سان خوان – مستجدات استبدال مفتاح توقيع شفرة الدخول الأساسية
الأربعاء، الموافق 14 آذار (مارس) 2018 - من الساعة 04:15 م إلى الساعة 04:45 م بتوقيت الأطلنطي الموحد
اجتماع ICANN61 | سان خوان، بورتوريكو

متحدث غير معروف: مرحبا بالجميع، سنبدأ جلسة بموضوع استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر خلال لحظات. هلا تفضلتم بعرض الشرائح على الشاشة، من فضلكم.

سوف نبدأ في غضون 30 ثانية رجاء.

مرحبا بالجميع، مرحبا بكم في جلسة بموضوع استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر. نأمل أن يكون هناك أشخاص في هذه القاعة لم يروني وأنا أقدم هذا المحتوى في هذا الاجتماع لمؤسسة ICANN. ها نحن. اسمحوا لي أن أبدأ بتذكير سريع حول كيفية وصولنا إلى وضعنا الحالي، كما أعتقد أن الجميع يعرف، إذا كان لديكم ما يكفي من الاهتمام بالتواجد معنا هنا، فقد كان من المقرر أن يتم استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر في 11 تشرين الأول (أكتوبر) 2017، ولكننا قررنا تأجيل ذلك. قاموا [غير مسموع] بتحليل بيانات إبلاغ مرساة الثقة CAD 145، ووجدوا أن حوالي 7-8% من المحللين الذين يقومون بالإبلاغ، وهو عدد قليل نسبيا في ذلك الوقت، لديهم ما نسميه KSK 2010 أو مفتاح توقيع شفرة الدخول الأساسية KSK الحالي والذين لم يكن لديهم مفتاح توقيع شفرة الدخول الأساسية الجديد لمنطقة الجذر. شيء ما لم يكن صحيحا بخصوص تلك النسبة 7-8%. وقد كرر مكتب ICANN لفريق أبحاث المدير التنفيذي للتكنولوجيا CTO هذا التحليل مع انتقال البيانات من خوادم الجذر المختلفة وحصلنا على نفس النتيجة بشكل أساسي. وحسب ما تبحث عنه بالتحديد، فقد تقل النسبة أو تزيد. ولا تزال النسبة أعلى من المقبول، والأهم من ذلك، لم نفهم السبب الذي جعل هؤلاء المحللين يقدمون إبلاغا بالمفتاح القديم. ولقد قررنا إيقاف استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر ومحاولة معرفة سبب استخدام هؤلاء المحللين للمفتاح القديم. لقد حصلنا على قائمة تضم 500 محلل في شهر أيلول (سبتمبر) 2017 قد قدموا إبلاغا بالمفتاح القديم فقط، KSK 2010 فقط، وحاولنا تعقبهم ووجدنا أن تعقب المشغلين استنادا إلى عنوان IP فقط أمر صعب، وهذا دليل حي على ذلك. ويمكننا

ملاحظة: ما يلي عبارة عن تفريغ لملف صوتي إلى وثيقة نصية/وورد. ورغم الالتزام بمعيار الدقة عند التفريغ إلى حد كبير، إلا أن النص يمكن أن يكون غير كامل ودقيق بسبب ضعف الصوت والتصحيحات النحوية. ولا ينشر هذا الملف رسمي كسجل ويؤخذ ألا ينبغي أنه الأصلي، إلا الصوت لملف مساعدة كوسيلة.

التواصل مع 20% فقط، والتي ستمثل حوالي 100 عنوان ومعظمهم نطاقات IP معروفة باستضافة أشياء عابرة مثل الحواسيب أو الحاويات الافتراضية.

هناك أيضا مشكلة في طلب تقديم التعقيبات RFC 8145 تتمثل في أن الإشارة نفسها يتم إرسالها كطلب بحث لنظام اسم النطاق DNS، مما يعني أنها تقوم ببعض الأمور مثل إعادة توجيهها من محلل إلى آخر. نحن نعلم أن إعادة التوجيه مستمرة والتي تتسبب في حجب الإشارة، ويمكنك أن تفكر في أن محللا معينا لديه KSK 2010 فقط، ومن الممكن أن يبقى المحلل يعمل جيدا، ومن الممكن أن يكون هناك محلل خلفه يعيد التوجيه إليه، والذي أبلغ عن KSK 2010 فقط.

ولم يكن هناك دليل واحد دامغ، والذي كان من شأنه أن يكون مثاليا، لوجود سبب أو اثنين من الأسباب الجذرية التي من الممكن أن تجعلنا نتواصل مع الموردين لإصلاح الخلل بها، حيث كان من الممكن ان نقوم بتعديل رسالتنا، لكن لم يكن الأمر كذلك. لذلك، مع عدم وجود مسار واضح تم الكشف عنه من خلال ذلك البحث، قررت منظمة ICANN أن تطلب من المجتمع مدخلاته.

نحن الآن في أواخر كانون الأول (ديسمبر) 2017. قلنا أننا سنقبل المدخلات والمناقشة حول الاستبدال المفاجئ لمفتاح توقيع شفرة الدخول الأساسية في قائمة منظمة ICANN، وهي قائمة مخصصة لمستجدات ومناقشات هذا المشروع. أود أن أقترح الاشتراك إذا لم تكن على هذه القائمة. والحجم متدن جدا في هذه المرحلة، ولكنه [غير مسموع] للمشروع. وكانت نتيجة المناقشة وجود اتفاق عام على أنه لم يكن هناك قياس جيد هنا. وقدم فريق التصميم الذي أنشأته ICANN منذ أكثر من عامين تقريره حول كيفية استبدال العكسي لمفتاح توقيع شفرة الدخول الأساسية للعودة، وقدموا توصياتهم. واقترح أن يكون القياس الجيد هو عدد المستخدمين المتأثرين واقترحوا أن نصف نسبة 1% من المستخدمين المتأثرين سيكونون علامة بعد استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر مفادها أن هناك مشاكل كبيرة بما يكفي لإلغاء الاستبدال. إذا كان المقياس هو عدد المستخدمين، فهذا مقياس معقول للغاية، ولكن هذا أيضا إجراء صعب جدا وليس ما تخبرنا به بيانات طلب تقديم التعقيبات RFC 8145. كان هناك أمل بين الأشخاص الذين انخرطوا في ذلك بتحسن القياسات في المستقبل، وكانوا يتطلعون إلى شيء يسمى

الآن الحراسة Sentinel، وهو مسودة بأن كل من وارين كومار من شركة Google و[غير مسموع] يعملان على السماح بقياس قاعدة المستخدمين، لكننا لم نصل إلى ذلك الحد حتى الآن. كان هناك توافق في الآراء بين هذه المجموعة على أنه ينبغي لمؤسسة ICANN أن تقوم بنقل المفتاح في الوقت المناسب وأن تستمر في القيام بالتواصل الذي كنا نقوم به.

واستنادا إلى هذه التعليقات، قمنا بنشر مسودة الخطة في 1 شباط (فبراير)، وأريد التأكيد على أنها مسودة الخطة لاستبدال مفتاح توقيع شفرة الدخول الأساسية. تمثلت مكونات تلك الخطة في أننا سنؤجل أولا الاستبدال لمدة عام واحد، وسنقوم به بتاريخ 11 تشرين الأول (أكتوبر) 2018، وكنا نأمل أن تسفر المناقشة حول هذه القائمة عن معايير لقياسها، ولم يكن لدينا أي شخص يقترح أية معايير خاصة. وسنواصل أيضا التواصل، وأشياء كهذه الاجتماعات، وسنعلن عن استبدال مفتاح توقيع شفرة الدخول الأساسية وسننشر المزيد من الملاحظات حول بيانات مرساة الثقة، ولا سيما بيانات طلب تقديم التعقيبات RFC 8145، وعلى الرغم من أننا نستمر في ذلك، تقل ثقتي كل يوم في ما تخبرنا به هذه البيانات. إذا كان الأمر يخبرنا بأي شيء مفيد أو أنه مجرد إشارة تنذر بالخطر وليست ذات صلة كبيرة بالمشروع.

ومن النقاط المهمة هنا أن لدينا فترة تعليق علنية مفتوحة، وهذه الخطة ليست سوى مسودة وتخضع لمدخلات المجتمع. ونريد حقا أن نسمع من المجتمع وأن نحصل على ردود الفعل على الاقتراح. وتنتهي فترة التعليق العام هذه بتاريخ 2 نيسان (أبريل) وهناك عنوان URL للصفحة التي تشرحه في الجزء السفلي من الشريحة. إذا انتهى بنا المطاف إلى الاستمرار في الخطة، والجدول الزمني، وما عليه الخطة الآن، ومشروع الخطة، فسيكون شيئا من هذا القبيل. وتنتهي فترة التعليق في 2 نيسان (أبريل). وفي منتصف نيسان (أبريل)، يجب نشر تقرير الموظفين، تماما مثل أي تعليق عام لمؤسسة ICANN. وسنراجع الخطة أيضا حسب الضرورة وننشرها. إذا كنت معتادا على وتيرة اجتماعات مجلس إدارة ICANN، فإن مجلس إدارة ICANN يجتمع 6 مرات في السنة، ويجتمع في كل اجتماع من اجتماعات ICANN، وهذا 3 مرات. ثم في ما بين كل اجتماعي ICANN، يكون لديه ما يسمى بورشة عمل المجلس. سيكون اجتماع مجلس إدارة

ICANN القادم في منتصف شهر آيار (مايو) في ورشة عمل المجلس وعندها وسوف نطلب من مجلس الإدارة إصدار قرار يسأل ASAC وكذلك SAC التابع لنا، فأنا لم أقم بتحديث الشرائح، للمراجعة والتعليق على الخطة بحلول الأول من تشرين الأول (أكتوبر). سيكون لدينا على الأرجح جلسة أخرى في بنما للتحدث عن حالة استبدال مفتاح توقيع شفرة الدخول الأساسية. وبحلول الأول من تشرين الأول (أكتوبر)، نأمل في تلقي تعقيبات كل من ASAC وSAC خاصتنا وسنقوم بإجراء أي تنقيحات على الخطة. وإذا لم تطلب تلك المراجعات تاريخا مختلفا عن 11 تشرين الأول (أكتوبر)، فعندئذ سنقوم بنشر هذه الخطة النهائية بحلول منتصف آب (أغسطس) وسنطلب من مجلس الإدارة، في ورشة عمل مجلس الإدارة في أيلول (سبتمبر)، قرارا يوجه منظمة ICANN إلى استبدال مفتاح توقيع شفرة الدخول الأساسية بتاريخ 11 تشرين الأول (أكتوبر).

هذا ما توصلنا إليه، وهذا ما سنفعله. مرة أخرى، لا يمكنني التأكيد بما يكفي على مدى رغبتنا في الحصول على تعليقات المجتمع، ونود أن يشارك الناس بقوة في التعليق العام. وأود إرسال بقية العرض التقديمي الذي يتحدث عن الإشارة التي نحصل عليها، والبيانات التي نحصل عليها عبر تقارير مرساة الثقة في طلب تقديم التعليقات RFC 8145.

عند هذه المرحلة، يتوفر لمكتب المدير التنفيذي للتكنولوجيا في ICANN إمكانية الوصول إلى بيانات طلب تقديم التعقيبات RFC 8145، في الواقع هذه الشريحة غير محدثة حاليا استنادا إلى آخر التطورات من 12 خادم جذر، فقد أضفنا H إلى قائمة الخوادم التي تقدم لنا البيانات. وقد استخدم التحليل الأولي في أواخر 2017 البيانات [غير مسموع] من B وD وF، ولكن منذ ذلك الحين، نستخدم، [غير مسموع] مكونا إضافيا لنقطة ارتكاز نظام اسم النطاق DNS. يقوم المشغلون الأساسيون بتشغيل نقطة ارتكاز DNS التي تحلل انتقال البيانات في الوقت الفعلي وكل 60 ثانية يقوم هذا المكون الإضافي بتكوين دفعات لإبلاغ الإحصائيات التي تمت مشاهدتها بالإضافة إلى تقارير مرساة الثقة التي تمت مشاهدتها. يرسلها على شكل استعلامات نظام اسم النطاق DNS وهي ذكية للغاية، إلى منطقة تعمل فيها ICANN [غير مسموع]. يمكنك الاطلاع على أمثلة لما تبدو عليه هذه التقارير، فهناك طابع زمني، وهناك مصدر IP محدد بفواصل بدلا من النقاط. يتم تسجيل مراسي الثقة في أرقام سداسية عشرية من أربعة أرقام، حيث

A5C4 يمثل KSK 2010، وF664 يمثل KSK 2017. سترى معرف مذكرة ومعرف خادم الجذر. ويمكننا تجميع هذا الرسم البياني استنادا إلى كل ذلك. ويمكنك أن ترى بمرور الوقت، كيفية حصولنا على المزيد والمزيد من التقارير من الخوادم الإضافية. دعوني أشرح هذا الرسم البياني لأنه قد لا يكون واضحا تماما للوهلة الأولى. الخطوط الثلاثة تظهر أمرين مختلفين. تقوم الخطوط الحمراء والخضراء برسم عدد من عناوين IP والتي توضح بيانات 8145، ويمكنك قراءة ذلك على المحور الأيسر، وهو عدد المصادر. ويمكنك أن ترى أنه بمرور الوقت، عند هذه النقطة، انظر إلى الخط الأخضر، وهو العدد الإجمالي للمصادر التي تشير إلى بيانات مرساة الثقة. وتعتبر هذه مصادر فريدة لليوم. في هذه المرحلة، يقوم حوالي 50000 عنوان IP فريد من نوعه بإبلاغنا ببيانات مرساة الثقة يوميا. والخط الأحمر هو الرقم الذي يبلغنا أن بحوزتهم المفتاح القديم فقط. إذا قسمت الخط الأحمر على الخط الأخضر فستحصل على نسبة مئوية وتلك النسبة يرسمها الخط الأسود وبذلك المقياس تحتاج إلى قراءة المحور Y الأيمن، ويمكنك أن ترى أن عند هذه النقطة يقول حوالي 20% من المحللين بأن لديهم المفتاح القديم فقط. لاحظ أن هناك ارتفاعا كبيرا في شهر كانون الثاني (يناير)، حيث حصلنا فجأة على عدد أكبر من الأشخاص الذين تم الإبلاغ عنهم، فساءت النسبة المئوية. نحن متأكدون إلى حد ما من أن ذلك كان نتيجة للترقية إلى 168 دون تقييد وقد تم إصدار القرار في منتصف شهر كانون الثاني (يناير) لذا فإن التوقيت يتناسب تماما وكان سبب ذلك الإصدار التعامل مع ثغرة أمنية، لذا كانت فرضيتنا بسبب أن هؤلاء الأشخاص كانوا على صلة بالأمن وتم تحفيزهم بترقيتهم دون تقييد. ومع ذلك، لا يوجد أي هبوط في تقارير KSK 2010 بعد 30 يوما.

وإذا قام شخص ما بترقية دون تقييد ولم يقم بتشغيل أداة المرساة غير المربوطة، دعني أقول هذا بطريقة أخرى، إذا قام شخص ما بترقية غير مقيدة وقام بتشغيل أداة المرساة غير المربوطة، فسيقومون على الفور بتحديث مخزن مرساة الثقة بالبيانات الصحيحة، وسيكون لديهم KSK 2010 و 2017. من الشائع ترقية عضو موجود بالفعل مع عدم تشغيل مرساة غير مقيدة، مما يعني أن لديك إصدارا غير مقيد ما زال يتم تكوينه باستخدام المفتاح القديم، ولكن إذا كان يشغل طلب تقديم التعقيبات RFC 5011 بشكل صحيح بعد 30 يوما، فيجب تشغيل هذه العملية وإدراك أن عليها إعداد KSK 2017 كذلك.

لماذا لم يحدث ذلك؟ إحدى الافتراضات لذلك هي أنه إذا كانت هذه الأجهزة أو الحاويات افتراضية عابرة، فيمكنك تخيل حيازة واحدة من القادمين للمفتاح القديم، والإبلاغ عن المفتاح القديم عبر RFC 8145، وعندما أتحدث عن المفتاح القديم، يجب أن أقول KSK 2010. إن تقارير KSK 2010 تعمل لبضع ساعات، أو بضعة أيام، ويتم إغلاقها. فهي ليس لديها الوقت لإكمال طلب RFC 5011 [غير مسموع] في المرة القادمة التي يبدأ فيها مرة أخرى، يبدأ من جديد في كل مرة ويبقى لديه KSK 2010 فقط، فهو يبلغ عن KSK 2010 فقط من خلال 8145 وتتكرر هذه العملية. نحن بحاجة إلى إجراء مزيد من التحليل في مرحلة ما، فأنت تحتاج إلى التوقف عن العمل على شرائحك والانتقال إلى بورتوريكو لتقديمها، حيث نتواجد الآن، وأحد الأمور التي نحتاج إلى مواصلة القيام بها هو النظر في عناوين IP الخاصة، كم مرة تحدث، وعدد التقارير. نحن نعلم أن الإلزام وعدم التقيد يجعل هذه التقارير 8145 على وتيرة منتظمة إلى حد ما. وإذا رأينا أن عناوين IP لا تقوم بهذا الدور، فإن أحد الافتراضات المعقولة هو أنها [غير مسموعة] ترتفع وتنخفض. هذا ليس السبب الوحيد، ولكن هذا هو السبب في أننا نجري أبحاثا لمحاولة معرفة ذلك.

فيما يلي رسوم بيانية لخوادم جذر فردية، هذه الرسوم البيانية هي نفسها، حيث أن هذا الرسم البياني لجميع خوادم الجذر، وهذه الرسوم في الوقت نفسه هي لـ 11 من خوادم الجذر التي لدينا بيانات لها. يمكنك أن ترى أن البيانات والخوادم المختلفة التي لدينا بيانات عنها في فترات زمنية مختلفة. وإذا نظرت إلى الرسوم البيانية، فهي متشابهة نسبيا باستثناء الجذر J، والذي جاء تقريره بنسبة مئوية أقل، لذا يبدو الجذر J أفضل من كل المجموعات الأخرى. على الأقل من حيث النسبة المئوية. [غير مسموع] فنحن لا نحصل على تقارير من جميع الحالات الجذرية J، لذلك ربما يكون لها تأثير على ذلك. والنقطة هنا هي أنه لا يوجد اختلاف كبير بين بيانات خوادم الجذر. ما أظن أنه مثير للاهتمام هو تغيير السلوك الذي حدث في منتصف كانون الثاني (يناير) عندما رأينا هذا الارتفاع. يعرض هذا الرسم البياني عناوين IP الفريدة التي تتم إضافتها كل يوم، وتمثل نقطة البيانات هنا في ذلك اليوم عدد المصادر التي تبلغنا بالبيانات التي لم نرها من قبل. وإذا نظرت إلى القراءة من اليسار إلى اليمين، فنبدو وكأننا لم نعد أكثر من 1000، بضع مئات من عناوين IP الجديدة كل يوم. إذن فجأة بعد حدث الترقية المفترض أن يحدث

في شهر كانون الثاني (يناير)، نرى الآن العديد من المصادر الفريدة التي تقدم تقارير يومية. حوالي 15000 إلى 16000 تقرير في اليوم. إذا كنت تخطط لرسم رسم بياني يتضمن عدد عناوين IP المتراكمة الفريدة التي نراها يوميا، فسيكون هذا ما سيبدو عليه الرسم البياني. يظهر الخط الأخضر عدد عناوين IP التي نراها في نقطة زمنية معينة. ومن الواضح أن هذا الرقم يبدأ صغيرا على اليسار، في وقت مبكر من الزمن، وكلما تقدمنا في الوقت، كلما زادت عناوين IP الفريدة التي نراها، حتى نصل الى هذا الرقم الآن وهو 730.000. حتى الآن، لدينا 730.000 عنوان IP مختلف، لم أذكر هذا في العرض التقديمي، بل هو مزيج من عناوين V4 وV6. وقد أبلغنا بالبيانات حوالي 730.000، منهم حوالي 250.000 في مرحلة أو أخرى أفادوا بأن لديهم KSK 2010 فقط. لقد قمت بحساب ذلك، وعندما تنظر إلى الأرقام التراكمية الموجودة اليوم، فإن النتيجة أسوأ. إن حوالي 35% من إجمالي العناوين التي رأيناها لا تبلغنا سوى عن KSK 2010.

قررت أن ألقي نظرة على هذا من خلال انخفاض 24، بحيث يمكنك أن ترى أن شكل هذا الرسم البياني مختلف قليلا. كان هناك ارتفاع في الانخفاضات الجديدة لـ 24 بعد الزيادة في شهر كانون الثاني (يناير)، ثم انخفض قليلا. ولو قمت برسم الخط التراكمي، فما زال لدينا الكثير من انخفاضات 24. وإذا نظرتم الى الخط الأخضر، فستجدون أنه يتخطى حوالي 350.000. سيكون هذا متوسطا، حيث نفقد الكثير من الدقة هنا، وهو المتوسط لكل عنوانين IP لكل انخفاض 24. كنت آمل أن يكون هذا الرقم أصغر من ذلك للإشارة إلى أنه ربما كانت هناك كتل كاملة تحتوي على مجموعة كاملة من العناوين ويمكننا التحقق من تلك النظرية والافتراض النظري لذلك هو أنه ربما كان عبارة عن مربعات العناوين التي لا تحتوي إلا على أجهزة ديناميكية عابرة.

هذا عدد كبير من العناوين، وما يثير الاهتمام هو أن العدد الإجمالي للعناوين التي تبلغنا بمفاتيح KSK 2010 و KSK 2017، يكون أكبر من العدد الإجمالي لعناوين IP الفريدة. ما يعنيه ذلك هو أن هناك مصادر أبلغت عن حيازتها لمفتاح KSK 2010، ثم أبلغت أن لديها مفتاحي KSK 2010 وKSK 2017. ليس بالضرورة بهذا الترتيب، لكنهم قدموا كلا التقريرين. أحد الأسباب التي قد تحدث، تخيل أن مصدرا يعطي تقريرا

بالمفتاح KSK 2010 وفي وقت لاحق يعطي تقريرا ب KSK 2010 و2017. سبب واحد، وليس السبب الوحيد الممكن، هو أن الجهاز قام بتحديثها. لديها الآن KSK الجديد، ولكن من أصل 750.000 عنوان IP فهناك فقط حوالي 1550 تقرير لكليهما. وهذا يعني أنه لا يوجد عدد كبير من الأجهزة التي يمكننا الإشارة إليها وأن نقول أنه أحد الفرضيات هي أنهم قاموا بالترقية. وجزء من المشكلة هنا هو أن هناك بالفعل مشكلة مع إشارة 8145، ونحن نعرف أن هناك وكلاء مشاركين، كما ذكرت، فرؤيتك لتقرير من مصدر IP لا يضمن بأن ما تشاهده هو الإعداد الأصلي لعنوان IP. قد يكون شخص آخر يعيد توجيه تقرير 8145 الذي يعكس إعداد عنوان IP، فيعيد توجيهه إلى خادم الجذر فنراه. وهذا تفسير آخر لرؤيتنا مصدرا واحدا يقدم تقرير KSK 2010 و KSK 2010 و2017.

ونعلم أيضا أن هناك إصدارا واحدا على الأقل من أحد التطبيقات التي أبلغت عن 8145 حتى إذا لم يكن هناك اثبات لصحتها. إذا كان لديه KSK 2010 لا يهم لأنه كان يتحقق من صحة DNS واستخدم ذلك كجزء من إعداده. تم إعداده لهذا السبب، ولكن لا يهم.

إذا كنت تريد الاطلاع على هذه الرسوم البيانية بنفسك، فنحن نحدثها أسبوعيا، وهذا هو عنوان URL لها. وهو العنوان Root trust anchor reports dot ICANN dot org. لقد بدأت للتو بتحليل البيانات على هذا النحو، وهذا يعتمد على هذا الجدول المعين، ولا يعتمد على عناوين IP الكاملة التي يبلغ عددها 250.000 والتي أصبحت حاليا لا تبلغ إلا عن KSK 2010. هذا يعتمد على رقم أصغر ولا أتذكر الرقم الإجمالي الذي مر مرور الكرام برأسي. هذا يبحث في عدد المصادر لكل نظام مستقل ومن ثم يقوم بالتصنيف العكسي بحيث تكون أرقام النظام المستقل ASN مع معظم عناوين IP. أستميحكم عذرا، وهذا ليس فقط مع KSK 2010، حيث هكذا يتم الإبلاغ عن كل أرقام النظام المستقلة. سيكون ذلك مخططا مختلفا إذا كنت تستخدم KSK 2010 فقط. ما يعنيه هذا، أننا بحاجة إلى تشغيل هذا مرة أخرى فقط للنظر إلىKSK 2010 وسيسمح لنا بإجراء بعض محاولات الاتصال لمعرفة ما يحدث مع الأنظمة الذاتية التي لديها أكبر عدد من المحللين والذين يبلغون بمفتاح KSK 2010 فقط.

لقد قمنا بتوزيع قائمة عناوين IP التي تبلغ KSK 2010 فقط إلى دائرة مزودي خدمات الإنترنت والإتصال ISPCP وأمناء السجلات والأهداف ذات ثنائية. بالطبع، من أجل ترقية هذه الأنظمة، ولكننا لا نزال مهتمين للغاية بمعرفة ما الذي يحدث وسبب عدم ترقية هذه الأنظمة. إذا وجدنا، على سبيل المثال، أحد أفضل النتائج هي اكتشاف أن هناك بالفعل مساحة عنوان حيث توجد مجموعة من [غير مسموع] الأجهزة التي تعمل على تشغيل إعداد قديم مع KSK 2010 فقط. وهذا من شأنه أن يكون نتيجة إيجابية. هذه الشريحة غير محدثة الآن، ولدي إذن من سلطات ICANN بجعل القائمة متاحة للجمهور. سنقوم بنشر صفحة، وستبدو هكذا، سأقوم بترتيبها ترتيبا عكسيا حسب رقم النظام المستقل ASN وستكون قادرا على النقر على ASN والحصول على قائمة بالعناوين من ذلك ASN الذي تم الإبلاغ عنه في KSK 2010. سيكون من الأسهل على المشغل معرفة ما يحدث في شبكته. من الواضح أننا سنصل إلى المشغلين بدءا من المشغلين الأكثر ابلاغا بمفتاح KSK 2010 فقط ومحاولة معرفة ما يحدث. الخطوات التالية، استمر في محاولة معرفة ما يحدث مع بيانات 8145، أنا لست سعيدا بالإشارة التي يقدمها، ولكنها الآن البيانات الوحيدة المتوفرة لدينا. الشيء المسؤول الذي ينبغي القيام به هو مواصلة التحقيق، ومحاولة معرفة ما تقوله لنا، وإذا وصلنا إلى النقطة التي نحن مقتنعون بأنها في الحقيقة لا تقول أي شيء ذا قيمة، وهذا في حد ذاته نتيجة إيجابية. سنحاول الاتصال بالشبكات التي تبلغ عن وجود عدد كبير من المحللين باستخدام KSK 2010 فقط، وسنسهل للأشخاص الآخرين القيام بهذا التحقيق. سنستمر في الحديث عن هذا الأمر حتى تستمرون في رؤيتي أنا وزملائي وسنستمر في الاستماع إلى المجتمع لأنه كما قلت، هناك طرق يمكنك المساعدة بها، يرجى التعليق على الخطة، هناك عنوان URL مرة أخرى ويرجى الانضمام إلى قائمة استبدال مفتاح توقيع شفرة الدخول الأساسية للبقاء على اطلاع على آخر المستجدات. بذلك، سأكون سعيدا لأتلقى أية أسئلة. لدينا القليل من الوقت قبل الفعالية التالية هنا على الساعة الخامسة.

هوارد بن: اسمي هوارد بن، وأمثل شركة Samsung Electronics. فقط فيما يتعلق بتلك الشريحة التي كانت لديك عن المشغلين، هذه هي. تخميني هو أن الشبكة الجغرافية

للاعتماد والتي ربما يتم تشغيل شبكة LTE التابعة لهم بالكامل على الأجهزة الافتراضية، ولا شك أنها لن تتخطى مهلة الـ 30 يوما. سيكون من المثير جدا أن نرى عددا كبيرا من مشغلي شبكات الهواتف المحمولة هناك، سواء كانوا جميعا يعانون نفس المشاكل أم لا. مرة أخرى، يسعدني تقديم بعض معلومات الاتصال بالشبكة الجغرافية لأن هذه معداتنا.

متحدث غير معروف: حسنا، شكرا لك.

مارك: مارك [غير مسموع] مع مزودي خدمة الإنترنت يتحدث نيابة عني هنا. هل يمكننا الانتقال إلى الشريحة 4 من فضلكم؟ هذه هي الشريحة رقم 4. أنا أبحث في أسفل الشريحة، حيث توجد نتائج المناقشة وهي الأولى من ثلاثة. سأصيغها بكلماتي الخاصة هنا ويمكنك أن تخبرني إذا كنت مخطئا. النقطة الأولة تقول أننا لا نعرف ما تأثير ذلك على الإنترنت. والنقطة الثانية تقول قم بذلك على أية حال. هل أخطأت في قراءة ذلك؟

متحدث غير معروف: وهذا من شأنه أن يكون نصف تفسير.

مارك: هل يمكنك تفسير الأمر بالكامل لي؟

متحدث غير معروف: أعتقد أن باقي هذا العرض هو لذكر الأمور الإيجابية. اسمحوا لي أن أقدم الجواب المهم. الإجابة الجادة هي أنه من الصعب معرفة ما يجب القيام به، عندما وصلنا إلى النقطة التي وصلنا إليها في الخريف الماضي، قررنا أننا بحاجة إلى إشراك المجتمع والحصول على مدخلات المجتمع. الملخص الذي قدمته هو ما أخبرنا به المجتمع. سأضير إلى أنه اختيار

ذاتي إلى حد ما لمن يعمل على استبدال مفتاح توقيع شفرة الدخول الأساسية، وهناك ميل للأشخاص المناصرين للإمتدادات الأمنية لنظام اسم النطاق DNSSEC وليهد رس مال شخصي، والذين يعرفون ماذا أيضا يمكن استثماره في DNSSEC ويرغبون في حدوث الاستبدال. أعتقد أن شعورنا لم يكن مفاجئا في الماضي، ولكن هذا هو السبب في أن التعليق العام مهم جدا حتى نتمكن من عرضه على جمهور أوسع، وإذا كان لدى الناس نصف تفسير لذلك، فيمكنهم التعليق على ذلك.

مارك: أقدر ذلك وشكرا على ذلك التفسير. لا زلت أرى الجانب السلبي هنا. لا أستطيع أن أشعر بأنني مدافع عن الإمتدادات الأمنية لنظام اسم النطاق DNSSEC، لذلك لا يمكنني قول أكثر من ذلك، وسأقدم تعليقات فردية على هذا. لا أستطيع تخطي النقاط الأولى والثالثة، هناك نوع من التنافر المعرفي لدي أن يمكن لأي شخص في الواقع تغيير الجذر بحيث لا يمكن معرفة الآثار المترتبة على ذلك. أتفق معك وأثق تماما بتحليلك لهذا النوع من النوعية الرديئة للإشارات التي تحصل عليها، ولكن بمرور الأيام، فإن الإشارات التي تحصل عليها هي المعلومات التشخيصية الوحيدة التي لديك، والإشارات الوحيدة التي تحصل عليها تزداد سوءا. وهذا هو وصفي للوضعية. أجد جميع الشرائح التي تأتي بعد هذا مقنعة للغاية، ولكن هذه الشريحة والنقطتين الأولى والثالثة تحت المناقشة التي لا أستطيع الاقتناع بها. لا أعرف لماذا سينصح أي شخص في المجتمع التكنولوجي بالاستمرار ومتابعة التغيير على الجذر دون معرفة النتائج. شكرا، وسآخذ تلك التعليقات في التقديمات الفردية كذلك.

متحدث غير معروف: اسمحوا لي أن أمرر ما أعتقد أنه قد يكون تفسيرا آخر. هذا ليس تفسيري، أنا فقط أكرر ما سمعت. وهو أن هناك جانبا سلبيا محتملا لعدم تغيير المفتاح. يمكن أن يقلل من الثقة في المفتاح على الرغم من عدم وجود تهديد فيما يتعلق بتشفيره في الوقت الحالي. إما تهديد لرسومات الخرائط نفسها، أو التهديد للأمن التشغيلي الفعلي للمفتاح. ومع ذلك، لا يمكن أن يؤدي التغيير إلى تقليل الثقة في المفتاح، وإذا جمعت ذلك مع الاعتقاد بأن ذلك

لن يكون سيئا للغاية، ويمكن للأشخاص إصلاحه بسرعة وقبول وجود بعض الخسارة، فيمكنك الجمع بين كل تلك الأمور للاقتناع بأنه يجب علينا تغيير المفتاح.

مارك: أتفهم النقاش المتعلق بالسمعة بشكل صحيح، وما نريد فعله هو تشغيل المفتاح لأننا نريد أن يثق الناس في الإمتدادات الأمنية لنظام اسم النطاق DNSSEC. أتفهم الجزء المرتبط بالسمعة، ومن ناحية أخرى، إذا كان الناس يخمنون خطأ، وأنا مصدوم إذا كان التخمين أسوأ مما كنا نعتقد أنه سيكون وعلينا التراجع عن التغيير، أليس كذلك. ليس لدينا واحد بعد في العالم الواقعي. أعتقد أننا نواجه مشكلة سمعة في كلتا الحالتين. وهذا يضع ICANN في موقف صعب وأنا حساس تجاه ذلك، لكنني لست مقتنعا بأن مسألة سمعة الإمتدادات الأمنية لنظام اسم النطاق، بشكل عام، هي نفسها التنفيذ غير المعروف في تشرين الأول (أكتوبر). شكرا.

متحدث غير معروف: هل ثمة أسئلة أو تعليقات أخرى؟ كاثي، هل ورد إلينا أي شيء من المشاركات عن بعد؟

متحدث غير معروف: لا.

متحدث غير معروف: آه، نعم.

متحدث غير معروف: شكرا لكم على العرض التقديمي. سؤالي هو أننا اكتشفنا أنه في نيجيريا، لدينا أربعة مشغلي شبكات متنقلة وعدد كبير من مزودي خدمات الإنترنت. لقد اكتشفنا أن واحدا فقط من مزودي خدمات شبكات الجوال الأربعة يستخدم DNSSEC، أما مشغلات الهاتف المحمول الثلاث الأخرى فكانت [غير مسموع] غير DNSSEC. ما الميزة التي تتمتع

بها DNSSEC على أنظمة التحقق من الأمان الأخرى؟ هل هناك أي حاجة إلى انتقال [غير مسموع] الآخر إلى DNSSEC؟ مرة أخرى، السؤال الثالث، من هم مزودي خدمة الشبكة [غير مسموع] الذين يستخدمون نظام التحقق الآخر بعد استبدال مفتاح توقيع شفرة الدخول الأساسية؟ شكرا جزيلا لكم.

متحدث غير معروف: هل يمكنك أن تكرر الجزء الأخير من سؤالك رجاء؟

متحدث غير معروف: الجزء الأخير من سؤالك رجاء، نعم.

متحدث غير معروف: ما قلته، الجزء الأخير من السؤال هو أن ثلاثة من مزودي خدمة شبكة الهاتف المحمول لا يستخدمون نظام تحقق DNSSEC. ما هو [يتعذر تمييزه] خاصتهم بعد استبدال مفتاح توقيع شفرة الدخول الأساسية؟

متحدث غير معروف: آسف جدا، ما هو... خاصتهم؟

متحدث غير معروف: [يتعذر تمييزه] خاصتهم. هل سيكون هناك أي تأثير على المستخدمين؟

متحدث غير معروف: هذا هو السؤال السهل، إذا لم تتحقق باستخدام DNSSEC فليس هناك أي تأثير على الإطلاق من استبدال مفتاح توقيع شفرة الدخول الأساسية. إنه موقف مؤسسة ICANN بأن التحقق باستخدام DNSSEC أمر جيد، لذلك نشجع الناس على القيام بعملية التحقق عن طريق DNSSEC وأنا آسف، الآن لا أتذكر الجزء الأول من سؤالك.

متحدث غير معروف: الجزء الأول من السؤال، قلت: هل هناك أية ميزة تدفع الذين لا يستخدمون الامتدادات الأمنية لنظام اسم النطاق DNSSEC إلى الانتقال إليها؟

متحدث غير معروف: إن موقف ICANN هو أنه ينبغي عليك القيام بتحقق DNSSEC لأنه بدون التحقق باستخدام DNSSEC لن تتأكد من أن الإجابة التي تتلقاها تجيب فعلا عن السؤال الذي طرحته، وأنه يأتي بالفعل من الجهة التي تظن أنه يأتي منها. ليس لديك تأكيد تشفيري بأن الإجابات التي تحصل عليها بالفعل تأتي من مصدرها. توفر DNSSEC، تعرف أن الإجابة تأتي من الجهة التي تقول أنها مصدرها وأنها لم يتم تعديلها منذ توقيعها. وتوصل المحللون العصريون بذكاء شديد إلى تجنب خداعهم، ولكن في نهاية المطاف للحصول على مستوى أعلى من التأكيد فأنت بحاجة إلى DNSSEC. بدون DNSSEC، إلى حد ما، أنت عرضة للتهويل أو الخداع لتصديق الردود غير الصحيحة.

متحدث غير معروف: شكرا جزيلا لكم، شكرا.

متحدث غير معروف: هل من أسئلة أخرى؟ رائع، نشكركم على الحضور.

[نهاية النص المدون]