AR

دان غلوك

مرحبًا بكم في جلسة اللجنة الاستشارية الحكومية بشأن الأمن والاستقرار ضمن فعاليات الاجتماع ICANN83، والمنعقدة يوم الأربعاء 11 يونيو/حزيران في تمام الساعة 07:00 بالتوقيت العالمي المنسق. يُرجى العلم بأن هذه الجلسة يجري تسجيلها وتخضع لمعايير السلوك المتوقعة في ICANN وسياسة ICANN لمناهضة التحرش. خلال هذه الجلسة، لن تُقرأ الأسئلة أو التعليقات إلا إذا قُدمت بالصورة المناسبة في مربع الدردشة بتطبيق Zoom. وستشمل الترجمة الفورية لهذه الجلسة اللغات الست للأمم المتحدة، بالإضافة إلى اللغة البرتغالية.

إذا أردت التحدث أثناء هذه الجلسة، فيُرجى رفع اليد في غرفة Zoom. عند الاستدعاء، سيتم منح المشاركين إذنًا لإلغاء كتم الصوت في Zoom. يرجى ذكر اسمك للعلم وإثبات ذلك في محضر الجلسة واللغة التي ستتحدث بها إذا كنت تتحدث لغة أخرى غير اللغة الإنجليزية وبرجاء أن تتحدث بوضوح وبسرعة معقولة للسماح بإجراء ترجمة فورية دقيقة. والآن أُحيل الكلمة إلى نائب رئيس اللجنة الاستشارية الحكومية، ماركو هوغوونينغ. شكرًا لك وإليك الكلمة.

ماركو هوغوونينغ

شكرًا لك يا دان. طاب صباحكم جميعًا. في الواقع، سأتولى إدارة هذه الجلسة، وآمل أن يكون رئيسنا الموقر، نيكو، جالسًا في الخلف مستمتعًا أثناء تناوله كوبًا من القهوة. كما تلاحظون، قمنا بتقسيم هذه الجلسة إلى قسمين. أولاً، سيأخذنا فريق اللجنة الاستشارية للأمن والاستقرار في جولة حول بعض المشاريع التي سيعمل على تنفيذها. وبعد ذلك، طلبت من كريستيان هيسلمان من مختبرات الشبكات المعرفة بالبرمجيات (SDNLabs) أن يرشدنا قليلاً حول كيفية تفاعل الحوسبة الكمومية مع الامتدادات الأمنية لنظام أسماء

	النطاقات (DNSSEC)، وذلك كمتابعة للجلسة التي عقدناها في سياتل خلال فعاليات اجتماع ICANN82. وقبل أن نبدأ، ربما نُجري جولة سريعة للتعريف بمن يجلسون خلف الطاولة. لقد سبق وأن قام دان بتعريفي إليكم. معكم ماركو هوغوونينغ ممثل اللجنة الاستشارية الحكومية عن هولندا. هل ترغب يا مارتن في الحديث والبدء بتعريف نفسك؟
مارتن أيرتسن	صباح الخير. معكم مارتن أيرتسن، وأنا عضو في اللجنة الاستشارية للأمن والاستقرار (SSAC).
وارن كوماري	معكم وارن كوماري، وأنا أيضًا عضو في اللجنة الاستشارية للأمن والاستقرار.
غريغ آرون	معكم غريغ آرون، من اللجنة الاستشارية للأمن والاستقرار.
رام موهان	معكم رام موهان. وأشغل منصب رئيس اللجنة الاستشارية للأمن والاستقرار.
كريستيان هيسلمان	معكم كريستيان هيسلمان، من مؤسسة تسجيل النطاقات الهولندية (SIDN)، السجل المسؤول عن نطاق المستوى الأعلى في هولندا، (NL.).
ماركو هوغوونينغ	حسنًا، شكرًا لكم. دون إطالة، أعتقد أنه يمكنني الآن إحالة الكلمة إليك يا رام، لبدء موضوعنا الأول: تسجيل النطاقات.

رام موهان شكرًا لك، ماركو. هل يمكننا الانتقال إلى الشريحة التالية. أردنا أن نشارككم بعض التعليقات حول موضوع الوصول إلى بيانات تسجيل أسماء النطاقات. لننتقل إلى الشريحة التالية رجاءً. ما نود التأكيد عليه مع لجنة الاستشارية الحكومية هو الهدف الذي نعمل لأجله. وأوضح في هذا الصدد رغبتنا في التأكد من أن أي سياسات تتعلق بإتاحة بيانات تسجيل النطاقات العامة (gTLD) تكون محددة بوضوح، وقوية من حيث البنية، وتلبي احتياجات مجتمع الإنترنت العالمي في التصدي للتهديدات الأمنية — هذا هو التحدي الذي نحاول معالجته.

ونرى أن الطريقة المثلى لتحقيق ذلك تكون من خلال إنشاء نظام وصول يتبع آلية منظمة وسريعة، بحيث تتم معالجة الطلبات المشروعة، وخاصة العاجلة منها، بطريقة ذات أولوية واستجابة سريعة. وينبغي أن تكون السياسات الخاصة بأوقات الاستجابة، وآلية المعالجة، وما يجب معالجته ومتى، محددة وواضحة ومتفقًا عليها داخل المجتمع. ونعتقد كذلك أنه يجب على ICANN – بصفتها المؤسسة المسؤولة – مواصلة نشر المؤشرات والبيانات المتعلقة بطلبات الوصول إلى بيانات تسجيل النطاقات.

نؤمن أن الوصول إلى بيانات التسجيل أمر بالغ الأهمية، فهو ركيزة أساسية ضمن منظومة الأمن والاستقرار. وقد قدمنا ملاحظاتنا إلى الفريق المعني بالعملية المعجّلة لوضع السياسات بهذا الخصوص، ونود أن نؤكد أن هذا المجال لا يتعارض مع متطلبات الخصوصية. ففي الوقت الذي يجب فيه مراعاة الخصوصية بشكلٍ ملائم، تظهر مجموعة من المخاوف الواضحة تتعلق بالأمن والاستقرار. لذا، نريد التأكد من أن آلية تنفيذ هذه التغييرات داخل المجتمع بحيث تأخذ بعين الاعتبار المبادئ التي استعرضناها على الشاشة. هذا كل ما أردنا قوله. نرحب الآن باستقبال أي أسئلة أو تعليقات.

ماركو هوغوونينغ شكرًا يا رام. بالطبع، أعتقد أن اللجنة الاستشارية الحكومية تتفق مع النقاط التي ذكرتها بشأن الوصول إلى بيانات التسجيل. هل وردت أي أسئلة أخرى بشأن هذا الموضوع؟ لا، يبدو أنه لا يزال الوقت مبكرًا. لا أرى أي أسئلة على Zoom، ولا أرى شيئًا من الفريق هنا. ربما يمكننا العودة إلى هذا الموضوع في نهاية الجلسة. أما الآن، ننتقل إلى الموضوع

التالي، وهو على ما أعتقد الحديث عن البرمجيات مفتوحة المصدر. مارتن، تفضل الكلمة لك؟

مارتن أيرتسن

أجل. نعمل حاليًا على موضوع قد يكون مألوفًا لبعضكم، وهو البرمجيات الحرة ومفتوحة المصدر، وهي البرمجيات التي يمكن استخدامها ومشاركتها وتعديلها ودراستها بحرية. ونركّز في هذا الموضوع تحديدًا على الدور الذي يلعبه هذا النوع من البرمجيات ضمن نظام أسماء النطاقات (DNS) العالمي. لقد لاحظنا أن هذا النوع من البرمجيات يُعتمد عليه بشكلٍ كبير، لكن لم تكن هناك دراسة موسعة متوفرة لهذا المجتمع حوله.

تتميز البرمجيات الحرة ومفتوحة المصدر تتميز بخصائص فريدة من حيث التطوير والحَوْكمة. وبينما تدور النقاشات حول العالم حول البنى التحتية والموثوقية والبرمجيات، وجدنا أنه من المفيد إظهار الدور الذي تلعبه هذه البرمجيات وخصائصها، لضمان أن يُؤخذ ذلك بعين الاعتبار عند إجراء مناقشات سياساتية. ينطوي هذا العمل على هدفين رئيسيين، وهما: رغبتنا في تسليط الضوء على هذا الاعتماد الحيوي، كما نرغب في إبراز الخصائص المميزة لهذه البرمجيات، وقد نسهم في تصحيح بعض الافتراضات العامة التي قد تكون منطقية عند الحديث عن البرمجيات التقليدية، ولكنها قد لا تنطبق على هذا النوع بالتحديد. إذًا، هذا العرض التقديمي بمثابة مقدمة تشويقية لما نعمل عليه.

لننتقل إلى الشريحة التالية رجاءً. نركّز في عملنا على أربعة مجالات رئيسية، حيث نقوم بإجراء مسح شامل لوصف الوضع الراهن، وندرس جانب تسجيل النطاقات وما يخصه من أدوات ونظم، كما نحلل جانب نظام أسماء النطاقات نفسه، أي الجزء المتعلق بنشر واسترجاع بيانات التوجيه، والذي يعكس لنا حالة النظام العالمي. علاوة على ذلك، نقوم بتحليل خصائص هذه البرمجيات، بما في ذلك نموذج تطويرها، والذي لا يتبع النماذج التقليدية المتعارف عليها في الصناعات الأخرى مثل السلع المادية أو البرمجيات التجارية. بعد ذلك، نُجري مقارنة ضمن هذا السياق لنفهم كيف تنطبق هذه الخصائص العامة على البرمجيات الحرة ومفتوحة المصدر المستخدمة على نطاق واسع في بيئة نظام أسماء النطاقات، أي تلك البرمجيات التي تهمنا تحديدًا في هذا الإطار.

يهدف الجزء الثالث من عملنا إلى توضيح الافتراضات — أي تلك الافتراضات التي لاحظنا أنها تُطبّق عمليًا لكنها في الواقع لا تنطبق على البرمجيات مفتوحة المصدر، وكذلك

توضيح المفاهيم المغلوطة الشائعة في هذا المجال. وأخيرًا، نحاول تحديد عوامل الخطر ذات الصلة التي ينبغي أخذها في الاعتبار عند وضع السياسات أو التشريعات. وهذه المخاطر لا تتعلق فقط بجوانب التطوير، بل تمتد أيضًا إلى تشغيل هذه البرمجيات في البيئات الفعلية. هذا باختصار هو نطاق العمل الذي نتناوله.

الشريحة التالية. نأمل أن نتمكن من مشاركة المزيد من التفاصيل معكم في اجتماع مسقط، حيث نعتزم نشر هذا التقرير خلال الأشهر القليلة القادمة بعد هذا الحدث. وكتمهيد بسيط، نؤمن بأن استخدام البرمجيات الحرة ومفتوحة المصدر في نظام أسماء النطاقات وتسجيل أسماء النطاقات يمثل نقطة قوة، ولكنه أيضًا ينطوي على بعض المخاطر التي يجب أخذها بعين الاعتبار. ونعتقد أننا قادرون على تقديم بعض الإرشادات في هذا السياق بشأن استخدام هذا النوع من البرمجيات. هذا كل ما لدينا لهذا اليوم، ويسعدني الرد على أي أسئلة.

ماركو هوغوونينغ

بالفعل، إنه عرض تمهيدي قصير ومختصر للغاية. هل هناك أي أسئلة لمارتن بخصوص هذا العمل؟ أنظر من حولي... أرى أن ممثل الهند قد رفع يده مرة أخرى.

ساجد.

شكرًا لك السيد الرئيس. معكم ساجد من الهند. سؤالي موجّه في الواقع إلى السيد/ رام موهان. لقد فاتنا هذا الجزء بسبب ضيق الوقت، لكن لدينا هدف مشترك يتمثل في أن تُقدَّم بيانات التسجيل خلال 24 ساعة. ولكن، لقد مرّ أكثر من 24 شهرًا ولا نزال نحاول التوصل إلى اتفاق مع ICANN بشأن الجدول الزمني، ناهيك عن الالتزام بفترة 24 ساعة. أقصد في الحقيقة أيًا كانت المدة المذكورة، فلا يوجد حاليًا أي إطار زمني محدد.

رغم أن مسألة الاستعجال قد تم التأكيد عليها مرارًا، سواءً من جانب اللجنة الاستشارية الحكومية أو اللجنة الاستشارية للأمن والاستقرار، إلا أن العملية الطويلة جعلت الأمر الآن ينقسم إلى مسارين: مسار المصادقة، ومسار السياسات. فما رأيك بصفتك رئيسًا للجنة الاستشارية للأمن والاستقرار — وربما أطرح هذا السؤال أيضًا على نائب رئيس اللجنة الاستشارية الحكومية — هل تعتقد أن إصدار بيان مشترك من اللجنتين قد يكون مفيدًا

للضغط على مجلس إدارة ICANN من أجل تحديد جدول زمني واتخاذ قرار بشأنه في أسرع وقت ممكن؟

رام موهان شكرًا لك على هذه المداخلة. نحن نتفق تمامًا على أن الطلبات العاجلة يجب أن تكون لها آلية واضحة ومحددة للتعامل معها. وأعتقد أن هناك بالفعل بعض المناقشات الجارية مع الأطراف المعنية بتنفيذ هذه التغييرات. لا يمكنني التحدث نيابةً عن جميع أعضاء اللجنة الاستشارية للأمن والاستقرار في هذه المرحلة، سأحتاج إلى التشاور مع الأعضاء، ولكننا كنا واضحين إلى حدٍ كبير في موقفنا: إذا تم تصنيف أمر ما على أنه عاجل، فيجب التعامل معه على هذا الأساس، ويجب أن تكون الاستجابات سريعة للغاية. وينبغي ألا تستغرق هذه الطلبات وقتًا طويلاً في المعالجة. إذا كان من المفيد القيام بخطوة مشتركة مع اللجنة الاستشارية الحكومية لتأكيد أهمية هذه القضية، فنحن منفتحون على ذلك، إذ نرى بالفعل أنها قضية بالغة الأهمية. وجزء من آلية حلها هو ضرورة وجود وضوح تام بأن كلمة "عاجل" تعني "عاجل" فعلاً، وليس مجرد إجراء اعتيادي ضمن الأعمال الروتينية.

ماركو هوغوونينغ شكرًا لك، رام، وأنا أتفق معك تمامًا. وكما تعلم، فإن اللجنة الاستشارية الحكومية قد ذكرت موضوع الطلبات العاجلة، على حد علمي، في آخر خمس بيانات ختامية على الأقل، حسبما أتذكر — بما في ذلك تقديم بعض المشورات ذات الصلة. فنحن بالفعل منخرطون، أو على الأقل هناك بعض زملائنا المنخرطين، في الفرق المصغرة التي تعمل على هذا الموضوع. ومن وجهة نظري، هناك تقدم حاصل بالفعل، لكنني أتفق تمامًا مع ملاحظتك — أنه بالنسبة للطلبات العاجلة، فإن وتيرة التقدم لا تعكس مستوى الاستعجال المطلوب. وأنا أرحب تمامًا بالتوافق مع رام في هذه النقطة. لذا دعونا نبقي هذا الموضوع في أذهاننا ونفكر فيما إذا كان من الممكن أن يساهم الجهد المشترك في دفع الأمور قدمًا. وأنا منفتح تمامًا لمناقشة هذا الخيار، لذا يمكننا العودة إليه لاحقًا في مرحلة ما. هل هناك أي أسئلة أخرى؟ أرى أن أحدهم يشير إليّ. نعم، راسل، عذرًا، تفضل الكلمة لك.

راسل وروبا

شكرًا لك السيد/ الرئيس، وشكرًا جزيلاً لزملائنا المحترمين من اللجنة الاستشارية للأمن والاستقرار. فأنتم تقومون بعمل رائع بالفعل، وأنا من أشد المعجبين بعمل اللجنة، فأشكركم بشكلٍ خاص على الجهود التي تبذلونها في الوقت الحالي بشأن هذا الموضوع. لدي بعض التعقيبات. أعتقد أن العديد من الدول في المناطق المهمشة تعتمد بشكلٍ كبير على البرمجيات مفتوحة المصدر، وعلى وجه الخصوص BIND، في تشغيل نظام أسماء النطاقات الخاص بها على مستوى ccTLD. وبالطبع، ومع تغيّر المشهد التقني الحالي، نحن نتطلع بشدة إلى نتائج هذه الدراسة. هل لديكم في هذه المرحلة أي معلومات أساسية يمكن مشاركتها عن الوضع الحالي، خاصةً فيما يتعلق بالتوزيع الجغرافي عبر المناطق المختلفة؟ فقط من باب التقدير والفهم العام. شكرًا لكم.

مارتن أيرتسن

شكرًا لك على هذا السؤال. سأشارككم هنا ببعض الملامح الأولية كمقدمة تشويقية. في المسح الذي أجريناه لرصد المشهد العام، حيث حاولنا جمع بيانات دقيقة حول "من يستخدم ماذا"، نعتقد — وفقًا للمسودة الحالية (التي لم تُنشر بعد) — أن العبارة التي سنستخدمها ستكون شيئًا من قبيل: "نظام أسماء النطاقات العالمي يعتمد على البرمجيات مفتوحة المصدر". إذًا، الأمر لا يقتصر عليكم فقط، بل هو واقع عالمي، ولدينا إحصائيات تدعمه. فعلى سبيل المثال، في نطاقات المستوى الأعلى لرمز البلد (ccTLD)، هناك 20 من أصل 25 من كبار المشغلين يستخدمون البرمجيات مفتوحة المصدر. وإذا أضفنا نطاقات المستوى الأعلى العامة (gTLD)، نجد أن 9 من أصل 10 من كبار المشغلين يعتمدون عليها. أما إذا نظرنا إلى نظام خادم الجذر، سنجد أن 9 من أصل 12 يستخدمون حصريًا برمجية المصادر المفتوحة المجانية (FOSS).

وأعتقد أن من أبرز القيم التي يمكن لهذا التقرير أن يقدمها، هي تسليط الضوء أمام جمهور أوسع على حقيقة قد تكون معروفة لدى العاملين في المجال التقني، وهي أن البرمجيات مفتوحة المصدر منتشرة في كل مكان. ونأمل أن تُظهر هذه المعلومات بوضوح، لأننا لاحظنا أن هناك مناطق يتم فيها تنظيم استخدام البرمجيات دون أن تُؤخذ برمجية المصادر المفتوحة المجانية (FOSS) بعين الاعتبار، وتُعامل كأمر ثانوي أو هامشي. ولأن خصائص هذه البرمجيات تختلف اختلافًا كبيرًا — سواءً من حيث أسلوب التطوير، أو مصادر التمويل، أو حتى الجهات التي تستخدمها — فقد لا يكون اتباع نفس الاستراتيجية

التقليدية معها هو الخيار الأمثل،

بل ربما لا تكون استراتيجية ناجحة على الإطلاق. أجل.

ماركو هوغوونينغ شكرًا لكم. سمعت أن ممثل ألمانيا أيضًا ينتظر دوره في قائمة المتحدثين. رودي

رودي نولد شكرًا لكم. معكم رودي نولد من ألمانيا. في البداية، كنت أرغب في طرح سؤال حول ما المشورة التي تقدمونها لواضعي السياسات؟ لفت انتباهي في شريحتك الختامية أنكم تعتزمون تقديم مبادئ توجيهية لواضعي السياسات، وقد أثرتم فضولنا بلمحة موجزة عنها. ولشغفي بمعرفة المزيد، هلا تفضلتم بذكر الخطوط العريضة لهذه الإرشادات أو المشورات التي ستقدمونها لنا — نحن المعنيين بصنع السياسات؟

ماركو هوغوونينغ حرصًا على وقت زملائي، سأوجز قدر الإمكان. تتمحور رؤيتنا المبدئية حول كشف النقاب عن بعض التصورات المغلوطة السائدة. ومن هذه التصورات، على سبيل المثال، الاعتقاد الشائع بإمكانية توظيف العلاقات التعاقدية كأداة فعالة في رسم السياسات. كأن يُقال مثلًا: "سنضع ضوابط تنظيمية لمشغلي البنية التحتية الحيوية في منطقتنا، ليقوموا بدورهم بفرض شروط على موردهم، الذين سيفرضونها بدورهم على موردهم، وهلم جرا."

قد ينجح هذا المنطق في عالم المواد المادية، وأحيانًا في مجال البرمجيات، بيد أن الأمر يختلف جذريًا حينما تكون البرمجيات متاحة للتنزيل مباشرةً من الإنترنت، إذ تنعدم حينها هذه السلسلة التعاقدية. وهنا يكمن التصور المغلوط؛ فهذه الأداة التي تبدو ناجعة نظريًا، تفشل في التطبيق العملي، نظرًا لوجود كم هائل من البرمجيات التي تطورها وتصونها فرق متخصصة، لكن نطاق استخدامها يتجاوز بكثير وجود عقود دعم أو أي أدوات تعاقدية أخرى.

من هنا، فإن مشورتنا قد تتناول هذا المجال تحديدًا، كأن نقدم أفكارًا حول كيفية التعامل مع المطورين في هذا السياق، أو حول طريقة التفكير في المسألة برمتها. وتجدر الإشارة هنا إلى أنه إذا ما فُرضت على المشغلين شروط تحول دون اختيارهم لأفضل البرمجيات المتاحة وأجودها – والتي قد تكون من هذا النوع من البرمجيات مفتوحة المصدر – فإن السياسات المرسومة قد لا تحقق أهدافها المرجوة. أعتقد أن هذا هو الإطار العام الذي سنتحرك ضمنه، ولكني بهذا أستبق الأحداث. إذ علينا أولًا أن ننشر التقرير، وبعدها يسعدني أن أعود إليكم للحديث عن هذا الموضوع باستفاضة.

ماركو هوغوونينغ

نسعد باستضافتك مجددًا بمجرد نشر التقرير، وبعدها يمكننا استكمال هذا النقاش. وأرى أن قائمة الأسئلة قد فرغت، وحرصًا على الوقت، أقترح أن ننتقل إلى آخر مواضيع اللجنة الاستشارية للأمن والاستقرار، وهو موضوع يثير اهتمامي شخصيًا، ألا وهو: "إعادة النظر في مسألة حجب نظام أسماء النطاقات". أعتقد أن غريغ سيأخذ الكلمة الآن، أليس كذلك.

غريغ آرون

حسنًا. شكرًا لك. تأتي هذه الورقة تحديثًا لورقتين سابقتين أعدّتهما اللجنة الاستشارية للأمن والاستقرار قبل نحو 12 عامًا. فحجب نظام أسماء النطاقات ليس بالظاهرة المستجدة، لكننا ارتأينا أن الوقت قد حان لإعادة النظر فيه، بالنظر إلى كثرة الأمثلة الحديثة على تطبيقه حول العالم، وما ترتب على تلك الإجراءات من نتائج ملموسة. أضف إلى ذلك ظهور تقنيات جديدة خلال هذه الفترة أثرت على آليات الحجب وقدرة المستخدمين على الوصول إلى الموارد عبر الإنترنت. وقد شارك في إعداد هذه الورقة نحو عشرين عضوًا من اللجنة، وتوليتُ مع زميلي وارن الرئاسة المشتركة للفريق.

إذن، ما المقصود بحجب نظام أسماء النطاقات؟ عندما ترغب في زيارة موقع ما على حاسوبك، فإنك تكتب عنوانه، أي اسم النطاق، فينتقل استفسارك إلى محلل نظام أسماء النطاقات. ونطلق على هذه المحللات اسم "المحللات التكرارية"، وهي غالبًا ما تكون تحت إدارة مزود خدمة الإنترنت لديكم. ثم يقوم هذا المحلل التكراري بالمساعدة على العثور على عنوان بروتوكول الإنترنت (IP) الخاص بوجهتك، مترجمًا اسم النطاق الذي

أدخلته إلى عنوان بروتوكول الإنترنت . وفي نهاية المطاف، يحدد نظام أسماء النطاقات موقع وجهتك، مما يتيح لك التواصل مع الموقع الذي قصدته.

وعادةً ما تتم هذه العملية برمتها بشكلٍ فوري، لتصل إلى مبتغاك. ولكن، يمكن للمحلل التكراري أن "يحجب" اسم نطاق معين. وهذا يعني أن المحلل سيقدم لك إجابة مغايرة للمتوقع. ويتم ذلك بإحدى طريقتين أساسيتين: الأولى، قد يخبرك المحلل التكراري بأن اسم النطاق الذي تبحث عنه غير موجود، مع أنه موجود في حقيقة الأمر. فتحاول مثلًا الوصول إلى موقع "Wikipedia"، ولكنك لا تتلقى إجابة، ولا يتم توصيلك به. أما الطريقة الثانية، فبدلاً من أن تُنقل إلى الموقع الذي تريده، يتم تحويلك وتوجيهك إلى وجهة أخرى تمامًا. بعبارة أخرى، يخبرك المحلل التكراري بشيءٍ غير متوقع، أو قد يذهب البعض إلى القول إنه "يكذب" عليك، فهو لا يمنحك الإجابة الصحيحة المسجلة في نظام أسماء النطاقات.

فعملية حجب نظام أسماء النطاقات تعتبر من الجوانب التقنية، أو يمكن القول بأن هذا المحلل عبارة عن أداة. وكأي أداة، يمكن استخدامها لغايات شتى؛ فيمكن توظيفها بحرفية وخبرة، أو بغير اكتراث، تمامًا كالمطرقة. فيمكنك استخدام المطرقة لبناء منزل، وهذا استخدام محمود. ويمكنك أيضًا استخدامها لتضرب بها رأس أحدهم، وهو شيء مذموم. فقد صُممت هذه التقنية أساسًا لمنع المستخدمين من الوصول إلى محتوى معين أو استخدام خدمة ما. ولا يقتصر تأثيرها على زيارة المواقع الإلكترونية فحسب، بل يمتد ليشمل أي استخدام لنظام أسماء النطاقات، مما يؤثر تباعًا على البريد الإلكتروني، وإدارة الشبكات، وسائر الخدمات التي تعتمد على هذا النظام.

لننتقل إلى الشريحة التالية رجاءً. لو كان محلل نظام أسماء النطاقات هي شخصية "غاندالف" — فلا بد لنا دائمًا من إشارة إلى الثقافة الشعبية هنا في اللجنة — لكان هذا ما سيقوله لكم. الشريحة التالية. يُستخدم حجب نظام أسماء النطاقات لدوافع كثيرة ومتباينة، لذا من المهم فهم هذه الدوافع. وأحد هذه الاستخدامات هو لأغراض أمنية. فالمحلِّل قد يمنع المستخدمين من... يا للمفارقة! انقطع التيار الكهربائي فجأة! فقد يُضبط محلل نظام أسماء النطاقات بحيث تمنع المستخدمين من الوصول إلى مواقع تحتوي على برمجيات ضارة أو محاولات تصيد واحتيال وما شابه. ويُعد هذا الإجراء خدمة نافعة،

ولعلنا جميعًا في هذه القاعة نحظى بحماية ما من خلال حجب نظام أسماء النطاقات. فعلى سبيل المثال، تكاد جميع متصفحات الويب اليوم تتضمن نظامًا يعرض صفحة تحذير تمنعك من الدخول إلى موقع تصيد واحتيال معروف، إلا إذا أصررت على المتابعة على مسؤوليتك. وهذا الإجراء متأصل في العديد من الأنظمة، وهو منتشر على نطاق واسع ويهدف عمومًا إلى مساعدة المستخدمين وحمايتهم، ويُطبق عادة على مستوى محلي، كأن تختار شركة ما مزود خدمة يساعدها على تعزيز أمن شبكتها الداخلية.

وبعض المستخدمين قد يستخدمها لضبط المحتوى. فعلى سبيل المثال، قد تمنع المكتبة العامة في مدينتك روادها من الوصول إلى أنواع معينة من المواقع التي يرى المجتمع المحلي أنها غير لائقة، كمواقع القمار أو المواد الإباحية، نظرًا لوجود أطفال في المكتبة. كما تطبق بعض الشركات نظام حجب نظام أسماء النطاقات داخليًا لمنع موظفيها من الانخراط في أنشطة معينة في أثناء ساعات العمل، كزيارة منصات وسائل التواصل الاجتماعي أو مواقع المقامرة. وهذا أيضًا مثال على سياسة محلية تقررها الشركة لمكان عملها.

أما الجانب الأكثر إثارة للجدل، فهو استخدام حجب نظام أسماء النطاقات لمنع الوصول إلى المحتوى، لا سيما عندما يتم الحجب على المستوى الوطني؛ أي منع مواطني بلد بأكمله من زيارة موقع معين أو الاطلاع على محتوى محدد. وهذا أحد الأسباب الرئيسية التي تدفعنا لتقديم هذه المعلومات لواضعي السياسات وأعضاء اللجنة الاستشارية الحكومية وغيرهم، لأن مثل هذه القرارات تؤثر على شريحة واسعة من الناس.

ويتم الحجب أحيانًا استنادًا إلى قانون، فبعض الدول مثلًا تمنع مواطنيها من زيارة المواقع المعروفة بنشر صور الاعتداء الجنسي على الأطفال، وذلك حمايةً للأطفال والمواطنين على حدٍ سواء. وتحتفظ هذه الدول بقوائم بأسماء النطاقات هذه وتوزعها على مزودي خدمة الإنترنت لديها. وفي أكثر الحالات إثارة للجدل، يُستخدم حجب نظام أسماء النطاقات في بعض الأنظمة لمنع الوصول إلى المحتوى الذي يعبر عن آراء سياسية، أي أنه يُوظف كأداة للرقابة.

الشريحة التالية. من المهم أن نميز بين "حجب نظام أسماء النطاقات" و"تعليق أسماء النطاقات". فكلاهما يهدف إلى منع الوصول إلى محتوى ما، لكنهما يختلفان في آلية العمل. فحجب نظام أسماء النطاقات لا يزيل المحتوى من الإنترنت؛ فحتى لو حُجِبَ عن البعض،

يظل متاحًا في متناول الآخرين. أما "تعليق النطاق"، فيسعى إلى منع الجميع من الوصول إلى المحتوى عبر تعطيل اسم النطاق نفسه ومنعه من العمل. ويتم تعليق آلاف أسماء النطاقات يوميًا لأسباب أمنية ولمكافحة إساءة الاستخدام، كمواقع التصيّد والاحتيال.

وفي أحيان أخرى، تُعطل المواقع بأوامر قضائية، فتتوقف عن العمل كليًا أمام الجميع. وكما يوضح هذا الرسم، قد تقوم جهات إنفاذ القانون بإغلاق موقع إلكتروني بموجب أمر من المحكمة لوقف نشاط إجرامي، وقد تكتفي بإغلاقه تمامًا، أو قد تعيد توجيهه وتستولي عليه وتضعه تحت إدارة خوادم أسماء جديدة. ويمكن القول إنهما إجراءان مختلفان، ولكنهما كثيرًا ما يُستخدمان لتحقيق غايات متشابهة، ألا وهي منع الوصول.

الشريحة التالية. هذه ملاحظة من الورقة البحثية: تتناول اللجنة الاستشارية للأمن والاستقرار في هذه الورقة التقنيات المستخدمة في حجب نظام أسماء النطاقات وبعض الدوافع الكامنة وراءها. وبطبيعة الحال، قد تتباين الآراء حول حالات بعينها؛ فما يُعد غير قانوني في بلد ما قد يكون مشروعًا في بلد آخر، وقد يختلف الناس حول وجاهة قرار قضائي بحجب محتوى ما. ولسنا بصدد إصدار أحكامًا قيمية على أي من هذه الحالات بعينها. الشريحة التالية.

وارن كوماري

شكرًا. كما ذكر غريغ، فإن حجب نظام أسماء النطاقات يُعد بمثابة أداة. وكما هو الحال مع أي أداة، فإن لها مواطن قوة ومواطن ضعف. ومن الضروري فهم آلية عمل هذه الأداة لنحسن استخدامها ونتجنب إيذاء أنفسنا بها عن غير قصد.

فحجب نظام أسماء النطاقات يتم عبر وضع قوائم على المحلل التكراري تحدد ما يُسمح بحلّه وما لا يُسمح به. وإحدى تداعيات هذا الأسلوب هي أن الحجب لا يسري إلا على المستخدمين الذين يعتمدون على ذلك المحلل التكراري تحديدًا. وهذا يعني أنه إذا قرر مستخدم ما اللجوء إلى محلل تكراري آخر، فسيتمكن من تجاوز الحجب أو الالتفاف عليه.

في الرسم البياني أدناه، يرسل المستخدم استفساراته إلى أحد المحللات القياسية التي يوفرها مزود خدمة الإنترنت. فإذا كان الاسم الذي يحاول البحث عنه مسموحًا به، يتم معالجته بشكلٍ طبيعي. أما إذا كان مدرجًا على إحدى قوائم الحجب، فيحدث أمر مختلف؛ فإما أن يتلقى المستخدم ردًا بأن الاسم غير موجود، أو قد يحاول المحلل التكراري إعادة توجيهه

إلى مكان آخر. ولكن، إذا لم يكن المستخدم يستعلم من هذا المحلل الخاضع للحجب، وذهبت استفساراته إلى محلل آخر لا يطبق الحجب، فسيتمكن من تصفح الإنترنت بحرية تامة.

الشريحة التالية. إذن، كيف يتسنى للمستخدمين استخدام محلل مختلف؟ أحد أبرز السبل لتحقيق ذلك هو وجود عدد كبير مما يُعرف باسم "المحللات العامة"، والتي يستخدمها عدد هائل من المستخدمين. وتشير أبحاث جيف هيوستن في مركز معلومات الشبكة لمنطقة آسيا والمحيط الهادئ (APNIC) إلى أن ما يقارب 21% من المستخدمين يعتمدون حاليًا على أحد المحللات العامة العالمية المعروفة. ومن أمثلتها: نظام أسماء النطاقات العام من جوجل، والمحلل العام المفتوح من كلاودفلير، وخدمة Quad9، فضلاً عن وجود نسخ حكومية من هذه الخدمات، ولعل المثال الأشهر على ذلك هو خدمة DNS4EU، وهي عبارة عن خدمة محلل عام مدعومة حكوميًا في أوروبا. وبالتالي، من السهل نسبيًا، حتى على المستخدمين غير المتخصصين تقنيًا، تحديث إعدادات المحلل التكراري لديهم وتوجيهها نحو أحد خوادم نظام أسماء النطاقات البديلة هذه.

الشريحة التالية. من المؤكد أن كل من شاهد خدمات البث خلال السنوات الماضية قد صادفته إعلانات لا حصر لها عن خدمات الشبكات الافتراضية الخاصة (VPN). ومن أشهرها NordVPN وSurfshark، والقائمة تطول. حيث تقدم هذه الخدمات مزايا جمة للمستخدمين؛ فهي تعزز خصوصيتهم وتوفر لهم قدرًا أكبر من إخفاء الهوية، لكنها أيضًا، كما توضح إعلاناتها بجلاء، مصممة لتجاوز القيود الجغرافية.

فمثلًا، إذا كنت مسافرًا وترغب في مشاهدة خدمة بث أو محتوى متاح فقط في بلدك الأم، فما عليك سوى تشغيل خدمة الشبكة الافتراضية الخاصة (VPN) وعندها سيبدو اتصالك بالإنترنت قادمًا من بلدك الأم. والعكس صحيح؛ فإذا كنت في بلدٍ ما وتريد مشاهدة محتوى غير متاح فيه، يمكنك ببساطة تشغيل شبكة افتراضية خاصة، واختيار نقطة اتصال في البلد الذي ترغب في الظهور منه، وفجأة يصبح مصدر اتصالك بالإنترنت ذلك البلد الذي اخترته.

وما يعنيه كل هذا هو أنك تستخدم مجموعة مختلفة من المحللات التكرارية، وبالنسبة للإنترنت، فإن مصدر اتصالك لا يبدو قادمًا من البلد الذي تقيم فيه بالفعل. وهذا بدوره يمكّنك من تجاوز أي حجب مفروض في مجموعة من المحللات التكرارية بسهولة تامة،

بمجرد تشغيل خدمة الشبكة الافتراضية الخاصة. الشريحة التالية. أعتقد أن الكلمة تعود إليك الآن.

مارتن أيرتسن

الشريحة التالية. إذن ما مكامن الخلل المحتملة، أو ما الذي قد لا يسير على النحو المنشود؟ يحدث "الحجب المفرط" عندما يكون نطاق الحجب أوسع مما ينبغي. فعلى سبيل المثال، حجب نطاق المستوى الثالث يكون أكثر دقة وتحديدًا من حجب نطاق المستوى الثاني أو الحجب الشامل على مستوى النطاقات العُليا (TLD). فإذا اتسع نطاق الحجب أكثر من اللازم، فقد ينجم عنه قطع الوصول إلى وجهات أو مواقع إلكترونية متعددة، مما يلحق الضرر بزوار تلك المواقع التي لا تُشكل أي تهديد.

وغالبًا ما يقع هذا الخطأ عند تطبيق الحجب في غير محله. وتزخر الورقة البحثية التي أعددناها بالعديد من دراسات الحالة التي توضح هذه النقاط بالتفصيل، لذا نحثكم على مراجعتها إن أردتم التعمق أكثر. ومن الأمثلة على الحجب المفرط، ما حدث في إيطاليا التي تتبع نظامًا لتوزيع أسماء النطاقات على مزودي خدمة الإنترنت لديها؛ ففي إحدى المرات، أدرجت السلطات عن طريق الخطأ نطاقًا مخصصًا للبنية التحتية ضمن قائمة الحجب، مما أدى إلى حجب خدمة "مستندات جوجل (Google Docs)" عن المستخدمين في إيطاليا لفترة وجيزة، إلى أن تنبه أحدهم للخطأ وصححه. لقد تسبب هذا الخطأ في إزعاج الناس وحرمانهم من الوصول إلى محتوى لم يكن إشكاليًا على الإطلاق. وهذا مثال حي على ما يُعرف باسم "الأضرار الجانبية"؛ فعندما يُنفَّذ الإجراء بصورة قاصرة، فإنه يطال أطرافًا لم يكن من المفترض أن تتأثر به.

الشريحة التالية. وكما أوضح وارن، فإن المستخدمين قادرون على التحايل على الحجب. لذا، عند فرض أي شكلٍ من أشكال الحجب، يجب أن نفترض أن شريحة من المستخدمين ستجد وسيلة لتجاوزه، لا سيما إن كانت دوافعهم قوية. إذ يمكنهم استخدام الشبكات الافتراضية الخاصة (VPNs)، أو اللجوء إلى محلِّلات أسماء نطاقات بديلة. بل إن هناك تقنيات أخرى تساعد على إبقاء المحتوى متاحًا أو تمكين المستخدمين من الوصول إليه. وعليه، فإن الجدوى من حجب نظام أسماء النطاقات تظل مسألة نسبية. فمن يعتقد أن حجب نطاق ما عبر إصدار أمر لمزودي الخدمة في بلده سيحل المشكلة من جذورها، فهو مخطئ؛

قد يحلها لعدد من المستخدمين، ولكن ليس لجميعهم على الأرجح. لننتقل إلى الشريحة التالية رجاءً.

وارن كوماري

عندما يُحجب نطاق ما، يمكن للمحلِّل التكراري أن يستجيب بإحدى إجابتين عامتين: إما أن يفيد بأن اسم النطاق غير موجود، وإما أن يعيد توجيه المستخدم إلى وجهة أخرى، وهو ما نرى أنه يُطلب أحيانًا، ويُلاحَظ أن هناك تزايدًا في اللجوء إلى هذا النوع من الحجب. ونحن نرى في هذا النهج الثاني خطرًا كبيرًا.

ويكمن السبب في أنه إذا حاول المستخدم الوصول إلى موقع مثل foo.bar.com، وأُعيد توجيهه إلى مكان آخر، فإن متصفح الويب سيُظهر له رسالة تحذيرية مفادها: "لقد حاولت الوصول إلى foo.bar.com، لكن الخادم الذي تتصل به لا يخص هذا الموقع". ومع تكرار هذا الموقف، سيعتاد المستخدمون على تجاهل هذه الرسائل التحذيرية وتجاوزها بنقرة زر، وهو ما تترتب عليه عواقب أمنية وخيمة. فببساطة، سيتعلمون تجاهل التحذيرات المنبثقة، وإن كان الأمر يتعلق اليوم بموقع محجوب عبر نظام أسماء النطاقات، فقد يتعلق في المرة القادمة بموقع المصرف الخاص بهم أو أي موقع حساس آخر. لذلك، فإن إحدى توصياتنا الأساسية هي: تفادوا اللجوء إلى إعادة التوجيه عند تطبيق حجب نظام أسماء النطاقات.

وهذا يقودنا إلى النقطة التالية، ألا وهي التوصيات. وهذه مسألة أخرى سأتولى الحديث عنها. كما أكدنا مرارًا، إن حجب نظام أسماء النطاقات هو في جوهره أداة، وكأي أداة أخرى، لا سيما القوية منها، يمكن تسخيرها للخير، ولكن الجهل بآلية عملها الدقيقة وتجاهل التحذيرات قد يؤدي إلى إلحاق ضرر بالغ بالنفس. وعليه، فإن كنتم بصدد تطبيق أو فرض حجب نظام أسماء النطاقات، فاحرصوا على فهم آلية عمله فهمًا عميقًا، واستيعاب ما قد يترتب عليه من أضرار جانبية وآثار غير مرغوب فيها.

مارتن أيرتسن

لننتقل إلى الشريحة التالية رجاءً. التوصية الثانية التي تقدمها اللجنة الاستشارية للأمن والاستقرار هي أنه عند فرض أي شكلٍ من أشكال الحجب – سواءً داخل شركة، أو على

مستوى مزود خدمة، أو على الصعيد الوطني – ينبغي الالتزام بالمبادئ التوجيهية التالية، والتي يستند بعضها إلى المبدأ الطبي الراسخ "لا ضرر ولا ضرار".

أولًا، عليكم أن تدركوا ما إذا كان حجب نظام أسماء النطاقات هو الوسيلة المثلى لتحقيق أهدافكم. فقد تكون هناك حلول بديلة لمشكلتكم. وكما ذكرنا، إذا لجأتم إلى الحجب، فمن المحتمل أن يتمكن بعض المستخدمين من تجاوزه. فهل هذا يخدم غايتكم، أم أنه لا يكفي؟ ثانيًا، لا بد من وضع سياسة وإجراءات واضحة بدقة تحدد ما الذي ستقوم بحجبه وكيفية القيام بذلك، مع وجود آليات مراجعة فعالة لما يُدرج في قوائم الحجب، والعمل على تقليل المخاطر إلى أدنى حدٍ ممكن. ومن الضروري، على سبيل المثال، أن تكون لديكم آلية واضحة لتصويب الأخطاء. ونحن لا نوصي بسياسات وإجراءات بعينها، إذ يجب أن تتناسب مع أهدافكم ومهامكم، ولكن المبدأ في حد ذاته جوهري.

ثالثًا، يجب تطبيق الحجب بأسلوب يقلل إلى أقصى حد من "الحجب المفرط" أو الأضرار الجانبية التي قد تلحق بالمستخدمين الذين يقعون تحت مسؤوليتكم الإدارية، كموظفي الشركة على سبيل المثال. وأخيرًا، يجب الحرص على عدم نفاذ التأثير إلى أفراد يقعون خارج نطاق مسؤوليتكم الإدارية. فهنا في أوروبا، على سبيل المثال، نجد أن بعض مزودي خدمة الإنترنت يخدمون عملاء في أكثر من دولة. فإذا كان مزود الخدمة يخدم عملاء في البلد "أ" والبلد "ب"، وتلقى أمرًا بالحجب من سلطات البلد "أ" التي يخضع لاختصاصها القضائي،

فكيف له أن يطبق الحجب دون أن يؤثر على عملائه في البلد "ب" الذين هم خارج ذلك الاختصاص القضائي؟ علينا أن نتذكر دائمًا أننا نرى على الخريطة حدودًا وطنية تفصل بين الدول، لكن الإنترنت لا يعترف بتلك الحدود. وخلاصة القول: توخوا الحذر كي لا تطال إجراءاتكم من لا تملكون الحق في التأثير عليهم. لننتقل إلى الشريحة الأخيرة رجاءً.

وارن كوماري

وارن كوماري: سأوجز بشدة لأن الوقت قد أدركنا. التوصية الأخيرة موجهة إلى مشغلي المحلِّلات، حيث توصي اللجنة الاستشارية للأمن والاستقرار باستخدام طلب تقديم التعقيبات (RFC) الجديد لتضمين رسائل الخطأ، بما فيها تلك الناتجة عن الحجب، شرحًا يوضح

سبب حدوثها. لننتقل للنقطة التالية. في الواقع، أعتقد أن الوقت المخصص للأسئلة قد انتهى أيضًا.

ماركو هوغوونينغ أجل، الوقت يداهمنا بشدة، ولكن شكرًا جزيلًا لكما. هذا عمل ثري ومفصل. وبصفتي من الجمهور المستهدف، أقدره حق التقدير، فهو يطرح الكثير من النقاط التي تدعو للتفكير. وعلى الرغم من ضيق الوقت، أعتقد أنه يمكننا أخذ سؤال واحد قصير. لمحتُ ممثل بابوا غينيا الجديدة في مربع الدردشة. راسل، هل تود طرح سؤالك؟

راسل وروبا: شكرًا لك، ماركو. لقد دُعينا، كدولة، للمشاركة في تجارب حول ما يُعرف باسم "نظام أسماء النطاقات الوقائي". وأردت فقط أن أتأكد: هل هذا هو ما تتحدثون عنه؟ هل هو في جوهره نظام أسماء النطاقات وقائي؟

مارتن أيرتسن نعم، يمكن تحقيق الحماية عبر نظام أسماء النطاقات الوقائي من خلال حجب نطاقات محددة. فالمحلِّلات العامة التي ذكرناها، على سبيل المثال، تقدم خدماتها في هذا المجال تحديدًا، حيث تحجب مواقع التصيد والاحتيال والبرمجيات الضارة لحماية مستخدميها. فهذه إحدى التقنيات المستخدمة لتوفير الحماية للمستخدمين. ونود أن نشير أيضًا إلى أن هذه الورقة البحثية قد استُعين بها بالفعل في بعض المداولات المتعلقة بالسياسات والجارية حاليًا في اليابان، حيث تدرس السلطات هناك حجب نوع محدد جدًا من المحتوى داخل البلاد.

وارن كوماري وإضافة موجزة جدًا على ذلك: إن شركة "كلاودفلير" هي إحدى الجهات التي توفر محلِّلات عامة، وتقدم ثلاثة عناوين رئيسية على الأقل. الأول هو العنوان القياسي 1.1.1.1، والذي لا يطبق أي حجب تقريبًا. ثم هناك العنوان 1.1.1.2، الذي يحجب البرمجيات الضارة.

وأخيرًا، العنوان 1.1.1.3، الذي يوفر حماية أوسع نطاقًا، فيحجب البرمجيات الضارة والمحتوى المخصص للبالغين.

وأعتقد أن وجهة نظر اللجنة الاستشارية للأمن والاستقرار، أو ربما هذا رأيي الشخصي، هو أنه عند تقديم خدمة نظام أسماء النطاقات وقائي لشريحة واسعة من المستخدمين، يجب أن يُمنح المستخدم حرية اختيار مستوى الحماية الذي يناسبه. فالآباء قد يرغبون في حجب المحتوى المخصص للبالغين، وبالتالي سيختارون الخدمة الوقائية التي توفر ذلك. أما البالغون الآخرون، فقد يرغبون في الوصول إلى ذلك المحتوى. وهنا تكمن أهمية أن يكون الأمر اختياريًا وليس إجباريًا. وهذا يعود بنا إلى نقطة سابقة، وهي أن أنواع الحجب تختلف باختلاف الفئات المتأثرة بها. فإذا كانت الحماية خيارًا اشتركت فيه طواعية، فإنها تلقى استحسانًا أكبر من حماية تُفرض عليك من جهة خارجية.

ماركو هوغوونينغ

حسنًا، شكرًا لك، وارين. لدينا ثلاث أشخاص في قائمة الانتظار. وسأغلق باب الأسئلة عند هذا الحد. أرجو من الجميع الإيجاز. إذا استطعنا تخصيص دقيقة واحدة لكل سؤال وجواب، فسنعود إلى المسار الزمني الصحيح. أعتقد أن السائل الأول من جمهورية الكونغو الديمقراطية، بليز.

بليز آزيتيمينا فونجي

نعم، شكرًا جزيلًا. معكم بليز آزيتيمينا من جمهورية الكونغو الديمقراطية للتدوين في السجل. لديّ هاجس يتعلق بالشبكات الافتراضية الخاصة (VPN). فبينما أقدر تمامًا ما توفره هذه الأدوات من أمن وسلامة، إلا أنني، من منظور السياسة العامة، أشعر بالقلق إزاء ظاهرة إخفاء الموقع الجغرافي. ففي العديد من البلدان المسماة بالنامية، لا يستخدم الناس هذه الشبكات بالضرورة لدواعٍ أمنية، بل في الأساس لإخفاء عنوانهم الحقيقي وإظهاره كأنهم في بلدٍ آخر. وهذا السلوك قد يشكل في بعض الأحيان خرقًا للسياسة العامة أو تهديدًا أمنيًا في بلداننا.

وقد رأينا بعض منصات البث التي توصلت إلى حل لهذه المشكلة، فعندما تتصل عبر شبكة افتراضية خاصة أو وكيل، فإنها تمنعك من الوصول. وسؤالي هو: كيف يمكن تحقيق

التوازن المنشود بين متطلبات الأمن والسلامة من جهة، ودقة تحديد الموقع الجغرافي من جهة أخرى؟ شكرًا لك.

مارتن أيرتسن

لا أعتقد أن اللجنة الاستشارية للأمن والاستقرار قد درست هذا الموضوع بكل أبعاده. والحقيقة أن الشبكات الافتراضية الخاصة متاحة على نطاق واسع، ومثلها مثل العديد من الأدوات، تُستخدم لأغراض حميدة وأخرى خبيثة. فالمجرمون يستخدمونها لإخفاء هوياتهم. وهذه الشبكات تستفيد من بنية الإنترنت نفسها، لذا فهي باقية ولن تختفي. وتحتفظ بعض الشركات بقوائم لعناوين بروتوكول الإنترنت الخاصة بالشبكات الافتراضية الخاصة المعروفة. وتستخدمها، على سبيل المثال، لتقييم درجة خطورة حركة المرور القادمة من تلك العناوين. إذن، توجد بعض الأدوات لكشف حركة مرور هذه الشبكات وفهمها.

وارن كوماري

وتعقيبًا على ذلك، صُممت الشبكات الافتراضية الخاصة لتبدو كأنها حركة مرور عادية على الإنترنت. وقد حاولت بعض الجهات، سواءً شركات أو دول، حجب استخدامها. ولكن ما حدث في نهاية المطاف هو أنهم تمكنوا من حجب خدمات الشبكات الافتراضية الخاصة الكبيرة والمعروفة، لكن المستخدمين، في سعيهم للوصول إلى المحتوى الذي يرغبون فيه، لجؤوا إلى الشبكات الافتراضية الخاصة الأقل شهرة وموثوقية، مما قد يعرضهم لمخاطر أكبر. لذا، أعتقد أن هناك دائمًا عواقب سلبية يجب أخذها في الحسبان عند محاولة حجب تقنية يستخدمها الناس للوصول إلى المحتوى الذي يريدونه؛ فهم سيجدون وسيلة للوصول إليه، ولكن ربما بطريقة أكثر خطورة.

ماركو هوغوونينغ

شكرًا لك، وارين. اسمحوا لي أن آخذ السؤالين التاليين معًا، ثم يمكنكم الرد عليهما بإيجاز. أول من طلب الكلمة هو ممثل الهند. نرجو الإيجاز.

سوشيل بال

شكرًا لك. معكم سوشيل بال من الهند. هل تعتقدون أن نظام أسماء النطاقات المدعوم حكوميًا، مثل النظام الخاص بالاتحاد الأوروبي "DNS4EU" الذي ذكرتموه، تقدم أي ميزة

جوهرية مقارنة بالأنظمة العامة الأخرى؟ والسؤال الثاني: لا شك أن للشبكات الافتراضية الخاصة أهميتها، شريطة أن تكون معروفة المصدر. فهل تبحث الأجهزة الأمنية عن أي سبل لرصد الشبكات الافتراضية الخاصة المجهولة؟

ماركو هوغوونينغ: آشوين؟ نعم.

مارتن أيرتسن: ما يمكنني قوله بشأن "DNS4EU" هو ما يعلنونه هم على موقعهم الرسمي. لقد ذكروا أنهم أنشأوه في إطار مساعيهم لتعزيز "السيادة الرقمية"؛ فبدلاً من توجيه حركة المرور إلى المحلِّلات العامة التجارية الكبرى، تقدم أوروبا الآن هذه الخدمة لتبقى حركة المرور داخل حدودها. وهذا ما يصرحون به. هل تبحث الأجهزة الأمنية عن سبل لرصد الشبكات الافتراضية الخاصة المجهولة؟ لا أعلم على وجه اليقين.

سوشيل بال: هل يمثل هذا الأمر مصدر قلق للأجهزة الأمنية؟

ماركو هوغوونينغ: السؤال الأخير لممثل إندونيسيا.

آشوين ساسونجكو ساستروسوبروتو: نعم، شكرًا لكم. أود فقط أن أستمع لتعليقكم بشأن الحجب، فقد تطرقتم إلى تأثيراته السلبية وما إلى ذلك. ماذا لو كان النهج المتبع ليس السماح لجميع استعلامات نظام أسماء النطاقات بالدخول إلى فضائنا السيبراني، بل أن نسمح فقط بما نريده نحن؟ على سبيل المثال، النطاق go.id.، حسنًا، هذا مسموح به بالكامل. أما النطاق .com، فسنقوم بمراجعة والبحث والتقرير بشأنه: حسنًا، هذا الموقع مسموح به، وهذا أيضًا، أما البقية فغير مسموح بها. فبدلاً من حجب نطاقات بعينها، نقوم في الواقع بحجب كل شيء من الأساس، ولا نسمح بالمرور إلا لاستعلامات نظام أسماء النطاقات التي نوافق عليها. شكرًا لك.

وارن كوماري: في الحقيقة، لا أعتقد أن هذا ممكن عمليًا. فهناك الملايين من المواقع على الإنترنت، وبالتالي فإن وضع قائمة بما هو مسموح به سيكون أمرًا في غاية الصعوبة. ولكن حتى إن تمكنتم من فعل ذلك، فإن حجب جميع اتصالات نظام أسماء النطاقات لم يعد ممكنًا من الناحية التقنية في وقتنا الحاضر. فهناك عدد من التقنيات الجديدة، مثل بروتوكول نظام اسم النطاق على أمن طبقة النقل، وحل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن، وبروتوكول DNS عبر QUIC، والتي تجعل من غير الواضح أن الاستفسار المرسل هو استفسار يتعلق بنظام أسماء النطاقات من الأساس. فهو يبدو تمامًا مثل أي حركة مرور أخرى على الإنترنت. وبالتالي، فإن الإجراء الحقيقي الوحيد الذي يمكنكم اتخاذه هو ببساطة حجب جميع اتصالات الإنترنت في بلدكم، وفصل البلد بالكامل عن شبكة الإنترنت العالمية، وحجب خدمات Starlink وغيرها من مزودي خدمات الأقمار الصناعية. لذا، فبمجرد الاتصال بالإنترنت، سيتمكن نوع ما من حركة مرور نظام أسماء النطاقات من التسرب إلى الخارج، وسيتمكن الناس من الوصول إلى المحتوى الذي يريدونه.

مارتن أيرتسن: والتقنيات التي ذكرها وارن هي في الأساس تقنيات مرتبطة بالتشفير، مصممة لحماية هوية المستخدم النهائي الذي يقوم بالاستفسار. وبالتالي، فإن هذه التقنيات هي محاولات لتوفير قدر أكبر من الخصوصية على الإنترنت. شكرًا لك.

ماركو هوغوونينغ: أعتذر عن المقاطعة، هذا موضوع شيق بالفعل وأرى نقاشًا تفاعليًا ثريًا، لذا أعتقد أنه يستحق جلسة متابعة. وفي هذه الأثناء، يظهر خلفنا رمز الاستجابة السريعة الخاص بالتقرير الكامل. لذا، نرجو منكم قراءته بالطبع، فقد صدر منذ فترة. وبهذا، هل لي أن أشكركم، رام، وغريغ، ووارن، ومارتن. تفضلوا بالبقاء معنا إن شئتم. ولكن دون مزيدٍ من الإطالة، أود أن أنتقل الآن إلى ما وصفته بأنه جلسة متابعة للنقاش الذي أجريناه حول الحوسبة الكمومية وبعض مخاطرها خلال اجتماعنا في سياتل. ويسرني أن أعطي الكلمة لكريستيان هيسلمان من القسم البحثي التابع لمؤسسة تسجيل النطاقات الهولندية (مختبرات SIDN)، ليحدثنا عن كيفية تأثير ذلك على الامتدادات الأمنية لنظام اسم النطاق وبشكلٍ

خاص، ما يمكننا نحن كممثلين حكوميين القيام به للمساعدة على التخفيف من حدة بعض هذه المشكلات. كريستيان، الكلمة لك.

رام موهان

ماركو، اسمح لي بلحظة قبل ذلك. أردت أن أتقدم بالشكر إلى اللجنة الاستشارية الحكومية نيابةً عن اللجنة الاستشارية للأمن والاستقرار. فنحن نُثمِّن جدًا تواصلنا وتعاوننا المستمر ونتطلع إلى المزيد من هذا التعاون المثمر. شكرًا لك.

ماركو هوغوونينغ

شكرًا لك. عذرًا، رام تفضل إذن يا كريستيان.

كريستيان هيسلمان

شكرًا لك، ماركو. حسنًا. هذا العرض التقديمي، كما قال ماركو، يدور حول الحواسيب الكمومية والامتدادات الأمنية لنظام أسماء النطاقات والتأثير المحتمل لهذه الأجهزة المستقبلية. وقد أدرجت في نهاية هذا الحديث بعض الإجراءات المقترحة لـ GAC من منظور حكومي. لقد اختفت الشرائح. على أي حال، سأواصل الحديث. إذن، الصورة التي رأيتموها هي صورة حصلتُ عليها من مركز لايبنتز للحوسبة في ألمانيا، حيث يعملون على تطوير هذه الحواسيب الكمومية. ولا أريد القول إنها ضرب من الخيال العلمي، ولكنها لا تزال في مرحلة تجريبية متقدمة للغاية. لذا، نحن نتحدث هنا عن أبحاث طويلة الأمد. حسنًا، لقد عادت الشرائح. حسنًا، شكرًا.

لننتقل إلى الشريحة التالية رجاءً. حسنًا. إذن، بادئ ذي بدء، ما التوقعات المنتظرة من الحواسيب الكمومية؟ وهنا، لا بد لي من التنويه بأنني لست خبيرًا في الحوسبة الكمومية، بل متخصص في النظم الموزعة. ففي اعتقادي، تقع الخبرة في مجال الحواسيب الكمومية ضمن نطاق اختصاص علماء الفيزياء، وأنا لست واحدًا منهم. وعليه، فإن ما سأعرضه هو خلاصة ما قرأته في الأدبيات العلمية. تشمل التوقعات المنتظرة من الحواسيب الكمومية تطبيقات جديدة، مثل ابتكار طرق حديثة لاكتشاف الأدوية، وتحسين تقنيات التعلم الآلي، وتطوير مواد ثورية.

ولكن، كما ذكر غريغ سابقًا، يمكن تسخير التقنيات بطرق شتى. فهذه هي "المطرقة" التي تحدث عنها غريغ؛ إذ يمكنك استخدامها لغايات إيجابية، ولكنها تنطوي أيضًا على مخاطر معينة. وعليه، فإن الجانب المظلم للحواسيب الكمومية يكمن في قدرتها المحتملة على كسر خوارزميات التشفير الحالية التي نستخدمها. ومن بين هذه الخوارزميات، تلك المستخدمة في الامتدادات الأمنية لنظام أسماء النطاقات، والتي تُوظَّف لتوثيق رسائل نظام أسماء النطاقات والتحقق من سلامة محتواها.

لقد اختفت الشرائح مجددًا. هل تريدون مني الاستمرار أم الانتظار حتى تعود الشرائح؟ حسنًا. لقد عادت. حسنًا. إذن، يكمن خطر الحواسيب الكمومية على الامتدادات الأمنية لنظام أسماء النطاقات في قدرتها المحتملة على كسر خوارزميات التشفير التي تستخدمها هذه الامتدادات للتحقق من أصالة وسلامة استجابات نظام أسماء النطاقات. وبالتالي، من المحتمل أن يتمكن طرف مهاجم من إعادة توقيع رسائل نظام أسماء النطاقات باستخدام مفتاح مخترق، ثم الادعاء بأن الرسالة حقيقية وصادرة عن مصدر موثوق. ونتيجةً لذلك، قد ينتهي الأمر بالمستخدمين في موقع إلكتروني خاطئ، أو قد تصل مكونات البرامج إلى وجهة غير صحيحة.

وهنا، أود أن أضيف، أن ما نفترضه في هذا السيناريو هو أننا نعيش بالفعل في "حقبة ما بعد الكَمّ". أي أن هذا لن يحدث الآن، بل في المستقبل. وهذا الهجوم ليس من نوع هجمات "خزّن الآن، وفك التشفير لاحقًا"، بل هو هجوم حقيقي يمكنك من خلاله فك تشفير مفاتيح الامتدادات الأمنية لنظام أسماء النطاقات أو اختراقها بشكل شبه فوري. لكن الخبراء يعتقدون أن هذا لن يحدث قبل 10 إلى 15 عامًا أخرى. لذا، فإن السؤال الذي قد تطرحونه هو: لماذا يتوجب علينا العمل على هذا الموضوع الآن؟

لننتقل إلى الشريحة التالية رجاءً. والسبب هو أن إضافة خوارزميات تشفير جديدة أو استبدالها في الامتدادات الأمنية لنظام أسماء النطاقات يستغرق وقتًا طويلاً جدًا. هذا رسم بياني مأخوذ من ورقة بحثية، ترون فيه مسار تطور إحدى خوارزميات التشفير في الامتدادات الأمنية لنظام أسماء النطاقات، بدءًا من المسودة الأولية في فريق عمل هندسة الإنترنت IETF، وصولًا إلى مستوى كبير من الانتشار على اليمين. وكما تلاحظون، يستغرق هذا الأمر ما يقرب من 10 سنوات. وأعتقد أن هذه السمة هي سمة مميزة لتحديثات البنية التحتية. وينطبق الأمر ذاته على إدخال خوارزميات جديدة للامتدادات الأمنية لنظام أسماء النطاقات. وعليه، إذا كانت الحواسيب الكمومية ستصبح حقيقة واقعة في غضون

10 إلى 15 عامًا، فمن الأحرى بنا أن نفكر فيما يجب فعله حيال ذلك بالنسبة لنظام أسماء النطاقات، الآن وليس غدًا.

حسنًا. لننتقل إلى الشريحة التالية، رجاءً. إذن، بالإضافة إلى عامل الوقت، هناك أيضًا انتشار واسع حاليًا للامتدادات الأمنية لنظام أسماء النطاقات. على اليسار، يمكنكم رؤية البلدان التي وقّعت نطاقات المستوى الأعلى لرموز البلدان (ccTLD) الخاصة بها باستخدام الامتدادات الأمنية لنظام أسماء النطاقات. فالبلدان الملونة بالأخضر والأزرق هي التي تطبقه بالفعل، وهذا يمثل ما يقرب من 48% من العالم. وكما ترون على اليمين، تلك هي خريطة التحقق من الصحة، وهي تبدو أكثر احمرارًا وبرتقالية. والسبب في ذلك هو أن مستوى تبني عملية التحقق من صحة هذه التوقيعات لا يزال منخفضًا. لذا، لا تزال هناك جوانب تحتاج إلى تحسين. ولكن كما تلاحظون، هناك انتشار كبير للامتدادات الأمنية لنظام أسماء النطاقات حاليًا. وهذا بحد ذاته يشكل تحديًا عند اقترانه بالحوسبة الكمومية، خاصةً إذا افترضنا أن عملية التحقق ستزداد في المستقبل، وكذلك عملية التوقيع على اليسار.

لننتقل إلى الشريحة التالية رجاءً. إذن، إذا أردنا حماية نظام أسماء النطاقات من الحواسيب الكمومية، فقد حددنا ثلاث استراتيجيات للقيام بذلك. أطلقنا عليها: الاستبدال، وإعادة التصميم، والإلغاء. فالاستبدال يعني استبدال خوارزميات التشفير الحالية في نظام أسماء النطاقات بخوارزميات جديدة آمنة في عصر ما بعد الكَمّ. وإعادة التصميم تعني إعادة تصميم نظام الامتدادات الأمنية لنظام أسماء النطاقات بالكامل، وهو الخيار الثاني في الجدول. والخيار الثالث هو الإلغاء، مما يعني التخلص من الامتدادات الأمنية لنظام أسماء النطاقات تمامًا.

ولكل من هذه المناهج الثلاثة إيجابيات وسلبيات مختلفة. على سبيل المثال، استراتيجية الاستبدال سهلة التنفيذ نسبيًا، وهي موحدة قياسيًا، ولكنها تنطوي على مخاطر تشغيلية، وسأتحدث عن ذلك لاحقًا. أما إعادة التصميم فهي في الواقع نهج "البداية من الصفر" للامتدادات الأمنية لنظام أسماء النطاقات، حيث ستستخدم تقنيات جديدة مثل أشجار ميركل، من شأنها أن تقلل من المخاطر التشغيلية، ولكن عليك بشكل أساسي إصلاح نظام وبروتوكولات الامتدادات الأمنية لنظام أسماء النطاقات بأكملها، لذا، سيستغرق ذلك وقتًا طويلاً.

ثم الإلغاء، حسنًا، قد يبدو ذلك سهلًا، ولكنه لن يخلو من تأثير؛ لأنه إذا تخلصت من الامتدادات الأمنية لنظام أسماء النطاقات، فإنك تفتح نظام أسماء النطاقات لجميع أنواع الهجمات التي يحاول نظام الامتدادات الأمنية لنظام أسماء النطاقات الحماية منها. وقد تؤثر أيضًا على البروتوكولات التي تعتمد على الامتدادات الأمنية لنظام أسماء النطاقات. لذا، في عملنا لدى مؤسسة تسجيل النطاقات الهولندية، اخترنا الخيار الأول، وهو الاستبدال. ولهذا السبب يظهر الصف الأول باللون الأخضر.

لننتقل إلى الشريحة التالية رجاءً. وسأركز حديثي على هذا النهج بالتحديد من الآن فصاعدًا. لن أشرح هذا الشكل، فلا داعي للقلق. ولكن ما ترونه هنا هو التفاعلات التي تحدث بين المحلِّلات وخوادم الأسماء الموثوقة مع عرض رسائل الامتدادات الأمنية لنظام أسماء النطاقات. والرسائل التي تحمل شارات حمراء وصفراء هي التي تحتوي على مواد المفاتيح، سواء كانت توقيعات أو مفاتيح عامة، وهذه هي التي تحتاج إلى تحديث.

لننتقل إلى الشريحة التالية رجاءً. ولإعطائكم فكرة أيضًا عن شكل هذه التوقيعات، إليكم هذا المثالان. في الأعلى، يوجد مفتاح عام على اليسار باللون الرمادي، موقع بمفتاح حالي... عذرًا، مفتاح حالي نستخدمه في الامتدادات الأمنية لنظام أسماء النطاقات. وعلى اليمين باللون الرمادي يوجد توقيع تم إنشاؤه بواسطة هذا المفتاح. وباللون الأزرق، ترون مفتاحًا عامًا وتوقيعًا تم إنشاؤهما بواسطة خوارزمية ما بعد الكَمّ، أي خوارزمية قوية بما يكفي للحماية من الحواسيب الكمومية. وكما ترون، إنها أطول بكثير. حسنًا. هذا فقط لإعطائكم مؤشرًا أو فكرة عن شكلها من منظور تقني.

لننتقل إلى الشريحة التالية رجاءً. هناك العديد من الخوارزميات الآمنة كموميًا التي يتم تطويرها حاليًا، عادةً في إطار مسابقة تشفير ما بعد الكم لدى المعهد القومي للمعايير والتكنولوجيا في الولايات المتحدة، يُشار إليه بالاختصار (NIST). حيث أقام مسابقة لعلماء التشفير لابتكار خوارزميات قادرة على الصمود في وجه الحواسيب الكمومية. وقد أجرينا تجارب على عدد قليل من هذه الخوارزميات. وكما ترون في هذا الجدول، من الأمثلة على ذلك MAYO، وFalcon، وSQISign.

والأسماء تبدو غريبة نوعًا ما، وهناك المزيد منها. ولكن ما قمنا به هو تجربة هذه الخوارزميات والتحقق من الوقت الذي تستغرقه لتوقيع ملف منطقة، على سبيل المثال، منطقة .nl، للتحقق من صحة سجلات نظام أسماء النطاقات. وقد فحصنا أيضًا أحجام

التوقيعات وأحجام المفاتيح المستخدمة، لأنه في الشريحة السابقة، رأيتم أنها تختلف اختلافًا كبيرًا. وكما يتضح من هذا الجدول، فإن الأمر برمته عبارة عن مفاضلة؛ فعندما تحصل على أحجام مفاتيح صغيرة، قد تزداد سرعة التوقيع، ولكن قد يكون ذلك على حساب حجم التوقيع، والعكس صحيح.

الشريحة التالية، من فضلك. ها هي. هذه هي التجربة الأولى التي أجريناها على منطقة .nl. حاولنا توقيع المنطقة... أو بالأحرى، لم نحاول، بل وقعناها بالفعل باستخدام خوارزميتين للتشفير ما بعد الكَمّ، وهما Falcon وMAYO. ويمكنكم رؤيتهما على يمين الشكل. لن أخوض في التفاصيل، ولكن ما يمكنكم ملاحظته هنا هو أن توقيع المنطقة باستخدام خوارزميات التشفير ما بعد الكَمّ هذه يستغرق ضعف الوقت تقريبًا. فعادةً، يستغرق توقيع منطقة .nl حوالي 10 دقائق، ومع هذه الخوارزميات، استغرق الأمر 20 دقيقة. وهذا لا يزال مقبولاً تمامًا. وهذه النتائج تعد جيدة من منظور تشغيلي.

لننتقل إلى الشريحة التالية رجاءً. هذا هو ما توصلنا إليه حتى الآن في مؤسسة تسجيل النطاقات الهولندية. وقد حددنا بعض بنود العمل الإضافية التي نود البحث فيها مستقبلاً، والتي تتعلق في معظمها بحجم هذه التوقيعات والمفاتيح العامة. ونود أيضًا أن ندرس وقت التحقق في المحلِّلات بمزيدٍ من التفصيل، على سبيل المثال، بالاقتران مع دور التخزين المؤقت. نعم، لقد لاحظت ذلك. شكرًا لك.

إذًا، الشريحة الأخيرة لدي تتضمّن بعض الإجراءات المقترحة للجنة الاستشارية الحكومية. فربما يمكنكم التعاون مع المعهد الوطني للمعايير والتكنولوجيا (NIST)، وهو وكالة حكومية أمريكية، لاستكشاف ما السُبل التي يمكن اتباعها لمواءمة خوارزميات تشفير ما بعد الكم (PQC) التي يقوم بتطويرها مع شروط نظام أسماء النطاقات. وأعلم أن هذا الاستخدام بالتحديد يثير اهتمامه. هناك إجراء آخر محتمل يتمثل في تحفيز تطوير برمجيات مفتوحة المصدر تدمج خوارزميات تشفير ما بعد الكمي في البنية التحتية لنظام أسماء النطاقات. وقد يكون من الممكن تنفيذ ذلك من خلال صناديق تمويل مثل NLnet أو "صندوق التكنولوجيا السيادية" (Sovereign Tech Fund). فعلى الأقل، هذان هما المصدران اللذان أعلم بأنهما يدعمان هذا النوع من المشاريع.

وربما يمكن أيضًا تحفيز عملية النشر الفعلي. ويمكن القيام بذلك، على سبيل المثال، من خلال موقع مثل internet.nl، الذي يتيح التحقق من خصائص أسماء النطاقات أو

خصائص اتصالك بالإنترنت. ومن الممكن إضافة فحوصات تتعلق بجاهزية اسم النطاق لتشفير ما بعد الكم. وأخيرًا، وبالتوسّع قليلاً على ما ورد في الشريحة السابقة، هناك حاجة أيضًا إلى إجراء المزيد من الأبحاث حول التأثيرات التشغيلية لهذه الخوارزميات الجديدة المتعلقة بتشفير ما بعد الكم في حال اعتماد استراتيجية "الاستبدال"، وما يعنيه ذلك بالنسبة لنظام أسماء النطاقات ومشغّليه، مثل التأثير على منطقة الجذر.

حسنًا. لننتقل إلى الشريحة التالية رجاءً. إذن، فإن البرنامج الذي قمنا بتطويره – والتجارب التي أجريناها – تم تنفيذها على منصة اختبار مفتوحة المصدر. وبإمكانكم تحميل البرنامج من موقعنا، وإليكم رمز الاستجابة السريعة (QR) الخاص به. إذا كانت لديكم أي أسئلة إضافية، فلا تترددوا في التواصل معي. كانت هذه شريحتي الأخيرة.

ماركو هوغوونينغ

شكرًا لك يا كريستيان. إذن، يبدو أننا جميعًا نستطيع ببساطة تحميل بعض البرمجيات الكمية أو البرمجيات الآمنة ضد الهجمات الكمية والتجربة بأنفسنا. هذا شيء لطيف للغاية. نعم، شكرًا لك. الخلاصة الأساسية بالنسبة لي هي أن هناك بالفعل إجراءات يمكن اتخاذها. ومن منظور حكومتنا في هولندا، بدأنا فعليًا بالعمل على إدارة الأصول، كما أشرتَ باختصار. فنظام أسماء النطاقات موجود في كل مكان، وهو ما ظهر أيضًا في العرض الذي قدمه وارن. وهذا يعني أن الامتدادات الأمنية لنظام اسم النطاق موجودة في كل مكان أيضًا. وبالتالي، فإن تقنيات التشفير هذه مدمجة في كل شيء تقريبًا. ولهذا، نعمل داخليًا بالفعل على بناء قائمة لتحديد أماكن وجود هذا التشفير، تحسّبًا لاحتمال الحاجة إلى استبداله. ومن واقع تجربتي وخبرتي الشخصية، أستطيع إخباركم أن قول ذلك أسهل بكثير من تنفيذه. والآن لدي سؤالان. معنا باري من الحضور، وبيتر عبر الإنترنت. سأبدأ مع باري، تفضل الكلمة لك.

باري ليبا

شكرًا لك. معكم باري ليبا من اللجنة الاستشارية للأمن والاستقرار. أود فقط توضيح نقطة أرى أنه من المهم التأكيد عليها دائمًا عندما نتحدث عن تشفير ما بعد الكم، وهي أن هناك مفهومًا خاطئًا شائعًا بأن الحواسيب الكمية تُعرّض جميع أنظمة التشفير لدينا للخطر. وأود أن أوضح، كما أشار كريستيان عند حديثه عن التوقيعات الرقمية والتوقيع الإلكتروني،

أن هذا نوع معيّن من التشفير وهو الذي يتأثر بالحواسيب الكمومية. أما التشفير العام الذي نستخدمه لتأمين حركة البيانات على الإنترنت فليس معرضًا للخطر بنفس الطريقة. الخطر يتركز تحديدًا على أنواع التشفير المستخدمة في التوقيعات الرقمية وتبادل المفاتيح. ولهذا السبب نُولي هذه القضايا أهمية خاصة عند مناقشة موضوع تشفير ما بعد الكم.

كريستيان هيسلمان أجل. وبشكلٍ خاص، فإن نظام أسماء النطاقات لديه شروط محددة، على سبيل المثال، ضرورة أن تتناسب البيانات كافة مع حزمة بروتوكول بيانات المستخدم. وهذه من حالات الاستخدام التي لا يأخذها فريق العمل في لدى المعهد الوطني للمعايير والتكنولوجيا بعين الاعتبار حاليًا. ولذا، سيكون من المفيد للغاية التواصل معه ولفت انتباهه إلى هذه الحالة، التي أعتبرها حالة استخدام بالغة الأهمية، وينبغي أخذها في الحسبان.

ماركو هوغوونينغ شكرًا لك. أعتقد أن بيتر معنا عبر الإنترنت، بيتر توماسون، هل أنت معنا؟

بيتر توماسون في الواقع، أنا هنا. مرحبًا. معكم بيتر توماسون، عضو في اللجنة الاستشارية للأمن والاستقرار. وأود أن أضيف جانبًا مهمًا: ألا وهي أن نسبة الدخول للامتدادات الأمنية لنظام اسم النطاق لا تزال منخفضة نسبيًا، فهي تمثل حوالي 5% في نطاق com. على سبيل المثال. ولكن إذا نظرنا إلى الأرقام المطلقة، فنحن نتحدث عن أكثر من 10 ملايين اسم نطاق. وهذا رقم كبير بالفعل. ولا يزال من غير الواضح حتى الآن ما هي طريقة الدخول التي سيتم اعتمادها في المستقبل عندما يتعين على الامتدادات الأمنية لنظام اسم النطاق الانتقال إلى طريقة خوارزميات ما بعد الكم. ولكن من المؤكد أنه ستكون هناك عملية انتقال من نوع ما. وفي ظل وجود أكثر من 10 ملايين نطاق موقع حاليًا – وربما سيكون العدد أكبر بكثير وقت الانتقال – فإن تنفيذ هذه العملية بشكلٍ غير منسق سيكون أمرًا بالغ الصعوبة. لذا، من الأهمية بمكان دعم هذا الانتقال من خلال عملية الأتمتة.

في الخريطة التي عرضتها – لا حاجة للعودة إليها الآن – كانت هناك بعض البلدان المظلّلة باللون الأزرق. وهذه البلدان تمثّل نطاقات المستوى الأعلى لرمز البلد (ccTLD) التي

تدعم الأتمتة في مثل هذه التغييرات. لذا، من الأمور التي ينبغي التفكير فيها هو ما إذا كانت بلدك – لا أعني بلدك تحديدًا بل أي بلد – يرغب في إضافة دعم لمثل هذه الانتقالات الآلية. وأعتقد أن اللجنة الاستشارية للأمن والاستقرار ستكون سعيدة بالتفاعل معكم بشكلٍ أوسع بخصوص أي جانب من هذه الجوانب. فلا تترددوا في التواصل معي أو مع أي عضو آخر من اللجنة إن كان لديكم اهتمام بهذا الموضوع.

كريستيان هيسلمان هذه نقطة ممتازة. شكرًا لك.

ماركو هوغوونينغ شكرًا لك. لا يزال لدينا بعض الوقت المتبقي، فإذا كان لدى أحدكم أي أسئلة أخرى، فليتفضل. نيكو، تفضل السيد الرئيس الكلمة لك.

نيكولاس كاباليرو شكرًا لك. شكرًا جزيلاً. وأتوجه بشكر خاص لرام وفريقه على العرض الرائع. إنه لمن دواعي سروري دائمًا وجودكم معنا. هناك أمران سريعان أود الإشارة إليهما: أولًا، إذا كان بالإمكان أن ننسّق – وكلامي موجه إلى رام وكريستيان – ونستفيد من وجود زميلي العزيز والمرموق جيم غالفين معنا في الغرفة، بأن ننسّق عرضًا تقديميًا لمجلس الإدارة خلال اجتماع مسقط في سلطنة عُمان، والمقرر عقده في أكتوبر/تشرين الأول. ربما نحتاج إلى تقديم نسخة مبسّطة نوعًا ما (نسخة "بسيطة ومفهومة" إن صح التعبير)، باستثناء ثلاثة أو أربعة أعضاء في المجلس ممن يتمتعون بخلفية تقنية قوية. ذلك من ناحية.

ومن ناحية أخرى، وبما أنني أجلس بجانب زملائي الأعزاء من البرازيل، أود أن أستغل هذه الفرصة للإشارة إلى أننا نقوم بتنظيم جلسة لبناء القدرات على المستوى الإقليمي موجهة لدول أمريكا اللاتينية، وستُعقد إما في ساو باولو أو برازيليا – لا زلنا بصدد تحديد المكان. وسواءً قبل انعقاد اجتماع عُمان أو بعده، هل سيكون بإمكانكم مساعدتنا في هذا السياق؟ سنركّز في هذه الجلسة بشكل أساسي على تنفيذ الامتدادات الأمنية لنظام اسم النطاق، إلى جانب مراجعة مختصرة حول التشفير، بنوعيه المتماثل وغير المتماثل، والإشارة إلى مسألة

خوارزميةRSA، التي – وأرجو تصحيح الأمر لي إن كنت مخطئًا – يُقال إنه قد تم كسرها منذ أسبوعين أو ثلاثة، لا أعلم إن كان ذلك مؤكدًا، لكن سمعت بعض الأحاديث بهذا الشأن.

على أي حال، هذا من جهة. ومن جهة أخرى، هناك العديد من المزايا التي توفّرها البرمجيات مفتوحة المصدر للحكومات. أنا شخصيًا مستخدم كبير ونشط لهذه البرمجيات، لكنني أجد صعوبة في شرح فوائدها بكلمات بسيطة للأشخاص الذين لا يملكون خلفية تقنية – سواءً من الناحية التقنية أو الاقتصادية أو غيرها من الجوانب. ومن الأمور التي أجد صعوبة في إيصالها، هي روعة تراخيص مثل GPL-2 وGPL-3، وأهمية هذه التراخيص بشكلٍ عام، ولماذا تُعدّ أمرًا جيدًا وجديرًا بالدعم. لذا، بمساعدتكم وخبرتكم، قد نتمكّن من إيصال هذه المفاهيم بشكلٍ أكثر نجاحًا وتأثيرًا. إذن، هذان هما الأمران الأساسيان: أولًا، عرض تقديمي لمجلس الإدارة؛

وثانيًا، المساعدة في جلسة بناء القدرات الإقليمية الموجّهة لدول أمريكا الجنوبية، والتي من المحتمل أن تُعقد في ساو باولو أو برازيليا.

رام موهان نيكو، شكرًا لك على ذلك. نحن متوافقون تمامًا مع هذين المقترحين، وسنكون سعداء بالمساهمة المباشرة فيهما معًا. يرجى التواصل مع لاحقًا، وسأكون سعيدًا بتيسير الأمر.

كريستيان هيسلمان نعم، وأنا كذلك.

نيكولاس كاباليرو الآن، عذرًا، لكن فيما يخص كسر خوارزمية RSA – هل يمكنك من فضلك توضيح ذلك؟

وارن كوماري نعم، أعتقد أنك تشير إلى ورقة بحثية نُشرت مؤخرًا من قبل شركة Google، وهي ورقة أكاديمية تُشير إلى أن "العتبة" اللازمة لكسر خوارزمية RSA قد انخفضت. لكن لم يحدث أي شيء فعلي حتى الآن – المسألة تتعلق فقط بكمية تشفير ما بعد الكم التي تحتاجها –

عذرًا، أقصد مدى تعقيد الحاسوب الكمي المطلوب – وهذا ما كان محل شك. السؤال الآن كم عدد البتات الكمية (الكيوبتات) التي تحتاجها فعليًا لبناء نظام كمي موثوق؟

ما ترشدنا إليه هذه الورقة هو أنك لست بحاجة إلى عددٍ كبير للغاية كما كان متصورًا، لكن ما زال من غير الواضح كم من الوقت سنحتاج لنقلق بشأن هذا الأمر بالفعل. إذا سألت مجموعة من الخبراء، ستحصل على تقديرات مختلفة تمامًا.

لكن المؤكد هو أن خوارزمية RSA لم تُكسَر بعد – إنما هناك مؤشرات على أنها قد تُكسَر في المستقبل، خلال عدد من السنوات، ولكن لا أحد يعرف على وجه الدقة متى. هناك صفحة (حاولتُ العثور عليها) تجمع متوسط التقديرات من عددٍ كبير من علماء الحوسبة الكمية، وهذا "المتوسط" يتغيّر باستمرار. قد يحدث الأمر غدًا، وقد يكون بعد 50 سنة، وقد يكون بعد 500 سنة، من الصعب جدًا التنبؤ بدقة. لكن الأرجح أن ذلك سيكون في غضون بضع سنوات، على الرغم من صعوبة الجزم بذلك.

الأمر يشبه الحديث عن طاقة الاندماج النووي: يُقال دائمًا إنها قادمة خلال العشرين سنة القادمة، وقد قيل ذلك منذ عقود. مع ذلك، فإن الاستعداد المسبق أمر بالغ الأهمية، لأنه إذا حدث فعلاً وتم كسر RSA بسهولة، أو أي خوارزميات تشفير أخرى، فعلينا أن نكون قد بدأنا التحضير لذلك قبل وقت طويل من وقوعه.

نيكولاس كاباليرو — إذن علينا الاستعداد للمشكلات وحلها قبل أن تتفاقم وتصبح أزمات، أليس كذلك؟

ماركو هوغوونينغ — حسنًا. شكرًا لك. تبقّى دقيقتان فقط قبل استراحة القهوة. هناك شخص يطلب الكلمة من أستراليا، أقترح أن نأخذ السؤال بسرعة. هل هذا إنغرام؟

إنغرام نيبلوك — مرحبًا بكم. شكرًا على ذلك. كنت أتساءل بشأن الجدول الذي ظهر في شريحة سابقة، والذي تضمن مقارنات مختلفة – مثل أحجام المفاتيح، وسرعة التوقيع، وما إلى ذلك. أفهم

تمامًا مسألة أحجام المفاتيح، نظرًا لقيود حجم حزم البيانات الخاصة ببروتوكول بيانات المستخدم. لكنني كنت أتساءل: ما الأثر العملي لزيادة أزمنة التوقيع؟ إذا زاد وقت التوقيع – لا أذكر الرقم الذي ذكرتموه بخصوص نطاق .nl – مثلاً من دقيقتين إلى عشر دقائق، فهل يُشكّل ذلك مشكلة؟ هل يتم التوقيع بهذه الوتيرة العالية لدرجة أن الزمن الإضافي يصبح عائقًا فعليًا في نظام أسماء النطاقات؟

كريستيان هيسلمان

حسنًا، لدينا حوالي 6.2 مليون اسم نطاق في منطقتنا، وحوالي 60% منها موقّعة، ونعمل ضمن نافذة نشر مدتها حوالي 30 دقيقة، ما يعني أننا بحاجة إلى إعادة التوقيع كل 30 دقيقة. فإذا استغرق توقيع البيانات وقتًا طويلاً جدًا، فقد لا يكون لدينا وقت كافٍ لإتمام العملية بالكامل. أجل. ولهذا السبب كنا نرغب في معرفة أثر زمن التوقيع.

مارتن أيرتسن

هذا الأمر يعتمد أيضًا على نموذج النشر المُتّبع. فكريستيان يصف نموذجًا معينًا يتم فيه توقيع المنطقة الكاملة بالكامل في كل مرة. لكن هناك أيضًا نماذج أخرى، مثل التوقيع المتزايد، أو حتى التوقيع الفوري لكل عملية استفسار. لذلك، من الصعب إعطاء إجابة عامة وشاملة على هذا السؤال، لكن ما يمكن قوله بثقة هو أن سرعة التوقيع تظل عاملاً مهمًا.

بيتر توماسون

ربما النقطة الرئيسية هي أنه كلما طال وقت التوقيع، زادت التعديلات الأخرى التي تحتاج إلى إجرائها على نموذج النشر.

ماركو هوغوونينغ

شكرًا لك. أرجو تكون هذه إجابة شافية عن سؤالك. لقد انتهى وقتنا الآن. ويسعدنا أن نرى أنه قد تم بالفعل تحديد بعض المواعيد للمتابعة. أنصحكم بالبحث عن زملائنا خلال استراحة القهوة إذا رغبتم في الحصول على مزيد من المعلومات. وأعتقد أن هناك عددًا لا بأس به من ممثلي مؤسسة تسجيل النطاقات الهولندية موجودون هنا،

وبالطبع، فإن أعضاء اللجنة الاستشارية للأمن والاستقرار متواجدون أيضًا بكثرة. ومرة أخرى، أتوجه بالشكر لكلٍ من رام، وورن، وغريغ، ومارتن، وكريستيان، على ما قدمتموه من معلومات قيّمة، ولاصطحابنا في هذه الرحلة التي كانت تتناول المسائل التقنية في كثير من جوانبها، ومحاولة مساعدتنا على فهم ما يجري بشكلٍ أوضح.

وقبل أن نذهب إلى استراحة القهوة، أود أن أذكّر أنه بعد انتهاء الاستراحة بنصف ساعة، سنعود إلى جلسة "WHOIS ودقة البيانات" هنا في القاعة الخاصة باللجنة الاستشارية الحكومية. لذا، إلى زملائنا في اللجنة الاستشارية الحكومية، آمل أن أراكم جميعًا هنا مجددًا. أما بالنسبة للآخرين، فأرجو أن تكونوا قد استفدتم من هذه الجلسة المثرية. شكرًا لحضوركم، واستمتعوا بتناول القهوة. شكرًا لك.

[نهاية التدوين النصي]