# AR

ICANN82 | الاجتماع المشترك: GAC وSSAC
الأحد، الموافق 9 مارس/آذار 2025 – من الساعة 04:30 م إلى 05:30 م بتوقيت المحيط الهادي

نيكولاس كاباليرو السيدات والسادة أهلاً ومرحبًا بكم جميعًا مرة أخرى. نحن على وشك أن نبدأ. تفضلوا بالجلوس رجاءً. جوليا، تفضلي للتسجيل.

غولتن تيبي مرحباً بكم في اجتماع اللجنة الاستشارية الحكومية في ICANN82 مع جلسة SSAC يوم الأحد 9 مارس/آذار في الساعة 16:30 بالتوقيت المحلي. يُرجى العلم بأن هذه الجلسة يجري تسجيلها، وتحكُمُها معايير السلوك المتوقعة في ICANN وسياسة مجتمع ICANN لمناهضة التحرش.

خلال هذه الجلسة ستقرأ الأسئلة أو التعليقات المقدمة في مربع الدردشة جهرًا إذا كُتبت بالشكل المناسب. ولا تنسوا رجاءً ذكر أسمائكم واللغة التي ستتحدثون بها في حال كنتم ستتحدثون بلغة أخرى غير الإنجليزية. يرجى التحدث بوضوح وبسرعة معقولة للسماح بالترجمة الفورية الدقيقة والتأكد من كتم صوت جميع الأجهزة الأخرى عند التحدث. ويمكنكم الوصول إلى جميع الميزات المتاحة لهذه الجلسة في شريط أدوات Zoom. والآن، سأعطي الكلمة لنيكولاس كاباليرو، رئيس اللجنة الاستشارية الحكومية. شكراً لك. إليك الكلمة يا نيكو.

نيكولاس كاباليرو شكرًا جزيلاً لك، غولتن. مرحبًا بالجميع في الجلسة الأخيرة، ولكنها الأكثر أهمية، على الأقل من وجهة نظري المتواضعة، مع SSAC، لجنة الاستشارات الأمنية والاستقرار. مرحبًا رام. مرحبًا بفريقك الرائع. في الواقع، كنا نتحدث عن بعض القضايا التي سنناقشها اليوم، أمس وأول أمس. وعندما ذكرت الحوسبة الكمّية وتأثيرها المحتمل على DNS واستقراره وتنفيذ DNSSEC والتشفير بشكل عام، سواء المتماثل أو غير المتماثل، نظر إليّ الجميع وكأنني مجنون! وقد يكون هذا صحيحًا. ولكن على أي حال، سنناقش هذا

الموضوع بعمق مع هذا الفريق من الخبراء. سنتطرق إلى الحوسبة الكمّية وتأثيرها على التشفير، كما ذكرت أمس.

ثم سنجري مناقشة حول Infermal. وبالنسبة لـ 60 عضوًا جديدًا في GAC، فقد شرحت بالفعل ما يعنيه هذا المصطلح. ولكننا سنتناول التفاصيل لاحقًا. وبعد ذلك سنناقش الخطوات التالية. لذا، مرحبًا بكم مرة أخرى، رام، وفريقكم الرائع. الكلمة لكم.

رام موهان نيكو، شكرًا جزيلًا لك. وبالنيابة عن SSAC، نعبر عن امتناننا العميق لـ GAC على هذه الدعوة. هذه هي المرة الثالثة التي نلتقي فيها بكم. وفي كل مرة، تصبح التفاعلات بيننا أكثر ثراءً وأكثر انخراطًا. نحن نقدر حقًا هذه الفرصة لتعزيز حوارنا التعاوني حول القضايا الحرجة المتعلقة بأمن الإنترنت واستقراره.

بالنسبة لأولئك الجدد على GAC ومجتمع ICANN، فإن SSAC يعمل كهيئة استشارية متخصصة داخل ICANN. ويكرس جهوده لتحديد وتحليل التهديدات المحتملة لأنظمة التسمية والعناوين في الإنترنت. تتألف SSAC من خبراء تقنيين متمرسين. ونحن نقدم توصيات موضوعية قائمة على الأدلة لمجتمع ICANN ولمجلس الإدارة.

وفي بعض الأحيان، عندما لا تكون توصياتنا مبنية على أدلة. نشير بوضوح إلى أنها تستند إلى آراء الخبراء التي نقدمها للمجتمع ولمجلس الإدارة. مجالات تركيزنا واسعة، تمتد من ثغرات DNS والمخاطر السيبرانية، إلى تأثير التقنيات الجديدة على بنية الإنترنت، إلى الجوانب المتعلقة بأمن واستقرار ومرونة حوكمة الإنترنت. لذا فإننا نغطي هذا الأمر بالكامل. لكن، بشكل أساسي، ينصب تركيزنا على البنية التحتية الحرجة. وهذا هو مجال انخراطنا الرئيسي.

ندرك أن GAC يلعب دورًا حيويًا في تمثيل وجهات النظر الحكومية حول حوكمة الإنترنت. وهذه الجلسة، نيكو، تتيح لنا في SSAC سد الفجوة بين المجالات التقنية والسياساتية، ونحن حريصون على مواصلة هذا التفاعل لضمان أن تكون توصياتنا قوية ومتوافقة مع المصلحة العامة. إذن، هذا هو الدافع الرئيسي لعملنا. وهو السبب الذي يجعلنا نقدر هذا التفاعل مع GAC، والمشاركة معًا لتأمين انترنت آمن وثابت ومستقر.

فهذا بالفعل دافع رئيسي لما نقوم به وسبب رئيسي لتقدير هذا التفاعل مع GAC. وشكرًا لكم على ذلك. كما ذكرت بالفعل، لدينا موضوعان رئيسيان نريد مناقشتهما معكم اليوم. روس هاوسلي هنا على يميني. وروس يتمتع بمسيرة مهنية طويلة ومتميزة. ومن بين اهتماماته البحثية، تأثير الحوسبة الكمّية على التشفير. لذا، رأينا أنه سيكون من المفيد أن يشارك روس أفكاره حول هذا الموضوع. هدفنا ليس إلقاء محاضرة عليكم. بل مشاركة أفكارنا وما وصلنا إليه، ثم ندعوكم للمشاركة والتفاعل معنا.

نحاول قدر الإمكان عدم جعل عروضنا التقنية معقدة للغاية، على الرغم من أن الموضوع الأساسي تقني جدًا. فهذا أحد أهدافنا. لذا، إذا شعرتم أننا نغرق في "حديث الخبراء"، فلا تترددوا في مقاطعتنا وطلب توضيح؟ نحن سعداء بترجمة المفاهيم التقنية إلى مصطلحات أكثر وضوحًا. بهذا، نعود إليك يا روس، الكلمة لك.

روس هاوسلي

شكرًا يا رام. لقد وضعت الفكرة الرئيسية مباشرة على الشريحة الأولى. لا أحد يعرف الإجابة بعد. لقد كانت الحوسبة الكمّية تتطور منذ فترة. وقد أجرى NIST (المعهد الوطني للمعايير والتكنولوجيا) مسابقة كبيرة. النتيجة التي خرجت منها تُعرف بـ ML-DSA. وهي خوارزمية توقيع رقمي تعتمد على تقنية "الشبكة". المشكلة هي أن هذه الحلول لا تتناسب مع DNSSEC. فهي ضخمة جدًا. المفاتيح العامة وقيم التوقيع ضخمة جدًا، وإذا كنت تستخدم DNS عبر UDP، فلن تتمكن من استيعابها. هكذا بكل بساطة.

لكن هناك جانب إيجابي، وهو أن لدينا متسعًا من الوقت. لأن أكبر تهديد للحوسبة الكمّية هو ما يسمى بـ هجوم "احصد الآن، فك التشفير لاحقًا". الخطر هنا هو أن يقوم المهاجم بتخزين البيانات المشفرة حاليًا، حتى يتمكن في المستقبل من فك تشفيرها باستخدام كمبيوتر كمّي قوي بما يكفي. لكن DNS لا يحتوي على بيانات سرية، لذا هذه ليست مشكلة. المشكلة الأساسية هنا هي أن التوقيع الرقمي يجب أن يكون غير قابل للتزوير عندما يصبح من الضروري مواجهة تهديد الحوسبة الكمّية.

لذا، في الشريحة الثانية، تطرقت إلى ما يمكننا فعله لتطبيق التوقيعات الكمّية. هناك أبحاث جارية حاليًا في هذا المجال. فرقة عمل أبحاث الإنترنت (IRTF) لديها مجموعة تبحث في DNSSEC ما بعد التوقيعات الكمّية. وسيكون هناك اجتماع جانبي حول هذا الموضوع الأسبوع المقبل. يبدو أن Merkle hash trees هي أساس الإجابة. وهذا ليس مفاجئًا،

لأنها تُستخدم في تقنيات مثل البلوكتشين وشفافية الشهادات والعديد من التقنيات الأخرى. لذا، ربما ليس من المستغرب أن تكون جزءًا من الحل هنا أيضًا. لقد أضفت بعض الروابط على الشريحة.

لمن يريد الاطلاع على المزيد من التفاصيل حول التوقيعات القائمة على hash-based signatures لكن هذه التوقيعات كبيرة الحجم أيضًا، لذا يتم البحث عن تقنيات أخرى. على أي حال، هناك الكثير من النقاشات التي ستجري الأسبوع المقبل في مؤتمر IETF 122 لاستكشاف هذه المواضيع بشكل أعمق. لكنني لا أتوقع الحصول على أجابة ولا بعد عام من الآن. لكن لدينا الوقت. لذا، إن كان لديكم أسئلة حول ذلك، أو ستحتفظون بها حتى النهاية، أو تريدون طرحها الآن؟ حسنًا، إذا كان لديكم أسئلة، فسيسعدنا الرد عليها.

نيكولاس كاباليرو شكراً لك. شكرًا جزيلًا. المايكروفون مفتوح لطرح الأسئلة. أود أن تشرح، لمصلحة جميع أعضاء GAC مرة أخرى، ما هي التوقيعات الرقمية، النسخة الأساسية منها، من فضلك.

روس هاوسلي بالتأكيد. التوقيع الرقمي هو الأساس الذي يقوم عليه DNSSEC. الفكرة هي أنه عندما تحصل على استجابة لطلبك، يكون التوقيع الرقمي مرفقًا بها. مما يعني أنها لم تتغير منذ نشرها في الأصل. إذن، هذا هو العنصر الذي يضمن سلامة البيانات وتوثيقها.

نيكولاس كاباليرو شكرًا جزيلًا. الكلمة الآن لممثل هولندا.

ماركو هوغوونينغ شكرًا سيدي الرئيس. لأغراض التسجيل، معكم ماركو من هولندا. وشكرًا على هذا العرض الموجز ولكنه عميق في الوقت ذاته. أوافق. ولكن لا يزال أمامنا طريق طويل. لكنني أمثل حكومة. وأعلم أن الفترات الزمنية الطويلة غالبًا ما تكون أقصر مما نظن. دون الخوض في الكثير من التفاصيل التقنية، هل لديكم أي نصيحة عملية تقدمونها لنا

كحكومات الآن؟ وماذا يمكننا أن نفعل للتحضير للنقطة الحتمية التي سيتعين علينا فيها تغيير خوارزمية DNSSEC؟

روس هاوسلي لا يزال الوقت مبكرًا بالنسبة لـ DNSSEC. بالنسبة للبروتوكولات الأمنية الأخرى، لدينا حلول. هناك أعمال جارية في مجموعات عمل أخرى في IETF، مثل LAMPS التي تعمل على PKI وSMIME. لدينا TLS. ولدينا IPSEC في هذه المجالات الثلاث. عفوًا، وأيضًا Secure Shell. في هذه المجالات الأربعة، لدينا حلول، ويجب نشر البنية التحتية الآن بحيث تكون جاهزة عند الحاجة إليها. لأن الأمر سيستغرق عدة سنوات.

إذا نظرتم إلى الانتقال من SHA-1 إلى SHA-256، كنت حينها مديرًا لمنطقة الأمن في IETF، وكنت أظن أن خمس سنوات ستكون كافية. لكنها استغرقت أكثر من ضعف ذلك. لذا، ابدأوا في بناء البنية التحتية الآن لضمان إمكانية الانتقال لاحقًا، لأن هناك أشياء كثيرة لن تكون ممكنة إذا لم تكن هناك بنية تحتية تربطها ببعضها. هذه هي نصيحتي.

نيكولاس كاباليرو ستيف، تفضل من فضلك.

ستيف كروكر شكراً لك. روس، سيكون من المفيد متابعة هذا السؤال، فهو منطقي جدًا عندما يأتي من حكومة تسأل: ماذا يجب أن نفعل؟ لقد أشرت إلى الانتقال السابق من SHA-1 إلى SHA-256. هل يمكنك أن توضح لنا كيف سيبدو الانتقال عندما يتم اتخاذ قرار بشأن الخوارزمية الجديدة؟ هل سيكون الانتقال إلى الخوارزمية الجديدة مختلفًا نوعيًا عن أي تغييرات سابقة في الخوارزميات، أم أنه مجرد تغيير آخر في الخوارزمية نمتلك بالفعل الخبرة الكافية للتعامل معه؟

روس هاوسلي لذا شكرا لك يا ستيف. لا نعرف الإجابة على وجه اليقين، لكن ما نعرفه هو أن هذا الانتقال سيكون أكثر تعقيدًا، لأننا لا نستبدل مجرد قطعة في محرك. بل نرمي المحرك بالكامل

ونضع محركًا جديدًا. لذا، أنه في هذا الموقف، ينبغي أن تفكر في، إذا فكرت في PKI، فإننا لا نتحدث فقط عن تغيير بعض الأجزاء، بل عن بناء بنية جديدة بالكامل من الجذر حتى القمة. أنت لا تغير أجزاء فقط من ذلك. أرجو أن يكون ذلك مفيدًا. لا؟ معذرةً.

نيكولاس كاباليرو

شكرًا لك يا ستيف على هذا السؤال. شكرًا يا روس. هل ثمة أسئلة أو تعليقات أخرى؟ لدي سؤال موجه لك يا روس. لنفترض أن حكومة X لديها تنفيذ قوي لـ DNSSEC وMANRS وRPKI وما إلى ذلك. بالإضافة إلى مجموعة من التشفيرات مثل Blowfish وRSA وDES وSHA-256 أو أي مزيج منها، ثم فجأة يحدث اختراق في الحوسبة الكمومية. صحح لي إن كنت مخطئًا، لكن في هذه الحالة، ستكون بنية DNSSEC الخاصة بهذه الحكومة قديمة تمامًا تلقائيًا. هل أنا على صواب؟

روس هاوسلي

نعم. نعم، ولكن مع ذلك ليس من الواضح أنك تعرف متى سيحدث ذلك. هناك الكثير من الأبحاث حول زيادة عدد الكيوبتات وحجم الحواسيب الكمومية. لكننا حتى الآن لسنا قريبين من أي شيء له صلة بالتشفير. كما أن هذه التطورات ليست على مستوى واحد.

فغالبًا تحدث على شكل قفزات. وعندما يحدث ذلك، قد لا نحصل على تحذير كافٍ، وهو ما يؤكد النقطة التي ذكرتها سابقًا حول البدء في العمل الآن. لكن RPKI وDNSSEC فريدان من نوعهما، حيث إنهما يركزان فقط على السلامة. ولا يتعاملان مع البيانات السرية. لذا، لدينا المزيد من الوقت للتعامل مع هذه المشكلة، حيث لا توجد هنا مشكلة "اجمع البيانات الآن وفك تشفيرها لاحقًا".

نيكولاس كاباليرو

إذن، سنكون بخير مع استخدام مجموعة قوية من DNSSEC وRPKI وMANRS

روس هاوسلي

حسنًا. نعم، لدينا المزيد من الوقت لحل هذه المشكلات لأنها تتعلق فقط بالبيانات العامة وسلامتها.

نيكولاس كاباليرو شكرًا يا روس. لدينا ممثل أستراليا، ثم هولندا. ممثل أستراليا، تفضل.

إنغرام نيبلوك مرحبًا بكم. معكم إنجرام نيبلوك من أستراليا. أعلم أن لكل منكم غرضًا مختلفًا. هل يمكنكم التعليق على دور DNS عبر HTTPS وDNS عبر TLS. من الواضح أن أحدهما يتعلق بالتوقيع، والآخر بأمان النقل. لكن هل سيكون من الأسهل تنفيذ التشفير بعد الكم في الأمور المتعلقة بأمان النقل؟ وهل سيؤدي ذلك إلى توفير بعض الفوائد التي نحصل عليها حاليًا من DNSSEC بفضل تشفير البيانات أثناء النقل؟

روس هاوسلي نعم، ستوفر هذه البروتوكولات حماية للبيانات أثناء انتقالها بين نقاط التشفير وفك التشفير. لكنها تعتمد على نموذج القفزات المتعددة عند تطبيقها على DNS. لذا فهي توفر الحماية في هذا السياق. وكما ذكرت، العمل على TLS جارٍ حاليًا. لكننا لا نمتلك بعد البنية التحتية لـ PKI التي سيتم ربطها بها. بالمناسبة، سيجتمع منتدى تصفح هيئة الشهادات الأسبوع الذي يلي اجتماع IETF في طوكيو لمناقشة هذا الموضوع تحديدًا. آمل أن يكون ذلك مفيدًا.

نيكولاس كاباليرو شكرًا لممثل أستراليا. شكرًا روس، مرة أخرى، لفائدة الأعضاء الجدد في GAC، يشير PKI إلى البنية التحتية للمفتاح العام، وMANRS إلى المعايير المتفق عليها لأمن التوجيه. يمكننا تقديم الروابط والمزيد من المعلومات حول ذلك. لدي هولندا، ثم السيد الجالس هناك. عذرًا، لا أعرف اسمك، ولكن هولندا أولاً.

ماركو هوغوونينغ شكرًا سيدي الرئيس. معكم ماركو مرة أخرى. بالانتقال إلى نقطة أخرى، وربما من باب لعب دور محامي الشيطان أيضًا، أحاول تجنب تحول النقاش إلى نقاش تقني بحت. لكن

في شريحتك السابقة، ذكرت التحديات التي تواجهها مع نقل UDP. وأتذكر أن هذه ليست المرة الأولى التي نواجه فيها حدودًا معينة مع UDP كوسيلة نقل في صناعة DNS.

أعتقد أنه يلعب دورًا أيضًا في تنفيذات DNSSEC الحالية فيما يتعلق بطول المفتاح. أتساءل، وبما يتماشى إلى حد ما مع ما سأله زميلي الأسترالي، نظرًا لأننا ننظر إلى الأفق البعيد، هل يمكن التفكير في خيارات نقل مختلفة لـ DNS غير UDP؟

روس هاوسلي حسنًا، خيارات النقل الأخرى مفهومة جيدًا ومحددة، لكنها غير منتشرة على نطاق واسع. لذلك، كجزء من هذا الانتقال، ربما سيتم نشرها.

ماركو هوغوونينغ وهذا يعيدنا إلى السؤال، نحن الحكومات، كيف يمكننا المساعدة؟

روس هاوسلي معك حقّ.

نيكولاس كاباليرو روس، هل يمكنك إعطاء مثالين أو ثلاثة حول هذه النقطة؟

روس هاوسلي مثالين أو ثلاثة؟

نيكولاس كاباليرو أعني لاستبدال UDP.

روس هاوسلي إذن، DNS عبر TCP، وDNS عبر QUIC، وDNS عبر TLS. هذه أمثلة على وسائل نقل لا تعاني من نفس قيود الرسائل الفردية.

نيكولاس كاباليرو شكرًا جزيلًا. ممثل هولندا؟

بيتر توماسن تفضل. مرحبًا، معكم بيتر توماسن. أنا أيضًا عضو في SSAC، وأشعر أن بعض ما قيل يمكن إعادة صياغته بطريقة أقل تقنية. وهذا ما سأحاول فعله. قال روس سابقًا إن التوقيعات تُرفق بردود DNS وتشهد بأن معلومات DNS لم يتم تغييرها منذ نشرها. الآن، بالطبع، إذا تمكن أي شخص من إرفاق توقيع، فلن يكون ذلك مفيدًا للغاية.

لذا، لإرفاق توقيع، تحتاج فعليًا إلى التحكم في مفتاح خاص، وتحتاجه لحساب التوقيع. لذا، فإن التهديد من الحوسبة الكمّية يكمن في استخراج هذا المفتاح بطريقة ما، حتى لو لم يكن لديك الإذن بذلك، مما يسمح لك بتزوير تلك التوقيعات.

الآن، تطبيق آخر للتشفير هو التشفير نفسه، الذي يحمي البيانات السرية ويجعلها غير قابلة للقراءة ما لم يكن لديك مفتاح فك التشفير. لذا فهذا أيضًا تطبيقًا للمفاتيح. ومن المهم أن ندرك أن الحوسبة الكمومية تهدد كلا التطبيقين، سواءً إنشاء التوقيعات باستخدام المفاتيح السرية أو أيضًا فك التشفير بالتشفير. لكن هذه حالات استخدام مختلفة، وDNS لا يهتم بالتشفير وفك التشفير. بل يهتم بالتحقق عندما تحاول الاتصال بمكان ما وإجراء استعلام DNS عما إذا كان التوقيع الذي تتلقاه صالحًا أم لا.

لذلك، إذا كنت تريد كسر ذلك باستخدام حاسوب كمّي، فيجب أن تفعل ذلك في وقت قصير جدًا، أي في الوقت الفعلي تقريبًا. بينما إذا كان لديك بيانات HTTPS مشفرة محفوظة، يمكنك قضاء خمس سنوات في فك تشفيرها إذا كنت ترغب في ذلك. لذا، إذا كان لديك حاسوب كمومي مفيد ولكنه بطيء، فسوف يهدد بياناتك المشفرة، لكنه لن يهدد معلومات DNSSEC، لأنه إذا استغرق الأمر خمس سنوات لتزوير التوقيع فلن يكون ذا فائدة، حيث لن يكون أحد مهتمًا باستجابة DNS بعد هذا الوقت، أليس كذلك؟ لأن الاتصال يستغرق بضع ثوانٍ فقط.

الخلاصة هي أنه بالنسبة للحكومات، والتي أعتقد أن هولندا سألت عنها، فيما يتعلق بـ DNSSEC، لا داعي للقلق. إنها حاليًا مشكلة بحثية. ومن الجيد متابعتها إذا كنت مهتمًا. لكن المشكلة الأكثر إلحاحًا هي حماية البيانات السرية المخزنة أو المنقولة، والتي تواجه نفس مشاكل استخراج المفاتيح، ولكنها أكثر إلحاحًا، وهناك أيضًا تقدم أكبر في هذا المجال مقارنة بمجال DNSSEC. نعم، هذا كان ملخصًا أردت توضيحه.

نيكولاس كاباليرو شكرًا جزيلًا.

روس هاوسلي شكرا لك على رئاسة الجلسة الأسبوع المقبل.

رام موهان شكرًا يا نيكو. أود أن أقدم لك ولـ GAC عرضًا، إذا كان من المفيد الحصول على نوع من الدليل السريع أو التمهيدي في هذا المجال، فيرجى مراسلتنا، وسنساعد في توفير بعض المواد التي قد تكون مفيدة لأعضائكم عند التعامل مع حكوماتكم. لأنني أعتقد أن هناك تمييزًا مهمًا يجب فهمه ونقله إلى الآخرين في حكوماتكم بشأن الفرق بين مخاطر الحوسبة الكمّية على DNSSEC ومخاطرها على الأسرار المشتركة.

نيكولاس كاباليرو شكرًا جزيلًا على مداخلتك. رام، شكرًا لك يا روس. لست متأكدًا تمامًا من الإطار الزمني الذي ذكرته عن الخمس سنوات. نسيت اسمه. بيتر، لكن شكرًا على التوضيح. أعتقد أننا قد نواجه، وآمل ألا نواجه، مفاجآت في المستقبل القريب. على أي حال، قبل أن أعطي الكلمة لجيف، هل لدينا أي أسئلة أخرى في القاعة أو عبر الإنترنت؟ ولا أرى أي يد مرفوعة. لذا، شكرًا جزيلاً لك روس. لننتقل إلى بند آخر. وفي هذه المرحلة، سأعطي الكلمة لجيف، الكلمة لك.

جيف بيدسر

شكرًا يا نيكو. أنا جيف بيدسر من SSAC. طُلب منا مناقشة دراسة INFERMAL. الشريحة التالية من فضلك. شكراً لك. دراسة INFERMAL هي دراسة أعدها OCTO مكتب المدير التقني في ICANN، كجزء من أبحاثهم. لديهم باحثون أكاديميون يدرسون تسجيلات النطاقات الخبيثة المستخدمة في الأضرار والإساءات عبر الإنترنت، وخصوصًا التصيد الاحتيالي.

إحدى النقاط التي يجب التأكيد عليها، وقد وضعتها بخط عريض في الفقرة الثانية، هي أن هذا التقرير لا يقدم حلولاً، بل هو تقرير مصمم للإجابة عن الأسئلة التي طرحها المجتمع منذ فترة طويلة حول تأثير بعض العوامل على أماكن حصول مجرمو الإنترنت على نطاقاتهم لهذه الأغراض الضارة. يسلط التقرير الضوء على الحوافز الاقتصادية، والتحقق الاستباقي، وبعض القيود الصارمة في الحد من إساءة استخدام النطاقات باعتبارها الأساليب المتبعة حاليًا وفقًا لحالة البحث وقت إصدار التقرير في نوفمبر الماضي.

إذن، بعض النتائج الرئيسية لمن لم يقرأ التقرير، الحوافز الاقتصادية: كل انخفاض بمقدار دولار واحد في رسوم التسجيل يقابله ارتفاع بنسبة 49% في عدد النطاقات الضارة، توفر الخدمات المجانية، مثل الاستضافة، يؤدي إلى زيادة معدلات الانتهاك بنسبة 88%. الخصومات على تسجيل النطاقات ترتبط بزيادة كبيرة في عمليات التسجيل الضارة. وفيما يتعلق بالإجراءات الاستباقية، فإن فرض قيود صارمة على مشتري النطاقات يمكن أن يقلل من الانتهاكات بنسبة 63%.

الوصول إلى واجهات برمجة التطبيقات (API)، التي تتيح شراء أعداد كبيرة من النطاقات دفعة واحدة، قد يؤدي إلى زيادة بنسبة 401% في عمليات تسجيل النطاقات الضارة. وبالطبع، فإن عمليات التحقق، التحقق الاستباقي من معلومات المسجل، مثل التحقق من البريد الإلكتروني ورقم الهاتف، يقلل بشكل كبير من عمليات التسجيل الضارة. الشريحة التالية من فضلك.

أما بالنسبة للإجراءات التفاعلية، فإن تأثير فترات التخفيف على الحد من إساءة استخدام النطاقات ضئيل. حتى الفترات القصيرة التي يكون فيها النطاق نشطًا يمكن أن توفر للمهاجمين بيانات اعتماد قيمة وأرباحًا مالية. أما بالنسبة لتفضيلات المسجّلين وأسماء النطاقات العليا (TLDs)، فإن عمليات التسجيل الضارة ليست موزعة بالتساوي، بل تتركز

في بعض المسجّلين وأسماء النطاقات العليا. كما أن ممارسات بعض المسجّلين، مثل تقديم الأسعار المنخفضة والخدمات المجانية، تجذب عمليات التسجيل الضارة بشكل أكبر.

هذه المعلومات مؤكدة ومعروفة منذ فترة طويلة في مجتمعات مكافحة إساءة الاستخدام. المسألة ببساطة هنا تتعلق بالجوانب الاقتصادية. المشترون يتجهون إلى أقل الأسعار. ويذهبون الأماكن التي يمكنهم فيها شراء كميات كبيرة. أعتقد أن هذا ينطبق على معظم دول العالم، حيث توجد كيانات كبيرة تبيع بالجملة لجميع أنواع المنتجات والسلع بأقل سعر. لذا، بينما تعكس البيانات هذا الواقع، فإنها لا تقدم بالضرورة حلًا للمشكلة، لأنه حتى لو رفعت الحد الأدنى للأسعار، سيظل هناك سعر أقل متاح. إلا إذا تم تثبيت الأسعار عالميًا عبر جميع الاقتصادات والعملات المختلفة، فلن يتم القضاء على المشكلة.

بالإضافة إلى ذلك، تتراوح تقديرات الخسائر السنوية بسبب الجرائم الإلكترونية من 1 تريليون دولار إلى 10 تريليونات دولار. أعلم أن هناك فارقًا كبيرًا بين الرقمين، لكن حتى تريليون دولار هو رقم يصعب تخيله. الفرق بين 1 تريليون و10 تريليونات كخسائر هو رقم ضخم جدًا. معظم الدراسات تشير إلى أن متوسط الخسارة لكل هجوم تصيد إلكتروني لكل ضحية يبلغ 136 دولارًا على مستوى العالم. لكنه يصل في الولايات المتحدة إلى 3500 دولار لكل ضحية.

لقد رأيت اختلافات في هذه الأرقام، ومن المؤكد أن معظم الأشخاص العاملين في مجال مكافحة إساءة الاستخدام يدركون أنها تختلف حسب الدراسة والمصدر. لكن الحقيقة هي أنه إذا كان الحد الأدنى لكل خسارة هو 136 دولارًا، فما هو السعر الذي يجب فرضه على تسجيل النطاقات لجعل العملية غير مجدية اقتصاديًا للمحتالين، في حين أنهم يجنون مبالغ كبيرة من الجرائم الإلكترونية؟ هذا أمر يجب التفكير فيه عند البحث عن السياسات والتغييرات اللازمة للحد من تسجيلات النطاقات الضارة المستخدمة في الجرائم الإلكترونية لسرقة الأموال من الناس.

فهل رفع السعر من 2 دولار إلى 10 دولارات سنويًا سيغير دافع المجرم لتحقيق أرباح بمئات الآلاف من الدولارات؟ أطرح هذا كمسألة للنقاش. بالنسبة لعمليات التحقق، وكما أشرت سابقًا، نُشرت الدراسة في نوفمبر واستندت إلى البيانات المتاحة آنذاك. قضايا الذكاء الاصطناعي تتسارع الآن بوتيرة تتجاوز حتى تطور الحوسبة الكمية.

أصبح من الممكن الآن إنشاء هويات رقمية مزيفة باستخدام الذكاء الاصطناعي، حيث يمكن توليد رخصة قيادة بتنسيق دقيق لأي بلد معين، مع اسم حقيقي لشخص من فئة عمرية محددة، وربما مع صورة مزيفة أو صورة الشخص نفسه. يمكن استخدام هذه الهويات المزيفة لتسجيل النطاقات، مما يجعل من الصعب الاعتماد على عمليات التحقق من هوية جميع المسجلين كحل نهائي للمشكلة.

القدرة على كشف الهوية الحقيقية من المزيفة، عندما يكون شخص حقيقي مع صورة مزيفة أو صورة مشابهة، في مستوى، حسنًا، ستحتاج لاستخدام الذكاء الاصطناعي لمكافحة ذلك، لأنه لا يمكن الاعتماد على التحقق البشري فقط عند هذا المستوى وبهذه السرعة المطلوبة. لذا ما هي أفضل العمليات التي سوف تساعد في الحفاظ على النطاقات من التسجيل باحتيال غير عمليات التحقق اليدوية؟

هناك أيضًا مسألة معدلات الكشف من التفويض وحتى اتخاذ إجراءات التخفيف. هل هذا قياس صحيح؟ ما أقترحه هنا هو أن معظم الدراسات التي أُجريت تعتمد على المصادر المتاحة علنًا حول حجم إساءة استخدام نظام أسماء النطاقات DNS. ولا تفهموني خطأ، فهناك أعداد هائلة جدًا، هذه الأرقام هائلة وصادمة. لكنني أود أن أطرح أن المشكلة الأكبر في إساءة استخدام DNS، وخاصة التصيد الاحتيالي، هي أنه يعتمد على أن تكتشفه الجهات المعنية، أو أن تقع ضحية له، أو يُحاول استهدافها، ثم تقوم بالإبلاغ عنه.

ما ننظر إليه الآن في معظم التقارير حول هذا الموضوع هو الأضرار المُبلَّغ عنها. كم شخصًا في هذه القاعة تلقى رسالة تصيد عبر الهاتف أو البريد الإلكتروني، نظر إليها، ثم قال: "لن تخدعني هذه المرة"، وقام بحذفها؟ إذا كان هناك شخص يبلغ عنها دائمًا، فأنا أشيد به. لكنني لا أتوقع رؤية أيادي مرفوعة. هناك حجم كبير من هذه الأضرار غير مُبلَّغ عنه. وإذا لم يتم الإبلاغ عنها، فإنها تظل غير مرئية لنا، وبالتالي لا يمكن معالجتها.

لذلك، تغيير منهجيات تسجيل النطاقات قد يكون حلاً أو مسارًا يمكن اتباعه، لكن الأهم هو إيجاد طرق أفضل للكشف عنها بحيث يتم التخفيف منها بسرعة. إذا تم تشغيل نطاق لمدة 6 أو 7 ثوانٍ قبل أن يتم اكتشافه وإيقافه، فهذا أفضل من أن يبقى لمدة يومين قبل أن يُبلَّغ عنه، ثم يستغرق يومين آخرين للتحقق منه، ثم يتم إسقاطه. كم عدد الضحايا الذين وقعوا في الفخ خلال تلك الفترة التي امتدت لأربعة أيام مقارنة بما لو تم اكتشافه وإزالته بشكل أسرع؟ والنقطة الأخرى المتعلقة بالقياس، وهي مسألة صعبة بطبيعتها، ليست فقط عدد

النطاقات المستخدمة في التصيد، بل عدد الضحايا لكل نطاق حيث يمكن أن يقع مائة شخص ضحية خلال ثانية واحدة إذا كان التصيد مُتقنًا بما فيه الكفاية.

إذن، القضية ليست في عدد النطاقات التي تقوم بالتصيد وحدها، بل في عدد الضحايا الذين يقعون فيها، لأن ذلك هو المقياس الحقيقي لحجم المشكلة. ونحن نعلم بالفعل أن الحجم الذي نراه في المصادر المتاحة علنًا يشير إلى وجود ملايين النطاقات المستخدمة في التصيد، لكننا ندرك أيضًا أن هناك المزيد من الحالات التي لم يتم الإبلاغ عنها، وبالتالي لا نراها، كما أننا لا نقيس التأثير الحقيقي من حيث عدد الضحايا والخسائر المالية العالمية الناتجة عن ذلك.

لذلك، أطرح هذه النقاط للنقاش والتفكير حيث أن تقرير INFERMAL قدم لنا تأكيدًا جيدًا على ما كنا نعرفه دائمًا، نعم، دائمًا نعرف أن الأسعار المنخفضة تشجع هذا النوع من النشاط، كما نعرف أن ضعف التحقق من المسجلين يسهل هذا النوع من الإساءات. تم إضافة صدى للتأثير. لكن الآن، كيف نخطو إلى الأمام؟ كيف يمكننا القيام بذلك بشكل أفضل؟ كيف يمكننا قياس التأثير بشكل أفضل وتحسين أساليب الكشف بحيث نصبح أكثر فاعلية في إيقاف المشكلة؟

لأنني أعتقد أنه حتى لو بدأنا في فرض رسوم قدرها 1000 دولار لكل نطاق سنويًا، فإن ما سنفعله في الواقع هو حرمان معظم الناس حول العالم من القدرة على تسجيل نطاق بسبب التكلفة، بينما لن نغير شيئًا بالنسبة لمجرمي الإنترنت، الذين يكسبون ما لا يقل عن 20,000 دولار لكل نطاق من عمليات الاحتيال التي يقومون بها، لذلك لن يأبهوا شيئًا للزيادة في التكلفة. لن يمانعوا في زيادة التكلفة لأنها ستؤثر قليلًا فقط على هامش ربحهم، لذا علينا العثور على حلول أخرى هنا. ولكم جزيل الشكر.

نيكولاس كاباليرو

شكرًا لك، جيف. حسنًا، كان هذا بالضبط ما كنت أقصده. الشريحة التالية من فضلك، نعم. الآن، دعونا نناقش مسألة الزيادة بنسبة 400%، وبالنسبة لواجهات برمجة التطبيقات (APIs)، ما رأيكم في هذا الأمر؟ هل المشكلة الحقيقية أن المجرمين لديهم إمكانية الوصول إلى API، ويستخدمون الذكاء الاصطناعي أو أي تقنيات أخرى لزيادة أنشطتهم الاحتيالية؟ هل هذا هو السبب الرئيسي؟

جيف بيدسر نيكو، ليس لدي أدنى شك في أن تسجيل أعداد كبيرة هو وسيلة سيئة للحصول على عدد كبير من النطاقات للاستخدامات الضارة. لكن مسألة الزيادة بنسبة 400% أو بالأحرى 401% يمكن أن تكون مضللة. إذا كان هناك مجرم واحد يستخدم خوارزميات توليد النطاقات (DGAs) لإنشاء نطاقات لخدمة شبكة بوت نت أو حملة برمجيات خبيثة، فقد يقوم بتسجيل 10,000 نطاق دفعة واحدة. وهذا لا يعني أن API هو المشكلة، لأن هذه النسبة يمكن أن تكون ناتجة عن مستخدم واحد من بين جميع المستخدمين الذين يستفيدون من API. ومن الجانب الآخر، هل يجب أن تكون هناك قيود أو "مكابح"، إذا جاز التعبير، بحيث عندما يقوم شخص ما بتسجيل 50 نطاقًا، سيكون هناك توقفًا مؤقتًا للتحقق مما إذا كانت هذه النطاقات تبدو وكأنها ستُستخدم في أنشطة ضارة؟ هناك الكثير من المعلومات والبنية التحتية التي يمكن الاستعانة بها لتحليل ذلك.

لذلك، نعم، تسجيل 10000 نطاق دفعة واحدة أمر غير مقبول، لكن المشكلة ليست في واجهات برمجة التطبيقات (API) نفسها. بل المشكلة في الوصول غير المقيد إلى تلك الواجهات.

نيكولاس كاباليرو شكرًا لك، جيف. لذا، اسمحوا لي أن أفتح المجال للتعليقات أو الأسئلة من أعضاء GAC سواء في القاعة أو عبر الإنترنت. الكلمة مفتوحة، لا أرى أي أيدي مرفوعة في الغرفة. عفواً، معذرة، نعم، هناك يدان مرفوعتان. لدينا ممثل الهند ثم ممثل أستراليا. ممثل الهند، تفضل رجاءً. شكراً لك.

سوشيل بال شكرًا لك، جيف. أعتقد أنه من الواضح أن التحقق يمثل مشكلة، أليس كذلك؟ إذا كان لدينا بيانات اعتماد موثوقة للمسجلين، فإن احتمالية إساءة استخدام DNS ستنخفض بشكل كبير، أليس كذلك؟ وهذا ينعكس أيضًا في استخدام خوارزميات DGA، حيث إن المشكلة ليست في الذكاء الاصطناعي نفسه. بل في بيانات الاعتمادات غير الموثوقة التي يتم مشاركتها عبر واجهات برمجة التطبيقات بالجملة، أليس كذلك؟

نوعًا ما، أعتقد ربما، على الرغم من أن المشكلة واضحة تمامًا، ولكن، لكننا ما زلنا نناقش مع GNSO كيفية تحديد دقة البيانات وما هو نطاق هذه البيانات، لأنه إذا لم نحدد نطاق دقة بيانات WHOIS، فلن نتمكن أبدًا من الانتقال إلى التحقق الفعلي، أليس كذلك؟ فهل يمكن لمجموعتي GAC أو SSAC الضغط على GNSO للإسراع في هذه العملية؟ أعني، لانه كما تعلمون، حتى الآن نحن نتحدث فقط، جميعنا نعرف المشكلة، دون اتخاذ خطوات فعلية لاحتواء المشكلة.

جيف بيدسر هناك نقطة لم أذكرها أثناء العرض التقديمي، ويجب أن أوضحها الآن، وهي أن الأشخاص الذين نحاربهم في هذا المجال، الأشخاص الذين يستخدمون النطاقات لهذا الغرض متقدمون علينا بعشر خطوات، بل بمئة خطوة. بدأ اتجاه جديد في الظهور، حيث يقوم أشخاص شرعيون بإنشاء حسابات حقيقية وبناء محفظة من النطاقات على مدى عدة أشهر، ثم يقومون ببيعها لاحقًا مع بيانات اعتمادها إلى مجرمين، الذين يستخدمونها في أنشطتهم الاحتيالية.

لذلك، رغم أن تعزيز عمليات التحقق والاعتماد سيكون مفيدًا بالتأكيد، إلا أن الاعتماد على ذلك وحده كحل هو أمر إشكالي. وهناك أيضًا مسألة أخرى، وهي أننا في جلسة علنية الآن، وأنا متأكد من أن الأشخاص الذين نحاربهم يشاهدون هذا الاجتماع، ليروا ما الذي نعرفه؟ لمعرفة ما نعرفه بالفعل عن أساليبهم وما يقومون به، حتى يتمكنوا من التكيف واتخاذ خطواتهم التالية.

لذا سؤالك حول نقل النقاس للمجموعات الصحيحة، وماذا بعد؟ أعتقد أن الأمر يرجع إلى النقطة التي أثرتها سابقًا، وهي، كما تعلمون، العودة إلى النقاط السابقة، في الشريحة السابقة، وهي تحسين عملية الكشف. يجب أن يكون التركيز على تحسين عمليات الكشف والتسريع في آليات التخفيف، لأننا لن نتمكن من القضاء على الحوافز الاقتصادية لارتكاب الجرائم. لقد حاول البشر تقليل الدوافع الاقتصادية للجرائم عبر التاريخ، ولم ينجح ذلك تمامًا.

الجريمة ستظل موجودة دائمًا، لكن إذا استطعنا ضبط عمليات الكشف بحيث يتم اكتشاف المخالفين وإيقافهم قبل أن يتمكنوا من استغلال الضحايا، أو على الأقل تقليل عدد الضحايا، فإن الدافع لارتكاب الجريمة سيقل، لأن هناك جرائم أخرى قد تكون أكثر ربحية للمحتالين. لذا، لا أدري إن كانت هذه نقطة جيدة، إن كانوا يقومون ببعض الجرائم، ولكن، يمكنكم

تحسين معدلات الكشف عن الجرائم وتخفيف أضرارها فهذا سيساعد كثيرًا في هذه المشكلات.

سوشيل بال

أعني، أنا لا أقلل من أهمية الكشف، فهو بالتأكيد الهدف النهائي. لكن عندما أتحدث عن التحقق، لا أقصد أنه الحل الشامل، لكنه الخطوة الأولى، أليس كذلك؟ ونحن حتى الآن لم نتخذ أي خطوات فعلية في هذا الاتجاه، فنحن نتحدث فقط، لكننا لم نتخذ خطوة فعلية، ولو حتى للوصول لأي مكان في عملية التحقق حتى الآن، خاصة في نطاقات gTLD أليس كذلك؟ لا نواجه هذه المشكلة في ccTLD التي نديرها.

يمكنني مشاركة تجربتنا في بلدي، حيث قمنا بتطبيق عملية تحقق ثنائية العوامل، ونتيجة لذلك انخفض عدد حالات إساءة الاستخدام بشكل كبير. أتمنى أن يتم تعميم هذه الإجراءات عالميًا. بالتأكيد، سيشكل ذلك عبئًا ماليًا إضافيًا على المسجلين، لكنه لا يقارن بالخسائر الهائلة التي نتكبدها جميعًا بسبب هذه الهجمات الإلكترونية، والتي قد لا نشعر بتأثيرها المباشر. لكنها تؤثر على المواطنين الذين نمثلهم، لذلك من المهم أن ندرك أن هذه هي الخطوة الأولى. دعونا نتخذ الخطوة الأولى ولا نقلل من أهمية تحسين أدوات الكشف والمراقبة.

نيكولاس كاباليرو

شكرًا جزيلًا. لدي الهند، واستراليا والمفوضية الأوروبية والمملكة المتحدة، وهولندا. تفضل ممثل استراليا.

إنغرام نيبلوك

معكم إنجرام نيبلوك من أستراليا. كنت أتساءل عن الخطوات التالية المتعلقة بأبحاث INFERMAL. هناك قيد واضح مذكور في التقرير، وهو أن هذا ليس ما يفعله المجرمون. إنها فقط خصائص المسجلين التي كانوا ينظرون إليها. لكن كنت أتساءل، هل هناك أي جهود للتحقق من هذه الفرضيات من خلال التواصل مع المسجلين أنفسهم؟ أعني، باستخدام بيانات النطاقات المحظورة التي تم استخدامها في البحث، هل هناك محاولات لجمع بيانات على نطاق أوسع حول ما يستخدمه الأشخاص المسيئين في هذه الحالات بناء على البيانات

التي لدى المسجلين. هل هذا نوع من، نعم، كنت أتساءل فقط عن الخطوات التالية للبحث الفعلي نفسه.

جيف بيدسر نعم، سيتعين علي إحالتك إلى مكتب المدير التقني CTO لهذه الأسئلة، حيث أعرف كتبة التقرير وخطواتهم التالية. في أفضل الأحوال، يمكنني أن أنقل لك بعض الأحاديث غير الرسمية من المناقشات. وهذا ليس الجواب المناسب الذي يجب أن أقدمه لك. إذن، نعم.

نيكولاس كاباليرو شكرًا لممثل أستراليا. المفوضية الاوروبية؟

جيما كاروليلو شكرًا جزيلاً لك، نيكولاس. معكم جيما كاروليلو من المفوضية الأوروبية. زميلتي مارتينا باربيرو هي المسؤولة عن موضوع إساءة استخدام نظام أسماء النطاقات DNS وقد أشارت إليه بالفعل في الدردشة. سنعرض التقرير في جلسة إساءة استخدام DNS مع مشاركة OCTO أيضًا، لذا قد نحيل بعض الأسئلة إليهم. لكن لدي سؤالان.

السؤال الأول، سؤال عام بشكل أكبر، وهو أنه نظرًا لأن تقرير INFERMAL لاقى صدى واسعًا، ونحن نسمع بعض ملاحظاتكم حول بعض الجوانب، فهل لديكم أي بيان أو تعليقات على التقرير يمكننا الوصول إليها لرؤية نقاط الإساءة أو بعض النقاط المحددة في التقرير، لأن هذا سيساعدنا أيضًا في قراءة الوثيقة. والسؤال الثاني، أفهم أن واجهات برمجة التطبيقات API ليست مشكلة بحد ذاتها، فهذا ينطبق على أي شيء في التكنولوجيا. لكن نظرًا لأن التسجيل يتم بأعداد كبيرة، فهذا يمثل مشكلة، فإن ما يمكن أن نستخلصه من ذلك هو أنه ينبغي فرض قيود على استخدام واجهات برمجة التطبيقات؟ ولكن هل من الممكن أن نعتمد ذلك كممارسة لمنهج واضح فيما يتعلق بالتسجيلات بالجملة؟ شكراً لك.

جيف بيدسر بالنسبة للجزء الأول من الإجابة، لا، هذه النقاط والتعليقات لا تستند في الوقت الحالي إلى وثيقة إجماع من SSAC في الوقت الحالي، ولكن يمكننا من حيث المبدأ أن نعيدها إلى

القيادة للنظر فيما إذا كان بالإمكان التوصل إلى إجماع بشأن بيان أو وثيقة يمكننا قراءتها في إطار INFERMAL وتحديد ما ينبغي أن تكون عليه الخطوات التالية، ويبدو أن هذا بالفعل أمر يستحق المتابعة. أعتذر، لقد نسيت السؤال الثاني الآن.

لكن شخصيًا، أعتقد أنني أستطيع تصور حالات تكون فيها هناك فرصة مشروعة، مثل عندما تقوم شركة بإنشاء علامة تجارية جديدة أو هوية جديدة، وقد تحتاج إلى تسجيل تلك الهوية عبر العديد من نطاقات المستوى الأعلى (TLDs)، وقد يصل ذلك إلى 2000 تسجيل في ذلك الوقت، وفي مثل هذه الحالة، يمكن اعتبار استخدام تلك الأدوات لغرض مشروع. ولكن يصعب عليّ أن أرى أن أي عدد يتجاوز هذا يمثل حجمًا معقولًا للتسجيلات الجماعية. ومع ذلك، قد تكون هناك حالات تجارية لا أعلم بها. ولكن أعتقد أنه، على سبيل المثال، كما قال الزميل من الهند، هناك قواعد للحصول على رخصة قيادة دراجة نارية.

وهناك قواعد أخرى لقيادة سيارة، وقواعد مختلفة تمامًا لقيادة شاحنة نقل ثقيل. يجب أن تحصل على ترخيص مختلف بناءً على قدرتك على التسبب في الأذى للآخرين عند قيادة تلك المركبة بشكل سيئ. إذا كان يجب استخدام هذه الأداة وأن تكون متاحة للناس، فأعتقد أن واجهة برمجة التطبيقات ذات الحجم الكبير تشبه إلى حد كبير شاحنة نقل ثقيلة أو قطارًا، حيث يجب أن تخضع لعملية تحقق أكثر صرامة حول هويتك وأغراضك التجارية قبل أن تتمكن من الوصول إليها. إذن، المشكلة ليست في الأداة نفسها، بل فيمن يُرخص له باستخدام هذه الأداة.

نيكولاس كاباليرو شكرًا جزيلًا. لدي المملكة المتحدة بعد ذلك.

نايجل هيكسون عفوًا، نايجل هيكسون، المملكة المتحدة. لقد كان من المثير للاهتمام للغاية وضع هذا التقرير المهم في سياقه، وأشكر SSAC على النظر في هذا الأمر. كنا دائمًا نعلم أنكم ستفعلون ذلك. كنت أتساءل فقط، أعني، أعلم أنه لا يزال مبكرًا ربما، ولكن هل يمكن أن يتحول هذا لاحقًا، وفقًا لنقاشاتكم، إلى نوع من التوصيات نظرًا لأهمية تلك التوصيات التي تصدرونها من حين لآخر. شكراً لك.

رام موهان شكرًا لك، نايجل. لم نصل بعد إلى تلك المرحلة لنحدد أو نقرر ما إذا كان ينبغي علينا إصدار توصية بشأنه. لقد قدمت OCTO عرضًا تقديميًا لـ SSAC حول هذا الموضوع أيضًا. ولكن ما لم نقم به هو النظر في هذا والتساؤل: هل هناك شيء إضافي يمكن القيام به؟ جزء من الأمر يعود إلى أن بعض العمل الذي قد يحتاج إلى الحدوث هنا قد يقع أكثر ضمن نطاق وضع السياسات في ICANN بدلًا من كونه استشارة تقنية.

لقد قدم تقرير INFERMAL الكثير من المشورة التقنية. لكن هذه مجرد أفكاري، ولم نجرِ مناقشة محددة داخل SSAC حول هذا الأمر. لكن شكرًا لك على الاقتراح، وسنطرحه في محادثتنا القادمة داخل SSAC لمعرفة آراء الأعضاء.

نيكولاس كاباليرو شكراً لك. رام، لديّ ممثل هولندا التالي. شكراً لك.

ماركو هوغوونينغ أتحدث ممثلاً عن هولندا مرة أخرى. اسمي ماركو للتسجيل. رام، لقد أثرت نقطة ممتازة هناك. أعتقد أنه من حيث الحد من الانتهاكات، فهذه مشكلة سياسات بشكل كبير. مع ذلك، اسمع جيف يتحدث عن تحسين الكشف عن الانتهاكات وغيرها، على سبيل المثال، واجهات برمجة التطبيقات. لذا، أتساءل، خارج مناقشات السياسات، هل هناك مجال، على سبيل المثال، لتحسين المعايير التقنية للكشف عن الانتهاكات أو سلوك واجهات برمجة التطبيقات لحل جزء من هذه المشكلة؟ هل هناك مجال للحلول التقنية؟

رام موهان شكرًا. سأتحدث باختصار، وجيف ربما يمكنك أيضًا المشاركة. لا أعتقد أن هناك حلًا تقنيًا بالضرورة، ولكن أعتقد أن هناك عنصرًا تعليميًا فيه. عندما تتعرض للتصيد الاحتيالي، أو الهجمات الإلكترونية، هل تعرف ماذا تفعل؟ ليس فقط كيفية اكتشافه، ولكن كيفية الإبلاغ عنه؟

لأن أحد المشكلات في هذه المرحلة، وفي مجتمعنا بالتأكيد، هي أنه إذا لم يتم الإبلاغ عنها، فلن يكون لدينا بيانات كافية تم جمعها لتخبرنا بأنه تم الإبلاغ عن ألف حالة، وألف حالة

أخرى، و10% منها لم يتم الرد عليها على النحو المطلوب، ثم دعونا ننظر في هذه النسبة، أو أيًا ما كانت النسبة، دعونا ننظر إلى من يقف وراء ذلك، ونعمل على تحليل الأنماط ونفهم من قد يكون وراء هذه التهديدات، لمحاولة فهم بعض السلوكيات والخصائص التي قد تكون داخل نظامنا البيئي.

لذلك، يمكننا القيام بإجراء عملي وهو بناء حملة توعوية قوية تقول: أبلغوا عن الإساءة، أبلغوا عن التصيد، أبلغوا عن هذه القضايا. وبعد ذلك يمكننا تتبع ما يحدث لاحقًا بعد ذلك. يمكننا عندها الحصول على بيانات توفر تركيزًا حقيقيًا على أماكن المشكلات، أو من قد يكون مساهمًا في حدوث المشكلات.

في الوقت الحالي، نحن، في رأيي، نحاول غالبًا تطبيق نهج شامل لهذه القضايا ونقول: دعونا نُنشئ سياسة جديدة تنطبق على الجميع، أو دعونا نُصوّر مجموعة كاملة من الجهات الفاعلة بطريقة معينة، بينما قد يكون هناك جهات ضمن هذه المجموعة تقوم بعمل ممتاز، وأخرى تقوم بعمل سيئ للغاية.

وأعتقد أن تركيزنا يجب أن يكون على أولئك الذين لا يرتقون إلى المستوى المطلوب. وبمجرد أن نحصل على تلك البيانات، يمكننا القول: هذه هي أفضل الممارسات، وهذه هي المعايير التي يجب اتباعها، أليس كذلك؟ وأعتقد أن أفضل الممارسات يمكن تنفيذها دون وضع سياسات، لأنك حينها تقول: هذا ببساطة شيء جيد من أجل صحة رقمية أفضل، ومن أجل نظام بيئي أفضل. ليس لدي شئ لأضيفه.

نيكولاس كاباليرو شكراً لك. جمهورية الدومينيكان هي التالية.

أمبارو أرانغو حسنًا، هذه جلسة مهمة. معكم ممثل جمهورية الدومينيكان. هذا أمر تقني للغاية، ولكن اعتقد أنه جوهر ما نواجهه اليوم في دولنا. وأود أن أرى هنا، كحكومة في دولة صغيرة، كما نحن، جمهورية الدومينيكان، في النهاية، لقد ذكرت ما يتوجب علينا مقاضاته، وما الذي علينا فعله كحكومة.

أولًا، نحتاج أن نعرف ما هو الوضع في بلداننا، لدى مديري نطاقاتنا، المشغلين. أنا هنا كمُنظِّمة في قطاع الاتصالات، من مشغلينا، من جميع مراكز الأمن السيبراني لدينا، ومراكز

الاستجابة فيما يتعلق بالهجمات، لأنه في السنوات الأخيرة، كوستاريكا، على سبيل المثال، قبل عامين، مرت بوضع سيء كلفها ملايين وملايين الدولارات إلى أن دمّر نظامها الصحي.

إذًا، هذا من منظور حكومي، وربما من جانبكم لا يمكن قول ذلك بهذه الصراحة، لكن أعتقد أننا بحاجة إلى استراتيجيات. بعض التوجيهات الواضحة فيما يخص كيفية تعزيز نظام DNSSEC في بلداننا. كم عدد الأشخاص الذين يعرفون عنه؟ سواء كانوا مشغلينا أو مراكز الأمن أو سجلاتنا الخاصة. لا أعرف ما إذا كان موجودًا في بلادي أم لا. لكن كيف يمكننا معالجة مشكلة انعدام الأمان والأمن السيبراني، وهي مشكلة كبيرة بالنسبة لنا؟ أود أن أسمع ربما بعض التوصيات منكم، لكن أعتقد أن هذا يجب أن يأتي من SSAC ومن GAC، لأنه على المدى البعيد يجب أن يتحول ذلك إلى أدوات ملموسة، لأنه يتعلق بالتعليم.

إنه مكلف أن يكون لديك استراتيجية وطنية حتى نتمكن من تنظيم جميع أنظمتنا ضمن DNSSEC. لا أعلم إن كان هذا سؤالًا يمكنك الإجابة عليه، لكن الأمر محبط للغاية. وأعتقد أن لدينا أدوات يمكننا من خلالها على الأقل التخفيف من هذه التأثيرات. شكراً لك.

رام موهان

أحد التحديات التي نواجهها في SSAC هو أننا يمكن أن نوفر قدرًا كبيرًا من الخبرة والمعلومات التقنية. ما لا نفهمه جيدًا ولا نمتلكه هو ما هي احتياجاتكم، وعلى أي مستوى تحتاجون أن تُقدّم لكم المعلومات، أليس كذلك؟ لذا، أعتقد أننا بحاجة إلى التعاون، حتى نتمكن من فهم نوع المعلومات التي تودون منا توفيرها.

أحد الأشياء التي بدأنا بفعلها، هو أنه كان المعتاد أن نقوم بالعمل ثم ننشر تقارير، تقارير فنية جدًا يتراوح طولها من 10 إلى 40 صفحة. وأحد الأشياء التي بدأنا في تنفيذها هو تلخيص تلك التقارير إلى ملخصات تتراوح من 500 إلى 1000 كلمة توفر نوعًا من الإحاطة التنفيذية، إذا صح التعبير، لجوهر ما نحاول قوله في تلك الأوراق. لكن ذلك لا يزال يركز على مجالات البحث الخاصة بنا، الأشياء التي نعتقد أنها احتياجات مهمة.

لذا، ما أشجعك على فعله، وأنت تحديدًا، من فضلك تحدث إلينا. يسعدنا العمل مباشرة معك. لكن GAC بشكل عام، نرجو أن تعملوا جنبًا إلى جنب معنا لتوضيح أمرين. أولاً، أنواع المعلومات التي تفيدكم. وثانيًا، مستوى المعلومات التي تريدونها، مستوى التفاصيل

الفنية. لأن مستوى الانطلاق الافتراضي لدينا هو المستوى التقني العميق جدًا. هذا ما أجيده. لكن إذا أردتم منا أن نرتقي بمستوى الشرح، أو بمستويين، تحدثوا معنا وسنساعدكم بذلك.

نيكولاس كاباليرو شكرًا جزيلًا. أمبارو، هل هذا كل شيء؟ حسنًا. لذا، نحتاج إلى الختام. بقيت لنا دقيقة واحدة متبقية. هل هناك أي سؤال أو تعليق نهائي من GAC؟ ممثل اليابان، تفضل من فضلك. تفضل، رجاءً.

متحدث لم يذكر أسمه شكرًا جزيلاً على العرض التقديمي. أعتقد أنكم شددتم على أهمية جمع البيانات عن التصيد وبعض أنواع انتهاك استخدام DNS. وأعتقد أن هناك أنواعًا مختلفة من انتهاك استخدام DNS، ليس فقط تلك التي تُعرّفها ICANN، بل أيضًا بعض أنواع الاستخدام الخاطئ الأخرى مثل CSAM وربما انتهاك حقوق النشر، كما هو الحال في اليابان، حيث يُعدّ قرصنة المانغا قضية كبيرة ونمو اقتصادي كبير. أعتقد أن المشكلة الجذرية متشابهة، وأعتقد أنه من الضروري جمع أنواع مختلفة من انتهاك الاستخدام وبيانات الانتهاك، وربما هناك مجال للتعاون مع الحكومة لجمع البيانات. ولكن ما رأيك في ذلك؟

رام موهان أعتقد أنه موضوع مهم، ونحن مستعدون للوقوف إلى جانبكم لتقديم التفاصيل التقنية والمشورة الفنية التي يمكن أن تساعد في جانب التعاون. لكنني أعتقد أن الحل النهائي سيكون مزيجًا من الجانب الحكومي، والجانب التقني، والجانب السياسي، وإيجاد طريقة لدمجهم معًا داخل هذا المنتدى.

نيكولاس كاباليرو شكرًا جزيلًا لك يا رام. ويتوجب علينا اختتام أعمال الجلسة الآن. شكرًا لأسئلتكم. لقد كانت جلسة رائعة يا رام، كالعادة. إنه لمن دواعي سروري دائمًا وجودك هنا. حتى لو كانت هذه المحادثات تقنية بعض الشيء لبعض الأشخاص، فإننا نحاول إيصال الرسالة.

لذا، تبذل قصارى جهدك لتقديم نصائح جيدة لنا من ناحية، ومن ناحية أخرى لمساعدتنا في محاربة المجرمين.

لذا، شكرًا لك مرة أخرى. شكرًا جزيلًا. شكرًا يا روس. شكراً لك. لديك فريق رائع، رام، ونأمل أن نتمكن من عقد جلسة أخرى في براغ. شكرًا جزيلًا. تصفيق حار لأصدقائنا من SSAC. شكرًا جزيلًا. تم رفع الجلسة. أراكم غدًا في الساعة 9 صباحًا في حفل الترحيب وتوزيع جائزة التميز المجتمعي. شكرًا جزيلًا. طاب مساؤكم.

**[إنتهاء التدوين]**