اجتماع ICANN71 | منتدى السياسات الافتراضي – جلسة عامة جامعة: فهم قوائم حظر المواقع المشبوهة
يوم الخميس، الموافق 17 يونيو/حزيران 2021 – الساعة 10:30 إلى 12:00 بتوقيت وسط أوروبا الصيفي

بريندا بريور: ستبدأ هذه الجلسة الآن. لنبدأ التسجيل رجاءً.

[يجري الآن التسجيل]

بريندا بريور: مرحباً. ومرحبًا بكم في جلسة اجتماع ICANN71 الجامعة، بعنوان فهم قوائم حظر المواقع المشبوهة.

أُدعى بريندا بريور وأنا مديرة المشاركة عن بُعد لهذه الجلسة. يُرجى العلم بأن هذه الجلسة يجري تسجيلها وتتبع معايير السلوك المتوقعة في ICANN.

أثناء هذه الجلسة، ستتم قراءة الأسئلة أو التعليقات بصوتٍ عال فقط إذا قُدمت في مربع الأسئلة والأجوبة. وسأقرأها عليكم بصوتٍ عالٍ خلال الوقت الذي حدده رئيس هذه الجلسة أو مديرها. ستشمل الترجمة الفورية لهذه الجلسة كلاً من اللغة الإنجليزية والصينية والفرنسية والروسية والإسبانية والعربية. انقروا فوق رمز الترجمة الفورية في برنامج زووم وحددوا اللغة التي ستستمعون إليها أثناء هذه الجلسة. إذا رغبتم في التحدث يرجى رفع يدكم في غرفة زووم. وبمجرد أن يناديك منسق الجلسة باسمك، سيتيح لك فريق الدعم الفني لدينا كتم صوت ميكروفونك.

وقبل التحدث، تأكدوا من تحديد اللغة التي ستتحدثون بها من قائمة الترجمة الفورية. يُرجى التكرم بذكر الاسم للتدوين في السجل وتحديد اللغة إذا كنتم ستتحدثون بلغة أخرى غير الإنجليزية.

ملاحظة: ما يلي هو ما تم الحصول عليه من تدوين ما ورد في الملف الصوتي وتحويله إلى ملف كتابي / نصّي. ورغم أن تدوين النصوص يتمتع بدقة عالية، إلا إنه في بعض الحالات قد تكون غير مكتملة أو غير دقيقة بسبب المقاطع غير المسموعة والتصحيحات النحوية. تنشر هذه الملفات لتكون بمثابة مصادر مساعدة للملفات الصوتية الأصلية، ولكن لاينبغي أن تُعامل كما لو كانت سجلات رسمية.

وعند التحدث يتعين التأكد من كتم صوت جميع الأجهزة والإشعارات الأخرى. ويُرجى التحدث بوضوح وبسرعة معقولة للسماح بالترجمة الدقيقة.

ويمكن لجميع المشاركين في هذه الجلسة نشر التعليقات في الدردشة. للقيام بذلك، يرجى استخدام القائمة المنسدلة في مربع الدردشة أدناه وتحديد "Respond to All Panelists and Attendees" (الرد على جميع أعضاء اللجنة والحضور). فسيتيح ذلك للجميع الاطلاع على تعليقك. ويُرجى ملاحظة أن الدردشة الخاصة ممكنة فقط بين أعضاء اللجنة بتنسيق ندوات Zoom عبر الويب. كما أن أي رسالة يرسلها عضو في اللجنة أو حاضر عادي إلى حاضرين عاديين آخرين سيراها أيضًا مضيف الجلسة والمضيفون المشاركون وغيرهم من أعضاء اللجنة.

ولعرض النص المدون في الوقت الفعلي، انقر فوق زر "التعليق الخطي المصاحب" في شريط أدوات برنامج زووم Zoom. وبهذا، أحيل الكلمة إلى أل جي فورسبيرغ. شكرًا.

أل جي فورسبيرغ: شكرًا لك، بريندا. أنا اسمي أل جي فورسبيرغ، وأنا منسق أعمال هذه الجلسة الجامعة في اجتماع ICANN71 بعنوان: فهم قوائم حظر المواقع المشبوهة.

بالنسبة لأولئك الذين لا يعرفونني، فأن أحد المخضرمين السويديين في مجال أسماء النطاقات ولدي خبرة في كل من جانب أمين السجل بصفتي مديرًا للمنتجات الفنية ومنسق اتصال سجلات وأيضًا من جانب السجل في العديد من الأدوار الفنية ذات الصلة بالقنوات.

وأنا أعمل حاليًا المسئول التقني الأول في شركة iQ، وهي أحد الموفرين التجاريين للخدمات المقدمة إلى مجال أسماء النطاقات مثل مدير إساءة الاستخدام في شركة iQ والبيانات التحليلية للنطاقات.

وعندما لا أكون بصدد تضمين ومكاملة القائمة التالية لحظر المواقع المشبوهة في منصب مدير إساءة الاستخدام، فإنني أقدم الاستشارات أيضًا لمختلف السجلات وأمناء السجلات في المسائل الفنية والمسائل الخاصة بالسياسة.

وأخيرًا وليس آخرًا، فإنني مؤسس ومنسق شركة Nordic Domain Days، وهي عبارة عن مؤتمر سنوي لعالم صناعة النطاقات الاسكندنافية، والتي لا تطيق الانتظار حتى تعود الاجتماعات المباشرة وجهًا لوجه للانعقاد مرة أخرى.

وخلال جلسة اليوم، سوف نشارك الجماهير. وقد أعددنا لكم ثلاثة أسئلة في اقتراع لكي تجيبوا عنها أثناء الاستماع إلى المناقشة. وسوف يتم طرح اثنين منها عليكم الآن. في حين سوف يبرز السؤال الأخير في الوقت المناسب للفقرة الأخير في جدول أعمال اليوم.

هلاّ تفضلتم بطرح أسئلة الاقتراع.

بريندا بريور: شكرًا. سوف ترون على الشاشة سؤال الاقتراع الأول. هل أنتم على دراية بالأنواع التالية من التهديدات الأمنية؟ الرجاء وضع علامة اختيار على جميع الاختيارات المنطبقة.

تشمل الخيارات كل من البريد غير المرغوب أو التصيّد أو البرمجيات الضارة أو الاستدراج أو شبكات بوت نت أو غيرها. مرة أخرى، هل أنتم على دراية بالأنواع التالية من التهديدات الأمنية مع التأكيد على وضع علامة اختيار على جميع الخيارات المنطبقة: البريد غير المرغوب أو التصيّد أو البرمجيات الضارة أو الاستدراج أو شبكات بوت نت أو غيرها. وسوف نغلق الاقتراع في غضون خمس ثوان تقريبًا.

شكرًا.

ويمكننا رجاءً إغلاق الاقتراع في هذا الوقت.

هل يمكننا الحصول على سؤال الاقتراع رقم 2؟

سؤال الاقتراع رقم 2: هل تعرض أي اسم نطاق تحت إدارتك لأي من هذه التهديدات الأمنية؟ ويمكنك الإجابة بنعم أو لا أو لا أعلم أو أنا لا أدير أي نطاقات. عفوًا، هناك أربعة اختيارات. برجاء اختيار واحد. مرة أخرى، هل تعرض أي اسم نطاق تحت إدارتك لأي من هذه التهديدات الأمنية؟ "نعم" أو "لا" أو "لا أعلم" أو "أنا لا أدير أي نطاقات".

وسوف نخصص حوالي خمس ثوان لهذا السؤال، رجاءً.

شكرًا جزيلاً لكم.

يمكننا إغلاق الاقتراع.

أل جي، الكلمة لك، تفضل.

أل جي فورسبيرغ: شكرًا لك، بريندا.

سوف أواصل من خلال إطلاعكم على مقدمة موجزة حول الموضوع قبل أن نواصل إلى القسم الخاص باللجنة. واليوم لدينا عدد من الأطراف التي تستمع إلى ذلك وبحاجة إلى الربط مع قوائم حظر المواقع المشبوهة بطرق مختلفة. ويمكنني القول بأن هذه الأطراف هي ICANN التي يمكنها توفير إحصائيات داخل نظام الإبلاغ عن نشاط انتهاك النطاق DAAR، وذلك من خلال استخدام قوائم حظر المواقع المشبوهة، كما أنها تشترط على نطاقات gTLD الجديدة أن تراقب على الأقل (يتعذر تمييز الصوت).

ولدينا أطراف متعاقدة تتخذ شكل السجلات وأمناء السجلات التي قد تستخدم واحدة أو أكثر من قوائم حظر المواقع المشبوهة من أجل مراقبة نطاقات TLD الخاصة بها، أو قائمتها الخاصة بأسماء النطاقات المسجلة في حالة أمناء السجلات.

وقد يكون لدينا موفري خدمات مثل شركات الاستضافة، ويمكنهم استخدام قوائم حظر المواقع المشبوهة من أجل الحفاظ على خلو البريد الإلكتروني لعملائهم من البريد غير المرغوب أو لضمان أن مواقع الويب التي يستضيفونها لا يتم الإبلاغ عن قيامها بأشياء سيئة، مثل التصيّد أو البرامج الضارة.

وأخيرًا، لدينا المستخدمين النهائيين ويمكن تعريفهم لأغراض هذه المناقشة بأنهم الأشخاص المسجلون أو المشغلون لاسم نطاق و/أو موقع على الويب وأعتقد أنه المجموعة الوحيدة هنا اليوم التي قد لا ترغب في أن تكون لها علاقة مع أي من قوائم حظر المواقع المشبوهة.

وبهذا القول، فإن قوائم حظر المواقع المشبوهة سوف تعني بالطبع أشياء مختلفة، وذلك اعتمادًا على من تقومون بتعريفهم ضمن هذه المجموعات. وبالنسبة لـ ICANN أو لأي سجل أو أمين سجل، فسوف تكون على الأرجح بمثابة أداة تستخدمها أو شريك تتعامل معه، في حين أنه بالنسبة لأي مستخدم نهائي قد تفضي إلى مشكلات كبيرة إذا انتهى بك المطاف إلى واحدة يتم فيها إرسال بريدك الإلكتروني إلى مجلد البريد غير المرغوب الاستنزافي أو تحصل على خطأ شاشة الموت الحمراء من Google التي تظهر في المتصفّح Chrome بدلاً من موقعك على الويب.

بالإضافة إلى ذلك، وفقًا لما قد يكون قد أخبرك به الموضوع، في حين أن قوائم حظر المواقع المشبوهة جزء لا يتجزأ من مناقشة انتهاك نظام أسماء النطاقات DNS، فلسنا هنا اليوم من أجل إجراء مناقشة على مدار 90 دقيقة حول ماهية تعريف انتهاك نظام أسماء النطاقات DNS. وعوضًا عن ذلك، فإننا حاضرون هنا اليوم من أجل اكتساب قدر

أكبر من الفهم حول كيفية أداء قوائم حظر المواقع المشبوهة لعملها وكيف يمكننا نحن الجمهور والأطراف المتعاقدة وموفري الخدمات والمستخدمين النهائيين العمل معهم.

والآن سوف نسمع كثيرًا حول قوائم حظر المواقع المشبوهة اليوم، لكن أن نبدأ ذلك بتذكير بسيط قبل هذه المناقشة فلن يضر أحدًا.

ومن ثم فإن أي من قوائم حظر المواقع المشبوهة عبارة عن إشارات أو تقارير مقدمة من أجل المساعدة في حجب ومنع سلوك الانتهاك بطريقة أو بأخرى. وغالبًا ما يشير الجزء بالخاص بالسمعة في الاسم إلى وجود بعض الظلال الرمادية في طريقة تحديد ما إن كان من المفترض إدراج اسم نطاق في القائمة أم لا. فالإجابة ليست ببساطة الرد بنعم أو لا.

وأحد الأمثلة على ذلك هو تنفيذ Spamhaus لسمعة المواقع، مع بدء كل اسم نطاق عند الصفر، واكتساب نقاط سلبية نظير القيام بأشياء جيدة ونقاط إيجابية نظير القيام بأشياء سيئة.

وبمجرد اكتساب ما يكفي من النقاط -- على سبيل المثال، خمس أو عشر نقاط -- يتم إدراج اسم النطاق في قائمة الحجب.

وكلمة الحجب الموجودة في الاسم تراعي إلى حد ما منشأ هؤلاء الموفرين حيث كان يتم تنفيذها أو يجري تنفيذها في خوادم البريد الإلكتروني وبرامج الجدار الناري من أجل منع وحجب البريد غير المرغوب أو مرور البيانات غير المرغوب. وكان الهدف من القوائم حجب الأشياء وما يزال كذلك.

إذن الحد من إساءة الاستخدام -- عفوًا. بالطبع.

إذن فالحد من الانتهاك قد لا يكون حالة الاستخدام الوحيدة أو في بعض الأحيان ليست هي حالة الاستخدام الأولية.

وسوف توفر بعض قوائم حظر المواقع المشبوهة قائمة كاملة بمعلومات حول الكيفية التي تم بها اكتشاف مصدر ما ضار، في حين توفر قوائم أخرى تلميحًا بأن شيئًا ضارًا قد حدث في اسم نطاق محدد.

وهناك شيء يبدو أنه شائع بين غالبية قوائم الحظر ألا وهو أن فهم ما يقومون به، وطريقة القيام بذلك وما الهدف تسعي البيانات إلى المساعدة فيه فهو ليس سهلاً دائمًا، لا سيما وإن كنت مستخدمًا نهائيًا بدون أي صلة سابقة بهذه الأنواع من الموارد.

ولكن لكي نتمكن من الوصول إلى أصل وكيفية جمع قوائم حظر المواقع المشبوهة للبيانات الخاصة بها، وتصنيف محتواها وسبر أغوار الطريقة التي تعمل بها هذه المعالجة الآلية الضخمة التي تتأتى عنها أحيانًا قائمة جديدة بشكل أو بآخر، فقد قمنا بجمع بضعة ممثلين من قوائم حظر المواقع المشبوهة هنا اليوم، وانضم إلينا كذلك مجموعة من الممثلين من الأطراف الذين تم التعريف بهم مسبقًا من أجل الحديث حول خبراتهم في قوائم حظر المواقع المشبوهة.

وبهذا، أود أن أعرّفكم بأول مشارك معنا اليوم وأتيح له المجال للتعريف بنفسه وبالشركة التي يعمل بها.

السيد كاريل بيتر من شركة Spamhaus، تفضل رجاءً.

كاريل بيتر: طاب يومكم جميعًا. أنا كاريل بيتر. وأنا أعمل لدى شركة Spamhaus، وبهذه الصفة فإنني مشارك في الأغلب في مجال قوائم حظر النطاقات في عملنا. كما أننا نقوم بإعداد العديد من قوائم البيانات، ولكن دعونا نركز اليوم على جانب النطاقات فيما نقدمه.

وقد شاركت في مجال قوائم حظر النطاقات لأكثر من عشر سنوات حتى الآن. وبالفعل، فقد كنت مشاركاً سابقًا في مجموعة كاملة من جلسات ICANN وما إلى ذلك.

إذن يسرني تقديم المساعدة وأي -- والإجابة عن ما قد تكون لدى المشاركين من أسئلة.

أل جي فورسبيرغ: شكرًا لك، كاريل.

السيد رومان هويسي من موقع abuse.ch، هلاّ تفضلت رجاءً بتعريف نفسك.

رومان هويسي: نعم، أنا رومان هويسي، وأنا مؤسس موقع abuse.ch. وموقع abuse.ch عبارة عن مشروع غير ربحي يدار في جامعة بيرن للعلوم التطبيقية، والهدف منه يتمثل في جمع معلوماته حول شبكات بوت نت وغيرها، بالإضافة إلى نشر ما يقابلها من معلومات مجانًا للجميع.

أل جي فورسبيرغ: شكرًا لك، رومان.

والمشارك الأخير معنا من قوائم حظر المواقع المشبوهة اليوم هو السيد بين كون من شركة WMC Global.

عرّفنا بنفسك رجاءً.

بين كون: شكرًا. أنا بين كون، من شركة WMC Global. نحن -- بالأساس -- نقوم بإدارة منصة للتصيّد. ونقدم قوائم حظر على روابط URL المستخدمة في التصيّد إلى موفري خدمات SMS وجدران الحماية ومن يتعرضون للهجمات بالأساس باستخدام تصيّد أوراق الاعتماد عبر قدر كبير من الإغراءات.

ويسرني أن أجيب عن أية أسئلة لدى أي شخص. شكرًا.

أل جي فورسبيرغ: شكرًا لك، بين.

لمواصلة المناقشات من جانب الأطراف، أود أن أبدأ بتعريفكم بسامانه تاجاليزاديخوب من ICANN. عرّفنا بنفسك رجاءً. وإذا كانت لديك أية نقاط أو وجهات نظر أساسية تود أن يضيفها إلى هذه المناقشة، فهذا هو الوقت المناسب لذلك.

سامانه تاجاليزاديخوب: مرحبًا بكم جميعًا. أنا سامانه تاجاليزاديخوب. وأنا أعمل في مكتب المسؤول الفني الرئيس في ICANN في مجموعة الأمن والاستقرار والمرونة. كما أنني قائدة المشروعات في مشروع الإبلاغ عن نشاط انتهاك النطاق DAAR ولدي خبرة سابقة في الأوساط الأكاديمية، وذلك من خلال العمل مع موجزات بيانات قوائم الحظر.

وسوف أتحدث اليوم أكثر حول الكيفية التي ننظر بها في منظمة ICANN إلى هذه الموجزات ونستخدمها وفي أي من المشروعات يتم ذلك.

شكرًا.

أل جي فورسبيرغ: شكرًا لك، سامانه.

بعد ذلك أود أو أعرفكم بالسيد مات توماس من شركة VeriSign. برجاء التعريف بنفسك وطرح أية وجهات نظر أو نقاط أساسية لديك على الطاولة.

مات توماس: شكرًا. أنا مات توماس. وأنا أعمل لدى شركة VeriSign في إدارة أبحاث واستراتيجية الأمن السيبراني مهندسًا معتمدًا.

كما أنني أحد أعضاء اللجنة الاستشارية للأمن والاستقرار في ICANN وأعمل نائبًا لرئيس مجلس الإدارة في مجموعة عمل المراسلة والبرامج الضارة ومكافحة إساءة استخدام الأجهزة المحمولة كما أنني أتطلع إلى اللجنة اليوم من أجل مناقشة حالات الاستخدام المتنوعة لقوائم حظر المواقع المشبوهة.

شكرًا.

أل جي فورسبيرغ: شكرًا لك، ماثيو.

من جانب أمناء السجلات، يشارك معنا اليوم ريغ ليفي من شركة Tucows. برجاء التعريف بنفسك وطرح أية وجهات نظر أو نقاط أساسية لديك.

ريغ ليفي: مرحبًا بالجميع. أنا ريغ ليفي، وأنا أعمل لدى شركة Tucows رئيسًا لإدارة الامتثال. كما أنني مشارك في مجموعة انتهاك نظام أسماء النطاقات DNS التابعة لمجموعة أصحاب المصلحة في أمناء السجلات. وفي واقع الأمر، فإنني رئيس مشارك في مجموعة انتهاك نظام أسماء النطاقات DNS.

صباح الخير. يبدو أنني ما زلت أحاول الإفاقة من النوم.

وأنا أتطلع إلى هذه المناقشة.

أل جي فورسبيرغ: شكرًا لك، ريغ.

وأخيرًا وليس آخرًا، لدينا جوانا كوليزا من مجتمع عموم المستخدمين. برجاء التعريف بنفسك وطرح أية وجهات نظر أو نقاط أساسية لديك على الطاولة.

جوانا كوليزا: شكرًا لك، أل جي. أشكركم على استضافتنا. شكرًا على استضافتي معكم وإعطائي فرصة التحدث بالنيابة عن المستخدمين النهائيين.

وأنا نائب رئيس مشارك في اللجنة الاستشارية العامة. ومجال عملي هو بناء القدرات، وأؤمن فعليًا بوجود مكون بناء القدرات في هذه المناقشة، وفي هذه اللجنة وفي قوائم حظر المواقع المشبوهة.

وأطرح عليكم نقطة أساسية فقط لإخلاء المسئولية، من خلال الاقتراع نفسه والمشاركة من مجتمع عموم المستخدمين، فليس صحيحًا أن المستخدمين النهائيين غير مهتمين بقوائم حظر المواقع المشبوهة. بل على النقيض تمامًا. وسوف أحاول المرور على هذه النقطة أساس سير أعمالنا في اللجنة.

أنا بالفعل سعيدة لحضوري هنا. شكرًا لاستضافتي.

أل جي فورسبيرغ: شكرًا لكِ، جوانا.

وسوف ننتقل بعد ذلك من القسم الخاص بالتعارف في هذه المناقشة إلى القسم الأول من الحوار حيث نتحدث حول قوائم حظر المواقع المشبوهة وسأحاول زيادة معرفتنا بالطريقة التي تسير بها الأمور.

وأود أو أبدًا بهذا القسم من خلال سؤال كاريل عن كيفية تعريف قوائم حظر المواقع المشبوهة.

كاريل بيتر: هذا سؤال جيد. لنبدأ بالجزء الخاص بالحجب.

أعتقد أنه في كثير من الحالات، لي يجدي الحجب وحده نفعًا. وإذا ما نظرتم إلى كامل منطور السجل/أمين السجل حيث تنظر السجلات أو أمناء السجلات في البيانات من أجل العثور على النطاقات المسببة لمشكلات أو العملاء المشاكسون، فليس هناك -- فإنهم غير مشاركين في أي من أعمال الحجب في حد ذاتها. بل يميل الأمر إلى حالة استخدام من نوع التصحيح.

إذن على المستوى الشخصي، فإنني دائمًا ما أتحدث حول مجموعات البيانات الخاصة بنا وليس حول قوائم حظر المواقع المشبوهة، وعلى وجه الخصوص في سياق مثل هذا. إذن -- وأعتقد أن هذا الأمر من الأهمية بمكان بحيث يتعين عليكم وضعه في اعتباركم كلما بدأتم العمل مع أي من مجموعات البيانات. ما الغرض منها؟ وما الذي تفعلونه بها؟ وهل تستخدمونها حسب الغرض المخصص لها؟ هل تستخدمونها بالطريقة التي -- بالطريقة التي صُممت من أجلها؟

وإن لم يكن، أعني، يجب أن تكونوا -- ولا أقول بأنه لا يمكنكم استخدام شيء مخصص للقيام بشيء واحد في غرض آخر. لكن يجب أن تكونوا على دراية بأن حالة الاستخدام الخاصة بكم قد تكون مختلفة إلى حد ما عند استخدامها في جانب واحد.

وكما ذكرتم سابقًا، فيما يتعلق بالطريقة التي تعمل بها أنظمتنا حيث نقوم فعليًا بوضع درجات ونقاط للنطاقات، فكلما كانت النقاط عالية -- كلما وصل نطاق من حيث النقاط بالنسبة لنا، زادت قناعتنا بأن هناك شيء فعليًا -- بأن هناك شيء غير صحيح يجري. فمن شأن هذا أن يتيح الفرصة للناس من أجل التصرف بشكل مختلف وفقًا لمختلف تصنيفات إعطاء الدرجات والنقاط.

إذن أعتقد أنه يتعين علينا فعليًا أن نفهم البيانات التي نتعامل معها. وإذا لم تفعلوا ذلك، فيتعين عليكم التواصل مع من يقومون باستحداث البيانات وأن تقولوا لهم، "اسمعوا، أنا لا أفهم فعليًا هذا الجانب أو أنني أحاول القيام بهذا من خلاله، فهل هذه فكرة جيدة؟ بعض الأشياء التي قد ترغبون في حجبها في سياق البريد الإلكتروني ولكن ربما ليس في سياس مستوى نظام أسماء النطاقات. ومثال ذلك أدوات الاختصار. فأدوات الاختصار في البريد الإلكتروني علامة شائعة للغاية على وجود بريد إلكتروني مشكل. فأي بريد إلكتروني صحيح لا يحتوي في الغالب على أدوات اختصار.

لكن حجب أدوات الاختصار في مستوى نظام أسماء النطاقات ربما يكون معالجة قاسية إلى حد ما بالنسبة للمستخدمين النهائيين. فبالتأكيد هناك الكثير من الأشياء التي يجب علينا وضعها في الاعتبار.

أل جي فورسبيرغ: شكرًا لك، كاريل.

أود أن أعلق على سؤالين من أسئلة المتابعة حول شركة Spamhaus خصيصًا. وهي: ما أنواع الأدلة النموذجية التي يمكن أن تعتبرها شركة Spamhaus قوية بما يكفي

لإدراج اسم نطاق في قائمة من قوائم حظر المواقع المشبوهة؟ وهل تتم مشاركة هذا الدليل بأي حال من الأحوال مع معتمدي مجموعات البيانات هذه؟

كاريل بيتر: في حالتنا نحن، ليس سهلاً دائمًا أن نشارك الدليل لأن جميع البيانات التي نحصل عليها -- تأتي من موفري خدمة الإنترنت وغيرهم من الشبكات التي تكون لديها اتفاقية من أجل مشاركة البيانات معنا، لكن لا يمكننا دائمًا مشاركة كل شيء. وفي حال كان لدى أي أحد شك في أي شيء، فإننا نتقبل كل الأسئلة.

أما من حيث حالة استخدام السجل/أمين السجل التي نتعامل معها، فهناك قناة دعم متاحة للناس من أجل التعبير بالقول، على رسلكم، نرى بأن هذا مدرج على القائمة ولا ندري ما الذي يجري هنا. هل هي نتائج إيجابية خاطئة؟ هل هناك شيء آخر يجري؟ يمكننا دائمًا النظر في هذا الأمر، وربما يتبين لنا أن لدينا ما يمكننا مشاركته. ولكنها ليست -- ليس هناك ما يمكن مشاركته افتراضيًا. كما هو الحال عندما تكون لدين على سبيل المثال، قائمة من 100 نطاق سيء، فهو لا يحتوي كذلك على 100 عينة بريد غير مرغوب، على سبيل المثال ولا 100 ثنائية من البرمجيات الضارة. وهذا بشكل رئيسي يقوم على أساس كل حالة على حدة حيث يتعين علينا تقرير ما يمكننا مشاركة وما إلى ذلك.

أل جي فورسبيرغ: شكرًا لك، كاريل.

رومان، هل -- ماذا تقول في الفرق في هذا المشروع مع موقع abuse.ch؟

رومان هويسي: أرجو المعذرة. هل يمكنك تكرار السؤال الأول؟ كنت فقط أجيب عن الأسئلة في مربع الأسئلة والأجوبة.

أل جي فورسبيرغ: عذرًا. لا بأس. إذن ما نوع الدليل النموذجي على وجود انتهاك وتعتبره شركة abuse.ch قويًا بما يكفي لإدراج اسم النطاق في مجموعة البيانات الخاصة بكم؟

رومان هويسي: هذا سؤال جيد. شكرًا.

إذن في المعتاد فإن نوع الدليل هو البرمجيات الضارة التي يتم طرحها على مواقع الويب المخترقة، فاسم النطاق أو أسماء النطاقات التي تم تسجيلها من خلال جهة فاعلة تمثل تهديدًا.

وما يعنيه ذلك هو أن النظام يقوم فعليًا بالتحقق من كل ما يتم تقديمه سواء كانت هناك حمولة ضارة يجري طرحها. وإذا كان هذا هو الحال، فإن الدليل يجري نشره على موقع المشروع على الويب بحيث يمكن للجميع استخدامه. وبعد ذلك يجري إرسال تقرير الانتهاك إلى شركة الاستضافة المقابلة.

ومن ثم فإن المشروع شفاف إلى حد ما من حيث توفير الدليل، حيث يتم إظهار وكشف كل دليل أمام الجمهور على موقع الويب ويمكن للجميع فعليًا التحقق من سبب إدراج أي شيء على القوائم.

أل جي فورسبيرغ: شكرًا لك، رومان.

لغرض فهم قوائم البيانات، هلا تفضلت بشركة دورة حياة أي تقرير عام، بمعنى البرمجيات الضارة في حالتك أنت، وبعد ذلك من أول -- من المرة الأولى التي يجري فيها تقديمها إليكم إلى أن تزول؟

رومان هويسي: بالتأكيد. وبالحديث عن ذلك، فإن البرمجيات الضارة تمثل بشكل أو بآخر موضوعًا سهلاً على العكس من نطاقات التصيّد أو على العكس من نطاقات البريد غير المرغوب كما أتوقع نوعًا ما من الرد من المضيف البعيد. إذن هذا يعني أنه يمكنني أن أتحدث بسهولة وبطريقة تلقائية مما إن كان هناك موقع ويب ما يزال يقدم محتوى ضارًا أم لا، إن جاز التعبير. وأنا أقوم بذلك بطريقة تلقائية. وبمجرد أن يختفي هذا المحتوى الضار، يتم تمييز هذا الموقع الإلكتروني أو اسم النطاق بأنه غير متصل بالإنترنت تلقائيًا. وهذا يعني حينها أن استخدام النطاق أو رابط URL فعليًا يختفي تلقائيًا من قائمة الحظر التي أقدمها.

ولهذا السبب، فإن الميزة الوحيدة في ذلك هو أن رابط URL هذا يظل مدرجًا طالما كان يمثل تهديدًا فعليًا. وسواء كان ما يزال يقدم فعليًا تهديدًا فهذه القضية تخضع للفحص عدة مرات كل ساعة، وغالبًا ما يكون ذلك كل عشر دقائق.

وبمجرد أن يقوم أحد المستخدمين النهائيين بتصحيح التهديد، فسوف يختفي النطاق أو رابط URL تلقائيًا من قائمة الحظر في غضون ساعة على الأغلب.

وعلى الجانب الآخر، فهذا يعني فعليًا أنه إذا لم يتم تصحيح المشكلة فعليًا، بالأحرى على سبيل المثال، تم محو المحتوى الضار للتور ولكن السبب الأصلي لم يتم تصحيحه، فهذا يعني أن مسبب التهديد يقوم بتحميل ورفع المحتوى الضار مرة أخرى، حيث يتحقق النظام تلقائيًا مما إذا كان المحتوى الضار موجود مرة أخرى أم لا. وإذا كان موجودًا مرة أخرى، فإن اسم النطاق أو رابط URL سوف يتم إدراجه مرة أخرى تلقائيًا.

أل جي فورسبيرغ: شكرًا لك، رومان.

بين، هل لك أن تقول بأن ما وصفه كل من كاريل ورومان هنا يختلف بشكل كبير عن ما تراه في شركة WMC Global من حيث تقارير التصيّد، ودورة حياتها ودليل التصيّد؟

بين كون: أنا أقول بأنه بالنسبة لشركة WMC Global، فإننا نتبع بشكل أساسي نفس النموذج الذي كان رومان يتحدث عنه.

فنحن نتحقق من الأضرار والبرمجيات الضارة على المواقع قبل أن يتم إدراجها. وعندما نقوم بتقديم قائمة حظر إلى موفر خدمة SMS على سبيل المثال من أجل وقف التصيّد باستخدام الرسائل القصيرة، فغالبًا ما يستخدمون تلك القائمة فقط لآخر 24 ساعة لأن مواقع التصيّد سوف تنقطع اتصالها بالإنترنت. وسوف نعيد إدراج أي موقع للتصيّد إذا ما عاد للاتصال مرة أخرى. وقد قمنا إجراء أتمتة لعمليات الفحص التي تتم، وسوف تقوم بفحص دورة حياة المدة التي يكون فيها رابط URL الخاص بالتصيّد نشطًا.

أما الأمر الآخر الذي يختلف عما نقدمه وما تقدمه بعض قوائم الحظر الآخر فهو أننا لا نقوم بإدراج النطاقات، بل ندرج رابط URL الكامل. فبهذه الطريقة يمكنك معرفة المكان الذي يوجد به المحتوى الضار على وجه التحديد. وبعد ذلك مرة أخرى، بمجرد أن ينقطع اتصال هذا المحتوى الضار عن الإنترنت، يتم إخراجه من القائمة ما لم يعد مرة أخرى للاتصال بالإنترنت.

أل جي فورسبيرغ: شكرًا لك، بين.

عودة إلى كاريل. ذكرت سابقًا أن أي مستخدم لقائمة حظر المواقع المشبوهة يتعين أن يكون على دراية بالغرض المخصص لاستخدام قائمة الحظر.

فما تقولون إن كانت حالة الاستخدام الأساسية لشركة Spamhaus؟ ومن هو المستخدم الأساسي الذي تحاولون خدمته إذن؟ وهل تقولون بأن هذا الأمر قد تغير على مدار السنوات العشر الأخيرة، أن نحو ذلك؟

كاريل بيتر: بشكل واضح، وبما أن لدينا كلة spam "بريد غير مرغوب" في اسم شركتنا، فإننا نتعامل بالأساس مع جانب ومجال البريد الإلكتروني.

فمجموعة البيانات -- فهذا الأمر معقد إلى حد ما. فمجموعة البيانات التي ننشرها على الملأ، أي قائمة حظر النطاقات، هي وجهة نظرنا لما عليه النطاقات في الوقت الحالي، والتي تحظى بسمعة سيئة. وهي تستخدم في الأغلب من أجل البريد الإلكتروني، إلا أن هناك بعض النطاقات الموجودة فيها أيضًا وتستخدم برمجيات ضارة. هناك أيضًا ضوابط تعريف لشبكات بوت نت. كما أن هناك نطاقات تصيد موجودة بها، أي كل النطاقات التي نرى أنها ضارة في كومة واحدة كبيرة.

وفي هذه الحالة، يجري التفريق من خلال أكواد عودة DNS. فمن الممكن إذن اقتطاع جزء واحد فقط، مثل التصيّد فقد أو البرمجيات الضارة فقط.

إذن -- لكن ما نقوم به هو أننا نوفر البيانات. وليس لدينا سيطرة تُذكر على كيفية استخدام الناس لها. إذن فالتنسيق الذي ننشره، أي الإصدار العام المجاني، المتوفر استخدامه للجميع، هو النسق الأكثر استخدامًا داخل خوادم البريد الإلكتروني. إذن فهي قائمة حظر لنظام أسماء النطاقات. حيث تقوم أنت بعمل استعلام DNS، وتحصل على استجابة، وتتعامل مع تلك الإجابة من أجل القيام بشيء ضمن أية سياسات محلية معمول بها لديك.

هناك بعض الإصدارات المتاحة تناسب تهديدات خاصة وحالات استخدام نوعية. إذن هناك مجموعات فرعية مختلفة متاحة، على سبيل المثال، يمكن استخدامها في مستوى وحدة حل مصادقة نظام أسماء النطاقات. وهناك إصدارات متاحة للاستخدام لكل من السجلات وأمناء السجلات من أجل إجراء تحقيق وتصحيح.

ومن ثم هناك -- ما هي حالة الاستخدام الرئيسية؟ وأعتقد أن حالة الاستخدام الأولية هي الأشخاص الراغبين في اتخاذ قرارات تخص السمعة استنادًا إلى اسم نطاق ما.

ولا أقول بأن هذا مخصص للبريد الإلكتروني وحده. ربما كان هذا الأمر ينطبق في الماضي، ولكن ليس بالتأكيد ما وصلت إليه الأمور الآن.

فغالبية أسماء النطاقات كما سيخبرنا رومان، والتي تستخدم في أغراض البرمجيات الضارة وشبكات بوت نت لن تصادفها مطلقًا في أي بريد إلكتروني. ومن ثم يمكنك التحقق من جميع رسائل البريد الإلكتروني للتعرف على هذه النطاقات، ولكنك لن تنجح مطلقًا في التعرف عليها. حيث يجري استخدامها في مستوى مختلف يتواصل فيه جهاز الكمبيوتر المصاب مع اسم نطاق ما من أجل الاتصال بمركز التحكم اليدوي فيه بغرض تنزيل برمجيات ضارة إضافية.

فالمكان الذي يتوجب عليه فيه التحقق من أسماء النطاقات تلك ليس في خادم البريد الإلكتروني الخاص بك، بل سيكون في وحدة حل مصادقة نظام أسماء النطاقات أو في IDS أو أي شيء من هذا القبيل.

إذن فحالة الاستخدام تعتمد فعليًا على نوع المشكلة التي تحاول أنت حلها.

وما قاله بين، بالنسبة للتحقق من رسائل SMS، على سبيل المثال، مرة أخرى، فإن الكثير من النطاقات التي نرى أنها مستخدم في الرسائل القصيرة أو أدوات الاختصار التي يعاد توجيهها في نطاق ما، فإنك لا تراها في البريد الإلكتروني.

لذا أعتقد بأن الأمر أوسع من مجرد البريد الإلكتروني. إذا كانت لديك مشكلة أمنية وأسماء النطاقات مشمولة فيها، فإن هناك مجموعات بيانات كالتي نقدمها وكالتي يقدمها رومان وكالتي يقدمها بين يمكن أن تكون مفيدة في حل مشكلاتك الأمنية أو في التعامل والإلمام بكل ما يجري.

أل جي فورسبيرغ: شكرًا لك، كاريل.

والآن لدي سؤال لكل موفري قوائم حظر المواقع المشبوهة الثلاثة لدينا. لقد سمعناكم جميعًا تتحدثون قليلاً حول كيفية استلام وجمع التقارير أو الإشارات. ولك أن ترى من خلال ذلك أننا نتحدث حول غالبية التقارير أو الاكتشافات الآلية التي تزخر بها الإنترنت وما إلى ذلك أو النظر في البريد الإلكتروني الذي يمكنكم الدخول إليه.

هل تقول بأنه كان هناك من قبل أي شكل من أشكال التحريات البشرية في -- داخل شركتك، في قوائم حظر المواقع المشبوهة؟ لنبدأ بتعليق بين.

بين كون: نعم. نحن نستخدم -- ونستخدم مضيفًا لمتصيدي التهديدات يقومون بالفحص والتحقق، أو إجراء فحص دقيق للكثير من أعمال التصيّد التي نراها لأوراق الاعتماد. كما سنلقي نظرة على أي شيء لا يحقق نقاط عالية بما يكفي للإدراج تلقائيًا في قائمة حظر المواقع المشبوهة الخاصة بنا قبل أن تُدرج.

وأي نوع من النتائج الإيجابية الخاطئة التي نصادفها سوف تعود مرة أخرى إلى الفريق. وسوف يجري الفريق استقصاءً وسوف يقوم بإضافة يدوية لها أو إزالتها يدويًا.

لكنني أود القول بأن لدينا القليل من التداخلات البشرية.

أل جي فورسبيرغ: شكرًا لك، بين.

رومان.

رومان هويسي: نعم. إذن بالحديث حول مشروع URLhaus، على وجه الخصوص، وهو مشروع يتعقب مواقع البرمجيات الضارة، وهو مشروع تحت قيادة المجتمع. وهذا يعني أن مجموعات البينات التي نقدمها ليست إلا جزء واحد من مجموعة البيانات. أما الجزء الآخر فيتم استخراجه من خلال المجتمع.

وعندما نتحدث حول المجتمع، من المهم القول بأن هناك نوعان من مقدمي التقارير. النوع الأول وهو مقدمي التقارير الغرباء، إن جاز القول. وهؤلاء هم المستخدمون الذين لا أعلم أنني لا أثق فيهم. وكلما قاموا بالإبلاغ عن شيء إلى المشروع، فيتم فحصه يدويًا.

وعلى الجانب الآخر، لدينا مقدمو تقارير معتمدين. ويقصد بمقدمي التقارير المعتمدين أنه إذا قام مقدم تقرير معتمد بالإبلاغ عن شيء إلى المشروع، فسوف يتم إدراج الموقع تلقائيًا. وعلى الرغم من ذلك، سوف يقوم النظام بالطبع بالتحقق مما إذا كان موقع الويب يخدم أي محتوى ضار أم لا. إلا أن رابط URL سوف ينتقل تلقائيًا إلى قاعدة البيانات.

وعلى الرغم من ذلك، إذا ما استخدمته بطريقة قائمة الحظر، والتي لا تعتبر سوى حالة استخدام واحدة لمجموعة البيانات، بالطبع، فإن الموقع سوف -- أو اسم النطاقات سوف يظهر فقط في قائمة حظر عندما يكون هناك بالفعل محتوى ضار يجري تقديمه.

ومن ثم للإجابة عن سؤالك باختصار، فهو عبارة عن مزيج من روابط URL المفحوصة يدويًا أو أسماء النطاقات وروابط URL التي يتم فحصها آليًا.

أل جي فورسبيرغ: شكرًا لك، رومان.

كاريل؟

كاريل بيتر: أجل. في حالتنا هذه، فهي عبارة عن مزيج بالإضافة إلى عملية الأتمتة والتحريات البشرية. وإذا ما أردتم تعيين سمعة لكل اسم نطاق موجود على الكوكب، فمن الواضح أنك سوف تكون بحاجة لعملية أتمتة. وهناك بالفعل الكثير من -- هناك الكثير جدًا من أسماء النطاقات الموجودة، وهناك الكثير جدًا من أسماء النطاقات الجديدة كل يوم يتعين على البشر النظر فيها من حيث كل شيء والتحري عن كل شيء.

إذن جزء من هذه العملية يتم بالأتمتة، ولكن هناك بالتأكيد مكون بشري في هذا الأمر أيضًا حيث يتفحص المحققون في الأشياء المريبة أو الأشياء التي تحقق نقاط قريبة بما يكفي من عدم إدراجها أو الأشياء التي تقول عندها، حسنًا؛ كنت أتوقع أن يحقق ذلك نقاطًا أعلى لكن غير ذلك. فهي دائمًا عبارة عن مزيد من الذكاء البشري والآلي في هذا الأمر.

أل جي فورسبيرغ: شكرًا لك، رومان.

لقد بدأ الوقت يدهمنا لهذا القسم من الجلسة. وعلى الرغم من ذلك، هناك سؤال شائع وهو السؤال التالي الذي أود أن أطرحه على اللجنة. كيف تقول على الأرجح بأن هناك تقرير أو إشارة إلى وجود نتائج إيجابية خاطئة؟ وما السبب الأكثر شيوعًا لوجود نتائج إيجابية خاطئة؟ لنبدأ بتعليق بين.

بين كون: وأنا أقول بخصوص -- ضمن البيانات التي نراها والتي يجري الإبلاغ عنها في قوائم الحظر، دائمًا ما يكون هناك نتائج إيجابية خاطئة. ويتعين علينا جعل هذه النتائج الإيجابية الخاطئة عند أقل مستوى ممكن.

وأود القول بأن السبب الرئيسي بشكل أساسي الذي أراه وراء النتائج الإيجابية الخاطئة هو عدم فهم ماهية ما هو ضار وما هو غير ضار أو الأشخاص الذين سيحصلون على أشياء لا يفضلونها، والتي يبلغون عنها بأنها ضارة، حتى وإن لم تكن كذلك.

أل جي فورسبيرغ: شكرًا لك، بين.

رومان.

رومان هويسي: إذن هناك بالطبع نتائج إيجابية غير صحيحة. وقد كانت موجودة دائمًا. ومن الممكن الإبلاغ عنها من خلال وجهة مستخدم الويب عن طريق أي شخص.

فإذا ما بدأ مبلّغ معتمد -على سبيل المثال- بتوفير بيانات يعرف بأنها برامج ضارة -- على سبيل المثال مواقع التصيّد أو مواقع البريد غير المرغوب أو غيرها من الأشياء -- فسوف يتم حظره ببساطة وإخراجه من المشروع.

ومن ثم أرى أن تدفق البيانات جيد إلى حد كبير. ولكن كما قلت، فإن النتائج الإيجابية الخاطئة يمكن أن تحدث.

أل جي فورسبيرغ: وأخيرًا، كلمة رومان. لا، أخيرًا كاريل. عذرًا.

كاريل بيتر: نعمن فإن النتائج الإيجابية الخاطئة سوف تحدث دائمًا. وكما قال بين، فإن مهمتنا تتمثل في التأكد من أن العدد عند أقل مستوى ممكن.

وبالنسبة لما يقوم الناس بالإبلاغ عنه، فهناك -- كما تعلمون، منذ سنوات عدة عدما بدأ موفرو البريد الإلكتروني الحصول على أزرار "هذا بريد غير مرغوب" في واجهات البريد الأبيض الخاص بهم، فإن من أكبر الأشياء التي أبلغ الناس عنها وتبين أنها ليست بريدًا غير مرغوب أو غير ضار فكانت رسائل البريد المقدمة من -- رسائل البريد التي لم تعجبهم، مثل فاتورة لم يرغبوا في سدادها أو خطاب رفض من طلب وظيفة. ومن ثم في تلك الحالة، فإن غالبية الأنظمة تعمل بطريقة إذا توفر فيها ما يكفي من الأشخاص، أو إذا أبلغ قطاع كبير من الجماهير عن شيء ما، فإن المعالجة التلقائية تعمل، وتقوم بإظهار علامات السمعة الرديئة لأي بروتوكول إنترنت أو اسم نطاق أو مرسل أو محدد برمجة بيكون أو أيًا كان. ودائمًا ما تتوفر الفرصة بأنه في الحالات الخاصة إذا كانت تقارير مستخدم جزء من الأشياء التي تقوم أنت بها ويقوم الناس بالإبلاغ عنها كما قال بين، بأنها الأشياء التي لا يحبونها، فقد لا تكون بريدًا غير مرغوب وربما لا يكون ضارًا وربما لا يعمل لأغراض التصيّد. ولكن بالنسبة للكثير من الناس، فإن الفارق بين زر الحذف وزر "هذا بريد غير مرغوب" غير موجود.

إذن، نعم، هذا يمثل تخوفًا دائمًا. لكن نعم، بشكل واضح إذا ما فكرت في الأمر، وأعتقد أن هذا الكلام موجه إلى رومان وبين أيضًا، وهو حقيقة أن أي نتيجة إيجابية خاطئة سوف نحصل عليها في مجموعات البيانات الخاصة بنا، وسوف تكون هناك مشكلات دائمًا. وربما تحظون بأسبوع لا يحدث فيه أي شيء سيء، وبعد ذلك في الأسبوع التالي من المحتمل أن يحدث ثلاثة أو أربعة أو خمسة منها أو أيًا كان. لكنها حقيقة حياتية بأنها سوف تحدث. الأهم من ذلك هو كيفية التعامل مع ذلك، وجعل من هناك أن يتأكدوا سريعًا من أن الأشياء يجري التعامل معها على الوجه الصحيح.

ولكن بشكل واضح، وباعتبارنا موفرين للبيانات، وباعتبارنا صناع للبيانات، فليدنا نحن اهتمام ومصلحة في التأكد من أن البيانات الخاصة بنا على أحسن ما يكون من الجودة. وكما تعلمون، إذا لم تكن البيانات الخاصة بنا جيدة، فسوف يتوقف الناس عن استخدامها، وبعد ذلك في تلك المرحلة، ما الهدف؟

وبالنسبة لصناع البيانات، وأنا أعتقد على وجه الخصوص، كما تعلمون، ربما يوافق رومان على ذلك، تصبح البيانات أكثر قوة كلما بدأ الناس في استخدامها. وإذا كان هناك اسم نطاق يجري استخدامها من أجل -- كما في سيناريوهات شبكات بوتنت" التي تعمل بنظام الأمر والتحكم، كلما زادت سرعة اسم النطاق أي تعطيله أو زاد عدد الأشخاص الذين يقومون بحجبه، زادت سرعة الإنترنت.

وإذا ما -- أو إذا أبلغ رومان عنه وقال الناس بأن هذه التقارير لا تجدي نفعًا، فإن هذا النوع الخاص بها على العكس من المهمة التي نريد الحصول عليها.

وما نريد الحصول عليه هو البيانات التي نقدمها، ونريد أن يتم استخدامها على أوسع نطاق ممكن ونريد من الناس بأقرب ما يمكنهم وبحيث يصبح في نهاية المطاف مكانًا أكثر أمانًا. لأن هذا في رأي موجه لنا نحن الثلاثة، لكل من بين ورومنا أيضًا، أن هذا ما يحرك العمل الذي نقوم به. ونحن نحاول أن نحل مشكلات الأمن الخاصة بالشبكات وبالسجلات وأمناء السجلات وللمستخدمين النهائيين في نهاية المطاف. وفي النهاية، الأمر كله منوط بحماية المستخدم النهائي. فكلما زاد عدد الأشخاص الذين يستخدمون البيانات، زاد مستوى حماية المستخدمين النهائيين. ولن يستخدم الأشخاص البيانات إذا لم تكن البيانات جيدة.

أعني أن هذا شيء هام للغاية ونرغب دائمًا في القيام به.

وثمة طرق لا محدودة في القيام بإجراءات عنيفة وحيث يمكنك القول، حسنًا، إذا قمت بهذا الأمر فسوف أحجب المزيد -- وسوف أكتشف المزيد من الأشياء السيئة التي تحدث. إلا أن هناك العديد من السيناريوهات التي يوجد فيها دائمًا شخص ما في مكان ما يقوم تقريبًا بنفس الشيء الذي يقوم به الأشرار أو لديه نفس نوع روابط URL الغريبة أو لديه نفس نوع أسماء المضيفين الغريبة. ويكون الوضع بأنه إذا ما رأيت اسم المضيف هذا، فلا بد أنه سيء. نعم، حسنًا، 99 من أصل مائة سيئين لكن الأخير غير ذلك فعليًا.

إذن فالأمر دائمًا ما يكون عبارة عن تصرف لتحقيق التوازن، وكل ما عليك هو التأكد من أنك تحاول أن تكون على أفضل حال ممكنة وأن تكون لديك إجراءات جيدة في التعامل مع أي من المشكلات التي تظهر.

وقد قمت بالفعل بتدوين ذلك في مربع الأسئلة والأجوبة، ولكن على سبيل المثال، يمكن لأي شخص معنا الدخول وإزالة أي اسم نطاق. ولا يتعين عليكم -- لا يتعين عليكم ملء وتعبئة نماذج مطولة ولا يتوجب عليكم التواصل معنا عن طريق الهاتف أو أيًا كان. فهذا من الأشياء التي يمكن لأي أحد التعامل معها ذاتيًا عبر الإنترنت مثل الزر الذي ذكره رومان.

ومن الواضح أن من مصلحتنا أن نتأكد من أن عملية التعامل مع أي نتائج إيجابية خاطئة قد تحدث تكون سلسة إلى أبعد الحدود بالنسبة لأي شخص يقع ضحية للنتائج الإيجابية الخاطئة.

أل جي فورسبيرغ: شكرًا لك، رومان. اسمحوا لي أن أقاطعكم في هذه النقطة.

نحن الآن في قطاع الأسئلة الخاصة بالجماهير، وأود أن أتناول سؤال آخر قبل أن ننتقل إلى القسم التالي من الجلسة.

أود أو أسأل رومان عن كيفية -- هل قوائم حظر المواقع المشبوهة أو موجزات استعلامات التهديدات التي كانت -- اسمحوا لي أن أطلق عليها اسم البيانات الأصلية، هل تتعاون على الإطلاق مع بعضها بعضًا؟ فعلى سبيل المثال، هل -- فهل يوفر مشروع abuse.ch على سبيل المثال لشركة Spamhaus بيانات حول النتائج الإيجابية الخاطئة أو الإشعارات الهامة التي قد تكون لديهم؟

رومان هويسي: نعم، هذا السؤال تم طرحه في مربع الأسئلة والأجوبة من قبل، وأعتقد أنه سؤال هام للغاية.

إذن هناك بالطبع عمليات يتم من خلالها الإفصاح عن المعلومات ذات الصلة بالتهديدات الحالية وذلك مع الموزعين أو مع قوائم حظر المواقع المشبوهة. والبعض من هذه العمليات ثنائي. فهي موجودة على سبيل المثال لدى شركة Spamhaus أو لدى خدمة التصفُّح الآمن أو لدى موفري قوائم حظر المواقع المشبوهة. إلا أنه -- من خلال موقع abuse.ch، فإن قاعدة البيانات متاحة للجميع. حيث يمكن للجميع الحصول عليها. كما أن هناك شطر كبير من موفري استعلامات التهديدات التجارية، على سبيل المثال، يستهلكون هذه الموجزات ويفعلون بذلك ما يحلوا لهم.

وحيث لا يلزم وجود أي تسجيل، فإن هناك بالطبع مشكلة لدي تتمثل في أنني لا أعرف من الذي يستخدم الموجز الخاص بي نطاقًا عامًا له.

وعلى الجانب الآخر، فيما يخص السؤال السريع الخاص بتبادل المعلومات حول النتائج الإيجابية الخاطئة، أعتقد أن هذا موضوع هام. وإلى حد ما أنا مهتم أو على دراية، فليست هناك آليات معمول بها في الوقت الراهن حول كيفية الإبلاغ عن أي نتيجة إيجابية خاطئة.

كيفية التعامل مع ذلك عندما يتم وضع علامة تمييز على نتيجة إيجابية خاطئة، فبالطبع -- فإنها تخرج بالطبع من الموجزات. وأنا أتوقع بأن موفري قوائم حظر المواقع المشبوهة أو غيرهم -- أو غيرهم من موفري معلومات التهديدات، سوف يلاحظون هذا الإدخال ويقومون كذلك بحذفه. لكنني بالتأكيد ليس لدي أي تأثير على هذا الأمر. وأعتقد أن هذا من الأشياء التي يمكن أن تكون -- يمكن أن تكون موضوعًا بحاجة لمناقشة، وأن تكون هناك منصة للتبادل حيت النتائج الإيجابية الخاطئة -- حيث يمكن للمعلومات حول النتائج الإيجابية الخاطئة على سبيل المثال -- يمكن الإعلان عنها ومشاركتها مع موفري الخدمات الآخرين.

أل جي فورسبيرغ: شكرًا لك، رومان.

لقد وصلنا الآن إلى الكلمة التعريفية الخاصة بـ ICANN في هذه الجلسة. والآن أترك الكلمة إلى سامانه.

سامانه تاجاليزاديخوب: مرحبًا بكم جميعًا. للعلم والإحاطة، أنا سامانه تاجاليزاديخوب. وأنا أمثل مكتب المسؤول الفني الرئيس في ICANN اليوم، وسوف أتحدث حول قوائم حظر المواقع المشبوهة ووجهة نظرنا فيها.

شكرًا. الشريحة التالية، رجاءً.

وحتى الآن فقد أجرينا مناقشات جيدة للغاية. وأعتقد أن بعض النقاط تمت الإشارة إليها بالفعل في العرض التقديمي وقام بتغطيتها أعضاء اللجنة وأيضًا من خلال الأسئلة التي تمت الإجابة عنها. وأعتذر إن كان هناك أي تكرار.

أردت أن أبدأ من الأساس أي من قائمة حظر المواقع المشبوهة. حيث يمكن أن تأتي في صورة قائمة حظر لبروتوكولات الإنترنت أو قائمة حظر مستندة إلى النطاقات. فما تمثله تلك القوائم بشكل عام هو كيانات تعتبر ضارة أو غير جديرة بالثقة أو ببساطة سيئة السمعة. وقد قمت بإعداد قائمة تضم بعضًا من حالات الاستخدام الموجودة في هذا المجال أو عالم الأبحاث أو الأوساط الأكاديمية. كما أن الناس يستخدمونها من أجل تغذية جدران حماية نظام أسماء النطاقات، لمنع مرور البيانات الضارة. كما أنها تستخدم في استبعاد مرور البيانات غير المرغوب، والذي يأتي في المعتاد في صورة بريد إلكتروني غير مرغوب أو رسائل بريد إلكتروني لغرض التصيّد. ويجري استخدامها من قبل شبكات إيصال المحتوى وذلك لمنع إيصال المحتوى الضار إلى عملائهم وأيضًا يتم استخدامها باعتبارها جزء من الرد على الأحداث أو لأغراض إنفاذ القانون لتحديد وتعريف البنية التحتية الضارة المتورطة في الهجوم.

ويمكن تصنيفها إلى آليات مشاركة مختلفة. ومن ثم أعتقد أننا اليوم لدينا بعض الأمثلة على القوائم التي تعد بالأحرى ذات مصدر مفتوح، لكنها أيضًا يمكن أن تتخذ شكلاً تجاريًا، وإما أن تكون متاحة من خلال قيد سعري، أو مستندة إلى الترخيص، أو الدفع على أساس الاستخدام، ويمكن أن تكون -- يتم الحفاظ عليها من خلال شركات غير ربحية متخصصة في استقصاء معلومات التهديدات.

كما أن هناك غيرها مفتوحة المصدر يتم استخدامها في الغالب من خلال القطاع الأكاديمي وغيره أيضًا. والأمثلة على ذلك شركة Spamhaus وabuse.ch وPhish Tank وتلك التي أنا على دراية بها، من بين آخرين.

ويمكن أن تكون أيضًا مقتصرة على التهديدات. إذن فإن بعض القوائم ترتكز فقط على بعض التهديدات. على سبيل المثال، abuse.ch الذي يقيمه رومان، يضم موجزات مختلفة تركز إما على شبكة بوت نت أو على البرمجيات الضارة أو برامج الفدية، وأعتقد أن هذا قد توقف الآن، إلى آخر، أو أنها عامة أو أكثر عمومية. وهي تضم جميع أنواع التهديدات، ومثال عليها هو قوائم SURBL.

الشريحة التالية، رجاءً.

وقد تحدثنا بالفعل عن ذلك وناقشناه مناقشة موسعة في اللجنة. شريحة العنوان تذكر خصائص وعيوب القائمة. وأود أن أسلط الضوء على كلا الجانبين لأنه بالنسبة لباحث ما فهذا يمثل ميزة ويمكن أن يمثل عيبًا بالنسبة لباحث آخر.

إذن بالغرض الأساس من استخدام أي قائمة حظر للمواقع المشبوهة من وجهة نظرنا أن من المهم أن نفهم ما الذي تريد القيام به. والأهم من ذلك في حقيقة الأمر أن نفهم ما هي الطريقة القائمة وراء أي قائمة حظر للمواقع المشبوهة وما الذي تمثله وكيف يمكنك استخدامها لتحقيق أفضل الأغراض لديك.

وتتمثل بعض المميزات في أن بعض القوائم يمكن تخصيصها وتركيزها إلى حد كبير، بحيث -- لأنها موجهة بالأساس إلى غرض محدد. ويجب على أي شخص يرغب في استخدامها فهم ذلك الغرض وتحديد ما إذا كان يناسب ما يبتغيه منها أم لا.

والبعض الآخر -- بشكل أساسي -- وأنا أسلط الضوء على هذه النقاط بشكل عام، وباعتباري أحد الباحثين. وفي المعتاد لديها تغطية محدودة للغاية بسبب القيود المادية ونقاط الأفضلية. وفي المعتاد يكون موقع عمل موفري موجزات البيانات في مواقع جغرافية معينة، ومن ثم قد يكون لديهم تمثيل أقل فيما يخص موقع جغرافي محدد.

وأنا أعلم أنه بمرور الوقت، وبما أن لدي الخبرة في العمل على هذا الأمر لمدة سبع أو ثماني سنوات، فإنه وبمرور الوقت تم تحسين غالبية هذه القوائم من حيث التغطية، لكن ما يزال من المهم جعل هذا -- وضع هذا الأمر في الاعتبار عند القيام بأي نوع من التحليل لهذه القوائم.

هناك نقطة صغيرة وهي أن فكرة النظر في الجودة ومؤشرات الاعتمادية المختلفة في قوائم الحظر ليست جديدة. فقد خضعت بالفعل للبحث منذ عام 2009 أو 2010. إذن، في هذا العرض التقديمي، فإنني أسرد بعض الأبحاث الأكاديمية وأبحاث الصناعة التي تم القيام بها فيما يخص القوائم، لكن يمكنكم التواصل معي للحصول على المزيد إن احتجتم ذلك.

وثمة أمر أو سمة أخرى في قوائم حظر المواقع المشبوهة وهي وجود وثائق محدودة بشكل نموذجي حول الطرق الداخلية. أحد الأسباب التي أفهمها من خلال الحديث، وإجراء المحادثات الشخصية مع موفري القوائم هو أنها غير مباشرة في توثيق كامل العملية والإجراءات حيث إن البعض منها يمكن أن يكون مخصصًا أو يمكن أن يكون مفصلاً أو ارتكاسيًا للغاية. لذلك من الصعب أن نحافظ على وثائق آنية في الوقت الفعلي تمثل كل ما تم -- بأن موفر قائمة حظر المواقع المشبوهة يجري موجزات نوعية.

كما أن هناك أيضًا -- بما أن لدينا العديد من موفري قوائم حظر المواقع المشبوهة، من المتوقع أن هناك مختلف -- هناك الكثير من التنويعات من حيث المنهجية، ومن ثم -- من حيث جمع البيانات والتصنيف والحفاظ على مسميات قوائم الحظر. وهذا يؤدي إلى تأثيرات مختلف على كل من التغطية والموثوقية والفاعلية وسرعة الإبلاغ.

والجدير بالذكر أن هذه ليست بالضرورة شيء سيء. فقد يكون في حقيقة الأمر شيء جيد. حيث يمكن للتنوع أن يحقق المزيد من المعلومات في القائمة طالما أن المستخدم يفهم التنوع ويتعامل معه تعاملاً صحيحًا.

الشريحة التالية، رجاءً.

لقد أوضحت هذه النقطة بالفعل. إذن ما -- ما أهمية معرفة هذه المآخذ، المعروفة أيضًا بلفظ الخصائص؟ في البداية، من المهم بالنسبة لكل مستخدم سواء كان مشغلي شبكات أو باحثين أو شركات أمنية تعتمد على هذه الموارد أن تعرف الفروق بين القوائم والخصائص أو العيوب، أو التحذيرات، وأيضًا معرفتها من أجل تصميم دفاعات أكثر فاعلية وطرق للتصنيف بالإضافة إلى وضع هذه الأشياء في الحسبان أثناء القيام بالأبحاث أو الإبلاغ عن النتائج.

وأحد الأمثلة الجيدة على هذا والذي صادفته كثيرًا على المستوى الشخصي في مجتمع ICANN هو أننا غالبًا ما نقول بأن هناك هذا البحث الذي أوضح أن التصيّد سوف -- أن اتجاه نشاط التصيّد في ارتفاع. ولماذا يتباين عن البحث الآخر الذي يقوم الشخص "ب" ويوضح أن الاتجاه في هبوط؟

إذن هذه هي النقطة الفعلية التي أحاول أن أبينها، وأعتقد أن هذه هي النقطة الرئيسية في مجموعة الشرائح التي أعرضها، وهي أنه بالاعتماد على ماهية مجموعة البيانات التي يجري استخدامها، واعتمادًا على طبيعة الإطار الزمني الذي يجري وضعه في الاعتبار، وما هي عملية التسمية التي استحوذت عليها مجموعة البيانات، إلى آخره، يمكن إجراء تغيير على أي اتجاه.

فليس هناك اتجاه مطلق في أي من الموجزات، على الأقل من واقع خبرتي، بحيث يمكن لأي شخص الإبلاغ بأن هذا الاتجاه مطلق. فالأمر دائمًا جزئي، فهو إذن دائمًا من منظور الموجزات. ووفقًا لما أبلغ به كل من كاريل وبين بالفعل عدة مرات، أنه من وجهة نظرنا الخاصة حيال قائمة حظر المواقع المشبوهة، فهذا ما نراه. فالأمر إذن دائمًا جزئي، ودائمًا ما يعتمد على المنهجية في العمل.

الشريحة التالية، رجاءً.

وفي الشرائح القليلة القادمة سوف أسلط الضوء على بعض حالات الاستخدام التي لدينا داخل ICANN. إذن كيف نستخدم قوائم حظر المواقع المشبوهة.

إن DAAR -- أو الإبلاغ عن نشاط انتهاك النطاق عبارة عن مشروع -- هو أحد المشروعات الرئيسية التي تستخدم قوائم حظر المواقع المشبوهة التي قد يكون غالبيتكم على دراية بها.

ولن أتطرق إلى تفاصيل ما يقوم به مشروع الإبلاغ عن نشاط انتهاك النطاق DAAR، ولكننا بإيجاز -- إذن يأخذ النظام أسماء النطاقات من ملفات منطقة السجل وبعد ذلك يأخذ أسماء النطاقات من مجموعة الموجزات المحددة مسبقًا للتصيّد والبرمجيات الضارة وشبكات بوت نت والأمر والسيطرة والبريد غير المرغوب باعتباره متجه للإرسال والتسليم. وبعد ذلك يتداخل مع النطاقات من ملفات المنطقة وقوائم حظر المواقع المشبوهة الخاصة بها ويقوم بمعالجة وحساب المؤشرات وإنشائها، أي مؤشرات يومية وشهرية لنوع مختلف من التحليل قد تكونون على دراية به من تقارير ICANN الشهرية -- تقارير الإبلاغ عن نشاط انتهاك النطاق DAAR الشهرية، التي تنشر بشكل عام على مواقع ICANN على الويب. فهي توضح الاتجاهات التي تتركز فيها تهديدات أمن نظام أسماء النطاقات لكل نقطة من الزمن وكيف أن هذا التركيز يتغير بمرور الوقت.

إذن ما يجب أن نضعه في الحسبان، هو أن النظام بالطبع يجري بالفعل معالجة مسبقة وموسعة بالإضافة إلى إخلال وتنظيف وتوحيد موجزات بيانات قائمة حظر المواقع المشبوهة التي نشرتها بالنظر إلى جميع الحالات الجانبية، إلخ. علمًا بأن التفاصيل ورادة في وثيقة منهجية العمل الخاصة بالمشروع.

الشريحة التالية، رجاءً.

بريندا بريور: عذرًا. قبل أن تواصل، هل لي أن أطلب منك التكرم بإبطاء سرعة كلامك لصالح المترجمين الفوريين. شكرًا.

سامانه تاجاليزاديخوب: بالتأكيد.

لقد قمنا أيضًا بعمل مشروع. باعتبار أننا مجموعة بحث الأمن والاستقرار والمرونة، فقد أجرينا أيضًا مشروعًا لإدارة دعم الامتثال في إدارة الامتثال في ICANN والتي قمنا فيها بإنشاء مؤشرات التقاط من أجل أمناء السجلات. إذن فهذه ليست -- ليست هذه -- كان هذا المشروع لمرة واحدة إلى الآن وقمنا فيه بنفس ما قمنا به في مشروع الإبلاغ عن نشاط انتهاك النطاق DAAR ولكن فقط لصالح أمناء السجلات. وسوف يركز ذلك على التصيّد والبرمجيات الضارة لفترة زمنية محددة، إذن فقد كانت فقط مقادير محددة.

وقمنا بحساب المؤشرات من أجل أمناء السجلات وأسر أمناء السجلات التي تبيّن تركيزات تهديد في نقطة واحدة وبمرور الوقت.

ولأجل هذا المشروع الخاص، حصلنا على إمكانية الوصول إلى الولوج إلى بيانات التسجيل الجماعي BRDA حيث لا يمكننا استخدام غيرها لأغراض الامتثال في الوقت الحالي.

الشريحة التالية، رجاءً.

المشروعات البحثية الأخرى الجارية في الوقت الحالي داخل مكتب المسئول الفني الأول، فإننا نستخدم قوائم حظر المواقع المشبوهة من أجل تطوير نماذج تنبؤية عندما يصبح أي نطاق ضارًا وأيضًا لاستخراج الأنماط من أجل توصيف وتصنيف النطاقات الضارة.

كما أننا نخطط لتوظيف واستخدام نفس الطريقة التي تم استخدامها من خلال دراسة COMAR التي تم طرحها في اليوم الفني خلال اجتماع ICANN السابق من أجل التفريق بين النطاقات المسجلة لأغراض ضارة والنطاقات المنتهكة من خلال استخدام قوائم حظر المواقع المشبوهة باعتبارها واحدة من المدخلات.

الشريحة التالية، رجاءً.

إذن كيف نقوم في الوقت الحالي -- أو بالنسبة لغالبية المشروعات التي أدرجتها في الشرائح السابقة، فقد قمنا بتقييم -- أو أجرينا تقييمًا على مجموعة قائمة السمعة المنتقاة، بالإضافة إلى مراقبة الموجزات لفترة من الزمن قبل تضمينها كجزء من عملنا البحثي.

وكان ما قمنا به بشكل أساسي هو انتقاء القوائم الأكثر شهرة ضمن الأوساط الأكاديمية وعالم الصناعة استنادًا إلى النشر. إذن ذات السمعة استنادًا إلى المنشورات لأنها قد تكون غير موضوعية. وقد ملنا إلى تلك التي تضم وثائق أفضل ومعايير محددة للبيانات، من خلال تسجيل عملياتنا وإتمام معاييرنا الحالية من حيث التغطية.

أجل.

الشريحة التالية، رجاءً.

وعلى الرغم من ذلك، فإننا نخطط للانتقال إلى معايير تقييم أكثر قوة. فهذا عمل مستمر.

وأؤكد مرة أخرى، أنني أود التأكيد على أن القيام بالعمل فيما يخص تقييم قائمة حظر المواقع المشبوهة ليس جديدًا، فقد تم من قبل. وما نقوم به هنا هو أننا فقط نجعله أكثر اكتمالاً ونعمل على جعله ذات صلة بالنسبة للموجزات على حالها اليوم.

ومن فإننا نعمل على تطوير مؤشرات لما نطلق عليه النقاء، وهو معدلات النتائج الإيجابية الخاطئة/النتائج الإيجابية الخاطئة للقائمة. وبين قوسين، ليس هذه مؤشرات مباشرة بالنظر إلى أن لها بيانات ميدانية فعلية، وهي البيانات التي تتم تسميتها يدويًا ضمن هذه المجموعة، وليست مباشرة؛ وهي في الواقع المشكلة الأولى لأي باحث يعمل مع قوائم حظر المواقع المشبوهة.

ونحن ننظر في مسألة تقدير التغطية للقوائم بالإضافة مستوى الاستجابة ووقت الرد والدقة ومدى تفصيل المعلومات التي يكون عليها الموجز، ومدى استقرارها بمرور الوقت، ومدى الحيوية، وما هو مقدار النطاقات المدرجة الإيجابية فعليًا والنشطة عندما تظهر في أي موجز بيانات.

وهي ليست ثابتة إلى الآن. ونحن نحاول العمل عليها لكي نعرف ما إن كان بإمكاننا تحقيق نتائج معتمدة أم لا. وقد تتغير بمرور الوقت ونحن نعمل على مشروع البحث أو أنها قد تظل كما هي. لكننا سوف نبقيكم على اطلاع حيال هذا العمل. وفي الوقت الحالي، ليس الأمر يتعلق العمل الجاري في الوقت الحالي.

الشريحة التالية، رجاءً.

إليكم المراجع التي استخدمتها خلال عرضي التقديمي. إذن فقد انتهى العرض التقديمي الآن. ثمة نقطة أخيرة أود أن أطرحها لأنني بصفتي المسئول التقني الأول في ICANN، فإننا نجري العديد من مشروعات المحاولة والخطأ من خلال استخدام قوائم حظر المواقع المشبوهة وعلى وجه الخصوص للسجلات وأمناء السجلات من أجل محاول توفير المزيد من المعلومات فيما يخص التهديدات الأمنية.

وبعض الأسباب وراء تطوير بعض المؤشرات التي تحدثنا عنها في السابق في المجتمع ليست مباشرة ليست مباشرة ولا نريد أن ننشر شيئًا غير معتمد وهذه هي المشكلة الفعلية التي نناقشها اليوم.

على سبيل المثال، فقد تحدثنا سابقًا حول وقت التشغيل، كما في الوقت الذي يستغرقه المشغلون للتفاعل مع أي انتهاك محدد يخص الأمن. وإذا ما قمت بربط الموضوع مرة أخرى بالمناقشة التي كانت جارية في اللجنة ولكن أيضًا في العرض التقديمي فيما يخص الفارق في المنهجية العمل خلف كل قائمة، فيمكن للمرء أن يدرك سريعًا أنه إذا ما تناولنا العديد من القوائم وحاولنا إنشاء مؤشر لمشغل محدد يمثل وقت التشغيل، فإننا بذلك نخلط بين المنهجيات. والمؤشر في حد ذاته لا يمثل شيئًا يمكن اعتباره معتمدًا حسب كل مشغل. كما أنه يعتمد على منهجية العمل المتبعة لدى موفر قائمة حظر المواقع المشبوهة.

إذن هذه أمثلة على بعض الصعوبات التي نواجهها في مشروعاتنا، والتي نحاول معالجتها. لكن من الجيد فعليًا أن نجلبها -- أن نطرح ذلك في مناقشات المجتمع، وقد كانت هذه فرصة جيدة.

شكرًا لكم جميعًا. ويسرني الإجابة عن أية أسئلة قد تكون لديكم. ولا أعلم شيئًا عن الوقت.

أل جي فورسبيرغ: أنا أل جي فورسبيرغ، منسق الجلسة. سوف يتوجب علينا الآن الانتقال إلى القسم التالي من هذه المناقشة بسبب قيود الوقت.

والجلسة التالي هي المناقشة الختامية والتي أود فيها العودة إلى الأطراف المتعاقدة لدينا فيما بين أعضاء اللجنة، وهذا يعني كلاً من ريغ وماثيو.

لذلك أود أن أسألكما عما إذا كنتما تستخدمان قوائم حظر المواقع المشبوهة اليوم، وإن كان الأمر كذلك، فكيف ذلك. لنتناول رد ريغ أولاً.

ريغ ليفي: شكرً لك، أل جي.

في هذا الوقت، لا تدفع شركة Tucows مقابل لتوزيع أي قائمة حظر من أجل بياناتها. وعلى الرغم من ذلك، فإننا نتلقى تقارير من العديد من الأسماء الكبيرة بشكل منتظم.

وللأسف، فإن غالبية التقارير تميل إلى عدم احتواء رابط URL الكامل، لذلك من الصعب بالنسبة لنا في كل حالة التخفيف منها، لأننا لا نميز بالضرورة وعلى وجه التحديد ماهية المشكلة من حيث ما إن كان نطاقًا مخترقًا أو إذا كان مسجلاً سيئًا.

ويمكننا ذلك في بعض الحالات. حيث يمكننا أخذ هذا النطاق والنظر فيها داخل نظامنا وأن نقول، حسنًا، نعم، لقد كان هذا أيضًا جزء من شراء بطاقة ائتمان للاحتيال. وفي تلك الحالات، غالبًا ما يتم فصل النطاق بالفعل عن الاتصال بالإنترنت قبل أن نحصل على التقرير أو البلاغ. ولكننا رغم ذلك نحصل على التقرير.

أما في هذا الوقت فإننا لا نحصل عليه. ونحن الآن بصدد النظر في بعض الخيارات المتاحة. والمهم بالنسبة لنا تضمين سرعة الإزالة من قائمة الحظر. إذن ليس كافيًا بالنسبة لي أن أبلغ فقط عن أن أحد النطاقات سيء ولكن أيضًا بالنسبة لي أن أقول، رائع، شكرًا جزيلاً على التقرير والبلاغ، لقد تعاملنا معه، وبعد ذلك نطلب منهم إزالته من القائمة.

أل جي فورسبيرغ: شكرًا لك، ريغ.

ماثيو؟

مات توماس: نعم. أود فقط أن أطرح بعض النقاط الإضافية حول عدم جدوى قوائم حظر المواقع المشبوهة التي أشار إليها بالفعل بعض أعضاء اللجنة، وهي تدور أكثر حول مفهوم السياق الذي بدأ فيه كاريل بالطرح وأيضًا ما جاء على ذكره أعضاء آخرون في اللجنة.

أعتقد أن من المهم للغاية أن نفهم السياق الذي يجري فيه تطبيق قوائم حظر المواقع المشبوهة. ويجب أن نبدأ من خلال القول بأنها أدوات فعالة للغاية عند استخدامها في السياق المناسب والصحيح. وأعتقد أن الكثير من ذلك يعود إلى فهم أصل ما كانت عليه قوائم حظر المواقع المشبوهة هذه والغرض الذي تم تصميمها من أجله. حيث تم تصميمها كأدوات لحماية المستخدمين النهائيين والشبكات والبيئات.

إذن في هذا النوع من حالات الاستخدام، فإن لها خصائص محددة مخصصة لذلك الغرض. وقد تكون تحررية أكثر إلى حد ما من حيث --عفوًا -- ما تشتمل عليه في قائمة حظر المواقع المشبوهة. لكنها قد تكون كذلك أكثر تحفظًا إلى حد ما من حيث إزالة بعض من تلك الإدخالات.

إذن من خلال منظور أو من خلال حالة استخدام أمن المشروعات باعتباره ممارسًا للأمن، فهذه خاصية جيدة، اتفقنا؟ وفي ذلك السيناريو، فإنك أقل قلقًا حيال النتائج الإيجابية الخاطئة وتكون أكثر انشغالاً بحماية هؤلاء المستخدمين النهائيين.

ولكن عندما نبدأ في استخدام قوائم حظر المواقع المشبوهة في سياقات أخرى، من المهم لنا أن نفهم خصائص قوائم حظر المواقع المشبوهة تلك وكيف أنها سوف تؤثر على مختلف الطرق المتنوعة التي تستخدمها قوائم حظر المواقع المشبوهة تلك بقياسات أو أدوات أو دراسات مختلفة. ومعرفة الفروق الدقيقة في الطريقة التي يتم بها إنشاء وتركيب قوائم حظر المواقع المشبوهة تلك، وكيفية الحفاظ عليها والكيفية التي تدار بها وكيف يتم فحصها سوف يؤثر في نهاية المطاف على قدرتك على استخدام قائمة حظر المواقع المشبوهة بأي نوع آخر من الطرق الشمولية.

وفي سبيل ذلك، أعتقد أن من المهم أن نظل جميعًا على دراية بكيفية استخدامها وكيفية تطبيقها وفقًا لذلك.

شكرًا.

أل جي فورسبيرغ: شكرًا.

ريغ ليفي: أود أن أسلط الضوء على هذه المسألة سريعًا، وهي أن الشفافية في فهم كيفية تركيب وتشكيل قوائم حظر المواقع المشبوهة مفيدًا للغاية بالنسبة لمن يستخدمون البيانات الخاصة بهم.

أل جي فورسبيرغ: شكرًا لك، ريغ.

مرة أخرى، ريغ ومات، هل تقولان بأن هناك المزيد مما يمكن للأطراف المتعاقدة والسجلات وأمناء السجلات القيام به بمساعدة من قوائم حظر المواقع المشبوهة إذا كانت أي نقطة من -- إذا ما تم تقديم البيانات لكم أو تحديثها بطريقة أخرى؟

مات توماس: أنا مات توماس للعلم والإحاطة.

هذا السؤال المطروح شيق للغاية، أل جي. وأعتقد أن ما يهمني في ذلك السؤال هو كلمة "المزيد". فماذا يعني ذلك بالضبط؟ وكيف نقيس كلمة "المزيد"؟

هل "المزيد" من حيث سياق انتهاك النطاقات تعني أن المزيد من النطاقات يجري تعطيلها؟ أم أنها تعني أننا أكثر فاعلية في قطع وتفكيك أدوات البنية التحتية الأساسية التي تدعم أنواع انتهاك نظام أسماء النطاقات DNS الموجودة فعليًا.

وأعتقد أن المقصد تقريبًا هو أنه يتوجب علينا الرجوع خطوة للوراء أي لا يتعلق الأمر فقط بقوائم حظر المواقع المشبوهة والأطراف المتعاقدة في هذه المنظومة. فهو مجتمع أوسع بحاجة إلى التركيز على انتهاك نظام أسماء النطاقات DNS. وهناك العديد من الكيانات المختلفة بالفعل يتعين عليها بشكل شمولي أن تتعاون معًا من أجل هذا الأمر قابلاً أكثر للتنفيذ بشكل فعلي، اتفقنا؟

ويجب علينا إشراك موفري الاستضافة، وشبكة إيصال المحتوى وموفري البريد وجهات إنفاذ القانون. ومن خلال التعاون الشمولي، يمكننا البدء في محاربة الانتهاك وتحقيق المزيد بهذه الطريقة.

وأنا على يقين من أن موفري قوائم حظر المواقع المشبوهة بإمكانهم طرح عشرات الأمثلة على قيامهم بجمع البيانات، وقيامهم بتحديد نطاقات التصيّد، وحالات وضعها في قائمة حظر المواقع المشبوهة، وحالات تعطيلها، وبعد ذلك بساعتين أو يوم يظهر مرة أخرى على مجموعة من النطاقات الجديدة. فهل عملية تصحيح الانتهاك تلك تحقق المزيد بفاعلية حقًا؟ أم أنها تسببت فقط في نشر الأسماء ودفع انتهاك النطاقات ذلك إلى مكان آخر، اتفقنا؟ هل يجري وقف الانتهاك الفعلي نفسه؟

إذن فالمشكلة الرئيسية هي أننا بحاجة إلى ملاحقة البينة التحتية والأشياء النظامية الكلمة التي يتوفر الدعم لها.

وثمة مثال رائع ألا وهو خوارزميات استخراج النطاقات وشبكات بوت نت. أعنى، أود إلقاء نظرة على سبيل المثال، على فيروس كونفيكر، اتفقنا؟ وهو موجود منذ أكثر من عقد وما يزال مستمرًا، أو أفالانش. وما تزال هناك حاجة لبذل المزيد من الجهود من

أجل محاربة هذه الأنواع من انتهاك نظام أسماء النطاقات DNS لأن المشكلة الأساسية المتمثلة في عدم إجراء تصحيح لمشكلات أجهزة المضيف وعدم تصحيح الأنظمة الأساسية هي صلب المشكلة الموجودة حاليًا، اتفقنا؟

ومن ثم أعتقد أن هناك فرصة أمام الجزء الأخير من سؤالك المطروح، أل جي، حول ما يمكن القيام به في قوائم حظر المواقع المشبوهة من منظور الأطراف المتعاقدة أكثر هو أنني أعتقد أن قوائم حظر المواقع المشبوهة في مكانها الصحيح في حقيقة الأمر من حيث المنظومة اعتمادًا على مساحتها الفريدة في المراقبة حيث يمكنها الحصول على بيانات قياس عن بعد للمساعدة في الوقوف على مدى فاعلية معدل الفاعلية في تفكيك هذه المنصات الأساسية التي توفر دعمًا نظاميًا لانتهاك النطاقات.

وأتمنى أن نتمكن من العمل والتعاون مع مجتمع ICANN من أجل الدفع في ذلك الاتجاه. شكرًا.

أل جي فورسبيرغ: شكرًا لك، ماثيو.

ريغ، هل لديك أي إضافة؟

ريغ ليفي: أجل. أنا أتفق مع صياغة مات لماهية كلمة "المزيد" في هذه الظروف.

ونحن نعمل باستمرار مع مختلف موفري قوائم الحظر من أجل الوقوف على ما إن كان بالإمكان استخدام خدماتهم أم لا وذلك بسبب الحد من النتائج الإيجابية الخاطئة بالإضافة إلى الإزالة بعد عملية الإصلاح من جانبنا لأنه وكما أن البعض من -- قدرًا من الملاحظات التي تمت الإشارة إليها مسبقًا، هناك عدد من النتائج الإيجابية الخاطئة ويجب علينا أن نفهم ما هو المستوى المقبول لدينا فيما يخص معاقبة أصحاب النطاق البرآء في محاولة للوصول إلى جميع أصحاب النطاقات المذنبين. أعتقد أن كلا هذين الأمرين مهمين.

أل جي فورسبيرغ: شكرًا لك، ريغ.

سوف أنتقل الآن إلى جوانا، ممثلتنا في مجموعة المستخدمين النهائيين في المجتمع الشامل. وأود أن أسألك: بأي طريقة تعتقدين أنه يمكن لموفري قوائم حظر المواقع المشبوهة تقديم مساعدة أكثر لأي مستخدم نهائي تم إدراجه أو لديه مشكلة في إحدى قوائم حظر المواقع المشبوهة؟

جوانا كوليزا: شكرًا لك، أل جي. أنا أفهم أن هناك قيود من حيث الوقت، لكن أسمحوا لي أن أثري هذه المناقشة الذاخرة سريعًا تلك التي نجريها إلى الآن.

أنا جوانا كوليزا لأغراض تسجيل وتدوين النص ولأغراض الترجمة.

وفي حقيقة الأمر، هذا هو السؤال الرئيسي الذي يحاول مجتمع عموم المستخدمين الإجابة عنه: كيف تؤثر قوائم حظر المواقع المشبوهة مباشرة على موقف ووضع المستخدمين النهائيين؟ أين يجب أن يلجأوا، هل يجب أن يكون اسم نطاقهم غير متقن -- أو تصنيفه بشكل غير صحيح بأنه ضار؟ فهذه تمثل بالنسبة لنا مشكلة من حيث إيصال الرسال من هذه الجلسة إلى المجتمع الأوسع لكنها أيضًا تمثل مشكلة للمستخدمين النهائيين ووضع المعايير من أجل قوائم حظر المواقع المشبوهة.

ونحن نرحب بفرصة المشاركة في المناقشات الجارية في دار الأطراف المتعاقدة وفي اللجنة الاستشارية الحكومية GAC، وفقًا لما أحاول قوله بإيجاز في مربع الدردشة.
وفي المعتاد وعادة ما يلجأ المستخدمون النهائيون إلى موفري الخدمات المحليين المتعاملين معهم أو إلى جهات إنفاذ القانون من أجل محاولة حماية نطاقهم، أو اسم نطاقهم أو علامتهم التجارية أو مواردهم أو الخدمات التي يحاولون تقديمها. ولكن قد يتبين أن هذه الطرق غير فعالة لأنه إذا كان من المفترض بمستخدم نهائي أن يسير على درب قوائم حظر المواقع المشبوهة، فسوف ينتهي به المآل إلى هذه الهيئة القائمة النوعية.

إذن فهذه المشكلة ذات وجهين. حيث نرغب من جانب أن نحصل على إجابة نوعية لمستخدمينا النهائيين حول الطريقة التي يمكنهم من خلالها إلغاء إدراج أي موقع ويب تم إدراجه لأسباب خاطئة، وتم إدراجه على نحو غير ملائم بسبب عدم وجود أي نشاط ضار تم استخراجه فيه.

ولذلك فإن مناقشة الإدراج التلقائي واليدوي في قوائم الحظر يمثل بالنسبة لنا عنصرًا لكل من بناء القدرات بين المستخدمين النهائيين ولكن أيضًا للتأكد من أن المعايير الخاصة بالإدراج في قوائم الحظر يعكس احتياجاتهم وتوقعاتهم. وفي حين يبدو كما لو كنا في هذه النقطة، وفقًا لما ذكره بيتر في مربع الأسئلة والأجوبة، ثمة قضية كبرى تتعلق بالحوكمة ومساءلة قوائم حظر المواقع المشبوهة.

وكما يمكننا أن نرى من خلال هذه المناقشة الجارية اليوم هنا، يجري وضع العديد من المعايير في الحسبان. وهناك مناقشة ما بين من يقدمون قوائم حظر المواقع المشبوهة؛ ولكن بالنسبة لنا، أن نعلم كيف تعمل هذه المنظومة الكاملة، فإننا نريد تحقيق قواسم مشتركة أو فرص مثل هذه من أجل تحقيق فهم أفضل لكيفية عمل النظام وأن تكون لنا القدرة على المشاركة في تطويره.

وفي الواقع، فإن المعايير التي سيتم استخدامها من أجل إدراج بعض مواقع الويب على قائمة الحظر لهي مناقشة تُجرى داخل مجتمع ICANN حيث يجب الاستماع إلى صوت المجتمع الشامل.

لقد سمعنا بشأن البريد غير المرغوب. وقد نظم مجتمع عموم المستخدمين ندوات ويب وجلسات ومناقشات داخلية للسياسات من أجل تحديد وتعريف فئات انتهاك نظام أسماء النطاقات DNS في محاولة لتحديدها وتعريفها. وقد أثبت البريد غير المرغوب أنه أحد أكثر الموضوعات خلافًا، لأنه قانوني في بعض المناطق وغير قانوني في أخرى.

إذن فإن النظر إلى قوائم حظر المواقع المشبوهة، بالنسبة لنا، يمثل عنصرًا أساسيًا وهو المعايير التي يتم ضبط هذه القوائم وفقًا لها. ونحن نرحب بالفرصة المتاحة للمشاركة في هذه المناقشات بالإضافة إلى جلسة يوم الإثنين الجامعة حول التطورات النظامية، والتي سيكون لها على الأرجح تأثير على طريقة عمل السجلات وأمناء السجلات في مختلف المناطق ذات الاختصاص القضائي.

سأتوقف هنا. أنا أعلم أن الوقت قارب على النفاد، أل جي، لكنني أرى أن هذه مناقشة يمكن ترحيلها لوقت لاحق.

شكرًا.

أل جي فورسبيرغ: شكرًا لكِ، جوانا. أود أن أعلق على هذا الأمر بطرح سؤال على موفري قوائم حظر المواقع المشبوهة والذي يرتبط ارتباطًا مباشرًا بالكلمة التي ألقتها جوانا.

هل تقترح بأن يقوم المستخدمون النهائيون الذين تم إدراجهم في قائمة حظر مواقع مشبوهة بالبدء في حل هذه المشكلة؟ كاريل.

كاريل بيتر: بالطبع، نعم. أنا لا أعرف ما الذي يفعله الآخرون. ولكن يمكنني إخباركم بما نفعله نحن. لدينا موقع على الويب يمكنكم فيه البحث عما إن -- بما أننا نتحدث حول النطاقات، هل النطاق الخاص بكم جزء من مجموعات بياناتنا أم لا. فإن كان كذلك، فيمكنكم في غالبية الحالات التقدم بطلب لإزالته مباشرة، وهو ما سيتم التعامل معه مباشرة، وسوف يكون النطاق خارج مجموعات بيانات على الفور أو نحو من ذلك. فنحن نقوم ببناء مجموعات البيانات كل دقيقة.

وفي بعض الحالات، سوف يتم إجبارك على إنشاء طلب حل مشكلة فنية بسبب بعض المؤشرات التي نقوم بجمعها. ولدينا أشخاص يعملون على مدار الساعة من أجل معالجة طلبات حل المشكلات الفنية وسوف يساعدونك في فهم طبيعة المشكلة، وما نرى أنه يجب القيام به من أجل تنفيذ عملية الإخراج من القائمة، وسوف يكون شخص بمراجعة القائمة وبعد ذلك سيقوم إما بمساعدتك على فهم ما يجري أو يلغي إدراج النطاق في القائمة.

أل جي فورسبيرغ: شكرًا لك، كاريل. بين، هل ترى أن هذا الأمر مختلف اختلافًا كبيرًا في حالتك؟

بين كون: هذا ممتع. في حالتنا والتي تُستخدم فيها قائمتنا بالأساس في قطاعات على مدار 24 بسبب التصيّد سوف ينقطع اتصالها بالإنترنت، لكننا في الأغلب نقوم بنفس الشيء الذي كان يقوله كاريل، حيث سنقوم -- في حالة قيام أي شخص بالإبلاغ عن وجود نتائج إيجابية خاطئة لنا أو قيام شخص بالإبلاغ عن شيء خارج المعتاد، فإننا نلقي نظرة فاحصة عليه، ليس فقط حول ما يجري في أتمتة ما يتم التقاطه وحسب ولكن أيضًا فيما يجري على وجه التحديد في هذا الأمر.

وكما تعلمون، عندما نقوم بالإبلاغ عن شيء لأمناء السجلات أو لموفري الاستضافة ويقوموا -- فإنهم يماطلون في الأمر، كما تعلمون، ونحن نتناول هذا الأمر على محمل الجد، وننظر بشكل مباشر جدًا في الأمر للتأكد من أن ما نعرضه حقًا هو تصيد أو أنه ضار فعليًا. وإذا لم يكن كذلك، فإننا نقوم بإزالته على الفور. وكما تعلمون، وكانت كان كاريل يقول، يتم ذلك في غضون دقائق.

أل جي فورسبيرغ: شكرًا لك، بين. من الواضح من خلال المناقشة هنا اليوم أنه لا توجد موجزات عامة -- دائرة التعقيبات المعمول بها للإبلاغ عن إشارة أو دليل على وجود انتهاك عند حله أو وجود نتائج إيجابية خاطئة.

رومان، هل تعتقد أنك ستكون على استعداد للعمل على طريقة معيارية في تلقي المعلومات مثل هذه من بين مجموعة كبيرة من الموارد؟ وما الذي يمكنك -- ما الذي يجب -- وكيف يجب أن يتم تسهيل الأمر لك لكي يحظى بثقتك؟

رومان هويسي: أعتقد أن هذه مناقشة شيقة. وبالطبع ليست لدي إجابة مباشرة على ذلك، لكنني أعتقد أن أفضل الطرق في -- أفضل طرق تسهيل ذلك أن نقوم باستحداث ثقة المجتمع في الحصول على شيء مثل هذا. فهذا بالتأكيد من الأشياء التي يمكن العمل عليها. والسؤال الذي يطرح نفسه هو من يمكن أن يكون مظلة لهذا -- لمثل هذا الشيء، سواء كان هذا أحد موضوعات ICANN أو شيء يجب حله من خلال العاملين في هذا المجال.

أل جي فورسبيرغ: شكرًا لك، رومان.

جوانا، أود الرجوع إليك وأن أطرح سؤالاً. هذا غير موجه بصورة غير مباشرة لقوائم حظر المواقع المشبوهة، ولكن ما هي الأنظمة الاحتياطية التي تعتقدين أنها لازمة من أجل ضمان أن السجلات وأمناء السجلات لا يتصرفون بما يتجاوز اختصاصهم عندما يتطرق الأمر إلى تعطيل أسماء النطاقات التي تمت الإشارة إلى أنها تشارك في انتهاك نظام أسماء النطاقات DNS؟

جوانا كوليزا: انا أؤيد ما قاله مات. معكم جوانا مرة أخرى من أجل التسجيل الكتابي. الأمر برمته يتعلق بالشفافية. فكلما زاد مستوى شفافية المعايير ومستوى انفتاح موفري قوائم حظر المواقع المشبوهة أمام المناقشات حول المعايير التي يجري تطبيقها، كان من السهل لأي مستخدم نهائي عادي أن يفهم العملية وأن يعبر عن رأيه ويُنظر فيه.

وأنا أؤمن بشدة أن هذا هو المجال الذي يمكن للمجتمع الشامل أن يساعد فيه من أجل تحديد ما هي هذه التوقعات. ويمكن أن تكون الإجابة إقليمية. وقد ناقشنا ذلك في جلسة يوم الإثنين أيضًا. علمًا بأن المجتمع الشامل يعمل على حملة لبناء القدرات فيما يخص انتهاك نظام أسماء النطاقات DNS وسوف يتم إطلاقها على المستوى الإقليمي. وفي حقيقة الأمر يمكن أن تكون هذه الردود إقليمية بالنيابة عن المستخدمين النهائيين. ويمكن أن تكون التوقعات مختلفة في مختلف المنظمات العامة الإقليمية (RALO) وفي مختلف الدول. وقد رأينا ما هي عليه في أوروبا خلال جلسة يوم الإثنين.

ولكن ما أفهمه أن هذا الأمر يمكن أن يعود بالنفع بإجراء مزيد من التطوير لنموذج أصحاب المصلحة المتعددين.

ومن ثم بالنسبة لنا لكي نكون قادرين على المشاركة في هذه الجلسة بشكل أفضل، كما أكد مات، والشفافية حول هذه العمليات، وفهم الطريقة التي تعمل بها ووفقًا لما قام به مجتمع ICANN دائمًا، العمل بحسن النية هو من الأشياء التي أعتقد أنها سوف تساعدنا على المضي قدمًا لتطوير قوائم حظر المواقع المشبوهة بفاعلية. شكرًا.

أل جي فورسبيرغ: شكرًا لكِ، جوانا.

سوف أتناول الآن سؤالاً من الجماهير للقسم التالي. وهو قادم من فولكير غرينمان، وهو يسأل: لماذا لا توفر العديد من قوائم حظر المواقع المشبوهة أي دليل في التقارير؟ فبدون

الأدلة أو الإشارات النوعية التي تتيح إمكانية التحقق من التقرير والبلاغ، فهذا يجعل اتخاذ إجراء أمرًا صعبًا بشكل متزايد.

وسوف نحيل هذا السؤال إلى كاريل.

كاريل بيتر: بالطبع، نعم. ولذلك دعونا نتحدث حول جانب البريد غير المرغوب في هذا الأمر. فهذا ما أنا ملمّ به على الأكثر.

ونحن نحصل على تقارير البريد غير المرغوب من المؤسسات ذات موفري خدمة الإنترنت الكبرى حيث يقومون بمشاركة بعض خصائص البريد غير المرغوب التي يحصلون عليه معنا أو من مصائد البريد غير المرغوب أو نت هوني بوت (مصائد مخترقي الشبكات) إن جاز القول.

وقد أتقن مرسلو الرسائل النصية والبريدية غير المرغوب فيها تضمين جميع أنواع تفاصيل التعقب البسيطة في روابط URL وفي النطاقات وفي الصور وفي رسائل البريد الإلكتروني الكاملة. كما أن معدل حصولنا على هذه الأشياء يجعل من المستحيل بشكل أساسي بالنسبة لنا التأكد من أننا نخرج كل شيء من ذلك المكان ونتأكد من أن أي دليل نقدمه تم إخلاؤه من أي شيء يحدد مصائد مخترقي الشبكات الخاصة بنا. ومن ثم في هذه المرحلة يصبح اتخاذ القرار هو أنك إذا لم تستطع مشاركة ذلك دون حماية مصادرك، فلا يمكنك المشاركة.

وكما قلت لكم، في أي من الحالات الفردية، دائمًا ما نكون على استعداد للعمل مع إعطاء الناس الدليل الذي يحتاجونه، وما إن كان بإمكاننا مشاركته. ولكن من الناحية التلقائية، فإن هذا الأمر من الأشياء التي يسهل القيام بها.

ولإعطائكم فكرة عن الأمر، فإن مجموعة واحدة من مصائد مخترقي الشبكات التي ندير ها تتلقى ما بين 2 من البريد الإلكتروني وعدد 3,000 بريد إلكتروني لكل ثانية. وليس ثمة طريقة يمكننا بها استعراض ومراجعة كل ذلك للتأكد من أن جميع المعرّفات الموجودة وللتأكد من أن البيانات التي نوفرها من شأنها -- سوف تكون خالية بحيث لا تحدد هوية المصادر.

وكما قلت لكم، إذا كان من -- إذا كان من يقومون بأعمال التصحيح بحاجة لدليل نوعي، فإن من يحصلون على بياناتنا لذلك الغرض سوف يعلمون أين يتصلون بنا، ويمكنهم الحصول على تفاصيل إضافة متى ما كان -- متى ما أمكن ذلك.

أل جي فورسبيرغ: شكرًا لك، كاريل. وللأسف، هذا هو ختام جلستنا اليوم حين نفد الوقت منا.

وبالنظر إلى الإجابات على أسئلة الاقتراع من هذه الجلسة السابقة، يمكنني القول بأننا حصلنا على جمهور عريض نسبيًا. وهناك من لم يسمع بالكثير من الأنواع المختلفة للانتهاك وهناك بالتأكيد من سمع بها. وهناك أشخاص لم يضطروا إلى التعامل مع مسألة الحد من الانتهاك وهناك من اضطروا إلى ذلك.

أتمنى أن يكون البعض منا قد تعلم قليلاً من خلال مناقشة اليوم ويمكنه المضي قدمًا في عمله من هلال هذا الموضوع الخاص.

وأود أن أتوجه بالشكر لجميع أعضاء اللجنة على ما بذلوه من وقت ومشاركة وإلى فريق عمل ICANN على دعمهم الذي لا يقدر بثمن، وأخيرًا وليس آخرًا، إلى الجمهور الذي خصص وقتًا من يومه خلال أسبوع الاجتماع المكتظ هذا من أجل الجلوس والاستماع إلينا.

إن فهم قوائم حظر المواقع المشبوهة والوظيفة التي تؤديها والغرض منها وكيفية البدء في استخدامها أو التواصل معها من أجل تصحيح خطأ ما يعد خطوة هامة للغاية في تطوير طرق العمل والتعامل معها وضد انتهاك نظام أسماء النطاقات DNS.

وما يزال الطريق أمامنا طويل في هذا الصدد، لكنني أعتقد على المستوى الشخصي أننا حققنا انطلاقة قوية اليوم.

مرة أخرى، شكرًا جزيلاً لكم جميعًا على المشاركة.

بريندا بريور: ومعنا بالفعل سؤال أخير فيما يخص الاقتراع. وسوف نفتح باب الإجابة عن سؤال الاقتراع هذا على الفور. رجاءً كونوا على استعداد.

وسوف يتم عرض سؤال الاقتراع على شاشتكم. هل تعلمون كيفية الإبلاغ عن تهديد أمني أو تتخذون إجراءات أخرى من أجل الحد من تلك التهديدات؟ برجاء الإجابة بنعم أو لا.

مرة أخرى، السؤال المعروض على شاشتكم هو: هل تعلمون كيفية الإبلاغ عن تهديد أمني أو تتخذون إجراءات أخرى من أجل الحد من تلك التهديدات؟ رجاء الرد بنعم أو لا.

شكرًا. وسوف نقوم بإغلاق باب الاقتراع ونطلعكم على النتائج.

شكرًا جزيلاً على مشاركتكم اليوم. انتهى هذا الاجتماع الآن.

شكرًا لكم جميعًا.

بريندا بريور: يمكنك إيقاف التسجيل.

شكرًا لكم جميعًا.

[نهاية التدوين النصي]