسهولة أكبر إلى اللغات المختلفة.

وعلى الرغم من أننا لسنا جامعة عالمية هنا، فنحن بالفعل نقضي الكثير من الوقت في محاولة تثقيف الأشخاص. أحد الأشياء إذا رأيتم في منصبي، لدي مصطلحات "الأمن والاستقرار والمرونة"، التي تقلق بشأن المنظومة. وأحد الأشياء التي تقوم بها لتحسين ذلك هو التأكد من أن الأشخاص لديهم وصول أفضل إلى المعرفة والقدرة على بناء أنظمة أفضل.

سيرانوش فاردانيان: شكرا. ليندون؟

ليندون تيليسفورد: مرحبا. معكم ليندون من جرينادا. لست متأكدا من أنه سؤال بشأن DNS نفسه أو إذا كان بشأن النظام بأكمله. لست متأكدا إذا كان هذا ممكنا، لكنني سأطرحه على أي حال.

في العرض التقديمي، تم إبراز Anycast وأمثال مختلفة لخوادم الجذر. سؤالي هو داخل خادم العميل ومخطط Anycast، ما هي الآليات الموجودة السارية للحماية من نوع هجوم الحجب المنتشر للخدمة DDoS الذي يؤثر على مفهوم القرب بحيث يصبح العملاء مرتبكين بشأن زيارة أي من الخوادم طلبا لاستجابة؟

جون كرين: أحاول التفكير في رد للسؤال. هل تريد الحديث هناك؟

مات لارسون: حسنا، أنا لست متأكدا تماما مما تقصده بأن يصبح العملاء مرتبكين بشأن أي خادم. وسأستخدم مفهوم الطبقة مرة أخرى في جوابي. Anycast حقا طبقة تحت DNS. ولدينا DNS، ثم Anycast جزء من نظام توجيه الإنترنت.

لنأخذ نظام خادم الجذر حيث أعتقد الآن في هذه النقطة أن كل واحد من عناوين IP هو Anycast. لنفترض أن لدينا خادم أسماء متكرر يعمل على إرسال استعلام إلى ملف الجذر L. من طبقة DNS، تقول فقط: "أقوم بإرسال استعلام إلى عنوان IP هذا."

ولكن عندما ينخفض ذلك إلى طبقة التوجيه، عندما تقوم الشبكة نفسها بنقل تلك الحزمة فعليا، سترى أجهزة التوجيه على الشبكة أن هناك بالفعل العديد من الأمثال، أماكن متعددة على الشبكة حيث يتوفر عنوان IP هذا. ومن حيث كيف يمكننا أن نقول أنه مع BGP، بروتوكول البوابة والتوجيه، يمكننا القول أن شبكات مختلفة تعلن عن التوجيه إلى تلك الشبكة بالتحديد. لذلك لديك شبكات متعددة عبر الإنترنت تقول: "يمكنني الوصول إلى ملف الجذر L." "يمكنني الوصول إلى ملف الجذر L." "يمكنني الوصول إلى ملف الجذر L."

تقوم أجهزة التوجيه الفردية حينئذ التي تستخدم المعلومات من BGP باتخاذ قرارهم. "من وجهة نظري، ما هي أفضل طريقة للوصول إلى ملف الجذر L؟" تقوم جميع أجهزة التوجيه بهذا. ما يعنيه ذلك هو عندما تقول: "أريد إرسال حزمة إلى ملف الجذر L،" استنادا إلى مكان وجودك في الشبكة، تنتقل إلى المثيل "الأقرب". إنها ليست مجرد مسافة

جغرافية. إنها ليست مجرد زمن وصول. هناك جميع أنواع العوامل التي تؤثر على سياسة التوجيه BGP.

لست متأكدا كيف نعالج الارتباك في ذلك. ما يمكن أن يحدث هو إذا كان هناك هجوم على مثيل واحد وأصبح مثقلا، فالطريقة التي عادة ما يستخدمها المشغلون لتكوين خوادم الأسماء في تكوين Anycast هي عندما يكون خادم الاسم نشطا، يقول للشبكة: "أنا هنا. يمكنك الإعلان عن طريقي، وأنني موجود." ولكن إذا أصبح مزدحما لدرجة الانهيار – اعتمادا على الفشل – إذا أخفق، فإنه فسيقول للشبكة: "أوه، لست على قيد الحياة بعد الآن. لا يمكنني قبول استعلامات DNS." ثم تعيد الشبكة حسابها، وقد تقوم بإرسال حركة البيانات إلى مكان آخر.

ليندون تيليسفورد: من جانب جهاز التوجيه، القرارات حول مكان التوجيه يصنعه بناء على معلومات BGP المستوفاة مسبقا؟

مات لارسون: لن أقول مستوفاة مسبقا. إنها تتغير طوال الوقت. كل شبكة، وكل رقم نظام ذاتي نستدعيه، عبارة عن شبكة من منظور BGP، والنظام الذاتي هو شبكة تحتوي على مجموعة من الطرق، للشبكات التي تعلن عنها، والتي تقول: "لدي عناوين IP هذه."

لذا فإن كل جهاز توجيه يعمل على BGP يقول باستمرار: "هذه هي الشبكات التي أعرفها"، ويستمع جهاز توجيه آخر ويقرر على أساس الوقت الحقيقي مكان كل شيء. هذه نسخة مبسطة للغاية لطريقة عملها، لكن BGP يحدث في الوقت الحقيقي باستمرار.

جون كرين: للإضافة إلى ذلك، هذا ليس شيئا يسببه بالضرورة Anycast. كان هذا قبل Anycast لأنك ترى مسارات متعددة إلى عقدة. إذا كان هناك شخص ما يعلن عن موقع ويب، إذا كنت بعيدا جدا، فمن المحتمل فقط أن أرى طريقة واحدة لإرساله، لكن إذا كنت قريبا إلى

حد كبير، فقد أرى مسارات متعددة لذلك. وفعلوا الشيء نفسه في الماضي. لذا فهي حيلة للتوجيه تم التعرف عليها، ثم تم استخدامها لإضافة المزيد من الخوادم. ولم يكن هناك أي تغيير في التكنولوجيا لـ Anycast. كان مجرد حيلة للتوجيه.

ليندون تيليسفورد: أعتقد أنني كنت أتساءل فقط إذا كان هناك طريقة لخداع حيلة التوجيه.

جون كرين: لا أعتقد أن هذا جزء من الحيلة. للتوجيه الآن مشكلات أمنية خاصة به، ولكنها مرتبطة بالتوجيه وليس بـ Anycast. للتوجيه بعض مشكلات الأمن، أو ربما يكون مشكلات عدم الأمن طريقة أفضل لقول ذلك. لكنها لا تخص Anycast.

سيرانوش فاردانيان: شكرا. هناك، تفضل.

شابنيل أنال سامي: مرحبا. معكم شابنيل من فيجي. سؤالي هو إذا أرادت دولة في استضافة خادم جذر، فما هي أفضل الممارسات عندما تقرر أي خادم للاستضافة؟ مثل واحد من الـ 13، A، L، F، وما إلى ذلك؟ أم أنها تستند إلى منطقة أو يمكن لأي شخص الاستضافة؟

جون كرين: إنها مبنية على من تقرر الذهاب للتحدث معه. أول شيء سأقوله هو أنه ليس دولة. إنها شبكة أو مشغل شبكة يرغب في استضافة مثيل. يمكنهم الذهاب إلى root-servers.org ومشاهدة قائمة للمشغلين. ونحن أحد المشغلين. أعتقد أننا في الواقع لدينا واحد في فيجي، وأعتقد أن اثنين آخرين يفعلان ذلك.

يمكنك فقط الوصول إلى أولئك المشغلين والسؤال عن شروطهم للقيام بذلك. وتختلف اختلافا طفيفا حسب كل مشغل، ولكنه ليس صعبا. هناك 990 مثيل أو مواقع اليوم. لذا

إضافة المزيد، إنها مجرد مسألة تواصل. انتقل إلى موقع الويب root-servers.org وهناك روابط في الواقع إلى كل من المشغلين ويمكنك رؤية وثائقهم حول كيفية الحصول عليهم. وسعيد للتحدث دون اتصال بالإنترنت ومساعدتك من خلال ذلك.

شابنيل أنال سامي: كنت قلقا بشأن أي واحد أستضيفه، مثل L وF. حتى مجرد الذهاب؟ لأنني رأيت بورتوريكو تستضيف L، لذا كانت فيجي تستضيف L، لذلك كنت مرتبكا حول الأمور الإقليمية من هذا القبيل. شكرا.

جون كرين: نعم، ليست مشكلة إقليمية. غالبا ما تكون مشكلة متعلقة بالعلاقة. السبب في أن فيجي لديها L، والتي كانت الثانية التي تذهب إليه، لأن لدينا موظف في فيجي، سيف ڤوسيا. لذا، فإن الكثير من الوقت يدور حول من لديك علاقات معه أو تقوم ببناء علاقات معه من خلال الانتقال إلى الموقع الإلكتروني وقولك: "أوه، هذا الشخص يبدو جيدا."

وأيضا، قد تختلف المعايير، ومعظمها المعايير المالية لكيفية القيام بذلك، من واحد إلى آخر. نحن، على سبيل المثال، في ICANN لدينا حل حيث تدفع للخادم وتقوم بوضعه على الإنترنت ثم نقوم بكل العمل. الآخرون، تعطيهم المال ثم يرسلون لك الخادم. إنه نموذج مختلف قليلا، لذا تحتاج إلى معرفة ما يناسبك.

جميع خوادم الجذر من منظور DNS متساوية. وجميعهم يعطونك نفس الإجابات. وجميعهم يعملون من منظور الاستعلام بالضبط نفس الشيء. وهو حقا علاقات تجارية وربما من تعرفه.

شابنيل أنال سامي: حسنا، شكرا.

سيرانوش فاردانيان: هل من أسئلة أخرى؟ نعم، تفضل.

شخص غير محدد: لدي سؤالان. كيف يمكن ضمان [الازدواجية] لمناطق سجلات الدول أن تكون صحيحة وليس [سحب] غير صحيحة [غير مسموع] مثل ما حدث قبل سنوات؟ والثاني هو نسخ خوادم الجذر المستضافة في الدول على سبيل المثال ليست سوى جزء من [غير مسموع] في جميع أنحاء العالم، فقط جزء من [غير مسموع] في هذا الجذر. على سبيل المثال، يحتوي الجذر L فقط على جزء من كل [غير مسموع] أو لديه كل السجلات هناك؟

مات لارسون: لا، جميع خوادم الجذر لديها نفس المعلومات. هناك منطقة جذر واحدة فقط بمعلوماتها، ومن ثم كل خادم جذر لديه نفس المعلومات.

هل يمكنك تكرار السؤال الأول؟

شخص غير محدد: على سبيل المثال، عندما سجل [متعذر تمييزه].

سيرانوش فاردانيان: مجرد سؤال، هناك ترجمة. يمكنك طرحه بلغتك.

شخص غير محدد: حسنا.

مات لارسون: ممتاز جدا. ممتاز جدا.

سيرانوش فاردانيان: لذلك انتهز هذه الفرصة.

شخص غير محدد: حسنا. لحظة من فضلكم.

سيرانوش فاردانيان: أجل. مجرد ثانية حتى يلتقط الأشخاص سماعات الرأس الخاصة بهم.

سيدة غير معروفة: تحقق. هل يمكنك الحصول على الترجمة باللغة الإنجليزية؟ هل تحصل على اللغة الإنجليزية؟ حسنا، عظيم. شكرا.

شخص غير محدد: [من خلال مترجم] عندما يكون للسجلات في كل دولة سجل في المنطقة مثل نطاق المستوى الأعلى لرمز البلد ccTLD، عندما يكون للسجل سجل في المنطقة ويتم نشره وتوزيعه في جميع أنحاء مناطق DNS، كيف يمكنك التأكد من أن تلك المنشورات صحيحة، وليس بها أخطاء في نشر تلك المناطق أو في التوزيع؟ لأنني أفهم أن هذا حدث بالفعل في الماضي.

جون كرين: كانت هناك بعض الأسئلة هناك. سوف أتأكد من المصطلحات والتقنية. وبغض النظر عن ccTLD أو gTLD، عند نشر المنطقة، فإن هذه المنطقة تتكون من البيانات التي تخرج من قواعد البيانات الخاصة بها، وتكون مسؤولة عن ضمان صحة تلك البيانات. بمجرد نشرها بالفعل، إذا قمت بتوقيع DNSSEC على المنطقة وكنت تصادق على استعلامات DNS، يمكنك التأكد من أنك حصلت على ما نشروه.

الآن هذا هو نهاية الأمر. هذا هو النشر وجانب DNS. كل جانب آخر هو حقا حول أمن الشبكة وأمن قاعدة البيانات وسلامة البيانات الخاصة بك. كانت هناك مشاكل في الماضي حيث اخترق الأشخاص أنظمة ccTLD، وهو ما أعتقد أنك تشير إليه.

شخص غير محدد: نعم.

جون كرين: لا يوجد شيء اسمه شبكة آمنة حقا. لذلك أعتقد أن الأشخاص سيكونون دائما عرضة للتأثر بهذا عند مستوى ما. ما نقوم به بصفتنا ICANN ومع أصدقائنا في تلك السجلات – تحديدا مجموعتي، مجموعة الأمن – عندما كان لديهم مشاكل سوف يتواصلون معنا وسوف نساعدهم على التعافي. وسوف نساعدهم كثيرا أيضا في العثور على خبراء لمساعدتهم في إعادة تصميم أنظمتهم.

كان لدينا حالتين، وأعتقد أنني أعرف إلى ما تشير إليه، لكنني لن أذكرهما. كان لدينا بضع حالات حيث كان لديهم هجمات حقن SQL. إنه نوع محدد من الهجوم ضد نظامهم.

سمح ذلك للمجرم، الشخص السيئ، أن يغير السجلات لمؤسسة كبيرة وتوجيه عنوان خادم الويب في مكان آخر. لذا بدا الأمر – لذا أنا أتحدث عن النقطة الصحيحة التي أعتقد أنني أتحدث عنها – ما يبدو بعد ذلك للعالم الخارجي هو أنه تم اختراق خادم الويب. لكن في الحقيقة ليس الأمر كذلك. كان الأمر مع أنظمة التسجيل.

لذا في تلك الحالة، قضينا الكثير من الوقت في العمل مع مشغل السجل، ولديهم الآن نظام جديد تماما لديه الكثير من التدقيق، وما إلى ذلك، ضده. ولقد تعلموا من أخطائهم وتقدموا إلى الأمام، وهذا ما تفعله في حالة التعرض للخطر. تفهم كيفية اختراقك، وتصلح أنظمتك، وتتعلم من ذلك، وتحسن العمليات الخاصة بك.

لكن هذا لا يعني أن بعض ccTLD الأخرى في مكان ما أو حتى gTLD لن يتم اختراقها أبدا لأن هذا ليس الواقع. نرى شركات كبرى بملايين الدولارات تتعرض أيضا للهجوم.

شخص غير محدد: شكرا جزيلا.

سيرانوش فاردانيان: نعم، تفضل.

جيسون هايندز: جون، مجرد متابعة لذلك.

سيرانوش فاردانيان: اسمك من فضلك؟

جيسون هايندز: عذرا. نعم. معكم جيسون هايندز من بربادوس. جون، سؤال المتابعة، هل هناك أي منشورات لمساعدة مشغلي السجلات على منع هذه التنازلات الشائعة قبل حدوثها؟

جون كرين: بالعمل مع بعض الشركاء الذين ذكرتهم سابقا حول بناء القدرات، قمنا بآلاف الساعات من التدريب مع المشغلين حول أشياء مثل، كيف تقوم بتأمين شبكة؟ كيف تراقب شبكة؟ وبالطبع، فإن المجتمع الذي تراه هنا من المشغلين لديه أيضا مجموعات خاصة به ويشارك الكثير من أفضل الممارسات والمساعدة، بما في ذلك المساعدة الهندسية.

لذا في جامايكا كجزء من منطقة أمريكا اللاتينية والكاريبي، هناك منظمة تسمى جمعية نطاق المستوى الأعلى لأمريكا اللاتينية ومنطقة الكاريبي LACTLD والتي تشمل جميع السجلات – ليس كلها ولكن معظم السجلات – من المنطقة. ويعقدون اجتماعات منتظمة، ولديهم جلسات تقنية. وعندما يكون لدى أحدهم مشاكل، يأتي الآخرون لمساعدتهم.

لذلك فهي ليست مشكلة يواجهونها بأنفسهم. إنها مشكلة تؤثر على المجتمع بأكمله. من خلال التدريب والمساعدة المتبادلة، هناك الكثير الذي يحدث هناك.

سيرانوش فاردانيان: هل هناك أسئلة؟ ليس هناك مزيد من الأسئلة.

أود أن أشجعكم على المشاركة بالتأكيد يوم الأربعاء في ورشة عمل DNSSEC التي ستكون من الساعة 9:00 ص حتى الظهر.

شخص غير محدد: حتى الساعة 03:00 ص.

سيرانوش فاردانيان: حتى الساعة 03:00 ص.

شخص غير محدد: تستغرق وقتا طويلا.

سيرانوش فاردانيان: حسنا، في الوسط، لدينا جلسة زمالة وقت الغداء. ولكن على أي حال، يرجى الانضمام إلى ورشة العمل. وهو أمر مهم للغاية.

هل هناك أي كلمات أخيرة من مقدمينا؟

راتشيل رييس: أشكر الجميع على وجودهم معنا. وأقدر وجودهم. شكرا جون ومات، لمساعدتي في الإجابة عن الأسئلة.

سيرانوش فاردانيان: أود أن أشكر مترجمينا الفوريين وفريقنا التقني. وتقديري الكبير لمات، جون، راتشيل على وقتكم. وأعلم أنكم مشغولون للغاية خلال هذا الاجتماع، ولكن أشكركم على حضوركم وتقديم هذا العرض التقديمي للزملاء. تصفيق لمقدمينا.

وبذلك، نختتم اجتماعنا. شكرا.

[نهاية النص المدون]