AR

ICANN81 | الاجتماع العام السنوي – اجتماع مشترك: GAC وSSAC
الأحد 10 نوفمبر/تشرين الثاني 2024 – 16:30 إلى 17:30 بتوقيت تركيا

جوليا تشارڤولين: أهلًا ومرحبًا بكم في اجتماع اللجنة الاستشارية الحكومية GAC واللجنة الاستشارية للأمن والاستقرار SSAC. معكم جوليا تشارڤولين من فريق دعم ICANN GAC. يُرجى العلم بأن هذه الجلسة يجري تسجيلها وتخضع لمعايير السلوك المتوقعة في ICANN وسياسة ICANN لمناهضة التحرش.

خلال هذه الجلسة، لن تتم قراءة الأسئلة أو التعليقات بصوت عال أثناء هذه الجلسة ما لم تُقدم في حيز الدردشة. 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. يُرجى ذكر اسمك واللغة التي ستتحدث بها إذا كانت غير الإنجليزية، وتذكر أن تتحدث بسرعة معقولة. وسأسلم الكلمة الآن إلى نايجل هيكسون. نايجل، من فضلك، دورك.

نايجل هيكسون: مرحبا مساء الخير. لقد سمعتم ما يكفي من صوتي اليوم، أليس كذلك؟ لذا، فلن تسمعوا الكثير منه في هذه الجلسة. وأعدكم أني سأكون هادئًا غدًا. إذن، نيكو يرسل اعتذاره. لقد كان عليه حضور جلسة لمجلس إدارة ICANN. ولكن ليس لدي الكثير لأفعله. وكما ترون، فإن نسبة GAC إلى SSAC هي كما ينبغي أن تكون. لا، هذه جلسة من جلسات SSAC.

يسعدنا أن يكون لدينا الفرصة لتلقي إحاطة منهم. لقد بذلوا على مر السنين الكثير من العمل للمساهمة في تشغيل ICANN الفعال. وأنا متأكد من أنكم ستجدون ما يقولونه مثيرًا للاهتمام حقًا. حسنًا، كل ما سأفعله الآن هو أنني سأقوم بتسيير الأسئلة والمناقشات لاحقًا. ولكن كل ما علي فعله الآن هو تسليم الأمر إلى رام.

رام موهان: شكرًا جزيلًا. وشكرًا على دعوة SSAC للاجتماع معكم هنا في GAC. وإنه من دواعي سروري دائمًا أن أكون معكم. معكم رام موهان. رئيس اللجنة الاستشارية للأمن والاستقرار SSAC.

قبل أن أبدأ بجدول الأعمال هنا، اسمحوا لي أيضًا أن أتوجه إلى زملائي المصطفين هنا وأطلب منهم أن يأخذوا لحظة لتقديم أنفسهم. كلهم أعضاء في SSAC. وتعلمون، سيكون لديكم الفرصة لرؤية تنوع المعرفة والخبرة والتخصص هنا. لنبدأ من يميني.

رود راسموسن. رود راسموسن.

ميريك كايو: ميريك كايو.

غريغ آرون: غريغ آرون.

روبرت جويرا: روبرت جويرا.

وارن كوماري: وارن كوماري.

جون ليفين: جون ليفين.

ستيف كروكر: ستيف كروكر.

تارا والين: تارا ويلان، نائب رئيس SSAC.

باري ليبا: باري ليبا. وأحاول، لكن وارن لديه قبعة أفضل.

سوزان وولف: سوزان وولف، التي ترتدي في بعض الأحيان الكثير من القبعات، SSAC.

رام موهان: شكرًا لك يا سوزان. وهناك بعض الأعضاء أراهم أيضًا هناك في الخلف. وسترونهم يرفعون أيديهم. وهم موجودون هنا أيضًا في الغرفة ليكونوا معنا في هذه الجلسة. شكرا لك يا نجمان على استضافتنا هنا. جيب، لم ترفع يدك. ينبغي عليك رفع يدك. هيا. شكرًا لاستضافتنا هنا. لقد فكرنا في أن نبدأ أولًا، نظرًا لأن ليس جميعكم قد رأونا من قبل، بقضاء بضع لحظات في تقديم أنفسنا، ومن نحن وماذا نفعل، ثم ننتقل إلى بقية الموضوعات.

إذا نظرت إلى مهمة ICANN نفسها، فهذا واضح إلى حد ما. تم إنشاء SSAC بشكل مباشر تحت مهمة ICANN. ونحن إذن لجنة استشارية، تمامًا كما أنكم لجنة استشارية. وليس لدينا أي نوع من السلطة الرسمية، إذا صح التعبير، داخل هيكل ICANN. نحب الأمر بهذه الطريقة لأن مشورتنا يجب أن تعيش وتموت بناءً على جدارتها بدلًا من أن يكون لدينا صوت أو لا يكون لدينا صوت، أليس كذلك؟ إذن، هذا هو نحن.

ننتمي إلى كافة أنحاء العالم، أو على الأقل من معظم أنحاء العالم. ونسير على الطريق الذي نعمل من خلاله على زيادة التنوع في العضوية بجميع الطرق التي تقيس بها التنوع. في هذا العام وحده، أضفنا تسعة أعضاء جدد. ومن بين هؤلاء الأعضاء التسعة الجدد، يسعدنا أن نرى أن اثنين منهم يأتون من أفريقيا، وأجزاء أخرى من العالم أيضًا. ولكن السبب الأساسي وراء وجود الأشخاص في SSAC، واختيارهم ليكونوا في SSAC، هو أنهم يجلبون خبرة محددة، وبشكل عام، عميقة في المجال الذي يتخصصون فيه. ومعظم الأشخاص في SSAC هم خبراء فنيون.

لديهم مجموعة متنوعة من الخبرة. لدينا أشخاص يتعاملون مع مجالات مختلفة من نظام معرفات الإنترنت. وهؤلاء هم في الغالب من نستمد منهم. لكن هناك قدرًا كبيرًا من المعرفة والخبرة

التي تبقى داخل SSAC. والسبب في ذلك هو أننا نركز في المقام الأول على تقديم المشورة الفنية للمجتمع الذي نخدمه، أليس كذلك؟ لذلك، نحاول أن يكون لدينا مجموعة من الأشخاص الفنيين ذوي الخبرة معنا. شكرًا.

هذا هو فريق قيادة SSAC. سترون، على يساري، وعلى يمينكم، الأعضاء الذين تم اختيارهم وانتخابهم ليكونوا داخل فريق القيادة. وما ترونه هو أيضًا موظفو دعم السياسة. وأود أن آخذ هذه اللحظة لذكر هذا. على عكس العديد من الأجزاء الأخرى في ICANN، حيث ينتهي الأمر بموظفي الدعم إلى الاضطلاع بدور الدعم، داخل SSAC، عندما تنظر إلى الأشخاص المدرجين هنا، ستيف تشنغ، على سبيل المثال، فإن الأشخاص الآخرين المتواجدين هنا هم خبراء مؤهلون للغاية في حد ذاتهم.

وبالتالي، فإنهم ينتهي بهم الأمر إلى المشاركة، والمساهمة في المناقشات التي نجريها، والقيام بأكثر من مجرد كونهم كتبة. إنهم غالبًا ما يقدمون إرشادات مفيدة للغاية ويقدمون مدخلات مفيدة أثناء عملنا على الموضوعات المختلفة التي تهمنا. وإذا نظرت إلى المهارات التي يتمتع بها فريق القيادة هذا فقط، فسوف ترى مجموعة منها. ولكن إذا نظرت إلى ذلك في جميع أنحاء SSAC، فهناك تنوع أكبر منه.

لدينا أشخاص يأتون من الأوساط الأكاديمية. لدينا أشخاص من المجتمع المدني، ومن خلفيات الأعمال، ومن خلفيات الحكومات، ومن خلفيات إنفاذ القانون. والطريقة العامة التي يتمكن بها الأشخاص من الالتحاق باللجنة SSAC هي عملية تقديم طلب مفتوحة. يقومون بتقديم طلباتهم. هناك لجنة عضوية داخل SSAC، وتقوم هذه اللجنة بفرز الطلبات وإجراء المقابلات. وبمجرد الانتهاء من تلك المقابلات، يقومون بترشيح الأشخاص للانضمام إلى SSAC.

يحق للجنة SSAC أن تبدي رأيها بشأن هؤلاء الأشخاص. وعندما ننتهي من كل هذه العملية، نقدم قائمة بالأعضاء الموصى بهم لمجلس الإدارة. يتم تعيين كل عضو في SSAC من قِبل مجلس إدارة ICANN. لذا، سأطلب من تارا أن تتحدث في هذا الموضوع، لأن هذا هو جوهر ما نقوم به.

تارا والين: شكرًا يا رام. بالنسبة لمن لا يعرفون SSAC، فإننا ننتج قدرًا كبيرًا من المواد التقنية ونقوم بذلك منذ عدة سنوات. وقد تختلف المواضيع. إنها تتعلق بأمن معرفات الإنترنت واستقرارها عبر مجموعة من المواضيع. ولكن هناك بعض المواضيع التي تعود مرارًا وتكرارًا وتعتبر مواضيعنا الدائمة. ولذلك، فإننا نعمل على إيجاد طرق للتركيز على هذه الأمور وجعل هذه المواد متاحة بسهولة للمجتمع.

ومع تطور هذه المواضيع المهمة المتكررة، يمكنك أن تأتي إلينا وتحصل على إجابات لأسئلتك. حسنًا، المواضيع التي حددناها هنا، أحدها هو انتهاك DNS. وبطبيعة الحال، يعد نظام DNS نظامًا مهمًا، وهذا ما يجعله مكانًا تحدث فيه أيضًا كميات كبيرة من الانتهاكات عبر الإنترنت. إنها أداة مفيدة للأشخاص الذين يريدون التسبب في قدر كبير من الضرر. لذا، إذا كان الناس يقومون بهجمات التصيد، أو يقومون بنشر البرامج الضارة، فإننا ننظر إلى دور DNS في هذا الأمر، وما الذي يمكننا فعله للتخفيف من حدته. لذا، فهذه منطقة نصدر فيها في كثير من الأحيان تحذيرات ونعمل مع اللجان لمحاولة التخفيف من هذا الضرر.

أما المجال الثاني، والذي قد يكون في أذهان العديد من الأشخاص الذين يتطلعون إلى الجولة القادمة، فهو نطاقات gTLD الجديدة. في كل مرة تريد إضافة أسماء جديدة إلى النظام، هناك مشكلات تتعلق بالأمان والاستقرار. ربما كان الناس يتابعون مشروع تحليل تضارب الأسماء، على سبيل المثال، للنظر إلى ما سيحدث عندما يكون هناك توسع. لذا، لا نريد أن نواجه مشاكل تتعلق بنوع من الارتباك بشأن السلاسل. هناك الكثير من العمل الذي يُبذل لتوقع هذه القضايا. وبما أن هذه قضية في وقتها المناسب، فقد طلب منا المشورة بشأن هذا الموضوع.

هناك أيضًا الامتدادات DNSSEC. فهذه واحدة من تقنيات الأمان الأساسية في مجال DNS. لقد عملنا مع آخرين في هذا المجال لبعض الوقت لتقديم المشورة، والترويج لهذه التكنولوجيا، ومحاولة التأكد من طرحها بشكل جيد، وتنفيذها بشكل جيد. ندرك أن الأمر معقد، وأن الناس غالبًا ما يحتاجون إلى بعض المساعدة لمحاولة جعله يعمل بالطريقة المقصودة. نود أن نضمن حصول الناس على مشورة جيدة. قد تكون هناك أشياء مثل تشغيل أتمتة أفضل، على سبيل المثال، لتسهيل على الأشخاص وضع وظيفة الأمان هذه وجعلها متاحة بسهولة مرة أخرى.

هناك أيضًا مشكلة فضاءات الأسماء البديلة. ربما رأى الناس هذا في السنوات الأخيرة عندما كانت تقنية سلسلة الكتل في الأخبار بشكل كبير. وهذا بالتأكيد لم يختفي. ولكن كان هناك الكثير من أنظمة التسمية الأخرى التي لم تكن مطابقة لتلك المقدمة في DNS. كان الناس يفعلون أشياء

للعملات المشفرة ويسمحون لك بشراء أنواع مختلفة من النطاقات، والتي، بالطبع، تثير مشكلات حولها، فكيف يتم ذلك، بأي طرق تتفاعل أو تتكامل مع DNS؟ كيف سنتوقع القضايا المختلفة التي يطرحها التعايش بين هذه الأنظمة؟ لذا، فإننا نستمر في النظر في هذا الأمر لأنه مجال متطور للغاية.

وأخيرًا، هناك موضوع قد يدور في أذهان العديد من الأشخاص في هذا الجمهور على وجه الخصوص وهو قضايا حوكمة الإنترنت، ولكن بشكل خاص تلك التي تتعلق بالأمن والاستقرار، وهذا هو محور تركيز مجموعتنا، لأن هناك العديد من القضايا في الإنترنت والتي تتداخل فيها المساحة الفنية والسياساتية مع الكثير من الأسئلة المعقدة للغاية على كلا الجانبين. وإذا كنت ستتخذ قرارات في هذا المجال، فمن المفيد جدًا أن يكون لديك إرشادات واضحة ومفيدة من الأشخاص الفنيين لمساعدتك في اتخاذ هذه السياسة.

نود أن نكون في وضع يسمح لنا بتقديم هذه المعلومات من وجهة نظرنا الفنية. ولكننا نلاحظ أيضًا أن عملنا يكون أقوى عندما نحصل على مدخلات من الأشخاص الذين يحتاجون إلى تلك المشورة لمحاولة توجيهها بالطرق الصحيحة، للتأكد من أننا نجيب على الأنواع الصحيحة من الأسئلة، للتأكد من أننا نوصل الرسالة بالمستوى الصحيح من التواصل بالمستوى الصحيح من التفاصيل.

لذا، فإننا نقدر كثيرًا عندما نتمكن من التفاعل مع، أو على سبيل المثال، التحدث مع، أو دعوة خبراء للتشاور مع الأشخاص أثناء وضع مشورتنا بحيث تكون مفيدة للجمهور في مجال السياسة، في الحالات التي يكون من المفترض أن تكون فيها مفيدة لجمهور ما، فهذا يمثل جانبًا تعاونيًا للغاية بالنسبة لنا لإنتاج النوع الصحيح من المشورة المفيدة للجمهور.

إذن، لدينا الآن مجموعتان عمل تنتجان بعض الأعمال. وبالمناسبة، فإن عملنا قد يمتد في كثير من الأحيان إلى أكثر من مجال واحد من هذه المجالات. لكن اثنتين من المبادرات الجارية الآن هي مجموعة خاصة بالبرمجيات الحرة والمفتوحة المصدر في البنية التحتية لنظام اسم النطاق DNS. حسنًا، قد يعرف البعض منكم أن العديد من المكونات التي يتم طرحها في البنية التحتية لنظام اسم النطاق، والأشياء التي قد تكون موجودة في المُحلِّلات، على سبيل المثال، الكثير من هذه المكونات هي جزء من مبادرات مفتوحة المصدر. ويمكن أن تكون هذه مجموعات كبيرة أو صغيرة بمبالغ مختلفة من التمويل وقد يكون لديها أنواع مختلفة من الالتزامات والاتفاقيات التعاقدية والعلاقات مع أطراف مختلفة. وهذا جزء من البنية التحتية الحيوية لتشغيل DNS.

لذا، اعتقدنا أنه سيكون من المفيد توضيح مكان بعض هذه التبعيات حتى يتمكن الأشخاص من رؤية مكان وجود هذه البرامج مفتوحة المصدر، وأين تعتمد عليها، وربما أيضًا للتشكيك في بعض الافتراضات التي لدى الأشخاص حول هذه البرامج، وما يمكنها وما لا يمكنها فعله، وما قد تفكر فيه بشأن موثوقية وقوة هذه البرامج.

الآن، لدينا على الأقل أحد رؤساء هذا الطرف هنا. مارتن ليس هنا. لدينا واحد. حسنًا، فقط أتحقق مما إذا كنت قد قمت بشكل صحيح -- نعم، لقد أعطاني الرئيس إبهامًا لأعلى لأنني قمت بتلخيص مجموعات العمل بشكل صحيح. وهذا العمل قد بدأ للتو. نأمل أن يتطلع بعضكم إلى النتائج عندما تظهر إذا كنتم مهتمين بالبرمجيات مفتوحة المصدر. هناك شيء آخر نعمل عليه وهو نوع من حظر DNS وتصفيته. إحدى آليات حظر المحتوى عبر الإنترنت هي استخدام DNS كأحد الأساليب لإدارة حظر المحتوى بين المستخدمين النهائيين والمورد.

وقد كان هذا الأمر مستمرًا لبعض الوقت باعتباره تقنية، وقد نظرت SSAC في هذا الأمر، ولكن آخر الاستشارات التي أصدرناها يعود تاريخها إلى ما يزيد عن عقد من الزمان. ومنذ آخر مرة كتبنا فيها عن هذا الموضوع، تغير المشهد التكنولوجي، وتغير المشهد التنظيمي. لذلك، اعتقدنا أنه حان الوقت لإلقاء نظرة على هذه الأمور مرة أخرى.

في العديد من الجوانب التقنية، على سبيل المثال، العديد من استعلامات DNS تعمل الآن عبر وسائل نقل تجعل الأمر أقل وضوحًا. لم يعد الناس قادرين على النظر إلى الاستعلامات بالطريقة التي اعتادوا عليها. لذا، ربما أدى هذا إلى تغيير الاستجابات والمعلومات التي يحصل عليها الأشخاص عند اكتشاف كيفية حظر المحتوى.

هذه بالتأكيد منطقة حيث يمكننا أن نستفيد من المدخلات، حيث تحدثنا مع أشخاص في مجال السياسة. لقد كنا محظوظين لأننا تمكنا مؤخرًا من مناقشة ما سمعوه من ما كانوا يتابعونه أثناء مواكبتهم لمجال السياسة مع الأشخاص المسؤولين عن السياسات في ICANN. ونحن ممتنون جدًا لحصولنا على هذا النوع من المدخلات لإثراء الاتجاه الذي يمكننا من خلاله نقل الوثائق بحيث تعالج مرة أخرى تلك الأسئلة الأكثر إلحاحًا. ومرة أخرى، نؤكد أننا نحب هذه العملية التعاونية.

هذه إذن وجهة نظر رفيعة المستوى لمواضيعنا. لدينا مستوى أعمق، وهو المستوى الذي قلت إن شخصًا آخر سيتناوله في الشريحة التالية.

رام موهان: قبل أن ننتقل إلى الشريحة التالية يا نايجل، أتساءل عما إذا كنا نريد أن نخصص لحظة هنا ونسأل ما إذا كان هناك أي أسئلة أو مداخلات يرغب الناس في تقديمها.

نايجل هيكسون: نعم، شكرا لك يا رام. كنت سأفعل ذلك لأننا حصلنا على قدر لا بأس به من المعلومات. ومن المثير للاهتمام للغاية أن لديكم موضوعات مستقرة تعودون إليها لأنها جميعها ذات صلة وثيقة. إذن، هل لديكم أي أسئلة أو ملاحظات قبل أن نتعمق أكثر في قضايا الذكاء الاصطناعي وسلسلة الكتل؟ عليكم لفت الانتباه إذا كان هناك أي شيء عبر الإنترنت. دانيال؟ أوه أصدقائنا. نعم، الاتحاد الأوروبي، من فضلك.

جيما كارولليلو: شكرًا لك يا نايجل. جيما كارولليلو من المفوضية الأوروبية. مجرد تعليق مختصر. أولًا، من الجيد جدًا أن نرى أن معظم ما هو على طاولتكم، هو على طاولتنا. لذا، ربما ينبغي لنا أن نراكم في كثير من الأحيان، أكثر مما نفعله اليوم. ثم السؤال السريع الآخر، بما أنني أفهم أن العمل على أمن المصادر المفتوحة قد بدأ للتو أو بدأ مؤخرًا، وهذا موضوع ذو أهمية كبيرة بالنسبة لنا، هل يمكننا تحديد نقطة محددة، هل هناك لحظة لإعادة الاتصال والحصول على مزيد من المعلومات حول هذا العمل. شكرًا.

باري ليبا: حسنًا، سأخذ ذلك. معكم باري ليبا. أشترك في رئاسة فريق العمل الذي سيعمل على إنتاج هذه الوثيقة. نعم، سنكون سعداء بتقديم هذا لكم بشكل دوري مع تقدمنا. نأمل أن يسير فريق العمل بسرعة وأن ننتهي منه خلال اجتماعيّ ICANN التاليين. لذا، ربما في المرة القادمة في سياتل، يمكننا أن نقدم لكم تحديثًا عن ما أنجزناه.

جيما كارولليلو: فقط أريد أن أقول أن ذلك سيكون رائعًا، شكرًا لك.

رام موهان: هناك شيء واحد أود إضافته علاوة على ما قاله باري للتو، وهو أن هناك أيضًا فرصة لفرق العمل وفقًا لتقدير الرؤساء لدعوة الخبراء أو دعوة الأشخاص الذين لديهم معلومات للحضور وتقديم إحاطة يمكن أن تكون مفيدة لما يفعله فريق العمل. هناك فرصة للقيام بذلك ربما في فترات ما بين الجلسات أيضًا، باري.

نايجل هيكسون: هل هناك المزيد؟ حسنًا، ستكون هناك فرص للعودة بعد الجلسة القادمة. إذن، رام، عودة إليك.

رام موهان: شكرًا جزيلًا. حسنًا، دعونا ننتقل الآن إلى الشريحة التالية. كان جيف بيدسر يخطط للحضور إلى هنا لتقديم هذا العرض، لكنه لسوء الحظ لا يشعر بأنه على ما يرام. لذا، سأتولى هذا الجزء. اعتقدنا أنه قد يكون من المفيد لكم سماع آراء بعض أعضائنا حول الذكاء الاصطناعي وانتهاك نظام اسم النطاق. ولم تقم اللجنة SSAC بتكليف فريق عمل لدراسة هذا الموضوع وتقديم مشورة التوافق في الآراء من SSAC.

لذا، ما ستشاهدونه هنا في الشرائح القليلة القادمة مأخوذ إلى حد كبير من خبرة بعض أعضائنا. وهذا لا يعني التحدث بصوت SSAC، بل التحدث بالمعرفة الفنية والخبرة التي يتمتع بها بعض أعضائنا في SSAC. لذا، كمجموعة من المستويات المبكرة، هناك التعلم الآلي ثم هناك الذكاء الاصطناعي. والتعلم الآلي هو جزء من ذلك. وفي هذه المجموعة الفرعية، تتعلم الخوارزميات من البيانات للتوصل إلى توقعات أو اتخاذ قرارات. في حين أن الذكاء الاصطناعي يشمل تقنيات أوسع نطاقًا تمكن الآلات من محاكاة الذكاء البشري. لذا، يعد التعلم الآلي أحد الأساليب الأساسية في مجال الذكاء الاصطناعي.

الآن، قد يكون انتهاك DNS في الواقع تطبيقًا جيدًا جدًا للذكاء الاصطناعي. ربما يكون هذا هو بالضبط نوع الشيء الذي يرغب الأشخاص الذين يريدون أن يكونوا مجرمين أو الذين هم مجرمون بالفعل في استخدامه واستغلاله. لأن الذكاء الاصطناعي، وخاصة الذكاء الاصطناعي التوليدي، لديه طريقة جيدة لإنشاء نصوص وصور ومقاطع فيديو جديدة وغيرها من التحف الفنية. على سبيل المثال، الشعارات الدقيقة جدًا للبنوك أو مواقع التجارة الإلكترونية. ومن خلال

القيام بذلك إلى جانب قدرات الذكاء الاصطناعي التوليدي والتعلم الآلي، والتعرف على الأنماط الموجودة في التعلم الآلي، فإن أنظمة الذكاء الاصطناعي قادرة على إنشاء رسائل بريد إلكتروني ورسائل نصية ومطالبات أخرى تبدو وكأنها كتبت بواسطة إنسان أو أنشأها إنسان. وبقدر ما تستطيع جعل الأمر أكثر أصالة، كلما زادت احتمالية وقوع الأهداف ضحية له.

ومرة أخرى، بالذكاء الاصطناعي التوليدي وقدراته الخاصة، في الماضي، عندما كنت أتلقى بريدًا إلكترونيًا تصيديًا، كان من الممكن أن تعتمد تقريبًا على بعض العيوب، أو شيء مصمم بشكل غير صحيح، أو قواعد نحوية خاطئة، أو تهجئة خاطئة، أو استخدام أحرف كبيرة بشكل غير صحيح. ولكن الآن، لم يعد كل ذلك يتم بشكل جيد في اللغة الأساسية فحسب، بل أصبح من الممكن ترجمته تلقائيًا إلى مجموعة كاملة من اللغات الأخرى. وهذا يعني أن حجم ونطاق المشكلة يتوسع بشكل كبير للغاية.

لذا، في الواقع، عندما تنظر إلى انتهاك نظام اسم النطاق، فإن مكافحتها على نطاق واسع كانت تستخدم حتى الآن التعرف على الأنماط ومطابقة الأنماط كآليات أساسية لمحاربة انتهاك نظام اسم النطاق على نطاق واسع. على سبيل المثال، يمكنك النظر إلى المعلومات الأساسية التي تكمن وراء اسم النطاق أو المعلومات الأساسية لمستوى معين من الاحتيال الذي يحدث. سجلات خادم الاسم NS، وأسماء المضيفين، وعناوين IP المرتبطة بها، ومن هو الاسم أو المورد المسجل به، وما هو السجل أو أمين السجل. تجد الأنماط أو تحلل المحتوى. عندما تنظر إلى ملف HTML، تنظر إلى القوالب، يتم إعادة استخدامها أو تنظر إلى قيم تجزئة الملف بسبب قيام البشر بذلك في الماضي، كانت هناك أنماط يمكن الوصول إليها وقابلة للتكرار.

باستخدام الذكاء الاصطناعي التوليدي، يمكن جعل كل نطاق أو عنوان URL محدد عشوائيًا تمامًا. مع كل عملية تصيد يتم إرسالها، فإننا نتحدث عن 100000 عملية تصيد يتم إنشاؤها خلال أربع ساعات، وغالبًا ما تتم إضافة الاسم إلى ملف المنطقة. في الماضي، كان من الممكن أن يكون لديك رسالة تصيد واحدة يتم إرسالها إلى 100000 هدف. الآن يمكنك الحصول على 100000 رسالة فردية يتم إرسالها، وكل واحدة منها تبدو أصلية، وكل واحدة منها تبدو كما لو أنها جاءت من إنسان، وكتبها إنسان. إذن، هناك طرق فعالة جدًا لجذب الأهداف.

ما هي بعض الاستخدامات الأخرى للذكاء الاصطناعي للانتهاك؟ نرى أيضًا أن الذكاء الاصطناعي يُستخدم حديثًا في التلاعب بالأشياء، وإنشاء واستخدام الهويات المزيفة، والحسابات المزيفة، والتقييمات المزيفة. اجمع ذلك مع تسجيل أسماء النطاقات وحسابات الاستضافة. ويتم

استخدامه أيضًا للصور الحميمة غير المقبولة، بالإضافة إلى المواد الإباحية الجنسية. ويتم استخدامها بشكل مباشر في التزوير وتزوير البيانات وتزوير الوثائق وتزوير الصور. ويمكنك إنشاء مستندات الهوية هذه أو مستندات أخرى في بعض الولايات القضائية. على سبيل المثال، لديك رموز البلدان التي تنص على ضرورة تقديم الهوية حتى تتمكن من الحصول على اسم النطاق.

حسنًا، الآن يمكن إنشاء هذه الهوية بدون الكثير من المتاعب. وبالتالي، فإن إحدى طرق الأمان التي تم إنشاؤها يمكن التحايل عليها بسرعة إلى حد ما. ستلاحظ أيضًا أنه ربما لاحظت ذلك، ولكنك ستلاحظ أن الصور المصاحبة لكل هذه الأشياء يتم إنشاؤها بواسطة الذكاء الاصطناعي وهي مرتبطة بالمحتوى الموجود هناك. لكنك ستجد أن بعض الصور تبدو واقعية، وبعضها لا يبدو كذلك، لكن الأمر يتحسن كثيرًا. إن نفس مجموعة المطالبات قبل عامين، ونفس مجموعة المطالبات قبل ستة أشهر، كانت ستنتج صورًا لا تبدو وكأنها تم إنشاؤها بواسطة مصمم جرافيكي.

من الصعب قليلًا قراءة كل شيء هنا على هذه الشريحة، ولكن هذه بعض البيانات التي تأتي من تقرير بحثي يتحدث عن تكرار تكتيكات الاستخدام الخاطئ التي تستخدم الذكاء الاصطناعي التوليدي. كما ترون، فإن أكبر استخدام له هو انتحال الشخصية، ولكنه يستخدم أيضًا لتوسيع وتضخيم الهجمات الموجودة، والتزوير، وما إلى ذلك. لقد تحدثت عن ذلك، اسحبها في الشريحة السابقة، لكن هذه الشريحة تأخذك إلى نهايتها تمامًا. لذا، يتم استخدامه على نطاق واسع جدًا.

وكما قال أحد مقدمي هذا العرض السابق، يبدو أن الذكاء الاصطناعي التوليدي للصور يقوم بتوليد صور أغمق فأغمق. مع تقدمنا في مجموعة الشرائح هذه، لم نحاول القيام بذلك. وهذا ما فعلته. ربما هناك إشارة هناك. لذا، على الرغم من أن القدرات قد لا تؤدي دائمًا إلى هجمات أكثر تعقيدًا، إلا أننا نعتقد أن الذكاء الاصطناعي التوليدي لديه القدرة على زيادة نطاقه ووصوله. ونقول هنا أن مجرمو الإنترنت سوف يتكاملون تدريجيًا. لقد أخطأنا. كان ينبغي لنا أن نقول، لقد قاموا بالفعل بدمج تقنيات الذكاء الاصطناعي واستخدام أنظمة الذكاء الاصطناعي في خططهم. هذا ما نراه في البرية. ولكن ليس كل الأخبار سيئة. باستثناء الصور، وسترى الوجوه الآن متشكلة. هذا ما طلبناه منه، مرة أخرى، قلنا للمحرك، بكل ما رأيته حتى الآن، قم بإنشاء هذا، وذلك ما حصلت عليه.

لذا، وعلى الرغم من إمكانية استخدام التعلم الآلي للذكاء الاصطناعي لزيادة نطاق وتكرار هذه الهجمات، إلا أن الذكاء الاصطناعي يمكن أن يكون فعالًا للغاية في الكشف عن رسائل البريد

الإلكتروني الاحتيالية. والحقيقة هي أن رسائل التصيد الاحتيالي التي يتم إنشاؤها بواسطة الذكاء الاصطناعي، على الأقل في شكلها الحالي، في جيلها الحالي، تختلف عن رسائل البريد الإلكتروني العادية التي ينتجها البشر. وهي أيضًا مختلفة عن رسائل البريد الإلكتروني الاحتيالية التي يتم إنشاؤها يدويًا. وإذا قمت بدمج التعلم الآلي ومعالجة اللغة الطبيعية، فإن ذلك يساعد في الواقع أدوات الذكاء الاصطناعي التوليدي على فهم النصوص ومعالجتها ثم تصنيعها بحيث تبدو إنسانية وأصيلة. لذا، بعد أن علمنا بوجود هذه التكنولوجيا، يمكننا نشر الذكاء الاصطناعي لالتقاط الذكاء الاصطناعي. وهذا هو ما يحدث حقًا.

لذا، فإن متجهات الهجوم والاستراتيجيات التي تستخدم الذكاء الاصطناعي لأغراض مسيئة، كثير منكم، إن لم يكن جميعكم، على دراية بهذا بالفعل. والتضليل السياسي، من السهل جدًا إنتاجه. لم تعد بحاجة إلى البشر للقيام بذلك كثيرًا بعد الآن. وبطبيعة الحال، هناك انتهاك يهدف إلى الربح وتوسع وتسريع المشاريع الإجرامية. ولكن في نهاية المطاف، ترتبط الجريمة الإلكترونية ارتباطًا مباشرًا بالأموال التي تنتجها هذه الجريمة لمرتكبيها. وهكذا، يغيّر الناس استراتيجياتهم كلما كان ذلك ضروريًا لضمان الربح.

لذا، فحتى باستخدام الذكاء الاصطناعي للإمساك بهذا النوع من المشاكل، سنرى أن التطور سوف يحدث. والذكاء الاصطناعي بحد ذاته يتطور بسرعة كبيرة. لكن بشكل عام، وجهة نظرنا هي أن هذا في الواقع استمرار لنفس مشهد التهديدات الذي ظل موجودًا منذ ظهور التكنولوجيا. لديك ممثلون قرروا استخدام التكنولوجيا والاستفادة منها لتحقيق مكاسب بطريقة ما، أو لتحقيق ميزة بطريقة ما. والحقيقة أن المهمة تكمن في التأكد من أننا نبقى على اطلاع بما يحدث، ثم ننشر التدابير التي يمكنها التخفيف من حدة هذه التهديدات، إن لم يكن مواجهتها.

حسنًا، لقد تحدثت للتو عن الذكاء الاصطناعي ونظام اسم النطاق DNS. لن أقضي قدرًا كبيرًا من الوقت على سلسلة الكتل وDNS. لقد تحدثنا عن هذا في منتديات أخرى هنا داخل ICANN. وقمنا بنشر تقرير متاح، الوثيقة SSAC123. كما استضفنا أيضًا حلقة نقاشية في ورشة عمل SSAC 2024 في واشنطن العاصمة في سبتمبر/أيلول من هذا العام. وهذا أيضًا عام. تم تسجيله. وهو متاح للجمهور. وكانت تلك حلقة نقاشية ضمت خبراء في مجال سلسلة الكتل اليوم. وشمل ذلك شخصًا من مكتب المسؤول الفني الأول في ICANN.

هناك قدر كبير من التعاون يحدث بين SSAC ومكتب المسؤول الفني الأول في ICANN للتأكد من أن لدينا توافقًا في مجالات البحث. لا نقوم بالتنسيق فيما يتعلق بالمخرجات الدقيقة للعمل الذي نقوم به، ولكننا نحاول التأكد من عدم التكرار في عملنا.

حسنًا، سأنتقل إلى الشريحة التالية. وهذه، على الأقل من وجهة نظري، هي الشريحة الأكثر أهمية، والطلب الأكبر منكم في GAC. وبمرور الوقت، وجدنا أن صناع القرار، على وجه الخصوص، لديهم حاجة إلى بناء القدرات. يرغبون في أن يتم إعلامهم بالموضوعات الرئيسية ذات الأهمية وأن يتم إعلامهم من قِبل أشخاص يعرفون بالفعل ما يتحدثون عنه، ولكنهم قادرون على التحدث عنه بطريقة يمكن فهمها لهم، وليس مجرد إلقاء المصطلحات المتخصصة عليكم. لدينا القدرة. ولدينا الفرصة للقيام بذلك.

نقدم أيضًا التقارير. وننشئ التقارير. لكن هذه التقارير عادةً ما تكون بطول عشرات الصفحات. ما نقوم به الآن هو تلخيص هذه المعلومات في ملخصات تتراوح من 500 إلى 1000 كلمة، أي صفحة أو صفحتين، ثم جمعها معًا. ولكن ما قد يساعدنا حقًا هو أن تخبرونا، كصناع سياسات، ما هي الموضوعات الأكثر أهمية بالنسبة لكم، لأن لدينا 126 ورقة بحثية كتبناها، ولا نعتقد أنه من الكفاءة أن ننطلق فقط ونجمع ملخصات لتلك الأوراق. أخبرونا بما قد يكون قيمًا بالنسبة لكم، وسنكون سعداء بالعمل جنبًا إلى جنب معكم للمساعدة في تقديم أوراق إحاطة لكم ولجمهوركم.

وأخيرًا، نود حقًا أن نفتح باب العمل معكم ومع حكومتكم. قد يكون لديكم اجتماعات مهمة حول مواضيع تتعلق بالأمن والاستقرار والمرونة. أحد الأشياء التي تحدث لكم بلا شك هو أنكم تدخلون بعض هذه الاجتماعات، ويحضرها زملاء آخرون أو صناع سياسات آخرون ليس لديهم معلومات كافية عن الحقائق الفعلية، ولكن ليس لديهم أي مشكلة في تقديم المشورة بشأن ما يجب القيام به بشأن هذا المجال المحدد. وما تجدونه بعد ذلك هو عدم التوافق بين حل السياسة والجدوى الفنية الفعلية. نعتقد أنه سيكون من الأفضل أن تستند هذه السياسة، أثناء مساهمتكم في صياغة السياسات، إلى الحقائق الثابتة والبيانات الفعلية التي يمكن أن تساعد في إنارتكم بينما تساعدون أنتم وحكوماتكم في صياغة هذه السياسات.

لذا، نود حقًا أن نفتح تلك القناة معكم ونقدم لكم النطاق والعمق من الخبرة الفنية التي نمتلكها بما يتجاوز الوثائق التي نقدمها. نعود إليك يا نايجل.

نايجل هيكسون: شكرًا جزيلًا على هذه النظرة العامة التفصيلية. وبالنظر إلى المشاعر في النهاية، أعتقد أنه من الواضح أننا، كصناع سياسات، مدينون إلى حد كبير للمشورة التي نحصل عليها من المجتمع الفني، والمشورة التي نحصل عليها من أجزاء أخرى من ICANN. أستطيع أن أتذكر جيدًا قبل بضع سنوات، وأعود قليلًا الآن، عندما كنا نناقش انتهاك DNS من حيث جولة نطاقات gTLD الجديدة والقضايا الأخرى التي وردت في تقرير SSAC الخاص بكم، ولا أتذكر رقمه، لكنني أتذكر قراءته بالتفصيل والتوصيات التي توصلتم إليها بشأن انتهاك DNS والتي كانت مؤثرة في المشورة التي توصلنا إليها في اجتماعاتنا.

أعتقد حقًا أن هناك مجالًا كبيرًا لنا للعمل معًا بشكل أفضل. وأستطيع أيضًا أن أفكر في الاهتمام الكبير الذي كان موجودًا على سلسلة الكتل على وجه الخصوص وانتهاك DNS والعمل على ذلك. وهذا بلا شك موضوع سنعود إليه في الوقت المناسب. لذا، نشكركم جزيل الشكر على إيجادنا في هذه القضايا. وسنفتح الآن بعض الأسئلة والتعليقات من جميع أنحاء القاعة. وأرى أصدقائنا من هولندا.

أليسا هيفر: شكرًا. وشكرًا لك على العرض حول كل عمل SSAC. ويجب أن يكون هذا على رأس معرفتي، ولكنني لست متأكدة فعليًا ما إذا كان هناك مسؤول اتصال بين GAC وSSAC أو العكس. إذا لم يكن هناك، أعتقد أن هذا يمكن أن يساعد بالفعل كثيرًا.

رام موهان: شكرًا لكم على كل ذلك. لا أعتقد أن لدينا دورًا رسميًا مثل هذا. وبالتأكيد نرحب بذلك إذا كنتم ترغبون في القيام بذلك. الشيء الوحيد الذي نقوم به داخل SSAC هو أن أي شخص، حتى مسؤولو الاتصال، ومسؤولو الاتصال الجدد ينتهي بهم الأمر بالمرور بنفس عملية التحقق حتى يتمكنوا من أن يكونوا أعضاء كاملين والمشاركة. ولكن لديكم الكثير من الخبرة بينكم. لذا، أعتقد أن هذا سيكون مفيدًا. لدينا جيب، وهو يجلس أمامكم مباشرةً. جيب هو عضو في SSAC. وهو في بعض الحالات يعمل بمثابة نقل غير رسمي للمعلومات، ولكن بالتأكيد ليس بطريقة رسمية.

نايجل هيكسون: شكرًا جزيلًا لك على طرح هذا السؤال المهم. وأعتقد أن الجواب هو أننا لا نفعل ذلك في الوقت الراهن. لكن من المؤكد أن هذا أمر يمكننا النظر فيه، لأنه يبدو لي أنه أمر مهم. أعني، أنتم لجنة استشارية شفافة للغاية وأوراقكم معروفة جيدًا. لكن مع ذلك، فمن المحتمل أن يكون من المهم أن يكون لديكم فكرة عن ملاءمة عملكم. فأنا عديم الفائدة بنظارتي أو بدون نظارتي. ولكن أي شخص آخر؟ آه هل كنت أنت؟ إيان أم لا؟ نعم، استمر. ثم، أمامك. ولكن إيان أولًا.

إيان شيلدون: عذرًا يا نايجل، هناك قائمة انتظار تتشكل عبر الإنترنت. أردت فقط توجيه انتباهك إلى ذلك. ولكنني كنت أيضًا في مقدمة هذا الطابور.

نايجل هيكسون: تفضل.

إيان شيلدون: شكرًا لك، رام. عضو GAC من أستراليا، إيان شيلدون معكم. شكرًا لكم على عرض المساعدة. أرى قدرًا كبيرًا من العمق والخبرة على المنصة. كما تعلمون، غالبًا ما يكون لدى أعضاء GAC ملف كبير الحجم. ونعتني بالعديد من الأمور، سواء داخل ICANN أو خارجها. ولذلك، كنت مهتمًا بسماع أفكاركم بشأن عرض الخبرة والدعم. ما مدى اتساع هذا النطاق؟ هل نتحدث فقط عن مشكلات DNS، أم أننا قادرون على الاستفادة من بعض تلك الخبرات التي قد تكون خارج هذا المنتدى هنا؟

رام موهان: شكرًا يا إيان. سؤال رائع. فيما يتعلق باللجنة SSAC نفسها، فإننا سنبقى ضمن نطاق اختصاصنا وما لدينا. ولكن لديك إمكانية الوصول إلى أعضائنا. وإذا كان الأعضاء على استعداد لمساعدتك في مواضيع خارج نطاق ICANN، فسيكون ذلك بمثابة قوة أكبر لكليكما.

نايجل هيكسون: شكرًا يا إيان. دعوني آخذ الولايات المتحدة أمامكم. وبعد ذلك سأذهب إلى القائمة الموجودة.

ليونارد هاوس: نعم، ليونارد هاوس، وزارة الخارجية الأمريكية. عندما يتعلق الأمر بمزيج الذكاء الاصطناعي التوليدي مع انتهاك DNS، فهل قاموا بأفضل الممارسات لكيفية حدوث ذلك، إما من خلال عملية التسجيل أو في مكان ما على طول الخط، فيمكنهم البحث بشكل أعمق قليلًا والوصول إلى جذر حيث يبدأ هذا الأمر، سواء كان نوعًا من اختبار تورينج أو شيء من هذا القبيل، والذي قادر على المرور وتثبيت الذكاء الاصطناعي التوليدي قبل أن يتم إطلاق العنان له، إذا صح التعبير. مجرد سؤال كجزء من التقارير حول أفضل الممارسات في هذا المجال. شكرًا. وشكرًا لكم على العمل الرائع الذي قمتم به.

رام موهان: شكرًا. لا أعرف الإجابة على هذا السؤال. لكن بإمكاني أن أسأل الخبراء داخل SSAC الذين يدرسون هذا الموضوع، وأن يعودوا إليك بهذا الشأن. أحد الأشياء داخل مساحة ICANN التي يجب أن تكون على الأقل جزءًا من الاعتبار هو، إذا كان صحيحًا أنه باستخدام الذكاء الاصطناعي التوليدي، يمكنك في غضون ساعات قليلة من إضافة نطاق إلى الحل، أن يكون لديك عدد كبير جدًا من الرسائل المسيئة تخرج. هل هناك أشياء يمكن القيام بها داخل نطاق ICANN للتخفيف من هذه المشكلة بسرعة؟ إذا حدث انتهاك خلال ساعات، فهل من الممكن التخفيف منه خلال دقائق من اكتشافه؟ أعتقد أن هذا سؤال مفتوح ينبغي لنا أن نتناوله هنا.

نايجل هيكسون: شكرًا جزيلًا. وشكرًا على هذه الإجابة. لقد حصلت الآن على شخصين أو ثلاثة أشخاص متصلين بالإنترنت. جيما من المفوضية الأوروبية أولًا.

جيما كارولليلو: شكرًا جزيلًا يا نايجل. نظرًا لأنك تسأل عن بعض المواضيع المحتملة المثيرة للاهتمام، فقد كنت أفكر هنا في GAC عند مناقشة انتهاك DNS من بين أمور أخرى، حيث ناقشنا استخدام الأدوات التنبؤية. ومن الاتحاد الأوروبي، لدينا بعض الخبرة في هذا المجال. وسيكون من الجيد حقًا أن تكون هناك مواد بالفعل أو إذا كان هناك مساحة لمزيد من العمل في إمكانات الأدوات التنبؤية لمنع انتهاك نظام اسم النطاق قبل أن نصل إلى التخفيف. وبعد ذلك أردت فقط توضيحًا صغيرًا.

إذا فهمت بشكل صحيح، باستخدام الذكاء الاصطناعي والذكاء الاصطناعي التوليدي، فإننا لا نقوم في الواقع بتوسيع نطاق التهديد. إنه أكثر، كما أود أن أقول، عدد هائل من الهجمات التي يمكنك الحصول عليها، ولكنها لا تصبح أكثر تعقيدًا. لم يعد لدينا المزيد من التهديدات، على الأقل للإبلاغ عنها في الوقت الراهن.

رام موهان: شكرًا. أما بالنسبة للسؤال الثاني، نعم هذا صحيح. لا نعتقد أن نطاق التهديدات قد توسع، ولكن وتيرة الحجم والتوسع قد توسع بشكل كبير. بالنسبة للسؤال الأول، هل هناك أي أعضاء هنا من SSAC يرغبون في الرد على زميلتنا؟

غابرييل أندروز: أستطيع أن أعطي لمحة موجزة عن إنفاذ القانون. ولكن ما نراه هو مجموعات تهديد متشابهة للغاية، نفس المجموعات الإجرامية التي كانت تقوم بالأشياء يدويًا أو تتبنى أدوات الذكاء الاصطناعي للقيام بها بكفاءة أكبر، تمامًا كما يفعل الأشرار. لذا، فإن أي شيء نلاحظه ليس جديدًا بشكل خاص. إنها نفس الحيل القديمة، فقط باستخدام أدوات جديدة لإنجازها، وهذا هو الاستنتاج العام الذي توصلنا إليه الآن من رؤيتنا في هذا الوقت.

رام موهان: شكرًا لك يا جيب. أتساءل فقط، أعتقد أنه يجب عليك إعادة صياغة هذا السؤال الأول حتى ينتبه الأعضاء الآخرون هذه المرة ومن ثم يمكنهم الرد ربما.

جيما كاروليلو: هذا لطيف جدًا. شكرًا جزيلًا. وسأحاول أن أصيغه بوضوح قدر استطاعتي. لذا، بما أنك سألت عن المواضيع المحتملة للعمل من جانب SSAC والإحاطة التي يمكن أن تكون مفيدة للجنة GAC. في GAC، عند مناقشة انتهاك DNS، أشرنا أحيانًا إلى وجود أدوات تنبؤية لمنع انتهاك DNS قبل أن نصل إلى مرحلة التخفيف. ومن ثم، كنت أتساءل عما إذا كانت هناك مواد في متناول اليد أو المزيد من العمل الذي يمكن القيام به في هذا المجال. شكرًا.

رام موهان: شكرًا. هل يريد أحد التعليق على ذلك؟ بندكت ثم ستيف.

بينيديكت أديس: مرحبًا. بندكت أديس. لقد فشلت في الحصول على مكان على المنصة. هناك بعض أجزاء انتهاك DNS التي تلائم بشكل جيد للغاية التنبؤ بها. لذا، تستخدم شبكات الروبوتات والبرامج الضارة على وجه الخصوص خوارزميات يمكن التنبؤ بها للغاية لتوليد النطاقات لأسابيع وأشهر وسنوات في المستقبل. الآن، هذه النطاقات غير موجودة. ويُطلق عليها اسم نطاقات DGA. يمكننا التنبؤ بها بدقة كبيرة. ولكن أود أن أحذركم، أي أدوات تدعي أنها قادرة على التنبؤ بالسوء بطريقة أكثر عمومية باستخدام الذكاء الاصطناعي لغبار الجنيات السحري، أود أن أكون حذرًا للغاية منها. وبالتالي، هناك بعض المجالات التي تصلح بشكل جيد للتنبؤ. ولكن ليس على نطاق واسع.

رام موهان: ستيف؟

ستيف كروكر: شكرًا. لكي تتمكن من تشغيل عملية تنبؤية، يجب أن يكون لديك إمكانية الوصول بسرعة ومرونة إلى بيانات التسجيل والتسجيلات نفسها. نحن في فترة رغوية للغاية، كما أود أن أقول، مع التركيز الشديد على الخصوصية، وهو أمر يهدف بحسن نية إلى الحماية من أشكال مختلفة من المضايقات، والرسائل الإلكترونية غير المرغوب فيها، وما إلى ذلك، وما إلى ذلك. ولكن في الوقت نفسه، أصبح من الصعب، بل من المستحيل، الوصول إلى البيانات لأغراض مشروعة، وخاصة لبعض هذه الأغراض، مثل إجراء التحليل التنبئي والارتباط عبر النطاقات.

لذا، هناك بعض الأسئلة الصعبة وغير السهلة التي يتعين علينا متابعتها حول كيفية توفير الوصول إلى المعلومات حتى نتمكن من القيام بعمل جيد في نوع التحليل التنبئي الذي تريده، وفي الوقت نفسه، لا نزال نحمي الخصوصية. وهناك تفاعل بين هاتين الفكرتين.

نايجل هيكسون: شكرًا جزيلًا. شكرًا لك على السؤال، الذي ولّد بعض الاستجابات الممتازة حقًا. وأعتقد أن صديقنا سانتوش من الهند كان التالي.

تي سانتوش: شكرًا لك يا نايجل. شكرًا لك يا رام موهان، على العرض التفصيلي حول الذكاء الاصطناعي وانتهاك نظام اسم النطاق DNS. حسنًا، دعونا نبدأ بالأساسيات. الآن، هل يمكن للذكاء الاصطناعي أن يساعد في العمل على دقة تحديد هوية الشخص لأن هذه هي القضية الأساسية التي تستخدمها الجهات الخبيثة، لأن معظم تحديد هوية الشخص ليس دقيقًا. هل يمكننا أن نمتلك نظامًا حيث يمكن لأداة الذكاء الاصطناعي أن تقول، حسنًا، هذا ليس دقيقًا في WHOIS، وبالتالي لا يمكن تفويض النطاق؟ شكرًا.

رام موهان: شكرًا. لذا، فإن الإجابات المحددة لذلك هي بالتأكيد أنه يمكنك أخذ الذكاء الاصطناعي أو خوارزميات التعلم الآلي الأخرى وتطبيقها على قاعدة بيانات ومقارنتها بالعناوين الحقيقية والأشخاص وما إلى ذلك، والتوصل إلى مستوى معين من الاستنتاجات. ولكن كما قال ستيف للتو، فإن الكثير من هذه البيانات أصبحت الآن غامضة أو غير متاحة. لذا، حتى لو كانت هذه التكنولوجيا موجودة اليوم ويمكن الوصول إليها، فإن مجموعات البيانات التي من شأنها أن تبلغ هذه الأدوات، ليست متاحة ببساطة.

باري ليبا: إضافة سريعة إلى ذلك يا رام. ليس فقط البيانات التي تحتاج إلى التحقق منها غير متوفرة، ولكن البيانات التي تحتاجها لتدريب محركك غير متوفرة حتى. إذن، إنها مشكلة مزدوجة.

غريغ آرون: سأقولها بطريقة مختلفة. بيانات الاتصال الخاصة بأسماء النطاقات غير متاحة لمعظمنا، على سبيل المثال، لشركات الأمن أو لأجهزة إنفاذ القانون، إذا لم تكن متوفرة في WHOIS، على سبيل المثال. ومع ذلك، هناك أطراف لديها البيانات، وهي أمناء السجلات ومشغلو السجل. ولدينا الآن مشغلي السجلات وأمناء السجلات الذين يقومون بالتحقق من الدقة باستخدام مجموعة

متنوعة من الأساليب. يقوم بذلك nl. في هولندا، على سبيل المثال، وuk.. لذا، لدينا الآن بشكل أساسي أمناء السجلات، وخاصةً كونهم الأطراف التي يمكنها التحقق من الدقة والجرائم الإلكترونية المحتملة.

لديهم بيانات WHOIS، ولديهم أيضًا بيانات الشراء، مثل الأدوات المالية المستخدمة لتسجيل أسماء النطاق وعناوين IP المصدر وأشياء أخرى. لذا، فإن الإمكانات لاستخدام الذكاء الاصطناعي موجودة، ولكنها الآن في أيدي تلك الأطراف.

نايجل هيكسون: شكرًا جزيلًا حقًا على ذلك. لدينا سؤالان أو ثلاثة أسئلة أخرى في الدردشة، لذا سأستمر في الإجابة عليها. لدينا سبع دقائق من الوقت، أو ست دقائق في الواقع، لأننا سنحتاج إلى التلخيص. لكن أعتقد أنني لا أفهم حقًا ترتيب هذه الأشياء، لكن ماركو، لماذا لا تأتي؟

ماركو هوغوونينغ: سأكون سريعًا جدًا ومختصرًا وأردد ما قاله زملائي وأقدر كثيرًا SSAC لوجودها هنا وأيضًا، أنتم تمدون أيديكم وتساعدوننا. لقد طرحت سؤالًا بسيطًا ولكنه صعب أيضًا، ما الذي نعتبره مهمًا؟ كل شيء، الأمر يتعلق باختيار طفلك المفضل، أشعر أنه سؤال صعب حقًا للإجابة عليه. أقدر حقًا العمل الذي تقوم به SSAC، وخاصةً في مساعدتنا على فهم تأثير التقنيات الجديدة والناشئة على استقرار نظام DNS والإنترنت على نطاق واسع. ولكن فيما يتعلق بالأولويات والعودة خطوة إلى الوراء، من ناحية، أود أن أسمع ما إذا كانت SSAC بهذا المعنى تنظر أيضًا إلى بعض الحوارات العالمية التي نجريها وبعض العمليات العالمية، على سبيل المثال، الميثاق الرقمي العالمي الذي نُشر مؤخرًا.

ومن حيث المكان الذي تعتقد أنه يمكن القيام فيه بعمل مهم لمساعدتنا جميعًا، ولكن أيضًا ما إذا كنتم ترون فرصة للجنة SSAC للمساهمة في بعض هذه المحادثات العالمية الجارية، على سبيل المثال، مراجعة القمة العالمية لمجتمع المعلومات WSIS أو العديد من خطوط عمل القمة العالمية لمجتمع المعلومات WSIS تشير أيضًا إلى أمن واستقرار النظام. شكرًا.

رام موهان: شكرًا جزيلًا. تشكل حوكمة الإنترنت وجوانب الأمن والاستقرار والمرونة أحد مجالات اهتمامنا الخمسة المستمرة. لذا، فإننا بالتأكيد نريد أن نشارك في هذا الأمر. ليس لدينا هيكل يمكننا من خلاله إرسال وسيط أو إرسال شخص ما إلى تلك المناطق. لكن لدينا الآن أعضاء يهتمون بذلك، ويشاركون فيه بشكل مباشر في وظائفهم اليومية. وهذا يوضح الكثير عن ما نقوم به. وفي الواقع، كان هذا جزءًا من ما أدى إلى إنشاء فريق عمل للمصدر المفتوح، حيث أدرك أحد أعضائنا أن هناك بعض التركيز على هذا الأمر على المستوى الحكومي. وقد يكون ذلك مفيدًا.

باري ليبا: الآن سأجيب على ذلك. في الأساس، هناك ثلاث طرق تقرر بها SSAC العمل على شيء ما. أحد هذه الاحتمالات هو أن يكون هناك عضو أو أكثر من أعضاء SSAC مهتمين بالموضوع ويقترحونه. الأول هو أن يطلب منا مجلس الإدارة أن ننظر في شيء ما. والأخر هي أن يطلب منا المجتمع أن ننظر في شيء ما. ومن الواضح أننا لا نستطيع أن نفعل كل شيء. ولكن إذا جاء بعض أعضاء المجتمع وقالوا إن هذا مهم حقًا بالنسبة لنا، فهل يمكنك إلقاء نظرة عليه؟ هذا احتمال.

نايجل هيكسون: شكرًا. لدينا بضعة أسئلة أخرى. أوين من الولايات المتحدة.

أوين فليتشر: مرحبًا يا نايجل. أعتقد أن وانغ لانغ كان قبلي.

نايجل هيكسون: أوه، صحيح. أعتذر. أنا آسف، وانغ لانغ. إن السبب هو عدم قدرتي على فهم ترتيب هذه الأشياء. تفضل يا سيدي.

وانغ لانغ: شكرًا لك يا نايجل. شكرًا لك يا أوين. أريد أن أشكر رام على العرض الرائع. لقد ذكرت للتو سلسلة الكتل وDNS، لكنك لم تتعمق في الأمر. ونحن نعلم أن ICANN تقبل الأمر باعتباره أمين سجل معتمد لا يمكن إيقافه. لذا، سؤالي هو، ما هو رأيكم في مستقبل Web3 DNS؟ شكرًا.

رام موهان: شكرًا. لم تصدر SSAC تقريرًا خاصًا حول سلسلة الكتل، لكننا أنتجنا تقريرًا حول تطور DNS والتقنيات الجديدة. وبشكل عام، فإن نهجنا هو أن التكنولوجيا سوف تتطور. يتعين علينا أن نحتضن هذه الأسماء الجديدة بدلًا من القول بأننا يجب أن نحمي أسماءنا فقط ونوقف كل من سوانا. ومع ذلك، فإن الأمر المهم هو أنه إذا أرادت مساحات أسماء أخرى لتتكامل في مساحة أسماء DNS، فيجب القيام بذلك بطريقة مسؤولة. وينبغي أن يتم ذلك مع وضع الاستقرار والأمن في الاعتبار. لذا، على مستوى عالٍ، هذه هي الطريقة التي ننظر بها إلى الأمر. هناك آثار أخرى وقضايا أخرى قد تكون موجودة. لو قمنا بإعداد تقرير عن تقنية سلسلة الكتل فقط، فأنا متأكد من أنه ستكون هناك قضايا أخرى لم يتم الكشف عنها. ولم نصل إلى هناك بعد.

نايجل هيكسون: شكرًا جزيلًا لك يا رام. ننتقل إلى أوين.

أوين فليتشر: شكرًا لك يا نايجل. معكم أوين فليتشر من الولايات المتحدة. أعتقد أن هذه كانت جلسة رائعة وأن الذكاء الاصطناعي وانتهاك نظام اسم النطاق DNS هي مثال مثالي لموضوع حيث يمكن لخبرة SSAC الفنية أن تفيدنا حقًا في GAC التي تحاول تطوير مواقف مبنية على الأدلة ومستنيرة حول أنواع الأشياء التي قد ترغب GAC في التعليق عليها.

لذا، أعتقد أنه سيكون من الرائع أن يكون لدينا المزيد من التفاعلات مثل هذه، ربما بما في ذلك جلسات بناء القدرات التي تعقدها اللجنة الاستشارية الحكومية GAC. ورأيت تعليقا آخر بهذا الشأن في الدردشة. رام، وصف العرض بعض أنواع الانتهاكات، من الواضح، والتي ليست انتهاكات DNS كما هو موصوف أو محدد في ICANN، على الرغم من أن العديد من الأشياء يمكن استخدامها من قِبل الأشخاص الذين يرتكبون انتهاكات DNS. لكن فيما يتعلق بانتهاك نظام

اسم النطاق DNS بموجب تعريف ICANN، هل تتوقع أن ما فهمته من العرض هو نوع من الوتيرة المتسارعة لإنشاء نطاقات سيئة تؤدي إلى أي زيادة في حالات الانتهاك المبلغ عنها؟ هل يجب علينا أن نضع هذا في الاعتبار عندما ننظر إلى الإحصائيات والتقارير حول انتهاك نظام اسم النطاق في الأشهر أو السنوات القادمة؟ شكرًا.

رام موهان: سأتحدث شخصيًا فقط، لأن SSAC ليس لديها موقف في هذا الشأن. لكن شخصيًا، أعتقد أن هذه هي الخطوة المنطقية التالية. عندما تجعل التكنولوجيا تعقيد الأمر وحجمه بسيطين للغاية، فيمكنك أن تتوقع ذلك، لأنه سيكون هناك الكثير من المال الذي يمكن جنيه. أعني، كان جيف بيدسر، في تعليق له بالأمس، يقول إن قيمة الصيد السهل تبلغ حوالي 20000 دولار. لذا، إذا كانت تكلفة تسجيل اسم نطاق 200 دولار، أو 100 دولار، أو حتى 1000 دولار، فهذا لا يشكل رادعًا كافيًا بالضرورة. لذلك، أعتقد أنه إذا أخذنا السلسلة المنطقية، يمكننا أن نتوقع رؤية المزيد من هذا النوع من الانتهاكات والتقارير. هذه وجهة نظري الشخصية. هل هناك غيرها، ميريك؟

ميريك كايو: نعم، من وجهة نظر شخصية، أعني أنني أقوم بأعمال أمنية على أساس يومي، وأنا لا أثق بأي شيء على الإطلاق. لكن الأمر كان مثيرًا للاهتمام بالنسبة لي حقًا. لا أقوم بتصفية رسائل البريد العشوائي لأنني أريد أن أطلع على الحملات والأشياء التي تحدث. وما هو مثير للاهتمام حقًا هو أن الذكاء الاصطناعي هو الذي يتسبب في ذلك، ولكن هذا النوع من رسائل التصيد الاحتيالي أصبح مقنعًا للغاية. وأعتقد أيضًا أنهم ينظرون فعليًا إلى ما تنشره على Facebook أو LinkedIn ويستهدفون بالفعل منظمات محددة وقيادات محددة، حتى يتوفر لديهم الذكاء، وهو الأمر الأكثر قابلية للتصديق. وأعتقد أن هذا هو شيء حيث أن سرعة تحركنا للكشف والردع هو أمر مهم حقًا.

نايجل هيكسون: شكرًا. شكرًا جزيلًا لك يا رام. أخشى أن نضطر إلى ترك الأمر عند هذا الحد. لقد نفد الوقت لدينا، ولكن هذا كان مثمرًا حقًا. إنه يظهر مدى الاهتمام بالعمل المذهل الذي تقومون به. ومن الرائع رؤية هؤلاء الخبراء على الطاولة. أشعر دائمًا بالفخر عندما أجلس على الطاولة مع

الدكتور ستيف كروكر، وهو مصدر إلهام لأن العديد منكم ساهموا ليس فقط في عمل ICANN، بل وفي عمل المجتمع الفني بشأن العديد من القضايا.

لذا، شكرًا لك على الحضور مرة أخرى. لن يكون هذا هو الأخير. ونشكركم على عروضكم الطيبة لمتابعة القضايا المختلفة. وبهذا أعتقد أننا سننهي الاجتماع على خير. زملائي الكرام في الخلف، هل يمكنكم أن تخبرونا متى سيكون اجتماع الجلسة في الصباح؟ هل يمكنكم أن تذكرونا متى؟

جوليا تشارڤولين: دقيقة واحدة. هل تعرفون ما هو؟

متحدث لم يذكر اسمه: نعم، الساعة 1:15. لا يزال هناك حفل الترحيب، والمنتدى السياسي للمنضمين قبل ذلك، ولكن GAC ستبدأ في الساعة 1:15 بالتوقيت المحلي لمناقشة قضايا بيانات تسجيل WHOIS.

نايجل هيكسون: ضاع الوقت.

رام موهان: نايجل، شكرًا جزيلًا لك نيابةً عن SSAC لاستضافتنا هنا. ونأمل ألا تكون هذه المرة الأخيرة. ونتطلع إلى مزيد من المشاركة.

[نهاية التفريغ الصوتي]